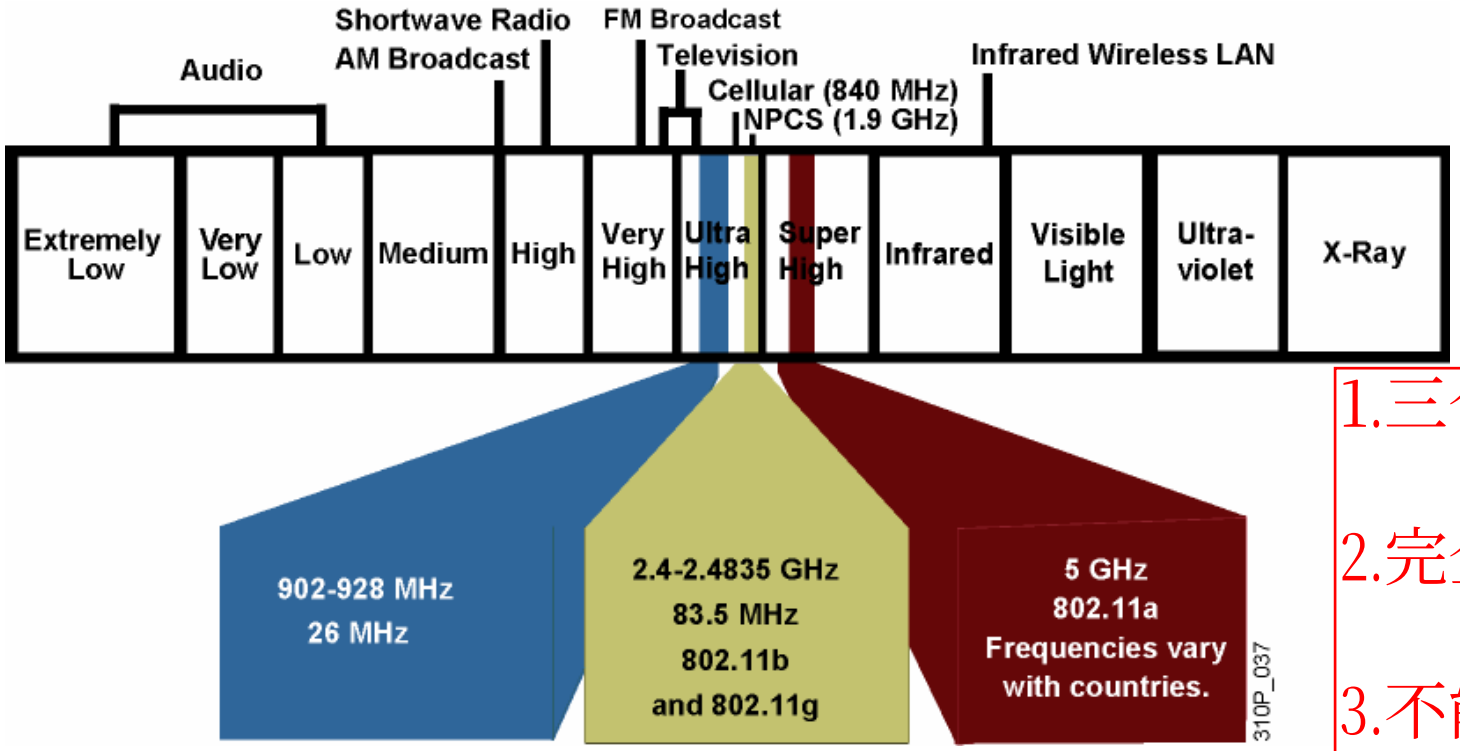
Wireless LANs

Explaining WLAN Technology and Standards

现任明教教主

数字签名者：现任明教教主
DN：cn=现任明教教主, o=北京WOLF安全实验室, ou=北京WOLF CCIE, email=collinsctk@gmail.com, c=CN-中国
日期 2008.05.20 18:52:01 +08'00'

Unlicensed Frequency Bands



1.三个ISM频段

2.完全不需要授权

3.不能够独占

4.相互干扰问题

- ISM: Industry, scientific, and medical frequency band
- No license required

- No exclusive use
- Best effort
- Interference possible

Radio Frequency Transmission

- **Radio frequencies are radiated into the air via an antenna, creating radio waves.**
- **Radio waves are absorbed when they are propagated through objects (e.g., walls).**
- **Radio waves are reflected by objects (e.g., metal surfaces).**
- **This absorption and reflection can cause areas of low signal strength or low signal quality.**

1.无线频率通过天线辐射到空气中，形成无线电播
2.无线电波会被吸收
3.无线电波会被反射
4.吸收和反射会造成低信号强度和低信号质量

Radio Frequency Transmission

- **Higher data rates have a shorter transmission range.**
  - **The receiver needs more signal strength and better SNR to retrieve information.**
- **Higher transmit power results in greater distance.**
- **Higher frequencies allow higher data rates.**
- **Higher frequencies have a shorter transmission range.**

1.高数据率的传输范围较短
接收者需要更强的信号强度和更好的信噪比才能够获取数据

2.更大的传输功率就能传输更远的距离（但是政府有限制）

3.更高的频率更高的数据率

4.更高的频率更短的传输距离

WLAN Regulation and Standardization

Regulatory agencies

- FCC (United States)
- ETSI (Europe)

标准化机构

Standardization

- IEEE 802.11
- http://standards.ieee.org/getieee802/

Certfication of equipment

- Wi-Fi Alliance certifies interoperability between products.
- Certifications include 802.11a, 802.11b, 802.11g, dual-band products, and security testing.
- Certified products can be found at http://www.wi-fi.org.

802.11b

© 2006 Cisco Systems, Inc. All rights reserved.

