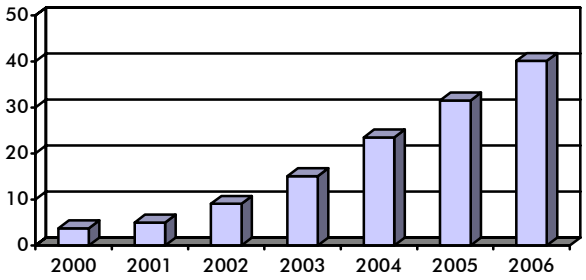
WLAN Standards and Wireless Gateways: Making the right choices to secure and manage your WLAN

Why Wireless LANs Need Standards

Despite the general downturn in enterprise IT expenditure, most industry analysts predict that we are about to see an explosion in the number companies installing Wireless Local Area Networks or WLANs. For example, a recent Microsoft poll of 180 US companies with 500+ PCs found that 40% have some WLAN deployment but that a further 31% intended to deploy in the next 18 months. Moreover, the poll found that WLAN deployment is broadening: over 70% of the companies that intend to deploy WLAN plan to give access to entire workgroups or divisions. These trends are confirmed by the Gartner Group which estimates that roughly 5 million people are using a WLAN today, but predicts that this number will increase to over 40 million by the end of 2006 (see chart below).

WLAN End User Forecast (millions)



Source: Gartner Inc. "Enterprise WLANs – How Will They Impact Network Productivity, ROI and TCO?", P. Redman

Convenience and cost savings are the two primary factors driving WLAN deployments. Yet there is considerable confusion in the marketplace about the various standards that exist (or are in development), how each vendor will deploy and integrate these different standards and how WLAN technology will mesh with existing security and management frameworks. John Pescatore of Gartner Group gives this opinion on evolving WLAN standards:

"Gartner believes that the ratification and adoption of 802.11i and 802.1x security enhanced standards will remove security fears from buyers' minds as a barrier to adoption of WLANs by the end of 2002. However, interoperability issues and the complexity of managing the variety of WLAN-enabled devices and applications will make WLAN security management an important issue for enterprises and service providers."

This Bluesocket BluePaper tries to explain in simple terms where the most talked about WLAN standards came from, what they aim to do, and what the implication is for an organization that intends to install or upgrade a WLAN. The paper also explains Bluesocket's position on each of these standards.

Who Sets Wireless LAN Standards?

The most influential standards-making body in the world of WLANs is the Institute of Electrical and Electronic Engineers (IEEE) a professional association for engineers which is headquartered in the USA. The IEEE 802 Standards Committee is responsible for Local Area Network and Metropolitan Area Network standards. The Committee comprises various Working Groups focusing on particular areas. The 802.11 Working Group looks at WLAN standards. Within the 802.11 Working Group there are various Task Groups. Some of these, such as 802.11a, 802.11b and 802.11g, concentrate on air interface standards. Others, such as 802.22e, 802.11f and 802.11i, concentrate on issues that cut across multiple air interfaces.

The European Telecommunications Standards Institute (ETSI) is also active in setting WLAN standards through its Broadband Radio Access Networks (BRAN) project. ETSI BRAN is responsible for the HiperLAN2 standard. ETSI is a trade association, most of whose members are equipment manufacturers, network operators or service providers.

Finally, the Bluetooth Special Interest Group (SIG) is, as you might guess, responsible for specifying Bluetooth, which is usually defined as a Personal Area Network standard rather than a Local Area Network standard. The Bluetooth SIG is an ad hoc group of companies with an interest in Bluetooth, led by nine promoter companies. The IEEE is not involved in setting the Bluetooth standard, but it is basing its own 802.15.1 Wireless Personal Area Network standard on Bluetooth.

The following sections discuss the standards developed by these groups in more detail.

Air Interface Standards: The 2.4 GHz Spectrum

802.11b

802.11b is today's most widely-used wireless LAN technology. 802.11b equipment that has been certified for interoperability by the Wireless Ethernet Compatibility Alliance (WECA) carries the Wi-Fi logo, so the standard itself is often referred to as Wi-Fi. 802.11b operates in the 2.4 GHz frequency band using a modulation system known as Direct Sequence Spread Spectrum (DSSS), which is similar to that used by CDMA (Code Division Multiple Access) cellular systems. There are three non-overlapping channels available for 802.11b networks in the license-exempt 2.4 GHz band. That enables users to run up to three access points in the same physical area.

