the Journal of CONTEMPORARY DENTAL PRACTICE at www.thejcdp.com
Volume 7 Number 1 February 15, 2006

Contemporary, Emerging, and Ratified Wireless Security Standards: An Update for the Networked Dental Office

Muralidhar Mupparapu, DMD, MDS

Abstract

Wireless networking is not new to contemporary dental offices around the country. Wireless routers and network cards have made access to patient records within the office handy and, thereby, saving valuable chair side time and increasing productivity. As is the case with any rapidly developing technology, wireless technology also changes with the same rate. Unless, the users of the wireless networking understand the implications of these changes and keep themselves updated periodically, the office network will become obsolete very quickly. This update of the emerging security protocols and pertaining to ratified wireless 802.11 standards will be timely for the contemporary dentist whose office is wirelessly networked. This article brings the practicing dentist up-to-date on the newer versions and standards in wireless networking that are changing at a fast pace. The introduction of newer 802.11 standards like super G, Super AG, Multiple Input Multiple Output (MIMO), and pre-n are changing the pace of adaptation of this technology. Like any other rapidly transforming technology, information pertaining to wireless networking should be a priority for the contemporary dentist, an eventual end-user in order to be a well-informed and techno-savvy consumer.

Keywords: Wireless security, wireless networking, local area network, wireless dental office

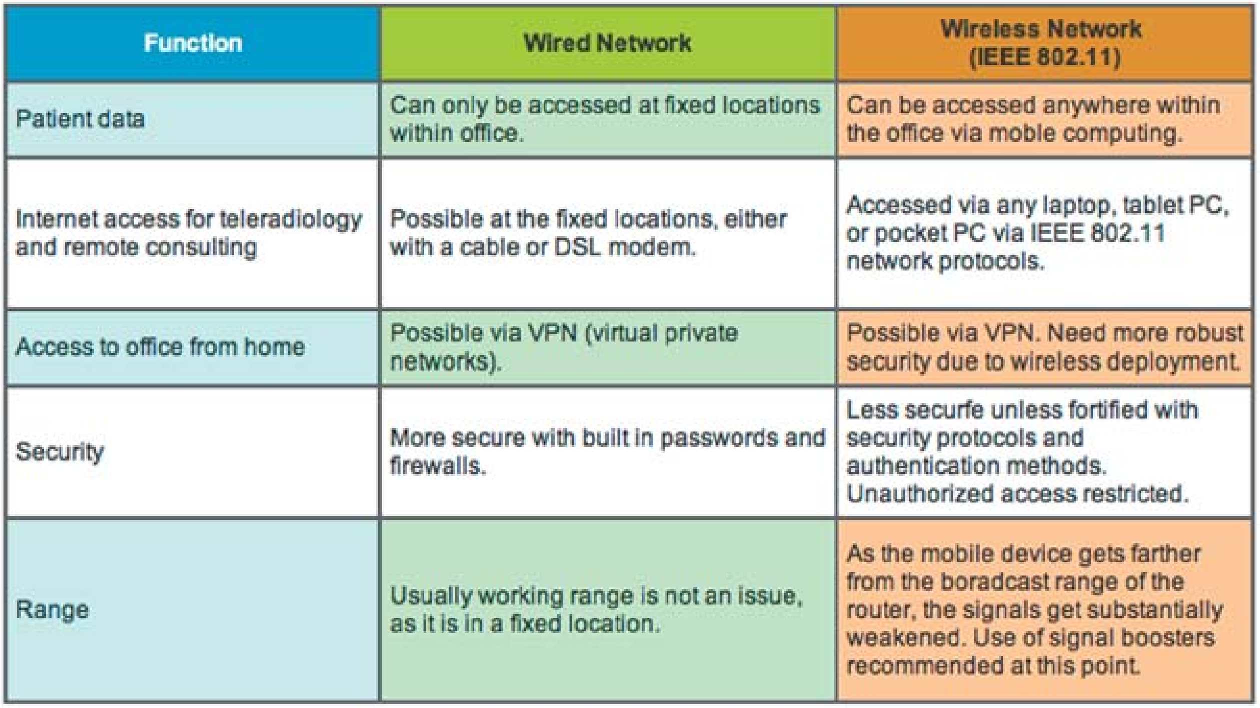
Citation: Mupparapu M. Contemporary, Emerging, and Ratified Wireless Security Standards: An Update for the Networked Dental Office. J Contemp Dent Pract 2006 February;(7)1:174-185.

