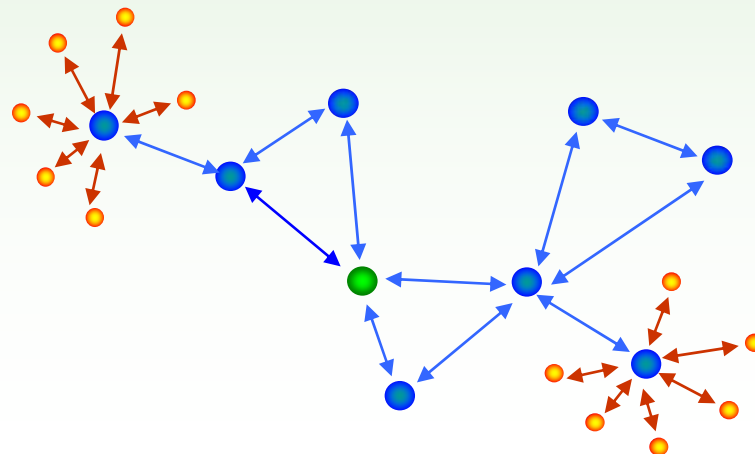




Emerging Wireless Technologies for the Internet of Things

Jacob Sharony, Ph.D., MBA
CEWIT, Director Network Technologies Division

LISTnet, October 14, 2008

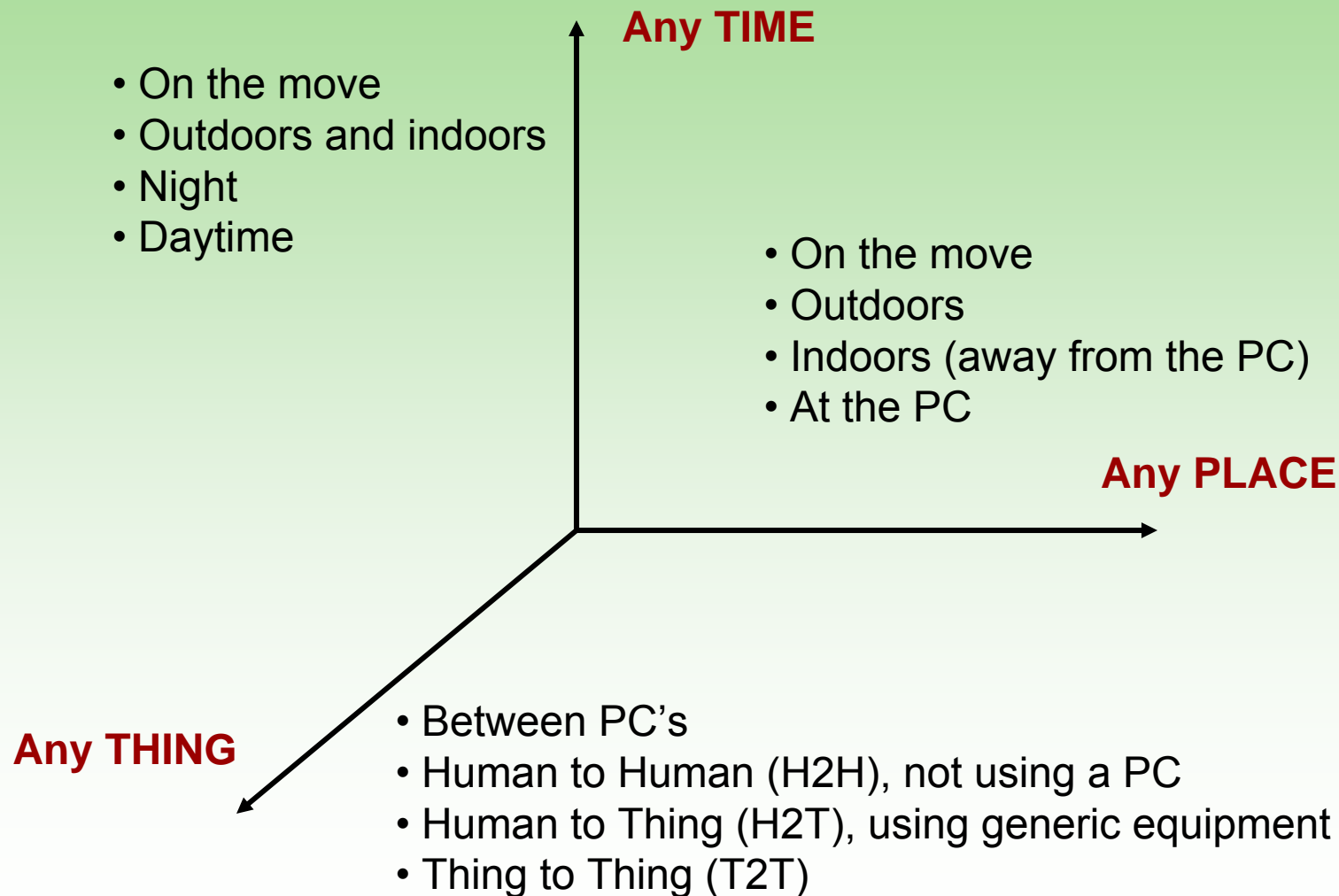


The “Vision”



networked physical world

A New Dimension



Total Enterprise Visibility

seeing what is not visible

What do we have?

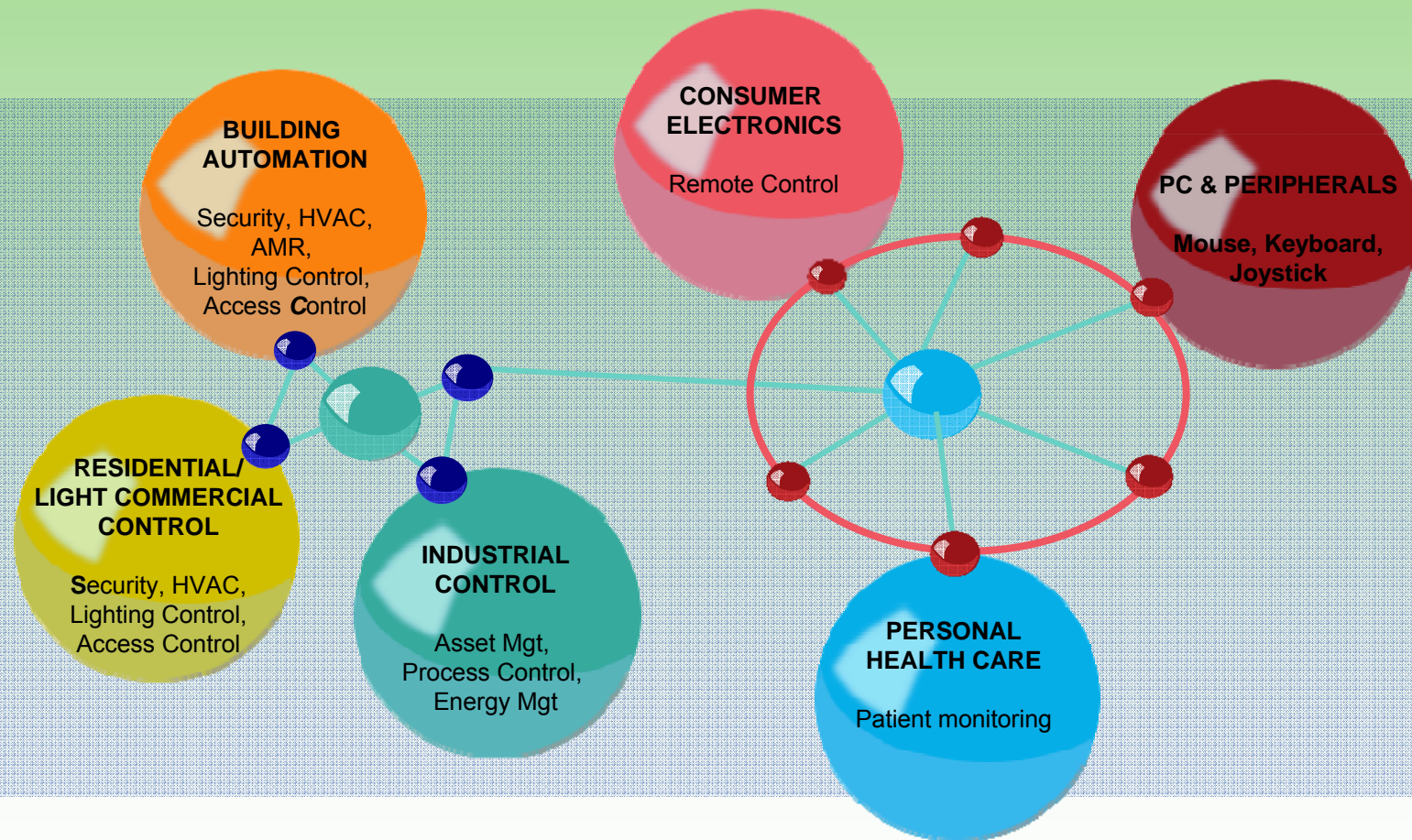
How many do we have?

Where is it?

What is its status?

- To be more efficient, cost effective and responsive → competitive
- No one wireless technology could provide end-to-end solution

Wireless Markets and Applications



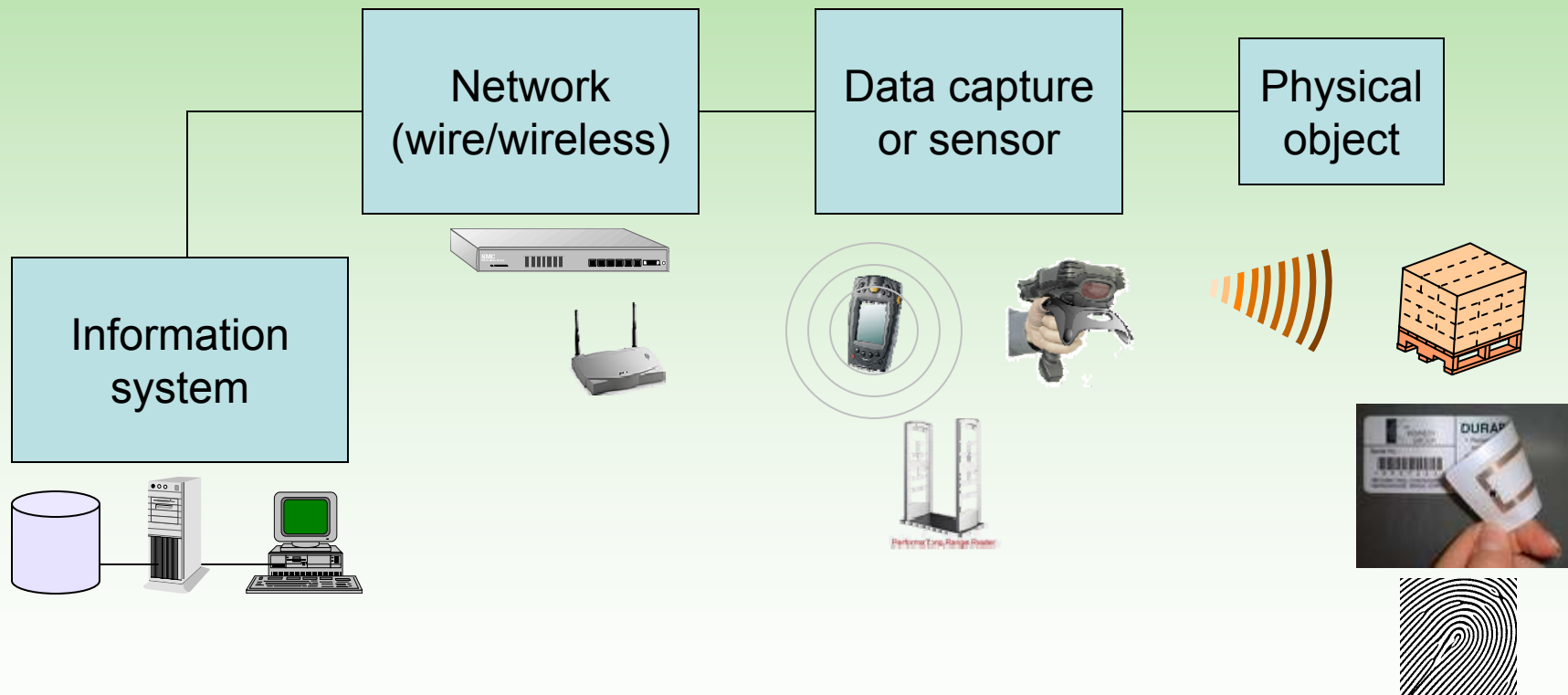
Hospitals order 30% more equipment because they never find where it is...

Capture, Move and Manage (cm²) Architecture

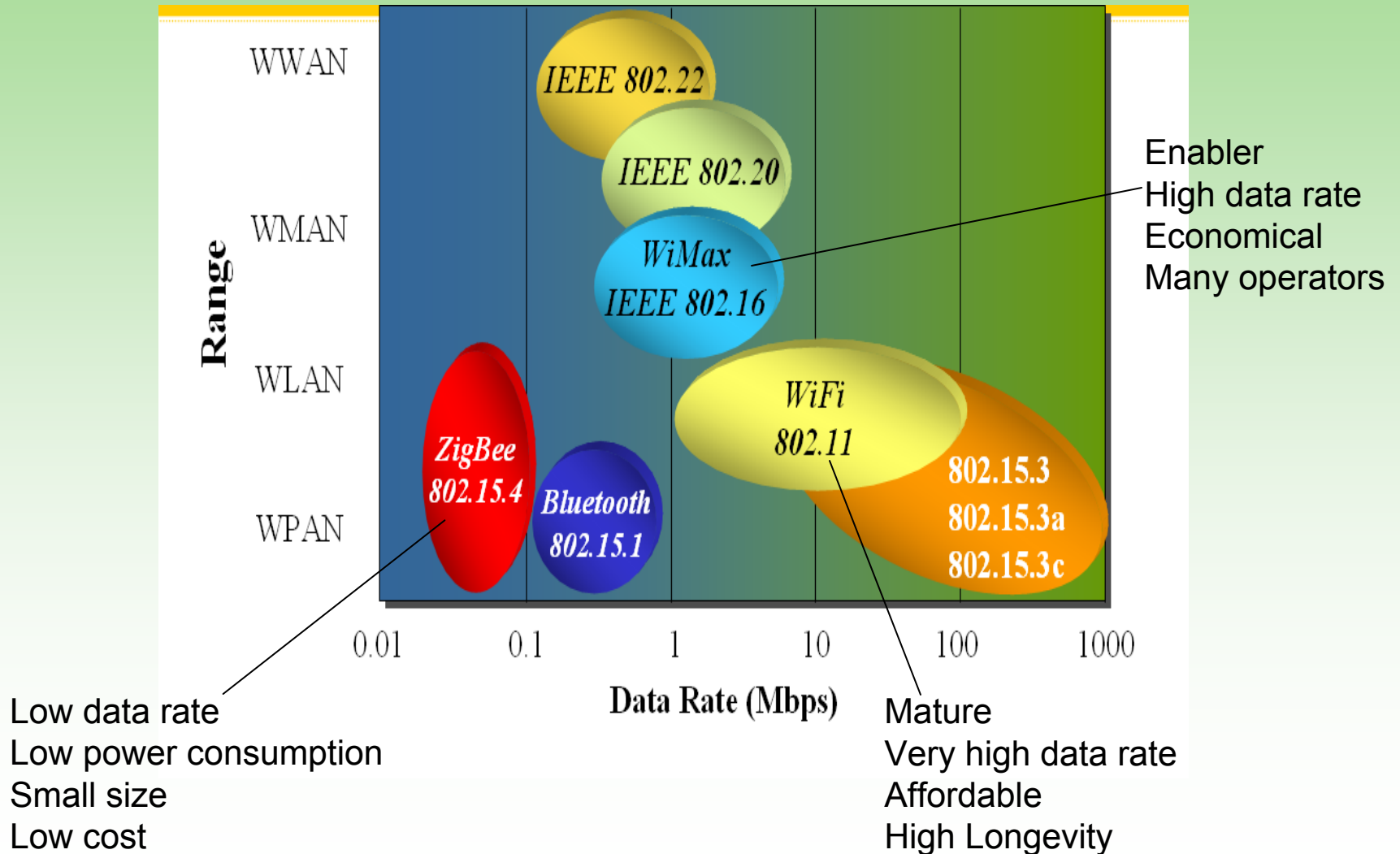
- Technologies and networks connecting *physical objects* to *information systems*
- No one architecture fits all
 - Depends on geographic location/terrain/site layout
 - Availability of backhaul technology
- ***Data capture technologies***
 - RFID
 - ZigBee-based wireless sensors
- ***Wireless transport system/networks***
 - ZigBee mesh networks
 - WiFi – 802.11a/b/g/n
 - WMAN/WWAN (WiMAX, 3/4G)

cm² System Architecture

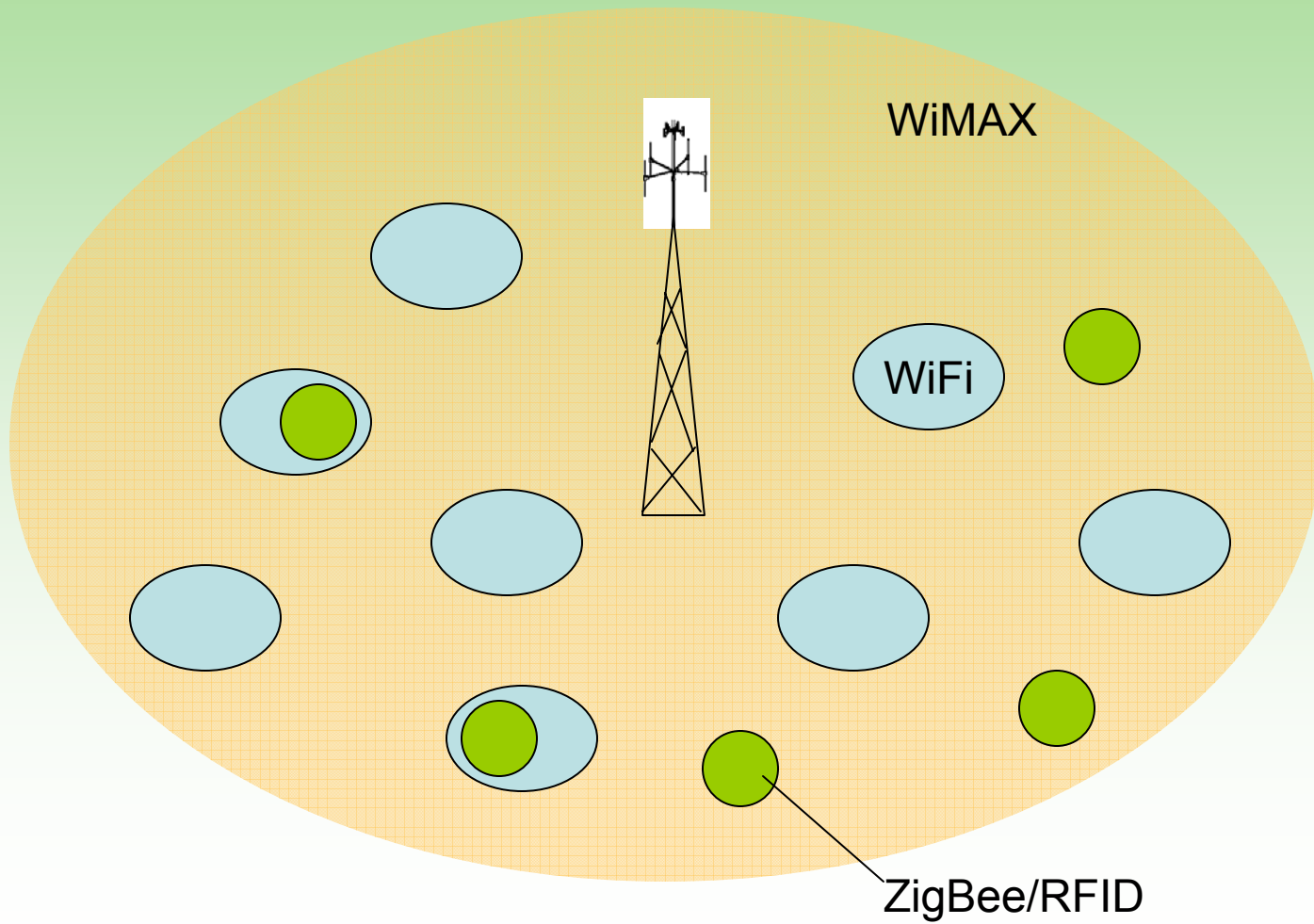
Connecting physical objects (atoms) to information systems (bits)



