Wi-fi wireless technology

Business data network and telecommunications

Wi-fi has entered in to our lives some years now. It solves some problems that wire networks have but generate new. At the moment there are few advantages and a lot of disadvantages. Wi-fi can be very useful in many cases and I think it deserves a deep look in to it. Also wi-fi has many prospects for further development. Wi-fi needs specified devices in order to work properly.

History

The term wi-fi (wireless fidelity) is used in order to determine the appliances that are based on specification IEEE 802. 11 and faction of ISM band, that is frequencies 2. 4Ghz for Europe . Wi-Fi uses single carrier DSSS (direct sequence spread spectrum) radio technology but also multi-carrier OFDM (Orthogonal Frequency Division Multiplexing) radio technology. These regulations that enabled the development of Wi-Fi, are HomeRF, and Bluetooth.

Unlicensed spread spectrum was available for first time by the Federal Communications Commission in 1985 and the FCC regulations were copied later with some changes in other countries and made the use of this technology enable in all major countries. Michael Marcus of the FCC staff proposed the FCC action in 1980 and the subsequent regulatory action in 5 more years. It was part of a proposal to allow civil use of spread spectrum technology and was opposed by the mainstream equipment manufacturers and many radio system operators. (Federal Communications Commission. 1985).

The Wi-Fi was invented in 1991 by NCR Corporation/AT&T. Initially the use was for cashier systems. The first wireless products that were brought on the market was under the name “ WaveLAN” with speeds of 1 Mbit/s up to 2 Mbit/s. Vic Hayes, was involved in designing standards such as IEEE 802. 11b, and 802. 11a. He has been named as “ the father of Wi-fi”. (Vic Hayes at 1 st Home Networking Conference, 2007).

Uses

A device with Wi-Fi enabled, such as a PC, PDA, cell phone, game console, or MP3 player can connect to the Internet within the range of a wireless network connected to the Internet (Access point). The interconnection between one or more access points in a certain area is called a hotspot. Hotspots can cover a single room up to many squares covered by overlapping access points. The devices can network each other and connect to the Internet, share files and digital cameras can transfer video wirelessly.

Wi-Fi also allows devices to connect directly with each other (peer-to-peer mode). This connectivity mode is useful most in gaming applications.

When the technology released in the market there were many problems because consumers were not sure if the products from companies would work together. The Wi-Fi Alliance began as a community to solve this and to address the needs of the end user and allow the technology to mature. The Alliance created the branding *Wi-Fi CERTIFIED* to show to the consumers that products are interoperable with other products displaying the same branding. (Wi-fi alliance, 2000).

Routers and Wi-Fi access points are used most in homes to provide Internet access and networking to all devices that are connected wirelessly or by cables into them. Devices can also be connected in ad-hoc mode for client-to-client connections without using a router.

In Business and industrial environments, as increasing the number of Wi-Fi access points we get faster roaming and increased network capacity by creating smaller cells or by using more channels. Wi-Fi can enable wireless voice applications such as WVOIP. Wi-Fi installations can provide a secure computer network, firewall, DHCP server and other functions.

In addition to home and office use, Wi-Fi is publicly available also at Wi-Fi hotspots provided either free of charge or under a certain price. Sometimes free Wi-Fi is provided by organizations or authorities who wish to promote business in their area. Metropolitan-wide WiFi (Mu-Fi) already has more than 300 projects in process. (Muniwireless, 2007).

Standard devices

Wireless access points can connect wireless devices to a wired LAN. An access point is something like an Ethernet hub, relaying data between the connected devices. Wireless adapters are connecting in the devices, externally or internally such as usb, pci and allow devices to connect to the wireless network. Wireless routers integrate a firmware application that provides IP Routing, NAT, and DNS forwarding through an interface.

Wireless range extenders (repeaters) can extend the range of the wireless network. Ig the repeaters are placed in the area smart then the signal can be

excellent. The devices that are connected through repeaters may have an increased latency for each hop. Each device will get signal from the device that gives better signal.

With wireless bridges we can connect two or more networks between them. This is different from an access point because an access point works at the data-link layer. We can use two wireless bridges when a wired connection may be unavailable, such as a connection between two separate buildings.

Most devices (routers, access points, bridges, repeaters) are designed for home or business environments. Pci cards use antenna connectors and usb only have internal antennas while some have external connections in addition to an internal antenna. In laptops it is commonly used mini pci cards. In a network between two buildings that the distance is a matter it is usually used big antennas in the roof of the buildings, so the signal can be remain strong enough.