Introduction

Conversion to a digital office and going both wireless and paperless is generally considered an enormous, expensive, and risky task by many dental practitioners; the techno-phobia will normally fade away with the small first step towards digital conversion by replacing patient charts with a paperless "practice management software." Integrating digital photography and filmless digital radiography is the next logical step in that direction. Medical, dental offices, and healthcare organizations have traditionally been slow in accepting WLAN technology in clinical practice. The major concerns have been the cost and security.[1-3] Once the office is digitally transformed, then comes the question of user access (to whom, where, and how). Traditionally dental offices have personal computers (PC) in fixed locations, usually at the reception/chart room. With digital conversion and networking, mobile computing devices can be used to access the same data throughout the office, including chair side locations. Scheduling, note entries, digital x-ray images, and intraoral photographs can all be accomplished chair side and images are embedded right into the practice management software that is being used in the office. Table 1 shows the differences between wired and wireless networks in their functionality.

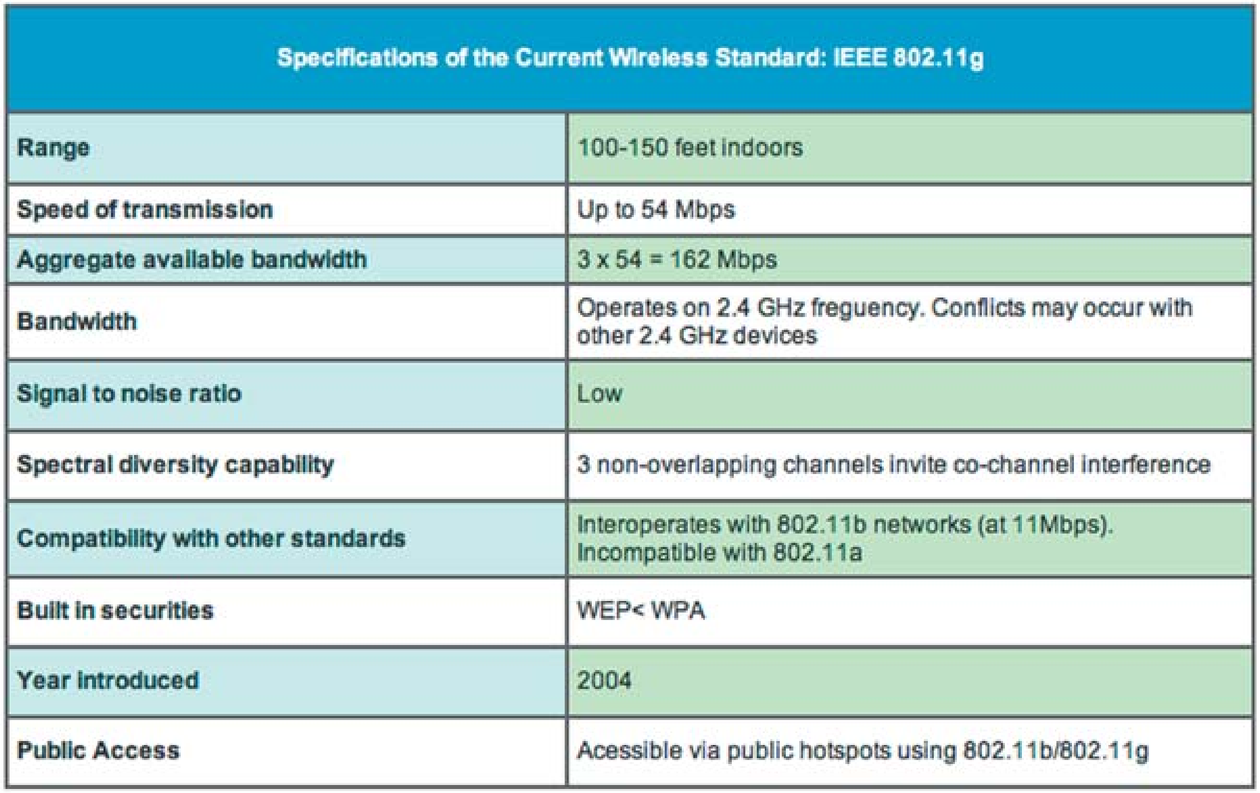
Currently, three standards are used for wireless networking within dental offices: 802.11a, 802.11b, and the newer, faster 802.11g (Table 2). Mupparapu and Arora (2004) in their review on wireless networking[4] discussed the advantages and disadvantages of utilizing different wireless standards in a dental office. They have addressed the security concerns using the 802.11b and made a case for utilizing 802.11a over the 802.11b in a dental office. While it beefs up the security, 802.11a has a limited wireless broadcast range and could be a disadvantage in a larger or a multilevel building. The 802.11g standard has been enhanced by several manufacturers who claim the newer versions transmit and receive data up to 125 megabits per second (Mbps) as compared to the current 11-54 Mbps rate. Although conflicts might still occur with other 2.4 GHz frequency sharing devices, the broadcast range is around 100-150 feet indoors

