

# The wireless picture

Dr. ir. Iris De Coster

The wireless picture



© 2005, Telinious High-Tech Institute

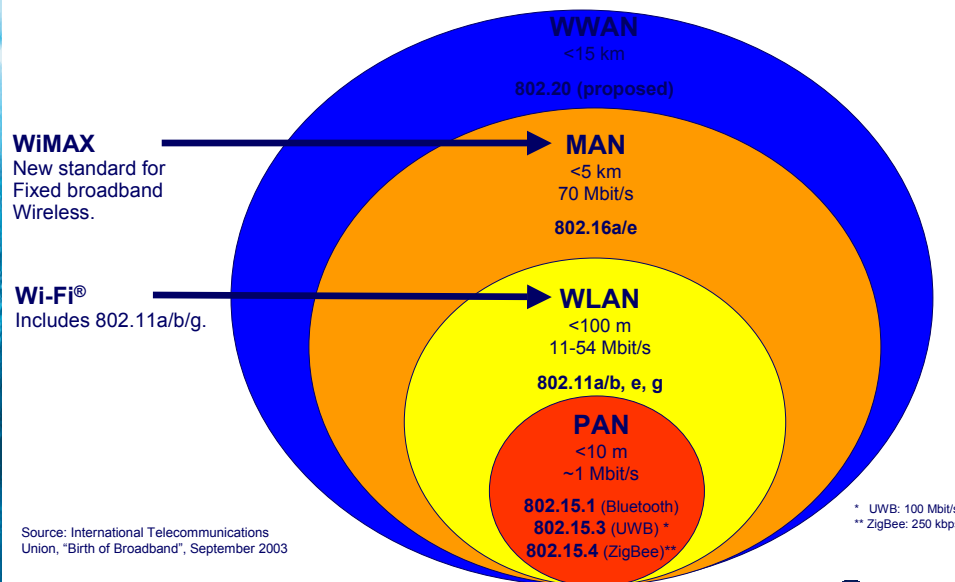
## Summary

- Wireless LAN
  - Standards
  - Architecture
  - Performance
  - Security
  
- Emerging technologies

The wireless picture



© 2005, Telinious High-Tech Institute



The wireless picture



© 2003, Telinus High-Tech Institute

## WLAN standards & trends

The wireless picture



© 2003, Telinus High-Tech Institute

- Increasing acceptance and use of Wireless LANs
  - Home use
  - Corporate networks
  - Hotspots
  
- Support of important market players
  - Microsoft has embedded support for Wi-Fi in the new XP and Pocket PC operating systems
  - Large laptop manufacturers all have built in WLAN today.
  - Many other devices are following

The wireless picture



© 2001, Telinus High-Tech Institute

- Laptop PC's
- PDA's
- Phones
- Printers
- Projectors
- Tablet PC's
- Security cameras
- Barcode scanners
- Custom devices for vertical markets
  - Healthcare
  - Manufacturing
  - Retail
  - Restaurants

**HP iPAQ 5450 PDA**



**IBM Thinkpad PC**

**HP Printers**



**Siemens Medical SIMPad**



**Cisco 7920 Phone**



**Intermec Barcode Scanner**



**Sharp M25X Projector**



The wireless picture



© 2001, Telinus High-Tech Institute

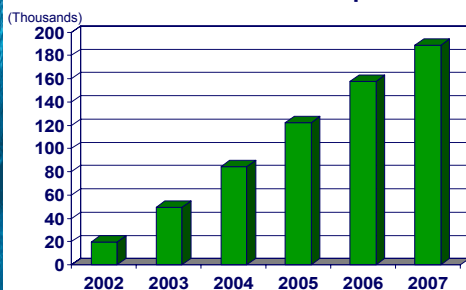
- 802.11b
  - 2.4 GHz, 3 non-overlapping channels
  - 1 – 2 – 5.5 – 11 Mbps
- 802.11a
  - 5 GHz, 8 non-overlapping channels
  - 6 – 9 – 12 – 18 – 24 – 36 – 48 – 54 Mbps
- 802.11g
  - 2.4 GHz, 3 non-overlapping channels
  - 6 – 9 – 12 – 18 – 24 – 36 – 48 – 54 Mbps
  - Compatibility with 802.11b possible

Shared bandwidths!!!!

