

**A Review of Switch Setup with Alta ENET Devices**  
**Alta Data Technologies**  
**October 2013: 131018**

This document reviews examples of Ethernet switch setup in use with Alta ENET devices. This is **not** comprehensive instructions of how to use your particular switch, but a review of one particular exercise that Alta conducted with IT consultants (who are experts in the field) with a Cisco 3750 managed switch.

Many customers use an ENET device with a point-to-point connection to a computer (PC) and this document doesn't apply to this configuration. Although there is important information in the Energy Efficient Ethernet paragraph at the very end of the document that is applicable to a point to point eNet/PC configuration.

The following discussions are targeted for readers very familiar with switch setup and management. Alta hired an IT consulting group to aid in this test and provide setup information. Although we (Alta) learned a lot about switch management in this exercise, we are not switch experts by any means. We strongly recommend your company have similar IT experts either in house or via consultants to help setup or debug your particular switch/LAN/WAN configuration.

First, a few important facts:

- ENET is an end-point Ethernet device that supports only ARP and UDP protocols.
  - ICMP ping is not supported (for security reasons).
- ENET is a Static IP Address device. The customer may use the AltaView application to reprogram the static IP address (please see the ENET hardware manual, Appendix B for details of using the AltaView Global ENET Config tool).
  - The ENET IP address will need to match your switch's "subnet", which is the first 3 octets XXX of an IP address (XXX.XXX.XXX.YYY or example 192.168.0.128). The 4<sup>th</sup> octet (YYY or 128 in the example) is the "host" number or computer's address in the subnet – this can be any value in your 1-254 range. The ENET default IP address is 192.168.0.128.
  - Once programmed, the ENET's IP address can be reset to the factory default by grounding pin 23 on the J2 connector during power-up of the device. Detailed instructions are provided in the ENET Hardware Manual.

### **Alta Cisco 3750 24-Port Switch Test Setup Information**

In the following discussions, Alta tested with a Cisco 3750 managed switch that had been reset to factory default settings. Cisco setup commands were done via the management console port. We setup the Cisco switch per the basic "Getting Started" instructions in the Cisco manual to a base IP address of 192.168.0.0 subnet (this took about 10 minutes from scratch with no previous switch experience – simple).

The very first task we did was to connect an ENET device to port 21 and a PC computer to port 19 to see if we could connect via AltaView between the PC and the ENET device. We powered-

up the switch with ENET and PC powered up. The ENET was at the default 192.168.0.128 IP address and the PC was set to static address 192.168.0.10. **The Cisco link lights are key for basic negotiation information!** It took about 30 seconds for the link lights to go green for both the PC and ENET (due to Cisco switch trying to negotiate switch spanning – trying to see if the device on the port is another switch). Both the ENET and PC automatically negotiated to 1G link indications on the switch.

We also had another computer connected to port 5 for testing. This was used to generate UDP flood traffic in VLAN testing. We used the common network test tool IPERF to generate UDP traffic in later tests. You can google and download this test program for free.

After the switch link lights had gone green, we were able to run the AltaView software on the PC and open the ENET device using Open Device in AltaView: **everything worked fine with the default setup of the Cisco switch!** We've had customer's comment that they could not get the ENET device to be seen with the same switch and we can only assume that the switch had been setup with customer specific settings that did not like static IP addresses or something...We cannot explain their difficulty since our test worked "out of the box" with default settings. In discussing this with our IT experts, we reviewed that "managed" switches can be setup in complicated scenarios and it is very difficult to guess what is going on.

Note: It does seem that the simpler the switch (unmanaged), the easier task of integrating ENET to the LAN. Managed switches can seem to present problems if they have been tailored for specific traffic management or security configurations. We (Alta) have not had a scenario where ENET has not worked – customers have eventually, successfully integrated ENET to their switch LAN after some research and proper configuration of their switch.

The following useful Cisco command will show configuration of ports (notes this example shows additional VLAN settings that will be discussed in later paragraphs).

"The customers can run a **show tech** command to display the switch's diagnostic data. It's a lot of output, so they'll want to enable logging in their terminal emulator to capture it all."

