User Manual

FRM220A-1000EAS/X

4-Port OAM/IP Gigabit Ethernet Media Converter/Switch

CTC UNION TECHNOLOGIES CO., LTD.

CTC Union Technologies Co., Ltd.
Far Eastern Vienna Technology Center
(Neihu Technology Park)
8F, No. 60 Zhouzi St., Neihu, Taipei 114,
Taiwan

T +886-2-26591021
F +886-2-26590237
E sales@ctcu.com
techsupport@ctcu.com
H www.ctcu.com

FRM220A-1000EAS/X Operation Manual

4-Port OAM/IP Gigabit Ethernet Media Converter/Switch

Version 1.0 July 22, 2011 (First official release)

This Manual supports the following models:

FRM220A-1000EAS/X : 2x100/1000Base-X (SFP) + 2x10/100/1000Base-T

ISO 9001 Quality System Certified

Legal

The information in this publication has been carefully checked and is believed to be entirely accurate at the time of publication. CTC Union Technologies assumes no responsibility, however, for possible errors or omissions, or for any consequences resulting from the use of the information contained herein. CTC Union Technologies reserves the right to make changes in its products or product specifications with the intent to improve function or design at any time and without notice and is not required to update this documentation to reflect such changes.

CTC Union Technologies makes no warranty, representation, or guarantee regarding the suitability of its products for any particular purpose, nor does CTC Union assume any liability arising out of the application or use of any product and specifically disclaims any and all liability, including without limitation any consequential or incidental damages.

CTC Union products are not designed, intended, or authorized for use in systems or applications intended to support or sustain life, or for any other application in which the failure of the product could create a situation where personal injury or death may occur. Should the Buyer purchase or use a CTC Union product for any such unintended or unauthorized application, the Buyer shall indemnify and hold CTC Union Technologies and its officers, employees, subsidiaries, affiliates, and distributors harmless against all claims, costs, damages, expenses, and reasonable attorney fees arising out of, either directly or indirectly, any claim of personal injury or death that may be associated with such unintended or unauthorized use, even if such claim alleges that CTC Union Technologies was negligent regarding the design or manufacture of said product.

TRADEMARKS

Microsoft is a registered trademark of Microsoft Corp.
HyperTerminal™ is a registered trademark of Hilgraeve Inc.

WARNING:

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and if not installed and used in accordance with the instruction manual may cause harmful interference in which case the user will be required to correct the interference at his own expense. NOTICE: (1) The changes or modifications not expressively approved by the party responsible for compliance could void the user's authority to operate the equipment. (2) Shielded interface cables and AC power cord, if any, must be used in order to comply with the emission limits.

CISPR PUB.22 Class A COMPLIANCE:

This device complies with EMC directive of the European Community and meets or exceeds the following technical standard. EN 55022 - Limits and Methods of Measurement of Radio Interference Characteristics of Information Technology Equipment. This device complies with CISPR Class A.

CE NOTICE

Marking by the symbol CE indicates compliance of this equipment to the EMC and LVD directives of the European Community. Such marking is indicative that this equipment meets or exceeds the following technical standards: EN 55022:2006, Class A, EN55024:1998+A1:2001+A2:2003, and EN60950-1:2001

Table of Contents

Chapter 1 Introduction

1.1 Welcome

Thank you for choosing **FRM220A-1000EAS/X** OAM/IP Gigabit Ethernet Media Converter/Switch. Throughout this document, this model will be referred to as **FRM220A-1000EAS/X** or in an abbreviated form as just **1000EAS/X**. If you would like to skip right to the installation of the converter, proceed to Chapter 2.

This manual is used to explain the hardware installation procedures and operation of **1000EAS/X**, and present its capabilities and specifications. This manual is divided into 4 chapters, the Introduction, Installation, Telnet Provisioning and Web Based Provisioning chapters.

Installers should carefully read Chapter 1&2, Introduction and Installation. The companion document, **FRM220 NMC Configuration Manual**, is also available in electronic format. The divisions in that manual are intended for use by personnel to answer questions in general areas. Planners and potential purchasers may read the Introduction to determine the suitability of the product to its intended use; Operating Personnel would use the Telnet Operations and Web Based Management Chapters to become familiar with the line cards and settings. Network Administrators should read the chapters on Telnet Operation and Web Based Management to become familiar with the diagnostic capabilities, network settings and management strategies for the SNMP managed chassis.

1.2 Product Description

FRM220A-1000EAS/X is a four port OSI Layer 2 Ethernet switch and media converter with two Dual-Rate Ethernet fiber ports (100Base/1000Base-X) plus two copper Ethernet ports (10/100/1000Base-T). The Layer 2 switch technologies include jumbo frame support, tag based VLAN, port trunking, fiber redundancy, 802.1D Spanning Tree Protocol, 802.3x Flow Control and ingress/egress bandwidth control per port. With its own embedded 32 bit processor, **1000EAS/X** supports stand-alone management via IP (Telnet, SNMP & HTTP) or in-band management via 802.3ah-OAM protocol when connected to another **1000EAS/X** in point to point or as a CPE device to **1000EAS/X** mounted in **FRM220** or **FRM220A** managed media converter rack.

1.3 Features

- Four port L2 switch
- Port based VLAN support
- Tag VLAN support
- Double VLAN tag support (Q-in-Q)
- Cisco Trunk Management VID support
- Ingress/Egress Bandwidth control per port
- Spanning Tree Protocol support
- 32bit embedded CPU for stand-alone management
- 802.3ah-OAM in-band management
- Firmware upgrade via TFTP
- Telnet, HTTP, SNMP and OAM management
- Dying gasp (remote power failure detection)
- Auto Laser Shutdown
- Link Fault Pass-Through (LFP)
- Transparent Link Pass Through
- Fiber Redundancy function
- Paused Frame flow-control
- Digital Diagnostic (DOM) SFP support
- OAM PDU and per port RMON counters
- SNTP client

WARNING: Fiber optic equipment may emit laser or infrared light that can injure your eyes. Never look into an optical fiber or connector port. Always assume that fiber optic cables are connected to a laser light source.

1.4 Specifications

▪ **Optical Interface**	
▪ **Connector**	SFP cage x 2
▪ **Data rate**	Dual Rate; 125Mb/s or 1.25Gb/s (manual setting)
▪ **Duplex mode**	Full duplex
▪ **Fiber**	MM 50/125um, 62.5/125um SM 9/125um (depending on SFP)
▪ **Distance**	MM 550M/2KM, SM 15/30/50/80/120KM (depending on SFP)
▪ **Wavelength**	Depends on SFP
▪ **Electrical Interface**	
▪ **Connector**	RJ-45 x 2
▪ **Data Rates**	10Mbps, 100Mbps, 1000Mbps (auto or forced)
▪ **Duplex**	Full or Half Duplex
▪ **Cable**	10Base-T Cat. 3,4,5,5e UTP
▪	100Base-TX Cat. 5, 5e or higher
▪	1000Base-T Cat 5, 5e, 6 or higher
▪ **Standards**	IEEE802.3, 802.3u, 802.3z, 802.3ab, 802.3ah 802.3x, 802.1W, 802.1p, 802.1Q, RFC 4330 (SNTP)
▪ **Maximum MTU**	10240 bytes
▪ **Indicators**	LED (PWR, Fiber 1&2 Link, Test, UTP 3&4 Link, UTP 3&4 Speed)
▪ **Power**	(Card supports hot-swapping)
▪ **Input**	Card : 12VDC, Standalone : AC, DC options
▪ **Consumption**	<8W
▪ **Dimensions**	155 x 88 x 23mm (D x W x H)
▪ **Weight**	140g
▪ **Temperature**	0 ~ 50°C (Operating), -10 ~ 70°C (Storage)
▪ **Humidity**	10 ~ 90% non-condensing
▪ **Certification**	CE, FCC, LVD, RoHS
▪ **MTBF**	65000 hrs (25°C)

1.5 Management Features

1000EAS/X has its own embedded processor which can be used to configure the device for stand-alone operation. When placed in a stand-alone chassis, this device supports a text based Telnet terminal with an easy to use menu system for configuration. The embedded **HTTP** server provides an easy to use **GUI** (Graphical User Interface) with any web browser. **SNMP** is also supported in the stand-alone operation. When using network management software and our proprietary MIB file specifically for the **1000EAS/X,** all settings can be performed, performance monitoring realized and alarm traps received. When placed in a managed chassis, such as our **FRM220-CH20** with **NMC** (Network Management Controller) card, the **1000EAS/X** card is configured and monitored through the chassis **NMC** via console, Telnet, Web HTTP or SNMP.

1. Stand-alone in CH01M 1-slot or CH02M 2-slot – Serial Terminal for initial setup
2. Stand-alone – IP settings allow management by Telnet, Web or SNMP
3. Rack management - When placed in **NMC** managed rack, all other settings can be overridden by the **NMC** management.

1.6 Panel

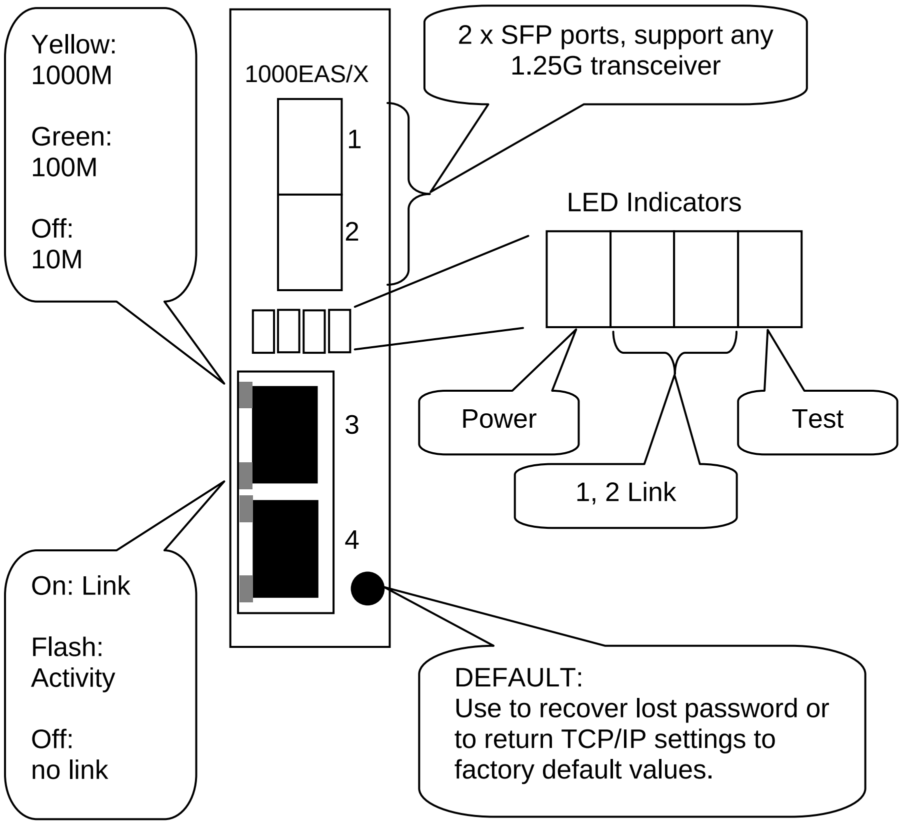

Yellow:
1000M
Green:
100M
Off:
10M
1000EAS/X
1
2
3
4
2 x SFP ports, support any 1.25G transceiver
LED Indicators
Power
Test
1, 2 Link
On: Link
Flash:
Activity
Off:
no link
DEFAULT:
Use to recover lost password or to return TCP/IP settings to factory default values.

Figure 1.1 Panel designations of **FRM220A-1000EAS/X**

1.7 Factory Reset Procedure

Apply power to **1000EAS/X** and allow 30 seconds to fully boot. Using a pencil or ball-point pen, press the 'DEFAULT' recessed push-button switch (located on the face plate) and hold for 5 seconds and release. DO NOT POWER OFF. Allow the unit to again fully reboot. The defaults are:

IP=10.1.1.1
netmask=255.0.0.0
GW=10.1.1.254
TFTP server=10.1.1.100

The username and password are both reset to 'admin' if enabled.

This page left blank intentionally.

Chapter 2 Installation

2.1 Chassis Options

Note: This converter card can be placed in any **FRM220** series chassis, including the single slot CH-01M, two slot CH02M or CH02-NMC or the full twenty slot CH-20 chassis. Chassis with built-in power are available with single AC (100-240VAC), single DC (18~75VDC), dual AC, dual DC or AC plus DC combo. The single slot chassis with external power adapter works with AC source voltage only with the provided 100~240VAC 12VDC@1A switching adapter.

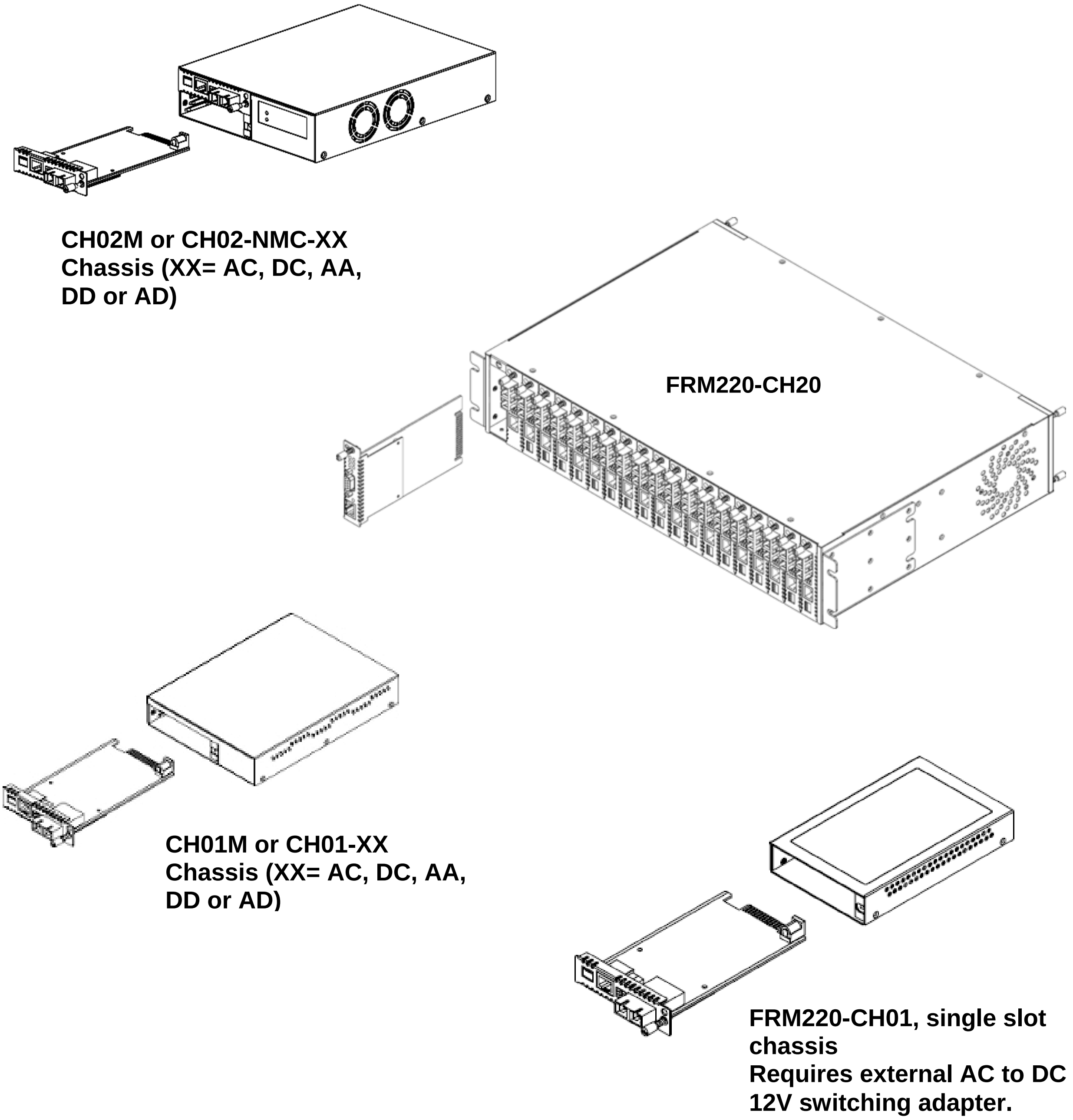


Figure 2.1 Chassis options for **FRM220-1000EAS/X** card

Follow all ESD precautions when handling the card and SFP modules.

2.2 Electrical Installation

With a built-in AC power chassis, AC power is supplied to the chassis through a standard IEC C14 3-prong receptacle, located on the rear of the chassis. Any detachable nationally approved power cord with IEC C13 line plug may be used to connect AC power to the chassis unit. With a built-in DC power chassis, DC -48V is connected to the terminal block located on the rear of the chassis, observing the proper polarity. The chassis should always be grounded through the protective earth lead of the power cable in AC installations, or via the frame ground connection for DC installations.

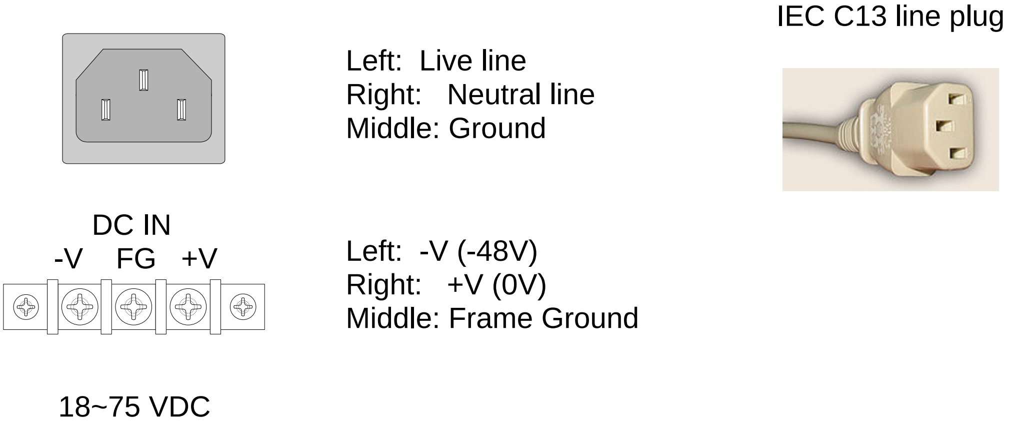


Figure 2.2 IEC (AC) & terminal block (DC) power connector pin assignment

2.3 Installation of SFP Modules

CTC Union supplied SFP modules are of the Bale Clasp type. The bale clasp pluggable module has a bale clasp that secures the module into the SFP cage.

2.3.1 Inserting a Bale Clasp SFP Module into the Cage

Step 1 Close the bale clasp upward before inserting the pluggable module.
Step 2 Line up the SFP module with the port, and slide it into the cage.

2.3.2 Removing a Bale Clasp SFP Module

Step 1 Open the bale clasp on the SFP module. Press the clasp downward with your index finger.
Step 2 Grasp the SFP module between your thumb and index finger and carefully remove it from the SFP cage.

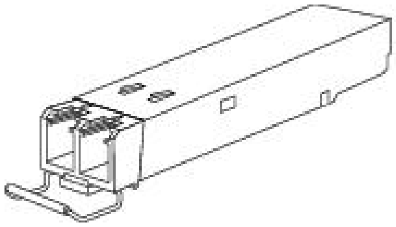


Figure 2.3 Bale Clasp type SFP with bale open

Chapter 3 Provisioning via Text Menu

3.1 Introduction

1000EAS/X has an easy to use menu system that is accessible both through a local serial console (terminal) connection and through a Telnet connection via TCP/IP network over Ethernet. Both the serial console and Telnet protocol management methods are employed to provide an easy to use, text based, menu system for performing all configuration functions. In most cases, we recommend that the networking engineer start configuration by using serial terminal. Configure the required TCP/IP parameters for the network deployment, and then continue detailed configurations using the Web Based GUI. For GUI operation, please refer to Chapter 4 Provisioning Via Web Based Management.

3.2 Serial Console Login

Serial console login is available when **1000EAS/X** is placed in a single slot chassis with DB9 serial connection such as the CH01M. Connect a 1:1 RS-232 serial cable between the DB9 female on the 1-slot chassis to any available COM port on a PC. Use a terminal emulation program such as HyperTerminal, PuTTY, or TeraTerm Pro. The latter two are freely available by searching the Internet. Configure the terminal for 115.2k, 8bit, no parity, 1 stop bit, no flow control and VT-100 emulation.

3.2.1 Main

From the factory, no username or password is required to access the console management of **1000EAS/X**. If the password is set and forgotten, please do a factory default (refer to 1.7 Factory Reset Procedure.) When factory reset, the username and password will both be ‘admin’, if password checking is enabled.

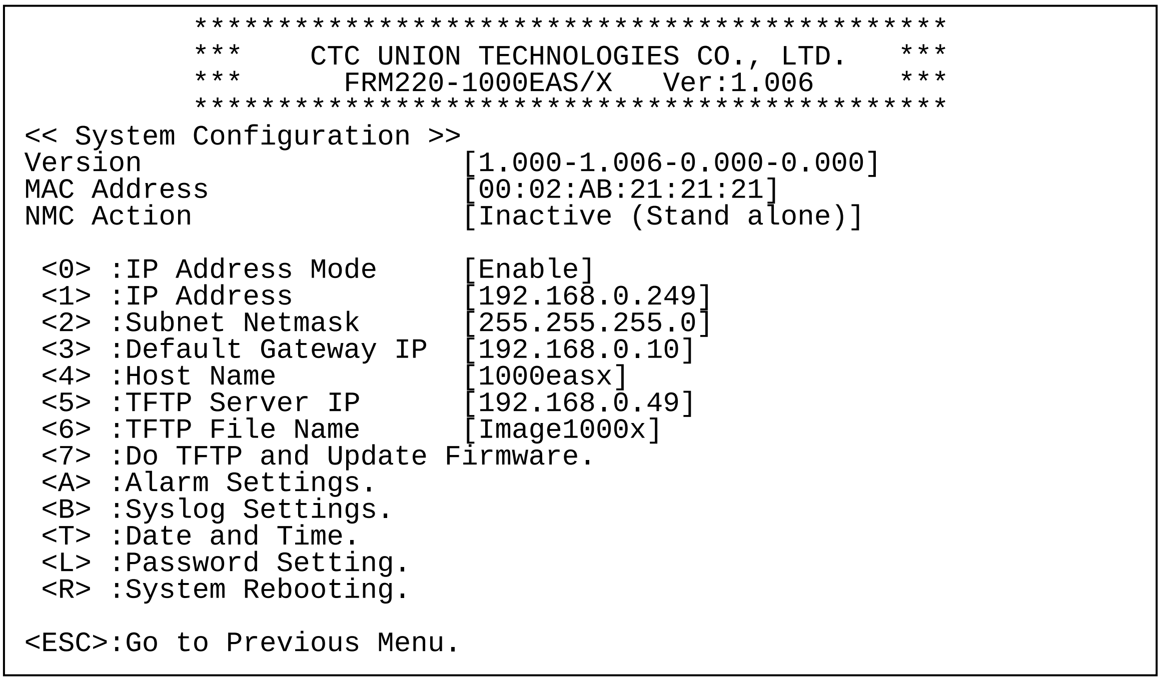
The console operation of **1000EAS/X** uses a simple menu system. From the main menu, using ESC will prompt for a logout. The menu items are selected by simply keying in the menu item's number (in the < > brackets). Some parameter settings are toggled by a single key stroke, while others are selected from additional sub-menus. Unless advised that the unit requires a reboot, all settings take effect immediately

The following is an example of the Main Menu.

```
          *********************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
          ***      FRM220-1000EAS/X   Ver:1.006     ***
          *********************************************
Fiber 1   [Link Up       ] [Remote LB: Off  ]
Fiber 2   [Link Down     ] [Remote LB: Off  ]
UTP   3   [Link Up       ] [Speed: 1000M] [Duplex: Full]
UTP   4   [Link Down     ] [Speed: -----] [Duplex: ----]
Remote A Module    [1000EAS/X       ]
Remote B Module    [Empty           ]
Port 1 OAM Mode    [Active ]
Port 2 OAM Mode    [Active ]
Advance Functions  [Normal ]

 <L> :Local    Status and Configuration.
 <A> :Remote A Status and Configuration.
 <B> :Remote B Status and Configuration.
 <M> :SNMP Manager.
 <S> :System Configuration.

<ESC>:Logout.
```

3.2.2 Configure TCP/IP settings.

From the Main menu select menu item “<S>” System Configuration.



```
          *********************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
          ***      FRM220-1000EAS/X   Ver:1.006     ***
          *********************************************
<< System Configuration >>
Version                   [1.000-1.006-0.000-0.000]
MAC Address               [00:02:AB:21:21:21]
NMC Action                [Inactive (Stand alone)]

 <0> :IP Address Mode     [Enable]
 <1> :IP Address          [192.168.0.249]
 <2> :Subnet Netmask      [255.255.255.0]
 <3> :Default Gateway IP  [192.168.0.10]
 <4> :Host Name           [1000easx]
 <5> :TFTP Server IP      [192.168.0.49]
 <6> :TFTP File Name      [Image1000x]
 <7> :Do TFTP and Update Firmware.
 <A> :Alarm Settings.
 <B> :Syslog Settings.
 <T> :Date and Time.
 <L> :Password Setting.
 <R> :System Rebooting.

<ESC>:Go to Previous Menu.
```

Set any of the parameters here by first selecting the menu item, then key in the parameter value. (For details, see 3.4 System Configuration.) After the parameters have been set, select <R> :System Reboot and **1000EAS/X** will reboot with the new TCP/IP parameters. Once TCP/IP parameters are set for the connected network, **1000EAS/X** will be available for TCP/IP management through Telnet, Web and SNMP.

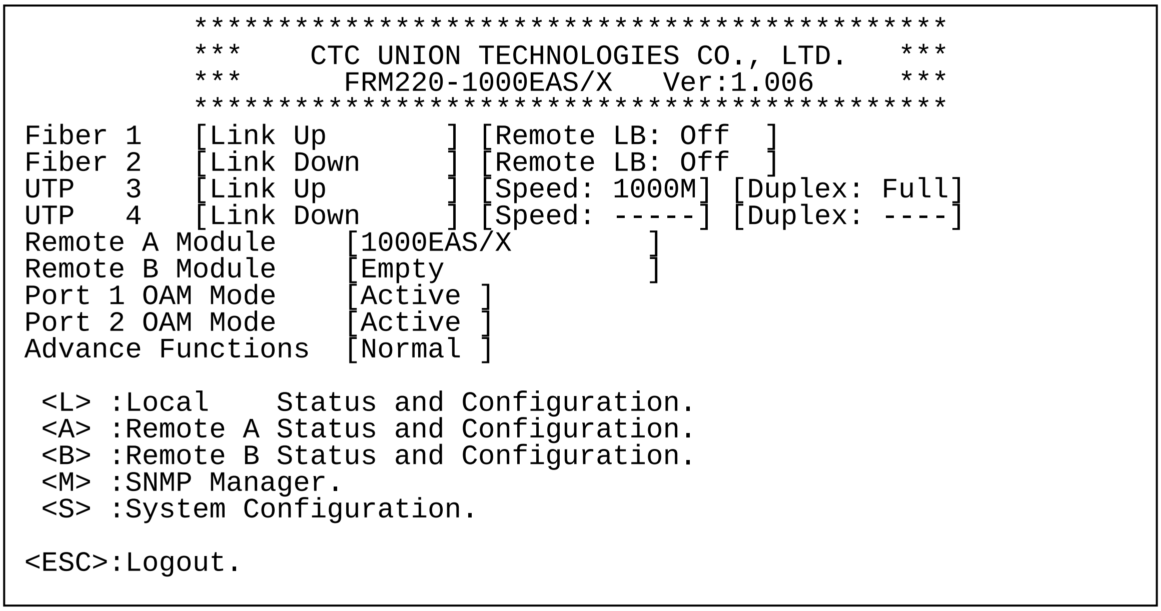
3.3 Telnet Login

Connect one of the copper Ethernet ports to a PC or LAN switch. If the TCP/IP settings have not been done through serial terminal and the unit is still with factory default settings, configure the PC to the same subnet as **1000EAS/X** (recommend 10.1.1.100). Use Telnet protocol (port 23) to connect to **1000EAS/X**. If the password has been enabled, then the factory default will be 'admin/admin'.

3.3.1 Main Menu

The Telnet operation of **1000EAS/X** uses a simple menu system. From the main menu, using ESC will prompt for a logout. It is recommended to use the logout function after finishing configuration or monitoring of **1000EAS/X** so that the Telnet session connection is closed normally. The menu items are selected by simply keying in the menu item's number (in the < > brackets). Some parameter settings are toggled by a single key stroke, while others are selected from additional sub-menus. Unless advised that the unit requires a reboot, all settings take effect immediately.

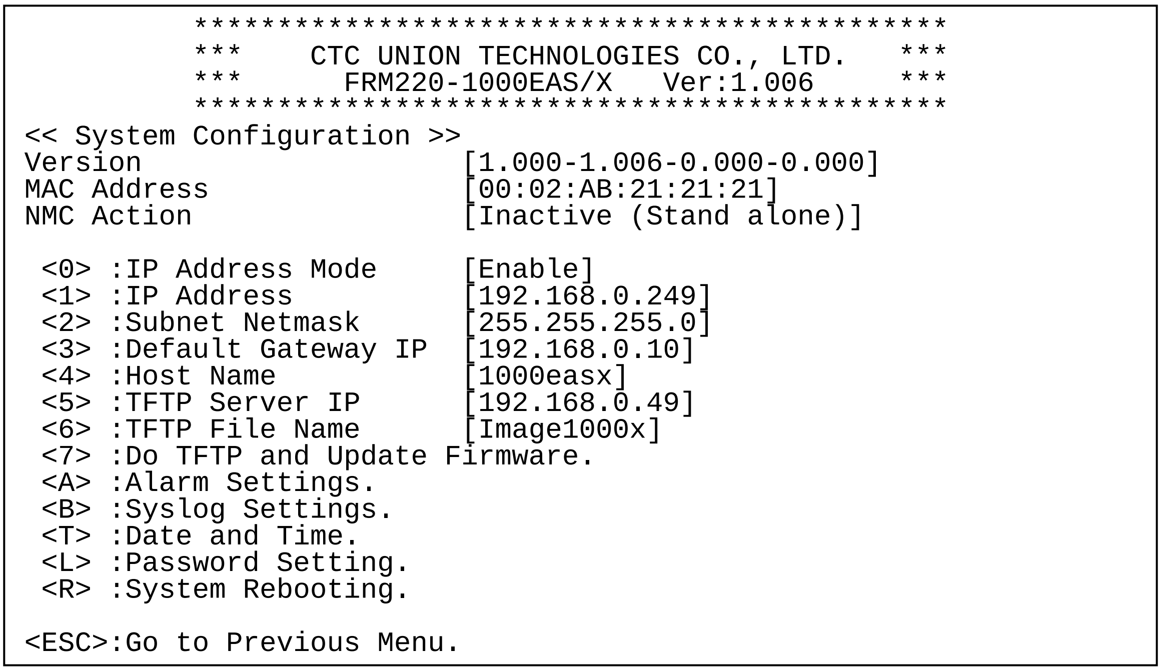
The following page has an example of the Main menu. This menu and all menu operations are identical between serial console with terminal or when using remote Telnet connection. This manual will explain in detail all of the settings as they can be done through the text based menu system. However, many users may prefer to just set the TCP/IP settings and then continue any configuration via the HTTP Web based GUI.



```
          *********************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
          ***      FRM220-1000EAS/X   Ver:1.006     ***
          *********************************************
Fiber 1   [Link Up       ] [Remote LB: Off  ]
Fiber 2   [Link Down     ] [Remote LB: Off  ]
UTP   3   [Link Up       ] [Speed: 1000M] [Duplex: Full]
UTP   4   [Link Down     ] [Speed: -----] [Duplex: ----]
Remote A Module    [1000EAS/X        ]
Remote B Module    [Empty            ]
Port 1 OAM Mode    [Active ]
Port 2 OAM Mode    [Active ]
Advance Functions  [Normal ]

 <L> :Local    Status and Configuration.
 <A> :Remote A Status and Configuration.
 <B> :Remote B Status and Configuration.
 <M> :SNMP Manager.
 <S> :System Configuration.

<ESC>:Logout.
```

3.4 System Configuration

Select item 'S' from main menu, ***System Configuration***



```
          *********************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
          ***      FRM220-1000EAS/X   Ver:1.006     ***
          *********************************************
<< System Configuration >>
Version                   [1.000-1.006-0.000-0.000]
MAC Address               [00:02:AB:21:21:21]
NMC Action                [Inactive (Stand alone)]

 <0> :IP Address Mode     [Enable]
 <1> :IP Address          [192.168.0.249]
 <2> :Subnet Netmask      [255.255.255.0]
 <3> :Default Gateway IP  [192.168.0.10]
 <4> :Host Name           [1000easx]
 <5> :TFTP Server IP      [192.168.0.49]
 <6> :TFTP File Name      [Image1000x]
 <7> :Do TFTP and Update Firmware.
 <A> :Alarm Settings.
 <B> :Syslog Settings.
 <T> :Date and Time.
 <L> :Password Setting.
 <R> :System Rebooting.

<ESC>:Go to Previous Menu.
```

<0> **IP Address Mode** : This toggle is used to able to enable or disable TCP/IP access to the converter. If this converter is placed in a managed chassis or is controlled remotely by OAM, it may be advantageous to disable the IP address so as not to cause IP conflicts.
<1> **IP Address** : This is the IPv4 32 bit Internet Protocol decimal formatted address used to identify this device over the network and provide remote access to it.
<2> **Subnet Mask** : The process of subnetting is the division of a computer network into groups of computers that have a common, designated IP address routing prefix.
<3> **Default Gateway IP** : A default gateway is the node on the computer network that is chosen when the IP address does not match any other routes in the routing table.

<4> : **Host Name** : A hostname is a label that is assigned to a device connected to a computer network and that is used to identify the device in various forms of electronic communication such as on the World Wide Web.
<5> **TFTP Server IP** : Trivial File Transfer Protocol (TFTP) is a file transfer protocol, with the functionality of a very basic form of File Transfer Protocol (FTP). This setting is the IP address of the TFTP server.
<6> **TFTP File Name** : This is the filename (case sensitive) of the firmware image that is placed on the TFTP server and that must be downloaded by the TFTP client in **1000EAS/X** when performing a firmware update.
<7> **Do TFTP and Update Firmware** : This command will start the upgrade process. First the image file will be downloaded into local RAM. If the image is not found or transfer fails, the upgrade process will abort. Once the image is successfully downloaded, it is check to be sure it is the proper image for the right model. At this point, if all is successful, the Flash will be erased and then reprogrammed with the new image. Any power failure during the erase and re-write will result in a 'bricked' unit. There is no recovery except to return to factory where the flash chip must be manually replaced. **DO NOT ALLOW ANY POWER INTERRUPTION DURING FLASHING**.
<A> **Alarm Settings** : This item will bring up a sub-menu for alarm settings. Alarms are indications of fiber or UTP link failure as well as remote converter power failure (dying gasp). Alarms are grouped into two categories; Major Alarms or Minor Alarms. When any alarm occurs, it is then sent as an unsolicited SNMP trap message. For more detailed information please see 3.4.2 Alarm Settings.
<B> **Syslog Settings** : This item brings up the sub menu to configure the alarms to syslog server functions. Alarms for fiber link, UTP link, dying gasp, loop back, login (from console, Telnet or Web) and cold start/reboot can be sent to remote syslog server. Please see 3.4.3 Syslog Settings
<T> **Date and Time** : This item will bring up a sub-menu for the Simple Network Time Protocol (SNTP) settings. For more detailed information please see 3.4.4 Date & Time Setup.
<L> **Password Setting** : This item will bring up a sub-menu for password authentication settings. For more detailed information, please refer to 3.4.5 Password Setup.
<R> **System Rebooting** : This menu item is used to do a "warm boot" of **1000EAS/X**. Any changes to the TCP/IP settings will become active after rebooting.
<ESC> : Pressing the escape key will leave the configuration menu and go back to the main menu.

3.4.1 Firmware Upgrade

Occasionally, **CTC Union** will release new firmware for their products. If new functions are added through software modification or if programming errors are uncovered and resolved, those items will be listed in the firmware ***release note*** which is included in an 'upgrade package' along with a detailed upgrade procedure and the firmware image code.

The ***System Configuration*** menu is where new firmware may be applied to **1000EAS/X**. The firmware is downloaded to the agent using Trivial File Transfer Protocol. Once the TFTP server's IP is configured and the image file name matches the update image placed in the TFTP root or path, item #7 will start the upload process. After the image has been downloaded into memory (approximately 20 seconds), and the check-sum and image ID confirmed, the flash memory will be erased and the image written to the flash memory (non-volatile memory). Following successful flash writing (approximately 50 seconds), **1000EAS/X** will automatically reboot.

WARNING: Never allow any power disruption during the flash erasing and writing process.

Prerequisites:
FRM220A-1000EAS/X in any **FRM220** chassis (1-slot, 2-slot, 4-slot, 8-slot, 20-slot).
Cat 5e or above Ethernet patch cable
Laptop or PC, TCP/IP ready
Telnet client software (PuTTY or HyperTerminal)
TFTP server (free/open source tftp32 by Ph. Jounin)
Upgrade firmware, for version 1.006, released as 'Image1000x' upgrade image file.

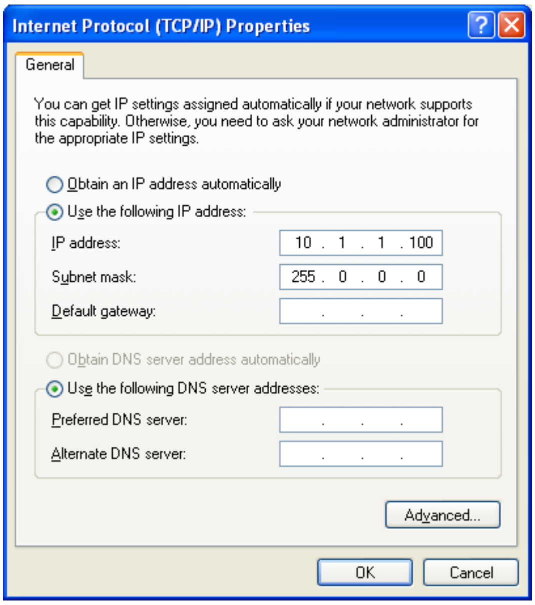
Procedure:

1. Connect **1000EAS/X** Ethernet to the desktop's or laptop's Ethernet port with 1:1 UTP patch cable.

2. Power on **1000EAS/X** and wait until fully booted (minimum 20 seconds). With pen or pencil point, press and hold at least 5 seconds, the 'DEFAULT' switch, located on the lower-right face of converter. Allow to fully boot again (about 30 seconds). This will restore the converter to factory default and known parameters.

3. Configure TCP/IP settings on the desktop or Laptop's Ethernet LAN port for:

a. static IP 10.1.1.100
b. subnet mask 255.0.0.0
c. gateway not necessary



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

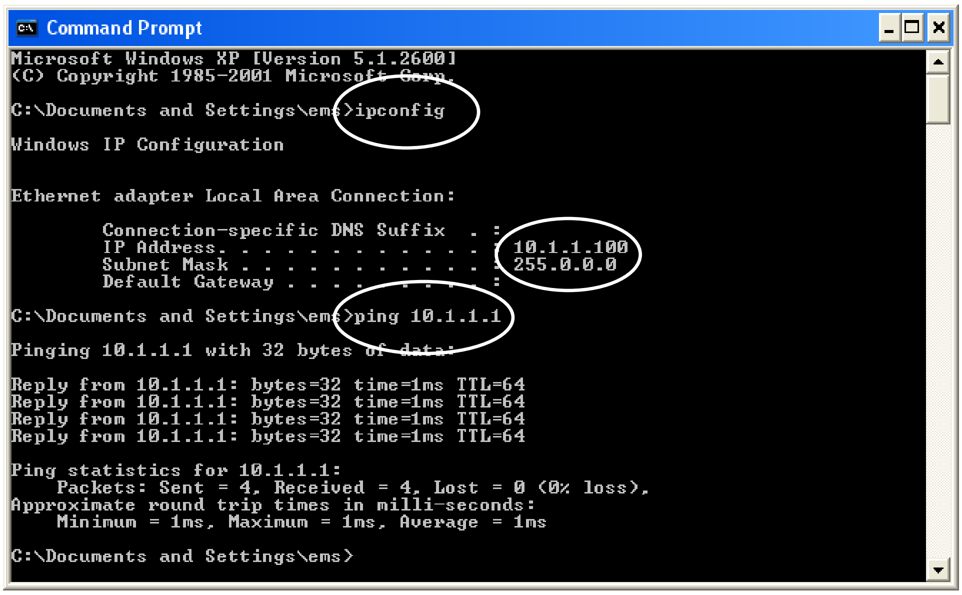
○ Obtain an IP address automatically
● Use the following IP address:

IP address: 10 . 1 . 1 . 100
Subnet mask: 255 . 0 . 0 . 0
Default gateway: . . .

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server: . . .
Alternate DNS server: . . .

