



Industry Brief

Wireless Technology Overview

August 2003

Overview

The purpose of this industry brief is to provide an overview of wireless technology – specifically the 802.11 standards, what they are and where they stand. Healthcare specific wireless success stories are also highlighted, along with some interesting wireless vendors.

802.11 Primer

Wireless devices connect to each other by transmitting and receiving signals on a specific frequency of the radio band. Components can connect to each other directly (“peer-to-peer”) or through access points or gateways. Wireless local area networks (WLANS) consist of two basic components: wireless devices (radios) and access points/gateways.

What exactly is 802.11?

Generally, 802.11 is a family of specifications for WLANS developed by the Institute of Electrical and Electronics Engineers (IEEE). The 802.11 standard specifies parameters for both the physical (PHY) and medium access control (MAC) layers of a WLAN. The PHY layer handles the transmission of data between nodes. The MAC layer consists of protocols responsible for maintaining order in the use of a shared medium.

“Exactly” becomes harder to describe – there are, as of this writing, twelve versions of the standard, including the original 802.11 standard and an alphabet soup of others ranging from “a” to “k”. Three of the specifications (a, b, and g) need to be considered when deciding how to set up a WLAN. The other members of the 802.11 family deal with issues of security and interoperability, amongst vendors, as well as countries. Appendix A contains a more in-depth description of each of the specifications.

802.11a operates at radio frequencies between 5 GHz and 6 GHz. It uses a modulation scheme called orthogonal frequency-division multiplexing (OFDM); it is this technology that makes higher data speeds possible (higher than the more popular 802.11b).

802.11a can carry up to eight channels. In theory, data speeds can go as high as 54 Mbps, but as the range increases, the speed diminishes. Miscellaneous industry testing generally places the 802.11a range at 20 feet at

its highest speed (54 Mbps) and its maximum range at ~200 feet, at a significantly lower speed of only 6 Mbps.

Advantages: 802.11a can be nearly five times faster than 802.11b. It has up to eight channels. The 5GHz band is relatively uncrowded, so there is less interference than in the 2.4 GHz band.

802.11b (often called Wi-Fi), the most popular of the specifications, operates in the 2.4 GHz frequency. This frequency can have significant interference problems from such devices as microwave ovens and cordless phones. The modulation method used in 802.11b is known as complementary code keying (CCK). The speed is slower than 802.11a, only 11 GHz, but the range is far superior, reaching up to 300 feet (although, as in 802.11a, there can be a trade-off between distance and speed). An 802.11b network has three channels to choose from within the broadcast frequency.

Advantages: Ranges of up to 300 feet.

802.11g is the newest member of the 802.11 family. Board approved on June 12, 2003, 802.11g may give the other two standards a run for their money. Like 802.11b, 802.11g operates in the 2.4-GHz frequency and can achieve ranges of up to 300 feet, but like 802.11a, it reaches speeds of up to 54 Mbps. 802.11g uses a hybrid CCK-OFDM modulation, combining the best of the 802.11a and b standards. Unfortunately, because 802.11g is in the 2.4-GHz frequency, it also has only three channels to choose from. Having ratified 802.11g in June, IEEE wasted no time in coming out with their first list of certified 802.11g products on July 8, 2003. Certified vendors include: Atheros, Broadcom, Intersil, Melco, Proxim, and Texas Instruments. (Cisco, Symbol where are you!?)

Advantages: Ranges up to 300 feet. Speeds up to 54 Mbps. Interoperable with 802.11b.

**Comparisons between
802.11a, 802.11b, and 802.11g
(the “better” standards are highlighted)**

| | 802.11a | 802.11b | 802.11g |
|-------------------|----------------------|---------------|----------------------|
| Speed | Up to 54 Mbps | 11 Mbps | Up to 54 Mbps |
| Frequency | 5-6 GHz* | 2.4 GHz | 2.4 GHz |
| Channels | 8 | 3 | 3 |
| Range | 20 – 200 ft | 300 ft | 300 ft |
| Modulation | OFDM | CCK | CCK-OFDM |

* - This designation of “better” frequency is based on fewer interruptions from such devices as cell phones/microwaves.

To “b” or not to “b”, “g” whiz!

