



# WiBand Communications

Security in Fixed Wireless Networks  
White Paper - October 2009



## Table of Contents

Corporate Overview .....	3
WiBand's Commitment to Customer Satisfaction .....	3
Defining the Different Wireless Technologies .....	4
WiBand's Fixed Wireless Network Topology .....	5
Wireless Security in WiBand's Network.....	6
Proprietary Data Scrambling and Encryption.....	6
Subscriber Authentication .....	6
Backhaul and Distribution Network Connections .....	7
Summary .....	7

## Corporate Overview

WiBand Communications, established in 1999 and headquartered in Winnipeg, Manitoba, is a facilities-based data communications carrier and Internet Service Provider focusing on targeted Canadian cities and rural markets. We use state-of-the-art wireless broadband technologies and fibre optic facilities for cost-effective, rapid and reliable deployment of 1.5 Mbps to 200+ Mbps data service, internet gateway, web hosting and e-mail solutions. In addition to providing commercial services WiBand Communications also provides wholesale service to other telecommunications carriers and builds privately owned networks for government, municipal organizations, private companies, and education systems.

Stability is important, and we assure you that WiBand Communications is a financially sound company that is positioned well for future growth and opportunity. The strong management team at WiBand have provided the company with the leadership and vision to become one of the largest and most successful service providers in Western Canada.

## WiBand's Commitment to Customer Satisfaction

As a valued customer of WiBand, you will receive the commitment from our team to deliver reliable service that exceeds your expectations and allows your business to operate in a cost-effective manner. Some of the highlights that set WiBand apart in the industry are:

- Quality data and Internet services using carrier-grade products and technology
- Personalized customer support via our 24x7x365 Network Operations Center (NOC)
- Quick installation and provisioning of data and Internet services
- Cost-effective solutions tailored to your business needs
- Industry leading Service Level Agreement (SLA)
- Redundant and secure network

## Defining the Wireless Technologies

There are many different wireless technologies used for IP and data service in the marketplace today, however this document will focus on the two most prominently used in corporate networks which are Wi-Fi and Fixed Wireless. They are two very different technologies with vastly different feature sets and security mechanisms, and to understand the difference between them will assist in the understanding of how WiBand secures transmissions within it's network.

### Wireless LAN (Wi-Fi)

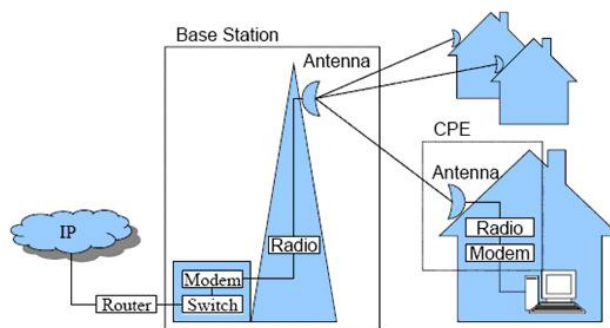
Typically referred to as Wi-Fi, this wireless technology was developed for use in small local area networks as a means of connecting network devices to the network without the use of copper or fiber optic cables. It has a major operational advantage of providing connections in situations where running cables may not be economically or physically possible, however the technology comes with several major disadvantages such as inadequate security features and interference problems. When using Wi-Fi products corporations need to be extremely concerned about the security of the transmissions in order to protect from an outside party gaining access to the network. Wi-Fi has garnered much attention worldwide due to it's tremendous success in the consumer market.

### Fixed Wireless

Defined as the operation of wireless devices or systems used to connect two fixed locations (e.g. buildings) with a radio or other wireless link. Fixed wireless services typically use a directional radio antenna on each end of the signal and signal transmissions occur through the air over a terrestrial microwave platform rather than through copper or optical fiber. Fixed wireless installations are typically an outdoor installation and connections can span very long distances, which is not the case for Wi-Fi based links. The wireless connection between the sites can be delivered either in a point-to-point configuration, or a point-to-multipoint setup which requires the base station radio to communicate with multiple subscribers simultaneously. Most fixed wireless products employ technology and security mechanisms that far exceed that of Wi-Fi based products and are considered to be much more viable for use in corporate networks.