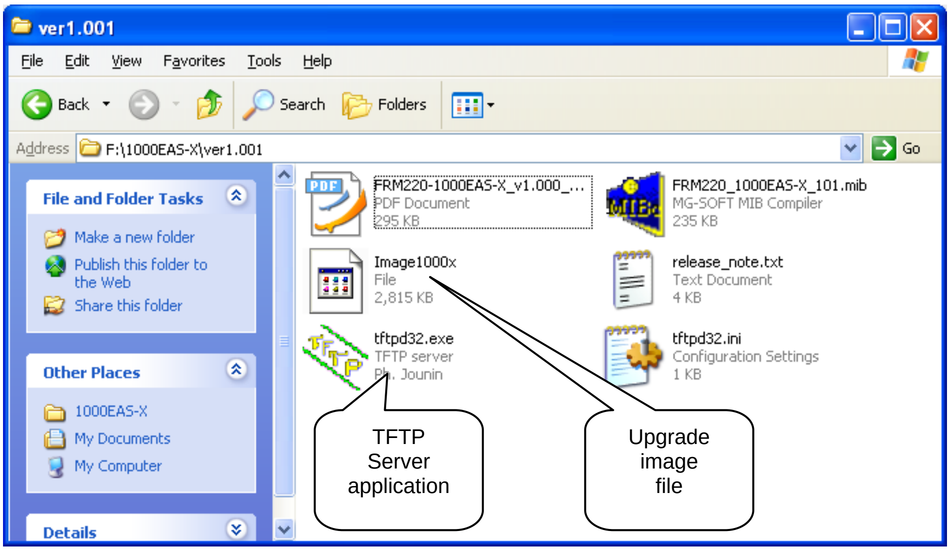
4. Open a command window on the laptop or desktop PC (for example click 'Start' button, click 'Run' and enter 'cmd' in the Run window and click 'OK'). Check the TCP/IP settings with the 'ipconfig' command and then 'ping' **FRM220A-1000EAS/X**. Make sure the network connection works and is reliable. (note: if ping times out, try doing 'arp –d' command, then if still unsuccessful check cables)



Command Prompt

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\ems>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 10.1.1.100
        Subnet Mask . . . . . . . . . . . : 255.0.0.0
        Default Gateway . . . . . . . . . :

C:\Documents and Settings\ems>ping 10.1.1.1

Pinging 10.1.1.1 with 32 bytes of data:

Reply from 10.1.1.1: bytes=32 time=1ms TTL=64
Reply from 10.1.1.1: bytes=32 time=1ms TTL=64
Reply from 10.1.1.1: bytes=32 time=1ms TTL=64
Reply from 10.1.1.1: bytes=32 time=1ms TTL=64

Ping statistics for 10.1.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Documents and Settings\ems>
```

5. Start the TFTP application program by double-clicking the tftp32.exe icon. The program was extracted with the upgrade package. If the firewall complains, select 'Unblock'. Make sure the 'Image1000x' file is located in the same directory as the TFTP application program.



ver1.001

Address F:\1000EAS-X\ver1.001

FRM220-1000EAS-X_v1.000_... PDF Document 295 KB

FRM220_1000EAS-X_101.mib MG-SOFT MIB Compiler 235 KB

Image1000x File 2,815 KB

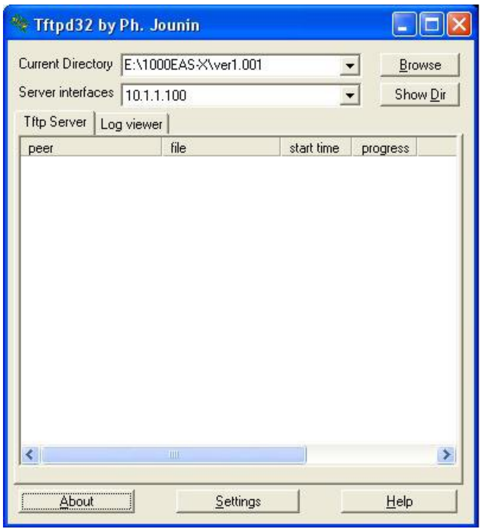
release_note.txt Text Document 4 KB

tftpd32.exe TFTP server Ph. Jounin

tftpd32.ini Configuration Settings 1 KB

TFTP Server application

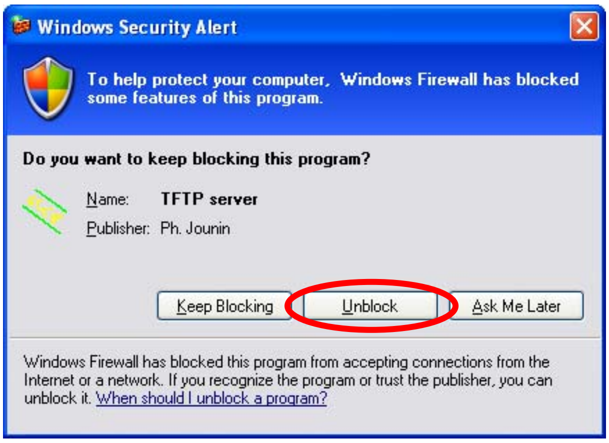
Upgrade image file



Tftpd32 by Ph. Jounin

Current Directory E:\1000EAS-X\ver1.001

Server interfaces 10.1.1.100



Windows Security Alert

To help protect your computer, Windows Firewall has blocked some features of this program.

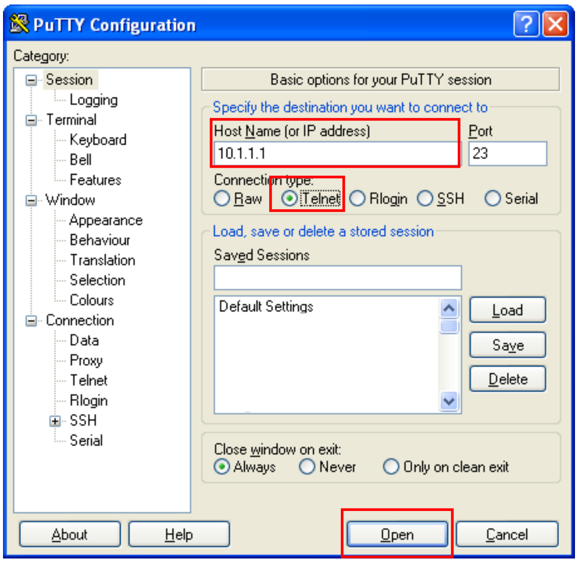
Do you want to keep blocking this program?

Name: TFTP server

Publisher: Ph. Jounin

Windows Firewall has blocked this program from accepting connections from the Internet or a network. If you recognize the program or trust the publisher, you can unblock it. When should I unblock a program?

6. Start the telnet client program of your choice. In this example we are using the PuTTY program, which is open source, free, and very popular with network engineers.



PuTTY Configuration

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): 10.1.1.1

Port: 23

Connection type: ○ Raw ● Telnet ○ Rlogin ○ SSH ○ Serial

Load, save or delete a stored session

Saved Sessions

Default Settings

Close window on exit: ● Always ○ Never ○ Only on clean exit

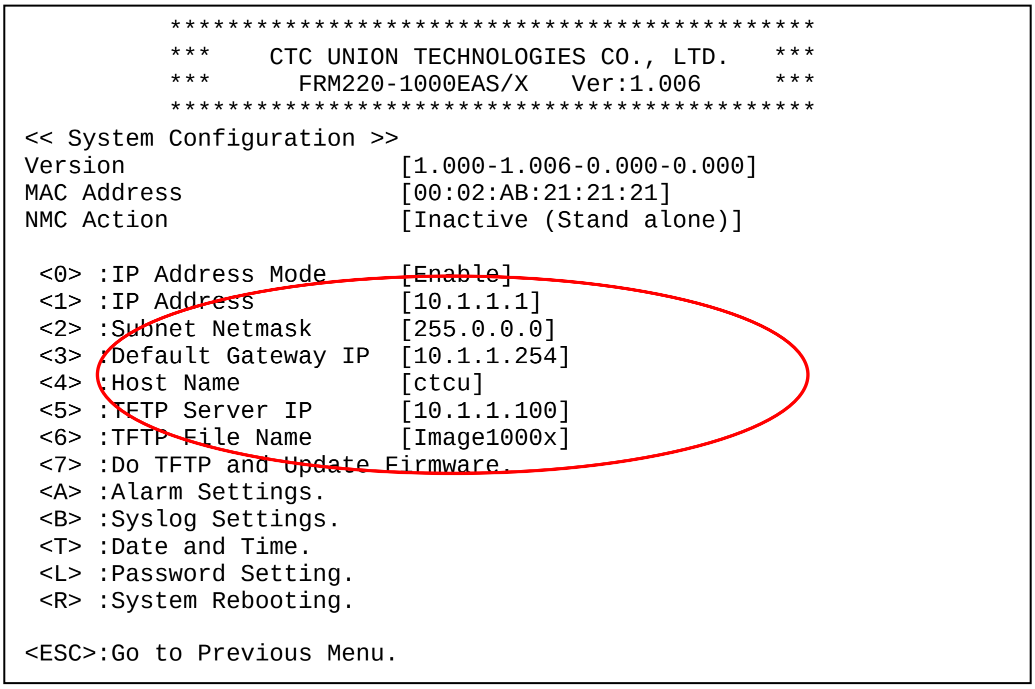
Key-in the IP address, select the 'Telnet' radio button and then click 'Open'.

7. The upgrade is performed by first selecting 'S', "System Configuration" from the Main menu.

The following screens are examples of menu on **FRM220A-1000EAS/X** , version 1.006.

Make sure the settings are correct. The screens below are what you should see if **1000EAS/X** has been returned to its factory default setting. Confirm that the TFTP server IP matches our PC or Laptop and that the image filename matches our upgrade file name.

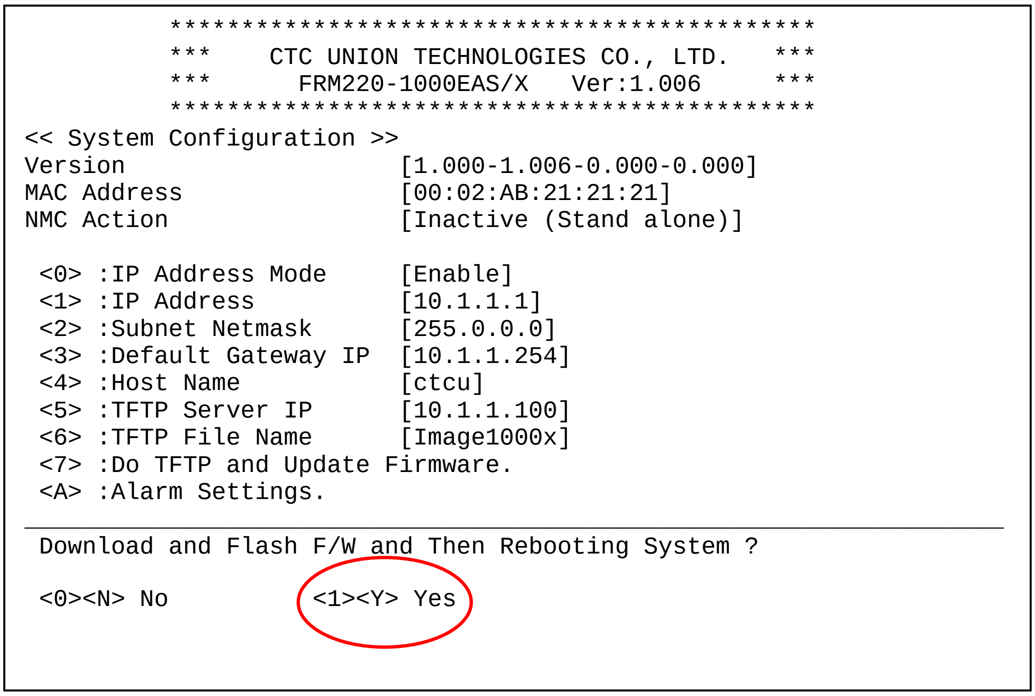
Version 1.00X Screen



```
           *********************************************
           ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
           ***      FRM220-1000EAS/X   Ver:1.006     ***
           *********************************************
<< System Configuration >>
Version                    [1.000-1.006-0.000-0.000]
MAC Address                [00:02:AB:21:21:21]
NMC Action                 [Inactive (Stand alone)]

 <0> :IP Address Mode      [Enable]
 <1> :IP Address           [10.1.1.1]
 <2> :Subnet Netmask       [255.0.0.0]
 <3> :Default Gateway IP   [10.1.1.254]
 <4> :Host Name            [ctcu]
 <5> :TFTP Server IP       [10.1.1.100]
 <6> :TFTP File Name       [Image1000x]
 <7> :Do TFTP and Update Firmware.
 <A> :Alarm Settings.
 <B> :Syslog Settings.
 <T> :Date and Time.
 <L> :Password Setting.
 <R> :System Rebooting.

<ESC>:Go to Previous Menu.
```

Press the '7' key "Do TFTP and Upgrade Firmware".

You will be prompted for a final Yes or No. (key in “1” or “y”)



```
           *********************************************
           ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
           ***      FRM220-1000EAS/X   Ver:1.006     ***
           *********************************************
<< System Configuration >>
Version                    [1.000-1.006-0.000-0.000]
MAC Address                [00:02:AB:21:21:21]
NMC Action                 [Inactive (Stand alone)]

 <0> :IP Address Mode      [Enable]
 <1> :IP Address           [10.1.1.1]
 <2> :Subnet Netmask       [255.0.0.0]
 <3> :Default Gateway IP   [10.1.1.254]
 <4> :Host Name            [ctcu]
 <5> :TFTP Server IP       [10.1.1.100]
 <6> :TFTP File Name       [Image1000x]
 <7> :Do TFTP and Update Firmware.
 <A> :Alarm Settings.
--------------------------------------------------------------------
 Download and Flash F/W and Then Rebooting System ?

 <0><N> No           <1><Y> Yes
```

8. Press the 'Y' key to start TFTP transfer and update. The message like “Write bootpImage to memory” will be displayed. The file transfer takes about 20 seconds.

```
<< System Configuration >>
Version                    [1.000-1.006-0.000-0.000]
MAC Address                [00:02:AB:21:21:21]
NMC Action                 [Inactive (Stand alone)]

 <0> :IP Address Mode      [Enable]
 <1> :IP Address           [10.1.1.1]
 <2> :Subnet Netmask       [255.0.0.0]
 <3> :Default Gateway IP   [10.1.1.254]
 <4> :Host Name            [ctcu]
 <5> :TFTP Server IP       [10.1.1.100]
 <6> :TFTP File Name       [Image1000x]
 <7> :Do TFTP and Update Firmware.
 <A> :Alarm Settings.
____________________________________________________________________
 Upgrade F/W, Please Waiting....

Download Size = 2904707 Bytes.
```

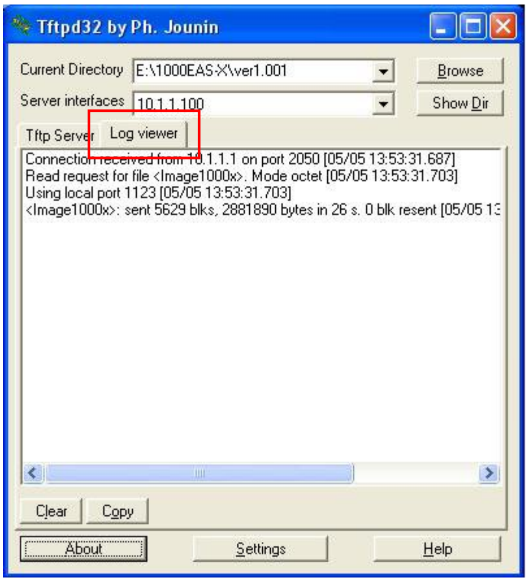
DO NOT CLOSE THE WINDOW OR ALLOW ANY POWER INTERRUPTION!!!! THIS IS VERY IMPORTANT.

The flash writing takes at least 50 seconds. The progress bar gives an approximation of the percent completed. When complete, the “Rebooting …” message will be displayed. **DO NOTHING!!**

```
_____________________________________________________
 Upgrade F/W, Please Waiting....

 Download Size = 2904707 Bytes.
 WARNING: Don`t close this window or turn off the power.
  0%                                       100%
 |############################################|
 Write 2904707 bytes done.

Rebooting ...
```

9. After update, **FRM220A-1000EAS/X** will automatically reboot. The current Telnet session will be closed. (During reboot, all LEDs will first go out, then all LEDs will light. The “Test” LED will extinguish first and a few seconds later the LEDs will return to normal running and link states.)

Check that the TFTP transfer was normal by clicking the ‘Log viewer’ tab.



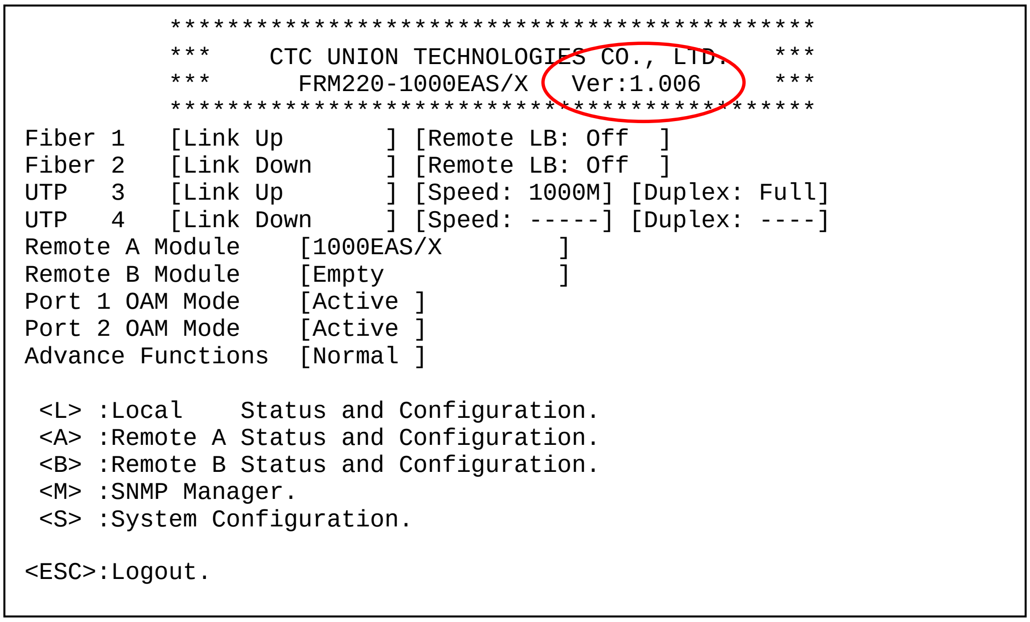
Current Directory E:\1000EAS-X\ver1.001

Server interfaces 10.1.1.100

```
Connection received from 10.1.1.1 on port 2050 [05/05 13:53:31.687]
Read request for file <Image1000x>. Mode octet [05/05 13:53:31.703]
Using local port 1123 [05/05 13:53:31.703]
<Image1000x>: sent 5629 blks, 2881890 bytes in 26 s. 0 blk resent [05/05 13
```

10. Use Telnet client and login to **FRM220A-1000EAS/X** again.

The following screen shows **1000EAS/X** updated to 1.006. For a newer version, this number should reflect this new version.



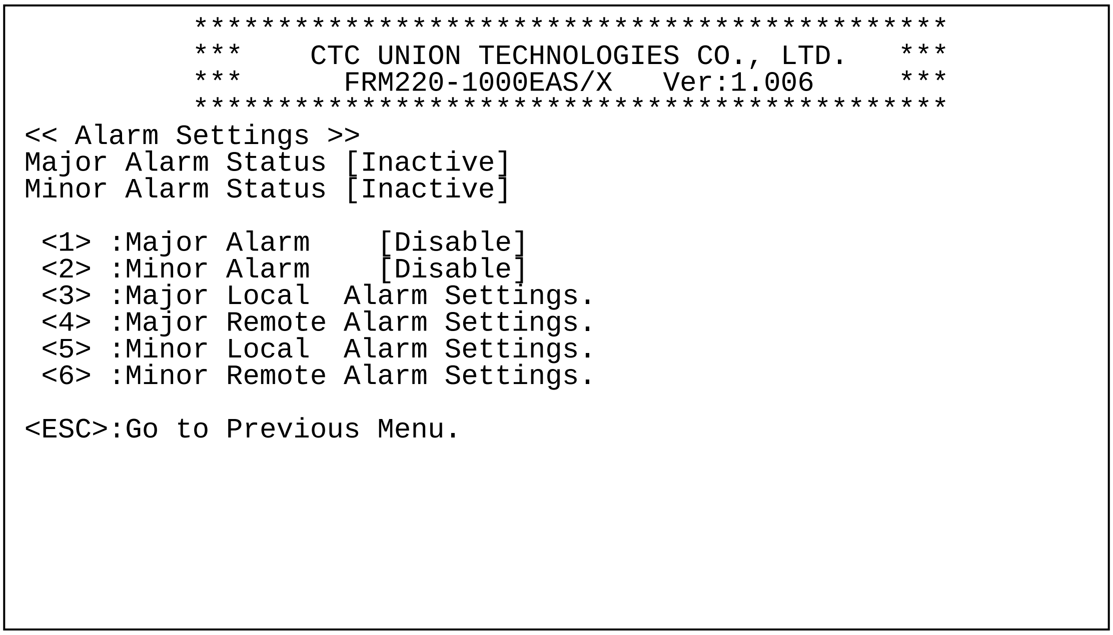
```
          *********************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.    ***
          ***      FRM220-1000EAS/X   Ver:1.006      ***
          *********************************************
Fiber 1   [Link Up       ] [Remote LB: Off  ]
Fiber 2   [Link Down     ] [Remote LB: Off  ]
UTP   3   [Link Up       ] [Speed: 1000M] [Duplex: Full]
UTP   4   [Link Down     ] [Speed: -----] [Duplex: ----]
Remote A Module    [1000EAS/X        ]
Remote B Module    [Empty            ]
Port 1 OAM Mode    [Active ]
Port 2 OAM Mode    [Active ]
Advance Functions  [Normal ]

 <L> :Local    Status and Configuration.
 <A> :Remote A Status and Configuration.
 <B> :Remote B Status and Configuration.
 <M> :SNMP Manager.
 <S> :System Configuration.

<ESC>:Logout.
```

Continue with normal re-configuration.

3.4.2 Alarm Settings

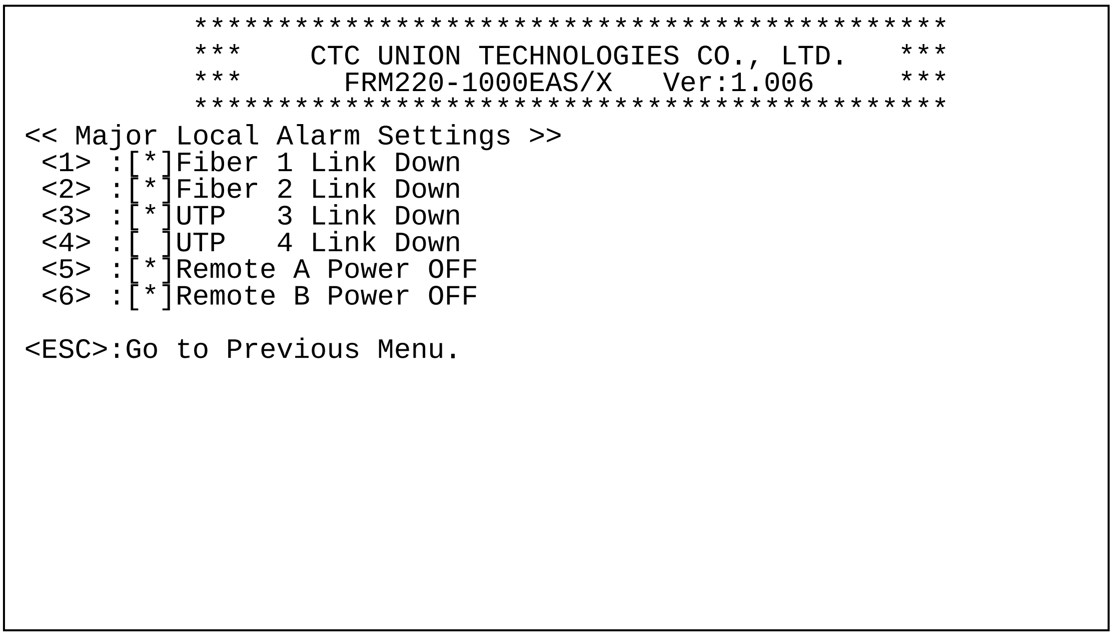
From the **Alarm Settings** menu, we can configure and assign different alarm conditions to either major or minor alarm status. In this way, the network administrator can determine which alarm conditions should be responded to with the highest priority, or which alarms do not need high priority responses.

From the Main Menu, select the <S> (System Configuration) and from this menu select <A> (Alarm Settings).



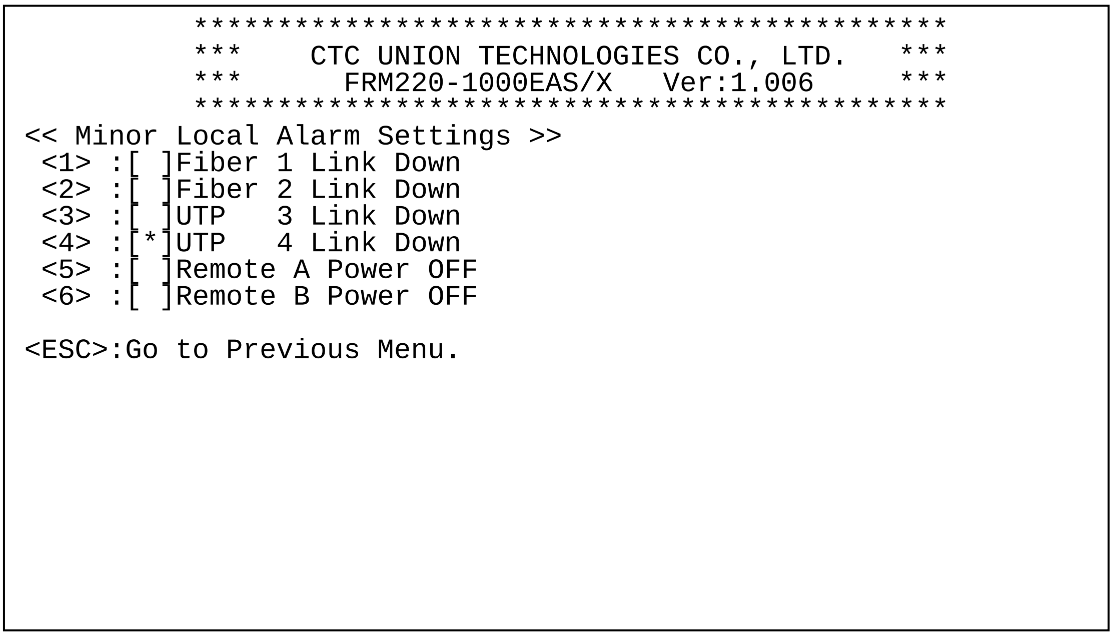
```
          *********************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.    ***
          ***      FRM220-1000EAS/X   Ver:1.006      ***
          *********************************************
<< Alarm Settings >>
Major Alarm Status [Inactive]
Minor Alarm Status [Inactive]

 <1> :Major Alarm    [Disable]
 <2> :Minor Alarm    [Disable]
 <3> :Major Local  Alarm Settings.
 <4> :Major Remote Alarm Settings.
 <5> :Minor Local  Alarm Settings.
 <6> :Minor Remote Alarm Settings.

<ESC>:Go to Previous Menu.
```

In the following example, the Major local alarm indication is presented whenever any of the "checked" events occur. Fiber 1 or 2, UTP-3 link down or remote power failure will be reported as Major alarms.



```
          *********************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.  ***
          ***      FRM220-1000EAS/X   Ver:1.006     ***
          *********************************************
<< Major Local Alarm Settings >>
 <1> :[*]Fiber 1 Link Down
 <2> :[*]Fiber 2 Link Down
 <3> :[*]UTP   3 Link Down
 <4> :[ ]UTP   4 Link Down
 <5> :[*]Remote A Power OFF
 <6> :[*]Remote B Power OFF

<ESC>:Go to Previous Menu.
```

Likewise, Minor local alarms can also be assigned by events. This example shows the local Minor alarms are reported only if UTP-4 link is down.



```
          *********************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.  ***
          ***      FRM220-1000EAS/X   Ver:1.006     ***
          *********************************************
<< Minor Local Alarm Settings >>
 <1> :[ ]Fiber 1 Link Down
 <2> :[ ]Fiber 2 Link Down
 <3> :[ ]UTP   3 Link Down
 <4> :[*]UTP   4 Link Down
 <5> :[ ]Remote A Power OFF
 <6> :[ ]Remote B Power OFF

<ESC>:Go to Previous Menu.
```

Important

In setting of the local and remote units, Major and Minor alarms are key when network management via SNMP is used. When enabled here and when SNMP trap receivers are configured, Major and Minor alarm conditions will be reported through the SNMP mechanism as traps.

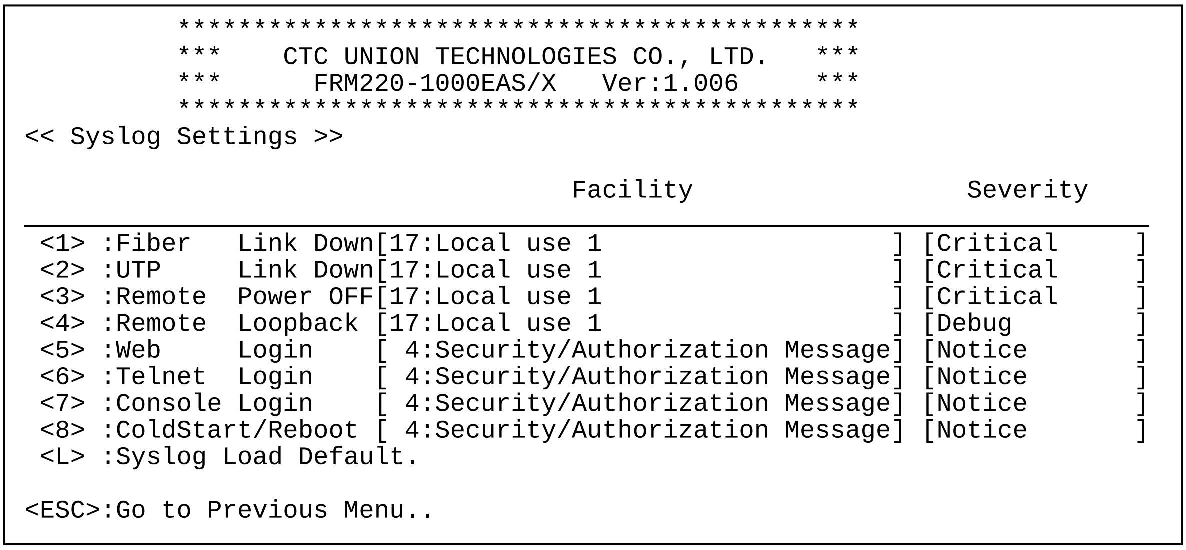
3.4.3 Syslog Settings

Syslog is a standard for logging program messages and is now standardized within the Syslog working group of the IETF. Syslog allows separation of the software that generates messages from the system that stores them and the software that reports and analyzes them.

Syslog, in **1000EAS/X**, can be used for security auditing (login) as well as generalized informational (link down), analysis, and debugging (loop back) messages. The syslog function of **1000EAS/X** can be used to integrate log data into a central repository.

Messages are assigned a priority/level (Emergency, Alert, Critical, Error, Warning, Notice, Info or Debug) by **1000EAS/X** and then sent to syslog server.

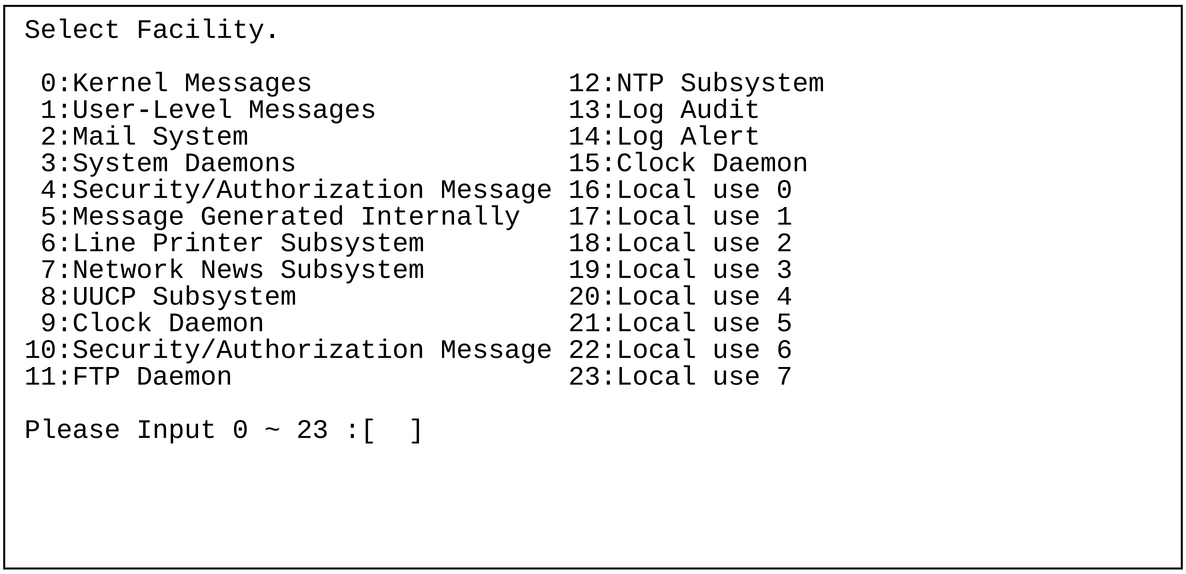
From the Main Menu, select the <S> (System Configuration) and from this menu select <B> (Syslog Settings).



```
          *********************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
          ***      FRM220-1000EAS/X   Ver:1.006     ***
          *********************************************
<< Syslog Settings >>

                                    Facility                  Severity

 <1> :Fiber   Link Down[17:Local use 1                   ] [Critical     ]
 <2> :UTP     Link Down[17:Local use 1                   ] [Critical     ]
 <3> :Remote  Power OFF[17:Local use 1                   ] [Critical     ]
 <4> :Remote  Loopback [17:Local use 1                   ] [Debug        ]
 <5> :Web     Login    [ 4:Security/Authorization Message] [Notice       ]
 <6> :Telnet  Login    [ 4:Security/Authorization Message] [Notice       ]
 <7> :Console Login    [ 4:Security/Authorization Message] [Notice       ]
 <8> :ColdStart/Reboot [ 4:Security/Authorization Message] [Notice       ]
 <L> :Syslog Load Default.

<ESC>:Go to Previous Menu..
```

3.4.3.1 Syslog Facility

For each of 8 items (fiber, UTP, dying gasp, loop back, web login, telnet login, console login and cold start) we can define one of 24 facility types and also define severity level.

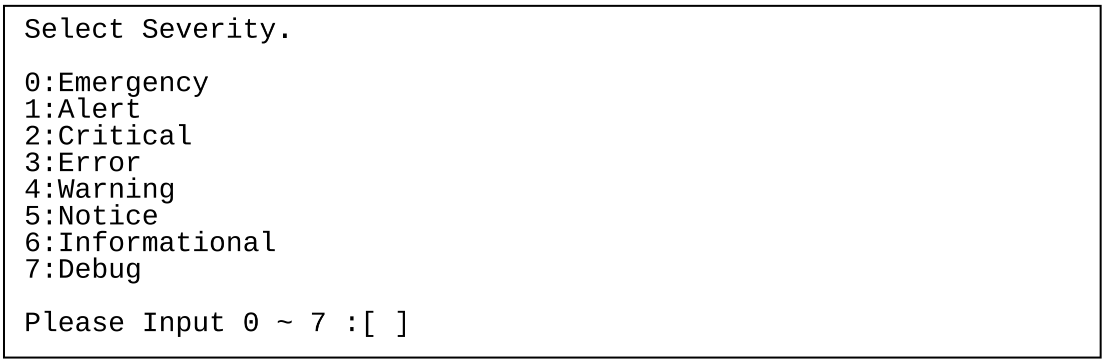


```
Select Facility.

 0:Kernel Messages                12:NTP Subsystem
 1:User-Level Messages            13:Log Audit
 2:Mail System                    14:Log Alert
 3:System Daemons                 15:Clock Daemon
 4:Security/Authorization Message 16:Local use 0
 5:Message Generated Internally   17:Local use 1
 6:Line Printer Subsystem         18:Local use 2
 7:Network News Subsystem         19:Local use 3
 8:UUCP Subsystem                 20:Local use 4
 9:Clock Daemon                   21:Local use 5
10:Security/Authorization Message 22:Local use 6
11:FTP Daemon                     23:Local use 7

Please Input 0 ~ 23 :[  ]
```

By default, the Fiber and UTP link down, dying gasp and loopback are all defined a user facility message. Any logins and reboot are assigned a security/authorization message.

3.4.3.2 Syslog Severity

Each message is also given a severity or priority level with values from 7 to 0 (least severe to most severe).

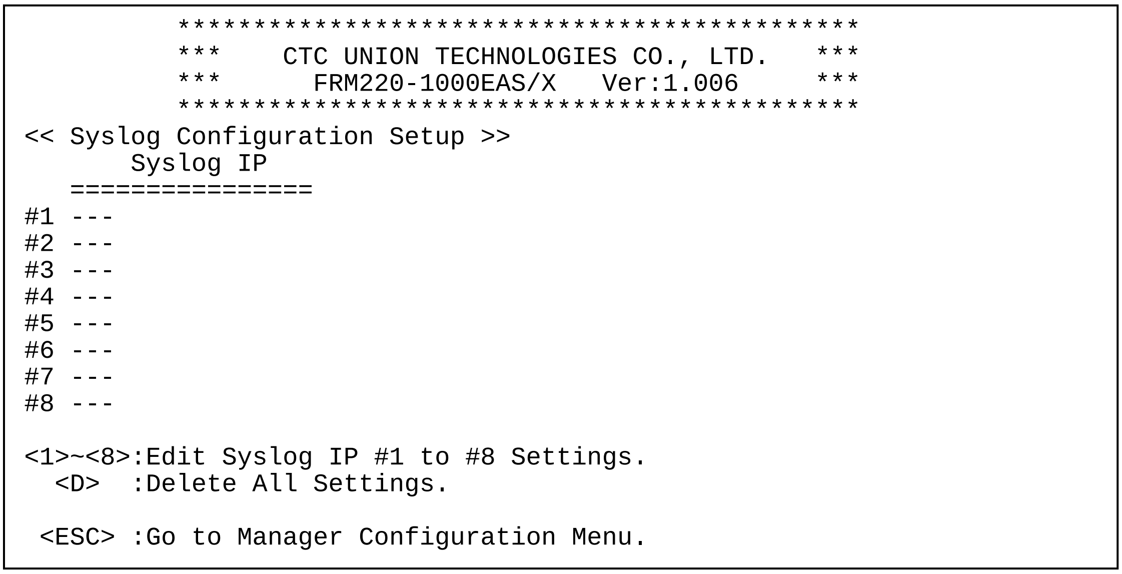


```
Select Severity.

0:Emergency
1:Alert
2:Critical
3:Error
4:Warning
5:Notice
6:Informational
7:Debug

Please Input 0 ~ 7 :[ ]
```

3.4.3.3 Syslog Server Destination

The syslog messages are sent to a syslog server via TCP/IP. Therefore, we must configure in **1000EAS/X**, the destination address for syslog messages.

From the Main Menu, select the <M> (SNMP Manager) and from this menu select <S> (Go to Syslog Configuration Menu).



```
          *********************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
          ***      FRM220-1000EAS/X   Ver:1.006     ***
          *********************************************
<< Syslog Configuration Setup >>
       Syslog IP
   ================
#1 ---
#2 ---
#3 ---
#4 ---
#5 ---
#6 ---
#7 ---
#8 ---

<1>~<8>:Edit Syslog IP #1 to #8 Settings.
  <D>  :Delete All Settings.

 <ESC> :Go to Manager Configuration Menu.
```

There are up to eight entries that can be filled for individual syslog server destination IP addresses. Press any number key, 1 through 8 and key in the syslog server's IP address. Press the <D> key to delete all entries. Using <ESC> will automatically save the settings and exit to a higher level menu. Press <ESC> twice to exit back to the Main Menu.

3.4.4 Date & Time Setup

The date and time setup are important so that any trap messages generated by the SNMP agent will have the correct timestamp. **1000EAS/X** supports setting time manually or automatic time configuration through the use of **NTP** (Network Time Protocol) or **SNTP** (Simple Network Time Protocol).

From the Main Menu, select the <S> (System Configuration) and from this menu select <T> (Date and Time).

```
          *********************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
          ***      FRM220-1000EAS/X   Ver:1.006     ***
          *********************************************
<< Date and Time >>
Current Date And Time [2011-07-20/11:18:20 Wed]
Time Server IP        [220.130.158.71]
Time Zone             [GMT +08:00]
Auto Adjust Time      [Enable]

 <1> :Adjust Current Time.
 <2> :Set Time Server IP.
 <3> :Set Time Zone.
 <4> :Enable/Disable Auto Synchronize Time.
 <5> :Synchronize Time with NTP Server.

<ESC>:Go to Previous Menu.
```

1. **Adjust Current Time** – Use this menu item to manually adjust the date and time.
2. **Set Time Server IP** – The time server IP is the IP address of a NTP server that provides time synchronization services on a network. Geographically close servers should be chosen from the pool of NTP servers.
3. **Set Time Zone** – All network time is synchronized to UTC (Coordinated Universal Time) which is based on International Atomic Time. The time zone setting will let the UTC time appear correctly for your geographic location. Time zone settings are + (East) or – (West) full or half hours from UTC coordinates or previously known as GMT (Greenwich Mean Time).
4. **Enable/Disable Auto Synchronize Time** – When auto synchronization is enabled, the SNTP daemon in **1000EAS/X** will poll and update time from the time server once every hour.
5. **Synchronize Time with NTP Server** – This action will cause the SNTP daemon to immediately poll and update date and time with the NTP server. The results will either be a 'timeout' or the time will be successfully synchronized.

3.4.5 Password Setup

Access to **1000EAS/X** via Telnet or Web is controlled by the use of user passwords. One user ID account can be created and assigned password for authentication. The management interface can only then be accessed by using the correct username and password.

From the Main Menu, select the <S> (System Configuration) and from this menu select <L> (Password Setting).

```
          *********************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
          ***      FRM220-1000EAS/X   Ver:1.003     ***
          *********************************************
<< Password Configuration >>
 <1> :Login Password      [Disable]
 <2> :Set New UID and Password.

<ESC>:Go to Previous Menu.
```

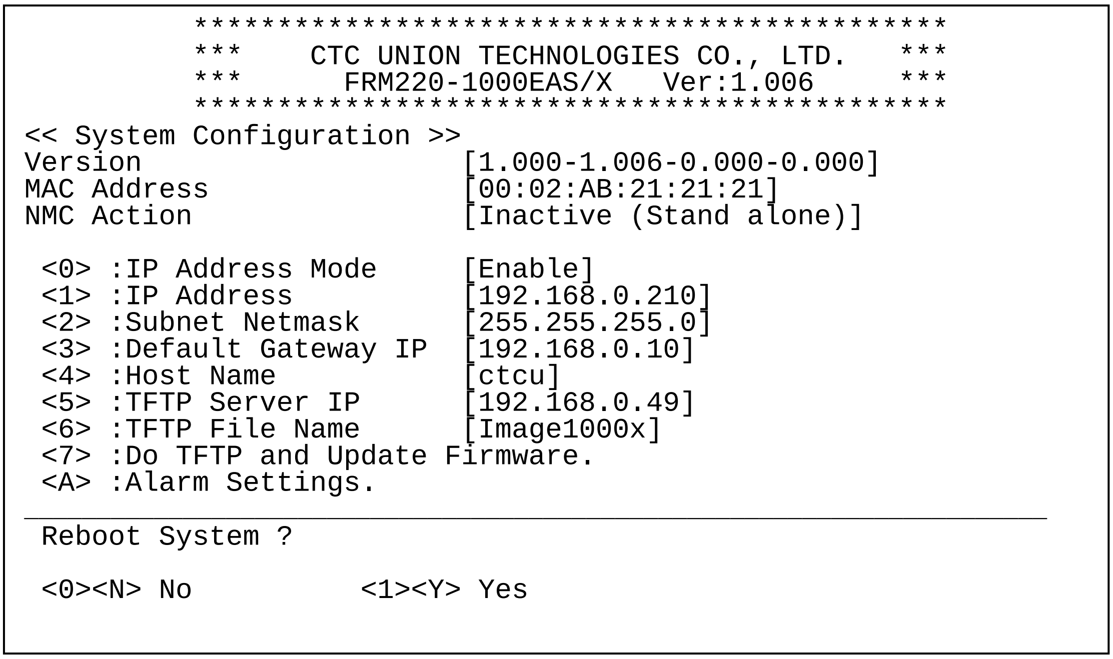
1. **Login Password** – Enable or disable the password authorization feature.
2. **Set New UID and Password** – Key-in username and password for management authentication. If the password is lost, the unit must be reset to factory default. See section 1.7.

3.4.6 System Reboot

The system reboot feature allows an operator to remotely cause **1000EAS/X** to do a 'warm boot'. The system reboot will send a reset signal to both the embedded CPU chip and to the L2 switch chip. The CPU will then reboot the kernel and reinitialize the switch chip with the stored configuration settings.

Caution should be exercised when doing a system reset as all traffic through all ports of the device will be blocked until the switch chip is initialized. In addition, the OAM discovery and negotiation will need to redo. If enabled, STP (Spanning Tree Protocol) discovery will need to rebuild path tables.

From the Main Menu, select the <S> (System Configuration) and from this menu select <R> (System Rebooting). Confirmation is required.

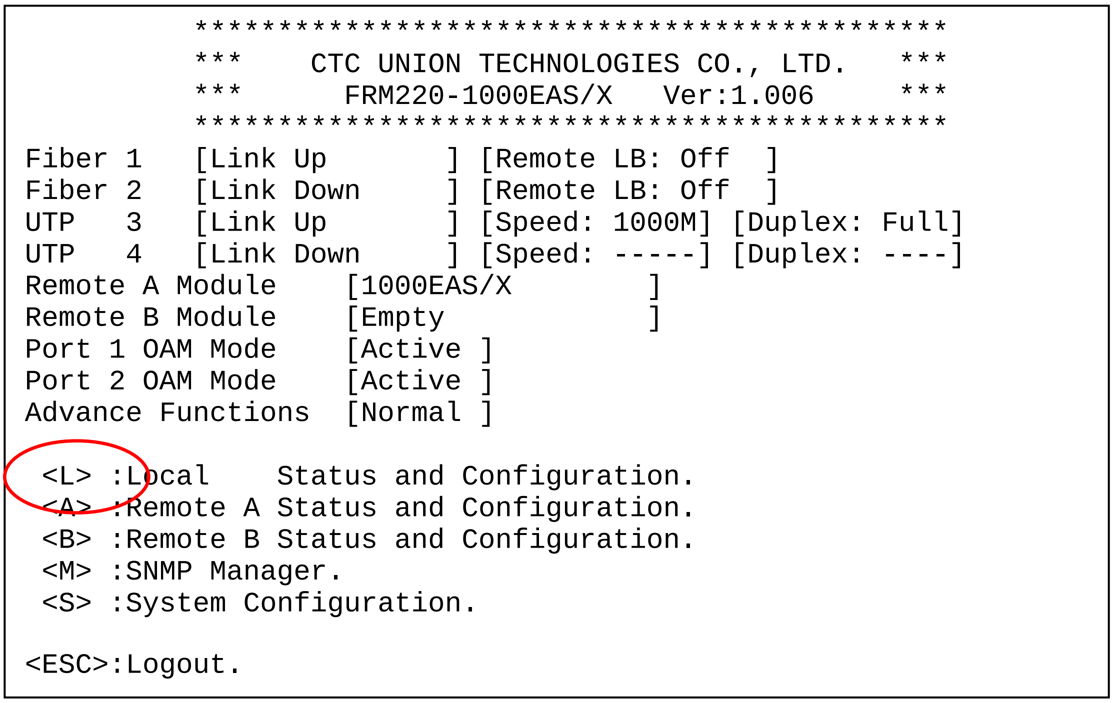


```
           *********************************************
           ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
           ***      FRM220-1000EAS/X   Ver:1.006     ***
           *********************************************
<< System Configuration >>
Version                    [1.000-1.006-0.000-0.000]
MAC Address                [00:02:AB:21:21:21]
NMC Action                 [Inactive (Stand alone)]

 <0> :IP Address Mode      [Enable]
 <1> :IP Address           [192.168.0.210]
 <2> :Subnet Netmask       [255.255.255.0]
 <3> :Default Gateway IP   [192.168.0.10]
 <4> :Host Name            [ctcu]
 <5> :TFTP Server IP       [192.168.0.49]
 <6> :TFTP File Name       [Image1000x]
 <7> :Do TFTP and Update Firmware.
 <A> :Alarm Settings.
_____________________________________________________________
 Reboot System ?

 <0><N> No          <1><Y> Yes
```

When **1000EAS/X** does a warm start, the process is almost identical to a cold start.

1. The switch chip is reset at which point all traffic is blocked.
2. The CPU is reset at the same time.
3. The boot process is started from the bootloader read from flash.
4. The bootloader instructs the CPU to copy the image from flash and decompress into RAM.
5. Once the image has decompressed into ram, the CPU continues to execute program from RAM.
6. The previous network settings stored in serial EPROM are used to configure the device's network configuration.
7. The configuration settings stored in the serial EPROM are read and the settings are programmed into the switch chip.
8. Traffic will then start to transmit through the switch normally.
9. If OAM is enabled, the OAM discovery will occur.
10. If STP is enabled, the switch won't start to forward packets until the path tables are rebuilt through learning.

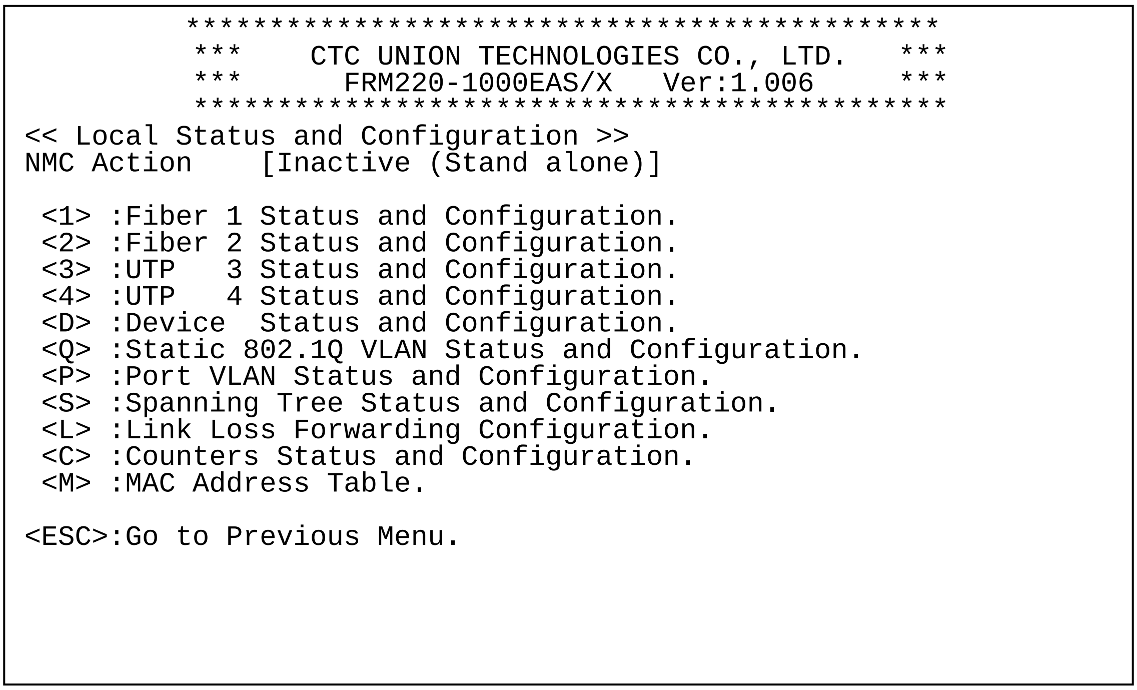
3.4.7 Fiber Port Provisioning



```
          *********************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
          ***      FRM220-1000EAS/X   Ver:1.006     ***
          *********************************************
Fiber 1   [Link Up       ] [Remote LB: Off  ]
Fiber 2   [Link Down     ] [Remote LB: Off  ]
UTP   3   [Link Up       ] [Speed: 1000M] [Duplex: Full]
UTP   4   [Link Down     ] [Speed: -----] [Duplex: ----]
Remote A Module    [1000EAS/X        ]
Remote B Module    [Empty            ]
Port 1 OAM Mode    [Active ]
Port 2 OAM Mode    [Active ]
Advance Functions  [Normal ]

 <L> :Local    Status and Configuration.
 <A> :Remote A Status and Configuration.
 <B> :Remote B Status and Configuration.
 <M> :SNMP Manager.
 <S> :System Configuration.

