Denver Tech Days 2002

Wireless LAN Technical Overview & Update
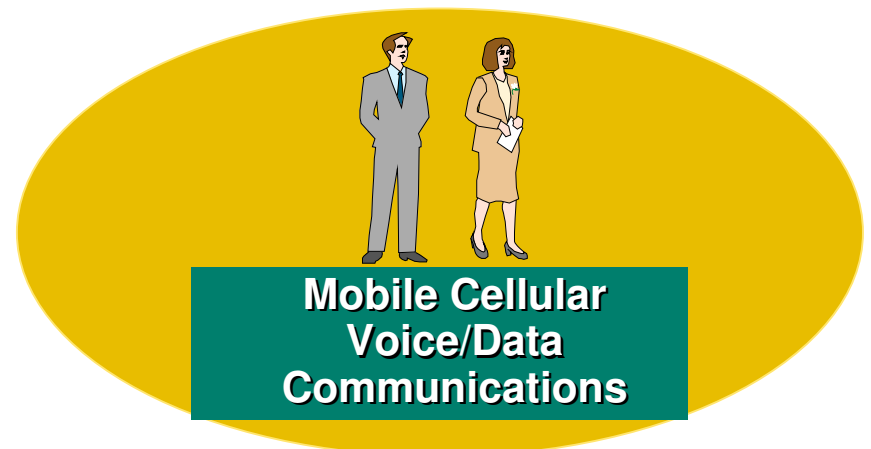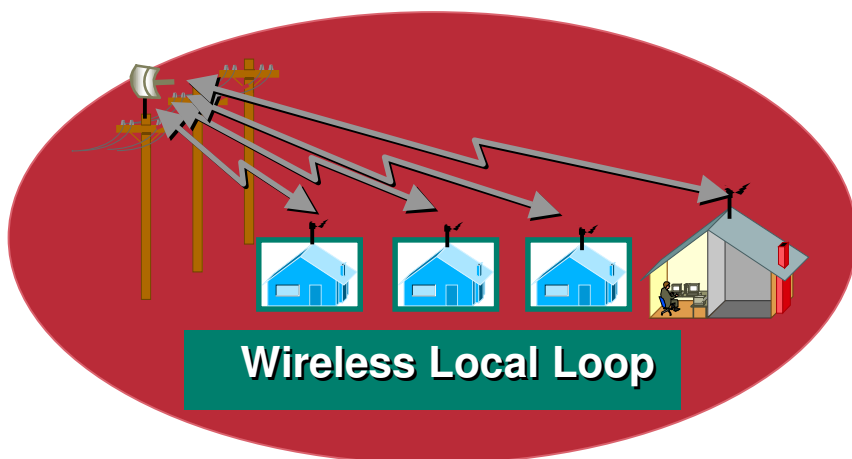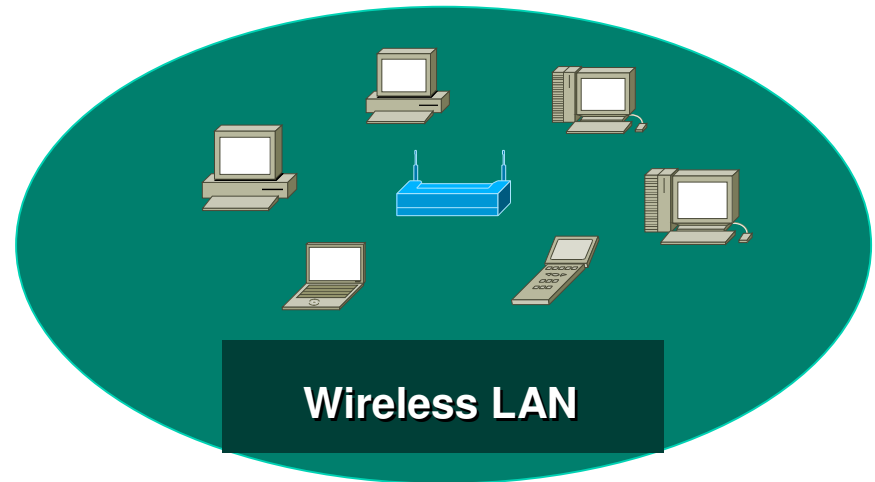
Mike Griffin

mikegrif@cisco.com
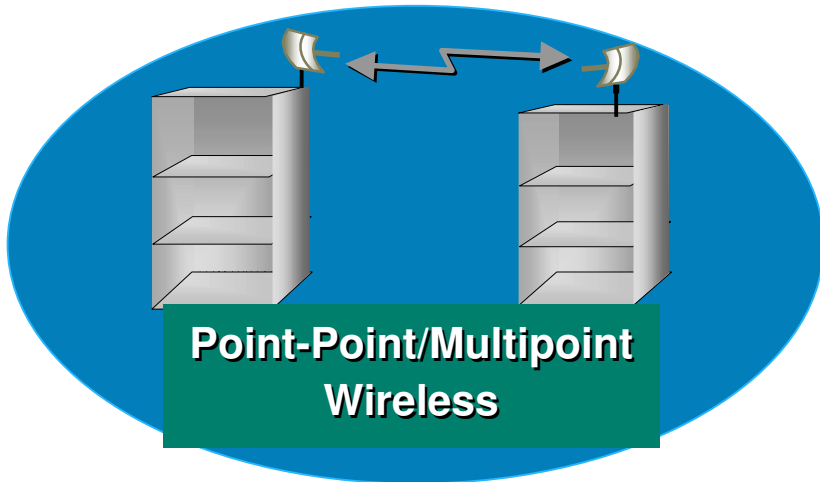
Agenda

- **WLAN Fundamentals**

- **RF Technologies**

- **Alphabet Soup**

- **Advanced WLAN Security**

- **Designing Wireless LAN**

- **Wireless Bridging**

- **What's next for WLANs?**

- **Demo & QnA**

 2

Types of Wireless Networks

Point-Point/Multipoint Wireless

Wireless LAN

Wireless Local Loop

Mobile Cellular Voice/Data Communications

WLAN Business Impact

- **Business Impact**

    Productivity Gains   **22% increase**

    Increased accuracy   **(50% in healthcare)**

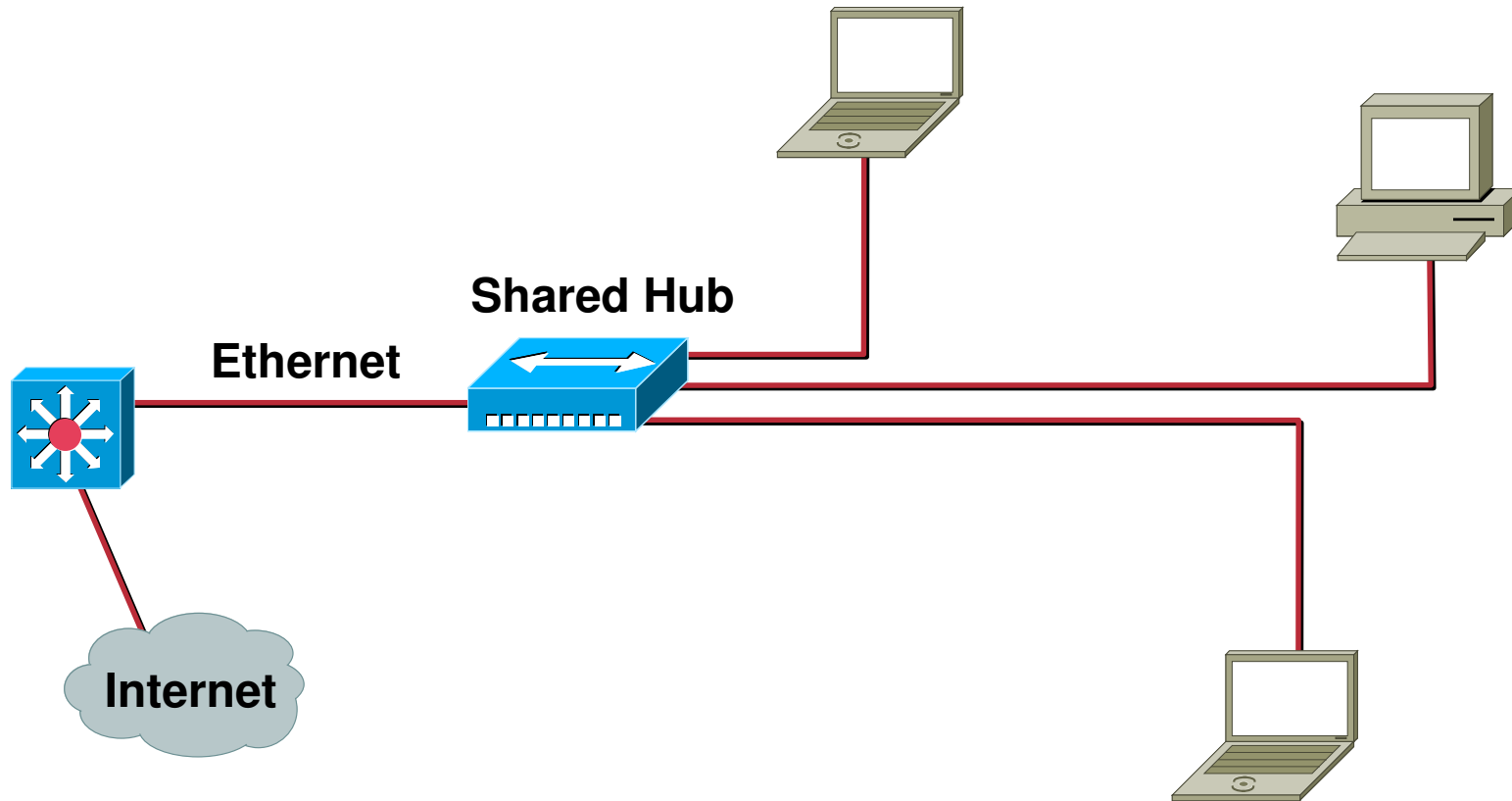   **Greater ROI than expected**

- **End User Impact**

    Quality of Life (convenience, time savings, flexibility)

    Mobility

Source: WLAN Benefit Summary Study – NOP World/Cisco Sept. 01

Shared Local Area Network (LAN)

Shared Hub

Ethernet

Internet

 5

Wireless Local Area Network (WLAN)