Table 1. Pertinent differences between wired and wireless networks



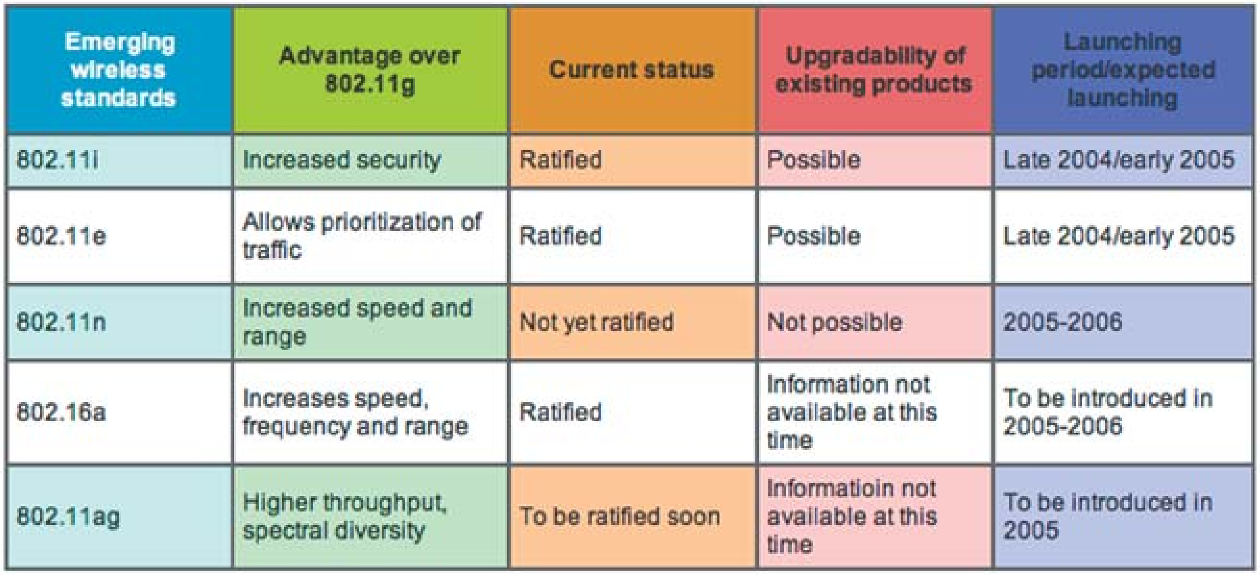
Function	Wired Network	Wireless Network (IEEE 802.11)
Patient data	Can only be accessed at fixed locations within office.	Can be accessed anywhere within the office via mobile computing.
Internet access for teleradiology and remote consulting	Possible at the fixed locations, either with a cable or DSL modem.	Accessed via any laptop, tablet PC, or pocket PC via IEEE 802.11 network protocols.
Access to office from home	Possible via VPN (virtual private networks).	Possible via VPN. Need more robust security due to wireless deployment.
Security	More secure with built in passwords and firewalls.	Less securfe unless fortified with security protocols and authentication methods. Unauthorized access restricted.
Range	Usually working range is not an issue, as it is in a fixed location.	As the mobile device gets farther from the boradcast range of the router, the signals get substantially weakened. Use of signal boosters recommended at this point.

Table 2. Features of the existing IEEE 802.11g - wireless standard.