<ESC>:Logout.
```

Select item 'L' from the main menu.

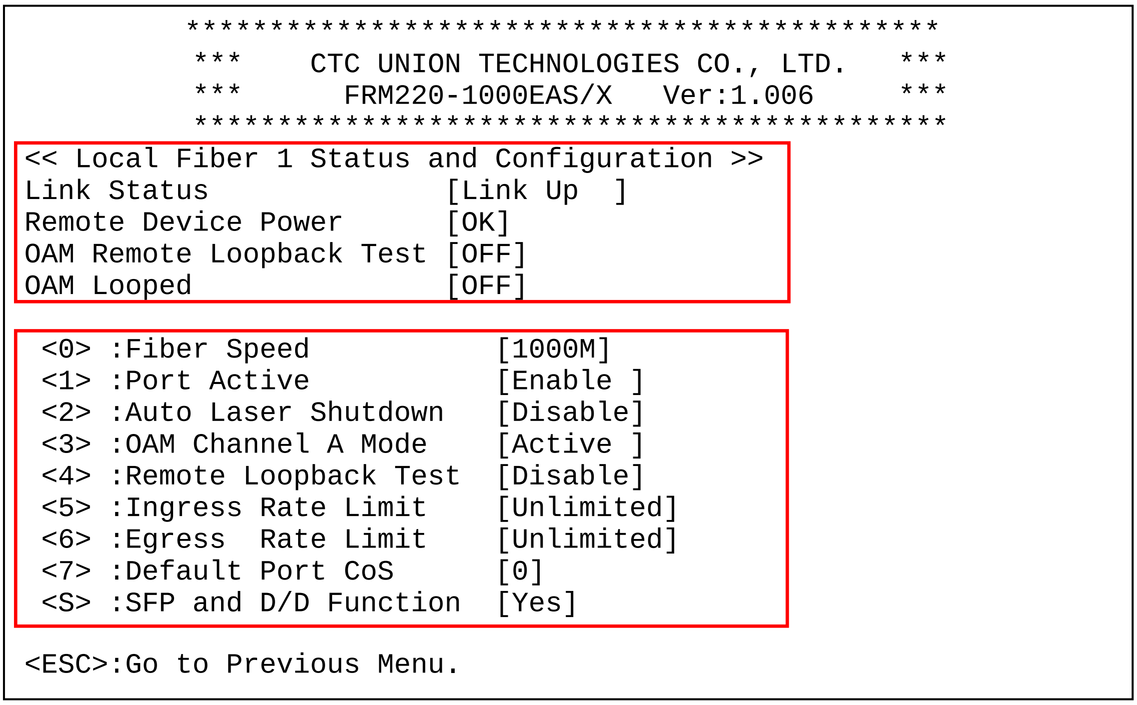
From the ***Local Status and Configuration*** menu, each port can be managed (activated or disabled, speed & duplex set, ingress & egress bandwidth rates set, and diagnostic loop back performed) and monitored (link status, RMON counters, DD functions, dying gasp) individually per port. Select port number. Select items by number/letters.



```
          *********************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
          ***      FRM220-1000EAS/X   Ver:1.006     ***
          *********************************************
<< Local Status and Configuration >>
NMC Action    [Inactive (Stand alone)]

 <1> :Fiber 1 Status and Configuration.
 <2> :Fiber 2 Status and Configuration.
 <3> :UTP   3 Status and Configuration.
 <4> :UTP   4 Status and Configuration.
 <D> :Device  Status and Configuration.
 <Q> :Static 802.1Q VLAN Status and Configuration.
 <P> :Port VLAN Status and Configuration.
 <S> :Spanning Tree Status and Configuration.
 <L> :Link Loss Forwarding Configuration.
 <C> :Counters Status and Configuration.
 <M> :MAC Address Table.

<ESC>:Go to Previous Menu.
```

Select the first fiber port by keying "1" at the console.

3.4.7.1 Fiber Port 1 Provisioning

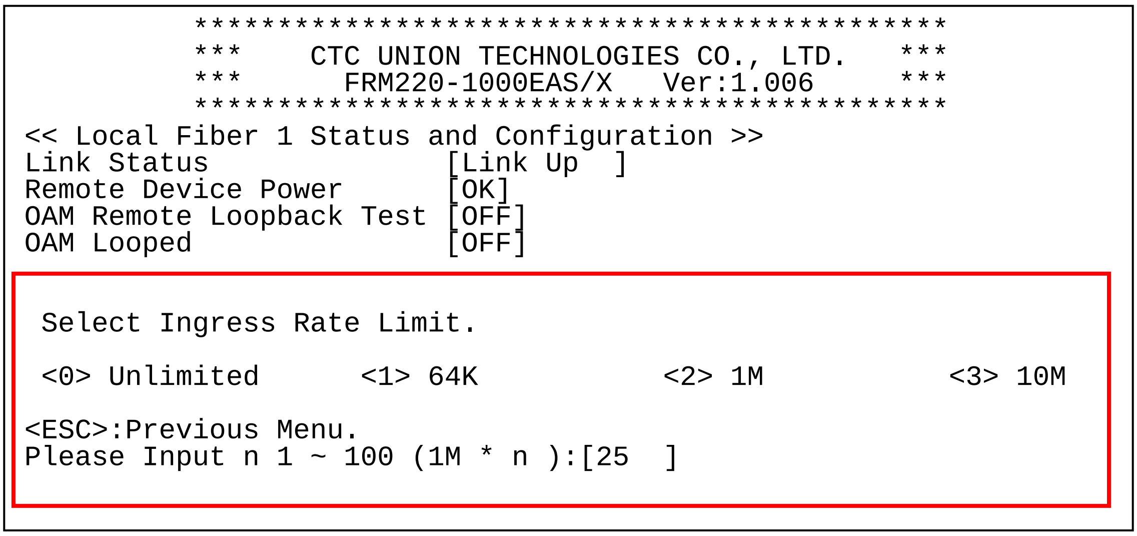


```
          *********************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
          ***      FRM220-1000EAS/X   Ver:1.006     ***
          *********************************************
<< Local Fiber 1 Status and Configuration >>
Link Status              [Link Up  ]
Remote Device Power      [OK]
OAM Remote Loopback Test [OFF]
OAM Looped               [OFF]

 <0> :Fiber Speed           [1000M]
 <1> :Port Active           [Enable ]
 <2> :Auto Laser Shutdown   [Disable]
 <3> :OAM Channel A Mode    [Active ]
 <4> :Remote Loopback Test  [Disable]
 <5> :Ingress Rate Limit    [Unlimited]
 <6> :Egress  Rate Limit    [Unlimited]
 <7> :Default Port CoS      [0]
 <S> :SFP and D/D Function  [Yes]

<ESC>:Go to Previous Menu.
```

<0> **Fiber Speed** : 1000EAS/X supports dual rate for the fiber ports. The selection must be done manually for either 100M or 1000M with 1000M being the default. For 1000M, 1.25Gbps SFP modules are required and for 100M, 155Mbps modules should be used. Multi-Rate type SFP may also be used, but in all cases the fiber port data rate must be manually set. There is no standard for fiber port speed negotiation.
<1> **Port Active** : When disabled, this port will no longer transfer any data and the link will be down.
<2> **Auto Laser Shutdown** : This safety feature, when enabled, will disable the transmit laser if there is no received signal. It is also referred to as 'ALS'.
<3> **OAM Channel A Mode** : The OAM can be disabled or enabled. Within an OAM broadcast link, there should only be one 'active' unit and other unit should be 'passive'.
<4> **Remote Loopback Test** : This function enables or disables the remote OAM loopback test. When active, OAM loopback frames are sent and the remote equipment should acknowledge them. The link integrity can be confirmed without using IP protocol. OAM loopback is non-intrusive to normal Ethernet traffic.
<5> & <6> **Ingress/Egress Rate Limit** : These bandwidth control settings are explained in more detail under 3.4.8 Fiber Port 1 Rate Limiting.
<7> **Default Port CoS** : The Class of Service is a 3 bit field within an Ethernet frame header when using 802.1Q tagging. The field specifies a priority value of between 0 and 7 inclusive that can be used by Quality of Service (QoS) disciplines to differentiate traffic. When 802.1Q is not enabled, there is no tag and therefore no 802.1p tag priority. Use this setting to set the default CoS for this port (0 to 7).
<S> **SFP and D/D Function** : The MSA (Multi-Source Agreement) information can be displayed for the inserted SFP module. An example is shown in 3.4.9 SFP and D/D Functions.

3.4.8 Fiber Port 1 Rate Limiting

1000EAS/X provides per port ingress and egress rate limiting. For bandwidth settings, IRL or ingress rate limit refers to limiting any packets coming into that switch port, while ERL or egress rate limit refers to limiting packets leaving that port. When rate limiting is applied, ERL will use pause commands (802.3X) when the desired rate limit is exceeded, while any IRL setting will cause packets to be dropped when the limit is exceeded. This is an important point when doing the rate limit settings. It is preferable to set ERL at each port for the path that requires limiting so that flow control can help connected devices cope with the limiting. If IRL is employed, a connected device which has its packets dropped without flow control, will continue to send packets at its full rate. Also, since the packets are dropped, the application layer must deal with the packet loss by timing out.

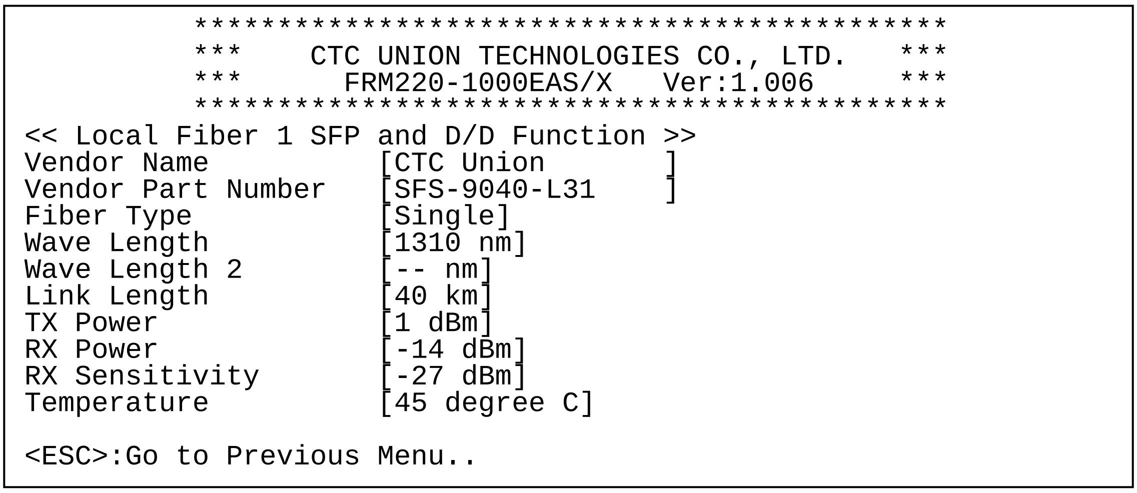


```
           *********************************************
           ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
           ***      FRM220-1000EAS/X   Ver:1.006     ***
           *********************************************
<< Local Fiber 1 Status and Configuration >>
Link Status              [Link Up  ]
Remote Device Power      [OK]
OAM Remote Loopback Test [OFF]
OAM Looped               [OFF]

 Select Ingress Rate Limit.

 <0> Unlimited      <1> 64K             <2> 1M             <3> 10M

<ESC>:Previous Menu.
Please Input n 1 ~ 100 (1M * n ):[25  ]
```

First choose the granularity of 64K, 1M or 10M. Then key the ‘n’ value. In the above example, granularity has been set at 1M. The n value of 25 results in 25M rate limit. The same setting rates can be applied to the egress direction.

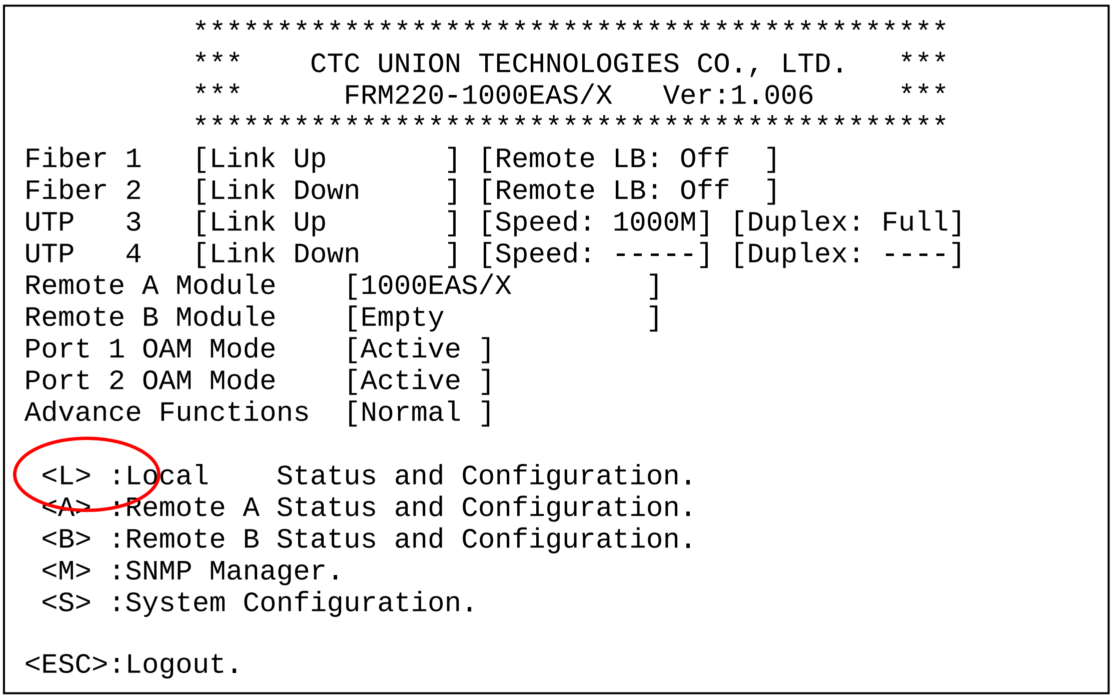
3.4.9 SFP and D/D Functions

Modern optical SFP transceivers support digital diagnostics monitoring (DD) functions according to the industry-standard SFF-8472. This optional feature in SFP is also known as digital optical monitoring (DOM) and gives the end user the ability to monitor real-time parameters of the SFP, such as optical output power, optical input power, temperature, etc. DD is not available in every SFP, so if the function says 'No' then the inserted SFP does not support DD. To view this menu, press "S" from the Fiber Status and Configuration menu.



```
           *********************************************
           ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
           ***      FRM220-1000EAS/X   Ver:1.006     ***
           *********************************************
<< Local Fiber 1 SFP and D/D Function >>
Vendor Name          [CTC Union        ]
Vendor Part Number   [SFS-9040-L31     ]
Fiber Type           [Single]
Wave Length          [1310 nm]
Wave Length 2        [-- nm]
Link Length          [40 km]
TX Power             [1 dBm]
RX Power             [-14 dBm]
RX Sensitivity       [-27 dBm]
Temperature          [45 degree C]

<ESC>:Go to Previous Menu..
```

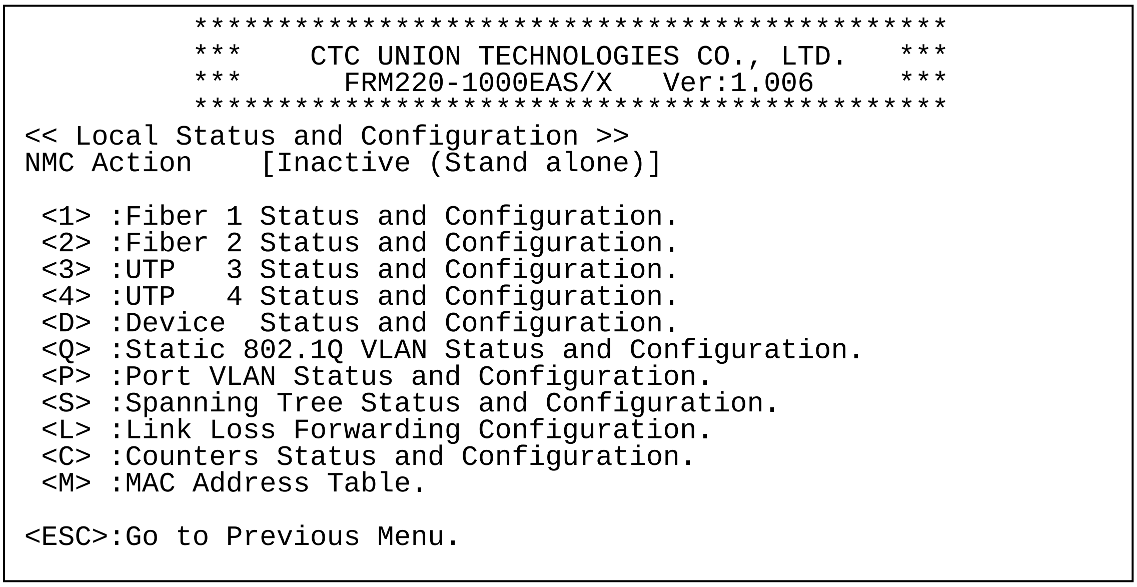
3.4.10 UTP Port Provisioning



```
          ********************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
          ***      FRM220-1000EAS/X   Ver:1.006     ***
          ********************************************
Fiber 1   [Link Up      ] [Remote LB: Off  ]
Fiber 2   [Link Down    ] [Remote LB: Off  ]
UTP   3   [Link Up      ] [Speed: 1000M] [Duplex: Full]
UTP   4   [Link Down    ] [Speed: -----] [Duplex: ----]
Remote A Module     [1000EAS/X         ]
Remote B Module     [Empty             ]
Port 1 OAM Mode     [Active ]
Port 2 OAM Mode     [Active ]
Advance Functions   [Normal ]

 <L> :Local    Status and Configuration.
 <A> :Remote A Status and Configuration.
 <B> :Remote B Status and Configuration.
 <M> :SNMP Manager.
 <S> :System Configuration.

<ESC>:Logout.
```

Select item 'L' from the main menu.

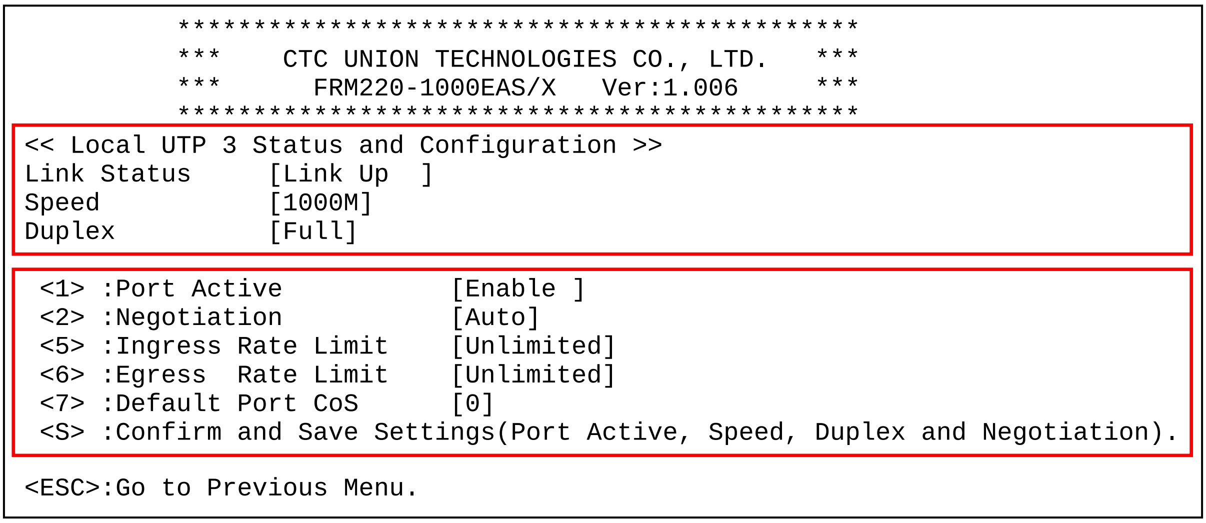
From the ***Local Status and Configuration*** menu, each UTP port can be managed (activated or disabled, speed & duplex set, ingress & egress bandwidth rates set, and diagnostic loop back performed) individually per port. Select port number. Select items by number/letters.



```
          ********************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
          ***      FRM220-1000EAS/X   Ver:1.006     ***
          ********************************************
<< Local Status and Configuration >>
NMC Action    [Inactive (Stand alone)]

 <1> :Fiber 1 Status and Configuration.
 <2> :Fiber 2 Status and Configuration.
 <3> :UTP   3 Status and Configuration.
 <4> :UTP   4 Status and Configuration.
 <D> :Device  Status and Configuration.
 <Q> :Static 802.1Q VLAN Status and Configuration.
 <P> :Port VLAN Status and Configuration.
 <S> :Spanning Tree Status and Configuration.
 <L> :Link Loss Forwarding Configuration.
 <C> :Counters Status and Configuration.
 <M> :MAC Address Table.

<ESC>:Go to Previous Menu.
```

Select the first UTP port by keying "3" at the console.

3.4.10.1 UTP Port 3 Provisioning

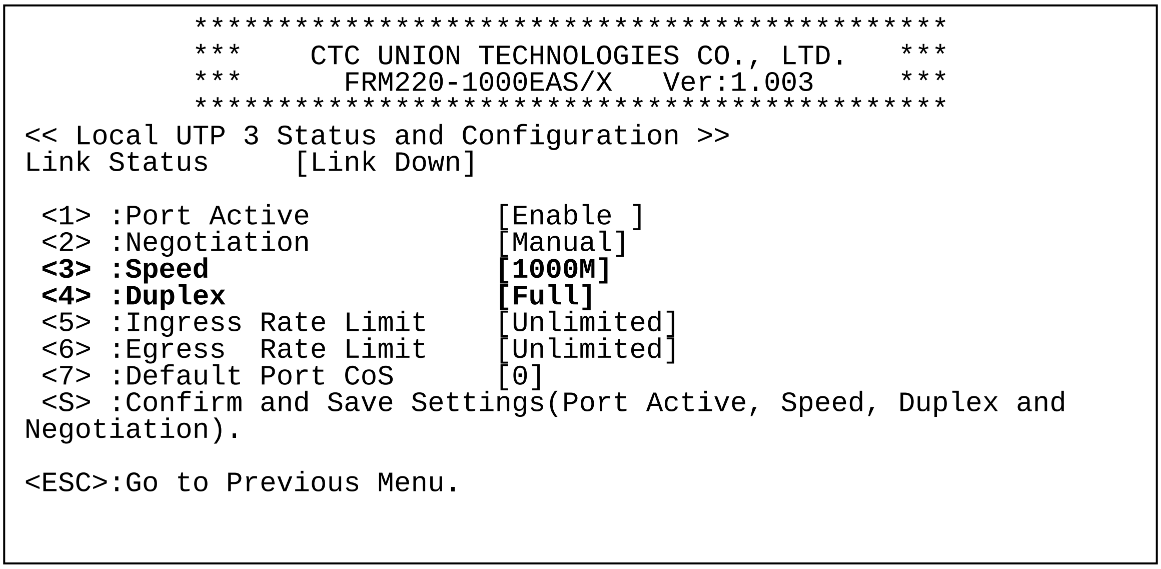


```
           *********************************************
           ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
           ***      FRM220-1000EAS/X   Ver:1.006     ***
           *********************************************
<< Local UTP 3 Status and Configuration >>
Link Status     [Link Up  ]
Speed           [1000M]
Duplex          [Full]

 <1> :Port Active           [Enable ]
 <2> :Negotiation           [Auto]
 <5> :Ingress Rate Limit    [Unlimited]
 <6> :Egress  Rate Limit    [Unlimited]
 <7> :Default Port CoS      [0]
 <S> :Confirm and Save Settings(Port Active, Speed, Duplex and Negotiation).

<ESC>:Go to Previous Menu.
```

<1> **Port Active** : When disabled, this port will no longer transfer any data and the link will be down.
<2> **Negotiation** : The UTP ports of this converter follow IEEE802.3u standards for n-way auto-negotiation. The port can also be manually configured, over-riding the auto-negotiation in "forced" or manual mode. These port settings are explained in more detail under 3.4.10.2 UTP Port 3 Negotiation.
<5> & <6> **Ingress/Egress Rate Limit** : These bandwidth control settings are explained in more detail under 3.4.10.3 UTP Port 3 Rate Limiting.
<7> **Default Port CoS** : The Class of Service is a 3 bit field within an Ethernet frame header when using 802.1Q tagging. The field specifies a priority value of between 0 and 7 inclusive that can be used by Quality of Service (QoS) disciplines to differentiate traffic. When 802.1Q is not enabled, there is no tag and therefore no 802.1p tag priority. Use this setting to set the default CoS for this port (0 to 7).
<S> **Confirm and Save Settings** : Any settings made in this menu are not saved and only become active when this save procedure is completed.

3.4.10.2 UTP Port 3 Negotiation

By changing the negotiation setting from 'Auto' to 'Manual', the additional menu items 3 & 4 are revealed.

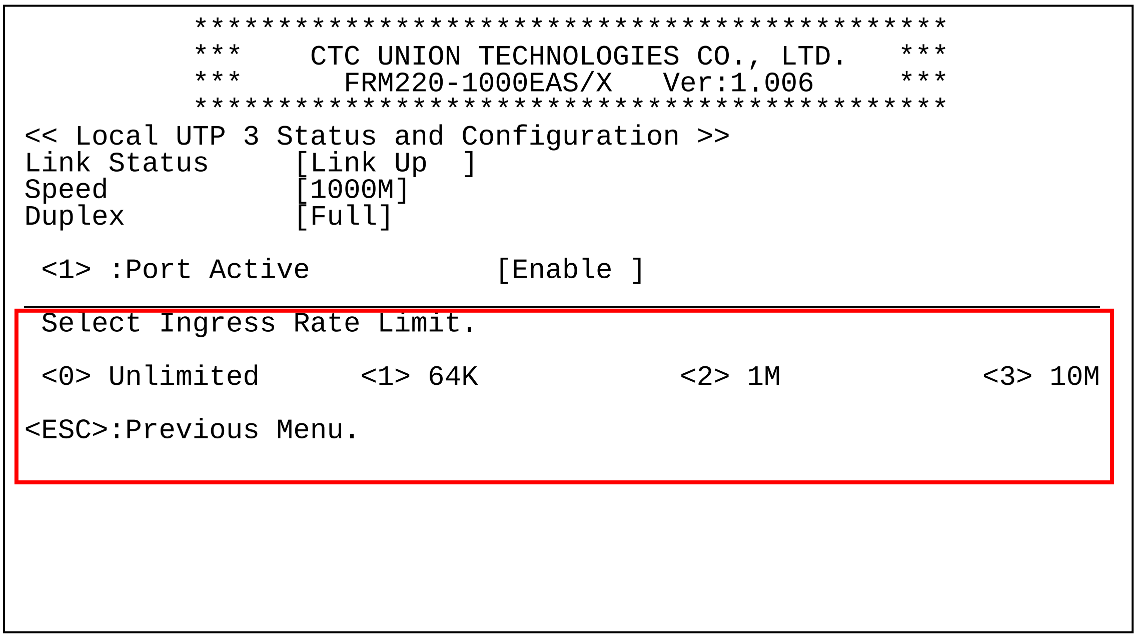


```
          *********************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
          ***      FRM220-1000EAS/X   Ver:1.003     ***
          *********************************************
<< Local UTP 3 Status and Configuration >>
Link Status     [Link Down]

 <1> :Port Active           [Enable ]
 <2> :Negotiation           [Manual]
 <3> :Speed                 [1000M]
 <4> :Duplex                [Full]
 <5> :Ingress Rate Limit    [Unlimited]
 <6> :Egress  Rate Limit    [Unlimited]
 <7> :Default Port CoS      [0]
 <S> :Confirm and Save Settings(Port Active, Speed, Duplex and
Negotiation).

<ESC>:Go to Previous Menu.
```

<3> **Speed** : The UTP ports support 10, 100, or 1000 forced configuration speed.
<4> **Duplex** : The UTP ports support Full or Half-Duplex forced operation modes. Gigabit Ethernet cannot be set to Half-Duplex as it is not IEEE standard.

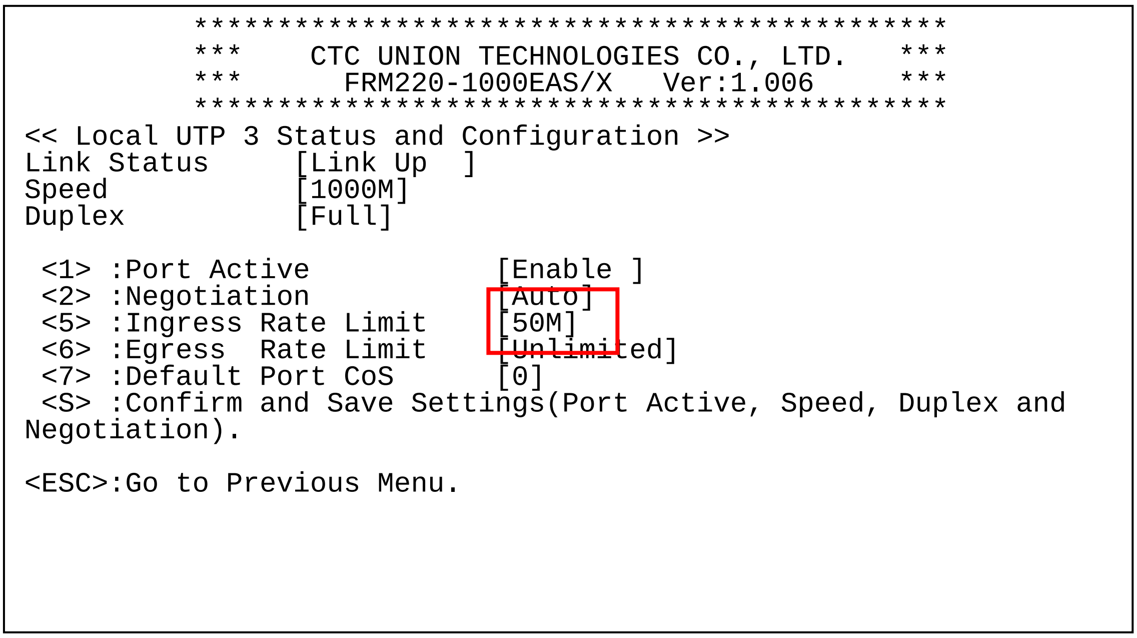
3.4.10.3 UTP Port 3 Rate Limiting

1000EAS/X provides per port ingress and egress rate limiting. For bandwidth settings, IRL or ingress rate limit refers to limiting any packets coming into the switch port, while ERL or egress rate limit refers to limiting packets leaving the port. When rate limiting is applied, ERL will use pause commands (802.3X) when the desired rate limit is exceeded, while any IRL setting will cause packet to be dropped when the limit is exceeded. This is an important point when doing the rate limit settings. It is preferable to set ERL at each port for the path that requires limiting so that flow control can help connected devices cope with the limiting. If IRL is employed, a connected device which has its packets dropped without flow control, will continue to send packets at its full rate. Also, since the packets are dropped, the application layer can only deal with the packet loss by timing out.



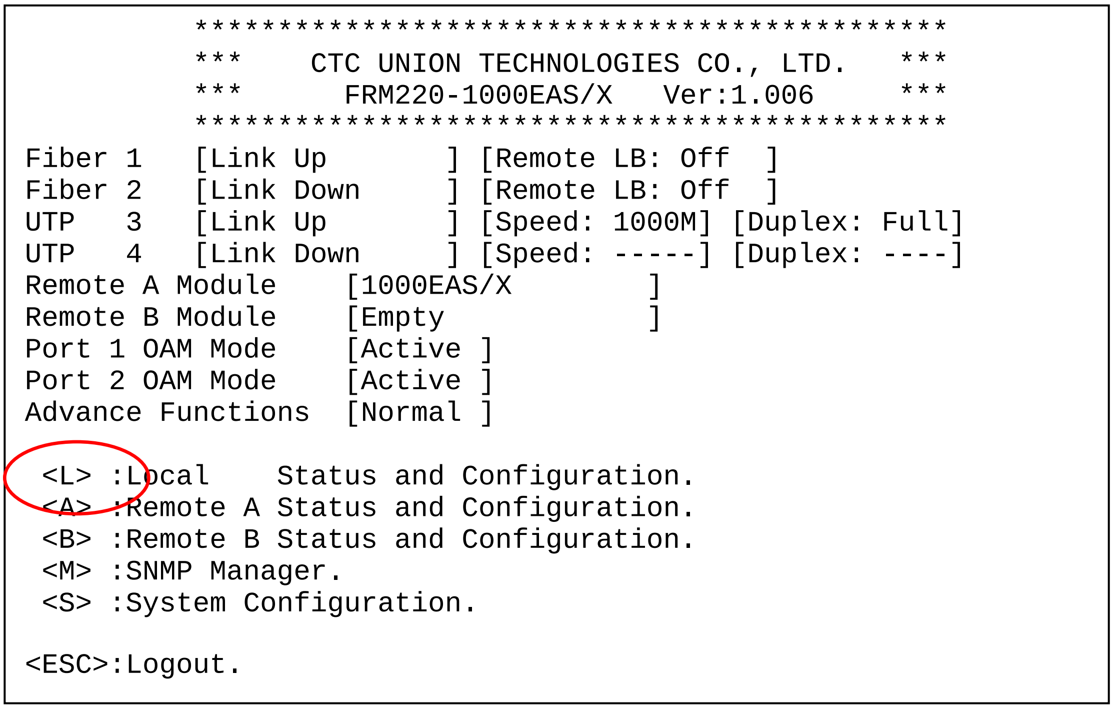
```
           *********************************************
           ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
           ***      FRM220-1000EAS/X   Ver:1.006     ***
           *********************************************
<< Local UTP 3 Status and Configuration >>
Link Status     [Link Up  ]
Speed           [1000M]
Duplex          [Full]

 <1> :Port Active           [Enable ]
_________________________________________________________________
 Select Ingress Rate Limit.

 <0> Unlimited      <1> 64K          <2> 1M           <3> 10M

<ESC>:Previous Menu.
```

First choose the granularity of 64K, 1M or 10M. Then key the 'n' value. In the above example, granularity has been set at 1M. The n value of 50 results in 50M rate limit. The same setting rates can be applied to the egress direction.



```
           *********************************************
           ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
           ***      FRM220-1000EAS/X   Ver:1.006     ***
           *********************************************
<< Local UTP 3 Status and Configuration >>
Link Status     [Link Up  ]
Speed           [1000M]
Duplex          [Full]

 <1> :Port Active           [Enable ]
 <2> :Negotiation           [Auto]
 <5> :Ingress Rate Limit    [50M]
 <6> :Egress  Rate Limit    [Unlimited]
 <7> :Default Port CoS      [0]
 <S> :Confirm and Save Settings(Port Active, Speed, Duplex and
Negotiation).

<ESC>:Go to Previous Menu.
```

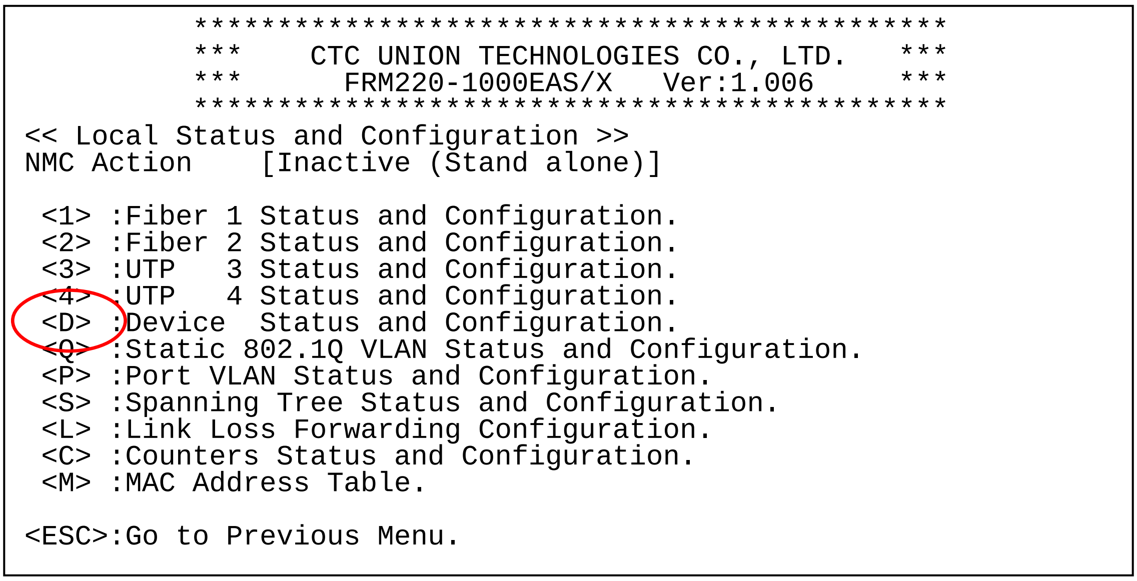
3.5 Device Status and Configuration



```
          *********************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.    ***
          ***      FRM220-1000EAS/X   Ver:1.006      ***
          *********************************************
Fiber 1   [Link Up       ] [Remote LB: Off  ]
Fiber 2   [Link Down     ] [Remote LB: Off  ]
UTP   3   [Link Up       ] [Speed: 1000M] [Duplex: Full]
UTP   4   [Link Down     ] [Speed: -----] [Duplex: ----]
Remote A Module    [1000EAS/X        ]
Remote B Module    [Empty            ]
Port 1 OAM Mode    [Active ]
Port 2 OAM Mode    [Active ]
Advance Functions  [Normal ]

 <L> :Local    Status and Configuration.
 <A> :Remote A Status and Configuration.
 <B> :Remote B Status and Configuration.
 <M> :SNMP Manager.
 <S> :System Configuration.

<ESC>:Logout.
```

Select item 'L' from the main menu.

From the ***Local Status and Configuration*** menu, the **Device Status and Configuration** menu can view the status and set the configuration mode.



```
          *********************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.    ***
          ***      FRM220-1000EAS/X   Ver:1.006      ***
          *********************************************
<< Local Status and Configuration >>
NMC Action    [Inactive (Stand alone)]

 <1> :Fiber 1 Status and Configuration.
 <2> :Fiber 2 Status and Configuration.
 <3> :UTP   3 Status and Configuration.
 <4> :UTP   4 Status and Configuration.
 <D> :Device  Status and Configuration.
 <Q> :Static 802.1Q VLAN Status and Configuration.
 <P> :Port VLAN Status and Configuration.
 <S> :Spanning Tree Status and Configuration.
 <L> :Link Loss Forwarding Configuration.
 <C> :Counters Status and Configuration.
 <M> :MAC Address Table.

<ESC>:Go to Previous Menu.
```

Select the Device Status and Configuration by keying "D" at the console.

```
<< Local Device Status and Configuration >>

 <1> :MAC Learning Function    [Enable ]
 <2> :Pause Frame              [Disable]
 <3> :Advance Functions        [Normal ]
 <4> :UPnP                     [Disable]
 <5> :QoS Priority Mode        [Weighted]
 <6> :Maximum OAMPDUs Size (60 ~ 1518 Octets) [1500]
 <7> :Accept Remote H/W Reset  [Disable]
 <8> :Tag's CoS Mapping to Internal Classify.
 <A> :Remote A H/W Reset.
 <B> :Remote B H/W Reset.
 <C> :Remote TLPT              [Disable]
 <L> :Load Default Settings and Write to System.
 <R> :System Reboot.

<ESC>:Go to Previous Menu.
```

<1> **MAC Learning Function** : Ethernet frames are processed by the MAC learning function and used to populate the MAC filtering address table. The table is then used to correctly forward outgoing frames to the right port. When the learning function is disabled, a packet arriving at one port will then be forwarded transparently to all other ports. No filtering will be done, because the MAC filtering table will be empty.

<2> **Pause Frame** : PAUSE is a flow control mechanism on full duplex Ethernet link segments defined by IEEE 802.3x and uses MAC Control frames to carry the PAUSE commands. Pressing the "1" key here will toggle this function between enabled or disabled.

<3> **Advanced Functions** : **1000EAS/X** acts as a normal 4 port switch when the setting here is 'normal'. Advanced functions are explained in detail in 3.6 Advanced Functions.

<4> **Upnp** : UPnP or Universal Plug 'n Play is a set of networking protocols promulgated by the UPnP Forum. When connected to a network, **1000EAS/X** will automatically announce its network address and supported device and services types, enabling clients that recognize those types to immediately begin using the device.

<5> : **QoS Priority Mode** : The priority mode may either be set as 'Weighted' or as 'Strict'. Note: 'Strict' mode could result in packet starvation.

<6> **Maximum OAMPDU Size** : This sets the maximum size of the OAM Protocol Data Unit (PDU). In order for two devices to communicate properly at the OAM level, this setting must be the same. We recommend setting the size to 1500.

<7> **Accept Remote H/W Reset** : When this parameter is enabled, the remotely connected unit will be allowed to reset this device if it gives the proper command. If this parameter is disabled (default), the remote unit's reset command will be ignored by this unit.

<8> : **Tag's CoS Mapping to Internal Classify** : The Class of Service is a 3 bit field within an Ethernet frame header when using 802.1Q tagging. The field specifies a priority value of between 0 and 7 inclusive that can be used by Quality of Service (QoS) disciplines to differentiate traffic. The internal Ethernet switch of **1000EAS/X** supports only 2 bit priority values, 0 to 3 inclusive. This function is used to map CoS 8 levels to the internal switch’s 4 QoS priority levels.

<A> **Remote A H/W Reset** : This function will request the remote A unit (fiber port 1 connected unit) to do a warm boot startup. This remote unit must have enabled the "Accept Remote H/W Reset" function, or it cannot be remotely reset.

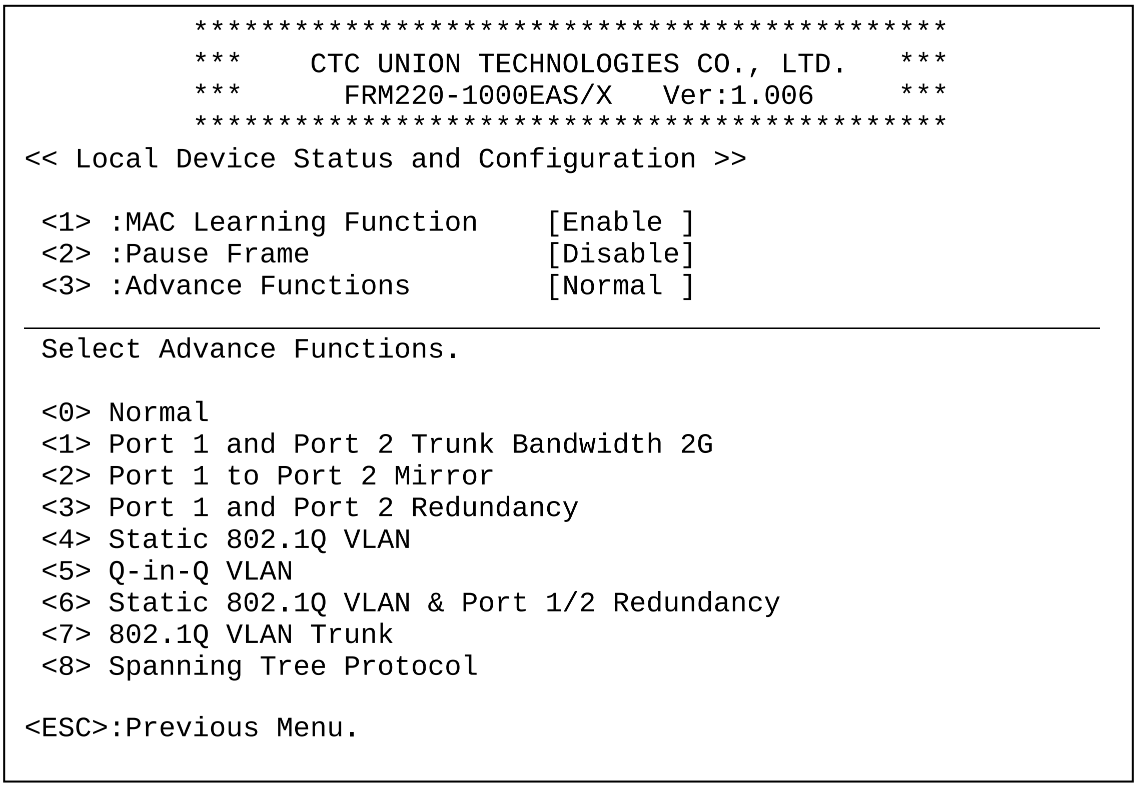
<B> **Remote B H/W Reset** : This function will request the remote B unit (fiber port 2 connected unit) to do a warm boot startup. This remote unit must have enabled the "Accept Remote H/W Reset" function, or it cannot be remotely reset.

<C> **Remote TLPT** : The transparent link fault pass through function can be enabled for fiber ports, A and/or B.

<L> **Load Default Settings and Write to System** : This function will load all the factory default settings and write them to the internal non-volatile ram. This is equivalent to doing the "Default" factory reset with the front panel 'Default' push-button switch.

<R> **System Reboot** : The unit will undergo a 'warm boot' if this function is selected and confirmed.

3.6 Advanced Functions

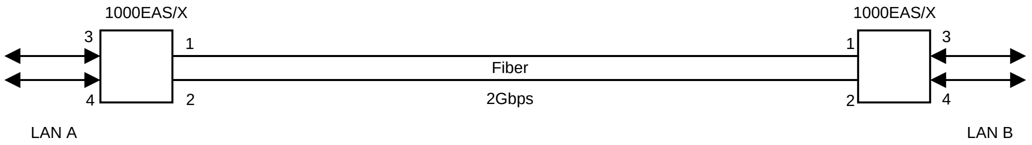


```
           *********************************************
           ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
           ***      FRM220-1000EAS/X   Ver:1.006     ***
           *********************************************
<< Local Device Status and Configuration >>

 <1> :MAC Learning Function    [Enable ]
 <2> :Pause Frame              [Disable]
 <3> :Advance Functions        [Normal ]
________________________________________________________________
 Select Advance Functions.

