

802.11 Technology, Application and Development

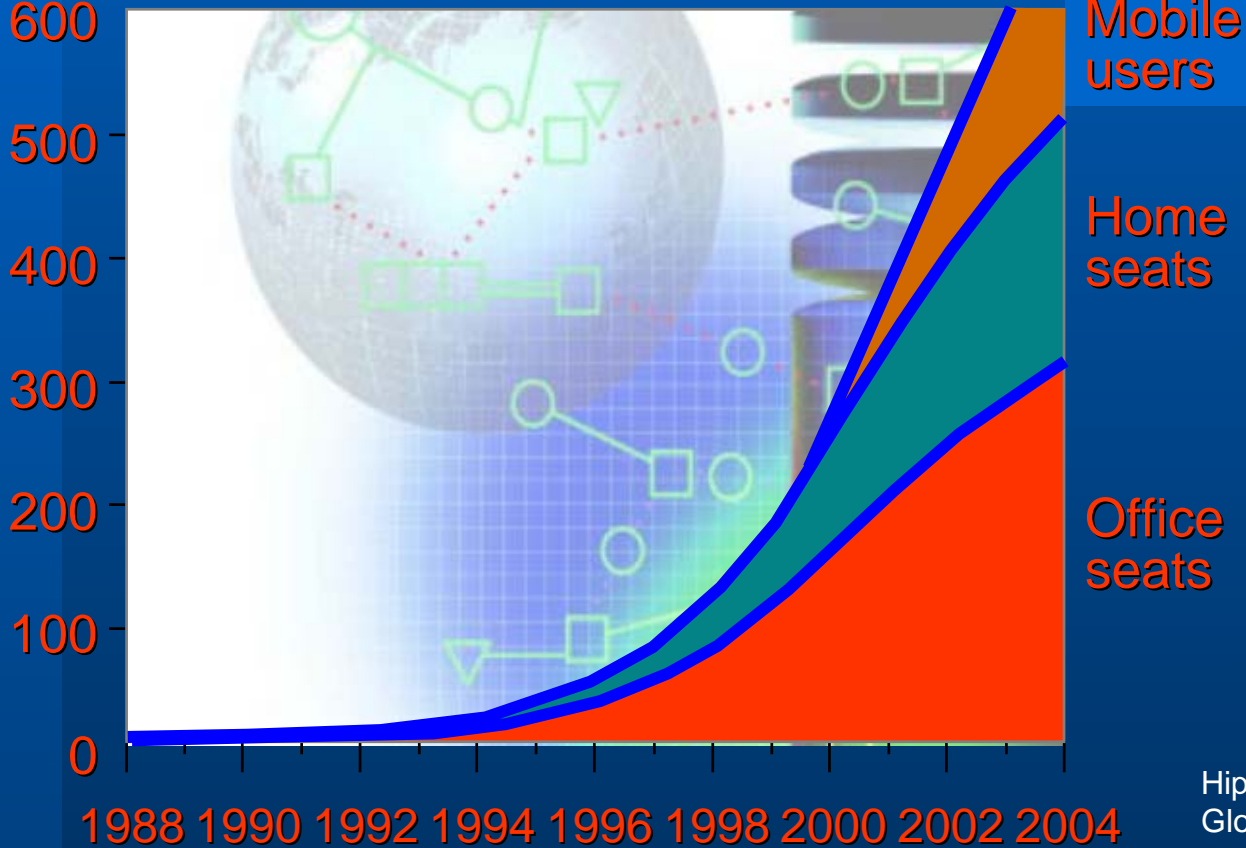
**MA Yan, BUPT
Hebei CERNET-2002
Shijianzhuang
2002 / 11 / 28**

Topics

- LAN and Wireless LAN (WLAN)
- 802.11 family standards
- Technique specifications
- Products on the market
- Deployment in the campus network
- Security issue
- Future development

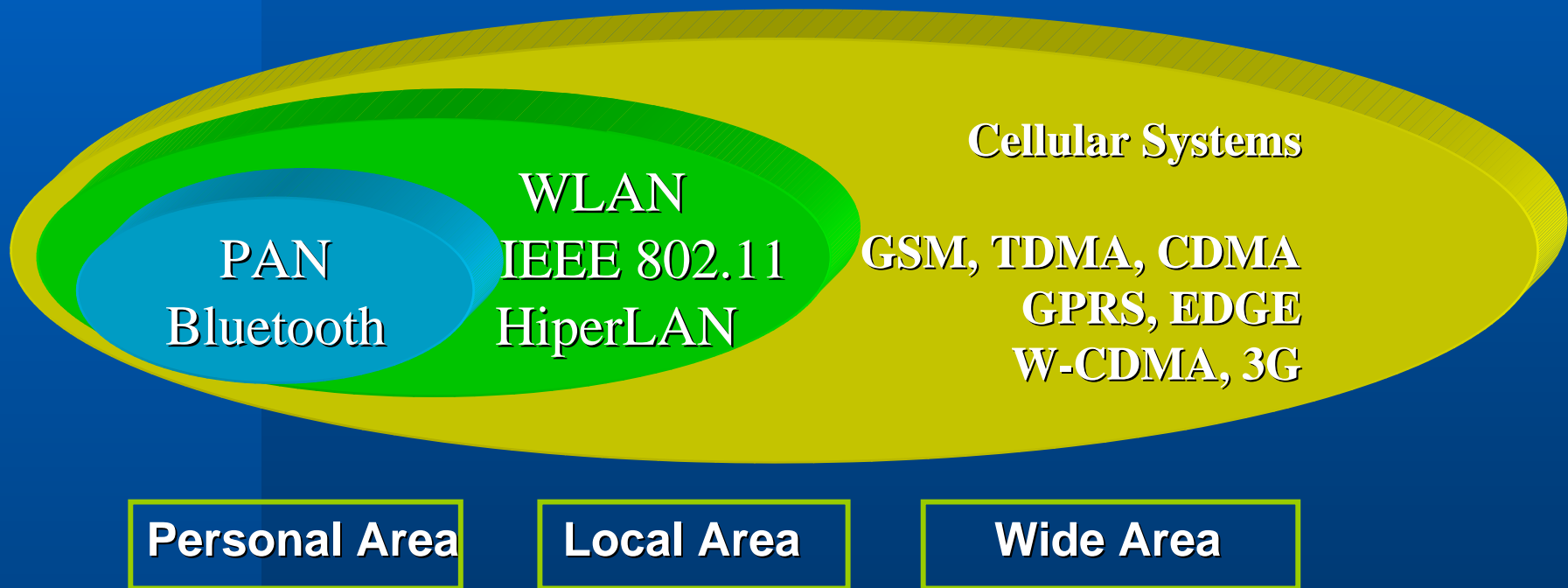
Growth rate: Mobile users of Internet

million



HiperLAN/2
Global Forum

PAN / WLAN / Cellular system



LAN and Wireless LAN (WLAN)

