In-Building Wireless Networks

Mitchell Shnier

Lance Communications

Wireless Local Area Networks

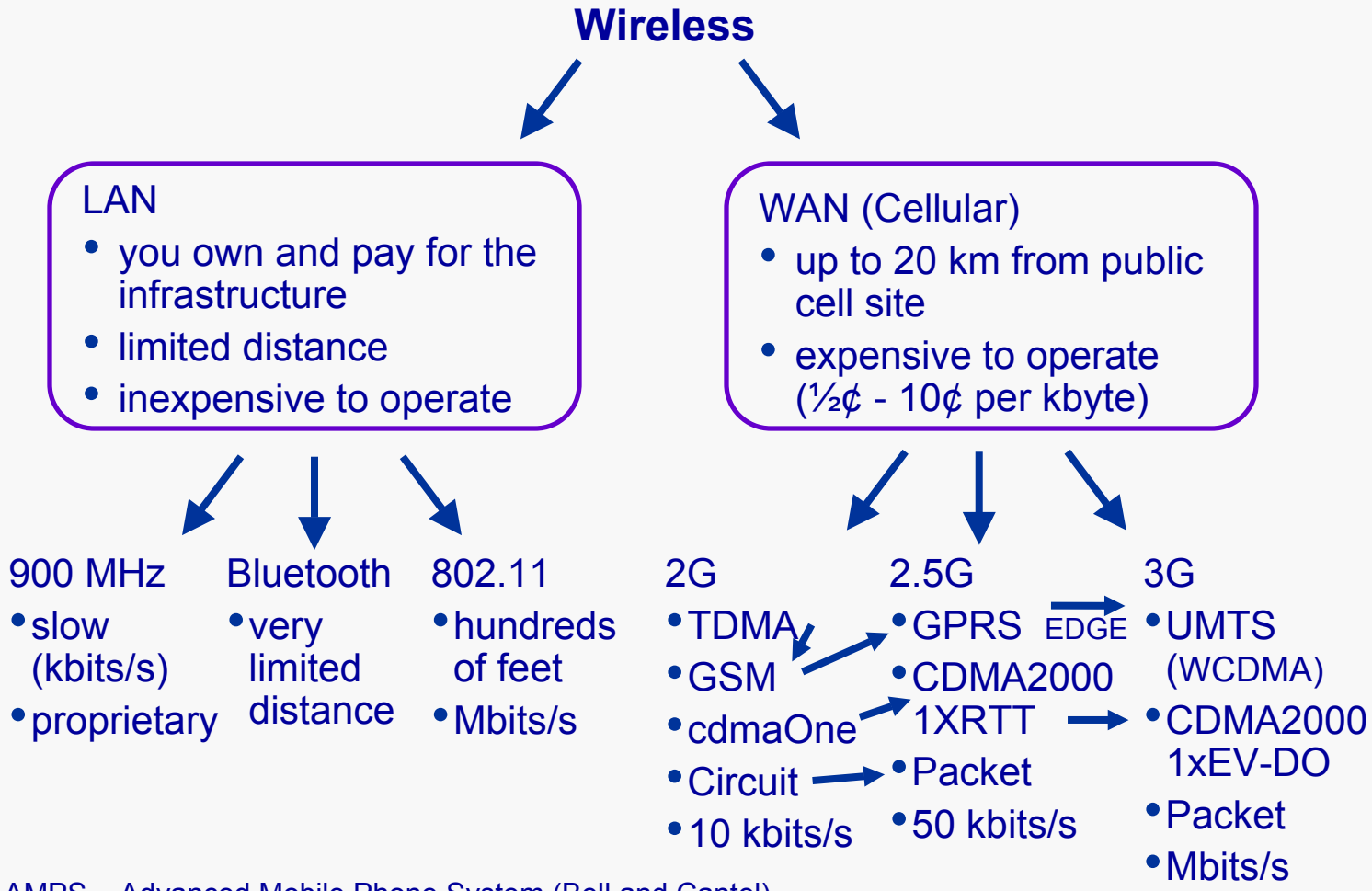
- Overview
  - motivation and perspective
- Background
  - history and standards
- Management
  - configuration and security
- Applications
  - Hot Spots and AS/400s

