

Application Note: 5721-0010

VIP 110-24 Security Features

This document discusses the security features of EION's VIP110-24. The VIP 110-24 has three levels of security as follows:

1. User Interface Security (User Configurable)
2. Radio RF Interface Security (User Configurable)
3. Data Scrambling Capability (Not User Configurable)

User Interface Security:

1. Prevents unauthorized VIP110-24 reconfiguration by assigning a password to each radio (node). Without having the specific password for the VIP110-24 radio one cannot configure such a VIP radio.
2. Once the VIP110-24 radio password is invoked, several fields (commands) will not be displayed such as the Network ID, which will prevent unauthorized users from obtaining this information.

Radio RF Interface Security

1. Prevents unauthorized users from entering the VIP network.
2. The Hacker must be able to match the radio frequency plans. The radio frequency plan is made up of two individual channels. The Hacker must match each transmit and receive frequency to be able to communicate with the RF Radio network. There are 30 frequency channels in the standard VIP110-24 unit, so there are 900 combinations of frequency plans.
3. The VIP110-24 has a 32 bit network ID password numbering scheme that is available and can be configured by the network administrator.
4. Once this 32 bit network ID is invoked in the parent radio, then any Child Radio (remote radio) that must be added to a specific VIP network of radios must have the same network ID code.
5. Since the network ID code is just a number then a Hacker can buy one VIP110-24 radio and try every number combination until he gets the right network ID number.
6. A Hacker will probably automate his ID number discovery method, however the process for creating every new ID combination number still needs 5 seconds to change the combination number and reboot his raiding VIP radio. Therefore a hacker would need 680 years to go through every possible combination.
7. A Professional Hacker will probably choose to use an advanced algorithm with one VIP110-24 radio operating in a binary search in order to find the network ID number. It still requires the hacker 150 years to find the right ID number.
8. The Network Manager using VIP110-24 radios can add further protection and security by frequently changing his network ID number combination at his Central Location.

Network ID changes not allowed over the air for remote radios (Optional Feature):

1. This feature will prevent a disgruntled employee at the central network location who already knows the network ID number from changing it at the Central Site and over the air (RF) for all the remote VIP radios.
2. This feature also prevents the Network Manager from making an error in the network ID at the central location rendering the whole network inoperable.
3. This feature ensures that the configuration of the network ID number for each remote VIP110-24 radio is done locally at each remote location.

Data Encryption

Lastly, the end user can configure whatever security he or she so chooses on a network level: DES [Data Encryption Standard] models featuring symmetric or public key encryption are used throughout the world. EION does not recommend the RC4 protocol employed by WEP considering the inherent ease in which it is defeated.