802.11 Secrets Revealed – Part 1
RF Signal Propagation

June 15, 2010

Joe Bardwell
President / Chief Scientist - Connect802 Corporation
www.Connect802.com - joe@Connect802.com

SHARKFEST **'10**
Stanford University
June 14-17, 2010

Connect802

CACE TECHNOLOGIES

SHARKFEST '10 | Stanford University | June 14–17, 2010

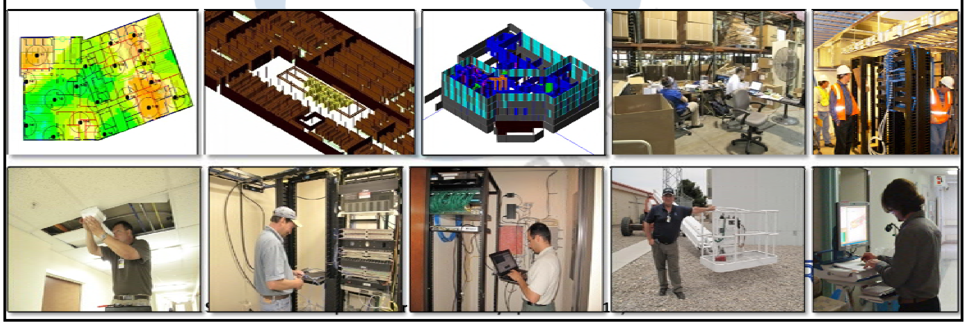
WIRESHARK UNIVERSITY

About Connect802 Corporation

- Founded in 1994 with headquarters in the San Francisco Bay area and East Coast engineering out of Knoxville, Tennessee
- Providing nationwide Wi-Fi, WiMAX, cellular and other wireless solutions
- Applying 3-dimensional RF CAD modeling and simulation to the design process
- Equipment sales, installation and support

Connect802 Wireless Data Solutions

www.Connect802.com



Your Wireshark Support Resource...

- Connect802 is your authorized AirPcap reseller
- Specialty Dual-Band (2.4 + 5 GHz) antennas for your AirPcap dual-band adapter
- 10/100 and GigE In-Line Port-Mirror Capture Switches with PoE Passthrough

AirPcap

Check out the Connect802 Wireshark enhancement products at:

www.Connect802.com/wireshark

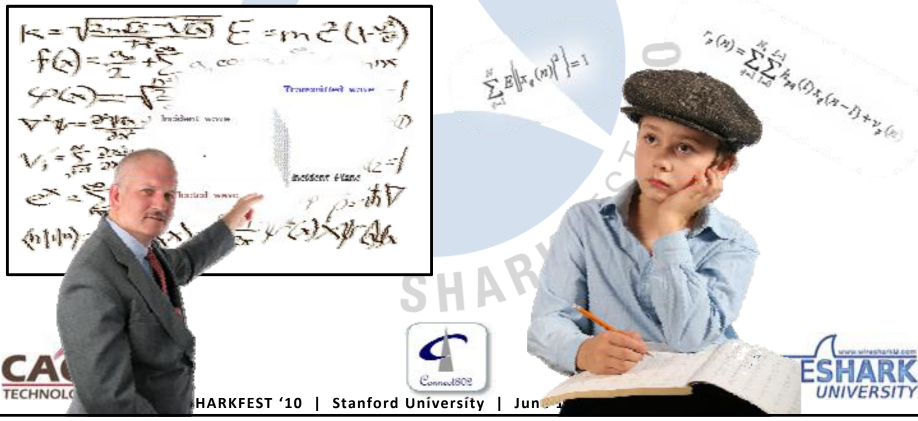
CACE TECHNOLOGIES

SHARKFEST '10 | Stanford University | June 14–17, 2010

WIRESHARK UNIVERSITY

The Math Won't Be On the Final Exam…

- RF engineering involves electromagnetic waves which are most accurately described mathematically
- You're going to see some "math" flash past you for perspective – BE NOT AFRAID!



The Radiotap Header

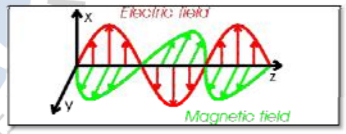
```
⊟ Radiotap Header v0, Length 24
    Header revision: 0
    Header pad: 0
    Header length: 24
  ⊞ Present flags: 0x000058ce
  ⊞ Flags: 0x10
    Data Rate: 1.0 Mb/s
    Channel frequency: 2447 [BG 8]
  ⊞ Channel type: 802.11b (0x00a0)
    SSI Signal: -84 dBm
    SSI Noise: -100 dBm
    Signal Quality: 35
    Antenna: 0
    SSI Signal: 16 dB
    802.11 FCS: 0xf3e1d41f [correct]
```

802.11a	802.11b	802.11g
-86 dBm @ 6 Mb/s	-90 dBm @ 1 Mb/s	-87 dBm @ 6 Mb/s
-85 dBm @ 9 Mb/s	-89 dBm @ 2 Mb/s	-86 dBm @ 9 Mb/s
-82 dBm @ 12 Mb/s	-87 dBm @ 5.5 Mb/s	-83 dBm @ 12 Mb/s
-81 dBm @ 18 Mb/s	-85 dBm @ 11 Mb/s	-82 dBm @ 18 Mb/s
-80 dBm @ 24 Mb/s		-81 dBm @ 24 Mb/s
-78 dBm @ 36 Mb/s		-80 dBm @ 36 Mb/s
-74 dBm @ 48 Mb/s		-75 dBm @ 48 Mb/s
-73 dBm @ 54 Mb/s		-74 dBm @ 54 Mb/s

5-GHz 802.11n (HT20)	5-GHz 802.11n (HT40)	2.4-GHz 802.11n (HT20)	2.4-GHz 802.11n (HT40)
-85 dBm @ MCS0	-85 dBm @ MCS0	-86 dBm @ MCS0	-86 dBm @ MCS0
-84 dBm @ MCS1	-84 dBm @ MCS1	-86 dBm @ MCS1	-86 dBm @ MCS1
-83 dBm @ MCS2	-83 dBm @ MCS2	-84 dBm @ MCS2	-84 dBm @ MCS2
-82 dBm @ MCS3	-79 dBm @ MCS3	-83 dBm @ MCS3	-80 dBm @ MCS3
-79 dBm @ MCS4	-76 dBm @ MCS4	-80 dBm @ MCS4	-77 dBm @ MCS4
-74 dBm @ MCS5	-71 dBm @ MCS5	-76 dBm @ MCS5	-72 dBm @ MCS5
-73 dBm @ MCS6	-70 dBm @ MCS6	-74 dBm @ MCS6	-71 dBm @ MCS6
-72 dBm @ MCS7	-69 dBm @ MCS7	-73 dBm @ MCS7	-70 dBm @ MCS7
-86 dBm @ MCS8	-86 dBm @ MCS8	-86 dBm @ MCS8	-86 dBm @ MCS8
-84 dBm @ MCS9	-84 dBm @ MCS9	-86 dBm @ MCS9	-86 dBm @ MCS9
-83 dBm @ MCS10	-83 dBm @ MCS10	-84 dBm @ MCS10	-84 dBm @ MCS10
-82 dBm @ MCS11	-79 dBm @ MCS11	-83 dBm @ MCS11	-80 dBm @ MCS11
-79 dBm @ MCS12	-76 dBm @ MCS12	-80 dBm @ MCS12	-77 dBm @ MCS12
-74 dBm @ MCS13	-71 dBm @ MCS13	-75 dBm @ MCS13	-72 dBm @ MCS13
-73 dBm @ MCS14	-70 dBm @ MCS14	-74 dBm @ MCS14	-71 dBm @ MCS14
-72 dBm @ MCS15	-69 dBm @ MCS15	-73 dBm @ MCS15	-70 dBm @ MCS15