Overview

Motivation

- mobile
  - lift-trucks, warehouse staff
- temporary
  - conference rooms, hotels, airports
- lower installation costs, easier moves
- no cables, no connectors
- simpler and faster connectivity for user

Wireless Communications



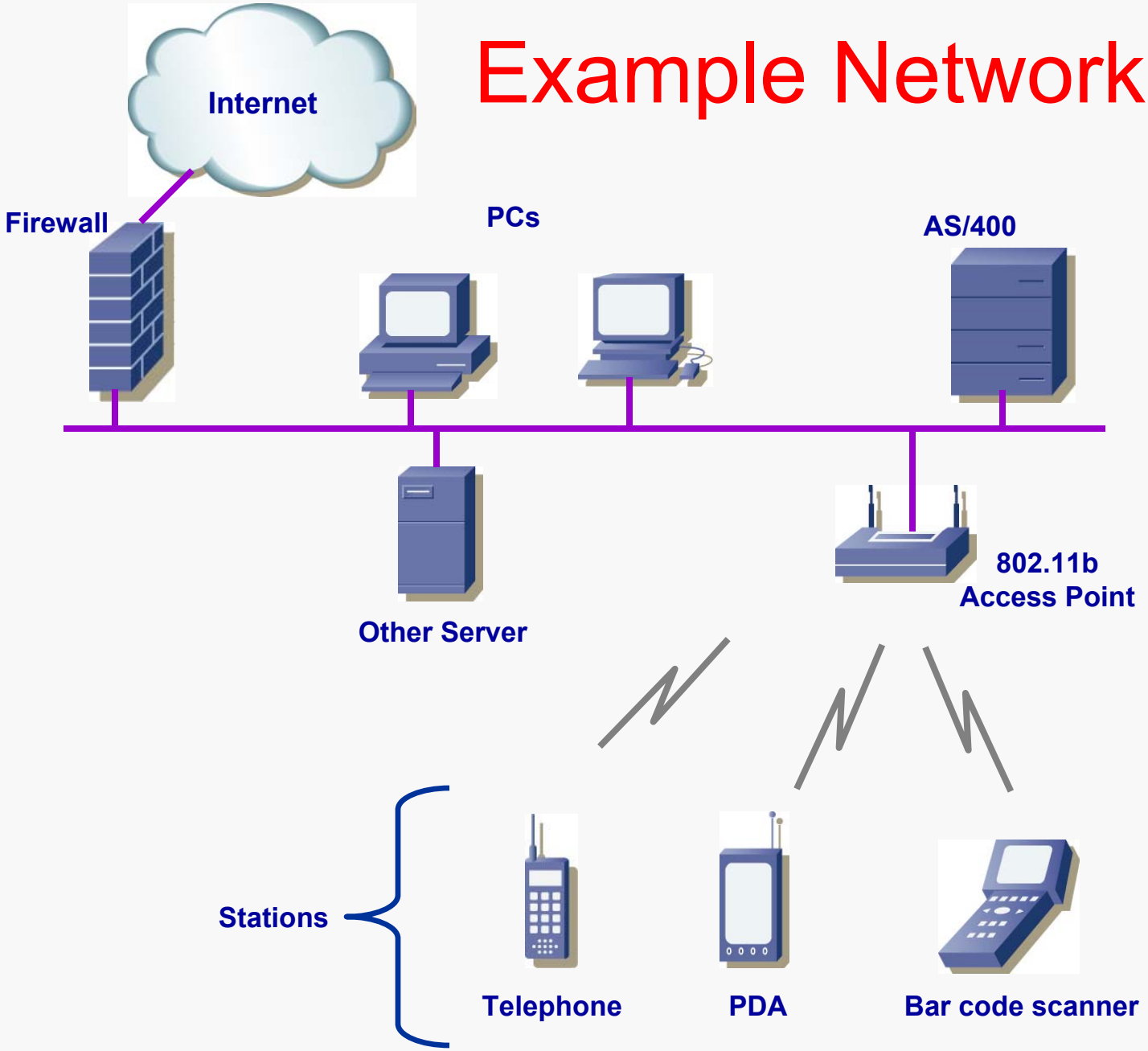
AMPS – Advanced Mobile Phone System (Bell and Cantel)
TDMA – Time Division Multiple Access (Rogers)
GSM – Global System for Mobile Communication (Fido)
CDMA – Code Division Multiple Access (Bell, Telus)
WCDMA – Wideband CDMA
GPRS – General Packet Radio Service
LAN – Local Area Network
WAN – Wide Area Network
EDGE – Enhanced Data Rates for Global Evolution
1XRTT – One times bandwidth (1.25 MHz) Radio Transmission Technology
1xEV-DO – Evolution, Data Optimized
UMTS – Universal Mobile Telecommunications System
*x*G – *x* Generation Cellular Telephones

