



FCM9004 User Manual Version 8.20

DATE:	8 th July 2013
DOCUMENT NO:	76-02-093
REVISION:	XH
PREPARED BY:	Ian Banbrook

Metrodata Ltd
Fortune House, Crabtree Office Village
Eversley Way, Egham Surrey, TW20 8RY, UK

Tel +44 1 784 744700
Fax: +44 1 784 744730
E-Mail: support@metrodata.co.uk

METRODATA LTD

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise, without the prior written permission of

**Metrodata Ltd, Fortune House,
Crabtree Office Village, Eversley Way,
Egham, Surrey, TW20 8RY, United Kingdom.**

DISCLAIMER

Metrodata Ltd makes no representations or warranties with respect to the contents hereof and specifically disclaims any implied warranties or merchantability or fitness for any particular purpose. Further, Metrodata Ltd reserves the right to revise this publication and to make changes from time to time in the content hereof without obligation of Metrodata Ltd to notify any person of such revision or changes.

Copyright © 2013 by Metrodata Ltd,

All Rights Reserved

Document History

22/10/2012	XA	Document Created
27/11/2012	XB	Document updated to include the SAM performance testing module, and the Tag mode descriptions
13/12/2012	XC	Document updated with change of terminology for Link State Forwarding to Link Loss Forwarding, Also include the L2CP functions
19/12/2012	XD	Document updated to reflect the Menu changes for the rev 8.8 firmware
11/1/2013	XE	Document updated to reflect changes to menu system for rev 8.9 firmware
03/04/2014	XF	Document Updated to reflect new base labels.
09/05/2013	XG	Document updated to reflect the 8.16 software release.
8/7/2013	XH	Document updated to reflect 8.20 Software Release.

1	INTRODUCTION	17
1.1	FCM9004 EDD	18
1.2	Safety	18
1.3	Electro Magnetic Compatibility	18
1.3.1	EN55022 Statement	19
1.3.2	FCC Declaration	19
1.4	WEEE Directive	19
1.5	RoHS Compliance	19
2	INSTALLATION	20
2.1	FCM9004 Rear Panel	20
2.1.1	Mains Power	20
2.1.2	DC Power	20
2.2	Base Label and Bit Switches	21
2.2.1	WAN Port Configuration	22
2.2.1.1	Switch 1, WAN Mode	22
2.2.1.2	Switch 2, Auto Negotiation	22
2.2.1.3	Switch 3/4, Speed	22
2.2.1.4	Switch 5, Duplex	23
2.2.2	Zero Touch Configuration Control	23
2.2.2.1	Switch 6, TAG Mode	23
2.2.2.2	Switch 7, Boot Location / (Autoboot)	23
2.2.3	Switch 8, Master Boot Control / (Factory Default)	24
2.3	Rackmounting	25
3	OPERATING MODES	26

3.1	C-Tag Mode.....	26
3.2	S-Tag Mode.....	28
3.2.1	Pushing S-Tag onto Untagged Frame	29
3.2.2	Pushing S-Tag onto Tagged Frame	30
3.3	Double Tag Mode	31
3.3.1	Untagged Frame Ingress.....	32
3.3.2	Tagged Frame Ingress	33
4	CONFIGURATION.....	34
4.1	System Configuration	35
4.1.1	Setting the Time and Date.....	35
4.1.1.1	Time Zone	36
4.1.1.2	NTP Server.....	36
4.1.1.3	Sync Now	36
4.1.2	Setting the Node Name	36
4.1.3	Provider ID	37
4.1.4	Access Control	37
4.1.4.1	Setting the Local Password.....	37
4.1.4.1.1	Default Unit Password.....	38
4.1.4.1.2	Password Recovery	38
4.1.4.2	View User	38
4.1.4.3	Super Me.....	38
4.1.4.4	TACACS+.....	39
4.1.4.4.1	Authentication	40
4.1.4.4.2	Timeout	40
4.1.4.4.3	Retries.....	40

4.1.4.4.4	Server	40
4.1.4.4.5	Encryption Key	40
4.1.5	Welcome Screen	41
4.1.5.1	Display Screen	41
4.1.6	Output Config	42
4.1.7	Input Config	42
4.1.8	Warm Start	43
4.1.9	Cold Start	43
4.1.10	Event Logs	43
4.1.10.1	System Event Log	45
4.1.10.2	Alarm Event Log	45
4.1.10.3	Config Event Log	46
4.1.10.4	Full Event Log	46
4.1.11	Zero Touch Configuration	47
4.1.11.1	Zero Touch State	47
4.1.11.2	Software Upgrade Time	48
4.2	Management Entity	49
4.2.1	Interface	49
4.2.1.1	STATE	50
4.2.1.2	Physical Address	50
4.2.1.3	DHCP	50
4.2.1.4	IP Address	50
4.2.1.5	Net Mask	51
4.2.1.6	AT Table	51
4.2.1.7	Stats	52

4.2.1.8	C-VLAN	52
4.2.1.9	QinQ/S-VLAN	52
4.2.1.10	802.1p Priority	52
4.2.2	IP Configuration.....	53
4.2.2.1	Default TTL.....	53
4.2.2.2	DSCP Priority	53
4.2.2.3	Routing Table	54
4.2.2.4	Forwarding	54
4.2.2.5	IP Statistics.....	55
4.2.3	UDP	56
4.2.3.1	SNMP Ports.....	56
4.2.3.2	Statistics	57
4.2.4	TCP	57
4.2.4.1	Statistics	58
4.2.4.2	Connection Table	58
4.2.5	SNMP	59
4.2.5.1	Communities	59
4.2.5.2	Managers	60
4.2.5.2.1	Dying Gasp Trap	61
4.2.5.3	Contact Person.....	61
4.2.5.4	Node Name	61
4.2.5.5	Location.....	61
4.2.5.6	SNMP Statistics.....	62
4.2.5.7	Trap Alarms.....	63
4.2.6	Telnet/SSH	64

4.2.6.1	Access Method	64
4.2.6.2	Timeout	65
4.2.7	TFTP	66
4.2.7.1	Client Mode	66
4.2.7.1.1	Remote IP	66
4.2.7.1.2	Get New Software	67
4.2.7.1.2.1	Failsafe Upgrade	68
4.2.7.1.3	Boot Software Upgrade	68
4.2.7.1.4	Get Config	69
4.2.7.1.5	Put Config	69
4.2.7.2	Server Mode	69
4.2.7.2.1	Remote IP	70
4.2.7.2.2	Software File Name	70
4.2.7.2.3	Config File Name	70
4.2.8	Ping	70
4.3	V.24 Set-up	71
4.3.1	Usage	71
4.3.2	Console set-up	71
4.3.2.1	Terminal Type	72
4.3.2.2	Via Modem	72
4.3.2.3	Baud Rate	72
4.3.2.4	Parity	72
4.3.2.5	Data Bits	73
4.3.2.6	Stop Bits	73
4.3.2.7	Load New Config	73

4.4	Port Set Up Menu	74
4.4.1	User LAN Port Configuration	75
4.4.1.1	State	75
4.4.1.2	Link Status	75
4.4.1.3	Speed	75
4.4.1.4	Duplex	76
4.4.1.5	Auto Negotiation	77
4.4.1.6	Negotiated	77
4.4.1.7	MDI / MDIX	77
4.4.1.8	OAM	79
4.4.1.8.1	OAM Mode	79
4.4.1.8.2	OAM Status	80
4.4.1.8.3	OAM Statistics	80
4.4.1.8.4	OAM Events	81
4.4.1.9	Link Loss Forwarding	81
4.4.1.10	Tagging and Priority	81
4.4.1.10.1	Add C-Tag to	82
4.4.1.10.2	C-Tag VID	82
4.4.1.10.3	Priority Source	82
4.4.1.10.4	Default Priority	83
4.4.1.11	L2CP Management	84
4.4.1.11.1	Bridge Group	85
4.4.1.11.1.1	OAM	85
4.4.1.11.1.2	STP/RSTP/MSTP	85
4.4.1.11.2	LACP / LACP Marker	86

4.4.1.11.2.1	OSSP.....	86
4.4.1.11.2.2	LLDP.....	86
4.4.1.11.2.3	Other Bridge	86
4.4.1.11.3	GARP Group.....	87
4.4.1.11.3.1	GMRP.....	87
4.4.1.11.3.2	GVRP	87
4.4.1.11.3.3	Other GARP	87
4.4.1.11.4	Cisco Group	88
4.4.1.11.5	Metrodata Group	88
4.4.1.11.5.1	Beacon	88
4.4.1.11.5.2	L2CP Tunnel.....	88
4.4.1.11.5.3	Other Metrodata	89
4.4.1.11.6	Other Group	89
4.4.1.11.7	L2CP Flow.....	89
4.4.1.12	Counters.....	90
4.4.2	User SFP Port Configuration	91
4.4.2.1	State	91
4.4.2.2	Link Status	91
4.4.2.3	SFP Type	91
4.4.2.4	Speed	92
4.4.2.5	Duplex	92
4.4.2.6	Auto Negotiation.....	92
4.4.2.7	Negotiated	93
4.4.2.8	SFP Management	93
4.4.2.8.1	Device Details	94

4.4.2.8.2	Notifications.....	94
4.4.2.9	Tagging and Priority	95
4.4.2.10	L2CP Management	95
4.4.2.11	OAM	96
4.4.2.11.1	OAM Mode	96
4.4.2.11.2	OAM Status.....	97
4.4.2.11.3	OAM Statistics.....	97
4.4.2.11.4	OAM Events	97
4.4.2.12	Link Loss Forwarding	98
4.4.2.13	Counters.....	98
4.4.3	WAN Port	99
4.4.3.1	State	100
4.4.3.2	Link Status	100
4.4.3.3	Interface	100
4.4.3.4	Speed.....	100
4.4.3.4.1	Copper Interface Mode	100
4.4.3.4.2	Fibre Interface Selected	101
4.4.3.5	Duplex	101
4.4.3.6	Auto Negotiation.....	102
4.4.3.7	SFP Management	102
4.4.3.7.1	Device Details	103
4.4.3.7.2	Notifications.....	103
4.4.3.8	Negotiated	104
4.4.3.9	MDI / MDIX.....	104
4.4.3.10	Tagging and Priority	105

4.4.3.11	OAM	105
4.4.3.11.1	OAM Mode	106
4.4.3.11.2	OAM Status	106
4.4.3.11.3	OAM Statistics	107
4.4.3.11.4	OAM Events	107
4.4.3.12	Counters	108
4.5	Operational Modes	109
4.5.1	VLAN Mode	109
4.5.1.1	VLAN Mode – STag	110
4.5.1.2	VLAN Mode – CTag	111
4.5.1.3	VLAN Mode – Double Tag	111
4.5.2	Max Frame Size	111
4.5.3	SLA/POLICING	112
4.5.3.1	Count CFM	112
4.5.4	Count L2CP	112
4.5.4.1	Bandwidth	113
4.5.4.2	Include S-Tag	113
4.5.4.3	Include C-Tag	113
4.5.4.4	Coupling	114
4.5.4.5	Colour Mode	114
4.5.5	Priority Translation	114
4.5.6	CFM Domains	114
4.5.6.1	Multicast Address	115
4.5.6.2	Edit a Domain	116
4.5.6.2.1	Domain Name	116

4.5.6.2.2	Domain Name Format.....	116
4.5.6.2.3	Domain Level	117
4.5.6.2.4	Remove Domain	118
4.5.6.2.5	Domain Status Summary	118
4.5.6.2.6	Add Maintenance Domain.....	118
4.6	Flow (Services).....	119
4.6.1	List Flows	119
4.6.2	Add / View / Edit / Modify Flow	120
4.6.2.1	Flow Number	121
4.6.2.2	Flow Name	121
4.6.2.3	Flow State	121
4.6.2.4	S-VLAN ID.....	121
4.6.2.5	User Port	122
4.6.2.6	C-VLAN Allocation.....	122
4.6.2.7	Control C-Vlan.....	122
4.6.2.8	SLA/Policing Definition	123
4.6.2.8.1	CIR.....	124
4.6.2.8.2	CBS.....	124
4.6.2.8.3	EIR	124
4.6.2.8.4	EBS	124
4.6.2.8.5	Maximum Frame Loss.....	125
4.6.2.8.6	Max Delay	125
4.6.2.8.7	Max Delay Variation	125
4.6.2.8.8	Availability	125
4.6.2.8.9	Policing	126

4.6.2.9	Flow CFM Configuration.....	126
4.6.2.9.1	MA, Maintenance Association Configuration.....	127
4.6.2.9.1.1	MA Name.....	127
4.6.2.9.1.2	MA Name Format	127
4.6.2.9.1.3	MA Domain.....	127
4.6.2.9.2	MEP, Maintenance End Point Configuration	129
4.6.2.9.2.1	MEP ID	129
4.6.2.9.2.2	MEP State	129
4.6.2.9.2.3	MEP CCM.....	130
4.6.2.9.2.4	MEP LMM.....	130
4.6.2.9.2.5	MEP DMM	131
4.6.2.9.3	Counters	131
4.6.2.9.4	Y.1731 Performance	132
4.6.2.9.5	Remove Flow	133
4.7	Circuit / Flow Tests	134
4.7.1	Port Loops	134
4.7.2	SAM Flow Testing, Service Assurance Module	135
4.7.2.1	SAM Mode	135
4.7.2.2	SAM Test Regime	136
4.7.2.3	Y.1564 Testing	136
4.7.2.3.1	State.....	136
4.7.2.3.2	View Results	137
4.7.2.3.3	Profile.....	138
4.7.2.3.4	Test Parameters.....	138
4.7.2.3.4.1	Background Rate.....	139

4.7.2.3.4.2	Go/No Go Test	139
4.7.2.3.4.2.1	Go/No Go Test Time	139
4.7.2.3.4.3	CIR Test	140
4.7.2.3.4.3.1	CIR Test Rate	140
4.7.2.3.4.3.2	CIR Test Time	140
4.7.2.3.4.4	CBS Test	140
4.7.2.3.4.4.1	CBS Test Rate	140
4.7.2.3.4.4.2	CBS Test Burst Size	141
4.7.2.3.4.4.3	CBS Test Time	141
4.7.2.3.5	CIR/EIR Test	141
4.7.2.3.5.1.1	CIR/EIR Test CIR Rate	141
4.7.2.3.5.1.2	CIR/EIR Test EIR Rate	141
4.7.2.3.5.1.3	CIR/EIR Test Time	141
4.7.2.3.6	Flows	142
4.7.2.4	Manual Mode Testing	143
4.7.2.4.1	Test Duration	143
4.7.2.4.2	Test State	143
4.7.2.4.3	Manual Setup	144
4.7.2.4.3.1	Flow	144
4.7.2.4.3.2	S-VLAN / C-VLAN	144
4.7.2.4.3.3	Local MAC	144
4.7.2.4.3.4	Remote MAC	145
4.7.2.4.3.5	Packet Size	145
4.7.2.4.3.6	Packet Rate	145
4.7.2.4.3.7	Bandwidth	145

FCM9004 USER MANUAL

4.7.2.4.3.8 Burst Size (Packets)145

4.7.2.4.3.9 Burst Size (CBS)146

4.7.2.4.4 Test Summary146

4.7.2.4.5 Clear Results.....146

APPENDIX 1 Base Label Versions147

1 INTRODUCTION

The Metrodata MetroConnect FCM9004 is a highly featured, cost effective Ethernet Service Demarcation Device (EDD) which allows carriers, or aggregate service providers to manage the service effectively.

The FCM9004 offers a user selectable network interface supporting either fibre or Copper interfaces. Fibre is supported through the use of plug in, SFP modules and supports either Gigabit 1000Base-X or Fast Ethernet 100BaseFX circuits. The copper port is presented on an RJ45 connector offering a 10/100/1000BaseT auto negotiating, auto switching connection.

The FCM9004 presents the user with four copper ports on RJ45 connectors along with a single fibre port supporting an SFP. All copper ports support 10/100/1000BaseT with auto negotiation and auto switching, whilst the Fibre port supports both 1000BaseX and 100BaseFX SFP modules.

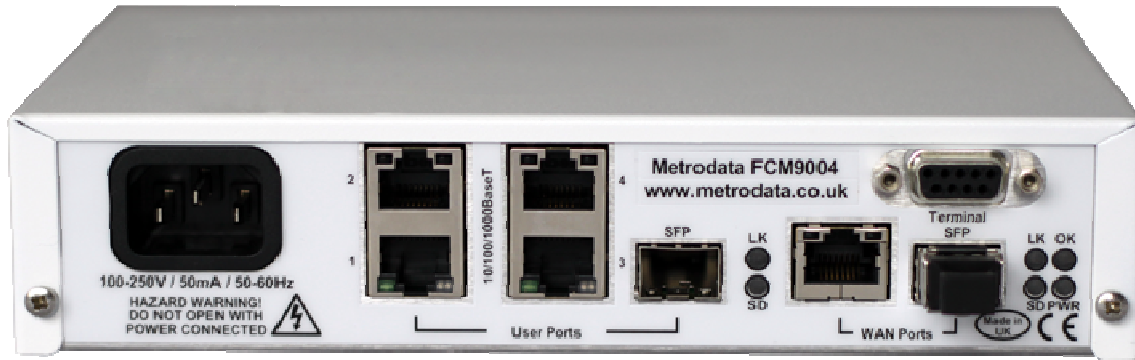
The FCM9004 uses a flow based architecture with flows being supported with either single or double tag push/pop operation. Both IEEE 802.1q VLAN C-Tags and IEEE 802.1ad Service Tags are supported with a fully programmable S-Tag for maximum compatibility.

Extensive operational diagnostic information is available through the use of OAM, both IEEE802.3 clause 57 Link OAM, and IEEE 802.1ag / Y.1731 Connectivity and Fault Management OAM (CFM). Y.1731 also offers in service verification of Service Level Agreements through the measurement of packet delays with sub microsecond accuracy and Frame loss / Frame Loss Ratios

To assist Service Providers in provisioning customer circuits the FCM9004 includes a highly featured packet generator and packet monitor allowing for RFC2544 and Y.1564 testing. The FCM9004 also includes a loopback facility with MAC DA/SA and IP SA/DA swapping capability.

The FCM9004 offers a “Zero Touch Configuration” facility whereby a unit will listen for a beacon and then automatically determine the management connection and load a configuration file from a central server.

1.1 FCM9004 EDD



The FCM9004 is a compact unit as shown occupying half a shelf in a traditional 19inch rack. All connectors and LED status indicators are accessible from the rear of the unit.

1.2 Safety

The FCM9004 must not be connected to cabling which would be required by BS6701 to be equipped with over voltage protection. The following ports on the FCM9004 are designated SELV (Safety Extra Low Voltage) within the scope of EN41003

Terminal Port 9 Way D-Type

LAN Port(s) RJ45 10/100/1000BaseT

SFP

These ports must only be connected to SELV ports on other equipment in accordance with EN60950 clause 2.3

1.3 Electro Magnetic Compatibility

In order to ensure EMC compliance, all signal and data cables must be shielded and use screened connector shells. The cable screens must be terminated to the screened connector shell and not connected to any pins of the connector. Failure to use the correct connectors may compromise EMC compliance.

1.3.1 EN55022 Statement

The FCM9004 is a Class A product. In a domestic environment, this product may cause radio interference, in which case the user will be required to take adequate measures.

1.3.2 FCC Declaration

This equipment has been tested and found to comply with the limits of the Class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the Installation and Operation manual, may cause harmful interference to the radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

1.4 WEEE Directive

The FCM9004 is covered by Directive 2002/96/EC (OJ:L37/24/2003) on Waste Electrical and Electronic Equipment (WEEE) Units must therefore not be disposed of in standard landfill.

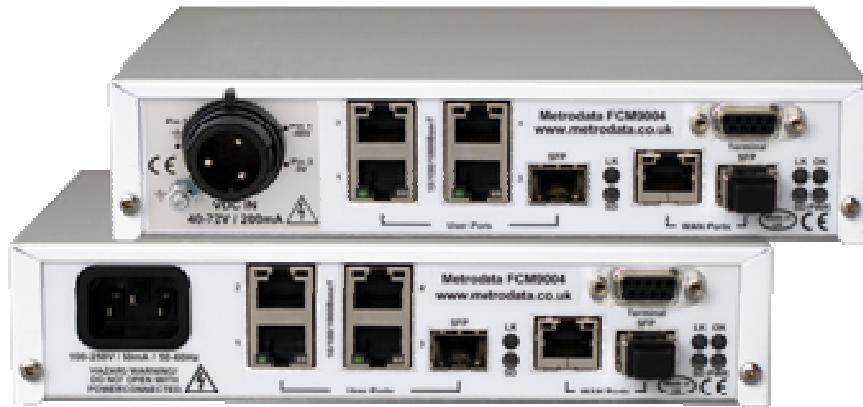
1.5 RoHS Compliance

The FCM9004 is compliant with the EU RoHS Directive 2002/95/EC. The RoHS directive bans the use of six hazardous materials in products placed on the market after July 1st 2006. The six banned materials are Lead, Mercury, Hexavalent Chromium, Polybrominated Biphenyls, Polybrominated Diphenyl Ethers and Cadmium.

The FCM9004 is manufactured using a lead free soldering process and as such is fully RoHS 6/6 compliant.

2 INSTALLATION

2.1 FCM9004 Rear Panel



The FCM9004 is available with either AC Mains or DC power options.

2.1.1 Mains Power

The FCM9004 has an internal power supply and is supplied via an IEC mains power socket. The FCM9004 operates over the wide range 100 to 250V AC and draws less than 6 watts.

2.1.2 DC Power

The FCM9004 is available with an internal DC power supply with two variants available,

DC -48V (36 to 72V DC)

DC 24V (7 to 36V DC)

DC powered units have an external earth stud which must be securely connected to an earth connection to ensure EMC compliance.

