Cranite™

Why Did You Drag That Ethernet Cable Onto The Street?

IEEE Oakland-East Bay ComSoc

Mike Coop
Director, Consulting Engineering

Wireless Networks Are Unique

- Wireless Network Vulnerabilities
  - Stolen bandwidth and assets
  - Network damage
  - Eavesdropping
- Evolving IT Challenges
  - Supporting enterprise wireless initiatives to gain competitive advantage
  - Securing data
  - Eliminating risk of network intrusion
  - Maximizing un-tethered experience for mobile users
  - Minimizing hands-on management & ongoing cost

Wireless Growth Inhibitors

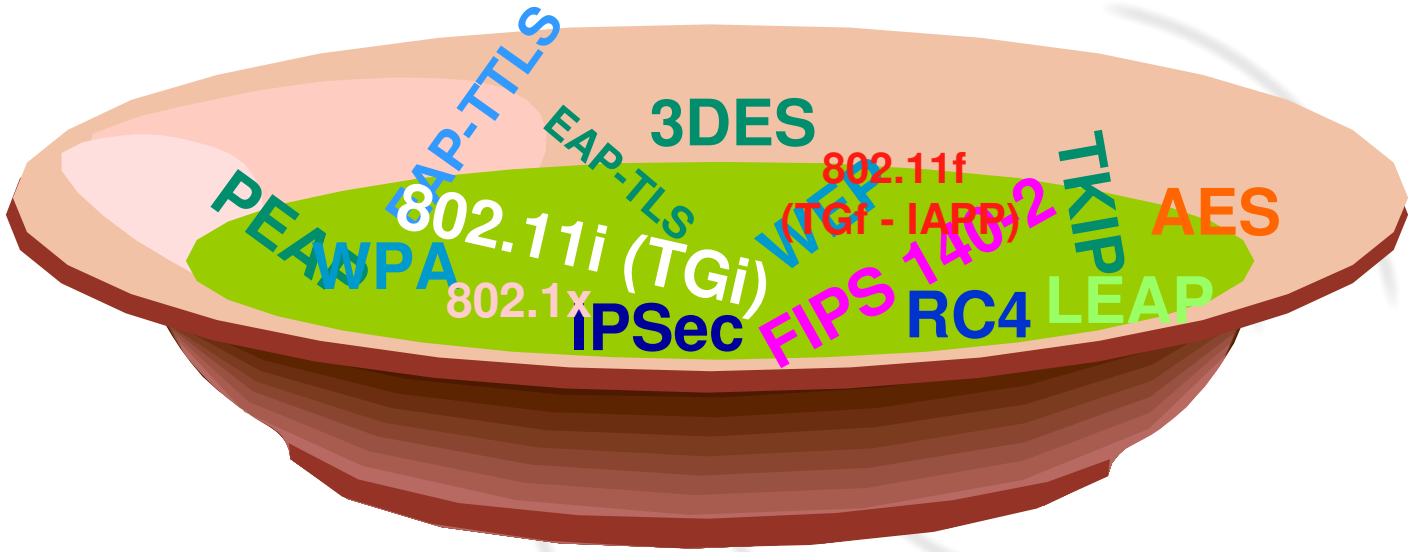
- Wireless LAN vulnerabilities
- Lack of system-level solutions
  - Supporting complex management tasks in a dynamic network environment
  - Meeting requirements for security, information assurance, network protection and data privacy
  - Delivering uncompromised mobility
- “Moving target” standards process

The State of Wireless LANs Today

- Solutions in use are re-purposed technologies
  - VLANs, VPNs, Mobile IP
  - All designed for fixed, wired networks
  - Impose counter-productive constraints
- The result:
  - Sub-optimal choices – never designed for wireless LANs
  - Loose collection of point products
  - Proprietary offerings - single vendor lock-in
  - Added complexity and cost

Wireless Security Initiatives

Standards & Protocols Stew



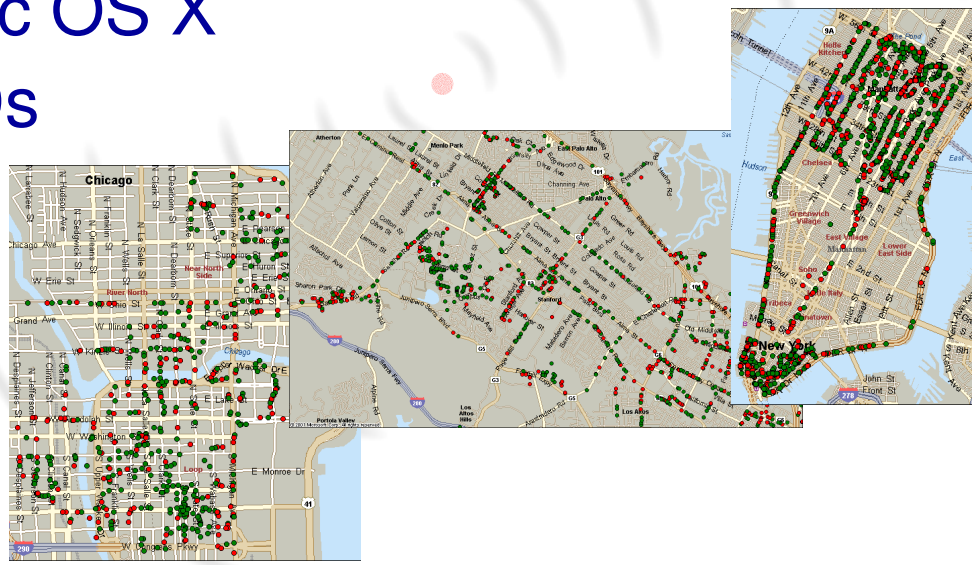
Continually evolving standards and protocols require obsolescence-proof solutions

Wireless *in*Security

- "Typical" 802.11 ranges
  - 802.11b/g is typically ~300 feet (2.4 GHz)
  - 802.11a/h is typically ~60 feet (5 GHz)
- Radio waves penetrate building walls — impossible to define and enforce perimeter
- Networks can be picked up 15 - 20 miles away with sufficient antennae
- Creates an entirely new category of espionage — one extremely difficult to detect
- Passive attacks capture data for offline analysis; active attacks compromise network real-time