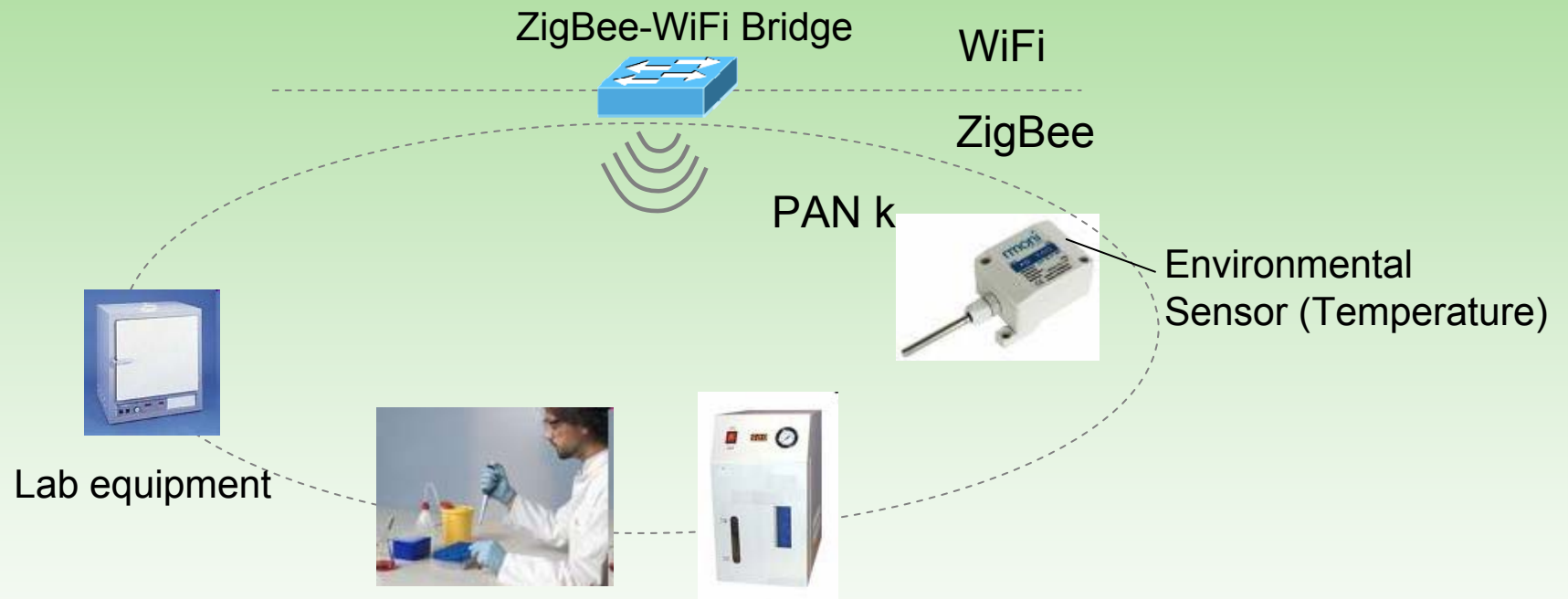
The 802 Wireless Space



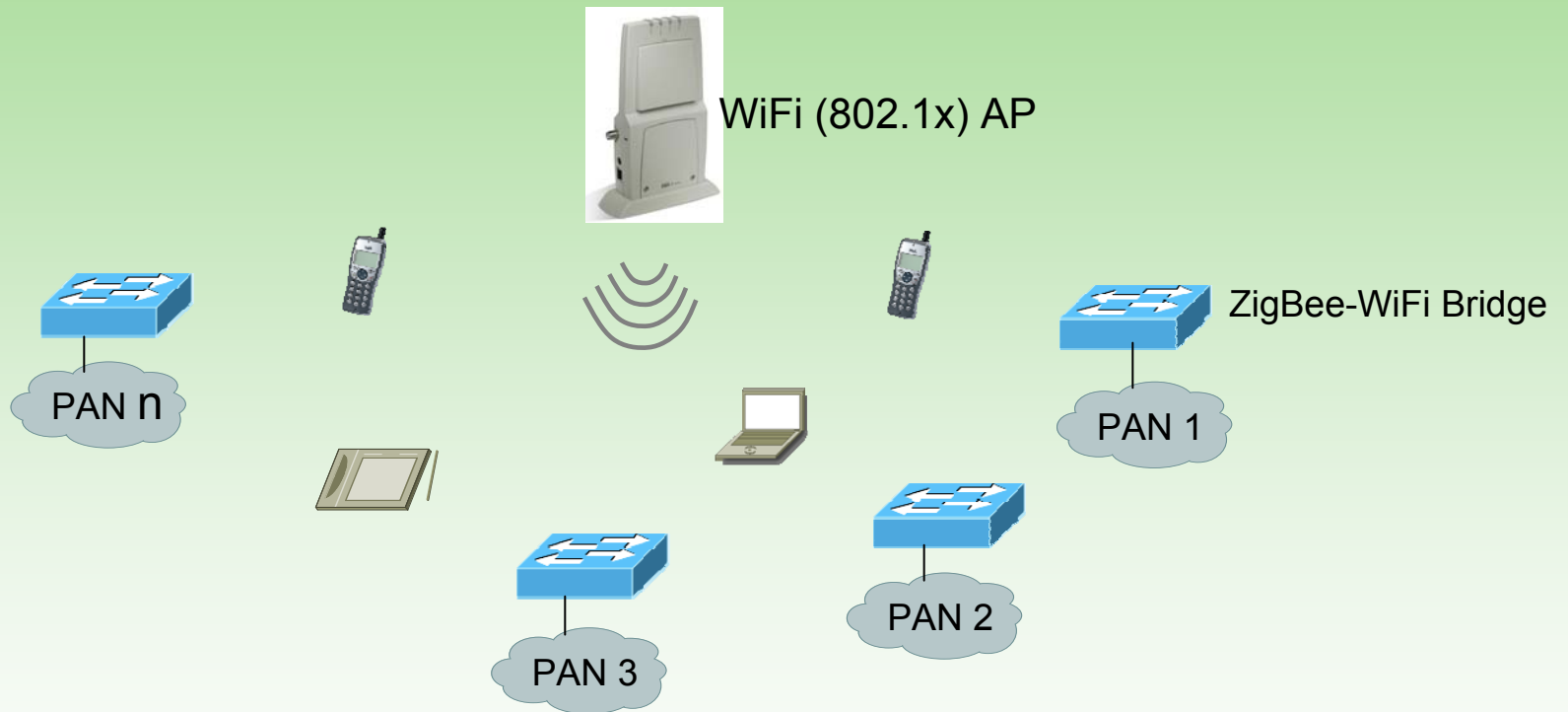
WiMAX-WiFi-ZigBee-RFID



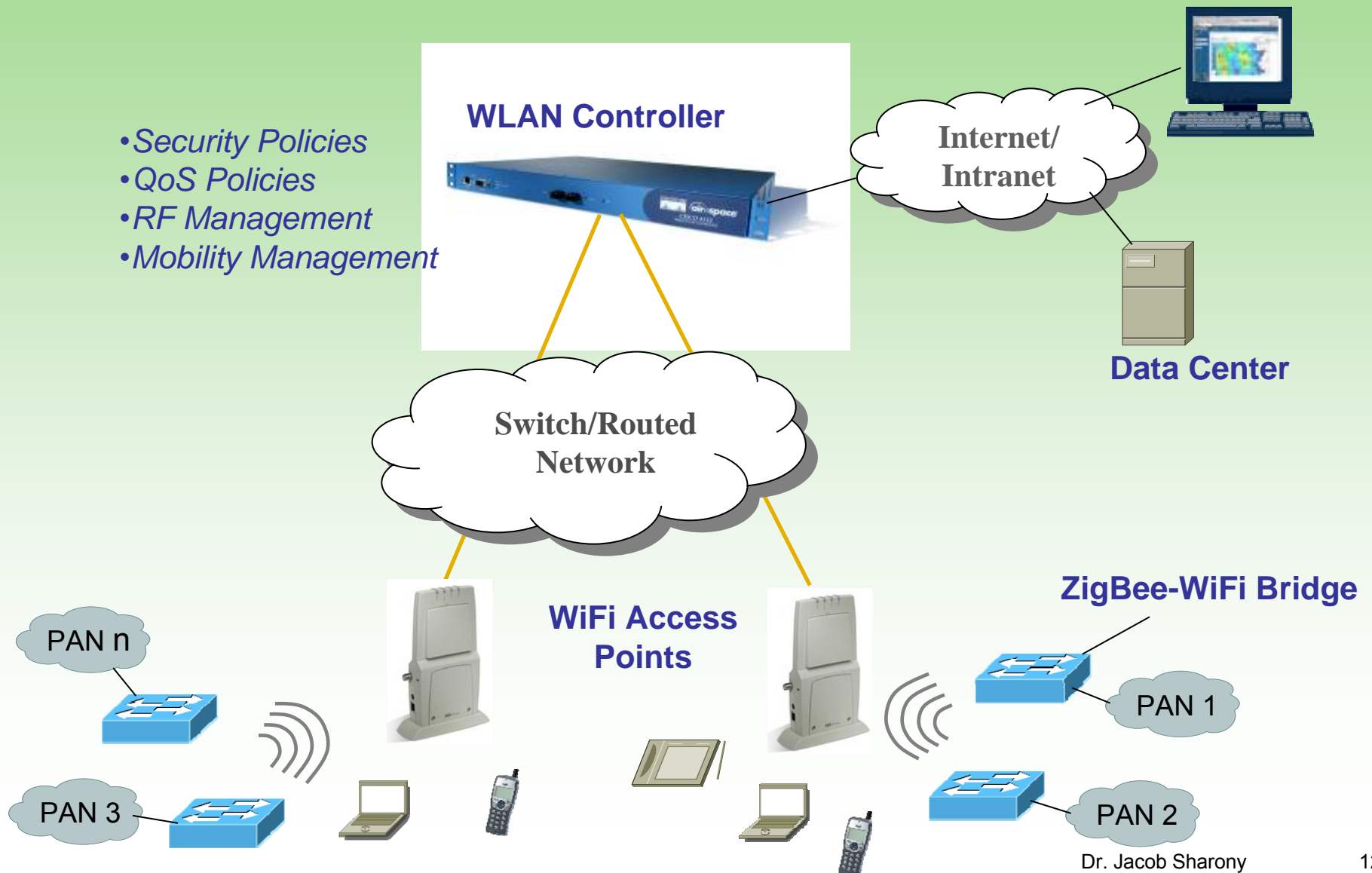
Data Capture Network (802.15.4)



Transport Network (802.11x)



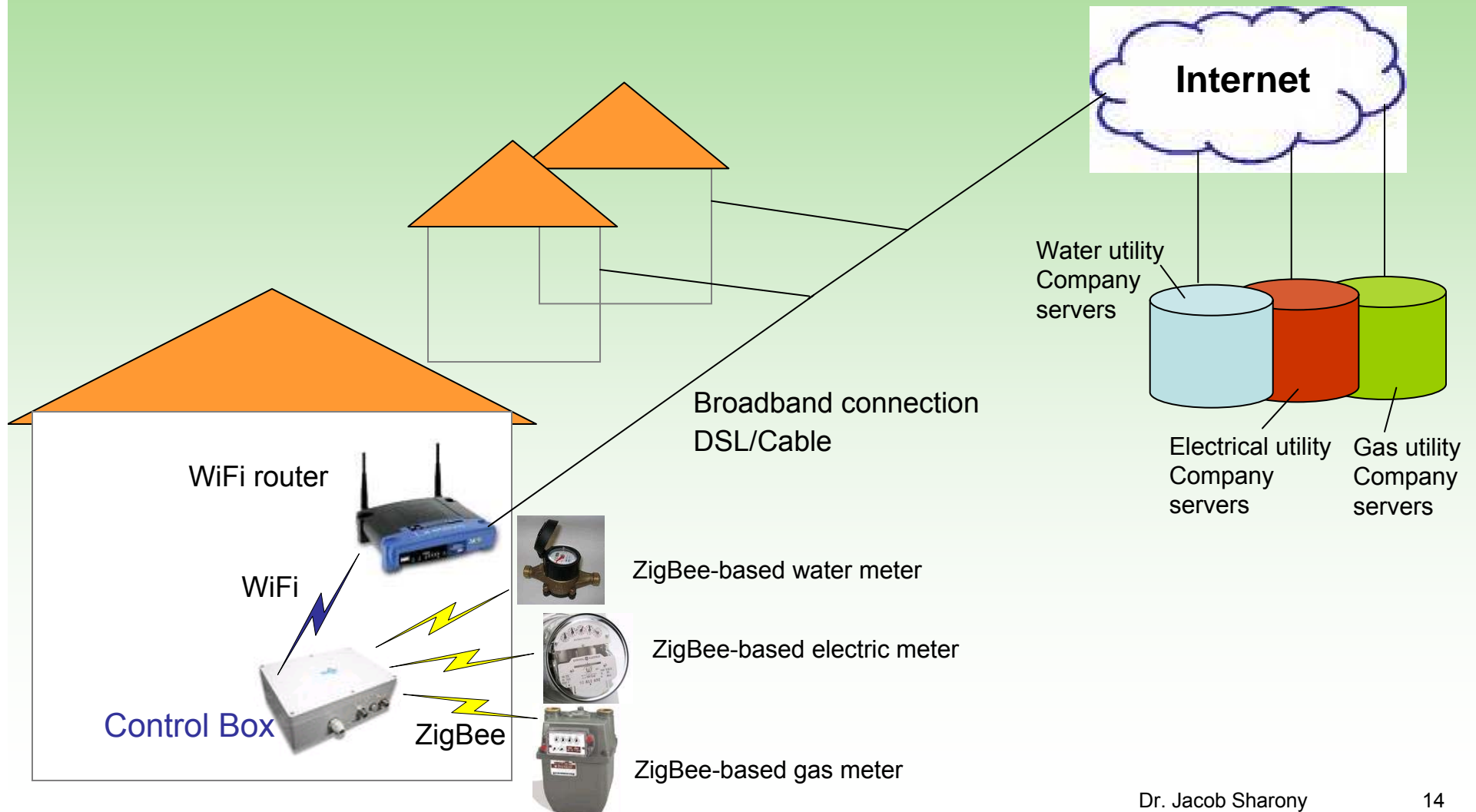
System Network Architecture



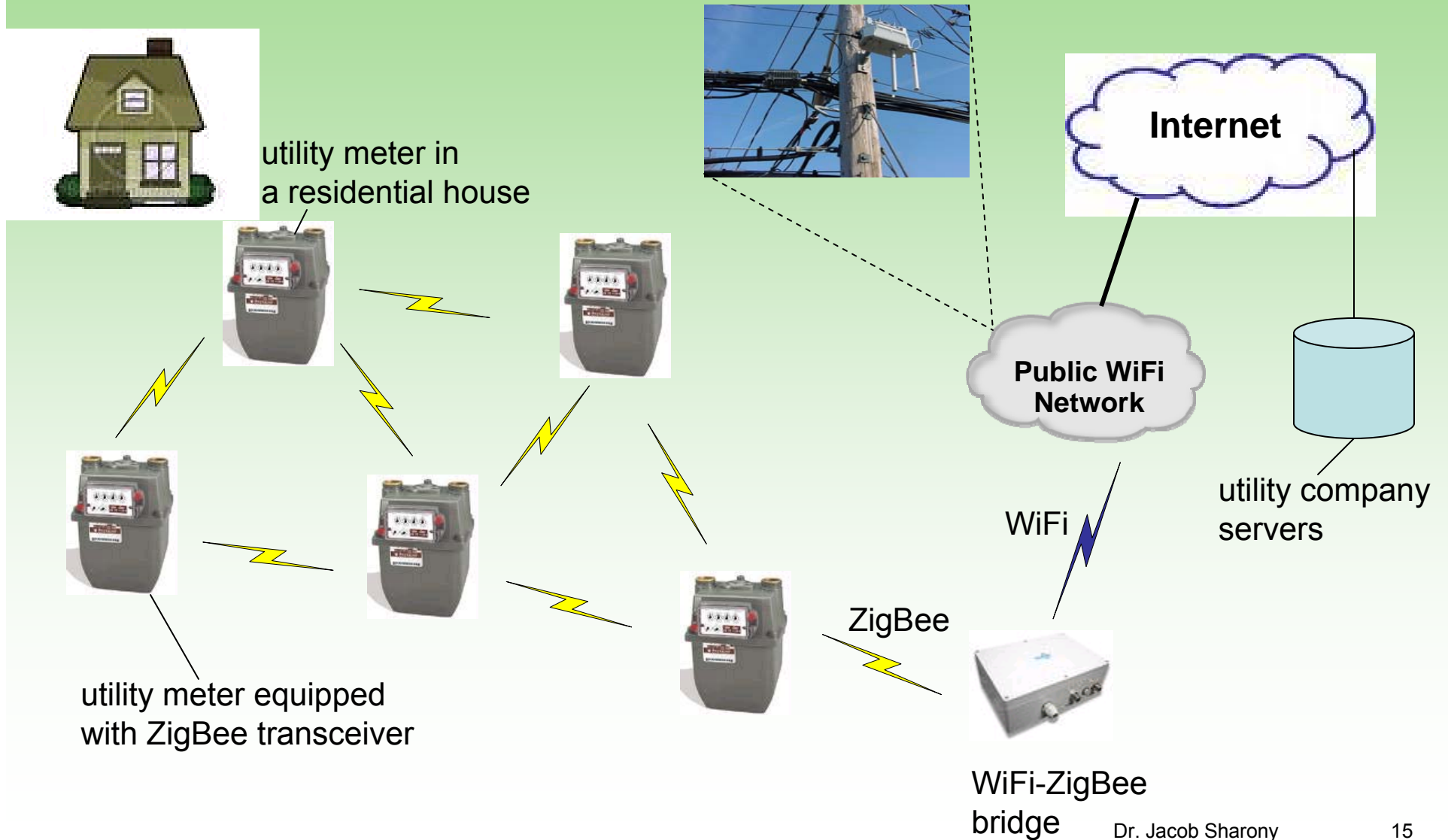
Main Challenges

- Network Scalability
- Data filtering at the edge
- Management/control
- Location accuracy
- Minimal power consumption
- Security and Privacy

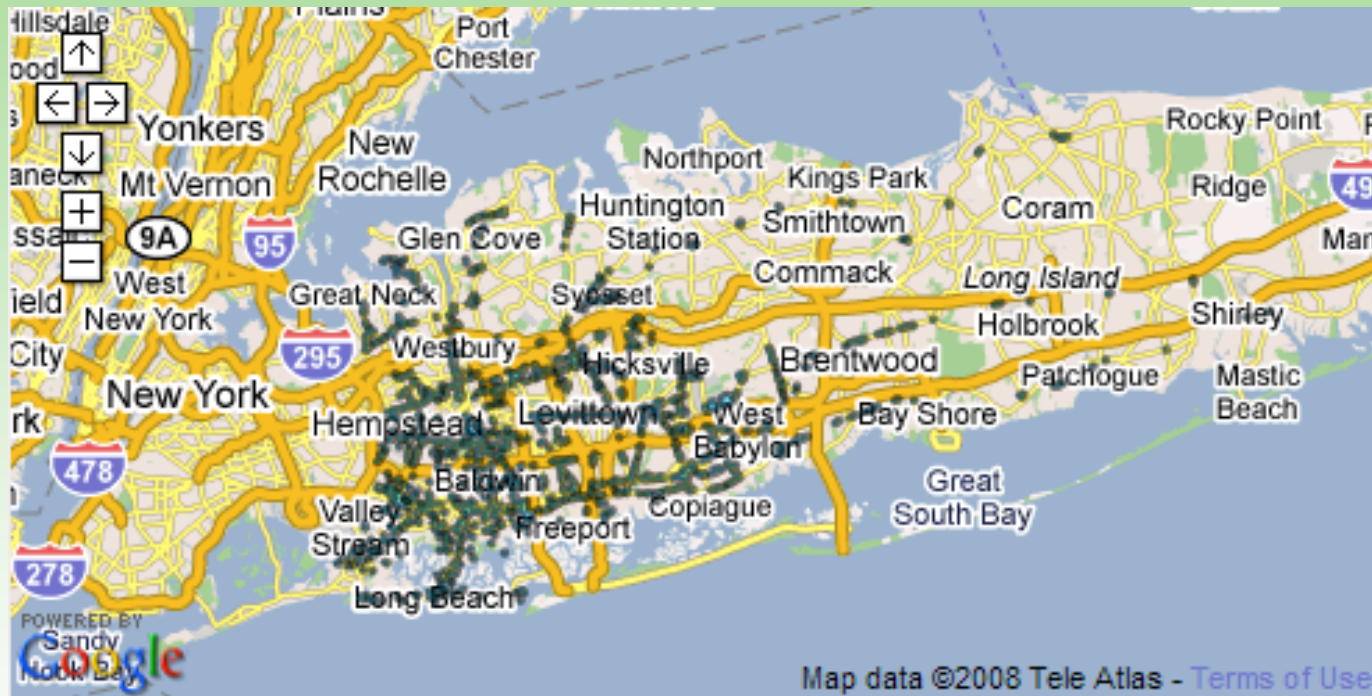
Energy Efficient Utility Monitoring/Metering System Architecture



ZigBee-based Mesh Architecture for AMR



WiFi in Long Island



Example of a project (cont.)

Wireless Meter Reading



Example of a project (cont.)

Wireless Meter Reading

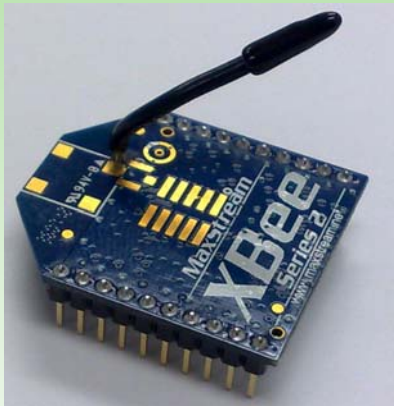


Example of a project (cont.)

