



PRODUCT

Quick Start Guide

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
info@ctcu.com
marketing@ctcu.com

H www.ctcu.com



ISO 9001 Quality System Certified

2008 CTC Union Technologies Co., LTD.
All trademarks are the property of their respective owners.
Technical information in this document is subject to
change without notice.



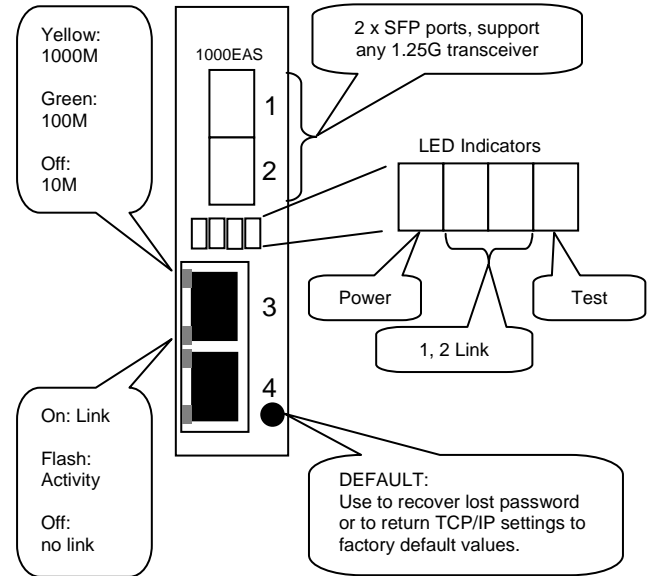
FRM220-1000EAS Quick Guide

Introduction

The FRM220-1000EAS is a two fiber port (1000) plus two copper port (10/100/1000) gigabit Ethernet media converter with OSI Layer 2 switch technologies that includes 802.1Q and port based VLAN, 802.3ad link aggregation or port trunking, 802.1D Spanning Tree Protocol, 802.3x Flow Control and ingress/egress bandwidth control. With its own embedded processor, the FRM220-1000EAS supports stand-alone management via IP (Telnet, SNMP & HTTP) or in-band management via 802.3ah-OAM protocol when connected to another FRM220-1000EAS in point to point or as a CPE device to an FRM220-1000EAS mounted in the FRM220 managed media converter rack.

Features

1. Four port L2 switch
2. Port based VLAN support
3. Port Trunking (Link Aggregation)
4. Bandwidth control
5. Spanning Tree
6. 32bit embedded CPU for stand-alone management
7. 802.3ah-OAM in-band management
8. Firmware upgrade via TFTP
9. Telnet, HTTP, SNMP and OAM management
10. Dying gasp (remote power failure detection)
11. Auto Laser Shutdown
12. RMON counters
13. NTP client



Factory reset procedure

Apply power to the 1000EAS 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 6 seconds. **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=10.1.1.91
username and password reset both to 'admin' if enabled

Login

Connect either copper Ethernet port to a PC. Configure the PC to the same subnet as the 1000EAS (recommend 10.1.1.91). Use Telnet protocol (port 23) to connect to the 1000EAS. If the password has been enabled, then the factory default will be 'admin/admin'.

Main Menu

```
*****
*   CTCU FRM220-1000EAS ver:2.005   *
*****

Remote A Module  [1000EAS  ]
Remote B Module  [Empty    ]
Port 1 OAM Mode  [Active  ]
Port 2 OAM Mode  [Disable]
PortTrunk        [Disable]
PortVLAN         [Disable]
Redundancy       [Disable]

<L> :Local States and Configuration
<A> :Remote A States and Configuration
<B> :Remote B States and Configuration
<M> :SNMP Manager
<S> :System Config And Image Download
Please select an item.
```

The operation of the 1000EAS 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 the 1000EAS so that the session connection is closed. 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, others are selected from additional sub-menus. Unless advised the unit requires a reboot, all other settings take effect immediately.