Devices that use 802.11b

- Wireless Internet routers
  - 14 million sold last year
- PCs
  - 100 million PCs sold last year
    - plus 30 million laptop PCs
  - usually laptops with PCMCIA cards
    - 10 million Wi-Fi cards sold last year
- Wireless bar code scanners
- PDAs (Windows CE / Palm)
  - usually with Compact Flash (CF) cards
- IP Telephones
  - available, but not popular yet

PCMCIA – Personal Computer Memory Card International Association PDA – Personal Digital Assistant

Example Network



Frequency Bands

Certain frequency bands don't require FCC or Industry Canada approval

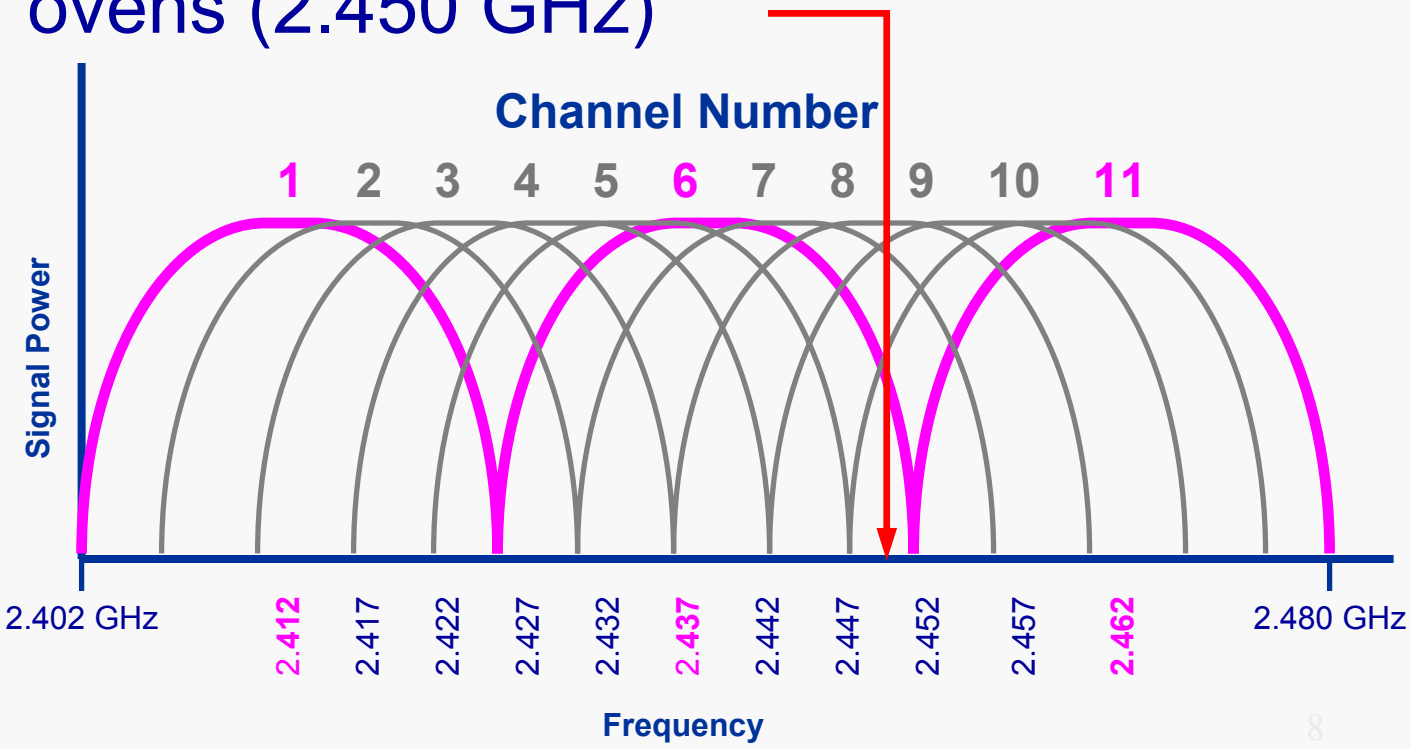
- ISM
  - 900 MHz (cordless telephones, proprietary wireless)
  - 2.4 GHz (cordless telephones, microwave ovens, Bluetooth, 802.11b, 802.11g)
  - 5.8 GHz (cordless telephones)
- U-NII
  - 5.2 GHz (802.11a)