802.11b is usually quoted as having a speed of 11 Megabits per second (Mbps). This is the maximum speed of the system under perfect conditions. However, as the distance between the user and access point or the amount of background noise or interference increases, the speed reduces in stages down to as low as 1 Mbps. The actual data transfer rate is also lower than the quoted speed because of system overheads. For example, an 802.11b link running at 11 Mbps will typically transfer data at a rate of 5-7 Mbps.

802.11g

802.11g is a draft standard developed jointly by Texas Instruments and Intersil. 802.11g allows operation at up to 54 Mbps in the 2.4 GHz band. The draft standard states that 802.11g devices must support existing 802.11b modulation techniques to ensure that an 802.11b client device can talk to an 802.11g access point and vice versa. For higher data rates the draft standard specifies Orthogonal Frequency Division Multiplexing (OFDM) as the mandatory modulation technique. OFDM has also been selected for 802.11a (see the following section on 5 GHz air interface standards). Two other optional modulation techniques are also included in the standard, but these techniques may not be implemented in commercial products. The 802.11g standard is expected to be ratified in January 2003 but "pre-standard" client cards and access points are already widely available.

Bluetooth

Another 2.4 GHz band solution is called Bluetooth™. Bluetooth operates at lower power points than 802.11b or 802.11g, which gives it a shorter effective range (commonly 10 meters). This seeming limitation actually makes it more suitable for use in small battery-powered handheld equipment. Due to this lower power consumption, Bluetooth is viewed as an excellent solution for completely unwired phone headsets, links between printers and laptops, etc.

Bluetooth devices communicate in groups known as piconets consisting of one master device and up to seven slaves. Each piconet hops 1600 times a second in a pseudo-random fashion among 79 different frequencies. This is important to understand since as the number of Bluetooth piconets in a given area increases, the chance of two piconets causing a data collision by trying to use the same frequency at the same time increases. In practice it is typically possible to run 8-10 piconets in a given area without losing a significant amount of data throughput.

Bluetooth transmissions also interfere with 802.11b transmissions. The interference can be quite serious if a Bluetooth device is placed right next to an 802.11b device (hence laptops that contain both technologies ensure only one transmits at a time) but the interference does not have much impact on the throughput of either technology if the separation is a few meters or more (so one person using a Bluetooth headset with their cell phone is unlikely to prevent everyone else in an office from using the 802.11b WLAN).

Air Interface Standards: The 5 GHz spectrum

802.11a

Contrary to what its name implies, 802.11a is a newer standard than 802.11b. Wireless vendors started shipping 802.11a equipment in late 2001 and it is expected to become widely available during 2002. 802.11a is designed to run at speeds of up to 54 Mbps in the license-exempt 5 GHz band. WECA also certifies 802.11a equipment for compatibility. 802.11a uses a modulation technique referred to as Orthogonal Frequency Division Multiplexing (OFDM) which uses multiple sub-carriers operating at slightly different frequencies.

There is more license -exempt spectrum available at 5 GHz than at 2.4 GHz and so it is possible to have more non-overlapping channels to increase coverage and density. In addition there are fewer existing sources of interference. However, 802.11a systems generally have a shorter range than 802.11b.

HiperLAN2

In Europe, the frequency regulations specify that WLAN systems operating in the 5 GHz band must support Transmit Power Control (i.e. they must be able to turn their "volume" controls up and down automatically) and Dynamic Frequency Selection (i.e. they must be able to move to a different part of the frequency band to avoid interference). The European HiperLAN2 standard supports both these features but 802.11a does not. For this reason, 802.11a is not generally approved for use in Europe, although it can be used under certain circumstances in particular countries.

