

		Georgia Technology Authority	
Title:		Small Office Home Office (SOHO)	
PSG Number:	G-06-001.01	Topical Area: Security	
Document Type:	Guideline	Pages: 14	
Issue Date:	04/01/06	Effective Date: 04/01/06	
POC for Changes:	GTA Security		
Synopsis:	To establish guidelines that encourage wise decisions when engaging in the usage of wireless technologies for the teleworker who is "working from home."		

STAKEHOLDERS

Name	Stake in Project	Organization	Title
Patrick Moore	Executive Sponsor	Office of the Governor (GOV)	Deputy Chief Operating Officer
Tom Wade	Business Owner	GTA	Chief Executive Officer
Charlie Sasser	Executive Sponsor of Work Group and Wireless Trials	GTA	Director of Support Services
Kimberly Gordon	Subject Matter Expert	GTA	Enterprise Architect
	Executive Committee - State of Georgia Agencies		
Wireless Oversight Committee	Hanna Hecke, GOV Tom Maier, BOR Randall Thursby, BOR Jim Flowers, BOR Mike Hall, DOE John Stewart, DHR Dee Ford, DEcD	Frank Howard, DTAE Mike Nixon, GPB Tony Mazza, P&P Cigdem Delano, GTA Renee Herr, GTA Steve Nichols, GTA Suhas Uppalapati, GTA Robert Woodruff, GTA	Executives from Various Agencies
ISO Council	Defining and verifying security requirements	State of Georgia Agencies	All Information Security Officers (ISO)
CIO Council	Final approval for operational turnover and Implementation	State of Georgia Agencies	All Chief Information Officers (CIO)
	Team Members - State of Georgia Agencies		
Wireless Standards Work Group	Bruce Bailey, DHR Rory McClure, DHR Walter Tong, DOE Geoff Catron, DTAE Steve Ferguson, DTAE Matt Sanders, GaTech Dan Brown, GEMA Chip Eberhart, GPB Mike Nixon, GPB	Eric Harris, GSP Brent Williams, KSU ¹ Bob Grafals, GTA Chuck Jordan, GTA Denise Techmeier, GTA, Program Technical Writer Jim Mollohan, GTA, Program Business Owner Wray Hall, GTA	Wireless Experts

Title:	Small Office Home Office (SOHO)
--------	---------------------------------

PURPOSE

To define the guidelines for teleworkers to use of wireless technologies deployed at an employee's home.

INDUSTRY STANDARD

The dominant standards to date have been the 802 standards series developed by the Institute of Electrical and Electronic Engineersⁱⁱ (IEEE). Any use of wireless strategy should comply with the most current version of the IEEE standards. The current version of 802.11 can be found at <http://grouper.ieee.org/groups/802/11/>. To further standardize the use and deployment of SoHo in the State of Georgia's environment, the following areas are clarified in this policy adoption: Default Settings, Cell Sizing, SSID Naming usage, Cloaking, MAC Filters, Encryption, Static IP, Common Security Practices (document settings, computer on/off, etc.), Mobile IP, WPA issues, VoIP and Software Interdependencies.

Although many government entities have already started using wireless technology, the intent of this document is to outline areas that need to be reviewed and explain areas that need to be considered on initial deployment.

The following standards are in commercial, office and industrial use: IEEE's 802.11a, 802.11b, 802.11g and 802.11i. These standards will serve as the de facto WLAN and SoHo standards. This document will be updated as applicable standards are ratified by IEEE.

IEEE 802 Standard	Description
802.11a	- Mandates support for data rates of 6, 12, and 24 Mbps - Works only in 5 GHz Unlicensed National Information Infrastructure (UNII) ⁱⁱⁱ Bands

ⁱⁱ IEEE, pronounced I-triple-E, was founded in 1884 as the AIEE. The IEEE was formed in 1963 when AIEE merged with IRE. IEEE is an organization composed of engineers, scientists and students. The IEEE is best known for developing standards for the computer and electronics industry. In particular, the IEEE 802 standards for local-area networks are widely followed.