2.2 Base Label and Bit Switches

On the underside of the FCM9004 there are bit switches which may be used to configure certain functions within the unit.



Metrodata Ltd

TW20 8RY UK

Tel +44 (0) 1784 744700

Fax +44 (0) 1784 744730

www.metrodata.co.uk

Manufactured in the UK

Status LED	Meaning
Off	No mains power present
Red steady	WAN
Red/Off Flashing	WAN / LAN Alarm
Green/Off Flashing	LAN
Green steady	Status OK

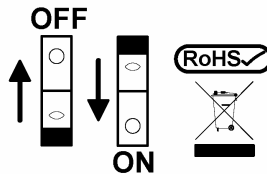
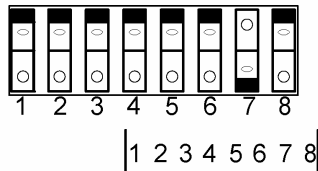
FCM9004

Advanced Ethernet

Demarcation Device (AC)

Part No. 80-70-941 Serial No:

SW	Control	ON	OFF
1	WAN Mode	Copper *	Fibre
2	Auto Neg	Enabled *	Disabled
3	Speed	1000M *	10/100M
4	Speed	100M *	10M
5	Duplex	Full *	Half
6	Tag Mode	Single Tag Push/Pop *	Double Tag Push/Pop
7	Boot Location	Remote (ZTC)	Local (EEPROM Stored Configuration)*
8	Master Boot Control	Boot Normally *	Erase EEPROM and boot using Switch Settings



**Bold * Characters =
Bitswitch Settings
As Shipped.**

17-70-1319D (Ai)

Note, older units may have previous versions of the base label which may be found in appendix 1. For clarity, switch descriptions have been changed, however the functionality of the switch has not.

The bit switches are ONLY used to configure the default settings following a cold start. A cold start may be triggered by setting switch 8 to the OFF position and power cycling before returning SW8 to the normal ON position. Alternately, a cold start may be requested from the User Interface.

2.2.1 WAN Port Configuration

Bit switches 1 to 5 are used to configure the default setting for the WAN Network port of the device and are used on installation to ensure the FCM9004 physical interface matches that of the network port it will connect to.

2.2.1.1 Switch 1, WAN Mode

The WAN mode switch selects between the two physical interfaces for the WAN port.

ON	Select the WAN copper interface, presenting a 10/100/1000BaseT interface on RJ45
OFF	Select the WAN Fibre interface, presenting either 100Base-FX or 1000Base-X when an SFP module is inserted.

2.2.1.2 Switch 2, Auto Negotiation

The Auto Negotiation switch controls whether the switch port is configured automatically, or manually.

ON	Auto Negotiation Enabled
OFF	Manual controlled selection of speed and duplex

Note,

When the Fibre interface has been selected, Auto negotiation must be enabled for 1000BaseX, however must be disabled for 100Base-FX operation.

2.2.1.3 Switch 3/4, Speed

There are two bit switches used to select the speed control of the WAN port. When auto negotiation is enabled, these switches control the options that are advertised, whereas in manual mode, the speed switches actually select the interface speed.

BitSw 3	BitSw4	Speed	Auto Neg Advertise
ON	Don't Care	1000M	10/100/1000
OFF	ON	100M	10/100
OFF	OFF	10M	10

Note,

When the fibre interface is used, only 1000M and 100M options are valid.

2.2.1.4 Switch 5, Duplex

This switch controls the duplex mode of the port. When auto negotiation is enabled this controls the advertised options, whilst in manual mode, it controls the duplex mode.

ON	Full Duplex
OFF	Half Duplex

Note,

When the fibre interface is selected, only Full Duplex modes are supported.

2.2.2 Zero Touch Configuration Control

There are two bit switches concerned with the setup of the unit to support the zero touch configuration mode. When the FCM9004 uses the Zero Touch, Auto Boot intialisation it will listen for a beacon on the WAN. The beacon allows the FCM9004 to determine the correct tag values to use for a management connection to DHCP/TFTP/SNMP servers.

2.2.2.1 Switch 6, TAG Mode

This switch selects between the single tag push C-Tag or S-Tag modes and the double Tag push mode.

ON	Single C-Tag/S-Tag Push/Pop
OFF	Double Tag Push Pop

2.2.2.2 Switch 7, Boot Location / (Autoboot)

This switch enables the autoboot, Zero Touch Configuration mode.

ON	Auto Boot, ZTC enabled
OFF	Disabled, boot from local configuration

When auto boot is enabled the FCM9004 will listen for a beacon on the WAN port and then use the information gathered from this beacon to set up a management channel connection to DHCP and TFTP servers, and also to an SNMP manager.

2.2.3 Switch 8, Master Boot Control / (Factory Default)

This bit switch will return the unit back to the factory default settings and will also read the bit switches and configure the operating mode of the WAN port and Auto Boot operation.

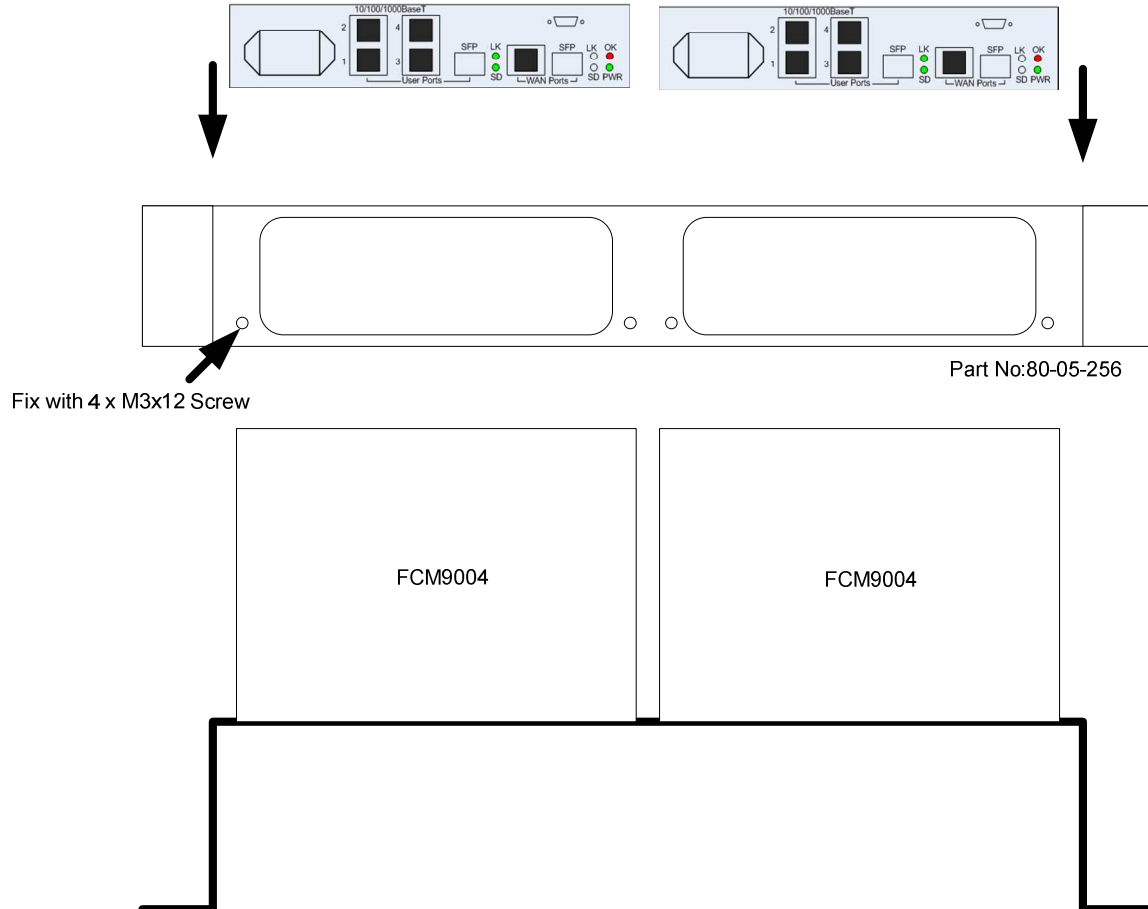
ON Normal Operation

OFF Return the unit to Factory Default on power up.

When a unit is returned to the factory default, the password will be returned to the default, "fcm9004" and all IP and remote access configurations will be lost.

2.3 Rackmounting

The FCM9004 is a standalone, desktop unit however it may be mounted in a standard 19 inch rack using the rack mounting kit, part number 80-05-256.



To mount the FCM9004 in the 19 inch rack mount adaptor first remove the two M3x12 screws and washers from the rear panel of the unit. Then align the FCM9004 rear panel with the mounting bracket, and secure the unit to the adaptor using the previously removed screws.

When rackmounting, please ensure that the bitswitches on the underside are correctly configured prior to mounting the units in the rack.

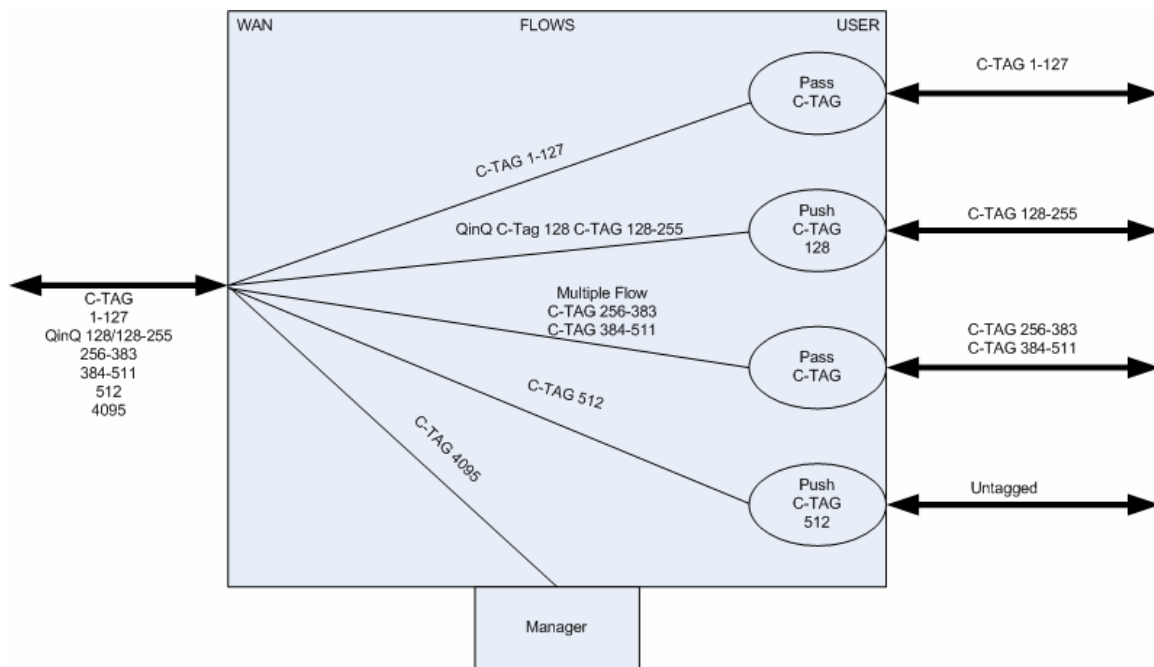
3 OPERATING MODES

The FCM9004 supports multiple modes of operation with support for pushing or popping tags. The FCM9004 supports two types of VLAN Tag, the basic IEEE 802.1q tag with Ethertype 8100, and referred to as C-Tag or Customer Tag within this manual. A second Tag type is referred to as the Service Tag, or S-Tag which has a configurable Ethertype with the default value of 9100.

The operating mode of the FCM9004 is defined in the traffic management section of the Data Port Setup Menu, see section 4.5.1

3.1 C-Tag Mode

In C-Tag mode, the FCM9004 will either push an IEEE 802.1q VLAN Tag onto a previously tagged or untagged frame, or will pass unchanged already tagged frames. The FCM9004 capabilities in C-Tag mode are shown below:



In C-Tag mode, flows are defined as groups of C-Tag VLAN ID's. A VLAN ID may be in the range 1 to 4095. In the above example, there are five flows defined as well as a management channel connection.

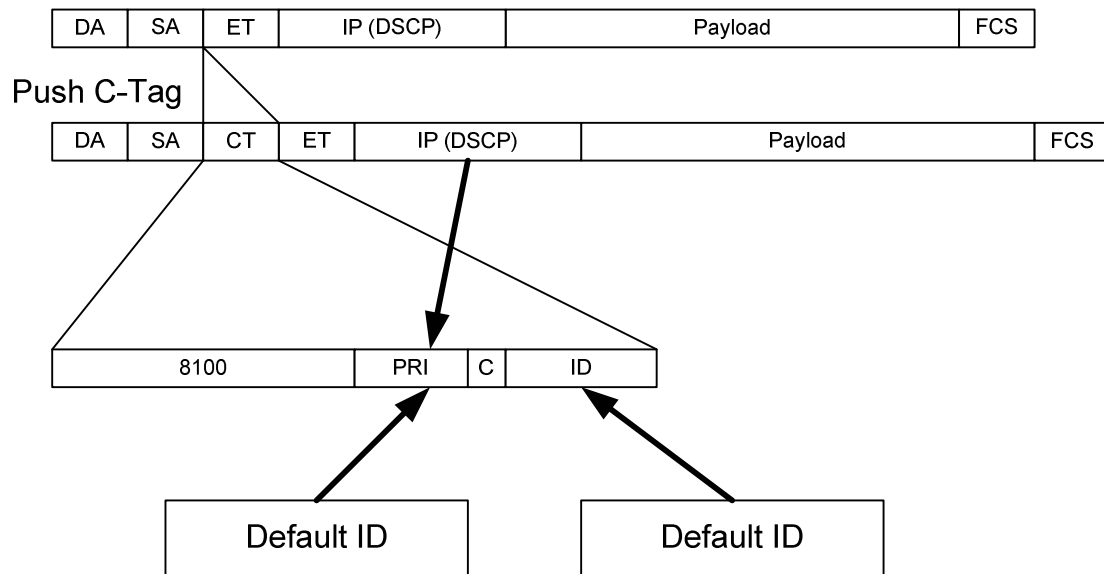
The user ports have the option of operating as an Access port where untagged frames will have a C-Tag pushed on ingress, and popped on egress. This is shown for C-TAG 512 which is pushed onto all untagged frames ingressing port 4.

Ports may also be configured to act as trunk ports where they will pass frames that ingress already containing VLAN Tags, and will discard any untagged frames.

Ports may also be configured for mixed mode operation where they will pass tagged frames and push a tag onto untagged frames.

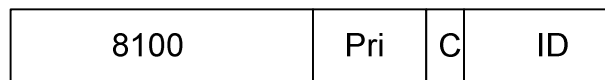
A port may also operate as a QinQ access port pushing a tag onto all incoming frames including those already tagged, as shown for C-Tag 128 above.

The action of pushing a C-Tag is shown below:



where a four byte VLAN Tag is inserted into the frame after the source address and before the Ethertype.

A C-Tag is made up of four bytes as shown below:



Where

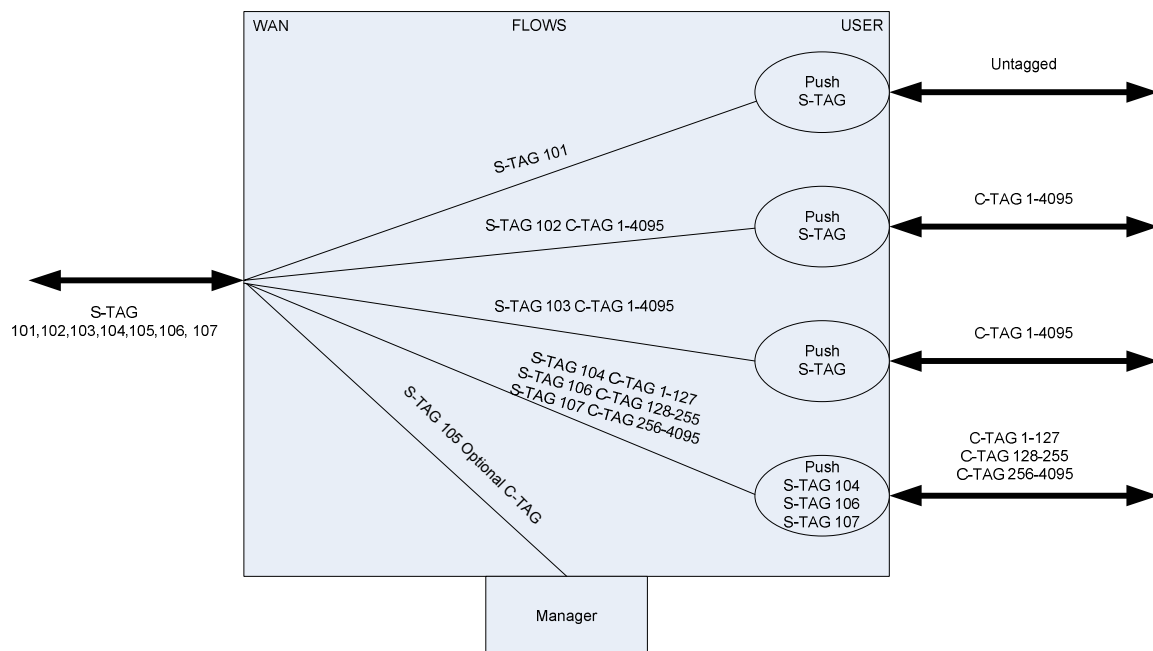
- 8100 A 2 byte Ethertype to identify IEEE 802.1q VLAN Tags
- Pri A 3 bit priority marker, 0 lowest – 7 highest
- C CFI, Canonical Form Indicator normally set to 0.
- ID A 12 bit identifier in range 1 to 4095

When a tag is constructed the ID is taken from the default setting for the port. The Tag Priority may either be set to the port default setting, or for IP packets with DSCP priorities the tag priority may be based on the packet DSCP value.

3.2 S-Tag Mode

In the FCM9004 Service Tags are used when an extra tag is to be pushed onto an already tagged frame. The Service Tag has a configurable Ethertype which by default is set to 9100. QinQ mode is supported by simply configuring the service tag ethertype to 8100.

The operation of the FCM9004 in the S-Tag mode is shown below:



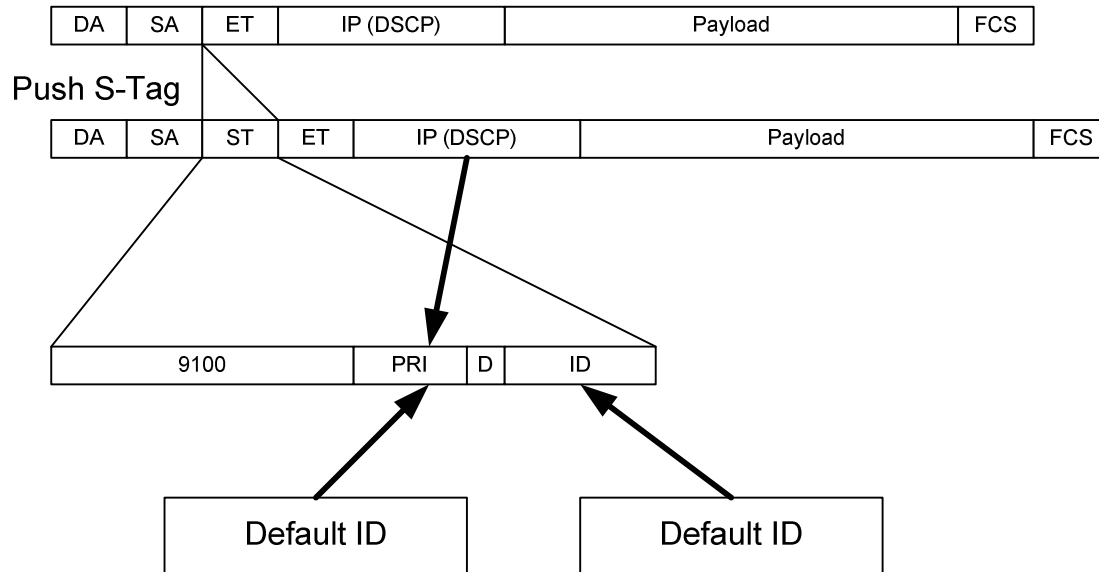
In this mode, both tagged and untagged frames are supported on the user ports. In the example above, port 1 is set to push the Stag 101 onto untagged frames at ingress.

On port 2, frames ingress already tagged and all have the Stag 102 pushed to give a packet with two tags, an Stag and a CTag

Port 4 shows the service multiplexing ability of the FCM9004 where which S-Tags is pushed is determined by the incoming CTag to give the multiple flows with Stag 104/106/107.

3.2.1 Pushing S-Tag onto Untagged Frame

When an untagged frame ingresses a user port in Stag mode it will have an Stag pushed as shown below:



Where

9100	S-Tag Ethertype
PRI	Priority
D	Discard Eligibility, 0 – Green, 1 = Yellow
ID	Stag ID in range 1 to 4095

When the pushed Stag is constructed it gains the Ethertype from the configured value. The default value is 9100, and setting this to 8100 will give QinQ operation, effectively VLAN within VLAN encapsulation.

