FUJ00171956

Document Title: CNIM Low Level Design

Document Type: Low Level Design

Release: S92

Abstract: CNIM is an NT service that runs on an outlet's gateway PC. It controls the parameters used by the Eicon card, if present, and provides call logging and diagnostic information.

CNIM also includes an interface DLL which is used by the Counter Call Scheduler to extract network status information.

CNIM 3 at S60 has been expanded to monitor the ADSL connection via Connection Manager and ADSL Diagnostic Monitor.

CNIM 4 at S92 for BNR will include backup connections over ISDN and GSM.

Document Status: APPROVED

Originator & Dept: Nick Johnson, Cryptography & Networking Team, POA.

Contributors:

Internal

For Originator to distribute following approval

Cryptography & Networking Development Team, BRA01

Mandatory Review Authorities (see 0.2)

Distribution:

External

For Document Management to distribute following approval

Dis

FUJ00171956

t r i b u t i o n :

Approval Authorities

Name	Position	Signature	Date
Roy Birkinshaw	**Development Manager**		

FUJ00171956

0 DOCUMENT CONTROL

0.1 Document History

Version No.	Date	Reason for Issue	Associated CP/PinICL No.
0.1	**2nd December 2002**	For review.	CP3423
0.2	**14th February 2003**	For review.	CP3423
0.3	**28th March 2003**	For review.	CP3423
1.0	**17th April 2003**	For approval - withdrawn from approval cycle.	CP3423
1.1	**3rd July 2003**	For review	CP3423
2.0	**30th July 2003**	For approval	CP3423
2.1	**13th November 2003**	For review	CP3468
2.2	**10th February 2004**	Not Circulated for Review	CP3594
2.3	**10th June 2004**	For review	CP3594
3.0	**9th July 2004**	For approval	CP3594
3.1	**5th January 2005**	For review	PC0093488
3.2	**18th April 2005**	For review	CP3898
3.3	**25th July 2005**	For review	CP3898
3.4	**4th August 2005**	For review	CP3898
3.5	**4th November 2005**	For review	CP4097 CP4103
3.6	**12th April 2006**	For review	PC0132421
4.0	**8th May 2006**	For approval	CP3986

0.2 Review Details

Review Comments by :	
Review Comments to :	*Nick Johnson, BRA01*

Mandatory Review Authority	Name
Development Team Leader	Peter Ambrose*
Design Authority	Mark Jarosz*
SSC	Mik Peach*
Optional Review / Issued for Information	
Development Manager	Roy Birkinshaw
CS Security Manager	Brian Pinder
CS Data Centre & Ops Service Manager	Peter Thompson

FUJ00171956

Test Manager	Peter Dreweatt
DU RV Manager	Sheila Bamber
DeLT Manager	Denise Morris
Software Distribution Team Manager	Karen Morley
Design Authority	Dave Tanner
Design Authority	Colin Mills
Developer	Mike Coon
Tester	John Rogers
Tester	Derek Elliott
Tester	Michael J. Welch

(*) = Reviewers that returned comments

0.3 Associated Documents

Reference	Version	Date	Title	Source
[Ref 1] [DOC_TPL]			ICL Pathway Document Template	PA/TEM/001
[Ref 2] [HLD_CNIM]	0.42		Counter Network Infrastructure Manager (CNIM)	TD/SDS/002
[Ref 3] [NB_SOD]	0.23	20/4/2002	Network Banking - Outlet Network Quality of Service Reporting.	SY/SOD/007
[Ref 4] [CAS_PIS]	1.1	31/10/2002	CAS Network Quality of Service Product Interface Specification	DE/IFS/003
[Ref 5] [HLD_NBA]			High Level Design Specification For Network Banking Agents.	AD/DES/065
[Ref 6] [CCS_NB]			Counter Call Scheduler Changes for Network Banking	AD/DES/068
[Ref 7] [HLD_CAS]	1.1	31/10/2002	CAS Network QOS HLD	DE/HLD/001
[Ref 8] [HLD_ACF]	0.3	20/04/2002	Autoconfig HLD	TD/DES/157
[Ref 9] [HLD_VPN]	2.0	26/11/01	VPN High Level Design	RS/DES/046
[Ref 10] [IDI]			IDI ISDN Driver Interface	Eicon
[Ref 11] [DIAPI]			Diapi ISDN interface for Windows NT	Eicon
[Ref 12] [TRACE]			Network Banking – Trace and Diagnostics LLD.	NB/LLD/025
[Ref 13] [UTP]	0.1	09/05/2003	CNIM Unit Test Plan	RS/UTP/001
[Ref 14] [SMS]	1.1	20/06/2003	ADSL Service Management System Outline Design	SY/SOD/018
[Ref 15] [CMN]	0.4	4/08/2003	Connection Manager Detailed Design	RS/DES/091
[Ref 16] [HLD_ADSL_1]	0.9	4/08/2003	ADSL High Level Design (S52)	TD/SDS/004
[Ref 17] [HLD_ADSL_2]	0.2	5/09/2003	ADSL High Level Design (S55)	TD/SDS/005
[Ref 18] [ADSL_DIAG_MON]	2.2	14/04/2004	ADSL Diagnostic Monitor Detailed Design	RS/LLD/005
[Ref 19] [DP_BNR]	0.2	18/03/2005	Design Proposal for Resilient Network	AS/DPR/021

FUJ00171956

[Ref 20] [SM_BNR]	0.1	4/08/2005	Branch Network Resilience Service management Reporting Outline design	SY/DES/037
[Ref 21] [EP_BNR]	0.1	10/08/2005	High Level Design - Branch Network Resilience Engineer's Counter Application	EP/HLD/002

Unless a specific version is referred to above, reference should be made to the current approved versions of the documents.

0.4 Abbreviations/Definitions

Abbreviation	Definition
ADSL	Asymmetric Digital Subscriber Line
ADM	ADSL Diagnostic Monitor (Service to monitor ADSL connection state)
API	Application Programming Interface
CPL	CNIM Programming Language
CDF	Communications Data File (may also be known as a CNIM Data File). Contains values to be set into the Eicon ISDN card by the CNIM (for Access numbers to the Data Centre Routers over the Energis voice and Data Networks) and by EiconConfig for CHAP usernames and network options. A CDF is installed during outlet ISDN G/W PC installation and replacement/swap-out. They form part of the mechanism for the delivery of OBC changes to a live outlet following relocation (with ISDN number change), conversion to/from Mobile outlet (although conversion to/from mobile outlet is only supported by the "end-to-end" system before the outlet goes live) and for network changes (by Energis.)
CHAP	Challenge Handshake Authentication Protocol
CNIM	Counter Network Infrastructure Manager
BNR	Branch Network Resilience
Blackhole Failure	A type of network failure that will not be detected by Connection Manager. CNIM pings will fail.
DLL	Dynamic Link Library
Data Network	Note that the Data network is the name for the non-ISDN or satellite network and may also apply to the FRIACO network.
FRIACO	Fixed Rate Internet Access Call Origination
FE	FRIACO Establish
FF	FRIACO Fixed
FC1P	FRIACO Primary (Geographical Area 1)
FC1S	FRIACO Secondary (Geographical Area 1)
FC2P	FRIACO Primary (Geographical Area2)
FC2S	FRIACO Secondary (Geographical Area 2)
DIAPI	Diapi ISDN interface for Windows NT
DP	Dial Around Primary
DS	Dial Around Secondary

FUJ00171956

IP	Internet Protocol
ISDN	Integrated Service Digital Network
IDI	Eicon ISDN Driver Interface
KMS	Key Management System
LAN	Local Area Network
MOD	Metered on Demand
MODG	Metered on Demand with GSM backup
MF	Metered Fixed.
MFG	Metered Fixed with GSM backup
MP	Metered Primary
MS	Metered Secondary
NST	Network Service Type (Voice, Bronze, Satellite etc.)
PC	Permanent Connection
RAS	Remote Access Service
RA	RAS ADSL
RG	RAS GSM
RAG	RAS ADSL/GSM
RAIG	RAS ADSL/ISDN/GSM
RIT	RAS ISDN for Test
RID	RAS at IDLE
RSSI	Received Signal Strength Indicator
SCM	Service Control Manager
UID	User ID
UTC	Universal Coordinated Time, same as GMT
VOD	Voice on Demand
VODG	Voice on Demand with GSM backup
VPN	Virtual Private Network
VP	Voice Primary
VS	Voice Secondary
VT	Voice Tertiary
WAN	Wide Area Network

0.5 Changes in this Version

Version	Changes
0.3	CNIM Test Sequence CNIM Programming Language
1.1	Test Sequence - Permanent Connection

FUJ00171956

	Table 35 - NST 11 Connection Type per Mode. Table 9 - Wait Times for Call Closure
2.0	5.12.1 Clarify detail. 5.13.1.a Updated - Fail values not required in CNIM 2. 5.13.1.b - CNIMConfig used. 8.4 Number of Events generated
2.1	5.9.4.b Dial Back test plan modified for PinICL PC0094556 CNIM behaviour modified when going to FRIACO Fixed and not in Mode 1 - PinICL PC0093827 Changes required for use with ADSL at S60
2.2	Updates to: GetStatus for ADSL Monitor File Format for ADSL Note: Not circulated for review.
2.3	Updates to: Test Plan operations. QOS Result codes. Engineers screen - availability of network state.
3.0	Comments added
3.1	PC0093488 – Correction to decimal values in Cause Code table in appendix.
3.2	2.2.4 – Branch Resilient Network – and links within that section 2.2.5 - Table 9 Network Service Types including Branch Resilient Network Types
3.3	1. Updates to section 5.11 concerning Branch Resilient Network. 2. Section 4.1.3.b and 4.1.3.c, interfaces for Connection Modes and Service Types 3. Updates to 5.13 Test Sequences for BNR 4. Appendix A2 Call Plan for BNR
3.4	1. Further updates to section 5.11 concerning Branch Resilient Network. 2. Further updates to 5.13 Test Sequences for BNR 3. Further updates to Appendix A2 Call Plan for BNR
3.5	CP 4097 - Connection Manager reset every 20 minutes CP 4103 - GSM Signal Strength Indicator 2.2.9.c Bandwidth logging with a maximum value (PC0106937) 2.2.17 CNIM to send reset to Connection Manager every 20 minutes. 2.2.18 GSM Network gives Received Signal Strength Information

FUJ00171956

	2.2.19 Event Logging of Network Switching for BNR and linked sections 5.24 Received Signal Strength Indicator Changing call result codes to 8 characters as shown in appendices: Appendix A4, Appendix A5, Appendix A6, Appendix A7, Appendix A8
3.6	2.2.9.a Monitor record generation – PC0132421

0.6 Changes Expected

Changes
Further updates for Branch Network Resilience.

0.7 Table Of Contents

0 DOCUMENT CONTROL 2
0.1 Document History 2
0.2 Review Details 2
0.3 Associated Documents 3
0.4 Abbreviations/Definitions 4
0.5 Changes in this Version 5
0.6 Changes Expected 7
0.7 Table Of Contents 7
0.8 Table Of Figures 13
0.9 Table Of Tables 13
1 INTRODUCTION 18
1.1 Background 18
1.2 Scope 19
1.3 Documentation Outline 20
1.4 Summary 20
2 REQUIREMENTS 21
2.1 Requirement Overview 21
2.2 Detailed Requirements 25
2.2.1 CNIM Service Requirements 25
2.2.2 Interface to ADSL Card 25
2.2.3 Interface to Connection Manager 25
2.2.4 Branch Resilient Network 25
2.2.4.a Connection Switching 26
2.2.4.a.1 Automatic Failover to ISDN 27
2.2.4.b Connection Manager Interface 28
2.2.4.c Engineers Button Interface 28
2.2.4.c.1 Initiate Connection 29
2.2.4.c.2 Test Connection 29
2.2.4.c.3 Drop Connection 29
2.2.4.c.4 Reporting Connection Status 29
2.2.4.d Counter Call Scheduler Interface 29
2.2.4.e QOS Interface 30
2.2.4.f Eicon Card Interface 30
2.2.4.g Testing of the Backup Network 30
2.2.4.h ADSL to GSM On Demand (Standard and Strategic Site) 30
2.2.4.i Standard ISDN to GSM On Demand 30
2.2.4.i.1 Manual Operation of Failover 31
2.2.4.i.1.1 Connection Manager and CNIM 31

FUJ00171956

2.2.4.i.1.2 Manual Operation....31
2.2.5 ISDN - GSM Switch Process....31
2.2.6 Event Reporting for BNR Switching....32
2.2.7 Eicon Card Configuration....32
2.2.7.a Eicon Parameters - Numerical Values....33
2.2.7.a.1 Version 2 Run Mode....35
2.2.7.b Network Service Types - Including ADSL....35
2.2.7.c Call Plan....36
2.2.7.c.1 Call Plan Input....36
2.2.7.c.2 Call Plan Data Output....36
2.2.7.c.3 Call Plan Connection Configuration....36
2.2.7.c.4 Call Plan File....36
2.2.7.c.5 Randomisation of Connection and Disconnection....37
2.2.7.c.5.1 ADSL Offsets....38
2.2.7.d Line Test Overview....38
2.2.7.d.1 Determination of Communication Failure....39
2.2.7.d.1.1 Cause Code Description....39
2.2.7.d.1.2 Ping Failure....39
2.2.7.d.1.3 Changes for ADSL....39
2.2.7.d.2 Run Mode Description....40
2.2.7.d.3 Failure Mode Description....40
2.2.7.d.4 Test Requirements....40
2.2.7.d.4.1 Wait Times for Call Closure....40
2.2.7.d.4.2 Behaviour on Failure - Version 2....41
2.2.7.d.4.3 Testing During Establish Periods....42
2.2.7.d.4.4 Testing During Fixed Periods....43
2.2.7.d.4.5 Testing During Dialled Periods....44
2.2.7.d.4.6 Test Sequence –VSAT - Permanent Connection....45
2.2.7.d.4.7 Test Sequence - ADSL....45
2.2.7.d.4.8 Failure Flag State....47
2.2.7.e Line Connectivity....48
2.2.8 CDF Data Storage Requirement....49
2.2.8.a CDF Content....49
2.2.8.b CDF - Network Configuration (for CNIM access numbers)....50
2.2.8.c Phone Number Mapping....50
2.2.9 Call Logging Requirement....50
2.2.9.a Monitor Record....50
2.2.9.a.1 Record Format and Description....51
2.2.9.a.1.1 Monitor Record Format - CNIM Version 2....51
2.2.9.a.1.2 Monitor Record Format - CNIM Version 3....51
2.2.9.a.2 Initial Record Format....51
2.2.9.a.3 Final Record Format....52
2.2.9.a.4 Changes for Version 2....52
2.2.9.a.5 Monitor Record Format for ADSL....52
2.2.9.a.6 Monitor Record Format for ISDN and GSM over RAS....54
2.2.9.a.7 File Name Format....55
2.2.9.a.8 Monitor File Creation and Renaming....55
2.2.9.a.9 Call Monitoring for Satellite connected Outlets....55
2.2.9.a.10 Call Monitoring for ADSL connected Outlets....55
2.2.9.b Summary Record....56
2.2.9.b.1 Summary Files for ADSL....58
2.2.9.b.2 Summary File Name Format....58
2.2.9.c Bandwidth Logging for ADSL....58
2.2.10 Dial Back Requirement....60
2.2.11 Keep Alive Requirement....60
2.2.11.a Ping Sequence....60
2.2.11.a.1 Methodology....61
2.2.12 Time Format Requirement....62
2.2.13 GetStatus Query Requirement....63
2.2.13.a GetStatus Query Requirement for ADSL....66
2.2.13.b GetStatus Flag Settings for ADSL with ISDN and GSM Backup....67
2.2.13.c GetStatus Flag Settings for ADSL with GSM Backup....67