802.11h

However, the 802.11h Task Group is working on a new version of the standard that would support Transmit Power Control and Dynamic Frequency Selection. Consequently, vendor support for HiperLAN2 is waning and it seems quite likely that the majority of 5 GHz systems in Europe will be 802.11h rather than HiperLAN2.

The Bluesocket Advantage:

> Equipment based on several different air interface standards is already on the market and the situation is likely to grow more complex over the coming months. Bluesocket's WG-1000 Wireless Gateway™ supports all of the standards described above, giving network administrators a common approach to management and security and minimizing the cost of future upgrades.

> As the number of users and the amount of data on a WLAN increases, Bluesocket's bandwidth management and functional control of access (e.g. who is allowed to access streaming video, FTP etc) provide the "traffic engineering" tools necessary to keep data flowing and users happy.

WLAN Security Standards

802.11 Wired Equivalent Privacy (WEP)

WEP was envisaged as a combined access control, link privacy and message integrity system for WLANs. Unfortunately some compromises that were made in developing WEP have resulted in it being much less secure than intended in all three areas: in fact you can now find free programs on the Internet, such as AirSnort and WEPCrack, that allow a hacker with minimal technical knowledge to obtain a WEP-enabled network's secret key and break into the network, without being detected, in no more than a few hours.

The discovery of WEP's deficiencies has resulted in a major effort to develop improved security standards for WLANs. Enhanced security is the responsibility of 802.11 Task Group I (see 802.11i section below). The most urgent need is to improve the level of security on existing equipment. Essentially this means changing the WEP key frequently so that a hacker has less chance of collecting enough data to work it out. At present the most likely candidate as a short term fix is a proposal from RSA Security and Hifn known as Temporal Key Integrity Protocol (TKIP) which combines a better algorithm for generating keys with improved message integrity checking and dynamic key management (i.e. the ability to change keys part way through a user session).

In the longer term it is expected that WEP will be replaced by a completely new security algorithm based on the US Government's recently-approved Advanced Encryption Standard (AES). However, it will probably not be possible to upgrade the majority of existing WLAN access points and network interface cards to support AES.

802.1x: Port-based Authentication

In June 2001 the new IEEE 802.1x standard for port-based user authentication was approved. It was originally designed to provide access control to wired networks, but it has been

taken up by many WLAN vendors as a way of overcoming the deficiencies in WEP access control and key management described above. The standard has also been given a boost by Microsoft's decision to provide native support for 802.1x in its new Windows™ XP operating system.

In a wireless environment, 802.1x works like this. When a mobile device first associates with an access point, all traffic apart from 802.1x authentication traffic is blocked. The mobile device sends its identity to the access point and the access point passes the information on to a Remote Authentication Dial-In User Service (RADIUS) server via an "uncontrolled port" that is only used for 802.1x traffic. The RADIUS server requests further credentials from the mobile device, such as a username and password, and uses this information to authenticate the device and its user against a central database. Assuming the authentication is successful, the RADIUS server issues an authentication key to the access point. This prompts the access point to issue a WEP key to the mobile device that is valid only for that particular user, and to accept other types of traffic to and from the mobile device via a "controlled port". The mobile device can also be asked to re-authenticate periodically, which results in the generation of a new WEP key.

The 802.1x protocol itself is not a single authentication method; rather it utilizes Extensible Authentication Protocol (EAP) as its authentication framework. While this provides a flexible environment, it introduces a new interoperability challenge. Since the introduction of the 802.1x specification, several competing alternatives have evolved as solutions that fit into the EAP framework. A further consideration is that 802.1x support needs to be built into the access point. If you already have a WLAN this generally means buying new access points since few legacy devices are capable of being upgraded.

The Bluesocket Advantage:

> With Bluesocket's WG-1000, you can support a mixed network of access points some of which are 802.1x enabled while others are not (bear in mind that over 1 million access points without 802.1x support are currently in use). In addition, Bluesocket adds functionality and supports vendor-proprietary access point functionality for EAP implementations.

> Bluesocket also enables interoperable communications between mobile devices that support 802.1x and those that do not, all on the same network. This includes support for older Microsoft operating systems as well as Microsoft Pocket PC™ 2002, which is not 802.1x-enabled.