Specifications of the Current Wireless Standard: IEEE 802.11g	
Range	100-150 feet indoors
Speed of transmission	Up to 54 Mbps
Aggregate available bandwidth	3 x 54 = 162 Mbps
Bandwidth	Operates on 2.4 GHz freguency. Conflicts may occur with other 2.4 GHz devices
Signal to noise ratio	Low
Spectral diversity capability	3 non-overlapping channels invite co-channel interference
Compatibility with other standards	Interoperates with 802.11b networks (at 11Mbps). Incompatible with 802.11a
Built in securities	WEP< WPA
Year introduced	2004
Public Access	Acessible via public hotspots using 802.11b/802.11g

Table 3. Emerging wireless standards, compatibility, and advantages over the existing 'g' standard.



Emerging wireless standards	Advantage over 802.11g	Current status	Upgradability of existing products	Launching period/expected launching
802.11i	Increased security	Ratified	Possible	Late 2004/early 2005
802.11e	Allows prioritization of traffic	Ratified	Possible	Late 2004/early 2005
802.11n	Increased speed and range	Not yet ratified	Not possible	2005-2006
802.16a	Increases speed, frequency and range	Ratified	Information not available at this time	To be introduced in 2005-2006
802.11ag	Higher throughput, spectral diversity	To be ratified soon	Informatioin not available at this time	To be introduced in 2005

and uses the advanced security encryptions like the Wireless Protected Access[4] (WPA) and the newer WPA2. Today even more advanced versions of 802.11g are available (Table 3) that are fortified with advanced security features, yet have the agility of a network that one expects within a dental office.

The load factor of data communication might curtail design and or implementation of its use. For example, on a 'G' network (rather than A/B) one can experience 54 Mbps. This, in terms of implementation, might be able to use a device to capture and transmit images without creating a bottleneck in the network. In other words, if such apparatus exists, it would transmit images easily without freezing or alternatively may transmit them at a higher speed. The encryption standards could be better for robust security.

Discussion

Wireless deployment in dental offices can be accomplished in various ways. Different standards can be simultaneously utilized in order to secure the network appropriately. Here are some of the common applications for the wireless networks in dental offices.

Patient Management Software (PMS)

Instantaneous availability of patient schedules, chart notes, and x-ray images via the patient management software is possible by wirelessly networking the designated server with the most current wireless standard that is fortified with built in securities to make it compliant with the HIPAA regulations for protecting patient data. The Institute for Electrical and Electronics Engineers (IEEE) 802.11g or 802.11ag would be appropriate. The addition of a wireless Multiple Input Multiple Output (MIMO) standard would speed up the data transfer. Chair side retrieval of patients' records can be performed using mobile computing equipment.[4] Deployment of pocket PCs or PDAs that are considered "ultra-mobile" can be included in the office network.

Digital Radiography (DR) Systems

This is another scenario where wireless networking could be deployed. Once the radiographs are obtained using a suitable digital sensor (CCD, CMOS, super CMOS, or PSP) and proprietary software, the transfer of the images to the database generally initiates the use of the wireless networking. Not only is short-term storage accomplished using the IEEE 802.11 standard, but the long-term storage and retrieval of the images from the databases can be accomplished as well. Again, appropriateness of the type of IEEE wireless security that is to be deployed has to be taken into consideration. HIPAA security standards became effective April 20, 2005, and compliance with the standards is mandatory for all Electronic Patient Health Information (PHI).

Contemporary Wireless Technology

The following discussion will lead the dental practitioner through the realm of emerging wireless technology, the knowledge of which is essential for the timely upgrades and proper functionality of existing office networks. The specific focus will be on the 802.11 Super G, 802.11 super G + MIMO, Super AG, and 802.11 pre-n standards that are making their debut in the consumer market with rapid succession. Efficient utilization of wireless routers, newer add-on wireless standards, and understanding the most common security lapses while installing an access point will be discussed. Finally, the discussion will focus on the "Multiple Input Multiple Output," popularly known as "MIMO" – a brand new wireless standard, the introduction of which has taken the consumer wireless technology to the next level.

Super G and Super AG Technology

With the rapid emergence of bandwidth consuming applications for wireless LAN, existing standards and schemes fall short. Super G enhancements are designed to provide the optimal bandwidth performance for the 802.11a, b, g networks that use TCP/IP protocols and exceed 60 Mbps. Super G has backward compatibility with all existing 802.11a, b, g, and third party products. The 108 Mbps super G technology that was originally developed by Atheros[5] (www.atheros.com) is currently adapted by D-Link[6] (www.D-link.com) and Netgear[7] (www.netgear.com), while the 125 Mbps high speed mode technology developed by Broadcom[8] (www.broadcom.com) is included in the products by Belkin[9], Buffalo[10], and Linksys[11], among other vendors. It is important to note the generic 802.11g standard is compatible with products from each other, where as the enhanced versions are not compatible. It is generally recommended to stick with one manufacturer for all the Wi-Fi components (router, wireless card, etc.)