FUJ00171956

2.2.14 Satellite Requirements *67*
2.2.15 Tracing Requirements *67*
2.2.16 Static Test Requirements *67*
2.2.16.a CNIM Test – Implementation 67
2.2.16.a.1 Implementation Test at S60 68
2.2.16.b CNIM Test – normal running 68
2.2.16.b.1 Normal Test at S60 68
2.2.17 BNR - CP4097 CNIM to send reset to Connection Manager every 20 minutes *68*
2.2.17.a Service Type 13 - ADSL only Outlets 68
2.2.17.b Service Type 14 - ADSL Outlets with ISDN Backup 68
2.2.18 BNR - CP4103 GSM Network gives Received Signal Strength Information *68*
2.2.19 Event Logging of Network Switching for BNR *68*

3 ARCHITECTURE 70

3.1 SYSTEM DIAGRAM 70
3.2 OPERATIONAL OVERVIEW 71

4 EXTERNAL INTERFACES 72

4.1 INTERFACES PROVIDED 72
4.1.1 NT Service Interface *72*
4.1.2 GetStatus Interface to Counter Call Scheduler *72*
4.1.3 Operational Control Interface *72*
4.1.3.a Call Plan Registry 72
4.1.3.b Connection Modes Registry 72
4.1.3.b.1 FRIACO Establish Connection Types 74
4.1.3.b.2 FRIACO Fixed Connection Types 74
4.1.3.b.3 FRIACO Fixed With GSM - Connection Types 74
4.1.3.b.4 Metered Fixed Connection Types 75
4.1.3.b.5 Metered Fixed with GSM Connection Types 75
4.1.3.b.6 Metered On Demand Connection Types 75
4.1.3.b.7 Metered On Demand with GSM Connection Types 76
4.1.3.b.8 Voice Connection Types 76
4.1.3.b.9 Voice with GSM Connection Types 76
4.1.3.b.10 RAS ADSL Connection Types 77
4.1.3.b.11 RAS ADSL-GSM Connection Types 77
4.1.3.b.12 RAS ADSL-ISDN-GSM Connection Types 77
4.1.3.b.13 RAS ISDN Only Connection Types 78
4.1.3.b.14 VSAT Connection Types 78
4.1.3.b.15 Frame Relay Establish Connection Types 78
4.1.3.b.16 Frame Relay Fixed Connection Types 79
4.1.3.c Service Mode Registry 80
4.1.3.c.1 Service Mode – FRIACO 1 80
4.1.3.c.2 Service Mode – FRIACO 2 80
4.1.3.c.3 Service Mode - Metered 81
4.1.3.c.4 Service Mode - RAS 81
4.1.3.c.5 Service Mode - Voice 81
4.1.3.c.6 Service Mode - VSAT 81
4.1.3.c.7 Service Mode – Frame Relay 82
4.1.3.d Mapping Service Type to Service Mode 82
4.1.3.e Live Registry 82
4.1.3.f Period Registry 85
4.1.3.g RPC Registry 85
4.1.3.h Test Results Registry 86
4.1.3.i Times Registry 87
4.1.3.j SubAddressing Registry 89
4.1.3.k Trace Registry 90
4.1.3.l TuneableTrace Registry 90
4.1.3.m Service Event Registry 91
4.1.3.n Service Dependency Registry 91
4.1.3.o Eicon Registry 92
4.1.3.p User Registry 92

FUJ00171956

4.1.3.q Connection Manager Registry ... 92
4.1.3.r Interface with ADSL Diagnostic Monitor ... 93
4.1.3.s CNIM NST Groups ... 94
4.1.3.t CNIM Network Settings ... 94
4.1.3.u Bandwidth Configuration Settings ... 94
4.2 INTERFACES USED ... 95

5 DESIGN OVERVIEW ... 96

5.1 SERVICE DEFINITION ... 96
5.2 CNIM SERVICE DESIGN OVERVIEW ... 96
5.2.1 Service Dependencies ... 96
5.3 EICON CARD CONFIGURATION DESIGN OVERVIEW ... 96
5.3.1 Card Parameter Storage ... 96
5.3.1.a Phone Numbers and Network Service Type ... 96
5.3.1.b CHAP Passwords and User Ids ... 97
5.3.1.c Shorthold, Minimum Call Duration and CHAP Interval Times ... 97
5.3.2 Card Parameter Application ... 97
5.4 NETWORK SERVICE TYPE DESIGN OVERVIEW ... 97
5.5 CDF DATA STORAGE DESIGN OVERVIEW ... 97
5.6 CALL PLAN DESIGN OVERVIEW ... 100
5.7 QOS LOGGING DESIGN OVERVIEW ... 100
5.7.1 Call Logging - ISDN ... 100
5.7.1.a The IDI Interface ... 100
5.7.1.b Call Activation and Closure ... 102
5.7.2 Call Logging - VSAT ... 102
5.7.3 Call Logging - ADSL ... 102
5.7.3.a ADSL Diagnostic Monitor Interface ... 103
5.7.3.b Connection Manager Interface ... 103
5.7.3.c Bandwidth Calculation - ADSL Only ... 106
5.7.3.c.1 Bandwidth Pinging ... 108
5.7.3.c.2 Bandwidth Return Codes ... 108
5.8 DIAL BACK DESIGN OVERVIEW ... 108
5.9 BRANCH RESILIENT NETWORK ISDN/GSM SWITCH PROCESS ... 111
5.10 BRANCH RESILIENT NETWORK INTERFACE WITH CONNECTION MANAGER ... 111
5.10.1 RAS Connection Type Information ... 113
5.11 DETERMINATION OF FAILURE CODE ... 114
5.11.1 Cause Code Ranges ... 115
5.11.2 Eicon Cause Codes ... 115
5.12 ENGINEERS BUTTON, DESIGN OVERVIEW ... 116
5.12.1 BNR Static Data ... 118
5.12.2 Network Resilience State ... 118
5.12.3 Network Resilience Modes ... 120
5.12.4 Network Resilience History ... 121
5.12.5 Returning Network State ... 123
5.12.6 ISDN/GSM Switch Process ... 124
5.13 TEST STRATEGY, DESIGN OVERVIEW ... 125
5.13.1 Run Mode – ISDN Outlet ... 126
5.13.1.a Pre Version 2.0 ... 126
5.13.1.b Version 2 Onward ... 126
5.13.1.b.1 Service Type 11 at Metered Fixed ... 127
5.13.1.b.2 Service Type 11 at FRIACO Fixed ... 127
5.13.2 Ping Sequence ... 127
5.13.3 Test Strategy Design ... 130
5.13.3.a Diversion Operations ... 133
5.13.3.b Test Plan Details ... 135
5.13.3.b.1 Test Plan - FRIACO Establish ... 135
5.13.3.b.2 Test Plan - FRIACO or Metered Fixed ... 136
5.13.3.b.3 Test Plan - FRIACO Fixed at S92 ... 137
5.13.3.b.4 Test Plan - Dialled (MOD) ... 138

FUJ00171956

5.13.3.b.5 Test Plan - Dialled (VOD) 141
5.13.3.b.6 Test Plan - Dial Back S60 144
5.13.3.b.7 Test Plan - Satellite 145
5.13.3.b.8 Test Plan - ADSL 145
5.13.3.b.9 Test Plans for RAS at BNR - S92 145
5.13.3.b.9.1 Test Plans - ADSL Only 146
5.13.3.b.9.2 Test Plan - ADSL with GSM Backup 148
5.13.3.b.9.3 Test Plan- RAS GSM Backup 151
5.13.3.b.9.4 Test Plan - ADSL with ISDN and GSM Backup 152
5.13.3.b.9.5 Test Plan - ISDN Only 155
5.13.3.b.9.6 Test Plan - RAS at Idle 156
5.13.4 Code Character for Test Ranges 156
5.14 KEEP ALIVE STRATEGY OVERVIEW 157
5.15 TIME FORMAT OVERVIEW 157
5.16 DESIGN OVERVIEW: GETSTATUS QUERY 157
5.16.1 Connection Status 159
5.16.2 Connection Type 159
5.16.3 TickNailedUp 160
5.16.4 TickLastConnectionChange 160
5.16.5 FailCode 161
5.16.6 TickPermanent 161
5.16.7 Timeout 161
5.17 STATIC TEST MODES 161
5.17.1.a CNIM Test – Implementation 161
5.17.1.b CNIM Test – normal running 161
5.18 CNIM RESET 162
5.19 SERVICE INSTALLATION AND CONFIGURATION 162
5.20 CNIM TRACE 162
5.20.1 Default Trace Levels 163
5.20.2 CNIM Log File 163
5.20.3 TuneableTrace File 163
5.20.4 Event Log 164
5.20.5 Debugging Output 164
5.21 TRACE LOGIC 164
5.22 CALL LOGGING LOGIC 166
5.23 CP4097 - 20 MINUTE RESET OF CONNECTION MANAGER 166
5.24 CP4103 - LOGGING OF GSM RECEIVED SIGNAL STRENGTH TO TUNEABLETRACE 166
5.25 EVENT LOGGING OF NETWORK SWITCH 168

6 IMPLEMENTATION 170

6.1 SERVICE 170
6.1.1 Threading 170
6.1.2 Service control notifications 171
6.1.3 Service status notifications 172
6.1.4 Inter-thread Communication 173
6.1.5 Service Events 173
6.1.5.a CCNIM 174
6.1.5.b CCallManager - Test Thread 174
6.1.5.c CEiconManager - Logging Thread 174
6.2 CLASSES 175
6.2.1 Class Overview 175
6.2.2 CService 176
6.2.3 CServiceInstall 176
6.2.4 CCNIM 177
6.2.5 CEiconManager 177
6.2.5.a Protected Members 178
6.2.6 CCallManager 180
6.2.6.a Protected Members 183

FUJ00171956

6.2.7 CCallPlan *183*
6.2.8 CTestManager *184*
6.2.9 CIPAddress *184*
6.2.10 CEventLog *184*

7 NON FUNCTIONAL REQUIREMENTS 185

7.1 PERFORMANCE 185
7.1.1 Registry sizing *185*
7.1.2 Event logging *185*
7.2 RESILIENCE 185
7.2.1 Corrupt Policy File *185*
7.2.2 Failure of the CNIM service *185*
7.3 SECURITY 185
7.3.1 Event Logging *185*
7.4 SYSTEMS MANAGEABILITY 185
7.4.1 Installation/Removal *185*
7.4.2 Startup and Shutdown procedures *186*
7.4.3 Maintenance *186*
7.4.4 Software Distribution *186*
7.4.5 Year 2K compliance *186*
7.4.6 Finite Date Limits *186*
7.5 EXTENSIBILITY 186

8 ERROR HANDLING AND EVENT LOGGING 187

8.1 LOGGING REQUIREMENTS 187
8.2 EVENT LOGGING 187
8.3 AUDITING 187
8.4 EVENT LOGGING ESTIMATES 187

9 TARGET ENVIRONMENT 188

10 TESTING REQUIREMENTS 189

11 DELIVERABLES 190

11.1 SOFTWARE 190
11.2 DOCUMENTATION 190

12 ASSUMPTIONS AND RISKS 191

12.1 ASSUMPTIONS 191
12.2 RISKS 191

13 DESIGN CONFORMANCE 192

APPENDIX A1. CALL PLAN - CNIM 1,2,3 194

APPENDIX A2. CALL PLAN - CNIM 4 - S92 FOR BNR 202

APPENDIX A3. EVENT LOG MESSAGES 213

APPENDIX A4. CAUSE CODE DESCRIPTIONS 217

APPENDIX A5. RAS ERROR CODES 220

APPENDIX A6. CONNECTION MANAGER CAUSE CODES 225

APPENDIX A7. FUJITSU DEFINED CAUSE CODES 226

FUJ00171956

APPENDIX A8. CNIM CAUSE CODES..... 227

APPENDIX A9. DIAPI INTERFACE..... 228

APPENDIX A10. RAS ERROR CODES - PRE S92..... 231

0.8 Table Of Figures

Figure 1 Document Hierarchy 20
Figure 2 ADSL-ISDN Switching Logic 27
Figure 3 Testing During FRIACO Establish 42
Figure 4 Testing During Fixed Periods 43
Figure 5 Testing During Dialled Period 44
Figure 6 Test Sequence - VSAT 45
Figure 7 Test Sequence - ADSL 46
Figure 8 Fail Flag State Mechanism 47
Figure 9 Ping Sequence (call to Data Centre) 62
Figure 10: System Diagram 70
Figure 11 Telephone number mapping from Registry 99
Figure 12 Call Reversal 110
Figure 13 Trace Logic 165
Figure 14 Call Logging Logic 166
Figure 15: Service threading 171
Figure 16 CNIM Class Overview 176
Figure 17 Eicon Interfaces 177
Figure 18 Logging Thread - IDI Interaction 178
Figure 19 Call Plan Conversion to Element List 181
Figure 20 CPL to Test Sequence Schematic 182

0.9 Table Of Tables

Table 1 Connection Types and Service Types 29
Table 2 Eicon Card Timer Parameters 33
Table 3 Eicon Card Timer Parameters - Version 1 33
Table 4 Eicon Card Timer Parameters - Version 2 34
Table 5 Eicon Card Timer Parameters - Version 3 34
Table 6 Eicon Card CHAP Parameters 34
Table 7 Eicon Card Called Party Numbers - CNIM Ver. 1 35
Table 8 Eicon Card Called Party Numbers - CNIM Ver. 2.0 35
Table 9 Network Service Types including Branch Resilient Network Types 36
Table 10 Call Plan Offsets – ISDN/Data/FRIACO 38
Table 11 Call Plan Offsets - ADSL 38
Table 12 Wait times for call closures 41

