Wireless LANs
June – September 2009

IEEE 802.11 Overview

รศ. ดร. อนันต์ ผลเพิ่ม

Assoc. Prof. Anan Phonphoem, Ph.D.

anan.p@ku.ac.th

Intelligent Wireless Network Group (IWING Lab)

http://iwing.cpe.ku.ac.th

Computer Engineering Department

Kasetsart University, Bangkok, Thailand

Outline

- IEEE 802 Standards
- IEEE 802.11 Overview
- IEEE 802.11 Services
- History and present of IEEE 802.11

Why Wireless LAN not so popular in last ten years?

- Low data rate
- High price
- Lack of standard
  - Proprietary products

Types of Standards

- Official Standard
  - Controlled by an official standard organization
  - E.g. IEEE
- Public Standard
  - Controlled by a private organization
  - E.g. Wireless LAN Interoperability Forum
  - Called “De Facto Standard”

Why Std. is so important?

- Interoperability
  - Multiple-vendor products
- Fast product development
  - Well-tested blueprint
- Stable for migration
  - IEEE 802.3 → 10 → 100/1000 Mbps
  - IEEE 802.11b → 802.11g
- Price Reduction
  - Low research & development budget
  - Increase price competition
- Easy to manage

IEEE

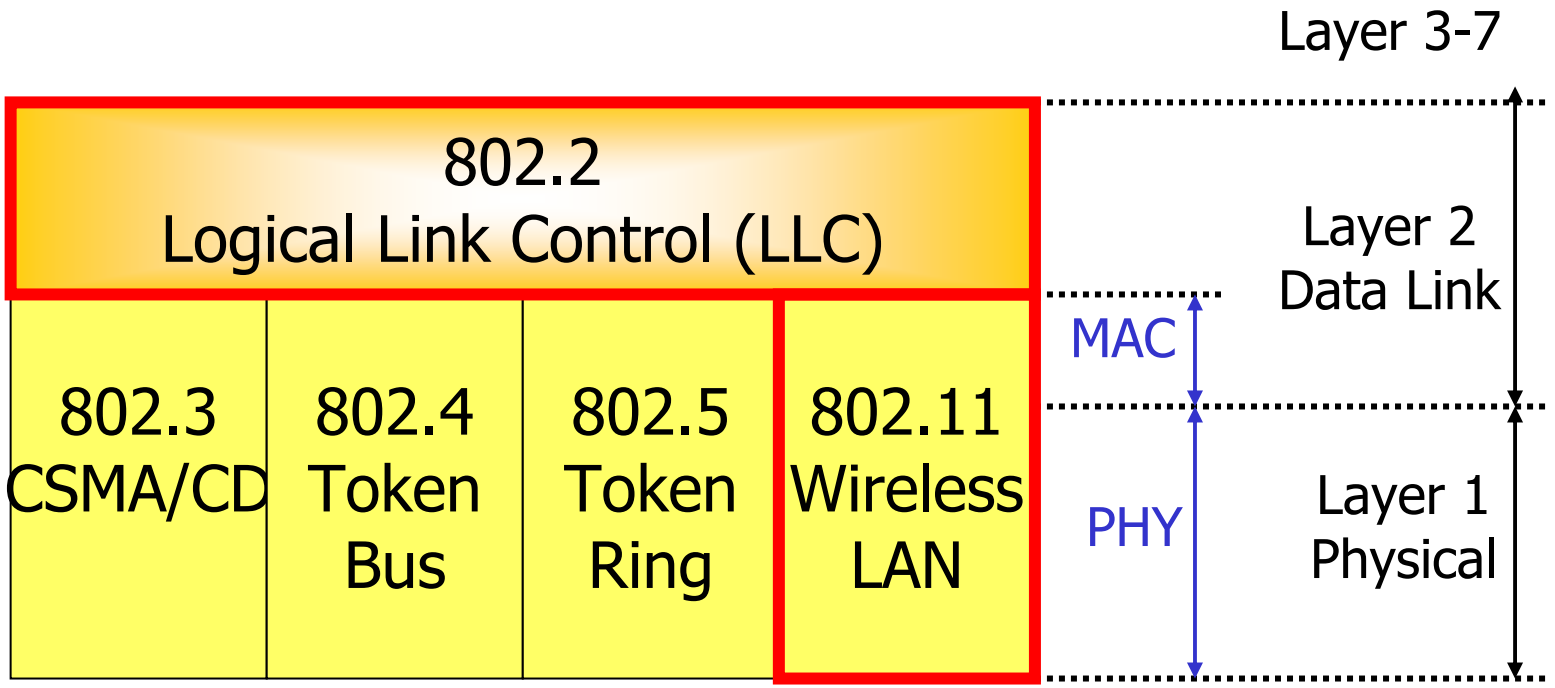
- **I**nstitute for **E**lectrical and **E**lectronic **E**ngineers
- Nonprofit organization
- Publication, conferences, accreditation, standard developments
- Based in the US. → 150 countries

IEEE 802 LAN Std. Family

802	Overview and Architecture
802.1	Network Management
802.2	Logical Link Control (LLC)
802.3	CSMA/CD - Ethernet
1802.3	Conformance Test Methodology for IEEE 802.3
802.4	Token Passing Bus
802.5	Token Ring
802.6	Metropolitan Area Network (MAN) : DQDB

802.7	Broadband LAN
802.8	Fiber Optic
802.9	Isochonous LAN
802.10	Integrated Service Security
802.11	Wireless LAN
802.12	Demand Priority
802.15	Wireless PAN
802.16	Broadband Wireless Access (Wireless MAN)
802.17	Resilient Packet Ring
802.18	Radio Regulatory

IEEE 802 LAN Std. Family



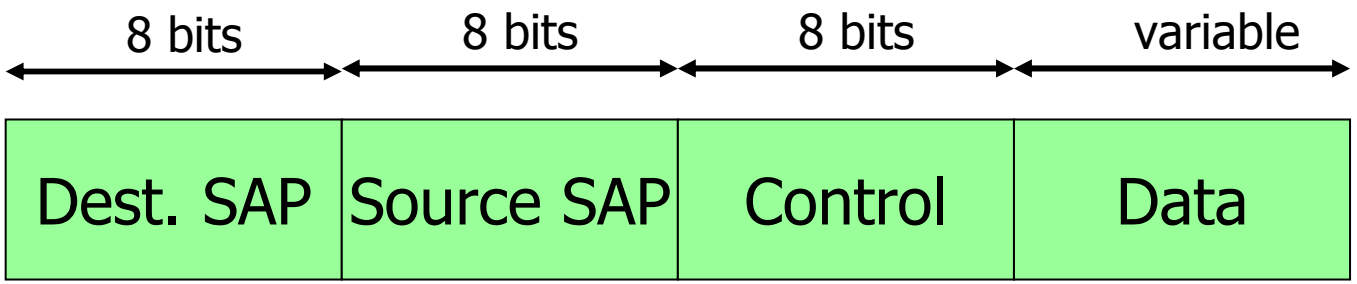
IEEE 802.11 → may be referred to as "**Wireless Ethernet**"

IEEE 802.2 LLC

- Data link control protocol
- Exchange data between end users across LAN using a 802-based MAC
- Independent
  - Network topology
  - Transmission medium
  - MAC