- In early 90's, 802.11 research group start to define the access method and physical layer specification for Wireless LAN.
- Documented by ISBN 1-55937-052-1
- Version info:
 - **ANSI/IEEE Std 802.11, 1997,1999 Edition**
 - **[ISO/IEC 8802-11: 1999]**

802.11 Working Group for WLAN

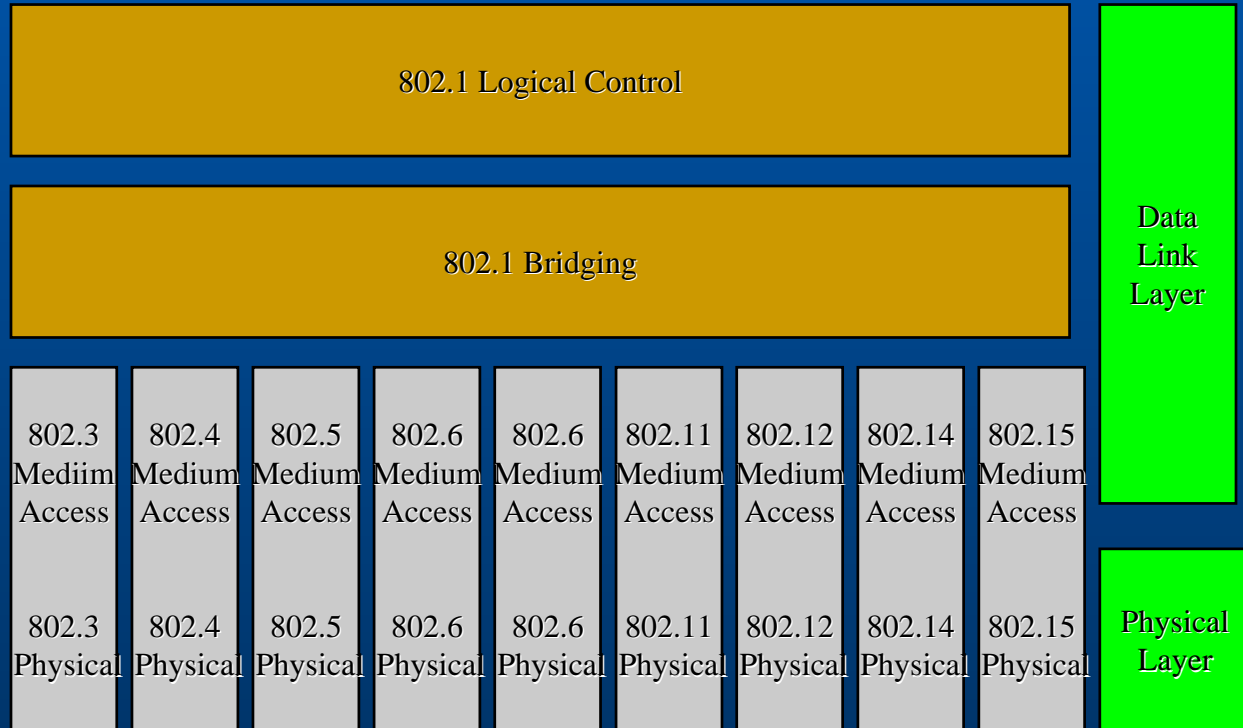
- The IEEE 802.11 specifications are wireless standards that specify an "over-the-air" interface for
 - between a wireless client and a base station (or Access Point)
 - among wireless clients.
- The 802.11 standards can be compared to the IEEE 802.3 standard for **Ethernet** for wired LANs.
- The IEEE 802.11 specifications address both the Physical (PHY) and Media Access Control (MAC) layers and are tailored to resolve compatibility issues between manufacturers of Wireless LAN equipment.
- <http://grouper.ieee.org/groups/802/11/index.html>
- <http://www.wirelessethernet.org/>