802.11b Standard

1.1999颁布的标准

2.使用2.4GHZ

3.使用直序展频技术

4.最大速率11Mbps

5.提供了厂商的互操作性

6.定义了基本的安全，加密，认证技术

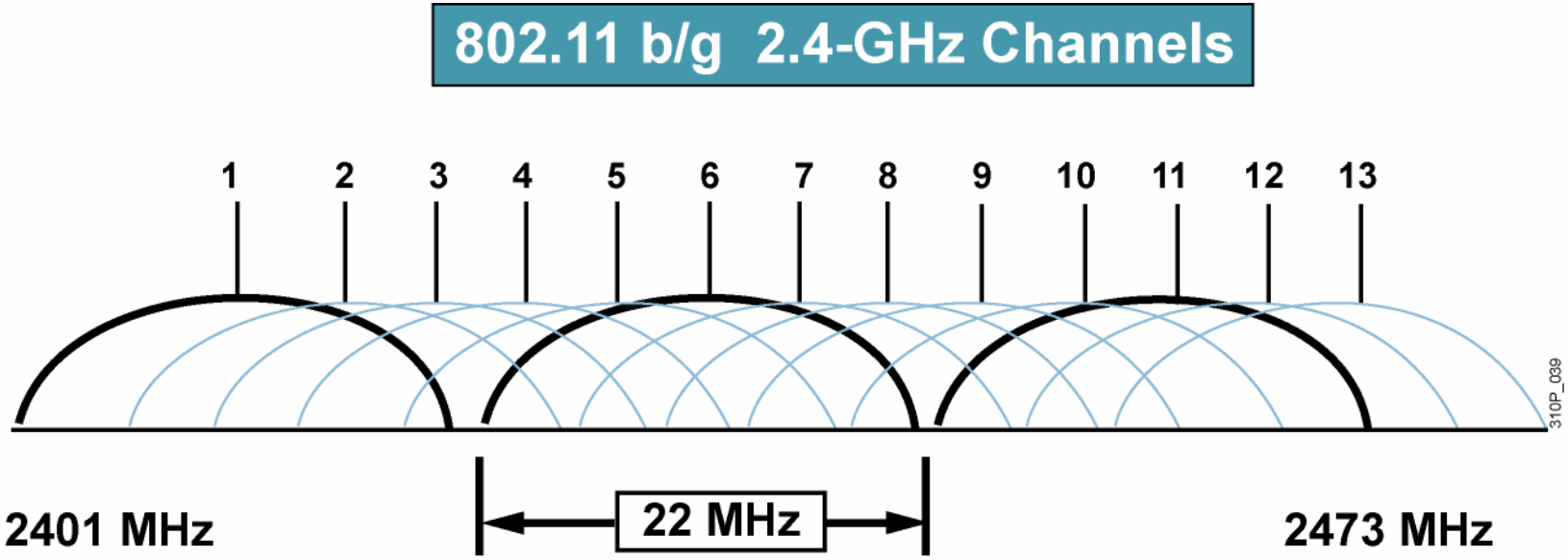
7.是实施得最为广泛的无线技术

- Standard was ratified in September 1999
- Operates in the 2.4-GHz band
- Specifies direct sequence spread spectrum (DSSS)
- Specifies four data rates up to 11 Mbps
  - 1, 2, 5.5, 11 Mbps
- Provides specifications for vendor interoperability (over the air)
- Defines basic security, encryption, and authentication for the wireless link
- Is the most commonly deployed WLAN standard

2.4-GHz Channels

Channel Identifier	Channel Center Frequency	Channel Frequency Range [MHz]	Regulatory Domain		
			Americas	Europe, Middle East, and Asia	Japan
1	2412 MHz	2401 – 2423	X	X	X
2	2417 MHz	2406 – 2428	X	X	X
3	2422 MHz	2411 – 2433	X	X	X
4	2427 MHz	2416 – 2438	X	X	X
5	2432 MHz	2421 – 2443	X	X	X
6	2437 MHz	2426 – 2448	X	X	X
7	2442 MHz	2431 – 2453	X	X	X
8	2447 MHz	2436 – 2458	X	X	X
9	2452 MHz	2441 – 2463	X	X	X
10	2457 MHz	2446 – 2468	X	X	X
11	2462 MHz	2451 – 2473	X	X	X
12	2467 MHz	2466 – 2478		X	X
13	2472 MHz	2471 – 2483		X	X
14	2484 MHz	2473 – 2495			X

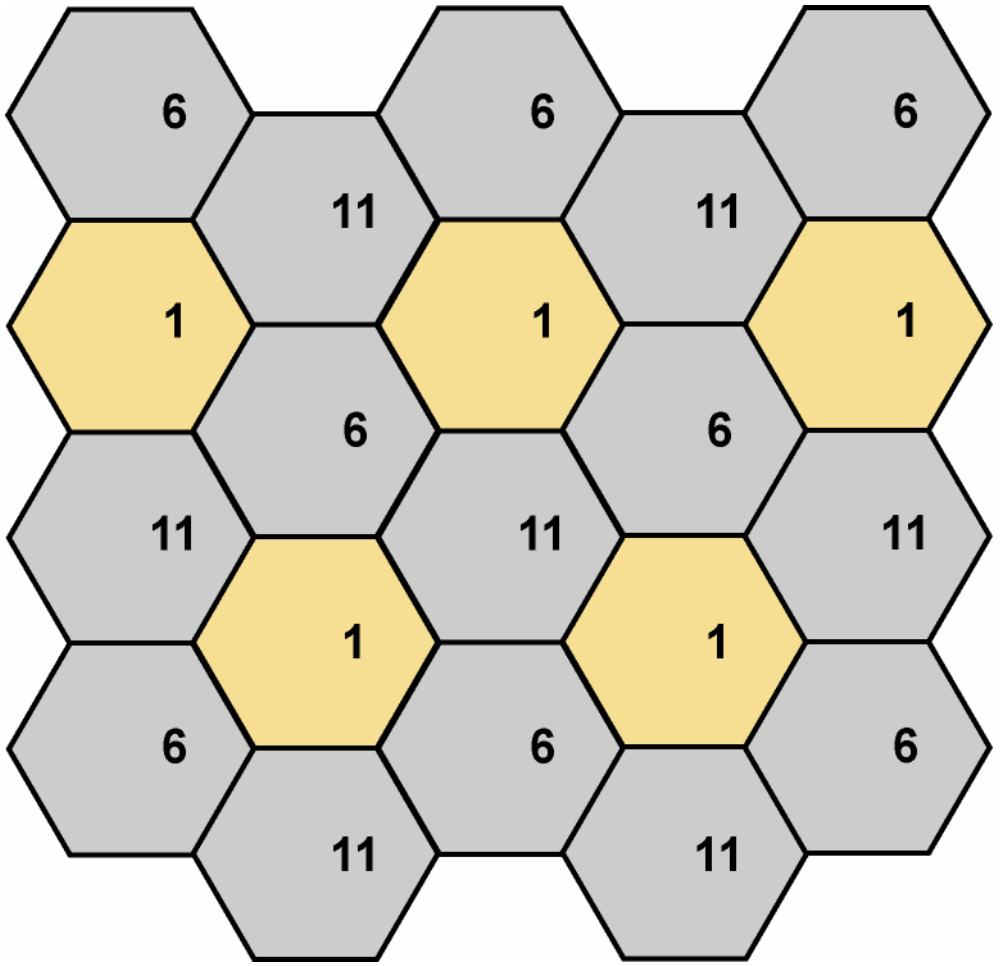
2.4-GHz Channel Use



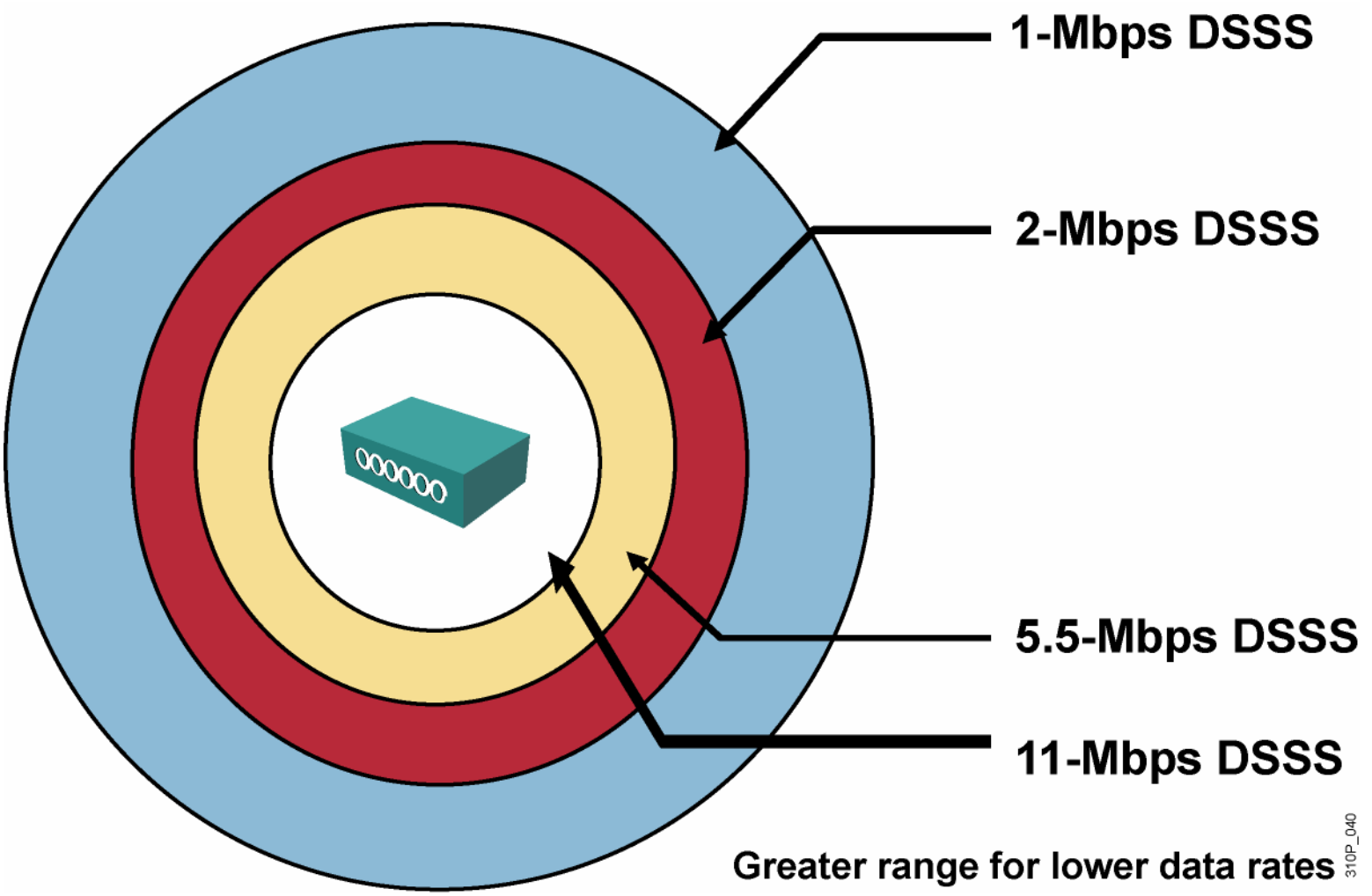
1.每一个信道22MHZ宽
2.北美使用11个信道
3.欧洲13个信道
4.只有三个不重叠信道1,6,11
5.使用其它信道会造成干扰
6.在一个区域只能使用3个AP