802.11a and 802.11g standards are not compatible because they use different frequency bands, nor is 802.11a compatible with the existing installed base of 802.11b devices. 802.11b and 802.11g devices, however, can coexist in the same network. There is, of course, a caveat – although 802.11b and 802.11g devices can coexist, older 802.11b devices may not be able to connect to an 802.11g network because of differing data rates.

What does all this mean? For those without a wireless network, 802.11g *seems* to be the way to go. Although the current list of certified products is not long, soon all the major vendors will have certified products. For those with an 802.11b network, because of the backward compatibility, 802.11g will be relatively easy to migrate to. For those on 802.11a, “migration”, per se, is not an option. From a “glass is half-full” perspective, 802.11a and 802.11g (or 802.11b) can be used together in the same coverage area because they do not conflict with each other, so having both types is definitely an option. One last thing to consider: in May 2003, the Federal Communications Commission (FCC) issued a proposal to nearly double 802.11a’s available bandwidth, increasing the available number of channels to 24, so it may not make sense to migrate to 802.11g, despite the added range that it offers.

The bottom line is that there is no clear-cut bottom line. Assess your organization’s physical environment (interference factors), assess your organization’s networking requirements (how big an issue *is* range?), and work closely with your vendors to make the choices that are the most appropriate for you.

The Wi-Fi Alliance is a nonprofit international association formed in 1999 to certify interoperability of wireless Local Area Network products based on IEEE 802.11 specification. Wi-Fi certification is considered by most of the industry to be the “final word” in 802.11 certification. For more information on the Wi-Fi Alliance visit their Web site:

<http://www.wi-fi.org>.

To view products that are certified for a specific standard, use the following link:

http://www.wi-fi.org/OpenSection/certified_products.asp?TID=2.

This rather neat utility not only shows products that are certified for a particular standard, but products that are certified for multiple standards, for example both 802.11b and 802.11g (important if considering migrating from 802.11b to 802.11g).

Wireless Security

Security is one the biggest issues still holding healthcare enterprises back from widespread WLAN deployments. The current 802.11 offering for addressing security, WEP, Wire Equivalent Privacy, is an *optional* encryption standard implemented in the MAC Layer that most wireless vendors support. However, WEP is something of a laughing stock. WEP uses a single **static** 40- or 128-bit key for both encryption and authentication. This rudimentary technology is an administrative burden (WEP key information must be entered manually on every device), as well as easily cracked (search the Web to find a myriad of utilities to help break WEP).

So, is wireless security a lost cause? Not necessarily, there *are* options. Common approaches include implementing an IP Security (IPSec) based VPN, using the existing 802.1x standard, coupled with an Extensible Authentication Protocol (EAP), and implementing architecture based on new standards that are currently in the works.

A **VPN (Virtual Private Network)** uses a tunneling protocol to connect the end-user's computer, through the end-user's access point or gateway, all the way to the enterprise servers and system. It uses a public telecommunications infrastructure (i.e. the Internet) to accomplish this. Information is encrypted prior to sending it through the Internet and decrypted at the other end. Although VPNs were designed for remote "wired" users (such as physicians at home or in their offices), it may also be applied to wireless network. There are mixed emotions regarding the use of a VPN in a wireless network. Many CIOs feel that it is simply another layer of overhead, i.e. "too much like work", additionally, it is limited to Internet traffic. On the other hand, if an enterprise is already using a VPN for remote users, they have the skill set to relatively easily modify existing systems to support wireless networks.

ReefEdge, Memorial Medical Center

Memorial Medical Center, Springfield, Illinois, is an acute care hospital with 562 licensed beds and more than 3,000 employees offering comprehensive inpatient and outpatient services. Memorial implemented a wireless LAN so that physicians may access the hospital's EMR. Memorial Medical Center has over 550 physicians on staff and a total of over 2,400 employees who are using the system on a regular basis, many of who constantly move between wireless coverage points. Security was a primary issue for Memorial Medical Center. To address their concerns, they chose ReefEdge's **IPSec VPN** and have been happy with the product. For more information on the ReefEdge solution, visit their Website at: <http://www.reefedge.com>.

802.1X and EAP – A powerful combination

A protocol does exist that addresses the 802.11 security concerns. 802.1X, also brought to us courtesy of IEEE, offers a framework for authenticating and controlling user traffic to a protected network, as well as **dynamically varying encryption keys** (verses the easily cracked static encryption keys that WEP calls for). 802.1X ties a protocol called EAP (Extensible Authentication Protocol, from the Internet Engineering Task Force) to both the wired and wireless LAN media and supports multiple authentication methods.

