



Security White Paper

March 2009



Table of Contents

| | |
|----------------------------------|----------|
| Security White Paper | 3 |
| Abstract | 3 |
| Towerstream Overview | 4 |
| Towerstream Difference | 4 |
| Wireless Concerns | 6 |
| Towerstream's Wireless Network | 6 |
| Towerstream's RF Security | 7 |
| Line of sight | 7 |
| Signal Theft | 8 |
| Physical Security | 8 |
| Vendor Security Overview | 9 |
| Redline AN-80i | 9 |
| Alvarion | 9 |
| DragonWave | 9 |
| BridgeWave | 9 |

Security White Paper

Abstract

The network world today can be a dangerous place. Network administrators need to worry about Viruses, Spybots and Denial of Service Attacks, to name a few. In addition, a company needs to maintain the integrity of their data and take all possible steps to protect their data whether being in house or being sent out on the network so it is not compromised.

Towerstream takes security very seriously and treats security as paramount when building out our Radio Frequency (RF) infrastructure. This whitepaper describes Towerstream's physical security and security standards in place at various hardware levels and the measures that Towerstream takes to ensure data cannot be compromised at the RF level.



Towerstream Overview

Towerstream is a leading fixed WiMAX service provider in the U.S., delivering high-speed Internet access to businesses in nine markets including New York City, Boston, Los Angeles, Chicago, the San Francisco Bay Area, Miami, Seattle, Dallas-Fort Worth, and the greater Providence area where the Company is based.

Towerstream delivers a reliable last mile solution. Unlike other internet service providers, Towerstream owns their entire network and is not dependent on the local exchange carrier network of phone wires or cable offering a faster installation seamlessly and securely for less money.

With Towerstream's guaranteed 99.99% uptime, we enable IT Managers to put what was once their top business concerns at the bottom of their list.

The Towerstream Difference

Towerstream delivers high quality symmetrical bandwidth to their customers with a faster install at a significantly lower price than other traditional broadband providers.

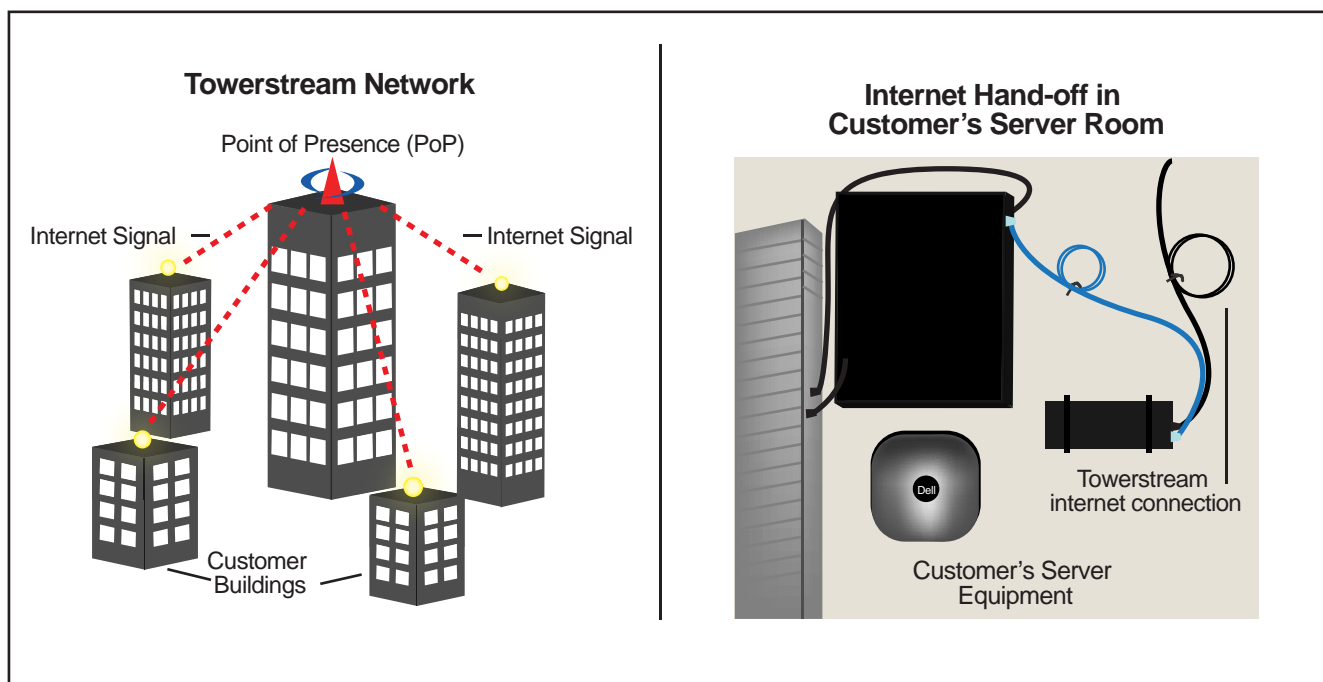
Towerstream's fixed wireless broadband network supports VoIP, bandwidth on demand, wireless redundancy, VPNs, disaster recovery, bundled data and video services.

