TeraGo Networks

Security white paper

TERAGO NETWORKS INC.

December 2007

Table of Contents

Executive Overview

Security on any type of network is of great concern to all end users and must be viewed as an integral part of every network. It is vital to an organization to maintain its security standards regardless of the medium of the connection (wire-line or wireless). TeraGo Networks Inc. understands the need to maintain the privacy and integrity of customer data and the Radio Frequency infrastructure that TeraGo uses is designed with security in mind. This whitepaper describes in detail the security that is built into TeraGo's network as well as the inherent security of Fixed Wireless Broadband technology. It explains the difference in network access philosophy in comparison to other wireless technologies and it outlines the security features of each hardware manufacturer TeraGo uses. Finally, it describes the overall security of the facilities that TeraGo has put in place.

TeraGo Networks Inc. Corporate Overview

TeraGo Networks Inc. has been providing Canadian businesses with carrier-grade wireless broadband and data communications services since 2001. TeraGo owns, manages and maintains its wireless IP network in major markets across Canada. It also serves an important and growing demand among businesses for network access diversity by offering customers wireless services that are redundant to their existing wire-line broadband connections. These services are provided utilizing state-of-the-art, secure wireless technologies which are vastly different from the wireless technologies that businesses would typically have experience with in the past.

TeraGo's Commitment to Service

High Capacity Broadband – we offer Internet access and data connectivity at speeds that typically exceed offerings from digital subscriber line (DSL) service providers and that are competitive with fibre-optic, cable based services;

Rapid Installation – our network is wireless, allowing us to install customers faster than our wireline competitors;

Excellent Customer Service – we focus on the needs of business customers by offering carrier-grade services which include a customer service and network operations centre available 24 hours a day, seven days a week and committed service levels backed by service level agreements;

On-Demand Scalability – our IP-based wireless network enables us to efficiently scale our broadband communication services to adapt to the requirements of our customers. As customer needs grow, we can increase their bandwidth seamlessly, typically without installation of additional equipment;

Network Access Diversity – with our wireless network, we offer truly redundant network access to existing wireline broadband connections.

