SONET/SDH

Reference Manual
For the IMUX 2000s

RFL Electronics Inc.

353 Powerville Road ● Boonton Twp., NJ 07005-9151 USA
Tel: 973.334.3100 ● Fax: 973.334.3863
Email: sales@rflelect.com ● www.rflelect.com

Publication Number MC2000S
Printed in U.S.A.
December 12, 2013

NOTICE

The information in this manual is proprietary and confidential to RFL Electronics Inc. Any reproduction or distribution of this manual, in whole or part, is expressly prohibited, unless written permission is given by RFL Electronics Inc.

This manual has been compiled and checked for accuracy. The information in this manual does not constitute a warranty of performance. RFL Electronics Inc. reserves the right to revise this manual and make changes to its contents from time to time. We assume no liability for losses incurred as a result of out-of-date or incorrect information contained in this manual.

WARRANTY

The RFL 2000s upgrade comes with a five year warranty from date of shipment for replacement of any part, which fails during normal operation. RFL will repair or, at its option, replace components that prove to be defective at no cost to the Customer. All equipment returned to RFL Electronics Inc. must have an RMA (Return Material Authorization) number, obtained by calling the RFL Customer Service Department. A defective part should be returned to the factory, shipping charges prepaid, for repair or replacement FOB Boonton, N.J.

RFL Electronics Inc. is not responsible for warranty of peripherals, such as printers and external computers. The warranty for such devices is as stated by the original equipment manufacturer. If you have purchased peripheral equipment not manufactured by RFL, follow the written instructions supplied with that equipment for warranty information and how to obtain service.

WARRANTY STATEMENT

The RFL 2000s is warranted against defects in material and workmanship for five years from the date of shipment. During the warranty period, RFL will repair or, at its option, replace components that prove to be defective at no cost to the customer, except the one-way shipping cost of the failed assembly to the RFL Customer Service facility in Boonton, New Jersey. RFL warrants product repair from five years from the date of repair or the balance of the original factory warranty, whichever is longer.

This warranty does not apply if the equipment has been damaged by accident, neglect, misuse, or causes other than performed or authorized by RFL Electronics Inc.

This warranty specifically excludes damage incurred in shipment to or from RFL. In the event an item is received in damaged condition, the carrier should be notified immediately. All claims for such damage should be filed with the carrier.

NOTE

If you do not intend to use the product immediately, it is recommended that it be opened immediately after receiving and inspected for proper operation and signs of impact damage.

This warranty is in lieu of all other warranties, whether expressed, implied or statutory, including but not limited to implied warranties of merchantability and fitness for a particular purpose. In no event shall RFL be liable, whether in contract, in tort, or on any other basis, for any damages sustained by the customer or any other person arising from or related to loss of use, failure or interruption in the operation of any products, or delay in maintenance or for incidental, consequential, indirect, or special damages or liabilities, or for loss of revenue, loss of business, or other financial loss arising out of or in connection with the sale, lease, maintenance, use, performance, failure, or interruption of the products.

Table of Contents

List of Effective Pages

When revisions are made to the 2000s Instruction Manual, the entire section where revisions were made is replaced. For this addition of the Instruction Manual dated December 12, 2013 the sections are dated as follows.

Section	Date
Front Section, TOC etc.	December 12, 2013
Section 1.	December 12, 2013
Section 2.	December 12, 2013
Section 3.	December 12, 2013
Section 4.	December 12, 2013
Section 5.	December 12, 2013
Section 6.	December 12, 2013
Section 7.	December 12, 2013
Section 8.	December 12, 2013
Section 9.	December 12, 2013
Section 10.	December 12, 2013
Section 11.	December 12, 2013

Trademark information:

“Windows” ,“Windows XP”, “Vista” and “Windows 7” are registered trade marks of Microsoft Corporation.

“Ethernet” is a trademark of Xerox Corporation.

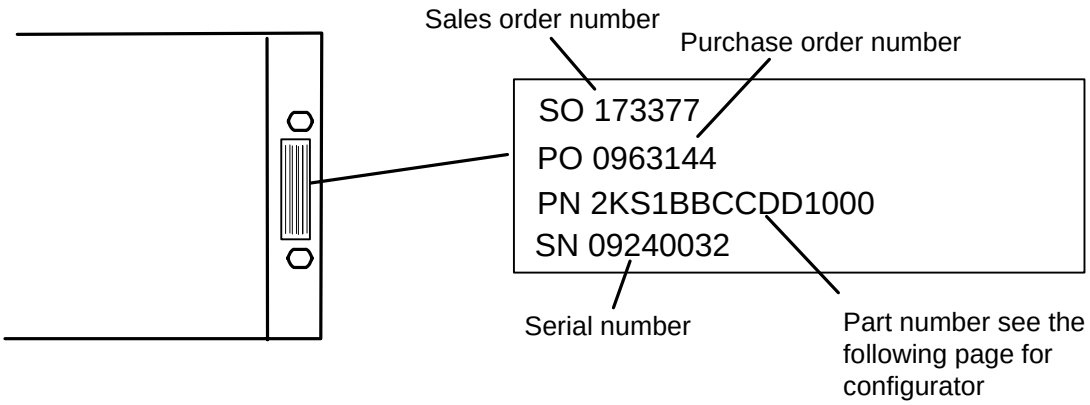
The trademark information listed above is, to the best of our knowledge, accurate and complete.

Revision Record

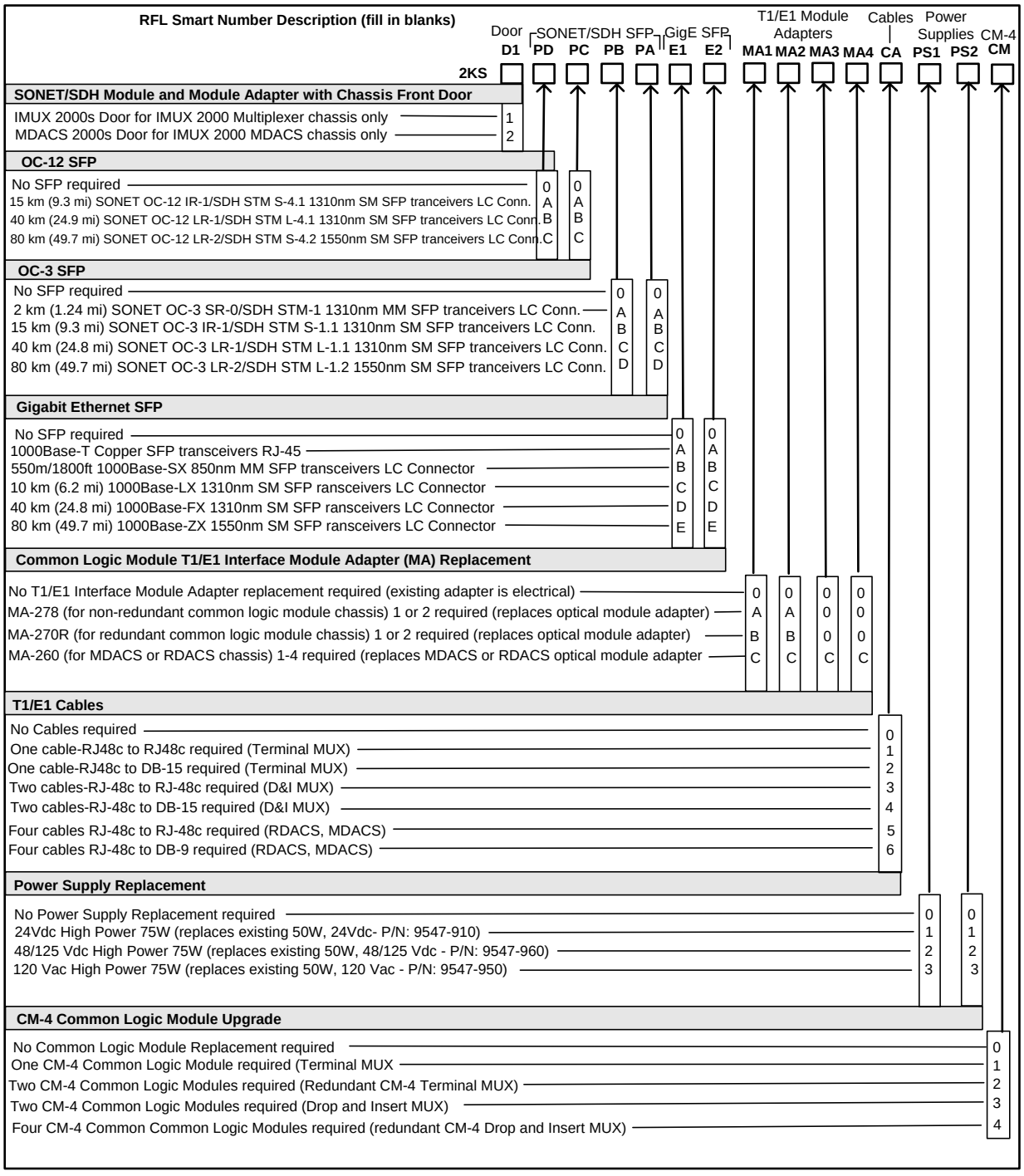
Rev. Date on Manual	Description of Changes	Actual Date Released
12/12/13	Initial Release under ECO 2000-860	Pending

Ordering Information, Decoding the Part Number

Serial and part number information is located on the right mounting bracket (ear) of the IMUX 2000s unit as shown below. The part number and **site name** (if provided by the customer) is also located on the other mounting bracket.



The following page lists the possible ordering options.


RFL Smart Number Description (fill in blanks)
Door
SONET/SDH SFP
GigE SFP
T1/E1 Module Adapters
Cables
Power Supplies
CM-4
D1 PD PC PB PA E1 E2 MA1 MA2 MA3 MA4 CA PS1 PS2 CM
2KS
SONET/SDH Module and Module Adapter with Chassis Front Door
IMUX 2000s Door for IMUX 2000 Multiplexer chassis only
MDACS 2000s Door for IMUX 2000 MDACS chassis only
1
2
OC-12 SFP
No SFP required
15 km (9.3 mi) SONET OC-12 IR-1/SDH STM S-4.1 1310nm SM SFP tranceivers LC Conn.
40 km (24.9 mi) SONET OC-12 LR-1/SDH STM L-4.1 1310nm SM SFP tranceivers LC Conn.
80 km (49.7 mi) SONET OC-12 LR-2/SDH STM S-4.2 1550nm SM SFP tranceivers LC Conn.
0 A B C
0 A B C
OC-3 SFP
No SFP required
2 km (1.24 mi) SONET OC-3 SR-0/SDH STM-1 1310nm MM SFP tranceivers LC Conn.
15 km (9.3 mi) SONET OC-3 IR-1/SDH STM S-1.1 1310nm SM SFP tranceivers LC Conn.
40 km (24.8 mi) SONET OC-3 LR-1/SDH STM L-1.1 1310nm SM SFP tranceivers LC Conn.
80 km (49.7 mi) SONET OC-3 LR-2/SDH STM L-1.2 1550nm SM SFP tranceivers LC Conn.
0 A B C D
0 A B C D
Gigabit Ethernet SFP
No SFP required
1000Base-T Copper SFP transceivers RJ-45
550m/1800ft 1000Base-SX 850nm MM SFP transceivers LC Connector
10 km (6.2 mi) 1000Base-LX 1310nm SM SFP ransceivers LC Connector
40 km (24.8 mi) 1000Base-FX 1310nm SM SFP ransceivers LC Connector
80 km (49.7 mi) 1000Base-ZX 1550nm SM SFP ransceivers LC Connector
0 A B C D E
0 A B C D E
Common Logic Module T1/E1 Interface Module Adapter (MA) Replacement
No T1/E1 Interface Module Adapter replacement required (existing adapter is electrical)
MA-278 (for non-redundant common logic module chassis) 1 or 2 required (replaces optical module adapter)
MA-270R (for redundant common logic module chassis) 1 or 2 required (replaces optical module adapter)
MA-260 (for MDACS or RDACS chassis) 1-4 required (replaces MDACS or RDACS optical module adapter
0 A B C
0 A B C
0 0 0 C
0 0 0 C
T1/E1 Cables
No Cables required
One cable-RJ48c to RJ48c required (Terminal MUX)
One cable-RJ48c to DB-15 required (Terminal MUX)
Two cables-RJ-48c to RJ-48c required (D&I MUX)
Two cables-RJ-48c to DB-15 required (D&I MUX)
Four cables RJ-48c to RJ-48c required (RDACS, MDACS)
Four cables RJ-48c to DB-9 required (RDACS, MDACS)
0 1 2 3 4 5 6
Power Supply Replacement
No Power Supply Replacement required
24Vdc High Power 75W (replaces existing 50W, 24Vdc- P/N: 9547-910)
48/125 Vdc High Power 75W (replaces existing 50W, 48/125 Vdc - P/N: 9547-960)
120 Vac High Power 75W (replaces existing 50W, 120 Vac - P/N: 9547-950)
0 1 2 3
0 1 2 3
CM-4 Common Logic Module Upgrade
No Common Logic Module Replacement required
One CM-4 Common Logic Module required (Terminal MUX
Two CM-4 Common Logic Modules required (Redundant CM-4 Terminal MUX)
Two CM-4 Common Logic Modules required (Drop and Insert MUX)
Four CM-4 Common Common Logic Modules required (redundant CM-4 Drop and Insert MUX)
0 1 2 3 4

Section 1. Safety Instructions

1.1 Warnings and Safety Summary

The equipment described in this manual contains high voltage. Exercise due care during operation and servicing. Read the safety summary below.

1.1.1 Safety Summary

The following safety precautions must be observed at all times during operation, service, and repair of this equipment. Failure to comply with these precautions, or with specific warnings elsewhere in this manual, violates safety standards of design, manufacture, and intended use of this product. RFL Electronics Inc. assumes no liability for failure to comply with these requirements.

Ground the Chassis

The chassis must be grounded to rCeduce shock hazard and allow the equipment to perform properly. Equipment supplied with three-wire ac power cables must be plugged into an approved three-contact electric outlet. All other equipment is provided with a rear-panel protective earth terminal, which must be connected to a proper electrical ground by suitable cabling. The location of the protective earth terminal on the IMUX 2000 is shown below. Refer to the wiring diagram supplied with the unit for additional information on chassis and/or cabinet grounding.

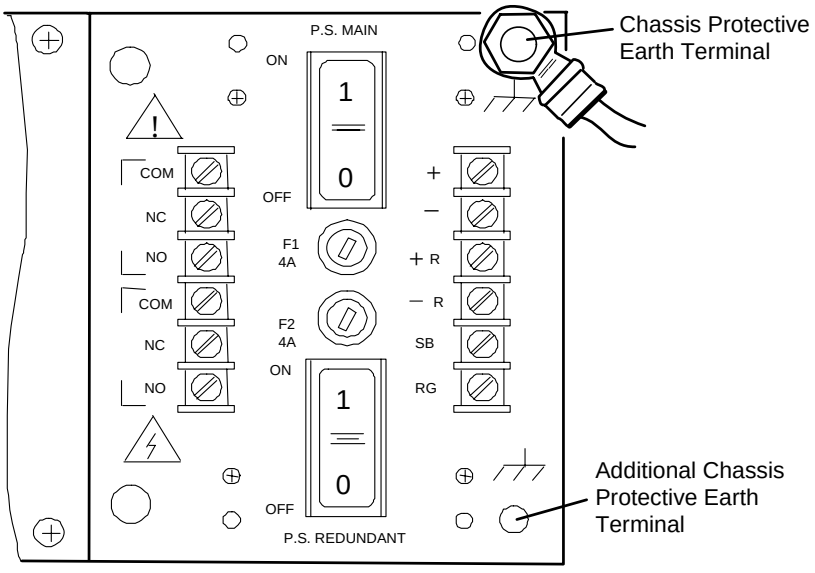


Figure 2-1. Location of Chassis Protective Earth Terminal on IMUX 2000s

Do not Operate in an Explosive Atmosphere or in Wet or Damp Areas

Do not operate the product in the presence of flammable gases or fumes, or in any area that is wet or damp. Operating any electrical equipment under these conditions can result in a definite safety hazard.

Keep Away from Live Circuits

Operating personnel should never remove covers. Component replacement and internal adjustments must be done by qualified service personnel. **Before attempting any work inside the product, disconnect it from the power source and discharge the circuit by temporarily grounding it.** This will remove any dangerous voltages that may still be present after power is removed.

Unrestricted operator access is only permitted to the front of the unit when hazardous voltage is applied. It is the responsibility of the installer to restrict access to the rear terminal blocks where hazardous voltage may exist.

Do not Substitute Parts or Modify Equipment

Because of the danger of introducing additional hazards, do not install substitute parts or make unauthorized modifications to the equipment. The product may be returned to RFL for service and repair, to ensure that all safety features are maintained.

Read the Manual

Operators should read this manual before attempting to use the equipment, to learn how to use the equipment properly and safely. Service personnel must be properly trained and have the proper tools and equipment before attempting to make adjustments or repairs.

Service personnel must recognize that whenever work is being done on the product, there is a potential electrical shock hazard and appropriate protection measures must be taken. Electrical shock can result in serious injury, because it can cause unconsciousness, cardiac arrest, and brain damage.

Throughout this manual, warnings appear before procedures that are potentially dangerous, and cautions appear before procedures that may result in equipment damage if not performed properly. The instructions contained in these warnings and cautions must be followed exactly.

1.1.2 Additional Warnings

WARNING!
The IMUX 2000s may use third party SFP Class 1 Laser Modules. These modules may be purchased through RFL or third parties. The class 1 certification originates with the SFP manufacturer, not RFL. Read the following safety information and any additional safety information included with the modules.

Class 1 Laser Products supplied by RFL are not considered dangerous and comply with the following standards:

US 21 CFR 1040.10 and 1040.11
IEC 60825-1: 2007

Laser light can potentially cause serious eye damage. The lasers used in the IMUX 2000s produce light that is invisible to the naked eye. It should be assumed that the laser is active at all times and it is imperative that the technician never look into the end of the fiber or the aperture with the naked eye or with optical instruments.

WARNING!
Extreme care must be used to avoid creating a safety hazard when employing long 2-wire telephone circuits which extend more than 100 feet (30 meters). Ground potential rise and/or induced AC voltages can result in injury or death under normal operating conditions and especially under fault conditions. RFL recommends against the use of this product in applications where the 2-wire telephone circuit extends beyond the perimeter of the substation ground mat. It is the installer's responsibility to ensure that all local, state, federal, and corporate safety standards and practices are complied with in any installation.

WARNING!
Follow all of your company's policies and procedures regarding the installation of AC powered or DC powered equipment. If there is a conflict between any procedure in this manual and your company's safety rules, then your company's safety rules must take priority.

WARNING!
Individual double pole disconnects must be installed between the building or station battery supply and the IMUX 2000s power supply(ies). This must be done for both the main and back-up supply.

WARNING!
75 Watt Power Supply(ies) must be installed in the chassis being upgraded to the SONET 2000s Multiplexer.

1.1.3 Additional Cautions

CAUTION

Any installation using an enclosed cabinet with a swing-out rack must be securely fastened to the floor. This will prevent the cabinet from falling forward when the rack is moved outward.

CAUTION

This equipment contains static sensitive devices. Persons working on this equipment must observe electro static discharge (ESD) precautions before opening the unit or working on the rear of the chassis. As a minimum you must do the following: Use anti-static devices such as wrist straps and floor mats.

Additional warnings and cautions appear throughout the manual, these warnings and cautions must be followed exactly.

CAUTION

The SFP cages on the front of the IMUX 2000s module may have sharp edges. Exercise caution when inserting or removing the IMUX 2000s module or connecting cables.

NOTICE

RFL products are not designed for safety critical direct control of nuclear reactors and should not be used as such.

Section 2. System Description

2.1 Key Features for the IMUX2000s

- **Bandwidth Increase 400x**

  Using existing IMUX 2000 T1 Networks.

- **Cost Effective Upgrade**

  Cost effective migration from T1 to OC-12 while retaining a TDM backbone.

- **Ethernet Interface**

  Two GigE WAN ports.

- **Existing NMS User Interface enhanced for SONET**

  Short learning curve for existing users.