IEEE 802.2 LLC services

- Unacknowledged Connectionless
- Connection-oriented
- Acknowledged Connectionless



LLC Protocol Data Unit (PDU)

Outline

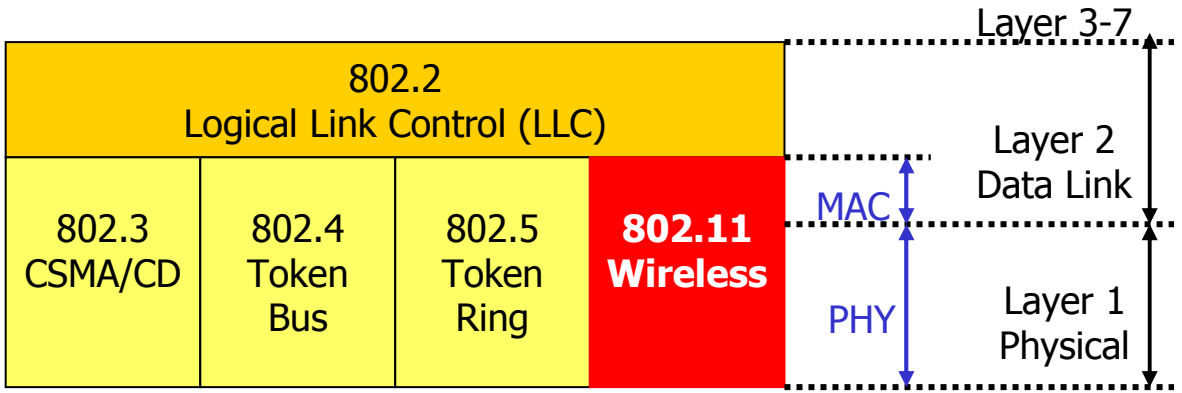
- IEEE 802 Standards
- IEEE 802.11 Overview
- IEEE 802.11 Services
- History and present of IEEE 802.11

IEEE 802.11 design concern

- Wireless / Wired LANs Differences
- Power management
  - Switch to low power mode (sleep)
- Bandwidth
  - Compress data, utilize of the available BW
- Security
  - Works with IEEE 802.10
- Addressing
  - Location / destination address → mobileIP

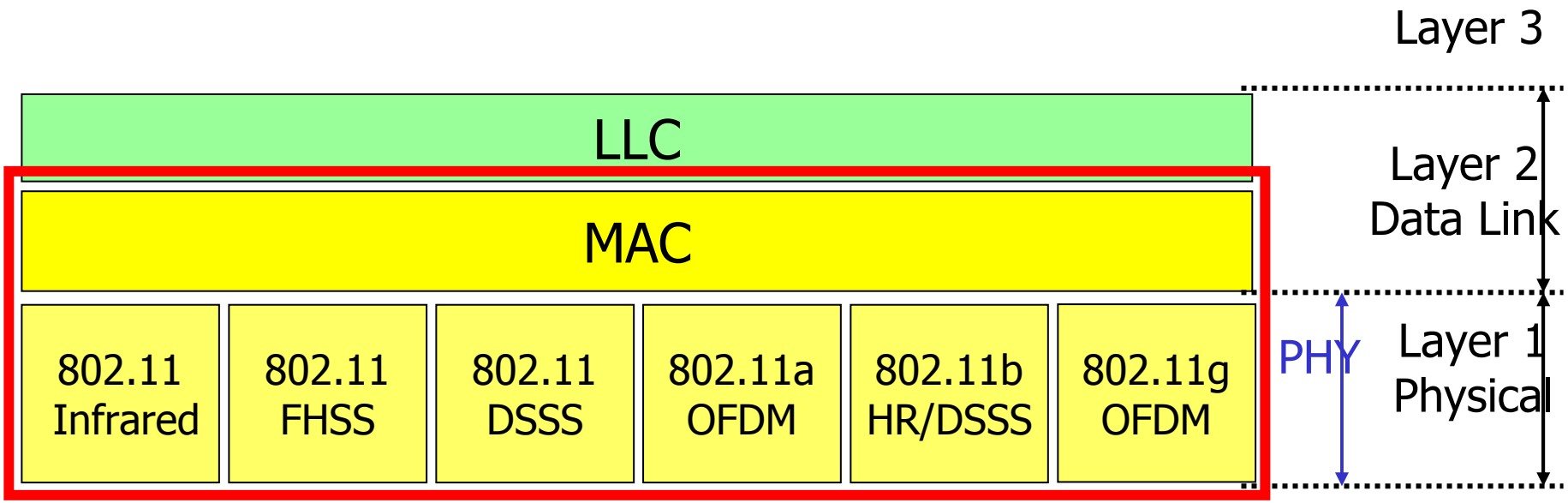
IEEE 802.11 Logical Architecture

- Deliver **M**AC **S**ervice **D**ata **U**nit (MSDU) between peer LLC
- Transparent to higher layer (LLC)
- Provide both MAC and PHY functionality
- Typically resides in NIC or Access Point



IEEE 802.11 Logical Architecture

- Define the network operation
  - Topology → necessary physical components



802.11 MAC Layer

- Provide access control functions
  - Addressing
  - Access coordination
  - Frame check generating / checking
  - LLC PDU delimiting
- CSMA/CA
  - Cannot Tx/Rx simultaneously

802.11 Physical Layers

Radio Frequency

- Frequency Hopping Spread Spectrum (FHSS)
- Direct Sequence Spread Spectrum (DSSS)
- Orthogonal Frequency Division Multiplexing (OFDM)

802.11 Physical Layers

Infrared

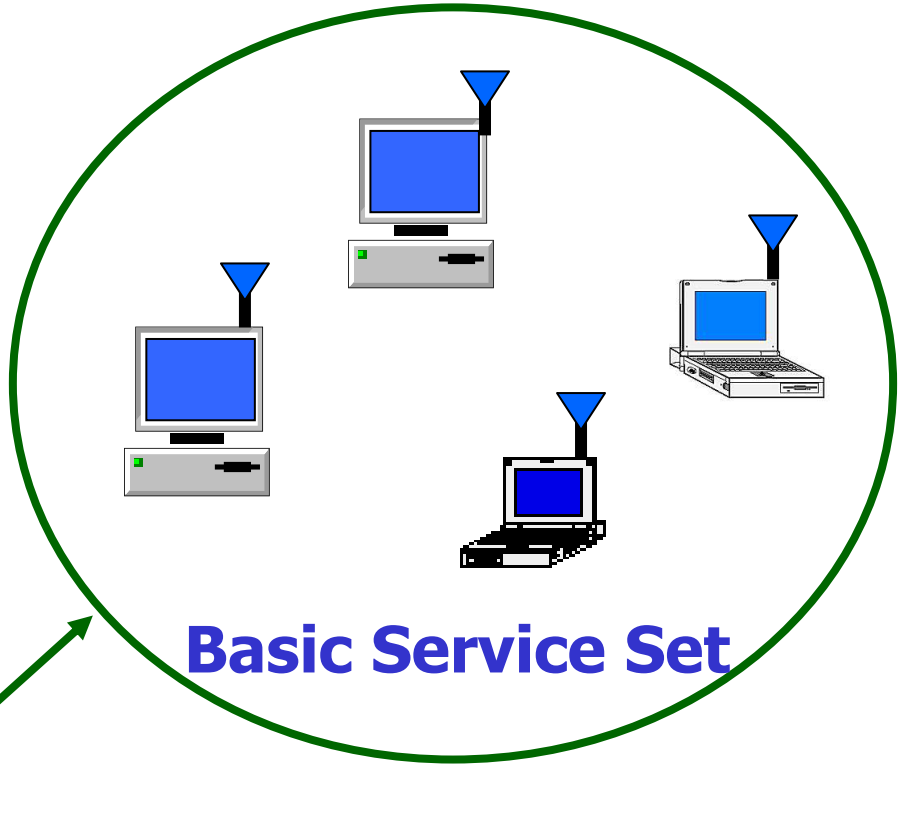
- 850-950 nM, Peak power = 2 Watts
- 16-Pulse position Mod, PPM (1 Mbps)
- 4-PPM (2 Mbps)