Network enabled components have been traditionally wired. A component which can communicate with other components using networking protocols like TCP/IP is called network enabled components. A component that can communicate using networking protocols wirelessly using wireless standards is called Wi-Fi components (Table 4) for maximizing the performance unless the laptop has a built-in Wi-Fi.[12,13] This important information is essential if the contemporary dentist is on the lookout for upgrading the existing network.[13]

The 802.11 Super AG[6], also known as the "*Clear Choice*," may overcome the limitations the 802.11g and super G standards may inherently have; that is the already congested 2.4GHz band they operate on. The dual band AG uses the 5 GHz band alongside the 2.4GHz band and will accommodate the high volume of traditional data traffic while ensuring a high quality of service for other consumer oriented wireless applications (Table 5). In other words the super AG has a better functionality in the long run. Wireless applications are either hardware or software applications that are programmed to communicate with other applications or appliances over a network using protocols like TCP/IP. (Examples are the various wireless access points, associated software, software related to security protocols, etc.)

Update on the Wi-Fi Routers and Adapters

The router, also known as Wireless Access Point (AP), is the single most important component in the Wi-Fi gear as it additionally connects the network to the Internet via cable or DSL modem.[13] It shares Internet access among multiple users and controls that can access your network. The access points that are available today are capable of supporting diverse station types simultaneously. Selection of the appropriate number of access points for the dental office depends on the area to be covered and the location of operatories.

Efficient Utilization of Wireless Lans

In order to increase the efficiency of the wireless LAN, the following important points should be taken into consideration.

Location of the Wireless Access Points

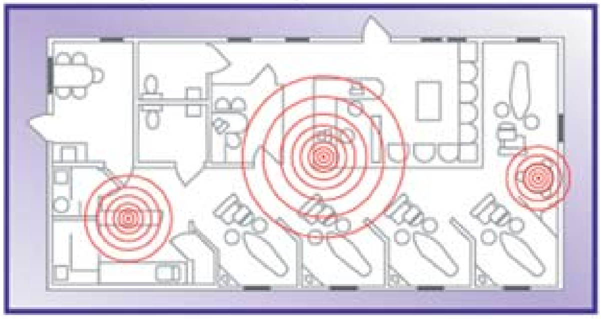
This is essentially the key to the transmission of wireless signals. The center of the office or clinic would be an ideal place for the access point. The location is usually determined by the trial and error method using 'wireless sniffing' with a mobile built-in wireless adapter within the office or clinic. Mobile sniffers are devices that read out the signal strength of the network in a numerical value. If the office area is rather large, signal extenders have to be considered that will boost the wireless signal and extend the range.[13]

Extending the Range of Wireless Products

In a multi-dimensional world, a signal from the router travels around until the power of the signal weakens. Signals bounce off an intrusion where possible. However, when bouncing from walls signal strength can weaken resulting in a particular location in a building without service. Such locations are called "dead spots." In spite of the wireless router location, if *dead spots*[13] still exist, range extending products are extremely helpful in situations like this. The easiest way to achieve this would be to replace the routers' external antenna with a more efficient antenna for transmission as well as for receiving the signal. Unfortunately, not all routers have removable antennas.[10] There are multiple varieties of antenna boosters available and they are typically:

- Unidirectional or sectional
- Omni directional

Both are useful devices depending on the need for enhancement of the signal in dead spots.



Security Protocols and Bandwidth Interferences with Phone Frequencies

As 802.11g Wi-Fi networks operate in the 2.4 GHz frequencies range, the same as microwave ovens and many cordless phones, the only solution is to change the phones to 900 MHz

Table 4. Common wireless components.

Wireless Components	
Linksys® Wireless Access Point (router)	
Linksys®Wireless signal booster	
Wireless PC Card	
Wireless laptop cards	

Table 5. Table showing the various wireless applications, their acronyms, and their role *in wireless networking*.

