SERVICE BULLETIN ASM-022

Product: Antenna Systems Monitor

Subject: Firmware 2.83 Release **Date: 14th September 2017**

Description

This Service Bulletin announces the release of baseline 2.83 firmware for the Antenna System Monitor (ASM) series products.

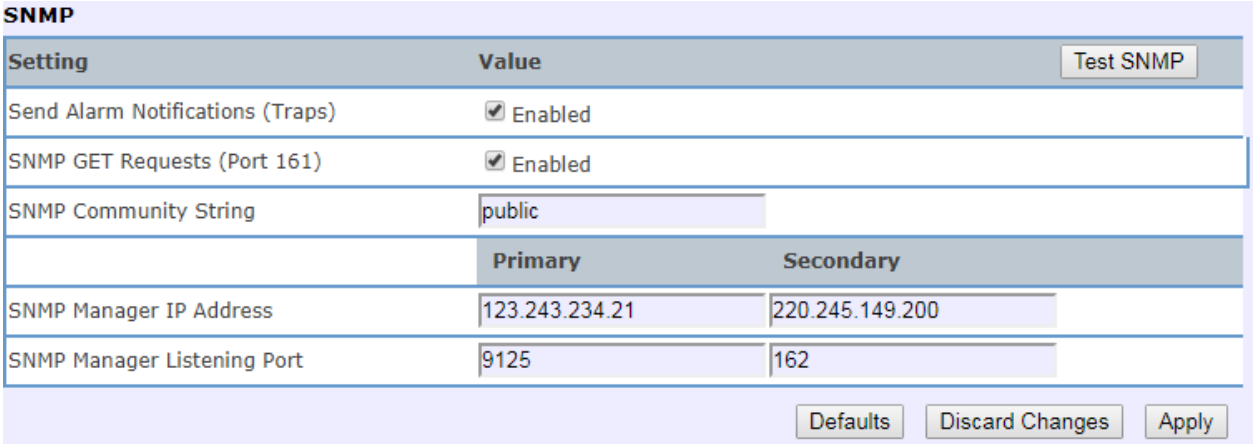
The version 2.83 firmware update file ("FFP") is available for download from the RFI website http://www.rfiwireless.com.au/multicoupling-monitoring/monitoring/antenna-system-monitor-asm3852.html#tab_downloads, and may be flashed into existing ASM models by following the *Maintenance – Firmware Update* process in the Graphical User Interface (GUI) or User Manual.

Product Enhancements

The version 2.83 firmware provides the following new features for the ASM;

i) Configurable SNMP Community String value

This feature allows the SNMP Community String value to be configured from the default 'public' string. Any case-sensitive string of up to 16 characters in length may now be entered. The same Community String is used for both GET requests and Alarm notifications (Traps). This feature is available in the *Configuration – Communications* screen. The latest SNMP MIB files must be used with this feature, and these files are available for downloading from the RFI website.



ii) SNMP Port enabling

To assist resiliency to Denial of Service (DoS) and port flooding attacks, the port used for SNMP GET requests (port 161) can now be disabled if desired. Due to security concerns when connected to an open network (such as the Internet), it is strongly recommended to only enable this port when the ASM is within a private network. The default configuration has this port disabled. This feature is also available in the *Configuration – Communications* screen (refer above).

iii) Command Line Interface (CLI) Port enabling

To assist resiliency to Denial of Service (DoS) and port flooding attacks, the port used for Command Line Interface communications (port 23) can be now disabled if desired. Similar to SNMP port disabling, it is strongly recommended to only enable this port when the ASM is within a private network. The default configuration has this port disabled. This feature is also available in the *Configuration – Communications* screen.