802.X family

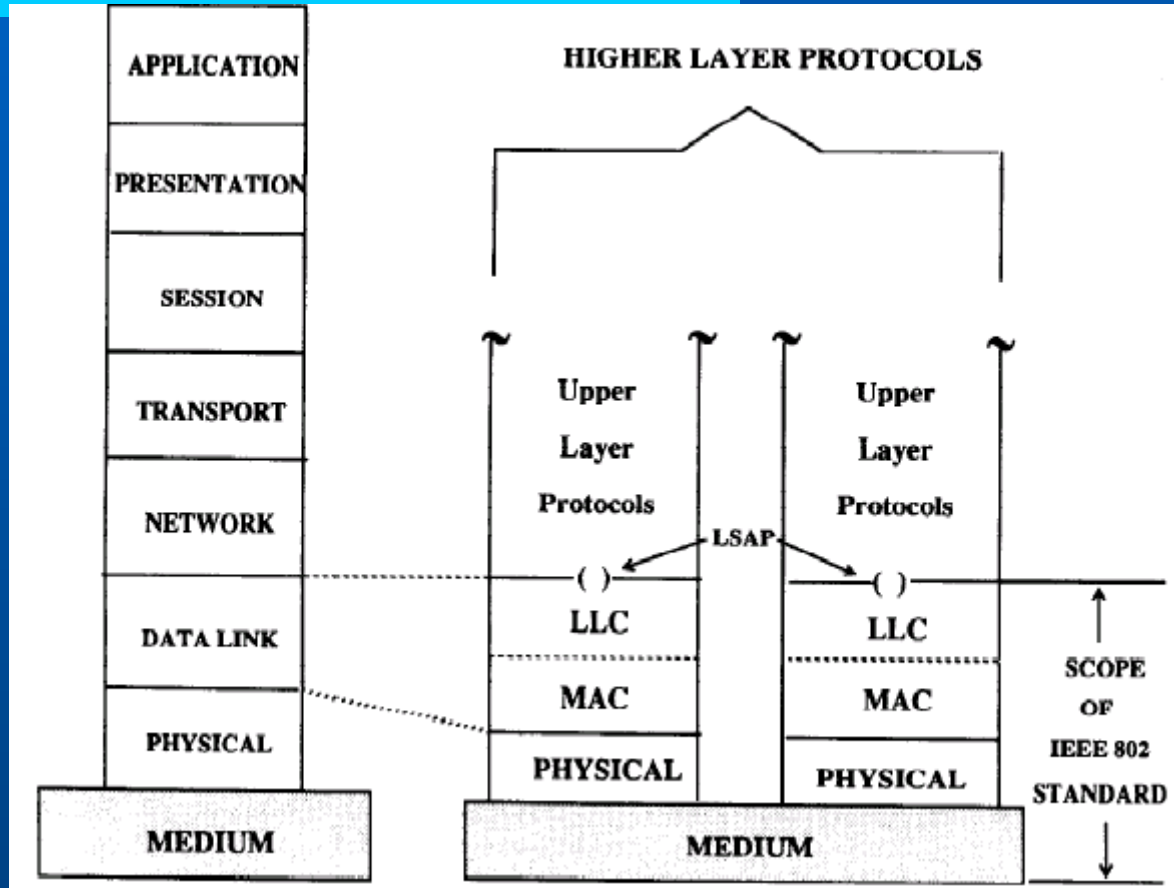
802.10 Security

802 Overview & Architecture

802.1 Management



802.11 with OSI/rm



802.11 standards family comparison

	802.11b	802.11a	802.11g
Date	1997	1999	2001
Speed	11Mbps	54Mbps	11/54Mbps
	CCK / spread spectrum	OFDM	CCK/OFDM
Freq.	2.4Ghz	5GHz	2.4/5GHz
Channels	3 1,6,11	8	3

OFDM parameters

- Orthogonal Frequency Division Multiplexing

Data rate	6,9,12,18,24,36,48,54
Modulation	BPSK,QPSK,16-QAM,64-QAM
Coding rate	1/2, 2/3, 3/4
Number of sub-carrier	52
Number of pilots	4
OFDM symbol duration	4us
Guard interval	800ns
Sub-carrier spacing	312.5KHz
-3DB bandwidth	16.56 MHz
Channel spacing	20MHz

802.11a modulation schemes

Mode	Modulation	Coding rate R	Nominal bit rate [Mbit/s]	Coded bits per sub-carrier	Coded bits per OFDM symbol	Data bits per OFDM symbol
1	BPSK	1/2	6	1	48	24
2	BPSK	3/4	9	1	48	36
3	QPSK	1/2	12	2	96	48
4	QPSK	3/4	18	2	96	72
5	16QAM (H/2 only)	9/16	27	4	192	108
5	16QAM (IEEE only)	1/2	24	4	192	96
6	16QAM	3/4	36	4	192	144
7	64QAM	3/4	54	6	288	216
8	64QAM (IEEE only)	2/3	48	6	288	192

Frequency Band Allocation

Location	GHz	
North America	2.400~2.4835	1000mw
Europe	2.400~2.4835	100mw
Japan	2.471~2.497	10mw
US (UNII Lower band)	5.150~5.250	min of 50mw
US (UNII middle band)	5.250~5.350	min of 250mw
US (UNII upper band)	5.725~5.825	min of 1000mw

Some of the Abbreviations and acronyms

- **AP:** Access Point. Each BSS has one AP to relay the Client STAs' traffic each other within a BSS and ESS.
- **BBP:** broadband Processor
- **BSS:** Basic Service Set. The BSS consist of an AP and several Client STAs
- **CSMA/CA:** Carrier Sense Multiple Access with Collision Avoidance
- **DSSS:** direct sequence spread spectrum
- **ESS:** extended service set
- **ESSID:** Extended Service Set Identification
- **WEP:** Wired Equivalent Privacy

STA's Function

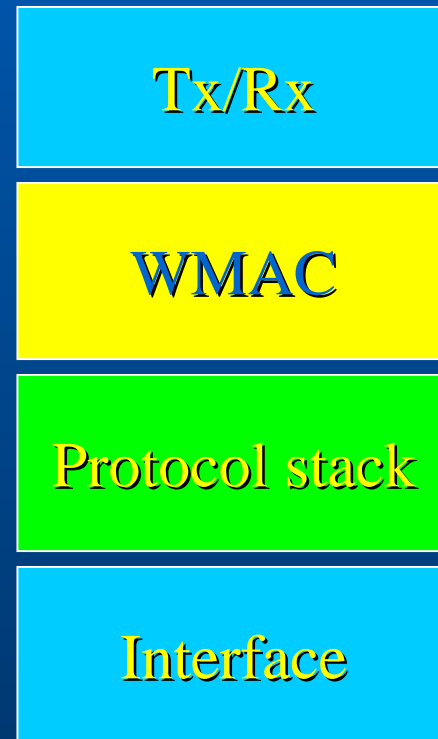
- **WLAN BBSs/APs discovery**
- **Synchronization with the BBS**
- **Authentication/deauthentication and privacy**
- **Data delivery**

Wireless MAC layer features

- Synchronization,
- MAC layer retransmission,
- MAC level ACK,
- MAC lever RTS/CTS,
- Virtual carrier sensitive,
- Fragmentation,
- DCF operation
- PCF polling response
- Data rate auto-selection,
- Power management
- Roaming.
- WEP