Towerstream is an affordable alternative to traditional broadband solutions.

Towerstream's service reliability is backed by an industry-leading Service Level Agreement (SLA).

Using WIMAX technology, Towerstream delivers a wide variety of features including:

- Fast and Simple Installation:** By completely bypassing the local phone company and using multiple broadcast sites in several major cities, service is often installed in 3-5 business days or less.
- Speed and Scalability:** With bandwidth options ranging anywhere between 0.512Mbps and 1Gbps Towerstream can create the customized broadband solution to meet your business's needs.
- Guaranteed 99.99% Reliability:** Towerstream delivers a very reliable last mile solution. We are the first wireless broadband provider to offer the "Five 9's" Guarantee to our customers.



Wireless Concerns

Since the WiFi Alliance was formed in 1999, untethered access has become an acceptable and even preferred method of connectivity. Although WiFi was the genesis for transmitting high speed wireless data in the mainstream, the initial encryption methods such as Wired Equivalent Privacy (WEP) and WiFi Protected Area (WPA) were considered easily breakable. WiFi was designed for open access in the Local Area Network (LAN). Since it was relatively low power and short range, long distance security measures needed in the outside Wide Area Network (WAN) were not a concern.

Ironically, the same open access convenience that made WiFi popular has become the “defacto” concern for any wireless medium by security conscious end users. The methods for securing wireless traffic today meet or exceed the most stringent of standards.