Ethernet

Access Point

Internet
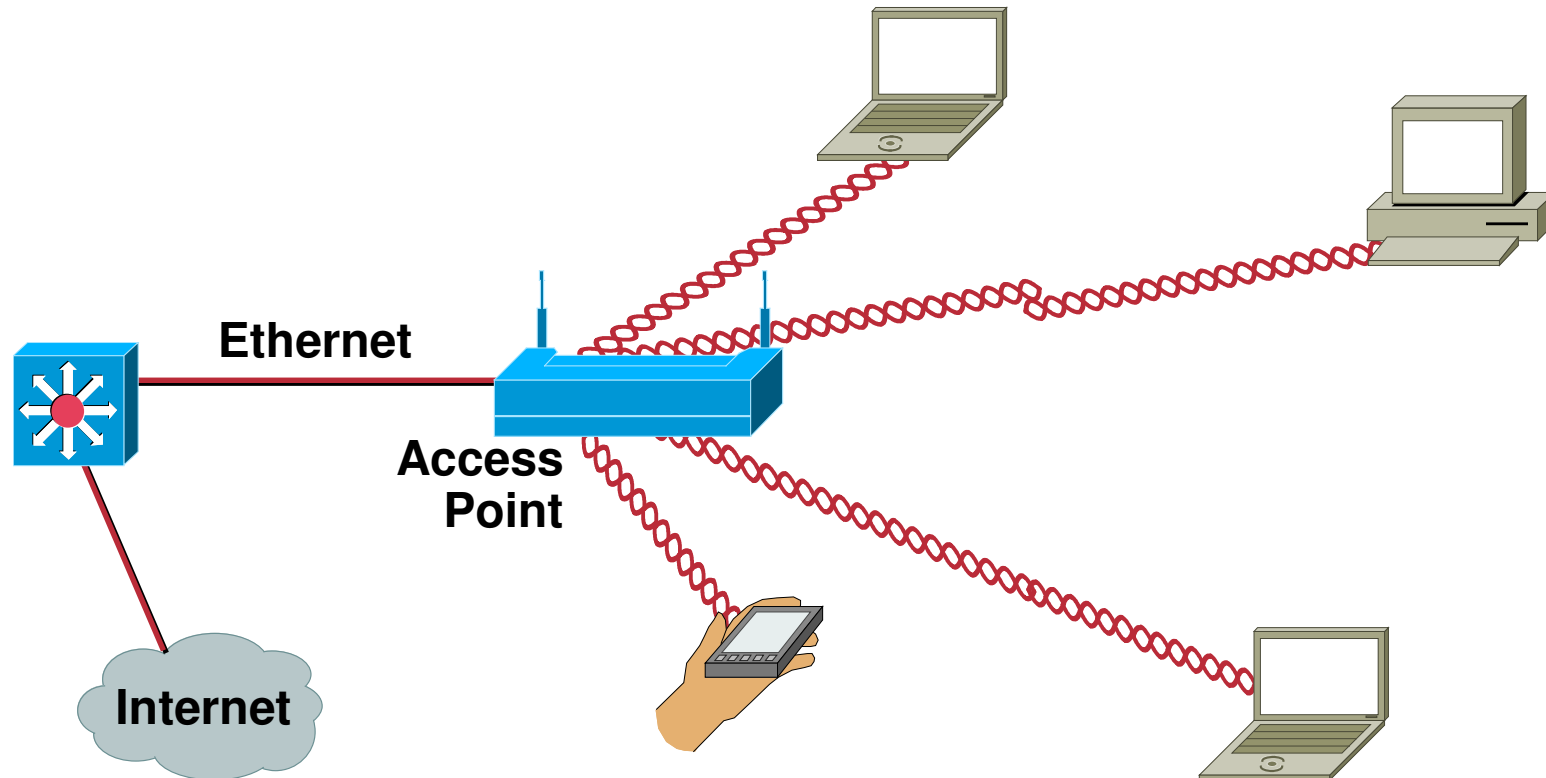
Remember: An Access Point is a SHARED device and has similar performance to a SHARED Ethernet HUB

Typical Single Cell Configuration

LAN
Backbone

Wireless
Cell

SSID=tsunami
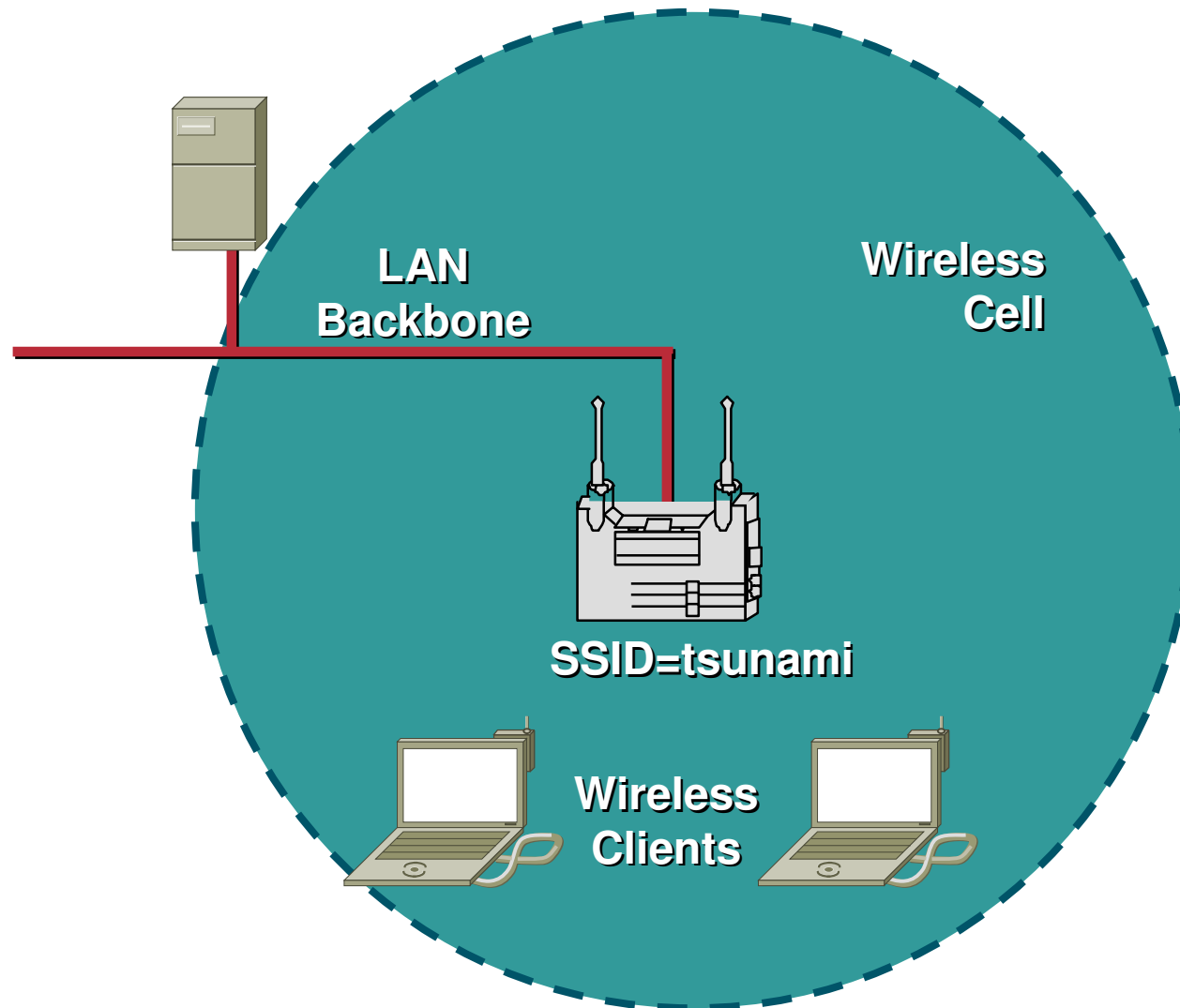
Wireless
Clients

Typical Multicell Configuration

Channel 1

Channel 6

LAN Backbone

Wireless Cell

Access Point

Wireless Cell

Wireless Clients

Wireless Repeater

Channel 1

Wireless Repeater Cell

Wired LAN segment

Channel 1
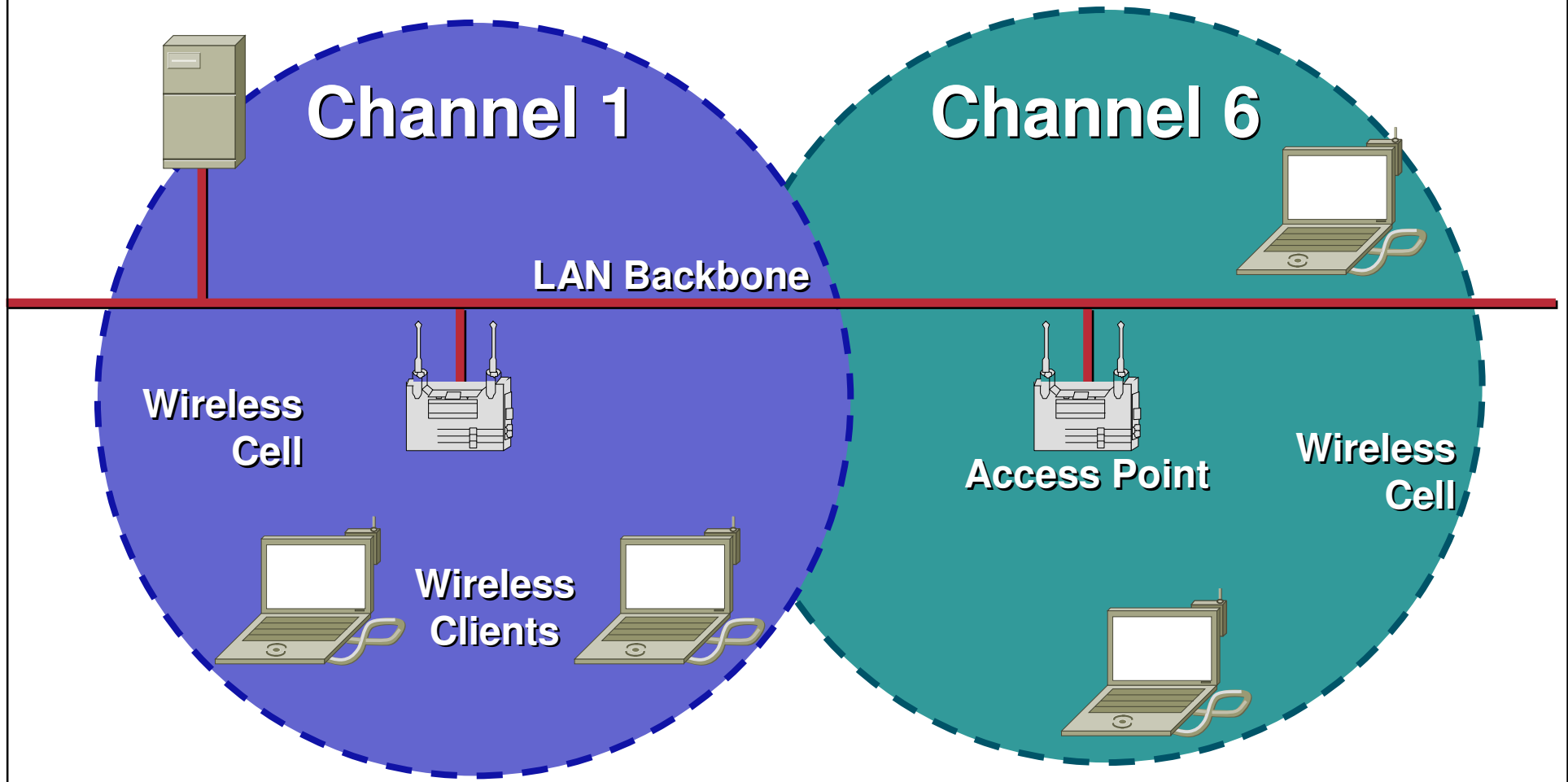
Access Point
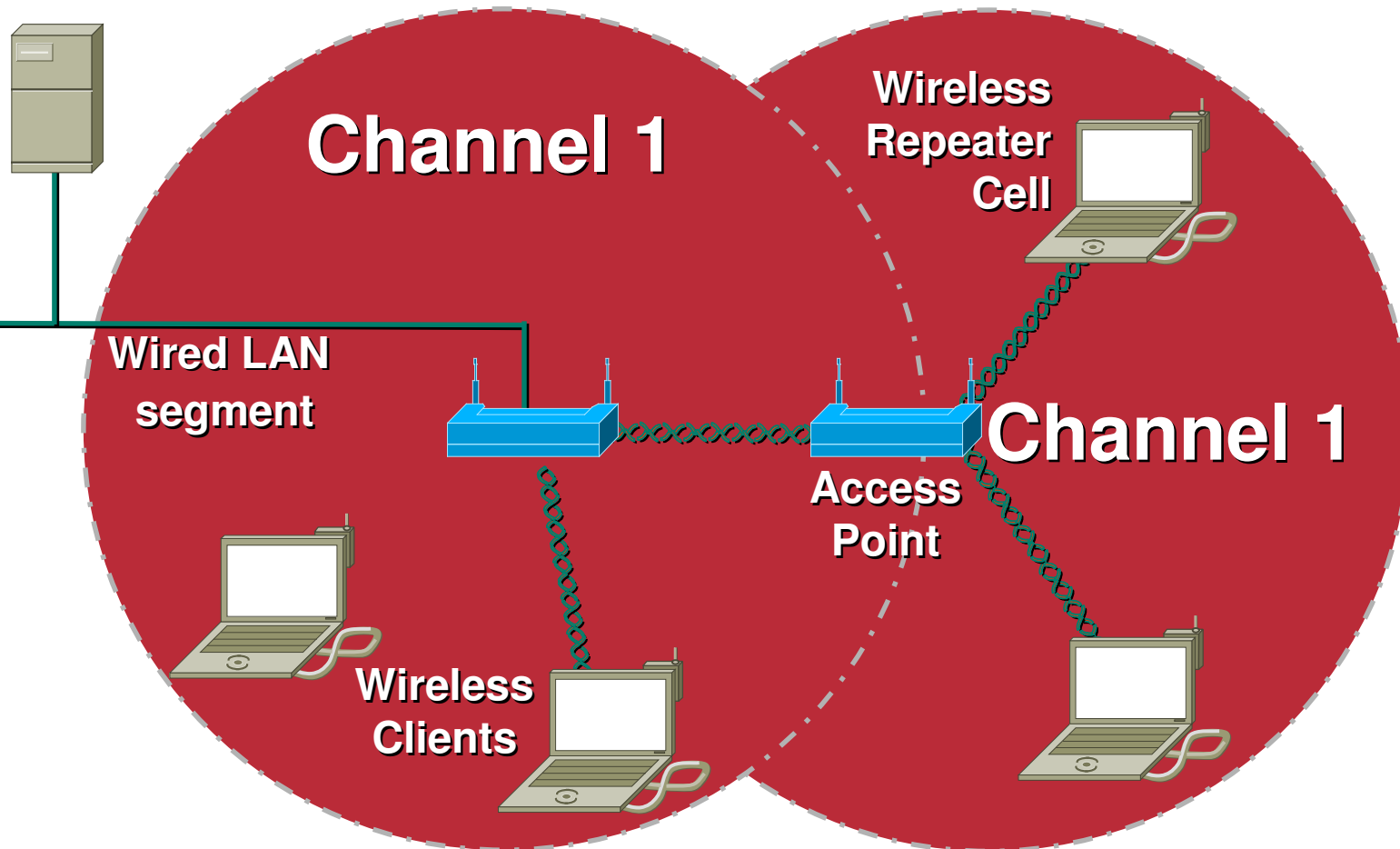
Wireless Clients