- Hotspots are 802.11(b) **public** areas, for use by guests
  - Airports, cafes, and hotels are early entrants
  - IBM/Intel/ATT/3i/Apax formed Cometa Networks, to create 20,000 hotspots within two years
- Main challenge: roaming, roaming, roaming...
- Pundits are already pronouncing these 'dead'
  - No consumer demand
  - Unfriendly and expensive
- But others say OK
  - WLAN will be incorporated into 4G architectures

- Market adoption will be driven by expanded coverage, not faster data speeds
  - Expanding coverage is CAPEX intensive due to the backhaul expense
  - 11 Mbit/sec (802.11b) is more than sufficient for most data applications today
  - 54 Mbit/sec (802.11a, g) data throughputs will be severely limited by the backhaul
- Combining Wi-Fi access with voice services will be necessary to sustain demand according to some

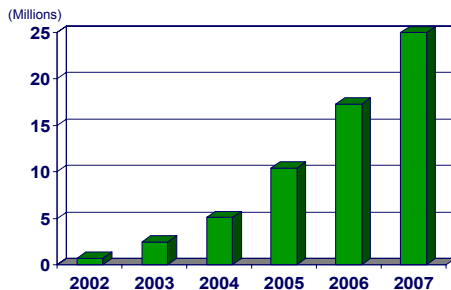
Worldwide Wi-Fi hotspots



Source: IDC, June 2003

The wireless picture

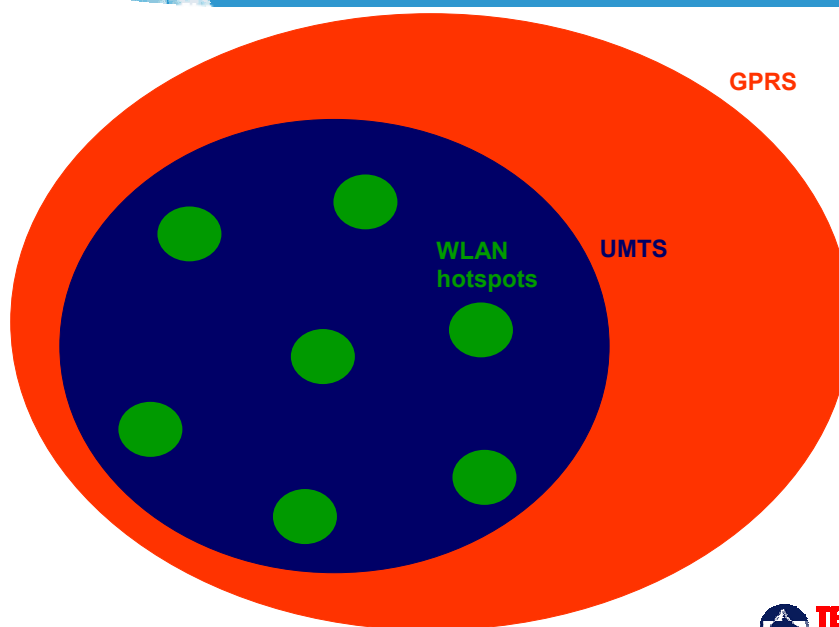
Worldwide Wi-Fi users



Source: IDC, June 2003



© 2003, Telinus High-Tech Institute



The wireless picture



© 2003, Telinus High-Tech Institute

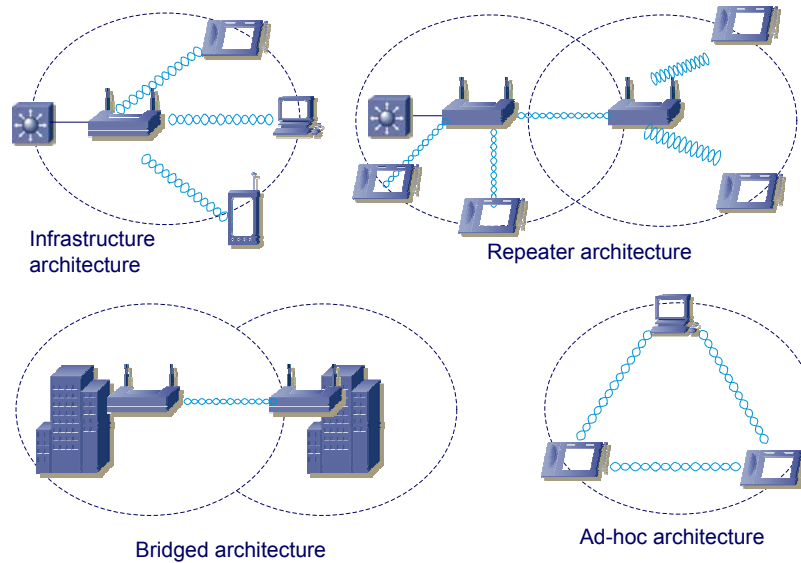
# WLAN architecture

The wireless picture



© 2005, Telinious High-Tech Institute

## WLAN architectures overview



The wireless picture



