Microwave Data Systems Wireless Security Strategy Summary

Summary

MDS wireless technology safeguards your network from data interception and insertion with multiple layers of security. What follows is a summary of the MDS Wireless Security Strategy.

**MDS provides extensive layers of security that prevent:**
- Accessing of data transmission using wireless packet sniffers
- Interception and insertion of wireless information
- Unauthorized/unauthenticated devices from joining the wireless network
- Denial of Service (DoS) attacks
- MAC IP spoofing
- Network Topology Discovery
- Intrusion Detection

**Standards-based, not standards-compliant equipment**
- MDS radios operate in 900 MHz instead of 2.4 GHz: not interoperable with WLAN 802.11
- MDS radios use Frequency Hopping Spread Spectrum (FHSS) instead of standard direct sequence spread spectrum (DSSS) communications. An intruder would have to have another MDS radio, know your network address, and know and set your exact same hopping pattern. (Not likely.) They would also need a promiscuous mode to look at all the over the air traffic to get the keys. There is no such mode in the iNET or entraNET.

**Encryption and dynamic key rotation**
- 128 bit RC4 encryption
- Initialization vector is pseudo-random number
- Encryption phrase used to derive secret set of key
- Keys are rotated every one million packets or three hours
- Forced key generation may occur by operator command
- Multiple keys for encrypting key exchange packets; others rotated for data encryption

**Two-way authentication:**
Authorized AP access lists remotes by MAC address. So each Access Point (AP) and remote in your network recognizes each other and knows only to communicate with legitimate parties in the network. Unauthorized radios will be denied access. Prevents:
- Unauthenticated access
- MAC/IP spoofing
- Network topology discovery

**System-level security features**
- Password protection of the configuration tools: embedded Web server, Telnet menu, local serial menu, and SNMP community strings
- Intrusion detection schemes (traps on remotes/endpoints)
  - alarm reporting of login/logout
  - trap/event generated each time a new radio is added (MAC address)
- Denial of service protection
  - Ethernet port rate limiting at the remote in bytes per second
  - SNMP traps/events generated based on traffic level (50%, 75%, and 100%)
  - Ethernet port remotely disable-able
- SYSLOG support: define a SYSLOG Server IP address and all local events will be sent to the specified server in SYSLOG format.