TCP/IP Configuration

Select item 'S' from main menu, *System Config And Image Download*

```
*****
*   CTCU FRM220-1000EAS ver:2.005   *
*****

<< System Config And Image Download >>
Target MAC Address = 00:02:ab:ff:fe:02
<1> Target IP           : 10.1.1.1
<2> Target Netmask     : 255.255.255.0
<3> Target Gateway     : 10.1.1.254
<4> Target Name        : ctcu
<5> TFTP Server IP     : 10.1.1.91
<6> TFTP File Name     : bootpImage
<7> TFTP Download File System :
<8> Load default settings and write to system.
<T> Adjust Date and Time.
<L> Password setting
<R> System Reboot.
Please select an item.
```

Change all required settings, but leave the target IP setting for last. The software is designed such that when the target IP setting is changed, the device will automatically reboot. So, by changing everything else first and doing the IP address last, the unit will reboot with all the new settings ready.

Firmware Upgrade

The *System Config And Image Download* menu is also where new firmware may be applied to the 1000EAS. The firmware is uploaded to the agent using Trivial FTP protocol. Once the TFTP server's IP is configured and the image file name matches the update image placed in the TFTP root, item #7 will start the upload process. Once the image has been uploaded into memory (approximately 20 seconds), and the checksum confirmed, the image will overwrite the flash memory (non-volatile memory). Following successful flash writing (approximately 50 seconds), the 1000EAS will automatically reboot.

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

Local Configuration

Select item 'L' from the main menu. From the **Local 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.

```
<< Local States and Configuration >>
<1> :Device States and Configuration
<2> :Fiber 1 States and Configuration
<3> :Fiber 2 States and Configuration
<4> :UTP 3 States and Configuration
<5> :UTP 4 States and Configuration
<L> :Link Loss Forwarding
<O> :OAM Configuration
<C> :Clear RMON Counter
<ESC>Go to previous menu
```

Device State (1) Select item 1

```
<< Local Device States and Configuration >>
```

Auto Laser Shutdown

```
<A>[ ]Port 1 Fiber Rx Loss --> Port 1 Fiber Tx OFF
<B>[ ]Port 2 Fiber Rx Loss --> Port 2 Fiber Tx OFF
```

Pause Frame

```
<C>Pause Frame [Disable]
```

Port VLAN

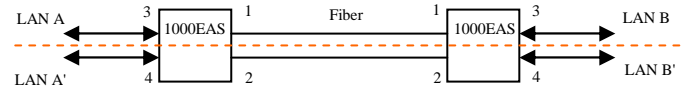
```
<D>[ ]Port 1 and Port 3 VLAN/Port 2 and Port 4 VLAN
<E>Switch Functions [-- Normal --]
0. Normal
1. Port 1&2 Bandwidth 2G
2. Port 1&2 Mirror
4. Port 1&2 Redundancy
```

```
<R>Accept Remote H/W Reset [Disable]
<S>Device Active [Enable ]
<L>Load default settings and write to system.
<T>System Reboot.
<ESC>Go to previous menu
```

This main device menu sets the 'Auto Laser Shutdown', pause frame and port based VLAN functions. Accept Remote H/W reset, when enabled, allows the remote unit to reset this unit.

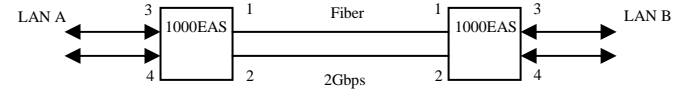
Port VLAN explanation

Port 1 and Port 3 VLAN/Port 2 and Port 4 VLAN



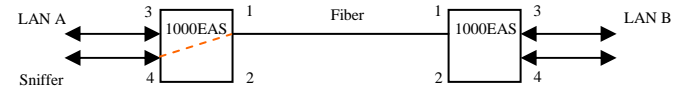
The single 1000EAS acts like two gigabit media converters in one package. The centrally located converter may also connect to two different remote locations with 1000EAS-1 at each remote.

Port 1&2 Bandwidth 2G



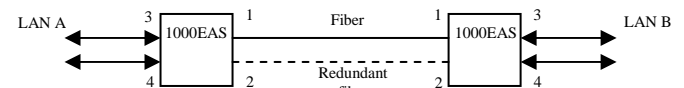
In this mode the fibers are aggregated or 'trunked' to provide 2G bandwidth.