There are three components in 802.1x wireless authentication:

- Supplicant - a software client running on the wireless workstation
- Authenticator - the wireless access point
- Authentication Server - an authentication database, usually a radius server.

The EAP is used to pass authentication information between the supplicant and the authentication server. The actual authentication is defined and handled by the EAP type. There are a variety of EAPs on the market today, including a proprietary version from Cisco (Lightweight EAP or LEAP). There is yet to be an obvious leader of the EAP pack. The caution with EAPs is that both the client and the access point must use the same EAP. If you implement an EAP that does not emerge as a leader, there is a potential that new clients will not be able to talk to the access point.

Dueling Standards

IEEE is certainly not unaware of the security issues surrounding 802.11 and WEP. They have been working on a standard, 802.11i, which is intended to fix all of the security problems in 802.11. 802.11i has been in the works since 2001, and although it is fairly far along, has not yet been board approved. It is expected to be approved by the end of the year, with compliant products due out in the 2nd quarter of 2004.

In October 2002, Wi-Fi announced a standard of their own, Wi-Fi Protected Access or WPA. Why? IEEE simply wasn't moving fast enough and vendors were developing too many proprietary solutions – a standard was needed! There does not appear to be any animosity between Wi-Fi and IEEE; Wi-Fi has worked closely with IEEE and WPA is meant only to be an interim solution, with the intent of easy migration to the 802.11i standard (or WPA2, as it has come to be known) when that standard is finally ratified. WPA adds authentication support using 802.1x/EAP protocols, hopefully accommodating easy upgrade or migration paths for those who have already implemented specific vendor solutions. Wi-Fi has already certified WPA products, including products from high profile vendors Cisco and Symbol.

As with the "802.11 a,b,g" choice, the answer on security is not completely black and white, but implementing a Wi-Fi certified WPA wireless security solution seems like a pretty safe bet.

Healthcare Applications

Despite the challenges in choosing a wireless standard and implementing a secure wireless environment, healthcare organizations have forged ahead and there are quite a few success stories. The remainder of this brief highlights some of these successes, as well as vendor innovations.

Voice over IP (VoIP)

VoIP is also known as IP Telephony or Internet Telephony. Simplistically, it is technology that uses Internet Protocol to carry and route two-way voice communications. Like the other wireless applications, this technology has been in use for years, but recent advances have finally made it a more viable option. Not all wireless systems can automatically handle VoIP. The system has to be a high quality system; 802.11a generally handles VoIP much better than 802.11b. It may cost a bit more to expand your WLAN capabilities to effectively deal with voice (such as implementing both 802.11a and 802.11b, one for voice, one for data), but industry experts agree that in the long run, it can save money, both reducing the cost of a wiring a phone system, as well as the cost of phone calls. There is (of course!), an 802.11 standard that deals with voice issues. 802.11e has been in the works since March 2000, but there is no

prediction as to when the standard will be ratified.

SpectraLink, Columbia Presbyterian Medical Center

Columbia Presbyterian Medical Center, New York, uses the SpectraLink (<http://www.spectralink.com>) Link Wireless Telephone System™. They have equipped doctors, nurses and other staff that work in the Operation Room, Interventional Radiology, Endoscopy, and Emergency departments, with Link Wireless telephones, enabling them to make and receive calls wherever they are within those areas. The system integrates to the hospital's existing telephone system and relays calls through Base Stations installed throughout the facility, so no airtime or usage charges are incurred.

McKesson, Symbol, Glenbrook Hospital

McKesson (<http://www.mckesson.com>) and Symbol (<http://www.symbol.com>) presented a wireless nurse communication system at the HIMSS 2003 conference. Horizon Care Access™ is a nurse communication solution that integrates nurse call systems and wireless phones utilizing Voice over IP. The announcement followed the successful implementation of the solution at Glenbrook Hospital, part of the Evanston Northwestern Healthcare System, in the Chicago land area.

At Glenbrook, nurses armed with Symbol's NetVision Phone can receive, at any given time, nurse call messages within a 30-bed wing of the hospital that is equipped with a Symbol Wi-Fi (802.11b) wireless local area network. The system interfaces with Dukane's (<http://www.dukane-ultrasonics.com>) ProCare 6000 Advanced Healthcare Communication System and uses the Nortel (<http://www.nortelnetworks.com>) Meridian 1 telephone switch.