FUJ00171956

Table 13 Connection Types 49
Table 14 Number Types and Descriptions 50
Table 15 Monitor Record Format for ADSL 54
Table 16 Monitor Record Format for ISDN and GSM 55
Table 17 Format of Summary Record 56
Table 18 – Network Connection Status from CNIM 64
Table 19 – QOS Flags from CNIM 65
Table 20 QOS Flags for Connection Types 66
Table 21 Flag Settings for Resilient Network 67
Table 22 Flag Settings for Resilient Network 67
Table 23 Registry Entries - Call Plan 72
Table 24 CNIM and BNR Modes for Connection Types - FRIACO Establish 74
Table 25 CNIM and BNR Modes for Connection Types - FRIACO Fixed 74
Table 26 CNIM and BNR Modes for Connection Types - FRIACO Fixed with GSM 74
Table 27 CNIM and BNR Modes for Connection Types - Metered Fixed 75
Table 28 CNIM and BNR Modes for Connection Types - Metered Fixed with GSM 75
Table 29 CNIM and BNR Modes for Connection Types - Metered On Demand 75
Table 30 CNIM and BNR Modes for Connection Types – MOD with GSM 76
Table 31 CNIM and BNR Modes for Connection Types – Voice 76
Table 32 CNIM and BNR Modes for Connection Types - Voice with GSM 76
Table 33 CNIM and BNR Modes for Connection Types - ADSL only 77
Table 34 CNIM and BNR Modes for Connection Types - ADSL with GSM 77
Table 35 CNIM and BNR Modes for Connection Types - ADSL with ISDN and GSM 77
Table 36 CNIM and BNR Modes for Connection Types - ISDN Only 78
Table 37 CNIM and BNR Modes for Connection Types – VSAT 78
Table 38 CNIM and BNR Modes for Connection Types – Frame Relay Establish 78
Table 39 CNIM and BNR Modes for Connection Types – Frame Relay Fixed 79
Table 40 Service Mode – FRIACO 1 80
Table 41 Service Mode – FRIACO 2 80
Table 42 Service Mode - Metered 81
Table 43 Service Mode - RAS 81
Table 44 Service Mode - Voice 81
Table 45 Service Mode - VSAT 81
Table 46 Service Mode – Frame Relay 82
Table 47 Mapping Service Type to Service Mode 82
Table 48 Registry Entries - Live 85
Table 49 Registry Entries - Period 85
Table 50 Registry Entries - RPC 86

FUJ00171956

Table 51 Registry Entries - Test Results 87
Table 52 Registry Entries - Times 89
Table 53 Registry Entries - Users 89
Table 54 Registry Entries - Sub Addressing 90
Table 55 Registry Entries - Tracing 90
Table 56 Registry Entries - TuneableTrace 90
Table 57 Registry Entries - CNIM TuneableTrace 91
Table 58 Registry Entries - Message Path 91
Table 59 Registry Entries - CNIM Service Dependency on RPC 91
Table 60 CDF Data Storage in Registry 92
Table 61 User Data Storage in Registry 92
Table 62 Connection Manager Registry 93
Table 63 ADSL Diagnostic Monitor Registry 94
Table 64 CNIM ADSL Diagnostic Monitor Data 94
Table 65 CNIM NST Groupings 94
Table 66 CNIM Network Settings 94
Table 67 Bandwidth Configuration Settings 95
Table 68 Bandwidth Result Codes 95
Table 69 IDI Parameter Description 102
Table 70 Connection Manager Switch Registry 111
Table 71 DialMode Description 112
Table 72 DialMode Strings in CNIM Registry 112
Table 73 Connection Manager Network Types 113
Table 74 Port Contents for Connection Types 113
Table 75 Connection Manager Phonebook Details 114
Table 76 Determination of Failure Code 114
Table 77 Cause Code Ranges 115
Table 78 Engineers Button Trigger Registry 116
Table 79 BNR Static Configuration Data 118
Table 80 Branch Network Resilience - State Information 119
Table 81 Mapping Mode to Connection Type 120
Table 82 Mapping History to Connection Type 121
Table 83 Engineers Button Options 121
Table 84 Resilient Network Status 123
Table 85 Network State Screen Information for BNR 124
Table 86 Called Party Numbers per Mode - Version 1 126
Table 87 Called Party Numbers per Mode - Version 2 127
Table 88 CPL Operations 132

FUJ00171956

Table 89 Diversion Operation Conditions 133
Table 90 E Range Test Elements - FRIACO Establish Period - S60 135
Table 91 F Range Test Elements - FRIACO Fixed Period - S60 136
Table 92 FRIACO Fixed Test Elements- S92 138
Table 93 D Range Test Elements - Dialled Period 140
Table 94 I Range Test Elements - Dialled Period - ISDN 143
Table 95 Dial Back 144
Table 96 Ping Result and Line Status 144
Table 97 P Range Test Elements - Permanent Connection (Satellite) - S60 145
Table 98 A Range Test Elements - ADSL - S60 - With Test On Line State Change 145
Table 99 RA Range Elements - S92 147
Table 100 RAG Range Elements - S92 150
Table 101 RG Range Elements - S92 151
Table 102 Test Plan - ADSL/ISDN/GSM 154
Table 103 RIT Range Test Elements - S92 155
Table 104 RID Range Test Elements - S92 156
Table 105 GetStatus Return Values 158
Table 106 Connection Status Values 159
Table 107 Connection Type - First Byte 159
Table 108 Connection Type - Second Byte 160
Table 109 Connection Type - Third Byte 160
Table 110 Implementation Test Flags 161
Table 111 Trace Flags 163
Table 112 Tracing Parameters 164
Table 113 Network Switch Event Requirements 168
Table 114 Events for Change of Connection Type 169
Table 115 Test Thread Events 174
Table 116 Eicon Manager Events 174
Table 117 Event Logging Estimates 187
Table 118 RAS Error Codes and CNIM Equivalents 224
Table 119 Connection Manager Cause Codes 225
Table 120 Fujitsu Defined Cause Codes 226
Table 121 CNIM Service State Codes 227
Table 122 DIAPI Functions 230

FUJ00171956

1 INTRODUCTION

1.1 Background

The introduction of FRIACO network service at BI3 instigated a fundamental change in the way the Post Office (PO) Outlets interface with the Data Centres. FRIACO provides a 'fixed price' connection for a specified period of time during the day and hence no call charges.

A number of the PO Outlets are 'permanently' connected via FRIACO, where the circuit is kept active and hence a permanent connection after the number has been dialled.

In areas where the FRIACO service is not currently available, a metered call is kept active and hence a permanent connection for the specified period of time during the day. These Outlets are classified as 'permanently' connected via a metered call.

Other Outlets utilise 'dial on demand' (pay-as-you-go) and maintain the connection for the duration of the transaction only incurring call charges for that duration.

The current proposed mix of 'permanent' against 'metered' is 12,000 'permanent' at full Network Banking implementation the rest on metered access.

The FRIACO service provides for 'in-bound' calls only (PO to Data Centre), thus a method for software distribution has to be devised, and additionally we must retain a mechanism to access an Outlet from the Data Centre for support access. Initially we will have 6000 daytime FRIACO outlets, rising to 12,000 over 2 years.

At S52 the use of ADSL will commence at a number of pilot sites. The use of ADSL will then spread across the entire estate.

Each gateway PC will be fitted with an ADSL modem card manufactured by Conexant. CNIM will not be able to interface to the card via the Conexant API as this is being used by the ADSL Diagnostic Monitor. Instead, CNIM will request low level connection state information from the ADM service itself. CNIM will be notified of the state of the RAS connection via registry information supplied by Connection Manager.

When running at ADSL, CNIM will provide only QOS data, including new bandwidth information, and an interface for Counter Call Scheduler.

CP3898 is concerned with the development of a Branch Resilient Network, primarily to provide a backup for ADSL outlets in that they may use either an ISDN or GSM connection in the event of network failure. In addition ISDN outlets may use a GSM connection under the same circumstances.

Note that this document version, 3.2, is not a complete specification for the Branch Resilient Network operation of CNIM but is primarily concerned with the interface specifications between CNIM and other applications. Further detail concerning modifications to the internal operation of CNIM will be added in the next version.

Section 2.2.4 gives an overview of the interface changes and contains links to other sections which contain further details of these changes.

1.2 Scope

This document specifies the detailed design of the Counter Network Infrastructure Manager (CNIM). CNIM is run on an outlet's gateway PC and its essential function is to control the

FUJ00171956

numbers used by the Eicon card and to log all calls. In addition the use of an interface .DLL (CNIM_API.dll) allows further status information to be extracted from CNIM.

CNIM deliverables comprise the service executable, CNIM.exe and an interface .DLL, CNIM_API.dll. A further executable, CNIMConfig.exe is also delivered which uses further functionality within the .DLL to cause the CNIM service to carry out functions such as testing all supplied phone numbers.

FUJ00171956

1.3 Documentation Outline

The organisation of the relevant documentation is shown in Figure 1.

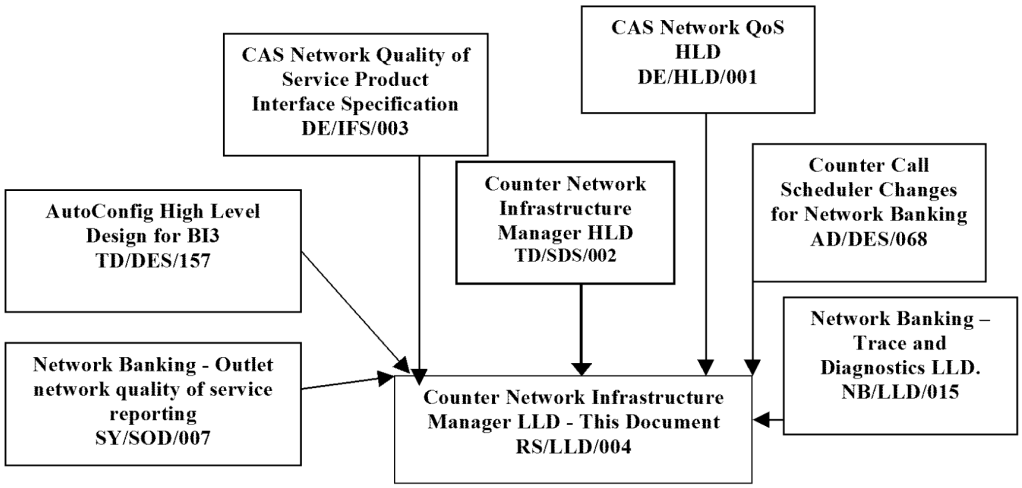

Figure 1 Document Hierarchy

1.4 Summary

This document conforms to the current template for design documents:

Section 2 defines the requirements

Section 3 describes the architecture and highlights the external boundaries

Section 4 describes the external interfaces in detail

Section 5 presents a design overview

Section 6 shows the implementation details

Section 7 describes how the Non Functional Requirements have been addressed

Section 8 describes details of error handling and event logging

Section 9 specifies the target environment

Section 10 describes the unit and integration test requirements

Section 11 defines the content of the software deliverables

Section 12 looks at the assumptions and risks associated with the activity

Section 13 tracks conformance to requirements

FUJ00171956

2 REQUIREMENTS

The requirements for the CNIM are derived from [HLD_CNIM] - see document [Ref 2].

The references given below for detailed requirements and design overview are internal references within this document.

2.1 Requirement Overview

Tag	Ref	Description
1	3.1	**CNIM Service.** CNIM will function as a Service. Under WinNT. Detailed Requirements: See Section 2.2.1 Design Overview: See Section 5.2
2	3	**Eicon Card Configuration.** CNIM will configure the Eicon card in a manner which is consistent with the mode of operation required. Detailed Requirements: See Section 2.2.7 Design Overview: See Section 5.3
3	3	**Network Service Type** CNIM configuration of the Eicon card and mode of operation will be within the concept of a Network Service Type that is assigned to the outlet. Detailed Requirements: See Section 2.2.7.b Design Overview: See Section 5.3.1
4	3.2.1	**CDF Data Retrieval and Usage** Outlet configuration data for phone numbers and Network Service Type is delivered via a CDF. See [Ref 21]. CNIM is required to retrieve CDF data from registry. Detailed Requirements: See Section 2.2.8 Design Overview: See Section 5.5
5	3.2.3	**Call Plan** CNIM configuration of the Eicon card and mode of operation will be within the concept of a Call Plan that is generic across all outlets. Detailed Requirements: See Section 2.2.7.c Architecture: See Section 5.5
6	4.5	**Call Logging** CNIM will log each call to a Monitor file and produce a Summary file of the calls for each day. Detailed Requirements: See Section 2.2.9 Design Overview: See Section 5.7
7	4.5	**Call Logging - ADSL** In addition to the Monitor and Summary files produced for normal

FUJ00171956

		logging CNIM will create a Bandwidth log as well. Detailed Requirements: See Section 2.2.9 Design Overview: See Section 5.7
8	4.3	**Dial Back** If CNIM detects that the Data Centre has attempted to contact the outlet whilst the line is disconnected, it will go into KeepAlive mode to cause the line to connect, see section 10. Detailed Requirements: See Section 2.2.10 Design Overview: See Section 5.8
9	4.8.3	**Test Strategy** CNIM is required to determine whether comms have become unavailable with as little loss of time as possible whilst minimising unnecessary line usage. In the event of comms failure CNIM will attempt to reconfigure the Eicon card such that comms are re-established. CNIM is not required to reconfigure the network interface for ADSL or Satellite outlets. However CNIM is required to determine the ADSL network bandwidth at regular intervals and to test that it can ping the Data Centre. Detailed Requirements: See Section 2.2.7.d Design Overview: See Section 5.12
10	4.4	**Keep Alive Strategy** During certain periods of the day CNIM is required to maintain the line connection to eliminate the call setup time. CNIM may also be required to maintain line connection if a call from the Data Centre to the outlet has been detected, see table entry 8. The Keep Alive mechanism will include pinging one or more of the Data Centres. Detailed Requirements: See Section 2.2.11 Design Overview: See Section 5.14
11	2.1.5	**Time Format** All times used by CNIM will be in UTC with the exception of times specified within the Call Plan. Call Plan times will be in local time so that the same Call Plan can be used throughout the year. Detailed Requirements: See Section 2.2.12 Design Overview: See Section 5.15
12	4.6	**GetStatus Query** CNIM will accept a "GetStatus" query from an external source. CNIM will return data related to the current connection type and status. Detailed Requirements: See Section 2.2.13

FUJ00171956

		Design Overview: See Section 5.16
13	4.10	**Static Test Modes** CNIM is required to supply two static test modes: 1) Implementation Test 2) Normal Test Detailed Requirements: See Section 2.2.16 Design Overview: See Section 5.17
14		**Branch Resilient Network (CP3898)** 1. CNIM will provide an automatic failover facility between ADSL and ISDN for Network Service Type 14 outlets. The ISDN connection will be managed via RAS. 2. CNIM will test the ADSL failover to ISDN every Wednesday night for NST 14 outlets. 3. CNIM will respond to an Engineers Application that will request a change to a new network type, i.e. ADSL, ISDN, GSM or NDIS. 4. CNIM will generate an event stating that it is moving to a new network type. The event will contain the name of the required network type.
15		**Connection Manager Reset (CP4097)** CNIM to send reset to Connection Manager every 20 minutes when network problem detected Currently CNIM on detection of a network failure sends a "reset" request to Connection Manager , on receipt of this call, Connection Manager drops the existing RAS connection, (whatever the status of the call), and attempts to re-establish the connection. In some instances Connection Manager re-establishes the connection and all appears ok, however no data flows. In this scenario CNIM does not send another "reset" request to Connection Manager, it remains in a "wait state" as it has not seen any change in packets sent or received. Under these circumstances the intention of this CP is that CNIM will send the "reset" request to Connection Manager every 20 minutes, and not just once as per current implementation. The sequence of events will be: (a) A CNIM "bandwidth" ping fails (bandwidth pings every 5 minutes) (b) CNIM enters error recovery mode and pings all 4 VPN servers (c) All 4 VPN pings fail (d) CNIM sends "reset" request to Connection Manager (e) CNIM starts two timers a 20 minute and a 15 minute timer (f) CNIM continues with 5 minute pings (g) If ping successful, cancel both 20 & 15 minute timers and exit error recovery

FUJ00171956

		(h) After 15 minute timer "off-Line" Indicator set (i) After 20 minute timer "reset" request sent to Connection Manager Reset 20 minute timer
16		**GSM Signal Strength Indicator (CP4103)** Backup Network GSM option provides Received Signal Strength information. In summary this change proposes making the GSM Received Signal strength information available to both the Engineer installing the GSM modem and within diagnostic logs on the Gateway PC. Additionally the unique identification of the modem is also written to the diagnostics logs. CNIM / Connection Manager Immediately prior to initiating a connection* over the BNR GSM modem, the following commands will be sent to the GSM modem; AT+CSQ Response is +CSQ:rssi,99 where rssi in range 0 through 99, note rssi is the abbreviation for received signal strength indication AT+CGSN Response is imei, where imei has format nnnnnn—nn-nnnnnn-n, note imei is the abbreviation for International Mobile Equipment Identity The responses will be written to relevant diagnostic logs by CNIM and / or Connection Manager as appropriate. Additionally when triggered via registry items for supporting the user interface, the AT+CSQ command will be sent to the GSM modem and the rssi response written to the registry. * Including automated redials by Connection Manager. User Interface Confirm Connection Screen – add extra display field GSM Received Signal strength. This is updated from an additional registry key "GMSSignalStrength" Confirm Connection Screen If GSM is selected then on the Confirm dialogue, set a Registry flag which causes CNIM to obtain rssi from modem. Display rssi on screen, reset flag and poll for changes updating display as necessary. Continue until confirm / cancel is selected Note this is necessary since the engineer may be moving the modem around / attaching an external antenna

FUJ00171956

2.2 Detailed Requirements

This section gives more details of the CNIM requirements.