- **Network Topology**

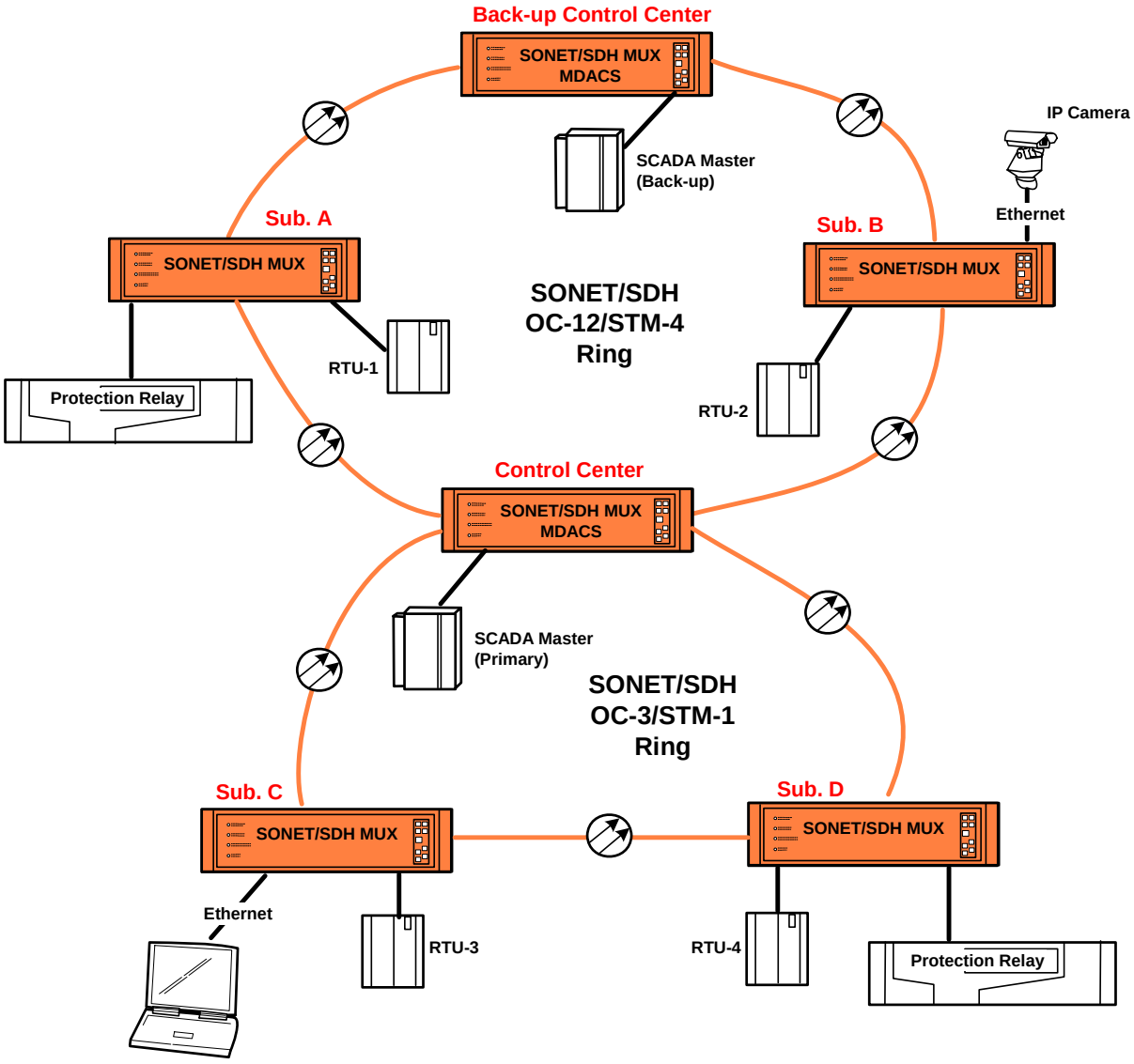
  Supports any network topology, including linear (bus), star and ring configurations.

- **Ethernet over SONET (EoS)**

  The IMUX 2000s has Ethernet over SONET with layer 1 physical separation meeting NERC CIP requirements.

- **Highly Resilient and Secure**

  Designed for harsh environments with immunity from SWC, ESD and RFI. Optional redundant power supply.



The IMUX 2000s is equipped with the following interfaces:

- **SONET/SDH Trunk**
  - 2 x 622Mbps/155 Mbps SFP receptacles
  - 2 x 155 Mbps SFP receptacles
- **Ethernet**
  - 2 x Gigabit Ethernet SFP receptacles (can be electrical or fiber)
  - 1 x 10/100BaseT, RJ-45 port for management
- **Craft Ports**
  - 2 x USB type B craft ports for CLI

- **TDM (On MA-491 Module Adapter)**
  - 4 x T1/E1 RJ-48c ports
- **RS-232 (On MA-491 Module Adapter)**
  - 1 x RS-232 (RJ-11) for connection to CM-4

2.2 Description of Upgrade Kit

The IMUX 2000s SONET/SDH module has been designed to fit into an existing IMUX 2000 T1/E1 and/or MDACS Multiplexer. This will instantly provide an upgrade from a T1/E1 (1.544Mbps/2.048Mbps) to an OC-12/STM-4 (622Mbps) bandwidth without replacing the existing IMUX equipment. This module upgrade provides a simple and easy migration path to an OC-12/STM-4 SONET/SDH communication backbone delivering Gigabit Ethernet and TDM services without having to replace the existing equipment.

- The constituent parts for the upgrade are easily installed, with minimum down time.
- The existing Visual Network Management Software (VNMS) has been modified to accept the SONET element; operation is seamless to the end-user.
- The IMUX 2000s SONET/Management module is hot swappable.

Front View of IMUX 2000s Upgrade

The following IMUX 2000 systems can be upgraded to use the IMUX 2000s SONET/SDH module.

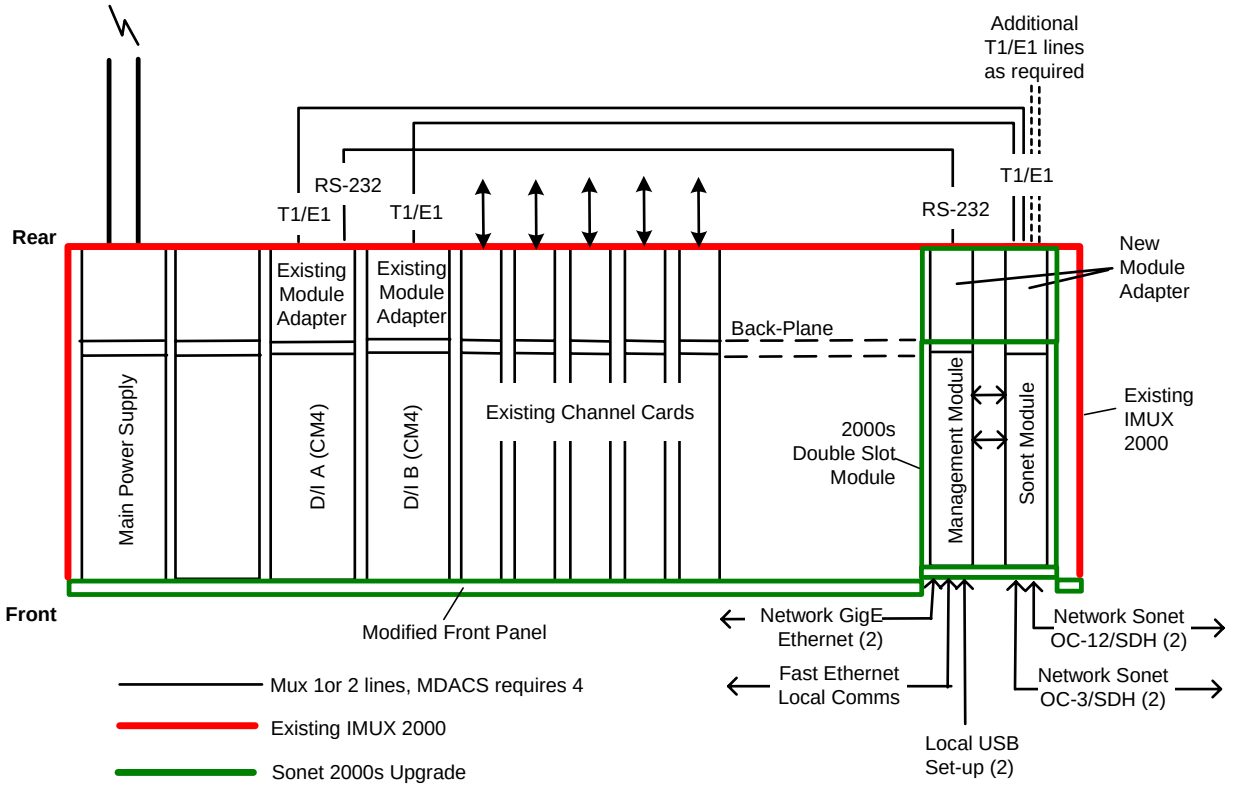
- IMUX 2000 T1/E1 Terminal End/Drop and Insert with CM-4
- IMUX 2000 MDACS Multiplexer

2.3 Interface Overview

The IMUX 2000s upgrade consists of a new IMUX front panel which replaces the existing panel. The front panel has a cut-out that covers a sub-panel on the new double slot 2000s SONET Module as shown below, thus ensuring EMI sealing. Additionally a special module adapter (MA-491) is provided that connects into the existing IMUX back-plane. The MA-491 adapter accepts T1/E1 and RS-232 cables provided with the upgrade kit. The provided cables are connected using existing T1/E1 (RJ-48c) and RS-232 (RJ-11) connectors on the existing module adapters as shown below.

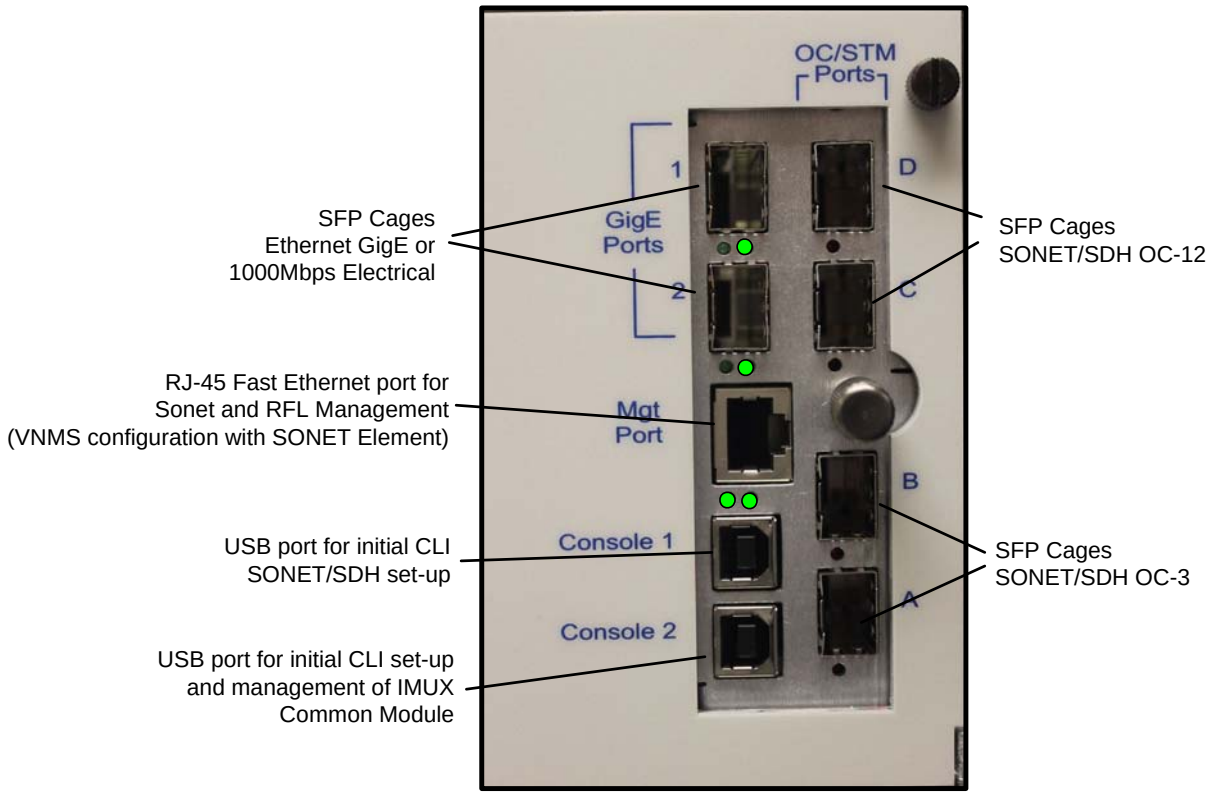
To summarize the provided parts for upgrade:

- Front Panel with associated hardware
- 2000s SONET/SDH Module
- 2000s Module Adapter (MA-491)
- 2000s Cables



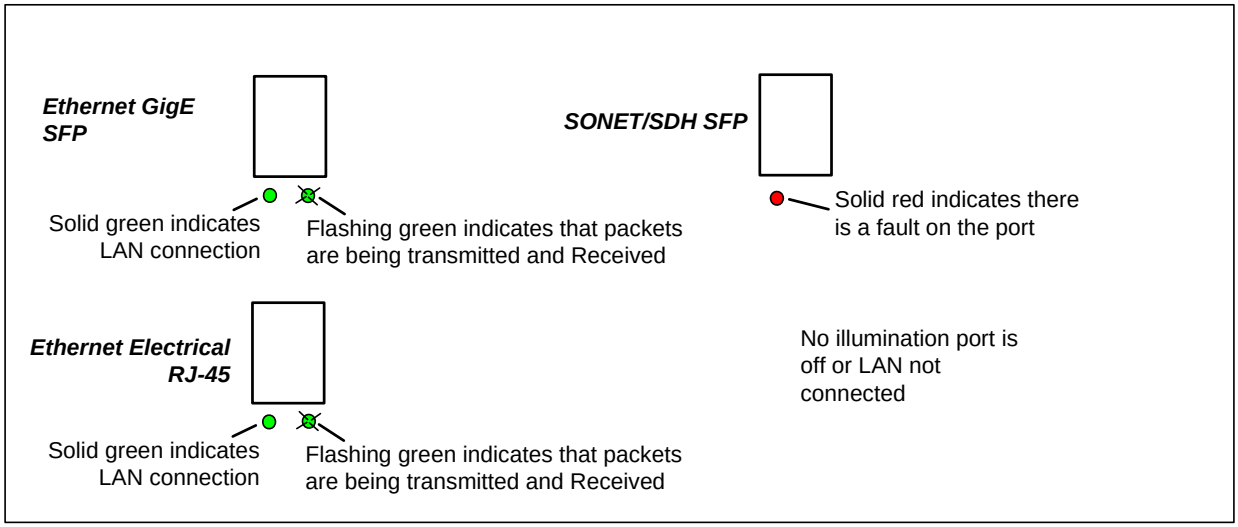
2.4 Front Panel Port Functions

The function and location of each of the front panel ports is shown below.



2.4.1 Front Panel LED Indicators

LED indicators are located on the front of the 2000s front panel, their function is shown below.



2.5 Rear Port Functions

The MA-491 Adapter at the rear of the IMUX 2000s module has four T1/E1 RJ-48c ports that transport TDM data between the SONET /SDH board and the existing IMUX CM4 module(s). Shown below are the possible number of T1/E1 port connections required.

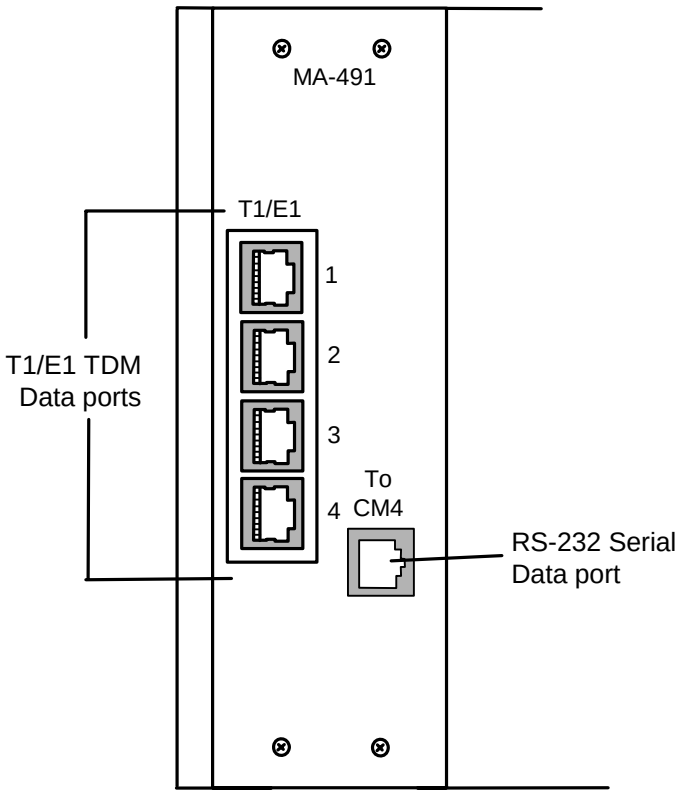
IMUX Applications	Number of connectors
IMUX terminal	1
IMUX D/I	2
IMUX MDACS	Up to 4

Also on the MA-491 adapter is an RS-232 (RJ-11) connector carrying configuration information between the Ethernet Management port on the front of the IMUX 2000s front panel and the CM4 module.

NOTE

The CM4 module(s) **MUST** have standard electrical interface adapters installed, not optical interface adapters.

The MA-491 port functions are shown below.



Section 3. Technical Data

3.1 2000s Specifications

Line ports	2 x OC-12/STM-4 (SFP)
Spur ports	2 x OC-3/STM-41(SFP)
Tributary ports	4 x T1/E1 (MA-491 module adapter – RJ48c)
	RS-232 (MA-491 module adapter – RJ-11)
IP ports	2 x 1000base-FX (SFP)
	1 x 10/100base-TX (RJ-45 IP Management)
Craft ports	2 x USB (IMUX and SONET/SDH set-up)
Power	+5 or +15V, less than 20 Watts
Environment	-20C (-4F) to 55C (131F)

3.2 SONET/SDH Compliances

Telcordia GR-253-CORE

Telcordia GR-499-CORE

(ITU) standards G.707, G.783, G.784, G.803

(ANSI) standard T1.105

ANSI T1.119/ATIS PP 0900119.01.2006: SONET

3.3 SFP Module Information

	RFL Part Number	Distance	Type	Connector
1000 Mb/s				
	104359-1	550m (1800ft)	850nm – MM Laser 1000Base-SX	LC
	104359-2	10 Km (6.2mi)	1310nm – SM Laser 1000Base-LX	LC
	104359-3	40 Km (24.8mi)	1310nm – SM Laser 1000Base-FX	LC
	104359-4	80 Km (49.7mi)	1550nm – SM Laser 1000Base-ZX	LC
	104359-5	120 Km (74.5mi)	1550nm – SM Laser 1000Base-ZX	LC

3.4 Approved OC-12 Interfaces (SFP)

RFL Part Number	Distance	Type	Connector
106272-1	15Km (9.3mi)	1310nm – SM Laser	LC
106272-2	40 Km (24.8mi)	1310nm – SM Laser	LC
106272-3	80 Km (49.7mi)	1550nm – SM Laser	LC

3.5 Approved OC-3 Interfaces (SFP)

RFL Part Number	Distance	Type	Connector
104358-1	2 Km (1.2mi)	1310nm –MM Laser 100Base-FX	LC
104358-2	10 Km (6.2mi)	1310nm – SM Laser 100Base-LX	LC
104358-3	40 Km (24.8mi)	1310nm – SM Laser	LC
104358-4	80 Km (49.7mi)	1550nm – SM Laser	LC

3.6 Disposal

When disposing of the equipment, it should be done in strict accordance with all local and national regulations for the disposal of electrical and electronic equipment. The printed circuit boards should be separated for recycling.

Section 4. Advanced Functionality

4.1 Advanced Encapsulation

The Advanced tab allows the network administrator to change control fields to provide interoperability with other network providers.

RFL recommends these settings are not altered and that the defaults as shown below are used.

The advanced tab will change according to Encapsulation scheme selected.

Encapsulation scheme is selected from the Interface dialog as in Figure 6-8 above.

4.1.1 LAPS

LAPS is a HDLC-like framing structure to encapsulate IEEE 802.3 Ethernet MAC frame to provide a point-to-point Full Duplex simultaneous bidirectional operation. The LAPS protocol is specified in the following standards: **ITU-T X.85/Y.1321** and **ITU-T X.86.**

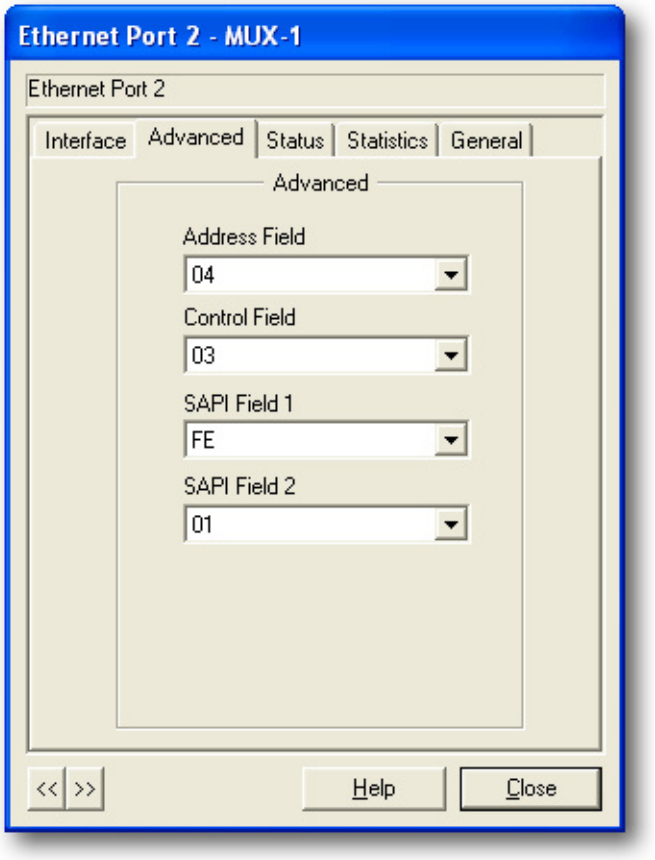


Figure 4-1. LAPS Control Fields

Table 4-1 IMUX 2000s Trap Descriptions

MSB	FLAG (0x7E)	LSB	1 octet
MSB	ADDRESS (0x04)	LSB	1 octet
MSB	CONTROL (0x03)	LSB	1 octet
MSB	First octet of SAPI (0xFE)	LSB	1 octet
MSB	Second octet of SAPI (0x01)	LSB	1 octet
	Destination Address (DA)		6 octets
	Source Address (SA)		6 octets
	Length / Type		2 octets
	MAC Client data		46 -1500 octets
	PAD		
	FCS of MAC 4 octets		
	FCS of LAPS 4 octets		
MSB	FLAG (0x7E)	LSB	1 octet

MSB	Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	LSB

4.1.2 GFP

Generic Framing Procedure (GFP) is protocol for mapping packet data into an octet-synchronous transport such as SONET/SDH. Unlike HDLC-based protocols, GFP does not use any special characters for frame delineation. Instead, it uses a cell delineation protocol, such as used by ATM, to encapsulate variable length packets. A fixed amount of overhead is required by the GFP encapsulation that is independent of the contents of the packet. The GFP protocol is specified in the **ITU-T G.7041/Y.1303** standard.