Advantages of Wi-Fi

Wi-Fi allows LANs to be deployed while it reduces the cost of the network deployment. WLANS can be hosted in areas that cannot be run by cables, such as outdoor areas or even historical buildings.

The prices for wireless products continue to drop, making it a fair networking option. Wi-Fi has become widespread and more and more devices obtain wi-fi technology.

Wi-Fi is a global set of standards. Products designated as “ Wi-Fi Certified” by the Wi-Fi Alliance are backwards inter-operable. Except mobile phones, any device with wi-fi standard will work anywhere in the world.

Wi-Fi use WPA encryption and it is not easily cracked if the passwords are strong enough. Nowadays it is used WPA2 also, an encryption that has no known weaknesses. A new protocol for Qos is WMM and makes Wi-Fi better for voice, video applications, and power saving methods. To make enable the WMM feature all devices in the network must support it.

Disadvantages of Wi-Fi

Wifi in Europe use for the 2. 4 GHz band (1-13) channels, in US (1-11) and Japan (1-14). A Wi-fi signal occupies around five channels in the 2. 4 GHz resulting in only 3 non-overlapped channels in the US: 1, 6, 11, and four in Europe: 1, 5, 9, 13

Power consumption is too high compared to with other low bandwidth standards, such as Bluetooth, making a concern about device’s batteries life of the.

WEP (Wired Equivalent Privacy) is the most usual wireless encryption standard that is used, but shown that can be easily breakable. Wi-Fi Protected Access (WPA, WPA2), solved this problem and its available on most products. Most Wi-Fi Access Points have default the security disabled thought, providing open wireless access to their LAN. You can always turn on the security by configuring the device, usually via the graphical user interface (GUI) of the router/access point. Unencrypted networks can be used

to read and copy data that are transmitted over the network, unless we have a security method to secure the data, such as VPN

The wireless networks have limited range. A typical Wi-Fi home router using 802. 11g with a stock antenna might have a range of 35 m indoors and 95 m outdoors. Range also varies with frequency band. Wi-Fi in the 2. 4 GHz frequency block has slightly better range than Wi-Fi in the 5 GHz frequency block. Outdoor range with improved (directional) antennas can be several kilometres or more with line-of-sight. IEEE 802. 11g-(2003)

When the range increases the performance of a wireless network is decreased. Ethernet or other cables are more reliable then wi-fi. An Ethernet connection can reach speed up to 1Gbit/s and in the other hand 802. 11g networks have a maximum of 54 Mbit/s. Protocol 802. 11n try to improve the speeds, but still does not achieve Ethernet’s reliability. People with adsl2+ can understand an increase in performance using wired connection rather than WiFi.

Wi-Fi in many cases has problems with the signal-to-noise ratio (SNR). SNR compares the level of the desired signal to the background noise. This can be a huge problem in high-density areas. All the devices must support the same protocol for example 802. 11g. And in case there are other access points in the network, the name (SSID) must maintain the same. In Wireless networks there are many times incompatibility problems between brands. Different standards may disrupt connections or low speeds. The new protocol 802. 11n use 5 GHz band and have more channels available.

Each node (access point, repeater) on the network is able to see the communication between other devices, allowing network traffic to be easily captured. When a WiFi network is not encrypted it is vulnerable to attacks.

Wi-fi is a new technology and still under development. Many people may adopt it cause it produce a non wire environment and others not. I think wi-fi will give better quality in the future and maybe it will get pass some main problem that it have at the moment.

References

Authorization of Spread Spectrum Systems Under Parts 15 and 90 of the FCC Rules and Regulations (TXT). Federal Communications Commission (June 18, 1985). Retrieved on 2007-12-01.

Wi-Fi Alliance – Certified Products. (2000) certifications. wi-fi. org. Retrieved on 2007-11-01. from http://certifications. wi-fi. org/wbcs_certified_products. php

V. Hayes at (November 04 2007). 1 st Home Networking Conference Retrived on 2007-12-03 from http://lirne. net/2007/11/vic-hayes-at-1st-home-networking-conference/

Muniwireless (2007). Muniwireless-technology Retrieved on 2007-12-01 from http://www. muniwireless. com/

IEEE 802. 11g-(2003) 802. 11g Retrieved on 2007-12-03 from http://en. wikipedia. org/wiki/IEEE_802. 11g-2003