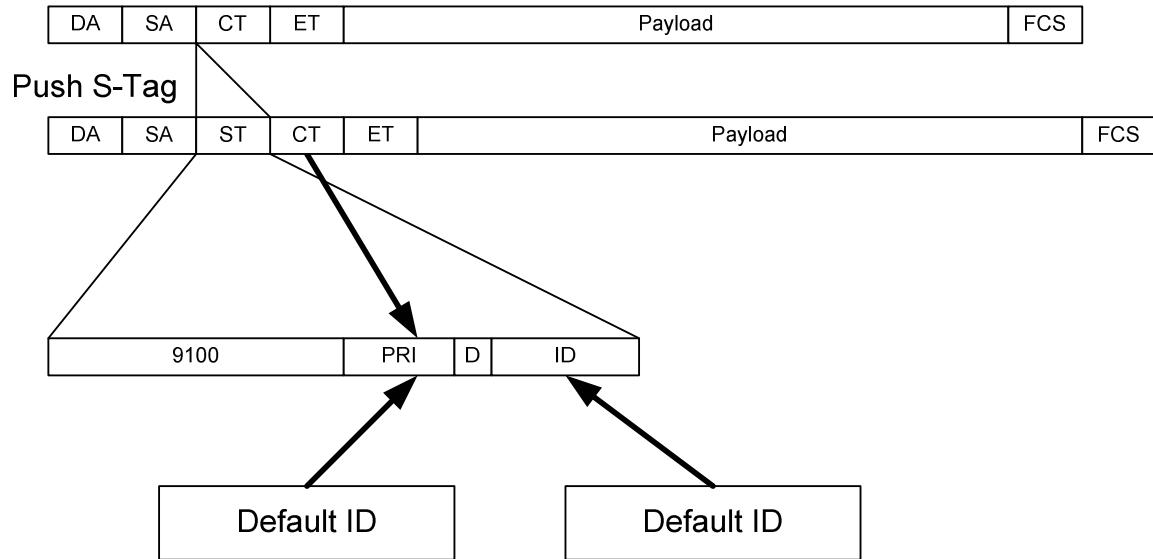
The priority for an untagged frame may either be set to the default port priority, or be set to inherit a value based on the incoming IP DSCP priority.

The D or DEI bit will be set by the policer to colour mark the packet on egress on the WAN port.

The ID is the value defined for the flow assigned to the port.

3.2.2 Pushing S-Tag onto Tagged Frame

When a tagged frame ingresses a user port in Stag mode it will have an Stag pushed as shown below:



Where

9100	S-Tag Ethertype
PRI	Priority
D	Discard Eligibility, 0 – Green, 1 = Yellow
ID	Stag ID in range 1 to 4095

When the pushed Stag is constructed it gains the Ethertype from the configured value. The default value is 9100, and setting this to 8100 will give QinQ operation, effectively VLAN within VLAN encapsulation.

The priority for an tagged frame may either be set to the default port priority, or be set to inherit a value based on the incoming C-Tag priority.

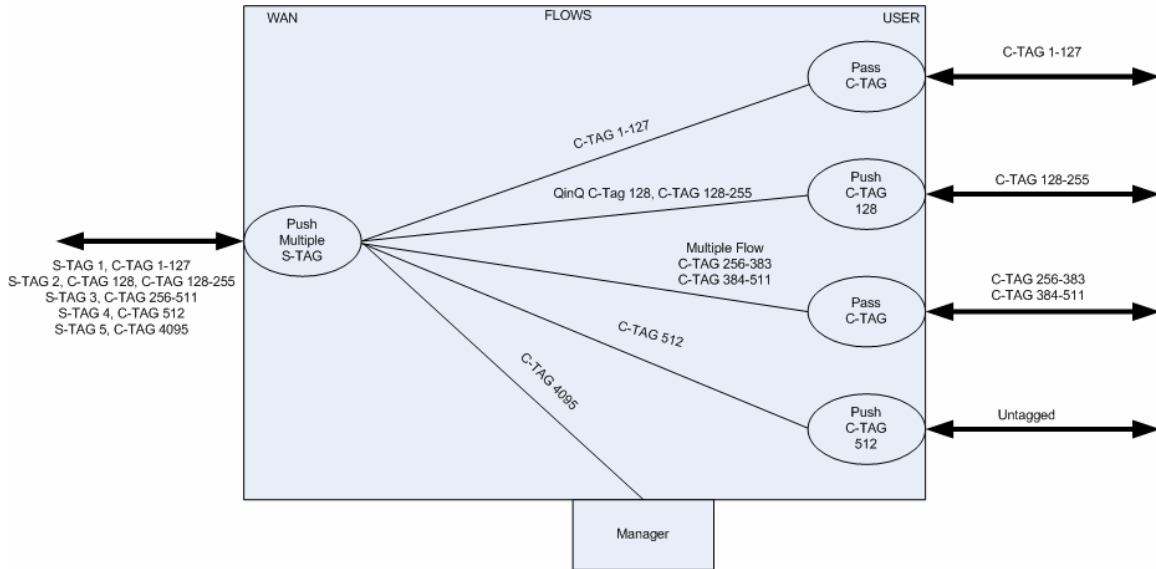
The D or DEI bit will be set by the policer to colour mark the packet on egress on the WAN port.

The ID is the value defined for the flow assigned to the port.

3.3 Double Tag Mode

Double tag mode allows the FCM9004 to push both a C-Tag and S-Tag onto a user frame. The double tag mode will push both C-Tag and S-Tags onto untagged frames at ingress. For tagged frames, if the ID is within the allocated range, the C-Tag will be passed, and the S-Tag will be pushed. In this mode, the allowable C-Tag ID's are limited to the range 1 to 4095 across all ports and flows.

The diagram below shows the operation of Double Tag mode



As can be seen in double tag mode, there are two separate tag processing functions, one on ingress to the user port and one on egress from the network port.

On ingress to a user port, an untagged frame may either be discarded or have a C-Tag pushed into the frame. A tagged frame ingressing a user port may have a QinQ tag pushed, may be passed unchanged if the ID is within a flow allocation, otherwise it will also be discarded.

One, or more, flows may be defined per user port with the flow being defined by the C-Tag range. In the example above, port 1 has a flow defined which includes C-Tag ID 1 to 127, whilst port 3 has two flows defined, one including ID's 256 to 383, and one including 384 to 511. Port 4, on the other hand is set to push the tag 512 onto incoming untagged frames.

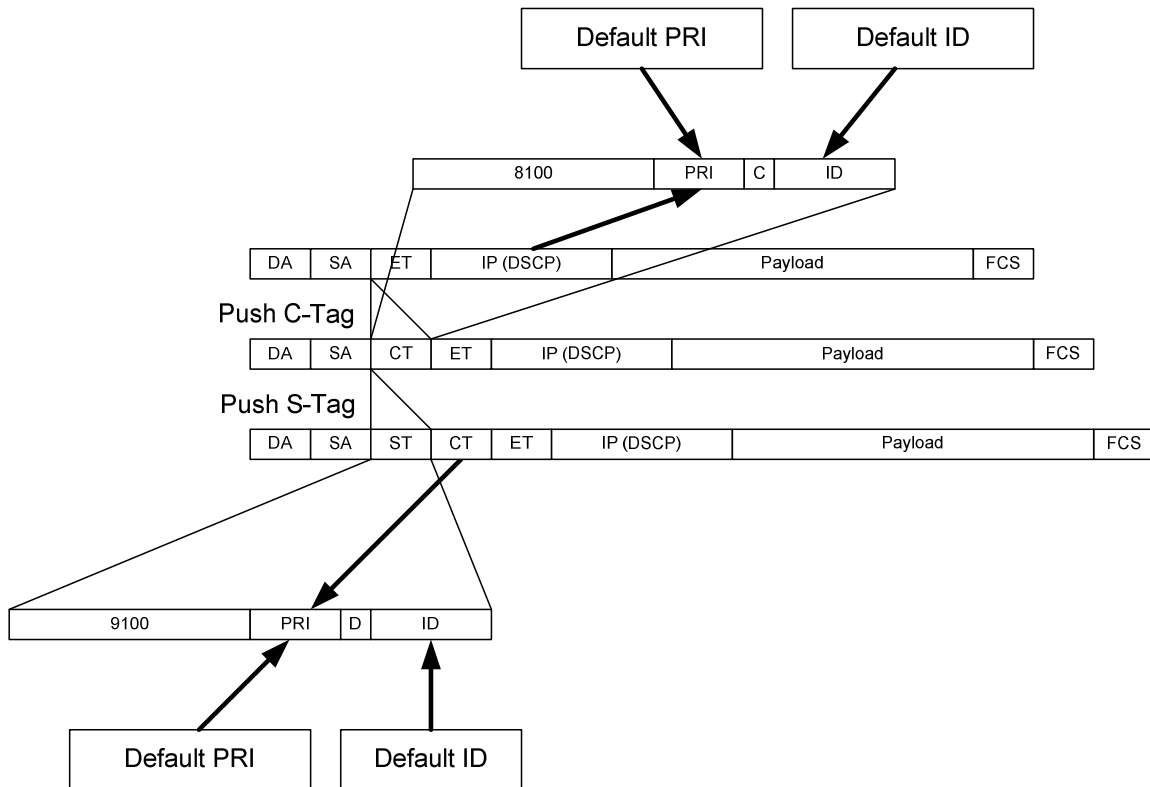
On egress from the WAN port, each flow has a defined S-Tag pushed onto it. Each flow may use a different S-Tag ID, or one or more flows may share S-Tag ID's.

A typical application of this mode would be to push C-Tags onto the user frames to identify which port or service the frames belonged to, whilst all frames had the same S-Tag pushed to identify the customer within the core network.

The construction of the frames traversing the FCM9004 in the double tag mode are as follows:

3.3.1 Untagged Frame Ingress

When an untagged frame ingresses a user port it will have both a C-Tag and S-Tag pushed onto the frame.

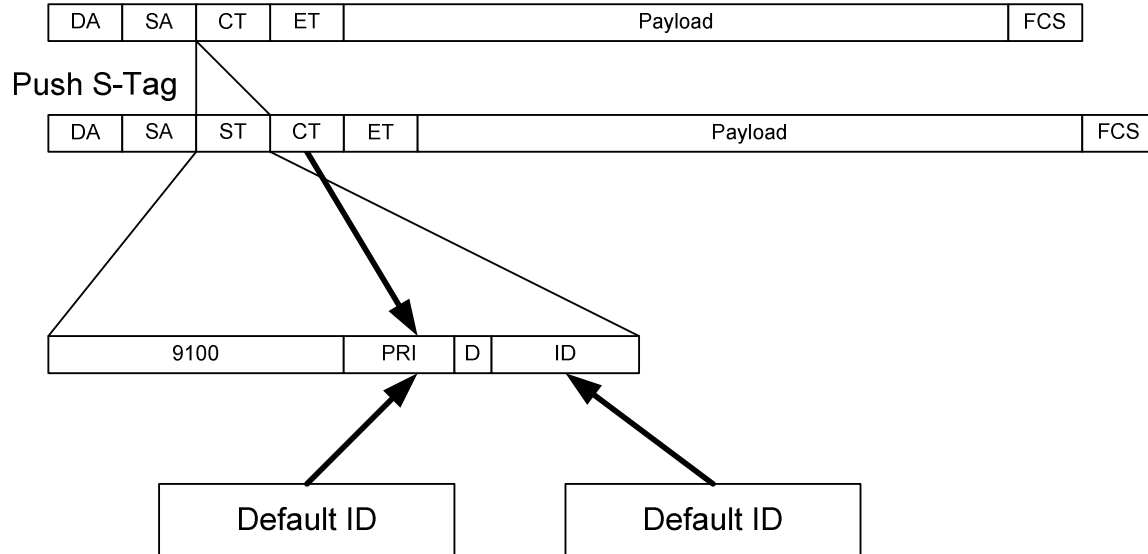


Here the untagged frame first has a C-Tag pushed. The ID used is the configured value for the port, whilst the priority may either be inherited from the incoming DSCP, or set to the default port value.

On egress, an S-Tag is then pushed into the frame using the configured values for ETYPE (9100) and ID. The priority for the S-Tag may be inherited from the C-Tag priority, or use the default value for the flow.

3.3.2 Tagged Frame Ingress

In double tag mode, when a tagged frame ingresses a user port, it will have an S-Tag pushed onto it. The priority within the S-Tag may be either defined for all frames, or be set to be inherited from the C-Tag as shown below:



Where

9100	S-Tag Ethertype
PRI	Priority
D	Discard Eligibility, 0 – Green, 1 = Yellow
ID	Stag ID in range 1 to 4095

When the pushed Stag is constructed it gains the Ethertype from the configured value. The default value is 9100, and setting this to 8100 will give QinQ operation, effectively VLAN within VLAN encapsulation.

The priority for an tagged frame may either be set to the default port priority, or be set to inherit a value based on the incoming C-Tag priority.

The D or DEI bit will be set by the policer to colour mark the packet on egress on the WAN port.

The ID is the value defined for the flow assigned to the port.

4 CONFIGURATION

The FCM9004 is configured and managed using a simple, menu driven user interface accessible using either a local craft terminal or remotely using TELNET.

Once you log onto the device the top level menu is as below:

```

Metrodata FCM9004 "FCM9004"                      Alarms: Major
MAIN SET-UP
Global status                                     <display>
Operational Modes                               <menu>
Flows (services)                               <menu>
Port set-up                                     <menu>
V.24 set-up                                     <menu>
Management Entity                             <menu>
System                                          <menu>
Update EEPROM
Circuit/Flow Tests                             <menu>
First CAPITAL - select item
<escape> - exit menu

```

To select a particular menu item, type the first, or highlighted, capital letter in the menu description, for example <d> for the Data port set-up, or <m> for Management.

The type of item is displayed alongside the description:

```

<menu>      There is a sub menu system below this item
<display>   There is a status display screen below this item
"value"     This item is a direct value which may be modified.

```

Value items come in two different types, those where a character string must be entered, or where a list of possible items may be toggled through. For toggle list items, use <SPACE> to select the next option and <ENTER> to accept.

To exit a menu, and return to the previous level type <ESCAPE>

4.1 System Configuration

The system menu provides the basic administrative configuration items for the FCM9004. The system menu is shown below:

```

Metrodata FCM9004 "FCM9004"                                Alarms: Major

SYSTEM

Time & data                                <menu>
Node name                                  FCM9004
pRovider ID
Access Control                            <menu>
welCome screen                          <menu>
Software version                          Main 8.20 / Boot 5.5

Output config                            <menu>
Input config                             <menu>

Warm start
Cold start
Event logs                                <menu>
>

First CAPITAL - select item
> - next page
<escape> - exit menu

```

and the second page, accessible through the ">" key

```

Metrodata FCM9004 "FCM9004"                                Alarms: Major

SYSTEM
<

Zero touch Config                            <menu>

First CAPITAL - select item
< - next page
<escape> - exit menu

```

Note, the previous page is accessed using the '<' key, <escape> will ext the system menu and return to the main setup menu.

4.1.1 Setting the Time and Date

The FCM9004 does not have a non volatile real time clock, instead it uses NTP to set the date and time following power up. In applications where NTP is not available, the FCM9004 defaults to providing a simple uptime display.

To configure the NTP parameters select the “Time and Date” menu from the system menu. The menu is shown below:

```

Metrodata FCM9004 "FCM9004"                               Alarms: Major

TIME & DATE

local Time           10:37:25
local Date           Mon 12/11/2012
system up time       0d1h14m25s
time Zone            GMT+0
NTP server            192.168.0.100
last sync            10:37:22 Mon 12/11/2012
Sync now

First CAPITAL - select item

<escape> - exit menu
    
```

If NTP is available, then the time zone and NTP server address must be configured.

4.1.1.1 Time Zone

Since NTP uses GMT as the baseline time, time zone adjustment is required to enable the correct time to be displayed wherever the unit is deployed globally.

The time zone may be adjusted by +/- 12 hours from GMT.

4.1.1.2 NTP Server

For NTP to operate correctly, the FCM9004 must be configured with the IP address of an authoritative NTP time server.

4.1.1.3 Sync Now

If the NTP server has not yet synchronised, it is possible for the user to force a manual synchronisation by issuing a Sync Now command.

Following power up, the NTP standard calls for a random delay before the NTP client will request sync from the server, manual sync will speed this process up if necessary.

4.1.2 Setting the Node Name

To enable identification of the FCM9004 it is useful to enter a meaningful name for the unit. The node name is entered as a string of upto 32 alpha numeric characters including spaces.

4.1.3 Provider ID

The provider ID is used during zero touch configuration and is used to identify the beacons that should be used when multiple beacons are present.

If the provider ID is left blank, the FCM9004 will listen for any beacon whatever the provider ID, whilst if a value is entered, only beacons with a matching ID will be used.

The provider ID is not cleared by a cold start, and must be cleared manually if necessary.

The provider ID is a string of upto 16 characters.

4.1.4 Access Control

The access control menu configures the user access security parameters for the unit. The Access Control Menu is shown below:

```
Metrodata FCM9004 "FCM9004_left"
Major
```

Alarms:

ACCESS CONTROL

```
Password          *****
'View' user       Enabled
Super Me         No
TACACS+          <menu>
```

```
First CAPITAL - select item
<escape> - exit menu
```

4.1.4.1 Setting the Local Password

The local password for the FCM9004 may be changed using the system menu. The default password is "FCM9004", however, for deployment a more secure password may be required.

To change the unit password, select "Password" from the system menu. The FCM9004 will display the following:

Enter new password

Password >

Enter the new password, upto 16 alphanumeric characters. For security each character is shown on screen as an asterisk “*”. Once the new password is entered the display changes to:

Enter new password

Password > *****

Verify >

Re enter the new password to verify the change. If the password is verified the unit will assume the new password for the next logon.

4.1.4.1.1 Default Unit Password

The default unit password is FCM9004 and is case insensitive.

4.1.4.1.2 Password Recovery

If the unit password is lost, it may be recovered by cold starting the unit using the bit switches on the underside of the unit. A cold start will erase the unit configuration and return the unit to factory default, with password FCM9004.

4.1.4.2 View User

The FCM9004 supports two levels of access, Admin and View. An ADMIN user has full access rights over the FCM9004 configuration. A View user has read only access to the configuration.

For security, it may be desirable to disable the view user, non password protected access to the unit. This can be achieved by selecting the View User menu item and toggling the option to Disabled. When disabled, it will not be possible to view the configuration without the correct password.

4.1.4.3 Super Me

The Super Me menu option provides a facility to promote an admin user to super user. In super user mode some further diagnostic menu options are made available. Super user Mode will only normally be required when instructed by Metrodata Technical Support in order to extract detailed status information from the unit.

4.1.4.4 TACACS+

Where greater access control and security is required, the FCM9004 units support TACACS+ for central password authentication.

Metrodata FCM9004 ""

Alarms: Major

TACACS+

Authentication	TACACS+, Local
Timeout	3
Retries	3
Server	192.168.100.45
Encryption key	*****

First CAPITAL - select item
<escape> - exit menu

4.1.4.4.1 Authentication

The FCM9004 supports three modes of password access control and authentication. The options are:

Local	(Default) The password access control is handled locally by the FCM9004 unit and the unit local password should be used to log in.
TACACS+, Local	In this mode, the FCM9004 unit will attempt to contact the TACACS+ server for authentication, however if the server cannot be accessed, it will fall back to local password administration.
TACACS+	Use TACACS+ for password authentication. If the server is unavailable, access to the unit will not be allowed.

4.1.4.4.2 Timeout

The timeout defines how long the FCM9004 unit will wait for a response from the TACACS+ server. The timeout is specified in seconds in the range 1 to 90 seconds.

4.1.4.4.3 Retries

This defines the number of attempts the FCM9004 unit will make when trying to access the TACACS+ server. The valid range is 1 to 10.

4.1.4.4.4 Server

This defines the IP address of the TACACS+ Authentication server. When a login attempt is made, this server will be accessed.

4.1.4.4.5 Encryption Key

This key is used by both the FCM9004 and the TACACS+ server to provide a secure, encrypted password exchange and authentication. This must be set the same on both FCM9004 and Server. For security, the key is hidden.

4.1.5 Welcome Screen

This menu allows for a user defined welcome screen to be used rather than the standard Metrodata screen. By default the user defined screen is disabled but once enabled it is configured line by line as shown:

```

Metrodata FCM9004 "FCM9004"                                Alarms: Major

WELCOME SCREEN

Welcome screen                                Enabled
1st line                                     This is an example
2nd line                                     of a customised
3rd line                                     Welcome Screen
4th line
5th line                                     You may define upto
6th line                                     8 lines of text
7th line
8th line                                     Here is line number 8
Clear all text
Display Screen                                <display>

First CAPITAL - select item

<escape> - exit menu

```

Once the welcome screen has been defined, it may be displayed for checking by selecting display screen.

4.1.5.1 Display Screen

This menu displays the welcome screen as it will be seen by users attempting to log on to the unit.

```

Metrodata FCM9004 "FCM9004"                                Alarms: Major

                                WELCOME SCREEN
                                -----

This is an example
of a customised
Welcome Screen

You may define upto
8 lines of text

Here is line number 8

<escape> - exit, other key - refresh

```

4.1.6 Output Config

This menu item allows the user to output the ASCII configuration file to the screen. If a text capture is enabled the file may be saved and reused to reload the configuration at a later date if necessary.

When the output config option is selected the following screen appears

```
Metrodata FCM9004 "FCM9004"                      Alarms: Major
Start capture then press a key
After transfer, stop capture then press another key
```

At this point enable the text capture and then press a key to continue.

The configuration file will be output to the screen in an ASCII form, readable but not really understandable as shown by the extract from a config file shown below:

```
cfmep.0.ma=0
cfmep.0.mid=101
cfmep.0.if=11
cfmep.0.d=1
cfmep.0.e=1
cfmep.0.s=1
rt.0.d=192.168.0.0
rt.0.i=1
rt.0.ty=3
rt.0.p=2
rt.0.m=255.255.255.0
rt.0.ti=2
rt.1.i=1
rt.1.n=192.168.0.254
rt.1.ty=4
rt.1.p=2
snmp.n=FCM9004
snmp.l=Test Network
welcome.0=This is an example
welcome.1=of a customised
welcome.2=Welcome Screen
welcome.4=You may define upto
welcome.5=8 lines of text.
welcome.8=Here is line number 8
```

To return the main system menu, stop the text capture and hit any key to proceed.