Ethernet

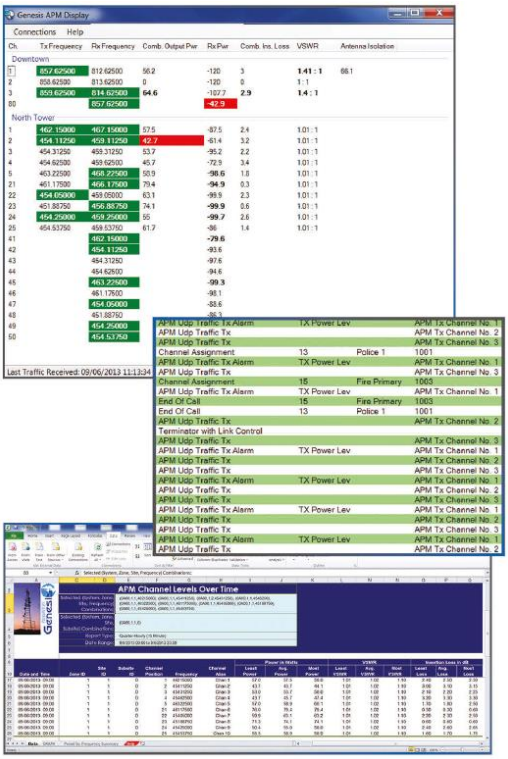
Setting	Value
DHCP	☐ Enabled
IP Address	192.168.1.202
Subnet Mask	255.255.255.0
Gateway	192.168.1.1
NOTE: After saving new values for any of the **above** settings, the system must be restarted to activate them. The Restart option is under the Maintenance menu.	
Port 23 Command Line Interface	☑ Enabled

iv) Improved Resiliency to Denial of Service (DoS) and Port Flooding Attacks

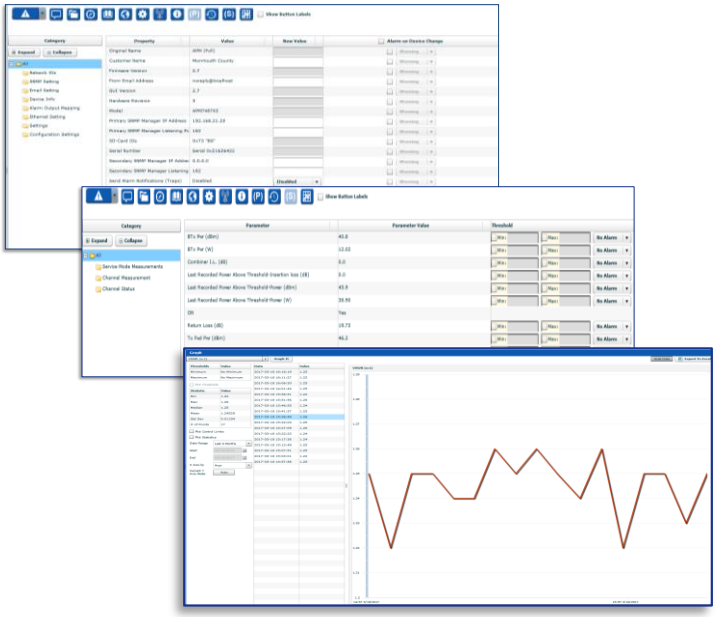
To assist resiliency to malicious Denial of Service (DoS) and port flooding attacks, the ASM IP port's traffic handling code has been enhanced. This will prevent the likelihood of an ASM Restart being triggered by IP stack traffic handling issues that can be triggered by such activities.

v) Supported by Network Performance and Alarm Monitoring Software

The ASM is already supported by Genesis GenWatch™, and also by C² Systems SitePortal® monitoring software packages. Many SNMP Manager software packages also support the ASM's SNMP alarm capabilities.



Genesis GenWatch™ screen examples



C² Systems SitePortal® screen examples

Upgrading to Firmware 2.83

Note: Please read all Service Bulletins published from the release of the firmware currently operating in your ASM prior to commencing an upgrade to this version 2.83 firmware. Upgrades may require a transition through an intermediate firmware version on the way to reaching this version - or may have other implications for your ASM.

The required intermediate firmware version transitions are;

- Firmware below version 2.0 must transition through version 2.0 or 2.05 prior to attempting an update to 2.1 or above.
- Firmware below 2.60 must transition through version 2.60 prior to attempting an update to 2.70 or above.

Cost Impact

Firmware version 2.83 is available to RFI customers at no charge.

- END -