© 2005, Telinious High-Tech Institute

- **Multi-mode** access points & NICs becoming customary
  - a/b, b/g, a/b/g (e.g., Proxim)
  - Soon will have cellular/3G added to these
- New architectures arriving: **wireless “switches”**
  - Ex: Mobius (Symbol), Harmony (Proxim), ReefEdge, Aruba, AirFlow, Blackstorm, Trapeze Networks, Extreme Networks, Nortel
  - Contrary to Cisco’s “smart AP” approach

The wireless picture

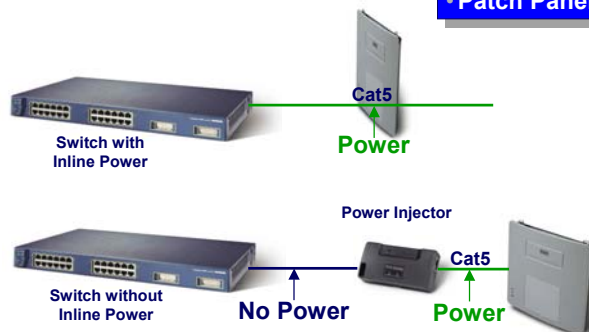


© 2001, Telinus High-Tech Institute

- 48 Volt DC power supplied over Cat 5 cable
- Eliminates cost of installing AC power
- Device discovery mode

**Ethernet In-line Power Sources:**

- Power Injector
- Switch
- Patch Panel



The wireless picture



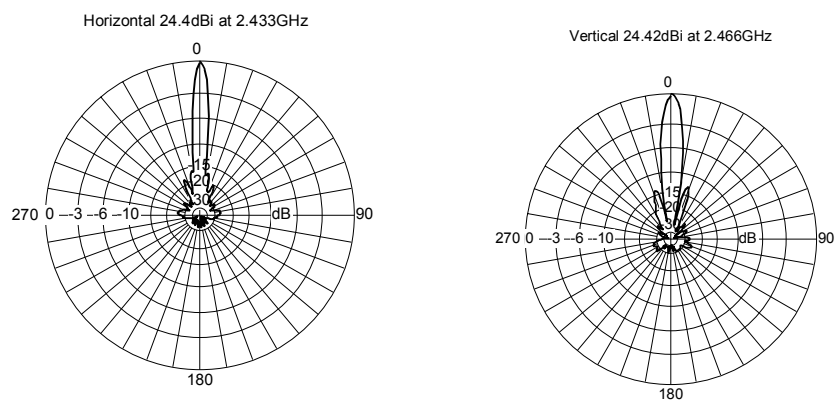
© 2001, Telinus High-Tech Institute

- Ideal antennas
  - Radiate equally in all directions
  - Called “isotropic” or “isotropic radiator”
- Real antennas
  - Have radiation patterns that concentrate the RF energy in different ways
  - Omnidirectional antennas, also called a dipole radiate in a donut shape, very common on APs
  - Directional antennas, i.e., biquad concentrates energy into a cone or a beam
- PCMCIA Antennas
  - Tend to be very directional
  - Effective gain is very low
  - External antennas make a big difference