ⁱⁱⁱ The 5 GHz bands are made up of three separate 100 MHz-wide bands which are used by 802.11a compliant devices. The FCC restrictions on these bands include for UNII-1 (5.15 GHz to 5.25 GHz) has the maximum output power of 40mW and the devices used in the band are restricted to indoor use. UNII-2 (5.25 GHz to 5.35 GHz) is specified at 200mW of output power and devices can be used indoors or outdoors. UNII-3 (5.725 GHz and 5.825 GHz) is specified to 800 mW and devices are outdoor, long-distance links.

IEEE 802 Standard	Description
802.11b	<ul style="list-style-type: none"> - Specifies Direct Sequence Spread Spectrum (DSSS) technology - Mandates support for data rates of 1, 2, 5.5 and 11 Mbps - Works only in 2.4 GHz Industrial, Scientific, Medical (ISM)^{iv} Bands
802.11g	<ul style="list-style-type: none"> - Specifies Orthogonal Frequency Division Multiplexing (OFDM) and DSSS technology - Mandates support for data rates of 6, 12, and 24 Mbps OFDM - Supports 6, 9, 12, 18, 24, 36, 48, 54 Mbps OFDM - Works only in 2.4 GHz ISM Band
802.11i	<ul style="list-style-type: none"> - Specific to wireless LAN security - Specifies 802.1x / EAP, AES and other technologies introduced to enhance security beyond 802.11 - WPA v1.0 is a stop-gap standard from the WiFi Alliance - WPA v2.0 will be fully 802.11i compliant

A significant challenge in providing wireless access is the protection of the computer networks connecting the wireless devices. These challenges include ensuring that:

- . • Only authorized users are allowed access to the network;
- . • Confidential information is secure during data transmission; and,
- . • The network is available and protected against malicious attacks.

^{iv} ISM is an acronym for Industrial, Scientific and Medical. This refers to the unlicensed radio bands which are typically unused due to interference from medical, industrial and scientific equipment. Technologies such as Bluetooth and Wireless LANs use these bands since no governmental approval is needed for transmission, making it a great deal cheaper. Whilst interference is still an issue, technologies for overcoming it are built into most technologies using these bands.

GUIDELINES

To address the risks associated with wireless computer networks, the State of Georgia has established a wireless network access policy (Policy 9.4.2). The policy requires agencies to take "appropriate steps, including the implementation of strongest-available encryption, user authentication, and virus protection measures, to mitigate risks to the security of State of Georgia data and information systems" the State of Georgia's standards require agencies to develop a wireless LAN Implementation Procedure Plan, assess the risks posed by a wireless network, mitigate those risks, and conduct periodic reviews to ensure that the network is secure. The standards prohibit open unsecured wireless network access technology. The ISO Council has adopted the National Institute of Standards and

Technology (NIST) 800 series as the security guidelines. Wireless security is specifically addressed in the following NIST standards:

- . • NIST 800-18 Guide for Developing Security Plans for IT Systems
- . • NIST 800-46 Security for Telecommuting and Broadband Communications
- . • NIST 800-48 Wireless Network Security: 802.11, Bluetooth and Handheld Devices

Security options:

- o Use IPsec^v-based encrypted-tunnel VPNs for security. Because of IPsec's strong encryption, it is useful for remote access VPNs. Small networks of fewer than 20-30 sites can use shared keys to initialize IKE, but managers of large networks must resort to other methods, i.e. PKI (public key infrastructure) for distributing keys to all sites and users; OR
- o Use SSL^{vi}-based encrypted-tunnel VPNs for security. The SSL protocol is a higher-layer security protocol that includes client and server authentication and data encryption for a limited set of applications (web, eMail, news and file transfer). SSL is suited to remote access and extranets because it is relatively simple to deploy; OR
- o Use the public Internet without a VPN. Some applications, such as Microsoft Exchange / Outlook can provide its own encryption. If the user application suite is limited to applications that can provide their own standards-based encryption, then it may not be necessary to further encrypt the traffic between the mobile device and the enterprise.