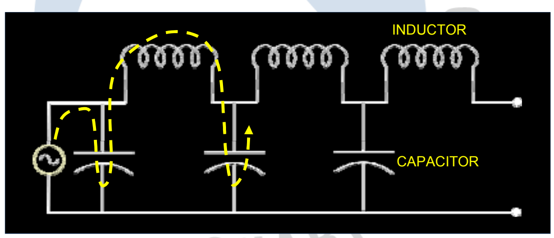
What Is an RF "Signal"?

- An oscillator circuit creates an electrical differential that alternates in a regular pattern
  - A sine wave carrier
- The alternating pattern is modified to represent bits
  - Modulation
- The modulated carrier is impressed on an antenna
  - The energy propagates outwards from the antenna
- The energy is present in an electrical and a magnetic component
  - Electrical → Magnetic → Electrical → Magnetic → …
- The propagating energy field is the "RF signal"
  - The electromagnetic field continues to propagate forever



Capacitance and Inductance

- Rising current creates a magnetic field around an inductor
  - The field collapses and releases its stored energy when the current falls
- Rising voltage causes current to be stored in a capacitor
  - The current is discharged and releases its stored energy as the voltage falls

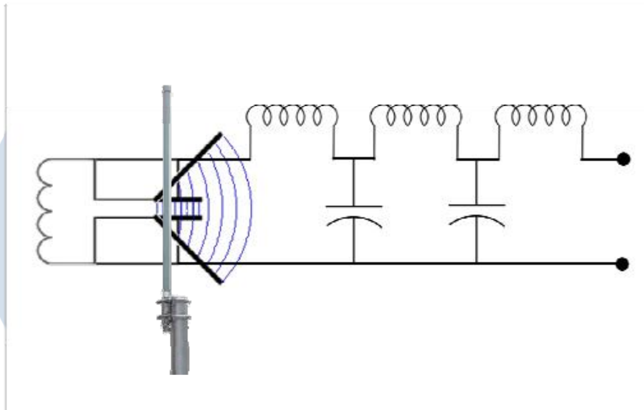


Electromagnetic waves propagate in free space as an continuous exchange between electric and magnetic fields

SHARKFEST '10 | Stanford University | June 14–17, 2010

Antenna Inductance and Capacitance

- Inductance is measured in Henrys (H)
- Capacitance is measured in Farads (F)
- Propagation is impeded by these effects



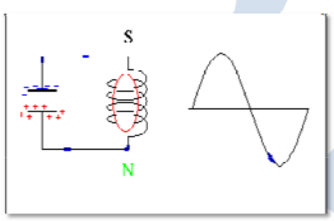
The antenna is an inductive / capacitive element in the end-to-end transmission circuit

SHARKFEST '10 | Stanford University | June 14–17, 2010

Impedance of Free Space

Wavelength Disappears !

- Permeability of free space: μ_0 is 1.257 X 10^{-6} H/m
- Permittivity of free space: ε_0 is 8.85 X 10^{-12} F/m
- Impedance of free space: $Z_0 = (\mu_0 / \varepsilon_0)^{1/2} = 377\Omega$
- Z_0 in moist air is slightly reduced



$$I = \frac{E}{R} \qquad I = \frac{V}{Z} \qquad P = I \times V$$

I = Amps
V = Voltage (RMS)
Z = Impedance

P = Watts

$$I \times Z = V$$

$$P = I^2 \times Z$$

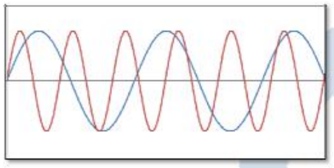
Free Space Impedance Is Independent of Distance
Power Is Independent of Wavelength
Power Varies As the Square Of the Current

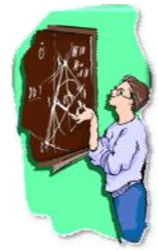
[RMS (DC equivalent): Square all +/- points on the waveform, take the root of the average]

SHARKFEST '10 | Stanford University | June 14–17, 2010

Frequency, Wavelength and Antenna Tuning

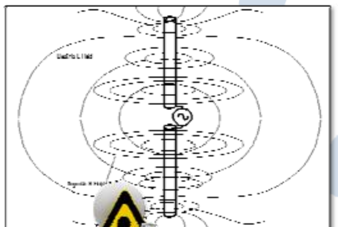
$$\text{Wavelength } (\lambda) = \frac{c}{f} = \frac{30000 \times 10^6}{\text{<MHz>} \times 10^6}$$





2.4 GHz = 12.5 cm = 5”
5 GHz = 6 cm = 2.5”

12.5 * 0.3937 = 4.91   6 * 0.3937 = 2.36

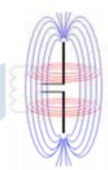


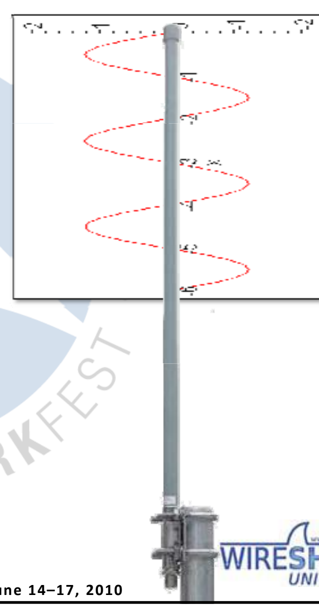
- Two quarter wavelength conductors or elements results in a standing wave on an element of λ/4 and yields the greatest voltage differential between the ends of the two elements.
  - One end is at the crest of the wave while the other end is at the trough

The physical construction of an antenna is based on the intended transmit/receive frequency

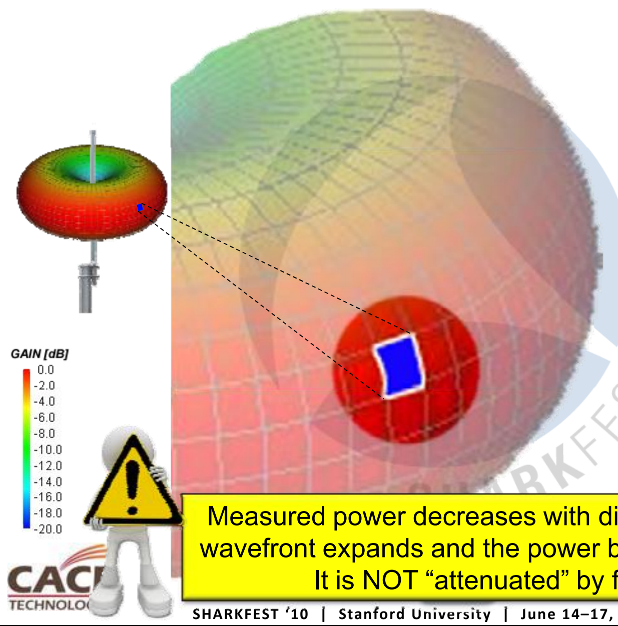
“Standing Wave” In a Tuned Antenna

- The length of an antenna element is determined by the wavelength of the signal to be transmitted
- The signal is reflected from the end of the antenna element and creates a “standing wave” that propagates its energy outward from the antenna.