The wireless picture



© 2001, Telinus High-Tech Institute

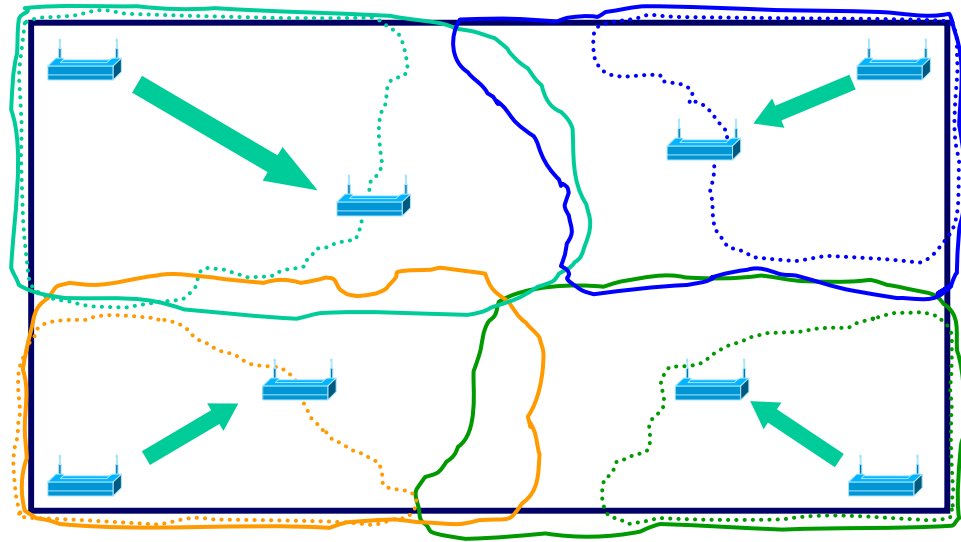


The wireless picture



© 2001, Telinus High-Tech Institute





The wireless picture

## WLAN performance

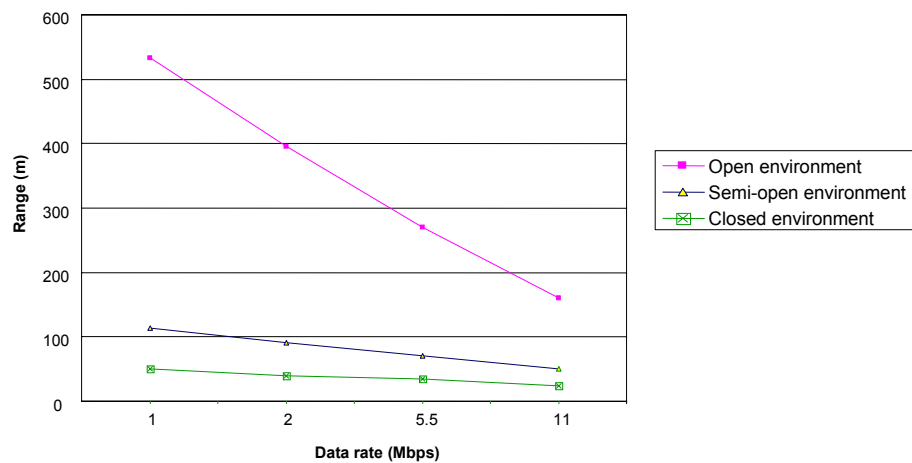
The wireless picture

- Theoretical maximum application-level throughput
  - 1500 byte packets, encryption enabled, zero packet errors

	Modulation	Maximum link rate	Theoretical maximum TCP rate	Theoretical maximum UDP rate
802.11b	CCK	11 Mbps	5.9 Mbps	7.1 Mbps
802.11g (with 802.11b)	OFDM/CCK	54 Mbps	14.4 Mbps	19.5 Mbps
802.11g (11g-only mode)	OFDM/CCK	54 Mbps	24.4 Mbps	30.5 Mbps
802.11a	OFDM	54 Mbps	24.4 Mbps	30.5 Mbps