Use 802.3f, specification of Power over Ethernet (PoE), to enhance AP operation via a stable power source and to simplify the installation process throughout the enterprise.

Wireless Local Area Networks (WLANs) should at the minimum implement, WPA (WiFi Protected Access) for security, but full 802.11i compliance is a standard with components and equipment that can adhere to 802.11i.

For areas not mentioned in this section, seek guidance in the external sources mentioned in the "Standards" section and the State of Georgia's WLANs standards.

^v IPsec imposes significant management requirements on network managers, due to its dependence on IKE (internet key exchange) protocol.

^{vi} SSL is secure socket layer

Title:	Small Office Home Office (SOHO)
--------	---------------------------------

SOHO (small office / home office) or home users need to enable security on their wireless networks. Encryption based on WiFi Protected Access (WPA), along with advanced authentication techniques will protect network traffic and initial access. The client/server model should be deployed to authorize only those clients given specific permission to access the LAN.

The following areas need to be considered when deploying wireless technology in a small home office or small agency.

- Change the default settings on all devices. Using the vendors default settings is analogous to leaving the front door of the house always open.
- Change the device's administrator login name, the admin login password, the SSID and default IP address.
- Adjust the power settings of the wireless gateway to a lower power for the waves to travel a shorter range. However, make sure that the power settings are enough to properly provide signal coverage for the mobility needs. In some devices the lower power is achieved through the "adjust antenna transmit power" setting. If the capability is not available on a wireless router, physically locate the unit in the center of the house and away from the windows.
- Use a network name (SSID) that cannot clearly identify the teleworker, such as a family surname or street address.
- Enable the "closed network" or disable the "broadcast SSID" features on the wireless device. This will cloak^{vii} the network being used by the teleworker.
- Apply MAC Filters by entering the allowed MAC addresses for the wireless cards to deny access to other cards that are not listed.
- All SOHO wireless networks should deploy encryption of TKIP (Temporal Key Integrity Protocol). The access unit and the wireless cards must be WPA certified.
- Implement common sense security practices on all computers that will have wireless access. This should include:
 - o Installing virus protection software and download the virus signature files on a regular basis
 - o Disabling file sharing on computers unless absolutely necessary
 - o Installing personal firewalls on every computer
- Document settings for SSID, WEP keys, TKIP passphrases, IP settings, MAC filters, channel, and power settings.
- Turn off wireless network when it is not in use.
- Service choices:
 - o Use mobile data services (1XRTT or EV-DO) if the wireless connection is always on. The data rates which can range from 40 Kbps to 500 Kbps, allow more data-intensive applications to be run on the mobile client; OR

^{vii} Cloaking is masking a name or identity of the wireless device to keep other devices from copying the identity for hacking. This will keep the wireless gateway from being recognized and / or located.

- o Use circuit-switched mobile services (TDMA/CDMA/HSCSD) if switch wireless connections are available. Circuit-switched mobile data services are billed based on the time that user devices are connected to the network. For occasional use, such as periodic checking of eMail or application execution, this can be a cost-effective solution. Security should be provided based on either IPsec or SSL; OR
- o Use low-earth orbit (LEO)^{viii} satellite-based services when there is not suitable wireless connection available. When network access is required in geographically remote locations, services provided by LEO satellite systems such as Iridium or Globalstar may be required. Security should be provided based on either IPsec or SSL. Unlike traditional mobile systems, these systems may require the user to be located outdoors to receive a strong signal.

1.1 ACCESS POINTS

- Some APs allow controlling access based on media access control address of the network adapter trying to associate with it. If the media access control address of the adapter is not in the table of the AP, it will not be available for association. If the access point has this feature, enable it and add the media access control addresses of the network adapters that are being used.
- Use APs and network adapters that support 128-bit WEP and have flashable firmware^{ix}.