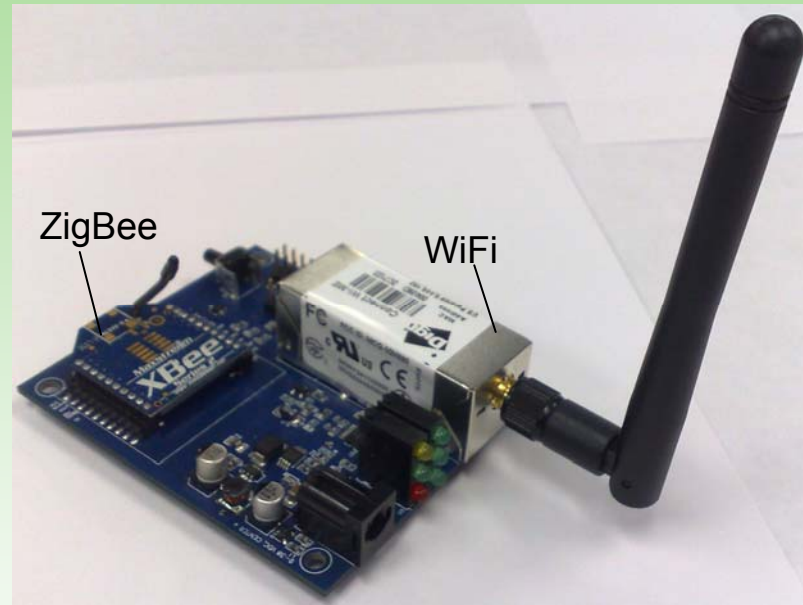
Wireless Meter Reading



ZigBee Devices/Components

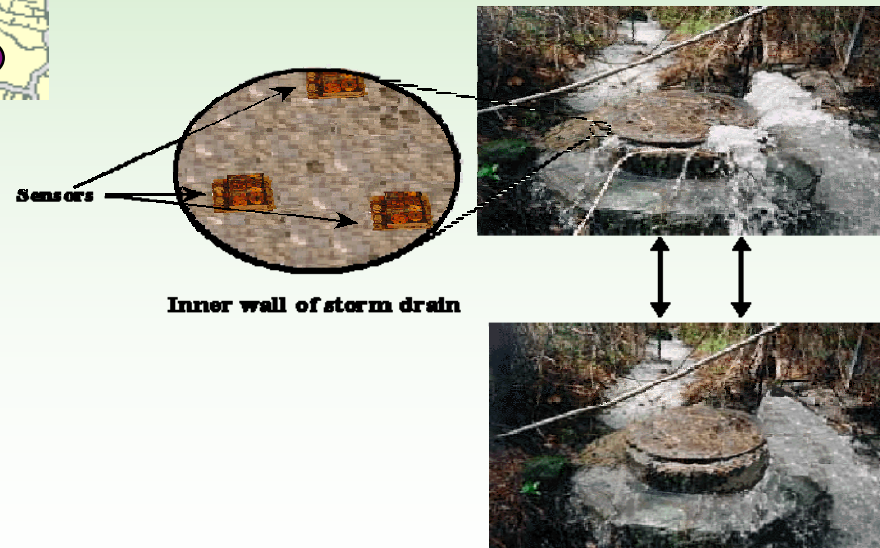


ZigBee Transceiver

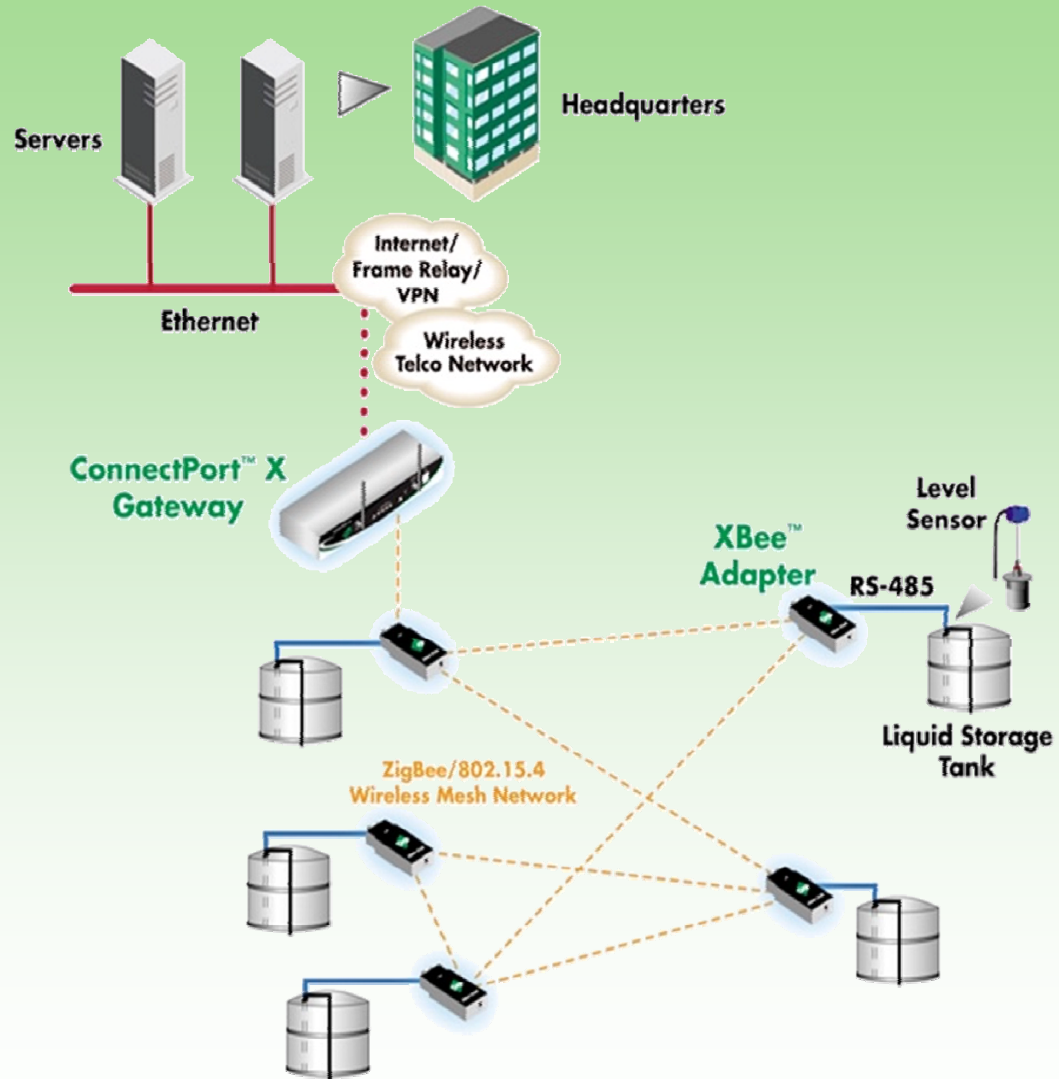


ZigBee to WiFi Bridge

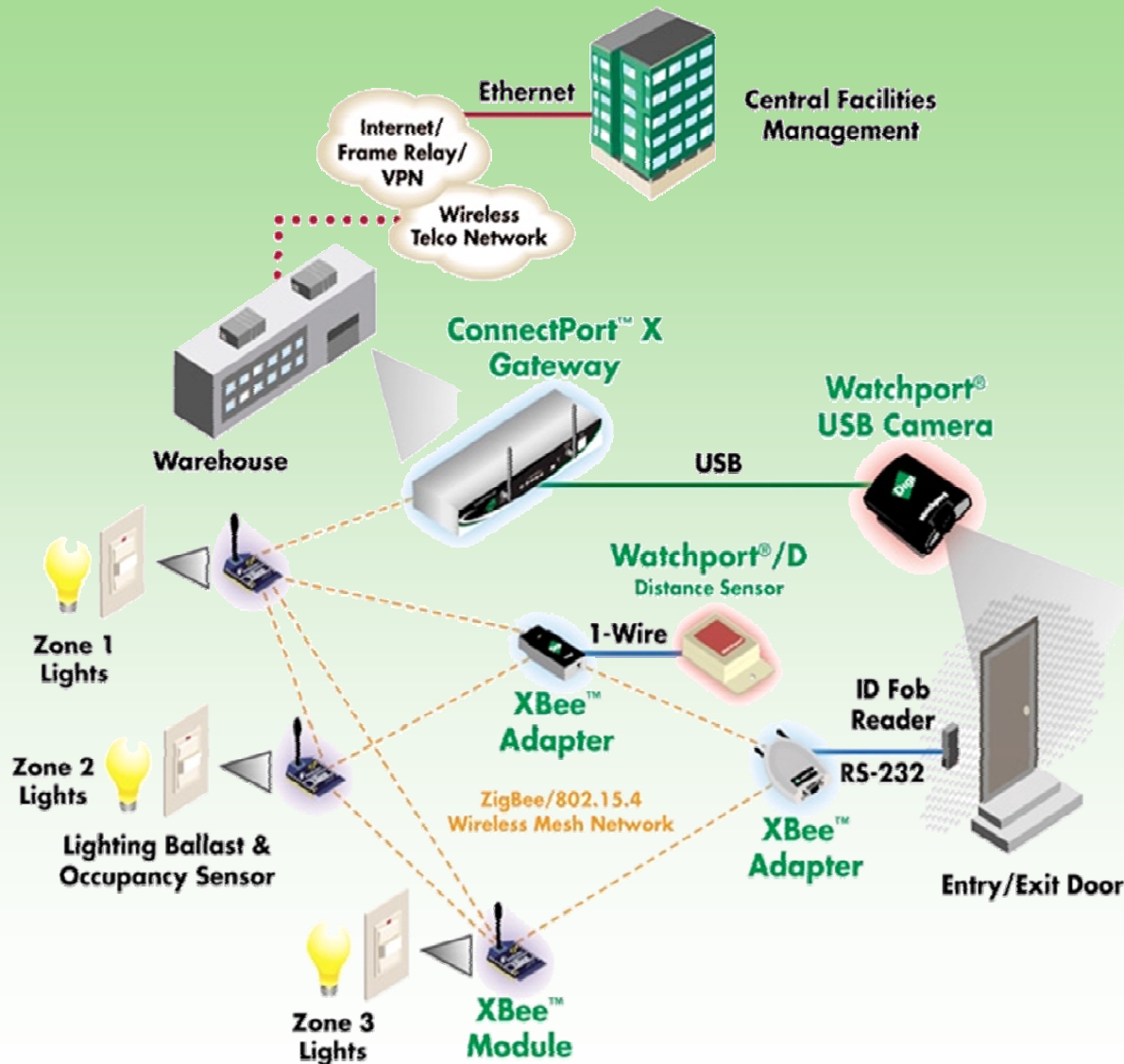
Transportation and Urban Monitoring



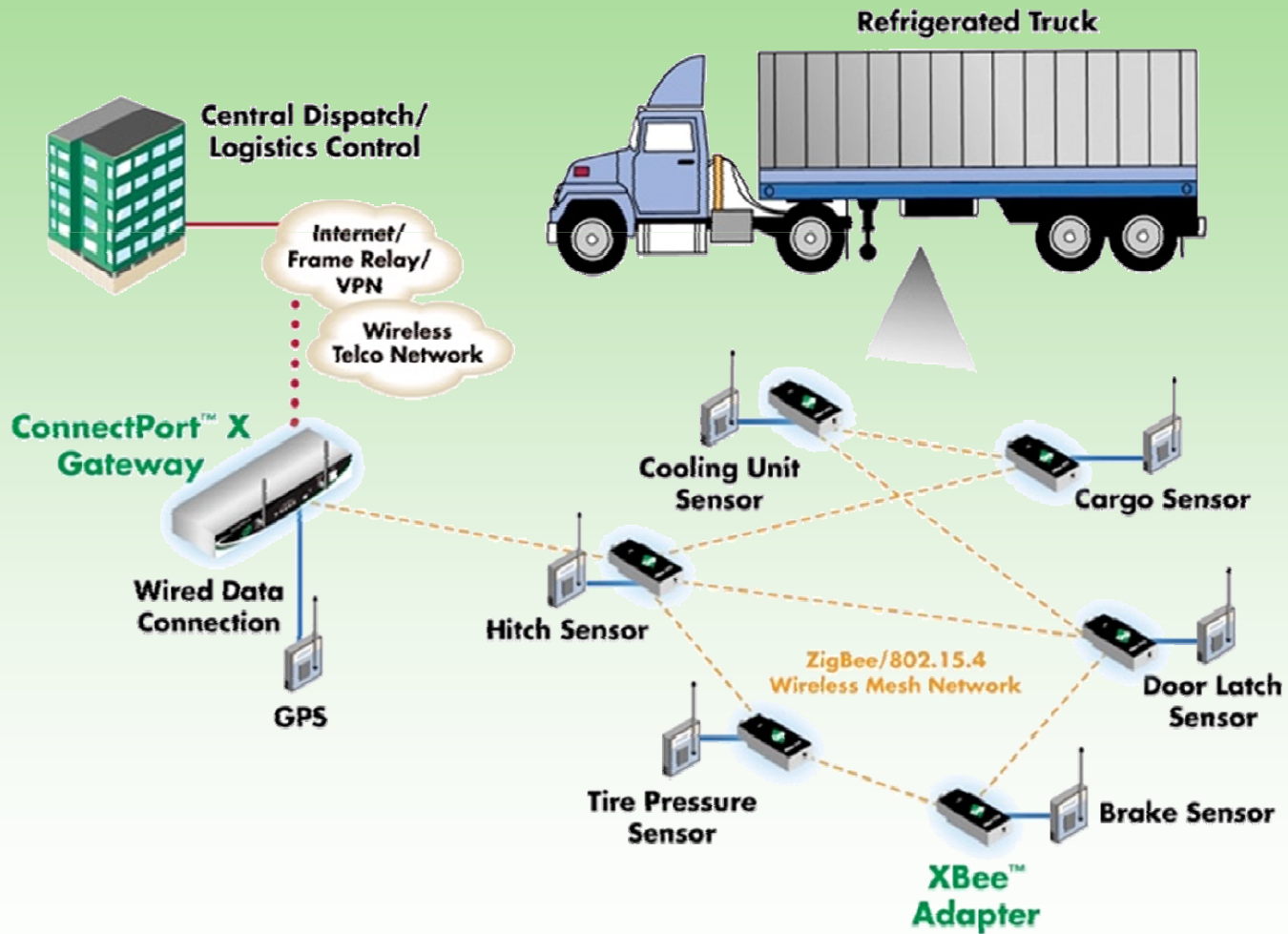
Tank-Level Monitoring



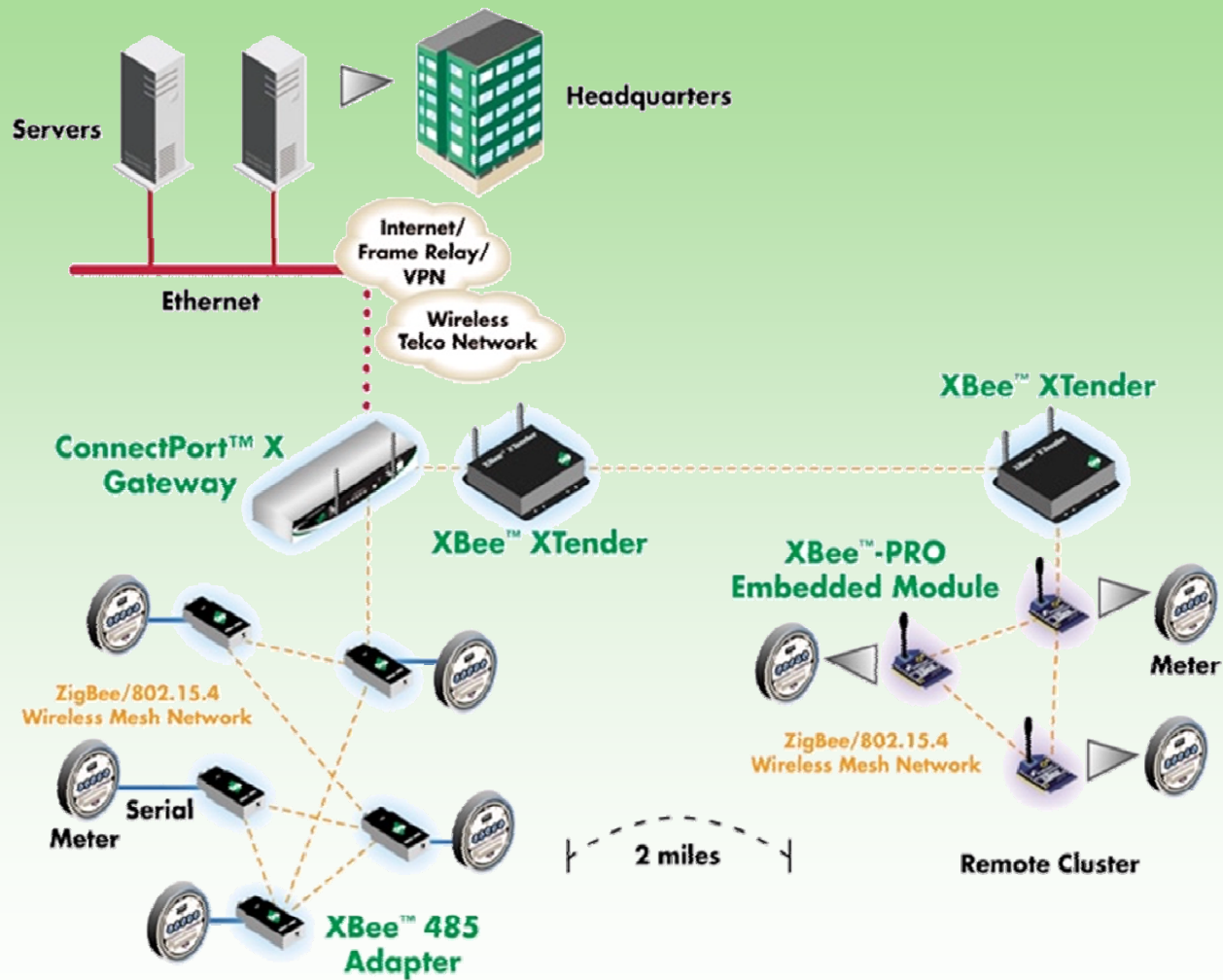
Building Control/Automation



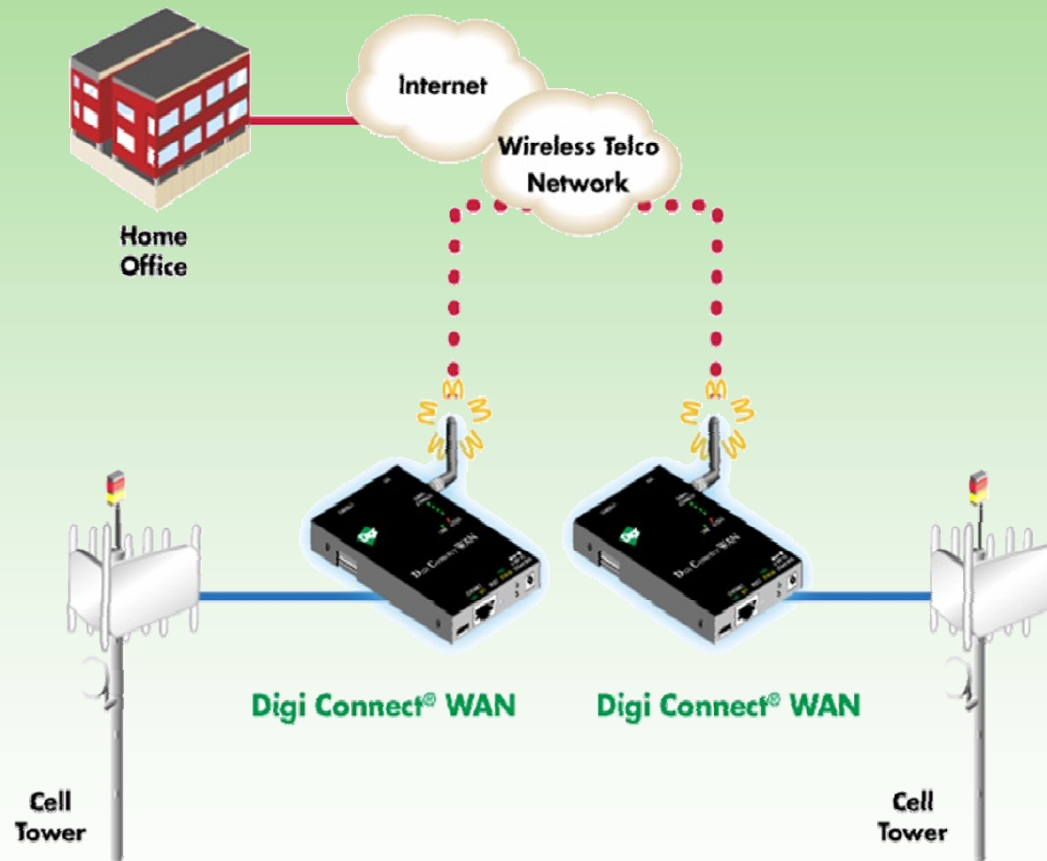
Supply Chain Management



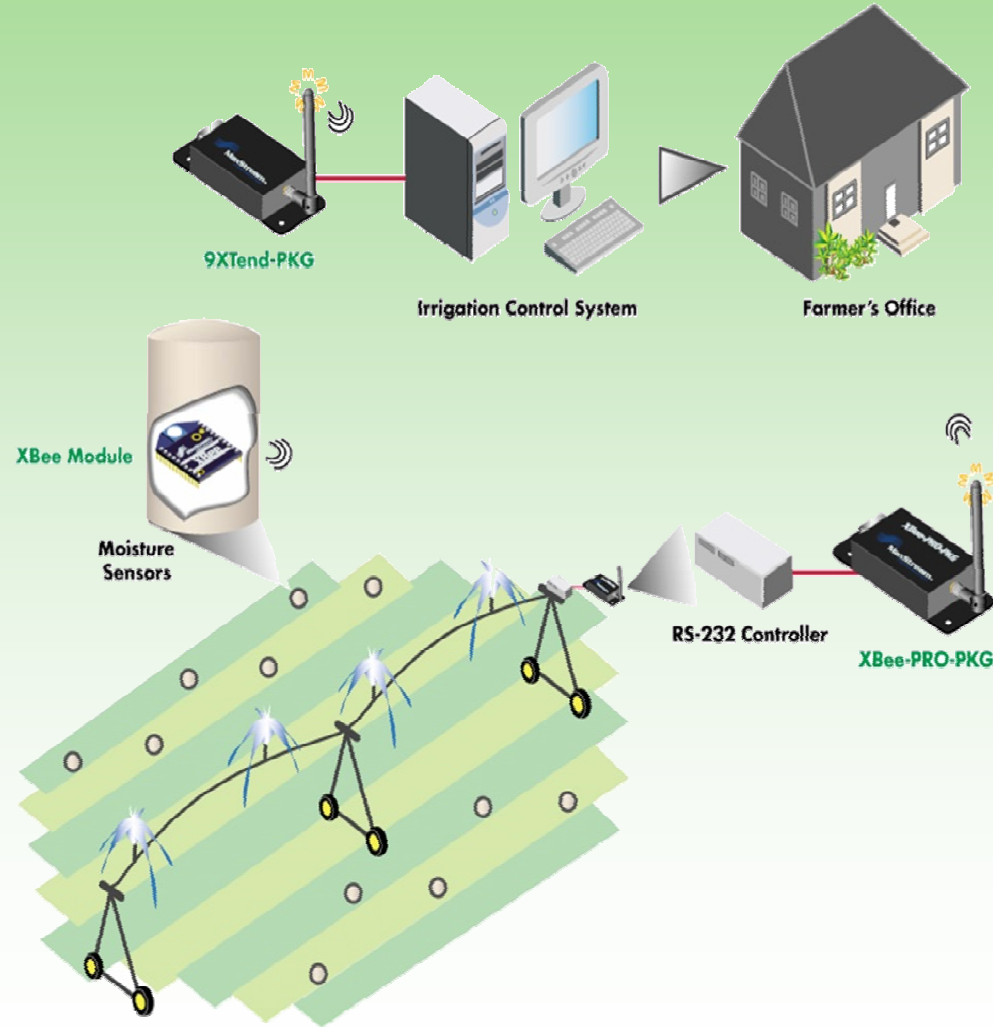
Automated Meter Reading



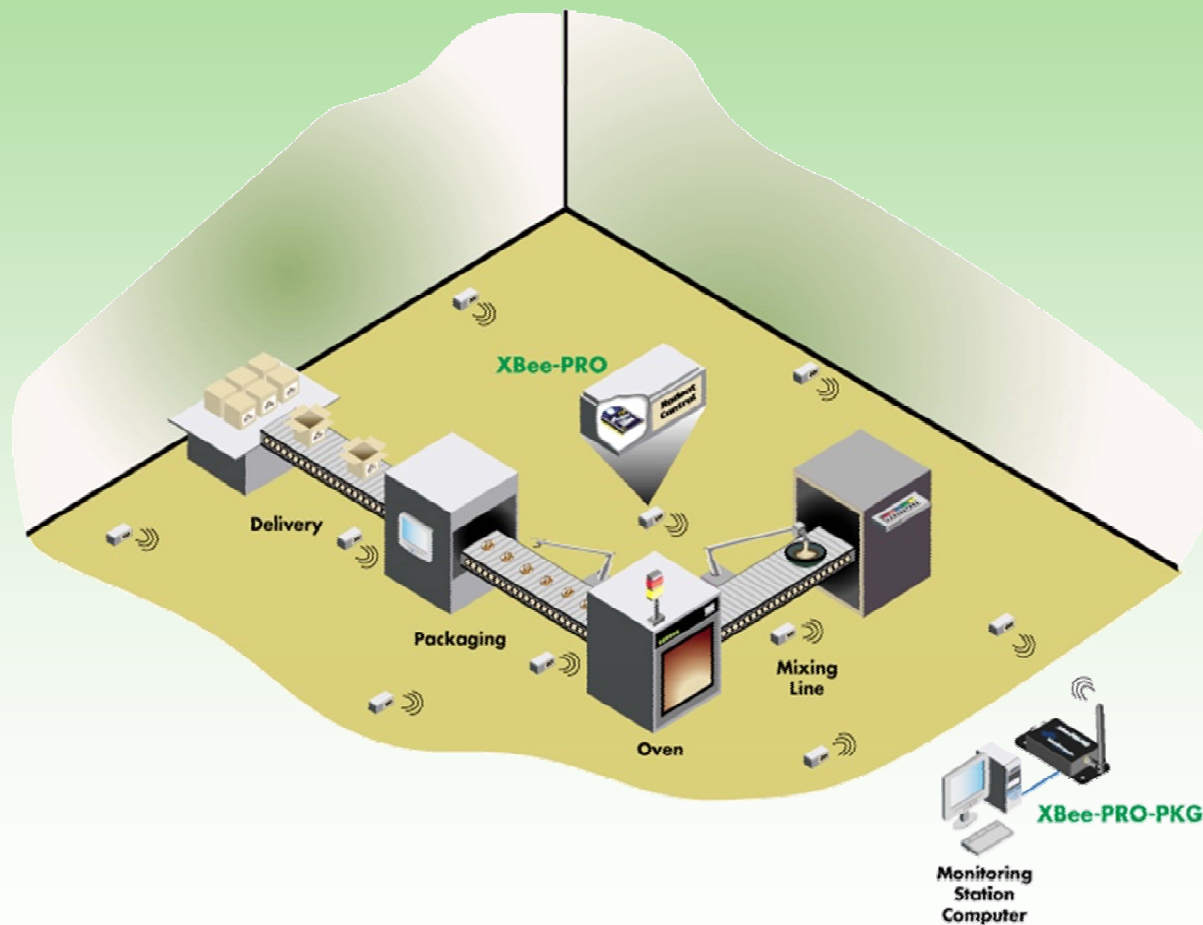
Cell Tower Remote Monitoring & Control



Irrigation System Remote Monitoring & Control



Even...Building a Better Mousetrap Remote Monitoring & Control



What is U-City?

Ubiquitous City

- "U-city" refers to an envisioned **futuristic** city that aims at offering a high quality of life for residents in terms of security, welfare and technology among others.
- It will be achieved by integrating IT infrastructure and ubiquitous information services into urban space. Ubiquitous information services refers to **seamless, wireless access from anywhere**.
- Applied technologies involve broadband convergence network, radio frequency identification, ubiquitous sensor network, home networking, WiBro, digital multimedia broadcasting, telematics, geographic information system, location based system, smart card system and video conference technologies, etc.

Songdo City, So. Korea




- ~ \$35B investment to build a new city from the ground up packed with wireless sensor technology
- 1500 Acre (6,000,000 sq meters)
- 65,000 residents
- Real city with all services (e.g., banks, shops, airport)

http://www.songdo.com/Uploads/DocumentRepository/songdo_medium.html

<http://www.songdo.com>

Main Wireless Technologies

- Radio Frequency Identification (RFID)
 - Real Time Location Systems (RTLS)
 - Wireless sensor networks (ZigBee / 802.15.4)
 - WiFi (802.11a/b/g/n)
 - WiMAX (802.16x) / 4G
- 
- main focus

RFID

Bar Codes and Common Applications



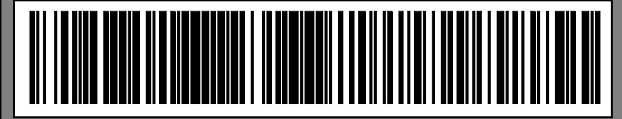
U.P.C.



Point-of-Sale
Shelf Labels



Code 128



UN 123456789 A2B4C6D8E

ID Verification



PDF417



Warehousing

Data Matrix



T & L



Code 39



421411371110780

Part Marking
Inventory
Sortation

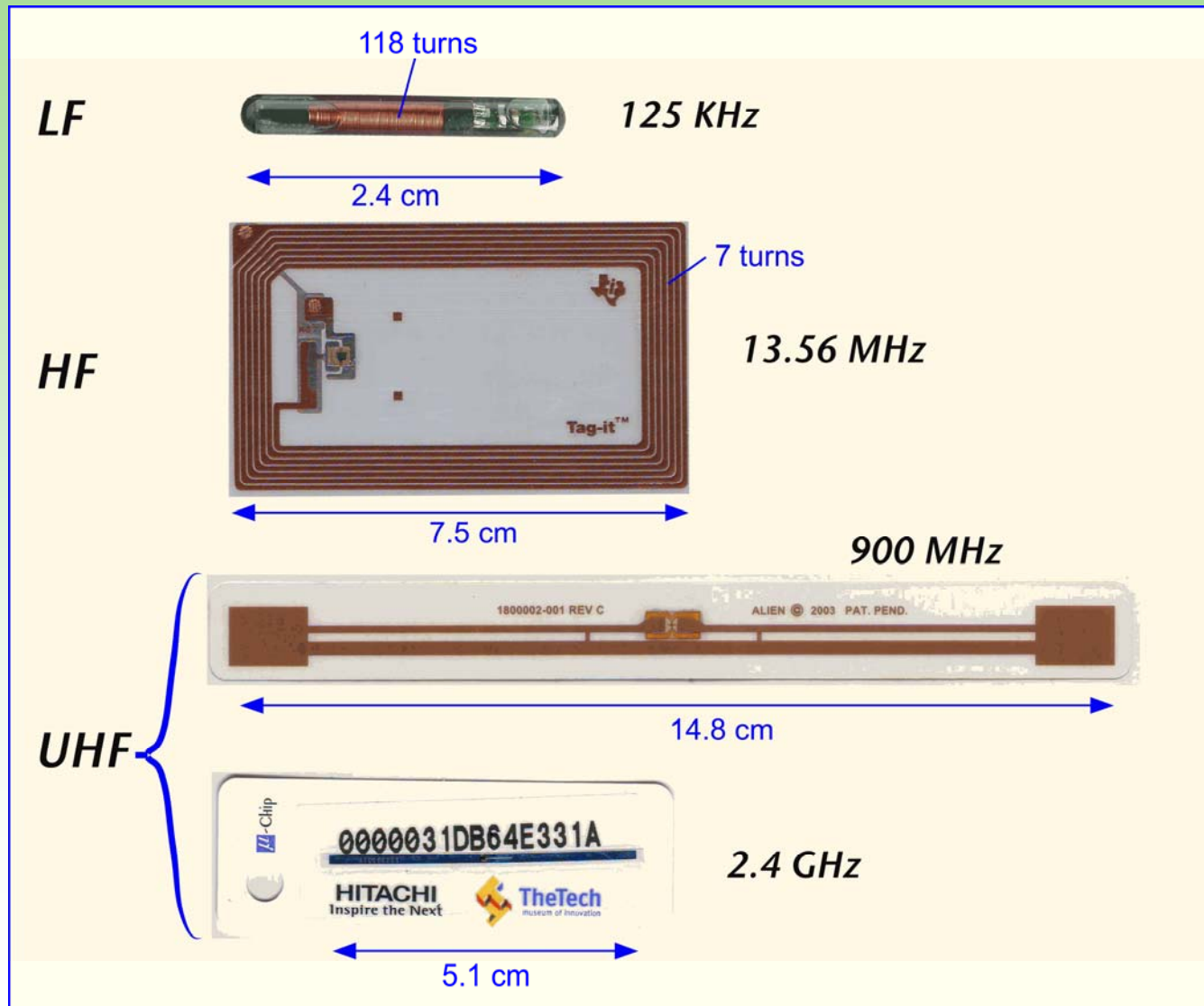


I 2 of 5



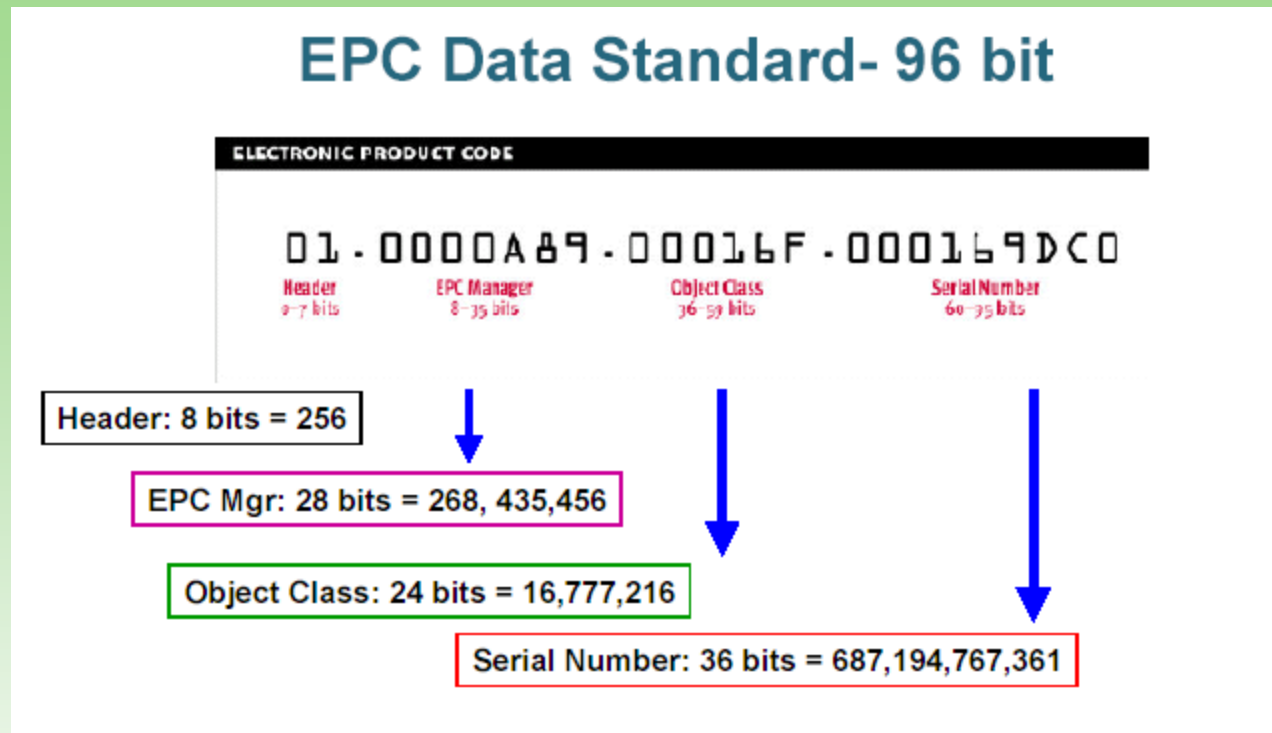
3 00 12345 67890 6

RFID



Electronic Product Code

EPC Data Standard- 96 bit



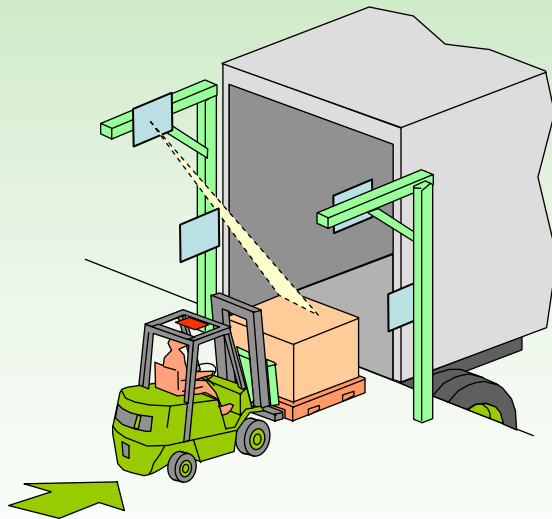
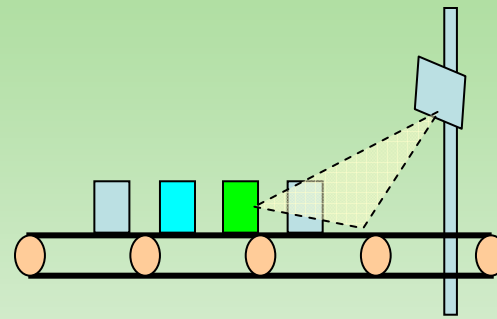
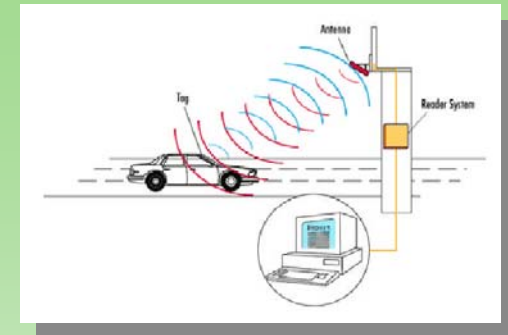
Header - Tag version number
EPC Manager - Manufacturer ID
Object class - Manufacturer's product ID
Serial Number - Unit ID

