Digital Energy
MDS

APPLICATION BULLETIN

NUMBER: AB12002
July 2012

MDS Mercury Series

GE MDS, LLC. 175 Science Parkway, Rochester, NY 14620 USA
Phone +1 (585) 242-9600, FAX +1 (585) 242-9620 Web: www.gemds.com

CONFIGURATION AND COMMON USE CASES OF MERCURY 16E VLANS

Introduction

Mercury 16E supports 802.1q VLAN operation. A radio may operate in *Trunk mode*, wherein both LAN and WiMax interfaces operate as VLAN trunks and pass all traffic, or in *Access mode*, wherein the LAN interfaces reject packets with VLAN tags upon ingress, and remove VLAN tags from packets upon egress. The WiMax interface remains a VLAN trunk in Access mode.

Moreover, Mercury 16E supports two distinct VLAN IP configurations; three on Wi-Fi-enabled subscribers. These VLANs are used to separate device management traffic from backhaul and serial data traffic.

Scope

This bulletin is intended for applications engineers and end users who wish to set up their Mercury 16E network for VLAN operation. The operation of VLANs in Mercury 16E is discussed, as are common network setups. Finally, considerations are provided for usage of VLANs with serial data traffic.

VLAN Ethport Modes

The WiMax interface is always a VLAN trunk; that is, all traffic, tagged or untagged, is allowed to pass unmodified. When VLANs are enabled, VLAN Ethport Mode may be set to **Access**, **Trunk**, or **Auto**. **Auto** defaults to the configuration typically used in systems: **Trunk** for Base Stations, and **Access** for Subscribers. The VLAN Ethport Mode controls how the unit's LAN ports operate.

When the VLAN Ethport Mode is set to **Trunk**, the LAN ports also operate as VLAN trunks and allow all traffic to pass unmodified. This mode of operation is typically used on Base Stations, where the LAN port is connected to another VLAN trunk, such as a router. When the VLAN Ethport Mode is set to **Access**, the LAN ports remove VLAN tags from packets as they egress the LAN port. The LAN ports also block ingress of any packet containing a VLAN tag, and allow only untagged packets. **Access** mode is typically used on Subscribers that have a wired network connection to VLAN-unaware devices, such as a PC.

If the VLAN Ethport Mode is in **Access** mode, the radio will add a VLAN tag to untagged packets that enter through the LAN ports. This tag is configurable by the user. The same tag can be used for both LAN1 and LAN2 ports, or a different tag may be specified for each port. Units that operate in **Access** mode will be the final VLAN-aware device in a system, because traffic exits the LAN ports without tags and tagged traffic cannot enter the LAN ports.

The Wi-Fi VLAN, available on Wi-Fi-enabled Subscribers, only operates in **Access** Mode. Only untagged packets are allowed to enter the radio through the Wi-Fi interface, and tags are removed before packets exit the Wi-Fi interface.

Management, Serial, and Wi-Fi VLANs

VLAN IDs and VLAN Tags

Management and Serial VLAN configurations are supported on all Mercury 16E radios. A Wi-Fi VLAN is also available on Wi-Fi-enabled Subscribers.

The Management and Serial VLANs are meant to separate management and data traffic and prevent crosstalk between them. Each VLAN has its own, separate IP configuration, as if it were a separate network interface. The Wi-Fi VLAN on Wi-Fi-enabled Subscribers may operate as a separate VLAN with a third IP configuration, or it may operate on the same VLAN as the Serial VLAN. In the latter scenario, the Wi-Fi and Serial VLANs share IP settings.

A VLAN ID must be configured for the Management and Serial VLANs, and these IDs cannot be the same. The Wi-Fi VLAN will have the same VLAN ID as the Serial VLAN if it operates as part of the Serial VLAN. To isolate the Wi-Fi VLAN from the Serial VLAN, assign it a different VLAN ID. Packets tagged with one of these VLAN tags are assumed to be traffic intended for that VLAN if the destination address is an IP address on the radio.