802.11 Built-in Security

- Service Set Identifier (SSID)
  - Simple mechanism for choosing wireless network association
  - Defines administrative domain but NOT a security mechanism
  - Easy to snoop with NetStumbler, APSniff, NIC client, WinXP or Mac OS X
  - Most common SSIDs
    - Linksys 15%
    - Default 6%
    - Wireless 3%
    - (none) 3%
    - Tsunami 2%



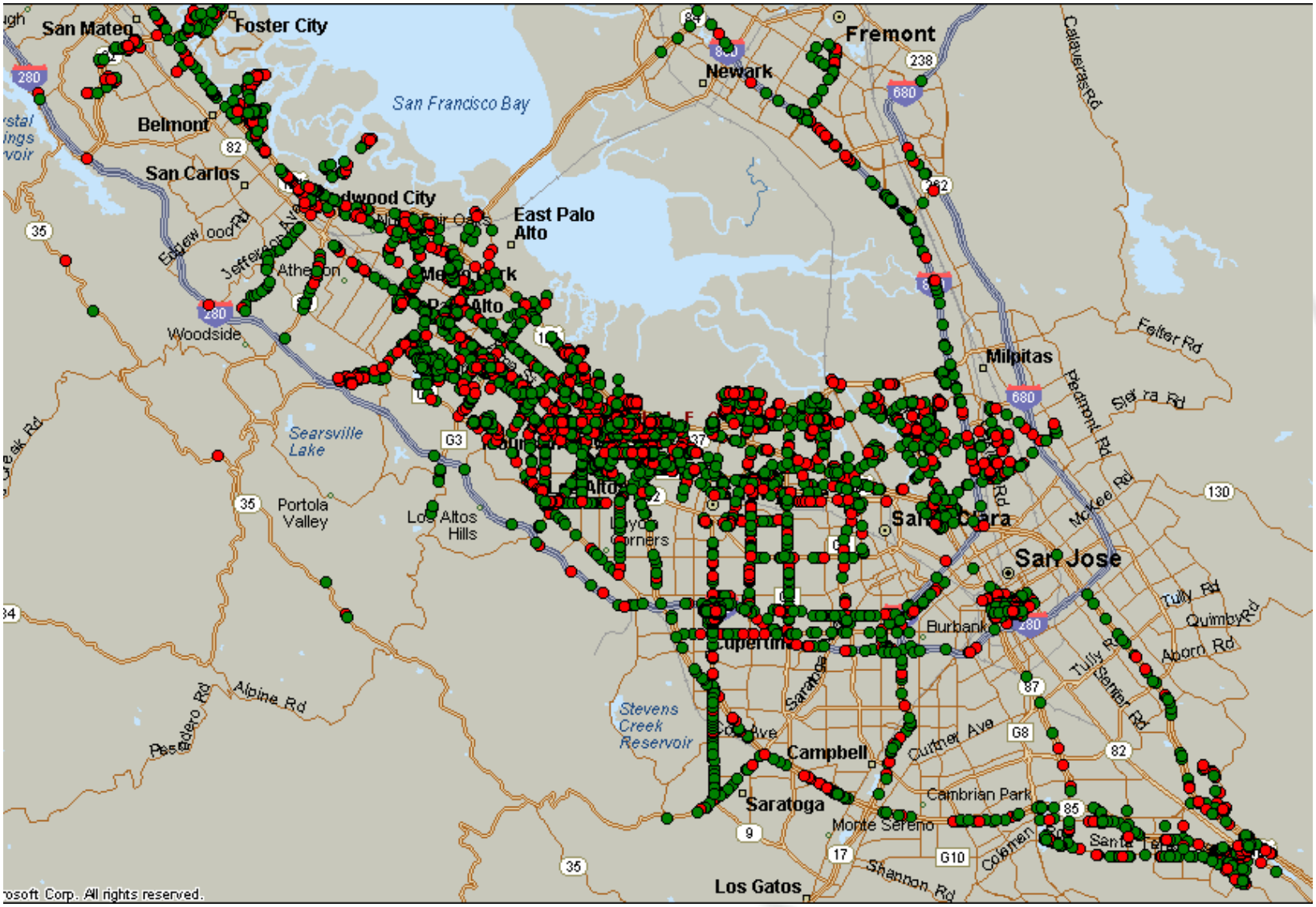
Wardriving Manhattan

Cranite

Wardriving San Francisco

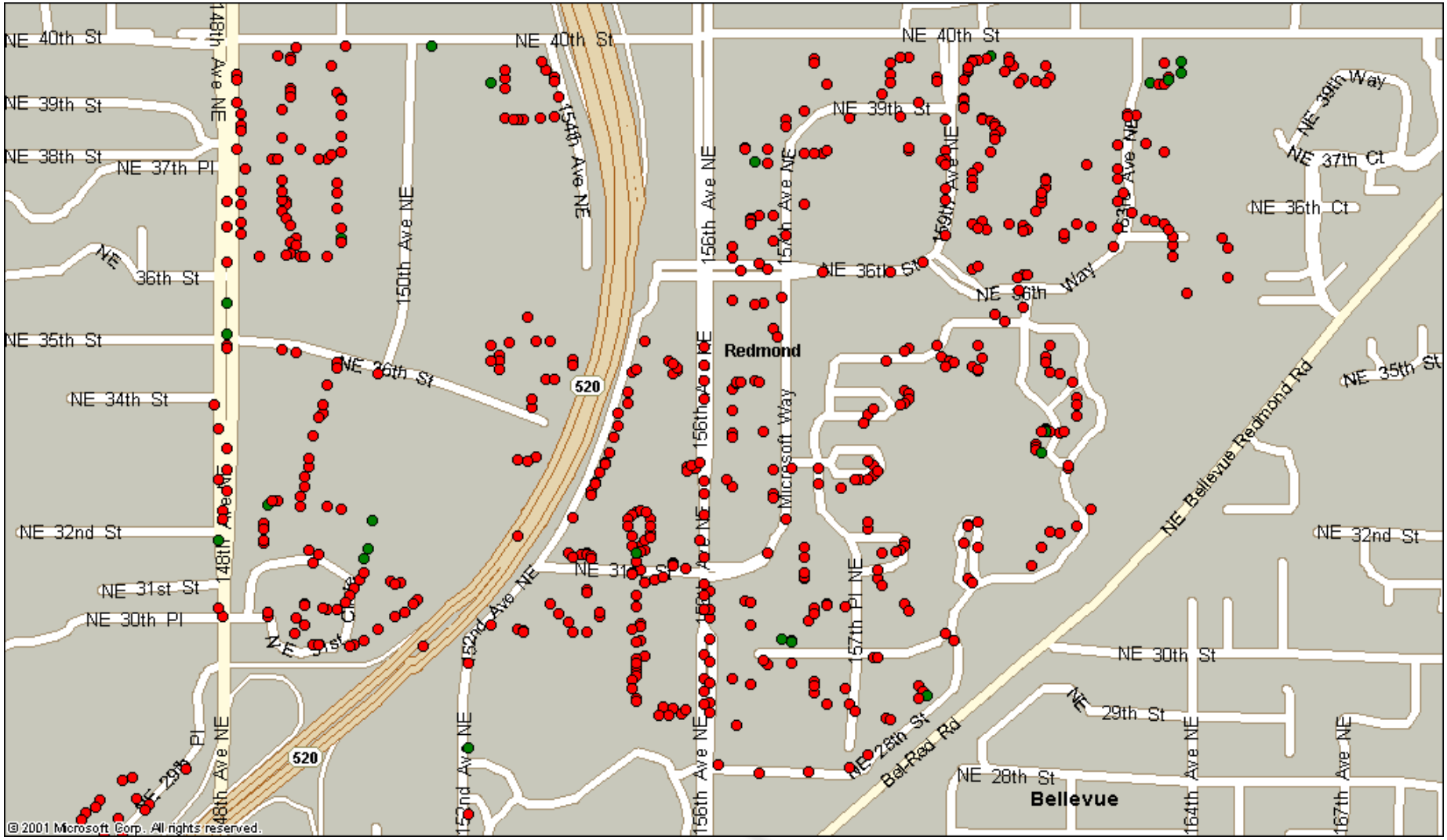
Cranite

Wardriving Silicon Valley

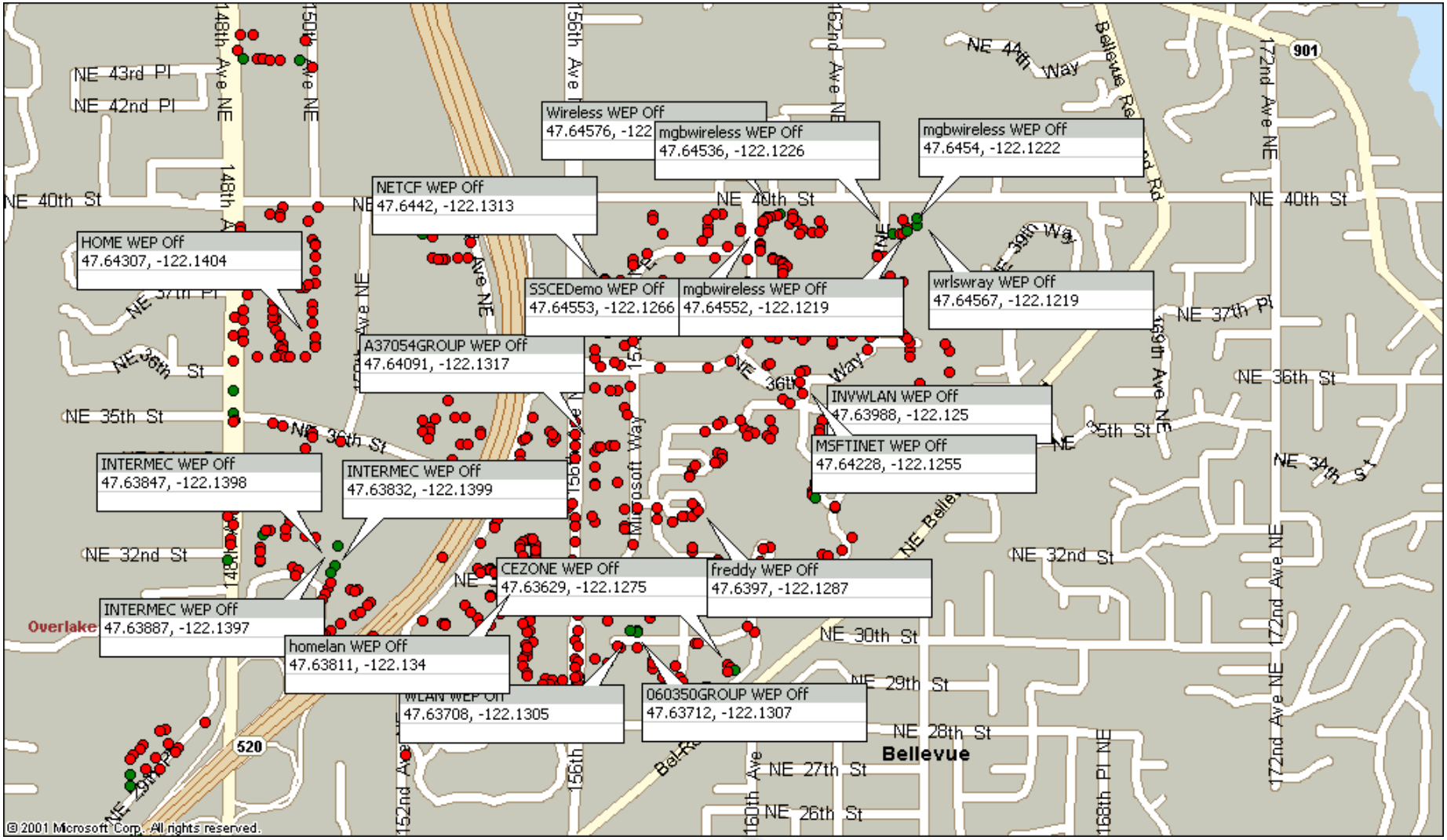


Cranite

Microsoft is VERY Secure



Or Are They?