2.2.1 CNIM Service Requirements.

Design Overview: See section 5.2

The CNIM shall run as an NT service under the LocalSystem account. The service shall start automatically.

2.2.2 Interface to ADSL Card

Design Overview: See section 5.7.3

The connection to the ADSL Conexant card is shared with the ADSL Diagnostic Monitor service. The Conexant API does not allow more than one concurrent connection and the ADM service will be responsible for storing the connection state from the card, in registry.

CNIM will use the ADM registry to retrieve the connection state.

CNIM will set a flag in the ADM section of registry, indicating that it requires the current connection state. CNIM will then wait for registry notification that ADM has updated registry and will then retrieve the current connection state. After setting the new connection state ADM will reset the flag. CNIM will check the flag state to ensure that it is reading the latest data.

The connection status data will be stored in the CNIM area of registry.

2.2.3 Interface to Connection Manager

Design Overview: See section 5.7.3

Connection Manager will store within registry, the ADSL connection state and the Day D status.

CNIM will request registry notification of changes to both these state flags. This state data may be the first indication to CNIM of a change in network state. When given this indication CNIM will attempt to determine the cause of failure from the lowest level upwards in order to give the greatest amount of diagnostic information.

CNIM will use this state information to determine the name format of the QOS files to be created.

2.2.4 Branch Resilient Network

Lack of reliability of the ADSL network has led to the requirement for a means of ensuring communications are available via the ISDN network at selected sites. In addition all ADSL sites will have backup available via a GSM modem.

The Branch Resilient Network operation is concerned with switching between different types of connection where the connection type required, ADSL, ISDN or GSM, is signalled by CNIM to Connection Manager.

2.2.4.a Connection Switching

The following design considerations for connection switching, are taken from the Design Proposal, [DP_BRN], version 0.3.

FUJ00171956

2.2.4.a.1 Automatic Failover to ISDN

Automatic failover between ADSL and ISDN is required for the Strategic Sites and the logic flow for this process is shown in Figure 2

- A backup ISDN connection would only be required during core hours.
- In order to ensure a robust backup policy, the ISDN connection will be maintained until the end of core hours.
- The ADSL connection will be tested at the end of core hours and throughout the night if the test continues to fail.
- The ISDN connection will be reconnected at the start of core hours if the ADSL connection is unavailable.

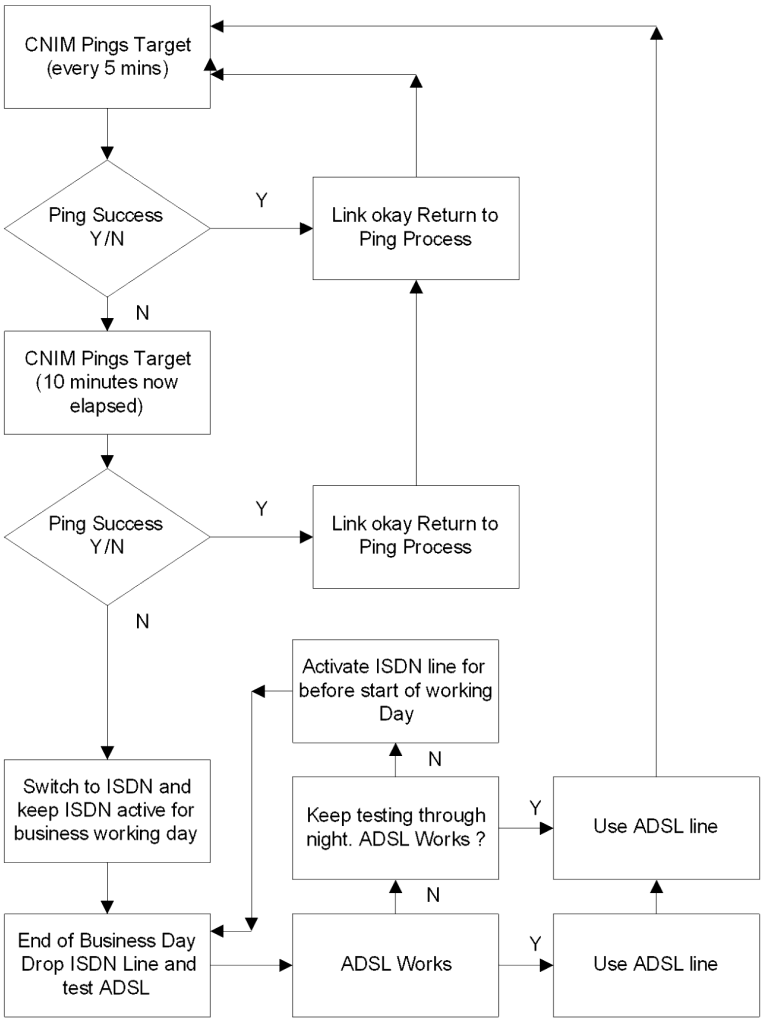

Figure 2 ADSL-ISDN Switching Logic

FUJ00171956

The backup connection will be dropped at 8.30pm to ensure that the end of day messages have been uploaded to the Datacentre. End of day messages have a shut off of 8.30pm.

After the connection has been dropped branches will be unable to connect to the Datacentre and similarly the Datacentre would not be able to initiate a call out to a branch.

2.2.4.b Connection Manager Interface

Design Overview: See section 5.10

CNIM will be responsible for setting the required connection type within the Connection Manager area of registry and then triggering a Connection Manager reset.

Connection Manager will then attempt to connect using the appropriate phonebook entry for the connection type required.

CNIM will set a simple registry flag specifying the connection type required and Connection Manager will respond by attempting a connection of that type. CNIM will monitor the standard Connection Manager output to determine the success or otherwise of the connection attempt.

2.2.4.c Engineers Button Interface

Design Overview: See section 5.12

A new set of engineer's buttons will be used to directly control the connection type currently in use and to test that connection.

The following requirements are taken from the design proposal.

- To Initiate/Test that ADSL is working
- To Initiate/Test and Drop the ISDN Backup connection for the Strategic Sites
- To Initiate/Test and Drop the GSM On Demand connection.
- A "one shot" password from the Helpdesk will be required to allow the initial start of the Manual switch to ISDN
- Once the ISDN line has been dropped at the end of the business day then CNIM will attempt to re-establish the ADSL connection.
- If the ADSL line has been re-established then the button for the subpostmaster or engineer should be disabled requiring a one off password again to allow initiation.

When the Backup Line is initiated or dropped as for the Automatic solution an NT Event should be generated and passed to SYSMAN so people are aware of which sites are running on the backup network.

The buttons must do one of three things, initiate a connection of a certain type, test the connection and register a working connection.

A new screen will be provided to the Post Master and the Engineer. This will allow the switch of connection type between ADSL, ISDN and GSM.

In order to switch to GSM the Post Master will require a one shot password. The engineer will not require a one shot password specifically for this switch as he will already be logged on using a one shot password.

FUJ00171956

The one shot password provided to the Post Master will expire at an appropriate time on or before midnight.

The screen will show the following buttons:

- Initiate Connection
- Test Connection
- Drop Connection

2.2.4.c.1 Initiate Connection

The Initiate Connection button will lead to a further screen offering a number of options for the connection type to be initiated. These are tabulated below. Note that all connections are managed using the RAS process except where NDIS is indicated.

Connection Type/ Network Service Type	ADSL	ISDN	GSM	VSAT
1,4,7 (Switch requires reboot)	No	Yes (NDIS)	Yes	No
2	No	No	No	Yes
13	Yes	No	Yes	No
14	Yes	Yes	Yes	No

Table 1 Connection Types and Service Types

Initiation of a connection will automatically lead to the connection being tested.

The Initiate Connection facility is not available if the Day D flag is set.

Initiation of a failover connection, i.e. ADSL to either ISDN or GSM or ISDN to GSM, if done within the working day, will cause CNIM to remain on that connection type until the end of the working day and then attempt to return to its primary connection type.

Manual initiation of a failover connection outside of the working day will cause CNIM to maintain the chosen connection type until the start of the next working day.

2.2.4.c.2 Test Connection

The Test Connection button will initiate a set of CNIM test pings. CNIM will not change connection type as a result of ping failure.

2.2.4.c.3 Drop Connection

The Drop Connection button will set the connection state to idle. The Post Master or engineer is responsible for initiating a new connection.

2.2.4.c.4 Reporting Connection Status

CNIM will maintain connection status information within registry which will be displayed either on the button screen or via a link from that screen.

A separate area of registry will be maintained for ADSL, ISDN and GSM connection types.

FUJ00171956

Within each area a status string will show the date/time for the last connection of that type, the call result in terms of success/failure codes and an interpretation of that code if available. The phone number dialled will also be included.

2.2.4.d Counter Call Scheduler Interface

See section 2.2.13 which has been updated to include the new Branch Resilient Network requirement.

2.2.4.e QOS Interface

The use of RAS to create ISDN and GSM connections requires that these be included as new connection types within the monitor record file for each day.

See section 2.2.9 which has been updated to include the new Branch Resilient Network requirement.

2.2.4.f Eicon Card Interface

The requirement to be able to switch between ISDN using the NDIS driver and GSM over RAS will require the Eicon card to be disabled prior to a reboot.

Disabling of the Eicon card will be carried out by setting the “Start” value of the TEDMULTI driver from Automatic (0x00000002) to Disabled (0x00000004) within the registry key shown below:

[HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\DiehI_DIVA_TEDMULTI
]
"Start"=dword:00000002

After rebooting the platform, the Eicon card will be disabled and this will ensure that all WAN communications are via the GSM card.

2.2.4.g Testing of the Backup Network

It is proposed that the ISDN backup network be tested once a week on a Wednesday which is the day of the week when Software Distribution is not carried out. This should be done on a random timer to avoid all sites trying to connect at once. This parameter must be easily configurable as there may be a need to change the date/time.

More detail on this is given in section 5.13.3.b.9.5

2.2.4.h ADSL to GSM On Demand (Standard and Strategic Site)

Deployments of the GSM On Demand solution will require the Postmasters to call the Horizon Service Desk each morning that they have the solution deployed. They will be issued a “One Shot” password that will allow manual initiation of the GSM connection.

A GSM modem is connected via a Serial cable to the Specialix Serial card which is installed in all Gateway PC’s. A dialled connection is established from the Gateway PC and operates in a similar manner to a normal PSTN connection.

FUJ00171956

This has been used in a form as a solution for Day D/J, but those solutions were more about clearing transactions from a branch to the Correspondence servers if a branch had been offline for a long period. It had no two way communications capabilities and Online Transactions were not available in that scenario either.

2.2.4.i Standard ISDN to GSM On Demand

There will be approximately 1000 sites still left on ISDN due to the inability to provide ADSL to those locations. These ISDN connected branches use the NDIS driver to control the Eicon ISDN card to deliver "dial on demand" capability.

Use of this NDIS driver means that there is a need to reboot the Gateway PC's to switch to the RAS drivers and unbind the IP address from the Eicon card. There are three scenarios where a reboot may be required:

- When switching from the failed ISDN to use the GSM solution
- Switching back once the ISDN line has been repaired
- Any testing required to establish the ISDN line is repaired satisfactorily

2.2.4.i.1 Manual Operation of Failover

The process as described previously is just as relevant for the ISDN sites to use GSM except for the expected need for a reboot when switching between modes of operation. All reboots will be "attended" reboots requiring the Postmaster to be present. There are some variances which are described in the Connection Manager and CNIM description.

2.2.4.i.1.1 Connection Manager and CNIM

Generally the operation of this service would be very similar to what has been previously defined except for the following differences:

2.2.4.i.1.2 Manual Operation

At this point it assumes the manual establishment of the call has already been done as per the descriptions earlier.

- At the end of Normal Business hours CNIM would check the Service type to see if it is an "ISDN service type" *(note: changes are occurring to usage of ISDN service types and a check should be made prior to the LLD phase to ensure the correct types are covered).* If the GSM Flag is set in the registry then CNIM will inform Connection Manager to drop the GSM call.
- The Gateway PC will be left in such a state that it is ready for the Postmaster to call the HSH the following morning and initiate the GSM connection on being issued with a "one shot" password.
- The Gateway PC will not try to switch back to ISDN during the evening to test the ISDN line, this adds unnecessary complication in terms of requiring an Unattended Reboot which adds cost and complicates the overall solution. As a call will already be open for the faulty ISDN line the need for a Reboot to

FUJ00171956

switch back to ISDN can be managed by the HSH once it is confirmed that the ISDN line has been fixed.

2.2.5 ISDN - GSM Switch Process

This process is specific to the ISDN sites running with the use of the NDIS driver. About 1000 sites of this type will remain in operation.

This will be carried out between CNIM and an external switch process.

CNIM will intercept the button press requiring a switch either to or from GSM and will ensure that no call is in progress before initiating a reboot via an external application.

2.2.6 Event Reporting for BNR Switching

The following details are taken from SY/DES/037

CNIM is responsible for controlling the switch between network types. On switch to a new network type CNIM will raise an event. CNIM will include the following information specifically within the event text:

- *The network type before the switch;*
- *The network type following the switch;*
- *The time and date the switch was attempted.*

CNIM will raise an information event where the switch was successful and an error event where the switch was not successful. A unique, to CNIM, event ID will be recorded against the event allowing Tivoli to filter the events to be forwarded to the data centre.

