SECURITY BRIEF

UNPARALLED SECURITY

There are wireless providers - and wireless providers. A poor network that sends signals over the airwaves can create the opportunity for a security risk in the form of data interception.

However, our network has the following techniques to provide protection at the physical and application layers of the network. The result is a highly secure and robust system without wireless eaves-dropping or malicious user attacks.

Proprietary Wireless and Data Formats

We use proprietary communications signalling and data-link protocols that make it almost impossible to intercept or spoof the wireless data streams.

Transmission Encryption

Encryption is deployed on every wireless link.

MAC Address Authentication

Base Stations maintain a user-configurable, password-controlled table of authorised subscriber unit MAC addresses. Subscriber units **cannot** talk to the network unless the Base Station Unit authenticates its MAC address.

MAC Address Filtering

The Subscriber Units are configured to filter the downlink traffic stream to prevent a Subscriber Unit from outputting based upon traffic that is destined elsewhere. The filtering restrictions can be Ethernet addresses, VlAN addresses, or IP addresses. Only our Network Operations Centre (NOC) can configure the filtering controls.

Contact a Channel Communications Representative if you require further security information.