Wireless WEP Off
47.64576, -122
mgbwireless WEP Off
47.64536, -122.1226
mgbwireless WEP Off
47.6454, -122.1222
NETCF WEP Off
47.6442, -122.1313
HOME WEP Off
47.64307, -122.1404
SSCEDemo WEP Off
47.64553, -122.1266
mgbwireless WEP Off
47.64552, -122.1219
wrlswray WEP Off
47.64567, -122.1219
A37054GROUP WEP Off
47.64091, -122.1317
INVWLAN WEP Off
47.63988, -122.125
MSFTINET WEP Off
47.64228, -122.1255
INTERMEC WEP Off
47.63847, -122.1398
INTERMEC WEP Off
47.63832, -122.1399
CEZONE WEP Off
47.63629, -122.1275
freddy WEP Off
47.6397, -122.1287
INTERMEC WEP Off
47.63887, -122.1397
homelan WEP Off
47.63811, -122.134
WLAN WEP Off
47.63708, -122.1305
060350GROUP WEP Off
47.63712, -122.1307
NE 43rd Pl
NE 42nd Pl
NE 40th St
NE 37th Pl
NE 36th St
NE 35th St
NE 32nd St
NE 30th St
NE 29th St
NE 28th St
NE 27th St
NE 26th St
148th Ave NE
150th Ave NE
156th Ave NE
162nd Ave NE
172nd Ave NE
NE 44th Way
Bellevue Redmond Rd
NE 39th Way
NE 36th Way
Microsoft Way
NE 34th St
NE 29th Pl
Overlake
Bellevue
520
901
© 2001 Microsoft Corp. All rights reserved.

802.11 Built-in Security

- WEP
  - Part of the 802.11 standard, provides only device authentication and encryption on WLAN access points and NICs
  - Allows for unauthorized access points and man-in-the-middle attacks
  - Cryptography implementation flaw makes WEP keys crackable, regardless of length
  - Airsnort, WEPCrack are simple, free cracking tools
  - Not FIPS-certifiable
  - Widely recognized as flawed
- Dynamic WEP
  - Vendor-specific solutions for key rotation/rekeying
  - Proprietary, non-interoperable
  - Not FIPS-certifiable

Other Security Options

- MAC Address Filtering
  - MAC addresses sent in clear
  - Trivial to sniff
  - MAC addresses forgeable with NIC software
  - Additional risk from theft of an (authorized) NIC
- VPN
  - Designed for remote users, not mobile users
  - 3DES solutions compute-intensive and resource-taxing
  - Time consuming to manage and support
  - Clients intended for low bit error rate networks—susceptible to radio fade common in wireless networks
  - Doesn't address roaming
    - Requires Mobile IP in addition to VPN
    - Adds complexity and costs

Wi-Fi Protected Access (WPA)

- Announced October ‘02
- Certified products not yet available (target is Q2:03)
- Uses TKIP for key rotation, “Michael” for message integrity
- Neither WEP nor WPA meet FIPS certification requirements
- Not a long-term solution—will be obsoleted in 2004 by 802.11i
- Does not support requirements for secure roaming

Some Recent Quotes re: WPA

"While seen as an improvement on the older standard, WPA could also complicate matters for some businesses since Wi-Fi firmware would also need to be updated to support the security technology."

"WPA is meant to be a temporary fix"

"Gartner analyst John Pescatore said that this [WPA] "temporary solution" would have to hold businesses over for "probably two more years." "I'm just worried that people will be fooled into upgrading the PCs and not the access points, or upgrade the access points and not the PCs," he said."

"But that WPA compliance could be a problem for many Wi-Fi users, since base stations, PC Cards, USB devices and wireless networking components integrated into notebooks would all need to be updated to support the security technology."

"Microsoft is still evaluating WPA (for its Wi-Fi hardware),"

Source: cNet News.com 3/31/2003

802.11i

- Standard not yet ratified
- To be voted on at September plenary
- Compliant products likely to hit market in Q2:04
- Uses 802.1x for authentication
- Uses RC4-based TKIP for encryption and Michael for message integrity (like WPA), or uses AES for encryption and message integrity (preferable moving forward)
- Goal is to be FIPS-certifiable
- Does not support requirements for secure roaming

Common EAP Types

- 5 common types of Extensible Authentication Protocol (EAP)
  - EAP-MD5 Since no authentication tunnel is created to hide credentials, is excluded as a wireless authentication method within Windows
  - EAP-Cisco (a.k.a. LEAP) Similar to EAP-MD5, no tunnel protects authentication credentials, hence Cisco's move away from LEAP to PEAP
  - EAP-TLS Based on Transport Layer Security (TLS), requires a CA infrastructure since each end device requires a unique certificate
  - EAP-TTLS Tunneled TLS, uses server-side certificate, obviating need for unique client-side certificates
  - PEAP (Protected EAP) Newer spec pushed by Cisco and Microsoft, very similar to EAP-TTLS; implementations from Cisco and Microsoft are currently not compatible

What the Standards Won't Do

- Deliver a systems-level solution for management, security, and mobility
- Be available any time soon
- Be supported across the installed base
- Ensure the integrity of keys
- Ensure secure, seamless subnet roaming
- Ensure multi-vendor interoperability

FIPS 140-2 Certification

- Industry's only independent cryptography validation
  - Validates encryption algorithms, random number generators
  - Ensures protection of keys
  - Ensures algorithms used to create keys meet specific requirements
  - Ensures all cryptographic interfaces are acceptable
- Other Cranite FIPS certified algorithms include:
  - 3DES FIPS certification number 130
  - AES-128 FIPS certification number 24
  - SHA-1 FIPS certification number 113
  - SHA-1 HMAC vendor affirmed
  - RSA PKCS #1vendor affirmed

Where the Standards Fit

Wired Equivalent Privacy (WEP)	Part of the 802.11 standard, provides device authentication and encryption on WLAN access points and client cards; not FIPS-certifiable and **widely recognized as flawed**
Dynamic WEP	• Addresses weak IV issue by rotating WEP keys periodically • Ties users to a **single vendor** for all devices
WiFi Protected Access (WPA)	WEP with periodic key rotation & 802.1x for authentication • Uses Temporal Key Integrity Protocol (TKIP), which is a 'quick-fix' patch • Does not support requirements for secure roaming • Interim security solution — will be obsoleted in 2004 by 802.11i • **Not** FIPS certifiable
802.11i	Station-to-station security standard for AP and peer-to-peer applications • Addresses privacy, integrity, authenticity of data between devices • Does **not** address system-level management, security, mobility issues
802.1x	IEEE standard for **authentication only**; supports multiple authentication modes for wired and wireless networks • Does **not** specify a secure communication channel between 'supplicant' (user) and 'authenticator' • Does **not** address system-level security, mobility, management issues
802.11f	Describes inter-AP communications among multi-vendor systems • Specifies fast handoff between APs • Only addresses roaming within the same subnet

Does Wireless = Mobility?