"We have seen an increase in patient satisfaction levels for nurse call response time ... compared to floors that don't have wireless nurse call administration," said Tom Smith, CIO of Evanston Northwestern Healthcare.

Patient Safety and Wireless Bar Coding

Medication error reduction has been high on most healthcare organization's priorities for several years now. Everybody is working on the right way to ensure the five rights (right patient, right medication, right dosage, right time, and right route). Bar coding has proven to be a very effective method of ensuring these rights. What is better than bar coding? Wireless bar coding, of course! The following two organizations, veterans of wireless technology, have implemented wireless bar coding solutions.

Palm, Bridge Medical Inc., Miami Children's Hospital

Miami Children's Hospital (MCH) has been wireless for several years now, since April 2001. Using a wireless Web, physicians monitor their patients from home, and from just about anywhere else. Developed and implemented by the team of Dr. Redmond Burke, Chief of Cardiac Surgery, and Jeff White, a onetime aerospace engineer, the system allows doctors and nurses to input patient information into PDAs (Palm VIIx and Palm IIIc handhelds, <http://www.palm.com/us/products/handhelds/>), the data then travels via wireless modem to the hospital's main server, where it is accessible to all authorized caregivers.

Late in 2002, MCH implemented a Bridge Medical's (<http://www.bridgemedical.com/>) MedPoint system, a barcode-enabled point-of-care system that combines medication and blood product administration verification with laboratory specimen identification. Nurses scan the barcode of the medication to be administered, the patient ID bracelet, and their own ID badge – complete verification of the five rights. "MedPoint uses bedside computers that interact with a radio wave-controlled wireless communication system," said Miami Children's Hospital Chief Information Officer Don Lewis. "Changes in medications and other patient information are instantly communicated from hospital information systems to the bedside unit, notifying nurses of changes." The most challenging part of the project was not implementing a wireless solution, something MCH was already adept at, but (per Connie Chan, Director of Pharmacy at MCH) ensuring that all medications dispensed by the pharmacy have a barcode.

Symbol, IDX

In 1998, Lehigh Valley Hospital and Health Network (LVHNN), Allentown, Pennsylvania, took important steps to implement an important initiative of theirs - Patient Centered Care. The goal of Patient Centered Care is to provide as many services as possible in the patient's rooms. Lehigh Valley Hospital made the strategic decision to use the Symbol (<http://www.symbol.com>) Spectrum24[®] wireless Local Area Network (LAN) system and mobile computers to provide mobile access to clinical information at the point-of-care. It was important to Lehigh Valley that wireless function as an extension of Lehigh Valley's existing information technology network. The Spectrum24[®] wireless LAN uses a 2.4 GHz high performance network for reliability, security and high transfer rate. Lehigh Valley initially considered putting a PC in each in-patient room, however, the cost of this would have been astronomical and the projected usage of each PC was less than one-half hour per day, leading to extensive wasted downtime per unit.

Pleased with, and skilled at wireless technology, in June 2003, LVHNN became the first customer to go live with IDX's (<http://www.idx.com>) wireless bar code medication charting technology. LVHNN, already users of the IDX LastWord CPOE product, implemented bar code medication charting on a 31-bed medical/surgical unit, and will roll it out to the remaining units in its three community hospitals over the next three months. "Bar code medication charting is an integral part of our efforts to promote patient safety", stated Terry Capuano, R.N., LVHNN's senior vice president of clinical services. Time will tell, but wireless bar coding appears to be another successful step in LVHNN's patient centered care strategy.

Bedside Registration

Arguably, one of the biggest challenges facing today's emergency department is patient registration. Between EMTALA (a statute implying that treatment should occur prior to registration), and the increasingly popular concept of bringing the care to the patient, not the patient to the care, registration has been a primary focus for emergency departments, as well as a great candidate for wireless technology. Although registration, in and of itself, is not a particularly sexy application, a wireless solution can reap great benefits for both the hospital and the patients.

Cisco, Wavelink, St. Vincent Hospital

St. Vincent Hospital, a 338-bed acute care hospital in Birmingham, Alabama piloted their Wi-Fi (802.11b) network concept with an in-house application that allows hospital staff to register incoming patients at remote clinics across the campus. They equipped a few rolling carts with wireless tablet computers, credit card scanners, and optical scanners for copying insurance cards and other patient documents. The benefits of bedside registration has proven the value of a hospital-wide wireless infrastructure.