MAC in 802.11

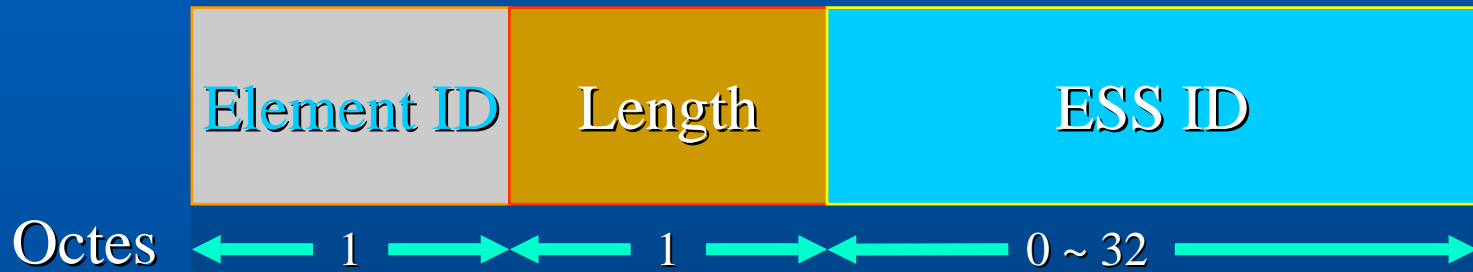
- **Spread Spectrum**
 - Direct sequence
 - direct spread spectrum
 - Frequency hopping
- **Infrared**
- **Narrow band**
- **Multi-channel roaming**
- **Security**
 - 35mW, 22Mhz bandwidth, 15dBm



BBP's function

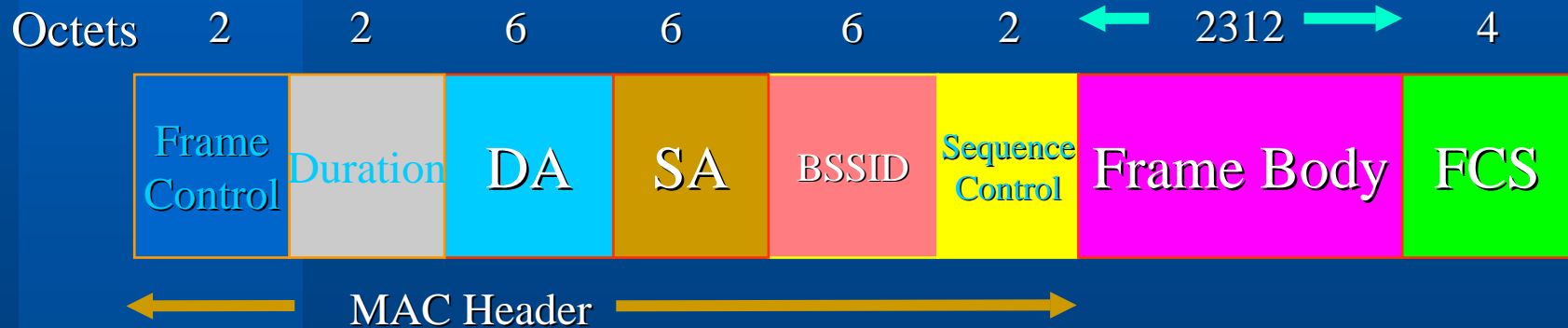
- Framing
- CRC generating and checking
- Data scrambler
- Symbol level synchronization
- Symbol Shaping
- AGC
- RSSI
- Other processing depends on the different modulation schemes, like coding, decoding, mapping, marching filter, etc.

SSID, ESSID



The SSID element indicates the identity of an ESS or IBSS.

Frame format example



The frame format for a Management frame is independent of frame subtype.

IEEE 802.11 standard family

- 802.11 1~2Mbps
- 802.11a 5G 54Mbps
- 802.11b 2.4G 11Mbps
- 802.11c Bridging
- 802.11d International Roaming
- 802.11e Quality of Service (Qos)
- 802.11f IAPP(Inter AP Protocol)
- 802.11g 2.4G 54Mbps
- 802.11h Compatibility Issue in Europe
802.11-HyperLAN integration
- 802.11i Enhanced Security

Products on the market

- Intel
- 3Com
- Avaya
- Cisco
- Enterasys
- Dlink
- 神州数码
- 上海贝尔
- ...

Products on the market

Vendor	Chip set	Product	OEM partner
Lucent		Wavelan, Orinoco	Apple Airport (customized) Enterasys RoamAbout 802
Intersil	PrismII(PHY+MAC) PrismII and Prism2.5Two MAC controller		BreezeCom, Alcatel, Cisco, Compaq, 3Com, Dell, D-Link, Nokia, Nortel, Samsung, Siemens, Sony, SpectraLink, Symbol Technologies, Zoom and other up to 50 companies use its PHY or entire chip set
AMD	AM79c930 core/80188(MAC) +PrismII PHY		Intersil PrismI chip set use AMD MAC controller.Zoom ZoomAir YDI and others
Symbol	NA (MAC)+PrismII PHY	Spectrum24 HR	Intel PRO/Wireless,3Com AirConnect, Ericsson
Cisco	NA (MAC) +PrismII PHY Acquire from Aironet 2ARLAN	Cisco 340, 350ARLAN 4800b	Dell TureMobile

Technique specifications

- **bandwidth**
- **Range: 100 Meters**
- **radio frequency**
- **interference tolerance**
- **power consumption**
- **standards**
- **drivers for OS: Win / Linux, ...**
- **card type: Internal / External**
- **...**

主要产品的类型和功能

- 无线网卡
 - PCMCIA网卡 适用于笔记本电脑
 - PCI网卡 适用于台式电脑
 - USB网卡 适用于台式电脑
- AP (Access Point) 无线网络接入点
- 无线网桥(Bridge) 子网间的无线联接设备

802.11b AP (Access Point)