Wireless application	Acronym	Role in wireless networking/Significance
Transmission Control Protocol/ Internet Protocol	TCP/IP	Suite of communication protocols used to connect hosts on the internet. TCP/IP is built into the UNIX operating system making it the *de facto* standard for transmitting data over networks.
Media Access Control	MAC	Addresses that are allowed to communicate on the network. MAC address monitors who can and can not associate with the router. These are specific to each mobile communication device. Also known as *hardware address.*
Router (Wireless Access Point)	WAP	A device that forwards data packets along networks. A router is connected to at least two networks, commonly two LANs or WANs. Routers are located at gateways, where two or more networks connect.
Service Set Identifier	SSID	A 32 character unique identifier attached to the header or packets sent over a WLAN that acts as a password when mobile device tries to connect to router. Also referred to as *network name* as it identifies a wireless network.
Institute of Electrical and Electronic Engineers developed wireless security protocols	IEEE 802.11 based protocols	IEEE 802.11a/b/g IEEE 802.11 super-g, super-ag & pre-n
Multiple In Multiple Out	MiMo	Wireless technology that uses the 'multipath' technology to send out multiple data streams simultaneously and uses multiple antennas to sort out signals.
Wireless Security Protocols	WEP	Wireless Equivalent Privacy. Encryption algorithm built into the 802.11 standard. Replaced by a more robust WPA protocol.
	WPA	Wi-Fi protected Access. More secure encryption standard than WEP.
	VPN	Virtual Private Network. Provides a secure, dedicated path or 'tunnel' over an insecure network like an Internet or an in-house wireless network. Uses tunneling protocols like Point to Point (PPTP) or Layer 2 Tunnelling Protocol (L2TP).
	PAP	Port based authentication programs. Developed via the IEEE standard 802.1X. Applies to both wired and wireless networks.
	TKP	Temporal Key Protocol
Wireless Personal Area Network	WPAN-Bluetooth	Low-cost radio solution to transmit data and link notebook computers, PDAs, phones, printers, digital cameras. Developed into a standard 802.15 by IEEE. Can operate within a range of 10 meters when the transmitting power is 1 mwatt. Range increases to 100 meters if the power is increased to 100 mwatt.

or 5.8 GHz models. Another chief source of interference is competing Wi-Fi networks within the same building or neighboring business locations. A free utility like netstumbler[14] (www.netstumbler.com) can identify nearby networks and their channels. It is easier to switch to another infrequently used channel. Most companies have the brand names of the routers as SSIDs. A simple change of SSID will prevent overlapping of networks. Enabling WEP or WPA will significantly lower the speeds of the signal. Hence, it is better to start with a stronger signal to balance the loss of a signal with wireless security activation. Use of Mac address filters will prevent unauthorized users accessing the network.

Newer Add-on Standards (Designed to Enhance the Existing 802.11g)

1. Multiple Traffic Priorities

A standard currently being developed, 802.11e, allows for different traffic priorities. Time critical data such as streaming video or VoIP phone call is selectively transmitted before less important messages such as e-mail or web pages. It is expected a sub-set of this standard called WMM (Wi-Fi Multimedia) will make its way into the consumer market late in 2005.

Connect to 192.160.01

DSL-604+

User name: ADMIN

Password:

2. Wireless Protected Access 2 (WPA2)

802.11i increases the security of a network by adding more encryption and network controls. A subset of this standard called WPA2 (Wireless Protected Access 2) is expected to appear in products by early 2005. Most existing routers will be upgradable to the new standard. The Wi-Fi Alliance (www.wi-fi.org) already started testing the products for WMM and WPA2 compatibility.[12] WPA2 is a big improvement on earlier wireless security standards, such as Wired Equivalent Privacy (WEP), which was clearly insecure. The WPA2 includes Advanced Encryption Standard, which supports 128-bit, 192-bit, and 256-bit keys. Components of WPA2 are included in the 802.11i standard, which was developed by the Institute for Electrical and Electronics Engineers (IEEE). The corporations that received approval to include WPA2 in their products via certification from the Wi-Fi Alliance include Atheros communications[5], Broadcom[8], Cisco systems, Intel, and Realtek.

Five Most Common Security Lapses in Wireless Access Point Set Up

The following are the most common Wi-Fi security lapses that might make the dental office network vulnerable.

1. Factory Set Password

While setting up the wireless router, it is important to change the factory set default password the first time the router is set up. Otherwise, an intruder may log into the router (using the default password) and be able to change the settings, giving them free access anytime.