The "Inverse Square Law"



Area = $4\pi r^2$

Radius	Area	Factor
1	12.57	1.0
2	50.26	4
4	201.06	16
8	804.24	64
16	3216.99	256

Power At the Receiving Antenna Resulting From Geometric Expansion

$$S = P_t \frac{1}{4\pi r^2}$$

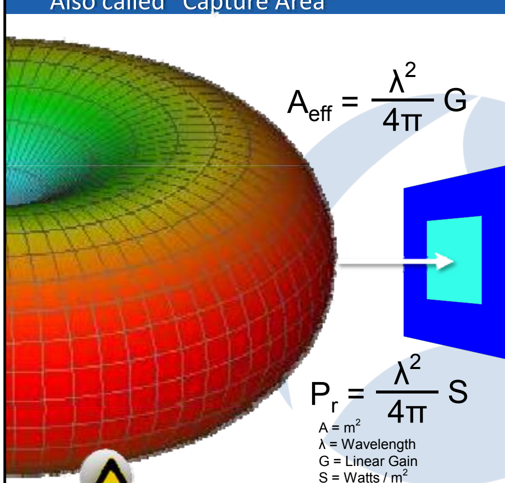
S = Watts / m^2
P = Power at Antenna
r = Radius (m)

Measured power decreases with distance because the wavefront expands and the power becomes less dense. It is NOT "attenuated" by free space.

SHARKFEST '10 | Stanford University | June 14–17, 2010

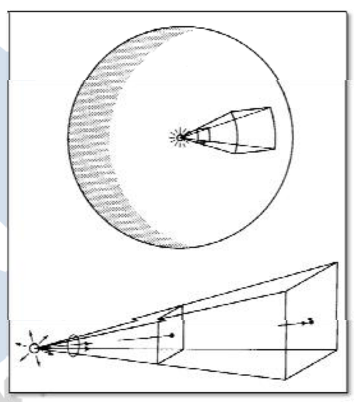
Effective Antenna Area (Aperture)

Also called "Capture Area"



$$A_{eff} = \frac{\lambda^2}{4\pi} G$$

"The solid angle subtended by the transmit beam at the receiver"



$$P_r = \frac{\lambda^2}{4\pi} S$$

A = m^2
λ = Wavelength
G = Linear Gain
S = Watts / m^2
P = Power at Antenna

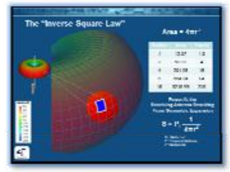
Short wavelengths make the receiver's effective aperture smaller so it captures a smaller amount of energy

2.4 GHz: λ = 5" 25/4π = 1.989 3dBi = $10^{0.3}$ = 1.995 1.989 x 1.995 = 3.96 in^2
5. GHz: λ = 2.5" 6.25/4π = 0.497 3dBi = $10^{0.3}$ = 1.995 0.497 x 1.995 = 0.99 in^2

The Two Factors In Path Calculations

- Transmit power increased by transmit antenna gain and reduced by geometric expansion

$$S = G_t P_t \frac{1}{4\pi r^2}$$

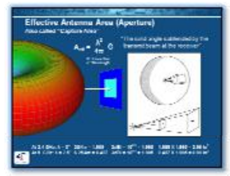


- The effective aperture of the receive antenna captures watts/cm^2 over its effective area resulting in gain

$$A_{eff} = \frac{\lambda^2}{4\pi} G$$

$$P_r = \frac{\lambda^2}{4\pi} S$$

A = m^2
G = Linear Gain
S = Watts / m^2
P = Power at Antenna



Geometric expansion of the wavefront and the size of the receiver's effective aperture are the primary factors that define the transmission path.

Combining Geometric Power Density Reduction With Effect Aperture Size

$$P_r = \frac{\lambda^2}{4\pi} S \Rightarrow P_r = \frac{S\lambda^2}{4\pi}$$

$$S = G_t P_t \frac{1}{4\pi r^2} \Rightarrow \frac{S}{G_t} = P_t \frac{1}{4\pi r^2} \Rightarrow P_t = \frac{S 4\pi r^2}{G_t}$$

$$\frac{P_r}{P_t} = \frac{\frac{S\lambda^2}{4\pi}}{\frac{S 4\pi r^2}{G_t}} = \frac{S\lambda^2}{4\pi} * \frac{G_t}{S 4\pi r^2} = G_t \left(\frac{\lambda}{4\pi r}\right)^2 \Rightarrow G_t G_r \frac{\lambda^2}{4\pi r}$$

Include possible transmitter gain

The two equations combine together:

$$\frac{P_r}{P_t} = G_t G_r \left(\frac{\lambda}{4\pi d}\right)^2$$

The Friis Transmission Equation

- The ratio of Receive to Transmit Power
  - Invert the factor to derive FSPL

$$\frac{P_r}{P_t} = G_t G_r \left(\frac{\lambda}{4\pi d}\right)^2 \rightarrow \left(\frac{4\pi d}{\lambda}\right)^2$$

$$\lambda = \frac{c}{f}$$

Use frequency instead of wavelength…

$$\left(\frac{4\pi df}{c}\right)^2$$

$$10 \times \log_{10}\left(\frac{4\pi df}{c}\right)^2$$

…and convert to a decibel representation.

$$20 \times \log_{10}\frac{4\pi df}{c}$$

$$20\log_{10}(d)+20\log_{10}(f)+20\log_{10}\left(\frac{4\pi}{c}\right)$$

P = Power at Antenna
G = Linear Gain
λ = Wavelength
d = Distance (i.e. "radius")
The inverse of the factor in parentheses is the FSPL

The standard FSPL formula incorporates both geometric expansion and receiver effective aperture:

$$FSPL(db) = 20\log_{10}(d)+20\log_{10}(f)+36.58$$

(Constant of Proportionality: d = MHz Statute Miles:36.58, km:32.45,

CACE TECHNOLOGIES — WIRESHARK UNIVERSITY

Calculating Free Space Path Loss

Friis Path Loss

Distance	2.4 GHz FSPL	5.8 GHz FSPL
10 Feet	49.75 dB	57.42 dB
50 Feet	63.73 dB	71.4 dB
100 Feet	69.75 dB	77.42 dB
200 Feet	75.77 dB	83.44 dB
500 Feet	83.73 dB	91.4 dB
1000 Feet	89.75 dB	97.42 dB

Additional Sources of Loss

Absorption
Reflection and Diffusion
Multipath Degradation

Additional Alterations to Propagation Characteristics

Refraction
Diffraction
Rician / Rayleigh Fading

CACE TECHNOLOGIES — WIRESHARK UNIVERSITY

SHARKFEST '10 | Stanford University | June 14–17, 2010

Absorption Of Signal Energy

- 2.4 GHz and 5 GHz Attenuation Is Almost the Same Through Most Obstructions
  - Most material differ by less than 1 dB
  - Exception include:
    - Red Brick: 10.1 dB
    - Glass: 1.2 dB
    - Fir Lumber: 3.3 dB
    - Cinder Block: 3.6 dB
    - Stucco: -1.6 dB !