© 2005, Telinus High-Tech Institute

The wireless picture



© 2005, Telinus High-Tech Institute

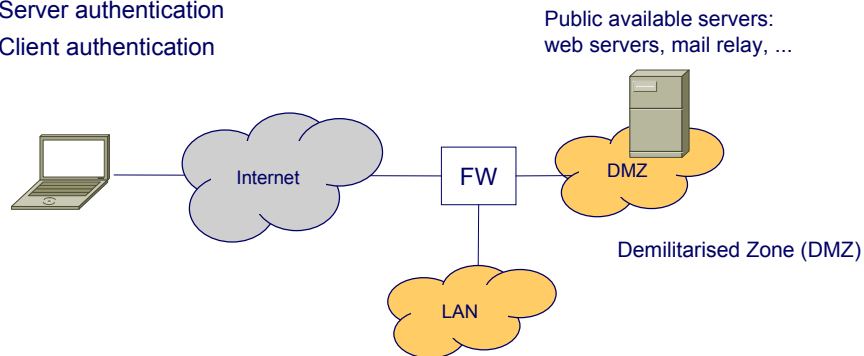
The wireless picture



- Strategies that work in a wired environment don't translate to WLAN
  - Packet error rate can be in the range 10 – 20 % (what does guaranteed QoS mean?)
  - Bit rates vary according to channel conditions (what does connection admission control mean?)
- Bandwidth reservation
  - Industry is moving away from RSVP (e.g. no longer supported in Windows XP)
  - 802.11e cannot assume RSVP is present
  - 802.11e must support 802.1p/q
- 802.11e introduces "hybrid coordination function"
  - Single channel access protocol that has elements of polled and CSMA based channel access

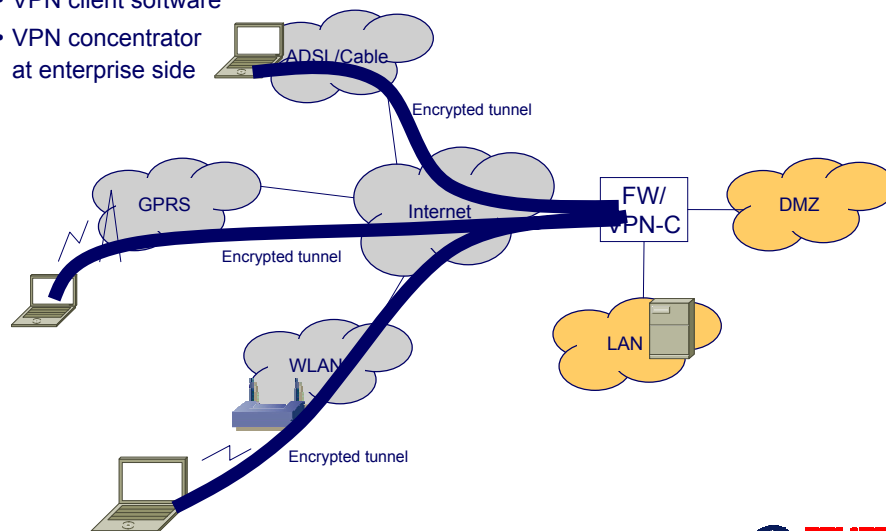
## WLAN security

- Public internet is not secure
  - Firewall between intranet and internet
  - Database of credit card numbers not in DMZ
- Communication over internet to e.g. bank sites using SSL
  - Encryption
  - Server authentication
  - Client authentication



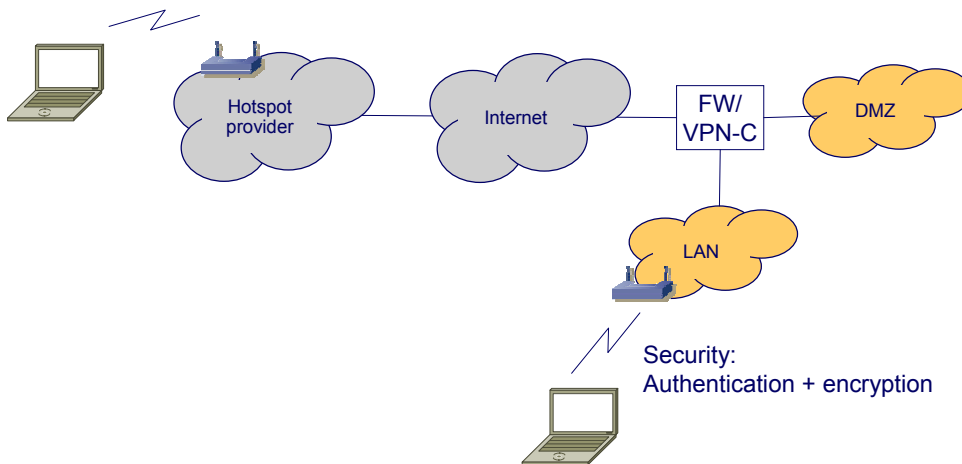
The wireless picture

- Virtual Private Network requires
  - VPN client software
  - VPN concentrator at enterprise side