- Each channel is 22 MHz wide.
- North America: 11 channels.
- Europe: 13 channels.
- There are three nonoverlapping channels: 1, 6, 11.
- Using any other channels will cause interference.
- Three access points can occupy the same area.

802.11b/g (2.4 GHz) Channel Reuse



802.11b Access Point Coverage



802.11a

© 2006 Cisco Systems, Inc. All rights reserved.

802.11a Standard

1.1999年颁布的标准

2.操作在5GHz

3.使用正交频分多路复用技术（OFDM）

6.最大速率54Mbps

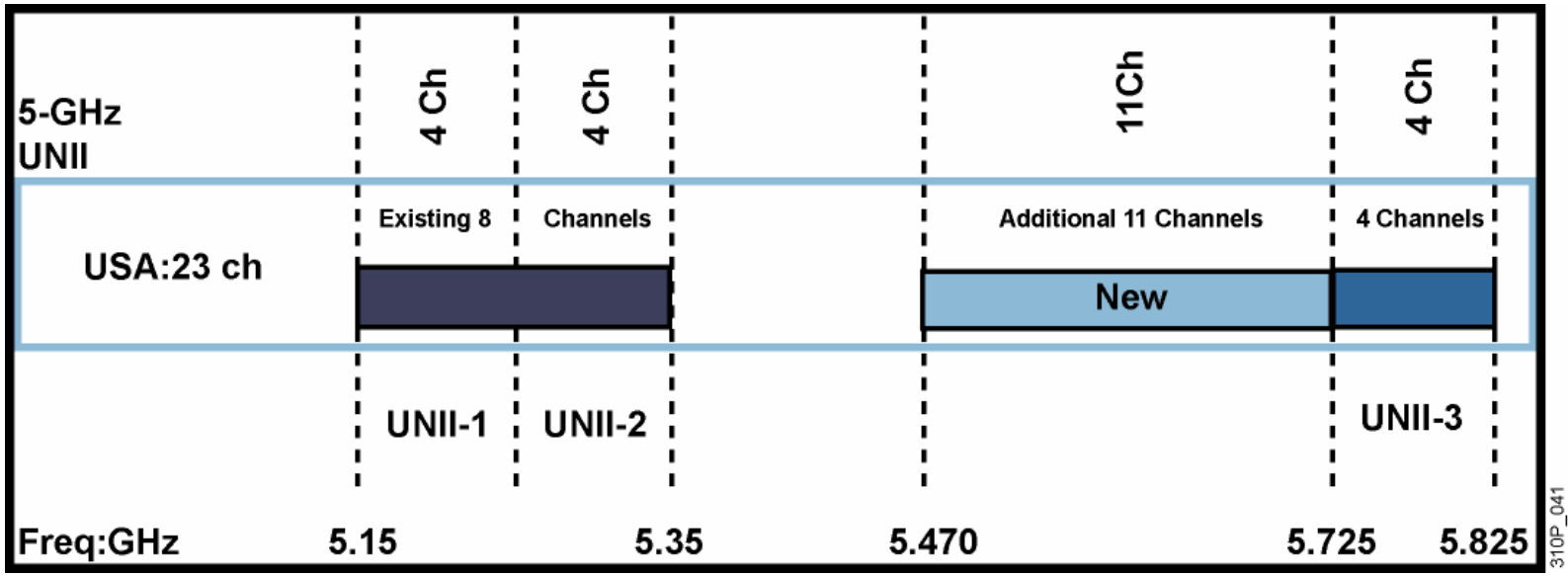
7.能够有12到23个不重叠信道（FCC）

8.能够有19个不重叠信道（ETSI）

9.不同的国家有不同的规范
所以TPC和DFS是需要的

- Standard was ratified September 1999
- Operates in the 5-GHz band
- Uses orthogonal frequency-division multiplexing (OFDM)
- Uses eight data rates of up to 54 Mbps
  - 6, 9, 12, 18, 24, 36, 48, 54 Mbps
- Has from 12 to 23 nonoverlapping channels (FCC)
- Has up to 19 nonoverlapping channels (ETSI)
- Regulations different across countries
  - Transmit (Tx) power control and dynamic frequency selection required (802.11h)

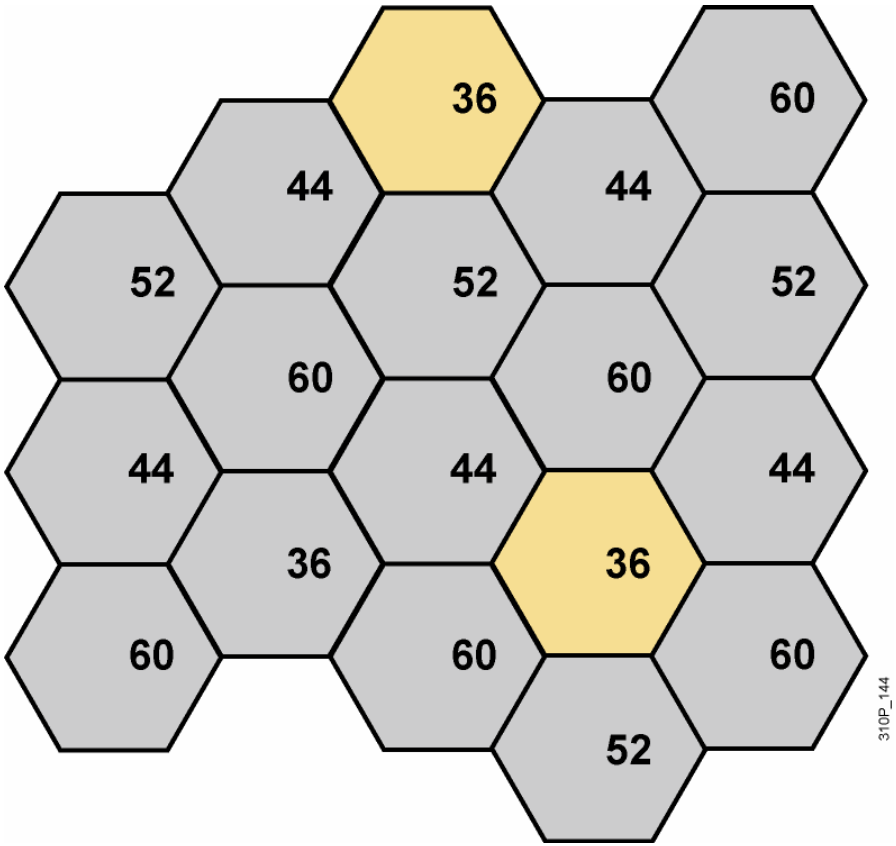
5-GHz Channels with 802.11h



- 802.11h implements TPC and DFS.
- With 802.11h in February 2004, the FCC added 11 channels.
  - 23 channels in the United States (FCC)
  - 19 channels in Europe (ETSI)
  - UNII-3 band currently not allowed in most of Europe

802.11a Channel Reuse

- 802.11h DFS not available
  - Manual channel assignment required
- 802.11h DFS implemented
  - Channel assignment done by Dynamic Frequency Selection (DFS)
  - Only frequency bands can be selected



802.11g

© 2006 Cisco Systems, Inc. All rights reserved.