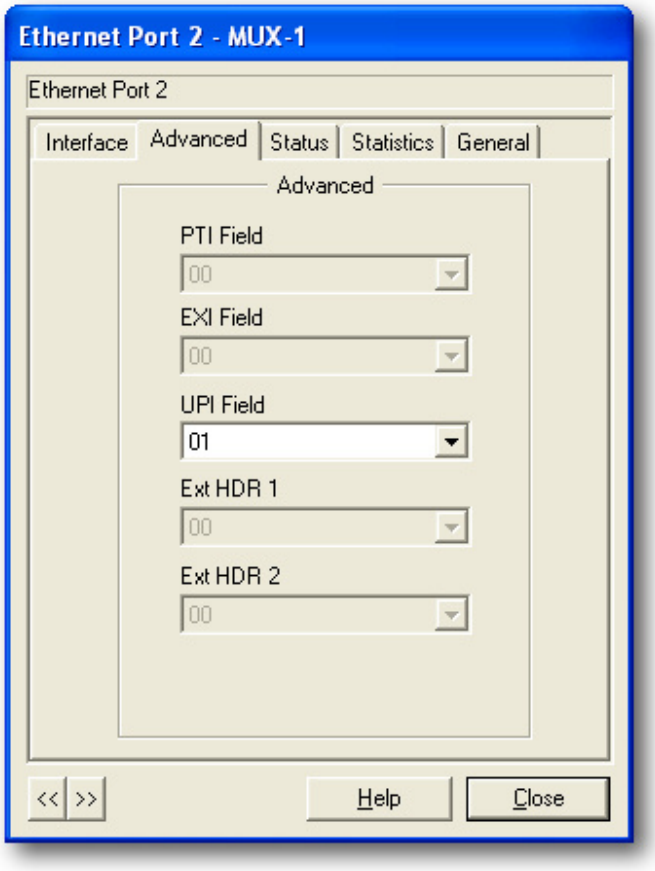


Figure 4-2. GFP Control Fields

Table 4-2 Format of GFP Frame with an Ethernet MAC Frame Payload

Ethernet MAC Frame										GFP Frame								
									Octets									
									2	PLI Field								
									2	cHEC Field								
									2	Type Field								
	7	Preamble							2	tHEC Field								
	1	Start of Frame Delimiter							0-60	Extension Header								
	6	Destination Address (DA)								GFP								
Octets	6	Source Address (SA)								MAC client data								
	2	Length/Type								Payload								
		MAC client data								Information								
		PAD								Pad Field								
	4	4 Frame Check Sequence (FCS)																
Bits		1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	

4.1.3 PPP

The Point-to-Point Protocol (PPP) is a HDLC-like framing structure and provides a standard method for transporting multi-protocol datagrams over point-to-point links. PPP can be used to encapsulate IEEE 802.3 Ethernet MAC frame to provide a point-to-point Full Duplex simultaneous bidirectional operation. The PPP Bridging Control Protocol (BCP) is specified in the following standards: **RFC 1661, RFC 1662, RFC 2878, RFC 2615** and **RFC 3518.**

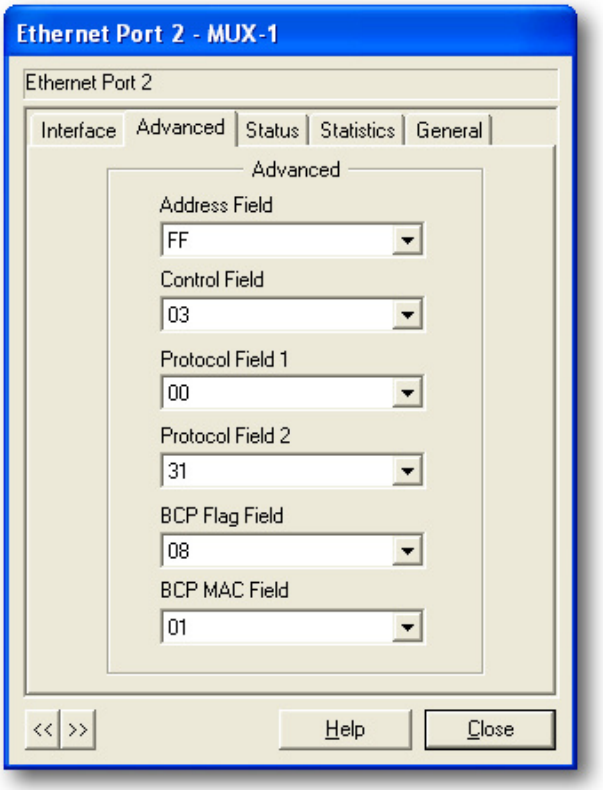


Figure 4-3. PPP Control Fields

Table 4-3 FDDI Frame Format (IEEE 802 Un-tagged Frame)

0										0										2										3	
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
HDLC FLAG																															
Address and Control																				0x00										0x31	
F	**0**	**Z**	**B**	**Pads**						MAC Type										Pad Byte										Frame Control	
Destination MAC Address																															
Destination MAC Address																				Source MAC Address											
Source MAC Address																															
LLC data																															
LAN FCS (optional)																															
optional Data Link Layer padding																															
Frame FCS																				HDLC FLAG											

Address and Control as defined by the framing in use.
PPP Protocol)x0031 for PPP Bridging

FLAGS bit F: Set if the LAN FCS field is present
bit 0: Reserved, must be zero
bit Z: Set if IEEE 802.3 Pad must be zero filled to minimum size
bit B: Set if the frame is a bridge control packet

Pads
Any PPP frame may have padding inserted in the optional Data Link Layer Padding" field. This number tells the receiving system how many pads octets to strip off.

4.1.4 Status

The Status Dialog will change according to the Encapsulation Scheme chosen.

If an **alarm** is any colour other than **green**, you may have to check these configuration items at the remote end. This may also include checking the status of the SONET/SDH parameters in the application section of the user interface.

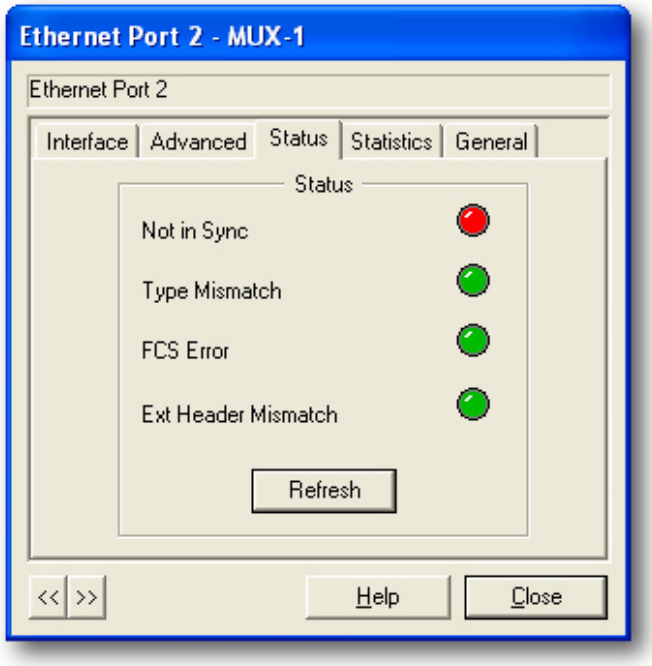


Figure 4-4. PPP Ethernet Status Alarms

4.1.5 Statistics

The **Statistics** section is used to monitor the traffic that has passed through the port (Ethernet Bridge) and over the WAN. Only packets that pass over the WAN will affect the statistics counters. The Transmit and Receive flow is shown in byte and packet counts.

The payload held in each packet adds to a byte counter. The byte counter does not include the Ethernet Frame overhead.

The **Refresh** button is used to get the current statistics from the port. This feature presents a "snap shot" of the network statistics at the time the button is pressed.

The **Clear** button is used to reset the traffic statistics, the counters are set to zero. Both Transmit and Receive directions will be cleared for byte and packet counters.

Both byte and packet counters are represented inside the Ethernet port as a 32-bit number. This represents 2^{32} bytes, and is equal to 4,294,967,296 bytes that can be counted before it rolls over to zero again. Please note: a byte counter will roll over much faster than a packet counter by orders of magnitude.

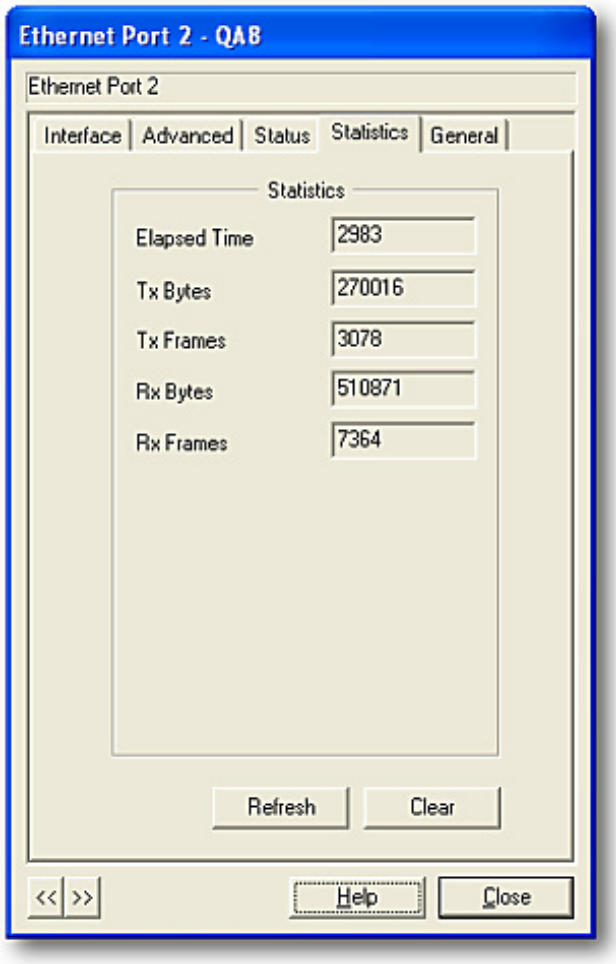


Figure 4-5. Ethernet Statistics

4.1.6 Ethernet Alarms

The Ethernet port has alarms that can be configured and monitored via the port alarm monitor setup window.

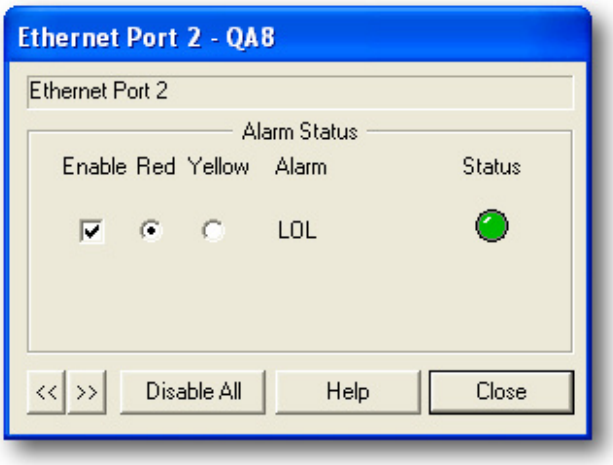


Figure 4-6. Monitoring Ethernet Alarms

4.2 Changing Routing Protocols

The networking tab allows the user to configure settings for a number of network items.

Table 4-2 lists the dialogs and provides a brief description of what each is used for. See each referenced section for further details.

See Section 4.3 for an example on using these parameters.

TCP/IP Network configuration should be completed in the following order:

1. Create user logins and assign system privileges.
2. Set node IP address
3. LAN IP address and network mask.
4. Enable Routing .
5. Routing specifics for the LAN interface.
6. Configure the WAN PPP, Link and routing specifics.
7. NTP client settings.
8. SNMP Communities.
9. SNMP trap targets.
10. Syslog.

Table 4-4 IMUX 2000s EMS Network Management Functions

Config Item	Description	See Section
Node	IP address used to access the node remotely.	
LAN	The local Ethernet IP address of the 2000s. Used for physical access as gateway for DCC connections. Provides IP connectivity for all of the 2000s IP network features.	
WAN	Used to setup internetworking across the DCC between adjacent IMUX 2000s nodes.	
WAN Status	A status window for DCC connections between adjacent nodes.	
Routing Table	A table displaying both static and dynamic route information held by the system.	
Static Routes	Static routes are entered in this dialog.	
SNMP Communities	SNMP community strings (names) and associated read/write permissions are entered in this dialog.	
SNMP Trap Targets	An IP address of a management console (computer configured to receive SNMP traps) is entered in this dialog.	
Syslog	An IP address of a management console (computer configured with a Syslog server) is entered in this dialog.	
NTP Client	An IP address of a NTP(computer configured with a NTP server) is entered in this dialog.	
IP Routing	IP Routing is configured in this dialog.	

4.2.1 Node

The node IP setting is accessed as follows:

System ⇨System Setup ⇨ Networking Tab ⇨ Node

Two different IP addresses must be set for the IMUX2000s SONET/SDH Module.

- LAN IP address (see 4.3.2)
- Node IP address

These are unrelated to the Management IP address used by the MA-491 Module Adapter to communicate with the IMUX 2000 Common Module.

The "Node IP address" is the WAN address of the node as seen remotely via DCC links. It is used by a managing computer to remotely connect to the node. See the Upgrade Manual for details on configuring node management via DCC.

4.2.2 Networking LAN

An IP address is required to identify and manage a node via TCP/IP in IMUX 2000s EMS. The IP address is also required if node is to be configured for Syslog or SNMP management, and is also required if the node is to be configured to have the system time synchronised using NTP.

The IP address for the node is the IP address of the console Ethernet interface only.

The node management IP address and mask is used for **local Ethernet** and **remote DCC** connections. The new IP address is activated immediately after the "Apply" button is executed. This will cause a loss of connection if the current connection is over IP.

The factory default IP address is 192.168.0.1 mask 255.255.255.0

The LAN IP address is configured from the main menu:

System ⇨System Setup ⇨ Networking Tab ⇨ LAN

4.2.2.1 Enable Routing

The IMUX 2000s supports two routing protocols, OSPF (Open Shortest Path First) and RIP (Routing Information Protocol) or can be configured to have no routing protocol running which is the default factory setting.

IMUX 2000s EMS is used to manage all IMUX 2000s nodes in a network via TCP/IP. The PC communicates with all nodes via gateway node and all other nodes over the DCC (Data Communications Channel). As nodes are configured with different network addresses, routing information must be maintained in the management PC as well as all other nodes in the network.

Routing protocols ensure that if a protected network configuration changes due to a fault or some other condition, all nodes in a managed network are updated periodically with current routing information.. This ensures nodes can communicate with one another providing a reliable management platform.

To configure routing on the IMUX 2000s:

Configure Global Routing parameters.

1. Select the *Networking Tab* from the System Setup dialog.
2. Select *IP Routing* from the *Network Item* list.
3. Select the protocol: None, RIP or OSPF from the routing protocol drop down list.
4. Configure options for the selected protocol.

Configure Interface Routing parameters.

5. Enable routing for the LAN and WAN interfaces.
6. Configure protocol interface options for the LAN and WAN interfaces.

On a managed network It is only necessary to enable a routing protocol on the LAN Ethernet interface on the gateway node. The gateway node connects to a management console, requiring only a one physical Ethernet connection to the IMUX 2000s network. The management console can then manage any of the nodes in a 2000s network via the DCC (Data Communications Channel)

Static routes can be used in conjunction with RIP. The network administrator will likely enter static routes into a managed network to reach networks beyond that of the gateway.

4.2.2.1.1 RIP Global Settings

Figure 4-7 displays RIP as the selected protocol. This dialog displays the global configuration parameters that RIP will use on either the LAN or WAN interfaces. Note that Figure 3-2 shows the default and recommended parameters. These parameters can be changed to interoperate with other manufacturer's equipment.

RIP can only be used as the routing protocol for a maximum of 15 hops (nodes). If the size of the network exceeds 15 hops then OSPF should be used.

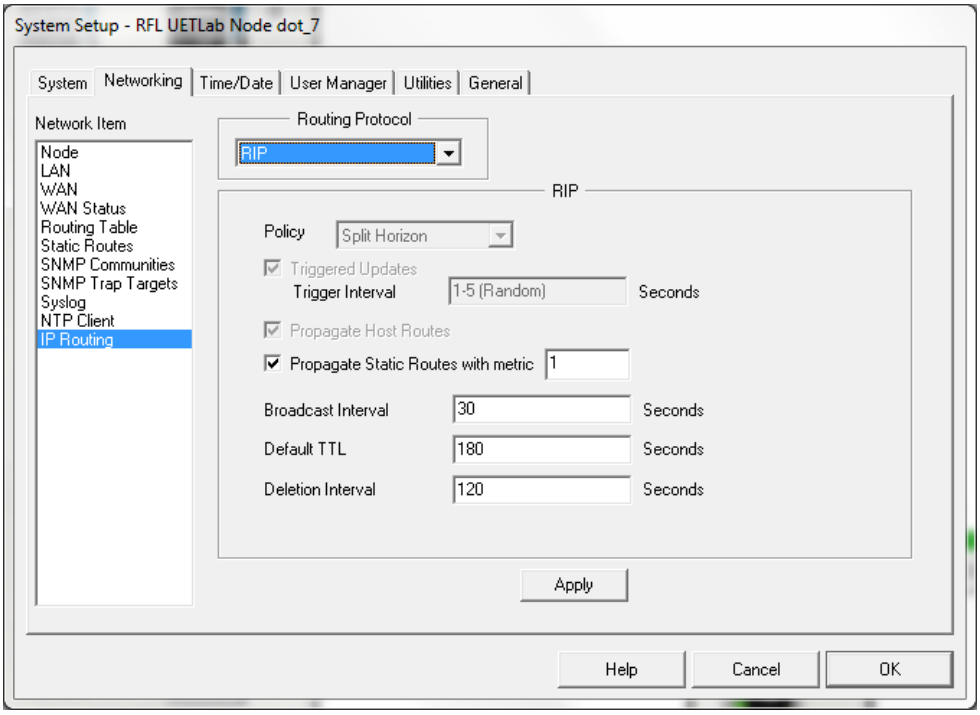


Figure 4-7. Rip Global Settings

Table 4-5 RIP Global Setting

Propagate Static Routes	Static routes created in the *Static Routes* panel will be propagated via RIP if enabled.
Broadcast Interval	The frequency of RIP announcements.
Default TTL	This setting specifies the time-to-live (TTL) for routes that are learned from other routers through RIP. Routes that do not update before they exceed the specified TTL are marked as invalid.
Deletion Interval	Specifies the amount of time a route will remain in the routing table before it expires and is removed

4.2.2.1.2 OSPF Global Settings

The figure below displays OSPF as the selected protocol. This dialog displays the global configuration parameters that OSPF will use on either the LAN or WAN interfaces. Note that Figure 4-8 is showing the default and recommended parameters. These parameters can be changed to interoperate with other manufacturers' equipment.

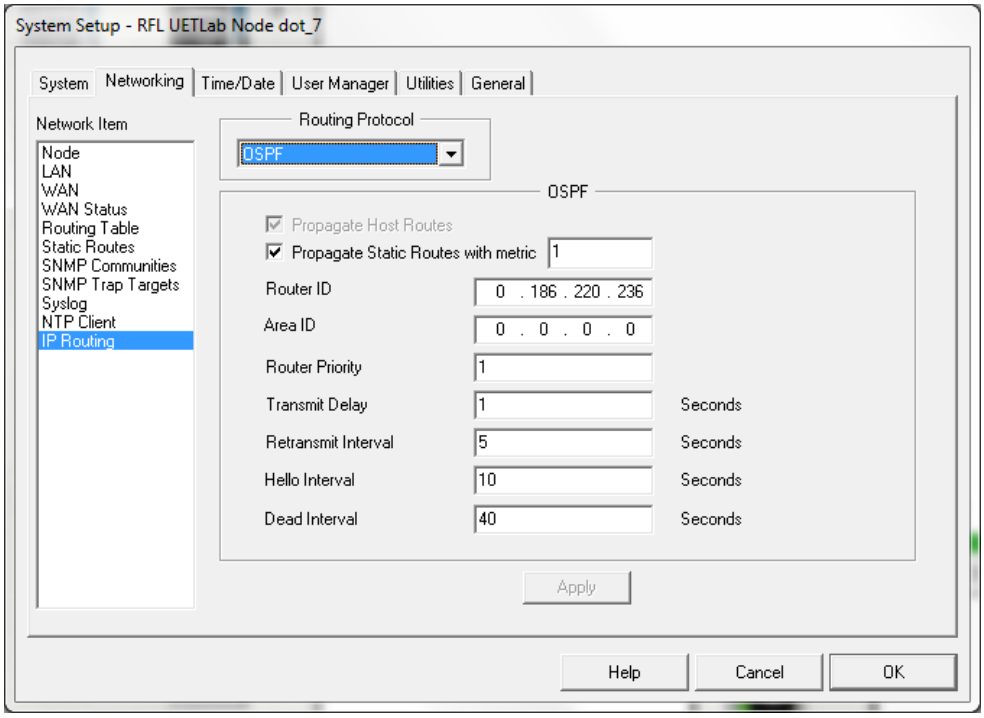


Figure 4-8. OSPF Global Settings

OSPF global configurable parameters:

Propagate Static Routes Static routes created in the *Static Routes* panel will be propagated via OSPF if enabled.

Router ID A 32-bit number that uniquely identifies this router in the AS (Antonymous System). This field is automatically populated with an ID derived from the system motherboard serial number and is therefore unique for the IMUX 2000s. This can be changed to any 32 bit number but must be unique within the network.

Area ID The Area ID of the area to which the attached network belongs. All routing protocol packets originating from the interface are labeled with this Area ID.

Router Priority An 8-bit unsigned integer. When two routers attached to a network both attempt to become Designated Router, the one with the highest Router Priority takes precedence. A router whose Router Priority is set to 0 is ineligible to become Designated Router on the attached network. Advertised in Hello packets sent out this interface.

Transmit Delay The estimated number of seconds it takes to transmit a Link State Update Packet over this interface. LSAs (Link State Advertisements) contained in the Link State Update packet will have their age incremented by this amount before transmission. This value should take into account transmission and propagation delays; it must be greater than zero.