Materials Tested

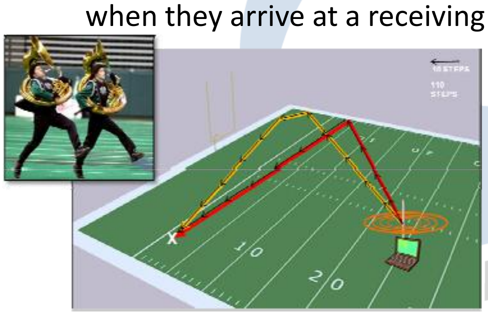
Metal slat blinds
Red Brick
Carpet
Ceiling Tile
Upholstery Fabric
Fiberglass
Glass
Drywall
Light Cover
Linoleum
Fir Lumber
Particle Board
Plywood
Ceramic Tile
Tar Paper
Cinder Block
Diamond Mesh
Stucco
Wire Lath

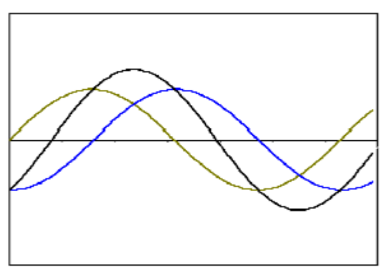
Portable Device Patch Antenna

Attenuation caused by interior walls and obstructions is less than 1 dB different at 5 GHz than at 2.4 GHz.
It's the tiny aperture of a mobile device that has the greatest impact on receiver capability.

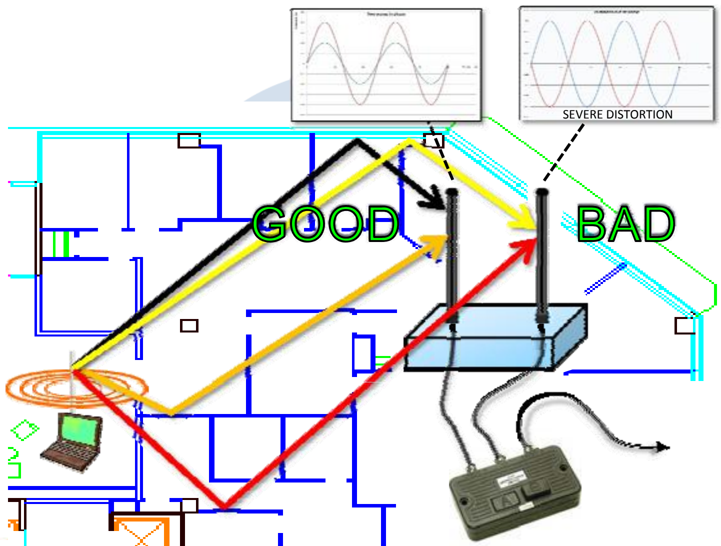
Reflection and Diffusion of Signal Energy

- When an electromagnetic wave meets an obstruction the energy that is not absorbed is either reflected or it passes through
  - Diffusion is the effect when the surface is uneven
- Reflection results in signal paths that are no longer in phase when they arrive at a receiving antenna

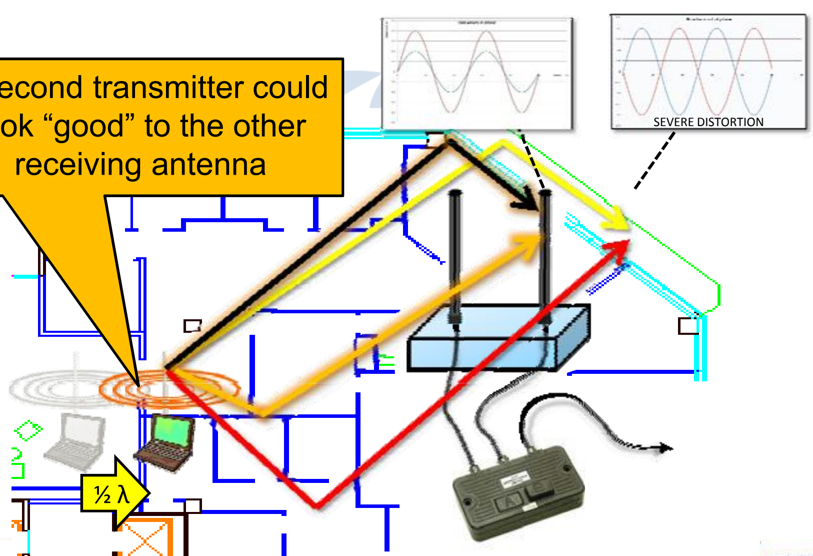




Multipath Degradation and Antenna Diversity

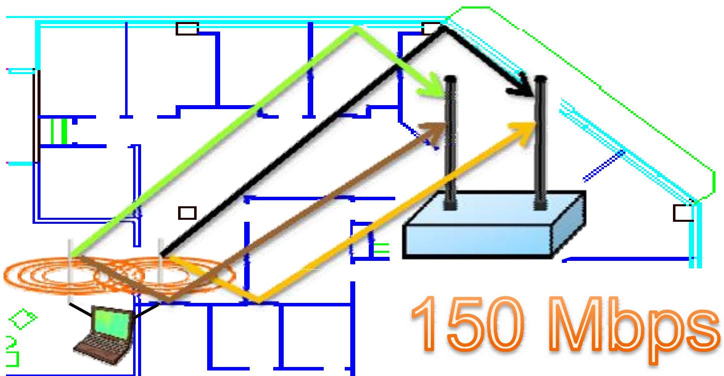


"Good" and "Bad" Are ½ Wavelength Apart



802.11n Multiple Input / Multiple Output (MIMO)

- Two transmitting antennas and two receiving antennas
- Multiple spatial streams

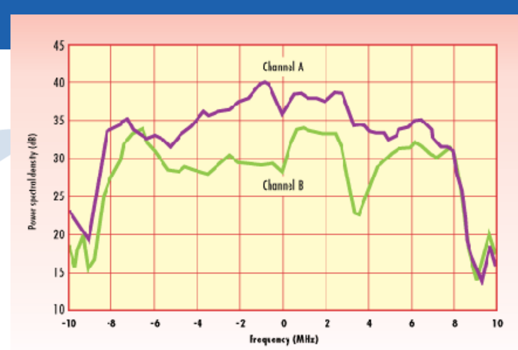


$$\psi(y;t+\epsilon)=\int_{-\infty}^{\infty}dx\;\psi(x;t)\int_{x(t)=x}^{x(t+\epsilon)=y} e^{\mathrm{i}\int_t^{t+\epsilon}(\dot{x}^2-V(x))dt}\,Dx(t)$$