802.11g Standard

1.2003年颁布的标准

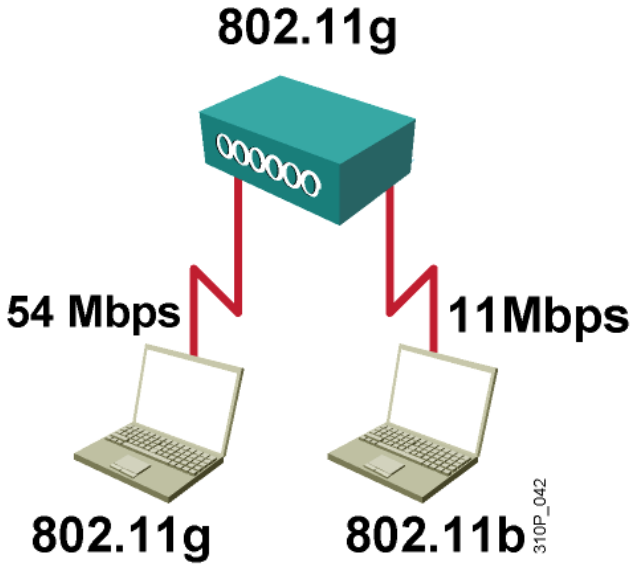
3.和802.1b一样都是使用2.4GHz频段
所以只有三个不重叠信道1 , 6 , 11

4.使用DSSS和OFDM传输

5.最大速率为54Mbps

6.完全兼容802.11b

- **Standard was ratified June 2003**
- **Operates in the 2.4-GHz band as 802.11b**
  - **Same three nonoverlapping channels: 1, 6, 11**
- **DSSS (CCK) and OFDM transmission**
- **12 data rates of up to 54 Mbps**
  - **1, 2, 5.5, 11 Mbps (DSSS / 802.11b)**
  - **6, 9, 12, 18, 24, 36, 48, 54 Mbps (OFDM)**
- **Full backward compatiblity to 802.11b standard**



802.11g Protection Mechanism 802.11g保护机制

1.802.11b的工作站不能分析802.11g的信号

2.802.11b/g的AP和802.11b的客户通讯最大速率为11Mbps

3.802.11b/g的AP和802.11g的客户通讯最大速率为54Mbps

4.802.11b/g AP使用RTS/CTS来避免和802.11b客户冲突

5.802.11b客户学习到CTS帧表示802.11g正在传输

6.这种保护机制降低了带宽

Problem: 802.11b stations cannot decode 802.11g radio signals.

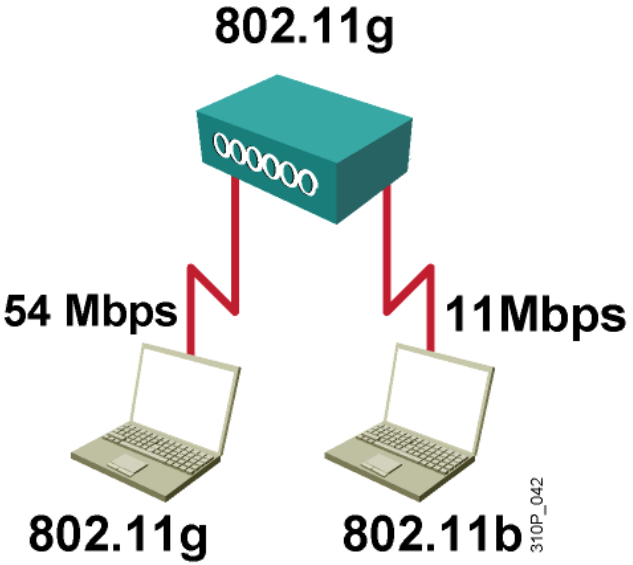
802.11b/g access point communicates with 802.11b clients with max. 11 Mbps.

802.11b/g access point communicates with 802.11g clients with max. 54 Mbps.

802.11b/g access point activates RTS/CTS to avoid collisions when 802.11b clients are present.

802.11b client learns from CTS frame the duration of the 802.11g transmission.

Reduced throughput is caused by additional overhead.



802.11 Standards Comparison

© 2006 Cisco Systems, Inc. All rights reserved.

802.11 RF Comparison

	802.11b – 2.4 GHz	802.11g – 2.4 GHz	802.11a – 5 GHz
Pro	• Most commonly deployed WLAN standard 运用的最广泛的无线标准	• Higher throughput • OFDM technology reduces multipath issues 1.高带宽 2.OFDM技术降低了多路干扰问题	• Highest throughput • OFDM technology reduces multipath issues • Provides up to 23 nonoverlapping channels
Con	• Interference and noise from other services in the 2.4-GHz band • Only 3 nonoverlapping channels • Distance limited by multipath issues	• Interference and noise from other services in the 2.4-GHz band • Only three nonoverlapping channels • Throughput degraded in the presence of 802.11b clients	• Lower market penetration 低的市场占有率

