

Wireless MAXg Technology

MAXimizing range, performance, security and simplicity for 802.11g networks



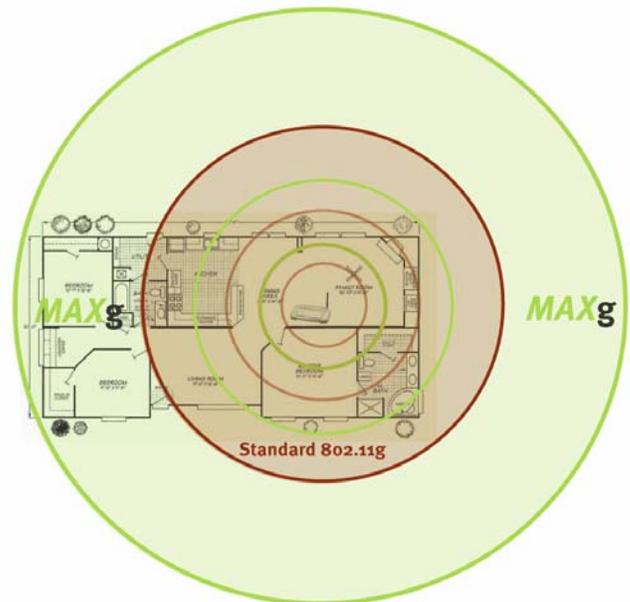
Technology Note

Wireless technology has undoubtedly become a ubiquitous presence in our computing environment, whether it's while conducting business in the office or enjoying a little leisure time online at home. The 802.11g wireless standard is the current standard for wireless networking ratified by the Institute of Electrical and Electronic Engineers (IEEE). By implementing wireless networks based on standards, rather than proprietary solutions, you are assured of a broad range of compatibility and consistent performance.

U.S. Robotics now offers a complete line of Wireless MAXg™ products that take the 802.11g standard a step further. These improvements go beyond the 802.11g standard and include 50% better wireless range than standard 802.11g, an even greater signaling rate of 125 Mbps*, a suite of advanced security features, and full compatibility with all 802.11g 54 Mbps and 802.11b 11 Mbps products. The following sections will discuss not only the 802.11g wireless standard, but also the improvements incorporated into the U.S. Robotics Wireless MAXg line of products.

Better Reception Sensitivity = Greater Range

One of the biggest problems with wireless is the performance throughout the whole of the house or office. Wireless signals get weaker the further away from the 'base station' you get. 802.11g has systems built in which 'downshift' the speed as the signal gets weaker. This results in slower connections as you move around the area covered. The ideal product should be able to receive signals at a lower level without downshifting or slowing down. USR have designed into the MAXg product range some extra capabilities to boost the wireless signals before they are converted back into data. Technically this is improving the receive sensitivity allowing the product to work at higher speeds over greater distances. The added advantage of MAXg's increased receive sensitivity is that it works enhances any other product. The enhancements that deliver this performance also work with any 802.11g signal, so your existing network will also benefit from MAXg technology.



* Actual speeds may vary due to environment and distances between wireless clients and access points

† Base on KeyLabs independent testing. Full report available at www.usr.com/maxg

Power Consumption

Wireless on laptops frees the user to make the most of the freedom that a laptop gives. However the biggest part of the weight of a laptop is the battery. Making efficient use of this battery and not having to carry spares batteries is very important to users. U.S. Robotics Wireless MAXg technology is designed for reduced power consumption as compared with other wireless devices, to improve the battery life of laptop PCs—certainly the mainstay of any traveling business people. The technology built into MAXg uses the absolute minimum power necessary. To ensure that all users benefit from reduced power requirements, the default configuration is set to use the MAXg technology ensuring that all users get the benefit without having to configure anything!

Performance – Data Throughput and Signaling Rate

One of the first things a purchaser of wireless networking wants to know is how fast the product is. Typically, this is expressed in a number, such as 54 Mbps or 11 Mbps; however, there's more to it than that when it comes down to true 'speed'.

In order to understand the true capabilities and efficiencies (as well as inefficiencies) of any network, wired or wireless, a distinction must first be made between two commonly misunderstood networking terms: data throughput and signaling rate. Data throughput is the actual 'amount' of data transmitted (upstream) and received (downstream) by a wireless product, while the signaling rate, or data rate, represents a theoretical maximum. So, while wireless networking products are often classified according to its standards-based signaling rate, such as 54 Mbps for 802.11g, the actual data throughput, or data being transmitted, is often just a fraction of the signaling rate's theoretical maximum.