4.1.7 Input Config

If a config file has been captured it may be reloaded to the unit using the Input Config command.

Selecting Input Config gives the following message:

Send File. Esc to end.

Use a send text file option from the terminal package, and select the stored configuration file. Once the file has been sent, type ESC to finish.

Once loaded the unit will reboot to load the configuration.

If errors are detected in the configuration file, the first error will be reported with the line number.

4.1.8 Warm Start

A warm start will force the unit to reboot and reload the configuration stored in the EEPROM. Note, any changes to the configuration made that have not been saved WILL be lost.

When a TELNET user issues a warm start request, the FCM9004 will indicate that a warm start is about to take place, and then close the connection.

4.1.9 Cold Start

A Cold Start will erase the configuration EEPROM and return the unit to the factory default condition as defined by the bit switch settings.

Note, that a cold start will erase all IP addresses and routing table entries and it is highly likely that remote access will be lost following a cold start.

Due to the drastic nature of a cold start, the command requires user confirmation before cold starting.

Note, the cold start will not clear the provider id used by the beacon system.

4.1.10 Event Logs

Where unexpected operation is observed, viewing the event logs may give an indication of when events occurred that may have given rise to the issue.

There are three event logs available to view, along with a full, amalgamated log of all events as shown:

Metrodata FCM9004 "FCM9004"

Alarms: Major

EVENT LOGS

FCM9004 USER MANUAL

System event log	<display>
Alarm event log	<display>
Config. event log	<display>
Full event log	<display>

First CAPITAL - select item

<escape> - exit menu

The individual event logs are shown below:

4.1.10.1 System Event Log

The system event log gives the time of system level events such as system restarts, or NTP updates.

Metrodata FCM9004 "FCM9004"

Alarms: Major

--- System Event Log ---

12/11/2012 10:37:22	clock set via NTP
12/11/2012 09:26:05	NTP failed
12/11/2012 09:23:00	performance log cleared
12/11/2012 09:23:00	rtc needs to be set
12/11/2012 09:23:00	config restored
12/11/2012 09:23:00	event logs cleared

press any key to continue

4.1.10.2 Alarm Event Log

The Alarm event log lists the time of all alarm events including start and finish time.

Metrodata FCM9004 "FCM9004"

Alarms: Major

--- Alarm Event Log ---

12/11/2012 09:26:45	Minor OFF Flow2
12/11/2012 09:26:45	Minor OFF Flow1
12/11/2012 09:26:45	Major OFF WAN
12/11/2012 09:23:38	Major ON WAN
12/11/2012 09:23:35	Minor ON Flow2
12/11/2012 09:23:35	Minor ON Flow1

press any key to continue

4.1.10.3 Config Event Log

The config event log shows the time of all configuration changes, though not the actual changes made. It is often the case that things stopped working after a configuration change.

Metrodata FCM9004 "FCM9004"

Alarms: Major

--- Config Event Log ---

12/11/2012 09:26:45	Config. updated
12/11/2012 09:26:45	Config. updated
12/11/2012 09:26:45	Config. updated
12/11/2012 09:23:38	Config. updated
12/11/2012 09:23:38	Config. updated
12/11/2012 09:23:35	Default config. set

press any key to continue

4.1.10.4 Full Event Log

The full event log shows all events in time order, this log can get quite large so the individual logs may prove more informative.

Metrodata FCM9004 "FCM9004"

Alarms: Major

--- Full Event Log ---

12/11/2012 10:37:22	clock set via NTP
12/11/2012 09:26:45	Config. updated
12/11/2012 09:26:45	Config. updated
12/11/2012 09:26:45	Config. updated
12/11/2012 09:26:45	Minor OFF Flow2
12/11/2012 09:26:45	Minor OFF Flow1
12/11/2012 09:26:45	Major OFF WAN
12/11/2012 09:26:05	NTP failed
12/11/2012 09:23:38	Config. updated
12/11/2012 09:23:38	Config. updated
12/11/2012 09:23:38	Major ON WAN
12/11/2012 09:23:35	Minor ON Flow2
12/11/2012 09:23:35	Minor ON Flow1
12/11/2012 09:23:38	Major ON WAN
12/11/2012 09:23:35	Minor ON Flow2
12/11/2012 09:23:35	Minor ON Flow1
12/11/2012 09:23:35	Default config. set
12/11/2012 09:23:00	performance log cleared
12/11/2012 09:23:00	rtc needs to be set
12/11/2012 09:23:00	config restored
12/11/2012 09:23:00	event logs cleared

press any key to continue

4.1.11 Zero Touch Configuration

The FCM9004 supports a zero touch configuration mode of operation whereby the unit will power up, listen for a beacon on the management channel and then automatically request an IP address using DHCP and configuration using TFTP.

The ZTC menu is as shown below:

```
Metrodata FCM9004 "FCM9004_left"
Major
```

Alarms:

```
ZERO-TOUCH CONFIG
```

```
State           Inactive
s/w Upgrade time Never
```

```
First CAPITAL - select item
<escape> - exit menu
```

4.1.11.1 Zero Touch State

This menu item serves as both an enable, and a status display for the units progress during zero touch configuration.

To enable Zero Touch, which is the normal factory default, select Zero Touch and toggle the state to START which will initiate the process of checking for a beacon, and then loading a config file.

To disable the Zero Touch Configuration, change the state to INACTIVE.

The possible states that the zero touch configuration may be in are listed below:

INACTIVE Zero Touch Configuration is disabled.

START Zero Touch Configuration is initialising

LISTENING Zero Touch Configuration is listening for the beacon on the network port.

FOUND A beacon has been detected and an IP address has been obtained.

CONFIGURING Zero Touch Configuration is downloading, or trying to download, the configuration file from the supplied TFTP server.

CONFIGURED Zero Touch Configuration is complete

4.1.11.2 Software Upgrade Time

Part of the Zero Touch Configuration Beacon protocol is to indicate the current software revision. When a new software revision has been checked out and is ready to release the file should be loaded to the TFTP server. The beacon software version number should be updated and then units that are enabled to automatically update their software will do so at a pre determined time. To prevent all units attempting to upgrade at once the time may be defined for each unit.

The options are:

NEVER	Do not automatically upgrade the firmware.
RANDOMIZED	Wait a random time of between 0 and 256 minutes from the beacon.
FIXED	Perform the upgrade the defined time.
IMMEDIATELY	Perform the upgrade immediately on receiving a beacon indicating a new version of code is available.

4.2 Management Entity

The Management Entity menu is where the remote access to the FCM9004 is configured. The top level management entity menu is as below:

```

Metrodata FCM9004 "FCM9004"                                Alarms: Major

MANAGEMENT ENTITY

intErface                                <menu>
Ip                                         <menu>
Udp                                       <menu>
tCp                                       <menu>
sNmp                                       <menu>
Telnet/SSH                               <menu>
tFtp                                       <menu>
Ping                                       <display>

First CAPITAL - select item

<escape> - exit menu

```

4.2.1 Interface

The interface menu configures the unit management interface.

```

Metrodata FCM9004 "FCM9004"                                Alarm: Major

INTERFACE

State                                     Up
Phys. address                             0:C0:81:0:13:ae
DHCP                                       Off
Ip addr                                   192.168.0.13
Net mask                                   255.255.255.0
At table                                   <display>
sTats                                     <display>

C-VLAN                                    none
QinQ/S-VLAN                              4095
802.1p priority                           7

First CAPITAL - select item

<escape> - exit menu

```

4.2.1.1 STATE

The Management port state may be either UP or DOWN as below:

UP	Management port is active and will pass traffic
DOWN	Management Port is down and is inactive.

For normal operation the state must be up.

Note, when ZTC is enabled the state shows as down while the unit is listening for the beacon to determine the correct management WAN interface and the correct S-Tag/C-Tag combination. As soon as the beacon is received, the state will automatically assume the UP state.

4.2.1.2 Physical Address

This is a display item only, and shows the unit MAC Address.

4.2.1.3 DHCP

DHCP allows the FCM9004 to get an IP address automatically from a centrally administered server.

DHCP can be enabled, or disabled where the IP address must be manually configured on each unit.

When DHCP is enabled, a unit powers up and broadcasts a DHCP request for an address. Once a server hears the request, it will respond with an address the unit can use.

DHCP is always enabled when ZTC is used.

4.2.1.4 IP Address

In order to access the FCM9004 remotely it must be configured with an IP address. This may be obtained either using DHCP, in which case this will be configured automatically, or Manually if DHCP is disabled.

The IP address should be entered in the format AA.BB.CC.DD

By default, the unit assumes the IP address 169.254.42.42 regardless of whether DHCP is enabled or not. If a DHCP is enabled and a server does not respond then it will keep this address, otherwise it will assume the DHCP supplied address.

4.2.1.5 Net Mask

The network mask is used to differentiate the network address from the host address. By default this is set to the class B value 255.255.0.0 to agree with the default IP address of 169.254.42.42

If DHCP is enabled, the net mask is served by the DHCP server and is configured automatically.

4.2.1.6 AT Table

The AT Table display allows the user to view the device ARP table. This may be useful when devices are having problems communicating. The ARP table is shown as below:

Metrodata FCM9004 "FCM9004"

Alarms: Major

AT TABLE

IP Address	Ethernet Address	Age
192.168.0.254	0.60.3e.99.f.e2	11231
192.168.0.100	0.9.5b.1c.2e.a8	6967

<Escape> - exit, other key - refresh

4.2.1.7 Stats

To enable diagnosis of communication problems a full set of SNMP statistics are provided for the management interface as shown below:

```

Metrodata FCM9004 "FCM9004"                                Alarms: Major

Interface Statistics
-----

ifInOctets           287935
ifInUcastPkts        2443
ifInNUcastPkts       406
ifInDiscards         0
ifInErrors           0
ifInUnknownProtos    0
ifOutOctets          2564
ifOutUcastPkts       109
ifOutNUcastPkts      53
ifOutErrors          0
ifOutQLen            0

<Escape> - exit, other key - refresh

```

4.2.1.8 C-VLAN

This is the value of IEEE 802.1q TAG that is used by the manager when transmitting or receiving frames.

When frames are to be sent with a TAG, the acceptable values are in the range 1 to 4095.

When frames are to be sent untagged, the value is NONE.

4.2.1.9 QinQ/S-VLAN

This value defines the outer tag that will be used. Acceptable values for tagged frames are 1 to 4095, or NONE for untagged.

Note, the Ethertype used for the S-VLAN is configurable, but defaults to 9100.

4.2.1.10 802.1p Priority

When the manager transmits tagged frames, they are sent with the configured priority.

0 Low Priority to 7 Highest Priority

4.2.2 IP Configuration

The IP configuration menu is as shown below:

```

Metrodata FCM9004 "FCM9004"                                Alarms: Major

IP

default TTL                                32
DSCP priority                             0
Routing table                             <display>
Forwarding                                Disabled
Stats.                                    <display>

First CAPITAL - select item

<escape> - exit menu

```

4.2.2.1 Default TTL

When packets are generated by the FCM9004 manager, they will be transmitted with the value configured here. It is unlikely that the default value of 32 will need to be changed, though it may be set in the range 1 to 255 bearing in mind that the TTL value is decremented by 1 for each router on the route.

4.2.2.2 DSCP Priority

When packets are transmitted by the FCM9004 manager, they will be transmitted with the configured DSCP (Differentiated Services Code Point) value. DSCP may be specified in the range 0 to 63 with 0 being best effort.

The exact meaning and priority of DSCP values are network dependant , though the following table usually applies for traffic classification.

Discard Probability	Class 1	Class 2	Class 3	Class 4
Low	DSCP 10	DSCP 18	DSCP 26	DSCP 34
Medium	DSCP 12	DSCP 20	DSCP 28	DSCP 36
High	DSCP 14	DSCP 22	DSCP 30	DSCP 38

4.2.2.3 Routing Table

In order to operate within a routed network, and access hosts that are not located on the same subnet, the routing table must be configured. The FCM9004 supports static routing only.

The routing table menu is as shown below:

```

Metrodata FCM9004 "FCM9004"
Destination Next Hop      I/F    Type      Prot. Age  Mask
-----
192.168.0.0 0.0.0.0      Mgmt   direct   local 12045 255.255.255.0
0.0.0.0     192.168.0.254 Mgmt   indirect local 12046 0.0.0.0

```

A - add entry
D - delete entry
any other key to exit:

To add a new route you need to know three parameters,

Destination Network Address

Destination Network Mask

Next Hop Router Address

For example, the table above has the default route included where

```

Destination = 0.0.0.0
Mask        = 0.0.0.0
Next Hop    = 192.168.0.254

```

When DHCP is enabled, the default route will be added automatically if it is supplied by the DHCP server.

4.2.2.4 Forwarding

The FCM9004 does not support routing between its ports, only switching and therefore Forwarding is disabled.

4.2.2.5 IP Statistics

The manager provides a full set of SNMP statistics for the IP layer as shown below:

```

Metrodata FCM9004 "FCM9004_Right"                Alarms: Major
IP Statistics
-----
ipInReceives          3031
ipInHdrErrors         0
ipInAddrErrors        0
ipForwDatagrams       0
ipInUnknownProtos    0
ipInDiscards          0
ipInDelivers          3031
ipOutRequests         2861
ipOutDiscards         0
ipOutNoRoutes         0
ipReasmReqds          0
ipReasmOKs            0
ipReasmFails          0
ipFragOKs             0
ipFragFails           0
ipFragCreates         0
ipRoutingDiscards     0

press any key to continue

```

The following two screens display the ICMP protocol statistics

```

icmpInMsgs            362
icmpInErrors          0
icmpInDestUnreaches  0
icmpInTimeExcds      0
icmpInParmProbs      0
icmpInSrcQuenchs     0
icmpInRedirects      0
icmpInEchos           362
icmpInEchoReps       0
icmpInTimestamps     0
icmpInTimestampReps  0
icmpInAddrMasks      0
icmpInAddrMaskReps   0
icmpOutMsgs           362
icmpOutErrors         0
icmpOutDestUnreaches 0
icmpOutTimeExcds     0
icmpOutParmProbs     0
icmpOutSrcQuenchs    0
icmpOutRedirects     0

press any key to continue

icmpOutEchos          0
icmpOutEchoReps       364
icmpOutTimestamps     0
icmpOutTimestampReps 0
icmpOutAddrMasks      0
icmpOutAddrMaskReps   0

press any key to continue

```

4.2.3 UDP

The FCM9004 uses UDP for SNMP management. This menu displays the port numbers used and statistics.

```

Metrodata FCM9004 "FCM9004"
UDP
snmp Port          161
snmp Trap port     162
Stats              <display>

First CAPITAL - select item
<escape> - exit menu

```

Alarms: Major

4.2.3.1 SNMP Ports

As defined by the IANA, the standard UDP port numbers are

```

SNMP      161
SNMP Trap 162

```


4.2.3.2 Statistics

The FCM9004 provides the SNMP UDP layer mib statistics

```

Metrodata FCM9004 "FCM9004_Right"                                Alarms: Major

UDP Statistics
-----
udpInDatagrams    2340
udpNoPorts        323
udpInErrors       0
udpOutDatagrams   2071

press any key to continue

```

4.2.4 TCP

The TCP menu gives information relating to the TCP layer

```

Metrodata FCM9004 "FCM9004"                                Alarms: Major

TCP

Stats.                <display>
Conn. table           <display>

First CAPITAL - select item

<escape> - exit menu

```

TCP is a connection orientated protocol and the conn table gives information relating to current TCP sessions, whilst the stats menu shows the SNMP MIB TCP statistics.

4.2.4.1 Statistics

The TCP statistics available are as shown:

```

Metrodata FCM9004 "FCM9004_Right"                      Alarms: Major

TCP Statistics
-----
tcpActiveOpens      7
tcpPassiveOpens     0
tcpAttemptFails     0
tcpEstabResets      0
tcpInSegs           450
tcpOutSegs          550
tcpRetransSegs      0
tcpInErrs           0
tcpOutRsts          0

press any key to continue

```

4.2.4.2 Connection Table

The Connection table displays the list of the currently open sessions as shown

```

Metrodata FCM9004 "FCM9004_Right"                      Alarms: Major

TCP CONNECTION TABLE
-----

State      LocalAddress      Loc Port  RemAddress      Rem Port
-----
established 192.168.0.13      23        192.168.100.48  2711
synReceived 192.168.0.13      23        192.168.100.48  2687

<Escape> - exit, other key - refresh

```

The FCM9004 supports five concurrent Telnet or other TCP protocol sessions. An attempt to open a sixth session will be rejected by the FCM9004.

Due to the five session limit, it is vitally important that a timeout value is used for Telnet to force close them after a period of inactivity.

4.2.5 SNMP

The FCM9004 supports management access via SNMP V1 or V2c, which may be configured using the SNMP menu,

```

Metrodata FCM9004 "FCM9004 "                      Alarms: Major

SNMP

Read community      public
Write community     public
Trap community      public
Managers            <menu>
contact Person      Metrodata Limited,Fortune House,
                   Crabtree Office Village,Eversl..
Node name           FCM9004
Location            Test Network
Stats.              <display>
trap Alarms         <menu>

First CAPITAL - select item

<escape> - exit menu

```

4.2.5.1 Communities

The FCM9004 supports separate communities for Read, Write and Trap access. Communities provide a limited level of security within SNMP V1 as only requests with the correct community name will be actioned.

By default, all communities are set to PUBLIC.

The community names must be changed to match those used by the network management system.

4.2.5.2 Managers

The FCM9004 supports upto 10 separate SNMP Managers which may be configured using the managers menu system. Only SNMP polls and get/set requests from configured managers will be accepted.

The managers menu is as below:

```

Metrodata FCM9004 "FCM9004 "                      Alarms: Major
MANAGERS
1 - 192.168.100.45      <menu>
2 - 192.168.100.70      <menu>
Add manager              <menu>

First CAPITAL - select item
<escape> - exit menu

```

Here there are two managers currently configured which may be selected for viewing, editing by typing the manager number, in this case 1 which will then display the parameters for this manager:

```

Metrodata FCM9004 "FCM9004_Right"                  Alarms: Major
1 - 192.168.100.45
IP address          192.168.100.45
Access rights       Read-Write
receives Traps      Yes
snmp Version        SNMPv2c
Remove manager

First CAPITAL - select item
<escape> - exit menu

```

The parameters required for an SNMP manager are the IP address. Note, that the routing table must be configured where the manager is not on the same subnet as the FCM9004.

The manager configuration controls the access rights that the manager has, which may be NONE, READ-ONLY, or READ-WRITE.

The manager may also be set up for traps, if enabled the FCM9004 will generate traps destined for this manager when alarm events occur.

The FCM9004 supports SNMP V1 or V2c on a per manager basis.

If a manager is no longer required, the it maybe removed.

4.2.5.2.1 Dying Gasp Trap

When multiple managers are configured, the FCM9004 will issue the dying gasp trap to each manager in turn starting with manager 1.

As there is limited time to generate the Dying Gasp Trap it is quite likely that higher numbered managers will not receive this trap as the power will have failed by then.

4.2.5.3 Contact Person

The SNMP Contact person is the RFC-1213 MIB-2 SysContact MIB definition. This item is a string of upto 255 characters.

4.2.5.4 Node Name

The SNMP Node Name is the MIB-2 SysName MIB definition. This item is a string of up to 255 characters.

4.2.5.5 Location

The SNMP Location is the MIB-2 SysLocation MIB definition. This item is used to show the detailed location of the device. This item is a string of upto 255 characters.

4.2.5.6 SNMP Statistics

The FCM9004 provides a display of the MIB-2 SNMP statistics as shown:

Metrodata FCM9004 "FCM9004"
SNMP Statistics

Alarms: Major

```
-----
snmpInPkts          2165
snmpOutPkts         2216
snmpInBadVersions   0
snmpInBadCommunityNames 0
snmpInBadCommunityUses 0
snmpInASNParseErrs  0
snmpInTooBigs       0
snmpInNoSuchNames   0
snmpInBadValues     0
snmpInReadOnlys     0
snmpInGenErrs       0
snmpInTotalReqVars  6023
snmpInTotalSetVars  0
snmpInGetRequests   2018
snmpInGetNexts      147
snmpInSetRequests   0
snmpInGetResponses  0
snmpInTraps         0
```

press any key to continue:

```
snmpOutTooBigs      0
snmpOutNoSuchNames  322
snmpOutBadValues    0
snmpOutGenErrs      0
snmpOutGetRequests  0
snmpOutGetNexts     0
snmpOutSetRequests  0
snmpOutGetResponses 2166
snmpOutTraps        51
```

press any key to continue

4.2.5.7 Trap Alarms

The Trap Alarm Menu allows the user to control which of the wide range of possible alarms generated by the FCM9004 should generate traps.

Under this menu are all the port and other sources of alarms and each alarm is listed and may be set to generate a Trap, or if it is deemed unimportant, No-Trap.