The following additional information will be gleaned from the event itself:

- *The time the event was raised and therefore the switch was complete, i.e. when the event was written;*
- *The Gateway counter machine name, which includes the FAD code of the Branch.*

CNIM is also responsible for testing the ISDN backup network connection at strategic outlets once per week. The event raised to record a successful test will include the information document above against the standard network type switch event plus the following additional information / changes:

- *The percentage of successful ping attempts made across the 10 minute test period.*

A different event ID will be used to allow the event to be distinguished from events relating to a switch required following a failure.

The events for this are shown in Appendix A3 - IDs 490 to 492

2.2.7 Eicon Card Configuration.

Design Overview: See section 5.3

CNIM is required to configure the Eicon card with the correct parameters, consistent with the network type and connectivity required throughout the day. The network and connectivity requirements are controlled by the Network Service Type for the outlet combined with a generic Call Plan which is applicable to all outlets.

FUJ00171956

The Eicon card is the network card connecting the Outlet Gateway to the Data Centres. The network to which the card is connected may be either ISDN, Data or FRIACO. If ISDN it will be a Dial on Demand connection and if Data it may be either a Dial on Demand or Fixed connection. If the network type is FRIACO the connection type will be Fixed.

The Eicon card must be configured to suit the type of network to which it is connected and the type of connectivity required.

The following Eicon card parameters will be configured by CNIM:

Parameter	Description
Inbound Password	CHAP Password expected from calling node.
Inbound User ID	UID expected from calling node.
CHAP Interval	Interval, in seconds, between CHAP authentication's
Shorthold Timer	Length of time, in seconds, after the last received data packet for which the line will be held open.
MCDT	Minimum Call Duration Time
CPN1	Called Party Number 1
CPN2	Called Party Number 2
CPN3	Called Party Number 3
CPN4	Called Party Number 4

Table 2 Eicon Card Timer Parameters

The Eicon card will contain a list of Inbound User IDs prior to CNIM installation. When CNIM is first run it will add the Inbound User ID for the Data network, to the list. Thereafter no further configuration of this parameter is required.

The Inbound Password differs between the ISDN and Data/FRIACO networks. Therefore one password applies to ISDN and one to Data/FRIACO.

CNIM will extract the Inbound Password from the card when the service is installed. This is unique to each outlet and is stored in registry to be reapplied to the card should it be reconfigured to use ISDN again.

CHAP Interval differs between ISDN and Data/FRIACO. One value is applied whilst on ISDN and another whilst on Data/FRIACO.

In CNIM version 1, Shorthold Timer and MCDT are independent of network type and vary only with the type of connectivity required. That is different values are used whilst at Dial on Demand or at Fixed.

Called Party Numbers 1 to 4 are used to determine which number is dialled by the card. Although it is possible for the card to move to the next number in this list in the event of network unavailability, in practise this facility is disabled. Therefore the card will only ever use the number configured in CPN1.

2.2.7.a Eicon Parameters - Numerical Values

In version 1 of CNIM the Eicon parameters are the values shown below in Table 3

FUJ00171956

Type	Minimum Data Time (MCDT)	Idle Time (Short Hold Timer)	Minimum Call Length
Dial On Demand	6	3	9
Fixed	10	40	50

Table 3 Eicon Card Timer Parameters - Version 1

In version 2 of CNIM the Eicon parameters will be modified to the values shown in Table 4, below, and have a dependency on network type.

Type	Minimum Data Time (MCDT)	Idle Time (Short Hold Timer)	Minimum Call Length
ISDN voice	20	5	25
Metered Dialled	0	5	5
Fixed	10	40	50

Table 4 Eicon Card Timer Parameters - Version 2

In version 3 of CNIM the Eicon parameters will be modified to the values shown in Table 4, below, and have a dependency on network type.

Type	Minimum Data Time (MCDT)	Idle Time (Short Hold Timer)	Minimum Call Length
ISDN voice	20	5	25
Metered Dialled	0	5	5
Fixed	10	60	50

Table 5 Eicon Card Timer Parameters - Version 3

The CHAP parameters values shown in Table 6 are used to optimise network connectivity whilst keeping line costs to a minimum.

Parameter	ISDN	Data/FRIACO
CHAP Interval	10	0
Inbound Password	Supplied in Registry	Supplied in Registry
Inbound User ID	N/A	Supplied in Registry

Table 6 Eicon Card CHAP Parameters

Configuration of the Called Party Number entries on the Eicon card are displayed in Table 7. Under normal operation CNIM will run in Mode 1 and will configure the card with the Mode 1 Primary number as CPN1. CPN2-CPN4 will not be used in any mode

For a description of Run Mode see section 5.13.1

Parameter	Description	Run Mode 1	Run Mode 2	Run Mode 3
CPN1	Called Party Number 1	Mode 1 Primary or	Mode 2 Primary or	Mode 3 Primary

FUJ00171956

		Secondary	Secondary	
CPN2	Called Party Number 2	Not Used	Not Used	Mode 3 Secondary
CPN3	Called Party Number 3	Not Used	Not Used	Mode 3 Tertiary
CPN4	Called Party Number 4	Not Used	Not Used	Mode 3 Primary

Table 7 Eicon Card Called Party Numbers - CNIM Ver. 1

2.2.7.a.1 Version 2 Run Mode.

For Version 2 of CNIM the run mode table above is amended to that shown in Table 8. In each case it may be seen that only one number is configured on the card at any time.

Parameter	Description	Run Mode 1	Run Mode 2	Run Mode 3
CPN1	Called Party Number 1	Mode 1 Primary	Mode 2 Primary	Mode 3 Primary
CPN2	Called Party Number 2	Not Used	Not Used	Not Used
CPN3	Called Party Number 3	Not Used	Not Used	Not Used
CPN4	Called Party Number 4	Not Used	Not Used	Not Used

Table 8 Eicon Card Called Party Numbers - CNIM Ver. 2.0

2.2.7.b Network Service Types - Including ADSL

Design Overview: See section 5.4

Each PO outlet is assigned one of thirteen Service Types, which, used in conjunction with the Call Plan, defines its connection type for each period of the day.

Service Type	Description
[1] Voice	24 hour Voice-On-Demand (VOD) connection to ISDN.
[2] Satellite	24 hour permanent (PC) connection
[3] Frame Relay	Frame Relay Fixed Connection
[4] Bronze	24 hour Metered-On-Demand (MOD) connection to establish an ISDN connection when an online transaction occurs.
[5] Silver Part Time A (Metered)	During a few defined hours, the ISDN line is kept open to a metered-fixed (MF) number. Outside these times a Metered-On-Demand (MOD) service is used, to the same metered number. The call plan specifies these times.
[6] Silver Part Time B (Metered)	As above but using different time periods as specified in the call plan.
[7] FRIACO Silver Daytime C1	During daytime hours the ISDN line is kept connected and open to an unmetered FRIACO number (FRIACO-Fixed (FF), FE=FRIACO Establish). Outside these times a Metered-On-Demand (MOD) service is used. (Circuit 1 connected). The specific hours are defined in the call plan.

FUJ00171956

[8] FRIACO Silver Daytime C2	As above but to different telephone numbers.
[9] Non FRIACO Silver Daytime	The same as (7 & 8) but in a geographic area not covered by FRIACO, hence these will be metered calls, MOD or MF for periods defined in the call plan.
[10] FRIACO 24Hr C1	The ISDN line is kept open 24 hours per day, alternating between MF and FF. (circuit 1 connected)
[11] FRIACO 24HR C2	As above but circuit 2 connected.
[12] Non FRIACO Silver 24HR	The ISDN line is kept open 24 hours per day using MF but in a geographic area not covered by FRIACO.
[13] ADSL	24 hour ADSL connection.
[14] ADSL with GSM	24 hour ADSL connection with GSM backup

Table 9 Network Service Types including Branch Resilient Network Types

The Service Type selected for each PO outlet is determined by the availability of connections (due to geography) and quantity/frequency of information that will need to be passed to/from the datacentre.

2.2.7.c Call Plan

Design Overview: See section 5.6

The Call Plan specifies the connection type required for each Network Service Type for a particular time of day.

2.2.7.c.1 Call Plan Input

The Call Plan will be supplied as a simple text file containing one table for each Network Service Type. See Appendix A1 for an example.

Each table will contain a set of days which in turn contain a set of elements with one element covering a certain period of the day. Each element contains the connection type required for each time of day.

CNIM will give an error if the required element is not present.

2.2.7.c.2 Call Plan Data Output

CNIM will extract the required table from the Call Plan as specified by the outlet type. CNIM will write this table to a separate file so that a data check may be made manually.

This file will be written to the CNIM directory and named CP_Out.txt.

2.2.7.c.3 Call Plan Connection Configuration

At the start of each Call Plan period CNIM will ensure that the Eicon card is configured with the correct parameters for the current connection type.

2.2.7.c.4 Call Plan File

The network call plan file (Call Plan) is a generic file in that the same file is distributed to all Outlets (see example in Appendix A). It has the following naming convention:

CALL_PLAN _<yyyymmdd>_<hh-mm>**.new**

With the issue of a new Call Plan the previous is renamed by CNIM with the extension **.old**

FUJ00171956

The Call Plan defines the connection type for each Service Type, by listing the day and time period for each method of connection (i.e. Metered-Fixed, MF; Voice-On-Demand, VOD etc). Each method of connection has a different cost associated to it. By having twelve different Service Types to assign to the PO outlets, the allocation of connection resources is made cost-effective.

The Call Plan lists these Service Types, specifying the method of connection, which will occur for a particular day of the week and time period. In the example below the Service Type is [9] Non FRIACO Silver Daytime and its Connection Type for Monday between 00:00 and 08:00 is Metered-On-Demand (MOD):

```
...
[9]
;Non FRIACO Silver Daytime
DefaultConnType = MOD

Day=     Monday
Period=  00:00-08:00,     08:00-17:30,     17:30-24:00
ConnType=      MOD,             MF,              MOD

Day=     Tuesday
Period=  00:00-08:00,     08:00-17:30,     17:30-24:00
ConnType=      MOD,             MF,              MOD

...
```

Note that as from BNR at S92 additional service types that will incorporate GSM backup, these will have the names MFG, MODG etc.

2.2.7.c.5 Randomisation of Connection and Disconnection

The initial connection time and shutdown of a connection specified in the Call Plan is not exact. It has to be randomised over ±15 minutes of the times listed to prevent the outlets from attempting to connect or trying to drop connections to the data centre at once. The exact offset to be used is set up in Registry : [HKEY_LOCAL_MACHINE\SOFTWARE\ICL\Pathway Configuration\CNIM\Live]:

Name	Offset	Description
OFFSET_FE_FF	"-15"	Maximum offset of boundary in minutes between FRIACO-Establish and FRIACO-Fixed.
OFFSET_FE_MOD	"10"	Maximum offset of boundary in minutes between FRIACO-Establish and Metered-On-Demand. **In version 2 this has been reduced to 10 minutes from 15 minutes.**
OFFSET_FF_MF	"15"	Maximum offset of boundary in minutes between FRIACO-Fixed and Metered-Fixed.
OFFSET_FF_MOD	"10"	Maximum offset of boundary in minutes between FRIACO-Fixed and Metered-On-Demand. **In version 2 this has been reduced to 10 minutes from 15 minutes.**
OFFSET_MF_FF	"-15"	Maximum offset of boundary in minutes between Metered-Fixed and FRIACO-Fixed.
OFFSET_MF_MOD	"10"	Maximum offset of boundary in minutes between Metered-Fixed and Metered-On-Demand.

FUJ00171956

		In version 2 this has been reduced to 10 minutes from 15 minutes.
OFFSET_MOD_FE	"15"	Maximum offset of boundary in minutes between Metered-Fixed and FRIACO-Fixed.
OFFSET_MOD_MF	"-15"	Maximum offset of boundary in minutes between Metered-On-Demand and Metered-Fixed.

Table 10 Call Plan Offsets – ISDN/Data/FRIACO

The offset values above are then used within CCallPlan class for each type of connection change to calculate the random point at which the connection will change. For example when changing from Metered-On-Demand to Metered-Fixed, the appropriate Registry item, in this case OFFSET_MOD_MF, is read which is "-15". The function GlobGetRandomVal takes 0 as it minimum value and –15 as the maximum value and generates a random number between the two. The number is then added to the change-over time defined in the Call Plan.

2.2.7.c.5.1 ADSL Offsets

Name	Offset	Description
OFFSET_AE_AF	"-10"	Maximum offset of boundary in minutes between ADSL-Establish and ADSL-Fixed.
OFFSET_AF_AE	"10"	Maximum offset of boundary in minutes between ADSL-Fixed and ADSL-Establish.
OFFSET_RIT	"160"	Maximum offset of boundary in minutes between ADSL-Establish and RIT (RAS ISDN Test)

Table 11 Call Plan Offsets - ADSL

2.2.7.d Line Test Overview

Design Overview: See section 5.12

In the event of line failure a balance must be struck between attempting to recover the situation quickly whilst not overloading the network with call attempts.

The test strategy required of CNIM needs to incorporate the following factors:

1) Method for Determining comms failure
2) Method of recovering from a network failure
3) Minimisation of call attempts during network testing and provision of a "back-off" facility in which CNIM will reduce the frequency of line testing under conditions of persistent line failure.
4) Provision of a default fail state if communication cannot be re-established immediately.
5) Provision of a "Failure Mode" status value which can be returned to the Counter Call Scheduler.

2.2.7.d.1 Determination of Communication Failure

The following methods will be used to determine if a network failure has occurred.

1) ISDN/Data Network: Examination of the Cause Code returned by the network following call closure.

FUJ00171956

2) ADSL Network: Examination of the network status written to registry by Connection Manager.
3) All Networks: Attempt to ping any well known Data Centre node (VPN Server or Correspondence Server) with which the outlet is configured to communicate.

2.2.7.d.1.1 Cause Code Description

Cause Codes are returned to the Eicon card, by the network, on call closure and are a numeric indication of the reason for the call closure. CNIM may interrogate the card to determine the last cause code received from the network.

A reference table of possible cause codes is shown in Appendix A4.

Certain cause codes are used to indicate a successful call whilst others indicate that the call closed due to a network problem.

See 5.9 for a design overview of failure code handling.

2.2.7.d.1.2 Ping Failure

Each outlet is configured to communicate with four Correspondence Servers via eight VPN servers located at either of the Data Centres. The IP addresses of the VPN servers are specified in the SGVPN.INI file found in the WinNT directory of the Gateway PC.

A complete description of the VPN solution may be found in [Ref 9].

CNIM is required to ping a configurable sequence of servers in order to determine whether it has comms to the data centre. If no server returns the ping then comms are assumed to have failed.

Pings should be spaced such as to allow the greatest chance of success and the time between pings will be configurable. The ping sequence and number of times the sequence is traversed will be configurable. Only when the full sequence has been traversed the appropriate number of times with no reply, will the test be taken as having failed.

2.2.7.d.1.3 Changes for ADSL

For ADSL the method of diagnosing network failure will switch from querying the Eicon card for a CauseCode, to using the network status values returned by Connection Manager. CNIM will retain the option to query ADSL Diagnostic Monitor for more low level status information from the Conexant ADSL modem.

2.2.7.d.2 Run Mode Description

For the purposes of comms testing CNIM is considered to run in one of three modes, namely Modes 1, 2 or 3. These modes are used to logically link the degree of communication failure with the phone numbers available to CNIM. For a detailed description of Run Mode see section 5.13.1.