The wireless picture

Security:  
Authentication



The wireless picture



© 2005, Telinous High-Tech Institute

## Hacking into WEP



## Employees



## "War Driving"

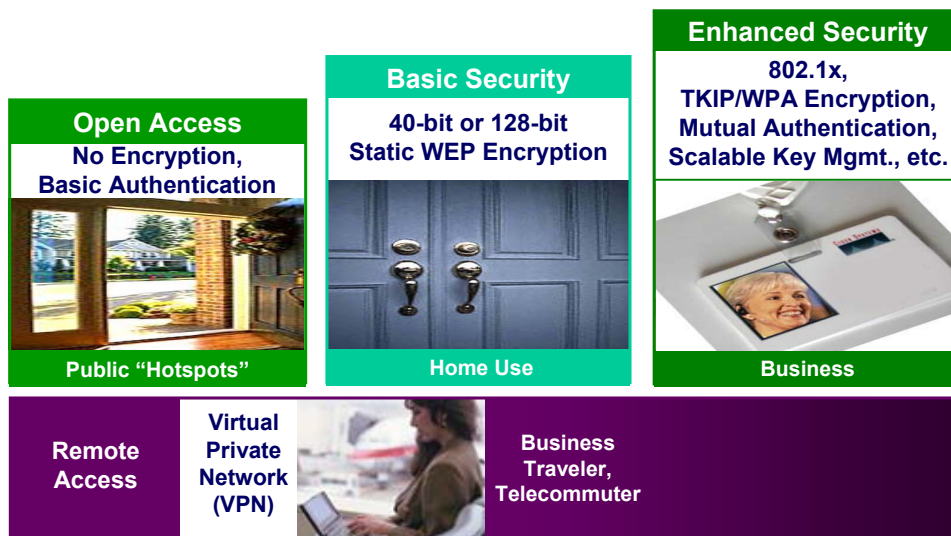
Credit: KNTV San Jose



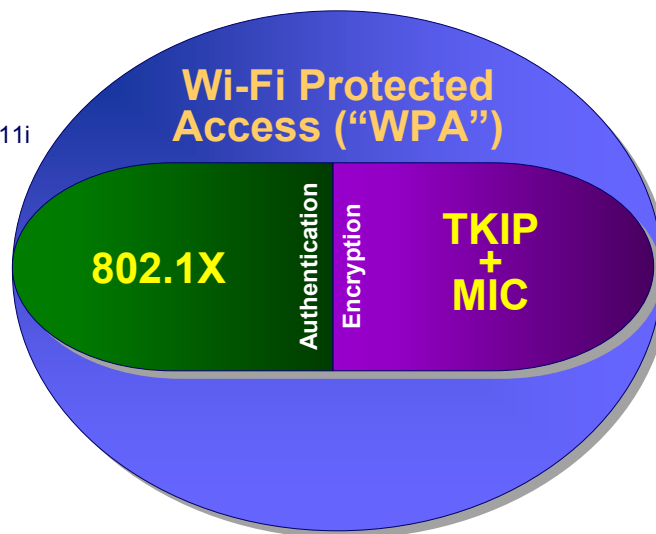
The wireless picture



© 2005, Telinous High-Tech Institute



- WPA (subset 802.11i)
  - 802.1x + TKIP + MIC
- WPA2
  - Aligned with final 802.11i (expected mid '04)
  - 802.1x + AES + MIC



### Remote Access



Dialing into Corporate Network from Home, Hotel, Airport, etc.



**VPN is the Best Solution!**

### On-Campus Access



Accessing Corporate Network while inside the Enterprise



**VPN may not be the Best Answer**

#### VPN/WLAN On Campus – Pros

- **Familiar**  
Is in use at most enterprises  
Makes user interface consistent for both WLAN & remote access
- **Trusted for authentication & privacy**  
Supports central security management  
Ensures 3DES encryption from client to concentrator
- **Compatible with wide range of client devices from multiple vendors**  
The wireless picture