FCC – Federal Communications Commission ISM – Industrial, Scientific, and Medical
U-NII – Unlicensed National Information Infrastructure

Channels

802.11b has 11 channels

- but only three (1, 6, and 11) don't interfere with each other
- channel 1 is farthest from microwave ovens (2.450 GHz)



IEEE 802.11b

- **IEEE**
  - Institute of Electrical and Electronics Engineers
- **802** Committee
  - formed in February, 1980
- **.11** Wireless Local Area Networks Working Group
- **b** standard
- *Wi-Fi Alliance* does interoperability testing
  - previously called WECA

The IEEE 802.11 Family Tree

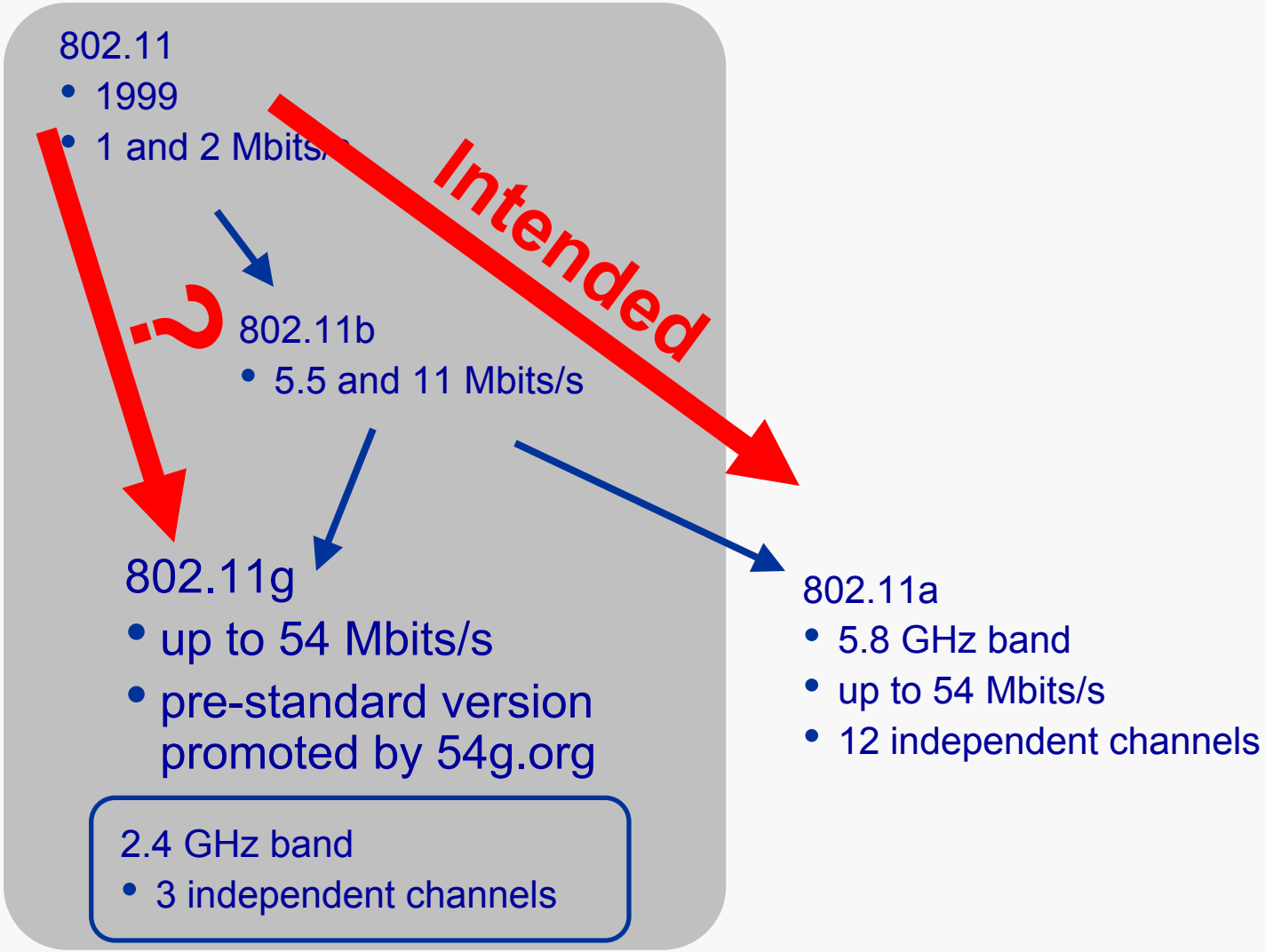
802.11
- 1999
- 1 and 2 Mbits/s

802.11b
- 5.5 and 11 Mbits/s

2.4 GHz band
- 100 mW per channel
- 3 independent channels

802.11a
- 5.8 GHz band
- Up to 54 Mbits/s
  - much lower useable throughput
- 12 independent channels
  - 4 low power (40 mW)
  - 4 medium power (200 mW)
  - 4 high power (800 mW)

The IEEE 802.11 Family Tree



RF Coverage and Installation

- Site survey
  - built-in tools (noise and signal strength)
  - specialized devices (airmagnet.com, bvsystems.com)
- Access Point location
  - not on an external wall
    - provides access outside your building
- Antenna's coverage pattern
- IP address assignment

RF – Radio Frequency

Power for Access Points

Convenient if power provided over UTP data cable

- called *Power over Ethernet* or *In-line Power*
- standardized in 802.3af, *DTE Power via MDI*
- 48DC, at up to 350 mA, over 2 pairs
  - either the Ethernet pairs (pins 1,2, and 3,6)