With 96 bit code, 268 million companies can each categorize 16 million different products where each product category contains up to 687 billion individual units

Note: 64 bit versions also defined, 256 bit version under definition

Radio Frequency Identification

- Tag wirelessly sends bits of data when it is triggered by a reader
- Power source not required for passive tags... a defining benefit
- Superior capabilities to barcode:
 - Non Line of Sight
 - Hi-speed, multiple reads
 - Can read *and* write to tags
 - Unit specific ID



Four main frequencies:

	Frequency	Distance	Example Application
LF	125khz	Few cm	Auto-Immobilizer
HF	13.56Mhz	<1m	Building Access
UHF	900Mhz	~7m	Supply Chain
μwave	2.4Ghz	1m	Traffic Toll

Types of Tags

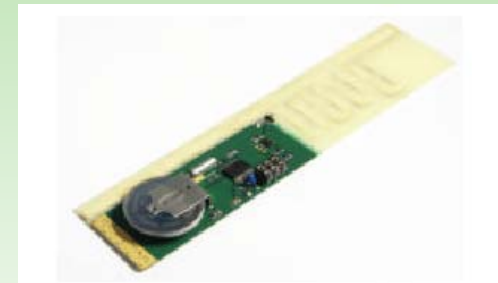
– Passive

- Operational power scavenged from reader radiated power



– Semi-passive

- Operational power provided by battery



– Active

- Operational power provided by battery - transmitter built into tag

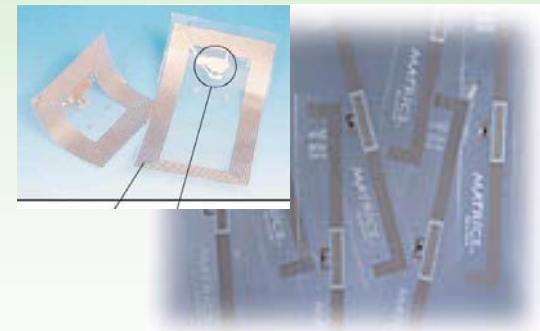


RFID Tag Attributes

	Active RFID	Passive RFID
Tag Power Source	Internal to tag	Energy transferred using RF from reader
Tag Battery	Yes	No
Availability of power	Continuous	Only in field of reader
Required signal strength to Tag	Very Low	Very High
Range	Up to 100m	Up to 3-5m, usually less
Multi-tag reading	1000's of tags recognized – up to 100mph	Few hundred within 3m of reader
Data Storage	Up to 128Kb or read/write with sophisticated search and access	128 bytes of read/write

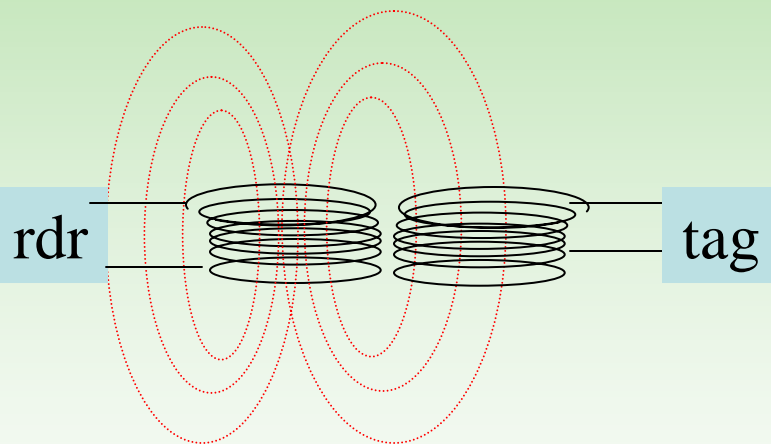
Passive RFID Tags

- “Traditional” tags used in retail security applications
 - Tag contains an antenna, and a small chip that stores a small amount of data
 - Tag can be programmed at manufacture or on installation
 - Tag is powered by the high power electromagnetic field generated by the antennas – usually in doorways
 - The field allows the chip/antenna to reflect back an extremely weak signal containing the data
 - Collision Detection – recognition of multiple tags in the read range – is employed to separately read the individual tags
- These passive tags form the basis of the Auto-ID designs, and, if manufactured in billions, will come down in price from \$0.80 to \$0.05 in the next 2 years.



Sending/Receiving RF Energy

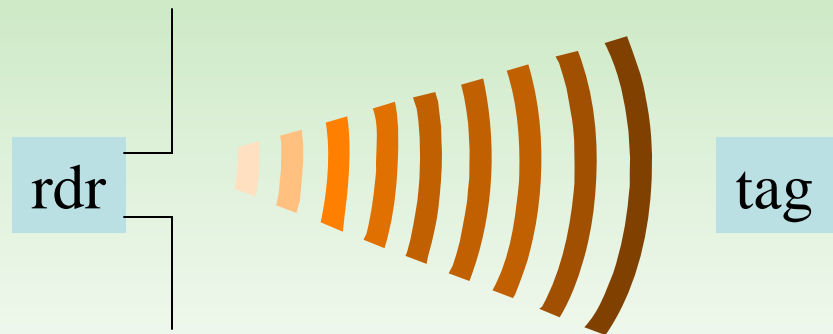
Magnetic Field
(near field)



125kHz & 13.56MHz

$$< \frac{\lambda}{2\pi}$$

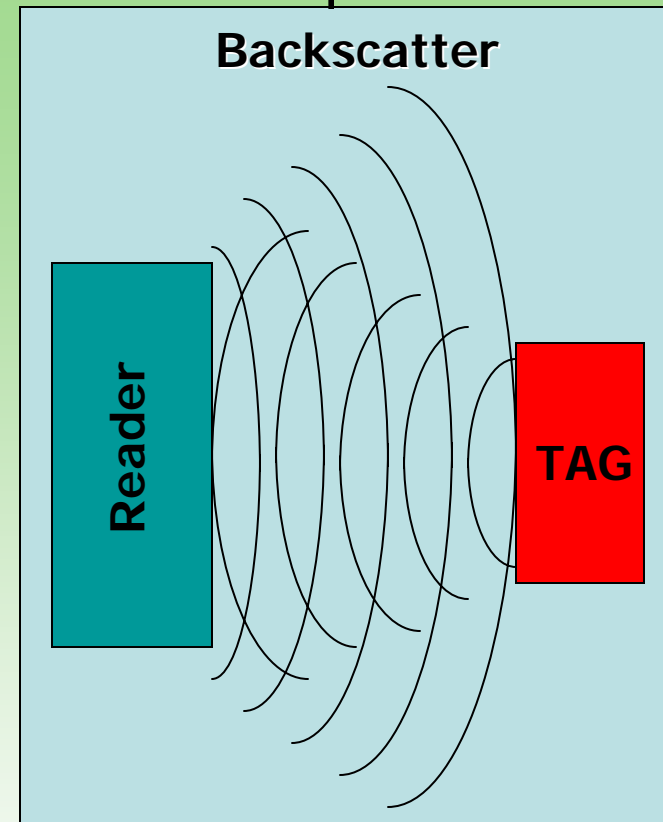
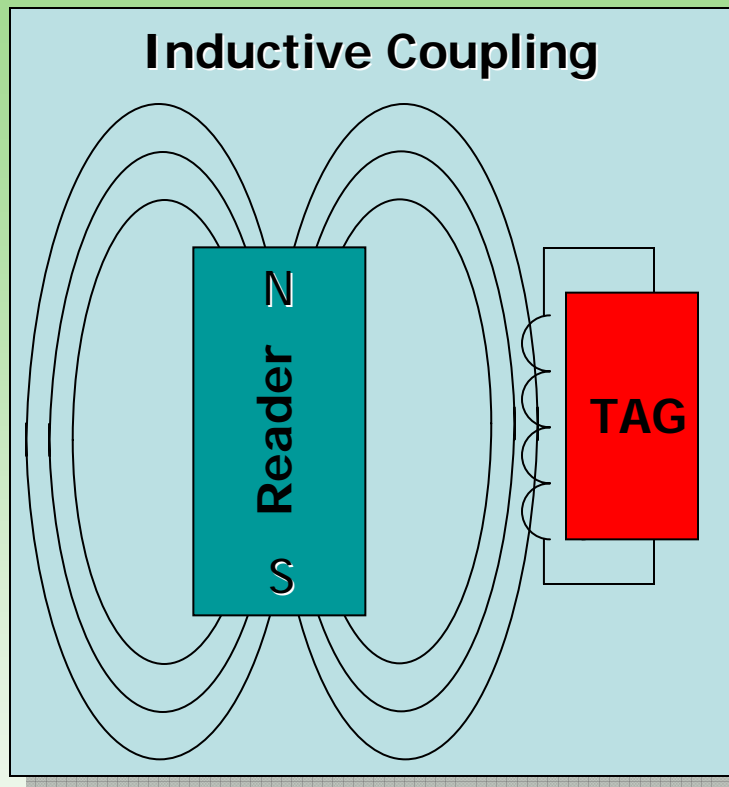
Electromagnetic
(far field)



400 – 2450MHz

$$> \frac{\lambda}{2\pi}$$

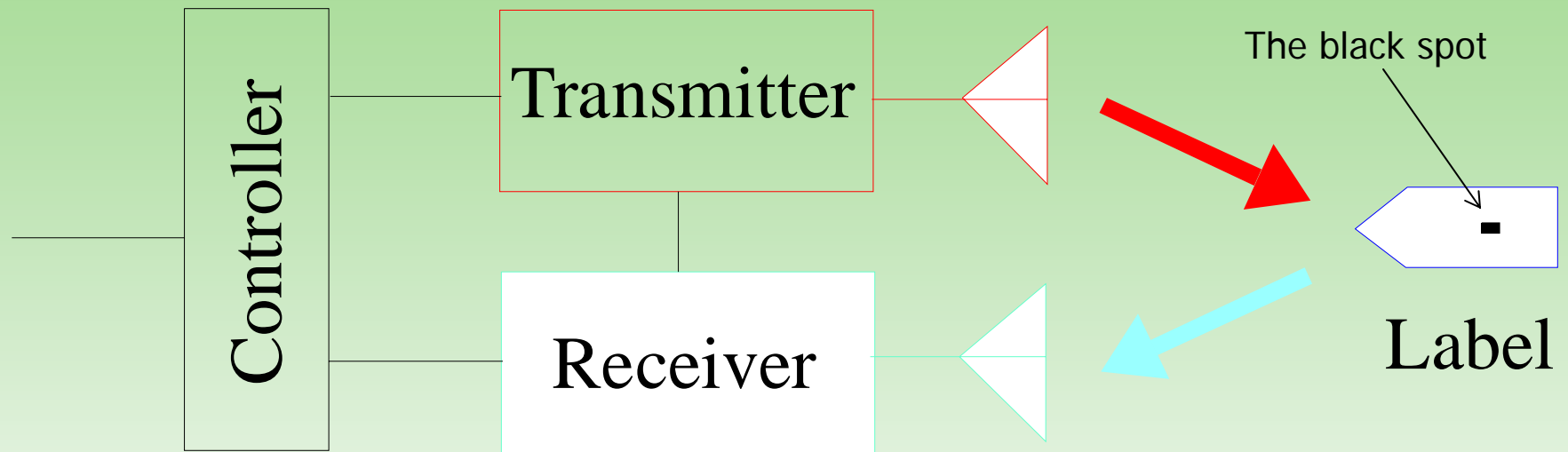
Basic Tag Operational Principles



- Near field (LF, HF): inductive coupling of tag to magnetic field circulating around antenna (like a transformer)
 - Varying magnetic flux induces current in tag. Modulate tag load to communicate with reader
 - field energy decreases proportionally to $1/R^3$ (to first order)
- Far field (UHF, microwave): backscatter.
 - Modulate back scatter by changing antenna impedance
 - Field energy decreases proportionally to $1/R$
- Boundry between near and far field: $R = \text{wavelength}/2\pi$ so, once have reached far field, lower frequencies will have lost significantly more energy than high frequencies
- Absorption by non-conductive materials significant problem for microwave frequencies

Source of data: "Introduction to RFID" CAENRFID an IIT Corporation

Tag reading

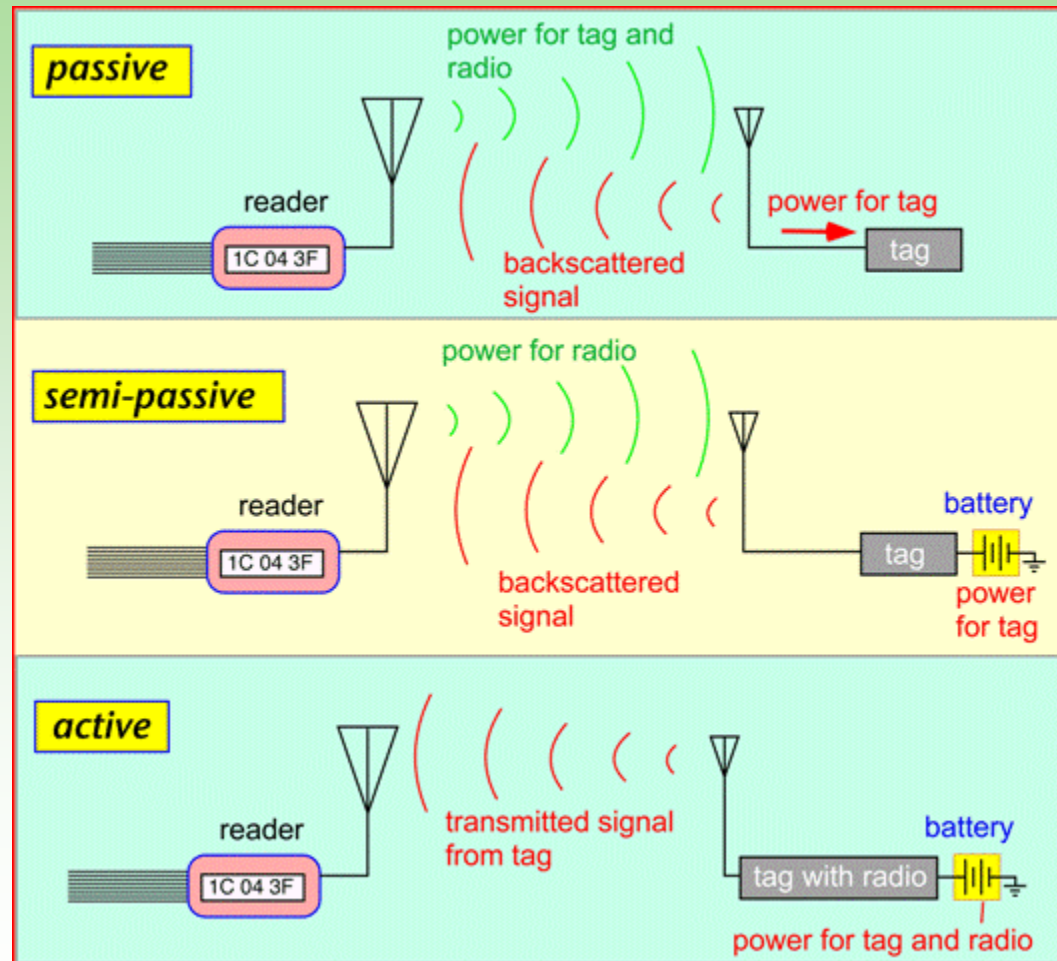


Normally a very weak reply is obtained

Limiting factors for passive UHF RFID

- Reader transmitter power P_r (Gov. limited)
- Reader receiver sensitivity S_r
- Reader antenna gain G_r (Gov. limited)
- Tag antenna gain G_t (size limited)
- Power required by tag P_t (silicon process limited)
- Tag modulator efficiency E_t

Tag Power/Transmit Configuration



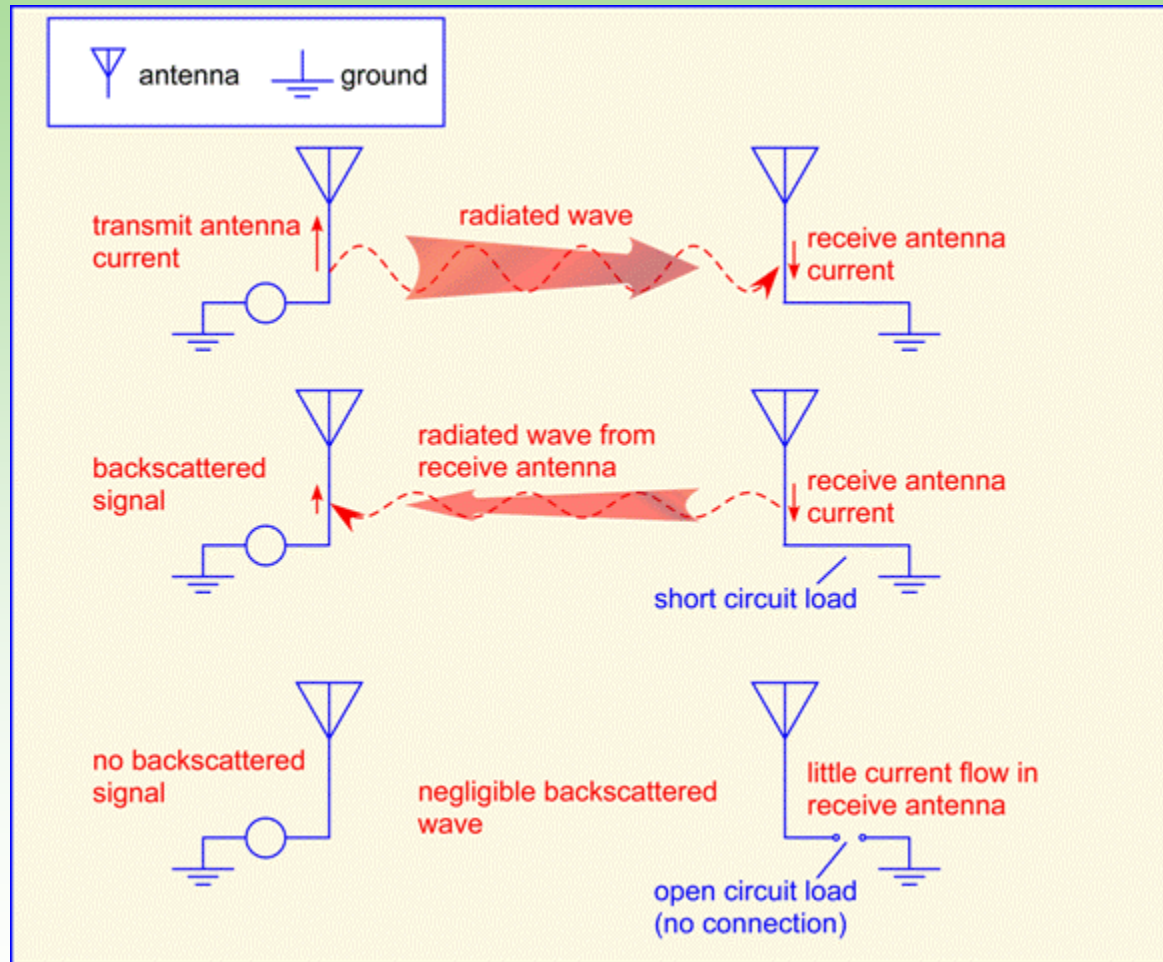
Typical UHF operating parameters

- Reader Transmit Power $P_r = 30\text{dBm}$ (1 Watt)
- Reader Receiver Sensitivity $S_r = -80\text{dBm}$ (10^{-11} Watts)
- Reader Antenna Gain $G_r = 6\text{dBi}$
- Tag Power Requirement $P_t = -10\text{dBm}$ (100 microwatts)
- Tag Antenna Gain $G_t = 1\text{dBi}$
- Tag Backscatter Efficiency $E_t = -20\text{dB}$
- System operating wavelength = 33cm (915MHz)

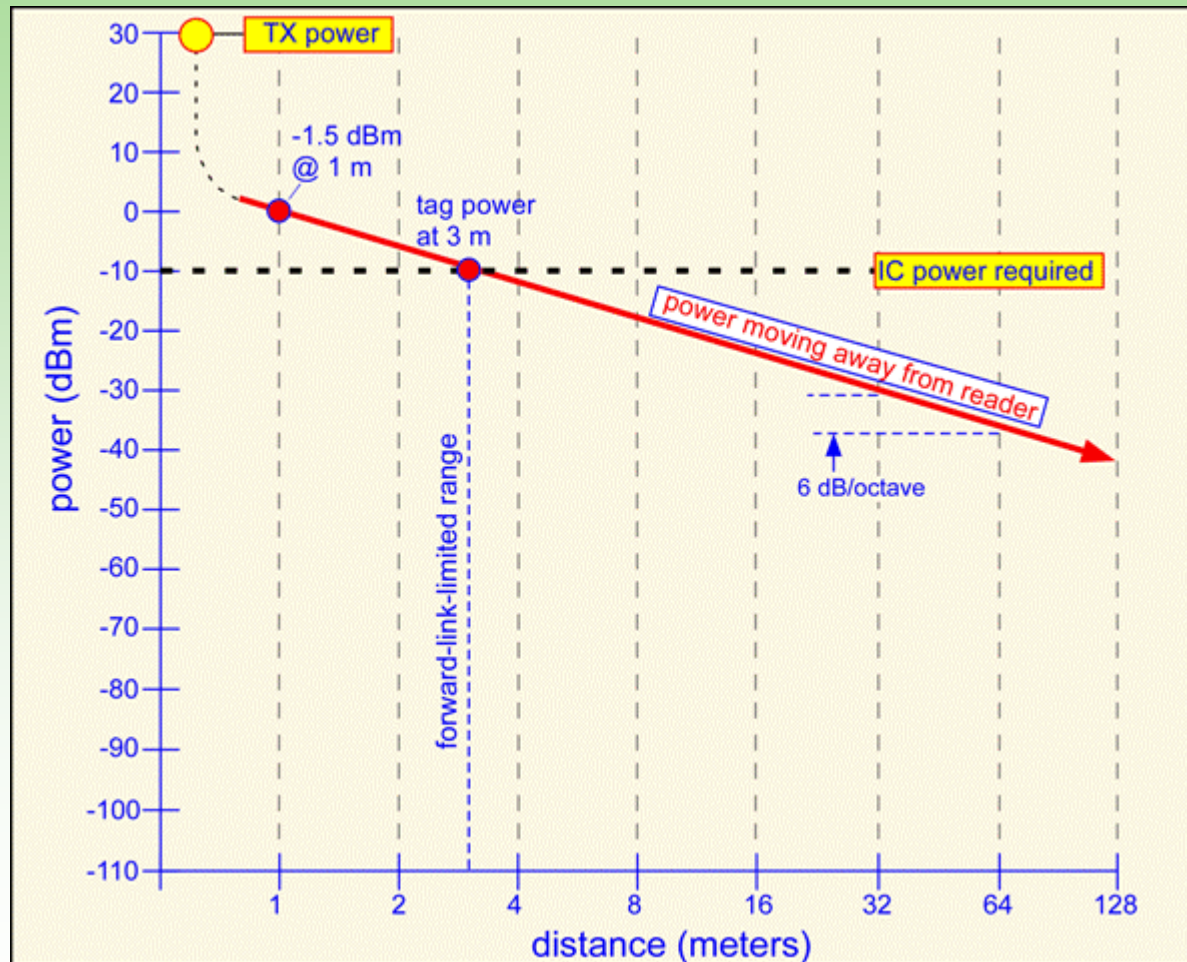
Link Margin

- How much loss the link can sustain for a given performance requirement
- Equals Receiver sensitivity minus transmit power including antenna gain
- Not necessarily symmetric (forward/reverse)
- Example:
 - *Forward link*: reader transmits at 30 dBm, tag power requirement is -10 dBm, total budget of 40 dB
 - *Reverse link*: tag reflects back -10 dBm -20 db (efficiency) = -30 dBm, receiver sensitivity is -80 dBm, total budget of 50 dB