Various 802.11a PC cards



SMC 802.11a Wireless CardBus Adapter



Proxim Harmony 802.11a CardBus Card

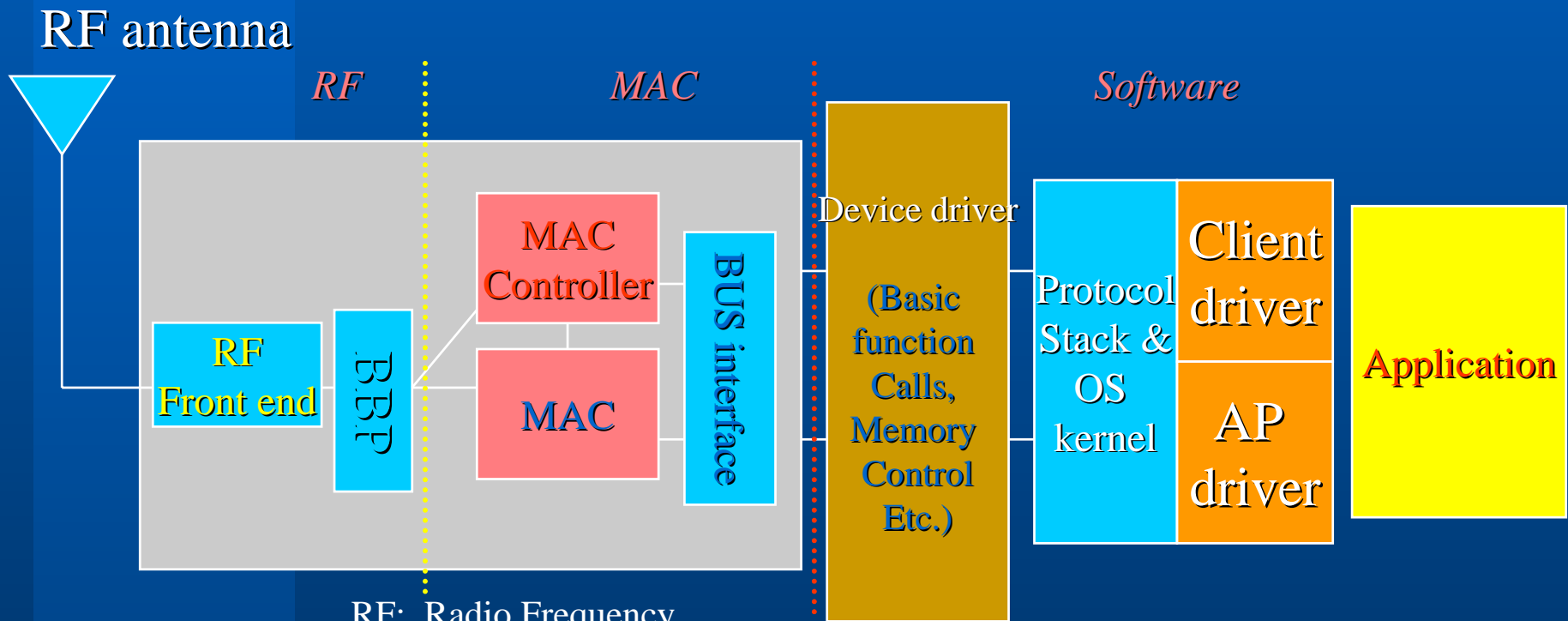


Intel PRO/Wireless 5000 LAN CardBus Adapter



Actiontec 802.11a Wireless Networking² Cards

802.11b PC Card Diagram



RF: Radio Frequency
 BBP: Base Band Process
 MAC: Media Access Control
 AP: Access Point

Wireless LAN Design

- Review of basic WLAN RF technology
- Access Point and NIC critical features
- Optimized WLAN design process
 - What to cover?
 - What tools do you need for testing?
 - How to save your budget
 - Power supply
- Real-world design examples: Office, Campus, Warehouse

WLAN Scenario 1: PC to PC

Wireless LAN PC Card

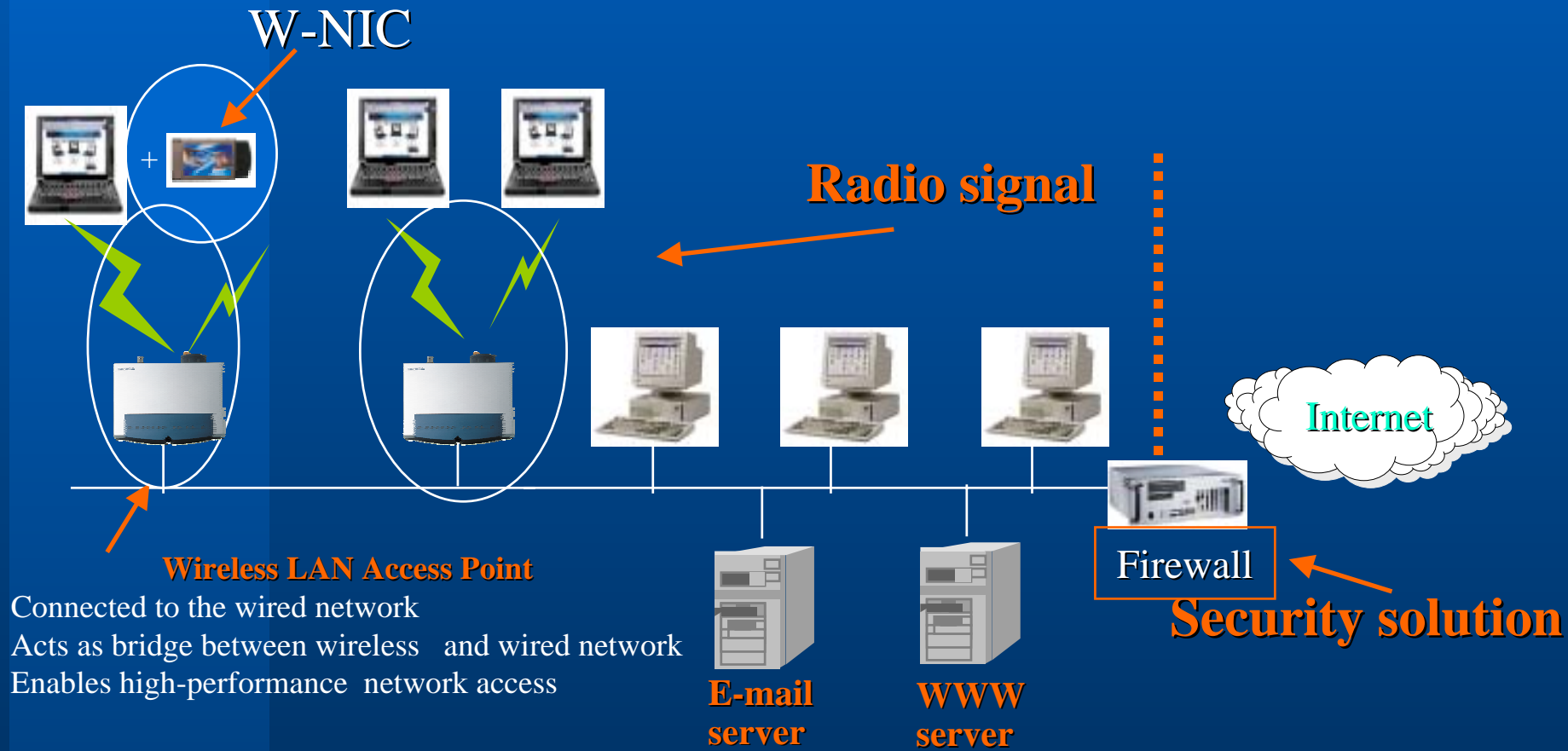
- Each wireless station and access point has a wireless LAN card
- Provides an interface between an end-user device and radio waves