The path integrals of the two streams are mathematically unique and identify the electromagnetic waves at the receiver

Antenna Diversity

- When two (or more) antennas received the signal the optimal antenna can be selected
  - Or, the received signals from all antennas can be algorithmically evaluated and optimized



Received signal power at two indoor antennas spaced ½ wavelength apart

Refraction

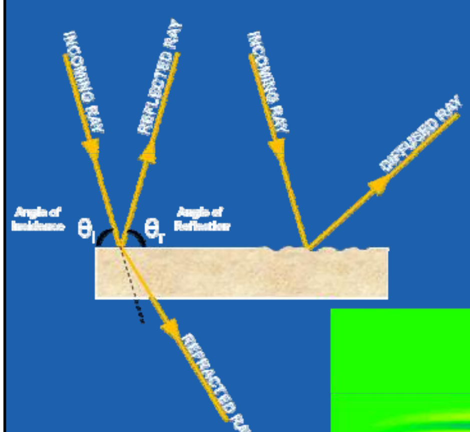
- Change in the direction of a wave as it passes into a medium of a different density
  - The refractive index of the medium changes because the speed of light changes
  - Wavelength changes but frequency remains the same

The refractive effects of interior glass partitions introduce factors that should be considered in a wireless network design

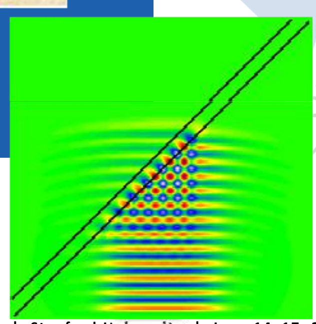
$$\frac{\sin\theta_1}{\sin\theta_2} = \frac{v_1}{v_2} = \frac{n_2}{n_1}$$

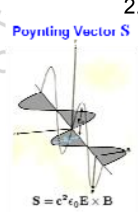
Snell's Law relates the wave velocities (v), the refractive indices (n) and the angles of incident and refracted waves (θ)

Diffusion, Reflection and Refraction



Less energy is reflected at 5 GHz as compared with 2.4 GHz

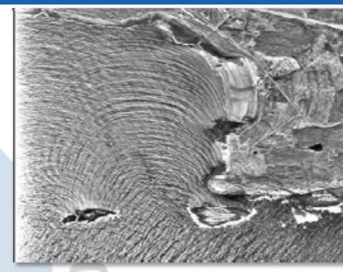


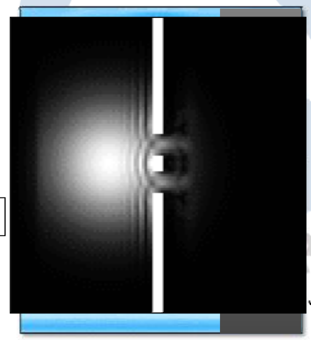


The direction in which energy is travelling at any instant is proportional to the cross product of the electric and magnetic fields, known as the Poynting vector.

Diffraction

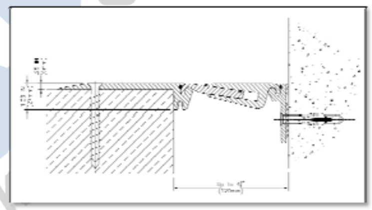
- The bending of waves around obstacles that are small, relative to the wavelength and the spreading out of waves passing through similarly small gaps and openings





$$I(\theta) = I_0 \operatorname{sinc}^2(d \sin\theta / \lambda)$$

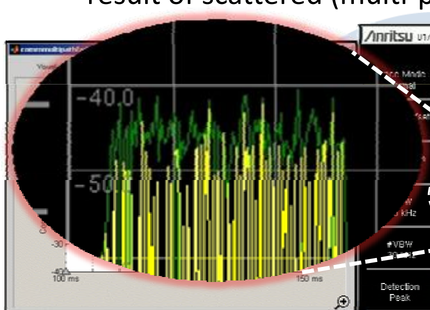
The Fraunhofer Diffraction formula to estimate the diffracted signal energy profile

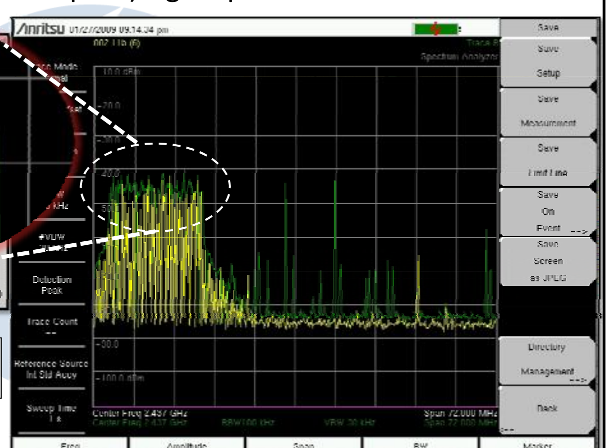


Signals Often Diffract Through Expansion Joints Where Poured Concrete Floors Meet Walls

Rician Fading

- A dominant signal component (direct ray) is degraded as a result of scattered (multi-path) signal power



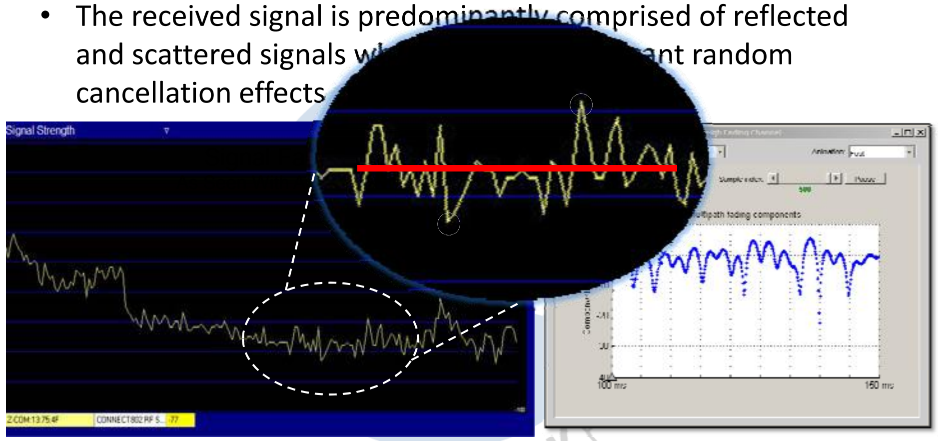


$$f_\rho(\rho) = (1+K)\, e^{-K} \frac{\rho}{\bar{p}} \exp\left(-\frac{1+K}{2\bar{p}}\rho^2\right) I_o\left(\sqrt{\frac{2K(1+K)}{\bar{p}}}\,\rho\right)$$

Power Density Model for Rician Fading
(K is the ratio of dominant / scattered)

Rayleigh Fading

- The received signal is predom... comprised of reflected and scattered signals w... ...nt random cancellation effects