    - Alternative A, preferred by Cisco (only 2 pairs required)
  - or the other two pairs (pins 4,5, and 7,8)
    - Alternative B, preferred by PowerDsine (allows mid-span power injectors)
- shutdown and remote reset too
- enables centralized UPS
- monitor device disconnect/cable break
- *probes* to check if device wants power

DTE – Data Terminal Equipment MDI – Media Dependent Interface UPS – Uninterruptible Power Supply

Power for Access Points (con't)

- Will be widely supported (Cisco, 3Com ...)
  - Powered Devices ("PD")
    - IP Telephones, cameras, building access devices ...
  - Power Source Equipment ("PSE")
    - Ethernet hubs and switches

Management

- Usually browser-based
  - mini web server built-in to each Access Point
- Centralized
  - convenient, but usually proprietary
- Some Access Points can detect *rogue Access Points*
  - that is, an unauthorized Access Point

Basic Configuration

- BSSID
  - all devices must match exactly
  - up to 32 characters
- Channel
  - 1 through 11 (in North America)
- Encryption
  - 5-byte or 13-byte secret shared key
- Infrastructure or Ad-hoc mode
  - also called ESS or IBSS (respectively)

BSSID – Basic Service Set Identification

ESS – Extended Service Set IBSS – Independent Basic Service Set

Problems

- Interference
  - microwave ovens
  - cordless telephones
  - Bluetooth
  - other 802.11b (and 802.11g) users
    - both within, and outside your organization
- Limited bandwidth and channels
  - 802.11a is a growth option
- Security and management are often proprietary

