

TSUNAMI MP.11 SECURITY

TSUNAMI MP.11A (MODEL 5054)

Tsunami MP.11a uses a proprietary protocol for communication and is very difficult to hack

Tsunami MP.11a uses the unique Wireless Outdoor Router Protocol (WORP). As this is a proprietary protocol specifically designed for Proxim's Tsunami MP.11 systems and not publicized or standardized, it is very difficult to hack. This means that Wi-Fi systems, for example, cannot tap into the radio communication of the Tsunami MP.11 solutions.

Tsunami MP.11 Base Stations Units only connect to known Subscriber Units and avoids rogue stations that are in the network

Before a data communication between a BSU and (R)SU starts, the units have to learn to know each other. A Base Station Unit will only connect to a Subscriber Unit that has the same Network Name and Base Station Name. This registration happens through an MD-5 CHAP mutual authentication.

High Data Security

For Data Security Tsunami MP.11a uses AES encryption to protect the data.

Radius authentication and access control table

Tsunami MP.11a provides access control via a local access control table and via Radius, securing the network for unknown stations.

Management security

All remote management methods are password-protected; different passwords can be set for SNMP read, SNMP read/write, Telnet and HTTP configuration.

TSUNAMI MP.11 (MODEL 2411)

Tsunami MP.11 uses a proprietary protocol for communication and is very difficult to hack

Tsunami MP.11 uses the unique Wireless Outdoor Router Protocol (WORP). As this is a proprietary protocol specifically designed for Proxim's Tsunami MP.11 systems and not publicized or standardized, it is very difficult to hack. This means that Wi-Fi systems, for example, cannot tap into the radio communication of the Tsunami MP.11 solutions.

Tsunami Base Stations Units only connect to known Subscriber Units and avoids rogue stations that are in the network

Before a data communication between a BSU and (R)SU starts, the units have to learn to know each other. A Base Station will only connect to a Subscriber Unit that has the same Network Name and Base Station Name. This registration happens through an MD-5 CHAP mutual authentication.

High Data Security

For data security Tsunami MP.11 uses WEP Plus encryption to protect the data

Radius authentication and access control table

Tsunami MP.11 provides access control via a local access control table and via Radius, securing the network for unknown stations

Management security

All remote management methods are password-protected; different passwords can be set for SNMP read, SNMP read/write, Telnet and HTTP configuration.