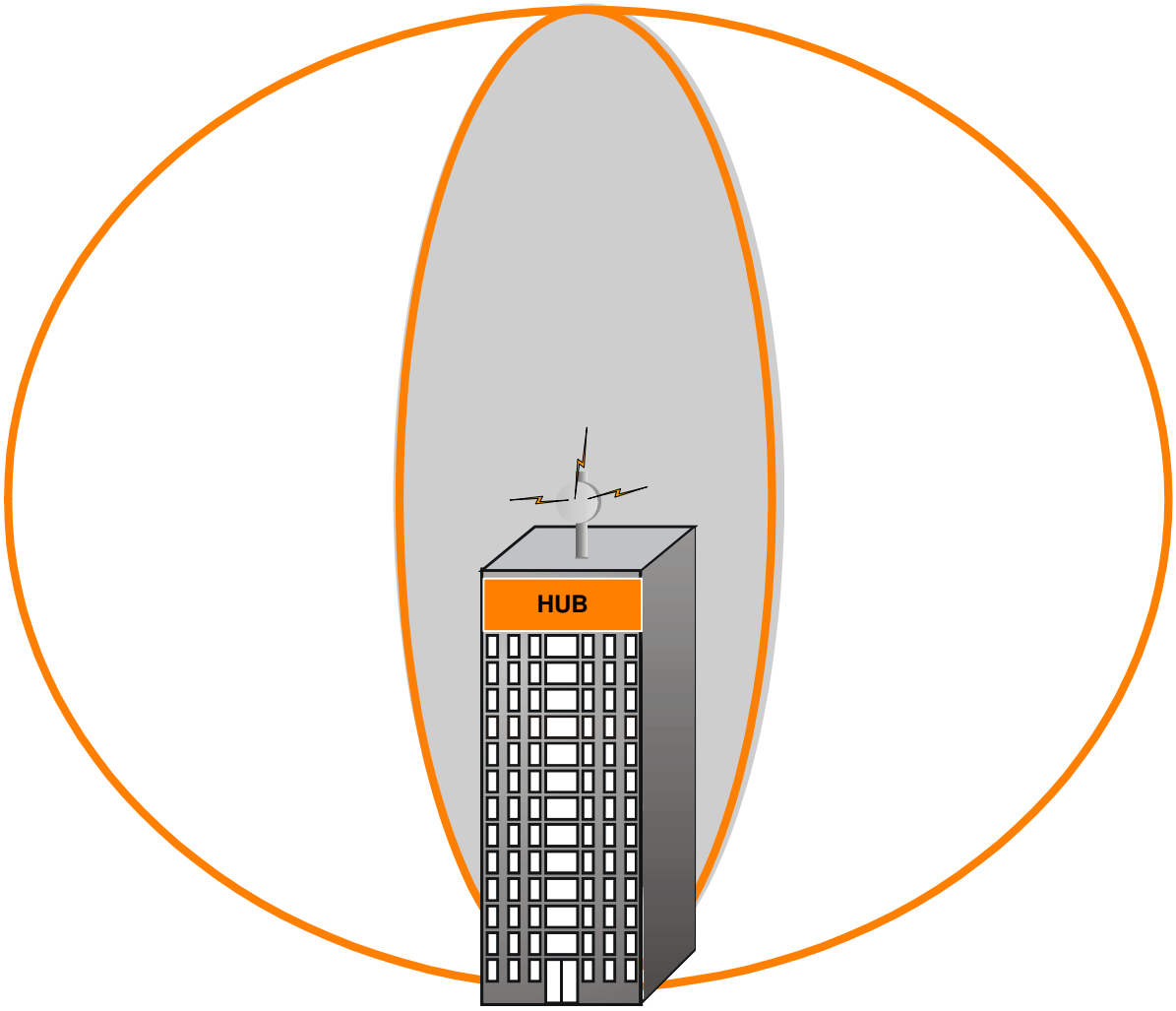
Fixed Wireless Networks Are Different From Other Wireless Networks

TeraGo's services are deployed using Fixed Wireless Broadband technology. Although this technology has been available over the past 20 years, it is not well understood by the business and consumer markets. 'Wireless' in the business market is generally understood as either wireless LAN technologies based on WiFi 802.11 standards or cellular technologies such as EVDO, GSM, etc. Fixed wireless systems have long been used for voice and data communications, generally in backhaul networks operated by phone companies, cable television companies, utilities, railways, paging companies and government agencies. Fixed wireless technology has continued to advance, utilizing higher frequencies and smaller antennas. These newer networks are also characterized by higher reliability and increased data and access security.

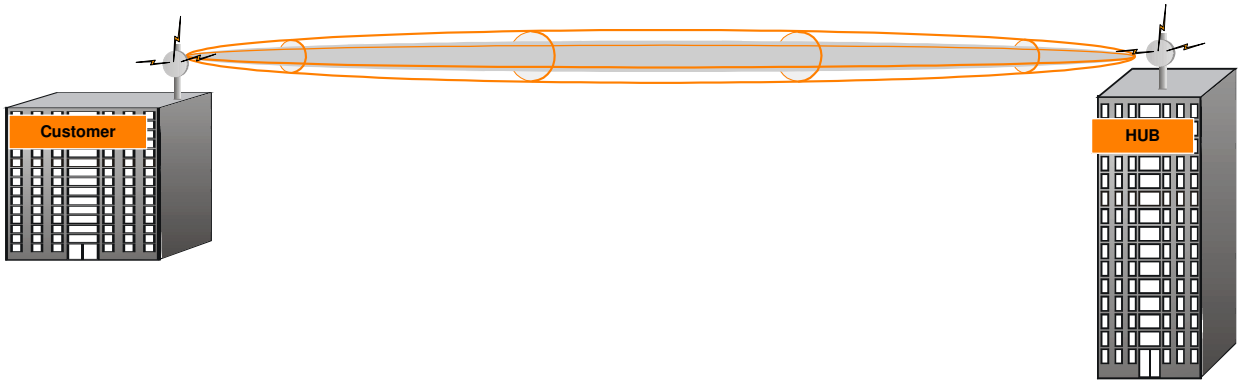
There are two fundamental differences between fixed wireless and the other wireless technologies: End User Network Access and Proprietary Communication Protocols.