Mirror



The mirror mode allows lawful intercept or packet sniffing. The traffic from the fiber link is 'copied' to the second UTP port.

1&2 Redundancy



In redundancy mode, the second fiber acts as a backup. If main fiber is broken, the second fiber will quickly take over the transmissions.

Reading DD of SFP

Fiber State and Configure Example:

```
<< Local Fiber 1 States and Configuration >>
Link Status           [Link up ]
LoopBack Test Status  [Disable]
Remote Power          [OK]
Rx Bytes(RMON IN)    [508352]
Tx Bytes(RMON OUT)   [598808]
<1> Fiber Port 1 Active [Enable ]
<2> Ingress Rate Limit
    IRL Mode          [No Limit]
    Limit Rate        [Disable]
<3> Egress Rate Limit
    ERL Mode          [No Limit]
    Limit Rate        [Disable]
<4> Digital Diagnostic (D/D) Function
<5> Local Loopback   [Disable]
<6> INFO ROM 1
<7> INFO ROM 2
<ESC>Go to previous menu
```

Informational

Port Active

Rate Limiting

Loop Back

The fiber always works at 1000M full-duplex. If SFP are used for fiber connection, this unit is capable of reading the SFP information, including the extended digital diagnostics information. Each port may be disabled or enabled through software.

For bandwidth settings, IRL or ingress rate limit refers to limiting any packets coming into the converter, while ERL or egress rate limit refers to limiting packets leaving the converter. When rate limiting is applied, ERL will use pause commands 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.

DD or digital diagnostics is an optional function of SFP transceiver modules where extra information such as internal temperature, laser Tx level, Rx receive level and Rx sensitivity can be read as well as the standard MSA (Multisource Agreement) SFP values such as vendor name, part number, optical wavelengths and supported link length. DD is not available in every SFP, so if the function says 'No' then the inserted SFP does not support DD.

The following is an example of an SFP that supports DD.

```
<ESC> Return.
@ Local Configuration -> Port 2 fiber ->Digital Diagnostic (D/D)
Function
D/D Function[Yes]
Vendor Name       [CTC Union      ]
Vendor Part Number [SFS-7040-L31-DD ]
Fiber Type [Single]
Tx Wave Length [1310 nm]
Rx Wave Length [1310 nm]
Link Length [40 Km]
D/D Status [Yes]
TX Power [0 dBm]
RX Power [-23 dBm]
RX Sensitivity [0 dBm]
Temperature [51 degree C]
```

The following is an example of an SFP without DD.

```
<ESC> Return.
@ Local Configuration -> Port 2 fiber ->Digital Diagnostic (D/D)
Function
D/D Function[No]
Vendor Name       [CTC Union      ]
Vendor Part Number [SFS-7020-L31  ]
Fiber Type [Single]
Tx Wave Length [1310 nm]
Rx Wave Length [1310 nm]
Link Length [20 Km]
D/D Status [No]
```

UTP Setting Example:

```
<< Local UTP 3 States and Configuration >>
Link Status      [Link up ]
Speed            [10M]
Duplex           [Half]
Rx Bytes(RMON IN) [0]
Tx Bytes(RMON OUT) [276116]
```

Informational

Configuration:

```
<1> UTP Port 3 Active [Enable ]
<2> Negotiation      [Manual]
<3> Speed            [10M]
<4> Duplex           [Half]
<5> Ingress Rate Limit
    IRL Mode         [Unlimited]
    Limit Rate       [Disable]
<6> Egress Rate Limit
    ERL Mode         [Unlimited]
    Limit Rate       [Disable]
<S> Confirm and Save Settings
```

UTP port settings

Rate Limiting

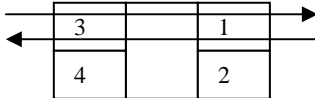
The UTP settings include the manual settings for 10, 100, 1000 speed, full or half duplex and the rate limiting settings.