\*\*\*\*\*example \*\*\*\*\*

```
Switch>
Switch>enable
Switch#
Switch#config terminal
Switch(config)#interface gigabitethernet1/0/19
Switch(config-if)#switchport access vlan 5
% Access VLAN does not exist. Creating vlan 5
Switch(config-if)#interface gigabitethernet1/0/21
Switch(config-if)#switchport access vlan 5
Switch(config-if)#end
Switch#show vlan
```

VLAN Name	Status	Ports
1 default	active	Gi1/0/1, Gi1/0/2, Gi1/0/3 Gi1/0/4, Gi1/0/5, Gi1/0/6 Gi1/0/7, Gi1/0/8, Gi1/0/9 Gi1/0/10, Gi1/0/11, Gi1/0/12 Gi1/0/13, Gi1/0/14, Gi1/0/15 Gi1/0/16, Gi1/0/17, Gi1/0/18 Gi1/0/20, Gi1/0/22, Gi1/0/23 Gi1/0/24, Gi1/0/25, Gi1/0/26 Gi1/0/27, Gi1/0/28
2 VLAN0002	active	
5 VLAN0005	active	Gi1/0/19, Gi1/0/21

### Virtual LAN (VLAN) Discussion

We've had several customer comments about ENET performance issues on heavily loaded switches, which would suggest that the switch is dropping IP-UDP packets in the traffic or allowing broadcast UDP traffic to be sent to the ENET port. Per our IT experts, this mainly due to improper switch setup for managed switches (unmanaged switches may simply copy data to ports and this could cause ENET UDP retry issues and would need to be changed to point to point or managed switch configurations).

NOTE: Switches generally manage traffic at the physical port level or IP level, which is above the UDP level. With proper setup, this means IP/UDP traffic can also be better managed for better reliability. The ENET UDP control protocol (ADCP – see AltaCore and AltaAPI manuals for details) provides UDP transfer with a handshake/retry mechanism for ENET setup/control information, and thus, is the focus of trying to properly setup switch management of IP packets. This UDP protocol is used because, in most cases, UDP packets are transferred successfully and UDP has much less overhead than TCP resulting in much faster transfer times and less ENET FPGA design space – making a better, real-time Ethernet product.

This brings us to the discussion to VLANs. Per our IT experts, VLANs are a “best practice” switch configuration to manage (shape) IP traffic for better performance between physical ports (ENET and client computer). VLANs are widely supported by most switches, even lower cost switches (<\$200 switches – many of which are very powerful thanks to the video game industry).

VLANs are essentially settings for switch physical ports (which then ARP the IP address) to configure a virtual LAN so that all other traffic is blocked and to keep a clean traffic path between the ENET and client computer. The following notes are for setting the Cisco switch ports 19 and 21 for a separate VLAN of 5.

- Placing switchports in separate VLANS
  - o Enter privileged mode
  - o Enter configuration context
  - o Enter interface context
  - o Assign port to VLAN

Placing sensitive switchports in their own VLAN will isolate them from unwanted broadcast traffic. Note that switchports Gi1/0/19 and Gi1/0/21 are the only two switchports in VLAN 5. They will not receive *any* traffic from ports 1-18, 20, or 22-28. VLAN 1 is created by default, and is where all of the ports reside by default.

VLAN Further discussion.

Question on VLANs to our IT experts: [Can you change the priority of a VLAN once assigned? If our ENET is mission critical, then we may want to be high/highest priority for packet routing.](#)

Answer: it would actually be simpler to set the quality of service setting on the specific switchport, not the VLAN. Here is an example:

```
interface GigabitEthernet1/0/12
description **** Cisco IP Phone ****
switchport access vlan 10
switchport mode access
switchport voice vlan 20
mls qos trust cos
mls qos cos 3 override
```

Using **mls qos cos <value> override**, the switch will override the incoming priority values (default of 0), with the value you choose (from 0 to 7 with 7 being the highest). In the example above, the switchport exists in two VLANs (10 and 20) because it connects to a phone, but it would work just the same if you only had it in one VLAN. This example was found in the 3750 QoS pages. For mission critical applications, we recommend setting the QoS value to highest allowed by your IT configuration.

## Example Setup for Faster Switch Port Negotiation

Here is an example of speeding-up

- Enabling portfast
  - o Enter privileged mode
  - o Enter configuration context
  - o Enter interface context
  - o Enable portfast

\*\*\*\*\*example\*\*\*\*\*

```
Switch(config)#int gi1/0/19
```

```
Switch(config-if)#spanning-tree portfast
```

%Warning: portfast should only be enabled on ports connected to a single host. Connecting hubs, concentrators, switches, bridges, etc... to this interface when portfast is enabled, can cause temporary bridging loops.  
Use with CAUTION

%Portfast has been configured on GigabitEthernet1/0/19 but will only have effect when the interface is in a non-trunking mode.

The portfast setting will prevent the switch from placing the switchport in “listening” and “learning” states before establishing a link. Instead, when the link comes online, it will transition immediately to a forwarding state. As the warning indicates, this should not be enabled on ports that connect to other switches/routers/etc, as this could cause network loops.

## Energy Efficient Ethernet (EEE) or Green Ethernet – Turn Off!

Several advanced NICs and switches have implemented EEE (to aggregate packets to single transmission bursts instead of real-time small packets). **You must turn this off!** EEE may work fine for office network traffic or web surfing, but do not use this with ENET real-time control or critical data devices.