U.S.Robotics

802.11g Wireless Turbo White Paper

Wireless technology has become an important tool in how we conduct business in the office and enjoy our leisure time at home. The 802.11g wireless standard is the latest to be ratified by the Institute of Electrical and Electronic Engineers (IEEE). It offers a number of improvements over the 802.11a and 802.11b standards, including 54 Mbps signaling rate, legacy 802.11b backward compatibility, and increased security features.

U.S. Robotics offers a complete line of 802.11g Wireless Turbo products that have taken the 802.11g standard a step further. These improvements go beyond the 802.11g standard and include an even greater signaling rate of 100 Mbps*, full compatibility with all 802.11g 54 Mbps, 802.11b+ 22 Mbps, and 802.11b 11 Mbps products at the highest speeds possible, and 256-bit WEP encryption for advanced security that goes beyond those of other 802.11g wireless products. The following sections will detail not only the 802.11g wireless standard, but also the improvements incorporated into the U.S. Robotics 802.11g Wireless Turbo line of products.

Data Throughput and Signaling Rate

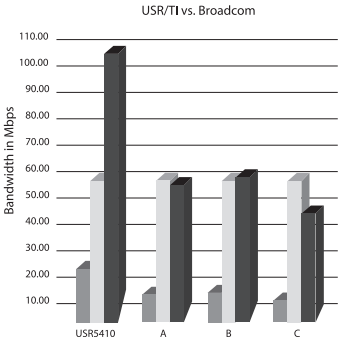
In order to understand the true capabilities and efficiencies (as well as inefficiencies) of any network, wired or wireless, a distinction must first be made between two commonly misunderstood networking terms: data throughput and signaling rate. Data throughput is the actual "amount" of data transmitted and received by a wireless product, while the signaling rate, or data rate, represents a theoretical maximum. So, while wireless networking gear is 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 Local Area Network (WLAN) devices: access points (APs) and network interface cards (NICs)
- Transmission power levels
- Building and home materials
- Radio frequency interference
- Signal propagation
- Antenna type and location

So, even though the new 802.11g wireless networking products available are capable of a 54 Mbps signaling rate, the practical, or"actual," data throughput rate is more likely to be in the 10 – 12 Mbps range. That is, except when using U.S. Robotics 802.11g Wireless Turbo networking products.

The new U.S. Robotics 802.11g Wireless Turbo portfolio of products with 100 Mbps Accelerator Technology is actually capable of delivering a signaling rate comparable to a 100 Mbps* wireless networking product, with all data transmission taking place on a single channel, leaving other channels open for a variety of other wireless devices. This translates to actual data throughput of 20 Mbps – nearly double that of other 802.11g products. This is due to the inclusion of exclusive U.S. Robotics 100 Mbps Accelerator Technology, and the key to this technology is Packet Binary Convolutional Coding.



	Average Total Throughput	Standard Bandwidth 54 Mbps	Theoretical Bandwidth
USR5410	20.50	54.00	103
A	10.43	54.00	52
B	11.02	54.00	55
C	8.33	54.00	42

Note that data throughput rates as stated herein (10-12 Mbps for 802.11g industry standard vs. 20 Mbps for U.S. Robotics 802.11g Wireless Turbo Products with Accelerator Technology) are based on practical, "real world" model office environments. Throughput rates can test substantially higher in a pristine environment (e.g., no walls, no computer interference, etc.) when using sophisticated testing equipment.

Packet Binary Convolutional Coding

Packet Binary Convolutional Coding (PBCC), sometimes known as 802.11b+, is a modulation/coding technique that was first developed for use in 802.11b networks as a means of doubling the signaling rate of the 11 Mbps standard to 22 Mbps while maintaining backward compatibility with legacy 802.11b 11 Mbps wireless equipment. U.S. Robotics first made full use of this advance in wireless technology by incorporating PBCC into its portfolio of 22 Mbps wireless networking products, resulting in a signaling rate of 54 Mbps

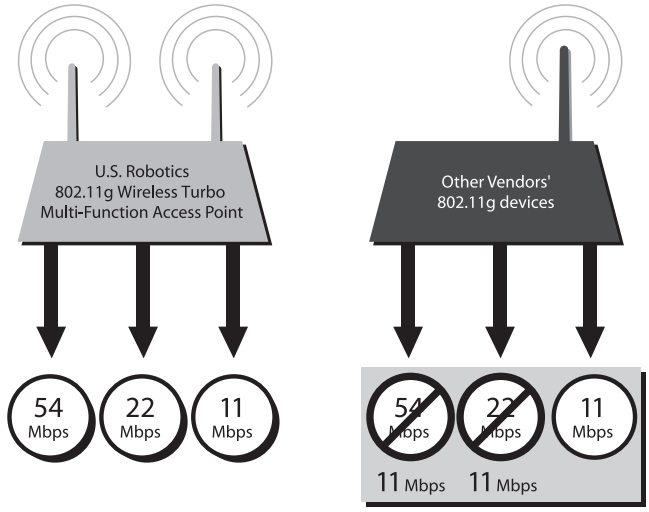
U.S.Robotics®

and comparable in data throughput to 802.11g wireless standardproducts. Though PBCC was not included in the final 802.11g 54 Mbps standard, it was included as an optional modulation technique and has since been incorporated into the U.S. Robotics 802.11g Wireless Turbo portfolio.