Security Problems

- Weak encryption
  - 40/64-bit and 104/128-bit supported
    - errors in implementation are a major problem
- No encryption
  - “war driving” (from “war dialing” hacking from the movie *War Games*)
    - recent survey found 72% of WLANs don’t use any encryption
    - check out NakedWireless.ca for a Toronto map, and NetStumbler.com for the software
- Rogue Access Points
  - what if someone installs their own Access Point on your LAN
    - lets anyone onto your LAN
    - lets them see your PC

Security Problems (continued)

- Key management
  - 802.11b requires all devices to have the same *static* (never changes), *secret* (not known to outsiders) key
  - major weakness
- Others at a Hot Spot might be able to see your files
  - Hot Spots don't usually use encryption

Security Enhancements

- VPNs (available now)
  - needs end-user software at both ends
- Proprietary extensions (available now)
  - Cisco's LEAP
- WPA (Wi-Fi Protected Access)
  - forward-compatible subset of 802.11i
    - software-only upgrade
    - addresses WEP's known weaknesses
  - uses TKIP to change encryption keys frequently and automatically ("*Dynamic WEP*" or "*Dynamic Key Distribution*")
  - adds *mutual authentication*
    - don't connect to a rogue Access Point, and don't let an unknown user onto the network

VPN – Virtual Private Network LEAP – Light Extensible Authentication Protocol
TKIP – Temporal Key Integrity Protocol

Security Enhancements

IEEE 802.1x (partially available now)

- deals with *authentication*
  - who to give access to
  - port-based, for LANs too
- also *key distribution*
  - changing the encyption keys
- EAP
  - supports external authentication servers
    - uses RADIUS (a centralized method of confirming user's username and password)
- can protect you from others snooping at a Hot Spot
  - everybody gets their own, unique, per-session encryption key

EAP – Extensible Authentication Protocol

RADIUS – Remote Authentication Dial-in User Service, RFCs 2865, 2866, and 2869

Future Security Enhancements

802.11i (might also be called WPA2)

- deals with encryption
- new encryption scheme called AES
  - up to 256-bit encryption key
- each client can use a different encryption key
  - PSK mode for small installations with no RADIUS server
- requires new hardware
- available next year

AES – Advanced Encryption Standard PSK – Pre-shared Key

Hot Spots

- Public access often called *Hot Spots*
  - airports, hotels, coffee shops, truck stops
  - private individuals too
  - VPN security is the only security
- Subscription-based service
  - Wayport, Boingo, i-Pass, T-mobile (US)
  - Cometa (IBM, Intel, AT&T)
  - Fatport (Vancouver), Dodo Wireless (Toronto), Spotnik Mobile (Toronto), BOLDstreet (Ottawa), BWireless (Vancouver)
  - Pass-One (roaming)
- Carriers are doing tests
  - Bell Canada (AccessZones), Telus Mobility

802.11b and AS/400s

So where does all this plug into an AS/400

- the answer is that brilliant technology called Ethernet

An Application

- Wireless bar code scanning used to receive and pick inventory
- To the AS/400, scanners appear as 5250 terminals connected through Ethernet
- Scanning bar codes appears as typing characters into fields on a 5250 screen
- Received inventory available sooner, fewer errors, less back-room paperwork, can interleave inventory checks when picking orders