The alarm types supported by the FCM9004 are listed below:

LKDN	Link Down
LLF	Link Loss Forwarding
FEFI	Far End Fault Indication, 100BaseFX only
OAM	Loss of link OAM connectivity messages
LOS	Loss of Optical Signal
NF	SFP Not Fitted
RDI	Receiving Service CFM RDI indications
NP	No CFM peer MEP discovered
XCON	Misconnected CFM MEP
ERR	Errored CFM messages
REM	Loss of remote CCM messages
MAC	Remote user port failure
RDI	Remote Defect Indication
SLA	SLA not being met
SFPA	SFP Diagnostic Alarm
SFPW	SFP Diagnostic Warning
OTDR	SFP OTDR value available

4.2.6 Telnet/SSH

The FCM9004 supports remote access using either TELNET or the more secure encrypted SSH V2. The menu is shown below:

```
Metrodata FCM9004 "FCM9004_left"
Major
```

Alarms:

```
TELNET/SSH
```

```
Access Method      SSH
Timeout            600
```

```
First CAPITAL - select item
<escape> - exit menu
```

4.2.6.1 Access Method

The access method selects between Telnet at SSH V2. By default following a cold start, Telnet is available.

If SSH access is enabled, two concurrent sessions are supported and access using Telnet is prevented.

The FCM9004 SSH V2 server has been verified with several of the more popular SSH clients including:

PUTTY

TeraTerm TTSSH

BitVise SSH Client

Note, when connecting to the FCM9004 SSH server there will be a delay of upto 15 seconds whilst the secure key calculation and key exchange process occurs. Once this is completed, the user interface operates as normal.

4.2.6.2 Timeout

To ensure that Telnet/SSH sessions are not left open, an inactivity timer is provided which will automatically shut down the session if it is not being used.

The default setting is 60 seconds, however a more practical value is 600, 10 minutes.

Setting the timeout to 0, disables the timer – however this must be done with care as unwanted Telnet/SSH sessions will never be cleared.

4.2.7 TFTP

The FCM9004 uses the TFTP protocol to enable file transfers into or out of the device. TFTP is a client/server protocol and the FCM9004 is capable of operating as either client or server.

4.2.7.1 Client Mode

In client mode, an external TFTP server must be running on a machine somewhere that is accessible at the configured address.

```

Metrodata FCM9004 "FCM9004"                      Alarms: Major

TFTP

Mode                      Client
remote IP                 192.168.0.100
Get new software          <display>
Boot s/w upgrade          <display>
get Config.
Put config.
put Report

```

```

First CAPITAL - select item

<escape> - exit menu

```

4.2.7.1.1 Remote IP

This is the IP address of the remote TFTP server which must be running in order for a TFTP transfer to take place.

4.2.7.1.2 Get New Software

This menu item is used to upgrade the system application firmware. Selecting this option will lead to the following display:

```

Metrodata FCM9004 "FCM9004_Right"                      Alarms: Major
TFTP Software Upgrade

CAUTION: Proceeding further will mean that the unit must be re-
started, and the performance log may be cleared, even if the
upgrade is unsuccessful. Are you sure you wish to continue?

```

At the prompt, confirm the action by typing <Y>, for Yes. The menu will now prompt for the file name.

Enter the file name.

The file will now download, with a block count to show activity and will then prompt the user to verify that the correct file has been downloaded

```

File name: fcm9004.87
Blocks received: 4371

File received successfully, length 2237623.
File contains:
Unit Description: fcm9004
Software Version: 8.7.[ib].1.24 25/10/2012 07:29:52 unreleased
This will replace:
Unit Description: fcm9004
Software Version: 8.7.[ib].1.34 08/11/2012 15:40:13 unreleased
The software will now be updated.
Are you sure this is what you want to do?

```

If this is correct, confirm <Y>, otherwise type <N> to stop the download. If the download is stopped, the system must be restarted.

Once the firmware upgrade has completed, the unit will automatically restart with the new firmware image and reload the configuration from EEPROM.

4.2.7.1.2.1 Failsafe Upgrade

The system software upgrade procedure uses a failsafe mechanism to prevent a system becoming unusable. When a unit is shipped from the factory, the base version of the application is stored in a locked portion of the flash memory. When a new version is loaded via tftp it will be programmed into flash as a second image, the original image is never erased, or overwritten. When the system reboots, the boot software compares the loaded versions of firmware and executes the most upto date version.

4.2.7.1.3 Boot Software Upgrade

There may be occasions when new features added to the main application code cannot be supported without changes to the boot loader code. The Boot S/W upgrade facility enables the boot software to be upgraded, and also installs a new base application.

Selecting the Boot Upgrade option will lead to the prompt:

```
Metrodata FCM9004 "FCM9004_left"
Major
```

Alarms:

```
TFTP Boot Software Upgrade
```

CAUTION: Proceeding further will mean that the unit must be re-started, and the performance log may be cleared, even if the upgrade is unsuccessful.

```
Are you sure you wish to continue? y
```

```
File name: FCM9004b.820
Blocks received: 5268
```

```
File received successfully, length 2697124.
File contains:
```

```
Unit Description: fcm9004
```

```
Software Version: 8.20.[mh].3.6 19/06/2013 13:15:33 unreleased
```

```
This will replace:
```

```
Unit Description: fcm9004
```

```
Software Version: 8.16.[mh].1.2 08/05/2013 23:37:46 unreleased
```

```
The software will now be updated.
```

```
Are you sure this is what you want to do?
```

Confirming Y at the prompt, and the system will reprogram the flash and then restart with the new boot and application code.

Note, Please ensure that the unit is not powered down during the boot programming process as this may corrupt the boot software and prevent the system from operating.

4.2.7.1.4 Get Config

To load a configuration file that has been saved on the TFTP server use the Get Config command. Enter the file name for the configuration file and it will then be loaded, validated and stored in EEPROM. The system will then be rebooted with the new configuration.

4.2.7.1.5 Put Config

To save the running configuration use the Put Config command to load the file onto the tftp server. Enter the filename and perform the transfer.

4.2.7.2 Server Mode

The FCM9004 can also be operated in TFTP server mode by setting Mode to server, as shown:

```
Metrodata FCM9004 "FCM9004_Right"           Alarms: Major
```

```
TFTP
```

```
Mode                Server
remote IP           192.168.0.100
Software file name  software
Config. file name   config
```

```
First CAPITAL - select item
```

```
<escape> - exit menu
```

4.2.7.2.1 Remote IP

The IP address is that of the remote client which will perform the transfer. In the event that the client sits behind a NAT enabled firewall, the external IP address is the one that must be configured.

4.2.7.2.2 Software File Name

This is the filename of a file that if downloaded, will be assumed to be a new software load.

When this file is downloaded, the unit will verify the transfer and then program the new firmware. Once upgraded the unit will restart automatically.

From a windows pc, the tftp transfer command would be as below

```
tftp -i device_ip_address put application_filename device_filename
```

4.2.7.2.3 Config File Name

This is the filename that will be uploaded/downloaded from the FCM9004 as a configuration file. When a new configuration file is PUT onto the device, once loaded the unit will automatically restart.

4.2.8 Ping

To provide connectivity checking capability the FCM9004 can generate ICMP ping requests to a configured IP address.

Once the ping is running, the display is as below:

```
Metrodata FCM9004 "FCM9004_Right"
Destination: 192.168.0.100
press any key to stop test
sending...okay, time=3.4ms
sending...okay, time=1.9ms
sending...okay, time=1.9ms
sending...okay, time=1.9ms
sending...okay, time=1.9ms
sending...okay, time=1.9ms
sending...okay, time=1.9ms
sending...okay, time=1.9ms
```

Alarms: Major

4.3 V.24 Set-up

The default setting for the V24 terminal port is

19200, 8bit, No Parity, 2 Stop Bits

The V.24 menu configures the terminal port for local access to the FCM9004..

Metrodata FCM9004 "FCM9004"

Alarms: Major

V.24 SET-UP

Usage	Console
Console set-up	<menu>

First CAPITAL - select item

<escape> - exit menu

4.3.1 Usage

To provide security for the unit the local terminal interface may be disabled to prevent access.

Usage	Console	The external console port is active
-------	---------	-------------------------------------

Usage	Disabled	The external console port is disabled
-------	----------	---------------------------------------

4.3.2 Console set-up

The console setup menu defines the parameters for the serial port and also for the display mode.

Note, that when Zero Touch mode is enabled, the console port will be disabled from power up.

4.3.2.1 Terminal Type

To give maximum flexibility and interoperability with most terminals / terminal emulator programs the display may take the following modes:

TTY	Simple scrolling menu system
VT100/VT220	Cursor controlled menu system
ANSI	Cursor controlled, and highlighted menu system.

4.3.2.2 Via Modem

When the FCM9004 is connected via a dial up modem, the unit may be configured to close the management session when the modem drops DTR.

No	Terminal ignores the state of DTR
Yes	Management Session closed when DTR negated.

4.3.2.3 Baud Rate

The default terminal baud rate is 19200 baud. It is possible to configure the terminal to support alternate rates including:

19200
2400
4800
9600

4.3.2.4 Parity

The parity defaults to NONE, however options include

NONE
EVEN
ODD

4.3.2.5 Data Bits

The terminal port defaults to 8 bit characters. The options are

7

8

4.3.2.6 Stop Bits

The terminal defaults to 2 stop bits, the options are

1

2

4.3.2.7 Load New Config

Once all the terminal communications parameters have been configured, the Load New Command will perform the configuration changes at which point the actual terminal must be changed.

4.4 Port Set Up Menu

The data port menu is where all configuration relating to the physical ports and the traffic flow parameters are configured. The top level data port menu is shown below:

```
Metrodata FCM9004 "FCM9004"                      Alarms: Major
PORT SET-UP
lan1                      <menu>
lan2                      <menu>
lan3                      <menu>
lan4                      <menu>
SFP                      <menu>
WAN                      <menu>

First CAPITAL - select item
<escape> - exit menu
```

The menu is divided into several sections. Lan1 through Lan4 and the SFP refer to the physical user ports on the rear of the unit. The WAN port configures the network port.

4.4.1 User LAN Port Configuration

The LAN port configuration defines the physical operating parameters for the four 10/100/1000BaseT ports on the rear of the unit.

The LAN port menu is as shown below:

```

Metrodata FCM9004 "FCM9004"                      Alarms: Major

LAN1

State                      Up
link status                Up
max spEed                  1000M
max Duplex                 Full
Auto-negotiation           Enabled
negotiated                 100M/FD
MDI/MDIX                   Auto

Tagging & Priority          <menu>
L2CP Management            <menu>
OAM                        <menu>
link loss Fwding           Disabled
Counters                   <display>

First CAPITAL - select item

<escape> - exit menu

```

4.4.1.1 State

The LAN Port State configuration item defines the administrative state of the port. The port states may be:

UP	Port enabled, normal operation
DOWN	Port disabled, alarm handling disabled

It is best practice to set ports to the DOWN state when they are not being used and have no flows defined, as they will then not generate link down traps or show in the alarmed state.

4.4.1.2 Link Status

The Link Status displays the operational state of the LAN port.

4.4.1.3 Speed

The Speed parameter has two meanings depending upon whether auto negotiation is enabled or not.

When Auto Negotiation is disabled, the Speed setting sets the operating speed of the port with valid options of:

10M	10 Base T
100M	100 Base T Fast Ethernet
1000M	1000 Base T Gigabit Ethernet

when Auto Negotiation is enabled, the speed setting defines the maximum speed advertised to the link partner and the menu item changes to max speed. The options are as below:

10M	Advertise 10M
100M	Advertise 10M, 100M
1000M	Advertise 10M, 100M, 1000M

4.4.1.4 Duplex

The Duplex parameter has two meanings depending upon whether auto negotiation is enabled or not.

When Auto Negotiation is disabled, the Duplex setting sets the operating mode of the port with valid options of:

Half	Half Duplex
Full	Full Duplex

When Auto Negotiation is enabled, the duplex setting defines the maximum mode advertised to the link partner and the option changes to max duplex. The options are as below:

Half	Advertise Half Duplex
Full	Advertise Half Duplex, Full Duplex

4.4.1.5 Auto Negotiation

Auto Negotiation allows the port to automatically determine the best operating parameters for the port. If both link partners support auto negotiation then they will select the best mode that is supported by both devices.

If one link partner does not support auto negotiation, an auto negotiating link partner will be able to determine the link speed, however it will be unable to determine the duplex mode so will default to the half duplex state.

An auto port connected to a non auto port is a very common fault on networks leading to errors on the line when significant traffic is flowing, but appearing to operate normally when diagnostics like ping are used to test the link.

4.4.1.6 Negotiated

When auto negotiation is enabled, the negotiated display item shows the operating mode that has been negotiated between the link partners.

10M/HD	10 Base T / Half Duplex
10M/FD	10 Base T / Full Duplex
100M/HD	100 Base T / Half Duplex
100M/FD	100 Base T / Full Duplex
1000M/HD	1000 Base T / Half Duplex
1000M/FD	1000 Base T / Full Duplex

4.4.1.7 MDI / MDIX

There are two possible pin outs for the RJ45 physical ports, one is defined as MDI and is typically found on data sources such as PC's or Laptops. The other is defined as MDIX, or MDI Crossover is typically found on switches. In order to use a straight through patch cable, an MDI port must connect to an MDI-X port otherwise crossover cables are required.

The FCM9004 LAN ports support auto switching technology whereby the port will automatically detect whether it should be MDI or MDIX and will configure itself accordingly. With auto switching ports, only straight patch cables are required.

The options are:

AUTO	Auto switching enabled
MDI	Port fixed in MDI configuration
MDIX	Port fixed in MDIX configuration

4.4.1.8 OAM

The LAN ports support IEEE802.3 Clause 57 (802.3ah) link OAM for peering or tunneling with L2CP.

The OAM menu is as below:

```

Metrodata FCM9004 "FCM9004 "           Alarms: Major
OAM, LAN1
Mode                                     Active
Status                                <display>
counTers                             <display>
Events                               <display>

```

```

First CAPITAL - select item
<escape> - exit menu

```

4.4.1.8.1 OAM Mode

The operating mode of the OAM on this port may be defined here. The valid operating states are:

Disabled Do not generate or respond to OAM packets and discard all OAM packets received.

Tunnel Do not generate or respond to OAM packets, simply tunnel all OAM packets received using L2CP

Active Generate and Respond to OAM packets

Passive Respond to OAM packets

4.4.1.8.2 OAM Status

The OAM Status display shows the current state of OAM on this link as shown below:

Metrodata FCM9004 "FCM9004_Right"

Alarms: Major

OAM STATUS

	Local Status	Local Support	Peer Mode	Peer MAC address	Peer VendorInfo	Peer Support
LAN1	ActiveLoc	L				

Remote Status

Not available

<Escape> - exit, other key - refresh

4.4.1.8.3 OAM Statistics

The OAM statistics show the counts for the various OAM packet types as shown:

Metrodata FCM9004 "FCM9004_Right"

Alarms: Major

OAM Statistics

	Rx	Tx
Unsupported Codes	0	0
Information	0	755
Unique Event	0	0
Duplicate Event	0	0
Variable Request	0	0
Variable Response	0	0
Loopback Control	0	0
Organisation Specific	0	0

<Escape> - exit, C - clear, other key - refresh

4.4.1.8.4 OAM Events

This display lists OAM events that have occurred since the unit was powered up.

4.4.1.9 Link Loss Forwarding

Link Loss Forwarding enables the port state to reflect the status of the full end to end link status rather than simply the cabled connection between local link partners.

When a port enters the Link Loss Forwarding alarm state, the port will be forced to the Link Down state such that the attached equipment will see there is a problem with this network connection allowing for protocols such as RSTP or LACP to remove this link from their network map and enable link restoration by alternative backup links if available.

The Link Loss may be forwarded from:

WAN If the WAN port is down then force the User Port to the Down state.

Flow The end to end flow state is determined using the CFM Connectivity messages and if these messages are not being received, the link will be forced down.

4.4.1.10 Tagging and Priority

The tagging and priority menu selects the actions to be taken with untagged frames.

Metrodata FCM9004 ""
Major

Alarms:

TAGGING & PRIORITY, LAN1

Add C-Tag to	Untagged
c-tag VID	4095

Priority Source	C-Tag, Default
Default Priority	0

First CAPITAL - select item
<escape> - exit menu

4.4.1.10.1 Add C-Tag to

This menu item defines the tagging action to take when a frame arrives at the port. The possible actions are

None	Pass frame unchanged
Untagged	Add the default tag as defined to untagged frames only, pass tagged frames unchanged
All	Add default tag to all frames received whether tagged or untagged

Note, that the default tag ID value must be within the range of ID's allocated in flows assigned to this port, otherwise it will be discarded.

Note, in S-Tag mode this option is fixed at NONE since an S-Tag rather than C-Tag will be pushed as defined in the flow configuration.

4.4.1.10.2 C-Tag VID

This menu item defines the default VLAN ID to add to frames ingressing this port when the action is set to Add Default Tag.

The available values are in the range 1 to 4095

4.4.1.10.3 Priority Source

The priority source selects the priority for the pushed TAG. The options are

Default	Use the default setting for the port
C-Tag,Default	Inherit the priority from the incoming c-tag if present, otherwise use the default value.
DSCP,Default	Inherit the priority from the incoming DSCP marker if present, otherwise use the default.
C-Tag, DSCP, Default	Inherit the priority from C-Tag if tagged, otherwise DSCP if present or use the default.

4.4.1.10.4 Default Priority

This menu item sets the value to be used as the p-tag value within the pushed VLAN Tag.

Available values are 0 to 7

4.4.1.11 L2CP Management

L2CP, Layer 2 Control Protocols are interactions between nodes on the same network segment, and as such are generally blocked by switches or bridges. The purpose of L2CP management is to enable these link layer protocols to be “tunneled” across the wide area network and regenerated at the remote location.

There are a number of layer 2 protocols and the FCM9004 offers individual controls for each with the following options:

Discard	Discard the Layer 2 Control Protocol on ingress to the FCM9004.
Tunnel	Receive the L2CP packet, encapsulate and then transfer to the remote end of the link where it can be recovered and transmitted.
Peer	Protocols that the FCM9004 supports may be peered, ie terminate and generate responses.

L2CP is a proprietary protocol and works by replacing the standard multicast address which may be blocked or peered by intermediate equipment with the Metrodata Multicast address 01:C0:81:00:01:02 which will not be blocked and will be received by an associated FCM9004 unit which will then regenerate the original L2CP packet.

The L2CP Management Menu is as below:

```

Metrodata FCM9004 "FCM9004_Left"                      Alarms: Major

L2CP MANAGEMENT, LAN1

Bridge Group      <menu>
GARP Group        <menu>
Cisco             <menu>
Metrodata         <menu>
Other             <menu>

L2CP Flow         None

First CAPITAL - select item
<escape> - exit menu

```

4.4.1.11.1 Bridge Group

The bridge group of protocols use the generic multicast destination address range:

01:80:C2:00:00:00 to 01:80:C2:00:00:0F

Within this range the following protocols are handled by the L2CP management process:

4.4.1.11.1.1 OAM

The IEEE 802.3 clause 57 (ah) OAM packets are part of the generic slow protocols group.

Address	01:80:C2:00:00:02
Etype	8809 Slow Protocols
Subtype	3 – OAM

The FCM9004 offers options to Discard, Tunnel or Peer with OAM layer 2 control packets.

4.4.1.11.1.2 STP/RSTP/MSTP

The STP/RSTP/MSTP BPDU's use the following addresses

Address	01:80:C2:00:00:00
---------	-------------------

The FCM9004 offers options to Discard or Tunnel BPDU frames.

4.4.1.11.2 LACP / LACP Marker

LACP, Link Aggregation Control Protocol packets are part of the generic slow protocols group:

Address	01:80:C2:00:00:02
Etype	8809
Subtype	01 – LACP
Subtype	02 – LACP Marker

The FCM9004 offers options to Discard or Tunnel LACP frames

4.4.1.11.2.1 OSSP

OSSP, Organisational Specific Slow Protocols are part of the generic slow protocols group:

Address	01:80:C2:00:00:02
Etype	8809
Subtype	10 – OSSP

The FCM9004 offers options to Discard or Tunnel OSSP frames.

4.4.1.11.2.2 LLDP

LLDP, Link Layer Discovery Protocol uses the following

Address	01:80:C2:00:00:0E
Etype	88CC - LLDP

The FCM9004 offers the option of Discard or Tunnel for LLDP frames.

4.4.1.11.2.3 Other Bridge

The Other Bridge protocols cover those protocols using multicast addresses in the range 01:80:C2:00:00:0x not specifically mentioned above as well as unrecognized protocols on those addresses already covered.

4.4.1.11.3 GARP Group

The GARP, Generic Attribute Registration Protocols group uses the range of multicast addresses

01:80:C2:00:00:20 to 01:80:C2:00:00:2F

Within this group there are some well know protocols which are dealt with individually.

4.4.1.11.3.1 GMRP

GMRP, GARP Multicast Registration Protocol uses the following

Address 01:80:C0:00:00:20

The FCM9004 provides options to Discard or Tunnel GMRP frames.

4.4.1.11.3.2 GVRP

GVRP, GARP VLAN Registration Protocol uses the following

Address 01:80:C2:00:00:21

The FCM9004 provides options to Discard or Tunnel GVRP frames

4.4.1.11.3.3 Other GARP

The other Garp options allows for tunneling of packets with multicast addresses in the range 01:80:C2:00:00:22 to 01:80:C2:00:00:CF.

The FCM9004 provides options to Discard or Tunnel these frames.

4.4.1.11.4 Cisco Group

The Cisco Group of Layer 2 protocols may be enabled for tunneling or for discard and the protocols supported are:

CDP	Cisco Discovery Protocol	01:00:0C:CC:CC:CC	2000
VTP	VLAN Trunk Protocol	01:00:0C:CC:CC:CC	2003
DTP	Dynamic Trunking Protocol	01:00:0C:CC:CC:CC	2004
PAgP	Port Aggregation Protocol	01:00:0C:CC:CC:CC	0104
UDLD	Unidirectional Link Detection	01:00:0C:CC:CC:CC	0111
PVSTP	Per VLAN Spanning Tree	01:00:0C:CC:CC:CD	010B
UplinkFast		01:00:0C:CD:CD:CD	200A

4.4.1.11.5 Metrodata Group

The Metrodata group of layer 2 protocols include the following to enable book ending of devices.