Towerstream’s Wireless Network

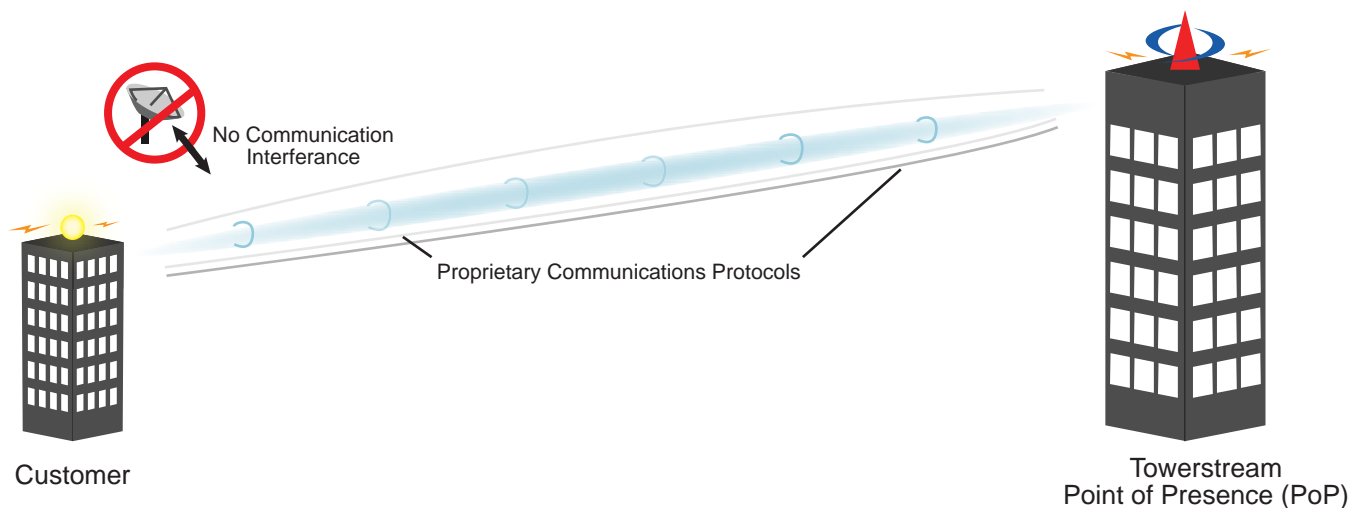
Towerstream deploys a combination of Fixed Wireless Networks and WiMAX (802.16e). Fixed Wireless Networks have been in production since the 1970s. They were primarily used for backhaul in voice networks for phone companies, government agencies, etc. One of the most popular questions is; “If the technology is so old, why are you still using it?” Similar to computers, the changes in size, speed and power have been dramatic. Radio’s that once could once only push 1.5Mbps of traffic with eight foot antennas can now push a Gigabit of traffic attached to a one foot antenna.

Towerstream's RF Security

Line of Sight

Unlike WiFi, the Towerstream RF devices do not advertise Service Set Identifiers (SSID's). Towerstream does not broadcast a frequency in 360 degrees. Towerstream service is considered "Line of Sight" (LOS). This means that a customer's antenna has to be pointed at a Towerstream facility and the corresponding Towerstream antenna has to be pointed at the customer. In order to interfere or intercept a signal, a potential intruder would have to be directly in that "Line of Sight". The intruder would have to have two antennas, one for each receiving end. Practically, an intruder would have to be hundreds of feet in the air to be in both data paths.

Even if the data could be captured and stored, the radio manufacturers utilize proprietary communication protocols at the RF layer. These proprietary modulation and protocol schemes make it virtually impossible to decipher even if the data is captured.



Signal Theft

One of the most common questions is: “If a person was to obtain equipment from the manufacturer, would they be able to compromise the infrastructure and/or steal service.” The short answer is, “No”. First, each piece of equipment is provisioned with a Towerstream link identifier. Secondly, every radio has a manufacturer specific identifier “burned-in” by the manufacturer. This can never be changed. Without both sets of ID’s matching, communication between the devices cannot occur.

Physical Security

All of Towerstream facilities are controlled access properties. Since the majority of our infrastructure is on roof tops, this is arguably the most difficult area of a building to compromise in this post 9-11 era. Since Towerstream's signal is out in the airwaves, the service cannot be compromised by a man-made disaster such as a broken telephone pole or a compromised street conduit. Comparatively, the customer side can be considered just as secure. For example, a typical T-1 generally terminates in a shared phone closet before it gets to the customer. Towerstream normally brings it service directly to the customer location bypassing common areas.

Vendor Security Overview

Redline AN-80i

- Proprietary RF modulation and communications protocol
- Proprietary encryption
- Primary and Secondary Authentication
 - o Hardware based identifier
 - o Towerstream configured authentication key

Alvarion

- Proprietary RF modulation and communication protocol
- Proprietary encryption
- Primary and Secondary Authentication
 - o Hardware based identifier
 - o Towerstream configured authentication key

DragonWave

- Proprietary RF modulation and communication protocol
- Proprietary data stream encoding
- Primary and Secondary Authentication
 - o Hardware based identifier
 - o Towerstream configured authentication key

BridgeWave

- Proprietary RF modulation and communications protocol
- 256-bit key length AES
- Cipher Block Chaining (128-bit blocks) conceals patterns