Wireless NIC link 2 PCs directly

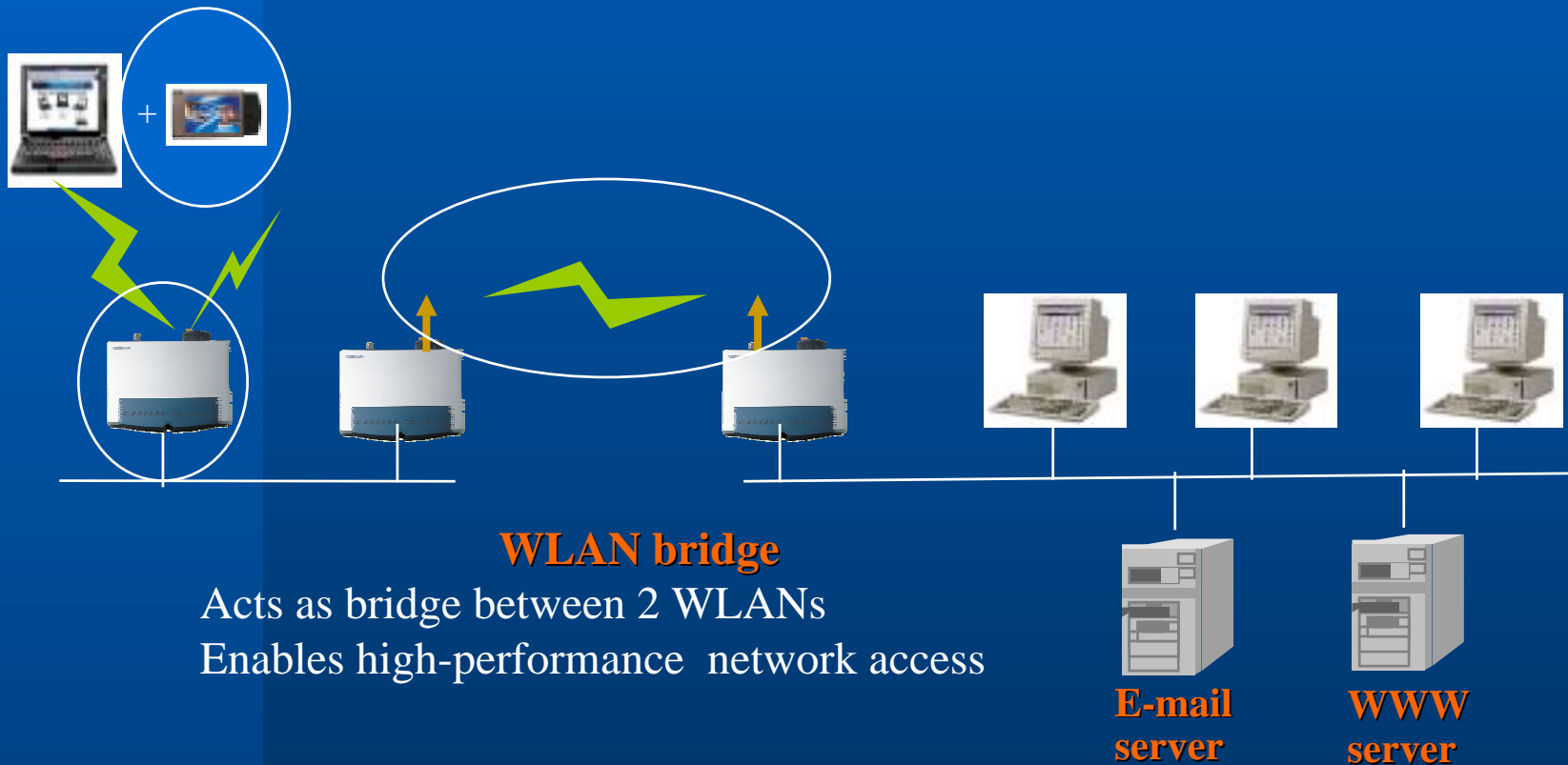
PC could communicate with each other sharing data
Enables information exchange with ease

WLAN Scenario 2: PC to LAN



Wireless LAN Access Point
Connected to the wired network
Acts as bridge between wireless and wired network
Enables high-performance network access