Data throughput can be limited due to a number of important environmental and product-specific factors, including:

- Distance between Wireless devices: access points (APs) or routers and wireless clients (PCs, laptops, etc.)
- Transmission power levels
- Building and home materials
- Radio frequency interference
- Signal propagation
- Antenna type and location

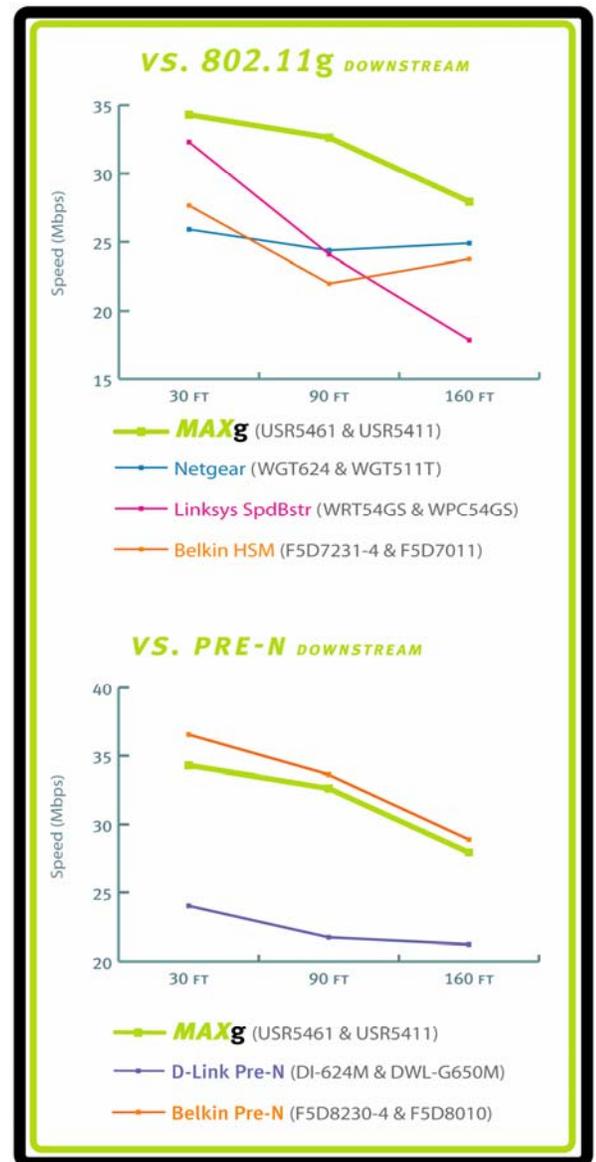
So, even though 802.11g wireless networking products are capable of a 54 Mbps signaling rate, the practical, or 'actual', data throughput rate will be significantly lower.

The new U.S. Robotics Wireless MAXg portfolio of products is actually capable of delivering signaling rate performance comparable to 125 Mbps*. Importantly, this performance boost occurs over a single wireless channel, eliminating the interference that often results when using other products that boost speed by using multiple channels simultaneously. This performance boost is over twice as fast as standard 802.11g, and 600% faster than 802.11b solutions.

The charts above show the throughput rates for U.S. Robotics MAXg products[†], at various distances, as compared to other 802.11g 'accelerated solutions' and Pre-N solutions, discussed briefly below.

* Actual speeds may vary due to environment and distances between wireless clients and access points

† Base on KeyLabs independent testing. Full report available at www.usr.com/maxg



Multiple In Multiple Out, or MIMO is one technology advances expected to become part of the 802.11n standard, which is anticipated to be finalized in late 2006/early 2007. In advance of the standard, some vendors are promoting Pre-N solutions that feature MIMO. These multiple radio products are significantly more expensive than MAXg (typically twice as much), and as is evident from the chart, provide little or no increased performance.

Security

Security is an obvious concern with any network: wired or wireless. Communication over a traditional wired network is over physical wires, security is often built into the physical infrastructure. WLANs operate over radio signals, so the same security measures will not necessarily apply. To address the unique nature of wireless data, there are a number of security features that a WLAN user can take advantage of to limit network susceptibility to hacker attacks, vandalism, and even corporate espionage, including:

- Wi-Fi Protected Access 2 (WPA2)/802.11i
- Wi-Fi Protected Access (WPA)
- 802.1x network authentication
- Wired Equivalent Privacy (WEP)
- Disable Broadcast SSID
- MAC address authentication

Wi-Fi Protected Access 2 (WPA2)/802.11i

Wi-Fi Protected Access 2 (WPA2) is based on the IEEE 802.11i standard and provides an encryption mechanism using Advanced Encryption Standard -Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (AES-CCMP). This provides a level of data privacy required by many financial and governmental institutions. WPA2/802.11i also provides a more current code set and support for wireless voice by preventing signal latency and the dropping of the voice content when roaming.