IP Addresses and Prevention of Crosstalk

To prevent crosstalk between VLANs on the radios, packets entering the radio on the Management VLAN intended for the Serial or Wi-Fi VLAN's IP addresses are dropped, as well as packets entering on the Serial VLAN intended for the Management VLAN's IP address. If the Wi-Fi VLAN exists and is separate from the Serial VLAN, packets entering on the Serial VLAN intended for the Wi-Fi VLAN address are also dropped. Likewise, packets entering the radio on the Wi-Fi VLAN destined for the Management VLAN's IP address are dropped, as are packets destined for the Serial VLAN IP address, if the Wi-Fi VLAN is separate from the Serial VLAN.

The Serial and Wi-Fi VLANs also disallow Management traffic that originates from or is destined for their IP addresses. Management traffic refers to network traffic intended to manage the devices. This includes the following network protocols:

- WWW
- HTTP and HTTPS
- FTP, TFTP, and SFTP

- NTP
- SNMP

Note that the user interfaces are *only* accessible through the Management VLAN when VLANs are enabled. These include the web, telnet, SSH, and SNMP interfaces.

Tagged vs. Native Management VLAN

IEEE 802.1q supports the concept of a "native" VLAN, wherein untagged frames that enter a VLAN trunk are assumed to belong to the native VLAN ID. Mercury 16E radios accommodate this by allowing the Management VLAN to be configured as a Tagged or Native VLAN. If the VLAN Management Mode option is set to Native, traffic intended to manage the radio is expected to be received without tags. Tagged traffic destined for the radio's Management IP address is therefore rejected.

If the VLAN Management Mode is set to Tagged, traffic intended to manage the radio is expected to be received with the Management VLAN tag. Untagged traffic destined for the radio's Management IP address is rejected. The VLAN Management Mode setting depends on network design and will vary on a per-system basis.

Common Use Cases

Simple Networked System

A typical VLAN use case is shown in Figure 1 below. This simple system contains one Base Station with a wired connection to a network device operating as a VLAN trunk, and one Subscriber with wired connections to two VLAN-unaware PCs.

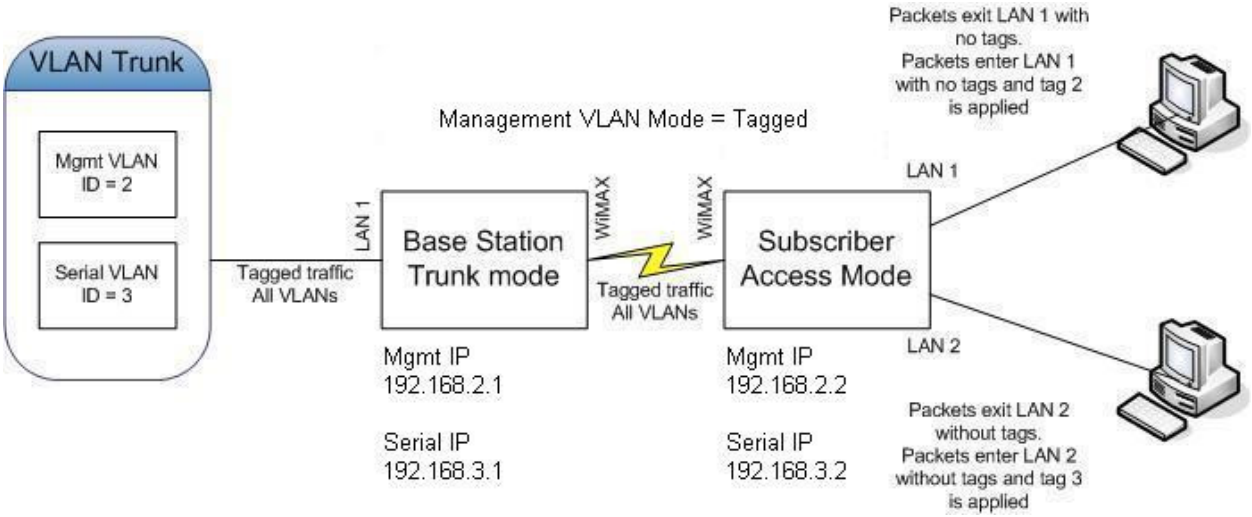

Figure 1. Typical use case--Management and Serial VLANs

In this example, the management VLAN is 2 and serial VLAN is 3. In order to isolate the VLAN traffic, IP addresses are chosen on different subnets as shown in the diagram, and the netmask applied to each is 255.255.255.0. The Management VLAN on both units is set to Tagged mode.