Rate Limit Example:

Select item #6 from the Port 3 utp menu.

```
<ESC> Return.
@ Local Configuration -> Port 3 utp -> Egress Rate Limit
    Limit Rate [UnLimit]
    <0>UnLimit
    <1>Limit
```

Initially, there is no rate limiting employed. Select item #1 to enable ingress rate limiting for UTP port 3.



To limit speed from port 3 to 1, set the speed as ERL on port 1.
To limit speed from port 1 to 3, set the speed as ERL on port 3.

Using ERL will ensure proper flow control with pause. If setting IRL, packets are simply dropped with rate threshold is reached.

OAM Configuration

Select item 'o' from the Local States and Configuration menu. The OAM in the 1000EAS uses the standard IEEE 802.3ah protocol.

```
<< Local OAM Configuration >>
<1> OAM Port 1 Mode [Active ]
<2> OAM Port 2 Mode [Disable]
<3> MAX OAMPDUs Size [1500] ( 60 - 1518 Octets )
<4> OAM A Statistics
<5> OAM B Statistics
<6> Show Remote A Configuration
<7> Show Remote B Configuration
<8> Remote A H/W Reset
<9> Remote B H/W Reset
<A> Remote A F/W Update
<B> Remote B F/W Update
```

The OAM function must first be enabled for Port 1, Port 2 or both. When the 'Admin state' is enabled, the OAM is active. In a network of 1000EAS devices, only one unit can be in Mode [Active], all others must be [Passive]. If all units are set [Passive], the one with lowest MAC address will be the master.

The maximum OAMPDU packet size must be the same setting on all units. The default is 1500 octets.

Using transparent OAM, the fiber remote connected converter can be monitored or configured (item #6).

Remote H/W Reset enabled is usually the condition for the remote converter. When set enabled, it allows the local managed converter to reset the remote converter, causing it to reboot.

Remote firmware upgrade is also available via OAM. It is very slow though, and if the remote can be accessed by IP, then it is better to log in locally to do the TFTP upgrade.

Link Loss Forwarding

Select item 'L' from the Local States and Configuration menu. Link Loss Forwarding is a method to report loss of Rx from any fiber or UTP port and effectively stop Tx on any other fiber or UTP port. Since the 1000EAS has 4 ports, the LLF function is configured via a 4x4 matrix table and with 'and' or 'or' logic operations.

<< Local Link Loss Forwarding >>

Condition	Port 1 Rx Loss	Port 2 Rx Loss	Port 3 Rx Loss	Port 4 Rx Loss
Port 1 Tx off <0>[And]		<1>[]	<2>[]	<3>[]
Port 2 Tx off <4>[And]	<5>[]		<6>[]	<7>[]
Port 3 Tx off <8>[And]	<9>[]	<A>[]		
Port 4 Tx off [And]	<C>[]	<D>[]		

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)

SNMP Configuration

Select item 'M' from the main menu. Set up to eight manager IP by single IP or by network address. In the following example, 172.24.1.251 has full read-write access when using community string name 'private'. Everyone on the 172.24.1.0 network has read access when using community string name 'public'.

<< SNMP Manager Configuration Setup >>

Manager's IP	Community String	Access
#1 172.24.1.251	private	read-write
#2 172.24.1.0	public	read-only
#3 ---	---	---
#4 ---	---	---
#5 ---	---	---
#6 ---	---	---
#7 ---	---	---
#8 ---	---	---

Command Function Key:

<1>~<8>: Edit manager #1 to #8 setting.

<D> : Delete all settings.

<A> : Alarm settings.

<N> : Go to Trap Configuration menu.

<S> : Confirm above setting and restart SNMP.

SNMP Traps: (press 'N' from the Manager Setup)

<< Trap Configuration Setup >>

Trap Receiver IP	Community String
#1 172.24.1.251	private
#2 ---	---
#3 ---	---
#4 ---	---
#5 ---	---
#6 ---	---
#7 ---	---
#8 ---	---

Command Function Key:

SNMP traps are unsolicited messages that will be send to the above listed SNMP managers. Make sure the trap manager in the management software is configured with the proper community string name.