- Most wireless security solutions require a combination of:
  - Layer 2 (dynamic WEP/WPA)
  - Layer 3 (VPN/IPSec) security technologies
- Subnet mobility requires use of Mobile IP
  - Mobile IP configuration, management, and troubleshooting are complex
  - Increases TCO

Defeats the freedom of wireless

If It Works Don't Fix It

- View wireless as an extension of the wired network
  - Apply best practices in overall network design
  - Address unique needs for the wireless component with purpose-built solutions
- Deploy a lower cost radio infrastructure
  - Reduces acquisition and replacement expenses
  - Obviates impact of continually evolving standards
  - Broadens choice of vendors
- Implement centralized management and control
- Physically secure the security technology – using physically unsecured APs to secure the network is an oxymoron

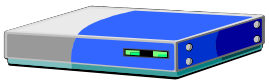
Where Does the Intelligence Belong?

In the Wiring Closet or in the Plenum/Open Office?

Data Center/Wiring Closet

Hubs/Switches

Firewalls



Authentication/ Directory Servers

Routers

- Centrally managed
- Physically secured
- Home for purpose-built devices

SECURE ←

Plenum/Open Office

Access Points

- Easily compromised
- Physically unsecured
- Requires expensive, complex APs

→ **UNSECURE**

Well, Not So Fast

- Available system level solutions are closed and proprietary
- Everything else is:
  - Round pegs in square holes, i.e. VPN's
  - Mix and match of point products
- Standards far from being ready or available
- The market needs an open, systems level solution
  - Must support existing and future standards
  - Needs to address management and mobility

How to Deploy Wireless LANs

- View as an extension of the wired network
  - Apply best practices in overall network design
  - Address unique needs for the wireless component with purpose-built solutions
- Deploy a low-cost radio infrastructure
  - Reduces acquisition and replacement expenses
  - Obviates impact of continually evolving standards
  - Broadens choice of vendors
- Implement centralized management and control
- Physically secure the security technology – using physically unsecured APs to secure the network is an oxymoron

Wireless Security Best Practices

- Disable broadcast SSID
- Don’t choose SSIDs which provide identifiers
- Assume WEP provides no security whatsoever
- Perform mutual authentication of users and network
- Authorize users uniquely, not by device

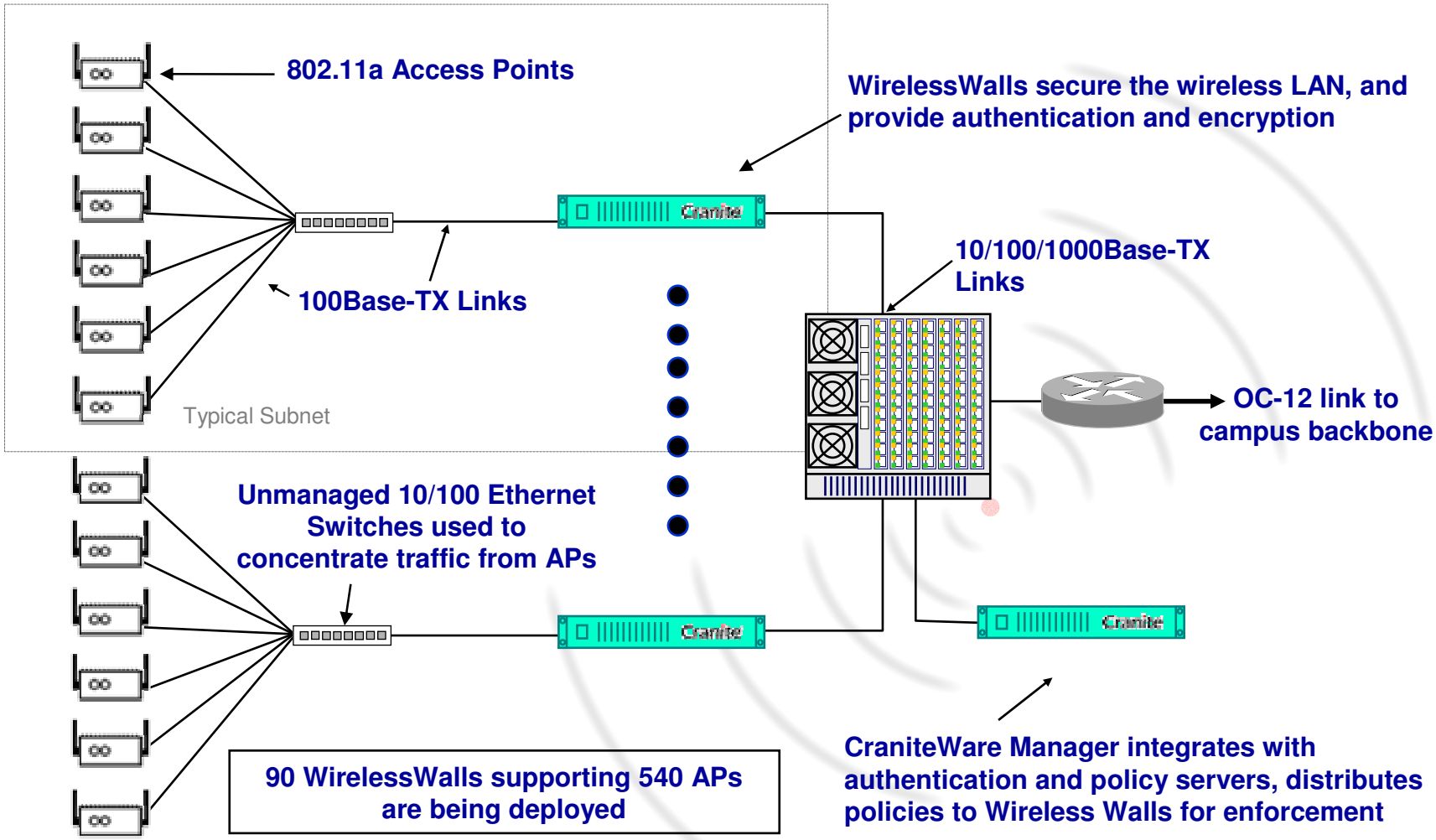
Wireless Security Best Practices

- Protect both Layer 2 and Layer 3 while retaining wireless' inherent mobility
- Adapt the infrastructure to user habits, not vice versa
- Integrate with existing directories and authenticators
- Utilize unidirectional, per-session, per-user encryption and message integrity keys
- Restrict traffic to pre-defined resources