1.高带宽
2.OFDM技术降低了多路干扰问题

3.能够提供最多23个不重叠信道

1.会被其它工作在2.4GHz的服务干扰

2.只有三个不重叠信道

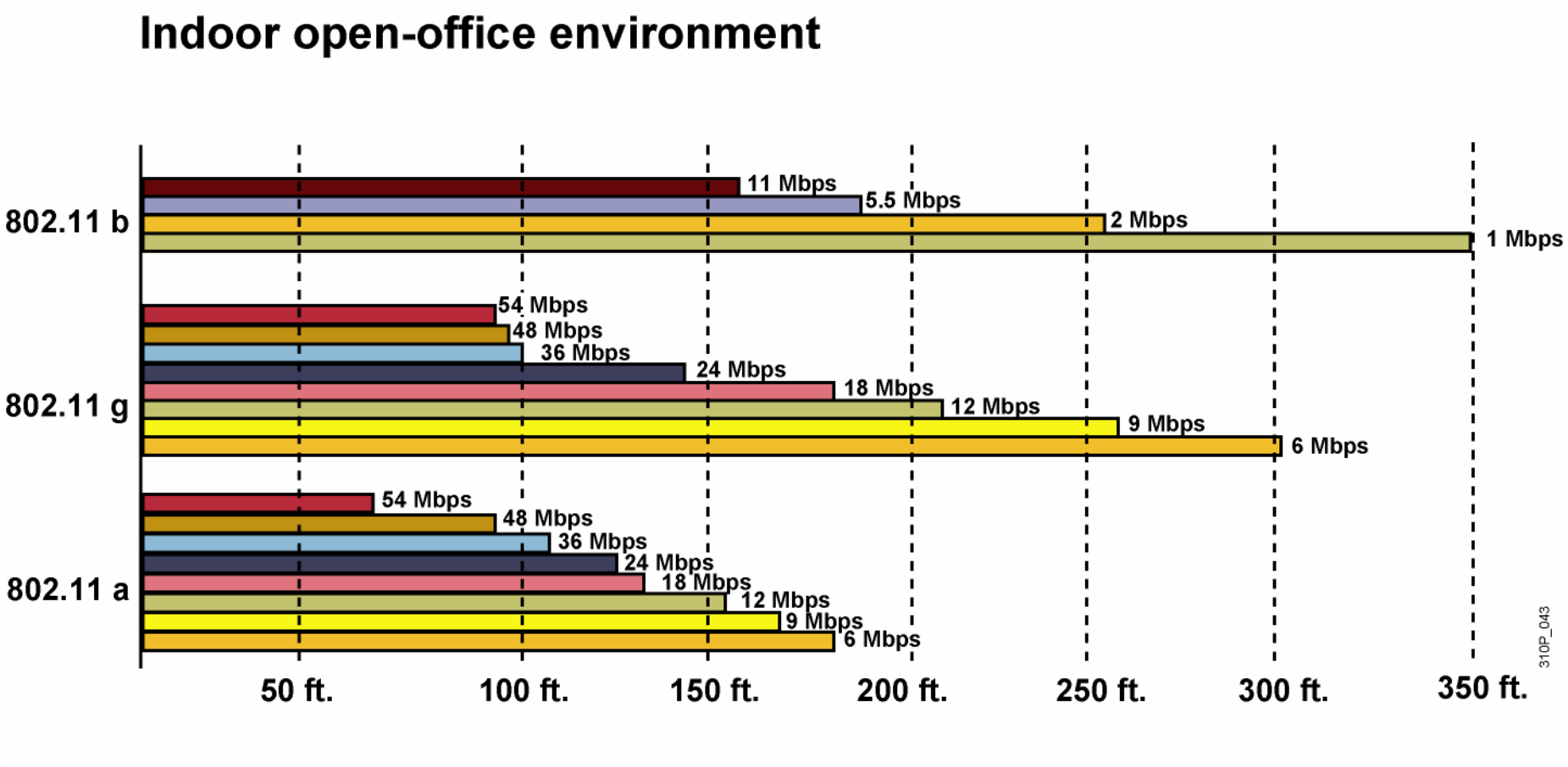
3.多路干扰影响传输距离

1.会被其它工作在2.4GHz的服务干扰
2.只有三个不重叠信道
3.和802.11b客户一起工作会降低带宽

802.11 Standards Comparison

	802.11b	802.11g		802.11a
Ratified	1999	2003		1999
Frequency band	2.4 GHz	2.4 GHz		5 GHz
No of channels	3	3		Up to 23
Transmission	DSSS	DSSS	OFDM	OFDM
Data rates [Mbps]	1, 2, 5.5, 11	1, 2, 5.5, 11	6, 9, 12, 18, 24, 36, 48, 54	6, 9, 12, 18, 24, 36, 48, 54
Throughput [Mbps]	Up to 6	Up to 22		Up to 28

Range Comparisons



Ratified IEEE 802.11 Standards

802.11: WLAN 1 and 2 Mbps at 2.4 GHz

802.11a: WLAN 54-Mbps at 5 GHz

802.11b: WLAN 11-Mbps at 2.4 GHz

802.11d: Multiple regulatory domains

802.11e: Quality of service

802.11f: Inter-Access Point Protocol (IAPP)

802.11g: WLAN 54-Mbps at 2.4 GHz

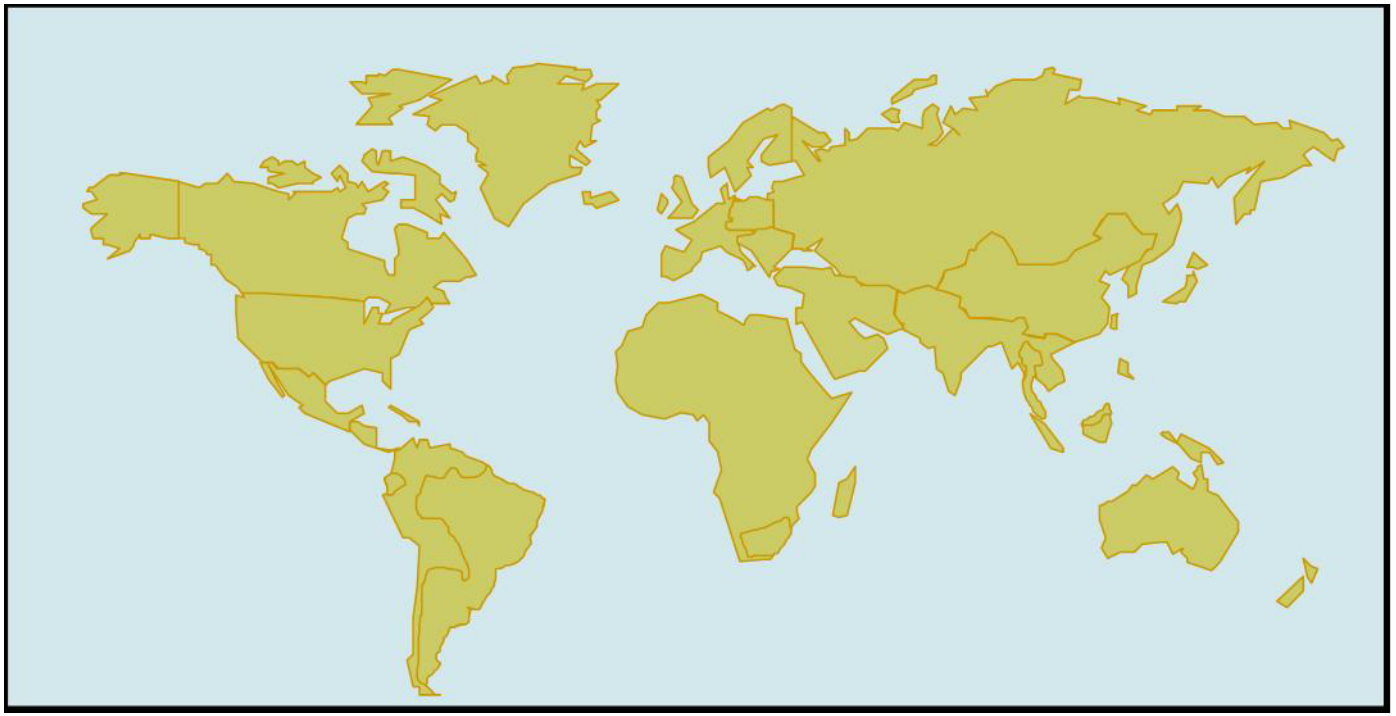
802.11h: Dynamic Frequency Selection (DFS)
Transmit Power Control (TPC) at 5 GHz