Cisco Aironet 350 Series WLAN Product Family

Access Points

Standard & Ruggedized

Wireless Bridges

•Point 2 Point
•MultiPoint

Client Adapters

•Windows
•PocketPC
•Linux
•MacOS
•Novell clts
•DOS

+Dell/IBM/Toshiba/Symbol
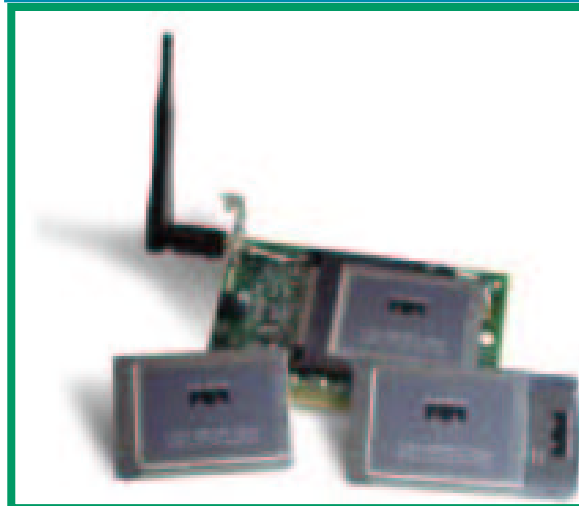
Antennas

Indoor & Outdoor

Omni & Directional

RF Technology

What's a Wireless LAN?

**Aironet Wireless LANs:
Ethernet Speed and Range**

Data Rates (vertical axis)

- 10 Mbps
- 4 Mbps
- 2 Mbps
- 1 Mbps
- 56 Kbps
- 19.6 Kbps
- 9.6 Kbps

Spread Spectrum Wireless LANs

Bluetooth

Metricom

Digital Cellular Broadband PCS

2-way paging

Satellite

Personal   Local   **Wide**

Coverage Area

License Free Bands

Short Wave Radio
AM Broadcast

FM Broadcast
Television

Audio

Cellular (840MHz)
NPCS (1.9GHz)

Infrared wireless LAN

Extremely Low	Very Low	Low	Medium	High	Very High	Ultra High	Super High	Infrared	Visible Light	Ultra-violet	X-Rays

902-928 MHz
26 MHz

Older Product

2.4 – 2.4835 GHz
83.5 MHz
IEEE 802.11B

5 GHz
IEEE 802.11A

WLAN Industry Standards

802.11g
2.4 GHz – OFDM
54Mbps

802.11a Standard
5 GHz – OFDM
54Mbps

802.11b Standard
2.4 GHz – DSSS
11Mbps

802.11 Standard
2.4Ghz 2Mb DSSS
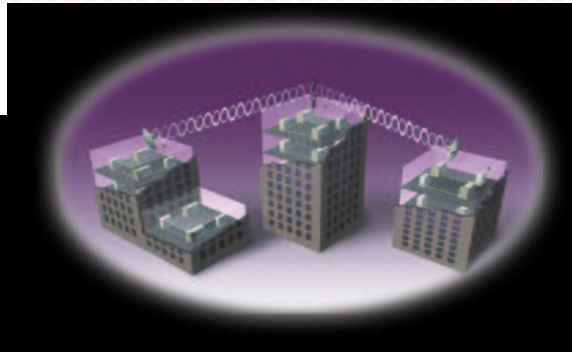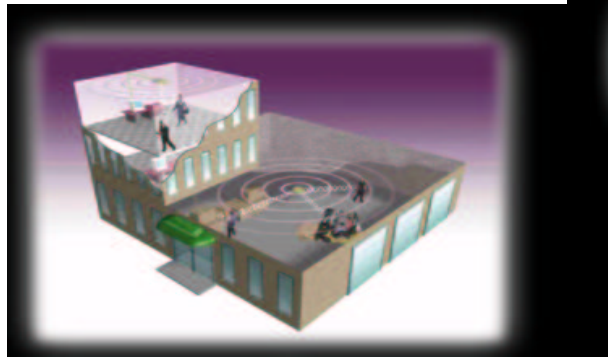
Proprietary-
900MHz/2.4GHz

IEEE 802.11
Ratified

IEEE 802.11a/b
Ratified

1997   1999   2000   2001   2002   2003

IEEE 802.11 Standard Activities

Cisco.com

- **802.11a** - 5GHz- ratified in 1999

- **802.11b** - 11 Mbps, 2.4 GHz, ratified in 1999

- **802.11d** - World Mode and additional regulatory domains – ratified in 2001

- **802.11e** - Quality of Service

- **802.11f** - Inter-Access Point Protocol (IAPP)

- **802.11g** - Higher Data rate (>20 Mbps) 2.4GHz

- **802.11h** - Dynamic Frequency Selection and Transmit Power Control mechanisms

- **802.11i** - Authentication and security

802.11b Overview

Channels
1 2 3 4 5 6 7 8 9 10 11 12 13 14

2.402 GHz ← 22MHZ → 2.483 GHz
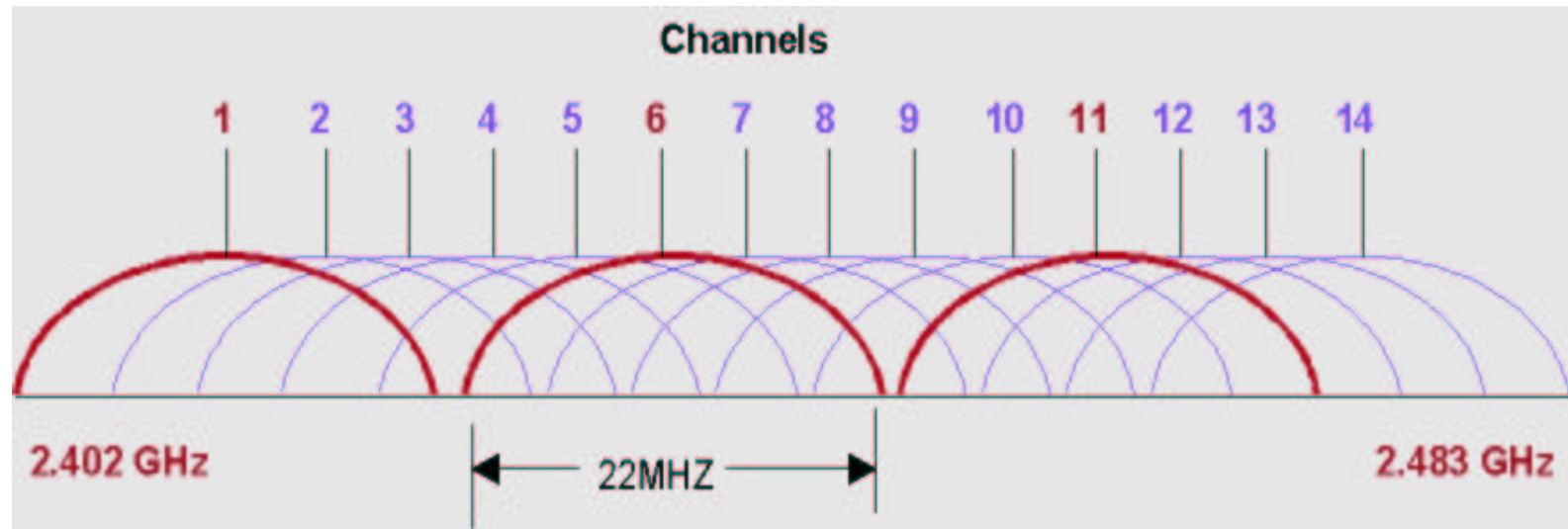
(14) 22 MHz wide channels (11 under FCC/ISTC)

3 non-overlapping channels (1, 6,11)

11 Mbps data rate

3 access points or bridges can be co-located in the same location for a total of 33 Mbps aggregate throughput