IEEE 802.11 Topology

- Independent Basic Service Set (IBSS)
- Extended Service Set (ESS)

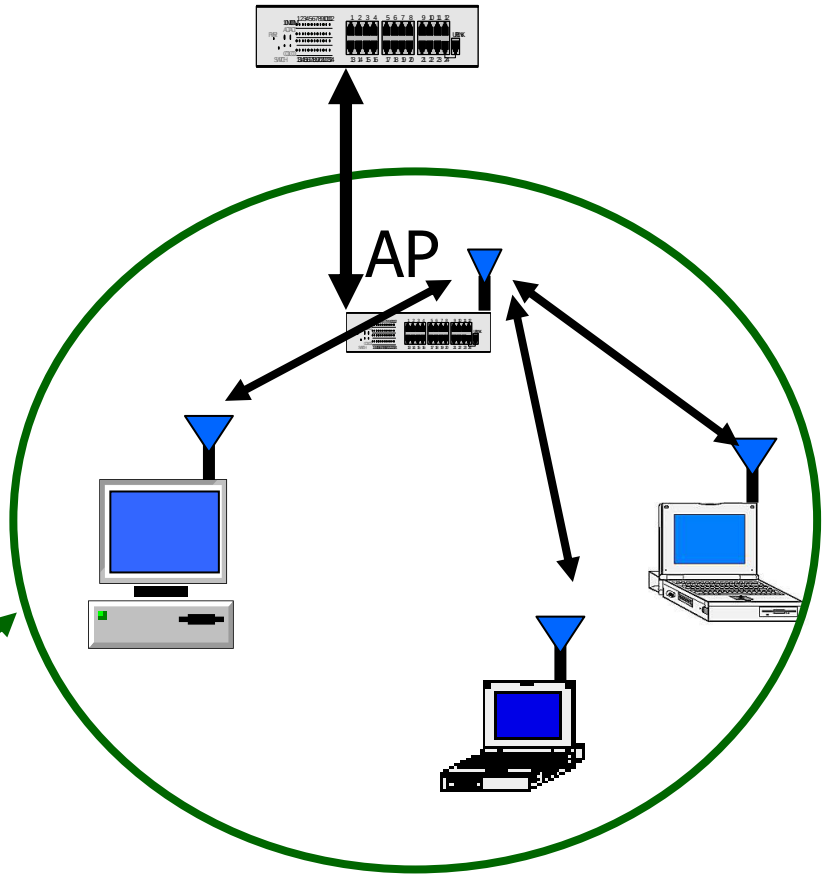
Independent Basic Service Set (IBSS)

- Stand-alone BSS
- No backbone infrastructure
- At least 2 stations
- **Ad hoc** Network
- Small area



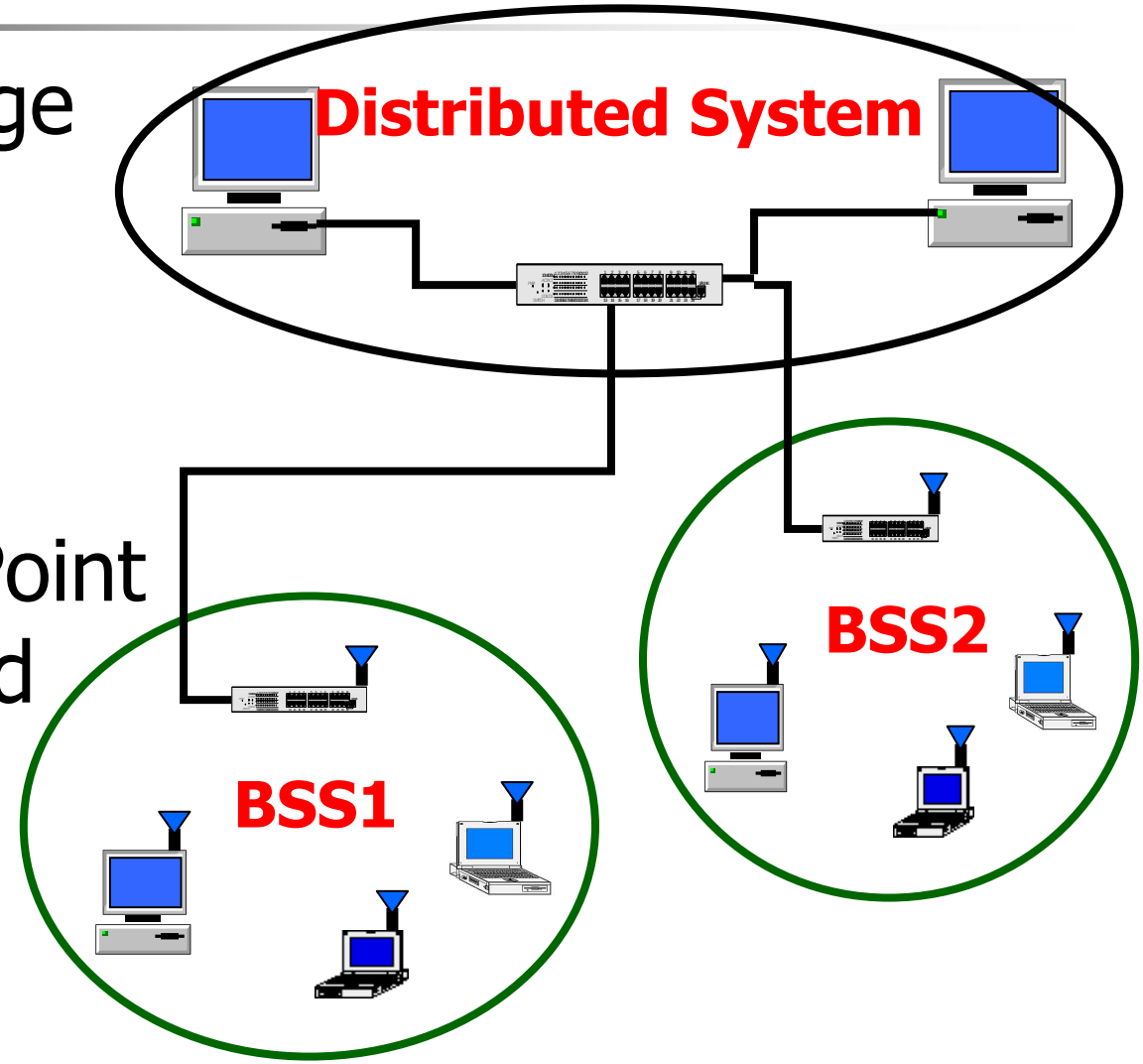
Infrastructure Basic Service Set

- Stand-alone BSS
- Connect to backbone infrastructure
- Access Point
- Small area