2. Encryption

If the office PC or server's encryption is not enabled, the network will be broadcasting the passwords and other confidential information to anyone in range who cares to intercept them using free sniffer software like the AirSnort[15] to capture and analyze wireless data. (www.airsnort.shmoo.com)

3. Router Security

The router should be fortified with security that will prevent any unauthorized access to the patient data. The security protocols can be chosen depending on the availability and compatibility with the wireless router.[16,17] This is a most important and desirable feature when accessing web based remote dental consulations[18] on the network.

4. Overzealous Security Settings

Choosing and applying security settings has to be done with care as overzealous security set ups can virtually lock the user out of the networks. Setting up and re-configuring takes additional time and leads to inconvenience.

5. Open Network ID

The default network ID should be changed to a secure, non-proprietary name so the network is not "open" and "hacker friendly."

Improving Signal Strength

Signal strength can be substantially weakened by the medium it passes through or gets deflected from. Wireless signal strength should be checked in the wireless adapter's administration software at various locations within the office periodically. Metal, stone, concrete, water, and human beings absorb or reflect signals, while wood and glass let them pass through relatively unchecked. As a rule, the router has to be placed high in the room. Also, by moving any compact disc (CD) collection out of the network's operating area (that is stored within the vicinity of the access point), signal strength of 802.11g can be substantially improved according to a recent observation. CDs reflect the wireless radio signals as much as they reflect light.[13]

Future Wireless Networks and Advanced Functions

MIMO (Multiple Input Multiple Output)

By compressing data more efficiently and boosting the signal strength via the Multiple In Multiple Out (MIMO) technique signal range can be improved. When used with other Super G with MIMO wireless products, the wireless range can reach up to 8x farther coverage than standard 802.11g to provide thorough wireless coverage throughout your home or office. The newer versions of 802.11g can provide more than 250 Mbps of bandwidth. MIMO technology allows the antennas to transmit more than one signal at a time. The Super G with MIMO Wireless Router offers industry-wide backward compatibility to all 802.11g and 802.11b networking devices. Some examples include Linksys[11] Wireless G with SRX (Speed and Range eXpansion) and the D-Link's[6] DI-624M Super G with MIMO.

The brand new wireless standard, 802.11n, is not likely to be available for public use until 2006. Some manufacturers[6,9] have released what they term pre-n devices which use their proposed version of the standard. The products can eventually be upgradablewhen the 802.11n standard will become available for consumer use. Security features for these applications include an advanced firewall like Stateful Packet Inspection (SPI).[6]

Also referred to as *dynamic packet filtering*, stateful inspection is a firewall architecture that works at the network layer. Unlike static packet filtering, which examines a packet based on the information in its header, stateful inspection tracks each connection traversing all interfaces of the firewall and makes sure they are valid. An example of a stateful firewall may examine not just the header information but also the contents of the packet up through the application layer in order to determine more about the packet than just information about its source and destination.

For sharing broadband Internet access in the office, the web-based wizard supports virtually all operating systems to assist the users in getting connected to the Internet within minutes. Once the router has been set up, both wired and wireless users can: access the web; access streaming media; and transfer, print, and store files throughout the office network relatively easily. As the wireless networks are based on constantly changing technology, it is important to keep track of the available updates on the routers, adapters, and upgrades.

Wireless Personal Area Networks (WPAN) and Bluetooth

Wireless Personal Area Networks[19] (WPAN) are based on a relatively new technology that was developed by the Bluetooth Special Interest Group established in 1998, which included more that 2000 member companies. Blue tooth technology uses short-range radiofrequencies to transmit both voice and data. This cable-replacement technology wirelessly and transparently synchronizes data across devices and creates access to networks and the Internet within a range of ten meters. Extremely useful in offices when data transfer across a small area is required quickly and efficiently. The range can be extended to 100 meters if the transmitting power can be bumped up to 100 *megawatt* from 1 *megawatt*. Bluetooth radios operate in the unlicensed Industrial Scientific Medical (ISM) band at 2.4 GHz and employ frequency-hopping (FH) spectrum to reduce interference and fading.