Cranite Case Study – West Point

- Application: Online, interactive instruction
- Problems: Wiring cost and security
- Alternatives: VPNs, WEP, and others
- Solution: Implemented 802.11a and CraniteWare in 95 classrooms with more than 1,000 cadets

West Point Network Topology



Cranite's Focus

Purpose-built solutions for managing and securing wireless networks that enable maximum mobility for users with the lowest total cost of ownership

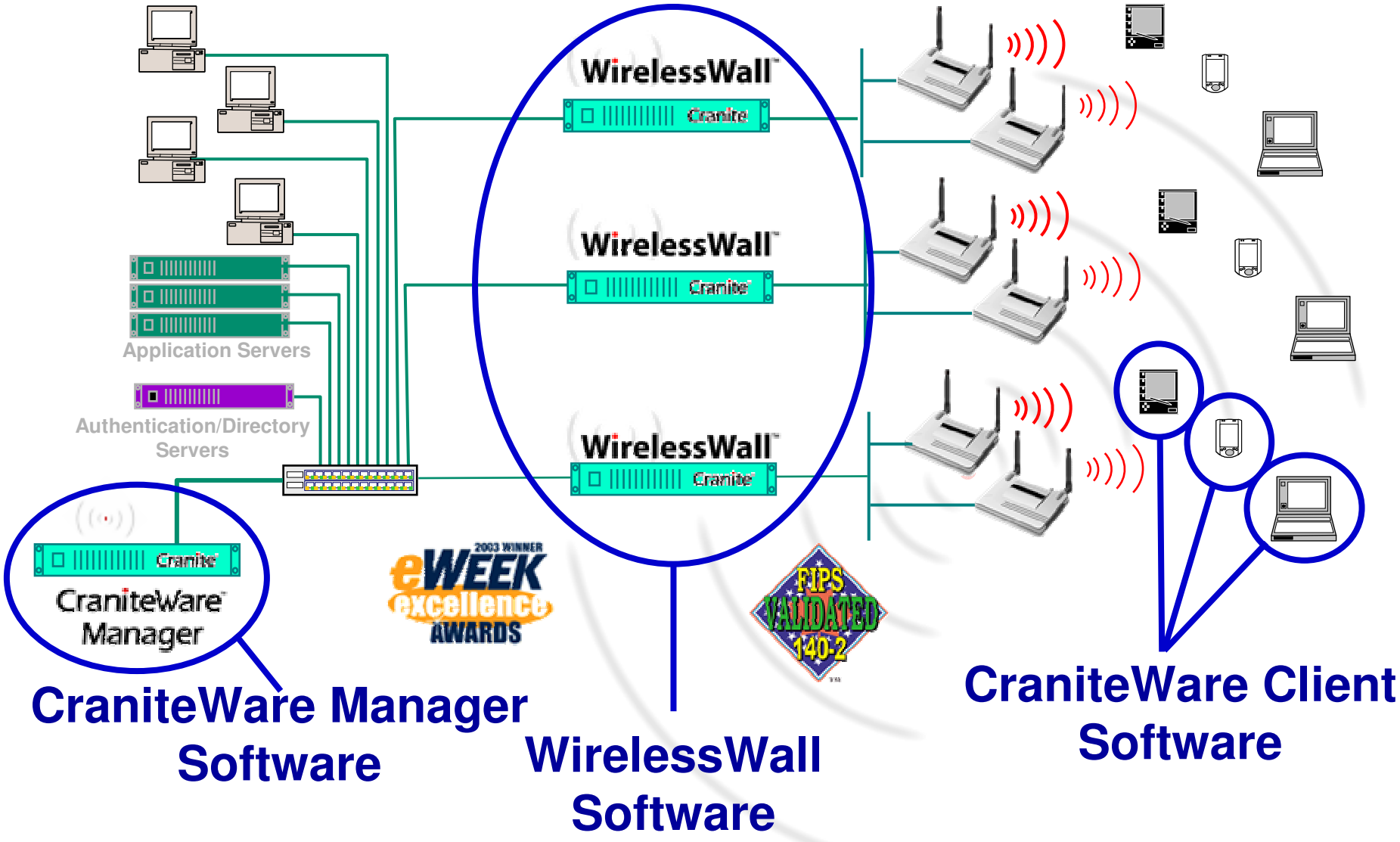
Company Background

- Cranite Systems founded in August, 2000
- Core technology originally developed by unit of U.S. Navy to secure and mobilize networks on warships and submarines
- Privately held, VC funded
- Headquartered in San Jose, CA
- Products shipping since February, 2001