End User Network Access – Fixed Wireless Is Different From Other Wireless

WiFi and cellular networks are designed to be easily accessible by users. The radios used are omni-directional (360 degree transmission) and operate in non-line-of-sight conditions (trees and buildings may be present within the signal transmission path). In the cellular environment, a provider's transmission equipment is located on a tower or building and the signal is accessible in every direction from that location. Users can access these networks within buildings and from any direction. Wireless LANs are based on the same principle of full access in any direction through obstructions. Essentially these are access networks whereby providers want to provide easy access for their customers.



Omni-Directional Technologies: WiFi, Cellular, etc.



Point-to-Point Technologies

The premise of Fixed Wireless is completely different: Fixed Wireless providers use directional, narrow beam, point-to-point antennas and radios that guarantee network access is available only to the specific customer who owns the communications link. Each radio at a customer location has a corresponding radio at the provider's hub site. In order to operate, these radios must be pointed directly at each other within the centre of the beam path with a clear, unobstructed line-of-sight. The physical configuration and the technology design of Fixed Wireless networks guard the integrity of customer data.

Proprietary Communication Protocols – Fixed Wireless Is Different From Other Wireless

WiFi and cellular access networks operate using standards-based radio frequency and network protocols that enable communication to occur between devices manufactured by different vendors. These protocols also enable the cellular network operators to offer services to customers when roaming (away from the home network). The mobile nature of WiFi and cellular access networks demands the use of standards-based protocols to allow connections between multiple devices and multiple networks. The fixed wireless user does not need mobility.

The Fixed Wireless Broadband technology used by service providers communicates over-the-air using a non-standard protocol that is designed to maintain security and optimize network performance and availability. Each wireless equipment manufacturer uses a proprietary, over-the-air protocol that makes it very difficult for any device to intercept and interpret data transmitted over the wireless link or to alter the protocol.

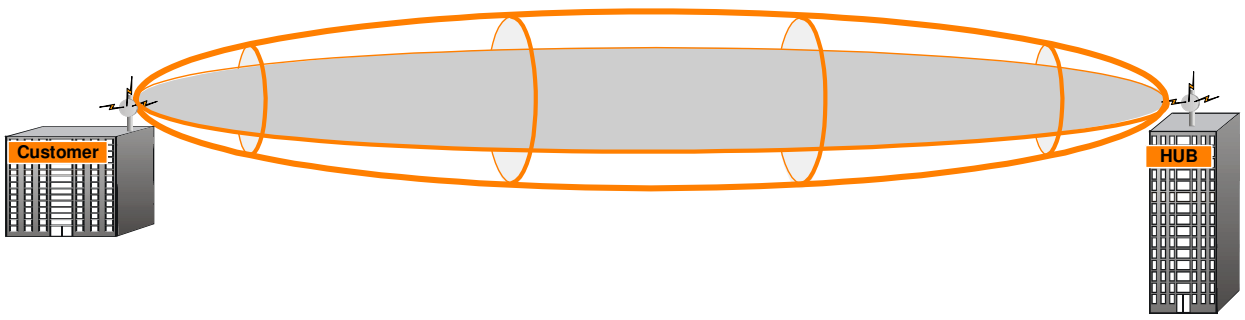
Essential Security Components of a Fixed Wireless Network

It is vitally important to TeraGo to ensure that all customer data traverses TeraGo's network both reliably and securely. TeraGo understands the need to maintain the integrity and privacy of all customer traffic. To this end, a number of security features have been implemented to ensure that customer traffic can only be accessed by the customer owning the circuit.