## WiBand's Fixed Wireless Network Topology

In most cases, WiBand uses fixed wireless technology to provide Internet or data service to a location. This requires that a directional antenna be installed on the customer premise and pointed back towards a base station point of presence that is connected into the core IP network. The diagram below shows a typical wireless installation:



Typically a fixed wireless connection from WiBand requires that the path between the base station antenna and the customer premise antenna have clear line of sight. This clear optical path between sites along with proper link engineering, radio configuration, and installation from WiBand's technicians ensures that a strong signal will be received at the customer premise and that reliable IP communications into the WiBand core network can be established.

## **Wireless Security in WiBand's Network**

When using fixed wireless network connections it is important to understand that your data is travelling through the airwaves, and that the radios on either side of the link are responsible for transmitting this data in a secure manner that cannot be intercepted by an intermediate radio device. How does WiBand ensure that your data is secure? We do so by using the many advanced security features included in the radios that are installed at your site. Some of the features are:

### **Proprietary Data Scrambling and Encryption**

It is very important to note that the technology used within WiBand's network is not based on the Wi-Fi standard, nor it is not based on any of the standards commonly associated with Wireless LAN's. As a result of this, WiBand's base station sites will not allow a Wi-Fi client device to associate to it, and will not allow a Wi-Fi client to transmit or receive any data on the network. The scrambling technique employed by WiBand's radios involves proprietary patterns of sequencing and combining of each data byte with one of 256 scrambling bytes. This technique offers a significant level of over-the-air security. The proprietary nature of the scrambling technique permits only authenticated radios to intercept and de-scramble the data. For additional protection, most radios used in WiBand's network employ spread spectrum modulation and there is no simple demodulator on the market nor is one easily constructible that can receive signal.

### **Subscriber Authentication**

The WiBand wireless system is comprised of one or more co-located Access Points (APs) and one or more Subscriber Units (SUs). In order for information to pass between AP and SU, the AP must authenticate the SU. This is achieved through a password protected database system administered through the AP. Each AP contains a database of SUs that are authorized to communicate with the AP. The SU database, located within non-volatile memory of the AP must contain the unique MAC identification (ID) of each SU authorized for operation on the network. In addition to the MAC ID, a unique SU number identifies each SU. Similarly, each SU must be set up to associate with a specific AP (referred to as the AP ID) and a specific base location (referred to as the Base ID). In addition to the above, another layer of authentication is added to each data packet outbound from an AP; a scrambled identifier is encoded with the data packet along with a target SU "address". In the event an unauthorized or rogue SU is brought into proximity to the wireless network, it will not authenticate to the AP and it will be impossible for the rogue SU to gain network access.

## **Backhaul and Distribution Network Connections**

The connections between base station sites that lead to the core of the IP network are referred to as backhaul connections. WiBand uses licensed wireless microwave links operating in the 18 GHz and 23 GHz bands to deliver the high capacity connections required in our backhaul.

Each of these links have an associated license issued by the Government of Canada that reserves the channel they operate on in the surrounding area. Our use of licensed frequency ensures that no other transmitter will be able to interfere with the backhaul connections, and no other wireless device will be able to receive the signal from the backhaul radios. The end result of deploying licensed backhaul connections is that they allow us to transmit your data through the network efficiently and reliably without the concern of interference from competing signals.

## **Summary**

Applications, users, and businesses in today's marketplace demand secure network connections and you can be assured that the team at WiBand has designed a carrier-grade network that can deliver performance while maintaining security levels equal to or better than that of any other competing technology. The use of non-WiFi equipment with proprietary authentication, data scrambling, and encryption ensure that your data cannot be intercepted and stays secure throughout the transmission through our network. Our technology has proven itself in the market as a viable alternative and many large corporations including banks, government agencies, hospitals, schools, and finance firms have successfully and securely deployed WiBand connections throughout Western Canada.

If you would like more information on this white paper or have any questions about WiBand's products and services please contact your local WiBand Account Representative today!