Extended Service Set (ESS)

- Extending range
- Arbitrary size
- Multiple cells interconnect
- Need Access Point and Distributed system

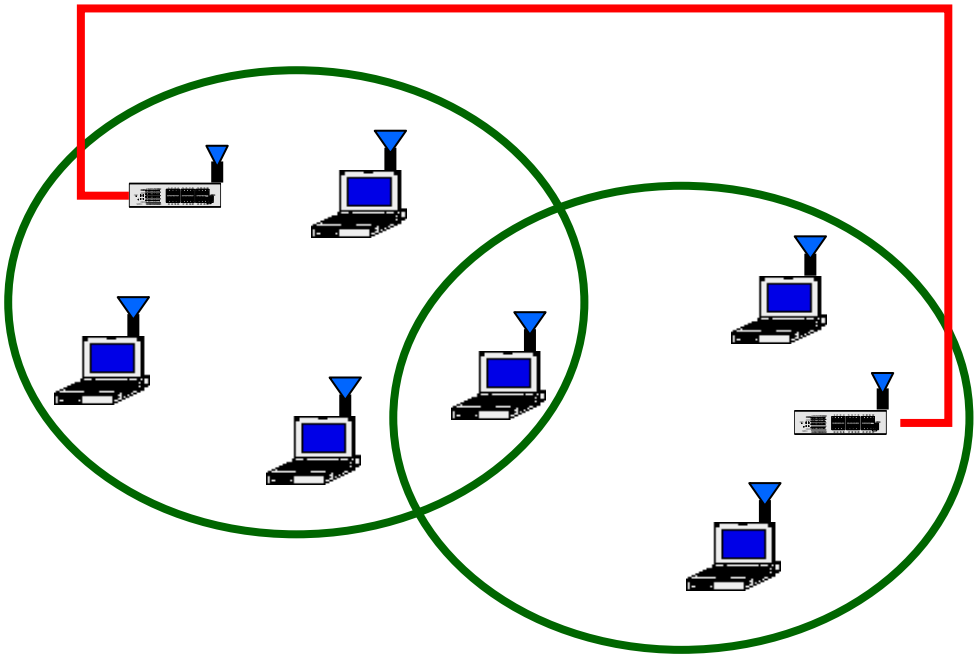


802.11 Mobility Types

- No-transition
  - Not move
  - Moving within a local BSS
- BSS-transition
  - Move from one BSS to another BSS, same ESS
- ESS-transition
  - Move from one BSS to another BSS, different ESS
- Guarantee for No-transition and BSS-transition
- IBSS & ESS are transparent to the LLC