Line-Of-Sight

All TeraGo services are provided based on achieving clear line-of-sight. In order for the link to function, there must be clear line-of-sight. Every radio used by TeraGo is directional, narrow beam, point-to-point. Each radio on a customer site has a corresponding radio at a TeraGo hub site. These radios must be pointed directly at each other and positioned within the centre of the path of the beam. Any radio placed within the path but not in the centre of the Fresnel zone, will not be able to detect a consistent data stream due to a weakness of the signal.

Fresnel Zone



Fresnel Zone: In optics and radio communications, a Fresnel zone (pronounced FRA-nel Zone), is one of a (theoretically infinite) number of a concentric ellipsoids of revolution which define volumes in the radiation pattern of a (usually) circular aperture. Fresnel zones result from diffraction by the circular aperture.

The cross section of the first Fresnel zone is circular. Subsequent Fresnel zones are annular in cross section, and concentric with the first.

To maximize receiver strength, one needs to minimize the effect of the out of phase signals by removing obstacles from the RF Line-of-Sight (RF LoS). The strongest signals are on the direct line between transmitter and receiver and always lie in the 1st Fresnel Zone.

Proprietary RF Modulation and Communications Protocol

The communication protocols for Fixed Wireless Broadband radios are dependent on the manufacturer. All of the radios that TeraGo uses to provide service utilize a proprietary communications protocol that has inherent security built into the link. By utilizing a proprietary communications protocol over-the-air, TeraGo is able to ensure the security of customer traffic. In the unlikely event that the RF signal could be captured and stored, the actual data itself is protected by proprietary modulation and protocol schemes that would be next to impossible to decipher.

Encryption

All Fixed Wireless Broadband radios employ some form of cryptography or data manipulation. TeraGo utilizes a number of different manufacturers to deploy services and the encryption scheme is dependent on the manufacturer.

Link ID

Link ID is comprised of two parts. The first part is configured by TeraGo. Each RF link in the TeraGo network is given an ID “number” which is made up of bits. This ID number is programmed into the radio. If a radio was inserted in front of an existing link without the proper Link ID, then communication would be denied by the device. The second security element involves the hardware Link ID which is “burned-in” by the equipment manufacturer. This ID number cannot be changed without destroying the radio itself. The numbers must match in order for communication to occur.

Network Monitoring

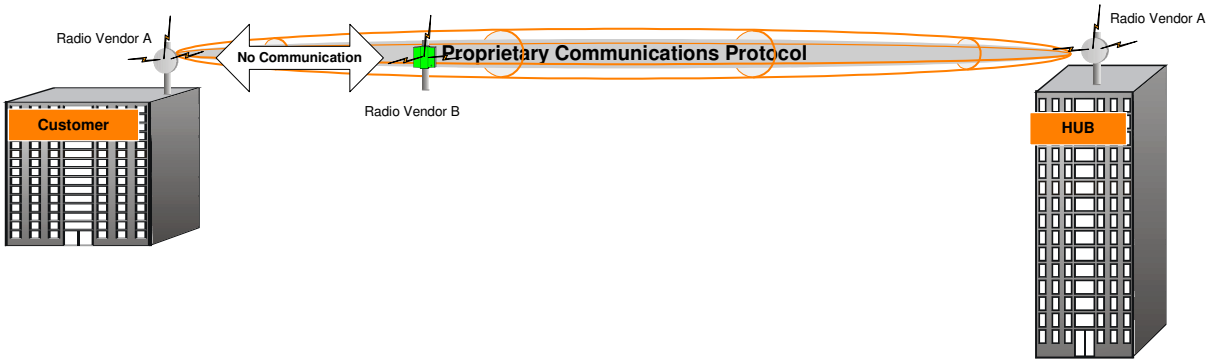
TeraGo has a 24 x 7 Network Operations Centre (NOC) that monitors network links and all TeraGo hub locations. Network operations constantly monitor signal integrity and network

security to ensure thresholds meet TeraGo's carrier-grade network availability performance of 99.999% network availability.

