TECHNOLOGY

Overview

Proxim WIRELESS NETWORKS

Take your network further

Tsunami™ Doesn't Talk To Strangers: Security in Fixed Wireless Ethernet Bridges

Security is an area of concern for those considering the use of fixed wireless devices to transmit data. Because fixed wireless bridges transmit signals into the "air," the perception has been that anyone could receive and possibly "steal" the user's data. Tsunami wireless Ethernet bridges provide exceptional throughput while minimizing the possibility of security breaches. From the beginning, security was a central focus for the Tsunami design team. The result: Tsunami's robust security framework features a variety of countermeasures which support an enterprise's rigorous security strategy.

Password Protection

Tsunami includes two levels of password protection with one for monitor and a second password providing monitor/modify privileges. This dual-level password protection enables staff in the field to monitor performance and check diagnostics while keeping critical information restricted to system managers.

Tsunami Transmission Protection

The Tsunami transmission signal is so unique that it requires another Tsunami bridge to receive and decode the signal. The Ethernet and T1/E1 traffic (along with associated Tsunami control & monitoring information for the link) is assembled in a proprietary framing structure and sent to the receiving Tsunami bridge. The data remains encoded until it is received and disassembled by the Tsunami bridge at the other end.

Data is scrambled in a nearly random pattern prior to transmission and subsequently processed by a Forward Error Correction encoder before being sent. This encoder adds specific bits of data to the information being transmitted: bits which are subsequently processed by the receiving bridge to ensure data integrity. These bits appear to be random but are actually used to correct errors in transmission and maintain 1x10-12 BER.

One basic tenet of the fixed wireless technology used by Tsunami is the requirement for "line of sight." The Tsunami transmitting and receiving antennas communicate through a relatively narrow radio frequency (RF) beam. This directional point-to-point RF approach is in stark contrast to some omnidirectional antennas used in "mobile" environments where anyone in the vicinity could receive the signal. With Tsunami, only an antenna firmly in the focused RF target area could receive information. By its very nature, Tsunami point-to-point wireless technology minimizes the opportunity for intrusion.

Data Coding

One of the most powerful aspects of Tsunami's security features is data coding. Potential intruders would have to obtain a unique data transmission code sequence set by the administrator. Tsunamis provide a binary security function that can provide up to 2^{48} security coding for data being transmitted (2^{8} for Tsunami 10BaseT Wireless Ethernet Bridge models). This coding is set by the administrator and can be changed in a secure fashion using a web browser or via SNMP using existing System & Network Management software. If someone attempted to break a Tsunami 100 model's security coding, it is estimated that it would take about 45 million years to try all of the possible codes (assuming about 5 seconds for the perpetrator to change codes and check for data).

The sending Tsunami bridge "handshakes" with the receiving bridge, at one second intervals, to verify that the user-assigned code matches. To protect this code further, the code is sent – not in clear text – but in an encoded fashion. If the code comparison does not match, then the Tsunami bridge immediately terminates transmission, causing any IP or T1/E1 traffic to cease flowing in either direction. At any time, through the use of SNMP and/or the HTTP user interface, the system manager can change the security code remotely in order to add another level of protection.

Enhanced Security Options

Third party products can be added to Tsunami's security framework to further encrypt the data stream. Products such as Cylink's NetHawk, a DES (Data Encryption Standard) device, can provide two levels of encryption with either a 56-bit or 168-bit key. Configurations including such products require a device at each end of the link to affect the data portion of the Ethernet packets. NetHawk is IEEE 802.3 compliant and connects with both the Tsunami 10BaseT and 100BaseT Bridges.

Tsunami and 802.11: Apples & Oranges

The IEEE standard for wireless LAN communications, 802.11, was recently featured in the news when the Wireless Equivalent Privacy (WEP) protocol used by 802.11 was discovered to have flaws. These flaws left the 802.11 technology vulnerable to attacks that could decrypt traffic. The 802.11 technology is used predominately in point-to-multipoint applications such as wireless LAN connectivity for PCs and local LAN devices.

Tsunami Wireless Ethernet Bridges are different than the devices impacted by 802.11 because Tsunami's design focus has been and continues to be on point-to-point communications rather than point-to-multipoint communications. Tsunami adheres to 802.3 standards and uses a different security scheme than used by 802.11 devices. The proprietary nature of Tsunami technology precludes challenges such as that encountered by 802.11 and WEP technology.

Proxim WIRELESS NETWORKS
Take your network further

Proxim Corporation
935 Stewart Drive
Sunnyvale, California 94085

tel: 800.229.1630
tel: 408.731.2700
fax: 408.731.3675