#### VPN/WLAN On Campus – Cons

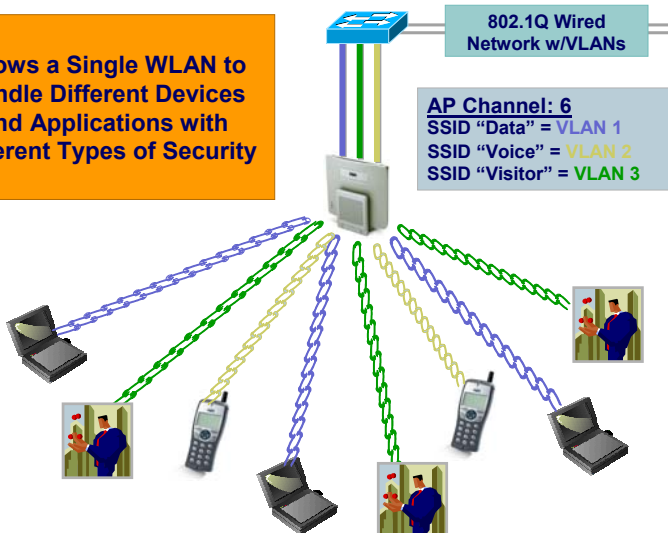
- **Cost:** Requires VPN concentrators behind APs
- **Performance:** Client software encryption lowers throughput
- **Roaming:** Roaming between VPN concentrators forces application restarts
- **QoS:** All traffic is IPSec traffic; no QoS, multicast, or multiprotocol support
- **Client Devices:** Not supported on phones, scanners, or other specialized devices
- **Convenience:** Additional steps required beyond Windows login



**TELINUS**  
HIGH-TECH INSTITUTE

© 2001, Telinus High-Tech Institute

**Allows a Single WLAN to Handle Different Devices and Applications with Different Types of Security**



**SSID: Data**  
**Security:**  
PEAP + AES



**SSID: Voice**  
**Security:**  
LEAP + WPA



**SSID: Visitor**  
**Security:**  
Open

The wireless picture



**TELINUS**  
HIGH-TECH INSTITUTE

© 2001, Telinus High-Tech Institute

- Mutual authentication is vital for WLANs
- Use VPNs for remote access
- Remember to use Strong Passwords!
  - Prompt users to select new passwords every 3-6 months
  - Passwords should not contain real words, to protect against dictionary attacks
- Create a WLAN Policy for your organization
  - Employees should not install rogue AP's at work
  - Remind users to enable security on their home AP's (even basic WEP is better than nothing)

## Emerging technologies





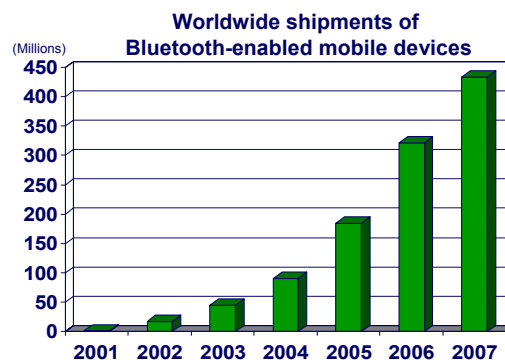
- Bluetooth technology
  - Low power, low cost
- Products
  - Cellular phones
  - Headsets
  - PDAs
  - Keyboards and mice

The wireless picture



© 2005, Telinus High-Tech Institute

- Nearly one fifth of the world's vehicles produced in 2008 will feature OEM-installed Bluetooth hardware (Source: ABI)
- Roughly 65% of Bluetooth-enabled devices are sold in Europe, 25% in Asia, and a paltry 10% in the United States.



Source: IDC, June 2003

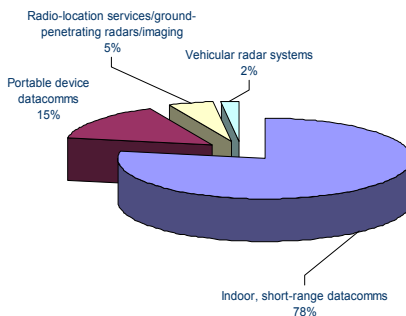
The wireless picture



© 2005, Telinus High-Tech Institute

- Developed by 802.15.3a
  - May impact the future market adoption of Bluetooth
- Two UWB standards proposals
  - Multi-band OFDM (MBOA) by Texas Instruments
  - Direct Sequence Spread (DSS) Spectrum by Motorola
  - Stalemate situation: A year delay in the standard may result
- Streaming video for the home consumer market appears to be the key market driver