The VLAN trunk connected to the Base Station passes all traffic, not just packets tagged with the Management and Serial VLAN tags. Since the Base Station is operating in trunk mode, it also passes all traffic through its LAN and WiMax interfaces. If, however, traffic destined for its Management IP address arrives with a Serial VLAN tag, or vice versa, the packets are ignored. If Management traffic using disallowed protocols arrives destined for its Serial IP address, those packets are also ignored.

The Subscriber operates in **Access** mode, but since the WiMax interface always operates as a VLAN trunk, all traffic sent from over the air from the Base Station is received. As they do on the Base Station, the Management and Serial VLANs ignore packets destined for their addresses with the incorrect VLAN tag, and the Serial VLAN ignores Management packets destined for its IP address.

The UI settings for this system setup are as follows.

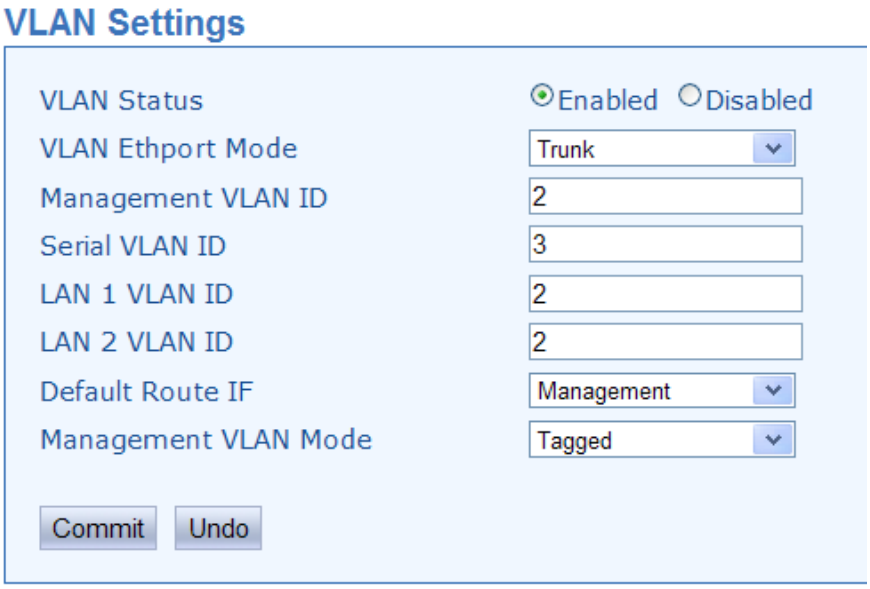

Figure 2. VLAN Settings on Base Station
*Note that the LAN 1/LAN 2 VLAN ID values are **not** applied in Trunk Mode.*

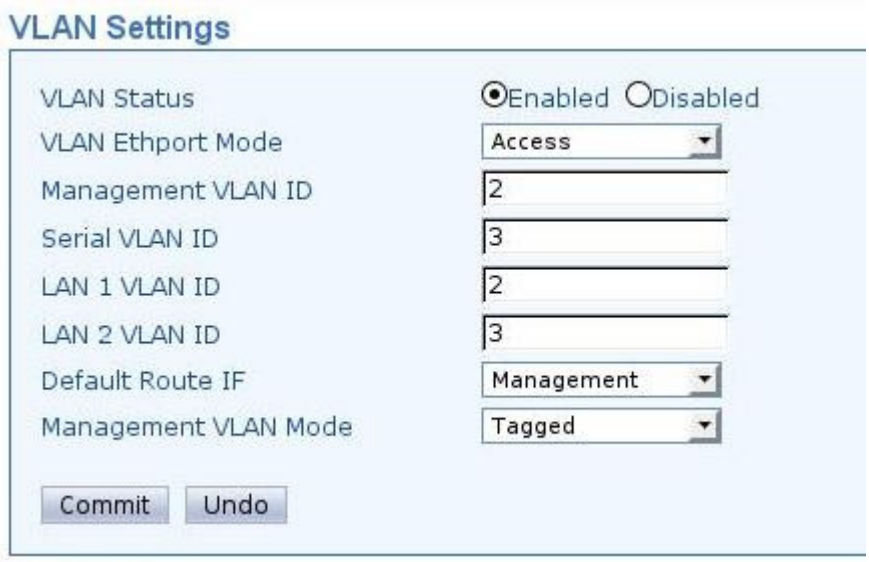

Figure 3. VLAN Settings on Subscriber.