Scenario 3: LAN to LAN



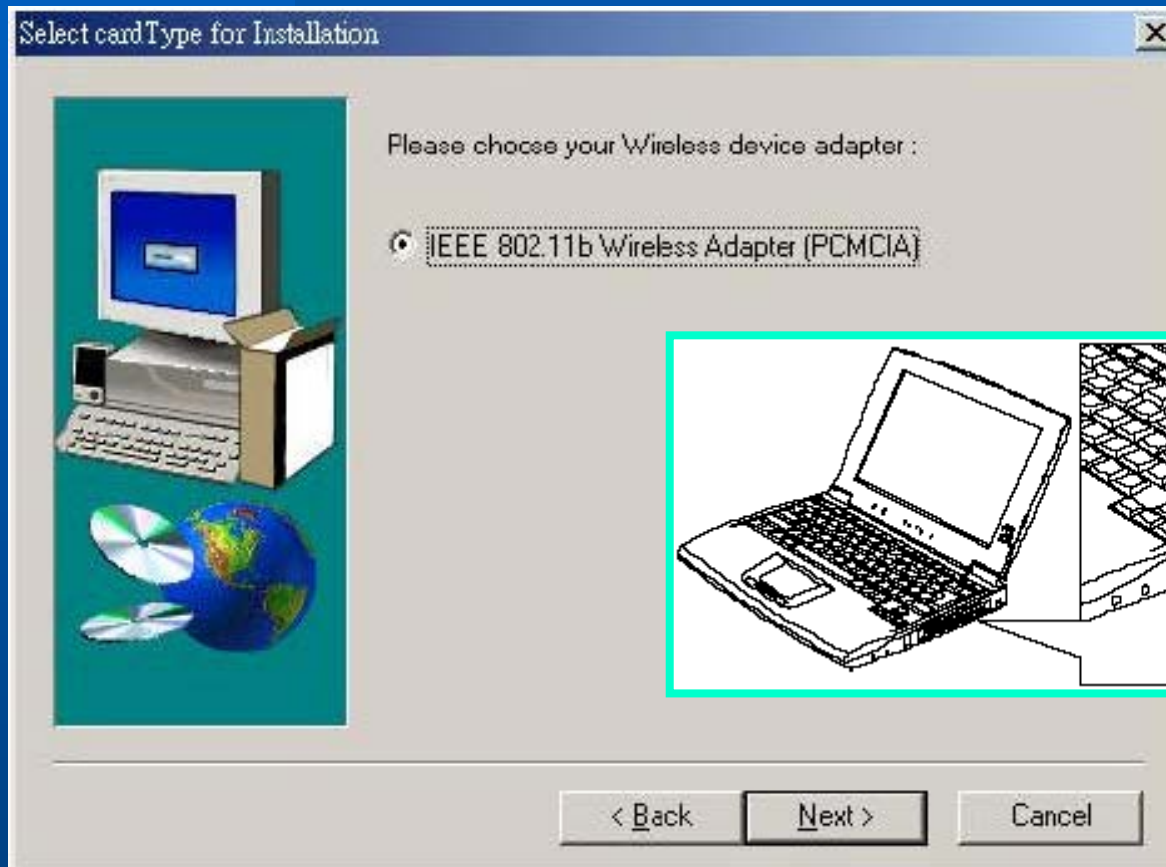
Scenario 4: Ad hoc network



Deployment in the campus network

- Conference hall
- Lecture area and Classroom
- Office area
- Entertainment area
- Sports center
- Others, ...


Installation of 802.11b PCMCIA card

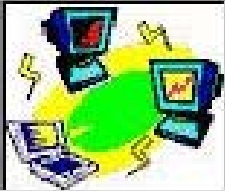


Link quality inspection

IEEE 802.11b Utility

Wireless LAN Neighborhood | Setting

Access Point SSID	Access Point MAC
 MyNetwork	00:90:4B:08:75:42



Rescan

More ...

Link Quality

100 %

Signal Strength

100 %

Deployment in the commercial market

- 国家无委会2002年7月22日发布《关于短距离微功率无线电设备使用2400MHz频段有关问题的通知》，也正式开放5.8GHz频段，并具体规定5.725G~5.85GHz为合法使用频段。
 - 网通开展“无限伴旅（Mobile Office）”活动
 - 上海电信的“天翼通”服务
 - 北京电信2001年试推无线局域网服务

Security issue

- **What You Need to Know to Protect Your WLAN**
 - It inherited all security problem from wired network
 - WEP, Encryption Key 64/104 bits, ...
 - ESSID still could be detected easily by hackers
- **Security Solutions**
 - Demonstrations include WLAN discovery and traffic analysis, 802.1x setup and more.

Roaming issue

- **Walking or Roaming?**
- **Moving in Layer 2: Walking**
 - Do not change IP address , roaming among APs
- **Moving in Layer 3: Roaming**
 - IP address changed, among 2 or more networks
- **No perfect solution yet.**

Authentication

- MAC/ IP/ MAC&IP/ BSSID/ WEP KEY/ UserName Password
- PPPoE/ Web + DHCP
- IPSEC/ VPN



Network management

无线局域网综合管理系统

文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)

地址(A) http://210.25.132.5/intal/wlan/index.jsp?leftURL=login.jsp&rightURL=introduce.html

无线局域网综合管理系统

首页 系统设置 AP 配置 访问控制 故障监控 性能查看 计费 帮助

无线局域网管理 / Wireless LAN

用户名: admin

密码: []

登录 重置

无线局域网综合网管

1. 功能介绍:

本无线局域网综合网管系统主要用来维护和管理组成无线局域网的所有支持 IEEE802.11 协议的各厂商的无线设备。通过使用本网管系统, 可以确保您的无线局域网安全、可靠、经济、有效地运行, 且具有以下特点:

功能的完善性:
本无线局域网综合网管系统基本实现了国际标准化组织 (ISO) 定义的网络管理的 5 个功能领域: 故障管理、性能管理、配置管理、安全管理以及计费管理;

安全性:
本无线局域网综合网管系统采用密码认证技术、客户访问控制技术、客户与无线设备之间数据传输的无线加密认证技术以及日志管理策略, 能够保证只有本系统的网络管理员才能有权限修改本系统和无线设备的配置, 只有事先许可的用户才能接入您的无线局域网, 可以有效地防止黑客的攻击;

平台无关性:
本无线局域网综合网管系统采用了与平台无关的 Java 面向对象技术和组件技术, “一次编译到处运行”; Web 页面采用基于 Java 语言的 JSP, 具有特别强的扩展能力, 良好的扩展;

本无线局域网综合网管系统可以方便地搜集在所有主流的 Unix 平台和 WINDOWS2000 以上操作系统平台上;

版权所有 2001 北京邮电大学信息网络中心 联系电话: 010-62283044-8001

WLAN application example

- One of the Newest applications——
Phone based on 802.11b



802.11b ? .11a? .11g?