Retransmit Interval The number of seconds between LSA retransmissions, for adjacencies belonging to this interface. Also used when retransmitting Database Description and Link State Request Packets. This parameter must have the same value set for all nodes in the network.

Hello Interval The length of time, in seconds, between the Hello packets that the router sends over the interface. This parameter must have the same value set for all nodes in the network.

Dead Interval The number of seconds before the router's neighbors will declare it down, when they stop hearing the router's Hello Packets. This parameter must have the same value set for all nodes in the network.

4.2.2.1.3 Configure LAN VRRP

When a LAN IP address has been entered and a connection is reestablished with the node, VRRP can be enabled as follows.

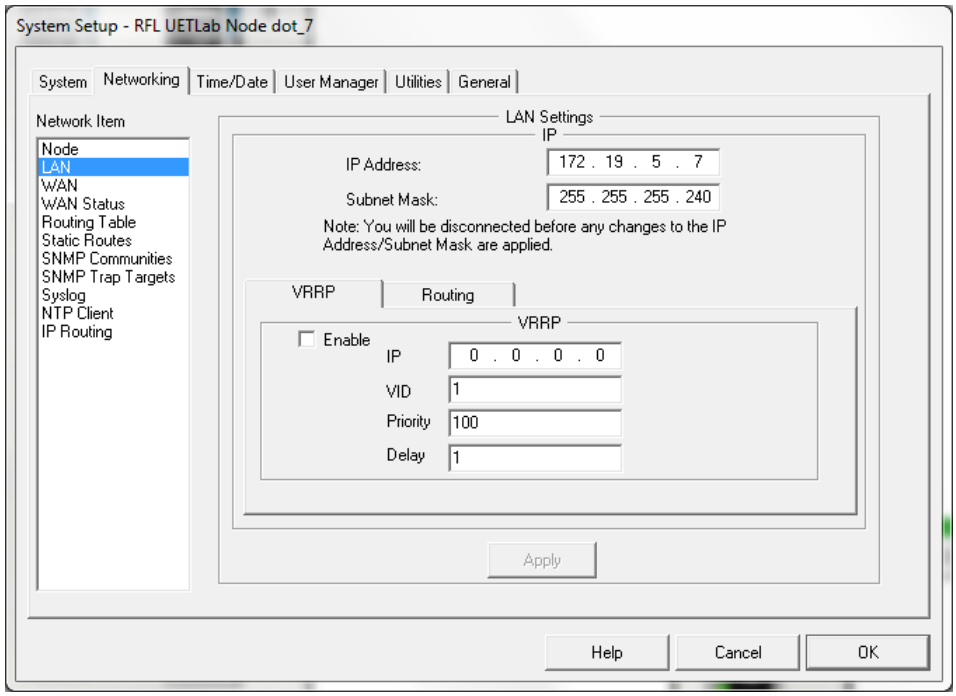


Figure 4-9. VRRP System Set-up – Networking

VRRP (Virtual Router Redundancy Protocol)
Note that the default values are shown; RFL recommends that these be used.

IP	Insert the VID IP number
Enable	Click to enable the VRRP protocol
VID	VRRP ID, the default is 1
Priority	1-254, 100 is the default
Delay	The default value is 1, can be changed

The user should verify that VRRP is working.

4.2.2.1.4 Configure LAN OSPF

When a LAN IP address has been entered and a connection is reestablished with the node, OSPF can be enabled as follows.

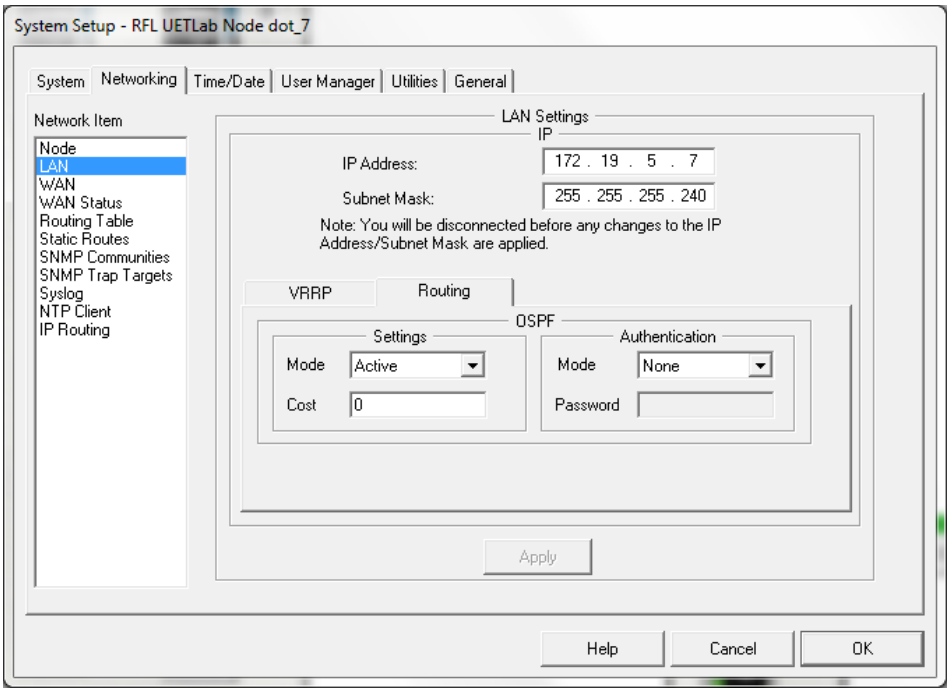


Figure 4-10. Configure LAN OSPF

Mode — Default: Passive

Set the Mode to *Active* if OSPF packets are required to be sent from this Interface. If the IMUX 2000s is required to exchange routes with another OSPF Speaker directly connected to this Interface, then *Active* should be selected. Otherwise, select 'Passive'.

.

Cost — A default Cost of 0 implies that the OSPF Shortest Path Calculations will be based on the bandwidth of the link connected to the Interface. Otherwise, the Shortest Path Calculations will be based on the face-value of the non-zero Cost. The default of 0 is recommended.

Authentication — Specify that simple password authentication should be used for the given area.

4.3 Setting Static Routes

4.3.1 Routing Table Flags

Table 4-6 Routing Table Flags

Flag	Definition	Description
C	Connected Route	A directly connected route, route to an adjacent node.
G	Gateway Route	Indirect route via Gateway Route via a distant node
I	ICMP Route	ICMP redirect dynamic route. An IP router (or other node) has updated this node's route table with information contained in an ICMP packet for a direct route
N	SNMP Route	Entry via SNMP MIB II. An IP router has updated this node's route table with information contained in an SNMP packet
O	OSPF Route	Route learned from OSPF. An IP router (or other node) has updated this node's route table with information contained in an OSPF routing protocol update
P	Private Route	This is a route private to this node and will not be exchanged with other nodes
R	RIP Route	Route learned from RIP. An IP router (or other node) has updated this node's route table with information contained in an RIP routing protocol update
S	Static Route	This is a route that has been manually generated or as part of the node boot sequence
T	Temporary route	This is a temporary route
Z	Zombie route	The interface that this route relates to is no longer active
?	Unknown Route	Route of unknown origin

4.3.2 Static Routes

Static routes are entered through the Static Routes dialog below.

A managed network of IMUX 2000S can be configured using static routes, however, if the network topology is "protected", the network will not converge in the advent of network failure and a connection to one or many nodes will be lost.

Static routes can be used in conjunction with RIP or OSPF. The network administrator will likely enter static routes into a managed network to reach networks beyond that of the gateway.

The routing table can be sorted on any of the columns by clicking the column heading.

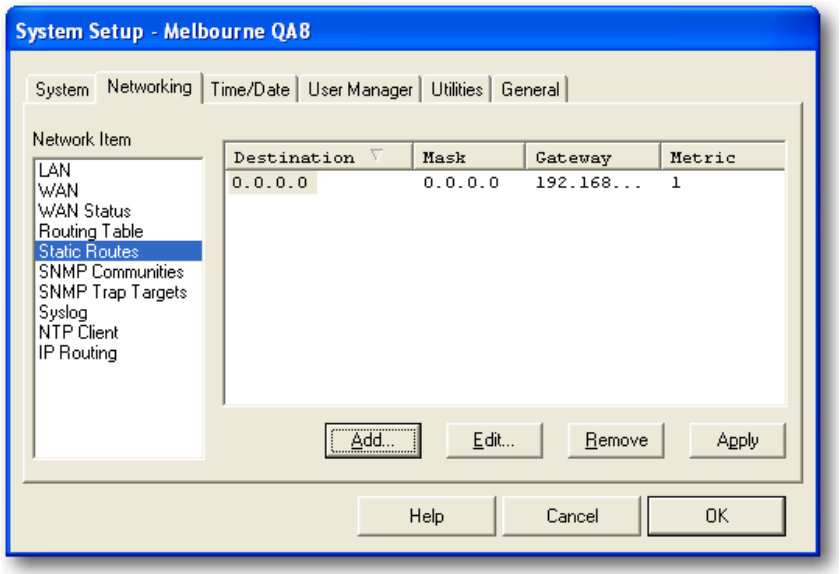


Figure 4-11. Static Routes Dialog

Section 5. System Functions Menu

The System Setup button in the IMUX 2000s EMS main window will open the system setup window. Each tab in this window is used to configure a set of system parameters.

5.1 System

This dialog allows the user to view system information of the node currently connected to the management system. The system dialog allows the operator to name the node, and add location and contact information. The name entered is displayed at the top left of the Main Window. The name given appears in all IMUX 2000s EMS dialogs after being saved.
In this example "RFL SONET Node P4" will appear in all system dialogs.

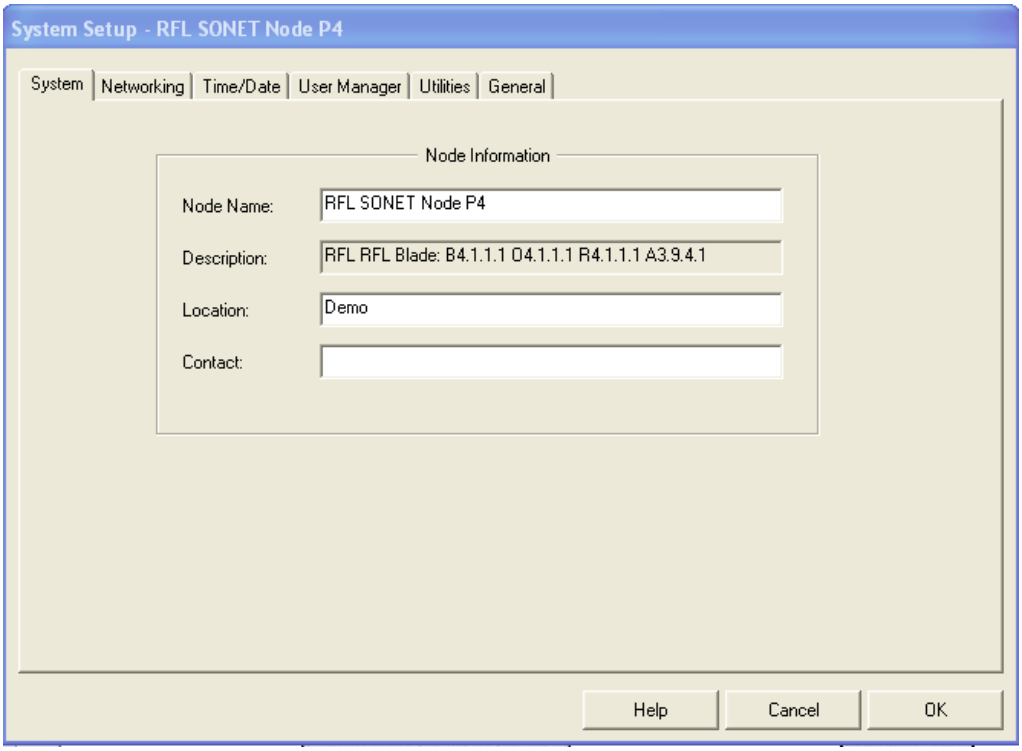


Figure 5-1. System Set-up Dialog

5.2 User Access Manager

The *User Manager* tab allows a network administrator to add/delete/change user profiles. The login name, level, and days remaining of all current user profiles are displayed.

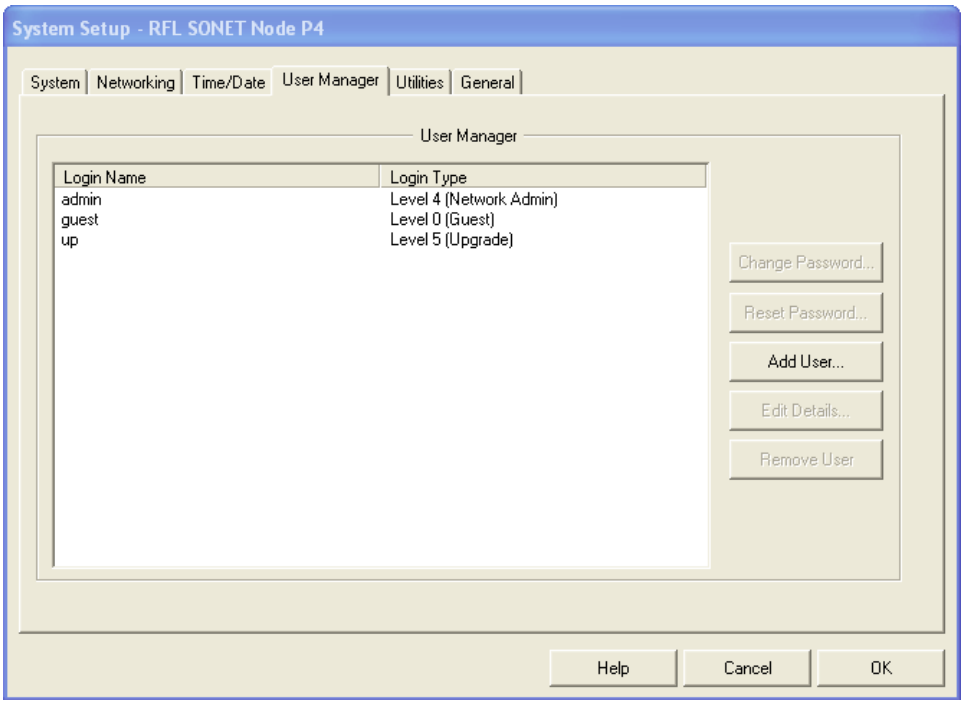


Figure 5-2. User Manager

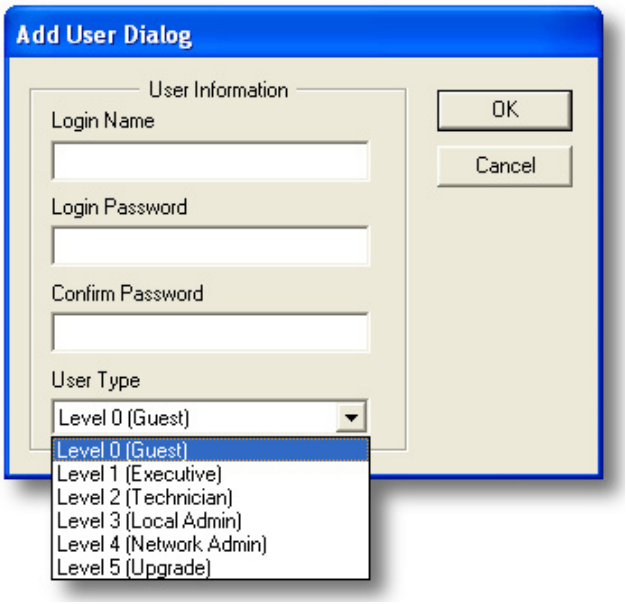


Figure 5-3. Add User Dialog

The factory default profile is username ***"admin"*** and no password. Logging in with the default admin profile will then allow the user to define a number of other profiles.

The *Add User* button in the *User Manager* tab will allow any user logged in as a level 4 or network administrator user to create a new profile. The add user dialog is shown in Figure 3-13. The administrator may enter the name, password and user level of each profile.

There are six operator profiles. The table below displays read or access to various parts of the application.

Table 5-1 Operator Profile Summary

Suggested Application	**Guest**		**Executive**		**Technician**		**Local administrator**		**Network administrator**		**Upgrade**	
ACTIVITY	Level 0		Level 1		Level 2		Level 3		Level 4		Level 5	
	Read	Write	Read	Write	Read	Write	Read	Write	Read	Write	Read	Write
Main IMUX 2000s EMS summary	✔		✔		✔		✔	✔	✔	✔		
IM configurations			✔		✔		✔	✔	✔	✔		
SS cross connect VC/VT			✔		✔		✔	✔	✔	✔		
Small DACS			✔		✔		✔	✔	✔	✔		
Event Log			✔		✔		✔	✔	✔	✔		
Trunk, APS and clock			✔		✔		✔	✔	✔	✔		
Initiate diagnostics			✔		✔	✔	✔	✔	✔	✔		
Set Window (IP/SNMP/time)			✔		✔		✔		✔	✔		
Reboot IM							✔	✔	✔	✔		
User accounts Management									✔	✔		
IMUX 2000s EMS Upgrade									✔		✔	✔
Device List							✔		✔		✔	✔
Reboot Node									✔	✔	✔	✔

Guest is a special profile that might be used by a non employee such as a contractor. In addition, this profile has a hard coded **10 second** timeout after use.

5.3 System Upgrade and Backup

The “Utilities” tab allows administrations to execute software system reboots, backup and restore of system configuration and the ability to reset the node to Factory Default.

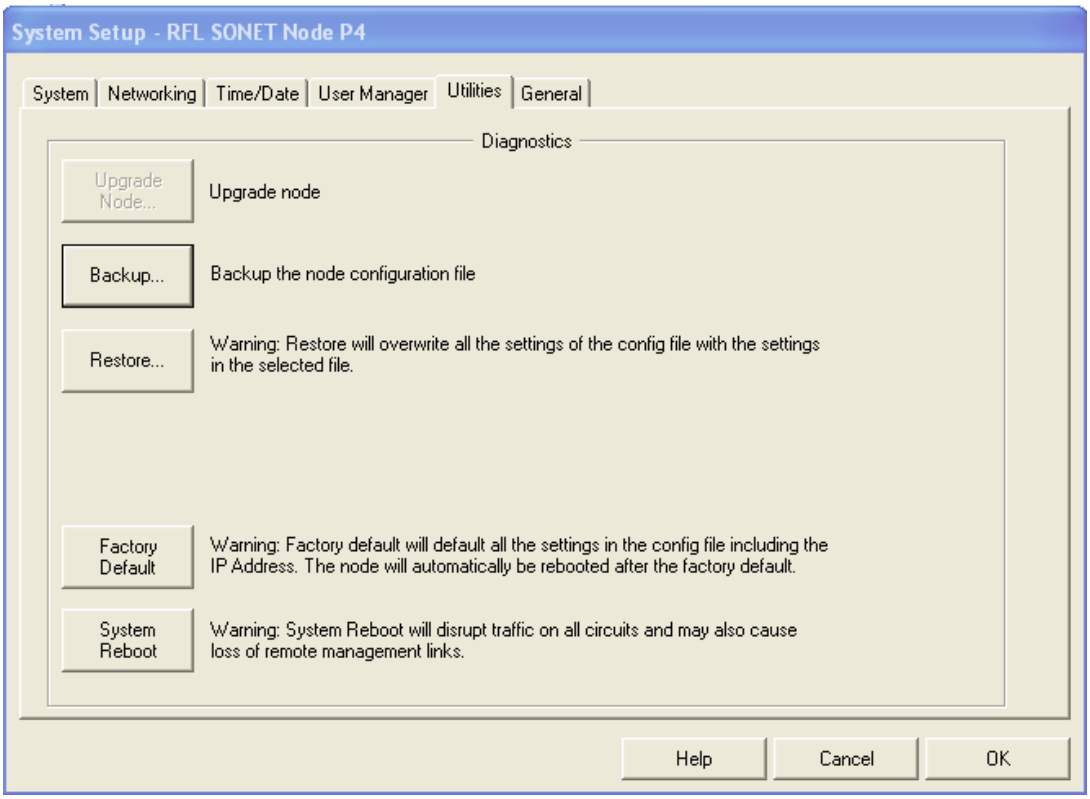


Figure 5-4. System Setup - Utilities

Pressing the ***Upgrade Node*** button will bring up a window that allows users to select a RFL upgrade (Service Pack) package file (*.HPK) to run a software upgrade on the IMUX 2000s . A reboot of the node will be required after the new software is installed.

You must be logged onto the node with Level 5 (Upgrade) privileges. See Section 3.3 User Manager.

The ***Backup*** button allows the user to backup by saving the complete network configuration.

The ***Restore*** button allows a previously saved node configuration to be loaded and will replace the current configuration. After loading a reboot is requested by the GUI. The restore feature can simplify the roll out of a large network as a configuration template can be created and imported into each node. Minor node specific address changes will need to be made to each node prior to activation.

The ***Factory Default*** button will remove any configuration information supplied and reset the node to the same configuration state as when the node was manufactured.

5.4 System Downgrade

The node can be downgraded by installing an earlier or previous service pack. The procedure is exactly the same as upgrading a node. See the previous Section 3.4 System Upgrade and Backup.

5.5 General Settings

The general property of the system setup allows the user to Save Position on Exit and Display Tooltips. Refer to the Figure below.