**UWB Application Types Worldwide (2007 Estimate)**



Source: Wireless Oracle

The wireless picture



© 2005, Telinus High-Tech Institute

- Target applications for 802.15.3a
  - MPEG video transmission (see table)
  - A "Wireless 1394" or USB2.0

	Home Theatre	Portable
Characteristics	<ul style="list-style-type: none"> <li>Typically static, unmoving</li> <li>Medium/large cabinet size</li> <li>AC powered</li> <li>Require highest isochronous throughputs (e.g. HDTV)</li> <li>Require very high QoS (equivalent to wired QoS)</li> </ul>	<ul style="list-style-type: none"> <li>Applies to Portable devices used in or outside home</li> <li>Typically battery powered, but occasionally AC powered</li> <li>Small size [less display resltn]</li> <li>Highest speeds needed for asynchronous transfer rather than isochronous</li> </ul>
Examples	<ul style="list-style-type: none"> <li>Television</li> <li>Video recording device (PVR, VHS, DVD-R)</li> <li>Set-top Box, Media server</li> <li>Stereo audio player</li> <li>Surround sound audio</li> </ul>	<ul style="list-style-type: none"> <li>Video Camera</li> <li>Audio player (MP3, CD)</li> <li>Digital still camera</li> <li>Cellular phone</li> <li>Notebook PC</li> <li>PDA</li> </ul>

The wireless picture



© 2005, Telinus High-Tech Institute

- Low-cost, low-power, low-data rate, cable/wire replacement technology
  - Up to 75m range
  - Data rates of 250 kbps and 20 kbps
  - Multi-year battery life
  - Star topology, with peer-to-peer, supporting up to 255 devices per network
- IEEE 802.15.4 Standard
- Target applications
  - Home and building automation and controls
  - Consumer electronics
  - PC peripherals
  - Medical monitoring
  - Toys



- |  |   |
|--|---|
| <ul style="list-style-type: none"> <li>▪ ZigBee               <ul style="list-style-type: none"> <li>• DSSS, 2.4 GHz band</li> <li>• Smaller packets over large network</li> <li>• 250 kb/s data rate</li> <li>• 30 m range</li> <li>• 255 devices per network</li> <li>• Non-rechargeable battery</li> <li>• Mostly static networks with many, infrequently used devices</li> <li>• Home automation, toys, remote controls, etc.</li> </ul> </li> </ul> | <ul style="list-style-type: none"> <li>▪ Bluetooth               <ul style="list-style-type: none"> <li>• FHSS, 2.4 GHz band</li> <li>• Larger packets over small network</li> <li>• 1 Mb/s data rate</li> <li>• 10 m range</li> <li>• 8 devices per network</li> <li>• Rechargeable battery</li> <li>• Ad-hoc networks</li> <li>• Hands-free audio, cell phones, headsets, PDAs, etc.</li> </ul> </li> </ul> |
|--|---|

- MAN = up to 50km/31 miles
- Last mile solution for broadband...
  - Both licensed and unlicensed spectrum used (10-66 Ghz and 2-11Ghz)
  - QoS for voice and video
- Intel and Alvarion working on silicon for WI-MAX (16a); 30 miles / 70Mbps max

Technology	Freq. Band	Distance	Speed	Features
802.16	10-66 Ghz	31 miles	70 Mbs	Requires Line-of-Sight (approved 2002)
802.16a	2-11 Ghz	31 miles	70 Mbs	No line-of-sight req'd (approved Mar03)

Intel promises WiMax versions of Centrino for 2004  
 Nokia will launch a WiMax cell phone in 2005

- Wireless LAN is a well developed standard
  - Security issues have been solved
  - QoS is being offered
- Additional technologies start to appear
  - Wireless PAN (Bluetooth, UWB, Zigbee)
  - Wireless MAN (Wi-MAX)
- Training @ THTI is available to help you see the wood for the trees

- Several courses
  - Wireless communications overview
  - Wireless LAN essentials
  - GSM essentials
  - GPRS essentials
  - UMTS essentials
  - UMTS advanced
  - Several security courses
- More info can be found on [www.thti.telindus.be](http://www.thti.telindus.be)
  - Course contents
  - Dates