 <0> Normal
 <1> Port 1 and Port 2 Trunk Bandwidth 2G
 <2> Port 1 to Port 2 Mirror
 <3> Port 1 and Port 2 Redundancy
 <4> Static 802.1Q VLAN
 <5> Q-in-Q VLAN
 <6> Static 802.1Q VLAN & Port 1/2 Redundancy
 <7> 802.1Q VLAN Trunk
 <8> Spanning Tree Protocol

<ESC>:Previous Menu.
```

1000EAS/X has several sets of pre-defined 'advanced functions' which allow the user to quickly configure the switch for specific applications. Each of these is shown below and will be explained in detail.

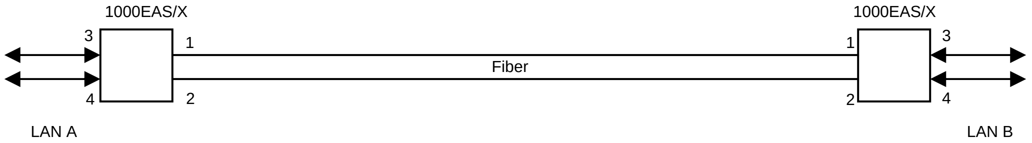
<0> **Normal** : This is the default mode of **1000EAS/X**. In this mode the unit is simply a 4 port managed Ethernet media converter/switch.
<1> **Port 1 and Port 2 Trunk Bandwidth 2G** : This mode creates a 2G trunk of the two 1GbE fibers by using Link Aggregation. The application drawing for this mode is shown in 3.6.1 Port 1 and Port 2 Trunk Bandwidth 2G.
<2> **Port 1 to Port 2 Mirror** : The port mirroring function is typically used by network engineers that require capturing packet data for analysis or troubleshooting. The application drawing for this mode is shown in 3.6.2 Port 1 to Port 2 Mirror.
<3> **Port 1 and Port 2 Redundancy** : This function provides a fiber redundancy so that if either fiber path losses transmission, the other path is a backup. The application drawing for this mode is shown in 3.6.3 Port 1 and Port 2 Redundancy.
<4> **Static 802.1Q VLAN** : This mode will open up the unit to further settings for 802.1Q VLAN settings. This mode's application drawing and details are shown in 3.6.4 Static 802.1Q VLAN.
<5> **Q-in-Q VLAN** : This advanced function supports 802.1ad VLAN stacking or what is commonly called QinQ. The application drawing and details for this mode are shown in 3.6.5 Q-in-Q VLAN.
<6> **Static 802.1Q VLAN & Port 1/2 Redundancy** : This special mode combines fiber port redundancy with tagged VLAN. The application drawing and details for this mode are shown in 3.6.6 Static 802.1Q VLAN & Port 1/2 Redundancy.
<7> **802.1Q VLAN Trunk** : This is a special mode designed for connecting a **1000EAS/X** pair on the 'trunk' between Cisco switches. The application drawing and details for this mode are shown in 3.6.7 802.1Q VLAN Trunk.
<8> **Spanning Tree Protocol** : The Spanning tree protocol (STP) is a link layer network protocol that ensures a loop-free topology for any bridged LAN. Use this protocol when setting up the converter/switch in ring or mesh topologies. The application drawing and details for this mode are shown in 3.6.8 Spanning Tree Protocol.

3.6.1 Port 1 and Port 2 Trunk Bandwidth 2G



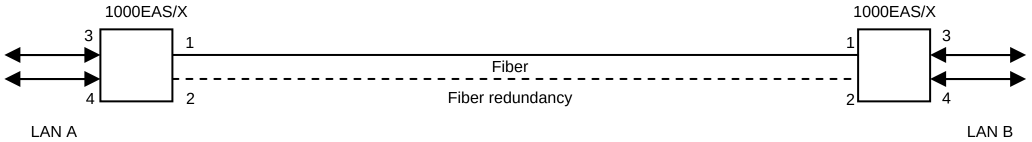
In this mode the fibers are aggregated or 'trunked' to provide 2G bandwidth. The application requires two fiber links at the same time, but logically they act as one link with up to 2G throughput. This mode can provide up to 1G throughput for each of the UTP ports at the same time.

3.6.2 Port 1 to Port 2 Mirror



The mirror mode provides fiber aggregation or 'trunking'. It uses one or two fiber lines to achieve this feature. The maximum combined throughput is about 1.5G.

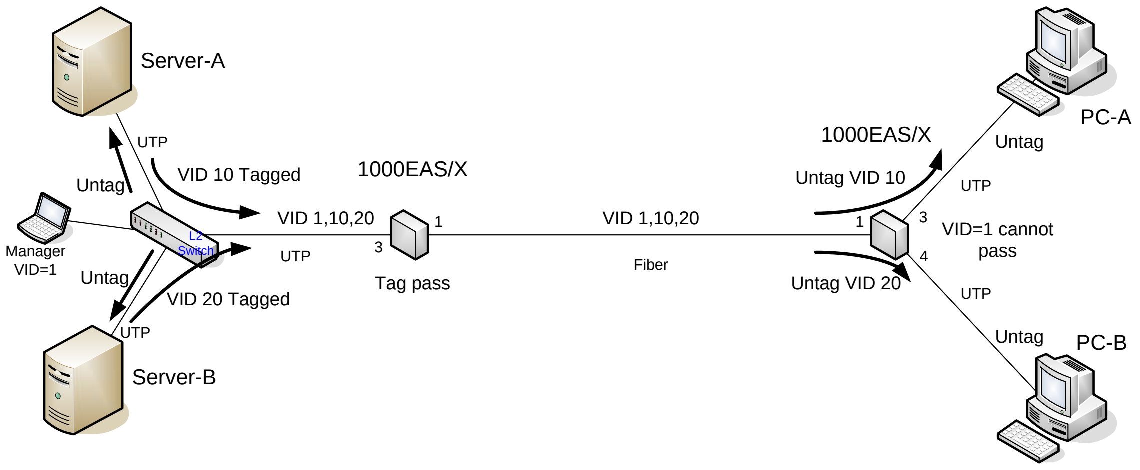
3.6.3 Port 1 and Port 2 Redundancy



In this mode one fiber is active, while the other is on standby. This creates a 1+1 redundant path protection. If main fiber is broken, the second fiber will quickly take over the transmissions. The application requires two fiber links at the same time, but one fiber is in standby.

3.6.4 Static 802.1Q VLAN

IEEE 802.1Q, or VLAN (Virtual LAN) Tagging, is a networking standard written by the IEEE 802.1 workgroup allowing multiple bridged networks to transparently share the same physical network link without leakage of information between networks.



In the previous drawing, an L2 switch creates two separate VLANs (VID10 and VID20) from two ports that link to servers A and B. A third port carries the two VLAN IDs to **1000EAS/X** media converter /switch pair by UTP. The management uses VID=1. **1000EAS/X** pair creates a fiber link over a longer distance than could be supported with UTP. The local side converter requires no additional configuration and passes the tag information transparently over the fiber link. The remote side requires VLAN configuration. One UTP port (port3) recognizes and untags VID10 to the client PC-A. The other UTP port, (port4) recognizes and untags VID20 to the client PC-B. On the return trip, packets are tagged, VID10 for port3 and VID20 for port 4 and returned to the L2 switch and then to the appropriate servers.

Configuration example, done to remote converter:

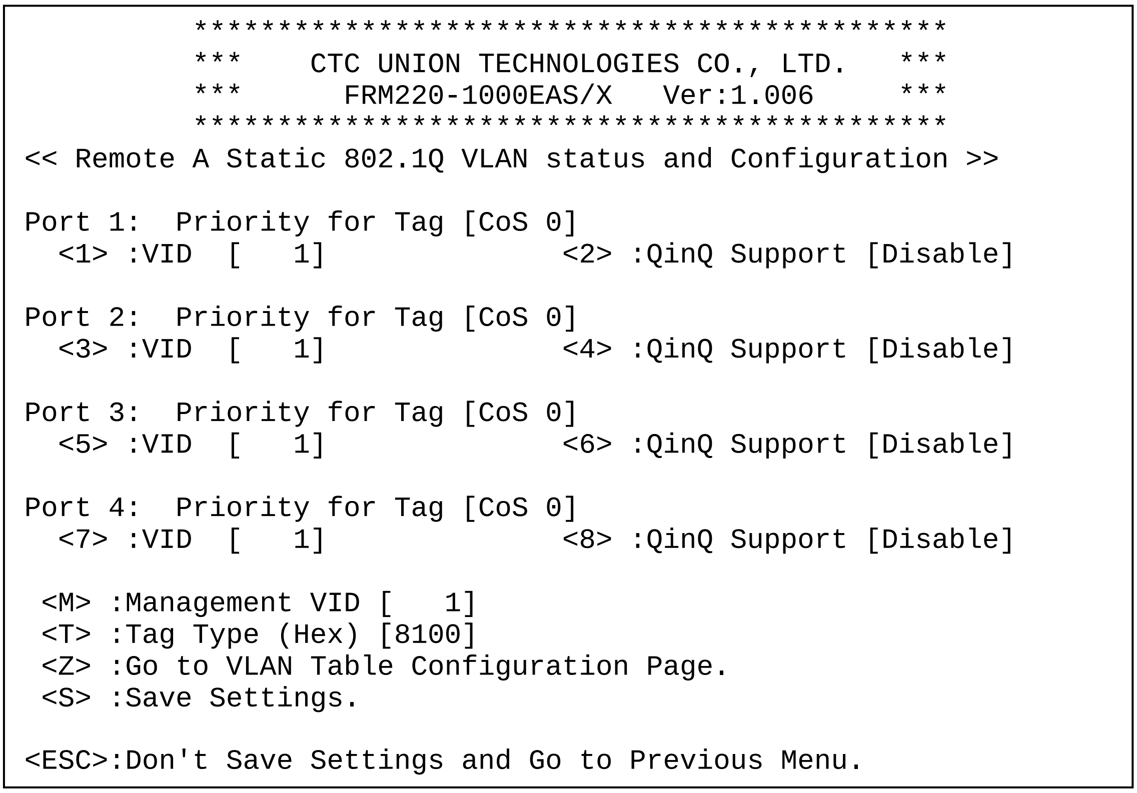
1. Return to the main menu on the local unit. Select the Remote A unit for configuration.

```
          *********************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
          ***      FRM220-1000EAS/X   Ver:1.006     ***
          *********************************************
Fiber 1   [Link Up       ] [Remote LB: Off  ]
Fiber 2   [Link Down     ] [Remote LB: Off  ]
UTP   3   [Link Up       ] [Speed: 1000M] [Duplex: Full]
UTP   4   [Link Down     ] [Speed: -----] [Duplex: ----]
Remote A Module    [1000EAS/X       ]
Remote B Module    [Empty           ]
Port 1 OAM Mode    [Active ]
Port 2 OAM Mode    [Active ]
Advance Functions  [Normal ]

 <L> :Local    Status and Configuration.
 <A> :Remote A Status and Configuration.
 <B> :Remote B Status and Configuration.
 <M> :SNMP Manager.
 <S> :System Configuration.

<ESC>:Logout.
```

2. This will take us back to the **Status and Configuration** page for Remote A.

```
          *********************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
          ***      FRM220-1000EAS/X   Ver:1.006     ***
          *********************************************
<< Remote A Status and Configuration >>
Firmware Version     [1.006]
Remote NMC Action    [Inactive (Stand alone)]

 <1> :Fiber 1 Status and Configuration.
 <2> :Fiber 2 Status and Configuration.
 <3> :UTP   3 Status and Configuration.
 <4> :UTP   4 Status and Configuration.
 <D> :Device  Status and Configuration.
 <Q> :Static 802.1Q VLAN Status and Configuration.
 <P> :Port VLAN Status and Configuration.
 <S> :Spanning Tree Status and Configuration.
 <L> :Link Loss Forwarding Configuration.
 <C> :Counters Status and Configuration.
 <U> :Upgrade F/W of Remote device by OAM.

<ESC>:Go to Previous Menu.
```

3. Select <Q>, **Static 802.1Q VLAN Status and Configuration**
The screen will look like that below.



```
          ********************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
          ***      FRM220-1000EAS/X   Ver:1.006     ***
          ********************************************
<< Remote A Static 802.1Q VLAN status and Configuration >>

Port 1:  Priority for Tag [CoS 0]
  <1> :VID  [   1]             <2> :QinQ Support [Disable]

Port 2:  Priority for Tag [CoS 0]
  <3> :VID  [   1]             <4> :QinQ Support [Disable]

Port 3:  Priority for Tag [CoS 0]
  <5> :VID  [   1]             <6> :QinQ Support [Disable]

Port 4:  Priority for Tag [CoS 0]
  <7> :VID  [   1]             <8> :QinQ Support [Disable]

 <M> :Management VID [   1]
 <T> :Tag Type (Hex) [8100]
 <Z> :Go to VLAN Table Configuration Page.
 <S> :Save Settings.

<ESC>:Don't Save Settings and Go to Previous Menu.
```

VID (VLAN Identifier) : a 12-bit field specifying the VLAN to which the frame belongs. A value of 0 means that the frame does not belong to any VLAN. In this case the 802.1Q tag specifies only a priority and is referred to as a priority tag. The hexadecimal values of 0x000 (0) and 0xFFF (4095) are reserved. All other values may be used as VLAN identifiers, allowing up to 4094 VLANs. The setting here in the 1000EAS/X operate on incoming packets at each designated port. The set VID will be tagged to the incoming packet.

Q-in-Q Support : With the IEEE standard 802.1ad, double-tagging can be useful for Internet service providers, allowing them to use VLANs internally while mixing traffic from clients that are already VLAN-tagged. The outer (next to source MAC and representing ISP VLAN) S-TAG (service tag) comes first, followed by the inner C-TAG (customer tag). In such cases, 802.1ad specifies a TPID of 0x88a8 for service-provider outer S-TAG.

<M> **Management VID** : By default this VID is 1. Set this to the VID that will be used to manage the **1000EAS/X** converter over Ethernet.

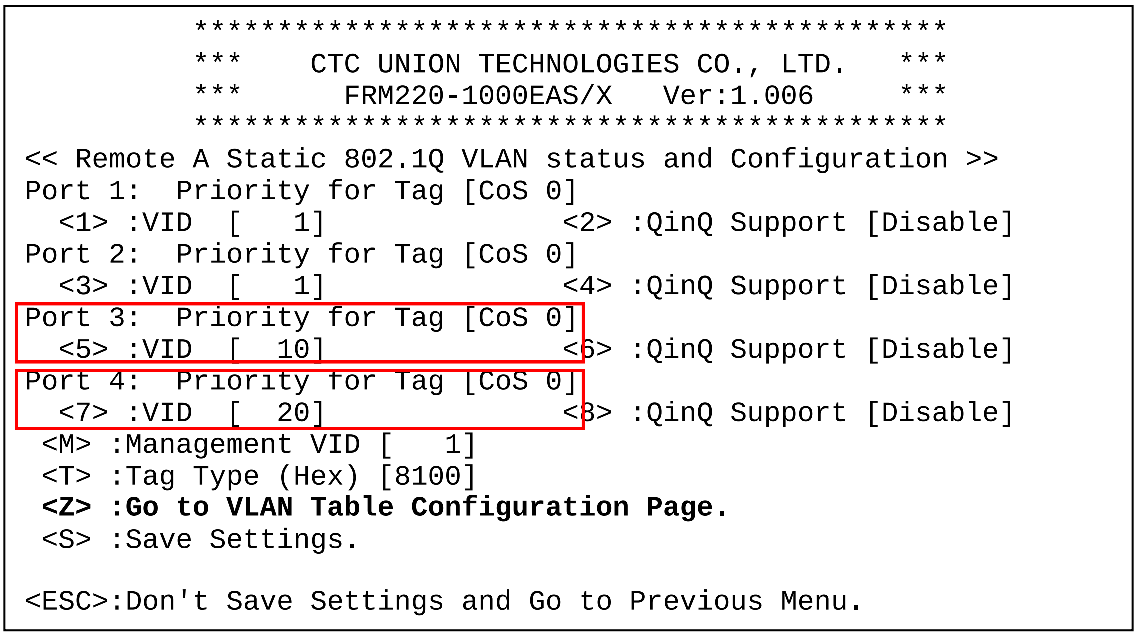
<T> **Tag Type** : or Tag Protocol Identifier (TPID) : a 16-bit field set to a value of 0x8100 in order to identify the frame as an IEEE 802.1Q-tagged frame. This field is located at the same position as the EtherType/Size field in untagged frames, and is thus used to distinguish the frame from untagged frames.

<Z> **Go to VLAN Table Configuration Page** : This menu item brings up the static VLAN table to review status or make additions or modifications.

<S> **Save Settings** : After making changes and before leaving this menu page, use this command to commit the changes to the **1000EAS/X**.

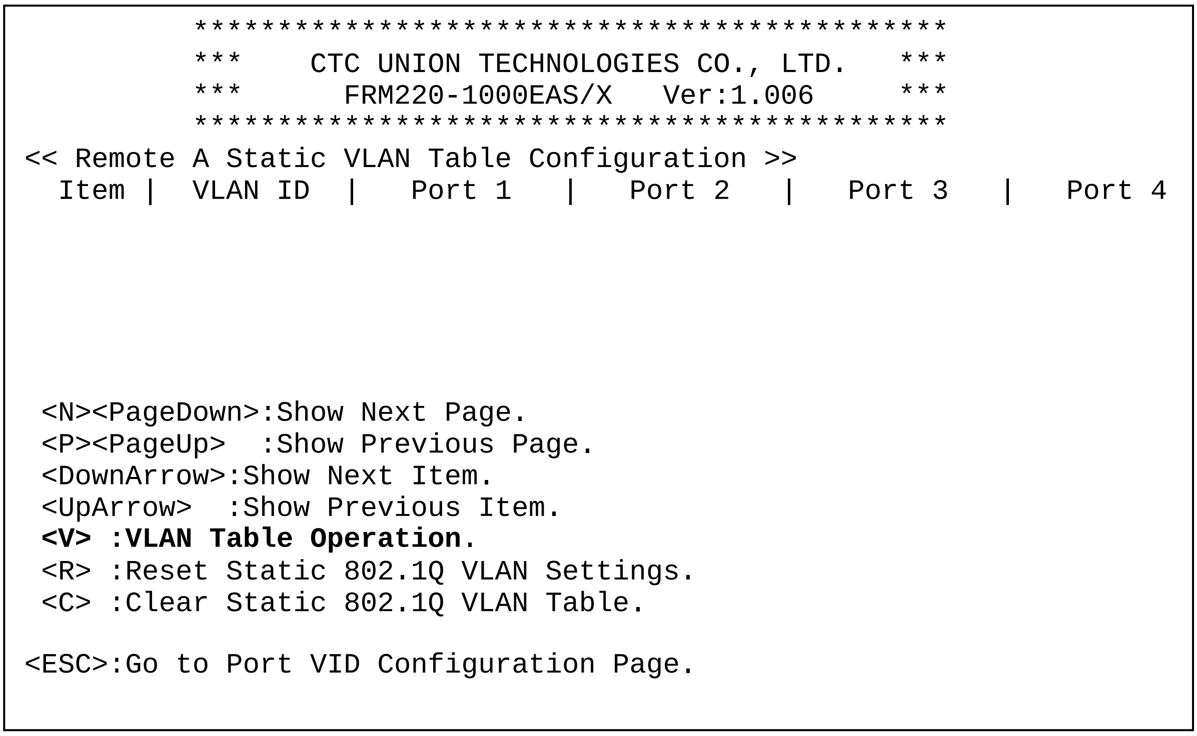
In the above screen, we can set different VID (VLAN Identifier) for each port of the converter. QinQ support can also be enabled.

4. We are going to set port 3 (UTP3) to VID 10 and port 4 (UTP4) to VID20. The screen will then look like this. This means that packets that ingress (come into) the UTP ports, from PC-A and PC-B will have their packets tagged for VID10 and 20 respectively. Save settings with <S>.



```
           ********************************************
           ***    CTC UNION TECHNOLOGIES CO., LTD.    ***
           ***      FRM220-1000EAS/X   Ver:1.006      ***
           ********************************************
<< Remote A Static 802.1Q VLAN status and Configuration >>
Port 1:  Priority for Tag [CoS 0]
  <1> :VID  [   1]              <2> :QinQ Support [Disable]
Port 2:  Priority for Tag [CoS 0]
  <3> :VID  [   1]              <4> :QinQ Support [Disable]
Port 3:  Priority for Tag [CoS 0]
  <5> :VID  [  10]              <6> :QinQ Support [Disable]
Port 4:  Priority for Tag [CoS 0]
  <7> :VID  [  20]              <8> :QinQ Support [Disable]
 <M> :Management VID [   1]
 <T> :Tag Type (Hex) [8100]
 <Z> :Go to VLAN Table Configuration Page.
 <S> :Save Settings.

<ESC>:Don't Save Settings and Go to Previous Menu.
```

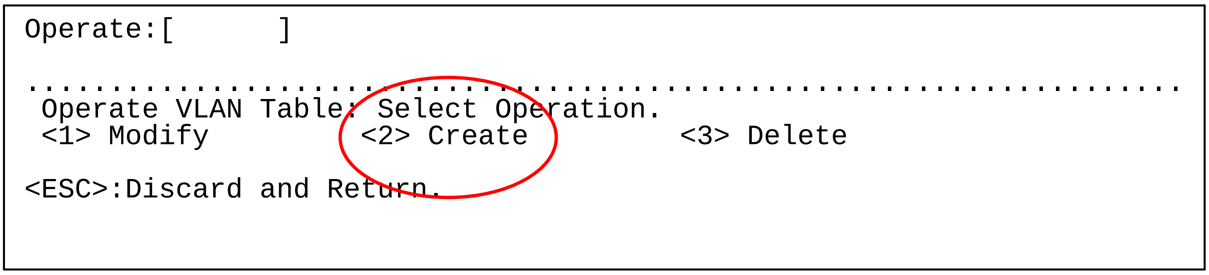
5. Next we need to go to the **VLAN Table Configuration Page**. Select item **<Z>**.



```
           ********************************************
           ***    CTC UNION TECHNOLOGIES CO., LTD.    ***
           ***      FRM220-1000EAS/X   Ver:1.006      ***
           ********************************************
<< Remote A Static VLAN Table Configuration >>
  Item |  VLAN ID  |   Port 1   |   Port 2   |   Port 3   |   Port 4







 <N><PageDown>:Show Next Page.
 <P><PageUp>  :Show Previous Page.
 <DownArrow>:Show Next Item.
 <UpArrow>  :Show Previous Item.
 <V> :VLAN Table Operation.
 <R> :Reset Static 802.1Q VLAN Settings.
 <C> :Clear Static 802.1Q VLAN Table.

<ESC>:Go to Port VID Configuration Page.
```

The static **VLAN table Operation** is accessed through the **<V>** menu item.

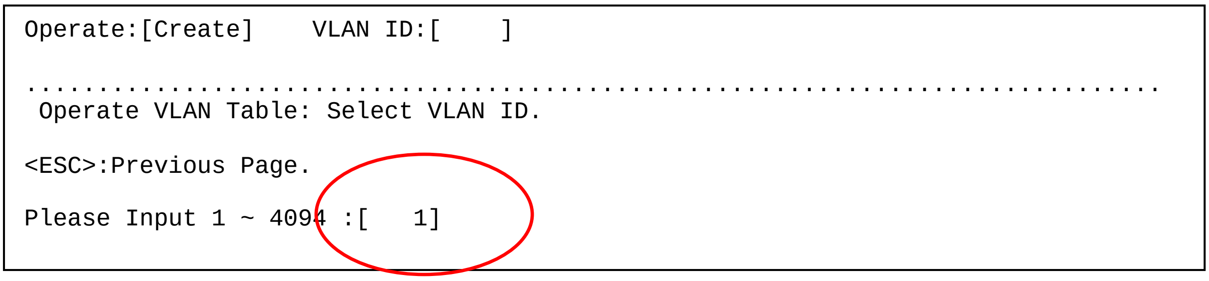
6. Select <V> **VLAN Table Operation**.



```
Operate:[       ]

.....................................................................
 Operate VLAN Table: Select Operation.
 <1> Modify         <2> Create          <3> Delete

<ESC>:Discard and Return.
```

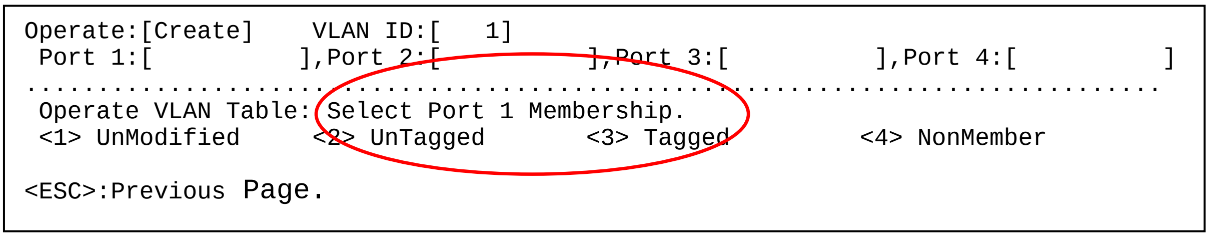
In our example, Port 1 is the fiber port or the main WAN link. Ports 3&4 are UTP ports. We will assign static VLAN to VID1, 10, and 20 as follows.

7. Select <2> **Create**. Input the VID 1



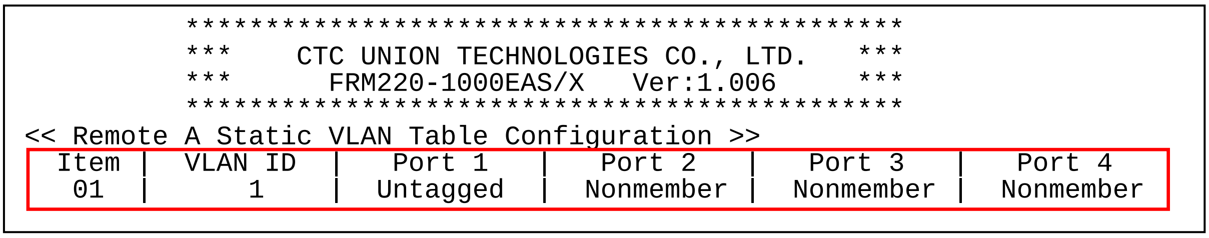
```
Operate:[Create]    VLAN ID:[    ]

..............................................................................
 Operate VLAN Table: Select VLAN ID.

<ESC>:Previous Page.

Please Input 1 ~ 4094 :[   1]
```

8. For VID 1 we will select the port membership in order for Port 1, Port 2, Port3 and Port 4 as 'untagged', 'nonmember', 'nonmember', and 'nonmember'.



```
Operate:[Create]    VLAN ID:[   1]
 Port 1:[          ],Port 2:[          ],Port 3:[          ],Port 4:[          ]
..............................................................................
 Operate VLAN Table: Select Port 1 Membership.
 <1> UnModified     <2> UnTagged       <3> Tagged         <4> NonMember

<ESC>:Previous Page.
```

The results look like this.



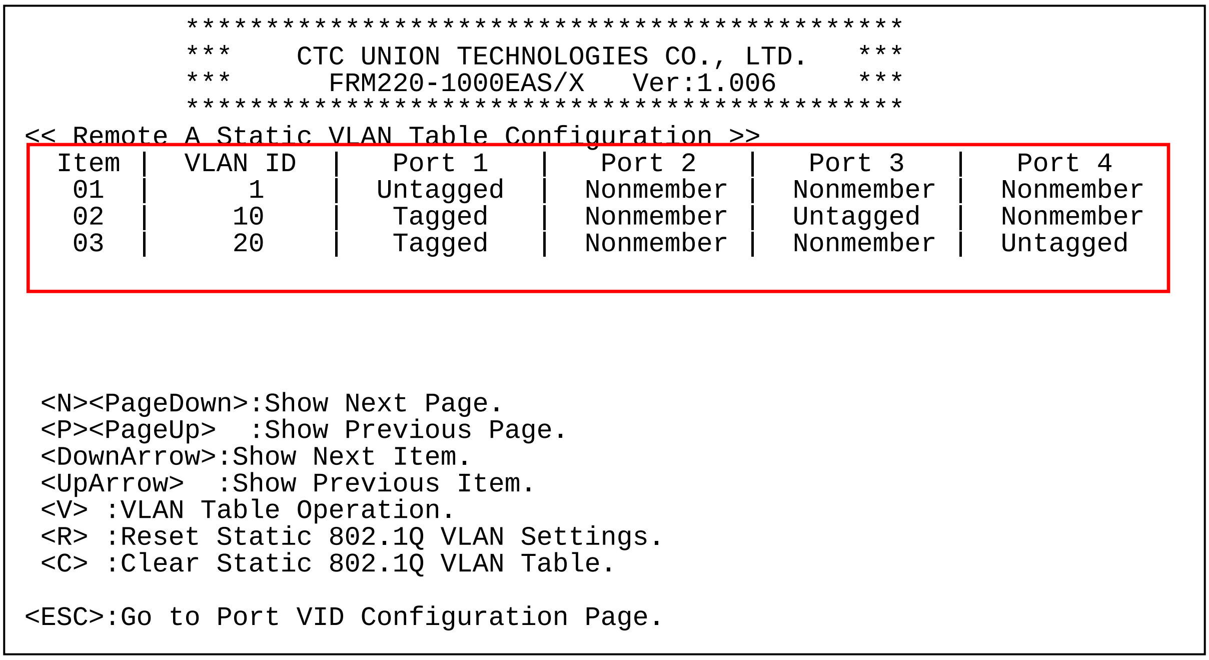
```
          *********************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
          ***      FRM220-1000EAS/X    Ver:1.006    ***
          *********************************************
<< Remote A Static VLAN Table Configuration >>
  Item |  VLAN ID  |  Port 1   |  Port 2   |  Port 3   |  Port 4
   01  |       1   | Untagged  | Nonmember | Nonmember | Nonmember
```

By making Port3&4 nonmembers of VID1, we have blocked any normal traffic between those two clients. They are essentially isolated from each other.

Some Tagging definitions:
Tagged: This means that packets exiting the assigned port will have the packets tagged with the VID assigned to that port.
Untagged: This means that any packets exiting the assigned port will have all tag information removed.
Non-member: When a port is not a member of a VID, packets tagged with that VID will not be allowed to exit that port.
Unmodified: This means that packets exiting the assigned port will still have the same tag as when they entered any other port of the switch, i.e., unmodified.

9. The next step will be to create the VIDs for 10 and 20. We will make Port3&4 untagged members of VID10 and 20 respectively. Port 1 (fiber) will be Tagged member for each VLAN.

The resulting Static VLAN table will look like this:

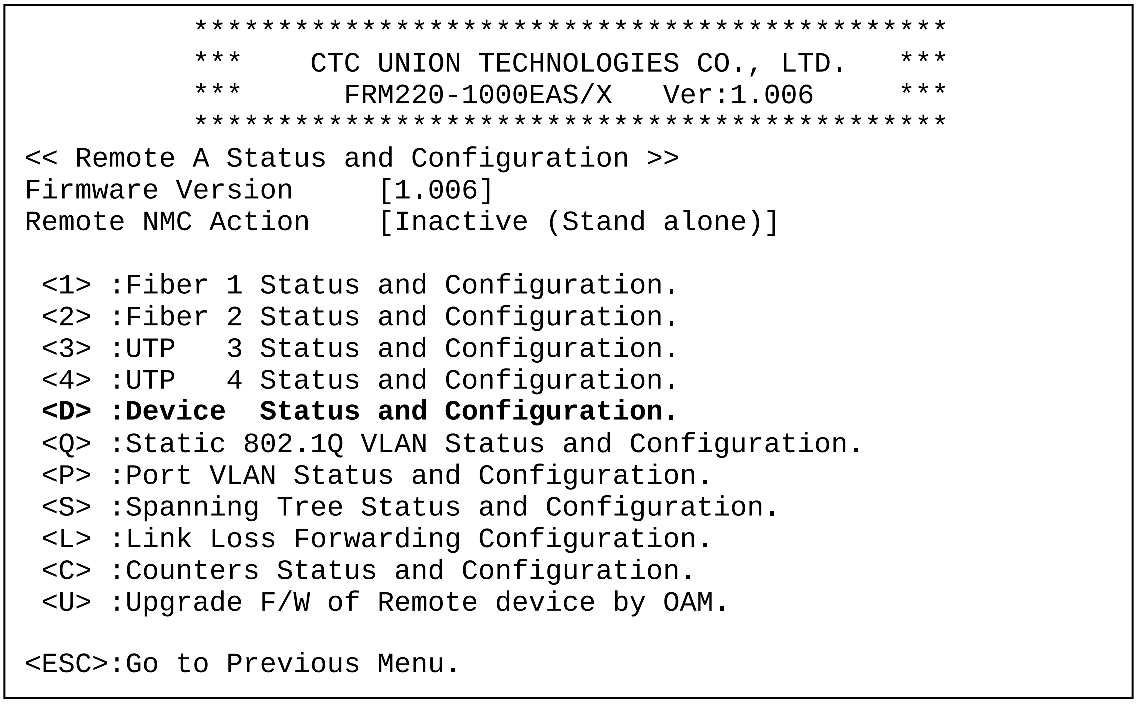


```
          *********************************************
          ***     CTC UNION TECHNOLOGIES CO., LTD.    ***
          ***       FRM220-1000EAS/X   Ver:1.006      ***
          *********************************************
<< Remote A Static VLAN Table Configuration >>
  Item |  VLAN ID  |   Port 1    |   Port 2    |   Port 3    |   Port 4
   01  |      1    |  Untagged   |  Nonmember  |  Nonmember  |  Nonmember
   02  |     10    |   Tagged    |  Nonmember  |  Untagged   |  Nonmember
   03  |     20    |   Tagged    |  Nonmember  |  Nonmember  |  Untagged




 <N><PageDown>:Show Next Page.
 <P><PageUp>  :Show Previous Page.
 <DownArrow>:Show Next Item.
 <UpArrow>  :Show Previous Item.
 <V> :VLAN Table Operation.
 <R> :Reset Static 802.1Q VLAN Settings.
 <C> :Clear Static 802.1Q VLAN Table.

<ESC>:Go to Port VID Configuration Page.
```

This simple VLAN scheme will now be working such that PC-A can only connect to Server A and PC-B can only connect to Server B.

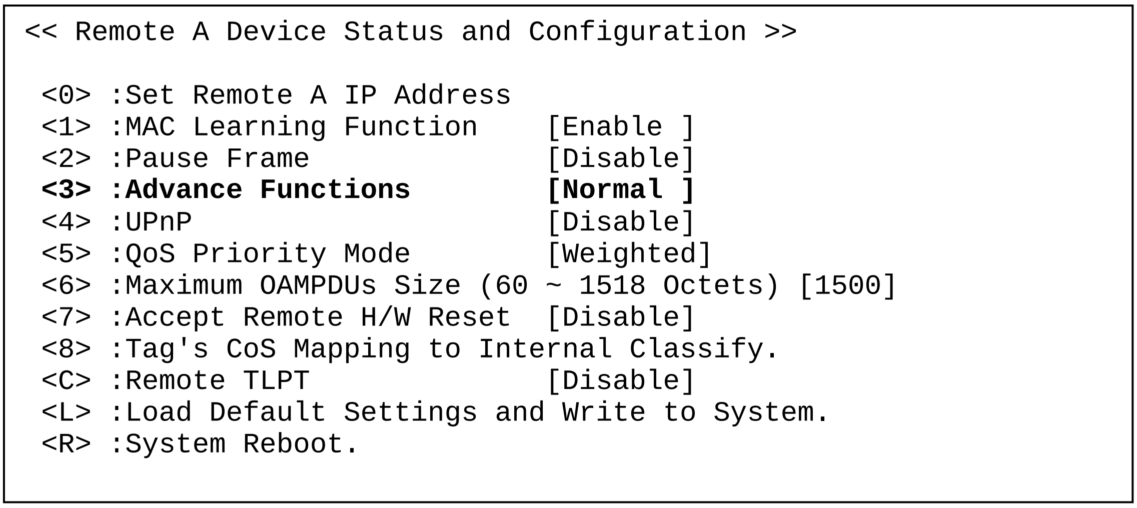
When assigning static VLAN ID, any ID from 1-4094 can be chosen. However, the maximum number of VID table entries for **1000EAS/X** is 64 static VLANs.

10. ESC back to the **Remote A Status and Configuration** menu.



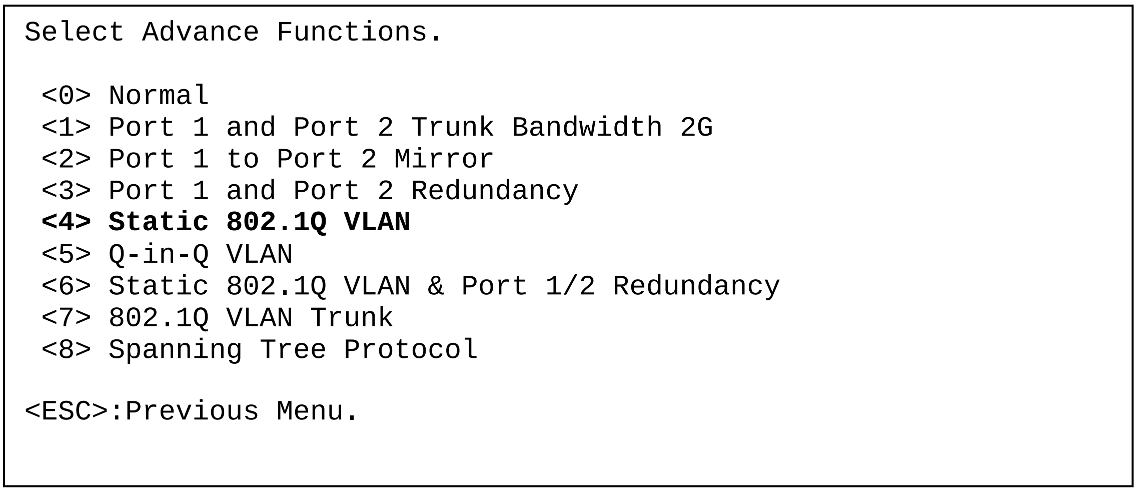
```
           *********************************************
           ***     CTC UNION TECHNOLOGIES CO., LTD.    ***
           ***       FRM220-1000EAS/X   Ver:1.006      ***
           *********************************************
<< Remote A Status and Configuration >>
Firmware Version     [1.006]
Remote NMC Action    [Inactive (Stand alone)]

 <1> :Fiber 1 Status and Configuration.
 <2> :Fiber 2 Status and Configuration.
 <3> :UTP   3 Status and Configuration.
 <4> :UTP   4 Status and Configuration.
 <D> :Device  Status and Configuration.
 <Q> :Static 802.1Q VLAN Status and Configuration.
 <P> :Port VLAN Status and Configuration.
 <S> :Spanning Tree Status and Configuration.
 <L> :Link Loss Forwarding Configuration.
 <C> :Counters Status and Configuration.
 <U> :Upgrade F/W of Remote device by OAM.

<ESC>:Go to Previous Menu.
```

11. Select **<D>**, **Device Status and Configuration**
The screen will look like the following.



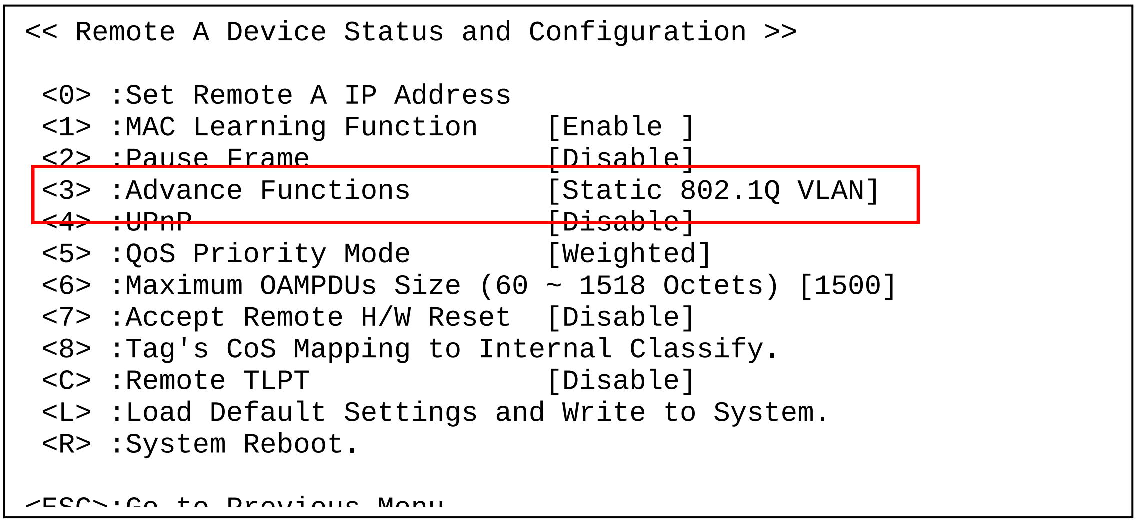
```
<< Remote A Device Status and Configuration >>

 <0> :Set Remote A IP Address
 <1> :MAC Learning Function    [Enable ]
 <2> :Pause Frame              [Disable]
 <3> :Advance Functions        [Normal ]
 <4> :UPnP                     [Disable]
 <5> :QoS Priority Mode        [Weighted]
 <6> :Maximum OAMPDUs Size (60 ~ 1518 Octets) [1500]
 <7> :Accept Remote H/W Reset  [Disable]
 <8> :Tag's CoS Mapping to Internal Classify.
 <C> :Remote TLPT              [Disable]
 <L> :Load Default Settings and Write to System.
 <R> :System Reboot.
```

12. Select **<3>**, **Advanced Functions**
The screen will look like the following.



```
Select Advance Functions.

 <0> Normal
 <1> Port 1 and Port 2 Trunk Bandwidth 2G
 <2> Port 1 to Port 2 Mirror
 <3> Port 1 and Port 2 Redundancy
 <4> Static 802.1Q VLAN
 <5> Q-in-Q VLAN
 <6> Static 802.1Q VLAN & Port 1/2 Redundancy
 <7> 802.1Q VLAN Trunk
 <8> Spanning Tree Protocol

<ESC>:Previous Menu.
```

13. From the Advanced Functions screen, select <4> **Static 802.1Q VLAN**. The following screen will be displayed.

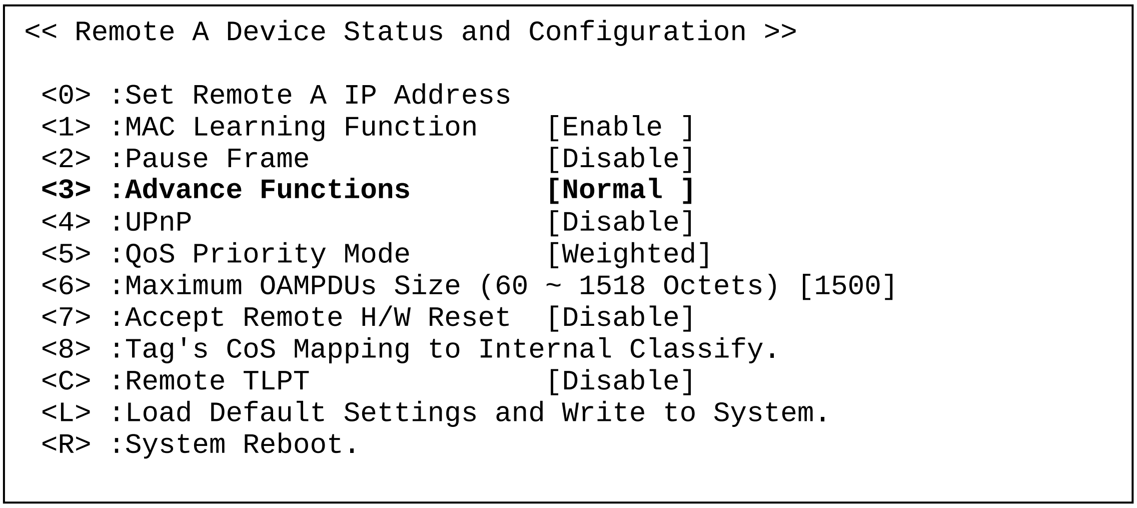


```
<< Remote A Device Status and Configuration >>

 <0> :Set Remote A IP Address
 <1> :MAC Learning Function    [Enable ]
 <2> :Pause Frame              [Disable]
 <3> :Advance Functions        [Static 802.1Q VLAN]
 <4> :UPnP                     [Disable]
 <5> :QoS Priority Mode        [Weighted]
 <6> :Maximum OAMPDUs Size (60 ~ 1518 Octets) [1500]
 <7> :Accept Remote H/W Reset  [Disable]
 <8> :Tag's CoS Mapping to Internal Classify.
 <C> :Remote TLPT              [Disable]
 <L> :Load Default Settings and Write to System.
 <R> :System Reboot.