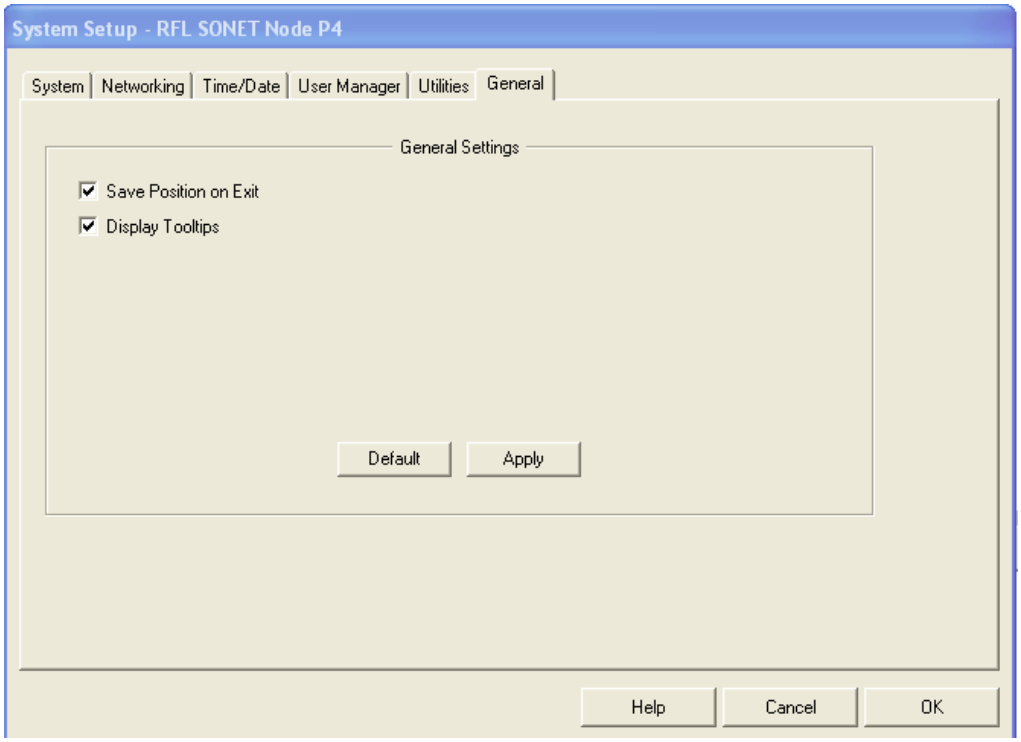


Figure 5-5. System Setup – General Dialog

Save Position on Exit: The user has the ability to alter the size and the position of the main window of IMUX 2000s EMS. *Save Position on Exit* Allows the user to save the size and placement of the main window. After exiting and re-opening IMUX 2000s EMS the position and size has not changed.

Display Tooltips: Enables and disables mouse over Tooltips. Usually found on interface ports and the Cross Connect window.

Default Button: Enables both properties, *Save Position on Exit* and *Display Tooltips.*

5.6 System Information

Log into the node, press “System Info” from the main screen and then press the “More Info” button as required.

Section 6. SONET Module Event Logging

System Event logging is implemented in the IMUX 2000s via the following methods:

- **IMUX 2000s EMS Event Log** (see below)
- **Syslog** (see section 6.2)
- **SNMP traps** (see section 7)

All events generated by the IMUX 2000s, are shown in the Event Log and are sent as Syslog messages. See Syslog below.

The Event Log acts as a FIFO (First In First Out) buffer. As the buffer has a finite amount of capacity to save event notifications, old events will be dropped to make way for new events. If the network operator wishes to save a history of events, this is best achieved with the use of Syslog.

6.1 EMS Event Log

IMUX 2000s EMS includes an Event Log that reports all system events and alarms generated by the connected node. See the Figure below.

To view the event log:
Log into a IMUX 2000s node and press the *Event Log* button at the top left of the main screen.

Refresh the event log:
When the *Event Log* is first opened, the contents of the event list will be empty until the log is refreshed. The log is refreshed by clicking the refresh button in the top right hand side of the dialog.

6.1.1 Event Categories

The event log can display all events in a single list, or can display system events/alarms in predefined categories by selection of the appropriate tab in the Event Log dialog.

The Event Log categories are:

Table 6-1 Operator Profile Summary

Port Alarms	Alarms the occur on any 800 interface port.
Sytem Alarms	Any alarm generated by the 800 internal system.
SONET/SDH Alarms	Alarms that correspond to any SONET/SDH specific event, excluding Protection switching and SONET/SDH clock alarms.
Clock Alarms	Alarms that relate to SONET/SDH clock source (synchronisation clock)
APS Alarms	Alarms that report SONET/SDH Protection Switching events.
Users	Any user event recorded by the system. Example: Logging in or out of the system.

6.1.2 Interpreting the Event Log

IMUX 2000s EMS uses the icons in table below to easily convey the meaning and severity of system events and alarms.

Table 6-2 IMUX 2000s EMS Event Log Icons

ICON	Colour	Description
	Red	Alarm severity - Critical
	Yellow	Alarm severity - Minor
	Green	Alarm severity - Normal (no alarm)
	Gray	Alarm severity - Disabled or alarms masked by other alarms.
	White	Alarm severity - Informational
		Interface Module Event - Information
		Information - General
		Root event - First line of the event log (root of the tree).
		Scripting Event
		Session(communications) event
		System generated
		Time stamp
		User log in
		User log out

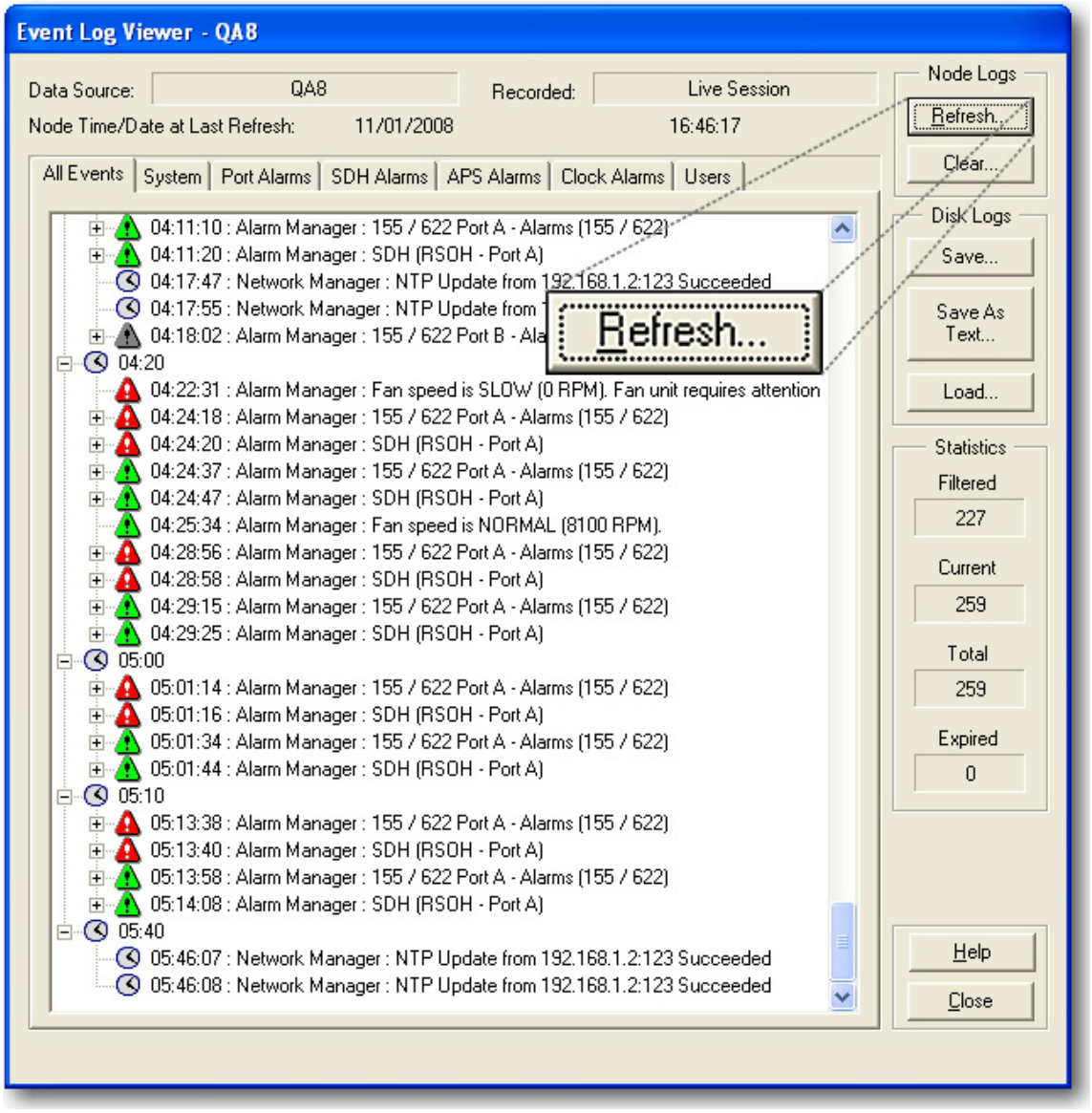


Figure 6-1. IMUX 2000s EMS Event Log – All Events

The Event Log can also be saved as a text file for analysis at a later date.

6.2 Syslog

The IMUX 2000s can be configured as a Syslog client to send Syslog messages to a Syslog server. The Syslog server would under most circumstances be a management console used to perform network and element management for a network of IMUX 2000s units

6.2.1 Configure Syslog

Syslog is configured from the main screen via:

System Setup ⇨ Networking Tab ⇨ Syslog

1. Enter the **IP Address** of the Syslog server to receive the messages.
2. Choose a **Facility Code** to append and categorise your messages.

6.2.2 Syslog Server

Below is a screen shot of a free Syslog server configured to receive Syslog messages from a IMUX 2000s. The server, *Kiwi Syslog Daemon*, is freely available over the internet.

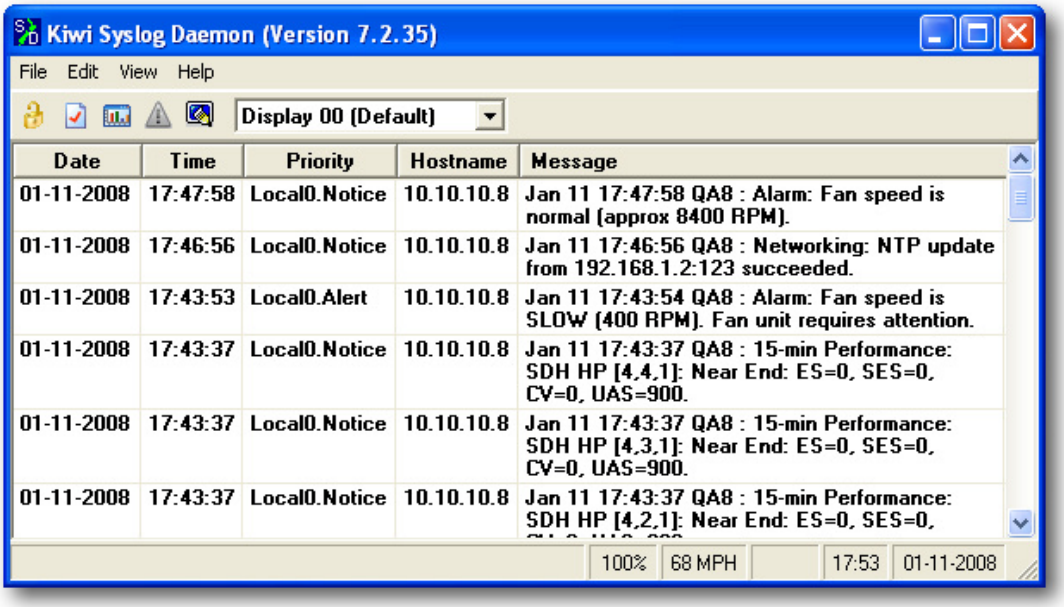


Figure 4-12. Syslog Message Capture

Section 7. SONET Module Management via SNMP

SNMP (Simple Network Management Protocol) Version 1 is implemented in the IMUX 2000s to execute system configuration (**gets** and **sets**), and to receive status information about the nodes as alarms (**traps**).

7.1 Locating the MIB Table

IMUX 2000s ship with an accompanying MIB (Management Information Base) which describes all SNMP objects.

The MIB, is an ASCII text file that describes SNMP network elements (IMUX 2000s nodes) as a list of data objects, using Descriptors and Identifiers. Think of it as a dictionary of the SNMP language, every object referred to in an SNMP message must be listed in the MIB.

The fundamental purpose of the MIB is to translate numerical strings into human-readable text. When an SNMP device sends a Trap or other message, it identifies each data object in the message with a number string called an object identifier, or OID. The MIB provides a text label for each OID. Your SNMP manager uses the MIB as a codebook for translating the OID numbers into a human-readable display.

7.2 Access via SNMP Communities

SNMP communities are used to define and set system access privileges.

SNMP communities are created and assigned **read**, **write** or **read/write** privileges.
The IMUX 2000s factory default community name is: **public** with **read** access.

To configure SNMP communities:

System Setup ⇨ Networking Tab ⇨ SNMP Communities

1. Enter a **Community name**.
2. Assign **read**, **write** or **read/write** access.

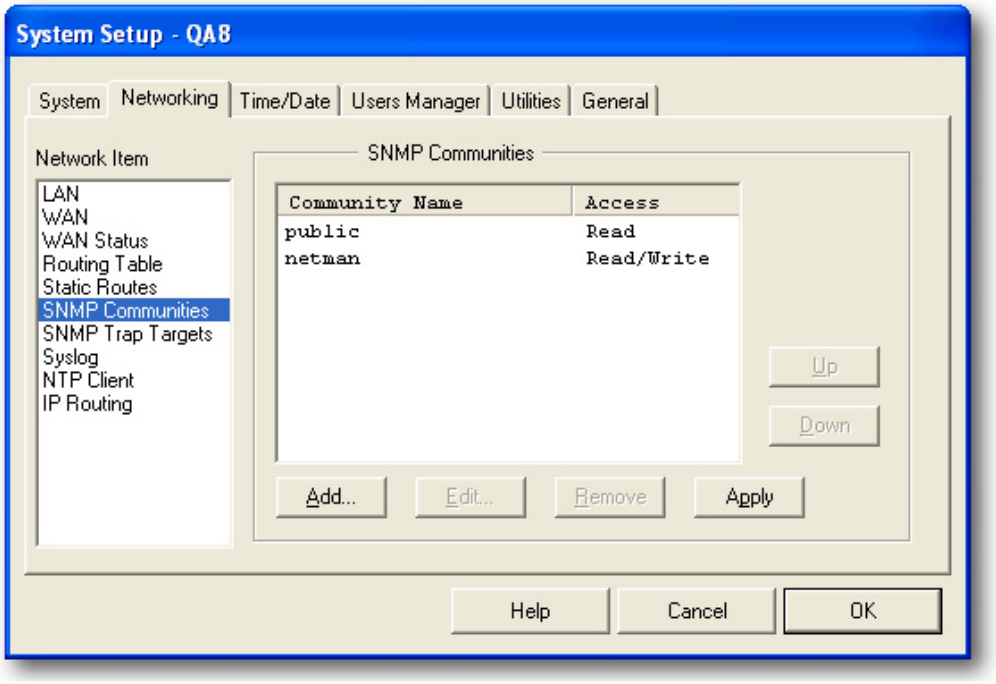


Figure 5-6. SNMP Communities

7.3 Sonet Module Configuration Using SNMP

The IMUX 2000s can be fully configured via SNMP Version 1. All system options (configuration items) that are set using IMUX 2000s EMS can also be set via SNMP.

To configure a IMUX 2000s via SNMP, a copy of the IMUX 2000s MIB must be loaded or compiled into a SNMP manager. The manager will display a list of MIB objects graphically as an inverted spanning tree.

It is beyond the scope of this manual to cover all MIB objects in detail. If you require further information, compile or load the MIB into a SNMP manager. Or you can read the object descriptions and identifiers directly by opening the MIB with a text editor/viewer.

The IMUX 2000s can only be configured via SNMP if a **community name** created and is assigned **write** access. The SNMP manager communicates with the node using the same community name. **Read** access is also required to be able to validate any configuration changes made.

7.4 Alarm Reporting using SNMP

The IMUX 2000s sends some alarm notifications as SNMP Traps. In a managed network, traps are sent from many nodes to a single management console. This allows the network operator to manage one to many networks from a centralized location.

Intelligence can also be built into a managed network with the use of SNMP management software. The software can be configured to create relationships between network elements providing a network centric view which will identify running services, and not isolated nodes.

Traps are more likely to be of interest to network operators so a description of the IMUX 2000s traps are included in this manual. These descriptions can also be read directly from the IMUX 2000s MIB.

Table 5-2 IMUX 2000s Trap Descriptions

SNMP Trap	Description
IMUX2000sSystemAlarmNotification	Indicates a state change in the systemAlarmStatus object.
IMUX2000sSdhSonetClockSwitch	Indicates SONET/SDH clocking has switched to a different source.
IMUX2000sSwitchActiveLine	Indicates the receiving line switched over to another line.
IMUX2000sSwitchActivePath	Indicates the receiving path has switched over to another channel
IMUX2000sSectionAlarmNotification	Indicates a state change in the value of the sectionCurrentAlarmStatus object, caused by a bit changing from 0 to 1 (alarm triggered) or 1 to 0 (alarm cleared).
IMUX2000sLineAlarmNotification	Indicates a state change in the value of the lineCurrentAlarmStatus object, caused by a bit changing from 0 to 1 (alarm triggered) or 1 to 0 (alarm cleared).
IMUX2000sPathAlarmNotification	Indicates a state change in the value of the pathCurrentAlarmStatus object, caused by a bit changing from 0 to 1 (alarm triggered) or 1 to 0 (alarm cleared).
IMUX2000sVtAlarmNotification	Indicates a state a change in the value of the vtCurrentAlarmStatus object, caused by a bit changing from 0 to 1 (alarm triggered) or 1 to 0 (alarm cleared).
IMUX2000sE1AlarmNotification	Indicates a change in the value of any E1 alarm.
IMUX2000sT1AlarmNotification	Indicates a change in the value of any T1 alarm.
IMUX2000sEthernetAlarmNotification	Indicates a change in the value of any Ethernet alarm.
IMUX2000sDs3AlarmNotification	Indicates a change in the value of any Ds3 alarm.
IMUX2000sStmAlarmNotification	Indicates a change of STM-n/OC-n alarm.

7.4.1 Setting SNMP Trap Targets

To receive SNMP Traps the IMUX 2000s must be configured with one or more IP addresses of a SNMP manager (or other trap receiving software) running on a computer that is reachable via TCP/IP. See below.

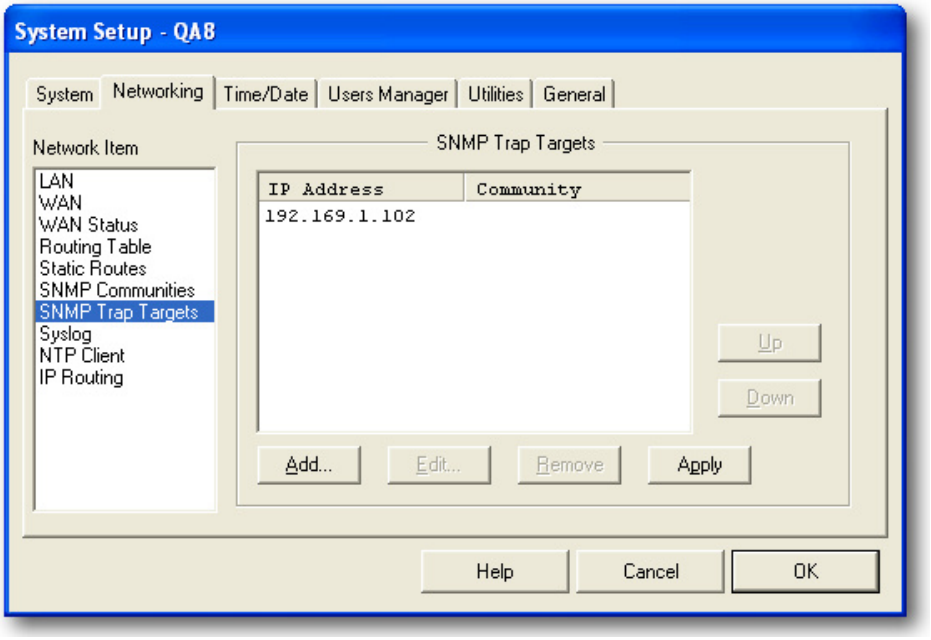


Figure 5-7. SNMP Trap Targets

7.4.2 Receiving IMUX 2000s Traps

For smaller networks, a functionally rich and expensive management system may not be necessary, or may not be cost effective.

Many free trap receivers are available over the internet and may be used to receive alarm notifications. Most free trap receivers will load or compile the IMUX 2000s MIB and will produce human readable notifications.

Section 8. Clock

The IMUX 2000s can be configured to generate an internal “master” network clock using its integrated Stratum 3 (4.6 ppm) clock. It can also obtain clocking from external sources:

- Trunk Ports
- T1/E1 circuit

Below is a figure of the clock configuration window. This can be accessed by pressing the **Clock** button on the main front GUI window.