In the case of an attempted security breach of a customer's connection, the TeraGo Network Operations Centre would immediately receive alarms triggered by signal loss from an unwanted radio intrusion in the customer's RF path. If the problem cannot be fixed remotely, TeraGo will then deploy a technician to the customer's site. In addition, all hubs on the TeraGo network are physically secure and monitored for unauthorized access.

Radio Security in the TeraGo Network

TeraGo deploys Fixed Wireless Broadband radios at both the customer location and on the backbone of the network to provide Internet and data communications services. TeraGo uses "best-in-class" hardware manufacturers that have been proven in commercial and military grade applications. TeraGo utilizes a variety of hardware vendors to provide these services. Each vendor utilizes a proprietary communications protocol that has inherent security built into the link. By utilizing a proprietary communications protocol over-the-air, TeraGo is able to ensure the integrity of customer traffic. In the event that the RF signal could be "sniffed" and stored, the data would be indecipherable.



Backbone Security – Licensed Frequencies

TeraGo is the only entity legally assigned to use specific frequencies in the 11 GHz, 18 GHz, 24 GHz and 38 GHz frequency bands. This legal ownership of spectrum provides TeraGo customers with access to hundreds of spectrum licenses in Canada nationally that are reserved solely for TeraGo's network operations.

Last Mile Security – License-Exempt Frequencies

In addition to the security provided by proprietary air link protocols used in line-of-sight communications, security measures are also included in Media Access Control authentication and the encrypted transmission scrambling function that prevents the deciphering of transmissions.

Last Mile Local Loop Radios

The following “best-in-class” radios are used to connect a customer location to a TeraGo hub site. As noted in the equipment description, each radio uses a proprietary communications protocol designed to ensure customer data integrity is guarded and maintained.

Axxcelera AB Access

- Employs a proprietary RF modulation and communications protocol
- Link access to the radios is required at each end to provision
- Cryptography using a proprietary 43 bit scrambling sequence frames
- Link ID
- Permanent Virtual Circuit

Motorola Canopy

- Employs a proprietary RF modulation and communications protocol
- Encryption using 56 bit DES or 128 bit AES
- Secure Virtual Connection
- Colour coding
- MAC address authentication

Ceragon 4800

- Employs a proprietary RF modulation and communications protocol
- CCM/AES 128 bit encryption key – both payload and MAC address is encrypted
- Two point authentication:
    - Hardware based, link specific authentication
    - Administrator configured authentication key

Redline AN-50

- Employs a proprietary RF modulation and communications protocol
- 64 bit private key proprietary stream cipher
- Two point authentication:
  - Hardware based, link specific authentication
  - Administrator configured authentication key

DragonWave

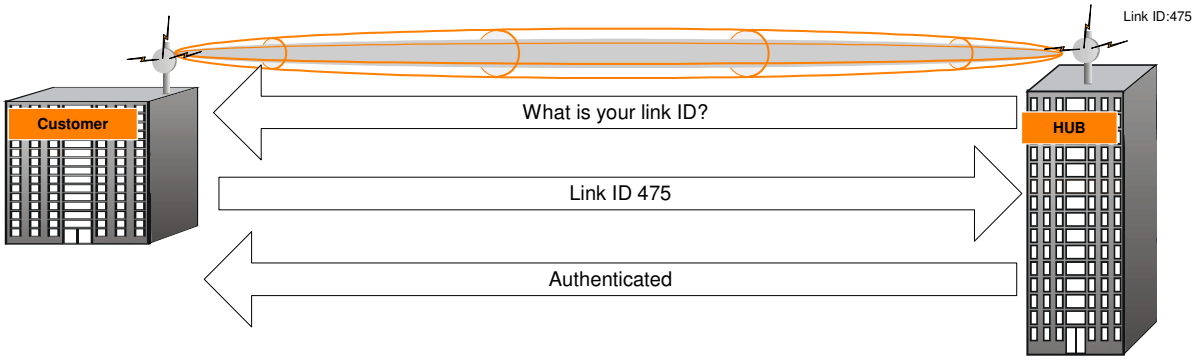
- Employs a proprietary RF modulation and communications protocol
- Proprietary data stream encoding into a seemingly random bit stream
- Two point authentication:
  - Hardware based, link specific authentication
  - Administrator configured authentication key