802.11i: Security

802.11j: 5-GHz channels for Japan

http://standards.ieee.org/getieee802/

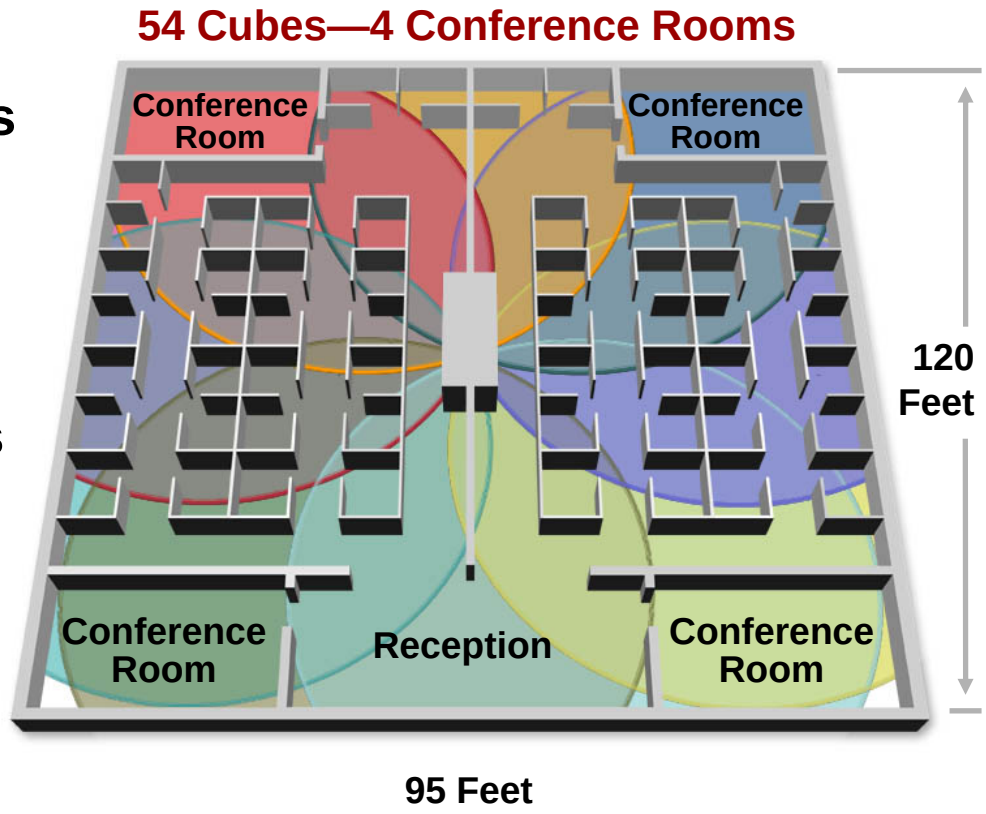
Worldwide Availability



http://www.cisco.com/go/aironet/compliance

General Office WLAN Design

- Eight 802.11g access points deployed
- 7 users per access point with no conference rooms provides 3.8 Mbps throughput per user
- 7 users + 1 conference room (10 users) = 17 total users, provides 1.5 Mbps throughput per user



WLAN as a Shared Medium: Best Practices

2.4-GHz 802.11b bandwidth calculations

- 25 users per cell; general office maximum users limited by bandwidth
- Peak true throughput 6.8 Mbps
  - 6.8 Mbps * 1024/25 = 278.5 kbps per user

2.4-GHz 802.11g bandwidth calculations

- 20 users per cell; general office maximum users limited by bandwidth
- Peak true throughput 32 Mbps
  - 32 Mbps * 1024/20 = 1683 kbps per user

5-GHz 802.11a bandwidth calculations

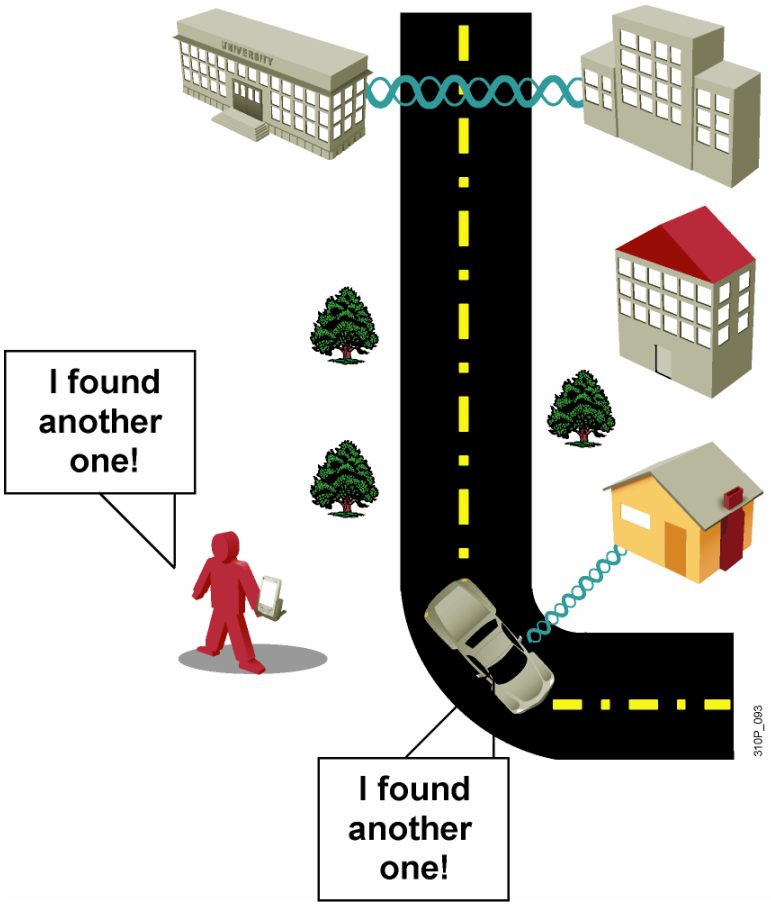
- 15 users per cell; general office users limited by coverage, not bandwidth
- Peak true throughput 32 Mbps
  - 32 Mbps * 1024/15 = 2188 kbps per user

WLAN Security

© 2006 Cisco Systems, Inc. All rights reserved.

Why WLAN Security?

- Wide availability and low cost of IEEE 802.11 wireless equipment
- 802.11 standard ease of use and deployment
- Availability of sniffers
- Statistics on WLAN security
- Media hype about hot spots, WLAN hacking, war driving
- Nonoptimal implementation of encryption in standard Wired Equivalent Privacy (WEP) encryption
- Authentication vulnerability



WLAN Security Threats 无线网络安全上的威胁

"WAR DRIVERS"	HACKERS	EMPLOYEES
Find "Open" Networks; Use Them to Gain Free Internet Access	Exploit Weak Privacy Measures to View Sensitive WLAN Info and Even Break into WLANs	Plug Consumer-Grade APs/Gateways into Company Ethernet Ports to Create Own WLANs
	 THE WALL STREET JOURNAL. Hackers Can Penetrate Wireless Network	

Mitigating the Threats

Control and Integrity	Privacy and Confidentiality	Protection and Availability
Authentication	Encryption	Intrusion Detection System (IDS)
Ensure that legitimate clients associate with trusted access points.	Protect data as it is transmitted and received.	Track and mitigate unauthorized access and network attacks.

Evolution of WLAN Security

Initial (1997)	Interim (2001)	Interim (2003)	Present
Encryption (WEP)	**802.1x EAP**	**Wi-Fi Protected Access (WPA)**	**Wireless IDS**
• No strong authentication • Static, breakable keys • Not scalable	• Dynamic keys • Improved encryption • User authentication • 802.1x EAP (LEAP, PEAP) • RADIUS	• Standardized • Improved encryption • Strong, user authentication (e.g., LEAP, PEAP, EAP-FAST)	• Identification and protection against attacks, DoS **IEEE 802.11i** **WPA2 (2004)** • AES strong encryption • Authentication • Dynamic key management

不应该在被使用了

1.static WEP (没有认证机制)
2.802.1x + dynamic WEP keys (Radius用户认证)
3.WPA pre-share (预共享密钥认证，TKIP加密)
4.802.1x + WPA (Radius用户认证+TKIP加密)
5.WPA2 pre-share(预共享密钥认证，AES加密)
6.802.1x + WPA2 (Radius用户认证+AES加密)

提供了WEP的动态KEY，
提供了Radius的用户认证

使用TKIP，兼容老的WEP设备，基本的安全底线

Wireless Client Association

1.AP通过beacons宣告自己的SSID，速率，和其它信息

2.客户扫描所有的信道

3.客户监听beacons并且响应AP

4.客户通过最强的信号来关联AP

5.客户将反复扫描，如果信号变低，它将重新关联到其它AP

6.一旦关联到SSID，MAC地址，安全设置都被客户传送到AP接受AP的检查

Access points send out beacons announcing SSID, data rates, and other information.