Suggested by Cisco (<http://www.cisco.com>), who supplied St. Vincent's 167 Aironet 350 access points, St. Vincent picked Wavelink Mobile Manager (<http://www.wavelink.com>) software to speed the deployment of the secure wireless LAN infrastructure across its five-building campus and to manage the associated network administration chores more efficiently and cost effectively from one location. In addition to the remote deployment capabilities, Wavelink Mobile Manager provides critical network security capabilities, including the ability to detect rogue access points. Since their initial bedside registration implementation, St. Vincent's has moved on to other applications, including providing nurses and doctors wireless access to patient charts and records updated in real-time.

Buffalo Technology, St. Joseph Hospital

St. Joseph Hospital, Huntingburg, Indiana, utilizes bedside registration so they can attend to their patients more quickly and effectively. They also have many physician practices outside of the hospital. David Gilmour, St. Joseph's Network Administrator installed fifteen of Buffalo Technologie's (<http://www.buffalotech.com>) 802.11b AirStation™ Pro Intelligent Access Points (WLM-L11G). The access points were placed in physician offices and clinical areas within the hospital (the ER, ICU, surgery, wound care, etc.) He also installed seventeen of Buffalo's client cards in the hospital's laptop computers and a few AirStation Indoor Omni Directional Antennas (WLE-NDR) to boost signal strength and distance.

"We decided to install a wireless network so we could continue to provide supreme patient care," stated Gilmour. "[Buffalo Technology] allows us to rapidly register patients, be extremely mobile and keep patient information protected and accurate." Maintaining highly sensitive patient data is a challenge every hospital faces. St. Joseph's chose Buffalo's Intelligent Access Point because of its enhanced security features such as 128-bit / 40-bit WEP, RADIUS, IEEE802.1x/EAP, password protection and MAC address registration.

Summary

Wireless technology has found a definite home in healthcare. There are an ever-growing number of successful wireless implementations, despite the fact that there are multiple standards and specifications, in various degrees of readiness. Regarding what and how to implement, there is no right answer. Each specification and security approach has its own pros and cons and each organization must decide what is right for them – but, rest assured, there is a right answer!

Appendix A – Description of 802.11 Standards

The following table describes the assorted 802.11 standards. It was derived from the “Standards Status” section on the IEEE Web site. The complete standards status may be viewed at <http://standards.ieee.org/cgi-bin/status?wireless>.

| Designation | Board Approved | Project Purpose |
|----------------|----------------|---|
| 802.11 | 1997 | To provide wireless connectivity to automatic machinery, equipment or stations that require rapid deployment, which may be portable or hand-held or which may be mounted on moving vehicles within a local area. To offer a standard for use by regulatory bodies to standardize access to one or more radio frequency bands for the purpose of local area communication. |
| 802.11a | 09/16/1999 | To create a higher speed wireless access technology suitable for data, voice and image information services {in the 5 GHz range} |
| 802.11b | 09/16/1999 | To extend the performance and the range of applications of the 802.11 compatible networks in the 2.4 GHz band by increasing the data rate achievable by such devices. This technology will be beneficial for improved access to fixed network LAN and internet work infrastructure (including access to other wireless LANs) via a network of access points, as well as creation of high performance ad-hoc networks. The purpose of 802.11a is also for higher data rates; however, that project is for operation in the 5 GHz band, whereas this project is for operation in the 2.4 GHz band. |
| 802.11d | 06/14/2001 | The current 802.11 standard defines operation in only a few regulatory domains (countries). This supplement will add the requirements and definitions necessary to allow 802.11 WLAN equipment to operate in markets not served by the current standard. |
| 802.11e | | To enhance the current 802.11 MAC to expand support for LAN applications with Quality of Service requirements. Provide improvements in security, and in the capabilities and efficiency of the protocol. These enhancements, in combination with recent improvements in PHY capabilities from 802.11a and 802.11b, will increase overall system performance, and expand the application space for 802.11. Example applications include transport of voice, audio and video over 802.11 wireless networks, video conferencing, media stream distribution, enhanced security applications, and mobile and nomadic access applications. |
| 802.11f | 06/12/2003 | IEEE P802.11 specifies the MAC and PHY layers of a Wireless LAN system and includes the basic architecture of such systems, including the concepts of Access Points and Distribution Systems. Implementation of these concepts were purposely not defined by P802.11 ... this project proposes to specify the necessary information that needs to be exchanged between Access Points to support the P802.11 DS functions. The information exchanges required will be specified for, one or more distribution Systems; in a manner sufficient to enable the implementation of Distribution Systems containing Access Points from different vendors which adhere to the recommended practices. |
| 802.11g | 06/12/2003 | To develop a new PHY extension to enhance the performance and the possible applications of the 802.11b compatible networks by increasing the data rate achievable by such devices. This technology will be beneficial for improved access to fixed network LAN and inter-network infrastructure (including access to other wireless LANs) via a network of access points, as well as creation of higher performance ad hoc networks. |