In its simplest form, PBCC works by reducing overhead (bandwidth used to transmit non-data) through the removal of extraneous information and optimizing transmission by using smaller data packets, cutting the response time in processing those packets, and thus, allowing for a greater amount of data to be transmitted between networked devices. Specific examples of overhead include:

- Protocol headers – carry information for controlling the device
- Frame interval times – allow users to gain access to the frequency band
- Error and flow control – ensure the integrity of the wireless transmission
- Received message acknowledgements – verify that messages were received correctly or need to be resent due to errors and/or message collisions

Some wireless networking products utilize "channel bonding," a method that combines two wireless data channels to effectively double data transfer speeds. One channel is reserved for transmitting data only, while the other channel is reserved for receiving data only. However, because two channels are used in the process, fewer channels remain available for other devices, reducing overall network capacity.



U.S. Robotics 100 Mbps Accelerator Technology, utilizing PBCC, uses only a single channel for data transmission to maximize capacity. Because PBCC uses the same type of protocol header as legacy 802.11b wireless devices, U.S. Robotics 802.11g Wireless Turbo products are fully compatible with all 802.11g 54 Mbps, 802.11b+ 22 Mbps, and 802.11b 11 Mbps standard products while delivering the best data throughput rates possible.

Compatibility

No small part of proper network design involves ensuring that clients and devices can access network data, send/retrieve e-mail, surf the Web, and perform other tasks with maximum efficiency. Network design becomes a much more complex issue when interconnecting both LANs and WLANs into a single seamless network. A major hurdle to overcome in WLANs is ensuring that each wireless device on the network achieves its optimal data throughput.

Until recently, the only way to ensure that each wireless networking device was achieving its optimal data throughput was to use wireless networking gear from only a single manufacturer utilizing a single wireless networking standard; e.g., 802.11a 54 Mbps, 802.11b 11 Mbps, or 802.11g 54 Mbps. This meant that users were "locked" into a single brand and technology standard, making network upgrades complicated and impractical. However, trying to maintain a WLAN that uses only gear from a specific manufacturer utilizing only a single wireless networking standard is also impractical and does not allow for upgrades to the latest high-speed technologies.

WLANs have become commonplace and wireless "hotspots" exist in airports, restaurants, and even in casual cafés. For example, many upscale cafés now offer WLAN services to their patrons. Assume the café is outfitted with an 802.11g 54 Mbps wireless standard access point (AP). The 802.11g standard is designed so that it can be used in a mixed mode environment and for backward compatibility with 802.11b 11 Mbps wireless products. So, for those users setting up their laptops utilizing 802.11b 11 Mbps wireless PC cards, the café's AP will be compatible.

However, this kind of compatibility will come at the cost of wireless speed optimization. The AP, upon sensing the 802.11b 11 Mbps PC card, will, in an effort to maintain a consistent speed throughout the WLAN, cause a network slowdown and will fall back to a data rate of 11 Mbps, irrespective to the other devices on the WLAN. This kind of network slowdown is caused by mixing different wireless products that utilize different wireless standards, also known as a mixed mode environment, and is a limiting factor for virtually any wireless network, from the smallest café to the largest enterprise office. And in a realistic working scenario, it is difficult to imagine any wireless network that utilizes a single manufacturer's gear utilizing a single wireless standard – it just isn't practical.

For the new U.S. Robotics 802.11g Wireless Turbo family of wireless networking products, such network slowdowns aren't a point of concern. In fact, U.S. Robotics 802.11g Wireless Turbo products eliminate network slowdown altogether and ensure that each wireless device on the network connects independently at that device's fastest speed possible. The same things can't be said for other competitive wireless products. Only U.S. Robotics offers full 802.11g 54 Mbps, 802.11b+ 22 Mbps, and 802.11b 11 Mbps wireless product compatibility. So, whether a wireless client is using the latest 802.11g gear, or a combination of 802.11g and 802.11b in a mixed mode environment, U.S. Robotics wireless networking solutions will continue to ensure maximum wireless network efficiency and security in any wireless network.

Security

Security is an obvious concern with any network: wired or wireless. Because communication over a traditional wired network is, by its very nature, 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. For business and enterprise users, as well as many home users, network and data security is of the utmost concern. To address this, there are a number of security features that a WLAN user can use to limit a network to hacker attacks, vandalism,

and corporate espionage, including:

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

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. U.S. Robotics 802.11g Wireless Turbo products include enhanced 256-bit WEP encryption that is not commonly available in the 802.11b and 802.11g standards for security up to 10 times greater than standard wireless networks. 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.