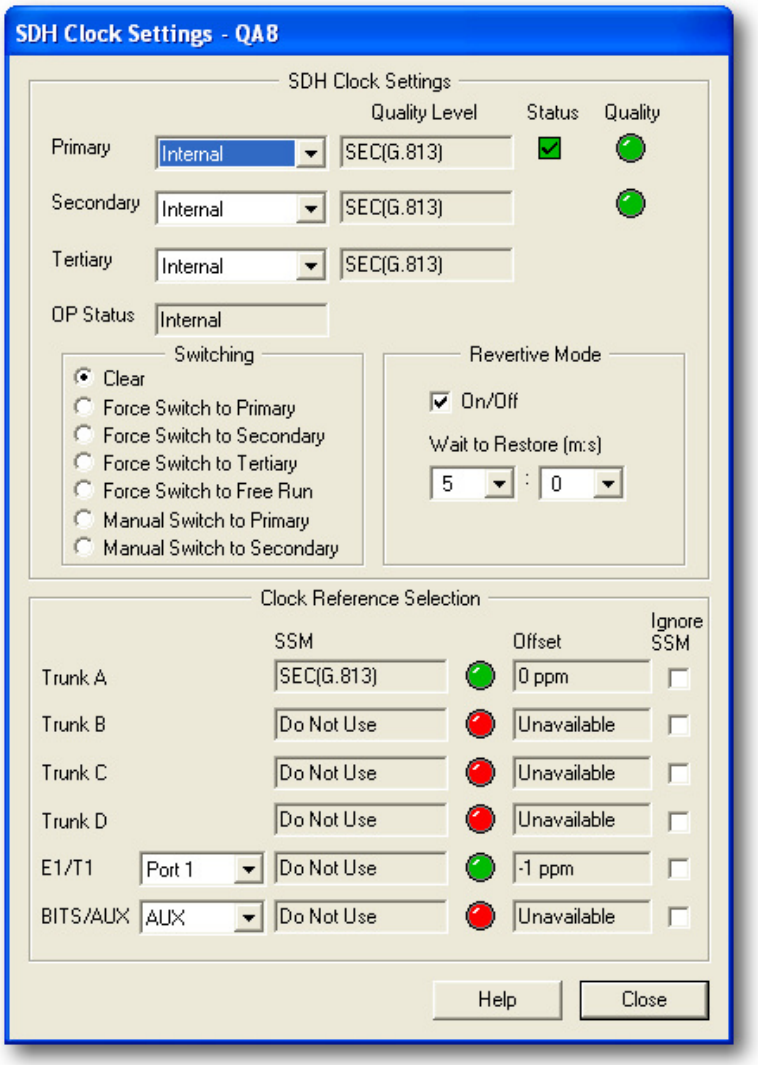


Figure 8-1. Clock Configuration Window

The primary and secondary clock references can be chosen from the internal clock or any of the clock sources in the **Clock Reference Selection** section. The Clock Reference Selection section describes where the clock source is obtained from, what type of clock type it is, the quality and accuracy of the clock source.

8.1 Clock Hierarchy

Primary	The node will first attempt to use the clock source selected as the Primary.
Secondary	If the primary clock cannot be recovered, the node will then attempt to recover the clock source selected as the Secondary.
Tertiary	If the secondary clock cannot be recovered, the node will then attempt to recover the clock source selected as the Tertiary.

The green "tick" icon identifies the current clock source in use. If the **Revertive** box is ticked, the active clock will switch from tertiary/secondary back to secondary/primary after a switch over when the clock quality of the clock source is within specification and the configured timer has expired.

8.2 Clock Types

8.2.1 Internal

This is a free running clock that is based on our internal Stratum 3 +/- 4.6 ppm TCXO. In this mode the PLL (Phase Locked Loop) is not locked to any external clock source. This clock is a valid G.813 synchronization source for a Stratum 3 SONET/SDH system.

8.2.2 Holdover

If the PLL has been locked to a valid reference and that valid reference has gone, the PLL can go into Holdover. This means that it will find the last time that reference was valid and hold the PLL to that frequency unless told to do otherwise. It will holdover to the G.813 specs for a Stratum 3 clock.

8.3 SSM

The clock source can be configured to *Ignore SSM* (Synchronization Status Messaging). SSM is a SDH SONET protocol used to convey information about the timing (clock) reference.

Ignore SSM can be enabled for interoperation with equipment that does not support SSM.

Section 9. Troubleshooting

9.1 USB Driver Installation on Windows XP

In some circumstances, the USB driver fails to fully install during the IMUX 2000s EMS installation process. This is due to the software configuration of the machine on which the IMUX 2000s EMS is to be installed.

The figure at right shows that the MSP USB Comm driver is unavailable.

To install the driver manually, follow the steps below.

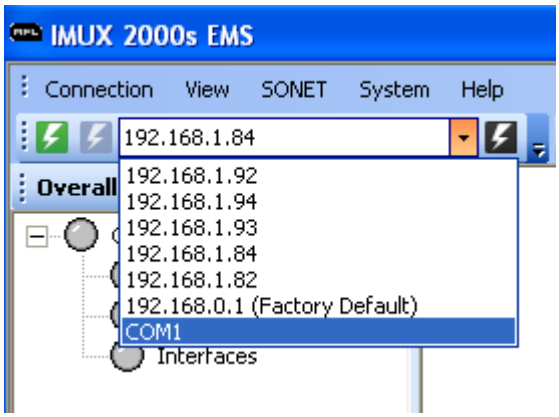


Figure 9-1. MSP USB Driver Unavailable

1. Click *Start* then right click on *My Computer* then click on *Manage*.

Figure 9-2. Manual USB Driver Install Step 1

2. Click on *Device Manager* in the left column, then right click on *MSPP USB-to-Serial Comm Port Driver*, then select *Update Driver*. Note the yellow exclamation mark over the driver.

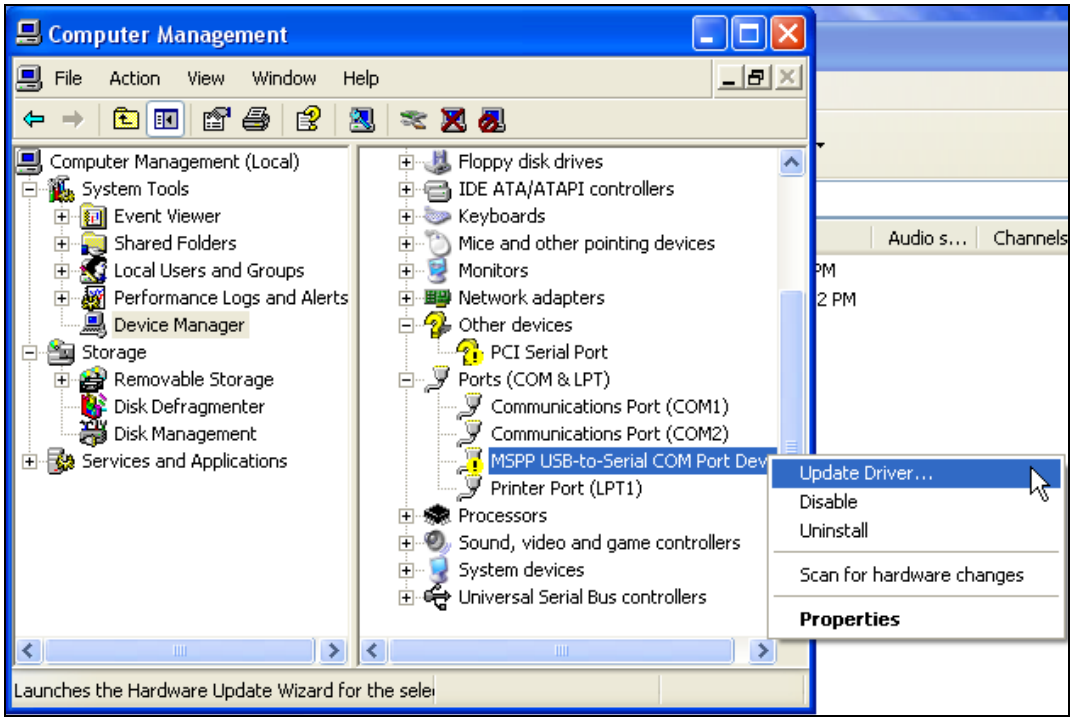


Figure 9-3. Manual USB Driver Install Step 2

3. Select the *No, not this time* radio button, then click *Next*

Figure 9-4. Manual USB Driver Install Step 3

4. Select *Install from a list or specific location(Advanced)*, then click *Next*.

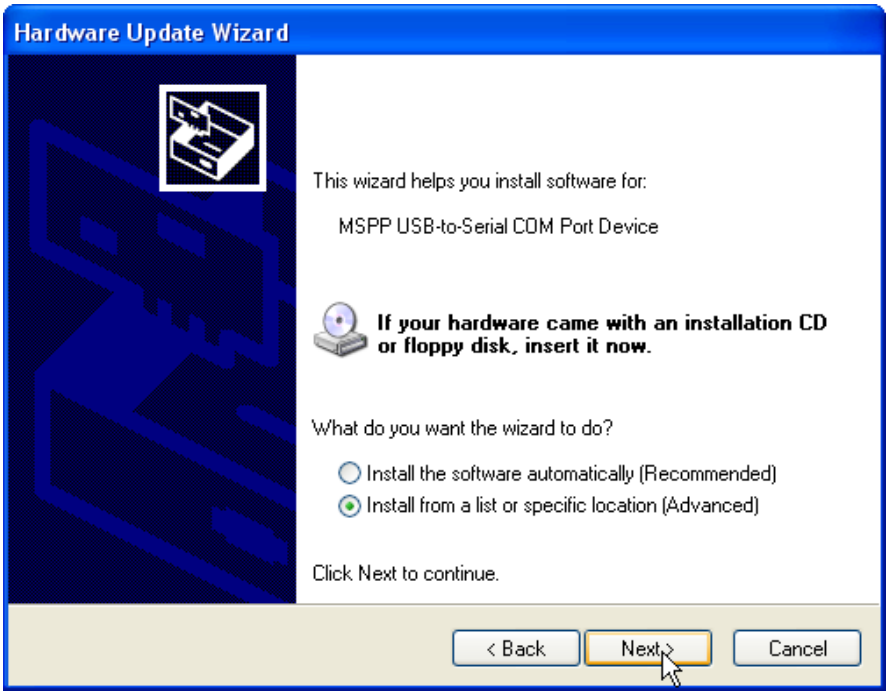


Figure 9-5. Manual USB Driver Install Step 4

5. Select *Search for the best driver in these locations*, then select *Include this location in the search*, then either browse to c:\IMUX 2000s EMS\Drivers\Win2k_KP (or to wherever you installed IMUX 2000s EMS) or type it into the combo box, then click *Next*.

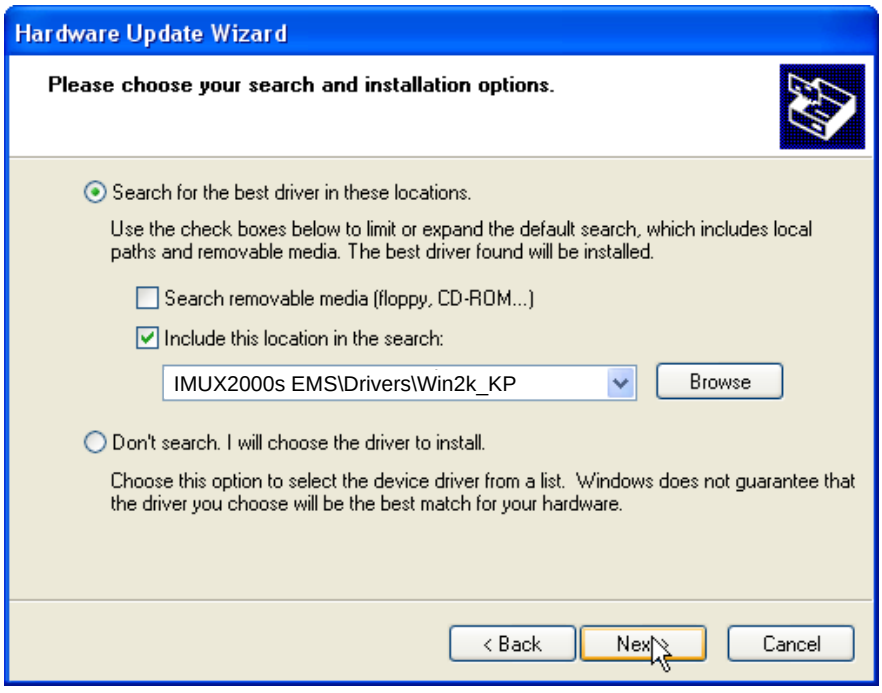


Figure 9-6. Manual USB Driver Install Step 5

6. Click *Continue Anyway*.

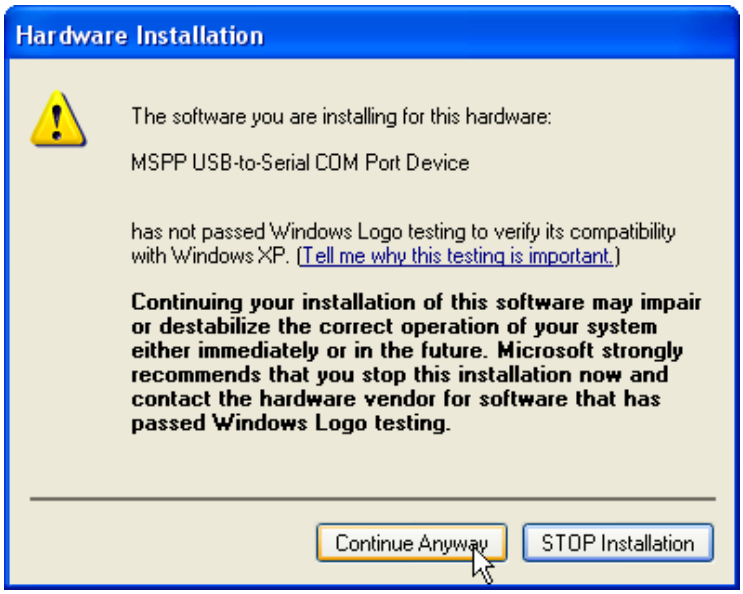


Figure 9-7. Manual USB Driver Install Step 6

7. Click *Finish*

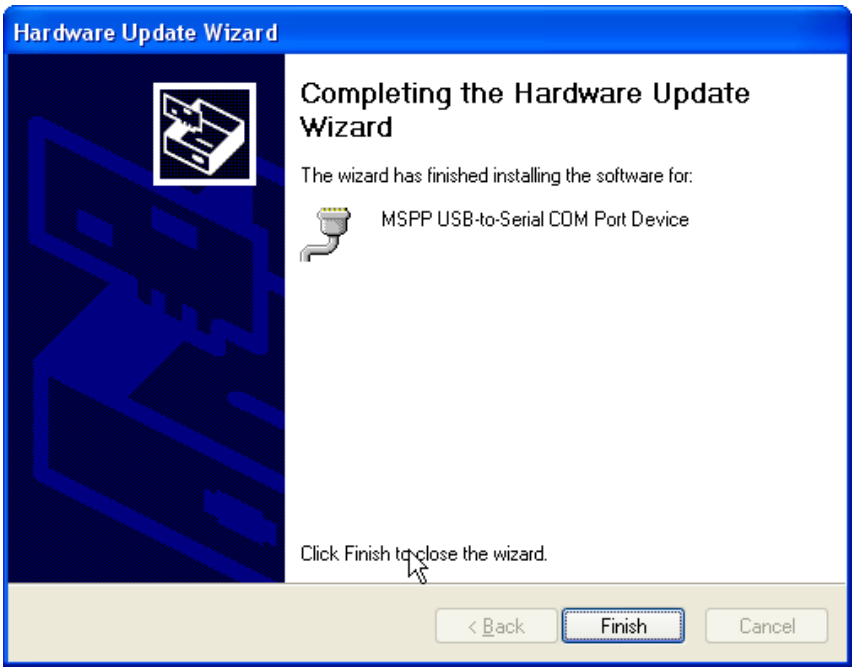


Figure 9-8. Manual USB Driver Install Step 7

8. Note the exclamation mark is now gone. The driver is now installed.

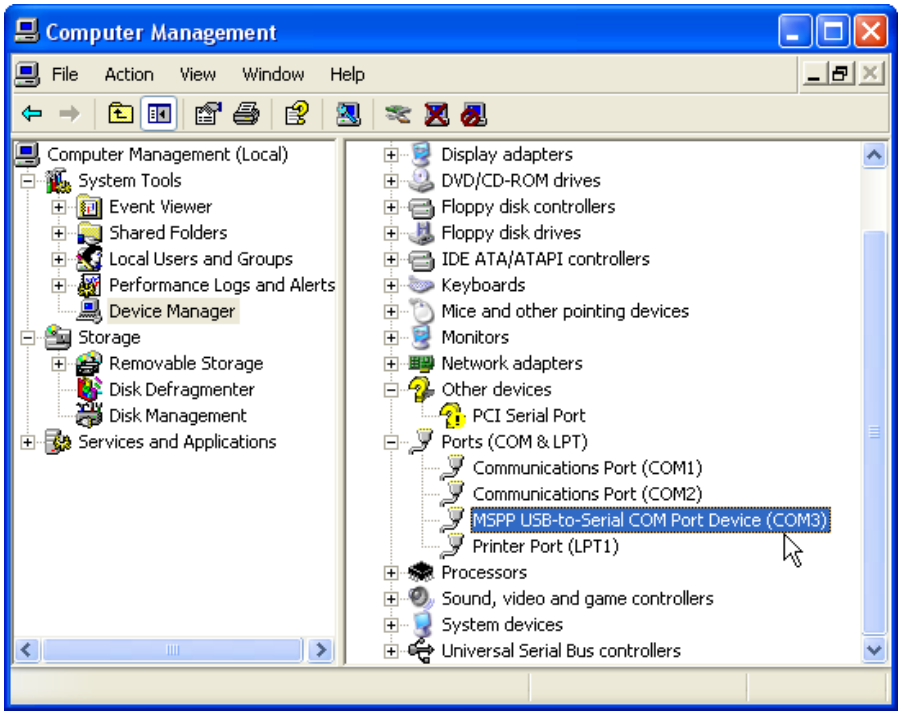
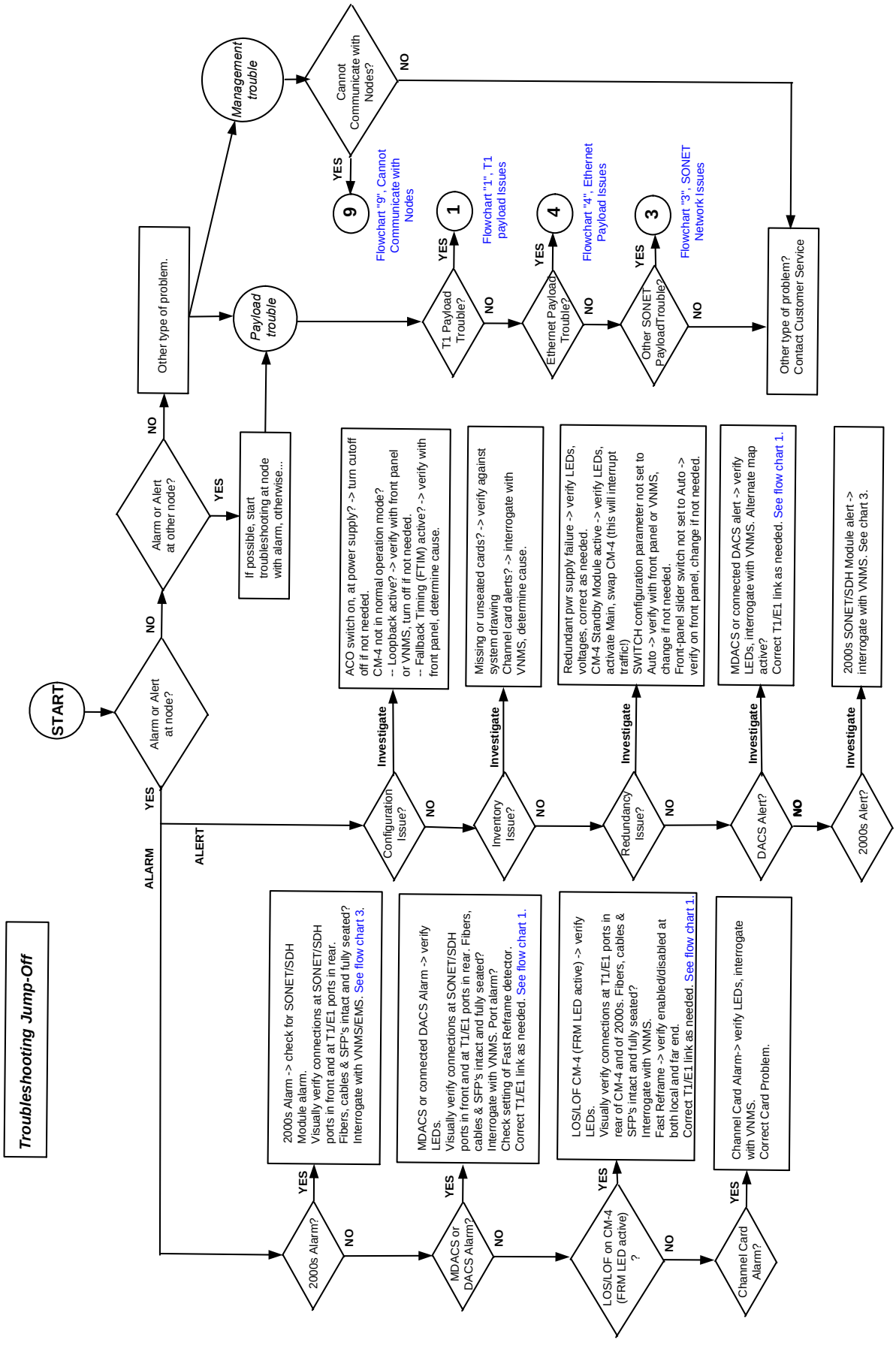
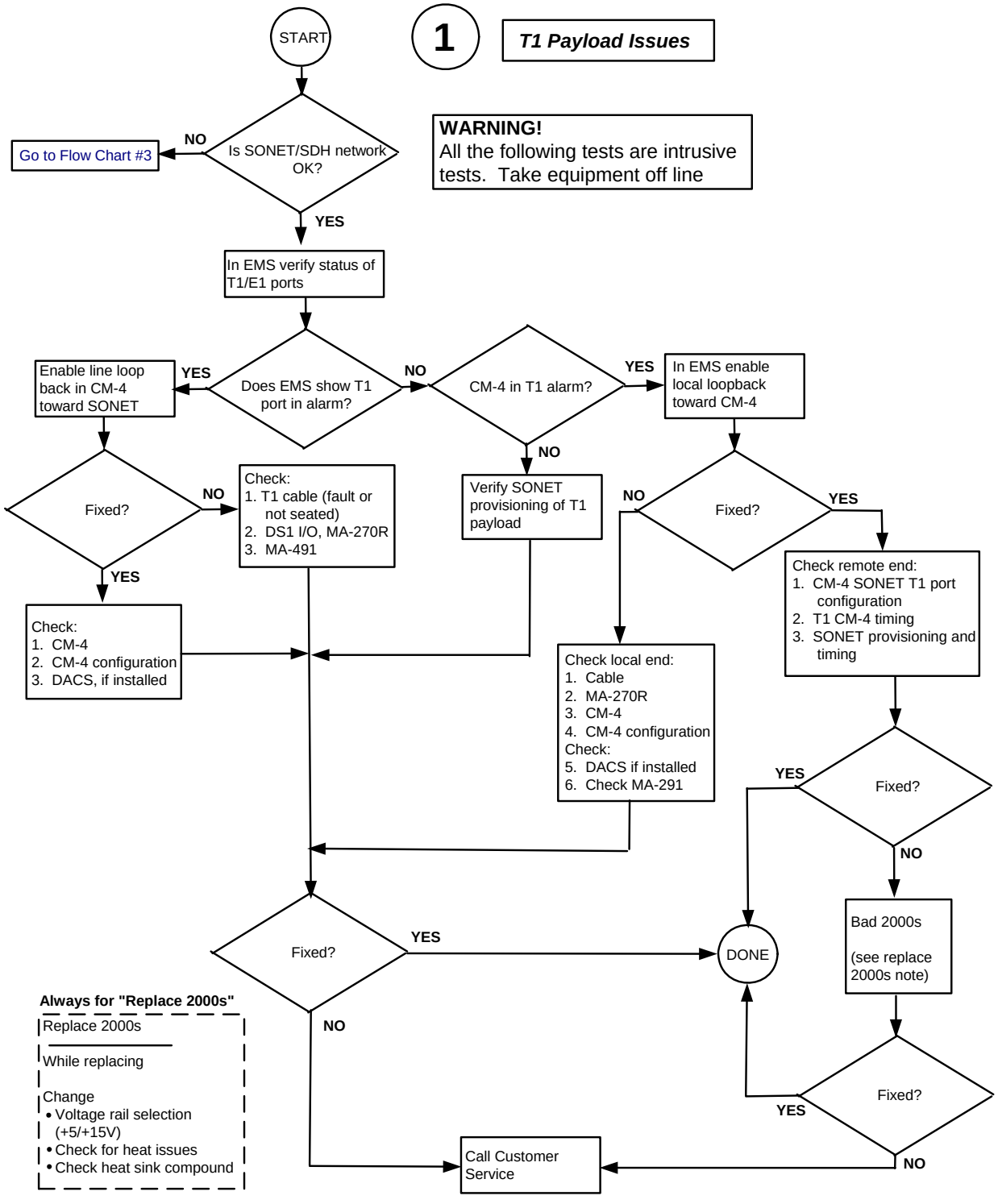