<ESC>:Go to Previous Menu.
```

Note: No VLAN settings are active until the Static 802.1Q VLAN is enabled in **Advanced Functions**.

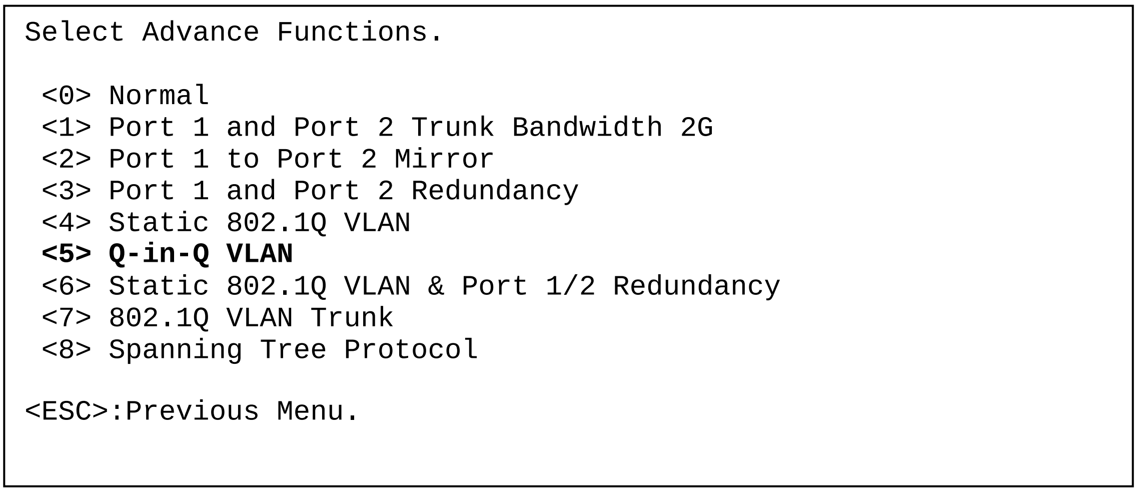
3.6.5 Q-in-Q VLAN

The VLAN settings are performed in the same manners as for Static 802.1Q VLAN. After the settings are completed, return to the Status and Configuration page and select item <D> :Device Status and Configuration.



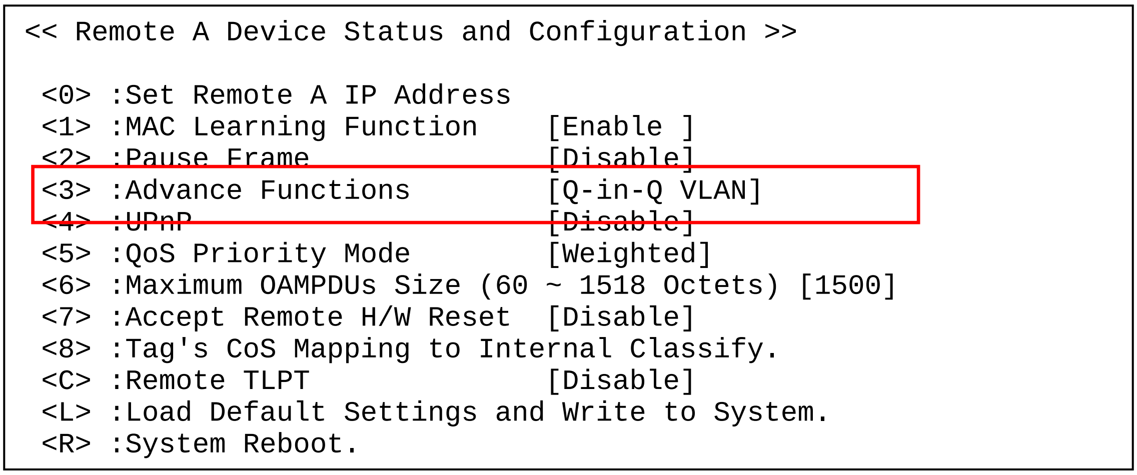
```
<< Remote A Device Status and Configuration >>

 <0> :Set Remote A IP Address
 <1> :MAC Learning Function    [Enable ]
 <2> :Pause Frame              [Disable]
 <3> :Advance Functions        [Normal ]
 <4> :UPnP                     [Disable]
 <5> :QoS Priority Mode        [Weighted]
 <6> :Maximum OAMPDUs Size (60 ~ 1518 Octets) [1500]
 <7> :Accept Remote H/W Reset  [Disable]
 <8> :Tag's CoS Mapping to Internal Classify.
 <C> :Remote TLPT              [Disable]
 <L> :Load Default Settings and Write to System.
 <R> :System Reboot.
```

Select **<3>**, **Advanced Functions**
The screen will look like the following.



```
Select Advance Functions.

 <0> Normal
 <1> Port 1 and Port 2 Trunk Bandwidth 2G
 <2> Port 1 to Port 2 Mirror
 <3> Port 1 and Port 2 Redundancy
 <4> Static 802.1Q VLAN
 <5> Q-in-Q VLAN
 <6> Static 802.1Q VLAN & Port 1/2 Redundancy
 <7> 802.1Q VLAN Trunk
 <8> Spanning Tree Protocol

<ESC>:Previous Menu.
```

From the Advanced Functions screen, select <5> **Q-in-Q VLAN**. The following screen will be displayed.



```
<< Remote A Device Status and Configuration >>

 <0> :Set Remote A IP Address
 <1> :MAC Learning Function    [Enable ]
 <2> :Pause Frame              [Disable]
 <3> :Advance Functions        [Q-in-Q VLAN]
 <4> :UPnP                     [Disable]
 <5> :QoS Priority Mode        [Weighted]
 <6> :Maximum OAMPDUs Size (60 ~ 1518 Octets) [1500]
 <7> :Accept Remote H/W Reset  [Disable]
 <8> :Tag's CoS Mapping to Internal Classify.
 <C> :Remote TLPT              [Disable]
 <L> :Load Default Settings and Write to System.
 <R> :System Reboot.
```

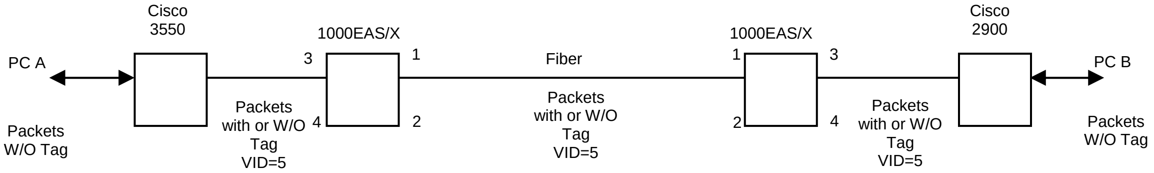
Note: No VLAN settings are active until the Q-in-Q VLAN is enabled in **Advanced Functions**.

3.6.6 Static 802.1Q VLAN & Port 1/2 Redundancy

By choosing the **Advanced Feature** of Static VLAN and Port Redundancy, the previous application in 3.6.4 Static 802.1Q VLAN can be combined with 3.6.3 Port 1 and Port 2 Redundancy.

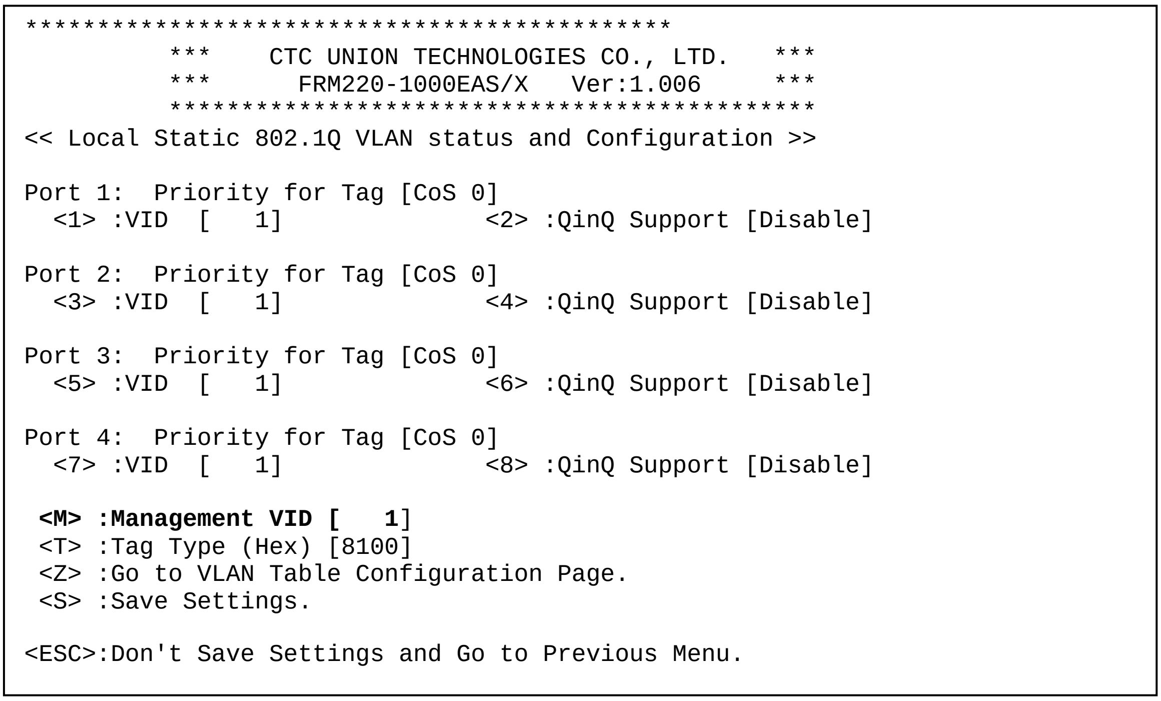
3.6.7 802.1Q VLAN Trunk

The **VLAN Trunk** feature is a quick way to configure **1000EAS/X** for management between two trunked Cisco switches. In the following application, the existing trunk VLAN is already provided between the two Cisco switches. The object here is to be able to allow the PC at either end (PC-A or PC-B) to manage **1000EAS/X** devices. In this example, the management VID=5.



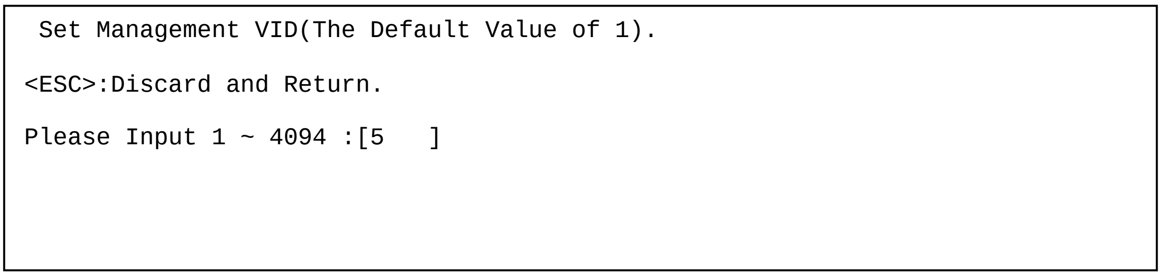
The above application configuration can be done manually through the normal 802.1Q setting menus. First we will explain the manual setting mode.

1. From the main menu, select either the Local or Remote A unit for configuration. Select <Q> for 802.1Q setting.



```
*********************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
          ***      FRM220-1000EAS/X   Ver:1.006     ***
          *********************************************
<< Local Static 802.1Q VLAN status and Configuration >>

Port 1:  Priority for Tag [CoS 0]
  <1> :VID  [   1]              <2> :QinQ Support [Disable]

Port 2:  Priority for Tag [CoS 0]
  <3> :VID  [   1]              <4> :QinQ Support [Disable]

Port 3:  Priority for Tag [CoS 0]
  <5> :VID  [   1]              <6> :QinQ Support [Disable]

Port 4:  Priority for Tag [CoS 0]
  <7> :VID  [   1]              <8> :QinQ Support [Disable]

 <M> :Management VID [   1]
 <T> :Tag Type (Hex) [8100]
 <Z> :Go to VLAN Table Configuration Page.
 <S> :Save Settings.

<ESC>:Don't Save Settings and Go to Previous Menu.
```

2. Select <M> **Management VID** and change to 5. Save.



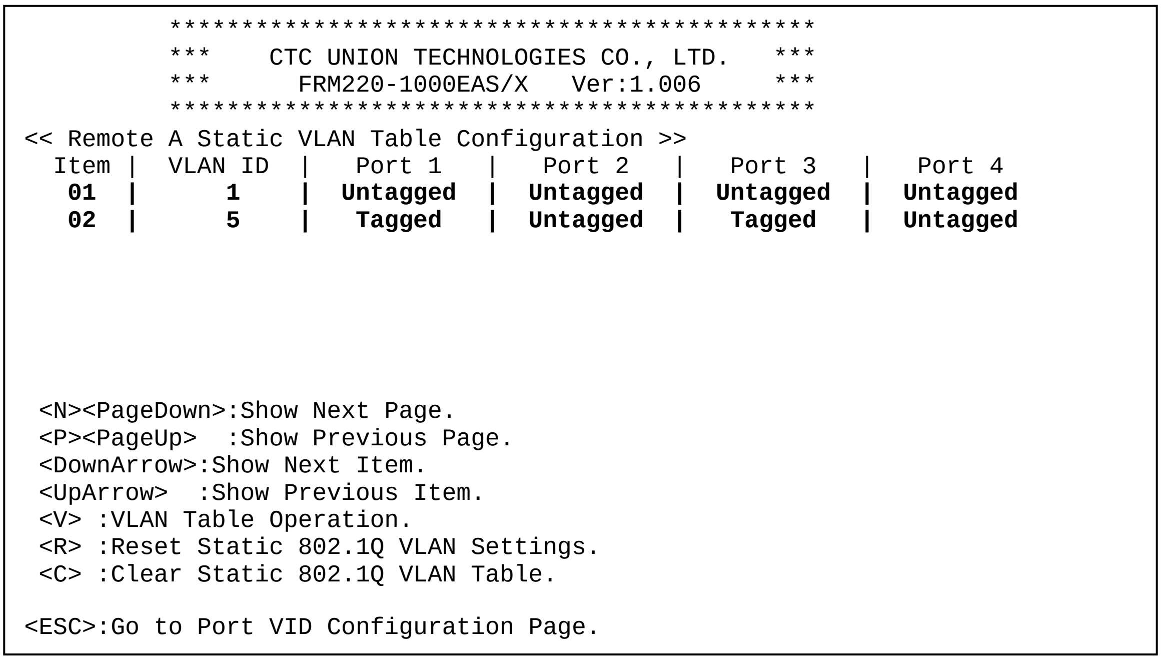
```
 Set Management VID(The Default Value of 1).

<ESC>:Discard and Return.

Please Input 1 ~ 4094 :[5   ]
```

Next, configure the Static 802.1Q VLAN table as follows:

A. Make VID=1 and 'Untag' for all ports.
B. Make VID=5 and make it 'Tagged' for port 1 (fiber) and 'Tagged' for port 3 (UTP). You can set ports 2 & 4 to 'Untagged' if they are not used.

3. From the VLAN Status and Configuration page, select <Z> **Go to VLAN Table Configuration**. Then select <V> **VLAN Table Operation**. Create VID 1 and untag all ports. Save. The create VID 5 and make sure it is 'Tagged' on ports 1 and 3. Save

The results look like this:



```
          *********************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
          ***      FRM220-1000EAS/X   Ver:1.006     ***
          *********************************************
<< Remote A Static VLAN Table Configuration >>
  Item |  VLAN ID  |   Port 1   |   Port 2   |   Port 3   |   Port 4
   01  |     1     |  Untagged  |  Untagged  |  Untagged  |  Untagged
   02  |     5     |   Tagged   |  Untagged  |   Tagged   |  Untagged







 <N><PageDown>:Show Next Page.
 <P><PageUp>  :Show Previous Page.
 <DownArrow>:Show Next Item.
 <UpArrow>  :Show Previous Item.
 <V> :VLAN Table Operation.
 <R> :Reset Static 802.1Q VLAN Settings.
 <C> :Clear Static 802.1Q VLAN Table.

<ESC>:Go to Port VID Configuration Page.
```

Now, PC-A and PC-B can both manage the **1000EAS/X**. PC-A can ping PC-B.

To do all the above without any other settings, simply choose the **<7> 802.1Q VLAN Trunk** Advanced Feature, from the **Device Status and Configuration** page and set the Management VID=5. All other settings will be automatically done.

Action performed by this application:

If an untagged packet ingresses at **1000EAS/X** port 1 (Fiber), VID=1 tag will be added to the packet from the switch. When the packet egresses port 3 (UTP) VID=1 tag will be removed (untagged).

If a tagged packet with VID=5 ingresses at **1000EAS/X** port 1 (Fiber), it will be passed through the internal switch and still be tagged with VID=5 as it egresses port 3 (UTP).

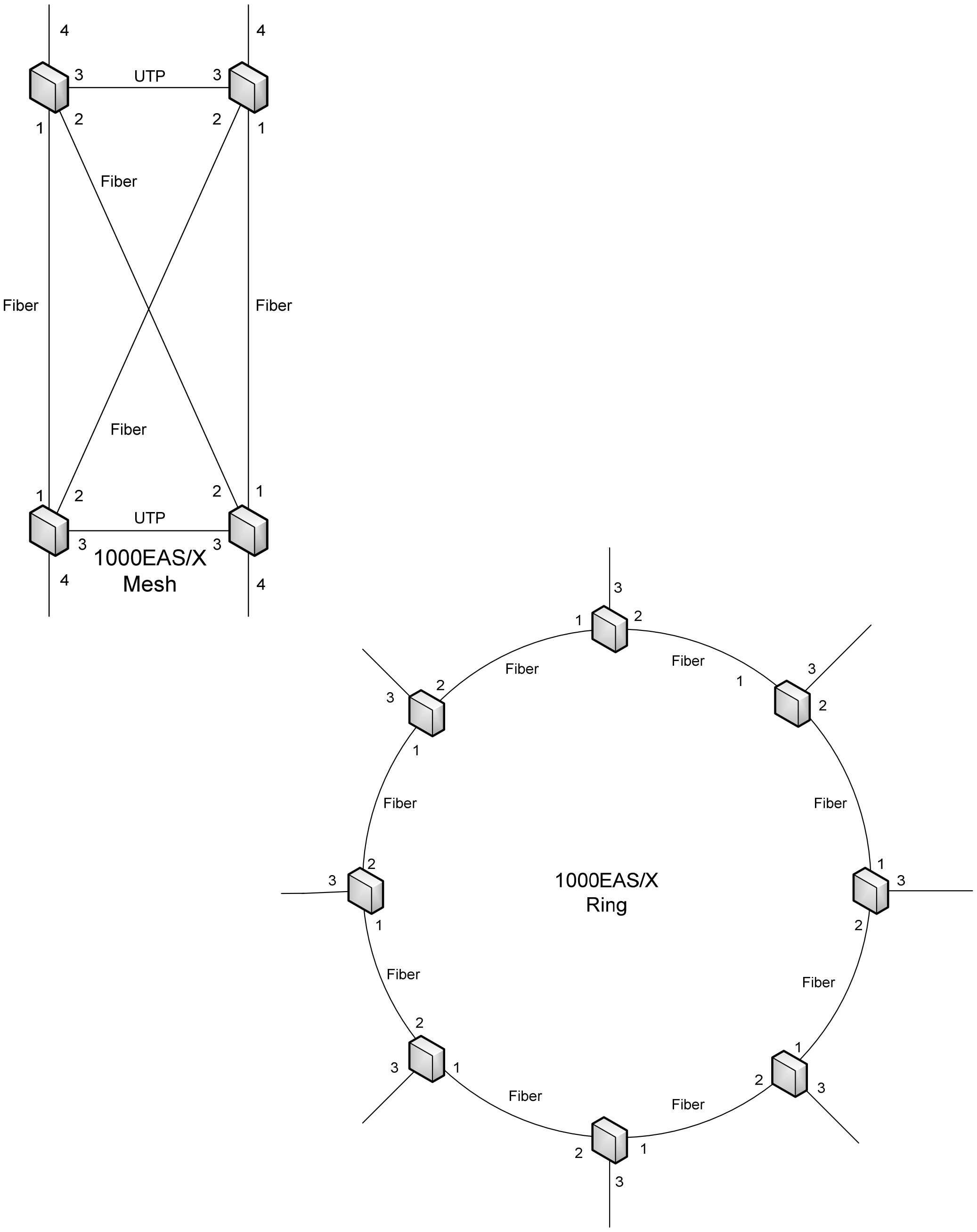
3.6.8 Spanning Tree Protocol

The Spanning Tree Protocol (STP) is a link layer (OSI Layer 2) network protocol that ensures a loop-free topology for any bridged LAN. The basic function of STP is to prevent bridge loops and ensuing broadcast radiation.

STP is standardized as 802.1D, while RSTP or Rapid Spanning Tree Protocol is standardized as 802.1W. STP creates a spanning tree within a mesh network of connected layer-2 Ethernet switches, and disables those links that are not part of the spanning tree, leaving a single active path between any two network nodes.

Spanning tree allows a network design to include spare (redundant) links to provide automatic backup paths if an active link fails, without the danger of bridge loops, or the need for manual enabling/disabling of these backup links. Bridge loops must be avoided because they result in flooding the internet network.

The following two examples that use STP are the ring and mesh topologies. Redundancy is built into these topologies as Mesh and Ring networks are self-healing through STP.



1. Return to the main menu on the local unit.

```
          *********************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
          ***      FRM220-1000EAS/X   Ver:1.003     ***
          *********************************************
Fiber 1   [Link Down     ] [Remote LB: Off  ]
Fiber 2   [Link Down     ] [Remote LB: Off  ]
UTP   3   [Link Up       ] [Speed:  100M] [Duplex: Full]
UTP   4   [Link Down     ] [Speed: -----] [Duplex: ----]
Remote A Module    [Empty            ]
Remote B Module    [Empty            ]
Port 1 OAM Mode    [Active ]
Port 2 OAM Mode    [Active ]
Advance Functions  [Normal ]

 <L> :Local    Status and Configuration.
 <A> :Remote A Status and Configuration.
 <B> :Remote B Status and Configuration.
 <M> :SNMP Manager.
 <S> :System Configuration.

<ESC>:Logout.
```

2. Select the **local unit** for configuration by choosing **<L>**.

```
          *********************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
          ***      FRM220-1000EAS/X   Ver:1.006     ***
          *********************************************
<< Local Status and Configuration >>
NMC Action    [Inactive (Stand alone)]

 <1> :Fiber 1 Status and Configuration.
 <2> :Fiber 2 Status and Configuration.
 <3> :UTP   3 Status and Configuration.
 <4> :UTP   4 Status and Configuration.
 <D> :Device  Status and Configuration.
 <Q> :Static 802.1Q VLAN Status and Configuration.
 <P> :Port VLAN Status and Configuration.
 <S> :Spanning Tree Status and Configuration.
 <L> :Link Loss Forwarding Configuration.
 <C> :Counters Status and Configuration.
 <M> :MAC Address Table.

<ESC>:Go to Previous Menu.
```

3. Select the Device Status and Configuration menu by choosing <D>.

```
           *********************************************
           ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
           ***      FRM220-1000EAS/X   Ver:1.006     ***
           *********************************************
<< Local Device Status and Configuration >>

 <1> :MAC Learning Function    [Enable ]
 <2> :Pause Frame              [Disable]
 <3> :Advance Functions        [Normal ]
 <4> :UPnP                     [Disable]
 <5> :QoS Priority Mode        [Weighted]
 <6> :Maximum OAMPDUs Size (60 ~ 1518 Octets) [1500]
 <7> :Accept Remote H/W Reset  [Disable]
 <8> :Tag's CoS Mapping to Internal Classify.
 <A> :Remote A H/W Reset.
 <B> :Remote B H/W Reset.
 <C> :Remote TLPT              [Disable]
 <L> :Load Default Settings and Write to System.
 <R> :System Reboot.
```

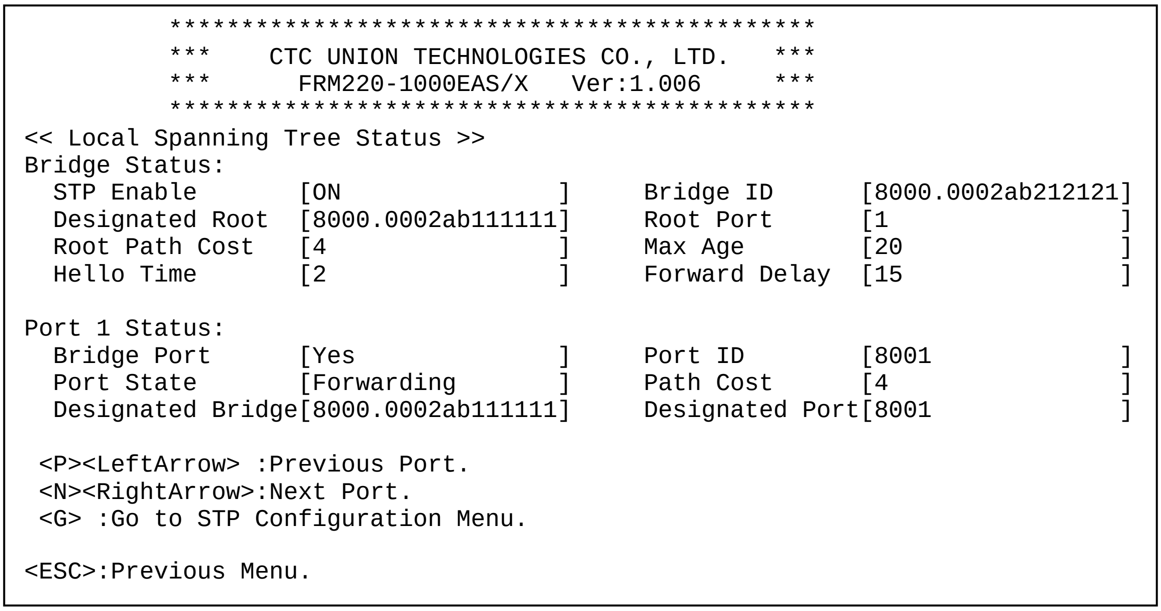
4. Select the **Advanced Functions** menu by choosing **<3>**.

```
Select Advance Functions.

 <0> Normal
 <1> Port 1 and Port 2 Trunk Bandwidth 2G
 <2> Port 1 to Port 2 Mirror
 <3> Port 1 and Port 2 Redundancy
 <4> Static 802.1Q VLAN
 <5> Q-in-Q VLAN
 <6> Static 802.1Q VLAN & Port 1/2 Redundancy
 <7> 802.1Q VLAN Trunk
 <8> Spanning Tree Protocol

<ESC>:Previous Menu.
```

5. Select the **Spanning Tree Protocol** menu by choosing **<8>**.
6. Return to the Local Status and Configuration menu by pressing **<ESC>**

```
<< Local Status and Configuration >>
NMC Action    [Inactive (Stand alone)]

 <1> :Fiber 1 Status and Configuration.
 <2> :Fiber 2 Status and Configuration.
 <3> :UTP   3 Status and Configuration.
 <4> :UTP   4 Status and Configuration.
 <D> :Device  Status and Configuration.
 <Q> :Static 802.1Q VLAN Status and Configuration.
 <P> :Port VLAN Status and Configuration.
 <S> :Spanning Tree Status and Configuration.
 <L> :Link Loss Forwarding Configuration.
 <C> :Counters Status and Configuration.
 <M> :MAC Address Table.

<ESC>:Go to Previous Menu.
```

7. Select <S>. to bring up the Spanning Tree Status and Configuration menu.



```
          *********************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
          ***      FRM220-1000EAS/X   Ver:1.006     ***
          *********************************************
<< Local Spanning Tree Status >>
Bridge Status:
  STP Enable       [ON                ]     Bridge ID      [8000.0002ab212121]
  Designated Root  [8000.0002ab111111]     Root Port      [1                ]
  Root Path Cost   [4                 ]     Max Age        [20               ]
  Hello Time       [2                 ]     Forward Delay  [15               ]

Port 1 Status:
  Bridge Port      [Yes               ]     Port ID        [8001             ]
  Port State       [Forwarding        ]     Path Cost      [4                ]
  Designated Bridge[8000.0002ab111111]     Designated Port[8001             ]

 <P><LeftArrow> :Previous Port.
 <N><RightArrow>:Next Port.
 <G> :Go to STP Configuration Menu.

<ESC>:Previous Menu.
```

The root bridge of the spanning tree is the bridge with the lowest bridge ID. Each bridge has a unique identifier (ID) and a configurable priority number; the **Bridge ID** contains both numbers. To compare two bridge IDs, the priority is compared first. If two bridges have equal priority, then the MAC addresses are compared. For example, if switches A (MAC=0002ab111111) and B (MAC=0002ab212121) both have a priority of 8000, then switch A will be selected as the root bridge (it has the lower value MAC address). If the network administrators would like switch B to become the root bridge, they must set its priority to be less than 8000.

Spanning tree computes its path by following the path of least cost, i.e., a path from the device to the root that has minimum cost among all paths from the device to the root. The cost of traversing a path is the sum of the costs of the segments on the path. The port connecting to that path becomes the root port (RP) of the bridge. Different technologies have different default costs for network segments. An administrator can configure the cost of traversing a particular network segment. The default **root path cost** in **1000EAS/X** is 0.

The switch sends a **BPDU** (Bridge Protocol Data Units) frame using the unique MAC address of the port itself as a source address, and a destination address of the STP multicast address 01:80:C2:00:00:00.

There are three types of BPDUs:

1. Configuration BPDU (CBPDU), used for Spanning Tree computation
2. Topology Change Notification (TCN) BPDU, used to announce changes in the network topology
3. Topology Change Notification Acknowledgment (TCA)

Hello Time is the time interval (number of seconds between) at which the root bridge transmits configuration BPDUs.

When a device is first attached to a switch port, it will not immediately start to forward data. It will instead go through a number of states while it processes BPDUs and determines the topology of the network. The time spent in the listening and learning states is determined by a value known as the **Forward Delay** (default 15 seconds and set by the root bridge).

Maximum Age, referred to by the switch as **Max Age**, is the amount of time a switch will retain a BPDU's contents before discarding it. The default is 20 seconds. It also influences the bridge table aging timer during the Topology Change Notification process.

Remember that these timers should not be changed lightly. If you decide to change any or all of these timers, that change must be configured on the root bridge! The root bridge will inform the non-root switches of the change via BPDUs.

3.6.9 Class of Service

Class of Service (COS) is a technique used to deliver Quality of Service (QoS) in a network. CoS is a way of classifying and prioritizing packets based on classification. A "first class" priority label is assigned to data applications - such as mission-critical data transactions, or video or voice transmissions - which require faster turnaround, while a lower-priority label is assigned to less time-sensitive traffic, such as e-mail and Web surfing.

CoS, as defined in IEEE 802.1p, uses Layer 2 VLAN Tagging and makes use of three bits in the Ethernet frame header that can be used to specify priority. The field specifies a priority value of between 0 and 7 inclusive that can be used by Quality of Service (QoS) disciplines to differentiate traffic.

CoS operates only on Ethernet at the data link layer.

Where QoS mechanisms are used, an aggregate traffic stream may be classified into a number of constituent classes, and different QoS guarantees may be provided to different classes within the aggregate. When a class has a defined minimum bandwidth assurance, this is referred to as the ***class capacity***.

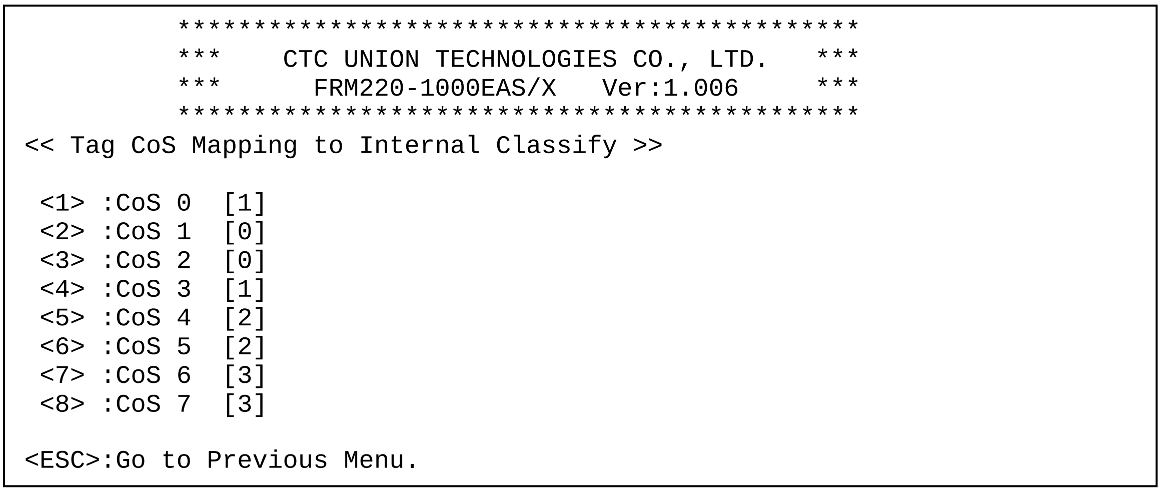
1000EAS/X supports either a fixed-priority (strict-priority) or weighted (fair-queuing) scheme.
In the strict priority scheme, all top-priority frames egress a port until that priority's queue is empty. Then the next lower priority queue's frames egress. This approach can cause the lower priorities to be starved of opportunity for transmitting any frames but ensures all high priority frames egress the switch as soon as possible.

In the weighted scheme, an 8, 4, 2, 1 weighting is applied to the four queue priorities. This approach prevents the lower priority frames from being starved of opportunity for transmission with only a slight delay to the higher priority frames.

The IEEE 802.3ac Tag contains IEEE 802.1p priority information, and it will override any default port CoS policy.

The switch in **1000EAS/X** has four internal priority queues (0~3) which need to be mapped to the 802.1Q QoS eight priority (0~7) levels. The switch requires that each port (two fiber and two UTP in **1000EAS/X**) have a mapping for queue priority.

To configure the CoS feature, first, from the main menu go to the <L> **Local Status and Configuration** menu, then select <D> **Device Status and Configuration**, then select <7> **Tag's CoS Mapping to Internal Classify**. This is where the Class of Service priority (0~7) can be mapped to **1000EAS/X** internal switch's priority queues (0~3). In the switch, 3 is the highest priority queue and 0 has the lowest priority.



```
           *********************************************
           ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
           ***      FRM220-1000EAS/X   Ver:1.006     ***
           *********************************************
<< Tag CoS Mapping to Internal Classify >>

 <1> :CoS 0  [1]
 <2> :CoS 1  [0]
 <3> :CoS 2  [0]
 <4> :CoS 3  [1]
 <5> :CoS 4  [2]
 <6> :CoS 5  [2]
 <7> :CoS 6  [3]
 <8> :CoS 7  [3]

<ESC>:Go to Previous Menu.
```

From the **Device Status and Configuration** page, the **QoS Priority Mode** can be configured either as a weighted classification or as strict classification.

```
Set Egress Scheduling Mode.

 <1> Weighted          <2> Strict

<ESC>:Previous Menu.
```

Next, for each of **1000EAS/X** ports (two fiber and two UTP) the CoS priority can be assigned.

```
<< Remote A Fiber 1 Status and Configuration >>
Link Status              [Link Up  ]
Remote Device Power      [OK]
OAM Remote Loopback Test [OFF]
OAM Looped               [OFF]

      Fiber Speed           [1000M]
      Port Active           [Enable ]
 <2> :Auto Laser Shutdown   [Disable]
 <3> :OAM Channel A Mode    [Active ]
 <4> :Remote Loopback Test  [Disable]
 <5> :Ingress Rate Limit    [Unlimited]

 Set Default Port's Class of Service(CoS).

 <0> 0          <1> 1          <2> 2          <3> 3
 <4> 4          <5> 5          <6> 6          <7> 7

<ESC>:Previous Menu.
```

So, for example, if the fiber port's CoS is set to '7' and CoS priority 7 is mapped to the internal switch's queue 3, then packets destined to egress this fiber port will have the highest priority.

3.6.10 Remote IP Setting

This feature allows setting up the TCP/IP for remotely connected converters (A and/or B) by utilizing OAM connection. From the main menu page, select either the **A or B Remote** unit. Select the **Device Status and Configuration** menu item. Then select **<0> :Set Remote A IP Address**.

```
Set Remote A IP Address

<1>:IP Address                [10.1.1.1]
<2>:Subnet Mask               [255.0.0.0]
<3>:Default Gateway IP        [10.1.1.254]

<ESC>:Previous Menu.
```

3.6.11 MAC Learning Function

This feature allows turning off the MAC learning function of the store & forward switch for special applications or for testing. From the main menu page, select the **Local**, **A or B Remote** unit. Select the **Device Status and Configuration** menu item. Then select **<1> :MAC Learning Function**.

```
Set MAC Learning Function.

 <0> Disable     <1> Enable

<ESC>:Previous Menu.
```

3.7 OAM Configuration

Ethernet in the First Mile (**EFM**) is the nickname of IEEE Std 802.3ah-2004, an amendment to the Ethernet standard, specifying "Media Access Control Parameters, Physical Layers, and Management Parameters for Subscriber Access Networks". The EFM standard was approved by the IEEE Standards Board in June 2004, and officially published on September 7, 2004. In 2005 it was included into the base IEEE 802.3 standard.

The "Last Mile" is the name traditionally given to the part of a public communication network that links the last provider-owned node (the central office, the street cabinet or pole) with the customer premises equipment (CPE). The "First Mile" is the exact same thing, viewed from the customer's perspective.

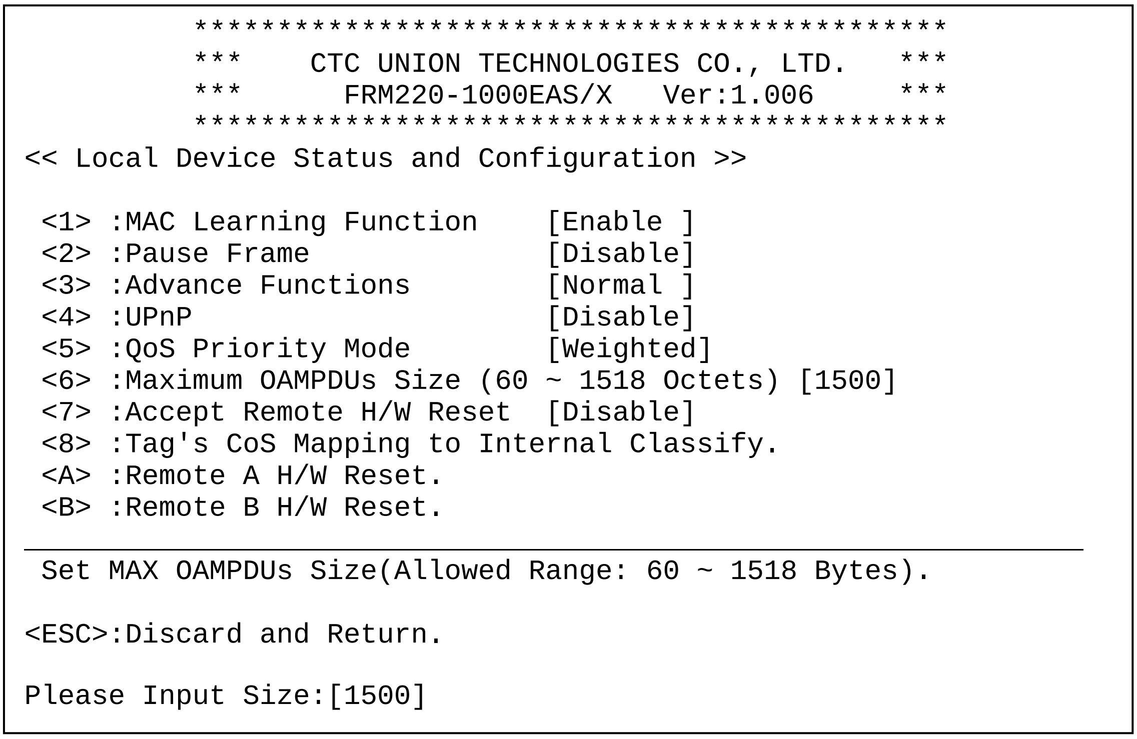
IEEE 802.3ah **OAM** (Operations, Administration, Maintenance) specification covers the OAM frames used across a physical IEEE 802.3 medium between a Provider and a Customer, or perhaps between two Provider ports or two Customer ports. In **1000EAS/X** product, OAM refers to the frames sent between units on a fiber link. OAM is **NOT** forwarded over links.

Ethernet **OAM** is complementary, not competitive, with **SNMP** (Simple Network Management Protocol) management in that it provides some basic management functions at layer two, rather than using layer three and above as required by SNMP over an IP infrastructure. Ethernet OAM provides single-hop functionality in that it works only between two directly connected Ethernet stations. SNMP can be used to manage the Ethernet OAM interactions of one Ethernet station with another.

3.7.1 OAM PDU frame size

OAM PDU frames must be within the legal Ethernet frame size range of 64 to 1518 bytes. OAM frames **MUST** be untagged. The maximum transmit rate of OAM PDU frames is 10 per second. In an OAM pair, only the 'Active' unit needs to set the frame size. The 'Passive' OAM unit will negotiate and follow the 'Active' unit during **OAM Discovery**. The default and recommended OAM PDU size is 1500 bytes. The active and passive units must have the same OAM frame size.

To configure, from the main menu, select <L> (Local Status and Configuration), then select <D> (Device Status and Configuration). From this menu select <3> (Maximum OAMPDUs Size) and set as follows.

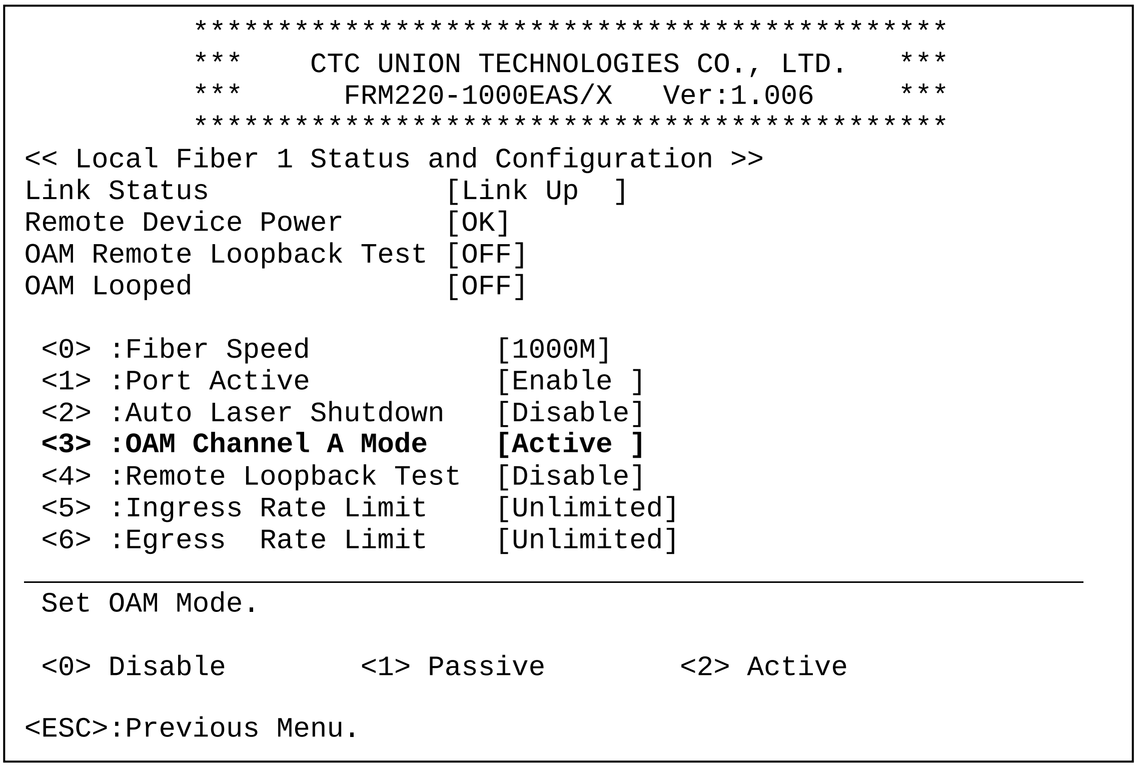


```
           *********************************************
           ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
           ***      FRM220-1000EAS/X   Ver:1.006     ***
           *********************************************
<< Local Device Status and Configuration >>

 <1> :MAC Learning Function    [Enable ]
 <2> :Pause Frame              [Disable]
 <3> :Advance Functions        [Normal ]
 <4> :UPnP                     [Disable]
 <5> :QoS Priority Mode        [Weighted]
 <6> :Maximum OAMPDUs Size (60 ~ 1518 Octets) [1500]
 <7> :Accept Remote H/W Reset  [Disable]
 <8> :Tag's CoS Mapping to Internal Classify.
 <A> :Remote A H/W Reset.
 <B> :Remote B H/W Reset.
_______________________________________________________________
 Set MAX OAMPDUs Size(Allowed Range: 60 ~ 1518 Bytes).

<ESC>:Discard and Return.

Please Input Size:[1500]
```

3.7.2 OAM Mode

The OAM in **1000EAS/X** converter only works on fiber links. Both units on the fiber link must be CTC Union **1000EAS/X** units. The OAM mode can be set to one of three choices: disabled, active or passive. In the OAM scheme, the 'active' unit will provide the OAM configuration to 'passive' unit during OAM discovery phase. If both units on the fiber link are set to 'active' mode, the one with lower MAC address will become the active node and the higher MAC address unit will assume passive mode.

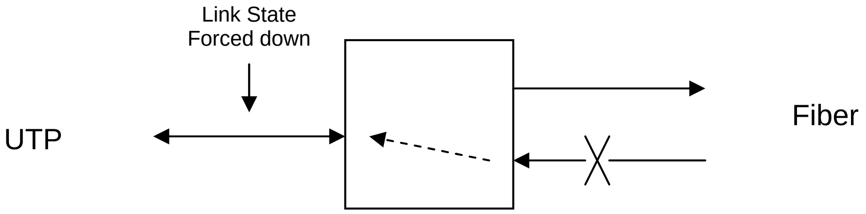
To configure, from the main menu, select <L> (Local Status and Configuration), then select the fiber port (1 or 2) <1> (Local Fiber 1 Status and Configuration). From this menu select <3> (OAM Channel A Mode) and set as follows.