2.2.7.d.3 Failure Mode Description

Failure mode is also known as the Connection Status and will vary from Connected/ Disconnected to First Failure, Temporary Failure and Permanent Failure.

For a detailed description of Failure Mode see Table 106.

FUJ00171956

2.2.7.d.4 Test Requirements

1) On service startup CNIM will attempt to configure the Eicon Card with a working number.
2) During Nailed Up periods CNIM will use each Keep Alive ping reply to determine that comms are available.
3) During non Nailed Up periods CNIM may, depending on connection type, do a Line Test each time the line is brought up by an external means such as Riposte sending data.
4) Should CNIM detect that any ping test has failed it will enter a test mode as described in the test sequence diagrams below. See section 2.2.7.d.4.2

2.2.7.d.4.1 Wait Times for Call Closure

During line testing or at the start of a new call plan period, CNIM will be required to reconfigure the Eicon card. If the line is active at this point then CNIM is required to wait for a specified period. If the line becomes inactive during that time then CNIM will be notified and will reconfigure the card. At the end of that time period CNIM will reconfigure the card in any event. The wait time is dependent on the connection type that was in use when the call started and there are three types of connection to consider.

1) Establish period for silver nominated Outlets, prior to fixed period.
2) Fixed period for silver nominated Outlets, where the Outlet maintains connection with the Data Centre for the specified time period (as per Call Plan).
3) Dialled period for Silver and Bronze Outlets during "Dial on Demand".

If a call is in progress there is a wait of 'n' seconds for the call to close, as per Table 12. If the call is still in progress after the specified period, then the call is dropped. On the dialled period entry in the table, a period of 2 hours is specified to allow for any software distribution that may be in progress.

Connection Type	Mode 3	Mode 1, Mode 2
MOD, VOD	60 seconds	2 hours
FF, MF	120 seconds	60 seconds
FE	120 Seconds	60 seconds

Table 12 Wait times for call closures

2.2.7.d.4.2 Behaviour on Failure - Version 2

CNIM has three sets of telephone numbers, it uses; Primary, Secondary, and Tertiary Numbers. In Primary and Secondary Network banking is allowed, whereas in Tertiary it is not. Primary mode is normal running, secondary mode is fall back telephone phone number, and is temporary. If in secondary mode after a period of time, CNIM will retry the primary mode.

The behaviour is detailed in the three flowcharts, where

Figure 3 – FRIACO Establish Period

Figure 4 – Fixed Period

Figure 5 – Dialled Period

FUJ00171956

CNIM will require test sequences for Voice on Demand (ISDN) outlets and Satellite outlets. In addition sequences will be required for Dial Back periods and for doing the "Normal" test. In effect every step of the CNIM test behaviour is controlled. Because of this every permutation of test sequence must be designed and tested.

Test – Ping the VPN servers using the number currently set in the Eicon card.

Call Okay – No ISDN failure code and “ping” process okay.

Call Fail – An ISDN failure code or “ping” process failure

All the parameters are held in Registry, so they can be modified if necessary at a later date.

On the “Period” flow diagrams each box is numbered, i.e. on the “Establish Period” diagram the boxes are numbered E1 to E13, “Fixed Period” diagram F1 to F13, and on the “Dialled Period” diagram D1 to D15. Tracing will be used to monitor the paths through the routines by capturing these box number sequences. This will be of particular importance during the testing phase where routes will be defined (via expected box sequence numbers), through the routines, thus ensuring all paths are exercised and proven. In addition the trace file will contain which “ping” in the sequence has worked, in order to give some indication as to the quality of the network at the time. An extra field will be added to the monitor record, which records the time taken for the ping. This will give us an indication as to which ping reached the destination, i.e. if the Energis CVX switched from the primary LNS to the associated secondary LNS router, this will have taken longer.

It should be noted that additional detail is required, over and above that shown in the following diagrams. The additional steps are given in the section describing the CNIM Programming Language (CPL) operations for each test sequence, later in this document. These diagrams will be updated to reflect the additional step.

FUJ00171956

2.2.7.d.4.3 Testing During Establish Periods

Figure 3 shows the test sequence required on entry to a FRIACO Establish period.

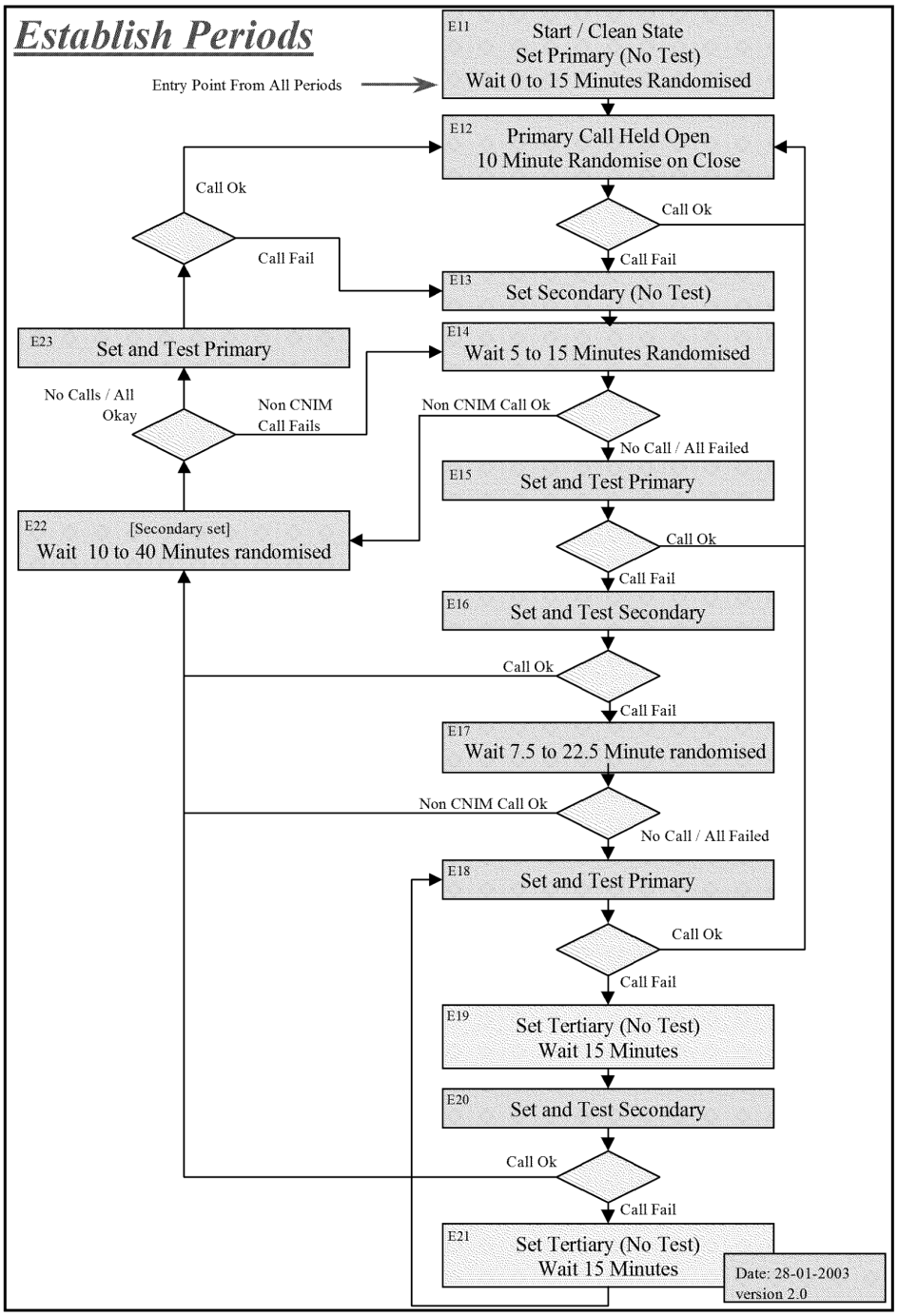

Figure 3 Testing During FRIACO Establish

FUJ00171956

2.2.7.d.4.4 Testing During Fixed Periods

Figure 4 shows the test sequence required on entry to a FRIACO Fixed or Metered Fixed period.

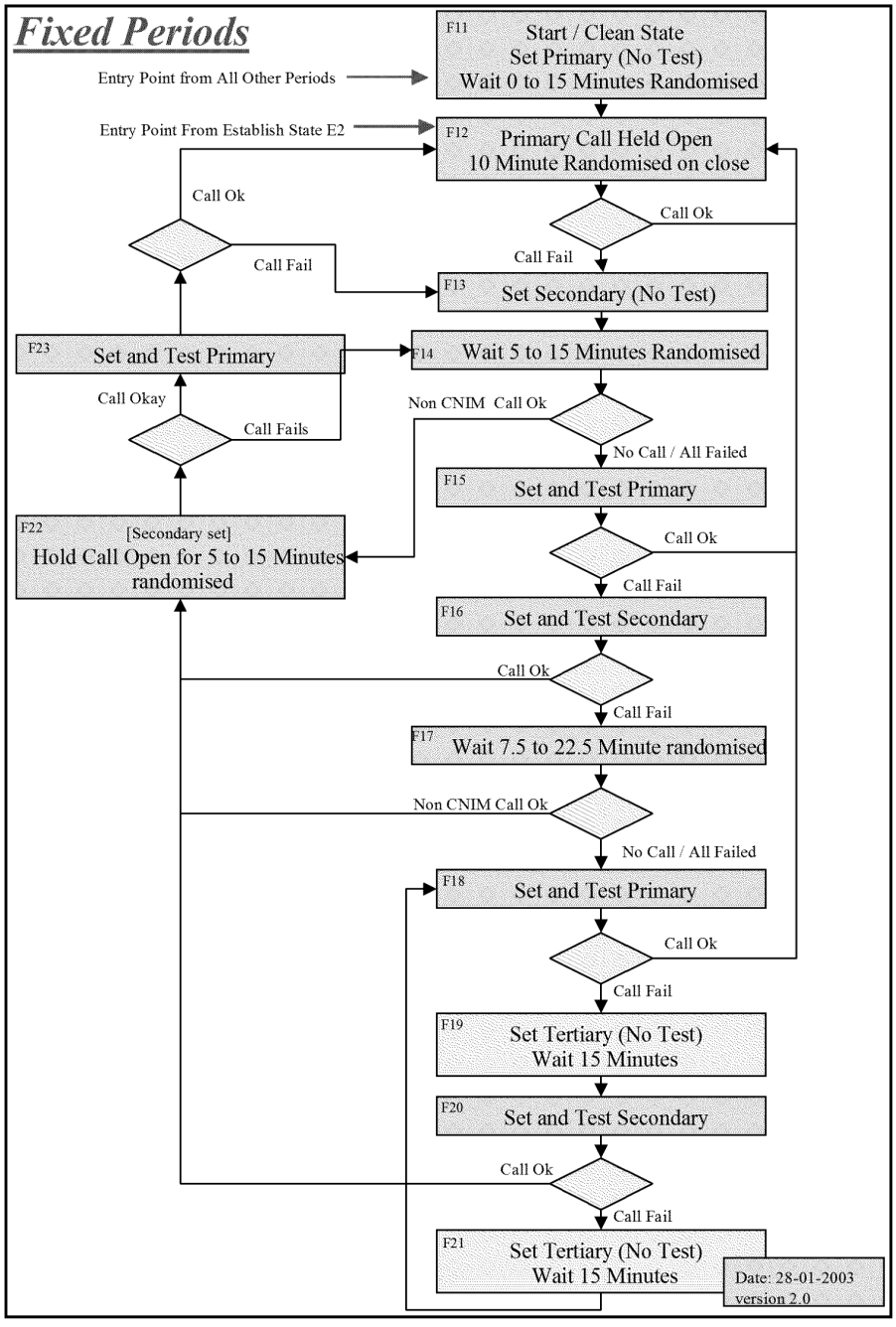

Figure 4 Testing During Fixed Periods

FUJ00171956

2.2.7.d.4.5 Testing During Dialled Periods

The following diagram applies to Metered Dialled, DialAround and Voice on Demand periods.

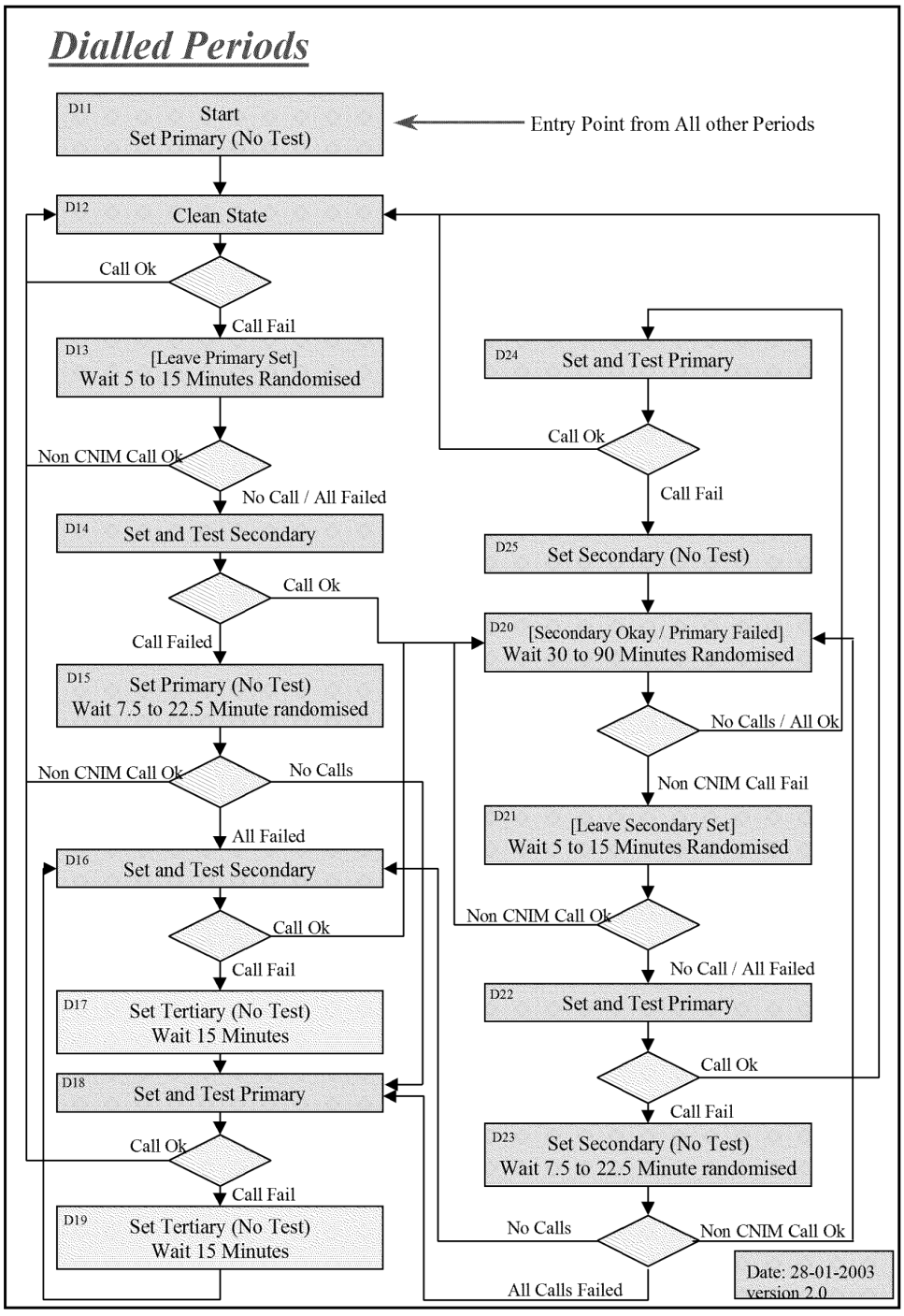

Figure 5 Testing During Dialled Period

Measurement of call success differs between dialled data calls and dialled voice calls.