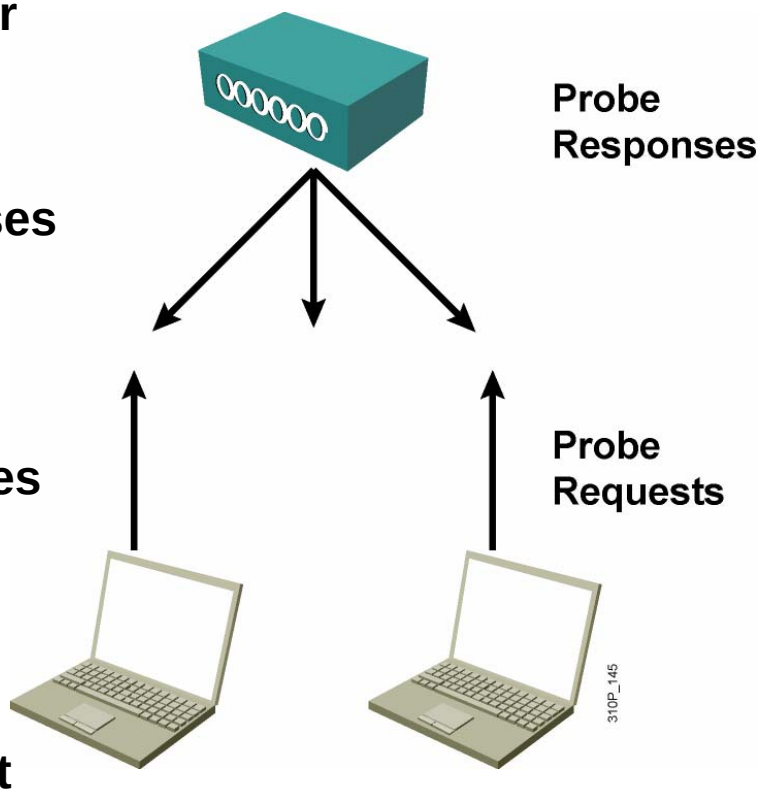
Client scans all channels.

Client listens for beacons and responses from access points.

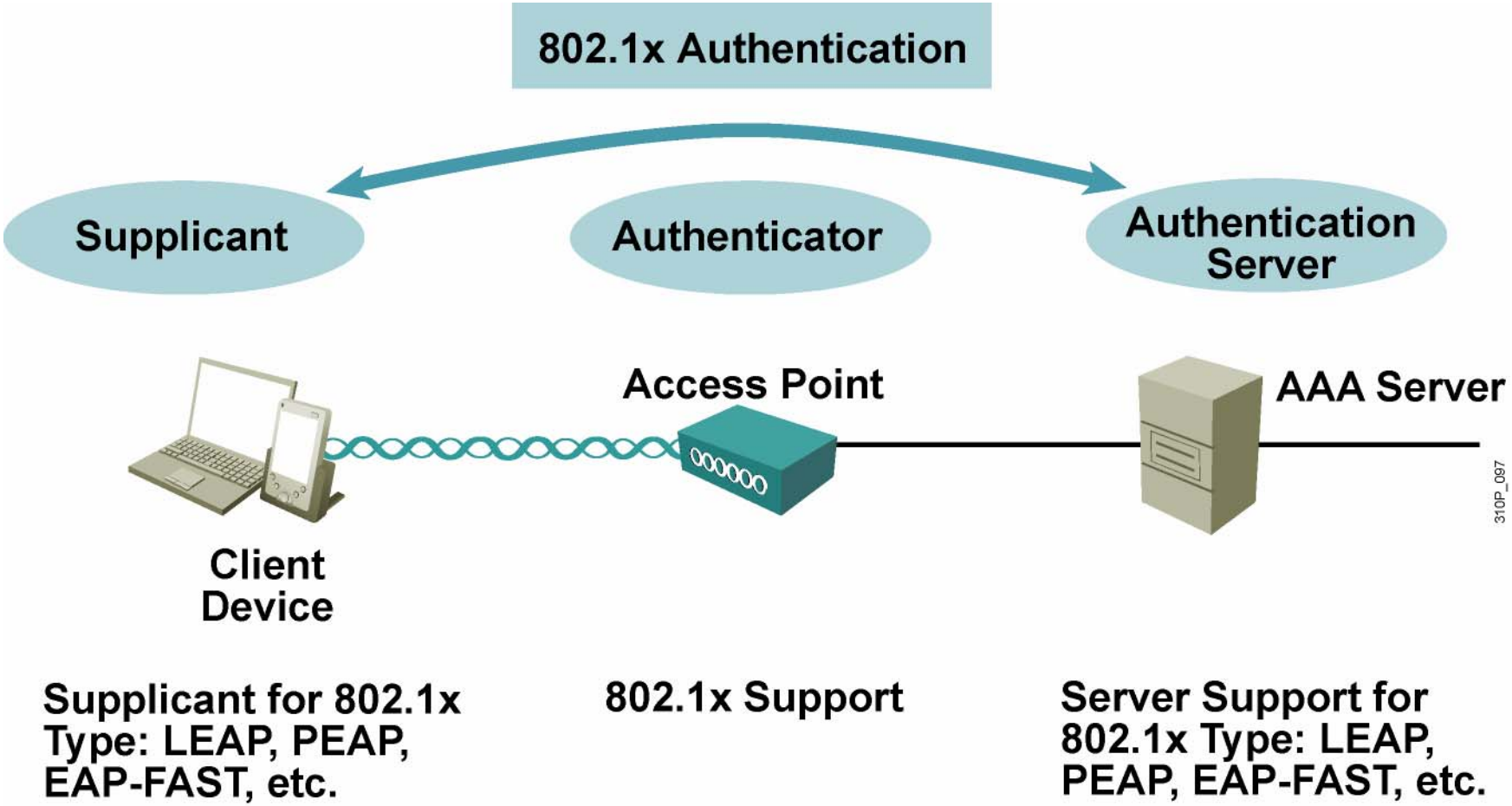
Client associates to access point with strongest signal.

Client will repeat scan if signal becomes low to reassociate to another access point (roaming).