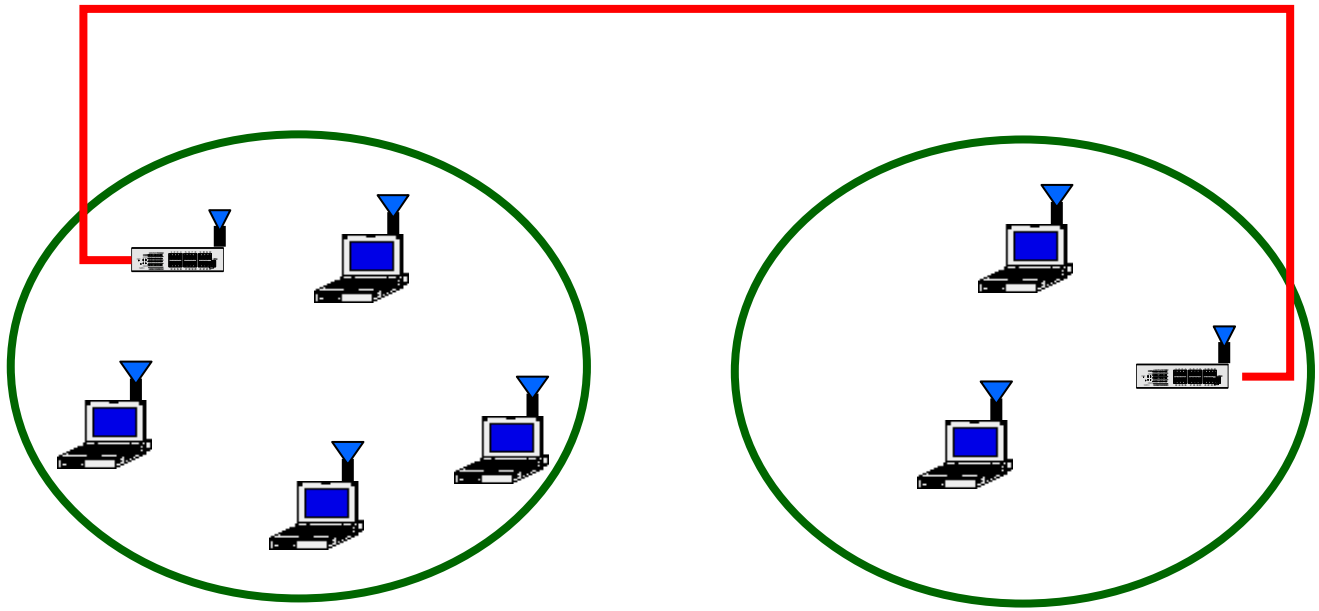
ESS Physical Configuration

- Partial overlap
  - Contiguous coverage in a defined area
  - No disruption



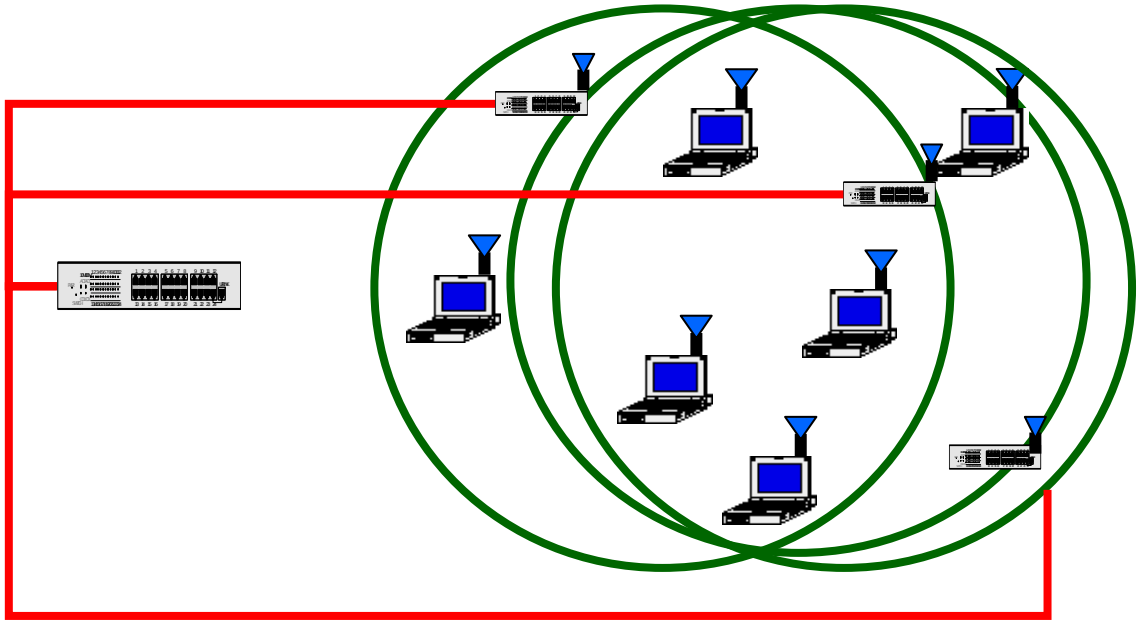
ESS Physical Configuration

- Physical disjoint
  - No contiguous coverage →no distance limit



ESS Physical Configuration

- Physical collocate
  - Redundant or high-performance network



Outline

- IEEE 802 Standards
- IEEE 802.11 Overview
- IEEE 802.11 Services
- History and present of IEEE 802.11

802.11 Services

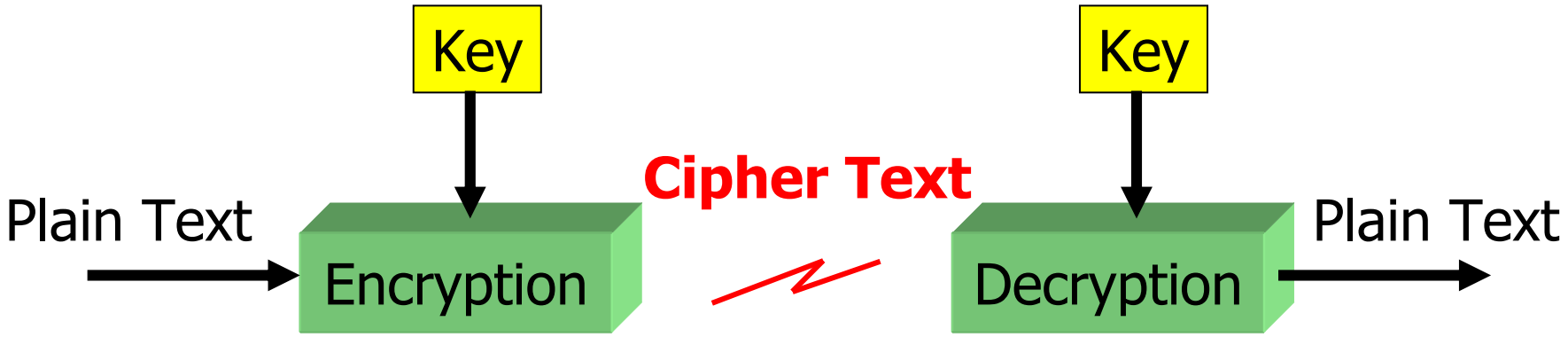
- Station Services (in wireless station)
  - Authentication / Deauthentication
  - Privacy
  - MSDU delivery
- Distribution System Services
  - Association / Disassociation / Reassociation
  - Distribution / Integration

Authentication

- Prevent unauthorized access
- Open system authentication
  - send authen. with ID → get back if recognize
- Shared key authentication
  - Secret shared key (through secure channel)
  - Authen. through shared key
  - Required Wireless Equivalent Privacy Algorithm (WEP)

Privacy

- 802.11 offers a privacy service option
- Based on 802.11 Wireless Equivalent Privacy (WEP) algorithm



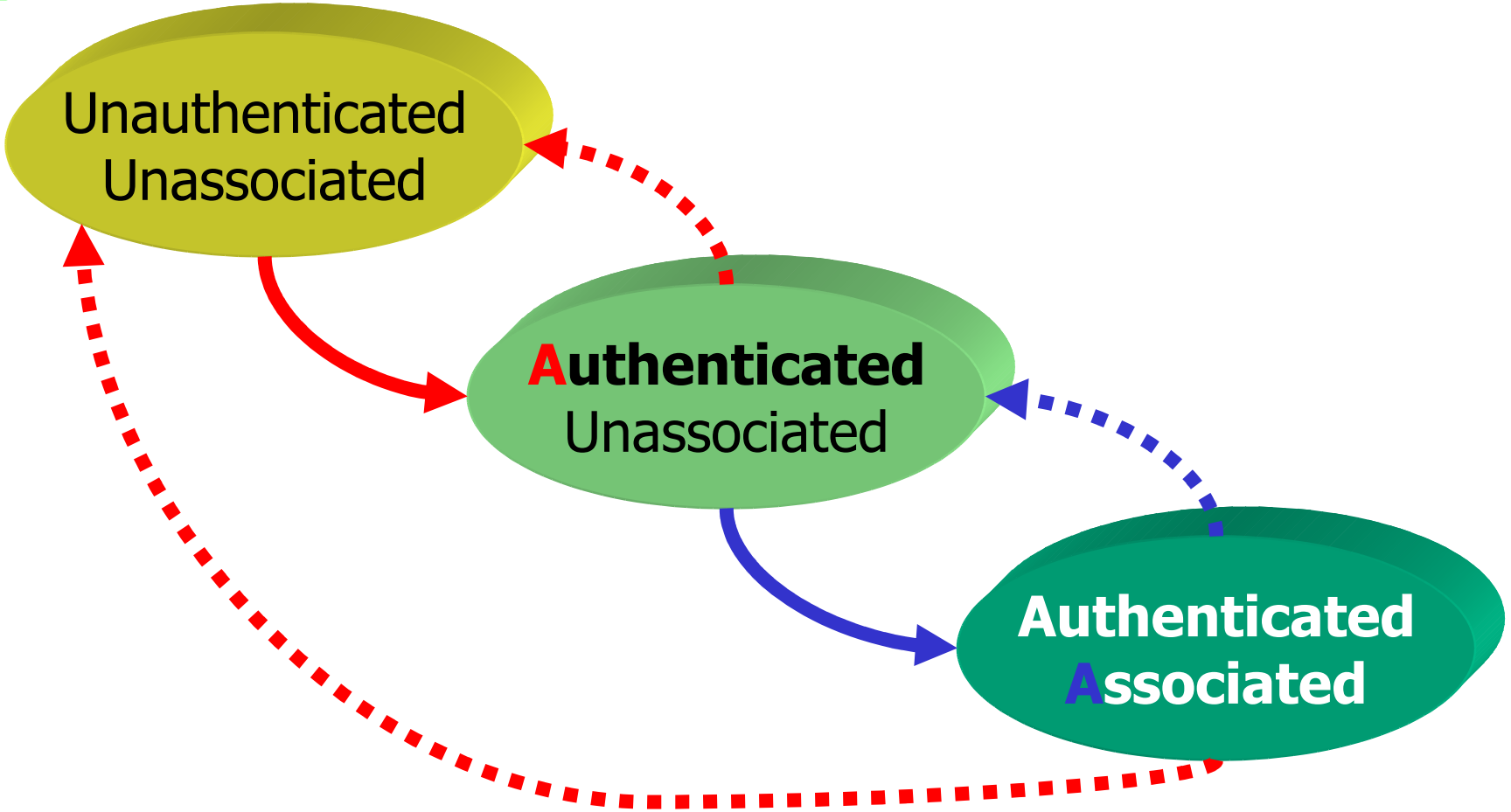
Association

- Perform @ access point
- Map a station to the distribution system via access point
- Otherwise the transmission is not allowed