802.11b

- **Ratified as Standard in Sept, 1999.**

- **11 Mbps, 2.4 GHz, Direct Sequence**

- **11 US channels**

- **13 ETSI channels**

- **14 Japan channels**

- **Power levels: 36 dBm EIRP-FCC**
  20 dBm EIRP-ETSI

- **Virtually approved for world wide use**

802.11a

- **Ratified as Standard in Sept, 1999**

- **Provides similar technology to HiperLAN2**

- **Data rates to 54 Mbps defined**

- **Provides 8 indoor WLAN channels**

- **Regulations differ extensively across countries**

Understanding the 5GHz Spectrum

| 5GHz UNII Band | 5.15 | 5.25 | 5.35 | 5.470 | 5.725 | 5.825 |

US (FCC) 12 Channels
(*can use up to 6dBi gain antenna)

| 4 Ch | 4 Ch | | 11 Ch | 4 Ch |

| UNII-1 40mW | UNII-2 200mW | | | UNII-3 1W |

Europe 19 Channels
(*assumes no antenna gain)

| 200mW | | 1W | |
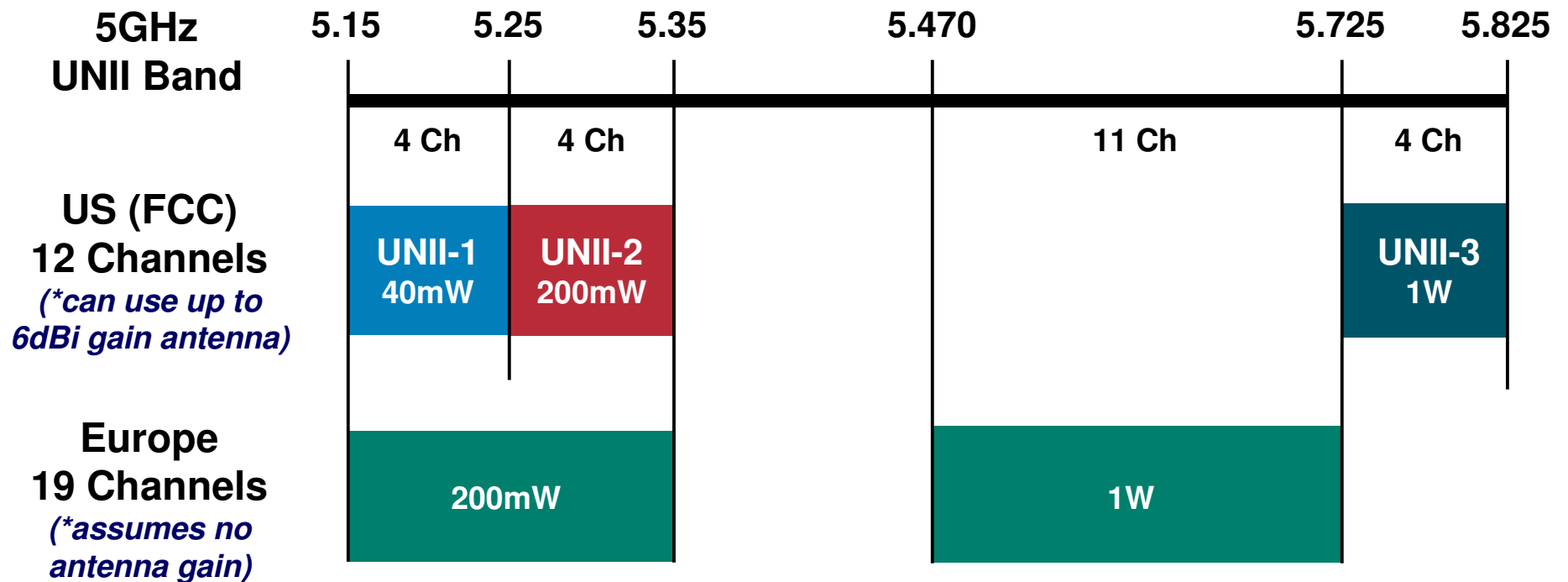
UNII-1: Indoor use, antenna must be fixed to the radio
UNII-2: Indoor/Outdoor use, fixed or remote antenna
UNII-3: Outdoor bridging only

---

*if you use a higher gain antenna, you must reduce the transmit power accordingly

UNII 1

- **Indoor use only**

- **4 channels**

- **Maximum FCC power limitation of 15 dBm and antenna gain maximum of 6 dBi**

- **Antenna must be permanently attached (No external antennas)**

UNII 2

- **Indoor/outdoor usage**

- **4 channels**

- **Maximum FCC power limitation of 23 dBm (200 mW) and 6 dBi antenna**

    Increased antenna gain by decreased TX power

- **External antennas permitted**

UNII 3

- **4 channels**

- **Outdoor usage**

- **Maximum power limits of 30 dBm (1 watt) and 6 dBi antenna.**

    Increased antenna gain by decreased TX power

- **Band for longer range 5 GHz Bridges**

Characteristics of 802.11a

- **Orthogonal Frequency Division Multiplexing (OFDM)**

    Data rates supported: 54, 48, 36, 24, 12, and 6 Mbps

    Can "downshift" to lower data rates for longer range

- **Compliant with FCC and Japanese regulations**

    Initial offering will not be available in EMEA and portions of Asia/Pacific

- **5 GHz band has more channels than 2.4 GHz band**

    UNII-1 + UNII-2 = 8 non-overlapping channels

    (vs. 3 channels for 2.4GHz) for greater scalability

- **5 GHz UNII-1 & UNII-2 bands are not wide-open ISM bands**

802.11d

Extensions to Operate in Additional Regulatory Domains

- **Ratified in June, 2001**

- **Defines frequency and power limitation for different regulatory domains**

- **'World Mode'**

  APs set to appropriate Regulatory domain

  Clients, upon association to AP, inherit the power and frequency requirements of regulatory domain

  Permits roaming across different regulatory domains with the same client.

802.11e
MAC Enhancements for Quality of Service

- **Draft 2.0 out for letter Ballot**

- **Provides quality-of-service (QoS) features**

    to support the existing 802.11b and 802.11a

- **QoS and multimedia support are critical to wireless**

- **Required for Networks with voice, video and audio**

- **Desired by most Broadband service providers**

802.11f

Recommended Practice for Inter Access Point Protocol

- ## Still in draft mode

- ## Inter Access Point Protocol (IAPP)

- ## Multivendor Infrastructure

  Improved Roaming

  Support for 802.11 authentication and privacy, including preauthentication

  Operation in a reasonably secure fashion

  Remote configuration, including AP attributes

IEEE 802.11g
Standard for Higher Rate (20+ Mbps) Extensions in the 2.4 GHz Band

- **Working on Draft for Letter ballot passed the task group committee in Nov.**

- **Provides higher data rates @ 2.4 GHz**

- **Similar speeds as 802.11a**

- **Backward compatible with 11 Mbps (802.11b**

- **Same modulation as 802.11a—OFDM**

- **Estimated to complete specification in Jan 2003**

802.11g

20–50 MB   **11 MB**

802.11g   **802.11b**
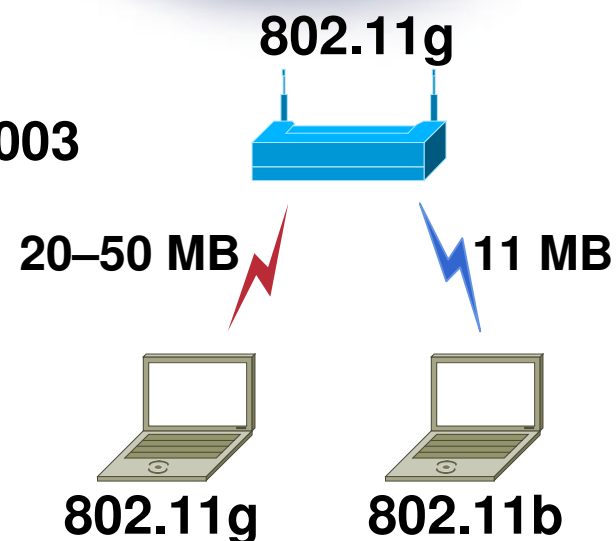
802.11h-
Spectrum Managed 802.11a

- ## Still in Draft mode

- ## Dynamic Frequency Selection (DFS)

  Enables transmitter to move to another channel when is encounters other RF on its channel

- ## Transmit Power Control (TPC)

  Provides minimum required transmitter power for EACH user

  Provides minimal interference to any other users or system

- ## ETSI Requirement for 5 GHz

IEEE 802.11i Security

- **Passed 1st letter ballot (Draft currently at version 1.6)**

  Fixes to WEP (Software)

  New AES proposals (Requires Hardware Changes)

  All MIC/IV Hash/IV Sequencing/Rapid Rekey to informative text: passed

  Replace WEP2 with TKIP : passed

  TKIP (Temporal Key Integrity Protocol)

  Text/hash function/MIC etc is Work in Progress.

802.1x
Port based network access control

- **Falls under 802.1 NOT 802.11**

- **This is a NETWORK standard, not a wireless standard**

- **Is PART of the 802.11i draft**

- **Provides Network Authentication, NOT encryption**

- **Incorporated as part of LEAP**

802.11a and 802.11b Comparison

802.11a

- **Maximum wireless LAN performance: 54Mbps**
- **Eight channels, but works only in U.S. and Japan**
- **5 GHz band has less interference than 2.4 GHz (at least initially)**

802.11b

- **Ethernet-like data rate of 11Mbps**
- **Three channels, but works worldwide**
- **Compatibility with installed base of 802.11b networks**
- **Wide selection of client devices**
- **Lower cost products**
- **Lower power products (important for handhelds)**
- **Compatible with 802.11g**

802.11a vs. 802.11b Range

- **Range of 5GHz is much less— about 30%**

- **Overall investment of infrastructure is much higher (more APs)**

2.4GHz Range

2.4GHz

5GHz

50'

150'