```
           *********************************************
           ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
           ***      FRM220-1000EAS/X   Ver:1.006     ***
           *********************************************
<< Local Fiber 1 Status and Configuration >>
Link Status              [Link Up  ]
Remote Device Power      [OK]
OAM Remote Loopback Test [OFF]
OAM Looped               [OFF]

 <0> :Fiber Speed           [1000M]
 <1> :Port Active           [Enable ]
 <2> :Auto Laser Shutdown   [Disable]
 <3> :OAM Channel A Mode    [Active ]
 <4> :Remote Loopback Test  [Disable]
 <5> :Ingress Rate Limit    [Unlimited]
 <6> :Egress  Rate Limit    [Unlimited]
---------------------------------------------------------------
 Set OAM Mode.

 <0> Disable        <1> Passive        <2> Active

<ESC>:Previous Menu.
```

3.8 Link Loss Forwarding

In a simple media converter (two ports), a loss of fiber receive signal (link failure) can be used to force down the electrical Ethernet link and vice versa. This mechanism is referred to as "Link Loss Forwarding" or "Link Fault Pass-thru".



Link Loss Forwarding (LLF) Mechanism

1000EAS/X model is a four port L2 Gigabit Ethernet switch with two fiber and two electrical Ethernet ports. With Link Loss Forwarding mechanism, when one Ethernet port detects a link down condition, this media converter can be programmed to logically force down any or all of the other Ethernet ports. The settings are done by check box in a 4x4 matrix.

To configure, from the main menu, select <L> (Local Status and Configuration), then select <L> (Link Loss Forwarding Configuration).

```
          ********************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
          ***      FRM220-1000EAS/X   Ver:1.006     ***
          ********************************************
<< Local Link Loss Forwarding Configuration >>
                            |                Condition                  |
                            |  Port 1  |  Port 2  |  Port 3  |  Port 4  |
                 | Logical  | Link Loss| Link Loss| Link Loss| Link Loss|
-----------------+----------+----------+----------+----------+----------|
Port 1 Power Off | <0>[AND] |          |  <1>[ ]  |  <2>[ ]  |  <3>[ ]  |
-----------------+----------+----------+----------+----------+----------|
Port 2 Power Off | <4>[AND] |  <5>[ ]  |          |  <6>[ ]  |  <7>[ ]  |
-----------------+----------+----------+----------+----------+----------|
Port 3 Power Off | <8>[AND] |  <9>[ ]  |  <A>[ ]  |          |          |
-----------------+----------+----------+----------+----------+----------|
Port 4 Power Off | <B>[AND] |  <C>[ ]  |  <D>[ ]  |          |          |
-----------------+----------+----------+----------+----------+----------+

 <R> :Reset Settings.
 <S> :Confirm and Save Settings.

<ESC>:Go to Previous Menu.
```

Example 1: FX port 1 Tx off if any port 2, 3, 4 Rx loss:
keyin 1,2,3 and keyin 0 to change 'and' to 'or'

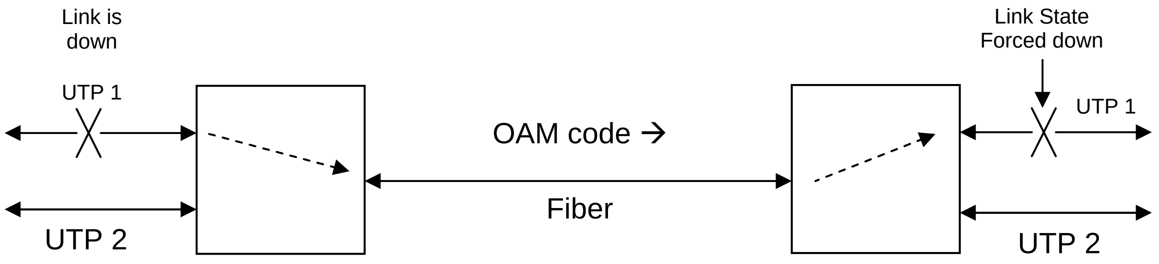
Example 2: FX port 1 Tx off if all ports 2, 3, 4 Rx loss
keyin 1,2,3 and leave Port 1 as 'And'

Example 3: FX port 1 Tx off if port 3 Rx loss
keyin 2 (only one selected so logic doesn't care)

After setting up the matrix, you must press <S> to **Confirm and Save** the settings.

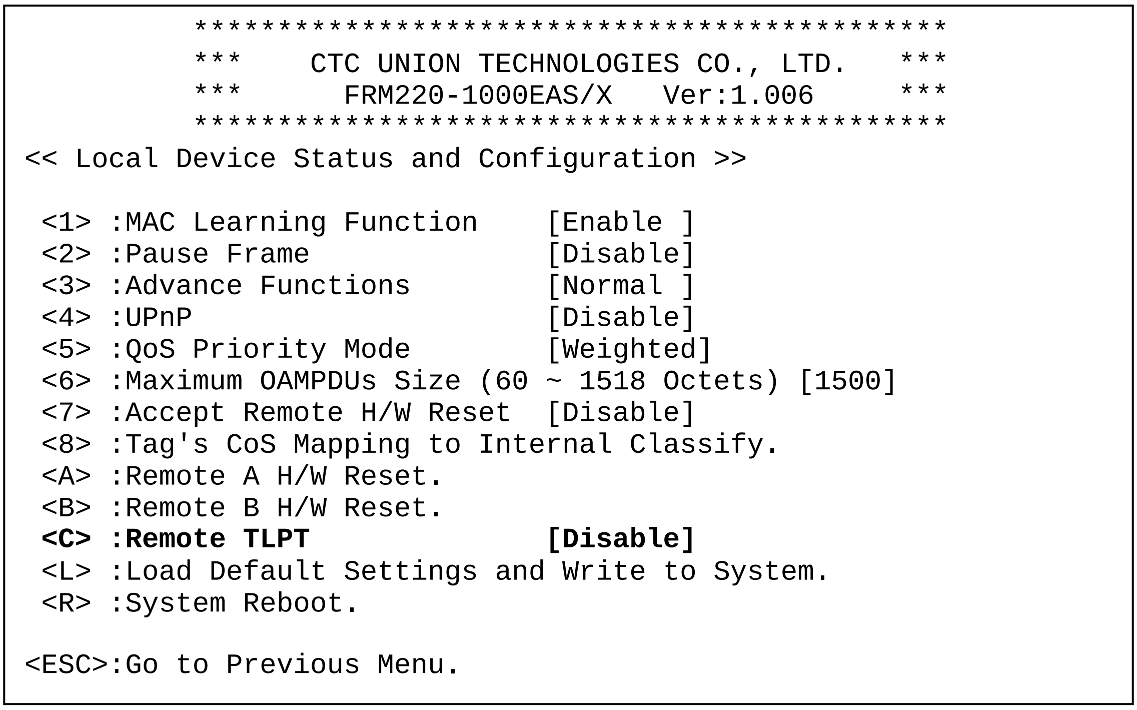
3.9 Remote Transparent Link Pass Through (TLPT)

When a media converter has multiple ports (two UTP ports in this case), a loss of UTP receive signal (link failure) cannot be used to force down the Ethernet fiber link without also affecting the traffic from the other UTP port. In order to provide a link loss forwarding or link fault pass-thru in this case, **1000EAS/X** can enable the **Transparent Link Pass Through** function. The converter that senses the UTP link loss condition will then generate an OAM signal to the remote of the condition. The remote will then disable the appropriate UTP port.



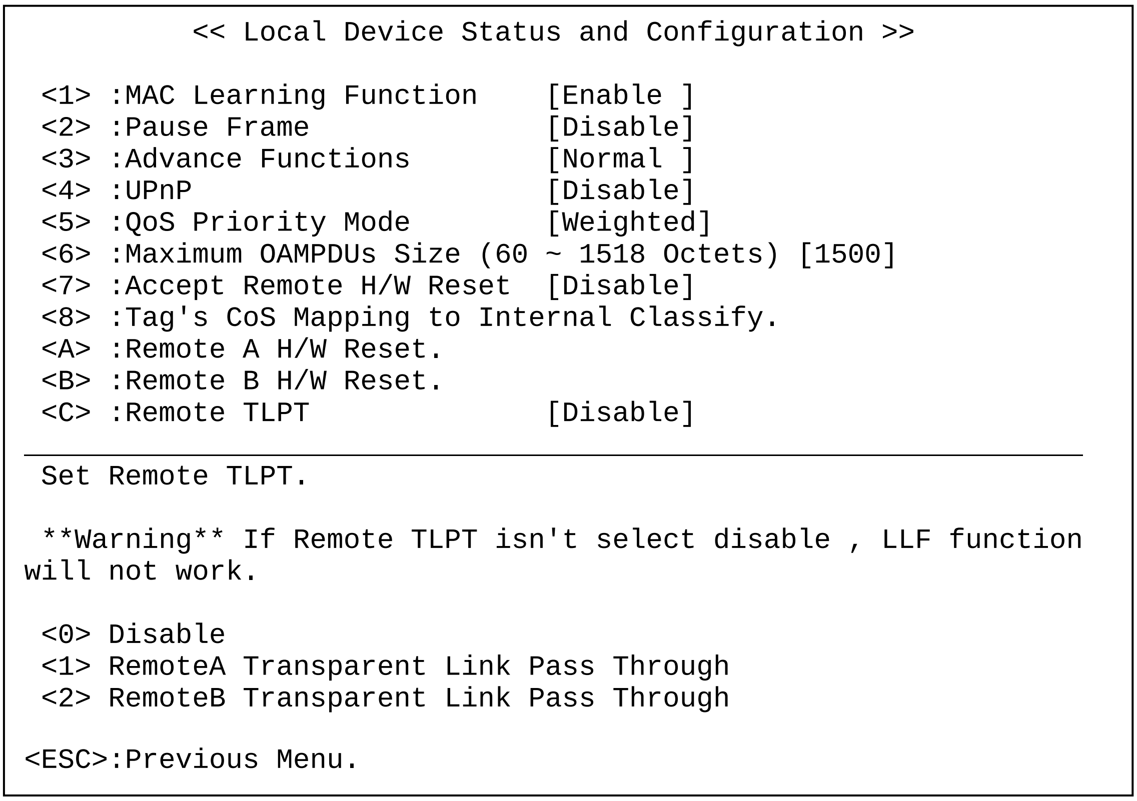
Transparent Link Pass Through (TLPT) Mechanism

From the main menu, select the Local Status and Configuration menu <L>, then select the Device Status and Configuration <D>



```
          *********************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
          ***      FRM220-1000EAS/X   Ver:1.006     ***
          *********************************************
<< Local Device Status and Configuration >>

 <1> :MAC Learning Function    [Enable ]
 <2> :Pause Frame              [Disable]
 <3> :Advance Functions        [Normal ]
 <4> :UPnP                     [Disable]
 <5> :QoS Priority Mode        [Weighted]
 <6> :Maximum OAMPDUs Size (60 ~ 1518 Octets) [1500]
 <7> :Accept Remote H/W Reset  [Disable]
 <8> :Tag's CoS Mapping to Internal Classify.
 <A> :Remote A H/W Reset.
 <B> :Remote B H/W Reset.
 <C> :Remote TLPT              [Disable]
 <L> :Load Default Settings and Write to System.
 <R> :System Reboot.

<ESC>:Go to Previous Menu.
```

Select <C> Remote TLPT



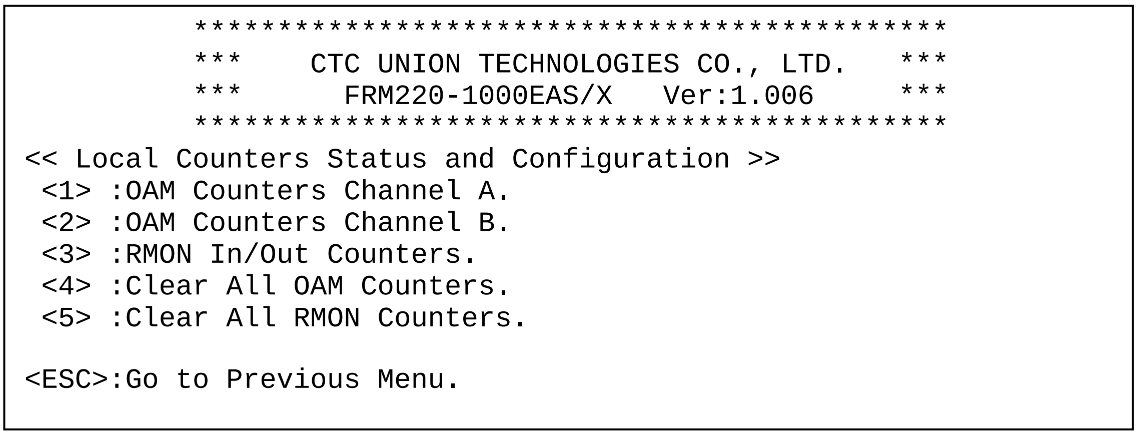
```
          << Local Device Status and Configuration >>

 <1> :MAC Learning Function    [Enable ]
 <2> :Pause Frame              [Disable]
 <3> :Advance Functions        [Normal ]
 <4> :UPnP                     [Disable]
 <5> :QoS Priority Mode        [Weighted]
 <6> :Maximum OAMPDUs Size (60 ~ 1518 Octets) [1500]
 <7> :Accept Remote H/W Reset  [Disable]
 <8> :Tag's CoS Mapping to Internal Classify.
 <A> :Remote A H/W Reset.
 <B> :Remote B H/W Reset.
 <C> :Remote TLPT              [Disable]
---------------------------------------------------------------
 Set Remote TLPT.

 **Warning** If Remote TLPT isn't select disable , LLF function
will not work.

 <0> Disable
 <1> RemoteA Transparent Link Pass Through
 <2> RemoteB Transparent Link Pass Through

<ESC>:Previous Menu.
```

<0> Disable : any TLPT previous setting
<1> RemoteA : Set link loss to transparently pass to Remote A unit (connected to fiber port 1)
<2> RemoteB : Set link loss to transparently pass to Remote B unit (connected to fiber port 2)

Note: When enabling TLPT, the normal LFP cannot be enabled. They are mutually exclusive.

3.10 Counters

1000EAS/X has internal counters that keep track of the number of frames received and transmitted on each port. It also keeps count of OAM packets in and out of the fiber ports. From the Local Status and Configuration page, use <C> to view the counters.

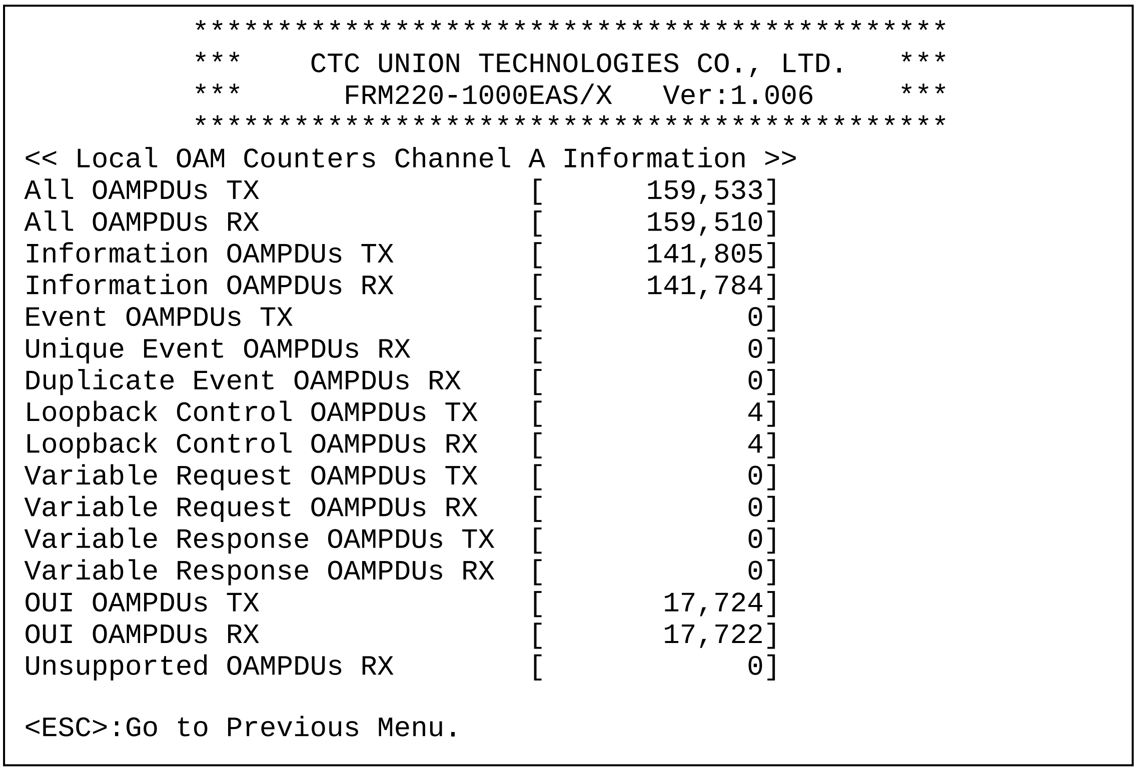


```
          *********************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
          ***      FRM220-1000EAS/X   Ver:1.006     ***
          *********************************************
<< Local Counters Status and Configuration >>
 <1> :OAM Counters Channel A.
 <2> :OAM Counters Channel B.
 <3> :RMON In/Out Counters.
 <4> :Clear All OAM Counters.
 <5> :Clear All RMON Counters.

<ESC>:Go to Previous Menu.
```

Select to view OAM counters from either fiber port, or the RMON counters for each port. The counters can also be cleared here.

3.10.1 OAM Counters

Each of the OAM counters is capable of keeping count via 32bit registers.
This is an example of OAM counters for fiber 1.

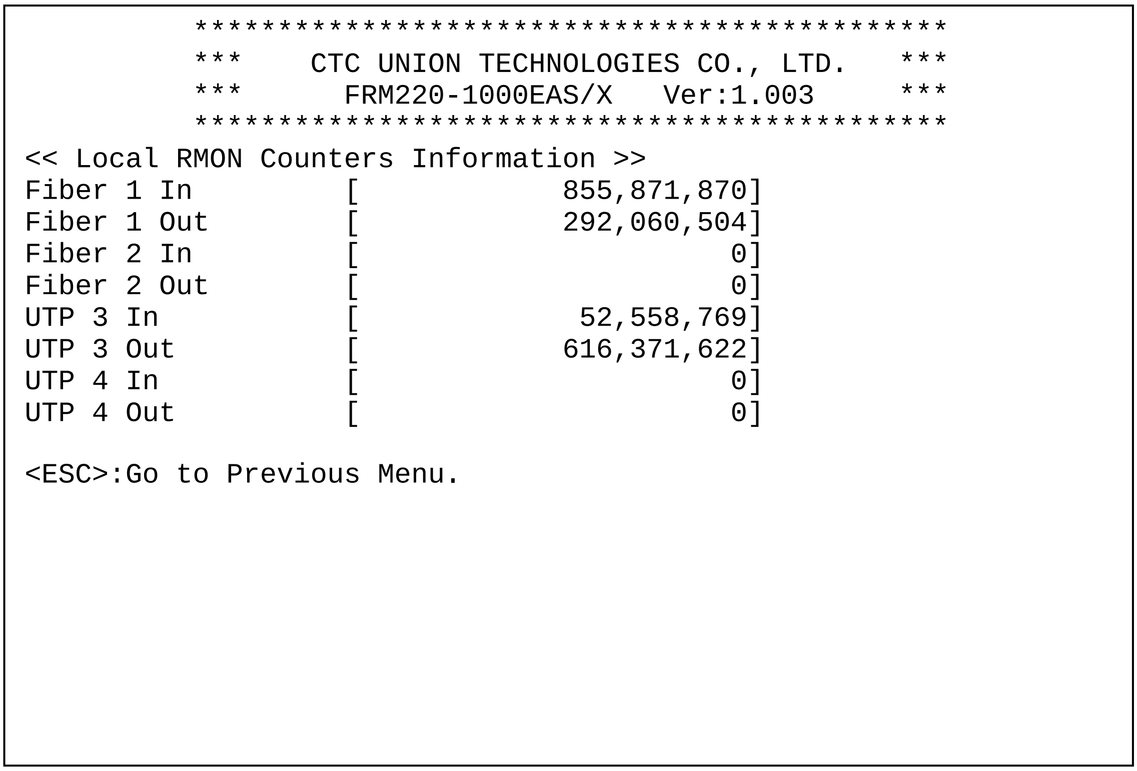


```
          *********************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
          ***      FRM220-1000EAS/X   Ver:1.006     ***
          *********************************************
<< Local OAM Counters Channel A Information >>
All OAMPDUs TX                [      159,533]
All OAMPDUs RX                [      159,510]
Information OAMPDUs TX        [      141,805]
Information OAMPDUs RX        [      141,784]
Event OAMPDUs TX              [            0]
Unique Event OAMPDUs RX       [            0]
Duplicate Event OAMPDUs RX    [            0]
Loopback Control OAMPDUs TX   [            4]
Loopback Control OAMPDUs RX   [            4]
Variable Request OAMPDUs TX   [            0]
Variable Request OAMPDUs RX   [            0]
Variable Response OAMPDUs TX  [            0]
Variable Response OAMPDUs RX  [            0]
OUI OAMPDUs TX                [       17,724]
OUI OAMPDUs RX                [       17,722]
Unsupported OAMPDUs RX        [            0]

<ESC>:Go to Previous Menu.
```

3.10.2 RMON Counters

RMON (Remote network MONitoring) for **1000EAS/X** supports statistics of frames transmitted and received for each port of the converter. The CPU of **1000EAS/X** will read the real time 64bit registers of the switch chip every 3 seconds and update the below counter information.

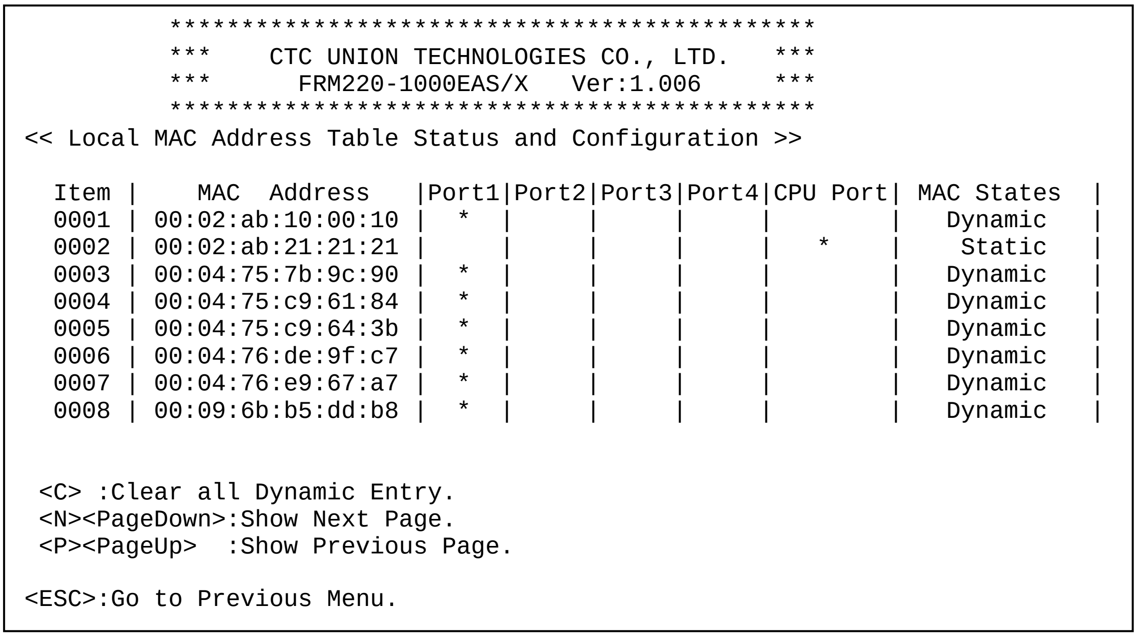
From the main menu, select the local or remote unit(s), then select **<C> Counters Status and Configuration**. The RMON counters are viewed by selecting **<3> :RMON In/Out Counters**.



```
          *********************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
          ***      FRM220-1000EAS/X   Ver:1.003     ***
          *********************************************
<< Local RMON Counters Information >>
Fiber 1 In         [            855,871,870]
Fiber 1 Out        [            292,060,504]
Fiber 2 In         [                      0]
Fiber 2 Out        [                      0]
UTP 3 In           [             52,558,769]
UTP 3 Out          [            616,371,622]
UTP 4 In           [                      0]
UTP 4 Out          [                      0]

<ESC>:Go to Previous Menu.
```

3.10.3 MAC Table

1000EAS/X has the ability to disable the MAC learning function of the L2 switch. By default, MAC learning is enabled. The default MAC aging is 5 minutes. From the main menu, select the local status, then select **<M> :MAC Address Table**.



```
          *********************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
          ***      FRM220-1000EAS/X   Ver:1.006     ***
          *********************************************
<< Local MAC Address Table Status and Configuration >>

  Item |    MAC  Address   |Port1|Port2|Port3|Port4|CPU Port| MAC States  |
  0001 | 00:02:ab:10:00:10 |  *  |     |     |     |        |   Dynamic   |
  0002 | 00:02:ab:21:21:21 |     |     |     |     |   *    |    Static   |
  0003 | 00:04:75:7b:9c:90 |  *  |     |     |     |        |   Dynamic   |
  0004 | 00:04:75:c9:61:84 |  *  |     |     |     |        |   Dynamic   |
  0005 | 00:04:75:c9:64:3b |  *  |     |     |     |        |   Dynamic   |
  0006 | 00:04:76:de:9f:c7 |  *  |     |     |     |        |   Dynamic   |
  0007 | 00:04:76:e9:67:a7 |  *  |     |     |     |        |   Dynamic   |
  0008 | 00:09:6b:b5:dd:b8 |  *  |     |     |     |        |   Dynamic   |


 <C> :Clear all Dynamic Entry.
 <N><PageDown>:Show Next Page.
 <P><PageUp>  :Show Previous Page.

<ESC>:Go to Previous Menu.
```

3.11 SNMP Configuration

3.11.1 General

The Simple Network Management Protocol (**SNMP**) is one of many protocols in the Internet Protocol (IP) suite. SNMP is the protocol recommended specifically for the exchange of management information between hosts residing on IP networks. Network management allows you to monitor and control network devices remotely using conventional computer network technology.

The SNMP management functions of **1000EAS/X** are provided by an internal SNMP agent, which utilizes communication over IP networks. The SNMP agent is compliant with the SNMPv1 and v2c standards. SNMP communications use the User Datagram Protocol (UDP). UDP is a connectionless transport protocol, part of the TCP/IP suite. The SNMP application uses an asynchronous command/response polling protocol and operates at the OSI Layer 7 (Layer 7 is the Application Layer. Other IP applications that operate at this layer are FTP, Telnet, HTTP, SMTP, etc.). All management traffic is initiated by the SNMP-based network management station. Only the addressed managed entity (agent) answers the polling of the management station (except for trap messages).

3.11.2 SNMP Operations

The SNMP protocol includes four types of operations:

getRequest Command for retrieving specific value of an "instance" from the managed node. The managed node responds with a getResponse message.

getNextRequest Command for retrieving sequentially specific management information from the managed node. The managed node responds with a getResponse message.

getBulkRequest Command for retrieving a block of management information from the managed node. The managed node responds with a getResponse message. getBulkRequest was introduced in SNMPv2c.

setRequest Command for manipulating the value of an "instance" within the managed node. The managed node responds with a getResponse message.

trap Management message carrying unsolicited information on extraordinary events (that is, events which occurred not in response to a management operation) reported by the managed node.

3.11.3 The Management Information Base

The management information base (MIB) includes a collection of managed objects. Managed objects are defined as parameters that can be managed, such as specific information on device configuring or on performance statistics values.

The MIB includes the definitions of relevant managed objects (MIB variables) for the specific node. Various MIB's can be defined for various management purposes, types of equipment, etc. The management data itself is a collection of integer, string and MIB address variables that contain all the information necessary to manage the node.

A leaf object's definition includes the range of instances (values) and the "access" rights:

Read-only Instances of an object can be read, but cannot be set.

Read-write Instances of an object can be read or set.

Write-only Instances of an object can be set, but cannot be read.

Not accessible Instances of an object cannot be read, nor set.

3.11.4 MIB Structure

The MIB has an inverted tree-like structure (root over leaves), with each definition of a managed instance forming one leaf, located at the end of a branch of that tree. Each "leaf" in the MIB is reached by a unique path. By numbering the branching points, starting with the top, each leaf can be uniquely defined by a sequence of numbers. The formal description of the managed objects and the MIB structure is provided in a special standardized format, called Abstract Syntax Notation 1, or **ASN.1** (pronounced A-S-N dot one).

Since the general collection of MIB's can also be organized in a similar structure, under the supervision of the Internet Activities Board (IAB), any parameter included in a MIB that is recognized by the IAB is uniquely defined.

To provide the flexibility necessary in a global structure, MIB's are classified in various classes (branches), one of them being the experimental branch, another being the management (mgmt) branch, and yet another the group of private (enterprise-specific) branches. Under the private enterprise-specific branch of MIB's, each enterprise (manufacturer) can be assigned a number, which is its enterprise number. The assigned number designates the top of an enterprise-specific sub-tree of non-standard MIB's.

Enterprise-specific MIB's are published and distributed by their creators, who are responsible for their contents. The MIB supported by **1000EAS/X** SNMP Agent follows RFC 1213 (MIB-2 standard).

3.11.5 SNMP Communities

To enable the delimitation of management domains, SNMP uses "communities". Each community is identified by a name, which is an alphanumeric string of up to 255 characters defined by the user. Any SNMP entity (this term includes both managed nodes and management stations) is assigned by its user a community name. In parallel, the user defines for each SNMP entity a list of the communities which are authorized to communicate with it, and the access rights associated with each community (this is the SNMP community name table of the entity).

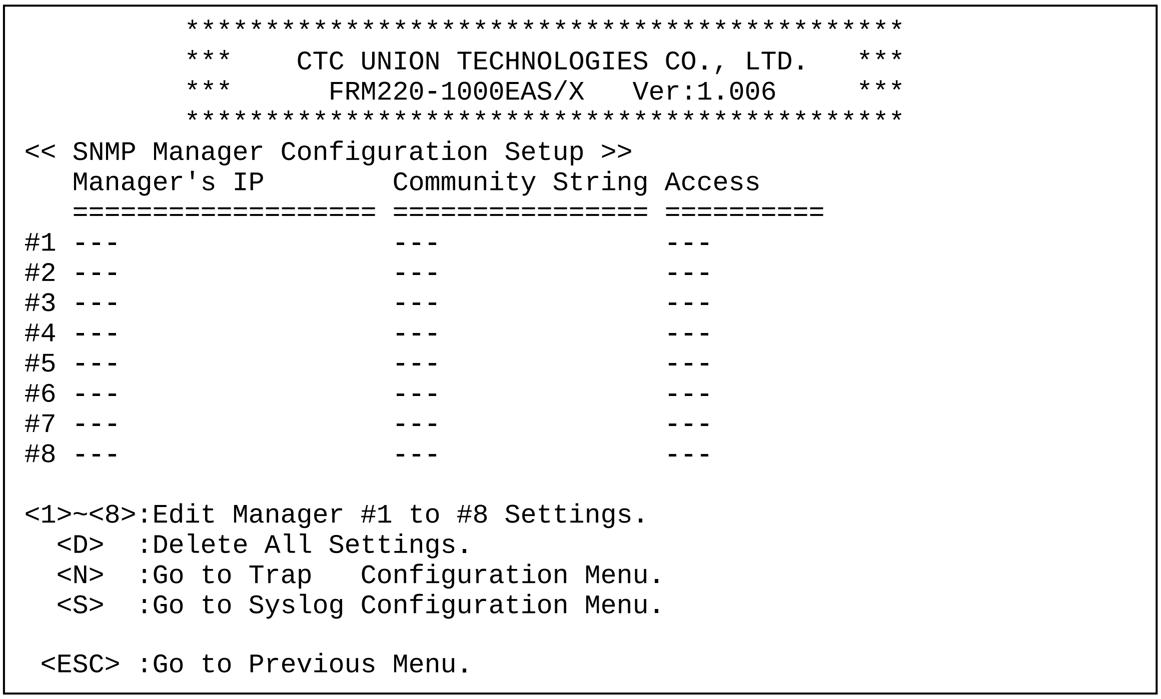
In general, SNMP agents support two types of access rights:

Read-only the SNMP agent accepts and processes only SNMP getRequest and getNextRequest commands from management stations which have a read-only community name.

Read-write the SNMP agent accepts and processes all the SNMP commands received from a management station with a read-write community name. SNMP agents are usually configured to send traps to management stations having read-write communities.

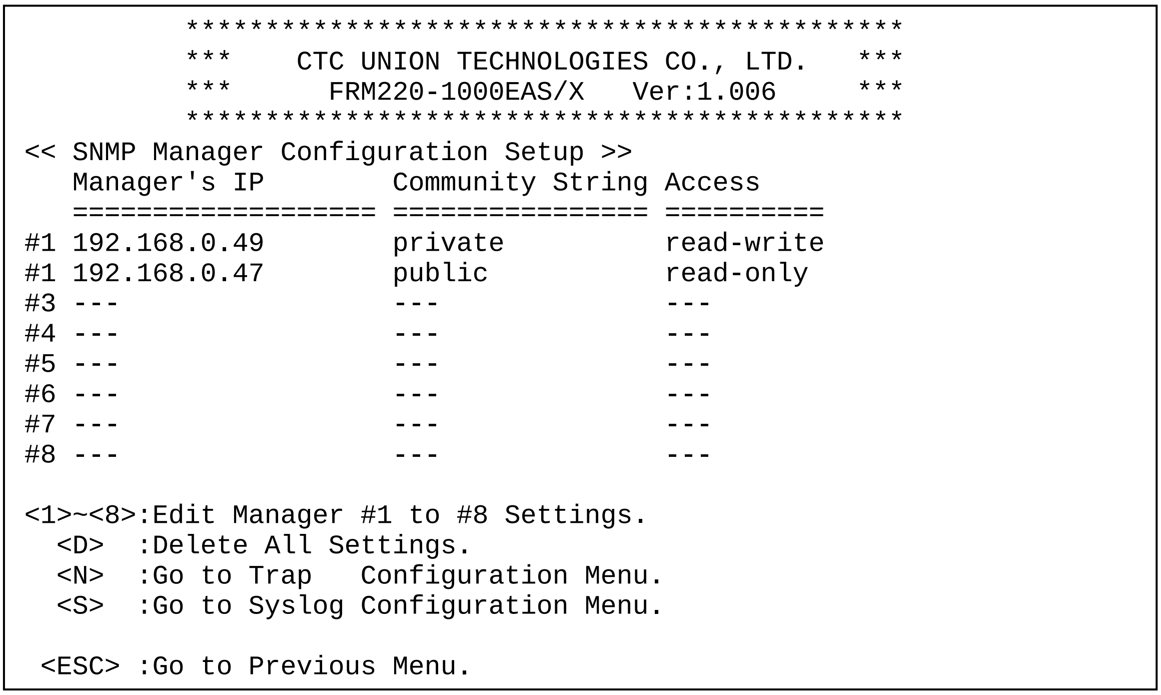
3.11.6 Configuring the SNMP Agent

The agent for **1000EAS/X** is embedded. From the Main Menu page, select <M> **SNMP Manager**. Manager configuration is required to tell the agent, who has the authority to access the SNMP via "Get" commands (read) or "Set" commands (write) and where to send "trap" messages (unsolicited messages that are usually generated by alarms in **1000EAS/X**).



```
          *********************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
          ***      FRM220-1000EAS/X   Ver:1.006     ***
          *********************************************
<< SNMP Manager Configuration Setup >>
   Manager's IP           Community String Access
   =================== ================ ==========
#1 ---                 ---              ---
#2 ---                 ---              ---
#3 ---                 ---              ---
#4 ---                 ---              ---
#5 ---                 ---              ---
#6 ---                 ---              ---
#7 ---                 ---              ---
#8 ---                 ---              ---

<1>~<8>:Edit Manager #1 to #8 Settings.
  <D>  :Delete All Settings.
  <N>  :Go to Trap   Configuration Menu.
  <S>  :Go to Syslog Configuration Menu.

 <ESC> :Go to Previous Menu.
```

The manager configuration has the ability to setup access for up to eight (8) different management workstations. The community strings act like passwords in dealing with the device via SNMP protocol. By assigning a manager's IP address, a community string, and assigning read/write or read only authority, an administrator can be granted control access to **1000EAS/X**.



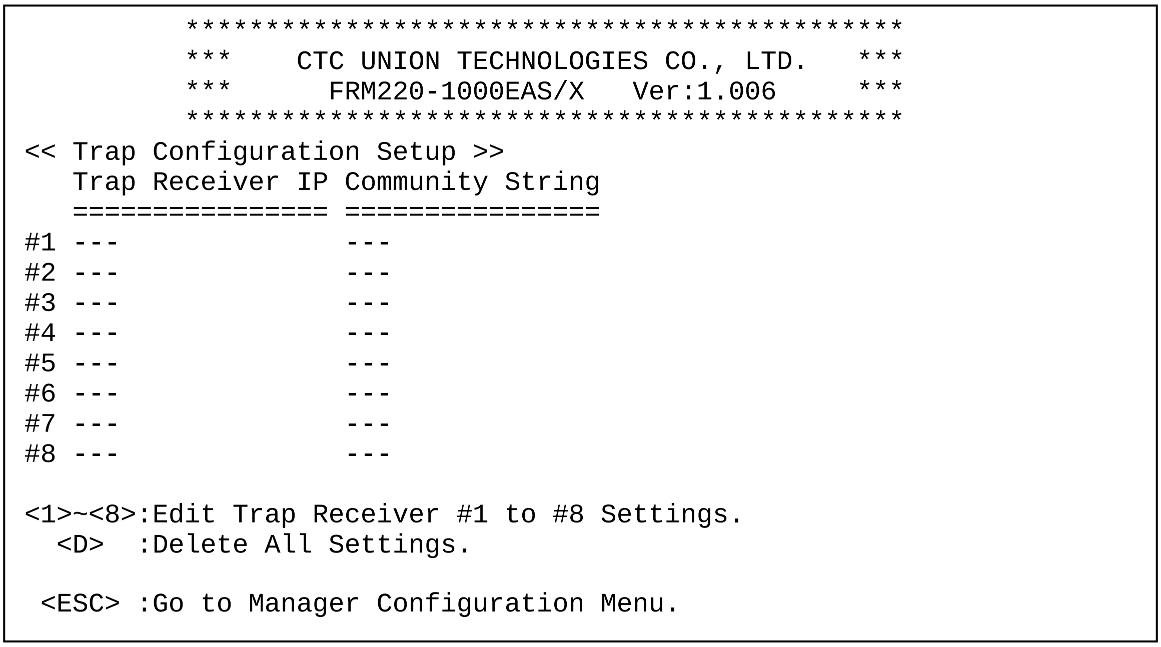
```
          *********************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
          ***      FRM220-1000EAS/X   Ver:1.006     ***
          *********************************************
<< SNMP Manager Configuration Setup >>
   Manager's IP           Community String Access
   =================== ================ ==========
#1 192.168.0.49        private          read-write
#1 192.168.0.47        public           read-only
#3 ---                 ---              ---
#4 ---                 ---              ---
#5 ---                 ---              ---
#6 ---                 ---              ---
#7 ---                 ---              ---
#8 ---                 ---              ---

<1>~<8>:Edit Manager #1 to #8 Settings.
  <D>  :Delete All Settings.
  <N>  :Go to Trap   Configuration Menu.
  <S>  :Go to Syslog Configuration Menu.

 <ESC> :Go to Previous Menu.
```

Note that in the above example, the management workstation with IP address 192.168.0.49 and using the community string 'private', has full read and write access. The management station at 192.168.0.47 has read only privileges when using the community string 'public'.

3.11.7 Configuring SNMP Traps

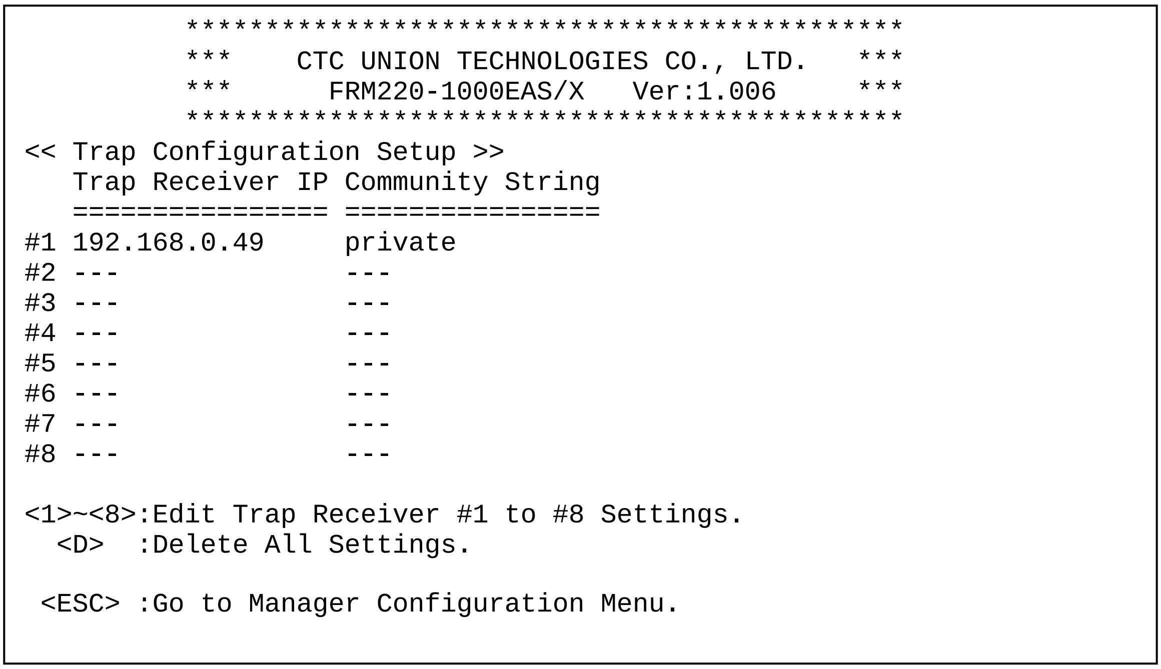
A **trap** is a type of **PDU** (Protocol Data Unit) used to report an alert or other asynchronous event about a managed subsystem. Traps are unsolicited messages sent by the agent to the network management software. They may be a system specifically generated message or they could be programmed through the Alarm Management, see 3.4.2 Alarm Settings.

The only configuration done here for traps is to enter the trap destination IP address. From the SNMP Manager menu, select <N> (Go to Trap Configuration Menu).



```
          *********************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
          ***      FRM220-1000EAS/X   Ver:1.006     ***
          *********************************************
<< Trap Configuration Setup >>
   Trap Receiver IP Community String
   ================ ================
#1 ---              ---
#2 ---              ---
#3 ---              ---
#4 ---              ---
#5 ---              ---
#6 ---              ---
#7 ---              ---
#8 ---              ---

<1>~<8>:Edit Trap Receiver #1 to #8 Settings.
  <D>  :Delete All Settings.

 <ESC> :Go to Manager Configuration Menu.
```

This SNMP agent supports up to eight (8) SNMP trap receivers that can be entered into this configuration menu.



```
          *********************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
          ***      FRM220-1000EAS/X   Ver:1.006     ***
          *********************************************
<< Trap Configuration Setup >>
   Trap Receiver IP Community String
   ================ ================
#1 192.168.0.49     private
#2 ---              ---
#3 ---              ---
#4 ---              ---
#5 ---              ---
#6 ---              ---
#7 ---              ---
#8 ---              ---

<1>~<8>:Edit Trap Receiver #1 to #8 Settings.
  <D>  :Delete All Settings.