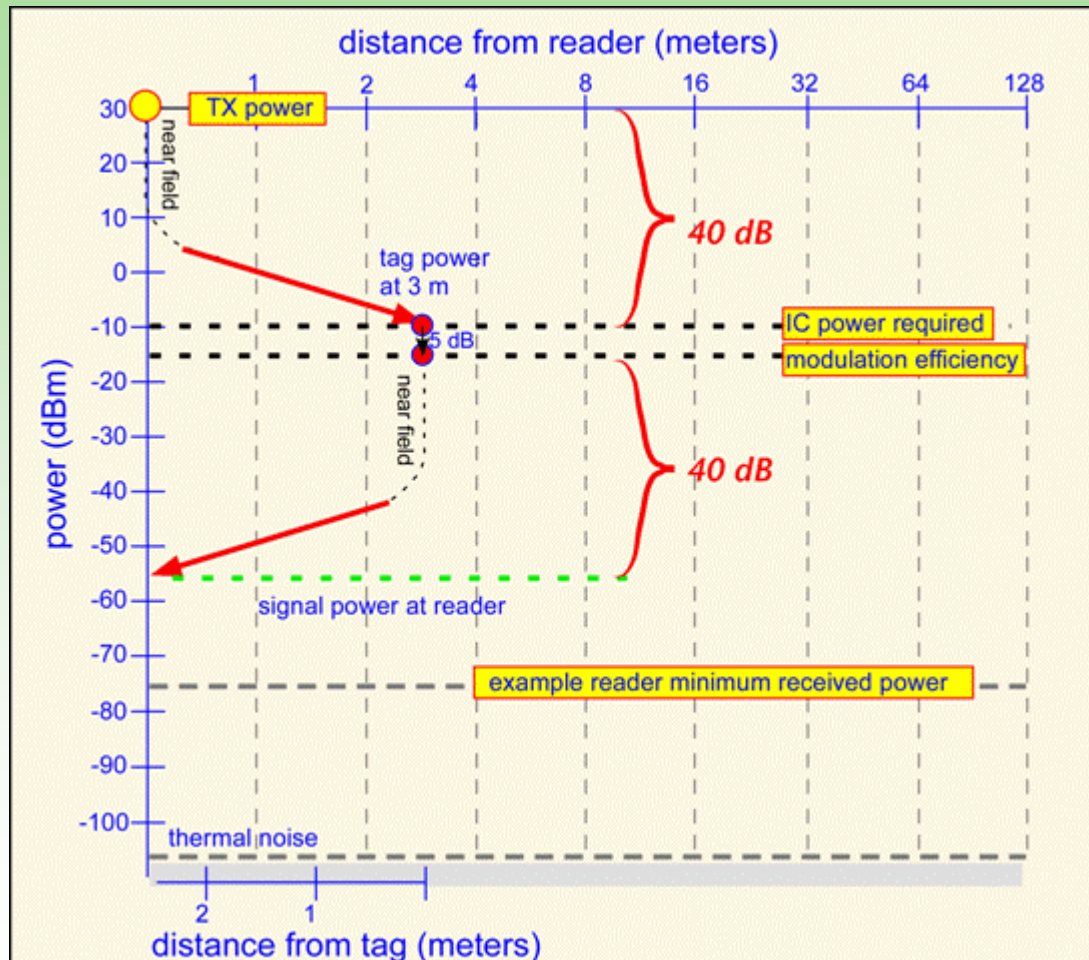
Physics of Backscatter Signaling



Forward Link Margin for Passive Tag

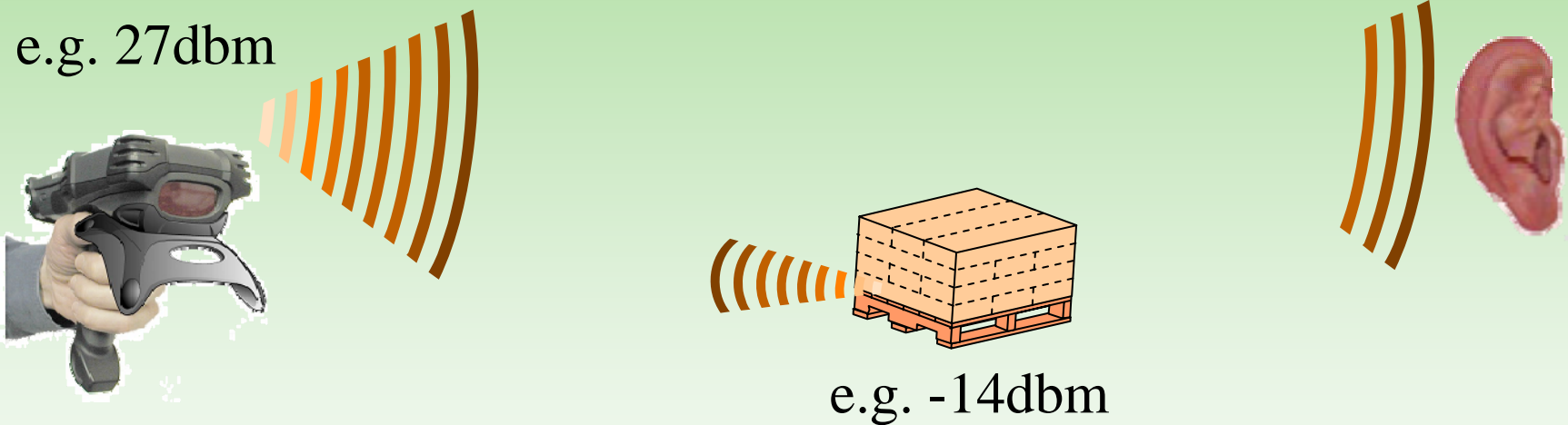


Forward & Reverse Link Margin for Passive Tag

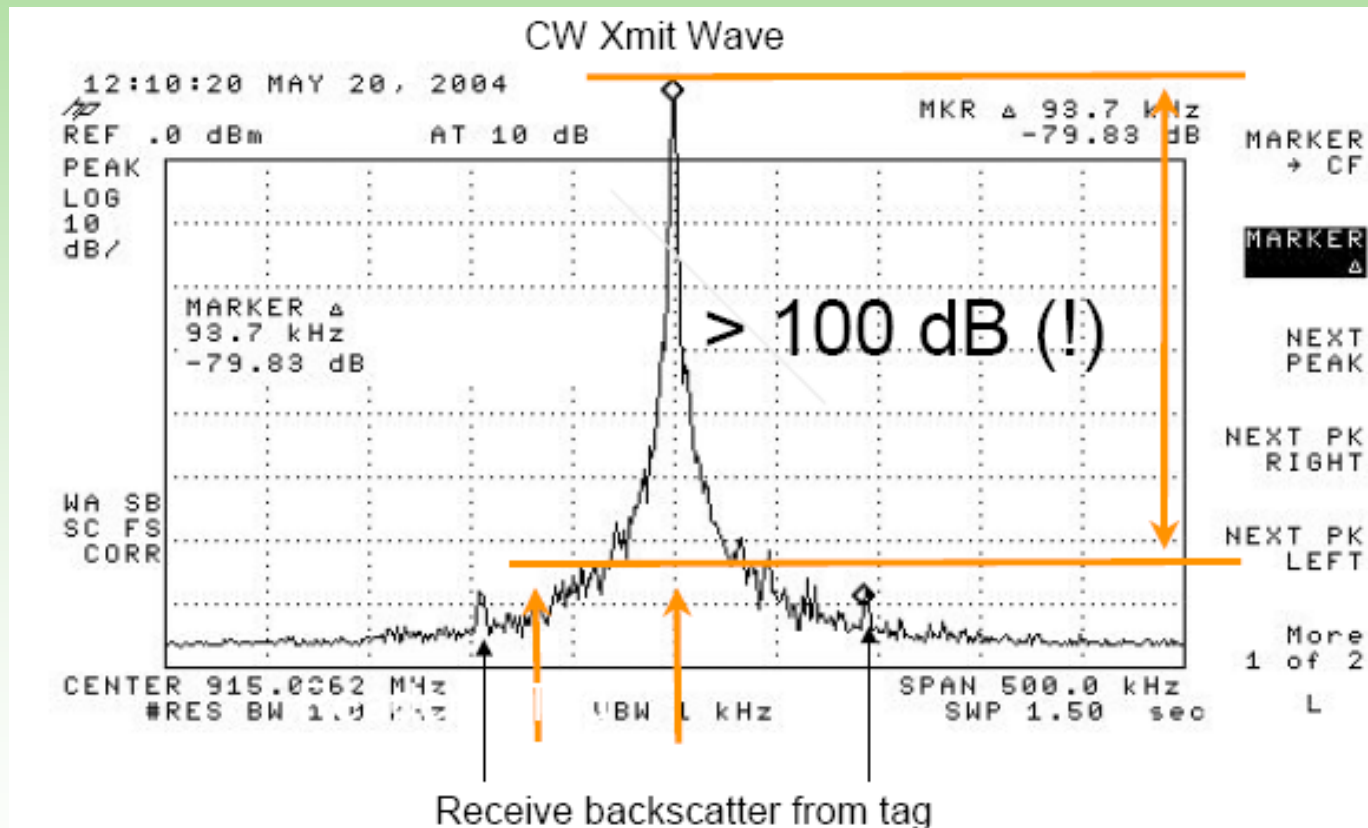


Asymmetric Channel Strength

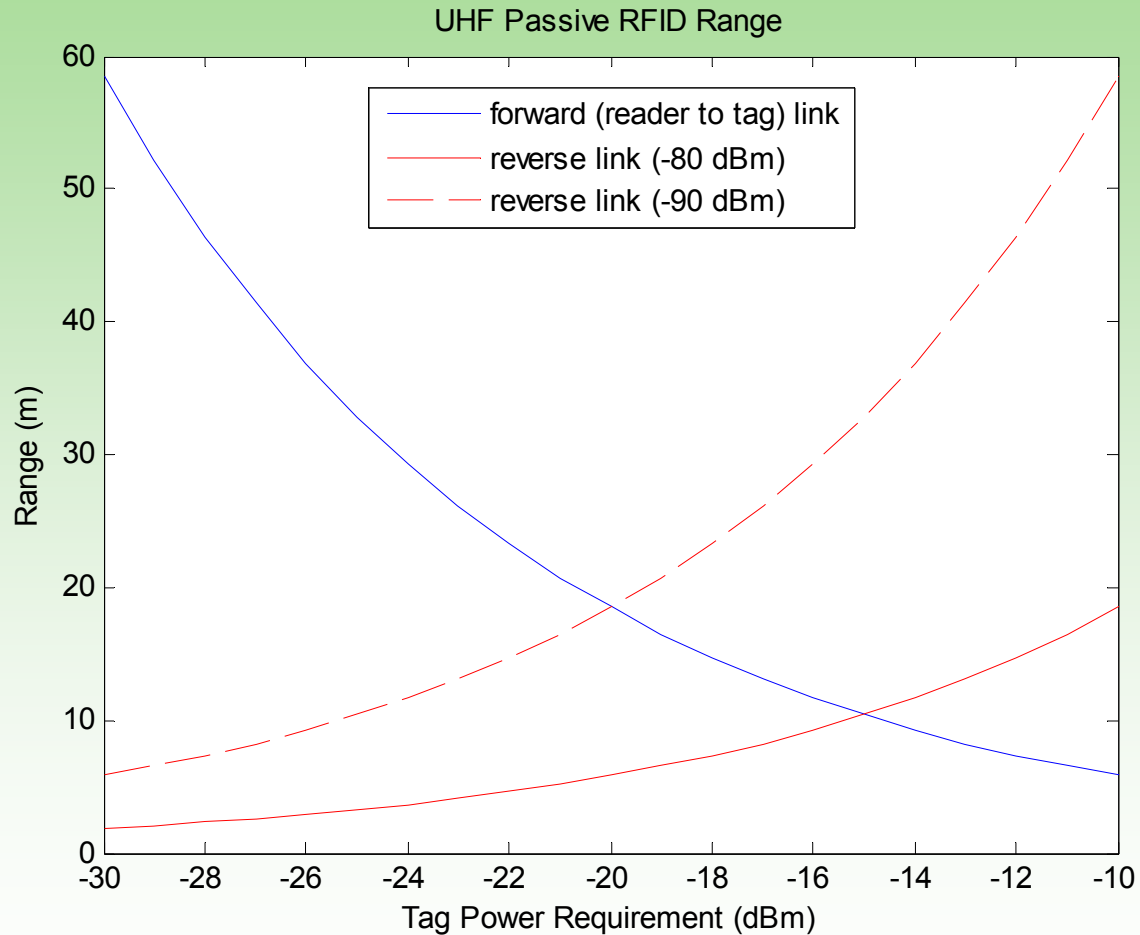
Security Issue



The Dynamic Range Challenge



Range of UHF Passive Tag



Lessons from the simple model

- Because $P_t \propto (1/d^2)$, doubling read range requires 4X the transmitter power.
- Larger antennas can help, but at the expense of larger physical size and narrower beamwidth.
- Smaller CMOS processes will help by reducing P_t
- But there is a fundamental limit – at large distances, receiver SNR dominates.
- Achieving high R at low cost remains a practical challenge

Regulatory

➤ *US: 36dbm (4 watts)*

➤ *Europe: 27dbm (500mw)*

BAND	REGION	MAX POWER EIRP
433.05 - 434.79MHz	Europe	25mW
868 - 870 MHz	Europe	500mW * Still under consideration
902 - 928 MHz	USA/Canada	50mV/m at 3metres (single freq systems)
	USA/Canada	4W using spread spectrum
	USA/Canada	30W FCC Part 90, LMS (3W conducted)
918 - 926 MHz	Australia	1W all new equipment designs
		30W low duty cycle (Grandfather clause)
915.3 - 915.6 MHz	South Africa	15W (5W conducted)
2.4 - 2.4835 GHz	Europe	25mW
	Europe	500mW spread spectrum
	USA/Canada	50mV/m at 3 metres (single freq systems)
	USA/Canada	4W using spread spectrum (1W conducted)
2.446 - 2.454 GHz	Europe	500mW (Automatic Vehicle Identification)
5.725 - 5.875 GHz	Europe	25mW
	USA/Canada	50mV/m at 3 metres (single freq systems)
5.725 - 5.850 GHz	USA/Canada	4W using spread spectrum (1W conducted)

- Region 1: Europe, Middle East, Africa and the former Soviet Union, including Siberia.
- Region 2: North and South America and Pacific east of the International Date Line.
- Region 3: Asia, Australia and the Pacific Rim West of the International Date Line.

Reader Implementation Challenges

- Reader must deliver enough power from RF field to power the tag
- Reader must discriminate backscatter modulation in presence of carrier at same frequency
- >70db magnitude difference between transmitted and received signals
- Interference between readers
- High volume of tag data – readers need to filter data before releasing to enterprise network

Traditional RFID Market Segments



Auto Immobilizers



Automated Vehicle Id

- *Isolated systems*
- *Simple reads*
- *Slow growth*



Access Control



Animal Tracking

The New Mkt Segment

Consumer Pkg Goods Supply Chain

Wal-Mart

- June '03 announcement
- Pallet/Case tagging
 - Top 100 suppliers Jan '05
 - Other 30K by end of '06
- 4 Billion tags/year
- 300k direct readers
- 18 Million indirect readers

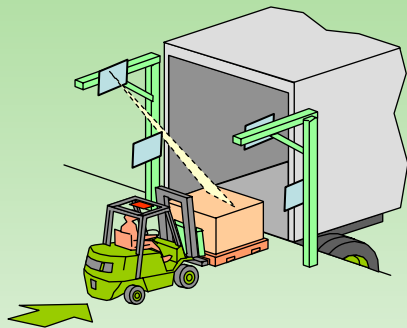


+

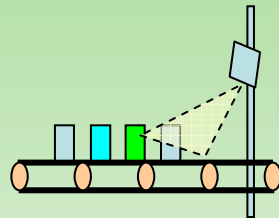


- *End to end systems*
- *Complex reads*
- *Emerging market*

Usage Models



Dock Door



Conveyor Belt



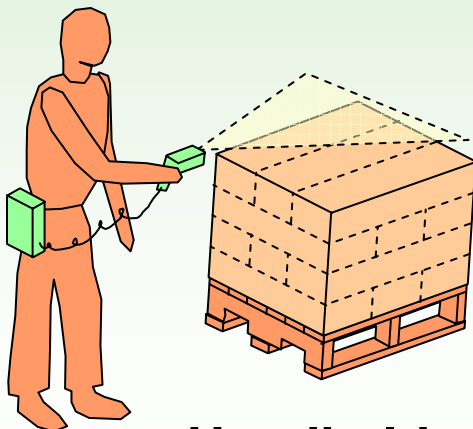
Forklift



Container, Pallet, Munitions



Printers



Handheld



Smart Shelves



Point of Sale

A Few RFID Applications

- Umbilical Clamp Tags
- Inventory
- Animal / Livestock Data
- Assembly/subassembly routing & documentation
- Trash Collection (customer ID-weight)
- Track items in transit
 - airport/passenger luggage
- Automated toll collection
- Automatic Vehicle Identification
 - Parking Lots
 - Admission Gates
- Security/item recovery
 - tag pairs for rights to remove equipment from premise
 - Automotive Keys (ignition enabler)
- Convenience
 - Automotive Keys (custom seat position)
 - Keyless Home Entry
 - Retail Purchasing (Link to credit card)
 - Proximity Monitor (children, pets)
- Time Critical Equipment Tracking
 - emergency medical equipment
 - medical staff
- Airline Baggage - Passenger Matching
- Intelligent Highways
- Access control
- Asset management
- Automotive identification (production control)
- Garment tracking and sorting (industrial laundries)
- Hazardous waste management and tracking
- Industrial gas cylinder identification and tracking
- Item shelf-life control
- Livestock identification
- Maintenance record management
- Meeting OSHA documentation requirements
- Pallet tracking
- Pet identification and registration
- Time and Attendance
- Tool tracking
- Ski lift ticketing
- Valuable items registration
- Warehouse/stock handling
- Wildlife and fisheries management

Read Range & Robustness

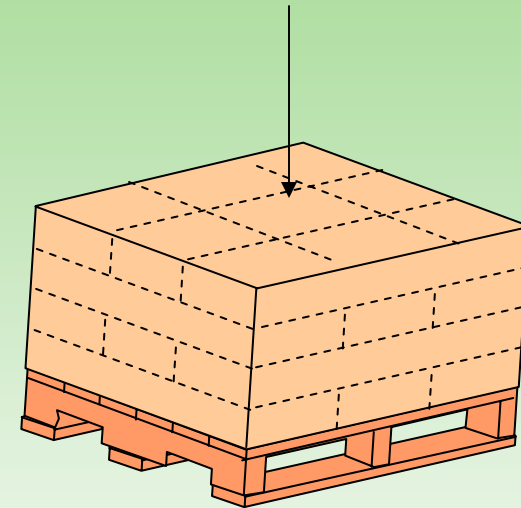


Pantene
Shampoo



Liquid, metal products,
Metal containers...

Military MRE's



Outside Read Rates 100% @ 3MPH
90% @ 5MPH
0% (always)

8 Inside Cases



72-92% Water
Foil Wrapped

M-Commerce

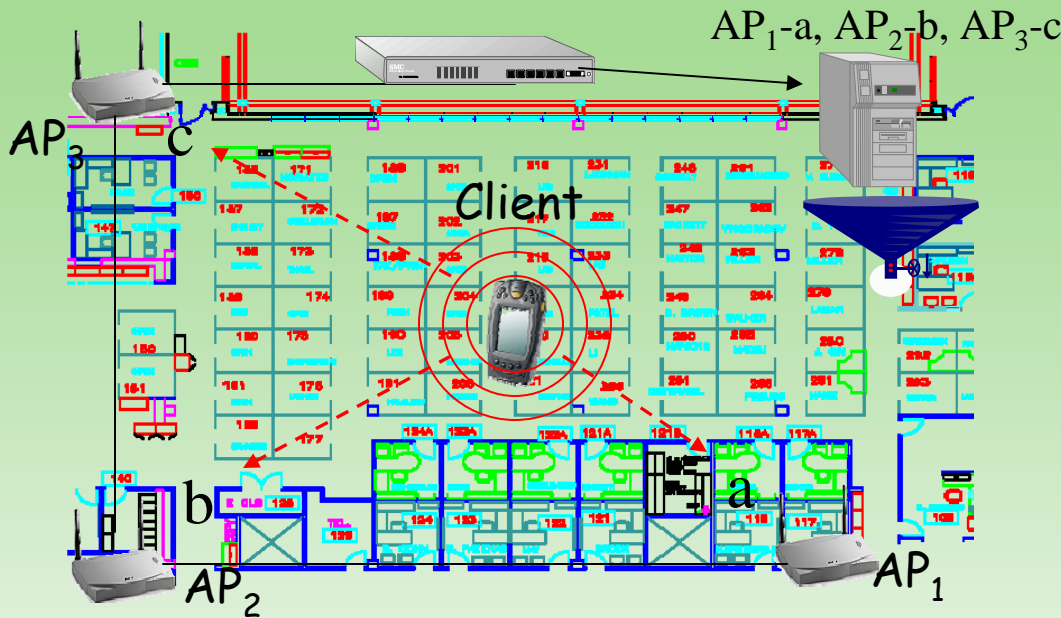


Have A
Cabernet Sauvignon
\$12.99
Excellent w/Sirloin

- Context Sensitive Advertising

RTLS

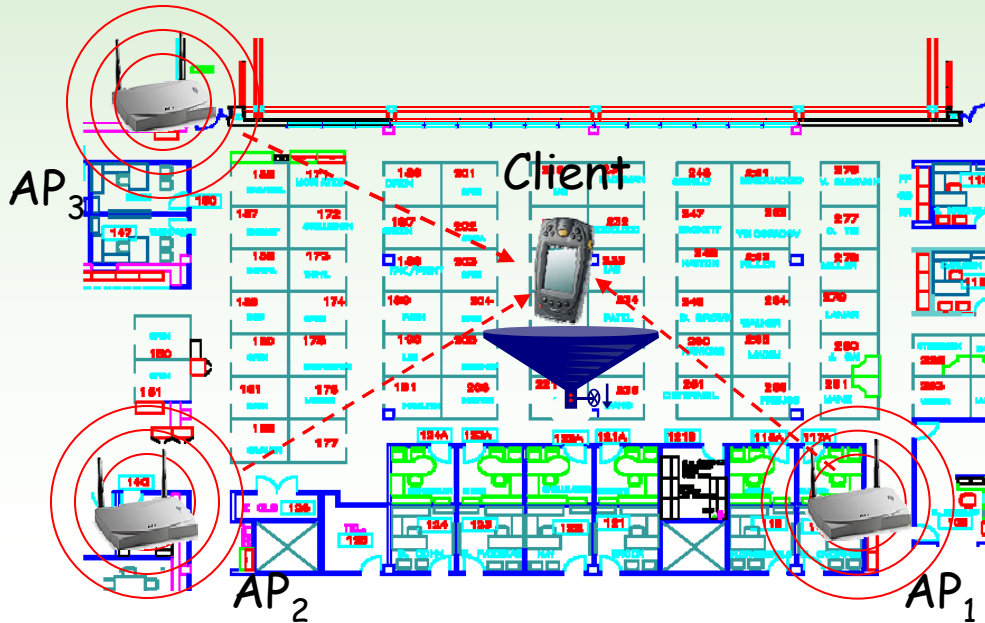
Terminology



Infrastructure Based

- ✓ Infrastructure elements collect ephemeral, telemetric data (a,b,c) on client
- ✓ Can be covert to the client
- ✓ Few or no customizations to the client