> Finally, Bluesocket provides role-based access control enabling the WLAN service to be tailored for different types of user. 802.1x access control on its own is still "on" or "off".

802.11i: Enhanced Security Networking

The 802.11i standard proposal which is currently in draft form includes an Enhanced Security Network (ESN) that uses 802.1x to deliver its authentication and key management services. 802.11i will also provide key distribution, data origin authentication and replay detection.

All stations and access points in an ESN must contain an 802.1x port entity and an 802.11i authentication agent. In addition, the standard requires an authentication server that participates in the authentication of all mobile devices and access points. It may authenticate these devices itself or it may provide information that the devices can use to authenticate each other.

The Bluesocket Advantage:

> Bluesocket is following and will support 802.11i as adopted.

> If all goes well, deployment of 802.11i will begin at the end of 2002. By that time, nearly 10 million wireless users and their devices will be accessing WLANs. Bluesocket will support "legacy" devices in combination with newly rolled-out 802.11i products.

> For 802.11i to work, every access point, every switch, every client device and every authentication server must be 802.11i and 802.11x enabled. Bluesocket will support the unique capabilities each vendor will put into their devices, their access points and their authentication servers to differentiate their offerings.

Roaming and Quality of Service Standards

802.11f: Inter-Access Point Protocol for Access Point Roaming

For a mobile device to move seamlessly from one access point to another, the access points need to communicate with each other using an inter-access point protocol (IAPP). The original 802.11 standard did not specify this IAPP (Bluetooth has no standard IAPP either). Most access point vendors implemented their own proprietary IAPPs with the result that today seamless roaming between access points from different vendors is generally not possible. 802.11f intends to remedy this situation by specifying a standard IAPP for 802.11 networks. 802.11f is currently in draft form, but expected to be finalized before the end of 2002.

802.11f does not address the issue of roaming between access points on different IP sub-nets, or the issue of roaming between networks belonging to different companies.

The Bluesocket Advantage:

> Bluesocket's WG-1000 provides roaming between access points from different vendors on the same subnet. Bluesocket's Secure Mobility™ also allows roaming between access points on different sub-nets. Other sub-net roaming products on the market require special client software to be installed on every mobile device but Bluesocket's Secure Mobility is entirely network-based and therefore clientless. Bluesocket is also committed to supporting future standards like 802.11f.

802.11e: Quality of Service

The IEEE's 802.11 Task Group e is responsible for proposing improvements to the 802.11 standard to make it better able to handle voice traffic (with a target of 20 ms or less delay), MPEG video at up to 3 Mbps, and data streams at up to 10 Mbps. The group is looking at ways of minimizing jitter and delay variations and maximizing access point throughput. The group is also considering ways of introducing load balancing between access points. The 802.11e standard is not expected to be finalized before the end of 2002.

The Bluesocket Advantage:

> Bluesocket's WG-1000 already provides bandwidth management features, allowing the capacity on an access point to be partitioned for different groups of users. In many cases this relatively simple approach is sufficient to enable a WLAN to support voice or streaming video applications. Bluesocket will continue to enhance its products to provide additional quality of service and packet shaping features.

> Once access points support 802.11e there will still be a need for intermediate gateways, to provide end to end packet shaping. It is likely that there will also be issues in supporting 802.11e across multiple APs, particularly in multi-vendor environments. Bluesocket will help advance the 802.11e standard when ratified to support vendor-agnostic as well as multi-AP implementations common to the enterprise.

About Bluesocket

Bluesocket develops solutions to manage wireless local area networks (WLANs) to enable secure wireless connection of mobile devices (e.g. laptops and PDAs) to corporate networks and the Internet. Bluesocket technology enables corporations and service providers to build scalable, secure and easily managed networks that re-use existing infrastructure.

The Mobile Internet Times says: *"Bluesocket is the most comprehensive solution for WLAN security and management. Bluesocket provides strong encryption, role-based authentication, seamless roaming, and an agnostic approach to wireless technology."*

Contact Bluesocket

Phone: US: 1.866.633.3358 (toll free)
UK: +44 845 458 8450

Web: www.bluesocket.com

Email: information@bluesocket.com