- IEEE 802.11g designed for bridging 11b/11a
- But, IEEE 802.11g will not be supported by EU.
- Vendor will provide .11b / .11a dual-stack NIC and AP for migration.



- What's the best solution do you think?

Other WLAN companion

- IEEE 802.15
- IEEE 802.16

802.15 Working Group for Wireless Personal Area Networks

- The IEEE 802.15 Working Group provides, in the IEEE 802 family, standards for low-complexity and low-power consumption wireless connectivity.

In March 1998, the Wireless Personal Area Network study group was formed. In May 1998, the [Bluetooth Special Interest Group \(SIG\), Inc.](#) was formed, and in May 1999 the IEEE WPAN Study Group became IEEE 802.15, the WPAN Working Group. In July 1999, Bluetooth released the Bluetooth Specification v1.0a.

- Today, there are currently four IEEE 802.15 standards projects in development:
 - [802.15.1](#) - 1Mbit/sec WPAN/Bluetooth v1.x derivative work
 - [802.15.2](#) - Recommended Practice for Coexistence in Unlicensed Bands
 - [802.15.3](#) - 20+ Mb/s High Rate WPAN for Multimedia and Digital Imaging
 - [802.15.4](#) - 200 kb/s max for interactive toys, sensor and automation needs
- <http://ieee802.org/15/index.html>

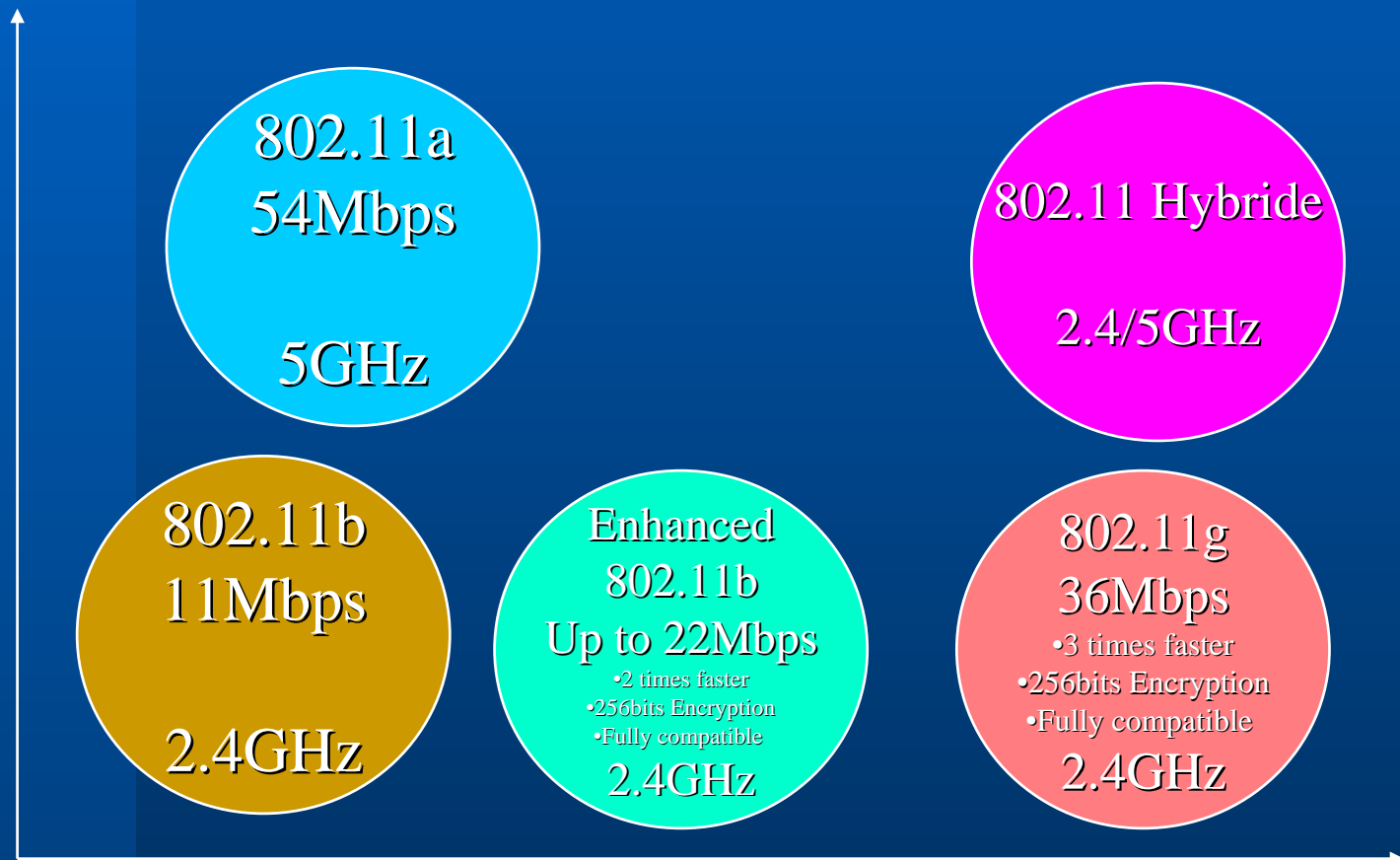
802.16 Working Group for Broadband Wireless Access Standards

- IEEE 802.16 specifications support the development of fixed broadband wireless access systems to enable rapid worldwide deployment of innovative, cost-effective and interoperable multi-vendor broadband wireless access products.
- <http://grouper.ieee.org/groups/802/16/index.html>

Future development

- **Roaming and Mobile IP**
- **Higher bandwidth**
- **Less interference**
- **WLAN vs. 3G**
- ...

Development Direction for 802.11





**Thank
You !**