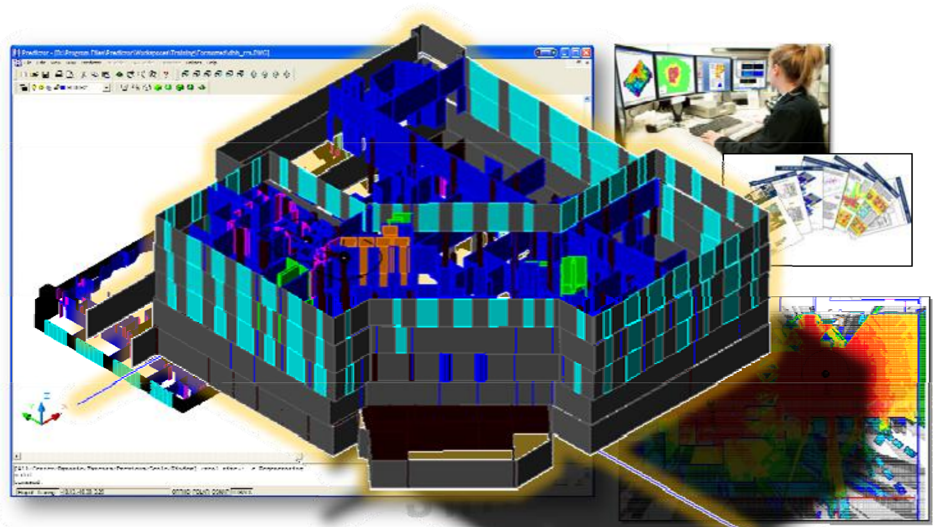


The measurements shown were taken in two locations. Signal strength drops from one location to the other. Channel fading can be seen throughout.

$$r(t)=\sum_{n=1}^{N} c_n \cos(2\pi f_c t+\psi+\phi_n+2\pi\Delta f_n t)$$

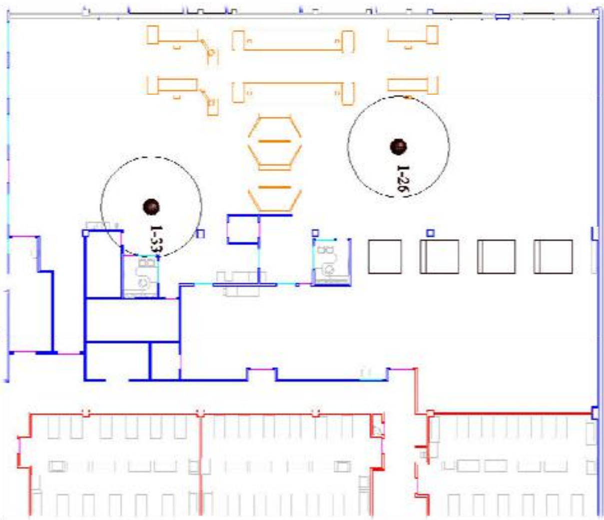
Power Density Model for Rayleigh Fading
(Power is the sum of combined waves)

3-Dimensional RF CAD Modeling and Simulation

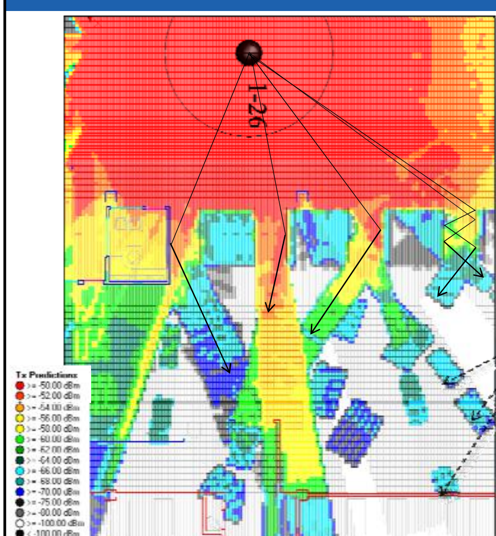


The software does the math,
the RF engineer creates the design

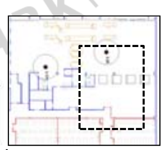
RF CAD Modeling and Simulation Of A Research and Manufacturing Facility



Signal Reflections Produce Subtle Interactions

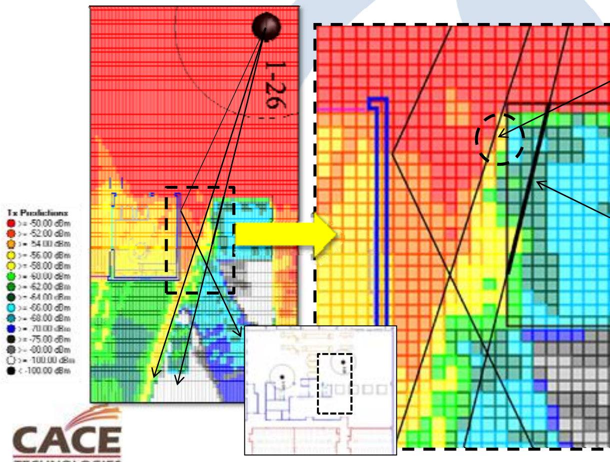


- Signal is reflected and provides non-line-of-sight coverage between the cold box rooms
- Unanticipated constructive interference between reflected rays produces zones of -68 dBm coverage in areas where general coverage falls to below -80 dBm