Figure 9-9. Manual USB Driver Install Step 8

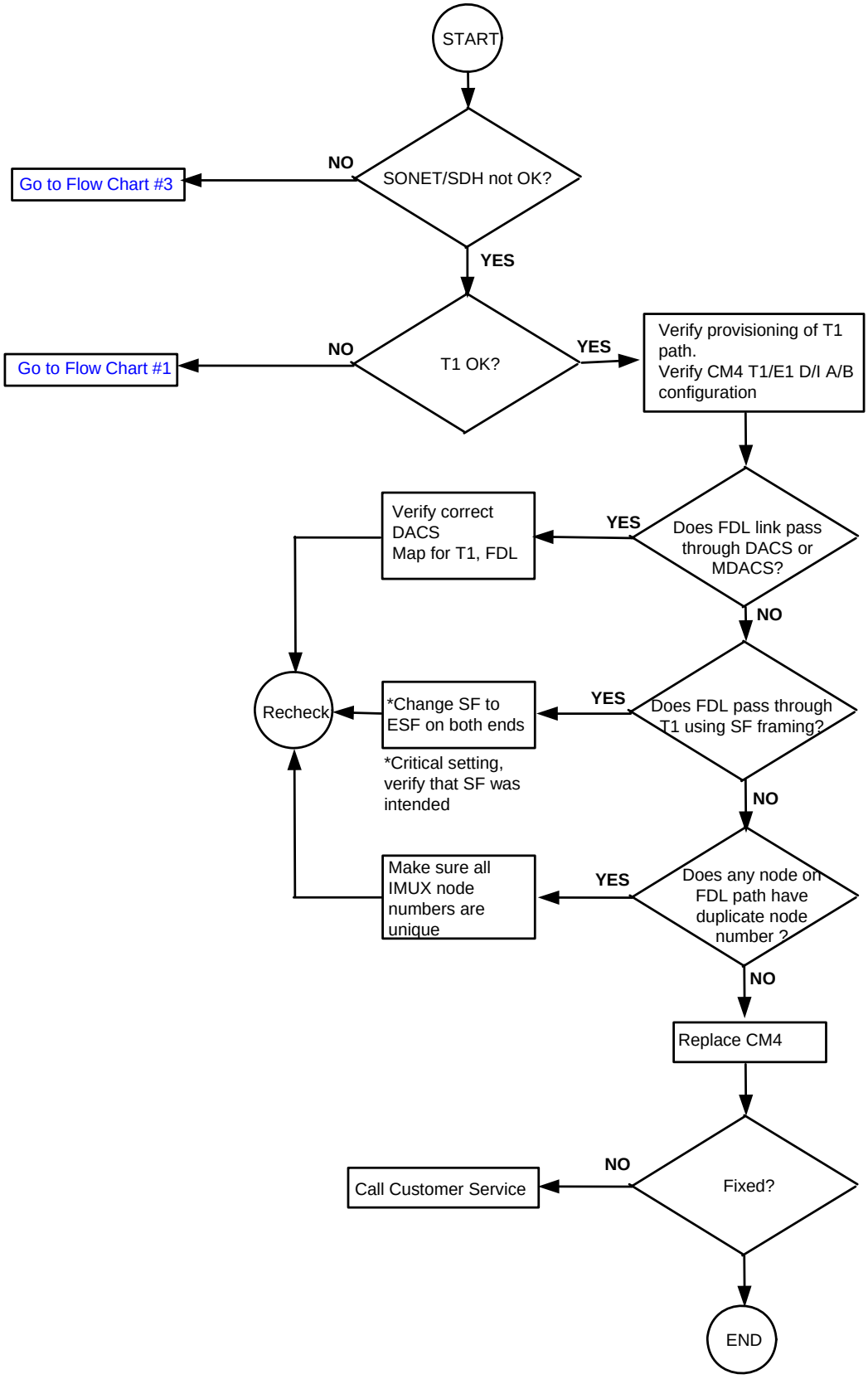
9.2 Fault Isolation Flow Charts

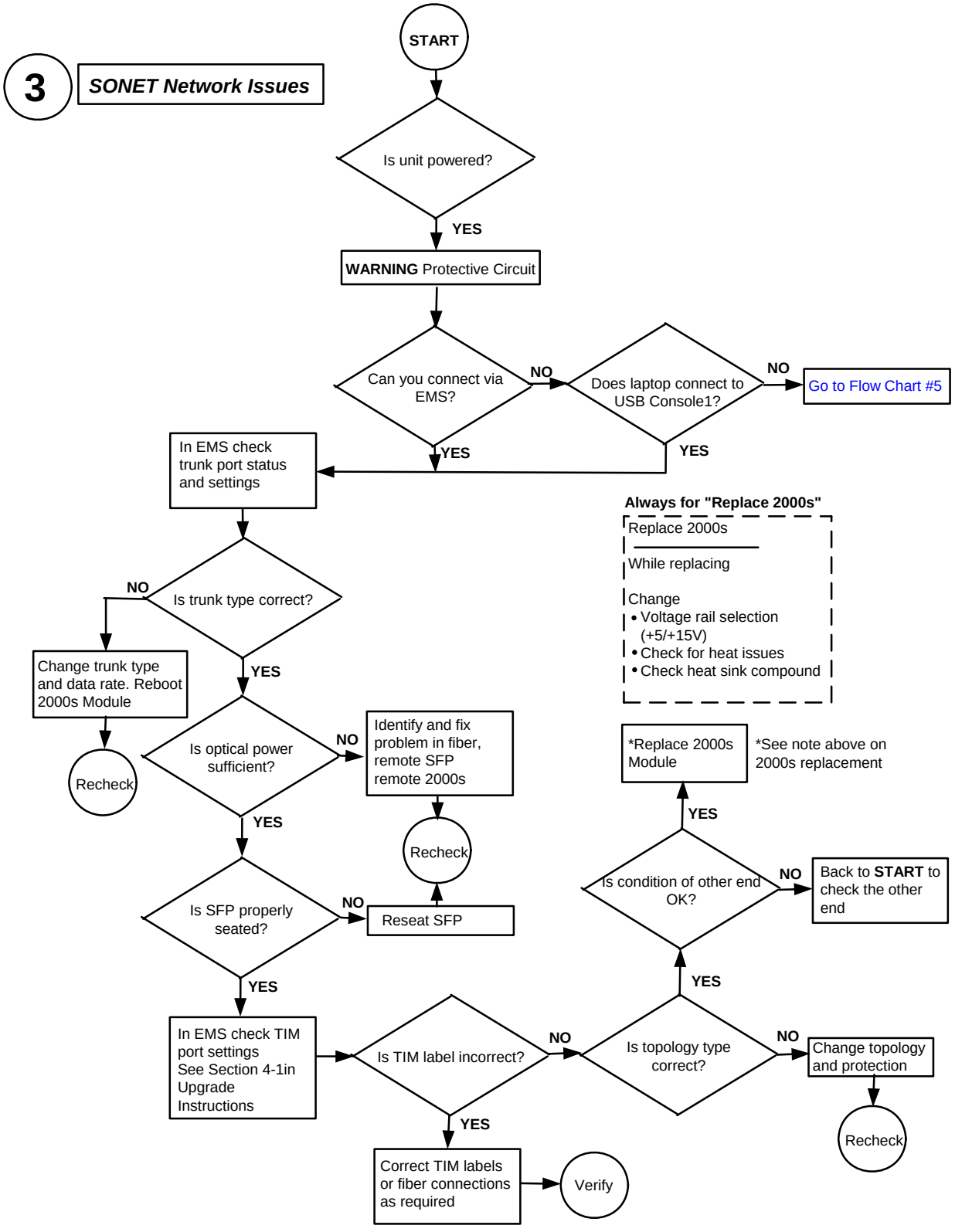
The following pages contain “Fault Isolation Flow Charts” for the IMUX 2000s. On page 9-2 is a lead in (jumping off chart) to assist users in getting to the root of the problem quickly. The flow charts are listed and hyperlinked below for your convenience.

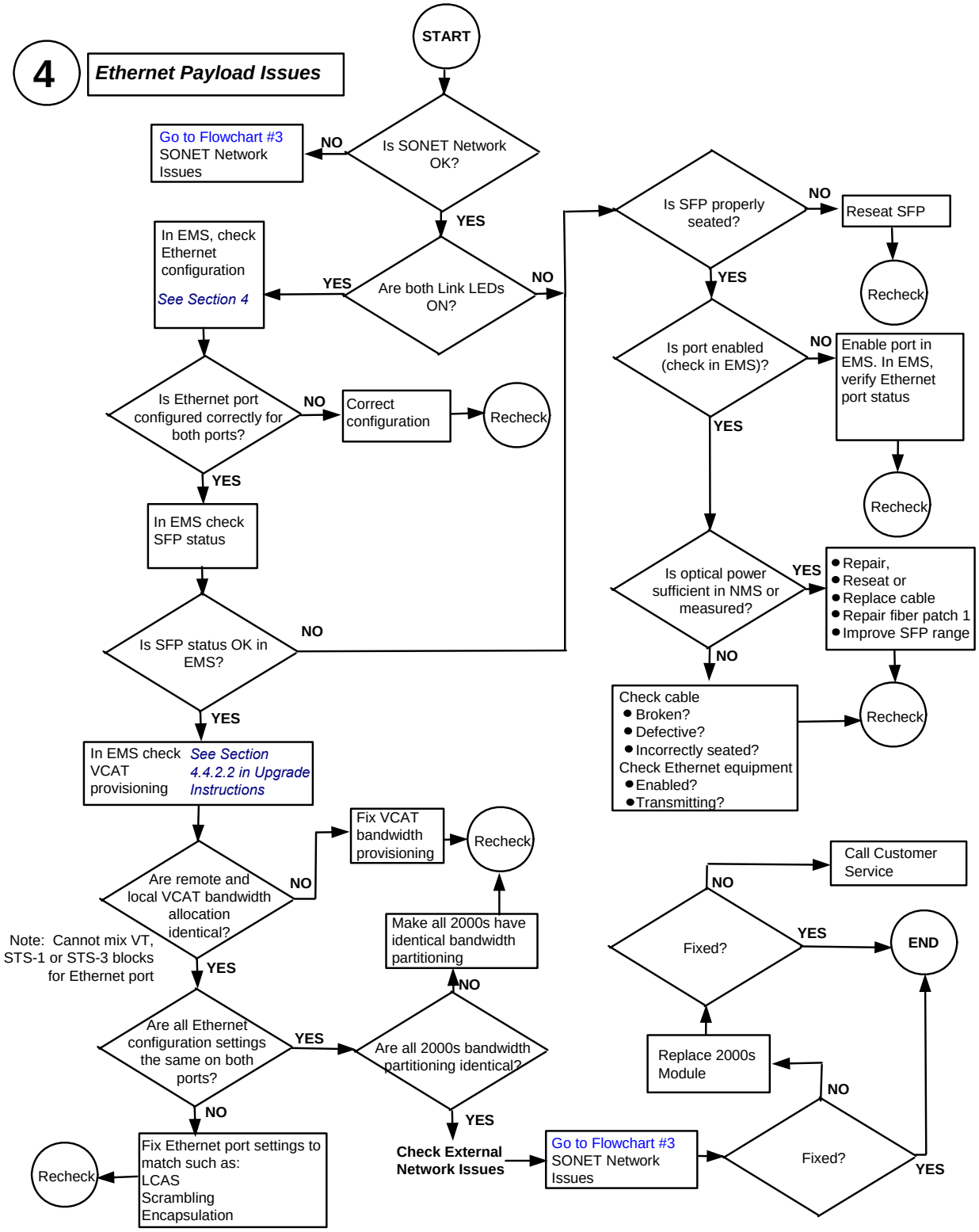

Troubleshooting Jump-Off
START
Alarm or Alert at node?
YES
NO
ALARM
ALERT
2000s Alarm?
MDACS or DACS Alarm?
LOS/LOF on CM-4 (FRM LED active) ?
Channel Card Alarm?
2000s Alarm -> check for SONET/SDH Module alarm.
Visually verify connections at SONET/SDH ports in front and at T1/E1 ports in rear.
Fibers, cables & SFP's intact and fully seated?
Interrogate with VNMS/EMS. See flow chart 3.
MDACS or connected DACS Alarm -> verify LEDs.
Visually verify connections at SONET/SDH ports in front and at T1/E1 ports in rear. Fibers, cables & SFP's intact and fully seated?
Interrogate with VNMS. Port alarm?
Check setting of Fast Reframe detector.
Correct T1/E1 link as needed. See flow chart 1.
LOS/LOF CM-4 (FRM LED active) -> verify LEDs.
Visually verify connections at T1/E1 ports in rear of CM-4 and of 2000s. Fibers, cables & SFP's intact and fully seated?
Interrogate with VNMS.
Fast Reframe -> verify enabled/disabled at both local and far end.
Correct T1/E1 link as needed. See flow chart 1.
Channel Card Alarm-> verify LEDs, interrogate with VNMS.
Correct Card Problem.
Configuration Issue?
Inventory Issue?
Redundancy Issue?
DACS Alert?
2000s Alert?
Investigate
ACO switch on, at power supply? -> turn cutoff off if not needed.
CM-4 not in normal operation mode?
-- Loopback active? -> verify with front panel or VNMS, turn off if not needed.
-- Fallback Timing (FTIM) active? -> verify with front panel, determine cause.
Missing or unseated cards? -> verify against system drawing
Channel card alerts? -> interrogate with VNMS, determine cause.
Redundant pwr supply failure -> verify LEDs, voltages, correct as needed.
CM-4 Standby Module active -> verify LEDs, activate Main, swap CM-4 (this will interrupt traffic!)
SWITCH configuration parameter not set to Auto -> verify with front panel or VNMS, change if not needed.
Front-panel slider switch not set to Auto -> verify on front panel, change if not needed.
MDACS or connected DACS alert -> verify LEDs, interrogate with VNMS. Alternate map active?
Correct T1/E1 link as needed. See flow chart 1.
2000s SONET/SDH Module alert -> interrogate with VNMS. See chart 3.
Alarm or Alert at other node?
If possible, start troubleshooting at node with alarm, otherwise...
Other type of problem.
Payload trouble
Management trouble
Cannot Communicate with Nodes?
9
Flowchart "9", Cannot Communicate with Nodes
T1 Payload Trouble?
1
Flowchart "1", T1 payload Issues
Ethernet Payload Trouble?
4
Flowchart "4", Ethernet Payload Issues
Other SONET PayloadTrouble?
3
Flowchart "3", SONET Network Issues
Other type of problem? Contact Customer Service

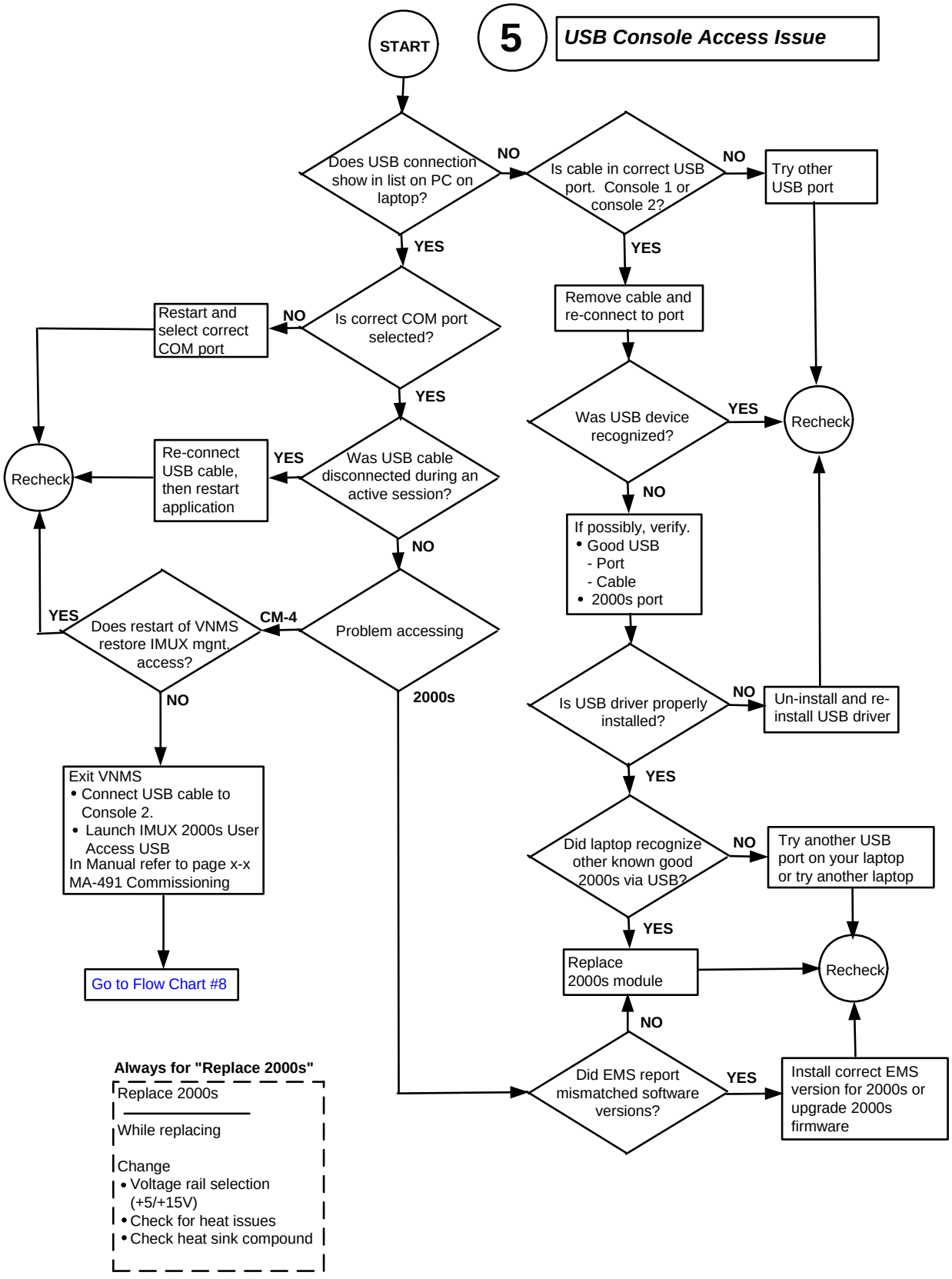

START
1
T1 Payload Issues
WARNING!
All the following tests are intrusive tests. Take equipment off line
Is SONET/SDH network OK?
NO
Go to Flow Chart #3
YES
In EMS verify status of T1/E1 ports
Does EMS show T1 port in alarm?
YES
Enable line loop back in CM-4 toward SONET
NO
CM-4 in T1 alarm?
YES
In EMS enable local loopback toward CM-4
NO
Fixed?
NO
Check:
1. T1 cable (fault or not seated)
2. DS1 I/O, MA-270R
3. MA-491
YES
Check:
1. CM-4
2. CM-4 configuration
3. DACS, if installed
Verify SONET provisioning of T1 payload
Fixed?
NO
YES
Check remote end:
1. CM-4 SONET T1 port configuration
2. T1 CM-4 timing
3. SONET provisioning and timing
Check local end:
1. Cable
2. MA-270R
3. CM-4
4. CM-4 configuration
Check:
5. DACS if installed
6. Check MA-291
Fixed?
YES
NO
Bad 2000s
(see replace 2000s note)
Fixed?
YES
NO
DONE
Always for "Replace 2000s"
Replace 2000s
While replacing
Change
• Voltage rail selection (+5/+15V)
• Check for heat issues
• Check heat sink compound
Fixed?
YES
NO
Call Customer Service