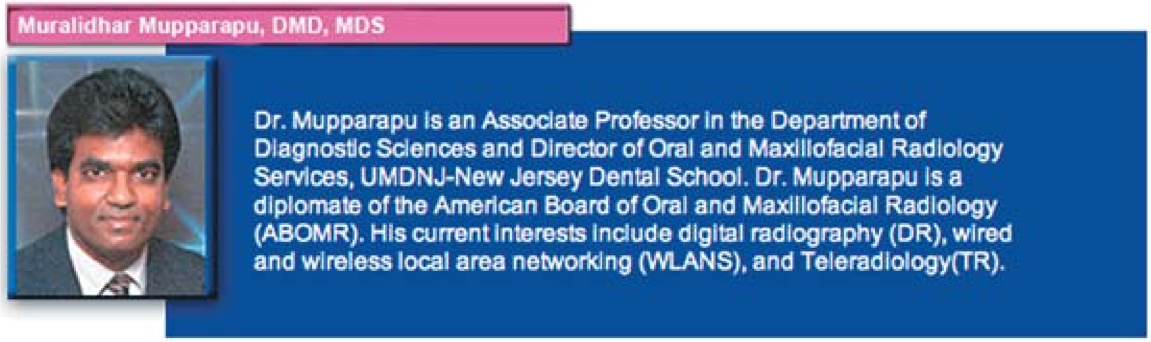
Summary

Amidst the implementation of HIPAA security protocols on April 20, 2005 and the accelerated deployment of IEEE 802.11 super G, Super AG, Super G +MIMO, and 802.11 pre-N in the consumer market, the networked Dentist as an end user and a high-tech consumer will have a hard time keeping abreast of the changes on the technology front. Unless the dental office periodically upgrades the existing networking components and standards, data transfer in the office via wireless deployment or remote access to the patient data might be less than ideal. Knowledge of the current wireless standards and security protocols will make the dentist a well-informed consumer.

References

1. Chen D, Soong S-J, Grimes GJ, et al. Wireless local area network in a prehospital environment. BMC Medical Informatics and Decision Making 2004; 4: 12.
2. Chin T. Is wireless technology ready to roll? Health data Manag 1998; 6:78-82, 84-6, 88-9.
3. Duncan R, Shabot MM. Secure remote access to a clinical data repository using a wireless personal digital assistant (PDA). Proc AMIA Symp 2000: 210-14.
4. Mupparapu M. Arora S. Wireless networking for the dental office: current wireless standards and security protocols. J Contemp Dent Pract 2004;5:155-62.
5. Available at: www.atheros.com Accessed December 20, 2005.
6. Available at: www.D-Link.com. Accessed February 15, 2005.
7. Available at: www.netgear.com. Accessed February 15, 2005.
8. Available at: www.Broadcom.com. Accessed February 15, 2005.
9. Available at: www.belkin.com. Accessed February 15, 2005.
10. Available at: www.Buffalotech.com. Accessed February 15, 2005.
11. Available at: www.Linksys.com. Accessed January 10, 2005.
12. Available at: www.Wi-Fi.org. Accessed February 15, 2005
13. Waring B, Brandt A, Baguley R. The ultimate wireless guide. Nov 2004; 94-105. Available at : www.pcworld.com. Accessed November 30, 2004.
14. Available at: www.Netstumbler.com. Accessed February 15, 2005.
15. Available at: www.airsnort.shmoo.com. Accessed February 15, 2005.
16. Mupparapu M. Wireless Local Area Network for the dental office. N Y State Dent J. 2004; 70: 28-31.
17. Mupparapu M, Binder RE, Cummins JM. Use of a local area network in an orthodontic clinic. Amer J Orthod Dentofacial Orthoped. 2005 Jun;127(6):756-9.
18. JC Stewart, Mupparapu M, DL Stewart, et al. Remote Dental Consultation: Image Testing for Diagnostic Capability. J Dent Edu 1999; 63: 66.
19. Bluetooth: The leading edge in wireless personal area networking. Available at: www. Symbol.com. Accessed April 22, 2005.

About the Author



Muralidhar Mupparapu, DMD, MDS

Dr. Mupparapu is an Associate Professor in the Department of Diagnostic Sciences and Director of Oral and Maxillofacial Radiology Services, UMDNJ-New Jersey Dental School. Dr. Mupparapu is a diplomate of the American Board of Oral and Maxillofacial Radiology (ABOMR). His current interests include digital radiography (DR), wired and wireless local area networking (WLANS), and Teleradiology(TR).