4.4.1.11.5.1 Beacon

The Metrodata Beacon protocol may be discarded, tunneled or peered.

Address	01:C0:81:00:01:01
Etype	88B7
OUI	00C081

4.4.1.11.5.2 L2CP Tunnel

The Metrodata L2CP tunnel protocol may be discarded or Tunnelled

Address	01:C0:81:00:01:02
EType	88B7
OUI	00C081

4.4.1.11.5.3 Other Metrodata

This option will allow for discard or tunnel action for the following range of Multicast addresses

01:C0:81:00:01:03 to 01:C0:81:00:01:0F

4.4.1.11.6 Other Group

The other group provides tunnel control for customer CFM packets. There is the option to discard, peer or tunnel CFM received on the user ports.

When user CFM is tunneled it is tunneled to the far end and therefore there is no requirement to use specific domains or associations and be compatible with the underlying core network.

CFM peering relies on the customer using a domain level which is higher than the underlying network.

4.4.1.11.7 L2CP Flow

In order to tunnel the L2CP frames to the remote end they must be allocated to a flow that has previously been configured. Only 1 flow may be allocated and it must be allocated to the particular user port.

4.4.1.12 Counters

The Counters menu shows the RFC-1213 MIB-2 statistics collected for the LAN port as shown below:

Metrodata FCM9004 ""
Major

Alarms:

Interface Statistics

ifInOctets	0	Tunnel In Packets	0
ifInUcastPkts	0	Tunnel In Errors	0
ifInNUcastPkts	0	Tunnel Out Packets	0
ifInDiscards	0	Tunnel Out Errors	0
ifInErrors	0		
ifInUnknownProtos	0	OAM In Packets	0
ifOutOctets	0	OAM Out Packets	1308
ifOutUcastPkts	0	OAM Out Discards	0
ifOutNUcastPkts	0		
ifOutDiscards	0		
ifOutErrors	0		

<Esc> - exit, C - clear, <Enter> - refresh

4.4.2 User SFP Port Configuration

The SFP port configuration defines the physical operating parameters for the user SFP port on the rear of the unit.

The SFP port menu is as shown below:

```

Metrodata FCM9004 "FCM9004"                      Alarms: Major
SFP
State                                             Up
link status                                     Up
sfp type                                         1000BASE-SX
max spEed                                       1000M
Auto-negotiation                               Enabled
negotiated                                     1000M/FD
SFP Management                                 <menu>

Tagging and Priority                             <menu>
L2CP management                               <menu>
OAM                                              <menu>
link loss Fwding                               Disabled
Counters                                       <display>

First CAPITAL - select item
<escape> - exit menu

```

4.4.2.1 State

The SFP Port State configuration item defines the administrative state of the port. The port states may be:

UP	Port enabled, normal operation
DOWN	Port disabled, alarm handling disabled

It is best practice to set the SFP port to the DOWN state when it is not fitted, not being used or has no flows defined, as it will then not generate link down traps or show in the alarmed state.

4.4.2.2 Link Status

The Link Status displays the operational state of the SFP port.

4.4.2.3 SFP Type

The SFP type is read from the SFP module and displays the type of module used.

Note, some cheaper SFP modules are not correctly programmed and in this case the type will be displayed as UNKNOWN.

4.4.2.4 Speed

The Speed setting sets the operating speed of the port with valid options of:

100M	100 Base FX Fast Ethernet
1000M	1000 Base X Gigabit Ethernet

Auto In the auto mode, the SFP module is read and the port parameters are set according to the SFP type installed. If a 1000BaseX SFP is installed the port will operate at 1000M, whilst if a 100BaseFX or OC3 SFP is installed, the port will operate at 100M.

4.4.2.5 Duplex

The Duplex parameter is valid for 100M operation only, 1000M ports must operate in full duplex modes.

Half	Half Duplex
Full	Full Duplex

4.4.2.6 Auto Negotiation

Auto Negotiation allows the port to automatically determine the best operating parameters for the port. If both link partners support auto negotiation then they will select the best mode that is supported by both devices.

1000M operation requires Auto Negotiation is enabled, whilst 100M operation does not support auto negotiation.

4.4.2.7 Negotiated

When auto negotiation is enabled, the negotiated display item shows the operating mode that has been negotiated between the link partners.

1000M/FD 1000 Base T / Full Duplex

Note, only 1000M operation supports auto negotiation, and only full duplex operation is supported.

4.4.2.8 SFP Management

The FCM9004 supports reporting of the SFP device type and diagnostic information. The FCM9004 may also be configured to generate alarms and traps when the diagnostic readings exceed the alarm or warning thresholds.

The SFP Management menu is shown below:

Metrodata FCM9004 "FCM9004_Fibre" Alarms: none

SFP MANAGEMENT

Device Details <display>
 Notifications <menu>

First CAPITAL - select item
 <escape> - exit menu

4.4.2.8.1 Device Details

SFP modules include an EEPROM to identify the module capabilities and these may be read using the SFP device details option. The information display is as shown below:

Metrodata FCM9004 ""

Alarms: Major

SFP Info				

Status	Type	Vendor	Part No.	Transmit Wavelength

Good	1000BASE-SX	HG GENUINE	MXPD-248S-F	850nm

SFP Diagnostic Info							

Diagnostic Item	Status	Current Value	Unit	Alarm High	Threshold Low	Warning High	Threshold Low

Tx Power	OK	8	dBm	8	8	8	8
Rx Power	alarm	-26	dBm	0	-17	-1	-15
Bias	OK	4.2	mA	20.0	1.0	15.0	1.0
Temp	OK	44	C	85	-5	80	0
Supply	OK	3.28	V	3.60	3.0	3.50	3.10

<Esc> - exit, <Enter> - refresh

4.4.2.8.2 Notifications

The SFP notifications menu configures the actions for alarm and trap generation when the diagnostic values exceed the alarm or warning threshold values.

Metrodata FCM9004 "FCM9004_Fibre"

Alarms: none

NOTIFICATIONS

1 - Temp High	Alarm & Warning
2 - Temp Low	None
3 - Supply High	None
4 - Supply Low	None
5 - Bias High	None
6 - Bias Low	None
7 - Tx Power High	None
8 - Tx Power Low	None
9 - Rx Power High	None
A - Rx Power Low	Alarm & Warning
B - SFP Removed	None
C - OTDR Fault	None

First CAPITAL - select item

<escape> - exit menu

Each diagnostic value may be configured for either:

None	No Action
Alarm	Generate an Alarm/Trap when the alarm threshold is exceeded.
Alarm & Warning	Generate an Alarm/Trap when either the Alarm or Warning thresholds are exceeded.

4.4.2.9 Tagging and Priority

For an explanation of the tagging and priority menu please refer to section 4.4.1.10

4.4.2.10 L2CP Management

For an explanation of the L2CP configuration, please refer to section 4.4.1.11 of the User LAN port configuration menu.

4.4.2.11 OAM

The SFP port supports IEEE802.3 Clause 57 (802.3ah) link OAM for peering or tunneling with L2CP.

The OAM menu is as below:

```

Metrodata FCM9004 "FCM9004 "           Alarms: Major
OAM, SFP
Mode                                     Active
Status                                <display>
counters                              <display>
Events                                <display>

```

First CAPITAL - select item

<escape> - exit menu

4.4.2.11.1 OAM Mode

The operating mode of the OAM on this port may be defined here. The valid operating states are:

Disabled Do not generate or respond to OAM packets and discard all OAM packets received.

Tunnel Do not generate or respond to OAM packets, simply tunnel all OAM packets received using L2CP

Active Generate and Respond to OAM packets

Passive Respond to OAM packets

4.4.2.11.2 OAM Status

The OAM Status display shows the current state of OAM on this link as shown below:

```

Metrodata FCM9004 "FCM9004 "                      Alarms: Major

                                OAM STATUS
                                -----
                                | Local | Local | Peer | Peer | Peer | Peer |
                                | Status| Support| Mode| MAC  | Vendor| Support|
                                |-----|-----|-----|-----|-----|-----|
                                | SFP   | Active| Loc  |      |      |      |
                                |-----|-----|-----|-----|-----|-----|
Remote Status
-----
Not available

```

<Escape> - exit, other key - refresh

4.4.2.11.3 OAM Statistics

The OAM statistics show the counts for the various OAM packet types as shown:

```

Metrodata FCM9004 "FCM9004 "                      Alarms: Major

OAM Statistics
-----

                                Rx          Tx

Unsupported Codes              0          0
Information                    0          755
Unique Event                   0          0
Duplicate Event                0          0
Variable Request               0          0
Variable Response              0          0
Loopback Control               0          0
Organisation Specific          0          0

```

<Escape> - exit, C - clear, other key - refresh

4.4.2.11.4 OAM Events

This display lists OAM events that have occurred since the unit was powered up.

4.4.2.12 Link Loss Forwarding

Link Loss Forwarding enables the port state to reflect the status of the full end to end link status rather than simply the cabled connection between local link partners.

When a port enters the Link Loss Forwarding alarm state, the port will be forced to the Link Down state such that the attached equipment will see there is a problem with this network connection allowing for protocols such as RSTP or LACP to remove this link from their network map and enable link restoration by alternative backup links if available.

The Link Loss may be forwarded from:

WAN If the WAN port is down then force the User Port to the Down state.

Flow The end to end flow state is determined using the CFM Connectivity messages and if these messages are not being received, the link will be forced down.

4.4.2.13 Counters

The Counters menu shows the RFC-1213 MIB-2 statistics collected for the LAN port as shown below:

Metrodata FCM9004 ""

Alarms: Major

Interface Statistics

ifInOctets	0	Tunnel In Packets	0
ifInUcastPkts	0	Tunnel In Errors	0
ifInNUcastPkts	0	Tunnel Out Packets	0
ifInDiscards	0	Tunnel Out Errors	0
ifInErrors	0		
ifInUnknownProtos	0	OAM In Packets	0
ifOutOctets	0	OAM Out Packets	1826
ifOutUcastPkts	0	OAM Out Discards	0
ifOutNUcastPkts	0		
ifOutDiscards	0		
ifOutErrors	0		

<Esc> - exit, C - clear, <Enter> - refresh

4.4.3 WAN Port

The FCM9004 WAN port supports either Copper (10/100/1000BaseT) or Fibre (1000Base-X, 100Base-FX) connectivity. The WAN menus are as shown below for the two modes:

WAN Copper Interface menu:

```

Metrodata FCM9004 "FCM9004"                      Alarms: Major

WAN

State                Up
link status          Up
Interface             Copper
max spEed            1000M
max Duplex            Full
Auto-negotiation      Enabled
negotiated            1000M/FD
MDI/MDIX              Auto

Tagging & Priority    <menu>
OAM                  <menu>
Counters             <display>

First CAPITAL - select item

<escape> - exit menu

```

WAN Fibre/SFP Interface menu:

```

Metrodata FCM9004 "FCM9004"                      Alarms: Major

WAN

State                Up
link status          Down
Interface             SFP
sfp type              1000BASE-LX
max spEed            1000M
Auto-negotiation      Enabled
negotiated            ---
sFP Management        <menu>

Tagging & Priority    <menu>
OAM                  <menu>
Counters             <display>

First CAPITAL - select item

<escape> - exit menu

```

4.4.3.1 State

The WAN Port State configuration item defines the administrative state of the port. The port states may be:

UP	Port enabled, normal operation
DOWN	Port disabled, alarm handling disabled

For normal operation, the WAN port must be in the UP state.

4.4.3.2 Link Status

The Link Status displays the operational state of the WAN port.

4.4.3.3 Interface

The FCM9004 WAN interface supports both copper and fibre options. The interface is selected with this item, the options are

Copper	10/100/1000BaseT Interface Enabled
SFP	100BaseFX, 1000Base-X Interface Enabled

Depending on the interface selection, some of the following menu items have different functions.

4.4.3.4 Speed**4.4.3.4.1 Copper Interface Mode**

The Speed parameter has two meanings depending upon whether auto negotiation is enabled or not.

When Auto Negotiation is disabled, the Speed setting sets the operating speed of the port with valid options of:

10M	10 Base T
100M	100 Base T Fast Ethernet
1000M	1000 Base T Gigabit Ethernet

when Auto Negotiation is enabled, the speed setting defines the maximum speed advertised to the link partner. The options are as below:

10M	Advertise 10M
100M	Advertise 10M, 100M
1000M	Advertise 10M, 100M, 1000M

4.4.3.4.2 Fibre Interface Selected

The Speed setting sets the operating speed of the port with valid options of:

100M	100 Base FX Fast Ethernet
1000M	1000 Base X Gigabit Ethernet

Auto In the auto mode, the SFP module is read and the port parameters are set according to the SFP type installed. If a 1000BaseX SFP is installed the port will operate at 1000M, whilst if a 100BaseFX or OC3 SFP is installed, the port will operate at 100M.

4.4.3.5 Duplex

The Duplex parameter has two meanings depending upon whether auto negotiation is enabled or not.

When Auto Negotiation is disabled, the Duplex setting sets the operating mode of the port with valid options of:

Half	Half Duplex
Full	Full Duplex

When Auto Negotiation is enabled, the duplex setting defines the maximum mode advertised to the link partner. The options are as below:

Half	Advertise Half Duplex
Full	Advertise Half Duplex, Full Duplex

When the Fiber interface is selected, only the 100baseFX setting will support half duplex operation.

4.4.3.6 Auto Negotiation

Auto Negotiation allows the port to automatically determine the best operating parameters for the port. If both link partners support auto negotiation then they will select the best mode that is supported by both devices.

If one link partner does not support auto negotiation, an auto negotiating link partner will be able to determine the link speed, however it will be unable to determine the duplex mode so will default to the half duplex state.

An auto port connected to a non auto port is a very common fault on networks leading to errors on the line when significant traffic is flowing, but appearing to operate normally when diagnostics like ping are used to test the link.

Note,

Auto Negotiation is not supported when the fibre interface is selected and 100BaseFX SFP modules are being used.

4.4.3.7 SFP Management

The FCM9004 supports reporting of the SFP device type and diagnostic information. The FCM9004 may also be configured to generate alarms and traps when the diagnostic readings exceed the alarm or warning thresholds.

The SFP Management menu is shown below:

Metrodata FCM9004 "FCM9004_Fibre"

Alarms: none

SFP MANAGEMENT

Device Details <display>
Notifications <menu>

First CAPITAL - select item
<escape> - exit menu

4.4.3.7.1 Device Details

SFP modules include an EEPROM to identify the module capabilities and these may be read using the SFP device details option. The information display is as shown below:

Metrodata FCM9004 ""

Alarms: Major

SFP Info				

Status	Type	Vendor	Part No.	Transmit Wavelength

Good	1000BASE-SX	HG GENUINE	MXPD-248S-F	850nm

SFP Diagnostic Info							

Diagnostic Item	Status	Current Value	Unit	Alarm High	Threshold Low	Warning High	Threshold Low

Tx Power	OK	8	dBm	8	8	8	8
Rx Power	alarm	-26	dBm	0	-17	-1	-15
Bias	OK	4.2	mA	20.0	1.0	15.0	1.0
Temp	OK	44	C	85	-5	80	0
Supply	OK	3.28	V	3.60	3.0	3.50	3.10

<Esc> - exit, <Enter> - refresh

4.4.3.7.2 Notifications

The SFP notifications menu configures the actions for alarm and trap generation when the diagnostic values exceed the alarm or warning threshold values.

Metrodata FCM9004 "FCM9004_Fibre"

Alarms: none

NOTIFICATIONS

1 - Temp High	Alarm & Warning
2 - Temp Low	None
3 - Supply High	None
4 - Supply Low	None
5 - Bias High	None
6 - Bias Low	None
7 - Tx Power High	None
8 - Tx Power Low	None
9 - Rx Power High	None
A - Rx Power Low	Alarm & Warning
B - SFP Removed	None
C - OTDR Fault	None

First CAPITAL - select item

<escape> - exit menu

Each diagnostic value may be configured for either:

None	No Action
Alarm	Generate an Alarm/Trap when the alarm threshold is exceeded.
Alarm & Warning	Generate an Alarm/Trap when either the Alarm or Warning thresholds are exceeded.

4.4.3.8 Negotiated

When auto negotiation is enabled, the negotiated display item shows the operating mode that has been negotiated between the link partners.

10M/HD	10 Base T / Half Duplex
10M/FD	10 Base T / Full Duplex
100M/HD	100 Base T / Half Duplex
100M/FD	100 Base T / Full Duplex
1000M/HD	1000 Base T / Half Duplex
1000M/FD	1000 Base T / Full Duplex

4.4.3.9 MDI / MDIX

There are two possible pin outs for the RJ45 physical ports, one is defined as MDI and is typically found on data sources such as PC's or Laptops. The other is defined as MDIX, or MDI Crossover is typically found on switches. In order to use a straight through patch cable, an MDI port must connect to an MDI-X port otherwise crossover cables are required.

The FCM9004 LAN ports support auto switching technology whereby the port will automatically detect whether it should be MDI or MDIX and will configure itself accordingly. With auto switching ports, only straight patch cables are required.

The options are:

AUTO	Auto switching enabled
MDI	Port fixed in MDI configuration
MDIX	Port fixed in MDIX configuration

4.4.3.10 Tagging and Priority

The tagging and priority menu is only available in S-Tag or Double Tag modes.

The tagging and priority menu allows the Ethertype for Service VLAN / QinQ tags to be defined. The default setting is 9100.

Some alternative values include:

8100	QinQ VLAN in VLAN
88A8	Provider Bridge

In order to support the maximum number of applications the service tag may be configured and it is important that both ends of a link match.

4.4.3.11 OAM

The LAN ports support IEEE802.3 Clause 57 (802.3ah) link OAM.

The OAM menu is as below:

```

Metrodata FCM9004 "FCM9004 "           Alarms: Major
OAM, WAN

Mode           Active
Status         <display>
counters      <display>
Events        <display>

```

First CAPITAL - select item

<escape> - exit menu

4.4.3.11.1 OAM Mode

The operating mode of the OAM on this port may be defined here. The valid operating states are:

Disabled	Do not generate or respond to OAM packets and discard all OAM packets received.
Active	Generate and Respond to OAM packets
Passive	Respond to OAM packets

4.4.3.11.2 OAM Status

The OAM Status display shows the current state of OAM on this link as shown below:

Metrodata FCM9004 "FCM9004 "

Alarms: Major

OAM STATUS

	Local Status	Local Support	Peer Mode	Peer MAC address	Peer VendorInfo	Peer Support
WAN	SendAny	L	active	00c081001368	00000046	L

Remote Status

Unit: FCM8000

Node name: ""

Interface: LAN2

Interface	AdSt	OpSt
LAN1	Up	Down
SFP	Up	Up

<Escape> - exit, other key - refresh

Note, Remote Status information is only available when directly connected to a member of the Metrodata MetroConnect product range as this used the Enterprise extension facility of OAM.

4.4.3.11.3 OAM Statistics

The OAM statistics show the counts for the various OAM packet types as shown:

Metrodata FCM9004 "FCM9004_Right"

Alarms: Major

OAM Statistics

	Rx	Tx
Unsupported Codes	0	0
Information	0	755
Unique Event	0	0
Duplicate Event	0	0
Variable Request	0	0
Variable Response	0	0
Loopback Control	0	0
Organisation Specific	0	0

<Escape> - exit, C - clear, other key - refresh

4.4.3.11.4 OAM Events

This display lists OAM events that have occurred since the unit was powered up.

4.4.3.12 Counters

The Counters menu shows the RFC-1213 MIB-2 statistics collected for the LAN port as shown below:

Metrodata FCM9004 ""

Alarms: Major

Interface Statistics

ifInOctets	0	Tunnel In Packets	0
ifInUcastPkts	0	Tunnel In Errors	0
ifInNUcastPkts	0	Tunnel Out Packets	0
ifInDiscards	0	Tunnel Out Errors	0
ifInErrors	0		
ifInUnknownProtos	0	OAM In Packets	0
ifOutOctets	0	OAM Out Packets	54
ifOutUcastPkts	0	OAM Out Discards	0
ifOutNUcastPkts	0		
ifOutDiscards	0		
ifOutErrors	0		

<Esc> - exit, C - clear, <Enter> - refresh

4.5 Operational Modes

The operational menu allows the settings of many parameters relating to the Flow configuration. The operational modes menu is shown below:

```
Metrodata FCM9004 "FCM9004_Right"                      Alarms: Major
```

```
OPERATIONAL MODES
```

```
VLAN Mode          S-Tag
Max frame size      10k
sla/Policing        <menu>
pri Translation     <menu>
CFM Domains         <menu>
```

```
First CAPITAL - select item
```

```
<escape> - exit menu
```

4.5.1 VLAN Mode

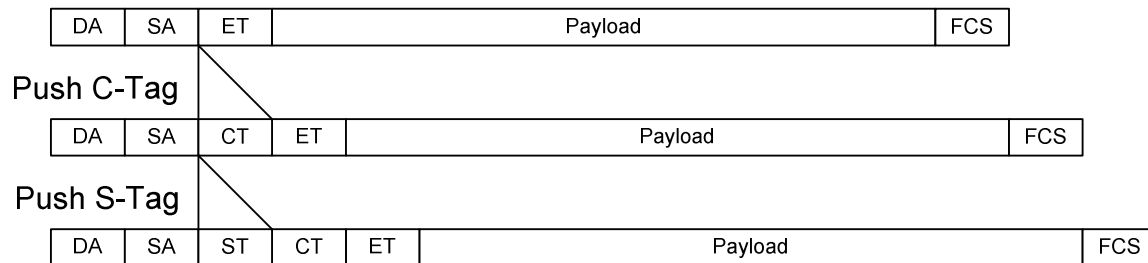
The VLAN mode setting defines the operating mode of the FCM9004. There are three options:

- S-Tag Add a Service VLAN Tag to all incoming frames.
- C-Tag Add a VLAN Tag to all incoming frames, or pass incoming frames tagged within the allocated range.
- Double Tag Add a Service VLAN Tag to all incoming frames, and add/pass VLAN Tag to all incoming frames.