FUJ00171956

During the quiescent states, such as D3, a phone number is set on the Eicon card but not proactively tested. When the line is activated by some external application such as Riposte then CNIM must determine if the call succeeded. In the case of a metered or dialaround call this is done by pinging one or more VPN servers and waiting for a response. In the case of an ISDN call the cause code returned at call closure is used as the measure of call success.

2.2.7.d.4.6 Test Sequence –VSAT - Permanent Connection

The Permanent Connection type applies only to Satellite outlets. CNIM will do a test ping every 15 minutes. The response to the test ping determines whether a call is considered to be open or closed.

If the PASS/FAIL flag is set to fail then the current call is recorded as closed with a FAIL closure marker. CNIM will continue to ping at 15 minute intervals. If a ping succeeds and the current call state is closed then a monitor record is opened to indicate the start of a new call.

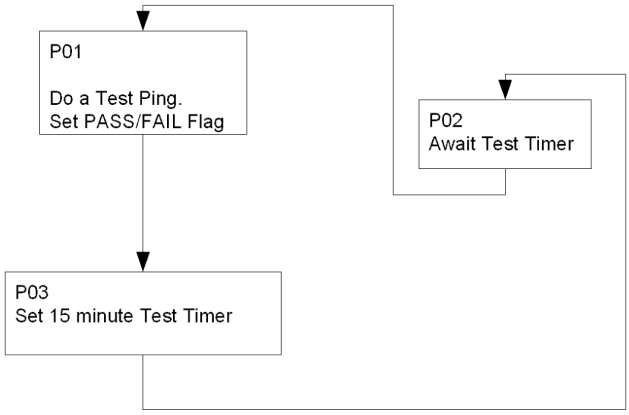

Figure 6 Test Sequence - VSAT

2.2.7.d.4.7 Test Sequence - ADSL

The ADSL Establish and ADSL Fixed connection types are tested using the same test sequence, shown below.

Test failure occurs when all the pings in the test ping sequence fail to produce a response.

If ping failure occurs during bandwidth testing then CNIM will move to a test ping sequence which will initiate the permanent failure timer should all pings fail.

FUJ00171956

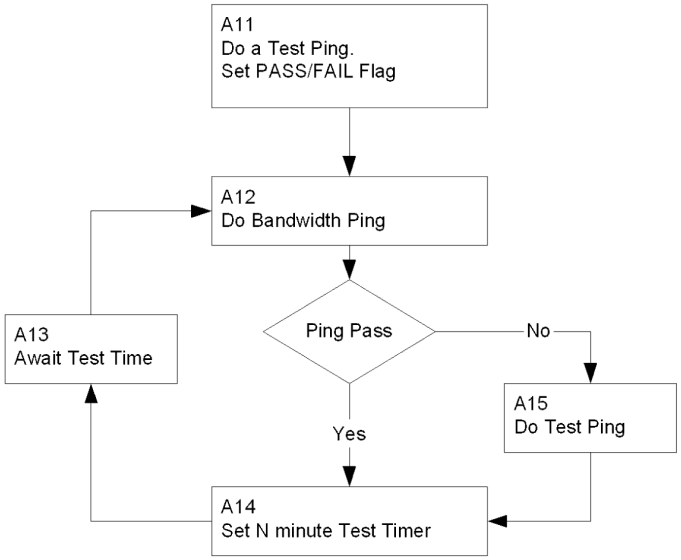

Figure 7 Test Sequence - ADSL

FUJ00171956

2.2.7.d.1.8 Failure Flag State

In addition to the "Period" flow diagrams there are triggers, which initiate the processes, this is best illustrated by Figure 8, where the "Fail Flag" is indicating OK, Temporary Fail or Permanent Fail, dependent on where it is within the cycle. The process is triggered by Timer Events. As a function of the failure flag state mechanism CNIM updates the Counter Call Scheduler (CCS) on transition between states. The CCS update refreshes the cause code information with the latest returned from the Eicon card. In the absence of an Eicon cause code, CNIM will substitute its own defined code (i.e. ping failure).

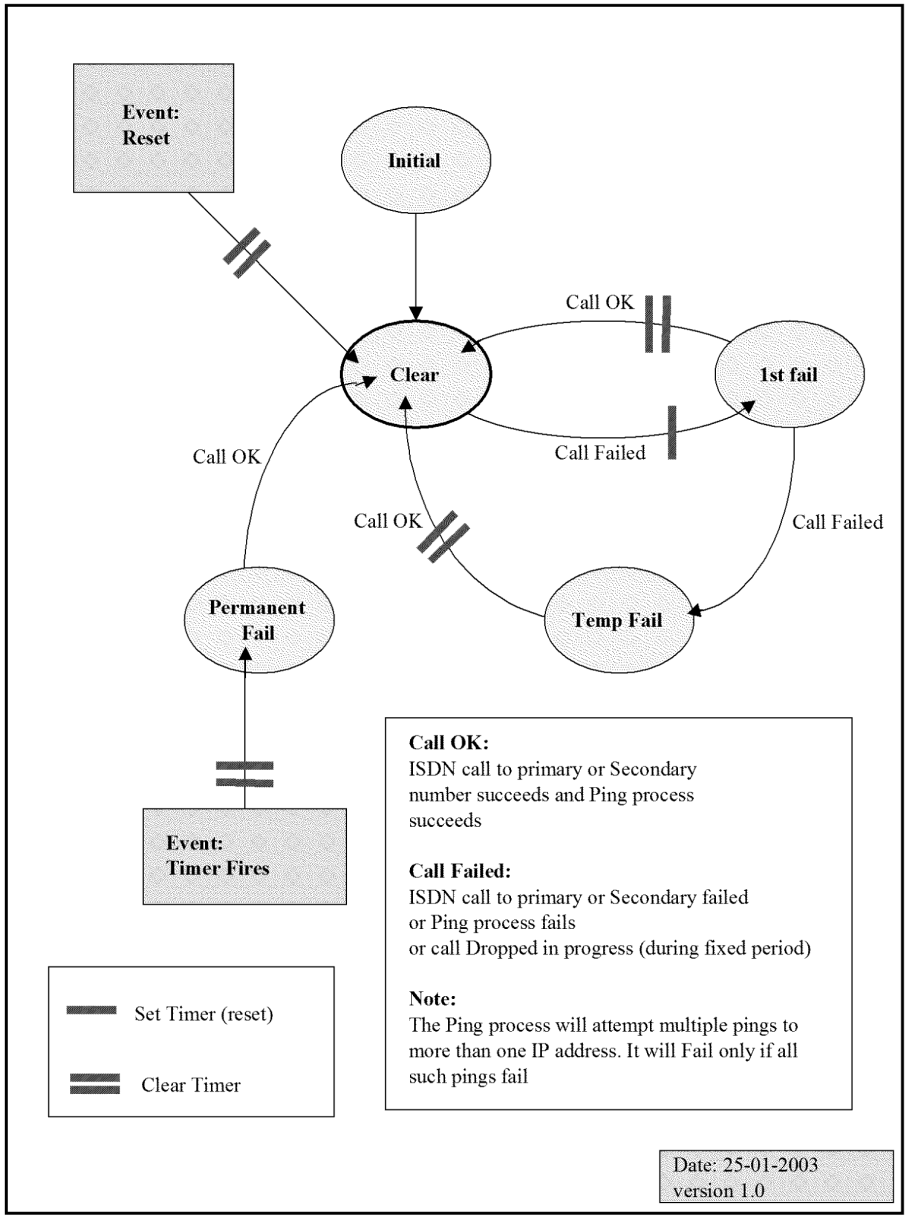

Figure 8 Fail Flag State Mechanism

FUJ00171956

2.2.7.e Line Connectivity

Under present (Pre BI3) operation the ISDN connection between the outlet Gateway and the Data Centre will drop, once data has ceased to flow, due to timeouts configured within the Eicon card on the Gateway PC.

Post BI3, Pathway is required to satisfy the service level agreements required for Network Banking. In particular the speed at which banking transactions can be processed is of importance. Therefore at certain times of day and for certain outlets, CNIM must eliminate the call setup time for each transaction and this will be done by keeping the line active.

Not all outlets require this degree of connectivity and so each outlet will be assigned a Network Service Type (NST). The NST defines the overall level of connectivity for the outlet and is held as one of a number of Tables within the generic Call Plan. The Call Plan, which is supplied to all outlets, defines the types of connectivity required for all Service Types throughout the day.

The types of connectivity to be made available by CNIM are defined in Table 13.

Name	Short Name	Network Type	Connection Type
Permanent Connection	PC	Satellite	Continuous
Voice On Demand	VOD	ISDN	Discontinuous
Voice On Demand (GSM)	VODG	ISDN with GSM backup	Discontinuous
Metered On Demand	MOD	Data	Discontinuous
Metered On Demand (GSM)	MODG	Data with GSM backup	Discontinuous
Metered Fixed	MF	Data	Continuous
Metered Fixed	MFG	Data with GSM backup	Continuous
FRIACO Establish	FE	FRIACO	Continuous if possible
FRIACO Fixed	FF	FRIACO	Continuous
FRIACO Fixed(GSM)	FFG	FRIACO with GSM backup	Continuous
ADSL Establish	RA	ADSL	Continuous
ADSL Fixed(GSM)	RAG	ADSL with GSM backup	Continuous
ADSL Fixed(ISDN + GSM)	RAIG	ADSL with ISDN and GSM backup	Continuous
ISDN Test	RIT	Test of ISDN backup	Continuous
Frame Relay	FRE	Frame Relay Establish	Continuous
Frame Relay	FRF	Frame Relay Fixed	Continuous

FUJ00171956

Table 13 Connection Types

2.2.8 CDF Data Storage Requirement

Design Overview: See section 5.5

CDF requirements are explained in [Ref 8] and repeated below:

2.2.8.a CDF Content

The CDF (CommsData File) is produced for ISDN Gateway PCs only. The primary content is to deliver the ISDN access numbers to the CNIM and additionally deliver the CHAP usernames and optional ISDN line parameters for installation by EiconConfig. Its content is as follows:

```
; Pathway CDF
;
; FAD:          <fad_id>
; Node:         <n>
; Date:         Aug 5 1999 11:29AM.
; ACDB:         <x.y.z>

[Version]
Signature="$Windows NT$"

[DefaultInstall]
AddReg=NCfg

[FileFormat]
Type=CDF

[NCfg]
HKLM,%NI%,VP,,<primary_isdn_rtr_phone_no>
HKLM,%NI%,VS,,<secondary_ isdn_rtr_phone_no>
HKLM,%NI%,VT,,<tertiary_ isdn_rtr_phone_no>
HKLM,%NI%,FC1P,,<C1_Primary Friaco_no >
HKLM,%NI%,FC2P,,<C2_Primary Friaco_no>
HKLM,%NI%,FC1S,,<C1_SecondaryFriaco_no>
HKLM,%NI%,FC2S,,<C2_Secondary Friaco_no>
HKLM,%NI%,MP,,<Primary Metered_no>
HKLM,%NI%,MS,,<Secondary Metered_no>
HKLM,%NI%,DP,,<Primary Metered Dial-around_no>
HKLM,%NI%,DS,,<Secondary Metered Dial-around_no>

[EICON_config]
In_mUid="%UID1%","%UID2%","%UID3%"
Out_Uid=<own_isdn_chap_name>
CLIlist=                                                    Optional
MSN=                                                        Optional
DSAlist=                                                    Optional
SUB=                                                        Optional

[Strings]
NI=SOFTWARE\ICL\Pathway Configuration\Eicon
UID1=<primary_rtr_chap_name >
UID2=<secondary_rtr_chap_name>
UID3=<tertiary_rtr_chap_name>
```

Note that the registry key pathname for the storage of the data values is set to:

HKLM, "SOFTWARE\ICL\Pathway Configuration\Eicon"

FUJ00171956

2.2.8.b CDF - Network Configuration (for CNIM access numbers)

The Network Configuration section [Ncfg] above, is set up to meet the delivery requirements for the Data Centre Router Access numbers to be dialled by the Eicon ISDN card under the control of the CNIM.

For Mobile outlets, all Data Network numbers (FP*n*, FS*n*, MP, MS, DP and DS) will be null.

The Primary, Secondary and Tertiary numbers will be no different from the values used prior to BI3. Hull outlets use 0800 backup numbers over the Voice network.

Number Type	Description
VP	Voice Primary
VS	Voice Secondary
VT	Voice Tertiary
MP	Metered Primary
MS	Metered Secondary
DP	Dial Around Primary
DS	Dial Around Secondary
FC1P	FRIACO Primary (Geographical Area 1)
FC1S	FRIACO Secondary (Geographical Area 1)
FC2P	FRIACO Primary (Geographical Area2)
FC2S	FRIACO Secondary (Geographical Area 2)

Table 14 Number Types and Descriptions

2.2.8.c Phone Number Mapping

Phone numbers from the table above are mapped onto the Eicon card depending on the connection type required.

For a detailed description see section 5.13.1.

2.2.9 Call Logging Requirement

Design Overview: See section 5.7

2.2.9.a Monitor Record

The CNIM Call Monitor record is specified in [NB_SOD] - see [Ref 3], which defines the Quality of Service reporting requirements. The CNIM Call Monitor receives information from the Eicon ISDN Driver Interface (IDI) when an event occurs. The events that are monitored are defined in the CNIM initialisation process. The events monitored relate to calls to and from the Data Centres and the status of these events. Information relating to each call initiated at the Outlet or received from the Data Centre is recorded in either 'In-Files' or 'Out-Files'. These daily files are generated for each connection type that the Outlet may invoke. Thus if an Outlet is deemed to be a silver Outlet, files will be generated for the FRIACO telephone number, the Dial-around telephone number, (metered call number). Within these files each individual record relates to a single call whether received or sent. Each record when complete provides the

FUJ00171956

history of that call. New files are created each day, with the extension of **.new** and files from the previous day are renamed with an extension of **.old**

Note that CNIM will only generate monitor files for the current day, regardless of the call state on service startup.

2.2.9.a.1 Record Format and Description

The monitor record will include the following information:

- Date of call
- Start time of call
- End time of call
- Length of call
- Direction of call (IN/ OUT)
- Phone number dialed
- Network Service Type
- Call status (SUCCESS/ FAIL/ OPEN/ UNKNOWN)
- Ping Roundtrip Time
- Failure code

2.2.9.a.1.1 Monitor Record Format - CNIM Version 2

The information held in the monitor record is designed to capture call information at ISDN based outlets. There are around 250 Satellite outlets that must also be included within network quality of service reporting. The low volume of outlets does not justify developing a separate record structure; therefore information gathered at Satellite outlets will be massaged into the above structure. The CNIM will write a monitor record if it determines a Satellite connection has failed. This record will record the call as having failed and will include a failure code specific to satellite outlets, i.e. not one of the cause codes that can be returned by a network supplier.