802.11a vs. 802.11b Range

- **Range of 5GHz is much less— about 30%**

- **Overall investment of infrastructure is much higher (more APs)**

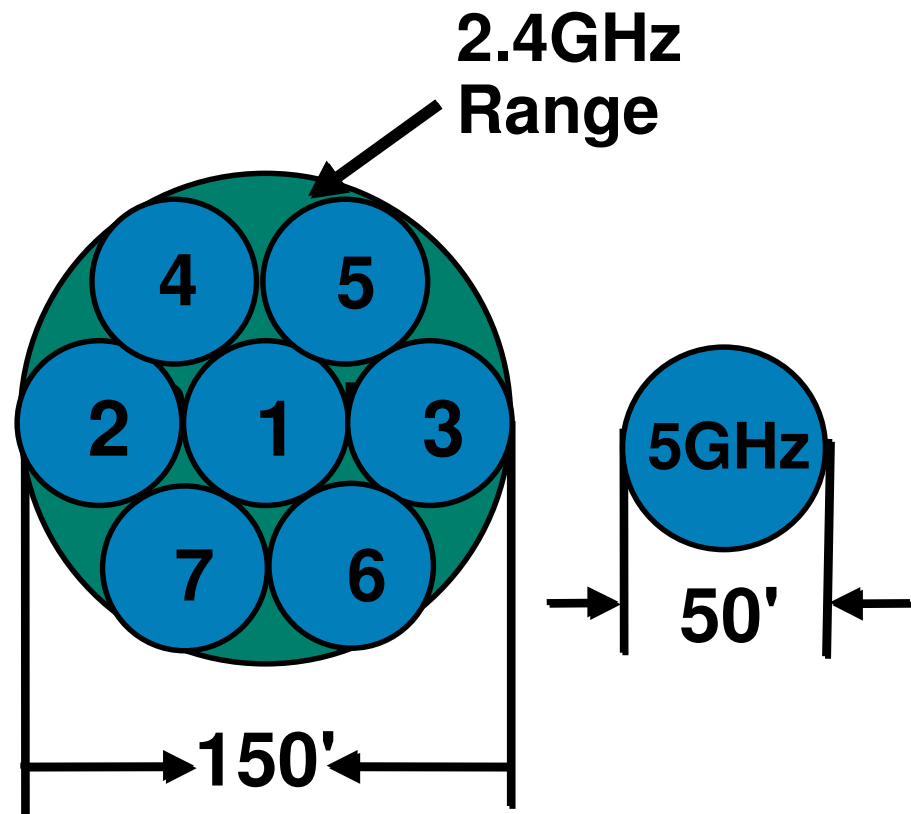**2.4GHz Range**

5GHz

150'   **50'**
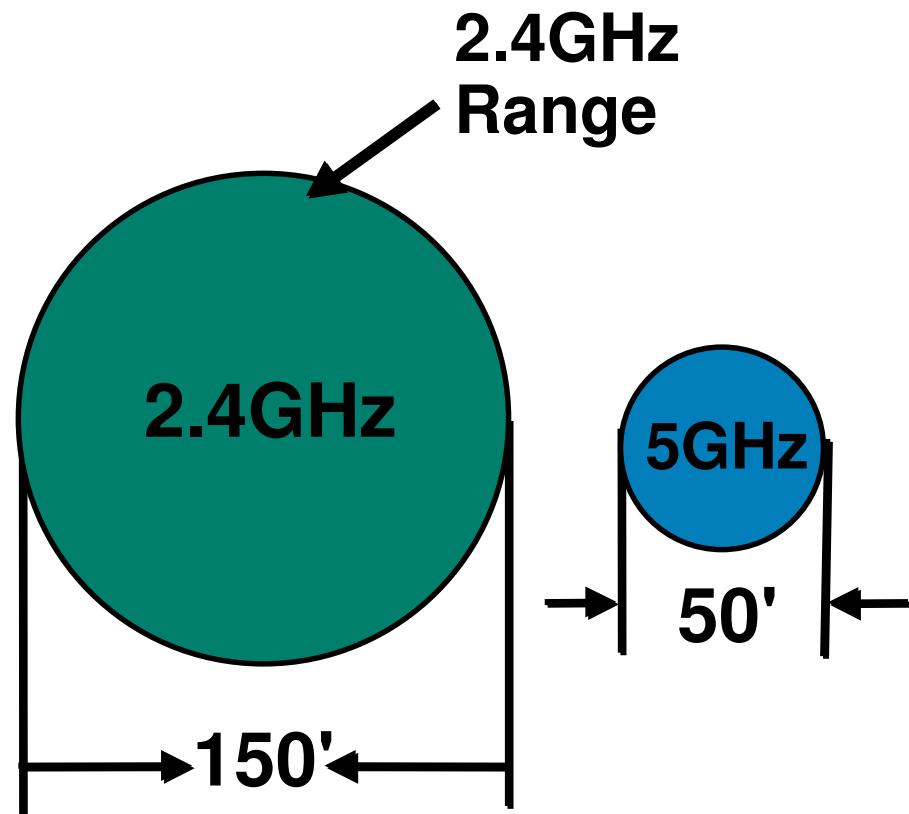
Analysis: 802.11a vs. 802.11b

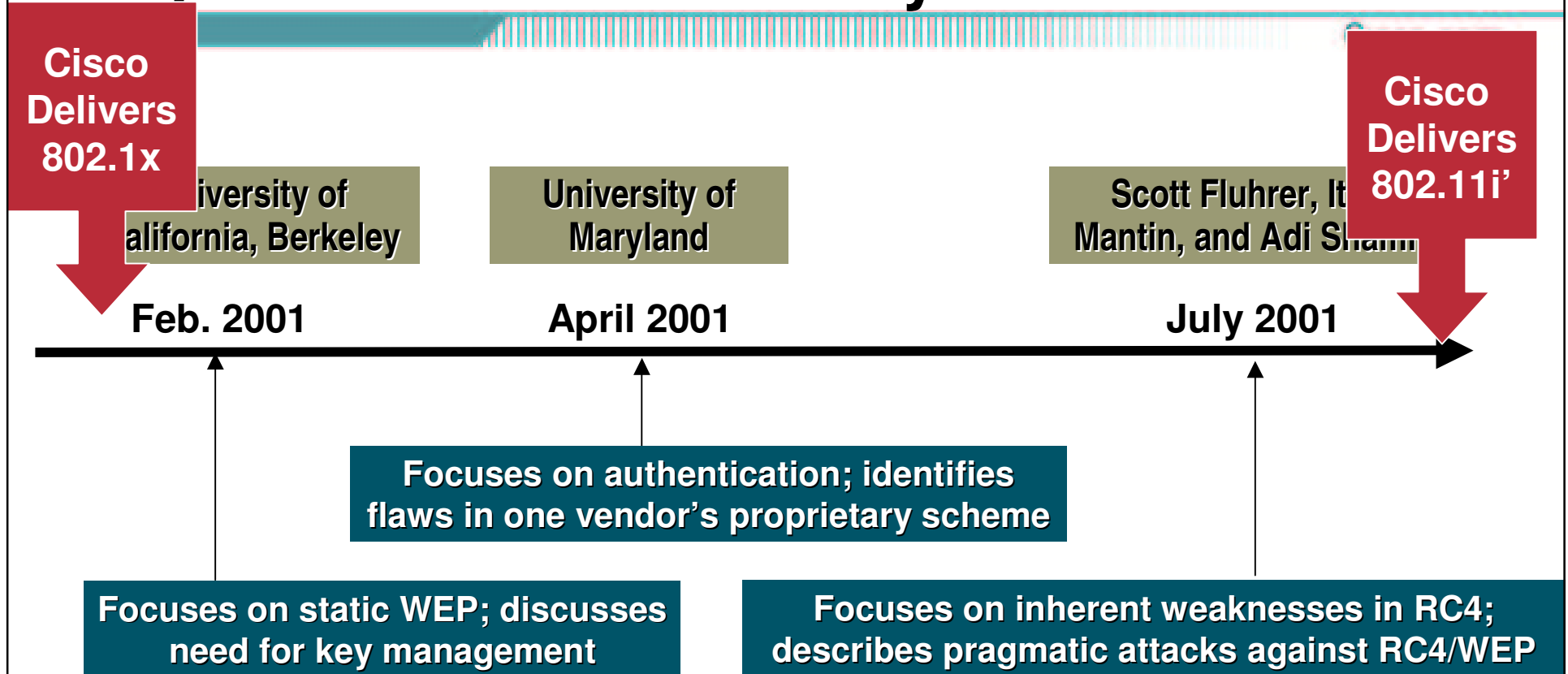- **802.11a is a complement, not a successor to 802.11b**

    Depending on the application, some customers will choose 802.11b, some will choose 802.11a, but many customers will deploy both for ultimate compatibility, flexibility, and performance

- **Organizations likely to support multiple standards for different client device types and performance needs**

    802.11b is optimal for PDAs and phones and will be the standard wireless LAN technology for embedded devices in the near term

    802.11a provides maximum data rate for performance and channels for scalability

- **Today's investment in 802.11b gear will be viable for many years**

- **Cisco is committed to driving the market for both 2.4GHz and 5GHz solutions and has invested accordingly**

Cisco.com

WLAN Security Options

Papers on WLAN Security ...

Cisco Delivers 802.1x

Cisco Delivers 802.11i'

University of California, Berkeley

University of Maryland

Scott Fluhrer, Itsik Mantin, and Adi Shamir

Feb. 2001

April 2001

July 2001

Focuses on authentication; identifies flaws in one vendor's proprietary scheme

Focuses on static WEP; discusses need for key management

Focuses on inherent weaknesses in RC4; describes pragmatic attacks against RC4/WEP

* "In practice, most installations use a single key that is shared between all mobile stations and access points. More sophisticated key management techniques can be used to help defend from the attacks we describe…"

– University of California, Berkeley report on WEP security, http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

Encryption

- **Encryption options**

    No encryption

    40-bit encryption

    128-bit encryption

    168-bit 3DES using VPN Client

- **Hardware-based encryption**

    3% performance hit (@128 bit)

- **Encryption choices (defined at access point)**

    No encryption

    Allow client to specify (optional)

    Forced (required)

802.1X over Wireless

- **802.1X is IEEE standard for port-based network access control**

- **Leverages existing standards**

    Extensible Authentication Protocol (EAP)

    RADIUS

- **802.1X for 802.11 overcomes limitations of 802.11 security**

    1 **Mutual authentication**

    2 **Dynamic, session-based encryption keys**

    3 **Centralized user administration**

    4 **Extensible authentication support**

client

EAP

1

2 *AP*

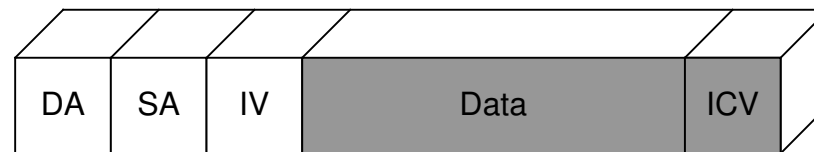**RADIUS**

RADIUS server

3 *user database*

4
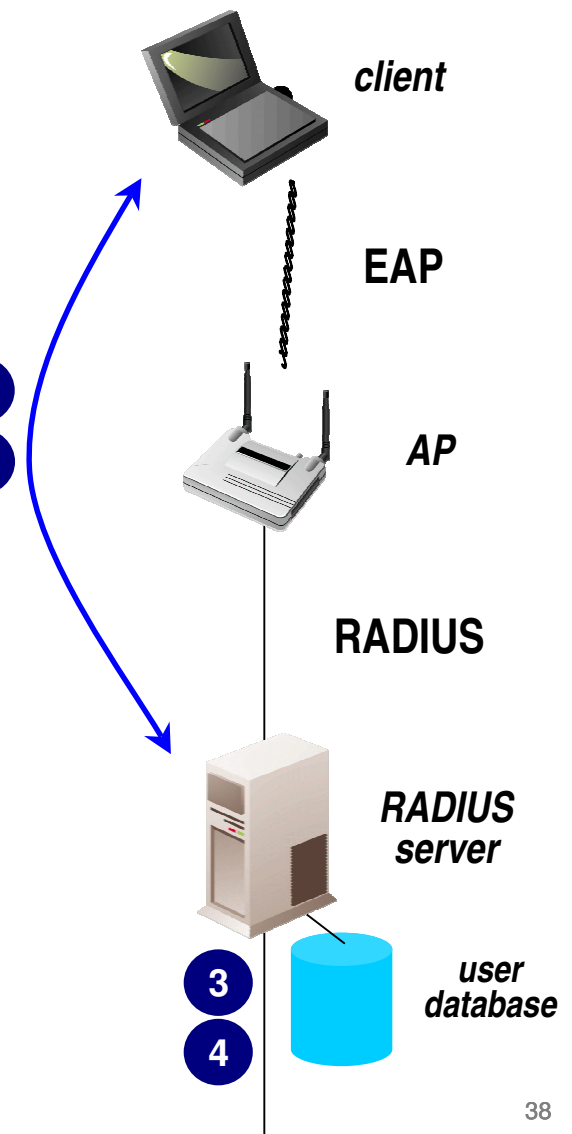
Cisco LEAP Overview

- **Provides centralized, scalable, user based authentication**

- **Algorithm requires mutual authentication**

    Network authenticates client, client authenticates network

- **Uses 802.1X for 802.11 authentication messaging**

    APs support WinXP's EAP-TLS also

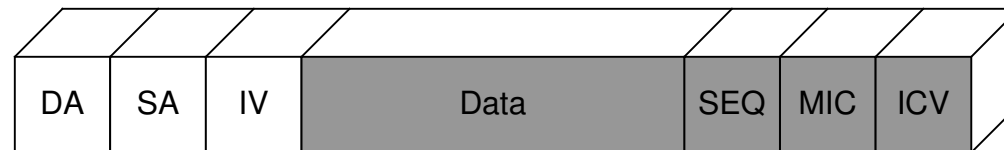- **Dynamic WEP key support with WEP key session timeouts**