| Designation | Board Approved | Project Purpose |
|--|----------------|---|
| 802.11h | | To enhance the current 802.11 MAC and 802.11a PHY with network management and control extensions for spectrum and transmit power management in 5GHz license exempt bands, enabling regulatory acceptance of 802.11 5GHz products. Provide improvements in channel energy measurement and reporting, channel coverage in many regulatory domains, and provide Dynamic Channel Selection and Transmit Power Control mechanisms. |
| 802.11i | | To enhance the current 802.11 MAC to provide improvements in security. |
| 802.11j | | The purpose of the proposed project is to obtain Japanese regulatory approval by enhancing the current 802.11 MAC and 802.11a PHY to additionally operate in newly available Japanese 4.9 GHz and 5 GHz bands. |
| 802.11k | | The original standard has a basic set of radio resource measurements for internal use only. These measurements and others are required to provide services; such as roaming, coexistence, and others; to external entities. It is necessary to provide these measurements and other information in order to manage these services from an external source. |
| 802.11ma | | The purpose of this project is to incorporate accumulated maintenance changes (editorial and technical corrections) into 802.11-1999, 2003 edition (incorporating 802.11a-1999, 802.11b-1999, 802.11b-1999 corrigendum 1-2001, and 802.11d-2001). |
| Although not part of the 802.11 family, 802.1X has been used to address some of the 802.11 security issues and so is included here. | | |
| 802.1X | 06/14/2001 | There is no standard mechanism that allows a network administrator to control access to and from a LAN segment based on the authenticated state of a port user. Simple network connectivity affords anonymous access to enterprise data and the global Internet. As 802 LANs are deployed in more accessible areas, there is an increasing need to authenticate and authorize basic network access. The proposed project will provide common interoperable solutions using standards based authentication and authorization infrastructures already supporting schemes such as dial up access. |

Appendix B – Glossary

Channels

Another name for frequencies, especially within a defined band.

Complementary Code Keying (CCK)

A code of a set of 64 8-bit code words used for transmitting at speeds above 2 Mbps; the technology employed by IEEE 802.11b.

CCK-OFDM

An optional transmit mode defined by the IEEE 802.11g standard that combines the access modes of IEEE 802.11a and IEEE 802.11b; capable of supporting transmission speeds of up to 22 Mbps.

EMTALA

Emergency Medical Treatment and Active Labor Act is a statute which governs when and how a patient may be (1) refused treatment or (2) transferred from one hospital to another when in unstable condition. However, the "refusal of treatment" has been broadly interpreted to mean the potential of refusal based on financial conditions – or ability to pay.

Gigahertz

Used as an indicator of the frequency of ultra-high-frequency (UHF) and microwave EM signals.

IPSec (IP Security Protocol)

Defines encryption, authentication and key management routines for ensuring the privacy, integrity and authenticity of data in a VPN as the information traverses public IP networks.

Mbps

Used for measuring the amount of data that is transferred in a second between two telecommunication points.

Media Access Control Layer (MAC)

The MAC is concerned with sharing the physical connection to the network.

Orthogonal frequency-division multiplexing (OFDM)

A method of digital modulation in which a signal is split into several narrowband channels at different frequencies.

Physical Layer (PHY)

The physical layer supports the electrical or mechanical interface to the physical medium.

RADIUS

Remote Authentication Dial-In User Service. The technology, initially developed to authenticate users dialing into an ISP, is now often used as a method of authenticating wireless network users. When combined with 802.1x and 128-bit data encryption, it provides a strong level of security.