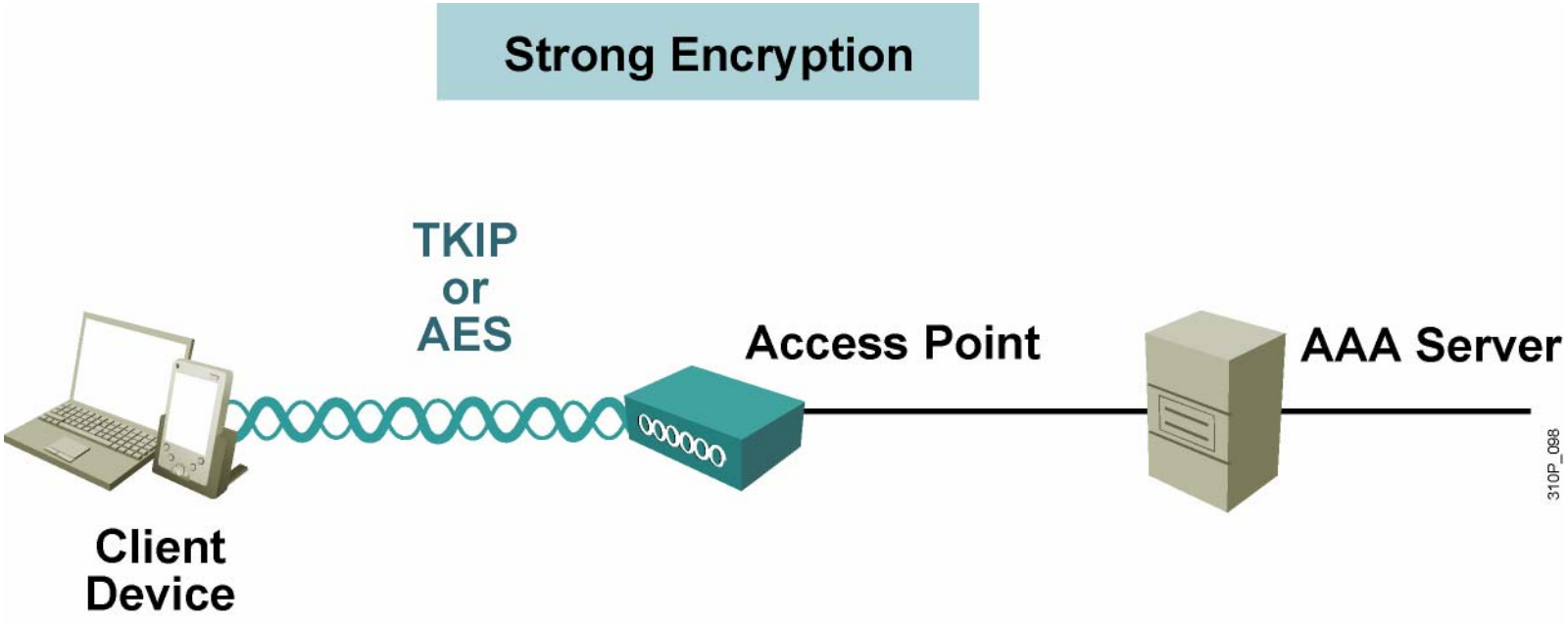
During association SSID, MAC address and security settings are sent from the client to the access point and checked by the access point.



WPA and WPA2 Authentication



WPA and WPA2 Encryption



WLAN Security Summary

Open Access

No Encryption,
Basic Authentication

Public "Hotspots"

Basic Security

WPA Passphrase
WEP Encryption

Home Use

Enhanced Security

802.1x EAP
Mutual Authentication
TKIP Encryption
WPA / WPA2
802.11i Security

Enterprise

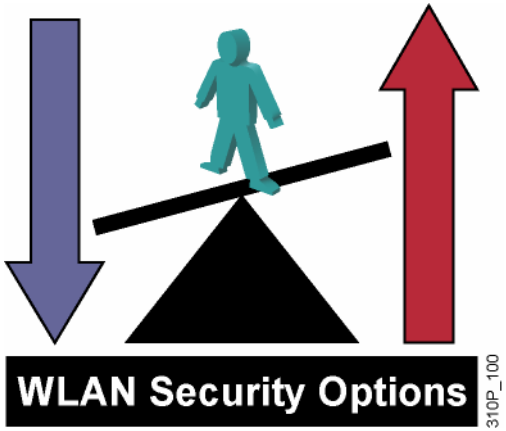
Remote Access

Virtual Private Network (VPN)

Business Traveler, Telecommuter

Security Evaluation

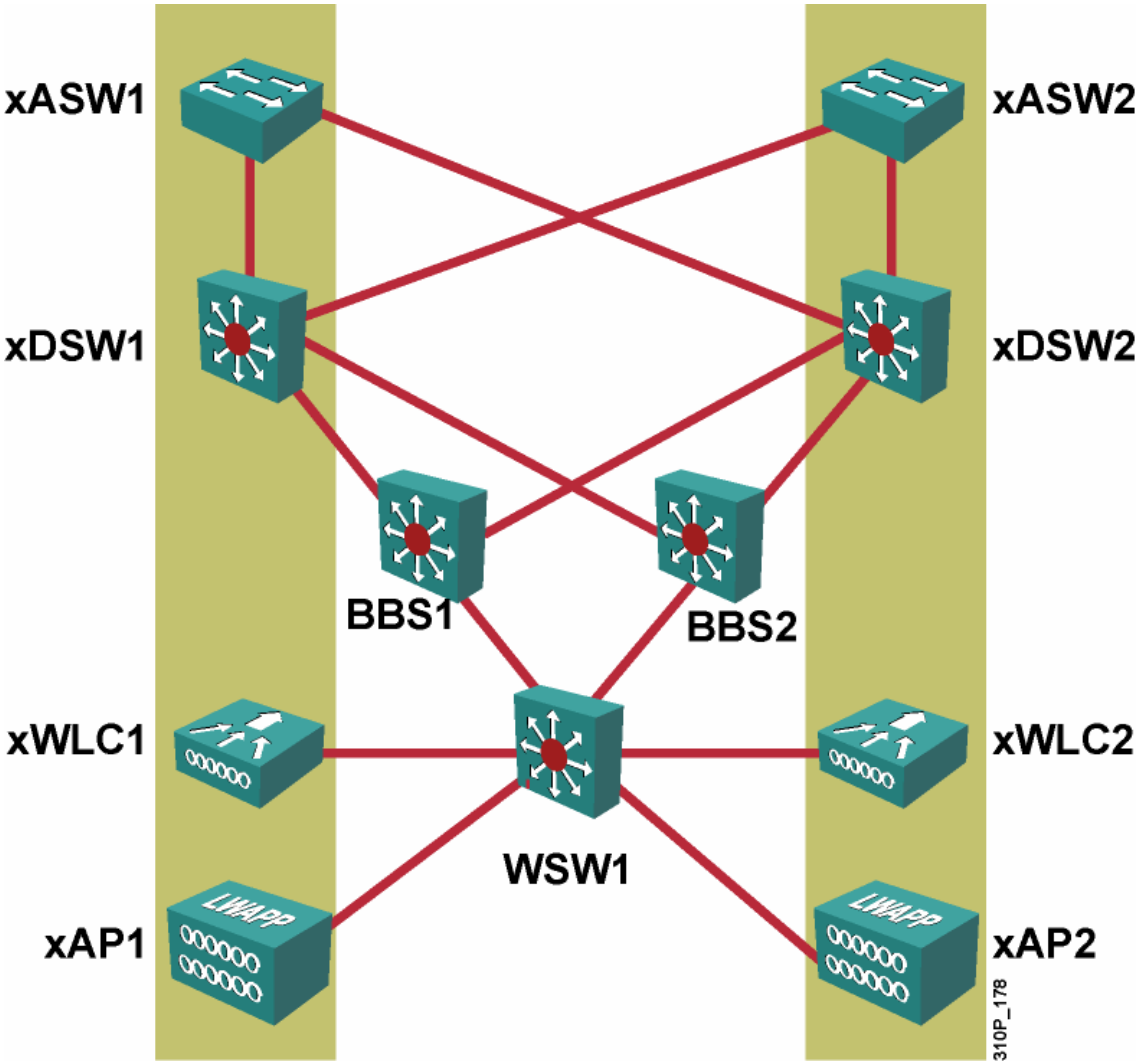
- Evaluate effectiveness of encrypted WLAN statistics.
- Focus on proper planning and implementation.
- Estimate potential security threats and the level of security needed.
- Evaluate amount of WLAN traffic being sent when selecting security methods.
- Evaluate tools and options applicable to WLAN design.



Summary

- The 2.4-GHz and 5-GHz frequency bands are used by WLAN 802.11 standards.
- The throughput per user depends on the data rate and the number of users per wireless cell.
- 802.11b has data rates of up to 11 Mbps at 2.4 GHz.
- 802.11a has data rates of up to 54 Mbps at 5 GHz.
- 802.11g has data rates of up to 54 Mbps at 2.4 GHz.
- 802.11a has a shorter range than 802.11g.
- For maximum efficiency, limit the number of users per cell.
- Different WLAN security types with authentication and encryption satisfy the security requirements of enterprise and home users.

WLAN Lab




CISCO SYSTEMS