Alternate Setup

The setup in the diagram below illustrates the use of Native Management mode and VLAN trunking on both radios. Both Base Station and Subscriber in this system have wired network connections to a PC or laptop, and a serial polling device is connected to the COM port of both radios. Since the Management VLAN is in Native mode, all Management traffic can be sent without tags from both computers.

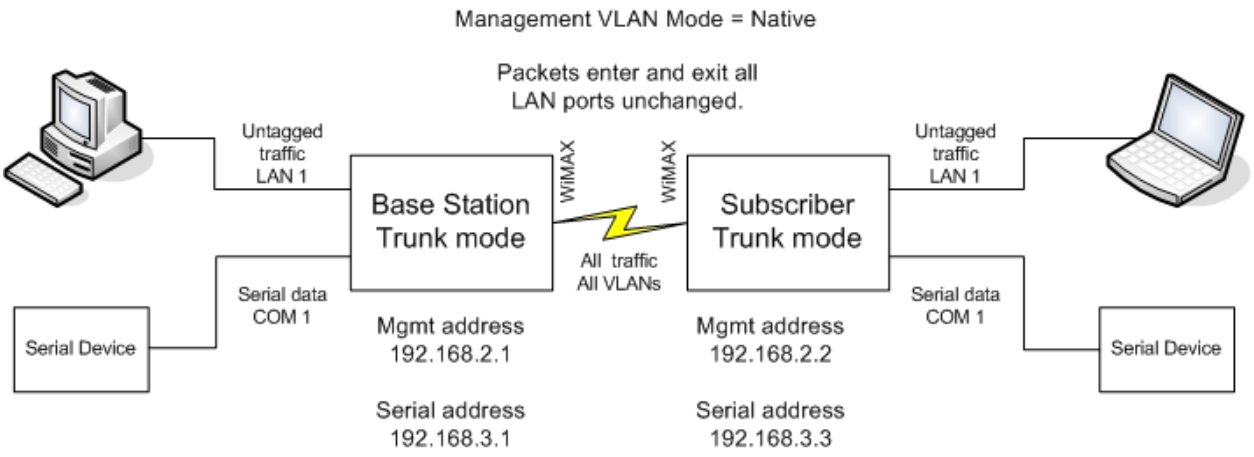

Figure 4. System utilizing VLAN trunking and Native Management mode

The UI settings for this system follow. The VLAN setup is identical on both the Base Station and Subscriber.

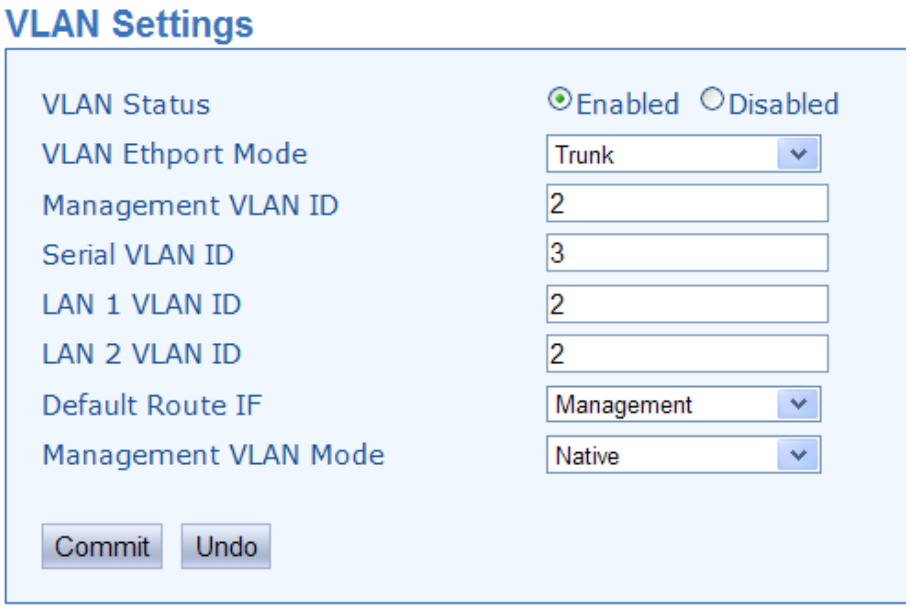

Figure 5. UI settings for the system depicted in Figure 4.
Note that LAN 1/LAN 2 VLAN IDs are unused in Trunk mode.