1.2 RISK MITIGATION

In mitigating the risks associated with wireless computer networks, all state agencies should:

- Have an IT security policy that addresses wireless computer network related issues. A thorough, well-enforced policy can protect an agency from unauthorized access as well as unnecessary performance degradation. Policies, standards and guidelines for all state agencies should forbid unauthorized access points and ad-hoc networks that can circumvent network security.

^{viii} LEO systems fly about 1,000 kilometers above the Earth (between 400 miles and 1,600 miles) and, unlike GEOs, travel across the sky. A typical LEO satellite takes less than two hours to orbit the Earth, which means that a single satellite is "in view" of ground equipment for a only a few minutes. As a consequence, if a transmission takes more than the few minutes that any one satellite is in view, a LEO system must "hand off" between satellites in order to complete the transmission. In general, this can be accomplished by constantly relaying signals between the satellite and various ground stations, or by communicating between the satellites themselves using "inter-satellite links."

^{ix} Allows the AP to be upgraded when new security enhancements are developed.

Areas to consider when reviewing office installation:

- Was the system deployed using user based authentication? This will secure the wireless connection, allow easy revoking of privileges, offer usage of static devices and achieve usage of 802.1x or VPN.
- Was a bluesocket, SSL or IPsec VPN approach used? This will encourage VPN termination close to the AP, supports 802.1z, and enables hybrid deployment of APs.
- Is the site survey information available? Were directional antennas used? This will minimize the amount of RF spilling.
- Are there any backdoors in the system? Check with a wireless sniffer, directional antenna and WiFi card with (internal channel hopping, external antenna connection, etc.). Do a "black box^x" and "white box^{xi}" testing. This will keep intruders from impersonation.
- Are anti-virus, personal firewalls certificates and mutual authentication in use?
- Who can reset APs and are the APs physically secure? Do APs have strong passwords?
- Are static IP addresses being used?
- In general has proper security configuration been used to allow network administrators to find vulnerabilities and / or capture wireless packets? Does the system:
 - o Track beacon packets to find all access points
 - o Determines SSID and AP name
 - o Track probe packets and probe responses
 - o Track data packets
 - o Determine link encryption packets, firmware versions and authentication packets.
- Is the system using secure protocols? Are EAP, TKIP and MIC or their equivalents in use?

Black Box testing includes coverage map, physical security of AP, SSID review, use of encryption, channel separation, unpredictable user names / passwords and denial of service.

^{xi} White box testing includes use or avoidance of VLANs, no servers on wireless VLAN, redundancy, what is on the wire once logged in, automatic access to wireless and broadcast key rotation.

EVALUATION CRITERIA

Before deploying SoHo systems for teleworkers, the following areas should be considered:

Evaluation Criteria #1: What is the geographic reach required for the remote access service?

The impact of remote access service selection increases with the geography covered by the nomadic user. The alternatives of wireless services range from local area services based on IEEE 802.11 hotspots to mobile data services (circuit-switched data and packet-switched data) to packet radio networks. Most of the mobile phones carriers have interoperability agreements with other wireless service providers to allow roaming between carrier networks. Selection of a wireless data network is similar to choosing a mobile voice service, where geographic reach is an issue.

Evaluation Criteria #2: What security mechanisms are required over the remote access connection?

Remote access services provide basic user ID / password security. One security feature included is the ability of the server / service provider to encrypt password information so that user passwords are not transmitted in the clear across the public network infrastructure. Consider end-to-end software-based encryption services such as those used by firewall vendors to create VPNs or hardware-based encryption devices placed at both ends of the connection.

Evaluation Criteria # 3: How much bandwidth is required to support the services required by remote users?

The bandwidth that is required to support the application accessed by the remote user may determine the preferred connectivity mechanism.

Evaluation Criteria # 4: How costly is the remote access alternative?

As with all services, the cost associated with implementing and maintaining the remote access service is a large factor which leads to an evaluation of whether the remote access service (such as an encrypted-tunnel VPN service) should be outsourced or deployed by the enterprise. These costs need to be analyzed from a technical and financial perspective. Intangible costs, such as those related to maintenance and management, need to be included.