 <ESC> :Go to Manager Configuration Menu.
```

In the above example, the SNMP network manager at 192.168.0.49 IP will receive traps.

This page left blank intentionally.

Chapter 4 Provisioning Via Web Based Management

4.1 Introduction

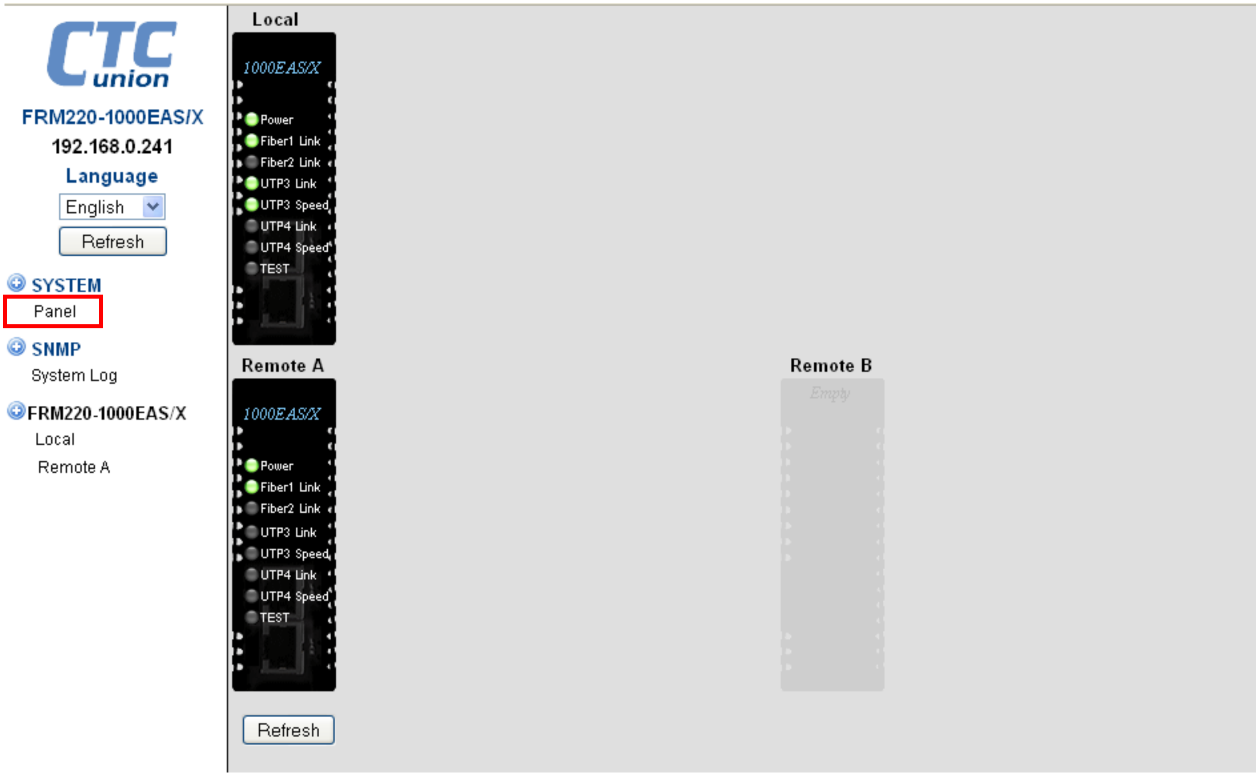
In an effort to make networking devices easier to configure, many devices can now be configured via a Web Page, which should be familiar to all Internet users.

The web page is accessed by the Default IP Address of the device from a Web Browser such as Internet Explorer or Firefox in the following way:

http://10.1.1.1/ (Assuming the Default IP Address is 10.1.1.1)

Before accessing this device by web browser, the IP address must be known or it must be reset or changed to be used on the desired network. Please refer to Chapter 1, section 1.8 for the factory reset procedure and to Chapter 3, 3.2 Serial Console Login for console login, 3.3 Telnet Login for Telnet login and 3.4 System Configuration for System Configuration settings.

4.2 Web Main Page



1000EAS/X has two fiber and two copper ports. Because it uses 802.3ah OAM on the fiber links for remote in-band management, it is able to see up to two (2) remote devices. The 'Remote A' device is connected to this unit's FIBER 1 port. If another **1000EAS/X** is connected to FIBER 2 port, then it will show up on this page as 'Remote B'. Each unit is shown with the exact LED status in real time.

The areas that support click on this screen are the graphic images themselves (directly into those units) and from the Menu item window on the left part of the screen,

1. System – The device's network settings, date & time and the alarm configurations are set here.
2. SNMP – The allowed SNMP managers, community strings and Trap Managers are set here. There is also a 'System Log' which can be viewed by selecting System Log under the SNMP main menu item.
3. The actual **1000EAS/X** unit’s graphic, local, Remote A, and Remote B can be entered for configuration with these items.

4.3 System

The following page is an example of the 'System' screen of **1000EAS/X**. There are three 'Tabs' for different setting windows.

4.3.1 Setup

The 'Setup' tab contains the networking settings for IP address, subnet mask, default gateway, hostname, TFTP server IP and image upgrade filename. After filling in, click the 'Apply Parameters' button.

4.3.2 Alias Information

Alias Information allows the user to enter identifying names to the local and/or remote devices. These alias names will be displayed on the front panel graphics when viewing the System Panel page. The alias names may contain up to 10 ASCII characters.

4.3.3 Parameter Management

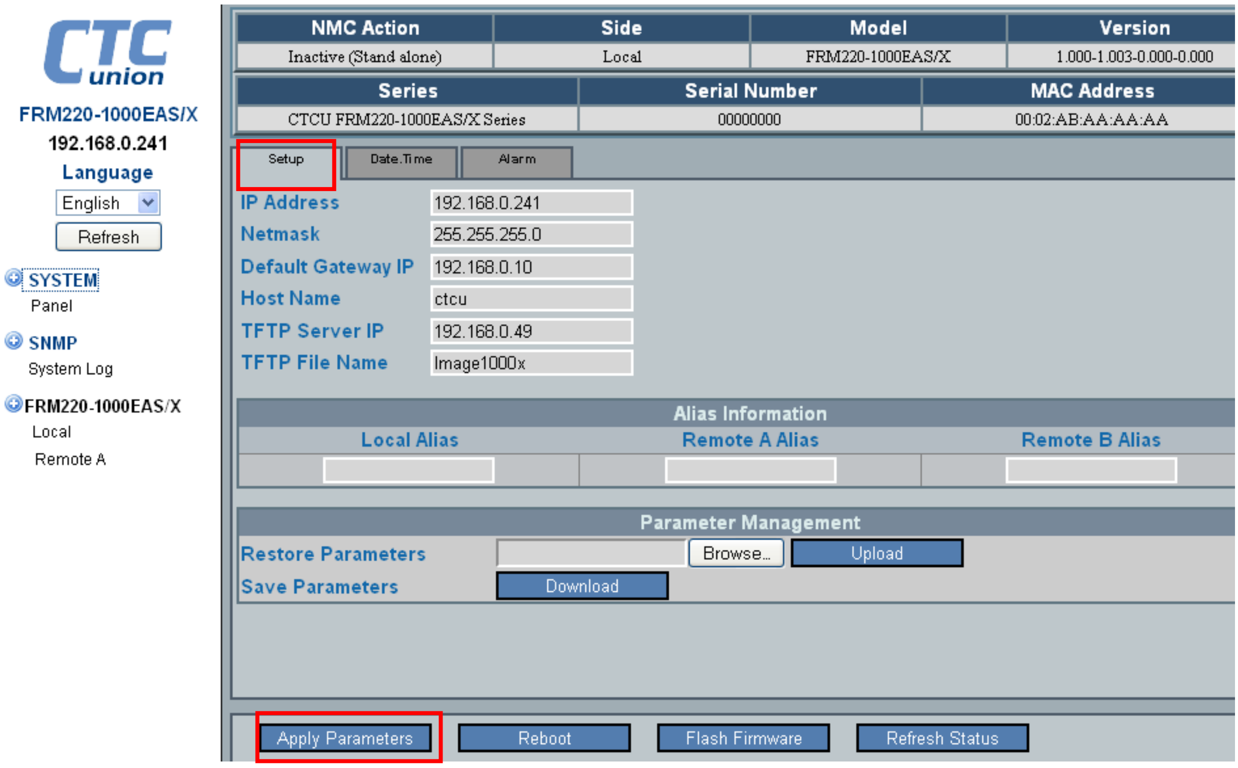
Parameter Management is provided and allows configuration settings to be downloaded from **1000EAS/X** (saved remotely on PC) or uploaded (restored) to an **1000EAS/X**. Parameter Management can be used to backup configuration data and allow quick recovery in case of hardware failure. It can also be used to clone configuration data quickly on different **1000EAS/X** units.

The ‘Apply Parameters’ button will immediately write all changes to **1000EAS/X** device.

The ‘Reboot’ button will force a cold start of **1000EAS/X** and should be used with caution.

Caution should be exercised when doing a **system reboot** as all traffic through all ports of the device will be **blocked** until the switch chip is initialized. In addition, the OAM discovery and negotiation will need to redo. If enabled, STP (Spanning Tree Protocol) discovery will need to rebuild path tables.

The ‘Refresh status’ button will update the display with any status changes.



NMC Action	Side	Model	Version
Inactive (Stand alone)	Local	FRM220-1000EAS/X	1.000-1.003-0.000-0.000

Series	Serial Number	MAC Address
CTCU FRM220-1000EAS/X Series	00000000	00:02:AB:AA:AA:AA

IP Address	192.168.0.241
Netmask	255.255.255.0
Default Gateway IP	192.168.0.10
Host Name	ctcu
TFTP Server IP	192.168.0.49
TFTP File Name	Image1000x

Alias Information

Local Alias	Remote A Alias	Remote B Alias

Parameter Management

Restore Parameters

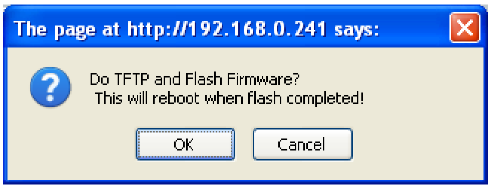
Save Parameters

4.3.4 Firmware Update

Occasionally, **CTC Union** will release new firmware for their products. If new functions are added through software modification or if programming errors are uncovered and resolved, those items will be listed in the firmware ***release note*** which is included in an 'upgrade package' along with a detailed upgrade procedure and the firmware image code.

Detailed instructions for upgrading are included in any upgrade package and may also be reviewed in Chapter 3 3.4.1 Firmware Upgrade. With a TFTP server setup and accessible from **1000EAS/X**, just enter the server's IP address and the flash image filename into the setup form, click the 'Apply Parameters' button, then click the 'Flash Firmware' button to initiate a firmware upgrade of **1000EAS/X** by downloading the image file (in the TFTP File Name field) from the TFTP server (in the TFTP Server IP field).

The following confirmation dialogue box will be shown. Click 'OK' to continue.



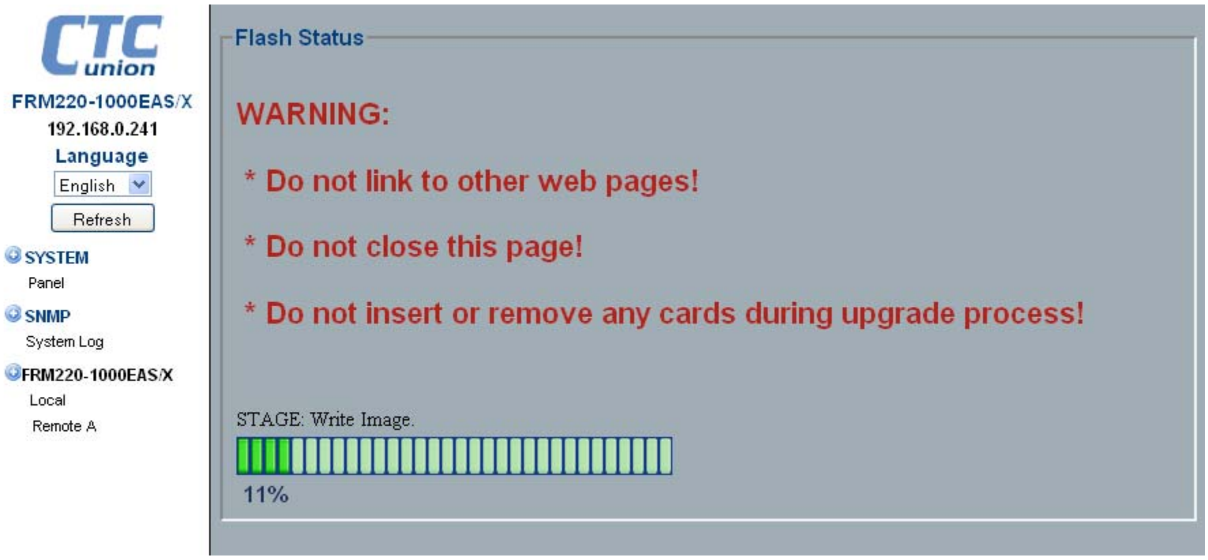
The page at http://192.168.0.241 says:

Do TFTP and Flash Firmware?
This will reboot when flash completed!

The upgrade will proceed by first downloading the firmware image and doing an ID code plus checksum check. Next the flash is erased and then written.

During the Erase and Write portion of upgrade, it is extremely important that nothing interrupt the upgrade or the device may be left with in-operable firmware code. Firmware upgrade failure will require factory repair to physically replace the flash chip.

Please heed the warnings on this page.



Flash Status

WARNING:

* Do not link to other web pages!

* Do not close this page!

* Do not insert or remove any cards during upgrade process!

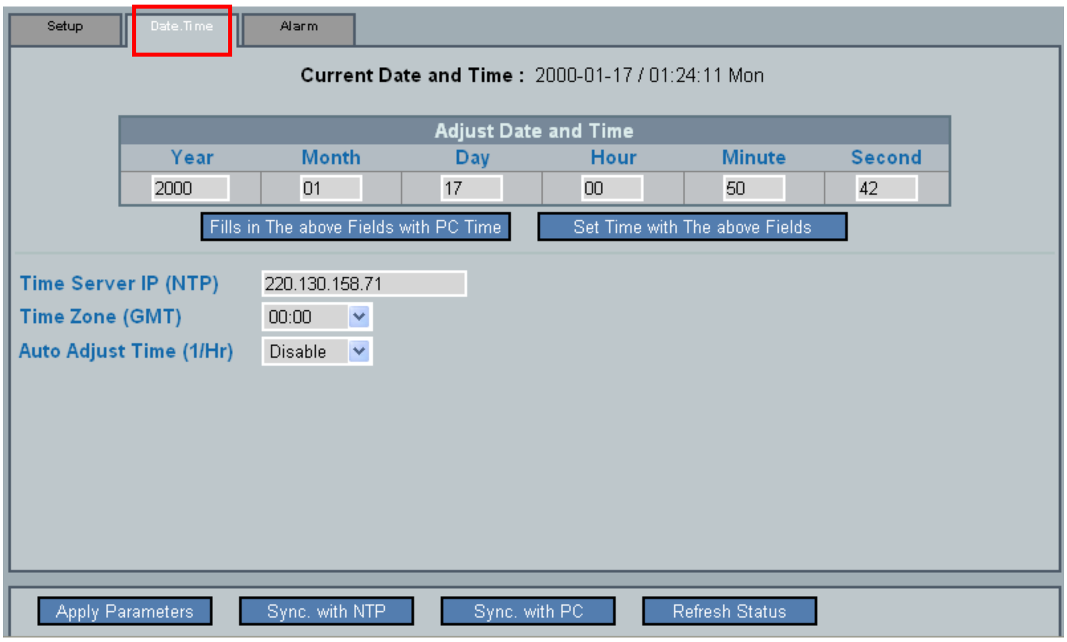
STAGE: Write Image.

11%

After the upgrade is completed, **1000EAS/X** will reset and reboot with the new firmware code.

4.3.5 Date & Time

The Date & Time tab provide manual setting or real time, from PC clock, or SNTP network time settings with time zone adjustment from UTC time. Proper time setting is important when the device is managed via SNMP on the network. Accurate time keeping will allow syslog messages to be correctly time stamped.



Current Date and Time : 2000-01-17 / 01:24:11 Mon

Adjust Date and Time					
Year	Month	Day	Hour	Minute	Second
2000	01	17	00	50	42

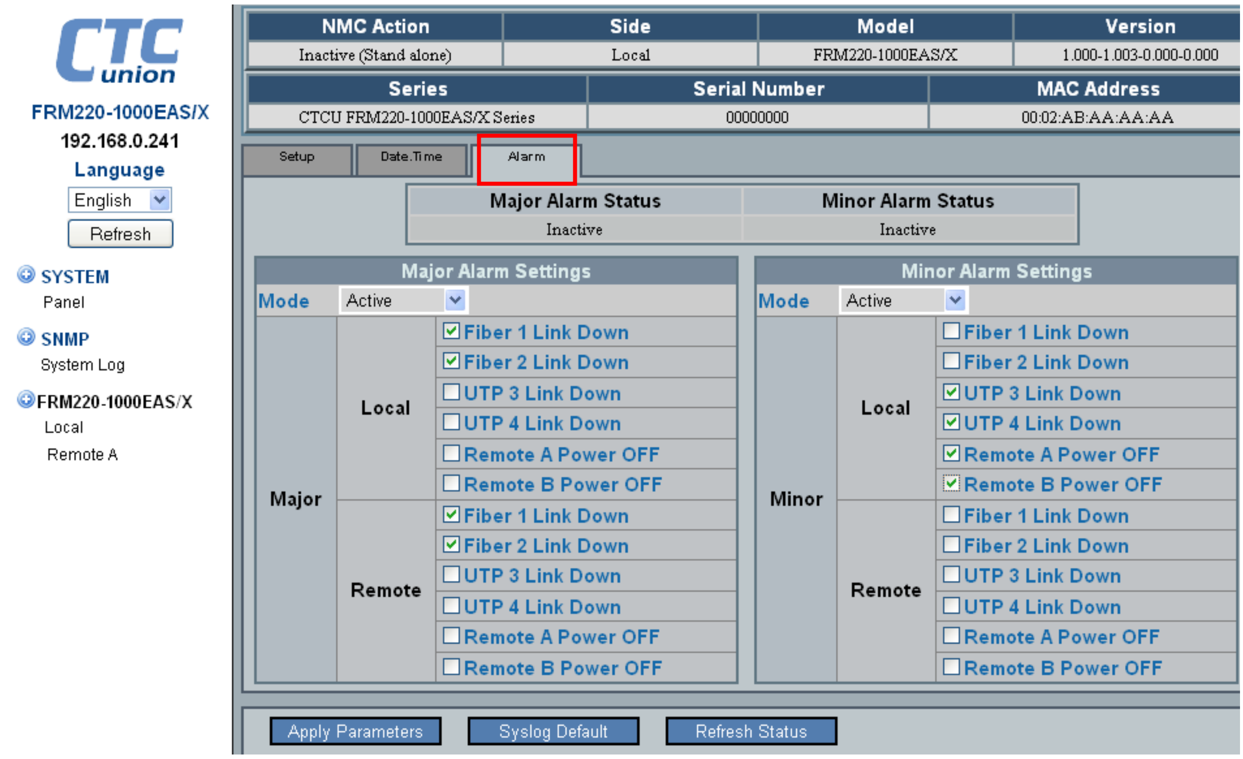
Time Server IP (NTP): 220.130.158.71

Time Zone (GMT): 00:00

Auto Adjust Time (1/Hr): Disable

4.3.6 Alarm Setting

The alarm settings here are used to generate SNMP traps for any of the Major and Minor conditions via simple to select 'check boxes'. In the example below, Major alarms are sent for Fiber link loss while Minor alarms are sent for UTP link loss or Remote power failure.



NMC Action	Side	Model	Version
Inactive (Stand alone)	Local	FRM220-1000EAS/X	1.000-1.003-0.000-0.000

Series	Serial Number	MAC Address
CTCU FRM220-1000EAS/X Series	00000000	00:02:AB:AA:AA:AA

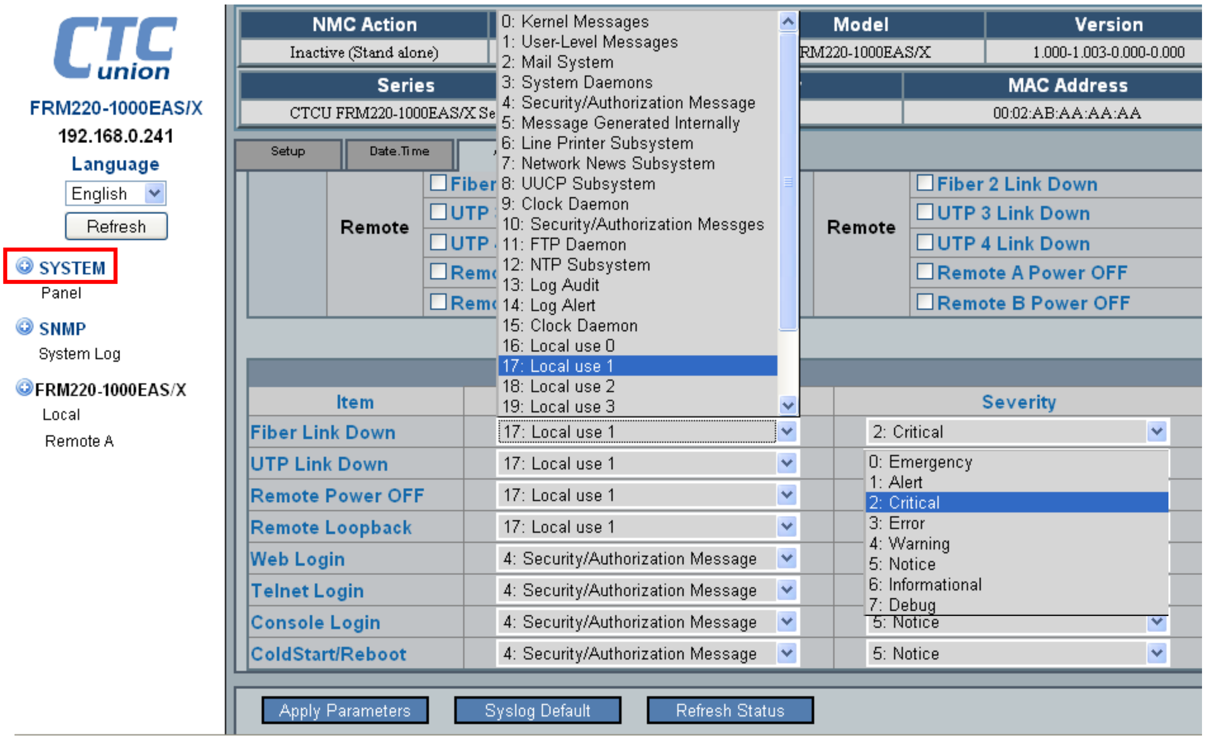
Major Alarm Status	Minor Alarm Status
Inactive	Inactive

Major Alarm Settings			Minor Alarm Settings		
Mode	Active		Mode	Active	
Major	Local	☑ Fiber 1 Link Down	Minor	Local	☐ Fiber 1 Link Down
		☑ Fiber 2 Link Down			☐ Fiber 2 Link Down
		☐ UTP 3 Link Down			☑ UTP 3 Link Down
		☐ UTP 4 Link Down			☑ UTP 4 Link Down
		☐ Remote A Power OFF			☑ Remote A Power OFF
		☐ Remote B Power OFF			☑ Remote B Power OFF
	Remote	☑ Fiber 1 Link Down		Remote	☐ Fiber 1 Link Down
		☑ Fiber 2 Link Down			☐ Fiber 2 Link Down
		☐ UTP 3 Link Down			☐ UTP 3 Link Down
		☐ UTP 4 Link Down			☐ UTP 4 Link Down
		☐ Remote A Power OFF			☐ Remote A Power OFF
		☐ Remote B Power OFF			☐ Remote B Power OFF

4.3.7 System Log Alarm Setting

Syslog, in **1000EAS/X**, can be used for security auditing (login) as well as generalized informational (link down), analysis, and debugging (loop back) messages. The syslog function of **1000EAS/X** can be used to integrate log data into a central repository.

Messages are assigned a priority/level (Emergency, Alert, Critical, Error, Warning, Notice, Info or Debug) by **1000EAS/X** and then sent to remote syslog server. Remote log server configuration is found in 4.4.2 Trap & Syslog.



NMC Action		Model	Version
Inactive (Stand alone)		RM220-1000EAS/X	1.000-1.003-0.000-0.000

Series		MAC Address
CTCU FRM220-1000EAS/X Se		00:02:AB:AA:AA:AA

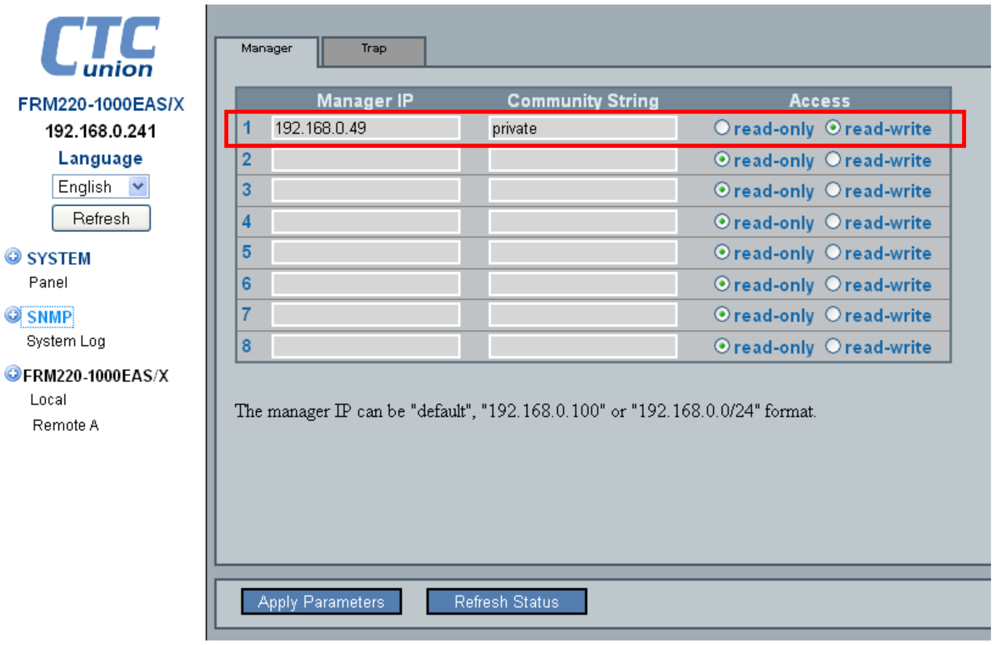
Item		Severity
Fiber Link Down	17: Local use 1	2: Critical
UTP Link Down	17: Local use 1	
Remote Power OFF	17: Local use 1	
Remote Loopback	17: Local use 1	
Web Login	4: Security/Authorization Message	
Telnet Login	4: Security/Authorization Message	
Console Login	4: Security/Authorization Message	5: Notice
ColdStart/Reboot	4: Security/Authorization Message	5: Notice

4.4 SNMP

The SNMP setting window is divided into two tabs, one for Manager Configuration and one for Trap Configuration.

4.4.1 Manager

By setting the manager's IP and community string in this window, authority is granted to the network manager. There are eight (8) locations for entering manager information.

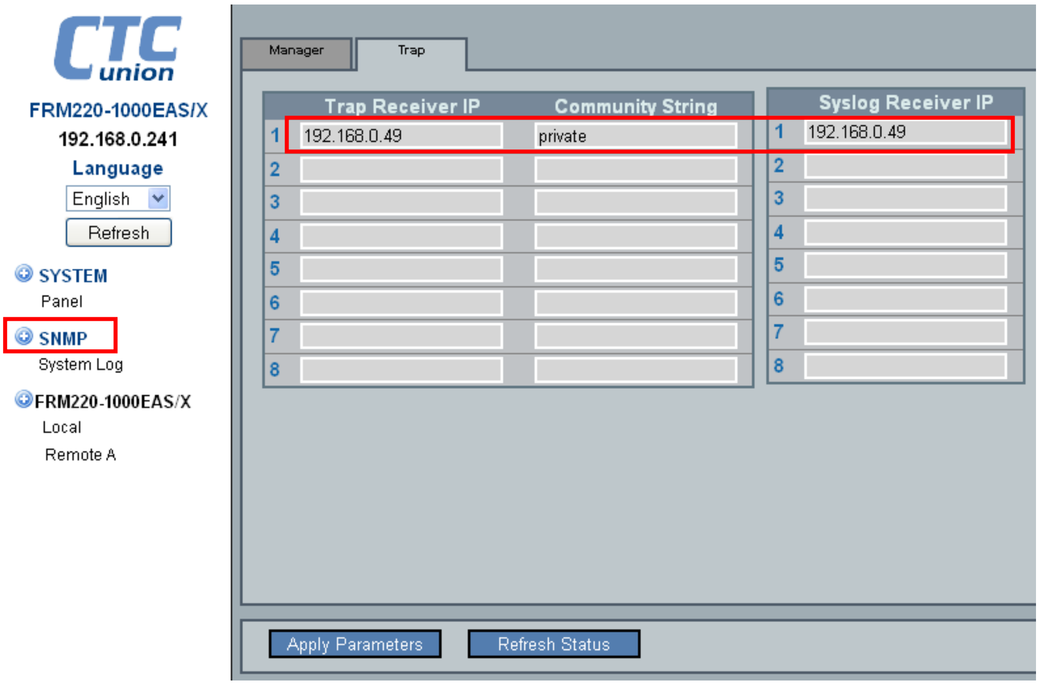


	Manager IP	Community String	Access
1	192.168.0.49	private	○ read-only ● read-write
2			● read-only ○ read-write
3			● read-only ○ read-write
4			● read-only ○ read-write
5			● read-only ○ read-write
6			● read-only ○ read-write
7			● read-only ○ read-write
8			● read-only ○ read-write

The manager IP can be "default", "192.168.0.100" or "192.168.0.0/24" format.

4.4.2 Trap & Syslog

Traps are unsolicited messages issued by the SNMP agent that typically indicate some alarm condition has occurred. The Trap managers (those who receive the traps) are configured here. System log messages are sent to a special syslog server. That server's IP address is also configured here. Syslog alarm settings are described in 4.3.7 System Log Alarm Setting.



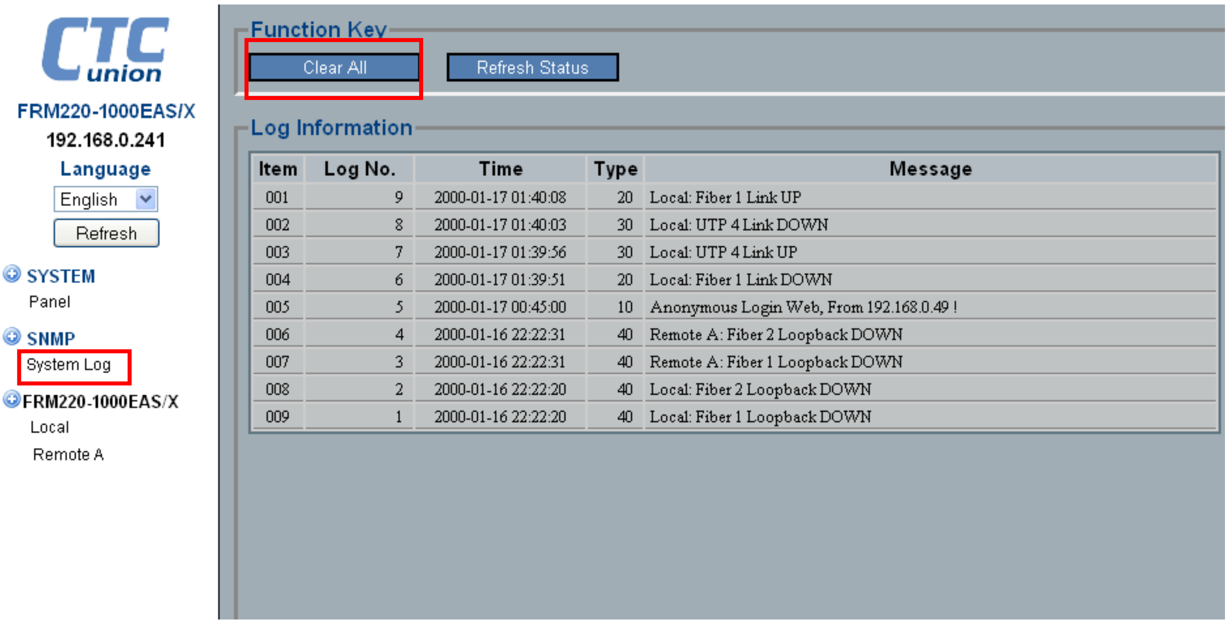
	Trap Receiver IP	Community String
1	192.168.0.49	private
2		
3		
4		
5		
6		
7		
8		

	Syslog Receiver IP
1	192.168.0.49
2	
3	
4	
5	
6	
7	
8	

SNMP manager at 192.168.0.49 receives traps with community 'secret'.

4.4.3 System Log

During the current up time of **1000EAS/X** converter, an internal log is maintained and can be viewed through the web interface. This is a first-in first-out log that holds up to 255 entries. The log will display information such as user logins from Web or from Telnet and any of the Major and Minor alarms as programmed in the alarm setting page (refer to 4.3.6 Alarm Setting).



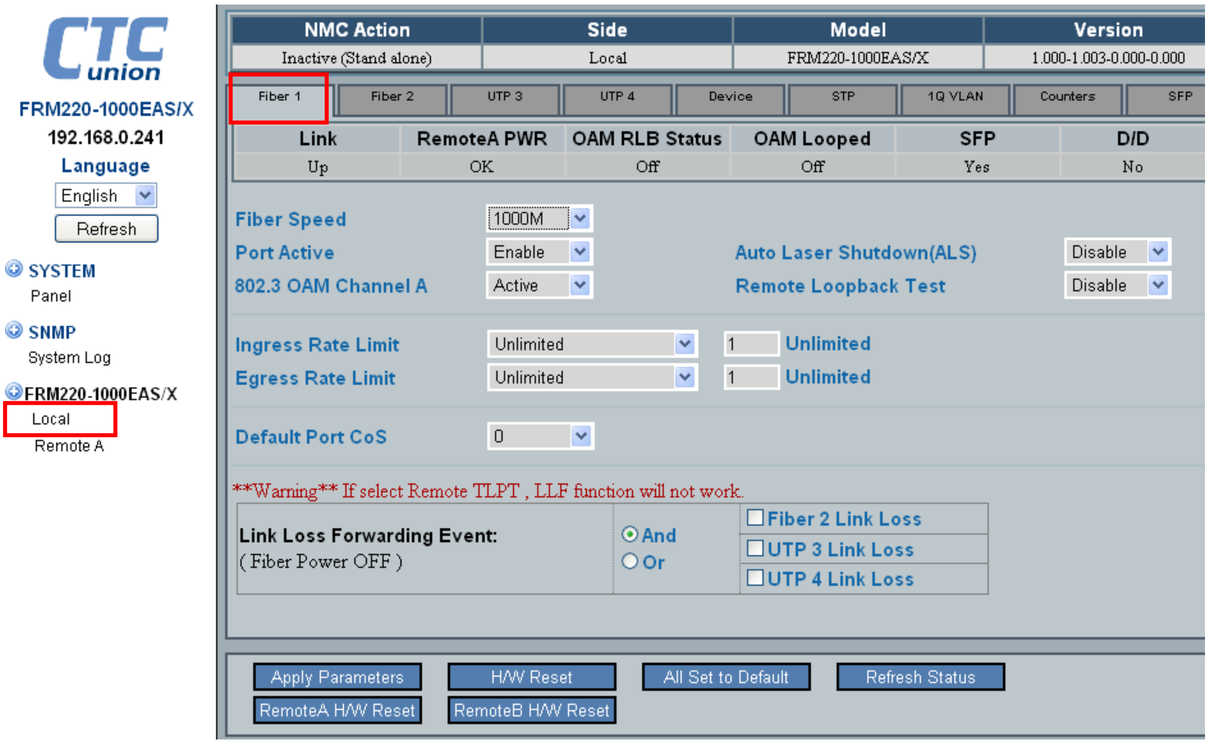
Item	Log No.	Time	Type	Message
001	9	2000-01-17 01:40:08	20	Local: Fiber 1 Link UP
002	8	2000-01-17 01:40:03	30	Local: UTP 4 Link DOWN
003	7	2000-01-17 01:39:56	30	Local: UTP 4 Link UP
004	6	2000-01-17 01:39:51	20	Local: Fiber 1 Link DOWN
005	5	2000-01-17 00:45:00	10	Anonymous Login Web, From 192.168.0.49 !
006	4	2000-01-16 22:22:31	40	Remote A: Fiber 2 Loopback DOWN
007	3	2000-01-16 22:22:31	40	Remote A: Fiber 1 Loopback DOWN
008	2	2000-01-16 22:22:20	40	Local: Fiber 2 Loopback DOWN
009	1	2000-01-16 22:22:20	40	Local: Fiber 1 Loopback DOWN

The "Clear All" button can be used to clear out all the log entries.

4.5 Local Unit Configuration

4.5.1 Fiber 1

This window tab will show current status and provide settings for the first fiber port.



NMC Action	Side	Model	Version
Inactive (Stand alone)	Local	FRM220-1000EAS/X	1.000-1.003-0.000-0.000

Link	RemoteA PWR	OAM RLB Status	OAM Looped	SFP	D/D
Up	OK	Off	Off	Yes	No

Fiber Speed: 1000M

Port Active: Enable

802.3 OAM Channel A: Active

Auto Laser Shutdown(ALS): Disable

Remote Loopback Test: Disable

Ingress Rate Limit: Unlimited 1 Unlimited

Egress Rate Limit: Unlimited 1 Unlimited

Default Port CoS: 0

Warning If select Remote TLPT , LLF function will not work.

Link Loss Forwarding Event:
(Fiber Power OFF)

● And
○ Or

□ Fiber 2 Link Loss
□ UTP 3 Link Loss
□ UTP 4 Link Loss

Parameters

Fiber Speed : **1000EAS/X** supports selection of fiber speed for 100Base-FX or 1000Base-Sx/Lx. Be sure to use the appropriate SFP module that supports the selected data rate.
Port Active : When disabled, this port will be completely inactive.
802.3 OAM Channel A : Active, Passive or disable. Refer to Chapter 3 3.7 OAM Configuration
Auto Laser Shutdown : This laser safety function which when enabled will disable laser transmit when a optical receive loss condition is detected.
Remote Loopback Test : This will enable the OAM based loop back. RLB status will be shown above.
IRL : Select the granularity of 64K, 1M or 100M and place the multiplier value to its right.
ERL : Select the granularity of 64K, 1M or 100M and place the multiplier value to its right.
Default Port CoS : The default Class of Service for this port is set here and explained in 3.6.9 Class of Service
LLF : Setting LLF uses and/or logic and check box selection of each port. LLF cannot be used if TLPT is enabled. Refer to 3.8 Link Loss Forwarding.

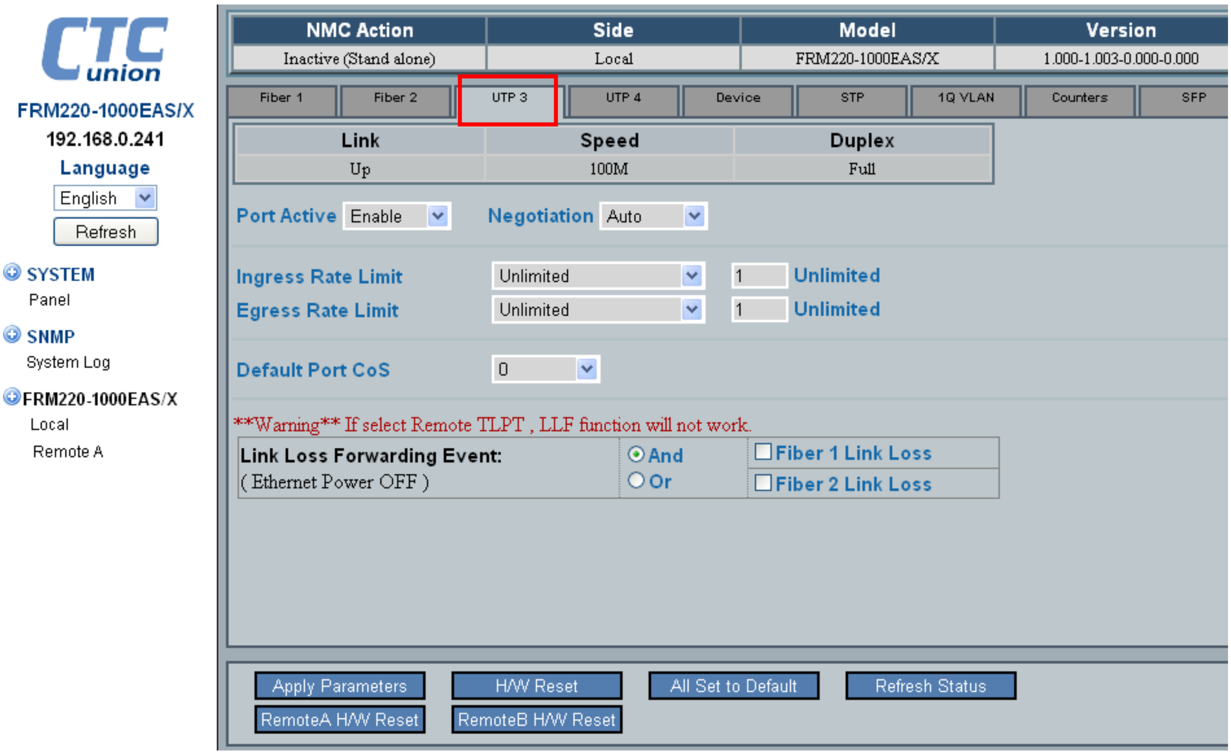
Buttons

Apply Parameters : Until this button is pressed, no changes are actually performed.
H/W Reset : This will reboot the CPU and reset the switch chip. Use with caution as traffic is blocked during a reset operation until the OS has booted and switch chip re-initialized.
All Set to Default : Very simply, the device is reset to factory default settings.
Refresh Status : Updates the display with current information.
Remote H/W Reset : Provides ability to reset device at remote A or B, if the device is configured to so allow.

The setting methods for Fiber 2 are identical to that of Fiber 1.

4.5.2 UTP 3

This window tab will show current status and provide settings for the first UTP port.



NMC Action	Side	Model	Version
Inactive (Stand alone)	Local	FRM220-1000EAS/X	1.000-1.003-0.000-0.000

Link	Speed	Duplex
Up	100M	Full

Port Active: Enable Negotiation: Auto

Ingress Rate Limit: Unlimited 1 Unlimited

Egress Rate Limit: Unlimited 1 Unlimited

Default Port CoS: 0

Warning If select Remote TLPT , LLF function will not work.

Link Loss Forwarding Event: (Ethernet Power OFF)	● And ○ Or	☐ Fiber 1 Link Loss ☐ Fiber 2 Link Loss

Parameters

Port Active : When disabled, this port will be completely inactive.

Negotiation : This sets up the UTP port for either auto-negotiation per 802.3u or sets manual configuration mode.

IRL : Select the granularity of 64K, 1M or 100M and place the multiplier value to its right.

ERL : Select the granularity of 64K, 1M or 100M and place the multiplier value to its right.

Default Port CoS : The default Class of Service for this port is set here and explained in 3.6.9 Class of Service

LLF : Setting LLF uses and/or logic and check box selection of each port. LLF cannot be used if TLPT is enabled. Refer to section 3.8.

Buttons

Apply Parameters : Until this button is pressed, no changes are actually performed.

H/W Reset : This will reboot the CPU and reset the switch chip. Use with caution as traffic is blocked during a reset operation until the OS has booted and switch chip re-initialized.

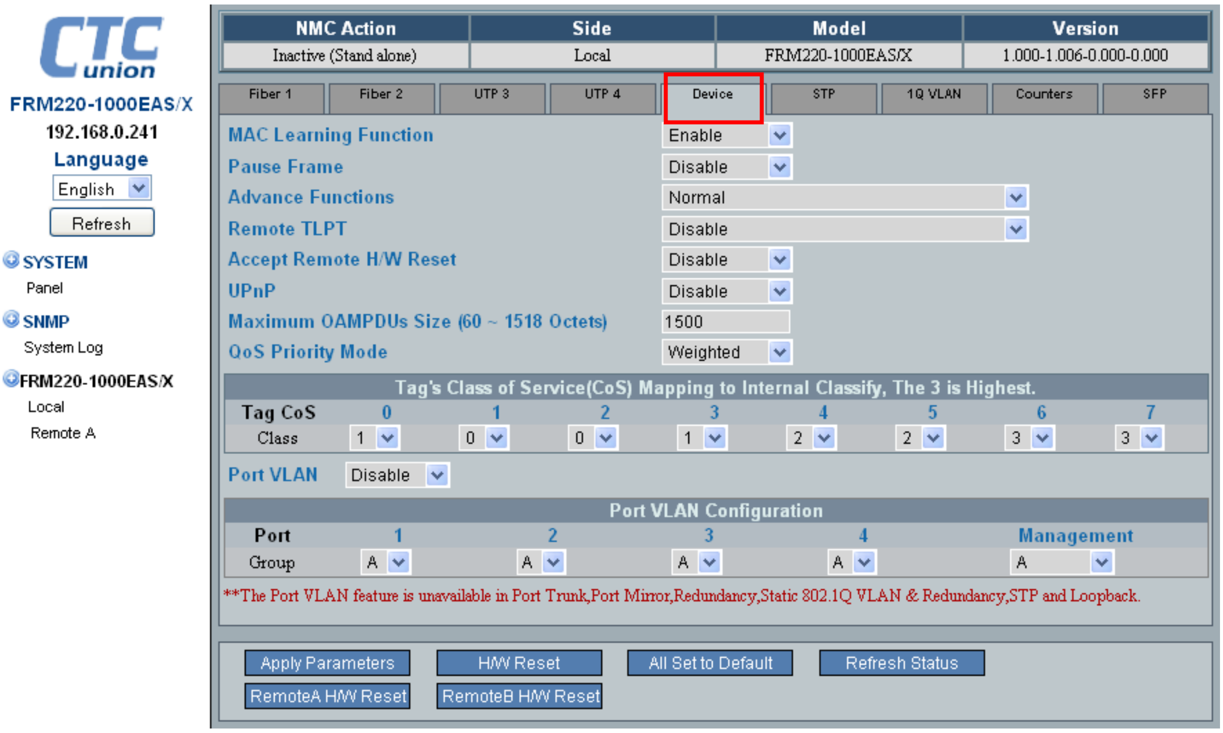
All Set to Default : Very simply, the device is reset to factory default settings.

Refresh Status : Updates the display with current information.

Remote H/W Reset : Provides ability to reset device at remote A or B, if the device is configured to so allow.

The setting methods for UTP 4 are identical to that of UTP 3.

4.5.3 Device Status and Configuration



NMC Action	Side	Model	Version
Inactive (Stand alone)	Local	FRM220-1000EAS/X	1.000-1.006-0.000-0.000

MAC Learning Function	Enable
Pause Frame	Disable
Advance Functions	Normal
Remote TLPT	Disable
Accept Remote H/W Reset	Disable
UPnP	Disable
Maximum OAMPDUs Size (60 ~ 1518 Octets)	1500
QoS Priority Mode	Weighted

Tag's Class of Service(CoS) Mapping to Internal Classify, The 3 is Highest.

Tag CoS	0	1	2	3	4	5	6	7
Class	1	0	0	1	2	2	3	3

Port VLAN: Disable

Port VLAN Configuration

Port	1	2	3	4	Management
Group	A	A	A	A	A

**The Port VLAN feature is unavailable in Port Trunk,Port Mirror,Redundancy,Static 802.1Q VLAN & Redundancy,STP and Loopback.

MAC Learning : **1000EAS/X** supports disabling MAC learning. The default is enabled.