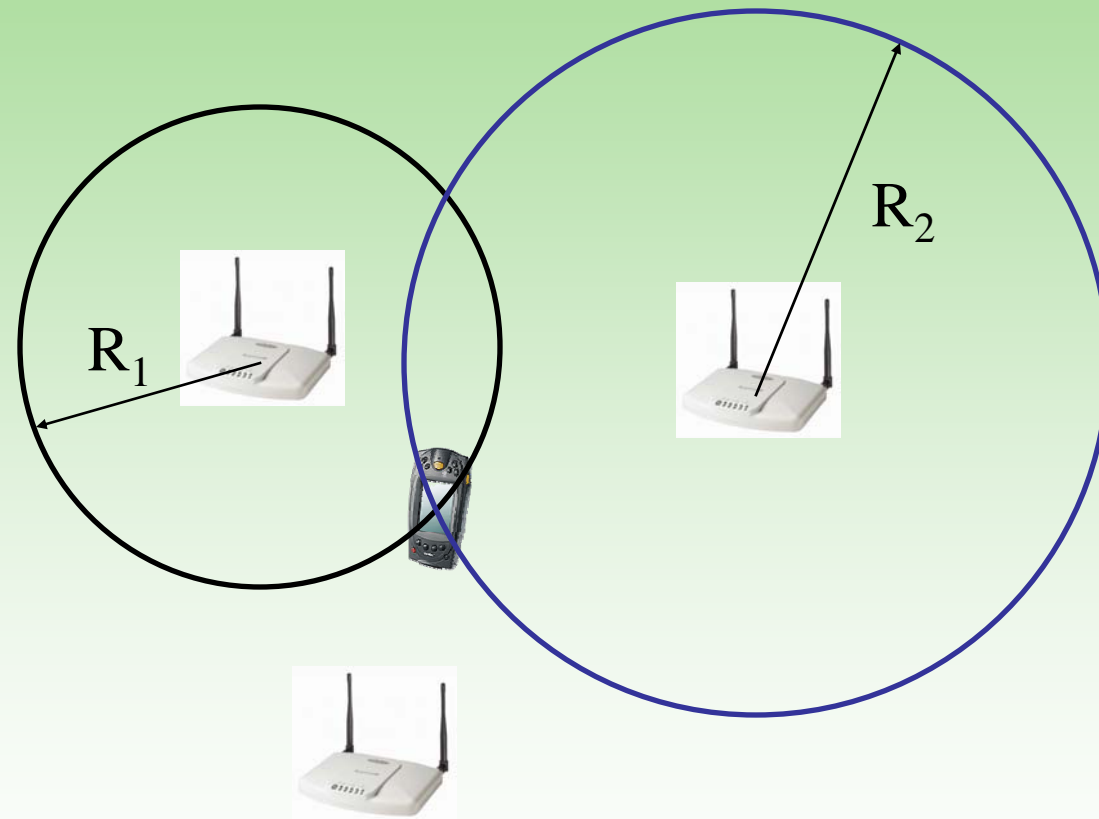
↑
HYBRIDS
↓



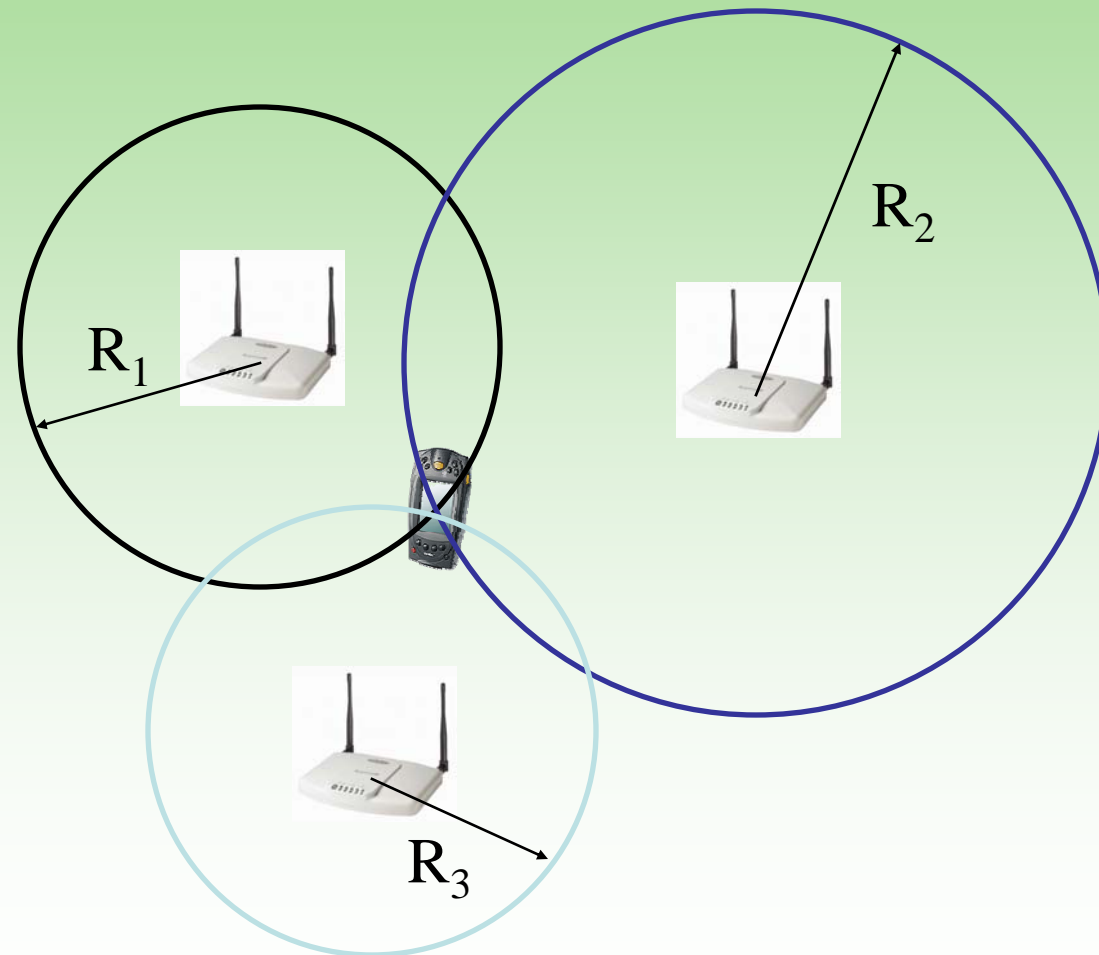
Client Based

- ✓ Client collects ephemeral, telemetric data on AP's 1,2,3
- ✓ Can “infrastructure independent”
- ✓ relatively high degree of client resources

RTLS – Basic Trilateration



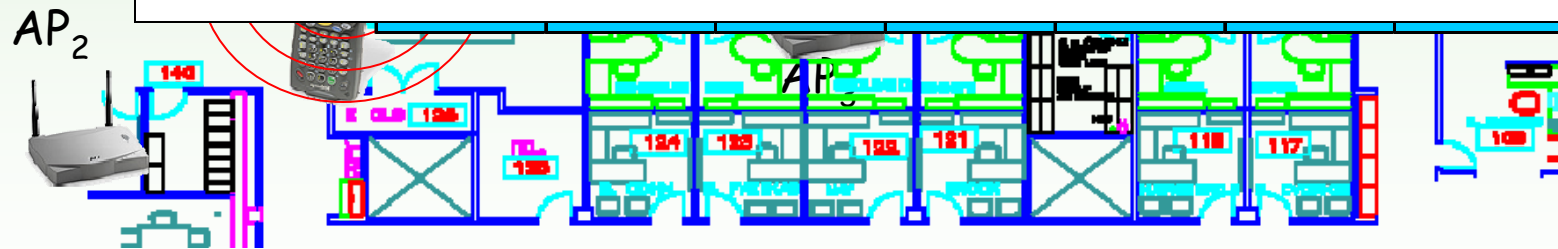
RTLS – Basic Trilateration



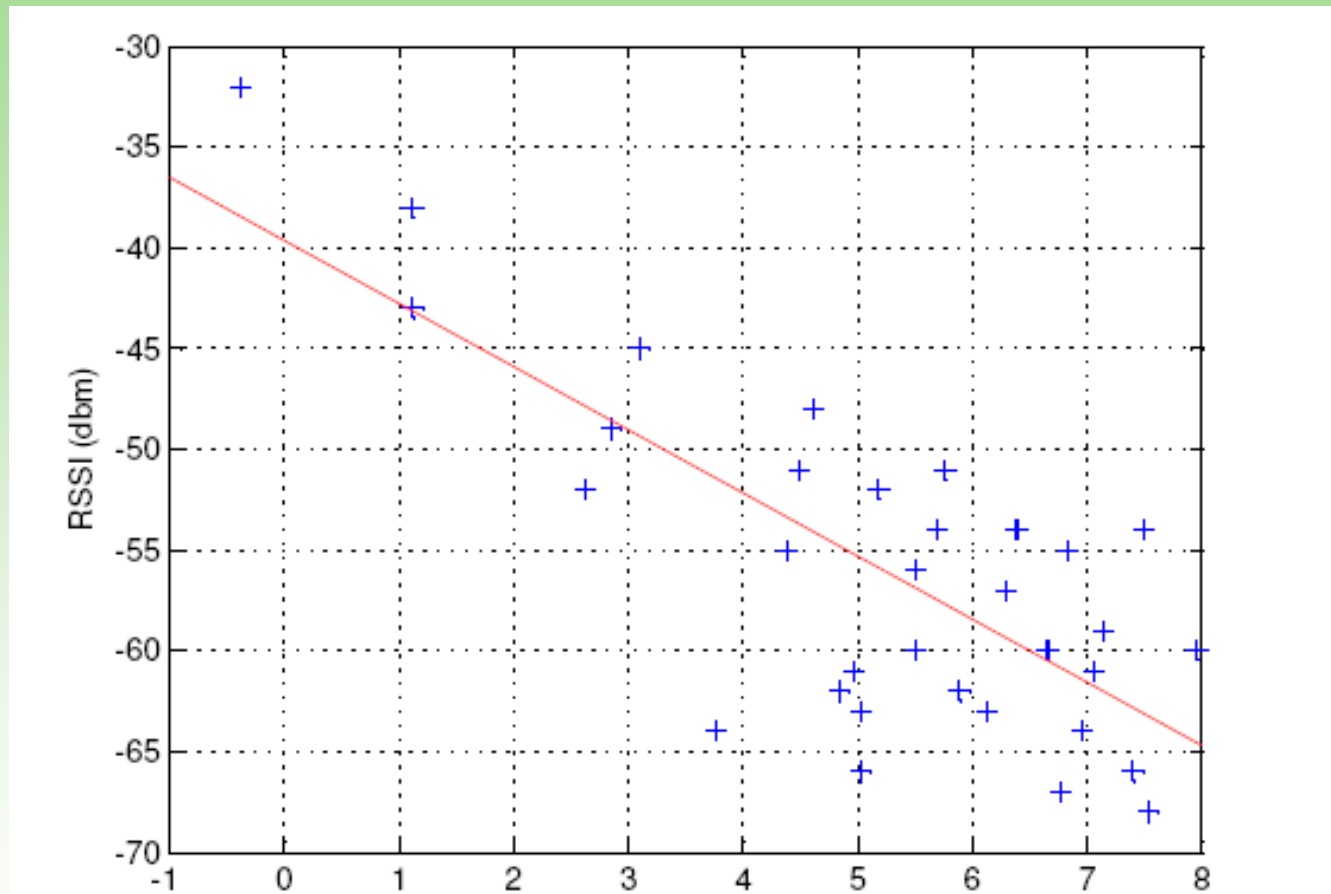
RSSI-based RTLS



- N-dimensional vector space of APs/RSSI
- Take a reading (0.4, 0.23, 0.44, 0.0, 0.57)
- Find minimum euclidean distance & associate w/XYZ



Parametric Approach

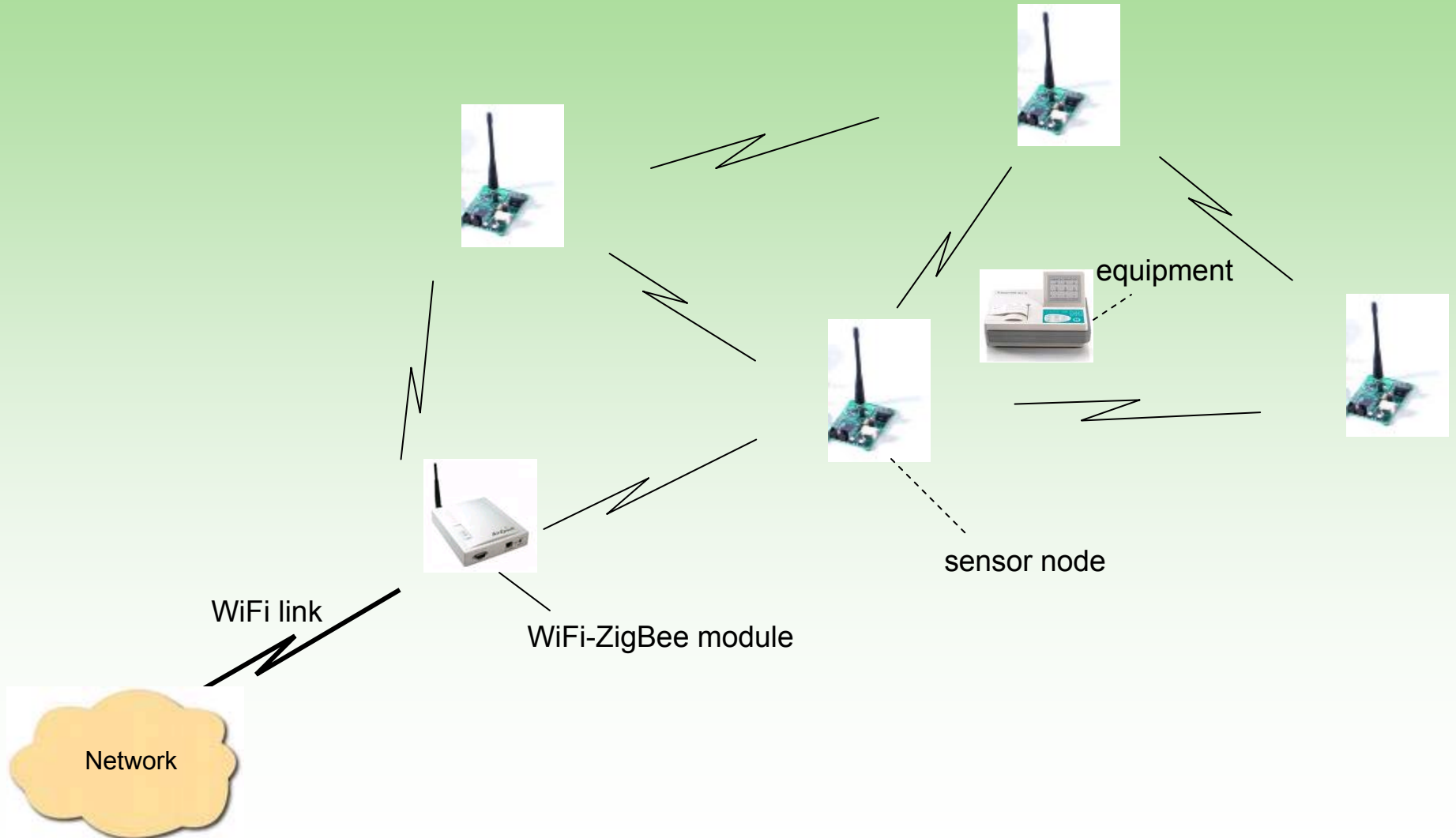


$RSSI = A + 10n/\log(d) \rightarrow$ find A and n

Measure $RSSI + A, n \rightarrow$ find d^*

ZigBee RTLS Network Architecture

Mesh Backbone



Wireless Sensor Networks / ZigBee

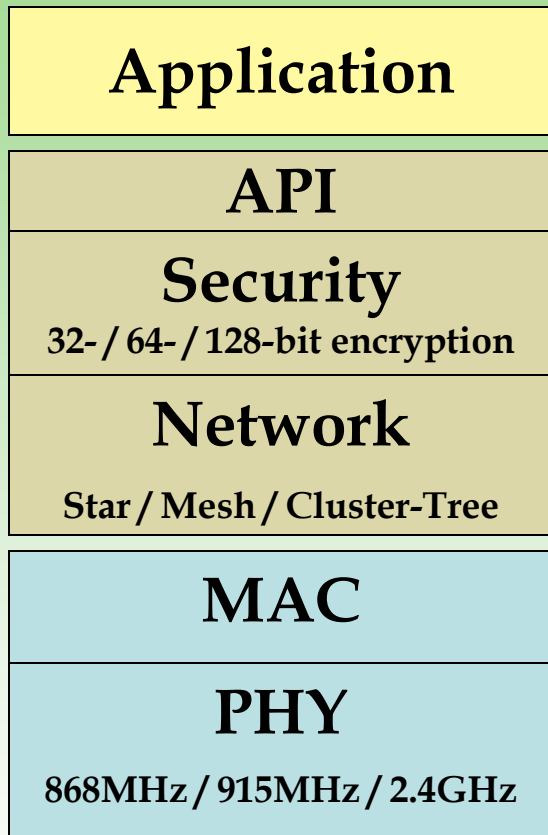
ZigBee Alliance Mission

- Industry alliance: ZigBee - IEEE 802.15.4 (like WiFi - IEEE802.11)
- The ZigBee Alliance is an association of companies working together to enable reliable, cost-effective, low-power, wirelessly networked, monitoring and control products based on an open global standard

ZigBee

- ZigBee is designed to be a low power, low cost, low data rate, wireless solution.
- ZigBee relies upon the robust IEEE 802.15.4 PHY/MAC to provide reliable data transfer in noisy, interference-rich environments
- ZigBee layers on top of 15.4 with Mesh Networking, Security, and Applications control
- ZigBee Value Propositions
 - Addresses the unique needs of most remote monitoring and control network applications
 - Infrequent, low rate and small packet data
 - Enables the broad-based deployment of wireless networks with low cost & low power solutions
 - Example: Lighting, security, HVAC,

IEEE 802.15.4 & ZigBee In Context



Silicon
 Stack
 App

Customer

ZigBee Alliance

IEEE 802.15.4



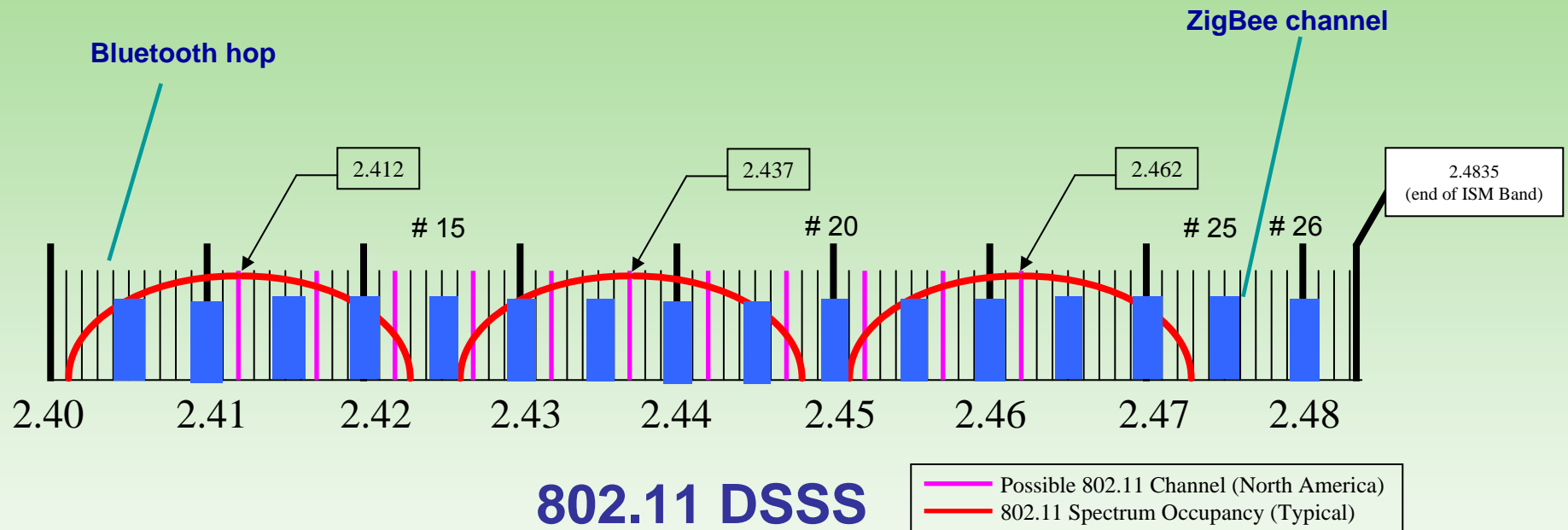
- “the software”
- Network, Security & Application layers
- Brand management

IEEE 802.15.4

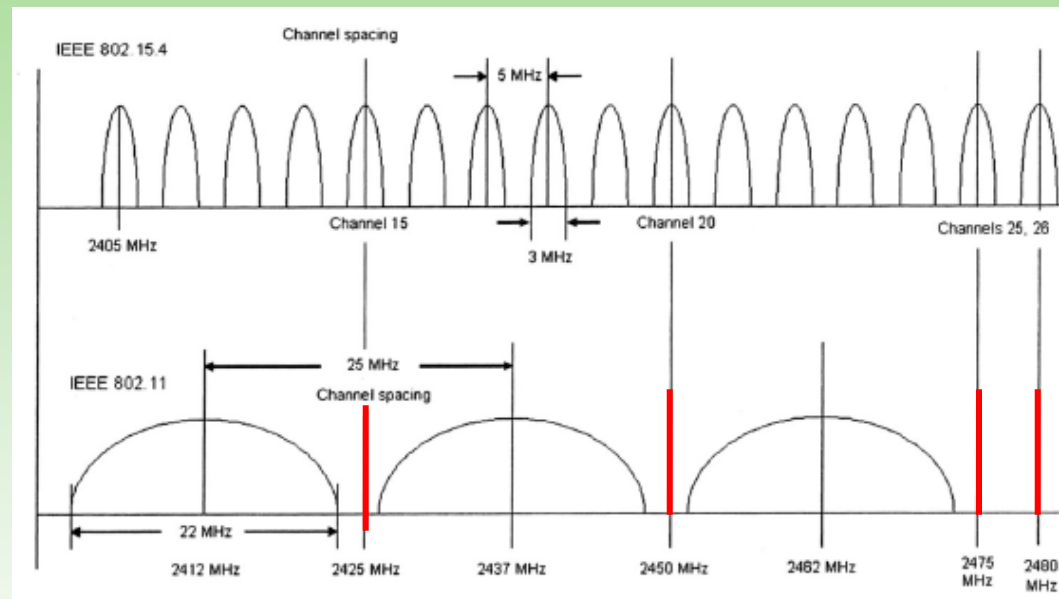
- “the hardware”
- Physical & Media Access Control layers

Source: http://www.zigbee.org/resources/documents/IWAS_presentation_Mar04_Designing_with_802154_and_zigbee.ppt

ZigBee/Bluetooth/WiFi Channel Occupancy in 2.4 GHz



ZigBee-WiFi Coexistence

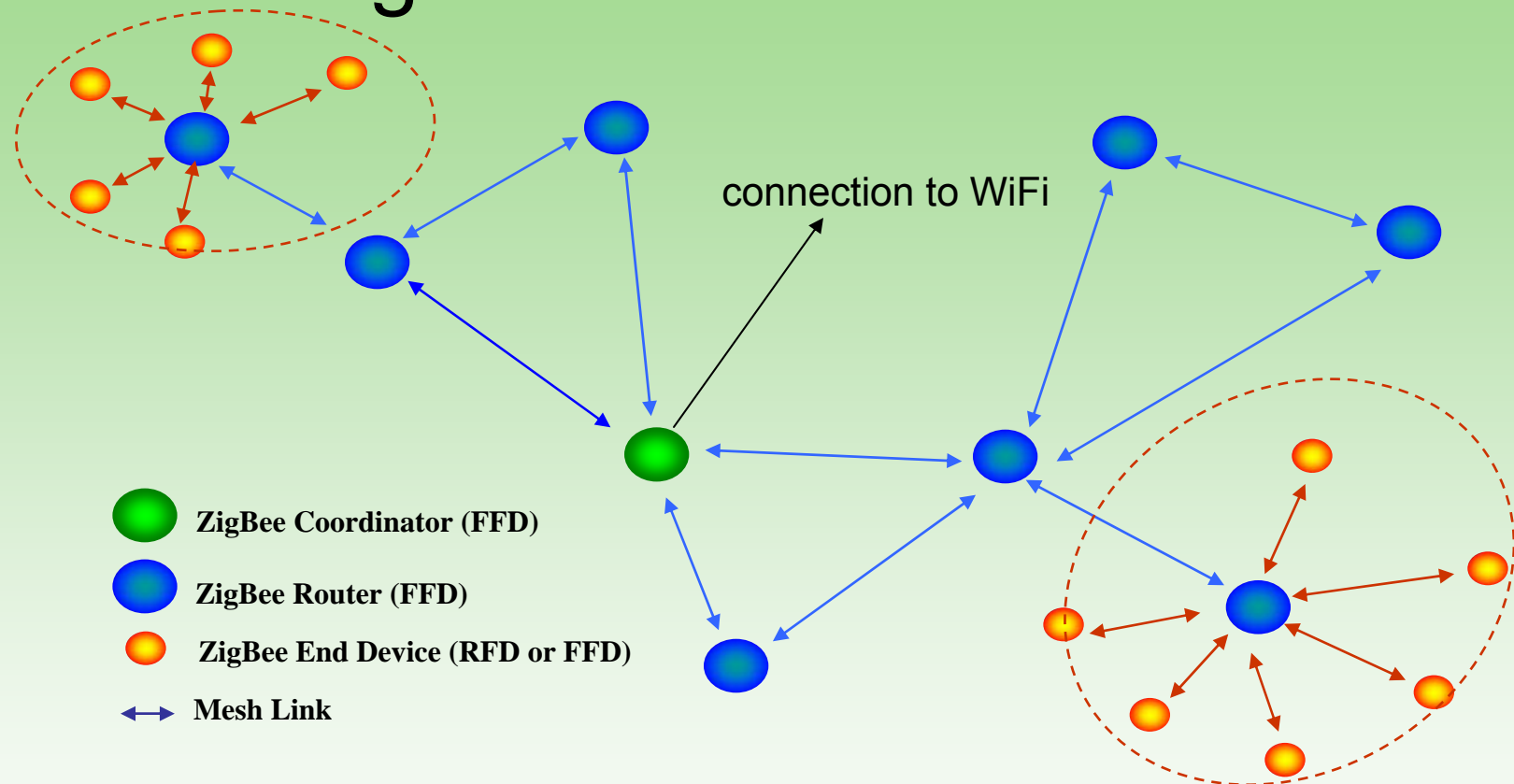


ZigBee

WiFi

- ZigBee channels 26, 25, 20 and 15 are less susceptible to WiFi interference
- Each ZigBee PAN coordinator scans for the best available channel