Reassociation

- Change the status of association
- Support BSS-transition mobility
- Change the association attribute

802.11 State Diagram



Outline

- IEEE 802 Standards
- IEEE 802.11 Overview
- IEEE 802.11 Services
- History and present of IEEE 802.11

IEEE 802.11 Family

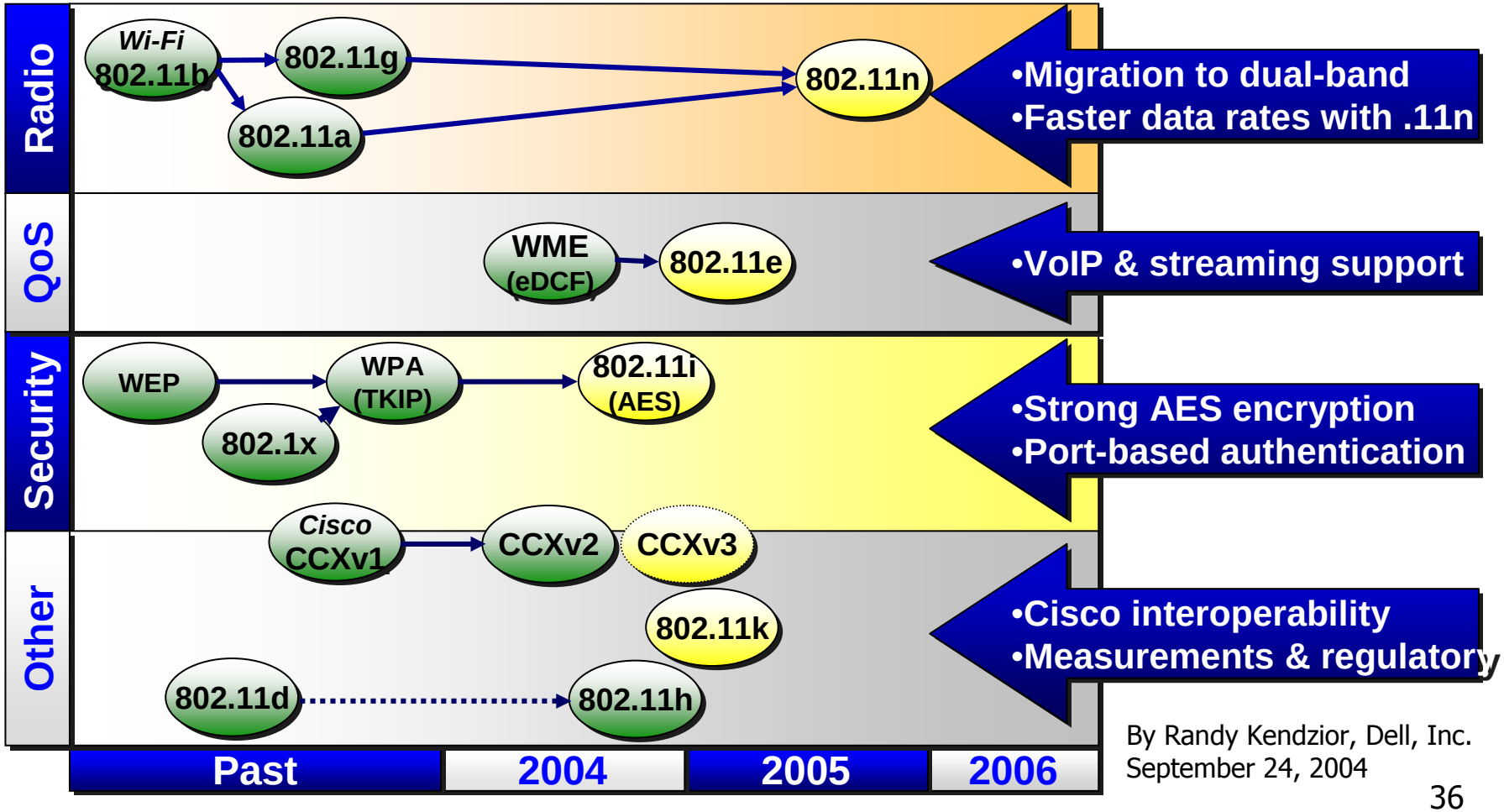
Standards	Band (GHz)	Raw Throughput
802.11	2.4	2Mbps (Legacy)
802.11a	5	54Mbps
802.11b	2.4	11Mbps
802.11g	2.4	54Mbps
802.11n	?	> 100 Mbps

IEEE 802.11 Family

Task Group	Descriptions
802.11c	Improves interoperability
802.11d	Multiple Regulatory Domains (Improve Roaming; New country)
802.11e	Quality of Service (QoS); prioritizing voice or video
802.11f	Inter-Access Point Protocol (IAPP)
802.11h	Supports measuring and managing the 5-GHz radio signals in 802.11a
802.11i	Enhanced Security (repairs WEP weakness)
802.11j	Extensions for Japan
802.11k	Passing specific radio frequency health and management data to higher-level management apps.