Pause Frame : **1000EAS/X** supports 802.3X. The default is disabled.

The 'Advanced Functions' for this device are detailed in Chapter 3, 3.6 Advanced Functions.

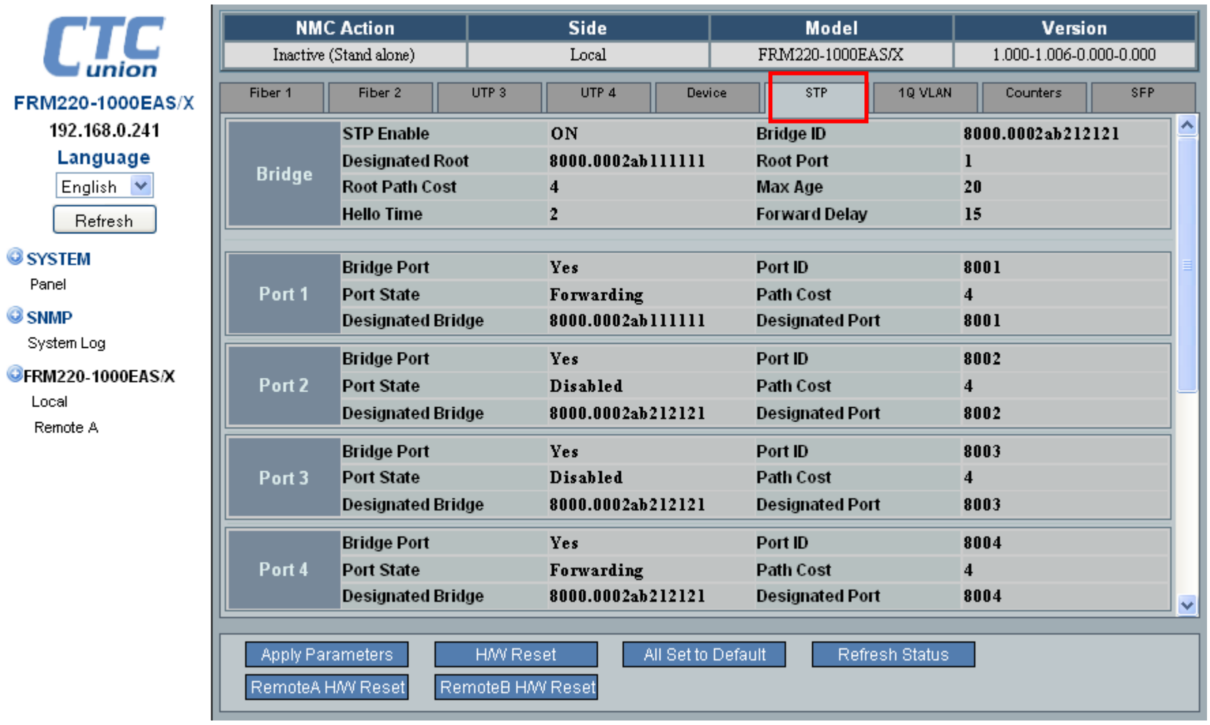
Remote TLPT : **1000EAS/X** supports transparent link pass through. See 3.9 Remote Transparent Link Pass Through (TLPT).
Accept Remote H/W Reset : When enabled, this device will reset when the request is received from the remotely connected **1000EAS/X**.
UPnP : **1000EAS/X** may enable the Universal Plug 'n Play protocol to allow IP discovery via this protocol. The default is disabled.
Maximum OAMPDU Size : The PDU size may be set on the OAM active unit. The default and recommended size is 1500 bytes.
QoS Priority Mode : **1000EAS/X** supports either weighted or strict QoS setting. The default is weighted.

Refer to 3.6.9 Class of Service for explanation of CoS settings.

Buttons
Apply Parameters : Until this button is pressed, no changes are actually performed.
H/W Reset : This will reboot the CPU and reset the switch chip. Use with caution as traffic is blocked during a reset operation until the OS has booted and switch chip re-initialized.
All Set to Default : Very simply, the device is reset to factory default settings.
Refresh Status : Updates the display with current information.
Remote H/W Reset : Provides ability to reset device at remote A or B, if the device is configured to so allow.

4.5.4 Spanning Tree Protocol

The Spanning Tree Protocol (STP) is a link layer (OSI Layer 2) network protocol that ensures a loop-free topology for any bridged LAN. The basic function of STP is to prevent bridge loops and ensuing broadcast radiation.



NMC Action	Side	Model	Version
Inactive (Stand alone)	Local	FRM220-1000EAS/X	1.000-1.006-0.000-0.000

Bridge	STP Enable	ON	Bridge ID	8000.0002ab212121
	Designated Root	8000.0002ab111111	Root Port	1
	Root Path Cost	4	Max Age	20
	Hello Time	2	Forward Delay	15
Port 1	Bridge Port	Yes	Port ID	8001
	Port State	Forwarding	Path Cost	4
	Designated Bridge	8000.0002ab111111	Designated Port	8001
Port 2	Bridge Port	Yes	Port ID	8002
	Port State	Disabled	Path Cost	4
	Designated Bridge	8000.0002ab212121	Designated Port	8002
Port 3	Bridge Port	Yes	Port ID	8003
	Port State	Disabled	Path Cost	4
	Designated Bridge	8000.0002ab212121	Designated Port	8003
Port 4	Bridge Port	Yes	Port ID	8004
	Port State	Forwarding	Path Cost	4
	Designated Bridge	8000.0002ab212121	Designated Port	8004

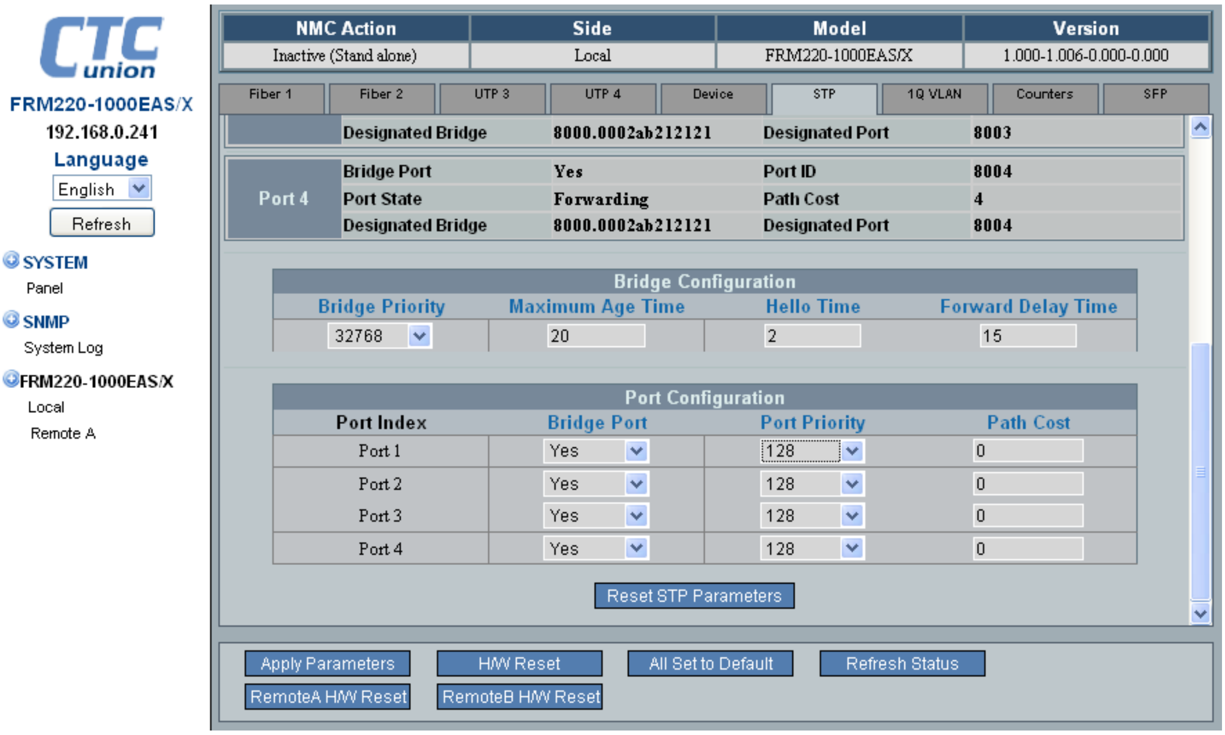
The root bridge of the spanning tree is the bridge with the lowest bridge ID. Each bridge has a unique identifier (ID) and a configurable priority number; the **Bridge ID** contains both numbers. To compare two bridge IDs, the priority is compared first. If two bridges have equal priority, then the MAC addresses are compared. For example, if switches A (MAC=0002ab111111) and B (MAC=0002ab212121) both have a priority of 8000, then switch A will be selected as the root bridge (it has the lower value MAC address). If the network administrators would like switch B to become the root bridge, they must set its priority to be less than 8000.

Spanning tree computes its path by following the path of least cost, i.e., a path from the device to the root that has minimum cost among all paths from the device to the root. The cost of traversing a path is the sum of the costs of the segments on the path. The port connecting to that path becomes the root port (RP) of the bridge. Different technologies have different default costs for network segments. For example, in the above capture the ‘Path Cost’s are shown with the value “4” which indicates a GbE port. In this manner, a 100M port would have a default port cost of “19”, while a 10M port would have a cost of “100”. An administrator can configure the cost of traversing a particular network segment.

The switch sends **BPDU** (Bridge Protocol Data Units) frames using a unique MAC destination address for STP multicast, 01:80:C2:00:00:00 and with port’s MAC itself as a source address.

There are three types of BPDUs:

1. Configuration BPDU (CBPDU), used for Spanning Tree computation
2. Topology Change Notification (TCN) BPDU, used to announce changes in the network topology
3. Topology Change Notification Acknowledgment (TCA), used to acknowledge changes



NMC Action	Side	Model	Version
Inactive (Stand alone)	Local	FRM220-1000EAS/X	1.000-1.006-0.000-0.000

	Designated Bridge	8000.0002ab212121	Designated Port	8003
Port 4	Bridge Port	Yes	Port ID	8004
	Port State	Forwarding	Path Cost	4
	Designated Bridge	8000.0002ab212121	Designated Port	8004

Bridge Configuration

Bridge Priority	Maximum Age Time	Hello Time	Forward Delay Time
32768	20	2	15

Port Configuration

Port Index	Bridge Port	Port Priority	Path Cost
Port 1	Yes	128	0
Port 2	Yes	128	0
Port 3	Yes	128	0
Port 4	Yes	128	0

The **Bridge Priority** is a customizable value that you can use to influence which switch becomes the root bridge. The switch with the lowest priority, which means lowest BID, becomes the root bridge (the lower the priority value, the higher the priority). The default value for the priority is 32768 (0x8000). The priority range is between 1 and 65536 (0x0001 to 0xFFFF); with 1 as the highest priority.

Maximum Age Time, referred to by the switch as **Max Age**, is the amount of time a switch will retain a BPDU's contents before discarding it. The default is 20 seconds. It also influences the bridge table aging timer during the Topology Change Notification process.

Hello Time is the time interval (number of seconds between) at which the root bridge transmits configuration BPDUs.

When a device is first attached to a switch port, it will not immediately start to forward data. It will instead go through a number of states while it processes BPDUs and determines the topology of the network. The time spent in the listening and learning states is determined by a value known as the **Forward Delay** (default 15 seconds and set by the root bridge).

These timers should not be changed lightly. If you decide to change any or all of these timers, the change must be configured on the root bridge! The root bridge will inform the non-root switches of the change via BPDUs.

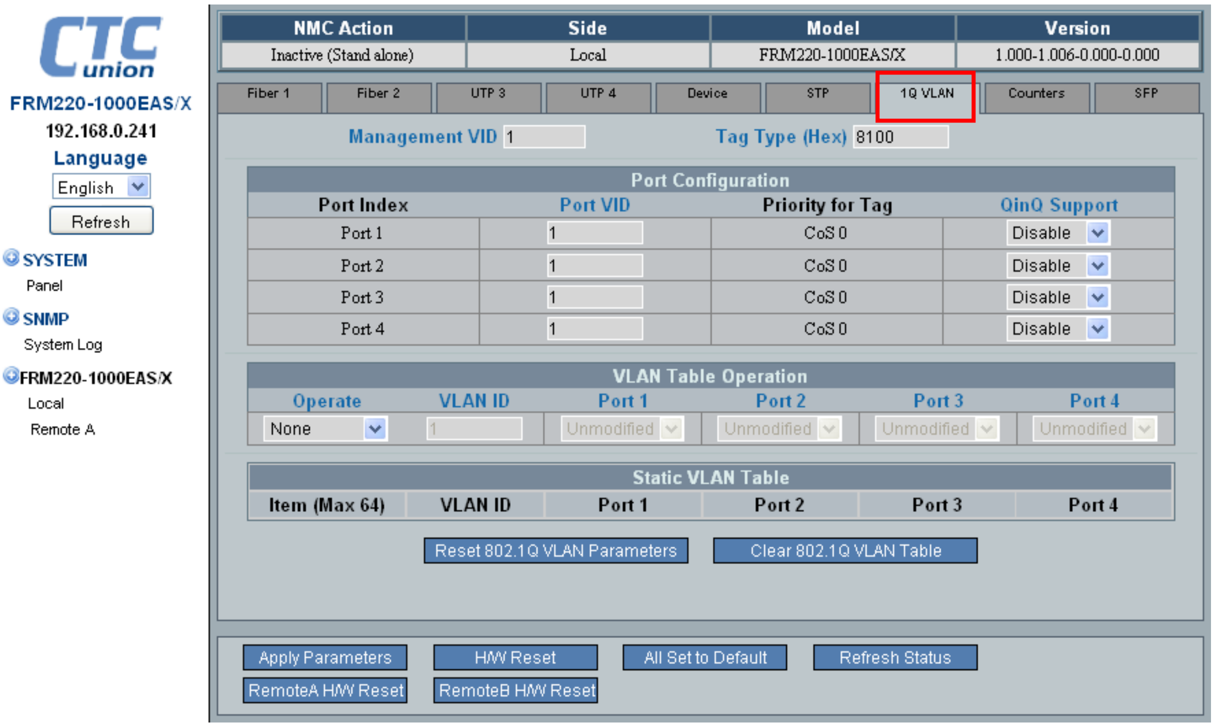
Within a bridge (switch) there will also be multiple ports (interfaces) that can be additionally assigned priority within the bridge (switch). By default, the lowest port number will have the highest priority. In the case of **1000EAS/X**, that would be the first fiber port, port 1. The ports may change assigned priority under the **Port Priority** pull-down for each port. The Port Priority plus the port number are combined to give the **Port ID**. For example, Port Priority of 128 (0x80) plus the port number (first fiber port 1 = 01) will give a Port ID of **8001**. Port Priority can be set and the results of the Port ID follow according to this conversion table:

Dec	0	16	32	48	64	80	96	112	128	144	160	176	192	208	224	240
Hex	00	10	20	30	40	50	60	70	80	90	A0	B0	C0	D0	E0	F0

The default port **Path Cost** in **1000EAS/X** is set at 0 (auto) and can be set in a valid range up to 200,000,000.

4.5.5 Static 802.1Q VLAN

Please refer to Chapter 3, 3.6.4 Static 802.1Q VLAN for a description of and operation of Static VLAN feature in this device and to 3.6.9 Class of Service for Class of Service settings.



NMC Action	Side	Model	Version
Inactive (Stand alone)	Local	FRM220-1000EAS/X	1.000-1.006-0.000-0.000

Management VID 1   Tag Type (Hex) 8100

Port Configuration

Port Index	Port VID	Priority for Tag	QinQ Support
Port 1	1	CoS 0	Disable
Port 2	1	CoS 0	Disable
Port 3	1	CoS 0	Disable
Port 4	1	CoS 0	Disable

VLAN Table Operation

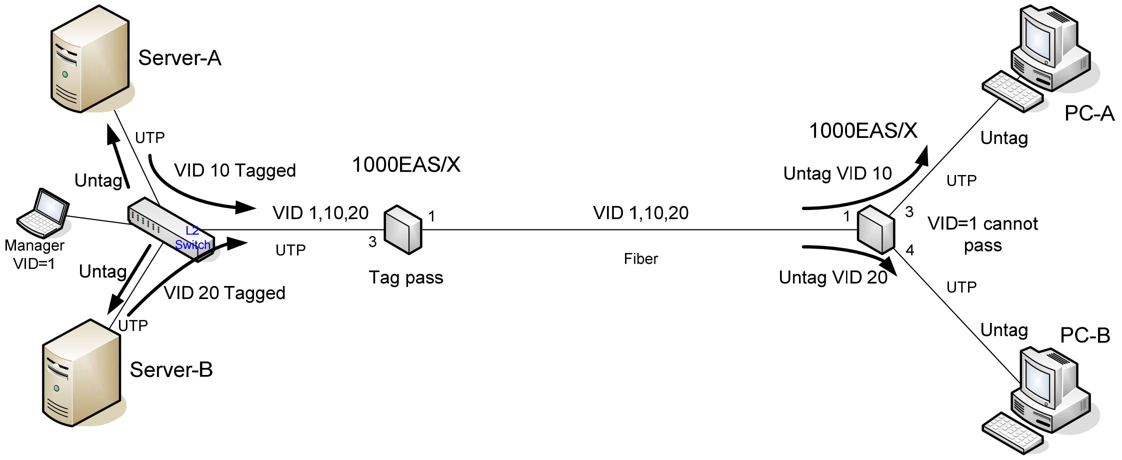
Operate	VLAN ID	Port 1	Port 2	Port 3	Port 4
None	1	Unmodified	Unmodified	Unmodified	Unmodified

Static VLAN Table

Item (Max 64)	VLAN ID	Port 1	Port 2	Port 3	Port 4

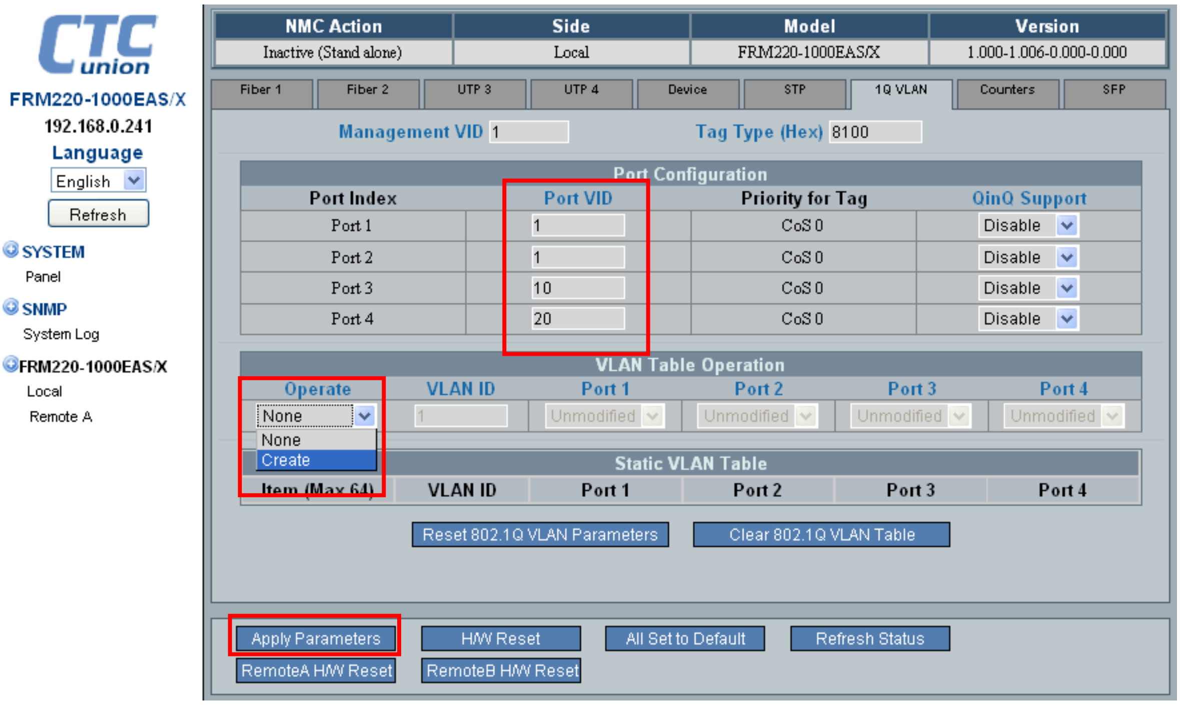
Static VLAN Example

This static VLAN application was used in Chapter 3, 3.6.4 Static 802.1Q VLAN. Here we will use the web based interface to do the settings rather than the Telnet menu system. This should help the end user to better understand the setting methodology using the friendlier web interface.



Connect to **1000EAS/X** via web browser and select the Remote A device for management. Click the 1Q VLAN tab.

Step 1. Setup the VID for 1, 10, and 20 for the fiber and two UTP ports. Then, from the 'Operate' pull-down, select 'Create' and one by one setup the VID1, VID10 and VID20 static VLANs.



NMC Action	Side	Model	Version
Inactive (Stand alone)	Local	FRM220-1000EAS/X	1.000-1.006-0.000-0.000

Management VID 1 Tag Type (Hex) 8100

Port Configuration

Port Index	Port VID	Priority for Tag	QinQ Support
Port 1	1	CoS 0	Disable
Port 2	1	CoS 0	Disable
Port 3	10	CoS 0	Disable
Port 4	20	CoS 0	Disable

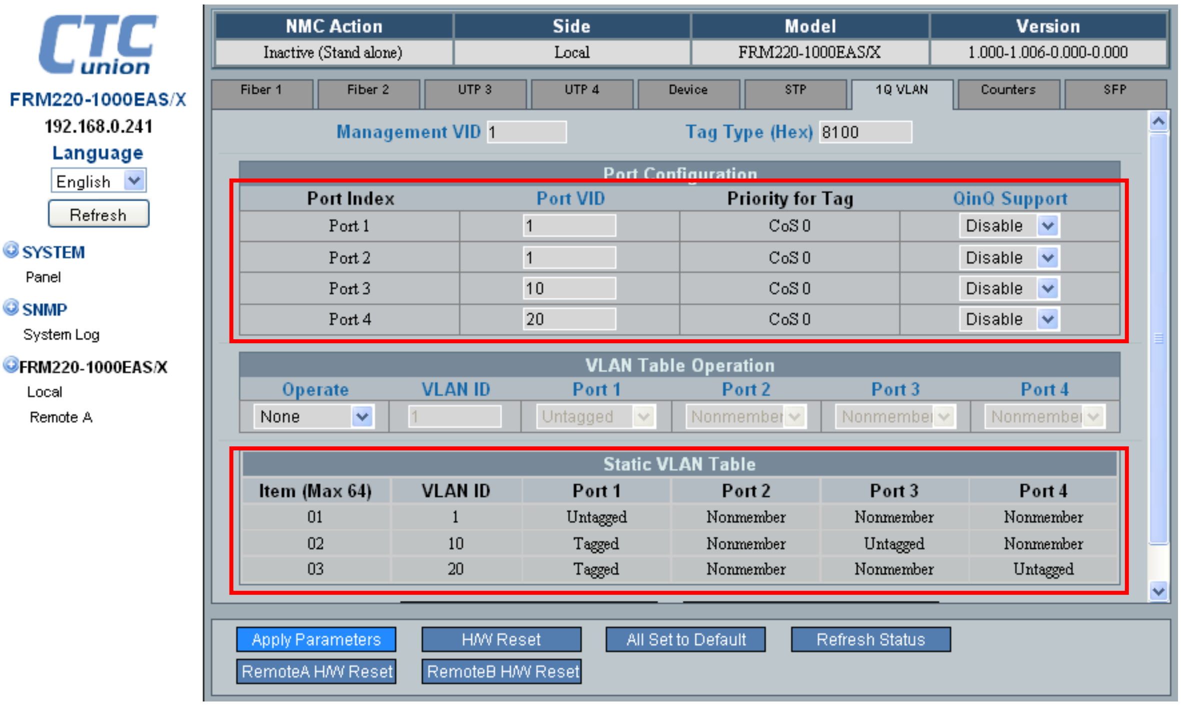
VLAN Table Operation

Operate	VLAN ID	Port 1	Port 2	Port 3	Port 4
None None Create	1	Unmodified	Unmodified	Unmodified	Unmodified

Static VLAN Table

Item (Max 64)	VLAN ID	Port 1	Port 2	Port 3	Port 4

Step 2. For each created VID click 'Apply Parameters'. When finished, the screen will look like the following.



NMC Action	Side	Model	Version
Inactive (Stand alone)	Local	FRM220-1000EAS/X	1.000-1.006-0.000-0.000

Management VID 1 Tag Type (Hex) 8100

Port Configuration

Port Index	Port VID	Priority for Tag	QinQ Support
Port 1	1	CoS 0	Disable
Port 2	1	CoS 0	Disable
Port 3	10	CoS 0	Disable
Port 4	20	CoS 0	Disable

VLAN Table Operation

Operate	VLAN ID	Port 1	Port 2	Port 3	Port 4
None	1	Untagged	Nonmember	Nonmember	Nonmember

Static VLAN Table

Item (Max 64)	VLAN ID	Port 1	Port 2	Port 3	Port 4
01	1	Untagged	Nonmember	Nonmember	Nonmember
02	10	Tagged	Nonmember	Untagged	Nonmember
03	20	Tagged	Nonmember	Nonmember	Untagged

Some Tagging definitions:

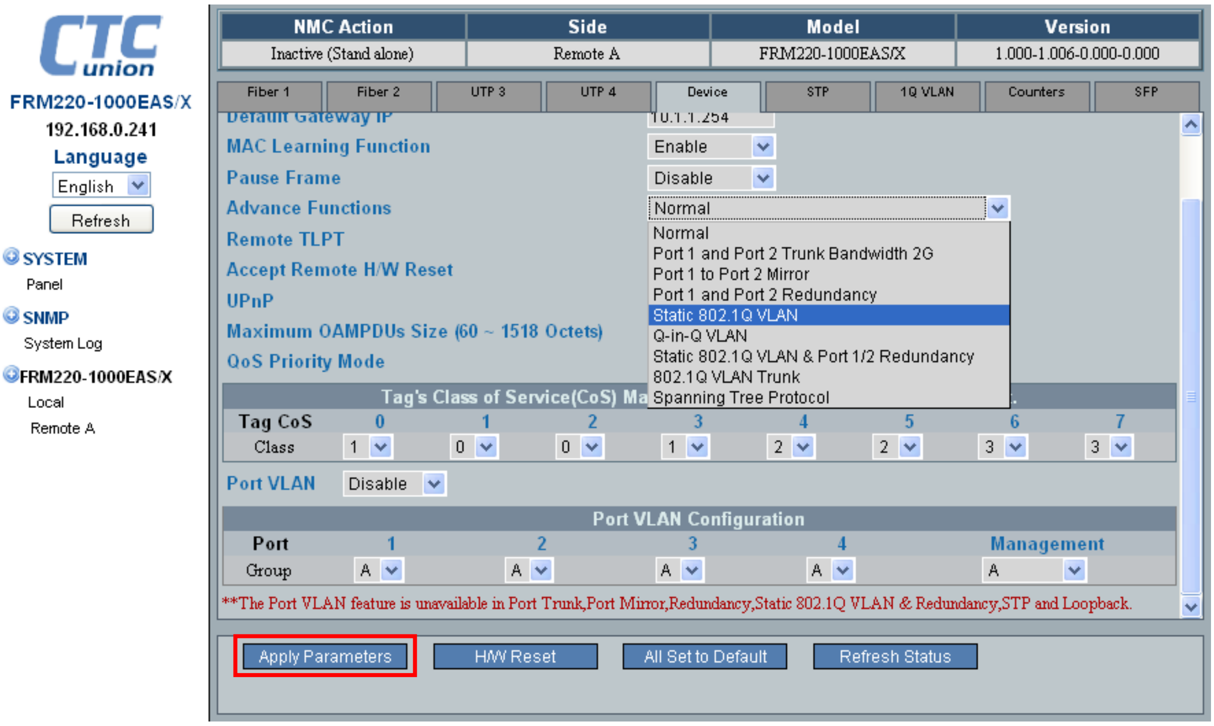
Tagged: This means that packets that egress the assigned port will have the packets tagged with the VID assigned to that port.

Untagged: This means that any packets that egress the assigned port will have all tag information removed.

Non-member: When a port is not a member of a VID, packets tagged with that VID will not be allowed to egress that port. (i.e. they will be dropped)

Unmodified: This means that packets exiting the assigned port will still have the same tag as when they entered any other port of the switch, i.e., unmodified

Step 3. Under the Device, Advanced Functions, enable the Static 802.1Q VLAN from the pull-down. Click 'Apply Parameters'.



NMC Action	Side	Model	Version
Inactive (Stand alone)	Remote A	FRM220-1000EAS/X	1.000-1.006-0.000-0.000

Default Gateway IP	10.1.1.254
MAC Learning Function	Enable
Pause Frame	Disable
Advance Functions	Normal
Remote TLPT	
Accept Remote H/W Reset	
UPnP	
Maximum OAMPDUs Size (60 ~ 1518 Octets)	
QoS Priority Mode	

Advance Functions pull-down:
- Normal
- Port 1 and Port 2 Trunk Bandwidth 2G
- Port 1 to Port 2 Mirror
- Port 1 and Port 2 Redundancy
- Static 802.1Q VLAN
- Q-in-Q VLAN
- Static 802.1Q VLAN & Port 1/2 Redundancy
- 802.1Q VLAN Trunk
- Spanning Tree Protocol

Tag's Class of Service(CoS) Ma

Tag CoS	0	1	2	3	4	5	6	7
Class	1	0	0	1	2	2	3	3

Port VLAN: Disable

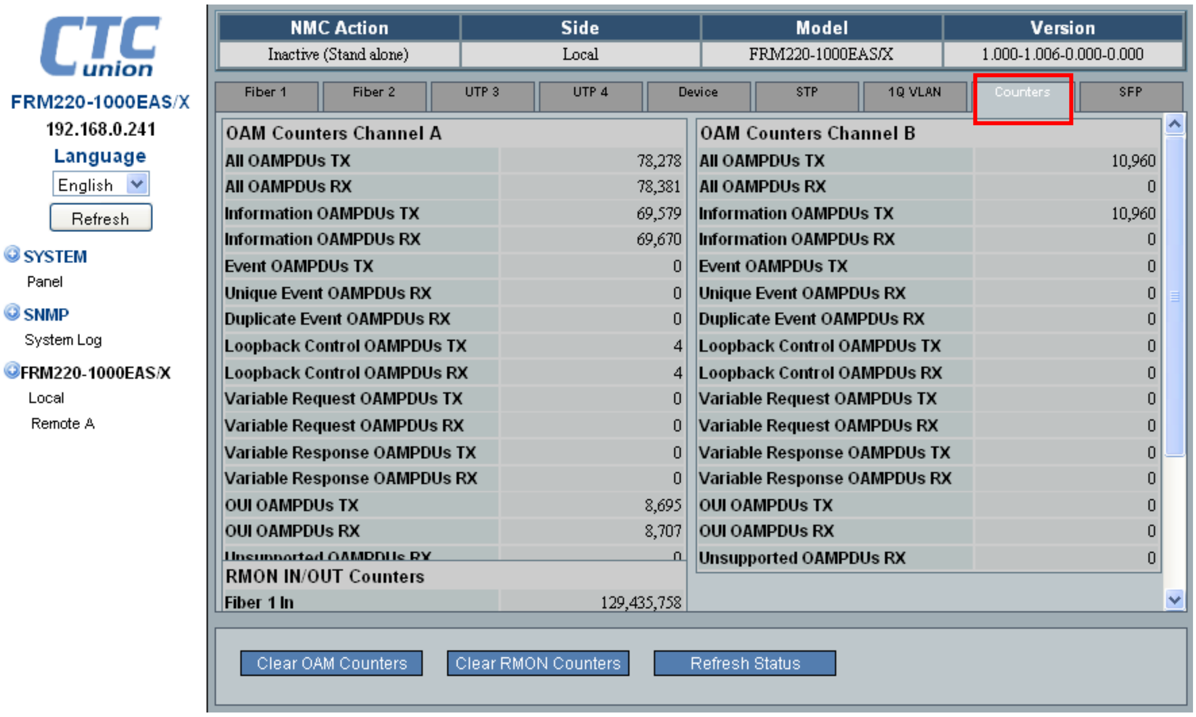
Port VLAN Configuration

Port	1	2	3	4	Management
Group	A	A	A	A	A

**The Port VLAN feature is unavailable in Port Trunk,Port Mirror,Redundancy,Static 802.1Q VLAN & Redundancy,STP and Loopback.

4.5.6 Counters

There are counters for OAM packets and counters for transmitted and received frames. They can be viewed under the 'Counter' screen.

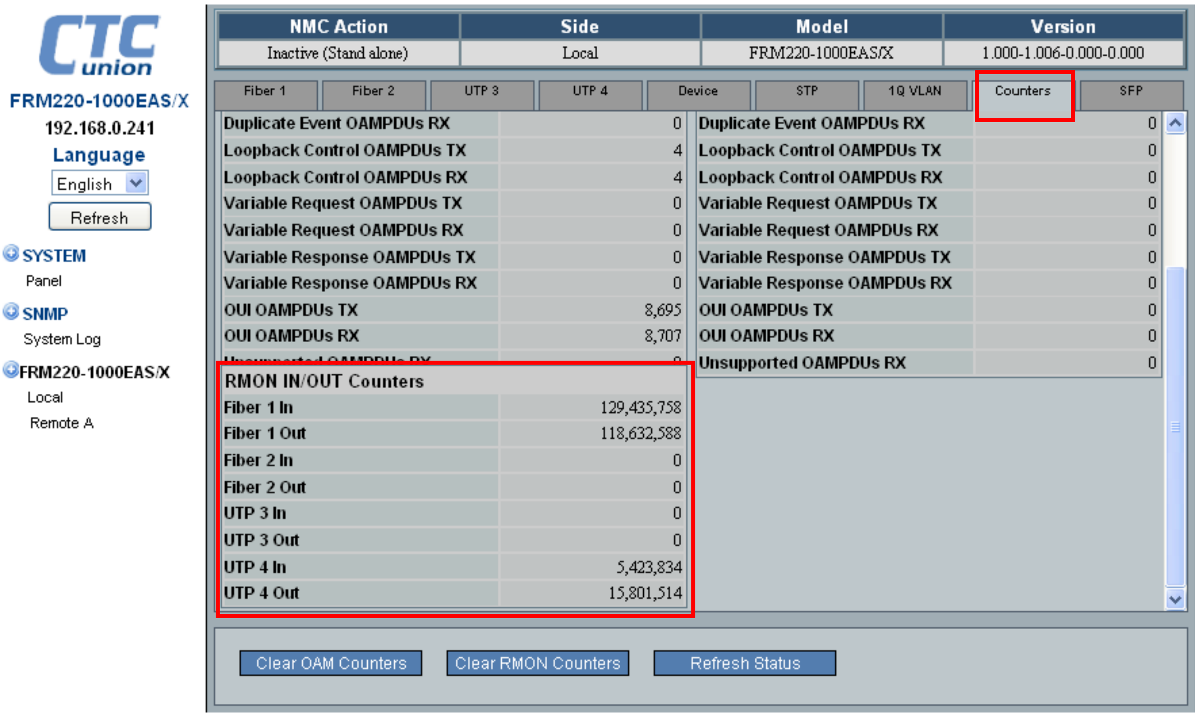


NMC Action	Side	Model	Version
Inactive (Stand alone)	Local	FRM220-1000EAS/X	1.000-1.006-0.000-0.000

OAM Counters Channel A		OAM Counters Channel B	
All OAMPDUs TX	78,278	All OAMPDUs TX	10,960
All OAMPDUs RX	78,381	All OAMPDUs RX	0
Information OAMPDUs TX	69,579	Information OAMPDUs TX	10,960
Information OAMPDUs RX	69,670	Information OAMPDUs RX	0
Event OAMPDUs TX	0	Event OAMPDUs TX	0
Unique Event OAMPDUs RX	0	Unique Event OAMPDUs RX	0
Duplicate Event OAMPDUs RX	0	Duplicate Event OAMPDUs RX	0
Loopback Control OAMPDUs TX	4	Loopback Control OAMPDUs TX	0
Loopback Control OAMPDUs RX	4	Loopback Control OAMPDUs RX	0
Variable Request OAMPDUs TX	0	Variable Request OAMPDUs TX	0
Variable Request OAMPDUs RX	0	Variable Request OAMPDUs RX	0
Variable Response OAMPDUs TX	0	Variable Response OAMPDUs TX	0
Variable Response OAMPDUs RX	0	Variable Response OAMPDUs RX	0
OUI OAMPDUs TX	8,695	OUI OAMPDUs TX	0
OUI OAMPDUs RX	8,707	OUI OAMPDUs RX	0
Unsupported OAMPDUs RX	0	Unsupported OAMPDUs RX	0

RMON IN/OUT Counters	
Fiber 1 In	129,435,758

The OAM counters are available for each fiber port. In this example the Fiber 2 channel is not connected, so there are no received PDUs.



NMC Action	Side	Model	Version
Inactive (Stand alone)	Local	FRM220-1000EAS/X	1.000-1.006-0.000-0.000

Duplicate Event OAMPDUs RX	0	Duplicate Event OAMPDUs RX	0
Loopback Control OAMPDUs TX	4	Loopback Control OAMPDUs TX	0
Loopback Control OAMPDUs RX	4	Loopback Control OAMPDUs RX	0
Variable Request OAMPDUs TX	0	Variable Request OAMPDUs TX	0
Variable Request OAMPDUs RX	0	Variable Request OAMPDUs RX	0
Variable Response OAMPDUs TX	0	Variable Response OAMPDUs TX	0
Variable Response OAMPDUs RX	0	Variable Response OAMPDUs RX	0
OUI OAMPDUs TX	8,695	OUI OAMPDUs TX	0
OUI OAMPDUs RX	8,707	OUI OAMPDUs RX	0
Unsupported OAMPDUs RX	0	Unsupported OAMPDUs RX	0

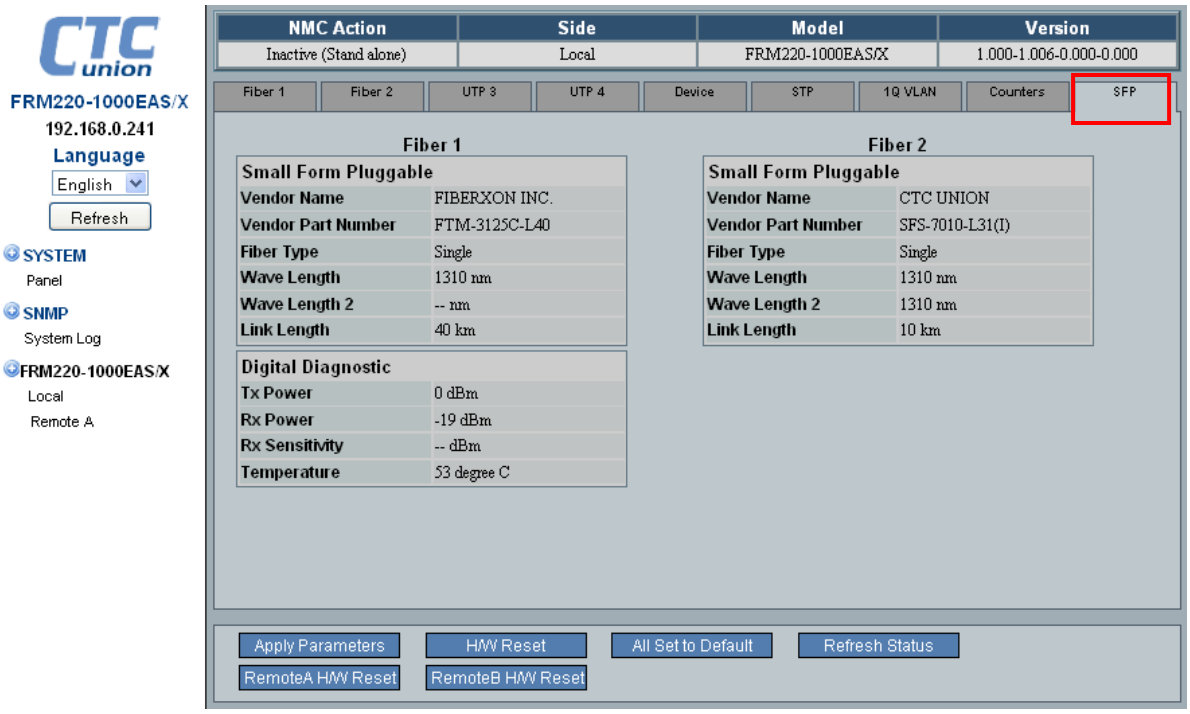
RMON IN/OUT Counters	
Fiber 1 In	129,435,758
Fiber 1 Out	118,632,588
Fiber 2 In	0
Fiber 2 Out	0
UTP 3 In	0
UTP 3 Out	0
UTP 4 In	5,423,834
UTP 4 Out	15,801,514

The RMON in/out counters show the received and transmitted frames for each of the interfaces on **1000EAS/X**.

To clear the counters, click either the 'Clear OAM Counters' or 'Clear RMON Counters' button.

4.5.7 SFP

Modern optical SFP transceivers support digital diagnostics monitoring (DDM) functions according to the industry-standard SFF-8472. This optional feature in SFP is also known as digital optical monitoring (DOM) and gives the end user the ability to monitor real-time parameters of the SFP, such as optical output power, optical receive power, temperature, etc. DDM is not available in every SFP, so if the inserted SFP does not support DD, there will be no view for it. However, every SFP should be able to view the manufacturer name, part number, fiber type and link length. To view the SFP particulars, click the 'SFP' tab.



NMC Action	Side	Model	Version
Inactive (Stand alone)	Local	FRM220-1000EAS/X	1.000-1.006-0.000-0.000

Fiber 1

Small Form Pluggable	
Vendor Name	FIBERXON INC.
Vendor Part Number	FTM-3125C-L40
Fiber Type	Single
Wave Length	1310 nm
Wave Length 2	-- nm
Link Length	40 km

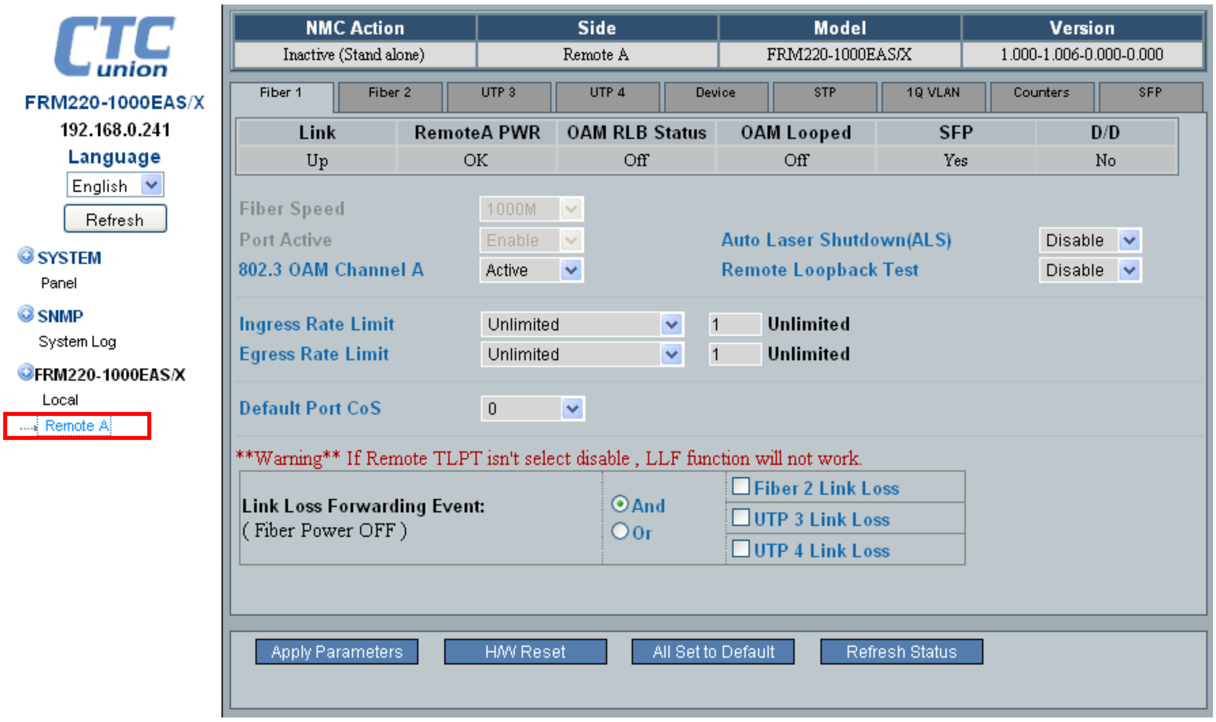
Digital Diagnostic	
Tx Power	0 dBm
Rx Power	-19 dBm
Rx Sensitivity	-- dBm
Temperature	53 degree C

Fiber 2

Small Form Pluggable	
Vendor Name	CTC UNION
Vendor Part Number	SFS-7010-L31(I)
Fiber Type	Single
Wave Length	1310 nm
Wave Length 2	1310 nm
Link Length	10 km

4.6 Remote Configuration

By utilizing 802.3ah proprietary OAM packets, **1000EAS/X** is able to view the status and manage the remote device without using Internet Protocol. All settings are done using the same methods as the local device.



NMC Action	Side	Model	Version
Inactive (Stand alone)	Remote A	FRM220-1000EAS/X	1.000-1.006-0.000-0.000

Link	RemoteA PWR	OAM RLB Status	OAM Looped	SFP	D/D
Up	OK	Off	Off	Yes	No

Fiber Speed: 1000M

Port Active: Enable

802.3 OAM Channel A: Active

Auto Laser Shutdown(ALS): Disable

Remote Loopback Test: Disable

Ingress Rate Limit: Unlimited 1 Unlimited

Egress Rate Limit: Unlimited 1 Unlimited

Default Port CoS: 0

Warning If Remote TLPT isn't select disable , LLF function will not work.

Link Loss Forwarding Event:
(Fiber Power OFF)

● And
○ Or

□ Fiber 2 Link Loss
□ UTP 3 Link Loss
□ UTP 4 Link Loss

Upgrade Note: Due to the size of the upgrade image, upgrading via OAM is not supported. The remote unit must be accessible via TCP/IP in order to upgrade.

www.ctcu.com

T +886-2 2659-1021 **F** +886-2 2659-0237 **E** info@ctcu.com