Message Integrity Check

WEP Frame - No MIC

DA	SA	IV	Data	ICV

WEP Encrypted

WEP Frame - MIC

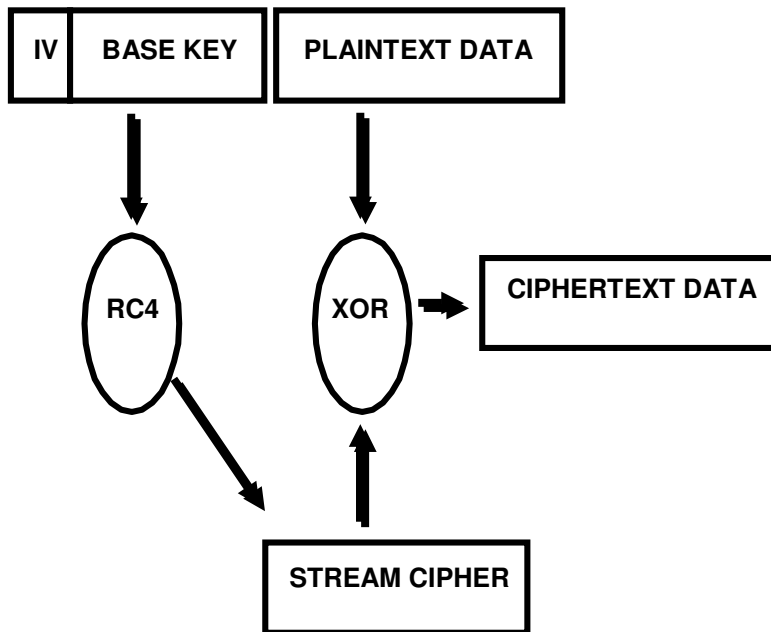| DA	SA	IV	Data	SEQ	MIC	ICV

WEP Encrypted

WEP Key Hashing

Standard

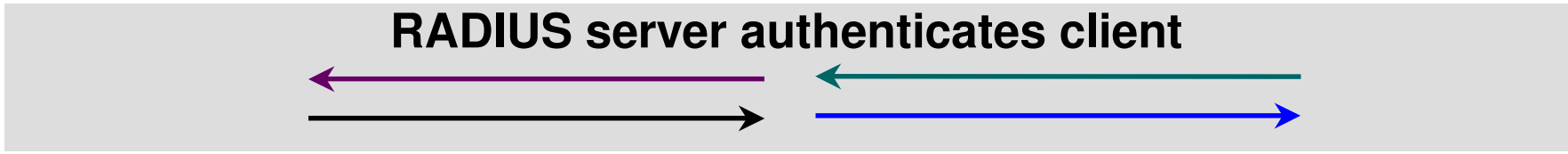**Cisco's Offering**

41
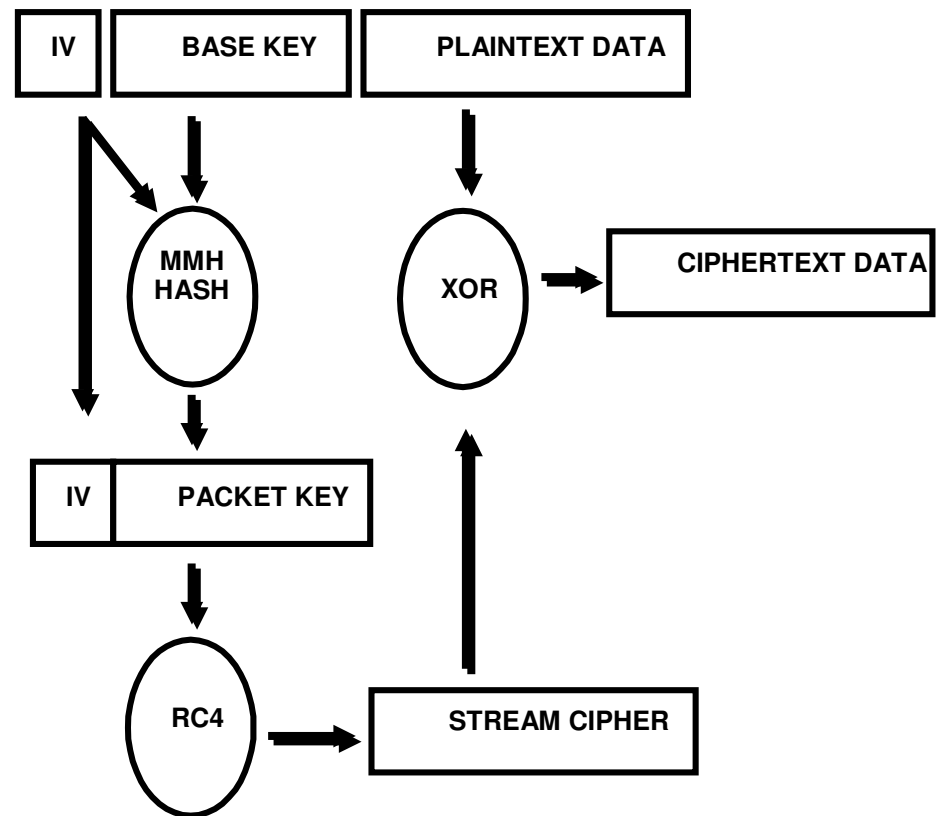
802.1X/LEAP Mutual Authentication

client

AP

RADIUS server

Start →

← Request identity

identity →

identity →

AP blocks all requests until authentication completes

RADIUS server authenticates client

←

→

←

→

Client authenticates RADIUS server

Derive key

→

←

Derive key

→

←

LEAP Authentication Process

Create
challenge

challenge

**password
from
database**

challenge

**one-way
hash**

**LEAP
algorithm**

response A

**password
hash**

**Using password from database,
generate response to own challenge**

LEAP Authentication Process

challenge

user-supplied password

response B

response A

one-way hash

challenge

password hash → **LEAP algorithm** → **response B**

Using user-supplied password, generate response to challenge

If response A = response B, then authenticate user

Why?

LEAP Authentication Process

user-supplied password

one-way hash

challenge

password hash → **LEAP algorithm** → *response B*

password from database

one-way hash

challenge

response A ← **LEAP algorithm** ← **password hash**

If response A = response B, then user-supplied password = password from database

The End User's Experience is the Same: Single Sign-On

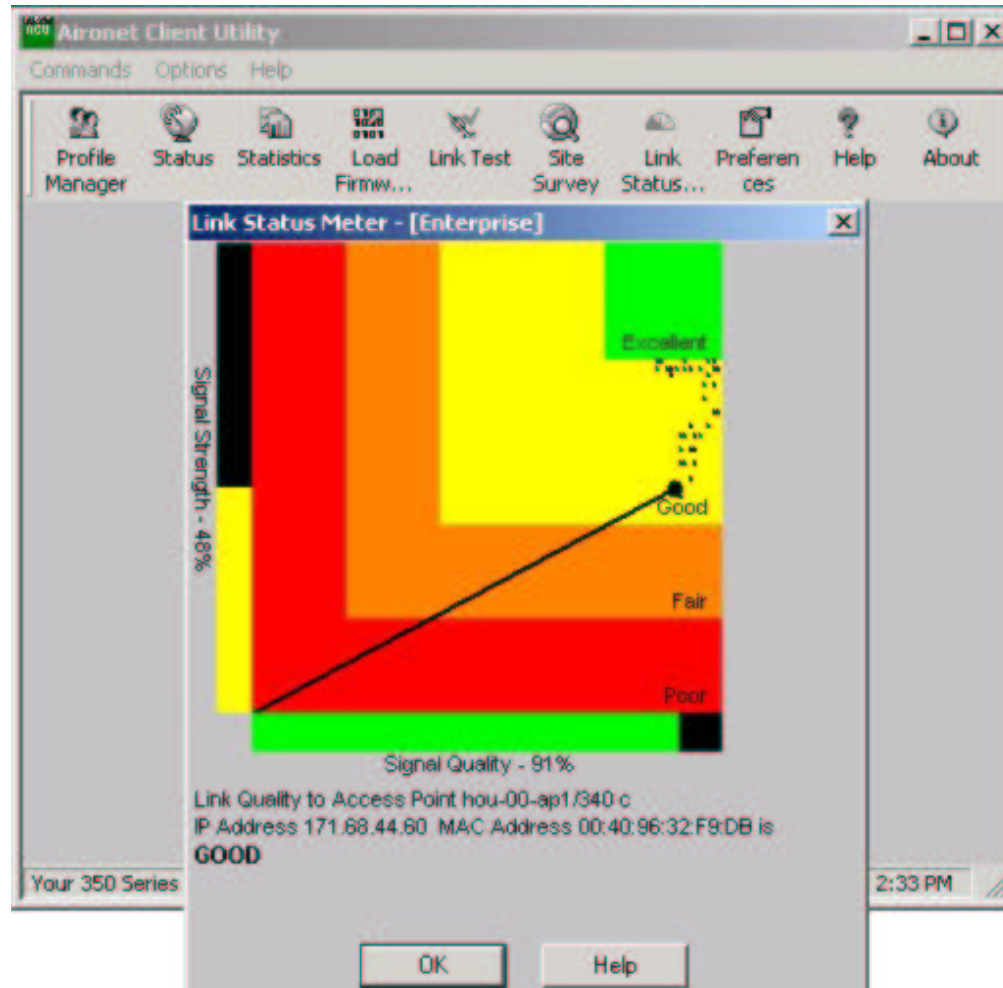Cisco.com

Designing Wireless LAN

Designing Wireless LAN

- **Key issues for designing wireless systems:**

    Required bandwidth per user

    Connectivity

    Security

    Redundancy

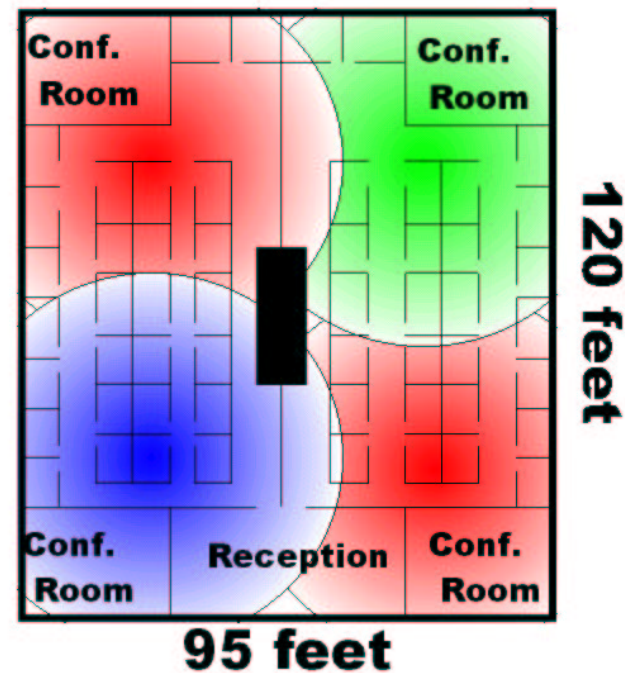   **Specific physical installation requirements**