4.5.1.1 VLAN Mode – STag

In S-Tag mode a service VLAN Tag is pushed onto the user packets and ingress and removed/popped on egress. The S-Tag has the Ethertype as defined in the WAN port setup traffic management menu, (4.4.3.10 Tagging and Priority). By default this is set to 9100.

In S-Tag mode, packets ingressing user ports may be untagged, or tagged with normal or alternative Service VLAN Tags giving rise to packets with multiple tags as shown below:



Where:

DA Destination Address

SA Source Address

ET EtherType

FCS Frame Check Sequence

CT IEEE 802.1q VLAN Tag, Etype 8100

ST Service VLAN Tag, default Etype 9100

In S-Tag mode, each port can support the full range of available C-Tags (1-4095) with the ability to allocate S-Tags based on the incoming C-Tag, or range of C-Tags.

4.5.1.2 VLAN Mode – CTag

In C-Tag mode, all user packets egress the WAN port with a C-Tag. Optionally, the FCM9004 may push/pop a single C-Tag to untagged only or all packets.

In C-Tag mode, the FCM9004 supports the full range of available VLAN ID's in the range 1-4095, but each ID may only be allocated to a single user port.

Packets ingressing already tagged will either pass unchanged, if the tag ID is contained within a flow allocation or be discarded. They may also have an extra tag pushed to form a QinQ frame.

The action taken on ingress of an untagged frame may be selected from DISCARD, or push a default Tag.

4.5.1.3 VLAN Mode – Double Tag

In Double Tag mode the FCM9004 can push both an S-Tag and C-Tag to user packets.

In Double Tag mode, the FCM9004 supports the full range of VLAN ID's 1-4095, however each ID may only be used once, unlike the S-Tag mode where each port supports the full range.

Packets ingressing already tagged will have the S-Tag added, if the tag ID is contained within a flow allocation.

The action taken on ingress of an untagged frame may be selected from DISCARD, or push both a default C-Tag and S-Tag.

4.5.2 Max Frame Size

The Maximum frame size may be defined for the FCM9004. The options for packet size are

1522 Max size is 1518 bytes for untagged, and 1522 bytes for tagged frames.

2048 Maximum packet size is 2048Bytes

10k Maximum packet size is 10k bytes

4.5.3 SLA/POLICING

This menu controls many of the parameters used by the policer module and by the SLA verification tools.

Metrodata FCM9004 "FCM9004"

Alarms: Major

SLA/POLICING

Count CFM	No
count L2CP	No
Bandwidth	Information Rate
include S-Tag	Yes
Include C-Tag	Yes
cOupling	Disabled
colour Mode	Blind

First CAPITAL - select item

<escape> - exit menu

4.5.3.1 Count CFM

The Count CFM control selects whether CFM packets are included in the user flow SLA measurements.

By default, CFM packets are not included as they are "internal" control packets used by the operator to monitor the circuit, rather than being customer traffic. As such if the customer has an SLA offering a CIR of 10Mbps, it should only be the customer traffic that is included.

The CFM packets are excluded for bandwidth calculations, policing and Y.1731 Loss measurement.

4.5.4 Count L2CP

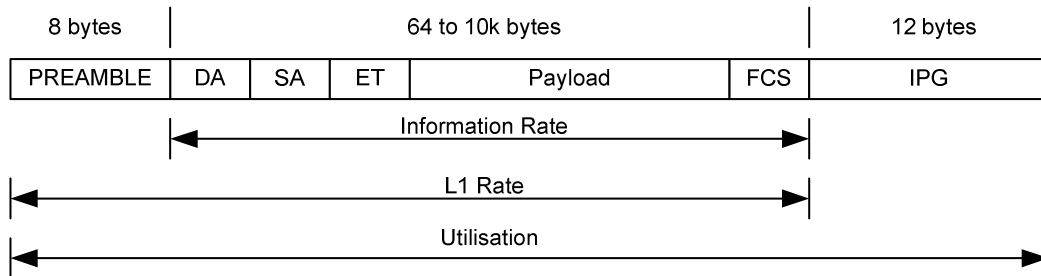
The Count L2CP control selects whether L2CP packets are included in the user flow SLA measurements.

The L2CP packets are excluded for bandwidth calculations, policing and Y.1731 Loss measurement.

4.5.4.1 Bandwidth

In the SLA definitions, the bandwidth is expressed in bits per second. The bandwidth configuration item defines what is actually included in the bandwidth calculations:

Information Rate	Packet from DA to FCS
L1 Rate	Preamble + Packet (DA to FCS)
Utilisation	Preamble + Packet (DA to FCS) + IPG



4.5.4.2 Include S-Tag

In S-Tag or Double Tag mode the FCM9004 is adding the S-Tag to the user frames. Since these 4 bytes are added by the operator and are not customer traffic, this option enables the 4 byte STag to be excluded from the bandwidth and policing measurements.

YES	Include the S-Tag as part of the frame
NO	Reduce packet size by four bytes for bandwidth calculations.

4.5.4.3 Include C-Tag

In C-Tag or Double Tag mode the FCM9004 is adding the C-Tag to the user frames. Since these 4 bytes are added by the operator and are not customer traffic, this option enables the 4 byte CTag to be excluded from the bandwidth and policing measurements.

YES	Include the C-Tag as part of the frame
NO	Reduce packet size by four bytes for bandwidth calculations.

4.5.4.4 Coupling

The coupling configuration controls the operation of the dual leaky bucket policer. Coupling only the effect of using the excess CIR tokens to increase the available EIR bandwidth.

4.5.4.5 Colour Mode

The policer is normally operated in a colour blind mode where all incoming packets are treated the same and first compared against the CIR, and then the EIR.

In colour aware mode, only green packets are checked against the CIR, whilst excess green and yellow packets are checked against the EIR.

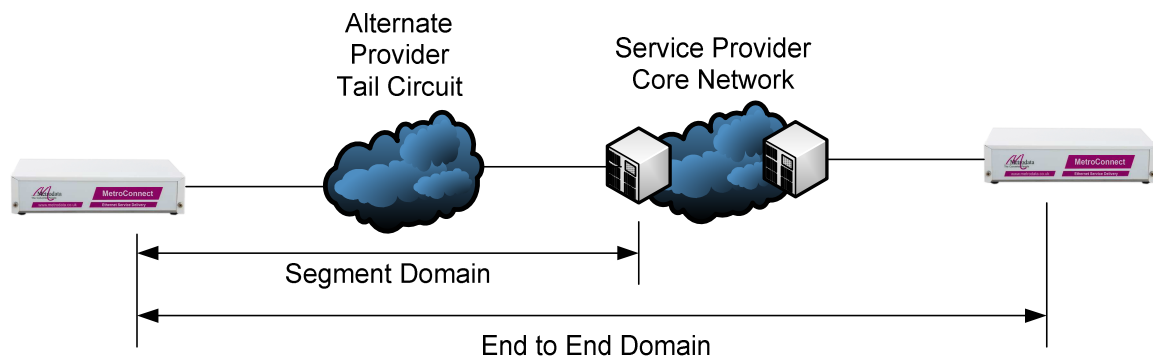
4.5.5 Priority Translation

When a port is pushing an S-Tag or C-Tag onto a previously untagged frame the tag priority may be sourced from the IP DSCP marker. However, since DSCP has 64 possible values and the Tag priority only has 8, a mapping is provided to support the different traffic classes.

4.5.6 CFM Domains

The global CFM, Continuity and Fault Management configuration menus allow for the configuration of the global parameters such as Maintenance Domains, MD and also for viewing the status of the CFM connections

CFM uses Maintenance Domains to indicate the span of the circuit to be monitored as shown below:



Here a service provider is using the FCM9004 as the EDD for the provision of a point to point network service for a customer. Connectivity to one customer site utilizes a tail circuit supplied by an alternative carrier. In this case, two CFM maintenance domains need to be defined, the segment domain to allow for monitoring of the tail circuit, and the End to End domain to monitor the complete customer circuit.

The Maintenance Domain configuration menu is as shown:

```
Metrodata FCM9004 ""                               Alarms: Major
```

```
CFM DOMAINS
```

```
Multicast Addr      IEEE 802.1 (01:80:c2:00:00:3x)
```

```
1 - "Metrodate"     <menu>
```

```
Add MD              <menu>
```

```
First CAPITAL - select item
<escape> - exit menu
```

4.5.6.1 Multicast Address

The IEEE 802.1ag CFM standard defines the range of multicast addresses to use the following:

01:80:C2:00:00:3x where x represents the Domain level.

In applications where the core network does not support CFM, or is not willing to peer the option to use an alternate multicast address is supported. The alternative Metrodata address range may be selected:

01:C0:81:00:01:3x where x represents the Domain level.

4.5.6.2 Edit a Domain

Once a domain has been defined it may be edited, or monitored. Domains are listed in the order that they were defined.

Select the domain to edit by typing the domain number,

```

Metrodata FCM9004 "FCM9004"                      Alarms: Major
MAINTENANCE DOMAIN
Name                                "Metrodata"
name Format                         String
Level                              5
Status Summary                     <display>
Remove MD

```

```

First CAPITAL - select item
<escape> - exit menu

```

4.5.6.2.1 Domain Name

The name allocated to the Maintenance domain should be meaningful and express the coverage of the domain.

The combined domain name and association name must not exceed 44 characters.

4.5.6.2.2 Domain Name Format

The domain name may be defined in several formats as defined in IEEE802.1ag and Y.1731 as follows

String	Character String
None	No name defined
DNS Like	Name based on DNS name
MAC and Int	Name based on the unit MAC address + a 16 bit integer.

4.5.6.2.3 Domain Level

Where Maintenance Domains overlap, for example End to End, and Segment Domains, they must be allocated different levels. The Domain may be assigned a level in the range 0 to 7 with the level indicating the span of the domain, the greater the span, the higher the level.

Typically,

Level 0,1,2	Core Network Operator
Level 3,4	Service Provider
Level 5,6,7	Customer

4.5.6.2.4 Remove Domain

If a domain is no longer required, it may be deleted by selecting the Remove Domain menu item.

Note, that if a domain is deleted, all associations and end points defined within this domain will also be deleted.

4.5.6.2.5 Domain Status Summary

This display shows a summary of all the MA/MEP's within the domain as shown below:

Metrodata FCM9004 "FCM9004_Right"

Alarms: Major

CFM STATUS

Domain "Metrodata" level 4

Association "Gold Service"

End Points

MEPid	Interf	Loc	MAC	AdmSt/ PortSt	IntSt	Defect
201	Flow1	Local	00:c0:81:00:13:ae	Up		None
101	Flow1	Remote	00:c0:81:00:13:ad	Up	Up	None

Association "Silver Service"

End Points

MEPid	Interf	Loc	MAC	AdmSt/ PortSt	IntSt	Defect
202	Flow2	Local	00:c0:81:00:13:ae	Up		None
102	Flow2	Remote	00:c0:81:00:13:ad	Up	Up	None

<Escape> - exit, other key - refresh

4.5.6.2.6 Add Maintenance Domain

The add domain menu allows the configuration of a new domain. The menu is as per the edit menu, refer to previous section for description.

4.6 Flow (Services)

In the FCM9004, Flows define how user traffic traverses the device. The Flow defines the Tag values that will be pushed as well as the SLA parameters.

The FCM9004 supports a maximum of 64 flows, however the actual number available in any application is dependant upon the complexity of the C-Tag range allocations.

The top level flow menu is as below:

```

Metrodata FCM9004 "FCM9004"                      Alarms: Major
FLOWs
List Flows                      <display>
View/EditRemove                 <menu>
Add Flow                        <menu>

First CAPITAL - select item
<escape> - exit menu

```

4.6.1 List Flows

This display item lists all the currently configured flows and displays the key parameters for the flows:

```

Metrodata FCM9004 "FCM9004_Right"                  Alarms: Major

```

		FLOWs					

#	Name	St	S-Tag	Port	C-VLANs	CIR	EIR

1	Gold Service	Up	1	LAN1	1-4095	10M	10M
2	Silver Service	Up	2	LAN2	1-4095	10M	10M

<Escape> - exit, other key - refresh

4.6.2 Add / View / Edit / Modify Flow

The Add Flow menu will automatically get the next available flow number and allow the user to create a new flow definition. View/Modify/Remove Flow will allow the user to modify a previously created flow.

Use the list flow display to determine which flow number you wish to modify when asked for the flow number:

```
Enter Flow number (1-16)
>
```

On entry to the Flow menu for either add or edit the menu is as shown below:

```
Metrodata FCM9004 "FCM9004_Right"           Alarms: Major

FLOW1

Name                Gold Service
State               Up
s-VLAN ID           1
User Port            LAN1
c-vlan Alloc         1-4095
coNtrol C-VLAN       1
sLA/Policing         <menu>
cFM                  <menu>

Counters             <display>
Y.1731 Performance  <display>

Remove Flow

First CAPITAL - select item
<escape> - exit menu
```


4.6.2.1 Flow Number

At the top of the screen the flow number (1-64) is shown. When adding a new flow, this is automatically generated. For edits, the Flow indicates the flow number selected.

4.6.2.2 Flow Name

To improve useability, each flow may be named with a name that represents the flow in a more understandable manner than the flow number. The name is a string of upto 31 characters.

4.6.2.3 Flow State

The flow state defines the administrative state of the flow.

UP	Flow Enabled, traffic can pass
DOWN	Flow disabled, all traffic discarded.

4.6.2.4 S-VLAN ID

In S-Tag or Double Tag mode, each flow has a single S-TAG pushed and this item defines the value in the range 1 – 4095.

This item is not present in C-Tag mode.

In S-Tag mode, all flows must have different S-Tag ID's as this is the flow marker, however in Double Tag mode multiple flows may use the same S-Tag ID as it is the internal C-Tag which defines the flow.

4.6.2.5 User Port

The FCM9004 has four copper user ports along with an SFP port. This config item defines which of the 5 ports the user frames will ingress for this flow.

Options:

LAN1

LAN2

LAN3

LAN4

SFP

4.6.2.6 C-VLAN Allocation

Customer traffic may be tagged or untagged.

In S-Tag mode, the full range of VLAN ID's (1-4095) are available per port, however in the C-Tag or Double Tag modes the full range of VLAN's are available for the unit, such that each ID may only be allocated to one port.

If a flow is to pass untagged frames, the allocation should include '0', to only pass tagged frames exclude 0 from the list.

In C-Tag, or Double Tag mode the untagged action is defined on a per port basis and may be set to either

DISCARD

Add default Tag

This action is defined in the port traffic management menu.

4.6.2.7 Control C-Vlan

The control VLAN is used to transmit CFM frames for the flow. The control C-VLAN must be included within the Allocation for the flow. The ID selected for the control C-VLAN may be one that will be used by the user, or alternatively be one generated by the FCM9004.

4.6.2.8 SLA/Policing Definition

For each flow, SLA parameters may be defined. If bandwidth parameters are defined, then the policer will be enabled for this flow to enforce this traffic profile. The remaining items are used by the Y.1731 monitoring module to determine adherence to the defined SLA.

The SLA/Policing bandwidths are calculated according to the bandwidth setting in the Operational Mode Menu (4.5.4.1) and may be defined in terms of:

Information Rate	Frame contents from DA to FCS
L1 Rate	Preamble + Frame (DA to FCS)
Utilisation	Min IPG + Preamble + Frame (DA to FCS)

Note, that a 100Mbps Utilisation will only yield an Information rate of only 76Mbps due to overheads.

The SLA/Policing menu is shown below:

```

Metrodata FCM9004 "FCM9004"                      Alarms: Major
SLA/POLICING, FLOW1
CIR                      100000000
cBS                      10000
EIR                      -
ebS                      -
max Frame Loss          1.000%
max Delay               100us
max delay Var           100us
Availability             95.000%
Policing                Enabled

```

First CAPITAL - select item

<escape> - exit menu

4.6.2.8.1 CIR

CIR, or Committed Information Rate is the guaranteed bandwidth that will be supplied to the customer.

CIR is defined in bits per second and may range from 100k through to 1G

User traffic that is within the CIR will be marked by the police as GREEN, and transported. Traffic exceeding the CIR will either be processed as Yellow against the EIR, or discarded as non conformant

4.6.2.8.2 CBS

CBS, or Committed Burst Size is the guaranteed burst size that will be supplied to the customer.

CBS is defined in bytes and ranges from the max packet size to 64kbytes.

User traffic upto and including the CBS will be passed, if within the CIR otherwise it may be marked yellow or discarded depending upon the EBS setting.

4.6.2.8.3 EIR

EIR, or Excess Information Rate is an amount of extra bandwidth that the operator may, but does not guarantee to, provide to the user.

EIR is defined in bits per second and may range from 100k through to 1G - CIR

User traffic that exceeds CIR but is within the EIR will be marked by the police as YELLOW, and transported otherwise it will be discarded as non conformant

4.6.2.8.4 EBS

EBS, or Excess Burst Size is extra burst capability that may be supplied to the customer.

EBS is defined in bytes and ranges from the max packet size to 64kbytes.

User traffic exceeding the CBS but within the EBS will be passed and marked yellow otherwise it will be discarded.

4.6.2.8.5 Maximum Frame Loss

This defines the maximum allowable Frame Loss Ratio which may be validated using the Y.1731 Loss Measurement Mechanism.

The FLR is defined as a percentage and is calculated according to MEF10.2 as the ratio of frames lost to the frames transmitted marked green. If the Y.1731 monitoring determines that the FLR has been exceeded alarm processing will begin.

4.6.2.8.6 Max Delay

The FCM9004 uses Y.1731 to measure the round trip delays and makes the assumption that the link is symmetrical. The FCM9004 does not support direct measurement of one way delays since it does not support clock synchronization to GPS or other such master clock.

Y.1731 uses the DMM/DMR frames to determine the actual packet flight times for the round trip, and reports the delays to sub microsecond accuracy.

The Max Delay configuration item defines the maximum one way delay (half round trip delay) allowed by the SLA, above this delay and the device will generate an alarm to indicate violation of the SLA.

4.6.2.8.7 Max Delay Variation

The FCM9004 uses Y.1731 to measure the round trip delay, and uses a comparison of the flight time of the current frame to the previous frame to determine the variation.

The Max Delay Variation configuration item defines the maximum variation allowed by the SLA, above this amount of variation and alarms will be generated to indicate a violation of SLA.

4.6.2.8.8 Availability

The availability is calculated according to MEF10.2 and is a measure of the ability to comply with the SLA, An available second is defined as a second during which the link is available, and that the FLR, Delay and DV are all compliant.

4.6.2.8.9 Policing

Policing is enabled when either the CIR or EIR are configured as non zero. This parameter is for information to inform the user that the policer is enabled.

4.6.2.9 Flow CFM Configuration

The Flow CFM menu allows for the configuration of the CFM parameters required per flow. In the data port CFM menu, the Maintenance Domains used in the network are defined, these are global across all flows. The Flow CFM menu configures the association and end points that are flow specific.

```

Metrodata FCM9004 "FCM9004"                      Alarms: Major
CFM, FLOW2
MA                      <menu>
mEP                     <menu>

```

```

First CAPITAL - select item
<escape> - exit menu

```

Per flow, there may be one instance of an MA (Maintenance Association), and one MEP (Maintenance End Point) defined for each MD (Maintenance Domain) that has been defined.

4.6.2.9.1 MA, Maintenance Association Configuration

An MA, Maintenance Association is defined as a group of MEP's that exist on a flow. Under Y.1731 terminology, the MA corresponds to the MEG or Maintenance Entity Group.

To configure the MA, the menu is as shown:

```

Metrodata FCM9004 "FCM9004"                                Alarms: Major

CFM MA, FLOW2

Name                "Silver Service"
name Format         String
Domain              1 - "Metrodata"

First CAPITAL - select item

<escape> - exit menu

```

4.6.2.9.1.1 MA Name

The Name given to the Maintenance Association is there to make it recognizable and should be in the format defined in the Name Format.

The length of the MA Name is limited by the requirement for the combined length of the MD name, and MA name to not exceed 44 characters

4.6.2.9.1.2 MA Name Format

This item defines the required format for the MA Name, the options are

String	ASCII Character String
None	Blank Entry
Primary VLAN Id	Use the specified control vlan ID
Int16	2 octet Number
VPN ID	RFC 2685 VPN ID
ICC	Y.1731 ITU Carrier Code

4.6.2.9.1.3 MA Domain

The MA must be assigned to be part of a previously defined Maintenance Domain.

4.6.2.9.2 MEP, Maintenance End Point Configuration

A Maintenance End Point, MEP is defined for each end of a flow, and defines how the end point will perform. The configuration menu is shown below:

```

Metrodata FCM9004 "FCM9004_Left"           Alarms: Major

CFM MEP, FLOW1

MEP Id           101
State            Up
CCM              Enabled
LMM              Enabled
DMM              Enabled

```

First CAPITAL - select item

<escape> - exit menu

4.6.2.9.2.1 MEP ID

This is an ID given to this end point in the range 1 to 8191. Each MEP assigned to the flow must have a unique ID within the MA.

In a point to point connection, there will be two MEP's defined, one on each end point device and the MEP ID used must be different.

eg Device A, MEP ID = 101

Device B, MEP ID = 102

4.6.2.9.2.2 MEP State

This item defines the administrative state for the MEP.

