

**CCNA**

640-802

**Cisco’s Wireless Technologies:**







Revision no.: PPT/2K804/04



# Introduction to Wireless Technology



* Wireless LANs (WLANs) use radio frequencies (RFs) that are radiated into the air from an antenna that creates radio waves.
* These waves can be absorbed, refracted, or reflected by walls, water, and metal surfaces, resulting in low signal strength.







Revision no.: PPT/2K804/04

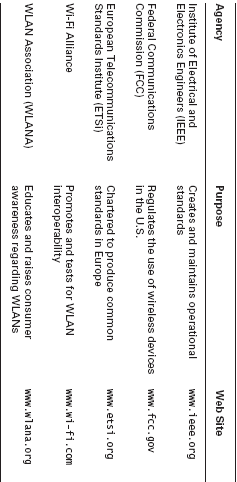


TABLE Wireless Agencies and Standards



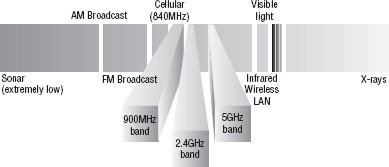
* The FCC has released three unlicensed bands for public use: 900MHz, 2.4GHz, and 5.7GHz.
* The 900MHz and 2.4GHz bands are referred to as the Industrial, Scientific, and Medical (ISM) bands, and the 5-GHz band is known as the Unlicensed National Information Infrastructure (UNII) band.





FIGURE Unlicensed frequencies



If you opt to deploy wireless in a range outside of the three public bands, you need to get a specific license from the FCC.





# The 802.11 Standards



* Taking off from what you learned in Chapter 1, “Internetworking,” wireless networking has its own 802 standards group—remember, Ethernet’s committee is 802.3. Wireless starts with 802.11, and there are various other up-and-coming standard groups as well, like 802.16 and 802.20.
* And there’s no doubt that cellular networks will become huge players in our wireless future. But for now, we’re going to concentrate on the 802.11 standards committee and subcommittees.





* IEEE 802.11 was the first, original standardized WLAN at 1 and 2Mbps. It runs in the 2.4GHz radio frequency and was ratified in 1997 even though we didn’t see many products pop up until around 1999 when 802.11b was introduced.
* All the committees listed in Table are amendments to the original

802.11 standard except for 802.11F and 802.11T, which are both stand-alone documents.







Revision no.: PPT/2K804/04

**TABLE 802.11 Committees and Subcommittees**





### 2.4GHz (802.11b)

* It operates in the 2.4GHz unlicensed radio band that delivers a maximum data rate of 11Mbps.
* The 802.11b standard has been widely adopted by both vendors and customers.
* 802.11b uses a modulation technique called Direct Sequence Spread Spectrum (DSSS).





### 2.4GHz (802.11g)

* The 802.11g standard was ratified in June 2003 and is backward compatible with 802.11b.
* The 802.11g standard delivers the same 54Mbps maximum data rate as 802.11a but runs in the 2.4GHz range—the same as 802.11b.
* 802.11g and 802.11a use Orthogonal Frequency Division Multiplexing (OFDM) modulation.





### 5GHz (802.11a)

* The 802.11a standard delivers a maximum data rate of 54Mbps with 12 non-overlapping frequency channels.
* The 802.11a products allow the person operating at 54Mbps to shift to 48Mbps, 36Mbps, 24Mbps, 18Mbps, 12Mbps, 9Mbps, and finally still communicate farthest from the AP at 6Mbps.

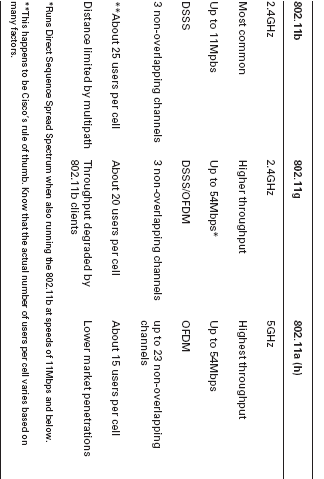






Revision no.: PPT/2K804/04

**Comparing 802.11**



Revision no.: PPT/2K804/04



# Wireless Security

### Open Access



* + All Wi-Fi Certified wireless LAN products are shipped in “open-access” mode, with their security features turned off.
  + Security needs to be enabled on wireless devices during their installation in enterprise environments.



Revision no.: PPT/2K804/04



# SSIDs, WEP, and

**MAC Address Authentication**



* + Basic security was include the use of Service Set Identifiers (SSIDs), open or shared-key authentication, static Wired Equivalency Protocol (WEP), and optional Media Access Control (MAC) authentication.
  + SSID is a common network name for the devices in a WLAN system that create the wireless LAN.
  + An SSID prevents access by any client device that doesn’t have the SSID. The thing is, by default, an access point broadcasts its SSID in its beacon many times a second.
  + And even if SSID broadcasting is turned off, a bad guy can discover the SSID by monitoring the network and just waiting for a client response to the access point



Revision no.: PPT/2K804/04

## Two types of authentication were specified by the IEEE 802.11 committee:



### Open authentication:

* + Involves little more than supplying the correct SSID.

### Shared-key authentication:

* + The access point sends the client device a challenge-text packet that the client must then encrypt with the correct Wired Equivalency Protocol (WEP) key and return to the access point. Without the correct key, authentication will fail and the client won’t be allowed to associate with the access point.
  + Client MAC addresses can be statically typed into each access point, and any of them that show up without that MAC addresses in the filter table would be denied access.



Revision no.: PPT/2K804/04



# WPA or WPA 2 Pre-Shared Key

* + WPA or WPA2 Pre-Shared Key (PSK) is a better form of wireless security than any other basic wireless security method.



* + The PSK verifies users via a password or identifying code (also called a passphrase) on both the client machine and the access point.
  + A client only gains access to the network if its password matches the access point’s password.
  + The PSK also provides keying material that TKIP or AES uses to generate an encryption key for each packet of transmitted data



Revision no.: PPT/2K804/04

permission.

prior the

without

emailed or

stored d,

reproduce be

may

material

this of

part No

reserved.

rights All

.

**2004**

**INSTITUTE, CMS**

**©**



**Design & Published by:**