Evaluation Criteria # 5: What is the viability of the selected service provider?

It is essential to examine the financial state of any carrier or ISP before selecting it to support remote access users and to monitor that financial state.

TERMINOLOGY

DSSS Direct Sequence Spread Spectrum is one of two types of spread spectrum radio, the other being [frequency-hopping spread](#)

	<p>spectrum. DSSS is a transmission technology used in local area wireless network transmissions where a data signal at the sending station is combined with a higher data rate bit sequence, or chipping code, that divides the user data according to a spreading ratio. The chipping code is a redundant bit pattern for each bit that is transmitted, which increases the signal's resistance to interference. If one or more bits in the pattern are damaged during transmission, the original data can be recovered due to the redundancy of the transmission.</p>
Hotspots	<p>Wireless LAN (local area network) that provides Internet connection and virtual private network (VPN) access from a given location. For example, a business traveler with a laptop equipped for WiFi can look up a local hot spot, contact it, and get connected through its network to reach the Internet and their own company remotely with a secure connection. Increasingly, public places, such as airports, hotels, and coffee shops are providing free wireless access for customers.</p>
iDEN	<p>iDEN (Integrated Digital Enhanced Network) is a mobile communications technology that provides its users with the benefits of a trunked radio and a cellular telephone. iDEN places more users in a given spectral space, as compared to analog cellular systems, by using Time Division Multiple Access (TDMA). Six communication channels share a 25 kHz space. Some competing technologies place only one channel in 12.5 kHz. Data (such as paging, text messaging and voice communications) are supported by iDEN. iDEN is a technology with no clear path for high speed wireless data.</p>
Interface	<p>A protocol of behavior that can be implemented by any class, anywhere in the class hierarchy. An interface defines a set of methods, but does not implement them. A class that implements the interface agrees to implement all the methods defined in the interface, thereby agreeing to certain behavior.</p>
MAC	<p>The Media Access Control address is a unique numeric identifier that is programmed into a wireless network interface card by the manufacturer. Some manufacturers allow this identifier to be reprogrammed by the user, therefore it must be assumed that the MAC address can be copied electronically (spoofed).</p>
Mobile	<p>Specification of physical and medium access control layers of an air interface for interoperable mobile broadband wireless access systems. These systems operate in licensed bands below 3.5 GHz, optimized for IP-data transport, with peak data rates per user in excess of 1 Mbps. This specification supports various vehicular mobility classes up to 250 Km/h in a MAN environment and targets spectral efficiencies, sustained user data rates and numbers of active users that are all significantly higher than those achieved by existing mobile systems.</p>
OFDM	<p><i>Orthogonal Frequency Division Multiplexing</i>, an FDM modulation technique for transmitting large amounts of digital data over a radio wave. OFDM works by splitting the radio signal into multiple</p>

smaller sub-signals that are then transmitted simultaneously at different frequencies to the receiver. OFDM reduces the amount of crosstalk in signal transmissions. 802.11a WLAN, 802.16 and WiMAX technologies use OFDM.

RADIUS

RADIUS (Remote Authentication Dial In User Service) is an AAA (authentication, authorization and accounting) protocol for applications such as network access or IP mobility. It is intended to work in both local and roaming situations.

When you connect to an [ISP](#) using a modem, DSL, cable or wireless connection, you must enter the [username](#) and [password](#). This information is passed to a Network Access Server (NAS) device over the Point-to-Point Protocol (PPP), then to a RADIUS server over the RADIUS protocol. The RADIUS server checks that the information is correct using authentication schemes like PAP, CHAP or EAP. If accepted, the server will then authorize access to the ISP system and select an IP address, L2TP parameters, etc.

The RADIUS server will also be notified when the session starts and stops, so that the user can be billed accordingly; or the data can be used for statistical purposes.