Using Serial Data Mode

It is important to use the correct IP settings when using VLAN-enabled radios in serial data mode. Consider the system in Figure 4 above. Since VLANs are enabled, the Serial VLAN IP addresses must be used when configuring serial data settings for COM 1 in the Serial Wizard. Otherwise, traffic from serial data devices will not pass over the air.

The settings shown in Figures 6 and 7 are used to enable UDP Unicast traffic between the serial data devices over the Serial VLAN. Any IP protocol may be used with VLANs, as long as the Serial VLAN IP settings are used when configuring the serial data settings in the Serial Wizard.

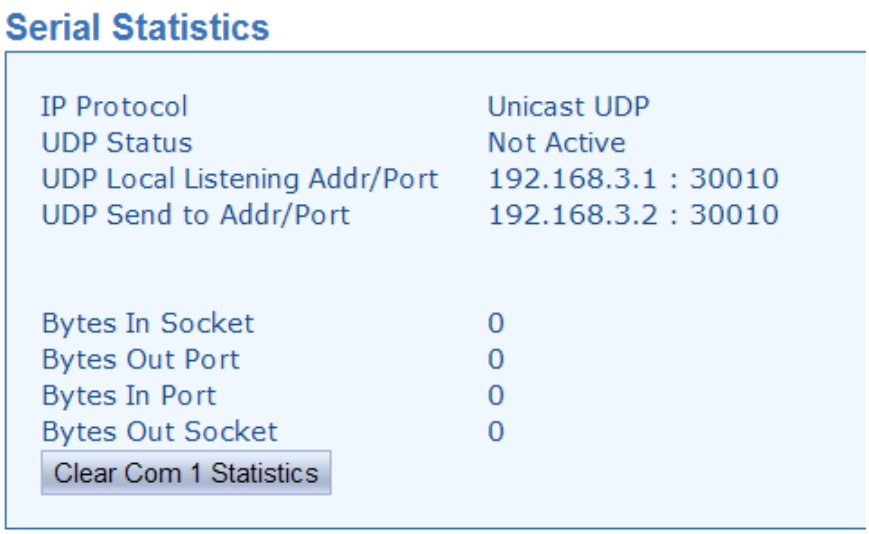

Figure 6. Serial data settings on Base Station, specifying Serial VLAN IP addresses.

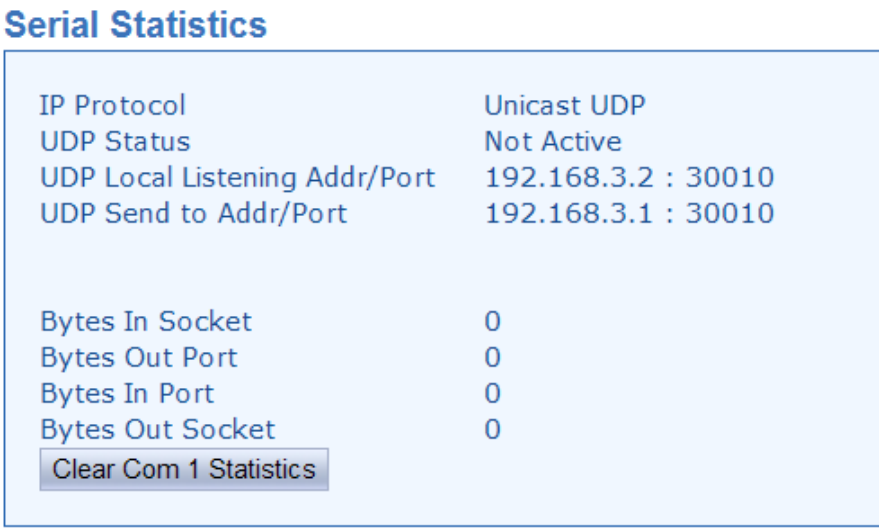

Figure 7. Serial data settings on Subscriber, specifying Serial VLAN IP addresses.

End of application bulletin.