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. A base station will essentially broadcast its presence, which is then picked up by client PCs (both authorized and unauthorized).

Newly purchased wireless networking gear will come with a default SSID assigned. Default SSIDs should be changed immediately to avoid network hacking. The U.S. Robotics 802.11g Wireless Turbo Router (model 8054) and 802.11g Wireless Turbo Multi-Function Access Point (model 5450) both come with Disable Broadcast SSID which, when turned on, allow only those base stations and clients with matching SSIDs to associate with one another, blocking out unauthorized users that lack the correct SSID.

Wi-Fi Protected Access (WPA)

Wi-Fi Protected Access (WPA) extends the functionality of WEP by using 802.1x network authentication and Temporal Key Integrity Protocol (TKIP) encryption measures. What 802.1x network authentication does, depending on whether the application is in "enterprise mode" (for businesses) or "home mode" (for home users), upon user authentication, is to either create a unique "pair-wise" key, or master key, for the client's computing session running in enterprise mode; or for home mode sessions, the user simply enters a password, or master key, onto each AP and PC on the wireless network. The pair-wise key is then distributed to the client and AP where unique encryption keys are dynamically generated to encrypt the data packets being transmitted during that particular computing session.

Upon successful authentication, TKIP then alters the single static 40-bit WEP security key into multiple dynamic 128-bit security keys, strengthening the basic framework of WEP into a much more complex, secure form of encryption. In essence, TKIP replaces the single repeatedly used WEP key with approximately 500 trillion other possible keys that could potentially be used for each data packet and that will never be used more than once.

MAC address authentication
Some 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 802.11g Wireless Turbo Router (model 8054) and 802.11g Wireless Turbo Multi-Function Access Point (model 5450) both come with built-in MAC address authentication.

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, whereby the client sends the AP an Extensible Authentication Protocol (EAP) start message. The AP responds by sending an EAP requesting the identity of the client. The client, in turn, acknowledges by sending its identity to the AP, which, it then forwards to an authentication server. Using an algorithm, the authentication server checks the identity of the client and responds to the AP with either an accept or reject message. If the client is accepted, the AP will change the client's previously forced unauthorized state into an authorized state and grant network access. 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 802.11g Wireless Turbo line.

U.S. Robotics 802.11g Wireless Turbo Portfolio

U.S. Robotics offers a total 802.11g Wireless Turbo high-speed wireless networking solution that incorporates our exclusive 100 Mbps Accelerator Technology to provide the performance and data throughput rates equivalent to 100 Mbps* but with the unsurpassed security features, reliability, and greater product compatibility only available from U.S. Robotics.

802.11g Wireless Turbo Router – Model 8054
The 802.11g Wireless Turbo Router is ideal for sharing high-speed Internet access among multiple computers.

- 4 products in 1: 802.11g Wireless Turbo Access Point, 4-Port Ethernet Switch, Router, and Firewall
- Includes built-in MAC address authentication
- Removable antennas easily detach for upgrading or replacement

802.11g Wireless Turbo Multi-Function Access Point – Model 5450
The 802.11g Wireless Turbo Multi-Function Access Point is a professional-grade access point that has the power and features to make a wireless network out of an existing wired network and wirelessly extend the reach of the Internet throughout your home or office.

- 5 products in 1: Access Point, Bridge, Multi-Bridge, Client, and Repeater
- Allows full Simple Network Management Protocol (SNMP) management for network administration
- Removable antennas easily detach for upgrading or replacement

802.11g Wireless Turbo PCI Adapter – Model 5416

The 802.11g Wireless Turbo PCI Adapter lets users wirelessly connect to the power on an entire network from their desktop computer. Connect your existing wired network to the wireless world and start accessing the Internet from almost anywhere*.

- For use in desktop computers
- Included Site Survey feature makes finding the closest access point easy and simplifies wireless network configuration
- Removable antenna easily detaches for upgrading or replacement

802.11g Wireless Turbo PC Card – Model 5410

The 802.11g Wireless Turbo 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
- Included Site Survey feature makes finding the closest access point easy and simplifies wireless network configuration
- Unique low-power design gets the most from a laptop's battery to keep users online longer

Wireless Turbo USB Adapter – Model 2220

The Wireless Turbo USB Adapter instantly turns your desktop or laptop PCs into a secure wireless network.

- For use with any computer's USB 1.1 port
- Ideal for instant laptop or desktop wireless networking
- Compact design – fits in your pocket

U.S. Robotics wireless networking solutions are built upon proven technology and backed by an organization that is committed to the highest standards of product quality and customer satisfaction. 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.

* Capable of data throughput rates equivalent to 100 Mbps performance. Actual performance may vary depending on operating environment and distance between networked computers.

www.usr.com