

Overview

Tsunami™ Multipoint System Security Capabilities

Wireless communications devices provide considerable flexibility by sending signals over airwaves instead of over wires or fiber. However, sending signals over airwaves creates an opportunity for new security risks for data interception. This document examines five methods employed by Tsunami Multipoint to ensure highly secure wireless communications.

Proprietary Wireless and Data Formats

Unlike a Wireless LAN like 802.11b or 802.11a where the standard is "open," Tsunami Multipoint uses a proprietary communications signaling and data-link protocol. Unless a customer has a Tsunami Multipoint Base Station Unit or Subscriber Unit, it would be almost impossible to intercept or spoof the wireless data streams.

Pseudo-random Transmission Scrambling

The proprietary signaling scheme pseudo-randomly scrambles the transmissions with one of over 500,000 scrambling sequences, thus increasing the difficulty of intercepting a transmission. Using another Subscriber Unit, it would take more than one year to search through all scrambling codes.

MAC Address Authentication

The Base Station Unit maintains a user-configurable and password controlled table of authorized subscriber unit MAC addresses. Subscriber units cannot talk to the network unless the Base Station Unit authenticates its MAC address and "adds" it to the network.

MAC Address Filtering

The Subscriber Units can be configured to filter the downlink traffic stream to prevent a Subscriber Unit from outputting traffic that is destined to another Subscriber Unit. The filtering restrictions may be based upon Ethernet addresses, VLAN addresses, or IP addresses. Only the network operator can configure the filtering controls. This prevents unauthorized access of another user's data.

Theft Protection

Base Station Units measure the distance of the connection to each Subscriber Unit. If one of the Subscriber Units is physically moved to another location, the Base Station Unit will detect that the distance is different and will signal an alarm to the network administrator. This protects against someone stealing a Subscriber Unit and using its valid MAC address to enter the network. Subscriber Units will not listen to a Base Station Unit unless they are "added" to the network via the Base Station Unit.

Summary

Using these five techniques, which provide protection at the physical, network and application layers of the network, Tsunami Multipoint provides both a highly secure and robust system to keep out wireless eavesdropping and malicious user attacks.