ZigBee Network Model



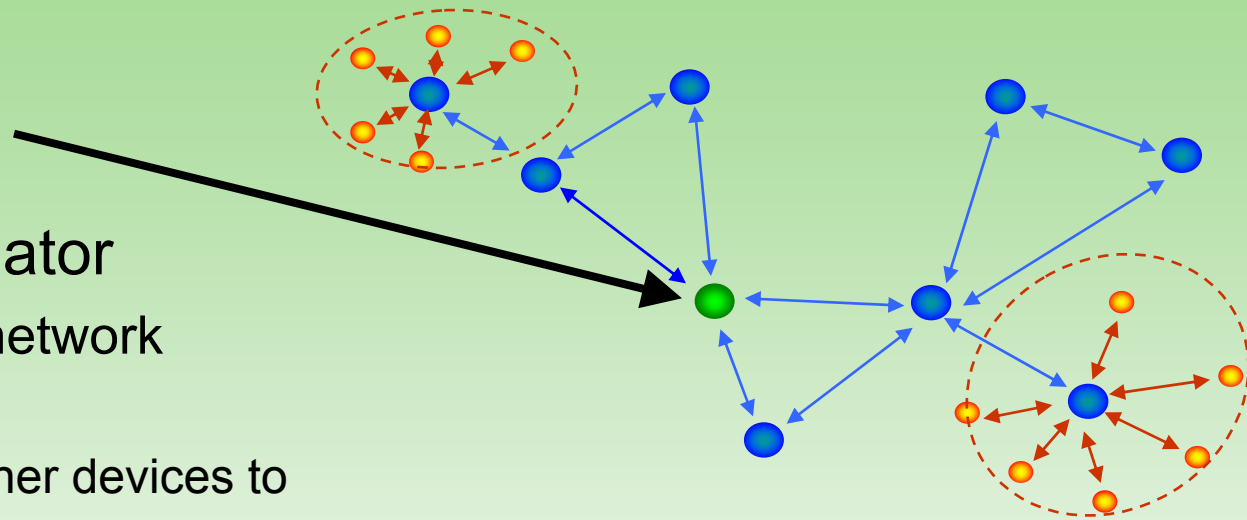
- Star networks support a single ZigBee coordinator with one or more ZigBee End Devices (up to 65,536 in theory)
- Mesh network routing permits path formation from any source device to any destination device

Wireless Networking Basics

- Network Scan
 - Device scans the 16 channels to determine the best channel to occupy.
- Creating/Joining a PAN
 - Device can create a network (coordinator) on a free channel or join an existing network
- Device Discovery
 - Device queries the network to discover the identity of devices on active channels
- Service Discovery
 - Device scans for supported services on devices within the network
- Binding
 - Devices communicate via command/control messaging

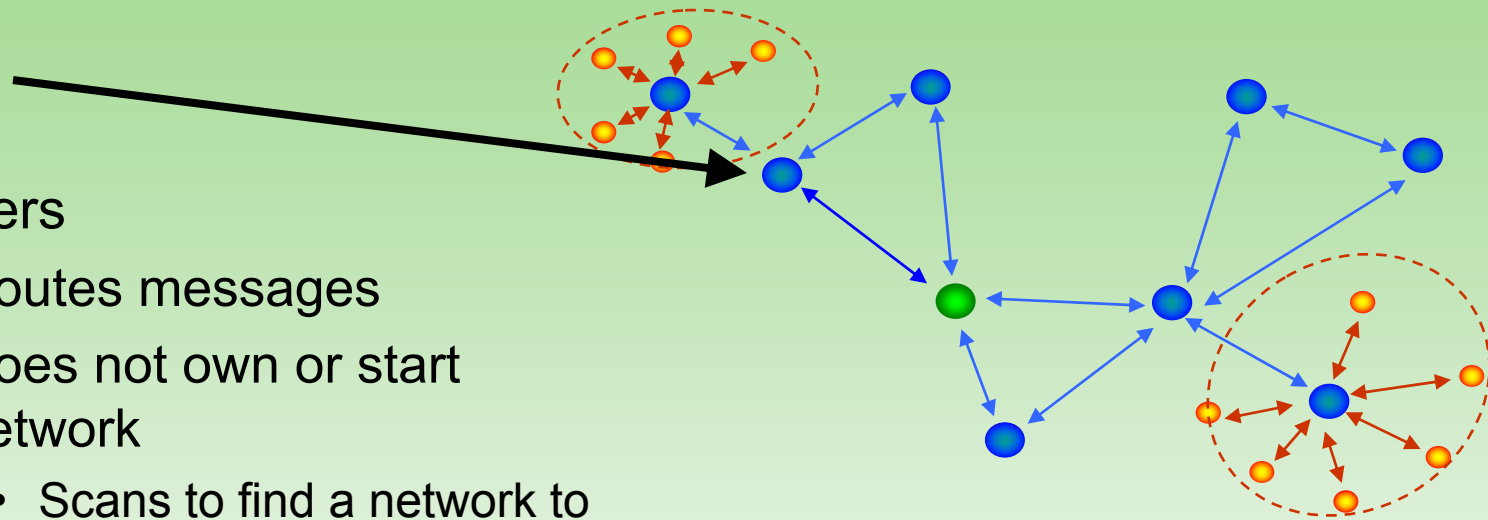
Network Pieces –PAN Coordinator

- PAN Coordinator
 - “owns” the network
 - Starts it
 - Allows other devices to join it
 - Provides binding and address-table services
 - Saves messages until they can be delivered
 - And more... could also have i/o capability
 - A “full-function device” – FFD
 - Mains powered



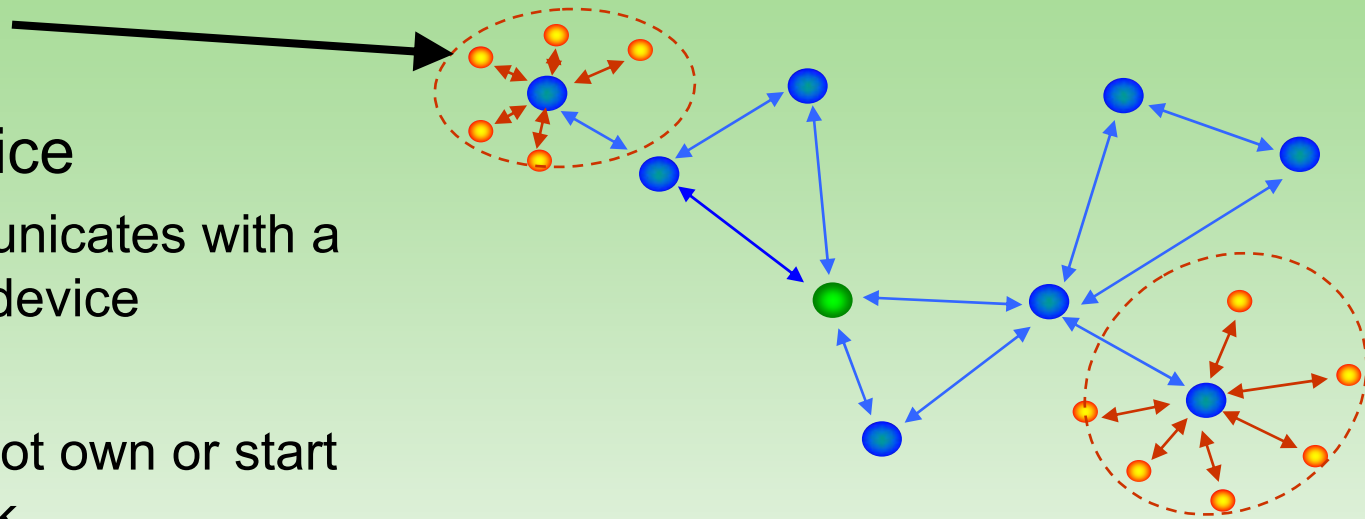
Network Pieces - Router

- Routers
 - Routes messages
 - Does not own or start network
 - Scans to find a network to join
 - Given a block of addresses to assign
 - A “full-function device” – FFD
 - Mains powered depending on topology
 - Could also have i/o capability



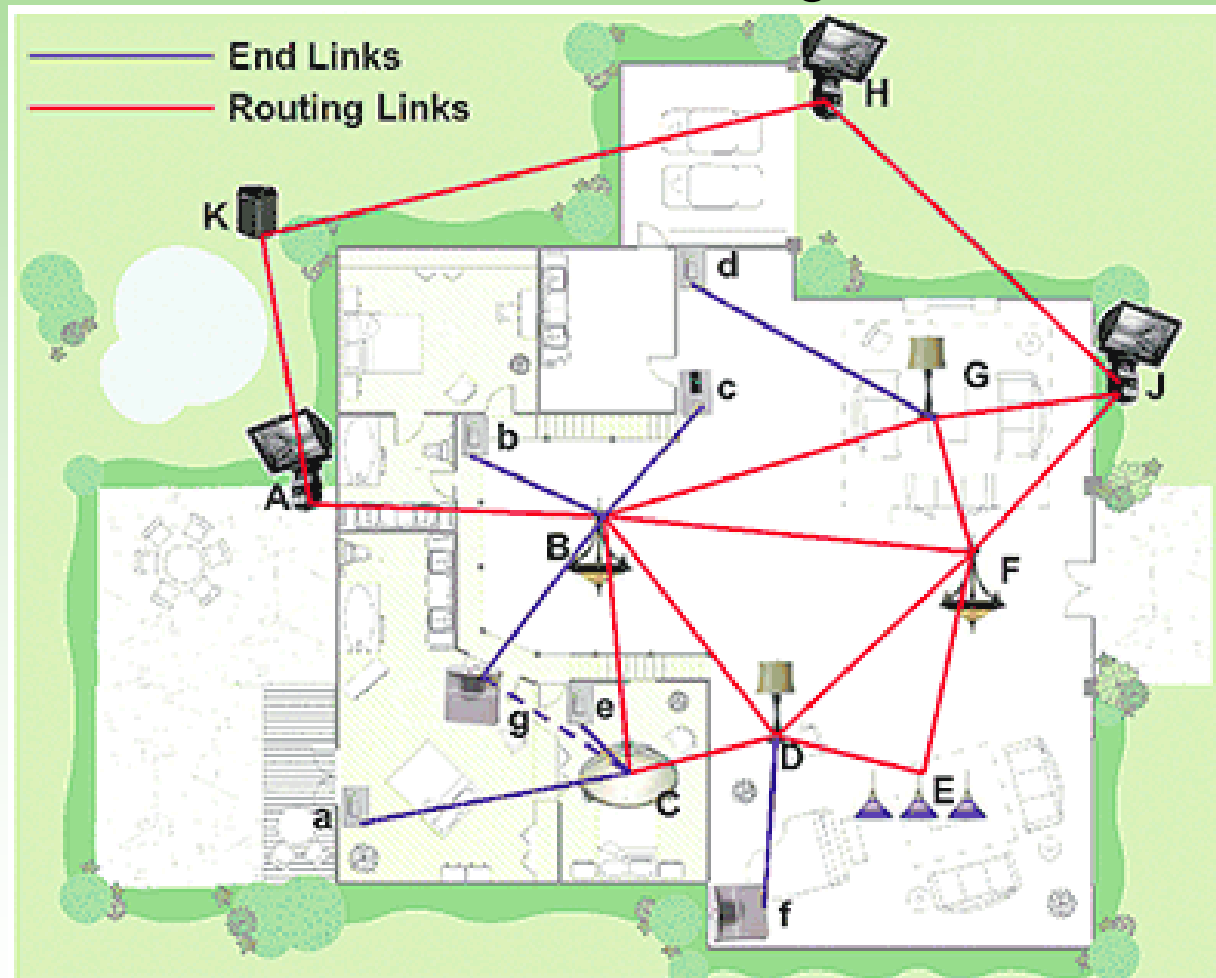
Network Pieces – End Device

- End Device
 - Communicates with a single device
 - Does not own or start network
 - Scans to find a network to join
 - Can be an FFD or RFD (reduced function device)
 - Usually battery powered



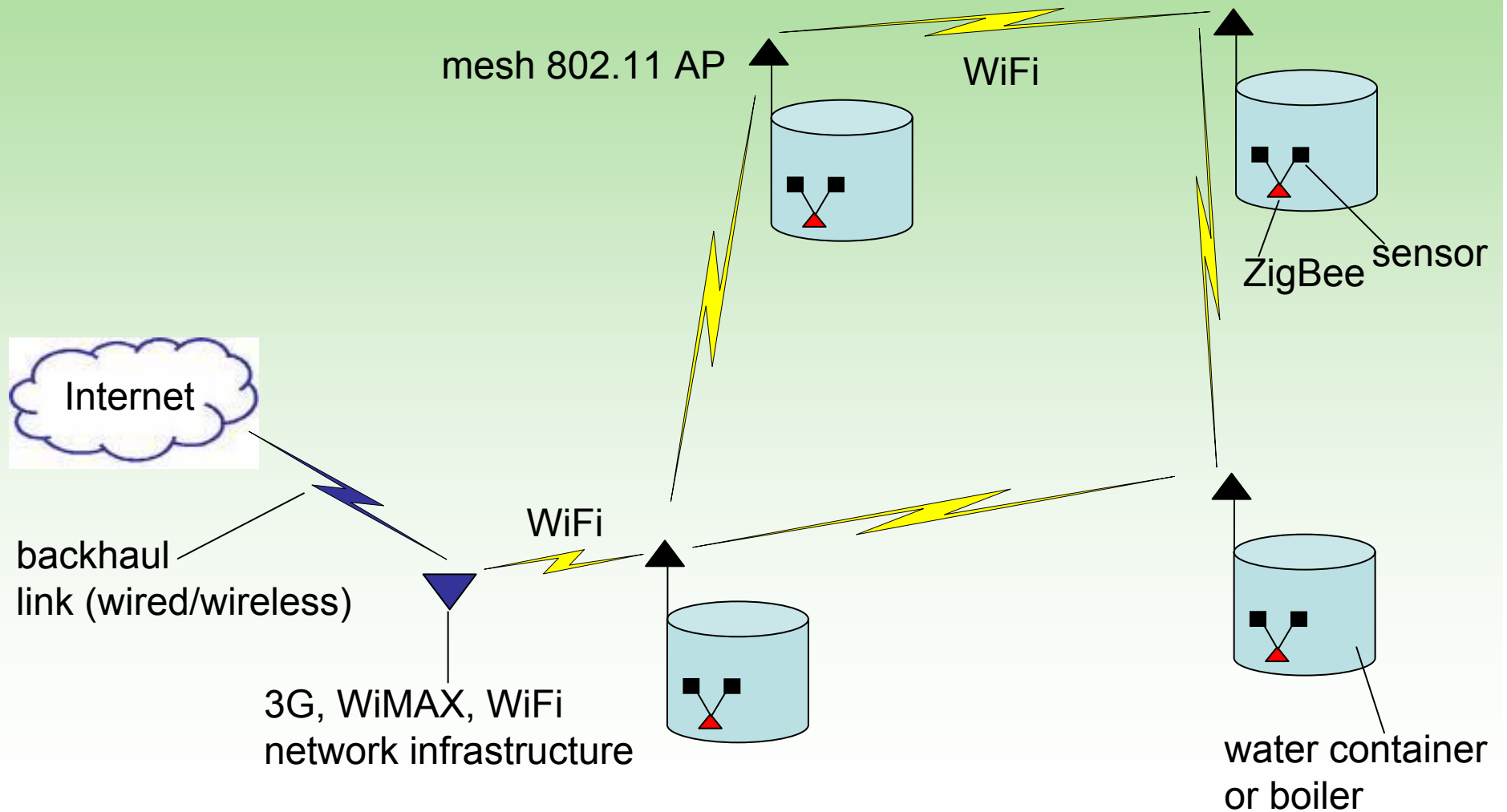
Zigbee - Home Sensor Network

for lights, security system, fire system, and the heating and air conditioning

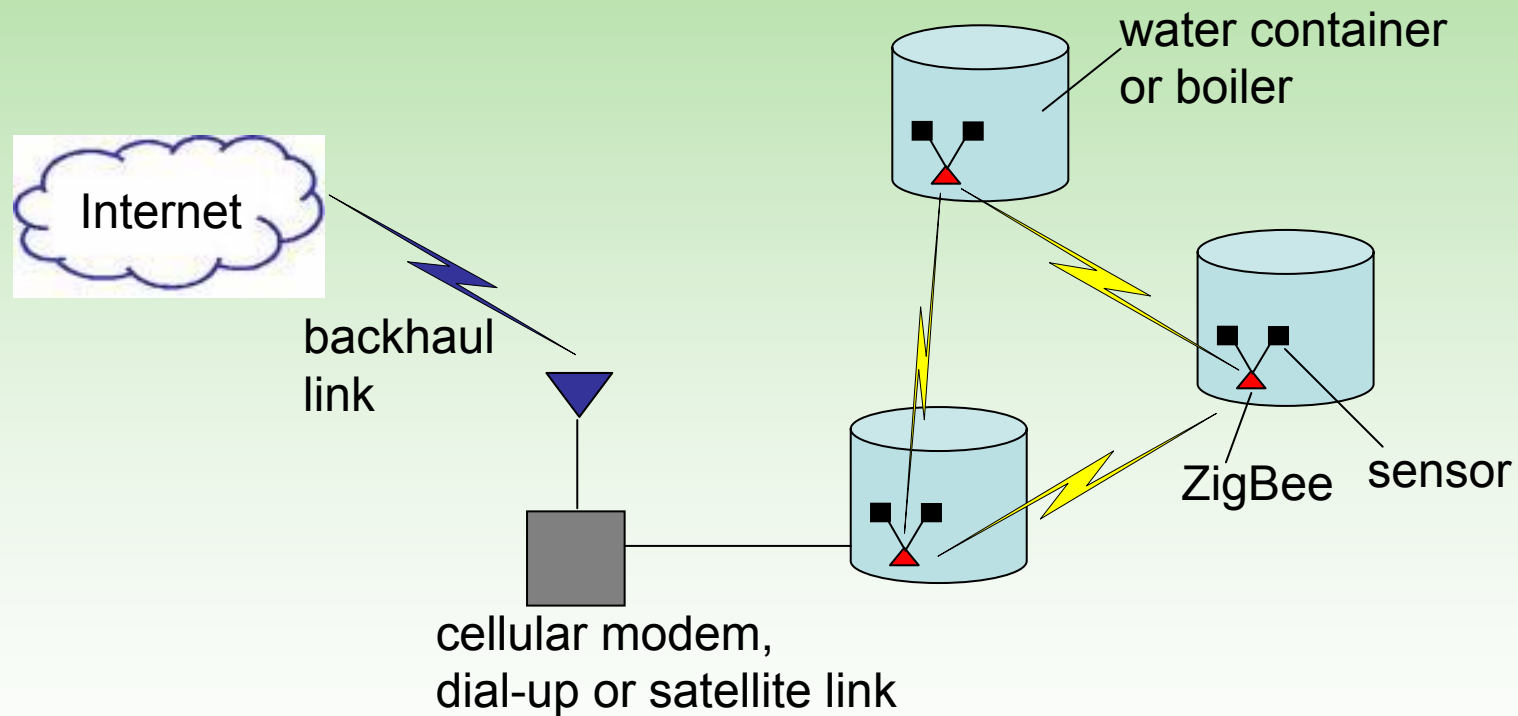


low power, low cost, low data rate

Wireless Field Data Collection

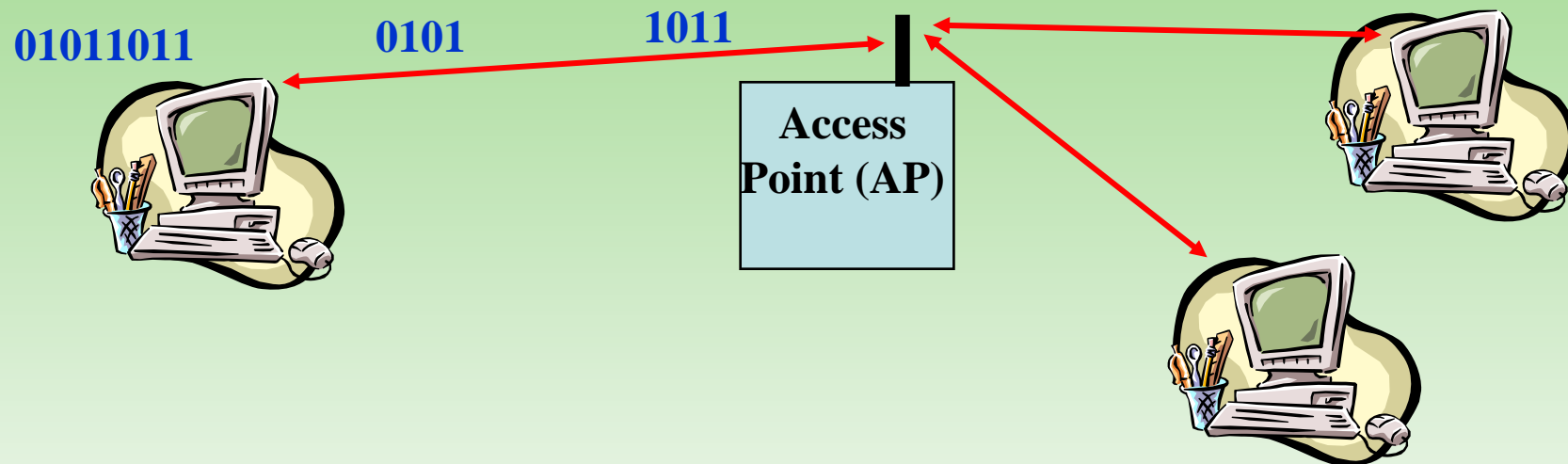


Wireless Field Data Collection (cont.)



Wireless LAN's (WiFi 802.11x)

Wireless Local Area Networks (WLANs)

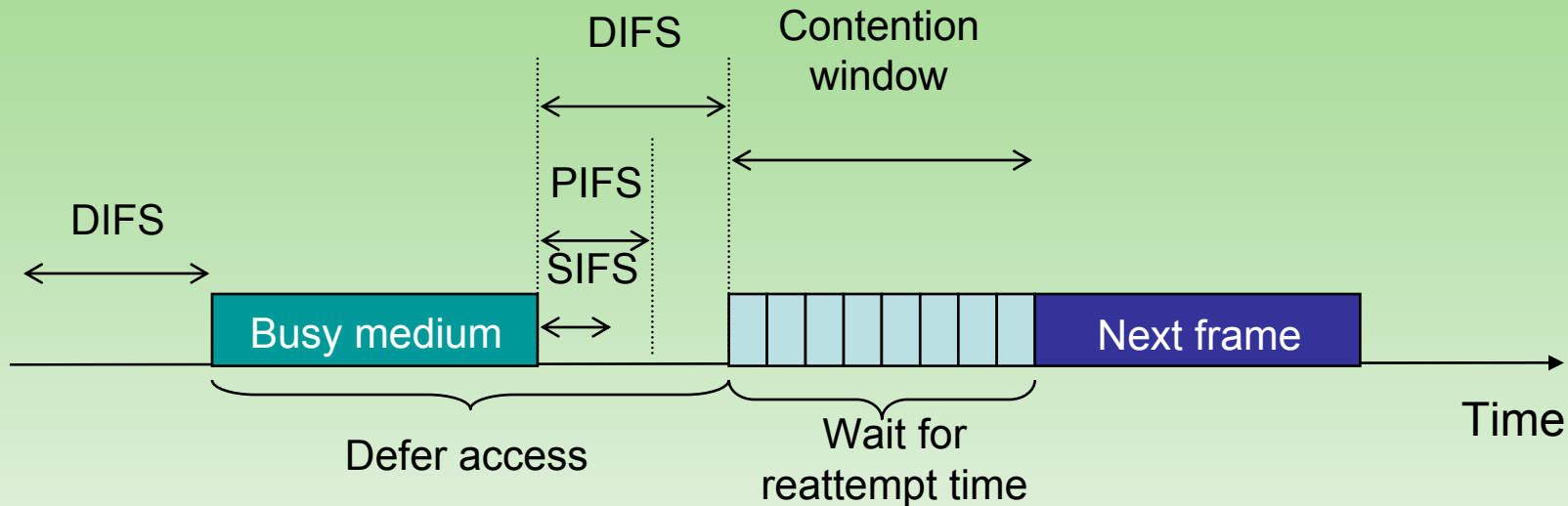


- WLANs connect “local” computers (100m range)
- Breaks data into packets
- Channel access is shared (random access)
- Backbone Internet provides best-effort service
- QoS needed for real-time apps (e.g. voice, video)

Wireless LAN Standards

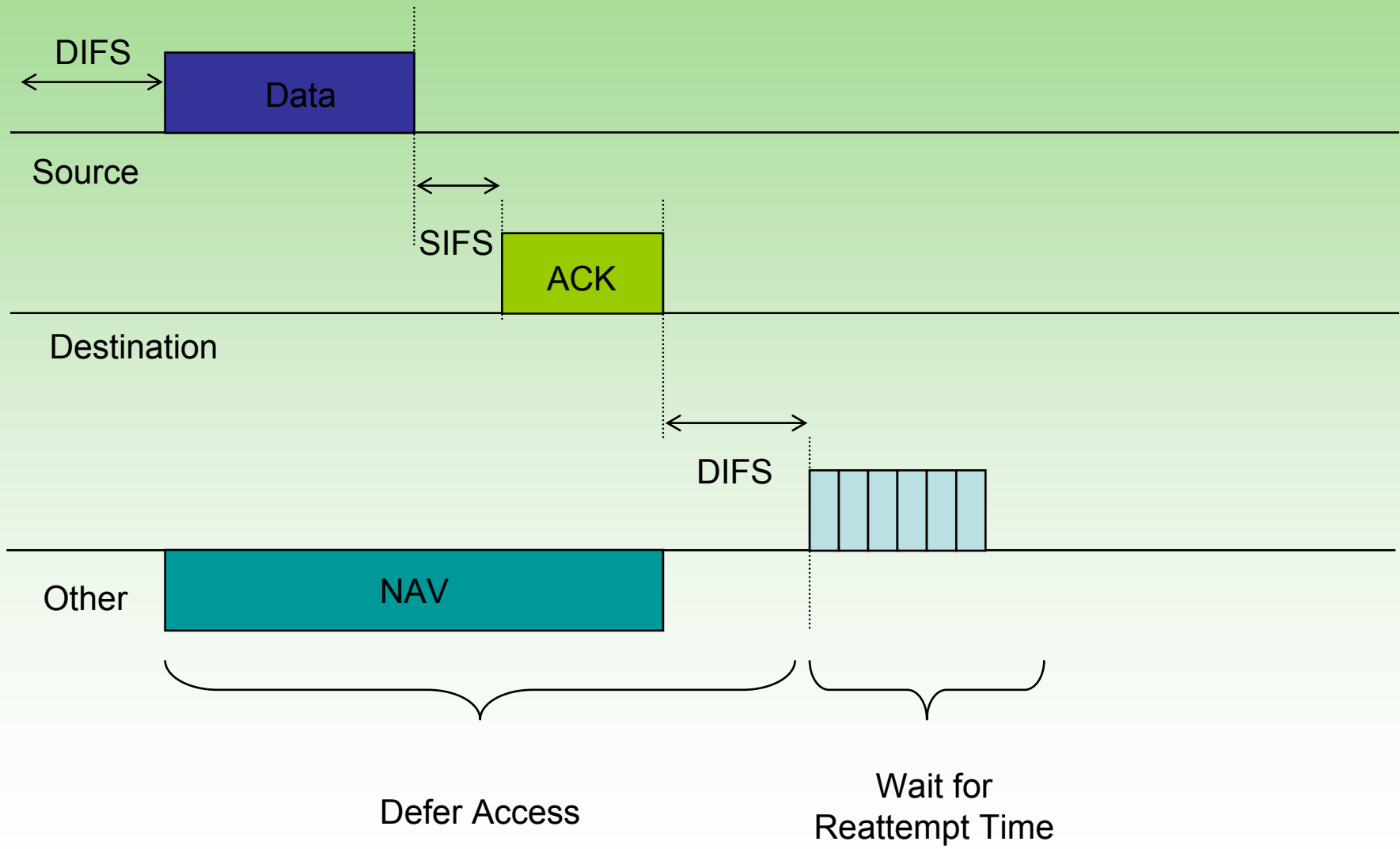
- 802.11b (**Older Generation**)
 - Standard for 2.4GHz ISM band (80 MHz)
 - Spread spectrum
 - Speeds up to 11 Mbps
- 802.11g/a
 - Standard in the 2.4/5.8 GHz band
 - OFDM
 - Speeds up to 54 Mbps
- 802.11n (**Newer Generation**)
 - Draft Standard in the 2.4/5.8 GHz band
 - OFDM and MIMO (20/40 MHz channel)
 - Speeds up to 600 Mbps