Site Surveys recommended

Standard Office Application

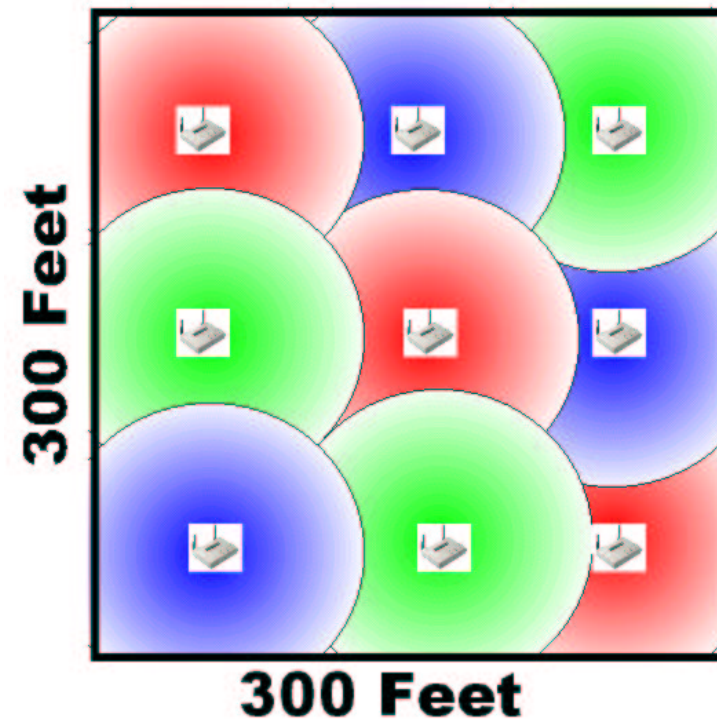- **Use three non-overlapping channels**

- **Rotate channels to fill in**

54 Cubes- 4 conference rooms

Conf. Room | Conf. Room | Conf. Room | Conf. Room | Reception

120 feet

95 feet

Dense Populations

- **Reduce cell size**

- **Reduce antenna gain or transmitter power to create smaller cell size**

- **Enable load balancing**

300 Feet

300 Feet

# WLAN Building Block for High Aggregation

3524-PWR

- **Up to 33 Mbps aggregate peak data rate**

- **Load balancing and redundancy**

- **Algorithm based on number of users, bit error rate, or signal strength**

- **Web-based management**

- **Very high aggregation with sectored antennas**

Catalyst 3524
Series XL

Inline Power

Channel 1   **Channel 11**   **Channel 6**
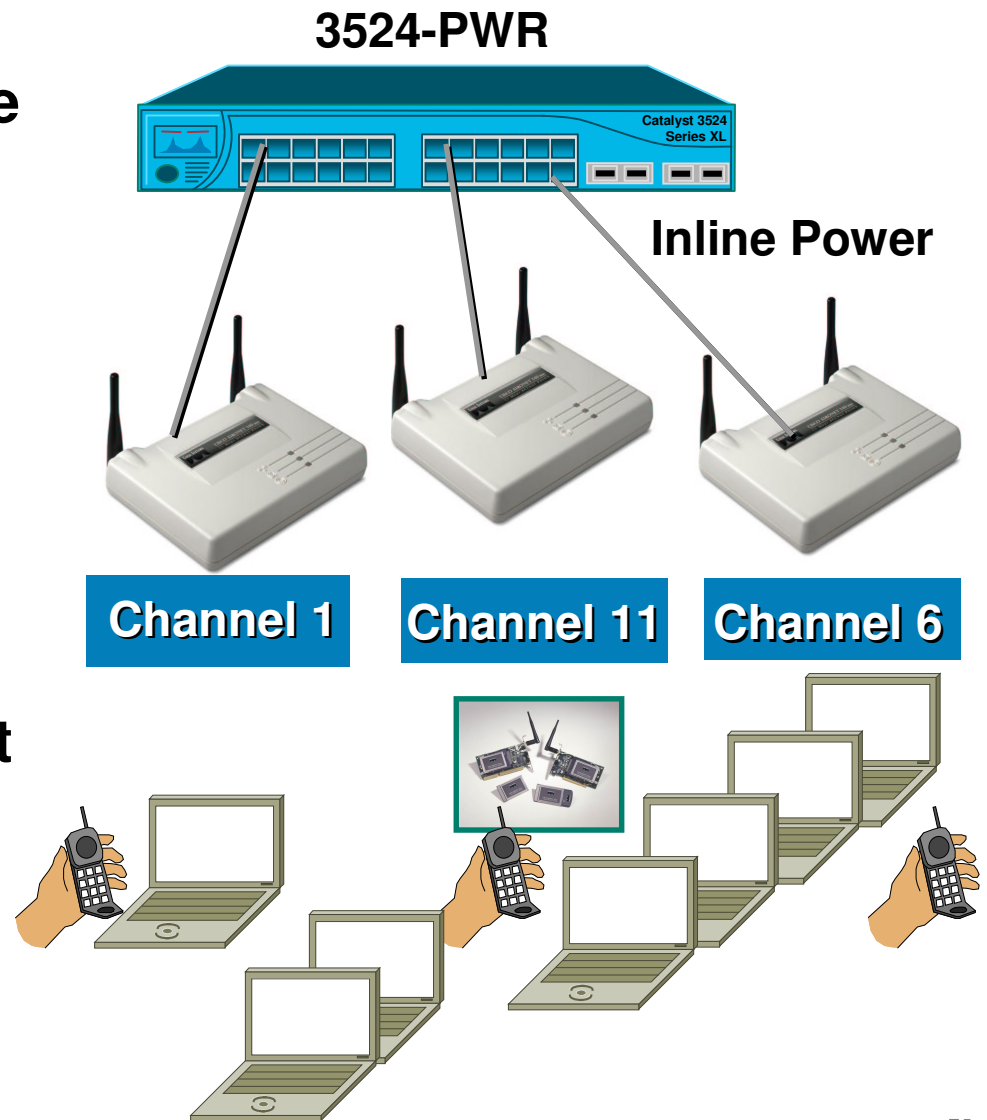
Mission Critical Application

- **Redundancy requirements**

- **Healthcare**

    ICU/ER

- **Production flow**

    Automotive—JIT

Standby

Active
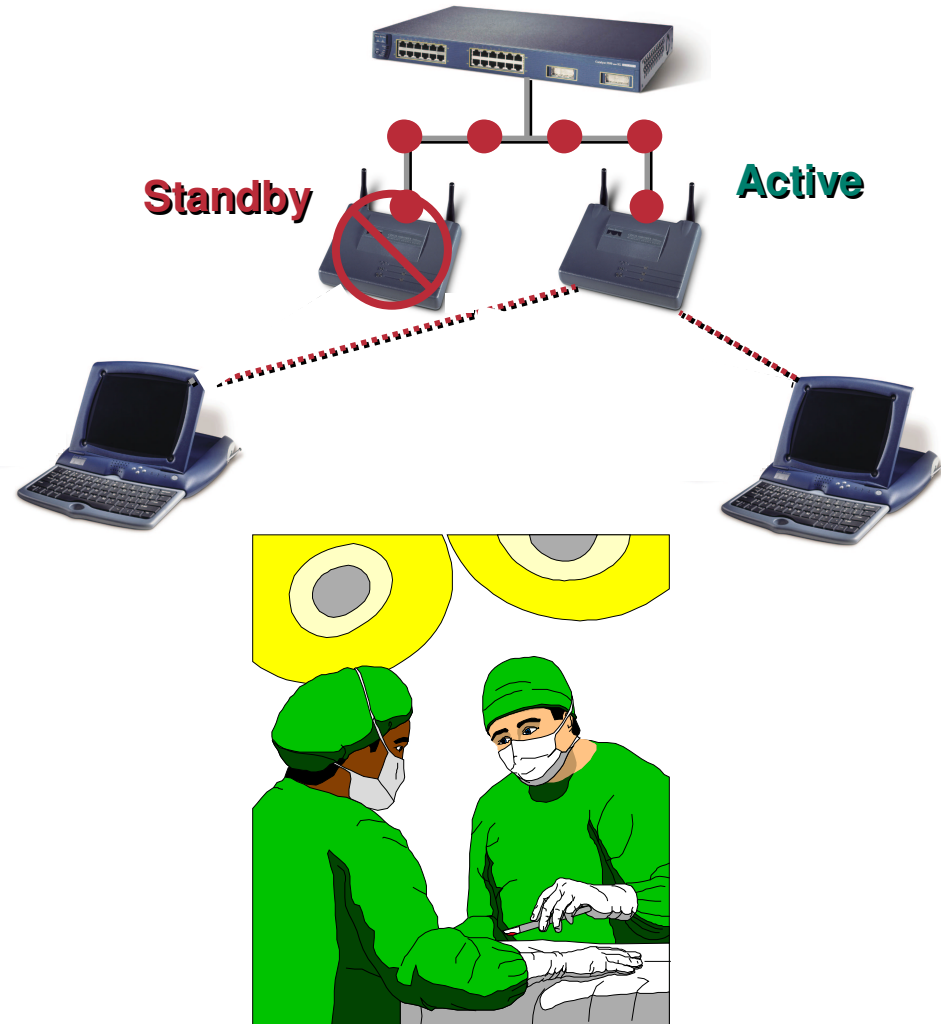
High Availability WLAN Building Block

- **1 hot standby AP per channel**

- **Tolerant to any single AP or link or switch failure**

- **Web-based management**

3524-PWR

Catalyst 3524 Series XL

Catalyst 3524 Series XL

Channel 6

Channel 11
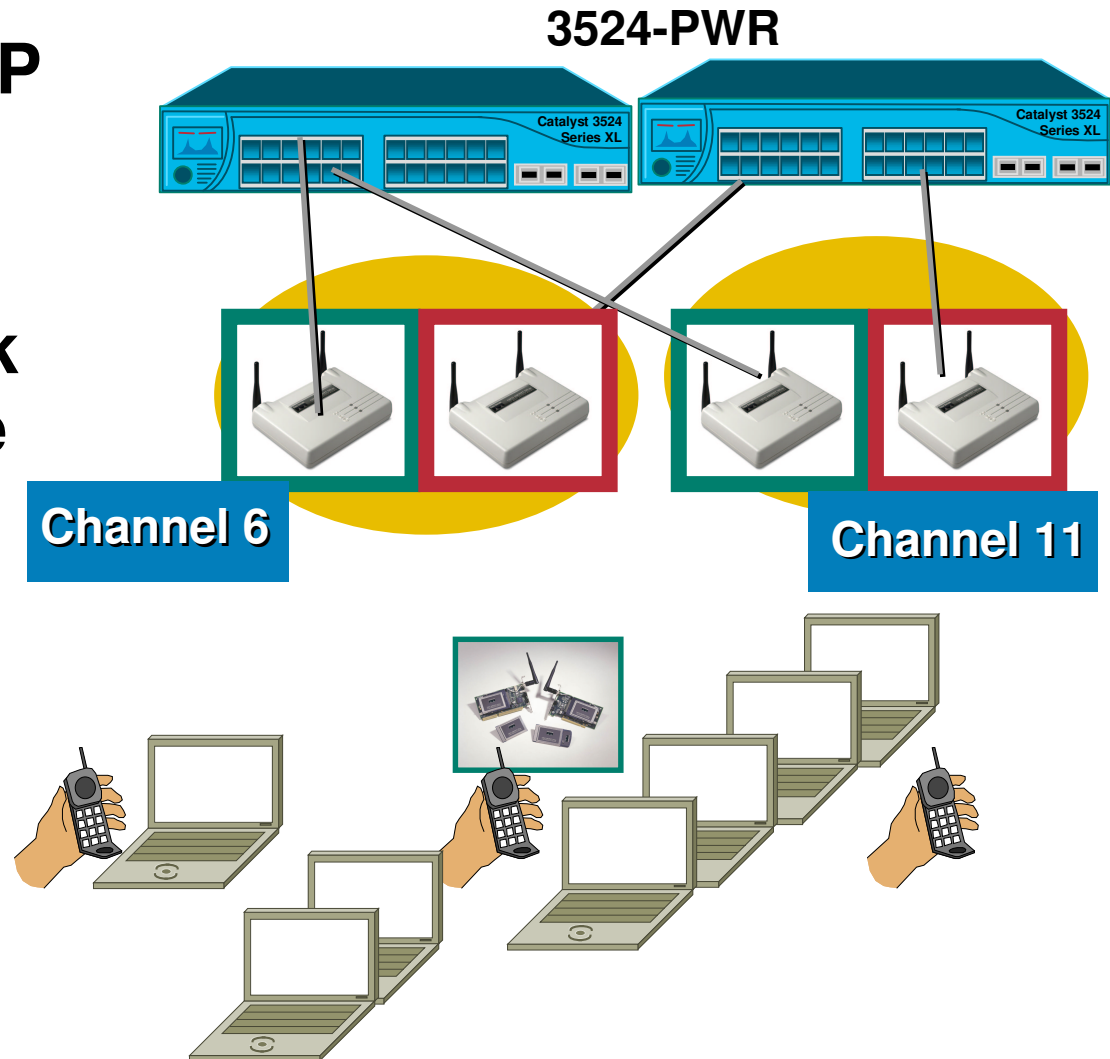
Unit in Standby

AC Power Requirements

- **Cost of AC cabling is astronomical**

- **As much as $30K for a 4-story Cisco building like building #19 in San Jose**

- **Inline power will reduce this cost**

Specific Suggestions

- **Cisco AP w/Cisco Client**

    WEP, MIC, Per Packet Hash, LEAP

- **Cisco AP w/Non Cisco Client**

    Mac Authentication, WEP, Access-list

Cisco.com

Wireless Bridging

Why Wireless Bridging?