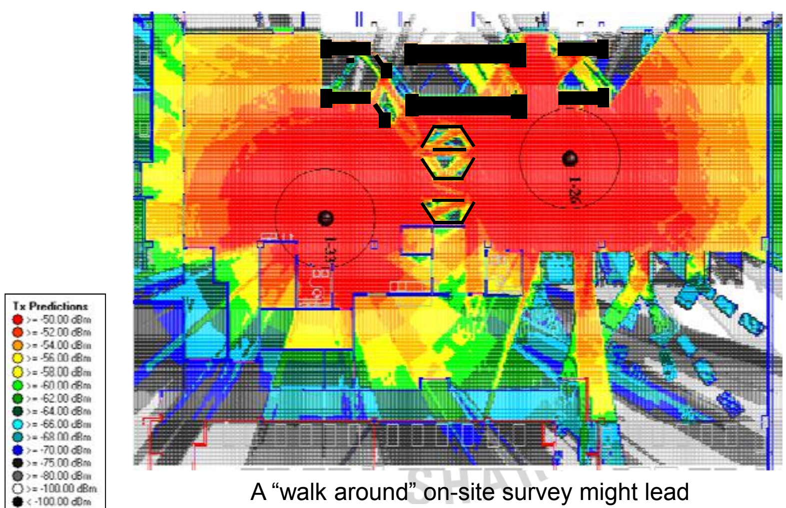
RF Waves Diffract Around Sharp Edges

Diffracted Energy Can "Fill In" Behind an Obstruction



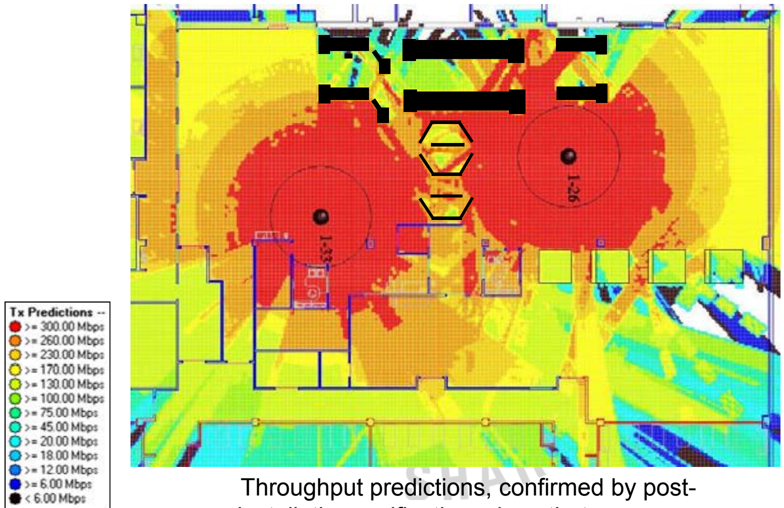
- Diffraction at the corner adds energy
- Rays passing through the obstruction are not the source of this signal

802.11n Signal Strength and Connectivity



A "walk around" on-site survey might lead someone to believe that several additional access points were needed in this space.

802.11n Signal Strength and Connectivity



Throughput predictions, confirmed by post-installation verification, show that coverage, throughput and capacity are excellent.

CACE TECHNOLOGIES

WIRESHARK UNIVERSITY

SHARKFEST '10 | Stanford University | June 14–17, 2010

Design of a Commercial 802.11 Network

The application of predictive RF CAD modeling and simulation provides the optimal preliminary design before any on-site work is performed

Design should not start with someone walking around, trying to figure out where to put radios

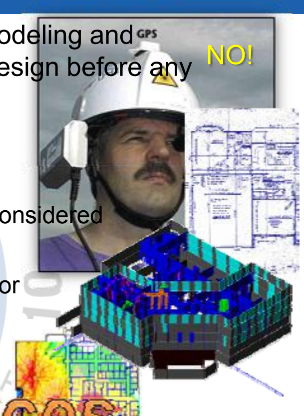
Design begins with the site plan
- Construction characteristics ar...
- Wiring closet locations ... e considered

A 3-Dimensional RF CAD ...
- The model accurately ... al behavior
- The design engineer c... the overall impact of d... s

Proper Coverage is Determined
- The "gue... wor... design surveys is eliminated
- Areas of specific concern are identified

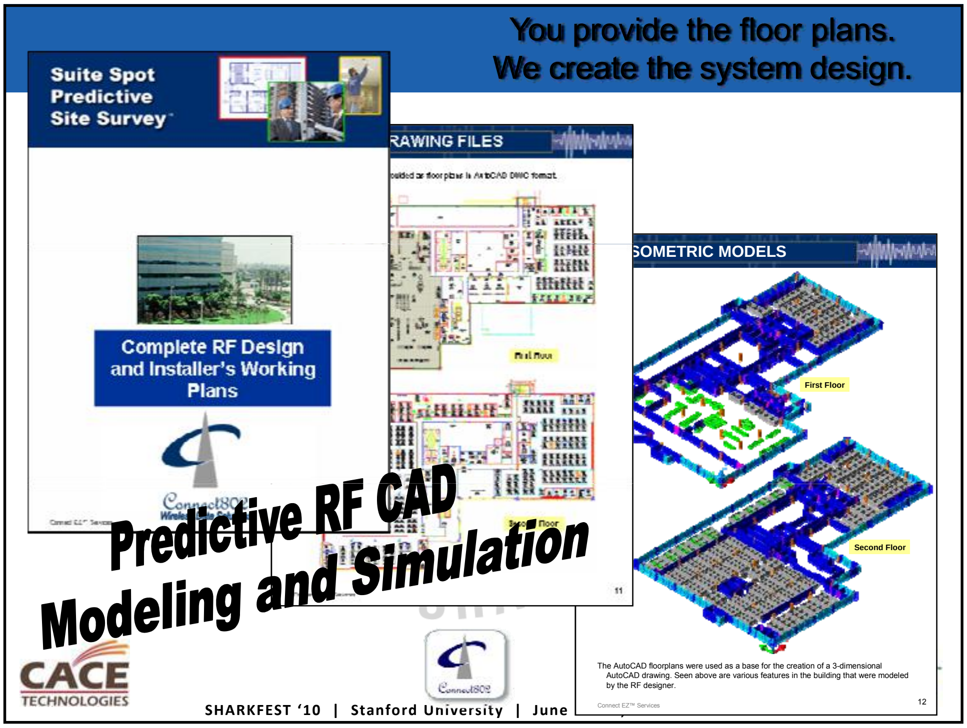
On-Site Sur... s Focused ... Areas
- The location of radio equipment has been determined
- On-Site calibration, noise and interference analysis, and coverage problem mitigation is facilitated