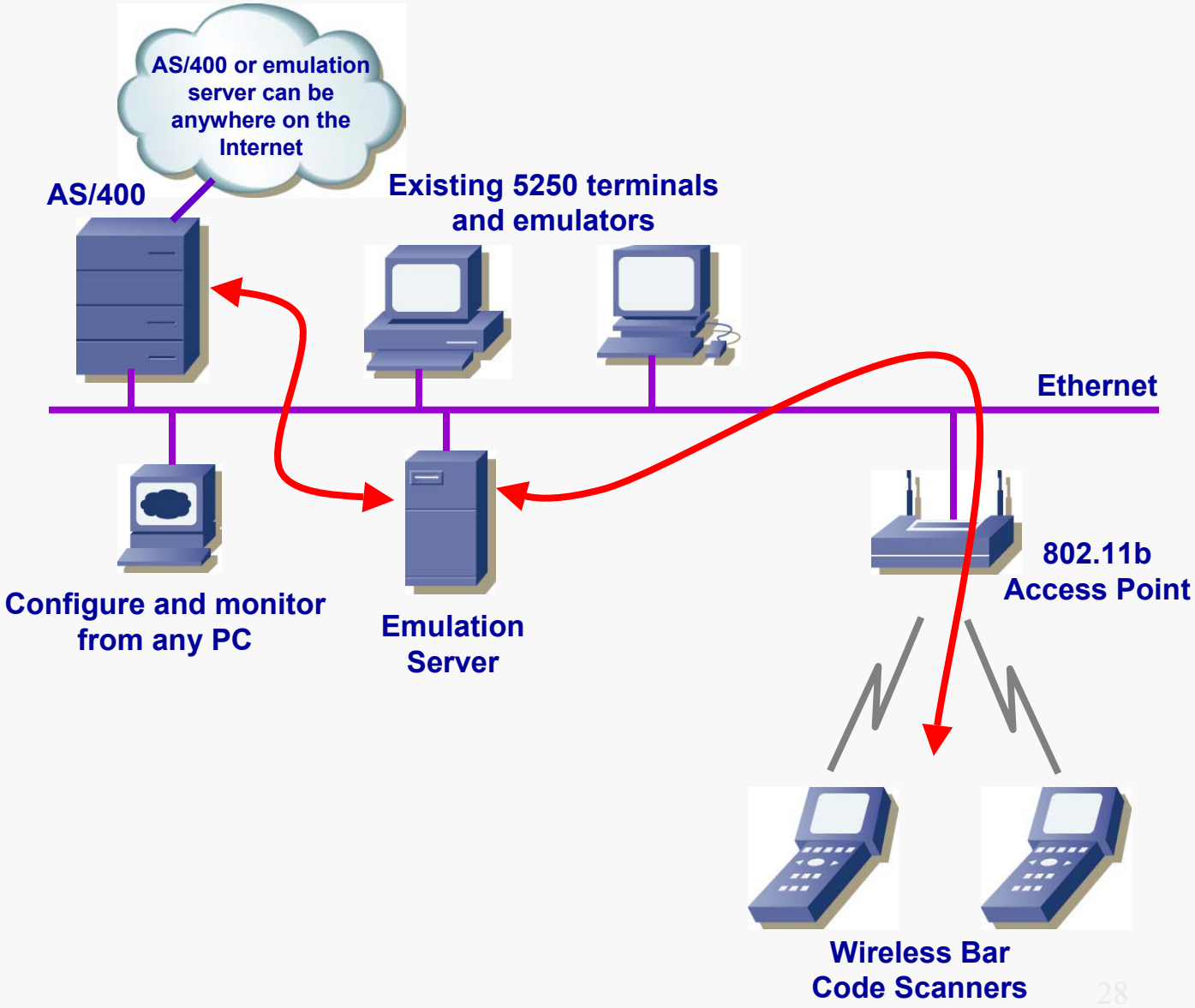
An Application (continued)

- 250,000 square foot warehouse
- 6 Access Points needed (more for office area)
  - $200 to $2,000 each
- Wireless bar code scanners
  - $3,000 to $8,000 each
- Is a big project
  - coordination required between warehouse, IT and upper management

5250 Terminal Emulation

- Some vendors do emulation on a central controller, some on the scanner
- Central emulation can provide
  - easier configuration changes and diagnostics
    - from a web interface
  - monitoring
    - signal strength, active Access Point

Wireless Bar Code Scanning



URLs for Further Information

- 80211-planet.com
  - industry news, technical information
- wi-fi.org
  - interoperability testing

- ieee.org
  - standards documents
- linksys.com, dlink.com, cisco.com
  - equipment
- SpotnikMobile.com, Fatport.com, BOLDstreet.com DodoWireless.ca, BWireless.ca
  - Canadian Hot Spot providers
- Wayport.com, Boingo.com
  - US-based Hot Spot providers

URL – Uniform Resource Locator

Thank you

Call or e-mail anytime:

MShnier@LanceCom.com

www.LanceCom.com

416 222-1430