RADIUS was originally developed by Livingston Enterprises for their PortMaster series of Network Access Servers, but later (1997) published as RFC 2058 and RFC 2059 (current versions are RFC 2865 and RFC 2866). Now, several commercial and open-source RADIUS servers exist. Features can vary, but most can look up the users in text files, LDAP servers, various databases, etc. Accounting tickets can be written to text files, various databases, forwarded to external servers, etc. SNMP is often used for remote monitoring. RADIUS proxy servers are used for centralized administration and can rewrite RADIUS packets on the fly (for security reasons, or to convert between vendor dialects).

RADIUS is extensible; most vendors of RADIUS hardware and software implement their own dialects.

The DIAMETER protocol is the planned replacement for RADIUS, but is still backwards compatible.

Teleworkers

Field workers, road worriers or nomadic personnel – Professionals who travel frequently, such as caseworkers, who spend the majority of their time out of the office. Whether they are organizational leaders, caseworkers, or other field representatives, they require access to the applications that enable them to collaborate with their colleagues and respond to their constituents. Field workers need access to the same applications as their peers in the office. They connect to customers and colleagues.

Corridor workers – Professionals who work in the office but spend most of their day away from their desks. Examples of these corridor workers include healthcare professionals and managers. They are usually dashing through the corridors from one patient or meeting to the next. They require access to information and applications while away from their desks, add-hoc collaboration with their colleagues, and a paperless environment. They spend most of their time away from the desk.

Telecommuters or SoHo users – Work at home at least 1 day a week. They often access organization applications and other resources from a home computer by using an Internet Service Provider broadband or dial-up connection. They need the same access to applications as their peers in the office, even though they access the applications through a public network. They have irregular access to the corporate network.

Field Technicians or untethered – State employees in various agencies who work in the field with a narrow focus of activity. Their activities tend to be centered around the collection and processing of data, or the delivery of enhanced services. Field technicians are out of the office a majority of the time. Examples would include delivery drivers, building maintenance, health inspectors, and other inspectors and regulators.

WiDen A software upgrade developed for **iDEN** enhanced specialized mobile radio (or ESMR) wireless telephony protocol. WiDEN allows compatible subscriber units to communicate across four 25 kHz channels combined for up to 100 kbit/s of bandwidth. The protocol is generally considered a **2.5G** wireless cellular technology.

WiFi Wireless Fidelity is another name for wireless devices running under the 802.11b standard, which operates in the 2.4 GHz range. The name is governed (or marketed) by the Wireless Ethernet Compatibility Alliance (WECA).

WiFi5, or WiFi 5, is a newer version for devices running under the faster 802.11a standard. It operates in the 5 MHz range.

Specifically, 5.15 MHz to 5.35Mhz for indoor use, and 5.725 MHz to 5.825 MHz for outdoor use.

WiFi-x is a generic name for devices that support 802.11b and 802.11a.

WMAN Metropolitan Area Networks (MANs) are large computer networks usually spanning a campus or a city. They typically use optical fiber connections to link their sites. For instance, a **university** or **college** may have a MAN that joins together many of their **local area networks** (LANs) situated around a site that is a fraction of a

square kilometer. Then from their MAN, they could have several [Wide Area Network \(WAN\)](#) links to other universities or the [Internet](#). Some technologies used for this purpose are [ATM](#), [FDDI](#) and [SMDS](#). These older technologies are in the process of being displaced by [Gigabit Ethernet](#)-based MANs in most areas. MAN links between LANs have been built without cables using either microwave, radio, or infra-red [free-space optical communication](#) links.

WiMAX WiMAX is another name for a set of broadband wireless communication standards, developed under IEEE 802.16, for metropolitan area networks. Originally called WirelessMANT, the name is governed (or marketed) by the WiMAX Forum. This forum was founded by a coalition of wireless companies including Intel, Proxim, and Nokia. (Nokia has now left.) WiMAX was ratified as a standard under the 802.16-2004 specification.

WiMAX is expected to compliment WiFi standards. It provides a wireless alternative to last mile local loops, such as T-1 links. WiMAX should also provide competition for broadband DSL and cable services.

