Wi-Fi EVOLUTION

The Institute of Electrical and Electronics Engineers (IEEE) ratified the initial version of the standard for Wireless Local Area Networks known as IEEE 802.11 in 1997 (IEEE Standards, 2004). Belonging to the same family of standards as the Ethernet, it was labeled “Wireless Ethernet” and considered an appropriate networking technology for offices because it did not rely on cables. Although burdened by a lack of strong security (Fluhrer, 2001) and lower throughput compared to its wired equivalent, IEEE 802.11 was a success. The cost of manufacturing 802.11 chipsets fell quickly, and 802.11 found its way from desktop PCs to laptops and next generation cellular phones. Wi-Fi, a consumer-friendly moniker for 802.11, was adopted and the Wireless Ethernet Compatibility Alliance (WECA), a non-profit international association, was formed in 1999 to certify the interoperability of Wi-Fi products. WECA changed its name to the Wi-Fi Alliance in 2002 (Wi-Fi Alliance, 2004).

The two main components of Wi-Fi networks are the wireless clients and the Wi-Fi access points, which are the wireless equivalent of Ethernet hubs. Clients equipped with Wi-Fi can communicate wirelessly with nearby access points that link them to each other, to the local wired network and to the Internet. Clients can also communicate with each other without access points (assuming their radios are within range) in a so called “ad hoc” mode (IEEE Std. 802.11, 1999).

Newer IEEE specifications include 802.11g, which enables clients and access points to connect to each other at speeds of up to 54 Mbps; and 802.11i, which employs advanced authentication and encryption algorithms to protect against unauthorized users that attempt to gain access to private networks (IEEE Standards, 2004). Standard 802.11i also protects the confidentiality and integrity of wireless sessions, which are usually susceptible to eavesdropping and hijacking attacks.

The term “Wi-Fi hotspot” is now being used to describe any area where Wi-Fi connectivity is available via nearby access point. Public hotspots can be found in airport lounges and shopping malls, in coffee shops and restaurants, and in hotels and exhibition centers. Wi-Fi users, which include business travelers as well as casual users, can use their portable devices in these hotspots to access e-mail, their corporate intranets and the Internet. Users can browse the Web, use instant messaging and location-based services, place cheaper voice-over-IP calls and conduct videoconferences. Nevertheless, such practice is still not commonplace (Stone, 2003).

Wi-Fi PROVISIONING: ISSUES AND PLAYERS

Ubiquitous high-speed and cost-effective Internet access is not available today. However, in major cities, Wi-Fi technology combined with the widespread availability of broadband Internet links such as DSL and cable can help realize this goal. The low cost of Wi-Fi equipment compared to their cellular—2G and 3G—equivalents greatly assists in deploying Wi-Fi globally. There are factors, however, that work against such a deployment.

One such factor is the range of Wi-Fi hotspots, which is smaller than its cellular equivalent. To cover a given area, a greater number of access points are necessary compared to, for example, the number of CDMA or GSM base stations. The fact that Wi-Fi access points are inexpensive and that Wi-Fi operates in unlicensed frequency bands offsets this cost. Nevertheless, as with cellular base stations, there are still OA&M costs involved.

To share the costs mentioned above, providers establish roaming partnerships so that customers from one provider can use the infrastructure of other providers. For roaming to work in the cellular world, Mobile Network Operators sign roaming agreements with each other and standardize on the technology to use (GSM technology is well known for its success throughout Europe). However, even though the technology has already been decided with Wi-Fi networks, other types of provider “incompatibilities” leave Wi-Fi resources under-exploited. A factor working against the establishment of a global Wi-
Related Content

Temporary Virtual Teams: An Empirical Examination of Team Development

Framework for Stress Detection Using Thermal Signature

Offending, Victimization, Forensic Investigation, and Prevention of Cyberstalking

Evaluating Organisational Readiness for Virtual Collaboration
Peter Gall and Janice Burn (2008). *Encyclopedia of Networked and Virtual Organizations* (pp. 530-537). www.igi-global.com/chapter/evaluating-organisational-readiness-virtual-collaboration/17656?camid=4v1a