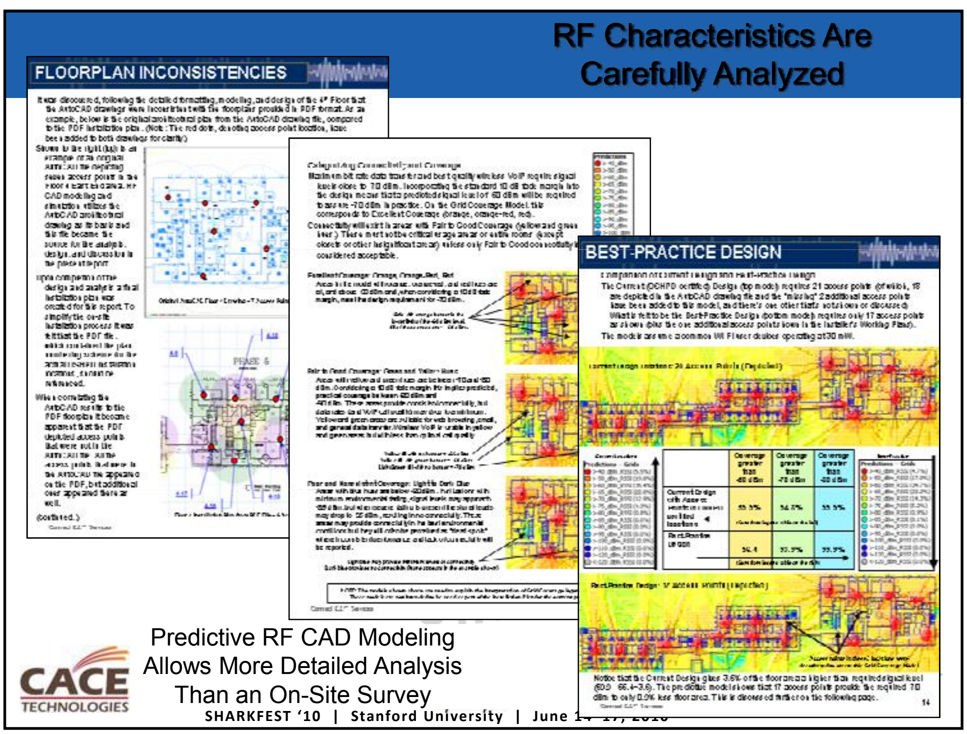
A Best-Practices Design is Created

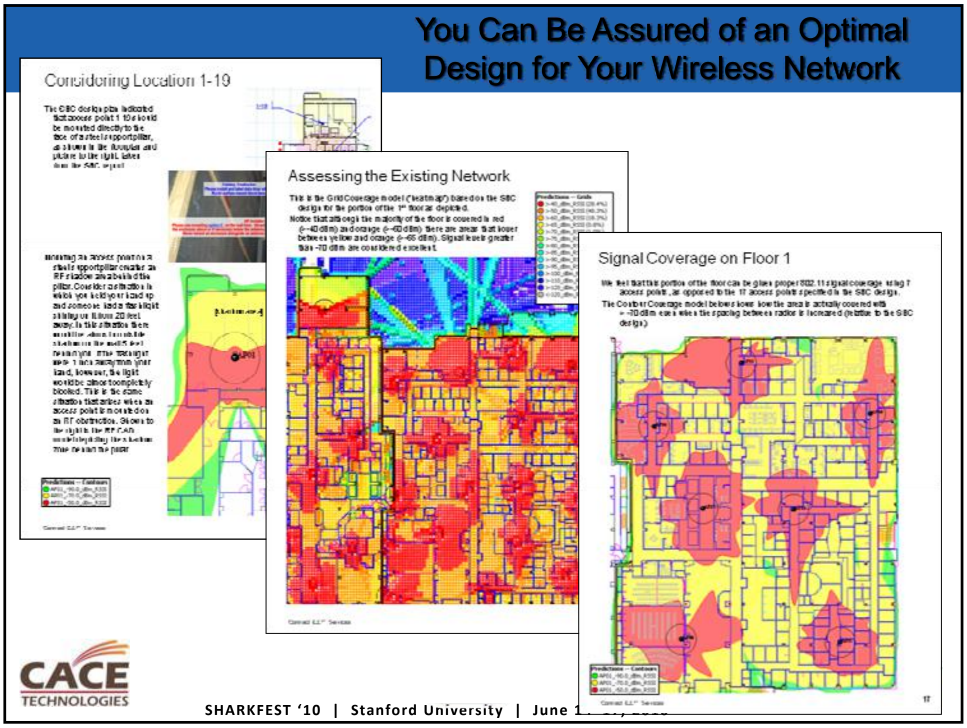


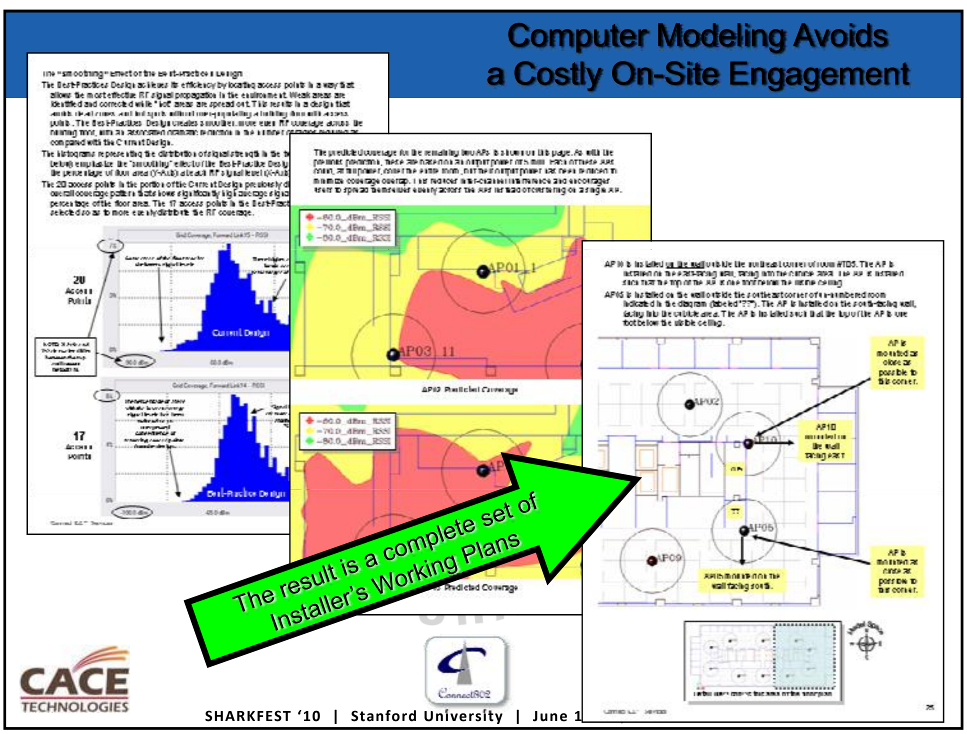
CACE TECHNOLOGIES

SHARKFEST '10 | Stanford University | June 14–17, 2010


You provide the floor plans.
We create the system design.
Suite Spot Predictive Site Survey
Complete RF Design and Installer's Working Plans
DRAWING FILES
ISOMETRIC MODELS
First Floor
Second Floor
The AutoCAD floorplans were used as a base for the creation of a 3-dimensional AutoCAD drawing. Seen above are various features in the building that were modeled by the RF designer.
Predictive RF CAD Modeling and Simulation
CACE TECHNOLOGIES
SHARKFEST '10 | Stanford University | June

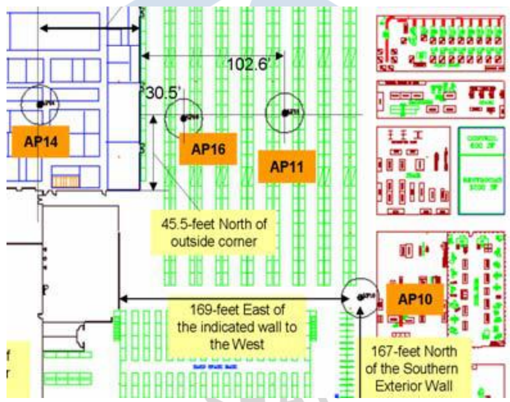

RF Characteristics Are Carefully Analyzed
FLOORPLAN INCONSISTENCIES
BEST-PRACTICE DESIGN
Predictive RF CAD Modeling Allows More Detailed Analysis Than an On-Site Survey
CACE TECHNOLOGIES
SHARKFEST '10 | Stanford University | June 14 - 17, 2010


You Can Be Assured of an Optimal Design for Your Wireless Network
Considering Location 1-19
Assessing the Existing Network
Signal Coverage on Floor 1
CACE TECHNOLOGIES
SHARKFEST '10 | Stanford University | June 1


Computer Modeling Avoids a Costly On-Site Engagement
The result is a complete set of Installer's Working Plans
CACE TECHNOLOGIES
SHARKFEST '10 | Stanford University | June 1

Your Accurate Installation Plans

- Installation of a commercial 802.11 network adheres to professional standards in the construction industry



These are part of the 802.11 Secrets Revealed!

Joe Bardwell - Connect802 Corporation
joe@connect802.com
www.Connect802.com - (925) 552-0802