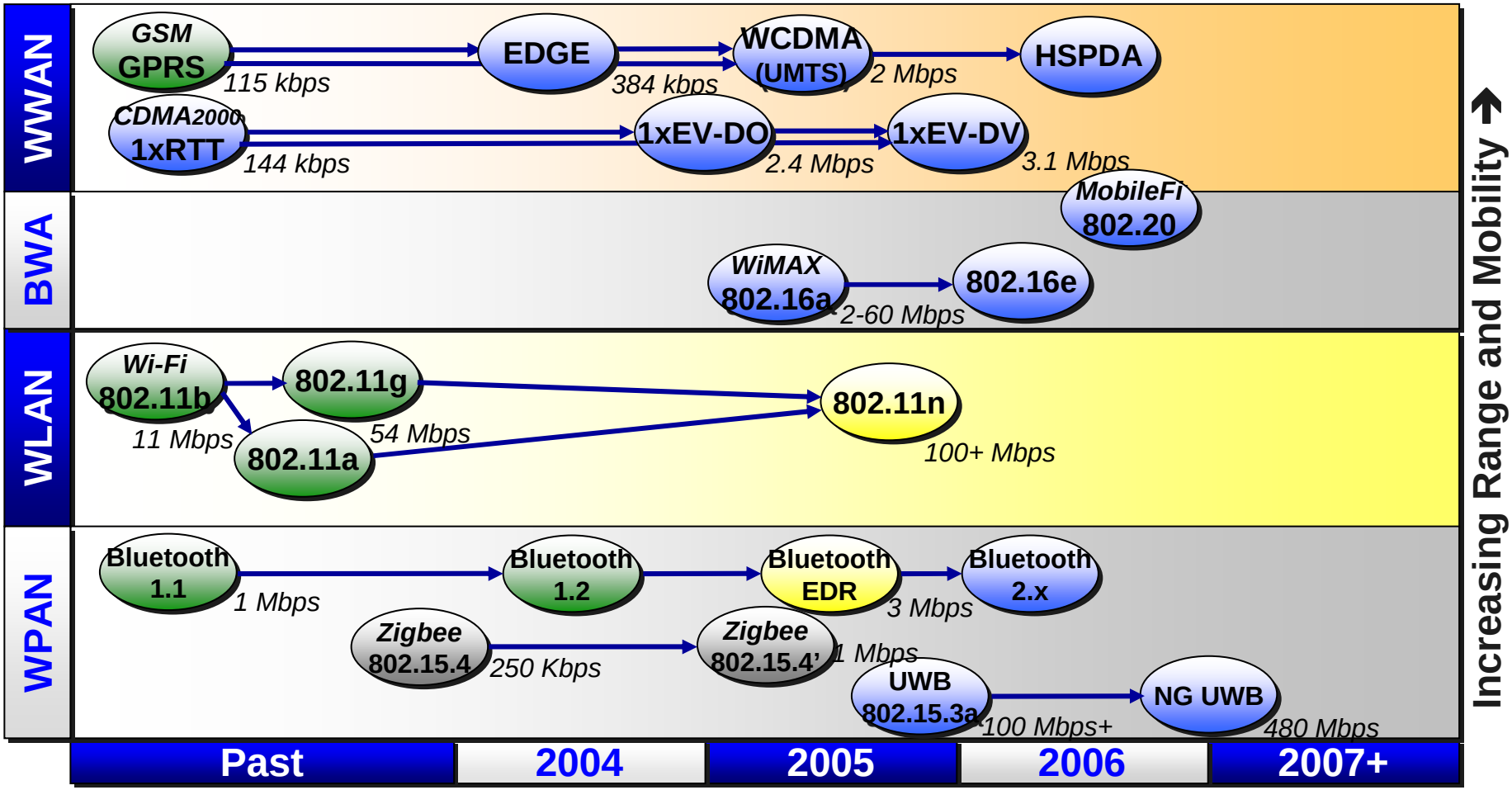
WLAN Technology Roadmap

WLAN standards will emphasize throughput, QoS, security & management…



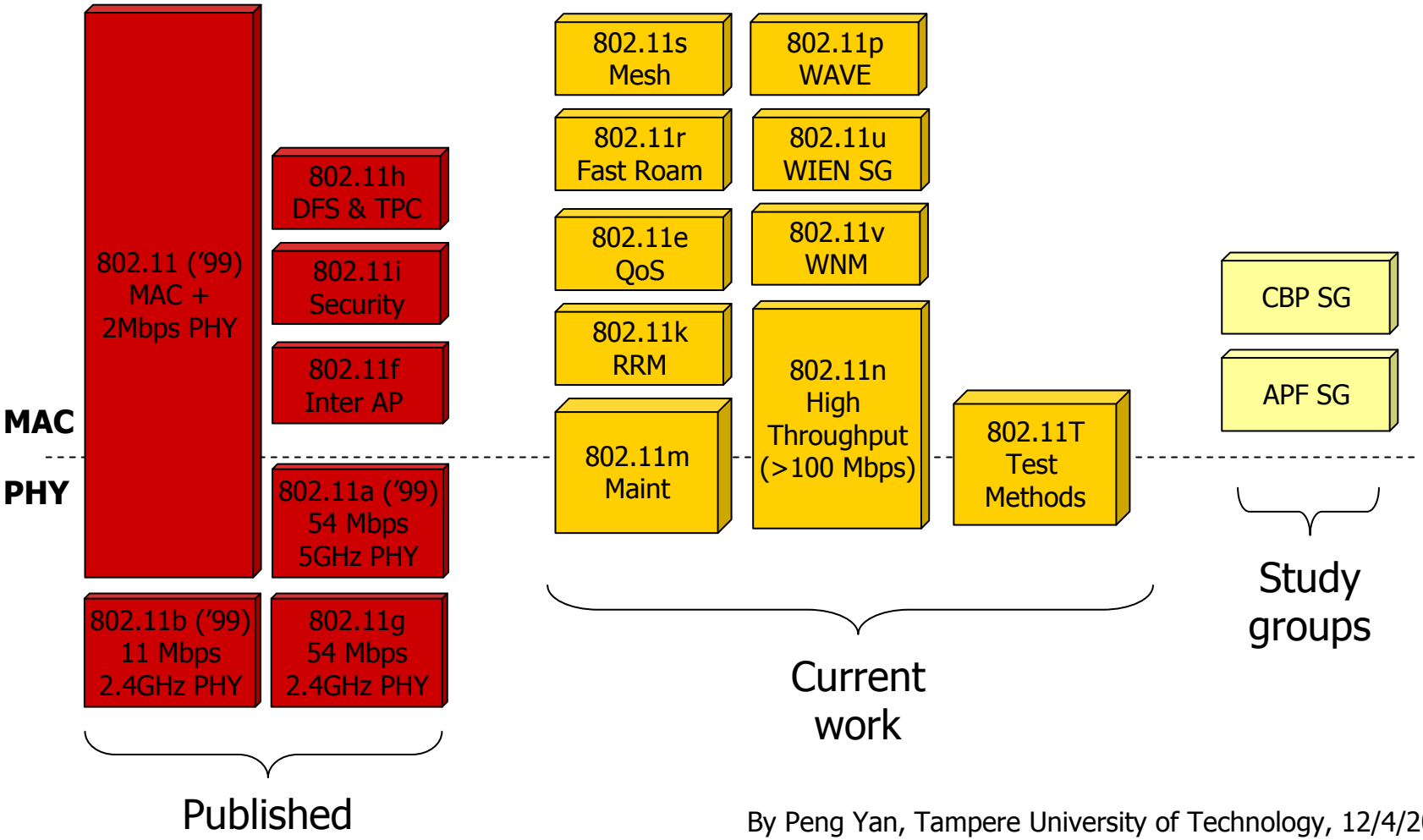
By Randy Kendzior, Dell, Inc.
September 24, 2004

Wireless Technology Roadmap



By Randy Kendzior, Dell, Inc.September 24, 2004

IEEE 802.11 Standards



History: 802.11 Legacy

- 1997: First standard
  - Standard name: IEEE 802.11-1997
  - Updated: IEEE 802.11-1999
  - Starting Point for “Standard-based WLAN”
- For 2 Mbps: (fallback to 1 Mbps – Noisy): Direct sequence Spread Spectrum (DSSS) modulation
- For 1-2 Mbps Frequency Hopping Spread Spectrum (FHSS)
- Both operate in ISM band 2.4 GHz
- FHSS, DSSS, and infrared medium

802.11b

- 802.11b-1999
- Range 50 – 100 m. (depends on obstacles)
- Omnidirectial antenna
- Indoor / Outdoor / Point-to-point (high-gain external antennas)
- Max throughput of 11 Mbit/s (5.5, 2,1 Mbps)

802.11b

- Attenuation: Metal, Thick walls, Water, etc.
- ISM Band 2.4 GHz; DSSS; CSMA/CA
- 14 overlapping ch. (Different ch.for different countries)
  - 3 simultaneously ch. (such as 1, 6, and 11)