Connect Separate LANs at High Speed

- Wired Infrastructure not available

  - Too expensive

  - No right of way

- Use as redundant or backup link

- Not Tariffed, No Recurring Fee

- Service Provisioning over a Metro Area

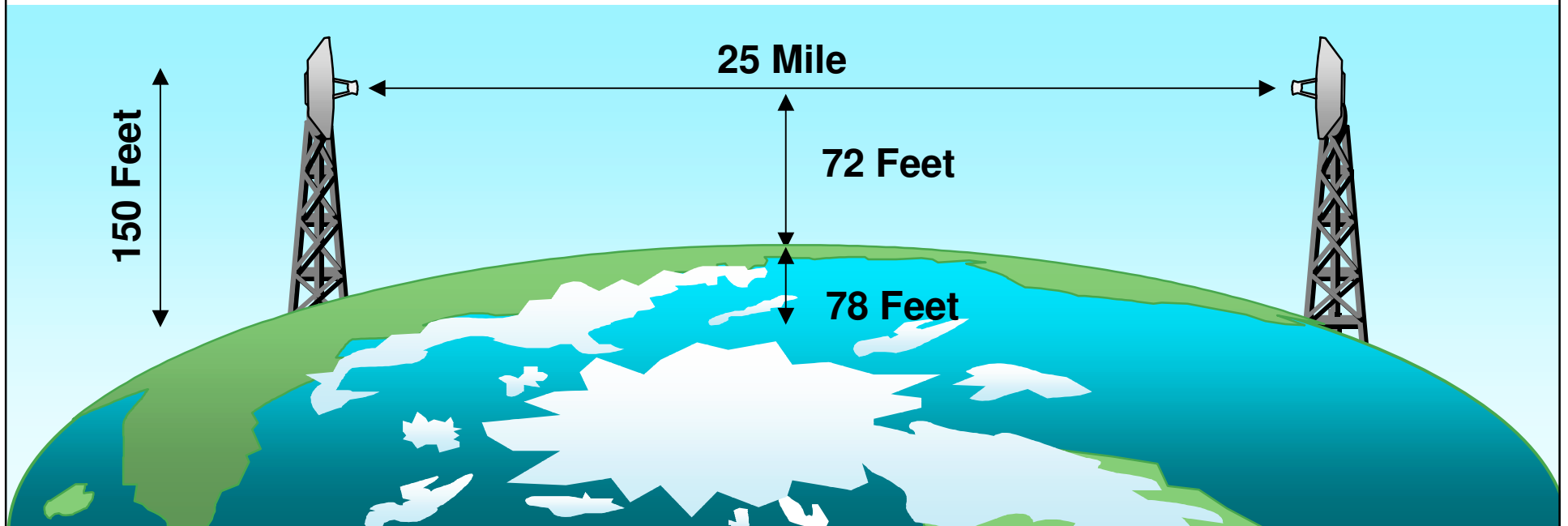- Rapid deployment of temporary work areas

- Mobility

Example
Antenna Height—25 Mile

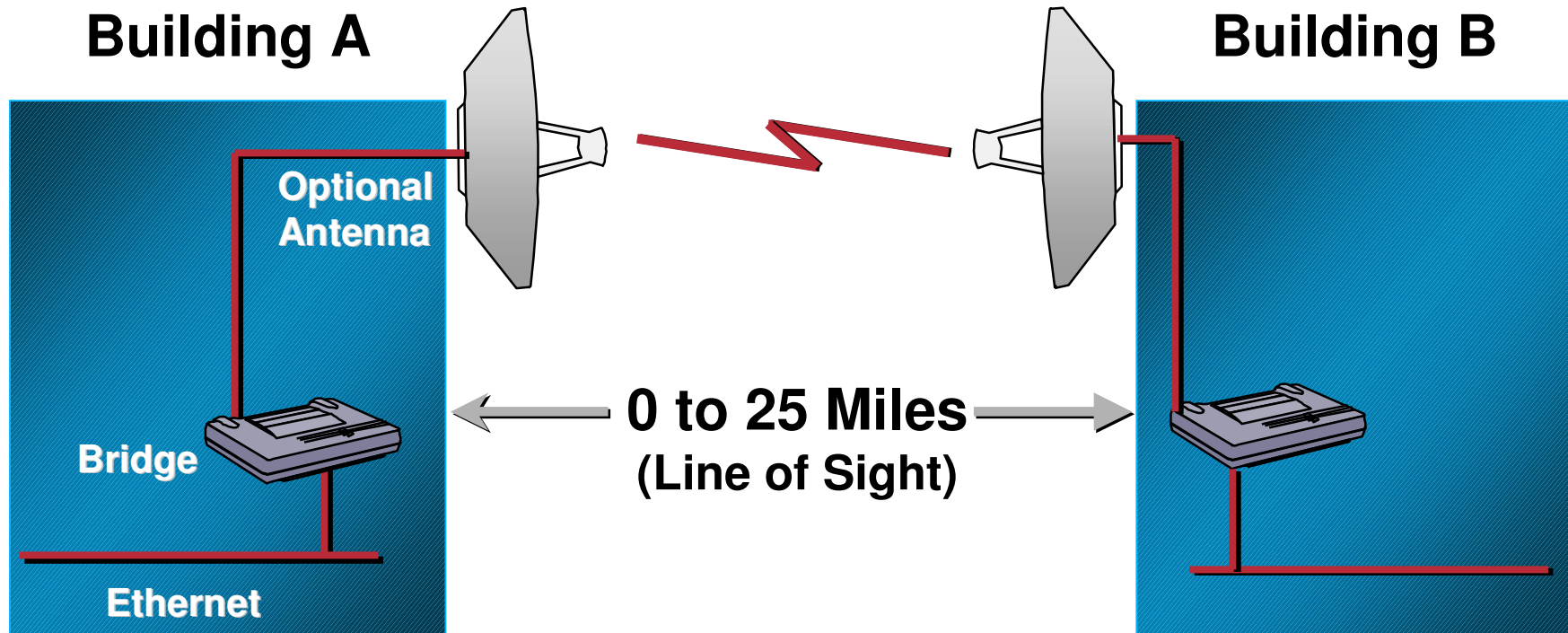- ## Antenna height

Total distance	25 Mile
Fresnel zone	72 Feet
Earth curvature	78 Feet
Required antenna height	150 Feet

Point-to-Point Configuration

10dB Rain Fade Margin is factored in!

Building A

Building B

Optional Antenna

Bridge

0 to 25 Miles
(Line of Sight)

Ethernet

Point-to-Multipoint Configuration

Ethernet

Building A

Bridge

- **Management capabilities:**

  SNMP, Telnet, FTP, HTML

  802.1d Spanning Tree

Omni-Directional Antenna

Building B

Bridge

Ethernet

Building C

Bridge

Ethernet
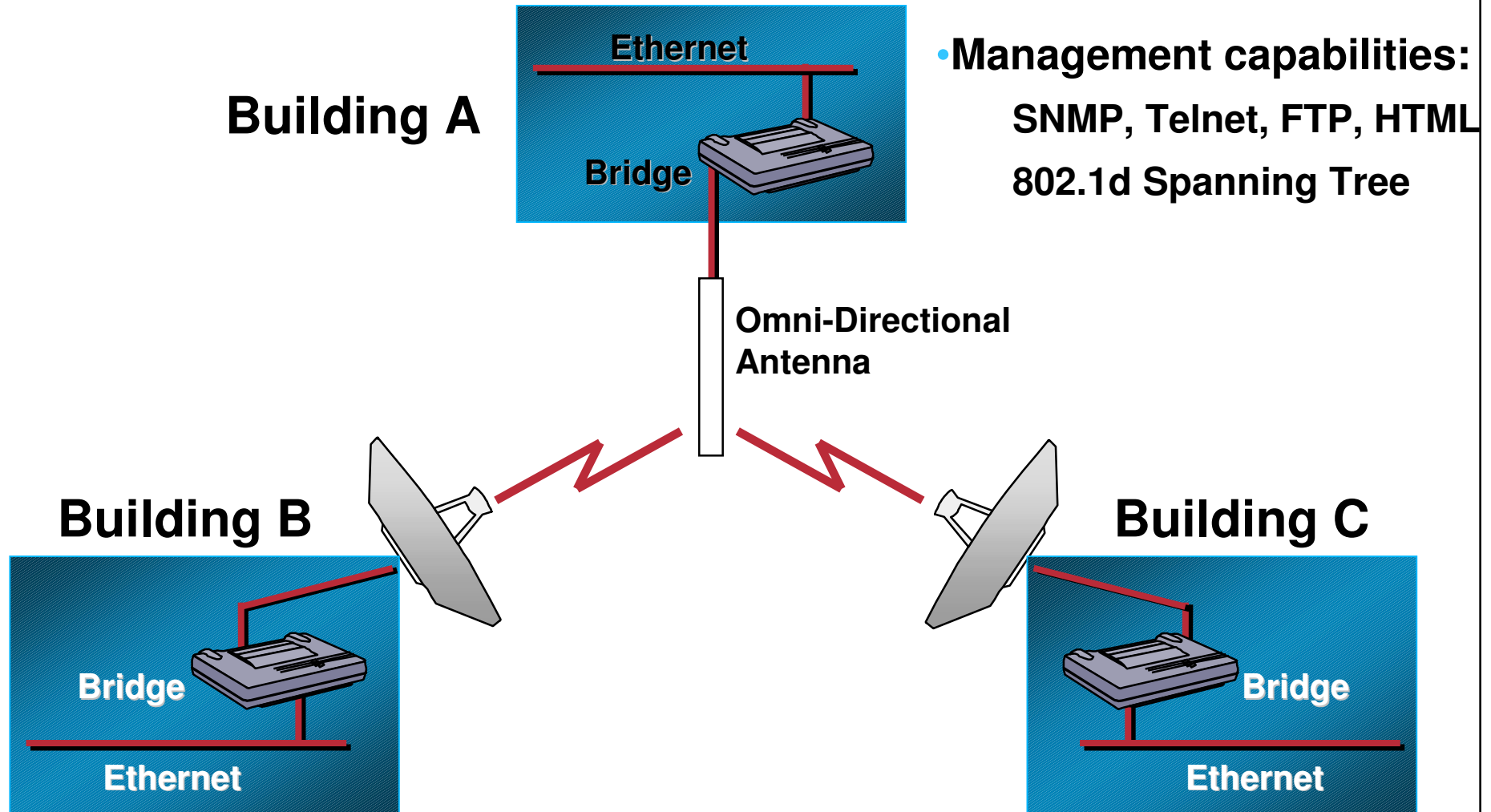
What's Next?

What's next for Cisco

QoS – Wireless is shared

Vlans – separate users

Layer 3 Roaming

Continued security enhancements

Modular hardware platform

CW2000 Bundle [WLSE]

Summary of Key Points

- **WLAN is a complement to a wired infrastructure**

- **Not all WLAN is created equal**

  - **Throughput, Range, Security, TCO**

- **Cisco's Security solution is class leading**

- **Cisco will continue to innovate then standardize WLAN technologies**

Please Complete Your Evaluation Form:

WLAN Technical Overview & Update

Make your plans to attend Cisco Networkers 2002!

- **San Diego, CA - June 24-28**

- **Orlando, FL - July 8-12**

CISCO SYSTEMS

EMPOWERING THE
INTERNET GENERATION℠