WPA2 is capable of running in two modes: WPA2-enterprise and WPA2-personal. WPA2-enterprise mode includes the entire set of WPA2 requirements and support for 802.1x/EAP-based authentication, while WPA2-personal mode is primarily for small businesses and home environments that require less complex key management schemes.

WPA2/802.11i is completely backward compatible with Wi-Fi Protected Access (WPA).

Wi-Fi Protected Access (WPA)

Wi-Fi Protected Access (WPA) is similar to WPA2/802.11i in many respects. The main difference between WPA and WPA2 is the type of encryption used: RC4/TKIP for WPA and AES-CCMP for WPA2. Both WPA and WPA2 are derived from 802.11i, with WPA2 being the latest version of the two.

WPA uses 802.1x network authentication and Temporal Key Integrity Protocol (TKIP) encryption measures to create either a 'pair-wise' key for the client's computing session running in enterprise mode; or for home mode sessions, the user simply enters a master key, onto each AP and PC on the wireless network. The pair-wise key is then distributed to the client and AP.

Upon successful authentication, TKIP then alters the single static 40-bit WEP security key into multiple dynamic 128-bit security keys. In essence, TKIP replaces the single repeatedly used WEP key with approximately 500 trillion other possible keys.

The U.S. Robotics Wireless MAXg family of products includes both WPA2 and WPA for maximum security and a greater level of interoperability with other wireless devices.

802.1x Network Authentication

802.1x is an authentication method that forces an individual client (laptop or desktop PC) attempting to log on to a WLAN access point (AP) into an unauthorized state by sending the AP an Extensible Authentication Protocol (EAP) start message. The AP requests the identity of the client, and the client, in turn, sends its identity to the AP and then to an authentication server. The authentication server checks the identity of the client and responds with either an accept or reject message. 802.1x network authentication is part of the 802.11g wireless standard and included in all 802.11g compliant wireless standard products, including the entire U.S. Robotics Wireless MAXg line.

Wired Equivalent Privacy (WEP)

Wired Equivalent Privacy (WEP) uses 64- and 128-bit encryption and is the cipher scheme designated for use in 802.11a, 802.11b, and 802.11g networking. WEP encrypts the data transmitted over a WLAN, protecting the once vulnerable communication between the client and access point. When combined with traditional security measures (password protection, authentication, encryption, virtual private networks), WEP can be very effective. All U.S. Robotics Wireless MAXg products include 64- and 128-bit WEP encryption.

Disable Broadcast SSID

A Service Set Identifier (SSID) is a uniquely assigned alphanumeric designator/name (from 1 - 32 bytes) that is used to identify a WLAN, ensuring that wireless devices will connect to the proper WLAN when multiple WLANs are operating in close, overlapping proximity. This identifier is broadcast and thus visible to wireless clients within range.

The U.S. Robotics Wireless MAXg Router (models 5461 & 805461) and Wireless MAXg Access Point (models 5451 & 805451) both come with Disable Broadcast SSID, which blocks the broadcast of this identifier so it is invisible to most random wireless devices. This provides another layer of wireless protection, since clients typically need to 'associate' with a particular SSID.

MAC address authentication

Some access points (or wireless routers that include access points) allow users to specify exactly which Media Access Control (MAC) addresses can communicate with the network. A MAC address is a hardware address that uniquely identifies each node of a network. Every network adapter in the world has a unique MAC address. By strictly specifying only those MAC addresses that can attach to a network, unauthorized users can be denied. MAC address authentication does just that. The network's base station (access point) maintains a database of authorized MAC addresses. Only those devices with authorized MAC addresses are allowed onto the network. The U.S. Robotics Wireless MAXg Router (models 5461 & 805461) and Wireless MAXg Access Point (models 5451 & 805451) both support MAC address authentication.

SureStart™ Installation Wizard

The U.S. Robotics MAXg line of wireless products isn't just rich on features and high on performance, it's also easy to install and use. All U.S. Robotics MAXg products include our exclusive SureStart™ Installation Wizard to ensure you harness all the power and capabilities MAXg has to offer.