Wireless Term used to describe telecommunications in which electromagnetic waves (rather than some form of wire) carry the signal over part, or all, of the communication path. Some monitoring devices, such as intrusion alarms, employ acoustic waves at frequencies above the range of human hearing; these are also sometimes classified as wireless.

WLAN A Wireless Local Area Network (Wireless LAN) is a computer network that allows a user to connect without a network cable. A laptop or PDA equipped with a wireless LAN card allows a user move around a building with their computer and stay connected to their network without needing to "plug in" with a cable. The most popular wireless LAN today is called an 802.11b network. Wireless LANs require an access point where all the wireless devices connect. This connection point connects the users to the wired network. The coverage of a wireless access point can span up to 100 m (330 feet) indoors.

Other names for wireless LANs are 802.11, or WiFi. There are also different versions of wireless LANs: 802.11b transfers data at speeds of up to 11 Mbps in the 2.4 GHz radio band. The next version, 802.11a, is supposed to transfer data at speeds up to 54 Mbps in the 5 GHz band. Wireless LANs are a successful and popular widespread technology that is being incorporated into many new laptops as standard equipment.

WPA WPA (WiFi Protected Access) is an interim standard by the WiFi Alliance. WiFi Protected Access is a specification of security enhancements that increases the level of data protection and access control for existing WiFi networks.

WPA will most likely be rolled into the eventual IEEE 802.11i standard.

WPA2 IEEE 802.11i (also known as WPA2) is an amendment to the 802.11 standard specifying security mechanisms for wireless networks (see WiFi). The draft standard was ratified on 24 June, 2004, and supersedes the previous security specification, Wired Equivalent Privacy (WEP), which was shown to have severe security weaknesses. WiFi Protected Access (WPA) had previously been introduced by the WiFi Alliance as an intermediate solution to WEP insecurities. It implemented a subset of 802.11i

WPAN Wireless Personal Area Network (WPAN) is a personal area network that is used for interconnecting devices centered on an individual person's workspace where the connections are wireless. Typically, a wireless personal area network uses some technology that permits communication within about a very short range, such as 10 meters. One such technology is Bluetooth, which was used as the basis for a new standard, IEEE 802.15.

A WPAN can interconnect all the ordinary computing and communicating devices that many people have on their desk or carry with them today. It can also serve a more specialized purpose such as allowing a surgeon and other team members to communicate during an operation.

A key concept in WPAN technology is *plugging in*. In the ideal scenario, when any two WPAN-equipped devices come into close proximity (within several meters of each other), or within a few kilometers of a central server, they can communicate as if they are connected by a cable. Another important feature is the ability of each device to lock out other devices selectively, preventing needless interference or unauthorized access to information.

The technology for WPANs is in its infancy and is undergoing rapid development. Proposed operating frequencies are around 2.4 GHz in digital modes. The objective is to facilitate seamless operation among home or business devices and systems. Every device in a WPAN will be able to plug in to any other device in the same WPAN, provided they are within physical range of one another. In addition, WPANs worldwide will be interconnected.

WWAN A Wireless Wide Area Network (Wireless WAN), covers a much more extensive area than wireless LANs. Coverage is generally offered on a nationwide level with wireless network infrastructure provided by a wireless service carrier (for a monthly usage fee, similar to a cellular phone subscription). While wireless LANs are used to allow network users to be mobile within a small fixed area, wireless WANs are used to give Internet connectivity over a much broader coverage area. For instance to meet the requirements of users such as business travelers or field service technicians. Wireless WANs allow users to have access to the Internet, e-mail,

and corporate applications and information while away from their office. Wireless WANs use cellular networks for data transmission. A portable computer with a wireless WAN modem connects to a base station on the wireless networks via radio waves. The radio tower then carries the signal to a mobile switching center, where the data is passed on to the appropriate network. Using the wireless service provider's connection to the Internet, data communications are established to an organization's existing network. Wireless WANs use existing cellular telephone networks, so there is also the option of making voice calls over a wireless WAN. Both cellular telephones and wireless WAN PC Cards have the ability to make voice calls as well as pass data traffic on wireless WAN networks.