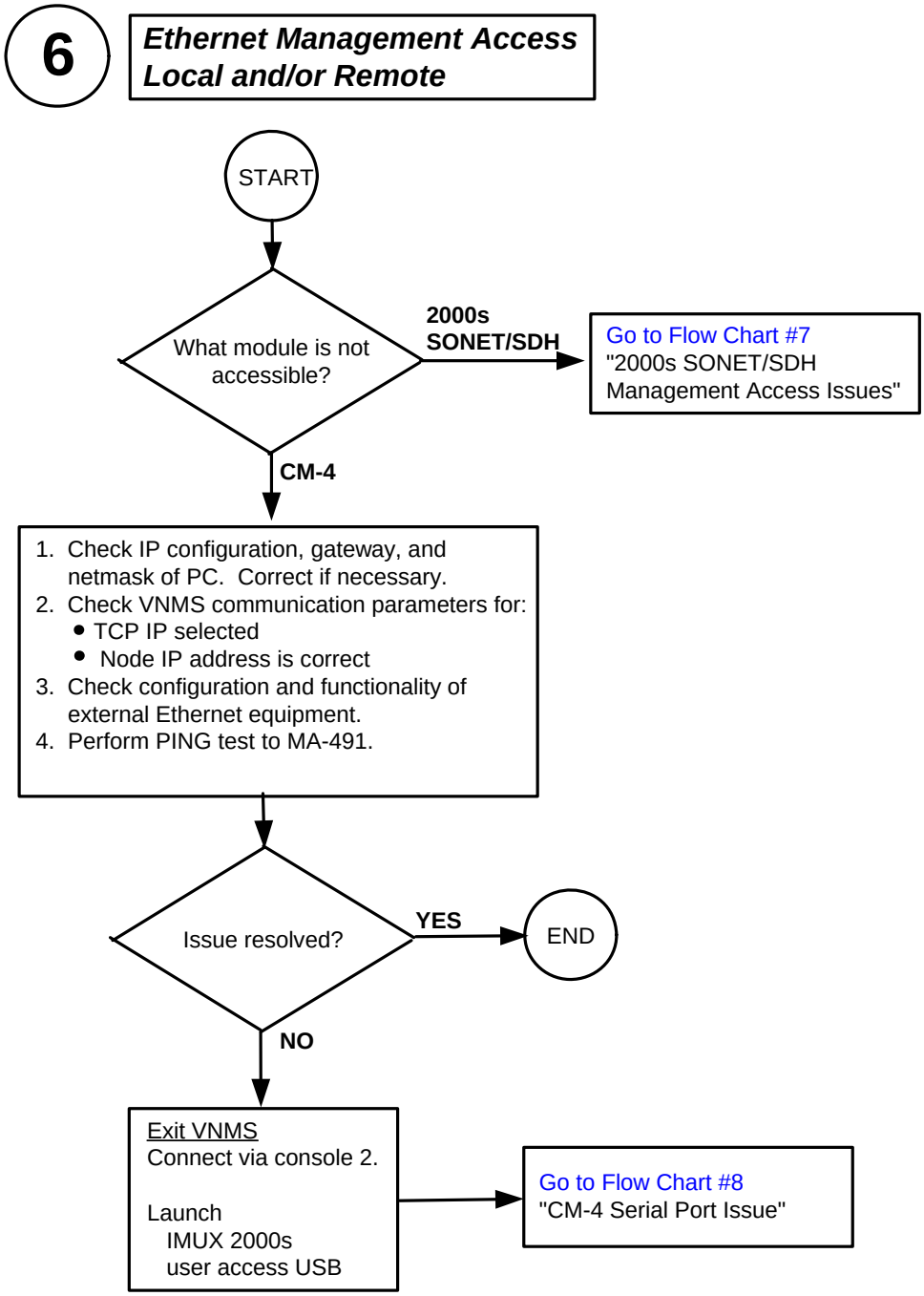
2 Remote T1 FDL Access Issues

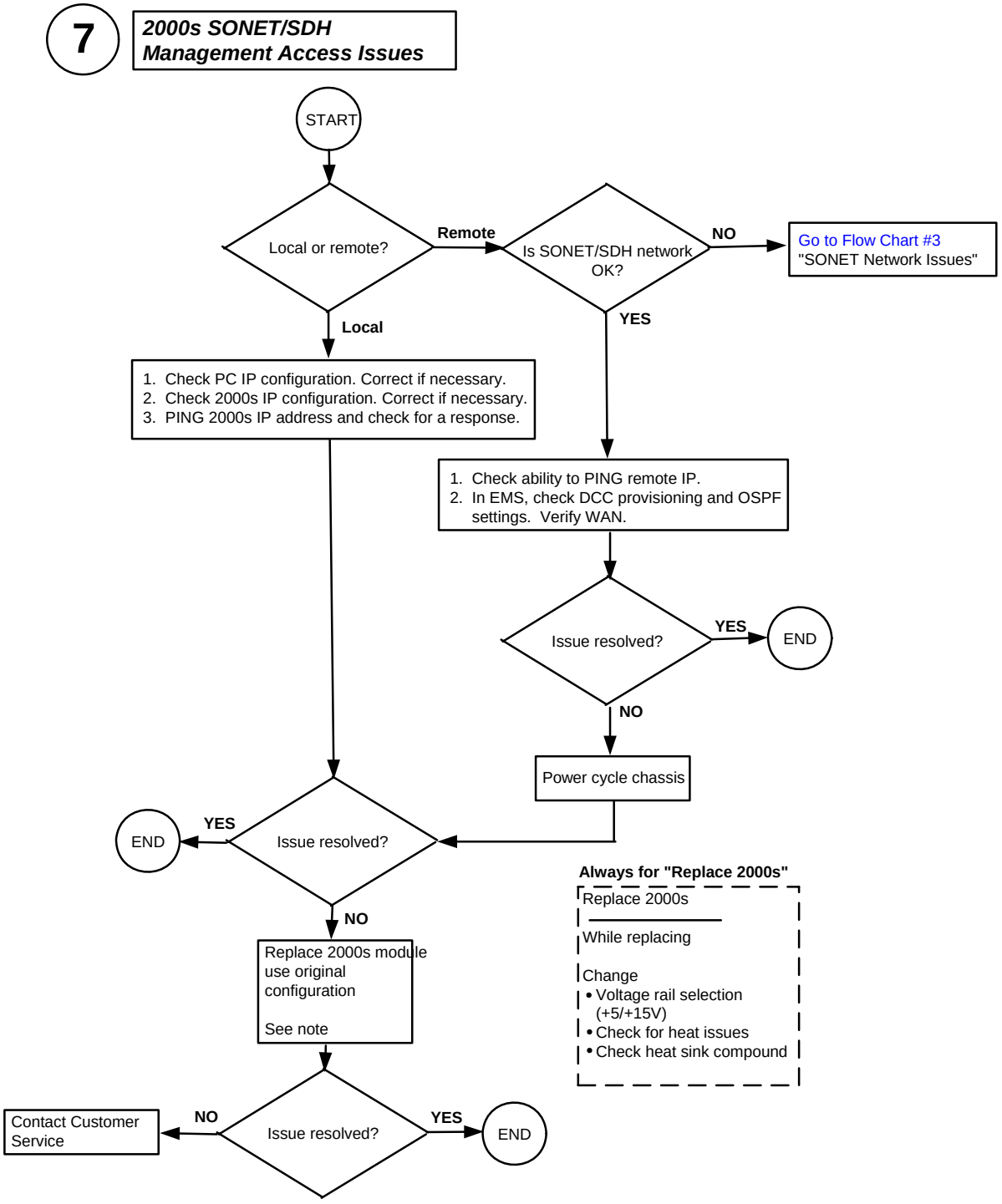


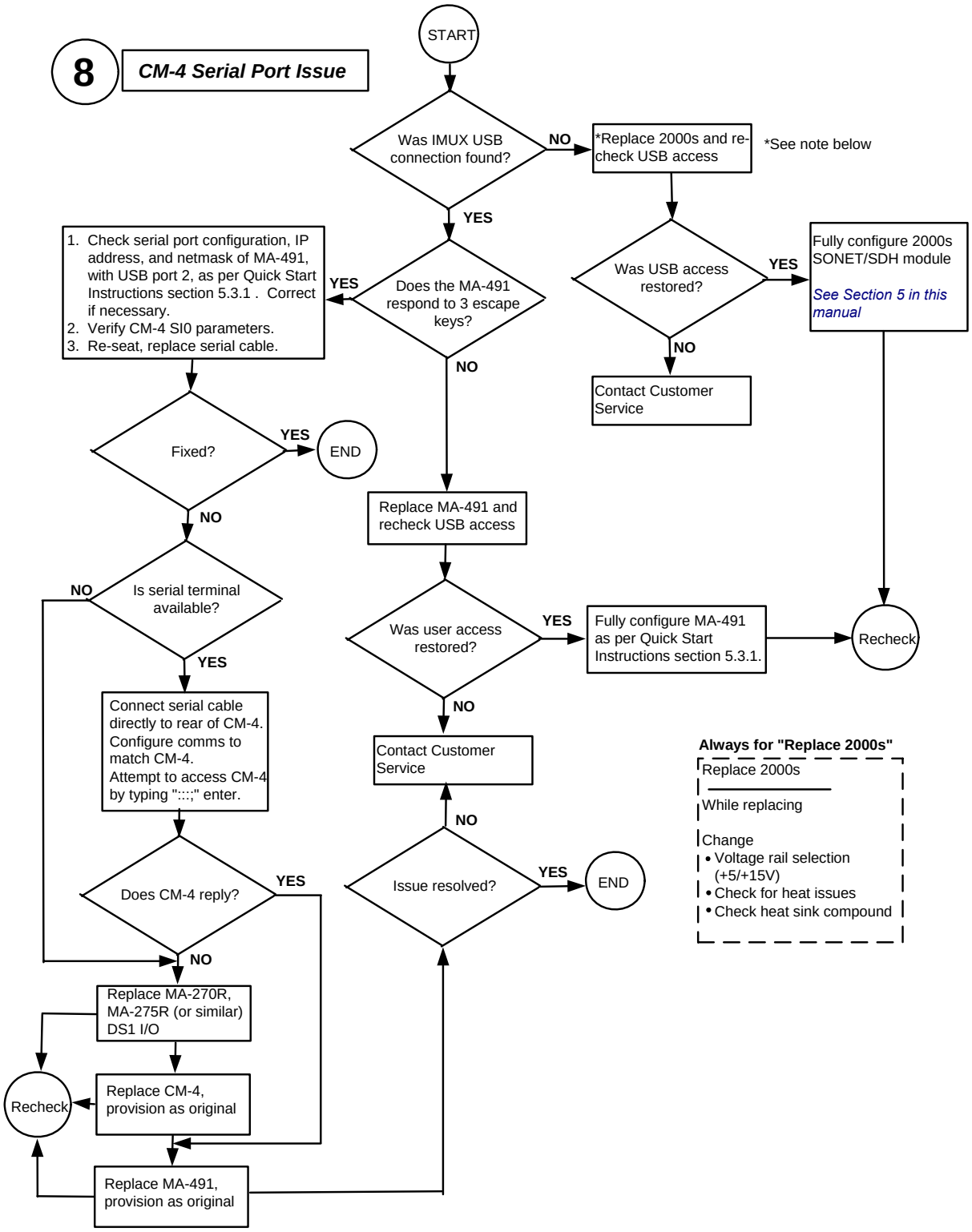

3
SONET Network Issues
START
Is unit powered?
YES
WARNING Protective Circuit
Can you connect via EMS?
NO
Does laptop connect to USB Console1?
NO
Go to Flow Chart #5
YES
YES
In EMS check trunk port status and settings
Always for "Replace 2000s"
Replace 2000s
While replacing
Change
• Voltage rail selection (+5/+15V)
• Check for heat issues
• Check heat sink compound
NO
Is trunk type correct?
Change trunk type and data rate. Reboot 2000s Module
Recheck
YES
Is optical power sufficient?
NO
Identify and fix problem in fiber, remote SFP remote 2000s
Recheck
YES
Is SFP properly seated?
NO
Reseat SFP
YES
In EMS check TIM port settings See Section 4-1in Upgrade Instructions
Is TIM label incorrect?
NO
YES
Correct TIM labels or fiber connections as required
Verify
Is topology type correct?
NO
Change topology and protection
Recheck
YES
Is condition of other end OK?
NO
Back to START to check the other end
YES
*Replace 2000s Module
*See note above on 2000s replacement


4
Ethernet Payload Issues
START
Is SONET Network OK?
NO
Go to Flowchart #3 SONET Network Issues
YES
Are both Link LEDs ON?
YES
In EMS, check Ethernet configuration
See Section 4
NO
Is SFP properly seated?
NO
Reseat SFP
Recheck
YES
Is port enabled (check in EMS)?
NO
Enable port in EMS. In EMS, verify Ethernet port status
Recheck
YES
Is Ethernet port configured correctly for both ports?
NO
Correct configuration
Recheck
YES
In EMS check SFP status
Is SFP status OK in EMS?
NO
YES
Is optical power sufficient in NMS or measured?
YES
Repair,
Reseat or
Replace cable
Repair fiber patch 1
Improve SFP range
NO
Check cable
Broken?
Defective?
Incorrectly seated?
Check Ethernet equipment
Enabled?
Transmitting?
Recheck
In EMS check VCAT provisioning
See Section 4.4.2.2 in Upgrade Instructions
Are remote and local VCAT bandwidth allocation identical?
NO
Fix VCAT bandwidth provisioning
Recheck
Note: Cannot mix VT, STS-1 or STS-3 blocks for Ethernet port
YES
Make all 2000s have identical bandwidth partitioning
NO
Are all Ethernet configuration settings the same on both ports?
YES
Are all 2000s bandwidth partitioning identical?
NO
YES
Call Customer Service
NO
Fixed?
YES
END
Replace 2000s Module
NO
Fixed?
YES
Check External Network Issues
Go to Flowchart #3 SONET Network Issues
Fix Ethernet port settings to match such as:
LCAS
Scrambling
Encapsulation
Recheck

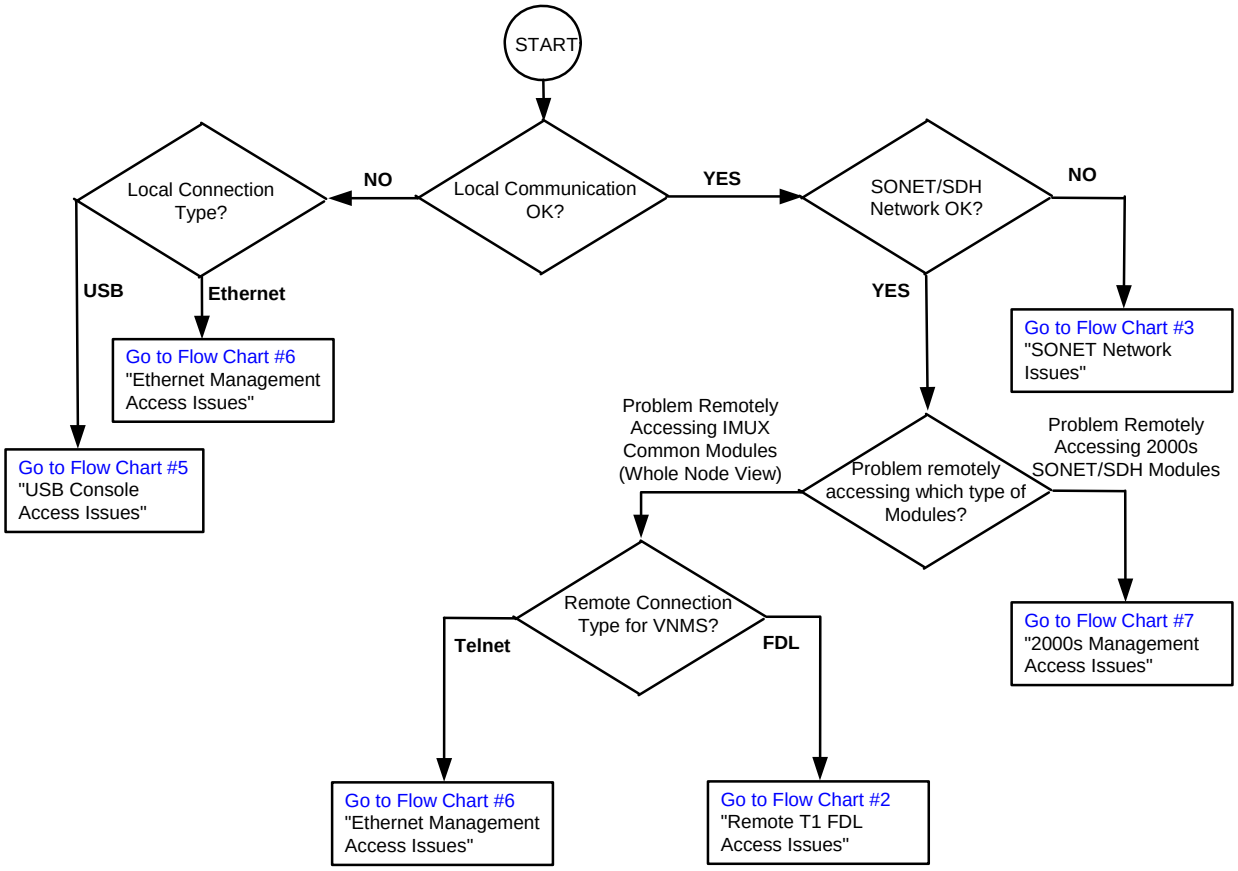

START
5
USB Console Access Issue
Does USB connection show in list on PC on laptop?
NO
Is cable in correct USB port. Console 1 or console 2?
NO
Try other USB port
YES
YES
Remove cable and re-connect to port
Is correct COM port selected?
NO
Restart and select correct COM port
YES
Was USB device recognized?
YES
Recheck
NO
Recheck
Re-connect USB cable, then restart application
YES
Was USB cable disconnected during an active session?
If possibly, verify.
• Good USB
- Port
- Cable
• 2000s port
NO
YES
Does restart of VNMS restore IMUX mgnt. access?
CM-4
Problem accessing
2000s
Is USB driver properly installed?
NO
Un-install and re-install USB driver
YES
NO
Exit VNMS
• Connect USB cable to Console 2.
• Launch IMUX 2000s User Access USB
In Manual refer to page x-x
MA-491 Commissioning
Did laptop recognize other known good 2000s via USB?
NO
Try another USB port on your laptop or try another laptop
YES
Go to Flow Chart #8
Replace 2000s module
Recheck
NO
Always for "Replace 2000s"
Replace 2000s
While replacing
Change
• Voltage rail selection (+5/+15V)
• Check for heat issues
• Check heat sink compound
Did EMS report mismatched software versions?
YES
Install correct EMS version for 2000s or upgrade 2000s firmware


6
Ethernet Management Access
Local and/or Remote
START
What module is not accessible?
2000s SONET/SDH
Go to Flow Chart #7
"2000s SONET/SDH Management Access Issues"
CM-4
1. Check IP configuration, gateway, and netmask of PC. Correct if necessary.
2. Check VNMS communication parameters for:
• TCP IP selected
• Node IP address is correct
3. Check configuration and functionality of external Ethernet equipment.
4. Perform PING test to MA-491.
Issue resolved?
YES
END
NO
Exit VNMS
Connect via console 2.
Launch
IMUX 2000s
user access USB
Go to Flow Chart #8
"CM-4 Serial Port Issue"


7
2000s SONET/SDH Management Access Issues
START
Local or remote?
Remote
Is SONET/SDH network OK?
NO
Go to Flow Chart #3 "SONET Network Issues"
YES
Local
1. Check PC IP configuration. Correct if necessary.
2. Check 2000s IP configuration. Correct if necessary.
3. PING 2000s IP address and check for a response.
1. Check ability to PING remote IP.
2. In EMS, check DCC provisioning and OSPF settings. Verify WAN.
Issue resolved?
YES
END
NO
Power cycle chassis
END
YES
Issue resolved?
NO
Always for "Replace 2000s"
Replace 2000s
While replacing
Change
• Voltage rail selection (+5/+15V)
• Check for heat issues
• Check heat sink compound
Replace 2000s module use original configuration
See note
Contact Customer Service
NO
Issue resolved?
YES
END


8
CM-4 Serial Port Issue
START
Was IMUX USB connection found?
NO
*Replace 2000s and re-check USB access
*See note below
YES
Was USB access restored?
YES
Fully configure 2000s SONET/SDH module
See Section 5 in this manual
NO
Contact Customer Service
Does the MA-491 respond to 3 escape keys?
YES
1. Check serial port configuration, IP address, and netmask of MA-491, with USB port 2, as per Quick Start Instructions section 5.3.1 . Correct if necessary.
2. Verify CM-4 SI0 parameters.
3. Re-seat, replace serial cable.
NO
Fixed?
YES
END
NO
Replace MA-491 and recheck USB access
Is serial terminal available?
NO
YES
Was user access restored?
YES
Fully configure MA-491 as per Quick Start Instructions section 5.3.1.
Recheck
NO
Connect serial cable directly to rear of CM-4. Configure comms to match CM-4. Attempt to access CM-4 by typing ":::;" enter.
Contact Customer Service
Always for "Replace 2000s"
Replace 2000s
While replacing
Change
• Voltage rail selection (+5/+15V)
• Check for heat issues
• Check heat sink compound
NO
Does CM-4 reply?
YES
Issue resolved?
YES
END
NO
Replace MA-270R, MA-275R (or similar) DS1 I/O
Recheck
Replace CM-4, provision as original
Replace MA-491, provision as original

9 Network Management - VNMS/EMS Cannot Communicate with Nodes



Section 10. Application Notes

This section contains application notes, which are intended to assist the user in configuring their IMUX 2000s unit(s).

Currently there are no Application Notes for this product.

Section 11. Index

11.1 Index

S

T

U

V

W

RFL Electronics Inc.
353 Powerville Road ● Boonton Twp., NJ 07005-9151 USA
Tel: 973.334.3100 ● Fax: 973.334.3863
Email: sales@rflelect.com ● www.rflelect.com