Backbone Radios

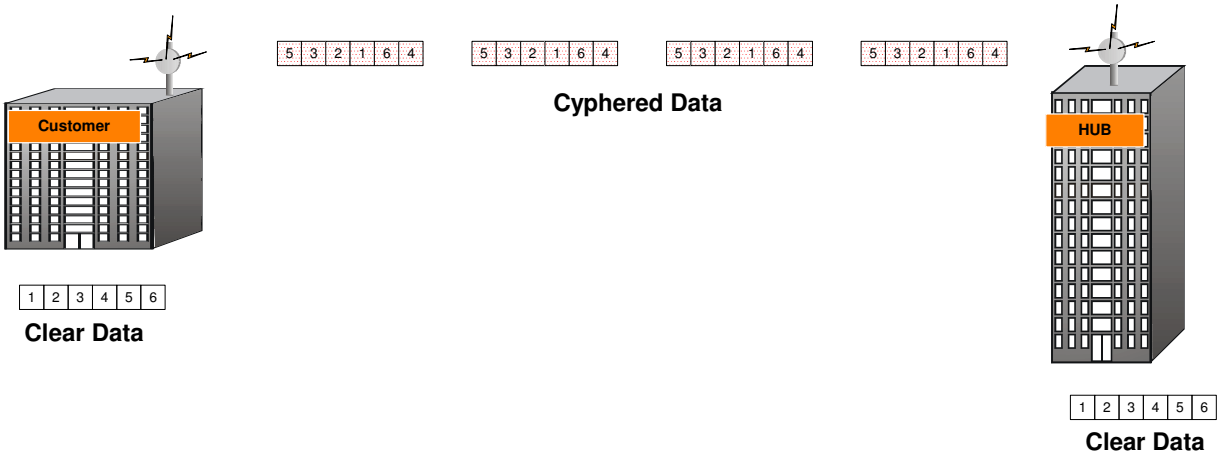
Ceragon 1500P

- Employs a proprietary RF modulation and communications protocol
- AES 256 bit encryption key – both payload and MAC address is encrypted
- Two point authentication:
  - Hardware based, link specific authentication
  - AES (Advanced Encryption Standard) algorithm, as specified by the FIPS 140-2 Level 2 Security standard. AES is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information.

The Federal Information Processing Standard 140 (FIPS) is a series of publications based on U.S. government computer security standards that specify requirements for cryptography modules. The current version of the standard is FIPS 140-2, issued on 25 May 2001.



Authentication Process



Data Cryptography Process

Summary

TeraGo Networks goes to great lengths to ensure that data transmission over its Fixed Wireless Broadband network is performed in a highly secure manner. Security is achieved via the technology deployed as well as link configuration within the network. There are many features within the TeraGo network that rival and even surpass the security of traditional wireline connections.

With respect to access options in the Fixed Wireless Broadband space, in order to gain access, the intruder must be on a roof, in the air, within line-of-site and in the centre of the transmission path of the radio. Once access to a fixed wireless network is gained, the proprietary communications protocols and data cryptography used render the data useless to the intruder. With wireline connections, the intruder requires access to the wire. In many cases, there are fibre pedestals outdoors and fibre and copper are aerially run into buildings on poles. Data that travels over wireline connections is clear, standards-based and unencrypted. Therefore once a wireline network is infiltrated, the data is open for inspection.

Thousands of customers rely every day on TeraGo's national network to transmit mission-critical, highly sensitive data. TeraGo is committed to providing customers with high speed, reliable and secure connections between customer offices and the Internet and will continue to be a true alternative to traditional wireline services.