802.11a

- 2001 (802.11a-1999)
- Max throughput of 54 Mbps (Normally around 20 Mbps)
- ISM Band 5 GHz (FCC may open more spectrum)

802.11a

- 12 nonoverlapping channels,
  - 8 dedicated to indoor
  - 4 to point to point
- Not widely deployed (US. / Japan)
  - 802.11b popularity
  - Less range / More attenuation
  - Lack of roll back compatibility (now support a,b,and g)
  - In Europe considering HiperLan2

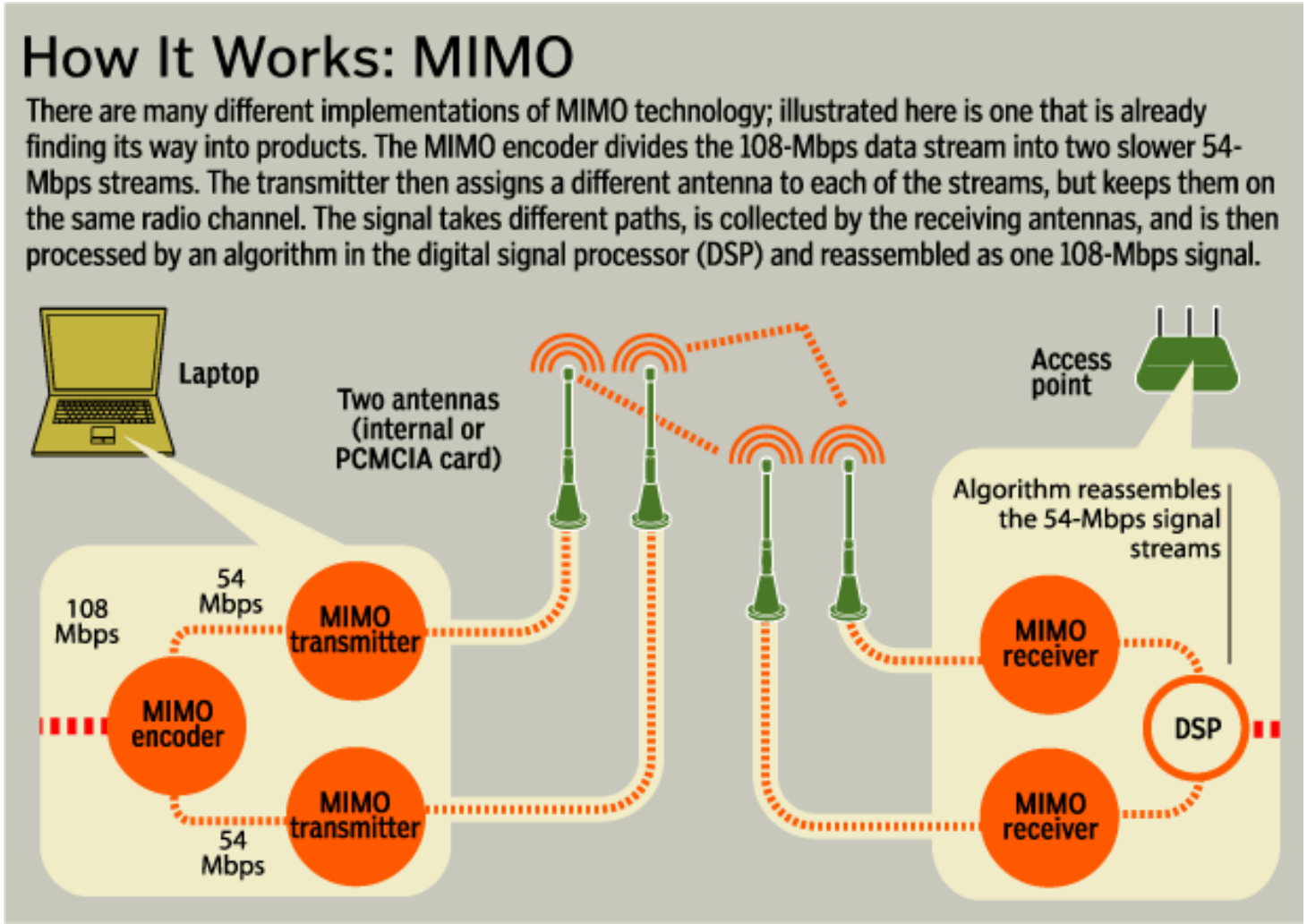
802.11g

- 3rd quarter 2003
- ISM Band 2.4 GHz
- Max throughput of 54 Mbps (Net 24.7 Mbps)
- Fully backwards compatible with 802.11b
- Dual-band / Tri-mode
  - supporting a, b, and g
  - A single wireless card / Access point

802.11n

- Established in Sep 2003
- 2 Competing Alliances (for the draft 802.11n)
  - Task group n synchronization (TGn Sync)
  - World Wide Spectrum Efficiency (WWiSE)
- Both agree on the usage of multiple input multiple output (MIMO) antenna technology
- Mostly differences on channel bandwidth allocation, PHY and MAC
- Max throughput (MAC SAP) ≥ 100 Mbps

MIMO


How It Works: MIMO
There are many different implementations of MIMO technology; illustrated here is one that is already finding its way into products. The MIMO encoder divides the 108-Mbps data stream into two slower 54-Mbps streams. The transmitter then assigns a different antenna to each of the streams, but keeps them on the same radio channel. The signal takes different paths, is collected by the receiving antennas, and is then processed by an algorithm in the digital signal processor (DSP) and reassembled as one 108-Mbps signal.
Laptop
Two antennas (internal or PCMCIA card)
Access point
Algorithm reassembles the 54-Mbps signal streams
108 Mbps
54 Mbps
MIMO transmitter
MIMO encoder
MIMO transmitter
54 Mbps
MIMO receiver
DSP
MIMO receiver

802.11n Channel Bandwidth

- TGn Sync uses 40 MHz channels in the 5 GHz spectrum, the same one used by 802.11a
- WWiSE prefers 20 MHz channels in the 2.4 GHz consistently used 802.11b/g spectrum

Throughput comparison

Std.	802.11b	802.11a/g	802.11n
Over the Air	11 Mbps	54 Mbps	>200 Mbps
MAC SAP	5 Mbps	25 Mbps	>100 Mbps

SAP = service access point

Application Comparison

- 802.11a/b/g focus on computer networking
- 802.11n interests on broad communication and entertainment areas
  - Consumer applications like HDTV
  - Streaming video

802.11 Wi-Fi

- Specification defined by IEEE (not Compatibity guarantee)
- A special group, Wi-Fi Alliance
  - Group of maufacturer
  - Test compatibility
  - Guarantees interoperability (by issue Wi-Fi Trademark)
  - Start with 802.11b → Dual band/Tri mode (a, b, or g)
  - Security standard Wi-Fi Protected Access (WPA)

802.11e

- MAC Enhancements for Quality of Service in the capabilities and efficiency of the protocol.
- VoIP

IEEE 802.11i

- Weakness reports in the WEP
- Create a larger number of initialization vectors for encryption.
- Dropping “WEP2” → Change to Temporal Key Integrity Protocol (TKIP)
  - a key retains its security over a period of time
- Need 802.1x
  - Authenticating method
  - Some weaknesses (man-in-the-middle style interception)