MAC: CSMA-CA using Distributed Coordination Function (DCF)



- DCF provides basic access service
 - Asynchronous best-effort data transfer
 - All stations contend for access to medium
- CSMA-CA
 - Ready stations wait for completion of transmission
 - All stations must wait *Interframe Space (IFS)*

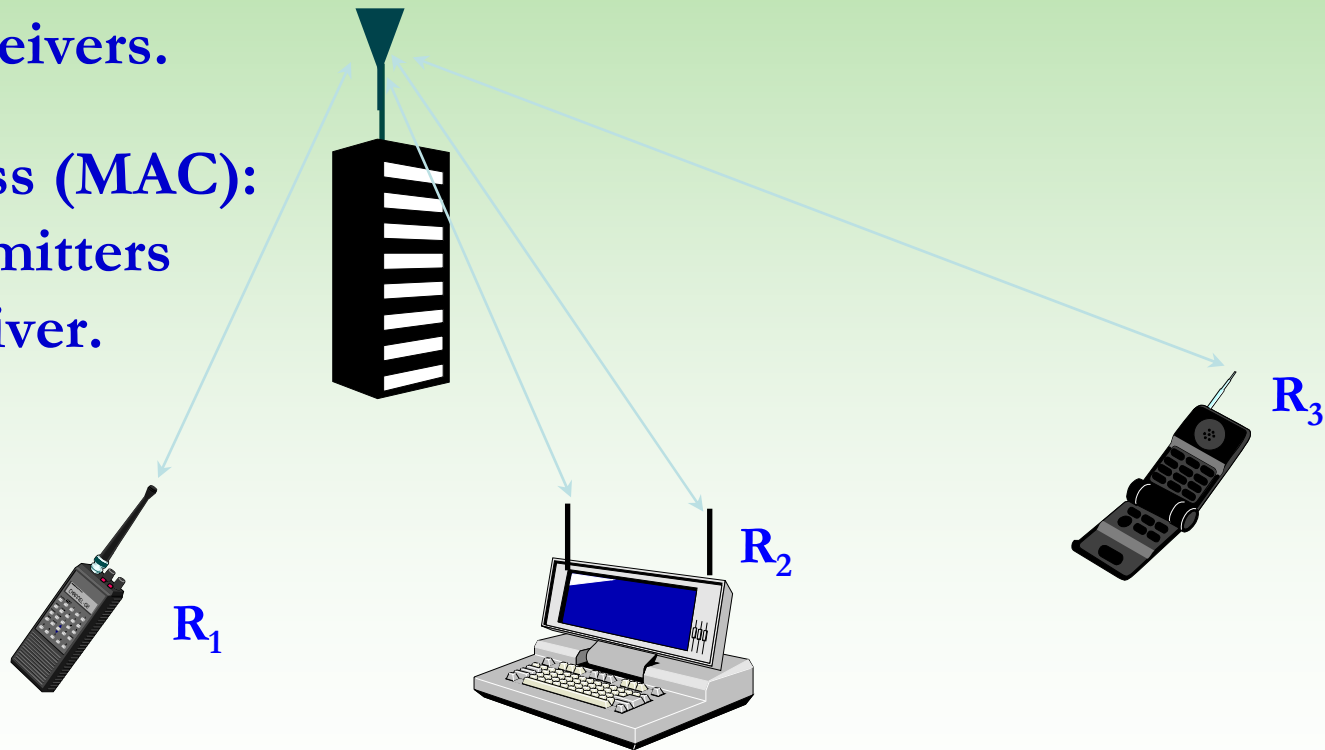
CSMA-CA (cont.)



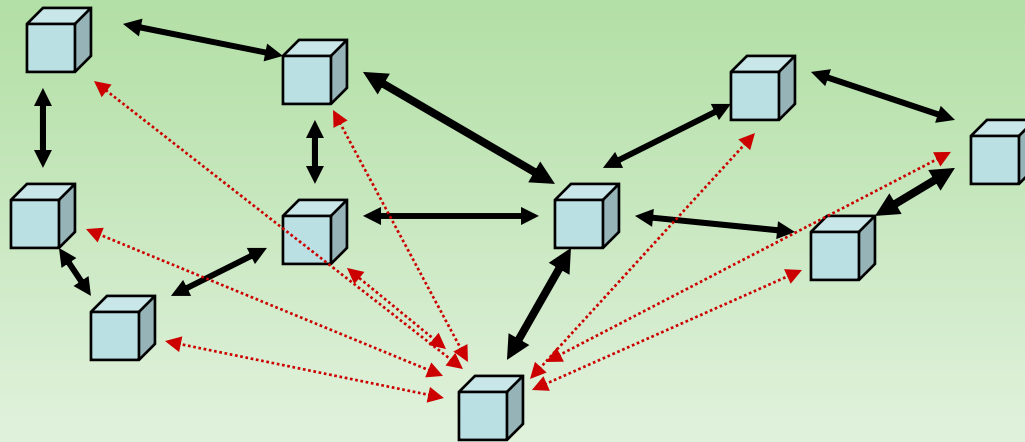
Broadcast and Multiple Access Channels

Broadcast (BC):
One Transmitter
to Many Receivers.

Multiple Access (MAC):
Many Transmitters
to One Receiver.



Ad-Hoc Networks



- Peer-to-peer communications.
- No backbone infrastructure.
- Routing can be multihop.
- Topology is dynamic.
- Fully connected with different link SINRs

WiMAX (802.16d/e)



Mobile-WiMAX 802.16e

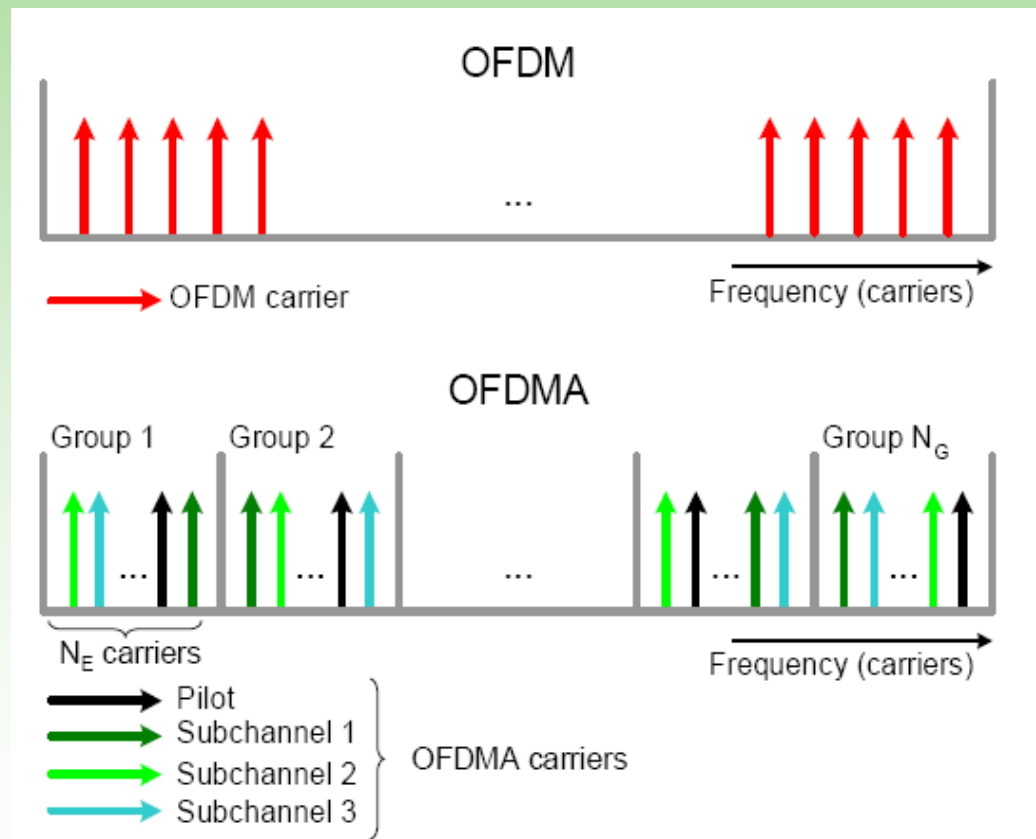
Technology Overview

- Non line of site, up to 4-6 mbps per user for a few km
- 2.5 GHz (US) and 3.5 GHz licensed bands
- Channel bandwidth from 1.25 to 20 MHz
- QPSK, 16 QAM and 64 QAM modulation
- OFDMA access (orthogonal uplink)
- TDD for asymmetric traffic and flexible BW allocation
- Advanced Antenna Systems (AAS): Beamforming, spatial diversity, spatial multiplexing using MIMO (2x2)

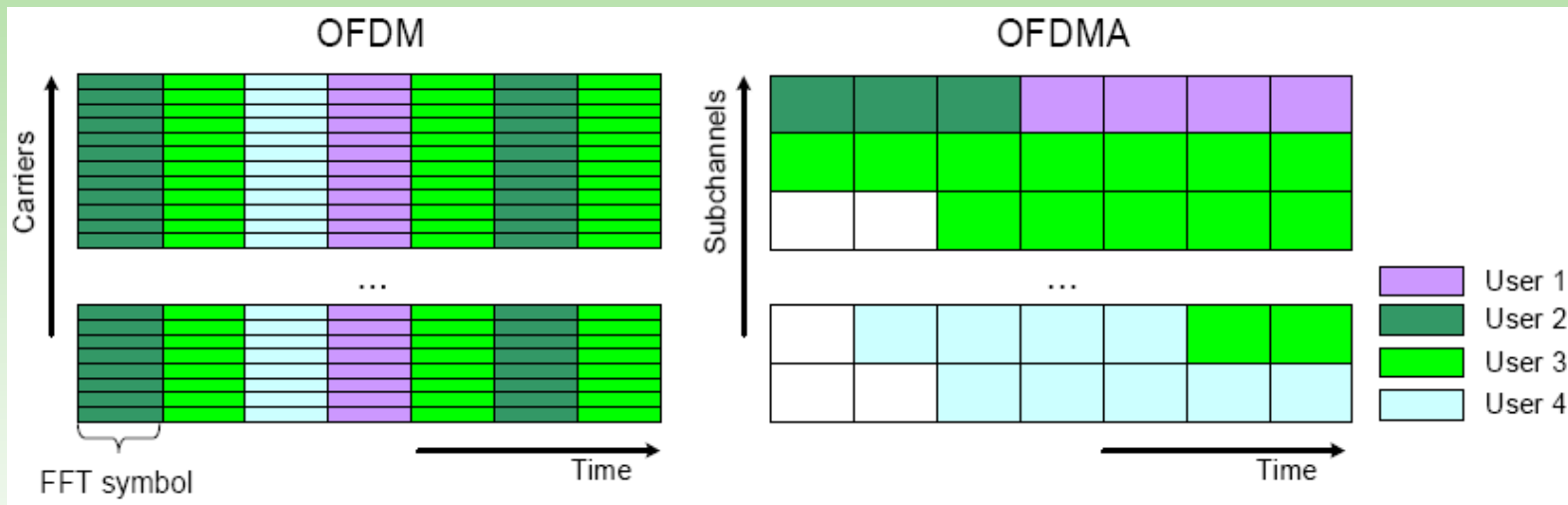
Notable WiMAX Deployments in NA



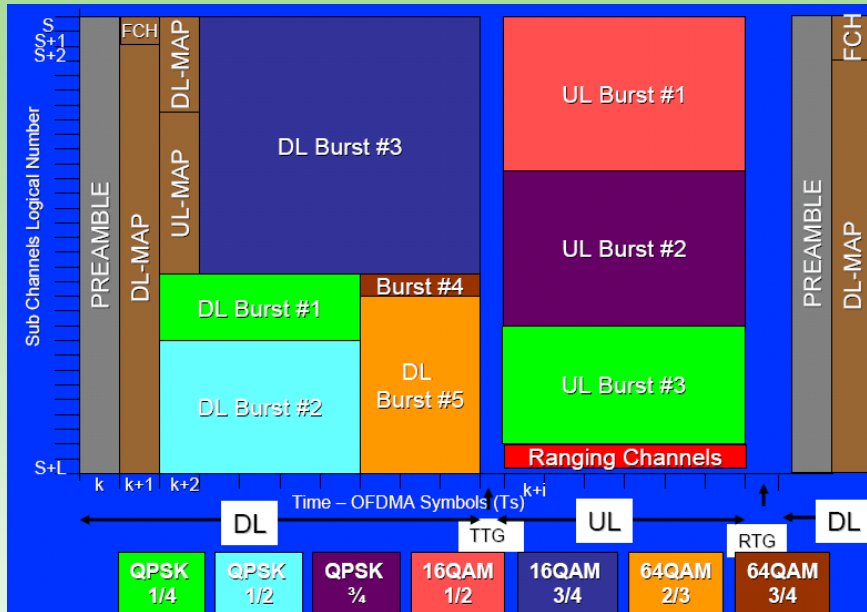
OFDM vs. OFDMA



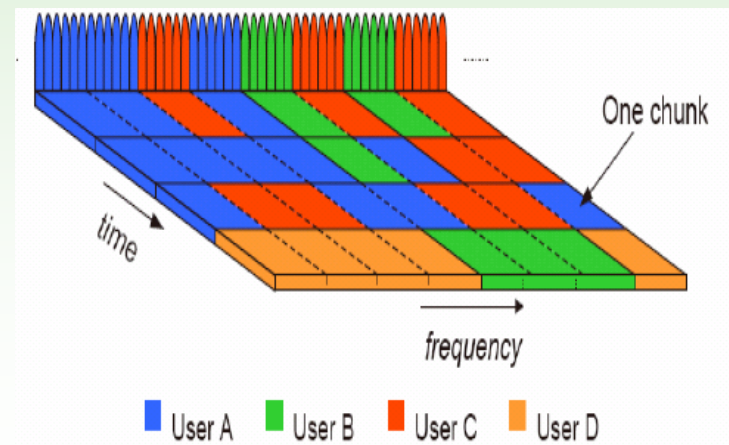
OFDM vs. OFDMA



WiMAX Frame Structure



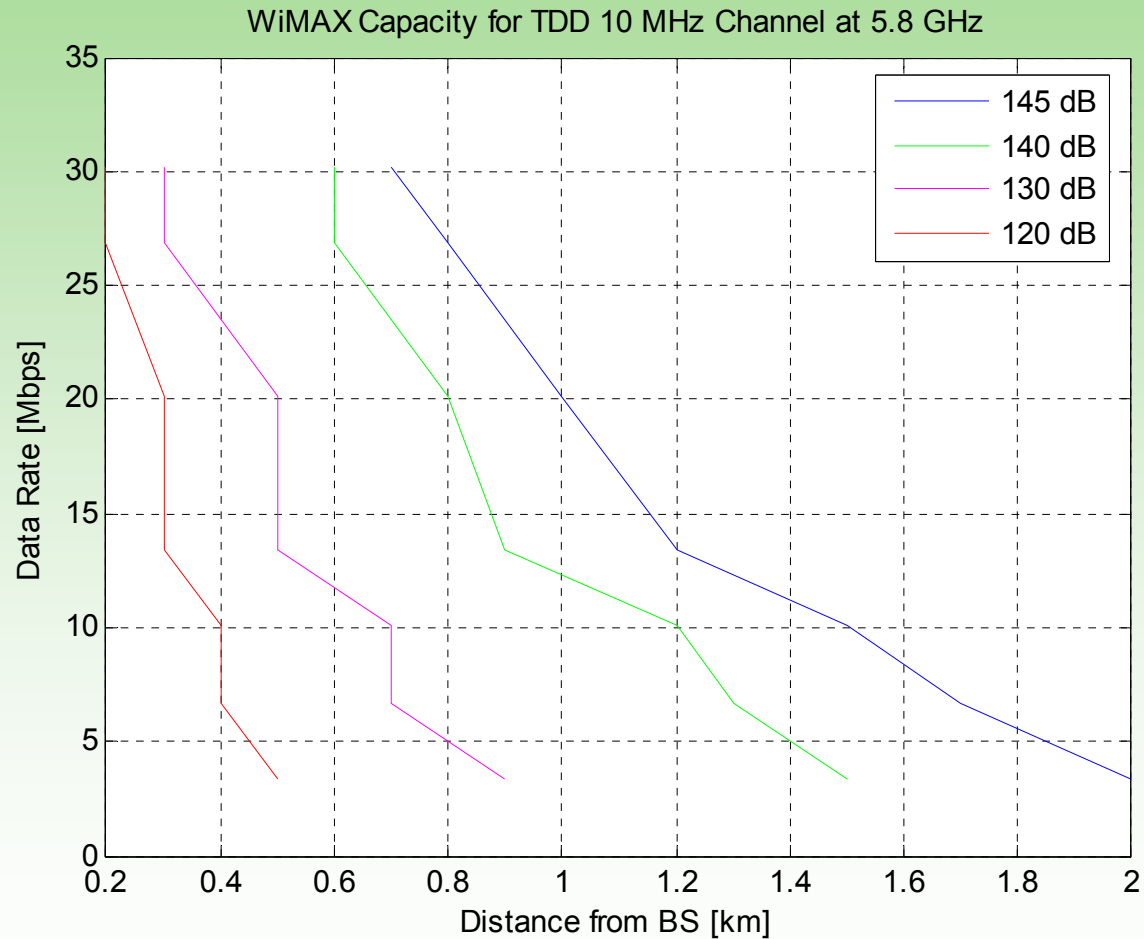
OFDMA TDD Frame Structure



Time/Frequency Multi-User Diversity

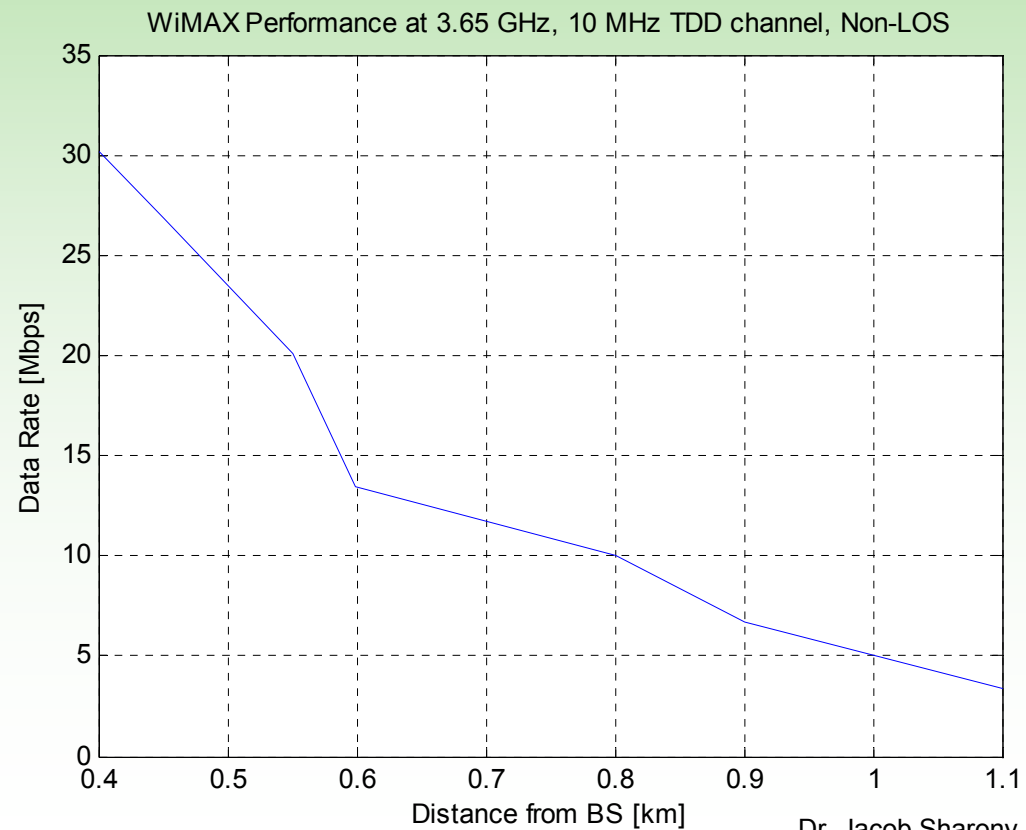
Expected Performance Per Sector

Capacity for Different Total Allowable Loss



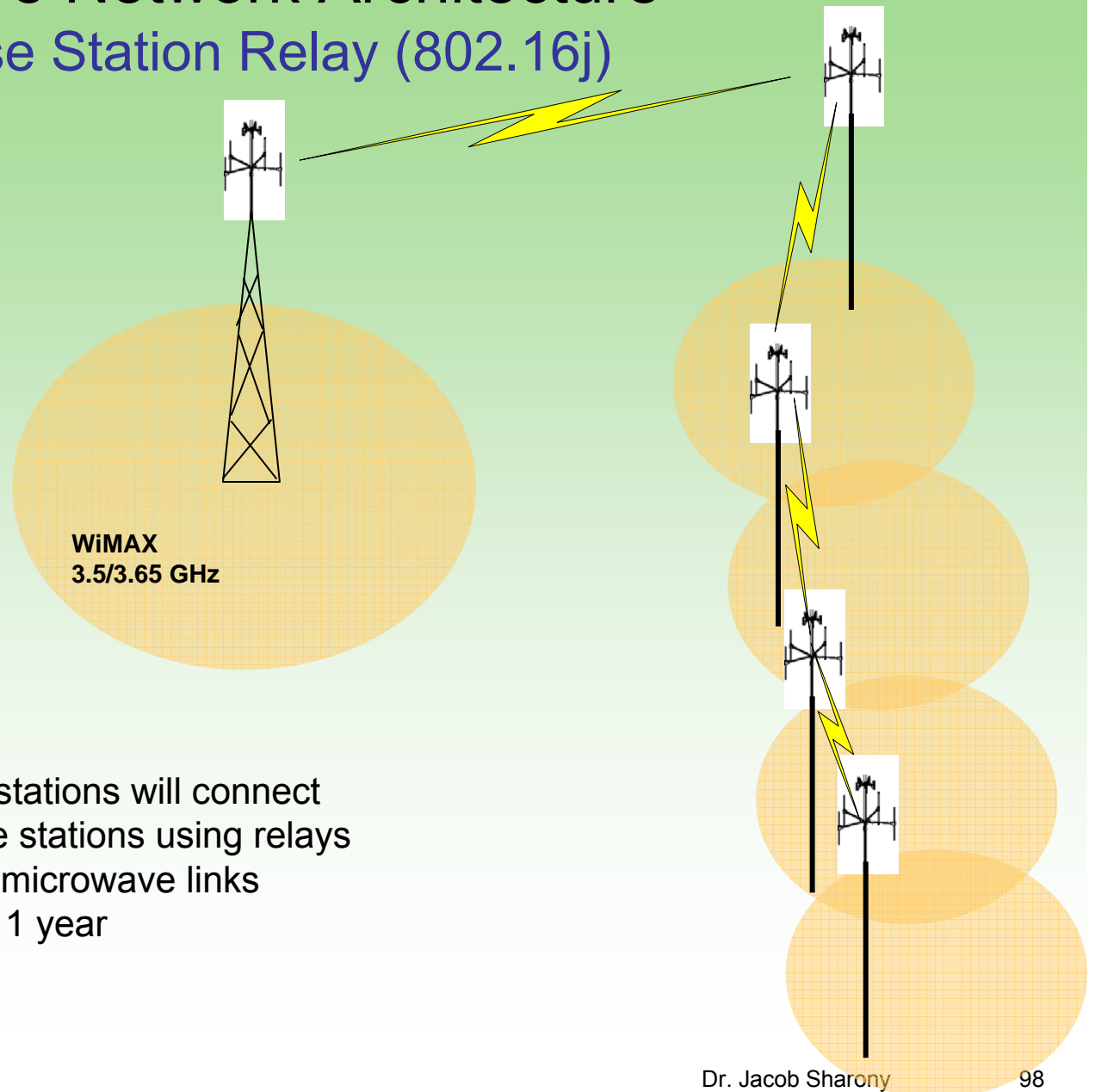
Expected Performance

- Range (3.65 GHz band): 1-2 km
- Max capacity (10 MHz TDD channel): ~30 Mbps
- Min capacity (10 MHz TDD channel): ~3 Mbps
- Performance will depend on SS location and channel conditions



Future Network Architecture

Base Station Relay (802.16j)



- Wired base stations will connect “floating” base stations using relays
- No need for microwave links
- Time frame: 1 year

3.65 GHz Map - Exclusion Areas



Thank You!

jacob.sharony@stonybrook.edu

www.ece.sunysb.edu/~jsharony

www.cewit.org