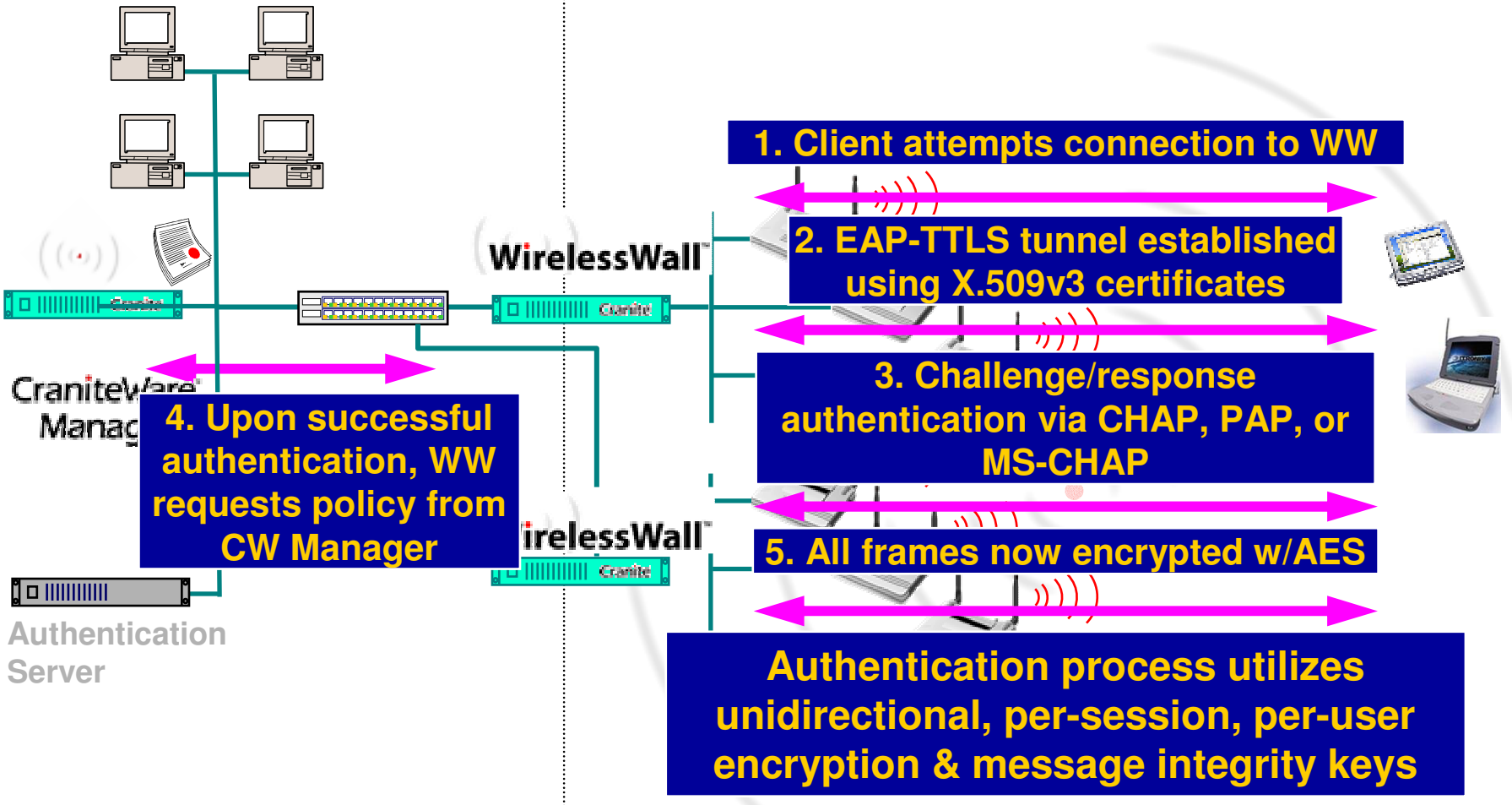
CraniteWare Characteristics

- Open architecture, standards based, non-proprietary
- Portable software running on off-the-shelf hardware
- Works with what you've got –
  - Existing wired and wireless infrastructure
  - Existing enterprise policy, management, and security applications
  - L2/L3 switches, routers, etc. from any vendor
  - AP's and NIC's running any standard from any vendor
  - Broad-based support for wide variety of wireless devices
- Works with what you'll get –
  - Agnostic to emerging WLAN protocols and standards
- Protects your investment and reduces TCO for wireless networks