Unique in the industry, SureStart seamlessly installs your MAXg PC Card, USB or PCI Adapter, if appropriate a MAXg Router, validates wireless connections, and helps to easily configure security. Complex WPA2 security is as easy as enabling security and typing in a pass phrase. PPPoE and cable modem detection are built in to make configuring your Internet connection a snap. Whether your networking needs are relatively simple or incredibly complex, U.S. Robotics

U.S. Robotics MAXg SureStart Installer

U.S. Robotics

Configure Your Wireless Security

Please enter a network name and pass phrase. Wireless devices will need to know the network name and pass phrase of your router in order to establish a connection with it.

The network name (also known as an SSID) is the name of your wireless network.

The pass phrase is used to secure your router from unauthorized wireless devices. It must be between eight and sixty-three characters long. U.S. Robotics recommends that you treat your pass phrase like a password and use a combination of alphanumeric characters that is not easy to guess (such as "5Rock2Fish95and" or "200ogs933Trol").

Network name:

Secure the router against unauthorized access (recommended)

Method: **WPA and WPA2**

Pass phrase:

Input a simple pass phrase to set up powerful security!

MAXg and SureStart™ will make short work out of setting you up and ensuring you get the most from your network.

Compatibility

Importantly, while MAXg Technology is unique to U.S. Robotics family of wireless products they maintain complete compatibility with standard 802.11b and 802.11g wireless solutions. This compatibility extends to many 802.11g accelerated products also. MAXg products also improve the range and performance of non-MAXg products, although not to the same degree.

U.S. Robotics Wireless MAXg Technology Portfolio

U.S. Robotics offers a total high-speed wireless networking solution incorporating our exclusive MAXg technology, with increased range, speed equivalent to 125 Mbps performance, unsurpassed security features, great product compatibility, and the simplicity & ease of the SureStart™ Installation Wizard.

Wireless MAXg Router—Models 5461 & 805461

The Wireless MAXg Router is ideal for sharing high-speed Internet access among multiple computers. Capabilities include:

- Full-featured router with 4-port Ethernet switch, , and high-security firewall protection
- Complete suite of security measures, including Wi-Fi Protected Access 2 (WPA2/802.11i), WPA, 802.1x Authentication, 64/128-bit WEP encryption, advanced Stateful Packet Inspection (SPI) firewall, support for VPN pass through, MAC address authentication and SSID disable
- USB port and Integrated print server that turns any USB printer into a network printer that can be shared among all network users[†]

Wireless MAXg Access Point—Model 5451 & 805451

The Wireless MAXg Access Point has the power and features to turn any wired network into a high-performance wireless network that extends the reach of the Internet throughout your home or office. Capabilities include:

- Removable swivel directional antenna that easily detaches for customizable performance
- Suite of security measures, including Wi-Fi Protected Access 2 (WPA2/802.11i), WPA, 802.1x Authentication, 64/128-bit WEP encryption, support for VPN pass through, MAC address authentication and SSID disable

Wireless MAXg PCI Adapter—Model 5417

The Wireless MAXg PCI Adapter lets users wirelessly tap into the power of an entire network from their desktop computer—an ideal solution for those PCs located off the network's beaten path. Connect your existing wired network to the wireless world for maximum networking performance.

- For use in desktop computers—quickly and easily installs into your PCI slot
- Seamlessly integrates your desktop into wired and wireless networks
- Removable swivel directional antenna that easily detaches for customizable performance

Wireless MAXg PC Card—Model 5411

The Wireless MAXg PC Card lets you take the power of an entire network with you—on your laptop computer. Stay connected to e-mail, shared files, and the Internet from wherever you need it.

- For use in laptop computers—simply plugs into your available Type II slot
- Seamlessly integrates your laptop into wired and wireless networks
- Unique low-power design gets the most from a laptop's battery to keep users online longer

Wireless MAXg USB Adapter—Model 5421

The Wireless MAXg USB Adapter provides flexibility for your desktop or laptop PCs to connect to a wireless network.

- For use with any computer's USB 1.1/2.0 port—laptop or desktop

- Compact design that easily fits in your pocket for instant wireless networking wherever you need it
- Swivel/directional antenna for better coverage

So whether you're starting off small, growing your network, or trying to communicate among multiple networks, U.S. Robotics has a solution that will fit your particular needs. U.S. Robotics continues to develop solutions to provide data access to both business professionals and home users, and the wireless networking solutions represented here are just some of our latest developments in keeping people connected worldwide—with information, entertainment, and each other.