UP	Transmit CCM,DMM and LMM messages if enabled
DOWN	Do not generate CFM packets, or generate alarms for failure conditions.

4.6.2.9.2.3MEP CCM

This item defines whether the MEP will generate a CCM, Continuity Check Message once per second.

If an MEP is in the UP state, and does not receive a CCM for 3 seconds, then the CFM Link Down Alarm will be generated.

Options

Enabled Send CCM once per second

Disabled Do not send CCM

4.6.2.9.2.4MEP LMM

This item defines whether the MEP will generate the Y.1731 LMM, Loss Measurement Messages at a rate of once per second.

If the MEP is in the up state, it will respond to a received LMM with an LMR response regardless of the state of the LMM enable control.

Options

Enabled Send LMM once per second

Disabled Do not send LMM

In order to verify the SLA parameter frame loss ratio, LMM packet generation must be enabled in order that the real time frame counters may be accessed.

4.6.2.9.2.5 MEP DMM

This item defines whether the MEP will generate the Y.1731 DMM, Delay Measurement Messages at a rate of once per second.

If the MEP is in the up state, it will respond to a received DMM with an DMR response regardless of the state of the DMM enable control.

Options

Enabled Send DMM once per second

Disabled Do not send DMM

In order to verify the SLA parameters Delay and Delay Variation, DMM packet generation must be enabled in order that the real time frame egress/ingress timestamps may be accessed.

4.6.2.9.3 Counters

This display shows the counters for the flow traffic flow as shown below:

Metrodata FCM9004 ""
Major

Alarms:

Flow Statistics

Out Bytes	0	CFM In Packets	0
Out Packets	0	CFM Out Packets	0
In Bytes	0	CFM Out Discards	0
In Packets	0		
Green Bytes	0		
Green Packets	0		
Yellow Bytes	0		
Yellow Packets	0		
Discarded Bytes	0		
Discarded Packets	0		

<Esc> - exit, C - clear, <Enter> - refresh

In the flow statistics display the following items are counted:

Bytes Total bytes traversing the WAN port for this flow. The byte count is defined by the bandwidth mode (may include preamble, and or IPG)

Frames Total frames traversing the WAN port for this flow. may or may not include CFM/Y.1731 control frames

In Bytes/Frames Received on the WAN port for this flow.

Out Bytes/Frames Transmitted on the WAN port for this flow

Green Bytes/Frames transmitted which are marked green as conforming with the CIR/CBS traffic profile.

Yellow Bytes/Frames transmitted which are marked yellow to indicate these exceed the CIR, but are within EIR/EBS

Discarded Bytes/Frames exceeding the traffic profile and discarded.

4.6.2.9.4 Y.1731 Performance

When Y.1731 performance monitoring is enabled, test packets are transmitted to measure the frame loss, and the round trip delays. Using Y.1731 allows for in service monitoring of the SLA.

The Y.1731 performance is displayed as shown below:

```

Metrodata FCM9004 "FCM9004_Left"                      Alarms: Major
Y.1731 Performance Statistics  Flow1
-----

```

	Outbound	Inbound	SLA
Time (s)	8068	8068	
Unavailable (s)	8068	8068	
Availability (%)	0.000	0.000	95.000
Sent Frames	0	0	
Lost Frames	0	0	
Frame Loss Ratio (%)	0.000	0.000	1.000
Maximum Delay (us)	0.0	0.0	100
Maximum Delay Variation (us)	0.0	0.0	100

<Escape> - exit, C - clear, other key - refresh

Y.1731 allows for the measurement of the following performance values:

Time This shows the time over which the Y.1731 performance has been monitored.

Unavailable shows the amount of time that the link has been unavailable

Availability The availability is calculated as per MEF 10.2 as a ratio of the total seconds, versus the time of non conformance to the flow SLA

Sent Frames are values retrieved from the Y.1731 LMR messages

Lost Frames are calculated using the LMR messages

Frame Loss Ratio This is the ratio of transmitted frames to frames lost traversing the network to the remote end point.

Maximum Delay Y.1731 allows for measurement of the round trip delay and this display shows the inbound/outbound delay as half the round trip delay.

Max Delay Variation The variation is measured on the round trip delay and is compared frame by frame to the previous frame delay.

4.6.2.9.5 Remove Flow

If a flow is no longer required, it may be deleted by selecting the remove Flow menu option.

4.7 Circuit / Flow Tests

The Testing menu serves two functions, it give access to the Layer 1 port loopback functions and also gives access to the SAM (Service Assurance Module) functions.

The top level testing menu is shown below,

```

Metrodata FCM9004 "FCM9004"                      Alarms: Major
CIRCUIT / FLOW TESTS
port Loops                      <menu>
SAM Flow Testing                <menu>

```

```

first CAPITAL - select item
<escape> - exit menu

```

4.7.1 Port Loops

This menu gives access to the port loopback controls and enables the use to apply a physical layer, layer 1 loopback to the user port or SFP port. The loops are physical layer loops and simply loop frames back as they are received.

To apply a loopback simply select the port to which the loop is to be applied. Then use the toggle function to select between:

NONE	-	No Loopback applied
LL	-	Local Loop, loop transmit back to receiver
RL	-	Remote Loop, Loop back receive to transmitter
OAM	-	Generate OAM loopback request to remote unit

WARNING:

Physical layer loops **MUST** be used with great care as they can introduce loops and therefore cause traffic instability on a live network. These loops are only intended for use with LAN Test Equipment.

4.7.2 SAM Flow Testing, Service Assurance Module

The Service Assurance Module provides the FCM9004 with a highly flexible, multi stream traffic generation, and Layer 2 (DA/SA swap) and Layer 3 (IP DA/SA swap) loopback functions.

By default, the FCM9004 has the loopback function enabled and will loopback test packets sent to the user defined loopback MAC address.

From factory default, the SAM test menu is as below:

```

Metrodata FCM9004 "FCM9004"                      Alarms: Major
SAM
test Regime          Manual Control
Mode                 Loopback

```

```

First CAPITAL - select item
<escape> - exit menu

```

4.7.2.1 SAM Mode

The Mode menu item selects the operating mode of the SAM module. The item is a toggle item and has the following options:

LOOPBACK	The loopback function is enabled, and any packets received on the WAN port with the WAN loop address, or User port with the USER loop address will be looped back with the MAC Destination and Source Addresses swapped.
TESTER	Enable the multi-stream traffic generator to generate test traffic streams to validate the SLA parameters of the provisioned flows.
DISABLED	The SAM module is disabled, neither loopback or traffic generation capabilities are available.

4.7.2.2 SAM Test Regime

This menu item is only valid for SAM tester mode. The regime selects how the traffic generator is to be controlled. The options are as below:

MANUAL	Manual Mode allows the traffic generator to be configured manually, and perform specific tests under user control.
Y.1564	Y.1564 Test Mode selects an automated test methodology which enables traffic flow SLA's to be verified in the presence of background traffic.

4.7.2.3 Y.1564 Testing

The testing standard ITU Y.1564 defines a methodology to verify the Service Level Agreements applied to customer services may be achieved. Y.1564 is an improvement over RFC-2544 which was targeted at simply finding the maximum throughput of a link, in that it uses multiple traffic flows to verify SLA parameters in the presence of background traffic.

When the SAM mode is set to Tester and the Regime Y.1564 is selected the menu changes to the following:

```

Metrodata FCM9004 "FCM9004"                                Alarms: Major
SAM
Regime                                                       Y.1564
Profile                                                       Custom
test pParameters                                             <menu>
Flows                                                         1
State                                                         Stopped
View Results                                                 <display>

```

```

First CAPITAL - select item
> - next page
<escape> - exit menu

```

4.7.2.3.1 State

The test state starts or stops the test in progress. Once the various parameters are configured to define the test features to run, the test state should be changed to RUNNING.

Once the test is running it will then cycle though and test each assigned flow according to the test definitions against the required SLA parameters.

4.7.2.3.2 View Results

While a test is running, the view results screen shows the current status. An example is shown below:

```

Metrodata FCM9004 "FCM9004"                                Alarms: Major

Test Report
-----
unit node name: "FCM9004"
unit mac address: 00:c0:81:00:13:ad
start time: 10:52:02 Tue 27/11/2012
test regime: Y.1564
---
testing Flow1 "Port1 Service 100M"
go/nogo test
%cir: 10..
test results:
tx frames                25
rx good frames           24
frame loss (%)           4.000002
max delay (us)           11.0
max delay variation (us) 0.0
go/nogo test failed
---
testing complete

<Escape> - exit, other key - refresh

```

The results report grows as the testing progresses, and may be refreshed whilst the test is running to show the latest progress. The report lists the outcomes of each test performed and gives a pass/fail indication.

Once the test is complete, indicated by the "Testing Complete" message in the report, it may be saved using TFTP as proof of the services meeting the SLA when the services are initially provisioned.

4.7.2.3.3 Profile

To assist with circuit testing several predefined test profiles have been defined from which you may select.

Custom	Custom profile based on the configured parameters
15-Min	Perform a test in 15 minutes
4-Hour	Perform a test in 4 hours
24-hour	Perform a test in 24 hours

4.7.2.3.4 Test Parameters

The test parameters allow the individual stages of the tests to be customized to your requirements

Metrodata FCM9004 "FCM9004_Left"

Alarms: Major

TEST PARAMETERS

```

Background Rate      0% of CIR
Go/NoGo Test Time   0s
CIR Test:
1 - Rate             0% of CIR
2 - Time             0s
CBS Test:
3 - Rate             0% of CIR
4 - Burst Size       0% of CBS
5 - Time             0s
CIR/EIR Test:
6 - CIR Rate         0% of CIR
7 - EIR Rate         0% of EIR
8 - Time             0s

```

First CAPITAL - select item

<escape> - exit menu

4.7.2.3.4.1 Background Rate

When multiple flows are being tested, the SAM module will select the flow that is not in foreground and has highest configured CIR. The background Rate menu setting defines the amount of background traffic based on percentage of CIR.

For example,

Testing flows 1-3 where they are defined as follows

Flow 1, CIR=50M, CBS=10k, EIR=50M, EBS=10k

Flow 2, CIR=50M, CBS=10k

Flow 3, CIR=10M, CBS=10k, EIR=10M, EBS=10k

While testing flow 1, flow 2 with the CIR of 50M will be selected as the background stream. When testing flow 2, Flow 1 will then be selected as the background stream.

The background rate is defined as a percentage of the CIR

Eg CIR = 50M, 95% = 47.5M

Generating background traffic allows the test to validate that the link has not been over provisioned for CIR traffic.

4.7.2.3.4.2 Go/No Go Test

The purpose of the Go / No Go test is to provide a quick test to validate that the flow has actually been provisioned and that a loopback is actually available.

The Go/No Go test starts with a low traffic rate and slowly ramps the traffic rate up to the configured value. The test starts by sending traffic at 10% of the flow CIR and ramps up to 90% of the CIR in 10% steps.

The Go/No Go Test monitors the received traffic and if the SLA cannot be achieved at any of the transmission rates, the test will fail. If the SLA is met, then the next test phase can continue.

4.7.2.3.4.2.1 Go/No Go Test Time

The Time menu item defines the time spent in each step of the test. The time is defined in seconds. Generally, as the go/no go test is intended to provide a quick check that the service is available this time should be kept short, and 30 to 60 seconds would provide a good balance taking between 5 and 10 minutes to run the full go/no go test

4.7.2.3.4.3 CIR Test

The CIR test will generate test traffic at a defined percentage of the flow CIR. If available background traffic will also be generated. The test will run for the defined test time and the test pass criteria are as defined by the flow SLA parameters.

The CIR test aims to prove that the network is correctly provisioned to provide the service within the SLA and for this reason should be run over an extended period of time, upto 24 hours to ensure service stability.

4.7.2.3.4.3.1 CIR Test Rate

The test rate settings sets the percentage of CIR that will be generated. For example, CIR = 50M, 95% = 47.5M and the CIR test will generate 47.5M of test traffic on the flow under test.

Note, it is not advisable to actually test at 100% of CIR as due to small differences in network timings the test is likely to fail even when correctly provisioned, 99% being the highest value normally set.

4.7.2.3.4.3.2 CIR Test Time

This configuration item defines the duration of the CIR test. Whilst the Go/No Go test aims to give a quick snapshot of the network, the CIR aims to prove the service over an extended period. As such it is typical to run the CIR test for between 1 and 24 hours.

4.7.2.3.4.4 CBS Test

In order to fully test the service the Y.1564 will test the burst capability of the network. In this test, the traffic generator will be configured to generate bursts of traffic where the burst size is defined as a percentage of the CBS and the bursts spaced such that the overall traffic bandwidth does not exceed the configured percentage of CIR.

4.7.2.3.4.4.1 CBS Test Rate

The CBS test rate defines the overall traffic rate as a percentage of the CIR for the flow. In this test packets are generated in a burst at wirespeed, and then the bursts are spaced such that the overall bandwidth averages out at the defined percentage of CIR.

4.7.2.3.4.4.2 CBS Test Burst Size

When a flow is defined the CBS, Committed Burst Size is one of the parameters defined. The CBS defines the size of a burst that can be handled before packets are discarded.

This parameter defines the burst size as a percentage of the CBS. For example with 64 byte packets and a CBS of 10kbytes a 95% setting will set the burst size to 9.5kbytes or 148 64 byte packets.

4.7.2.3.4.4.3 CBS Test Time

Burst capabilities need to be verified over a reasonable length of time. For a typical test, with a 24 hour CIR test, this would be set to 1 hour.

4.7.2.3.5 CIR/EIR Test

Where flows have been defined with both CIR and EIR values this test generates two streams of traffic, one colour marked green as CIR conformant and a second stream marked yellow as EIR conformant. During this test traffic is generated at a constant rate.

In a colour aware network, the service guarantees to pass traffic at rates of up to the CIR. This conformant traffic is marked Green. Where an EIR is defined extra capacity may be made available to the flow but it is not guaranteed.

Where the underlying network is colour aware, the test verifies that the CIR Green traffic is transported without exceeding the SLA, whilst in a colour blind network the test simply verifies that traffic is received that at least meets the CIR.

4.7.2.3.5.1.1 CIR/EIR Test CIR Rate

This menu item defines the traffic rate for the CIR/Green traffic stream. This value is defined as a percentage of the flow CIR.

4.7.2.3.5.1.2 CIR/EIR Test EIR Rate

This menu item defines the traffic rate for the EIR/Yellow traffic stream. This value is defined as a percentage of the flow EIR.

4.7.2.3.5.1.3 CIR/EIR Test Time

This menu item defines the duration of the CIR/EIR test. Typically for a 24 hour CIR test this would be set to 1 hour.

4.7.2.3.6 Flows

The Flows menu item is used to assign flows to be tested. Flows may be assigned using the comma, or range markers, eg

- 1 Test Flow 1
- 1,2 Test Flows 1 and 2
- 1-7 Test Flows 1 to 7

On initial installation, all defined flows should be tested to prove that the network has been correctly provisioned to meet the SLA required for each service.

After initial installation, then only specific flows should be selected to be tested whilst other flows pass traffic and are not affected.

When 2 or more flows are defined, the traffic generator will choose one of the flows not currently being tested for background testing. For example, if flows 1 and 2 are selected for test, then when flow 1 is being verified, flow 2 will be used for background traffic generation.

4.7.2.4 Manual Mode Testing

Whilst Y.1564 testing allows for semi automated validation of the SLA defined per flow, it may be desirable to perform a more detailed or tightly controlled test to diagnose a network, or service problem and this is the purpose of the Manual Mode tester.

The manual mode test setup menu is shown below:

```

Metrodata FCM9004 "FCM9004"                      Alarms: Major
SAM
Regime                      Manual Control
Mode                        Tester
test Duration               00:01:00
Test State                  Stopped
maNual Setup                <menu>
tEst Summary                <display>
Clear Results

First CAPITAL - select item
<escape> - exit menu

```

4.7.2.4.1 Test Duration

The manual tester will run for the configured time. The time is entered in the format:

Hours : Minutes : Seconds

Note, the duration must include all three parameters, such that a 30 second test is configured as 0:0:30

4.7.2.4.2 Test State

When the test traffic is configured, clear the results and then change the state to Running. The test will then run for the defined test period.

Stopped	Test Not Running
Running	Test Running

4.7.2.4.3 Manual Setup

The Manual Setup Menu configures the tester parameters. The menu is shown below:

```

Metrodata FCM9004 "FCM9004_Left"           Alarms: Major

MANUAL SETUP

Flow                      1
s-VLAN                   None
c-VLAN                   128
Local MAC                00:c0:81:00:13:ad
Remote MAC               00:c0:81:ff:00:00
Packet size              68
pAcket rate              17462
Bandwidth                94.999% of CIR
bUrst Size                1 packet(s)
burst size               0.680% of CBS

First CAPITAL - select item

<escape> - exit menu

```

4.7.2.4.3.1Flow

In order for a test to be performed, at least one flow must have been configured. When the flow number is entered, the S/C-Tag information is retrieved and used for the test traffic stream.

4.7.2.4.3.2S-VLAN / C-VLAN

This menu item shows the Tag structure for the test packets.

By default, the C-VLAN will assume the ID of the Control VLAN as defined in the flow configuration. This may be changed to use any other ID that is part of the flow definition.

4.7.2.4.3.3Local MAC

This is the MAC address of this unit. It is a fixed value, and is used as the Source Address for all test packets.

4.7.2.4.3.4 Remote MAC

This is the MAC address used as the destination address within the test packets. By default it is set to the Metrodata WAN Loopback address.

00:C0:81:FF:00:00 WAN Loopback Address

00:C0:81:FF:00:01 User Port Loopback Address

Where another FCM9004 is not available at the remote end, but another device is providing the MAC DA/SA swapping function this address may be changed.

4.7.2.4.3.5 Packet Size

The test stream sends a stream of packets of a constant size. The value configured is the size of the packet, in bytes, including TAGs, and the FCS.

Note, the minimum packet size is set to 68 bytes to ensure that the minimum packet size when tags are removed does not fall below 64 bytes. In many switches, tag removal from 64 byte packets will lead to the packet being padded and thereby effectively growing as it transits the network.

4.7.2.4.3.6 Packet Rate

The transmission rate for the test may be defined by either directly entering the packet per second rate.

4.7.2.4.3.7 Bandwidth

Where a flow has an SLA configured, the option to set the transmit rate to be a percentage of the CIR is available to simplify test setup.

4.7.2.4.3.8 Burst Size (Packets)

The Test generator can send traffic as either a constant, evenly spaced traffic stream or as bursty traffic sending bursts of packets.

- | | |
|----|--|
| 1 | Constant Rate Traffic |
| 2+ | Burst of 2+ packets at a time with the burst spaced such that the bandwidth/packet rate is adhered to. |

4.7.2.4.3 Burst Size (CBS)

Where a flow has an SLA configured, the option to setup the burst size as a % of the CBS is available to simplify configuration.

4.7.2.4.4 Test Summary

The results of the test are displayed in the test summary display as shown below:

Metrodata FCM9004 "FCM9004"

Alarms: Major

Test Summary		Running Time: 0:00:02	
Flow/SLA		Test Results	
Flow	1		
S-VLAN	-	Tx Frames	35112
C-VLAN	128	Tx Bytes	2387616
Frame Size (bytes)	68	Tx Bandwidth (bps)	9499202
CIR (bps)	10000000	Rx Frames	35110
CBS (bytes)	10000	Rx Bytes	2387480
EIR (bps)	-	Rx Bandwidth (bps)	9498661
EBS (bytes)	-	Lost Frames	2
Frame Loss (%)	1.000	Frame Loss (%)	0.006
Delay (us)	100	Delay (us)	11.4
Delay Variation (us)	100	Delay Variation (us)	0.3

<Escape> - exit, other key - refresh

The running time shows the time that the test has been running for and will keep incrementing on each refresh until the test duration is complete.

Whilst a test is in progress, the Lost Frame count includes both Lost Frames and Frames currently in transit. While a test is running, it is likely that the lost frames count will show a number of packets, if this is increasing it means packets are being lost, if it stays constant then these are packets in flight.

At the completion of the test, the lost frame count truly reflects the number of frames lost during the test.

4.7.2.4.5 Clear Results

Before running a test, the results should be cleared.

APPENDIX 1 Base Label Versions

Section 2.2 of this manual shows the currently shipping version of the base label for the FCM9004 product. This label has been revised in an attempt to improve the clarity of the label and to reduce confusion regarding the operation of the switches.

Only the labelling of the switches has changed, the function of the switch has not.

Older products may have previous versions of the base label as shown below:



Metrodata Ltd
 TW20 8RY UK
 Tel +44 (0) 1784 744700
 Fax +44 (0) 1784 744730

Status LED	Meaning
Off	No mains power present
Red steady	WAN
Red/Off Flashing	WAN / LAN Alarm
Green/Off Flashing	LAN
Green steady	Status OK

FCM9004
Advanced Ethernet
Media Converter (AC)

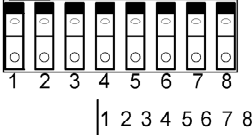
For product manual and other information :-
www.metrodata.co.uk
 Manufactured in the UK

Part No. 80-70-941

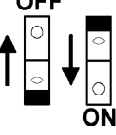
Serial No:

Bitswitch	Control	ON	OFF
1	WAN Mode	Copper *	Fibre
2	Auto Neg	Enabled *	Disabled
3	Speed	1000M *	10/100M
4	Speed	100M *	10M
5	Duplex	Full *	Half
6	Tag Mode	Single Tag Push/Pop *	Double Tag Push/Pop
7	Autoboot	Enabled *	Disabled
8	Factory Default	Normal Operation*	Return to Default Settings

Bold * characters = Factory Default



OFF



ON



17-70-1319B (Ai)