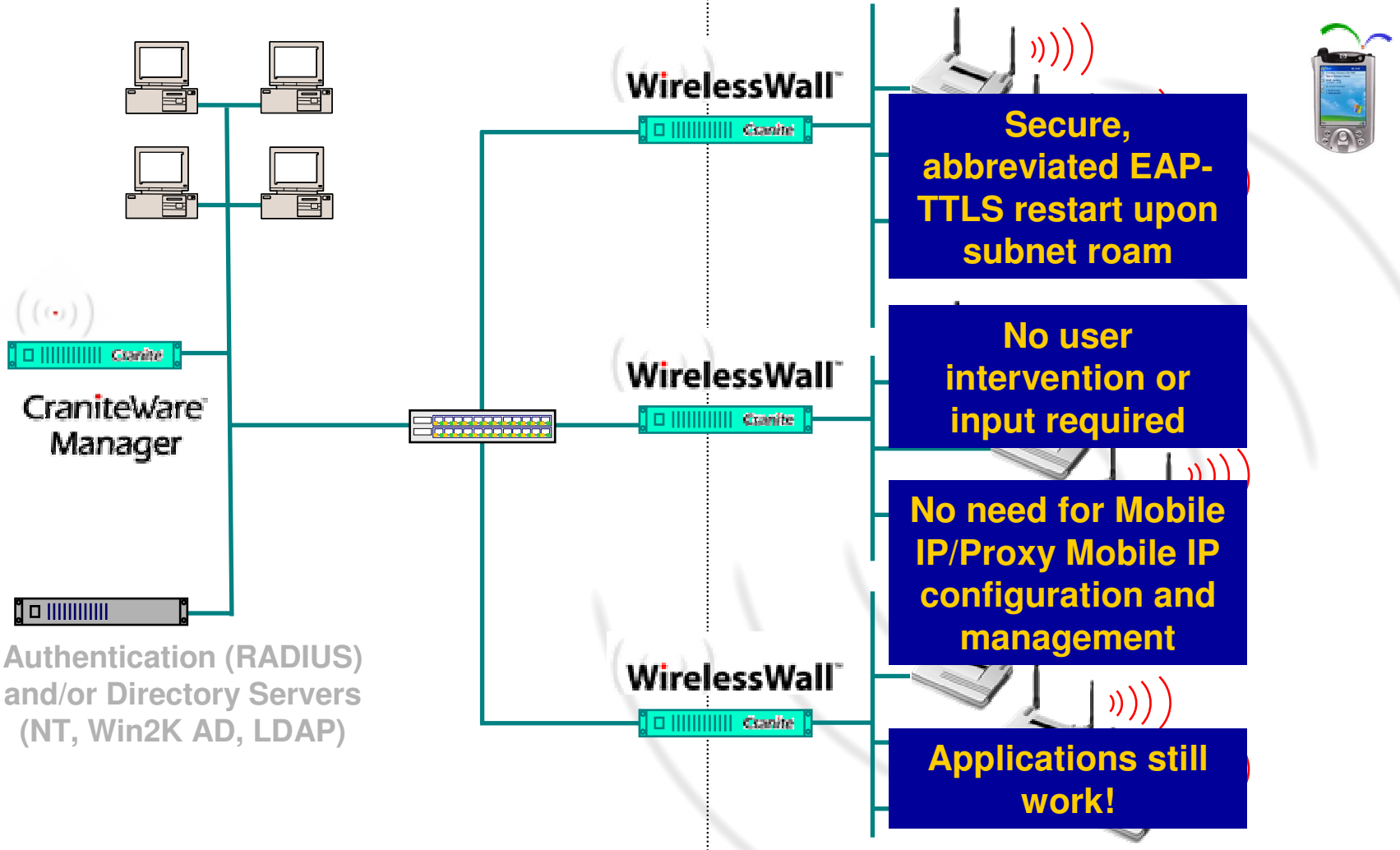
CraniteWare Components



Secure Authentication Process



Quick, Seamless, Secure Mobility

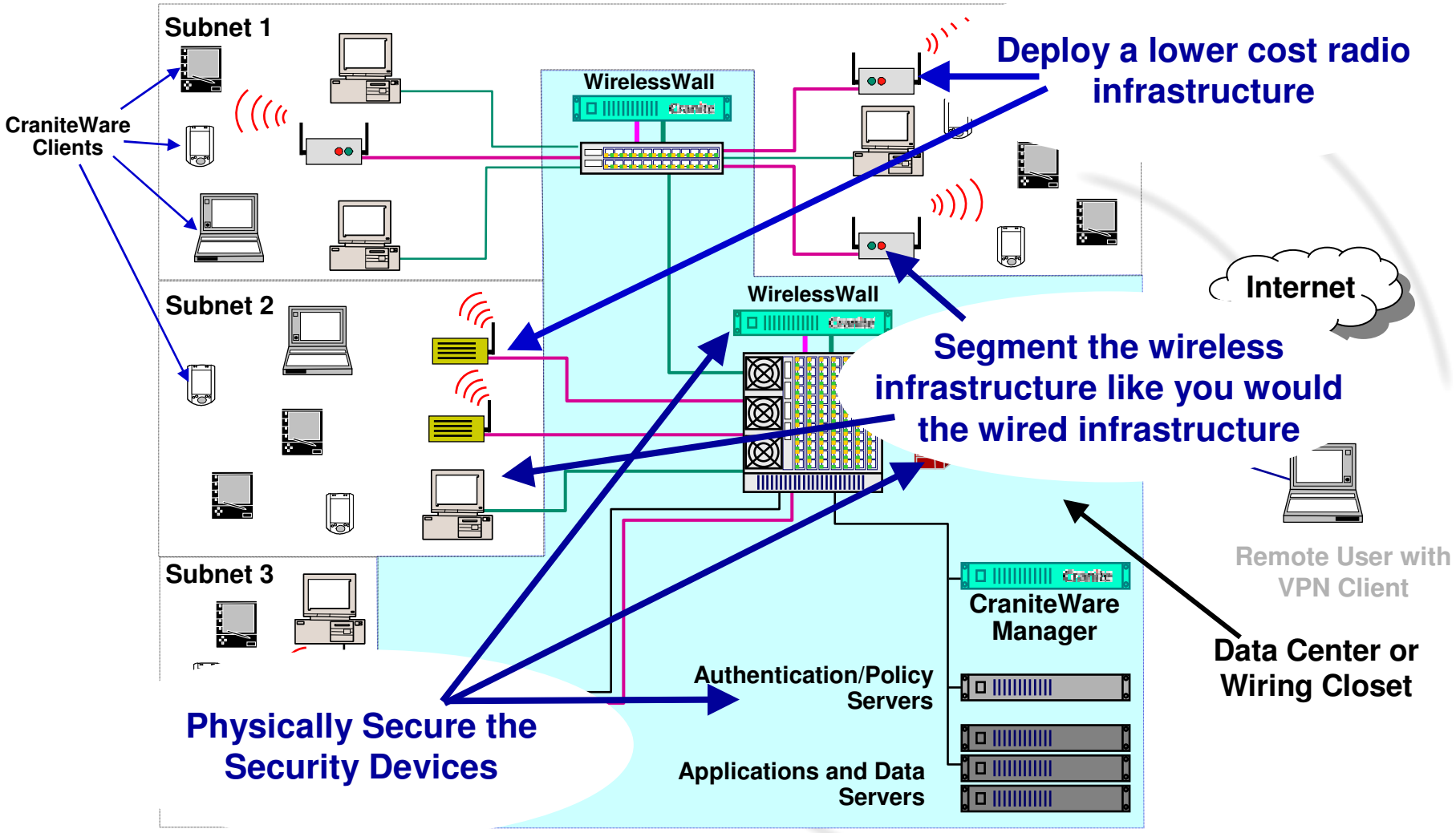


Cranite

Cranite Completes the Picture

Mechanism	Management	Security	Mobility
WEP	NO	Widely recognized as flawed Being replaced with WPA	NO
WPA	NO	Improvement over WEP Temporary fix until 802.11i	NO
802.11i	NO	Device level only	NO
802.1x	NO	Authentication only	NO
802.11f	NO	NO	Between APs on same subnet only
WirelessWall	YES	Network level security Strong authentication AES encryption	Robust roaming across subnets
CraniteWare Manager	YES	Enforces enterprise wide security policies	Policy enforced while roaming

CraniteWare Integrated Network



CraniteWare Advantages

- Allows use of a wide variety of *low-cost* infrastructure devices running any 802.11 protocol
- Provides simple, cost-effective integration and management
- Secures both the *network* and the *data* at Layer 2
- Supports secure client mobility across subnets without complex, labor-intensive configuration & management

CraniteWare Benefits

- Interoperability
- Operational simplicity
- Security granularity
- Lower acquisition costs
- Obsolescence-proof investment protection
- Lower ongoing management costs

Cranite™

Thank You!

Mike Coop

mcoop@cranite.com

mcoop@ieee.org