In the situation where a 'call' can be permanently connected, for example at satellite and 24 hour outlets, the CNIM will write a closure record shortly after midnight, ensuring a record of all calls made within a day are included in reports returned to data centre within a reasonable timeframe.

2.2.9.a.1.2 Monitor Record Format - CNIM Version 3

Details of the change in Monitor File format are given in section 2.2.9.a.5.

2.2.9.a.2 Initial Record Format

When a record is first created certain data will be unavailable such as call duration and the Call Status value. A record of the format shown below will be created.

28/10/2002, 15:24:55:853, 00:00:00:000, 0000000000, OUT, 01344868735, 07, DP, OPEN, 0000

It may be seen that the end time and duration are set to null whilst the Call Status is set to OPEN. The cause code is set to our own code of 0000.

2.2.9.a.3 Final Record Format

FUJ00171956

When the call is closed a record of the format shown below, will be produced.

28/10/2002, 15:24:55:853, 15:24:59:853, 0000004000, OUT, 01344868735, 07, DP, SUCCESS, 00

The end time, duration and Success/Fail details are added.

However it is possible that CNIM will not receive an indication that the call has closed, either due to a failure of the IDI interface or if the CNIM service is stopped and restarted. In these cases it is important that any OPEN record is changed to have the success code UNKNOWN (Code 0x0100, appearing in the monitor record as 0100). This will allow the CASNetworkQOS application to correctly parse the file.

If CNIM crashes during a call and is not restarted until the next day then that last call will be left as OPEN. If a call is left as OPEN over midnight then there should be a corresponding record in the next days monitor file when the call was closed. If this corresponding record in the next file does not exist, then the call must have failed and must be changed to UNKNOWN in the previous file. The next day's record will not be written until the previous days file has been renamed. At service startup if a file exists as .new from a previous day, then none of its records should be OPEN. Any OPEN records should be changed to UNKNOWN.

Also at service start up and assuming the service has previously been run that day, then looking in today's NEW file, none of its records should be OPEN either.

Therefore on service startup any .new monitor files should have any OPEN records changed to UNKNOWN and the files then renamed to .old as appropriate.

2.2.9.a.4 Changes for Version 2

An extra field will be added to the monitor record, which records the time taken for the ping. This will give us an indication as to which ping reached the destination, i.e. if the Energis CVX switched from the primary LNS to the associated secondary LNS router, this will have taken longer.

2.2.9.a.5 Monitor Record Format for ADSL

The following details are taken from [Ref 14]

1) There is no concept of an inbound call (call initiated from the data centre) with an ADSL network; therefore all calls will be recorded as out-bound.
2) The length of the call measured in milliseconds – where a connection is not successful this field will contain a zero value. Due to the naturally long calls expected at ADSL outlets the length of call field will record only the time that the call was open on the day indicated in the filename. Where a call crosses many days a record for the call will be included in each call monitor file that the call was open for. In each record the length of call field will record just the time the call was open within the day. Note this change will apply to all network service types.
3) Dialled number will be the RAS phone book entry used for the call.
4) An error code indicating the reason why the call failed, or zero if the call was successful. Within this code is should possible to identify those calls which failed to connect as opposed to those calls where connection is successful however the call dropped at some point later. Only those calls deliberately closed, closed due to gateway shutdown, or closed at midnight will be recorded with a zero success code.

FUJ00171956

5) CNIM will use its registry interface with Connection Manager to determine the connection state and reason for failure.
6) At midnight when CNIM switches to a new monitor file it will not close a call record, rather leave the last call record indicating the call is open, with the start date /time, and length of call field set to record the milliseconds the call was open on that day. The 1st entry in the new summary file will be a copy of the last record in the file just closed (initially with the length of call field blank, to be populated once the call is closed or at midnight) – this will maintain the call start date / time. When the call does close the last file will have a complete record of the call start / stop time. The duration will include the length of time the call was open today.
7) At midnight when CNIM switches to a new monitor file it will not close a call record, rather leave the last call record indicating the call is open, with the start date /time, and length of call field set to record the milliseconds the call was open on that day. The 1st entry in the new monitor file will be a copy of the last record in the file just closed (initially with the length of call field blank, to be populated once the call is closed or at midnight) – this will maintain the call start date / time. When the call does close the last file will have a complete record of the call start / stop time. The duration will include the length of time the call was open today.

Field	ADSL?	Meaning
Date of call	Yes	
Start time of call	Yes	In normal circumstances this will be artificially set to 00:00. ADSL call will normally be always connected, in order to provide daily feedback on the availability of the ADSL network CNIM will close the call record at midnight and reopen a new one.
End time of call	Yes	In normal circumstances this will be artificially set to 00:00. ADSL call will normally be always connected, in order to provide daily feedback on the availability of the ADSL network CNIM will close the call record at midnight and reopen a new one.
Length of call	Yes	The length of the call in milliseconds for that day. Where a call spans midnight each part of the call is recorded in a record for that day.
Direction of call	No	There is no concept of an inbound call (call from the data centre) with an ADSL network; therefore all calls will be recorded as out-bound.
Called number	Yes	ADSL has no concept of a called number, however it does have a data centre specific user/domain name used to login to the radius servers. The

FUJ00171956

		called number field will record the RAS phonebook entry.
Network Service type	Yes	Set to the service type for ADSL which is 13 or 14.
Network connection type	Yes	All ADSL calls will have a connection type of ADSL.
Call status (success / fail / reject)	Yes	Reject calls are only applicable to inbound calls which are not possible on an ADSL network. The call status will be either success or fail.
Failure code	Yes	An error code indicating the reason why the call failed, or zero if the call was successful. Within this code is should possible to identify those calls which failed to connect as opposed to those calls where connection is successful however the call dropped at some point later. Only those calls deliberately closed, closed due to gateway shutdown, or closed at midnight will be recorded with a zero success code.

Table 15 Monitor Record Format for ADSL

Note that the final field of "Ping Return Time", incorporated for CNIM 2, has been removed from the monitor record.

2.2.9.a.6 Monitor Record Format for ISDN and GSM over RAS

The Branch Resilient Network requires that calls may be made over ISDN or GSM during network failure. RAS ISDN calls may be made from an ADSL outlet whilst RAS GSM calls may be made from an ADSL or ISDN outlet.

These calls would be made using RAS and the appropriate phonebook entry.

The table below shows the monitor file format for these calls.

Direction of call	No	Inbound calls will not be allowed when using RAS, therefore all calls will be recorded as out-bound.
Called number	Yes	RAS has no concept of a called number, however it does have a data centre specific user/domain name used to login to the radius servers. The called number field will record the phonebook entry.
Network Service type	Yes	Set to the service type for that outlet.
Network connection type	Yes	All RAS ISDN calls will have a connection type of ISDN. All RAS GSM calls will have a connection type of GSM.

Table 16 Monitor Record Format for ISDN and GSM

FUJ00171956

2.2.9.a.7 File Name Format

The file names have the following naming convention, where the <fad code> is the six digit unique Outlet identifier, and <ct> is the connection type as defined in the CDF, which will be one of the following VP, VS, VT, FC1P, FC2P, FC1S, FC2S, MP, MS, DP, or DS.

From CNIM 3 onwards, the connection type will include the types ADSL for normal ADSL running and MODM when running using the PSTN modem at Day D. For more detail on DayD operation see [Ref 15].

At CNIM 4 for Branch Resilient Network operation the connection types will include the types ISDN for ISDN over RAS and GSM for GSM over RAS.

QOS_MON_I_<fad code>_<yyyymmdd>_<ct>.new (In-bound files)

Or

QOS_MON_O_<fad code>_<yyyymmdd>_<ct>.new (Out-bound files)

2.2.9.a.8 Monitor File Creation and Renaming

A monitor file will be created when a connection of a particular type is first made. Thereafter the same file will be used for all connections of that type, until midnight (GMT) when the file will be renamed to <FILENAME>.old.

2.2.9.a.9 Call Monitoring for Satellite connected Outlets

In the case of satellite connected outlets, CNIM will still be in operation, however the information in the file, will in the majority of cases, be a single record, unless the satellite connection is lost for any reason. The reason for satellite connection fails is not easily determined without analysis of the Personal Earth Station (PES), which is beyond the scope of CNIM. If the satellite connection fails the current record closed with a fail entry in the Call Status field. On the link being re-established a new record will be appended to the file. If at Midnight the current record is still open then this will be closed as a successful record.

2.2.9.a.10 Call Monitoring for ADSL connected Outlets

On ADSL outlets CNIM will carry out regular bandwidth pings to determine current bandwidth. Failure of the bandwidth ping will trigger a sequence of test pings which may trigger use of the permanent failure timer if all pings fail.

CNIM will receive notification from Connection Manager as to changes in line state and will use this information to update monitor records as appropriate.

2.2.9.b Summary Record

This requirement is specified in [NB_SOD].

This record provides a summary of the network quality of service achieved during a defined period of the day. The record will include the following information:

- Start date / time in UTC time of QOS period;
- Length of time covered in seconds;

FUJ00171956

- The defined Service type for the outlet (one of those listed in TD/SOD/006);
- FRIACO seconds connected (zero for non FRIACO outlets);
- Metered seconds connected;
- Number of metered calls made;

The primary purpose of the QOS record is to, for FRIACO connected outlets, input into a centrally generated report recording the levels of congestion the network is subject to. In situations where FRIACO congestion exceeds a defined value on a particular day that's days service availability is removed from any penalty calculations. Only those hours within the core POCL day should be included therefore the QOS record will include the hours of 8 am until 5:30 PM on weekdays and 8 am until 13:00 on Saturday. On Sunday no FRIACO network is available therefore a zero value record will be written:

Start Date	Start Time	Total Time	Defined Service Type	FRIACO Time	Metered Time	Metered Call Count
dd/mm/yyyy	24hr	Seconds	01 - 12	Seconds	Seconds	No. of metered calls

Table 17 Format of Summary Record

Where:

Start Date - is the start date of the monitoring of the form dd/mm/yyyy

Start Time - is the start time of the monitoring of the form hh:mm:ss

Total Time - is the total FRIACO Fixed time if the Call Plan includes FRIACO Fixed for that day. If no FRIACO Fixed is used that day then Metered Fixed time is used if available. If neither Metered Fixed nor FRIACO Fixed is available then the total length of the day is given.

Defined Service Type - indicates the Network Service Type as per table.

FUJ00171956

Network Service Type	
Value	Meaning
01	Voice (mobile)
02	Satellite
03	Frame Relay
04	Bronze (Metered dial on demand)
05	Metered 'nailed-up' (Silver part time **A**)
06	Metered 'nailed-up' (Silver part time **B**)
07	FRIACO 'nailed-up' (Silver Daytime) (**C1**)
08	FRIACO 'nailed-up' (Silver Daytime) (**C2**)
09	Non-FRIACO (Metered) 'nailed-up' (Silver Daytime)
10	FRIACO 24hour (Silver) (**C1**)
11	FRIACO 24hour (Silver) (**C2**)
12	Non-FRIACO (Metered) 24hour (Silver)
13	ADSL
14	ADSL with ISDN automatic backup (S92 BNR)

FRIACO Time - is the total connected time in seconds during the 'nailed up' period for FRIACO.

Metered Time - is the total connected time in seconds during the 'nailed up' period for Metered access when the FRIACO service has failed for whatever reason, otherwise zero.

Metered Call Count - is the number of metered calls made during the 'nailed up' period when the FRIACO service has failed for whatever reason, otherwise zero.

For example:

24/10/2001, 14:23:56:382, 1523672, 7, 987654, 536018, 3

Notes:

- Fields are separated by ,space
- File are created with an extension of **.new**
- Riposte Nail Up occurs when the connection type is FRIACO Fixed, Metered Fixed, Permanent Connection or ADSL Fixed and no ping failure has occurred.

File from previous day are renamed with an extension **.old**

The QOS record will also be written at outlets that do not make use of the FRIACO network. Outlets which do not used the FRIACO network will write a QOS record to cover any period where the ISDN line is nailed up, or in the case where there is no nail up period then the whole

FUJ00171956

day will be recorded in the QOS record. Outlets that do not use the FRIACO network will write a zero value in the FRIACO seconds connected field.

The Time Covered field will be the length of time of the FRIACO fixed or Metered-Fixed Period. If no such period exists for that day then the whole day will be included in this time, i.e. 24 * 60 * 60 seconds.

For service types 10 and 11, which include MF and FF periods, the primary purpose of the summary records is to record FRIACO congestion, therefore CNIM should only include FF period for these records.

2.2.9.b.1 Summary Files for ADSL

These requirements are taken from [Ref 14].

The FRIACOSecs, MeteredSecs and MeteredCalls will not be included within the daily summary record for an outlet with an ADSL connection type. New field types will be used which will specify the time periods for which Riposte is expected to be nailed up:

1) Within the summary file on an ADSL outlet CNIM will just include details of the period to be covered by today's summary record, in the form of Start Time and Total Connected time.
2) The filename of this file will follow the current summary file naming convention.
3) The record format within the file will follow the format used in the current call summary file; fields not required will remain blank. Fields included are:
   - Date
   - Start Time
   - End Time
   - Service Type (13 in the case of ADSL)
4) Where the NST changes during the day CNIM will take no special action, rather attempt to construct the record using the information available.

2.2.9.b.2 Summary File Name Format

Summary file names have the following naming convention, where the <fad code> is the six digit unique Outlet identifier.

QOS_P_<fad code>_<yyyymmdd>.new

2.2.9.c Bandwidth Logging for ADSL

These requirements are taken from [Ref 14].

Detailed design is given in 5.7.3.c

Logging of connection bandwidth is only required for an ADSL connection.

1) A new file will be generated each day at midnight, with a .new suffix. The old file will be renamed with an .old suffix – CASQOS will process all .old files since the last time it executed. CASQOS will be responsible for housekeeping old files.
2) Bandwidth information required only on ADSL outlets when it is using the ADSL connection.

FUJ00171956

3) Bandwidth information will be extracted every (n) seconds
4) A registry entry is required to specify frequency of logging.
5) Bandwidth report placed in Summary folder.
6) Format will be Date, Time, Bandwidth (in Bits/second) and Failure Code as comma separated values. For instance: 24/10/03, 14:25:00:00, 200000, <failure code>
7) Bandwidth will be recorded as zero whenever the actual bandwidth cannot be determined
8) The last field in the record contains a fail code. indicating the reason for the failure
9) The following errors can occur:
   - 1st ping fails
   - 2nd ping fails
   - Both pings fail.
   - 1st ping takes longer than 2nd ping
   - Bandwidth value calculated to be higher than the maximum possible value of 512Kb/sec
10) The ping frequency and sizing information will be included as registry parameters. Also a maximum threshhold will be included. See section 4.
11) Bandwidth is measured from Ping roundtrip time.
12) One bandwidth file will be created/day
13) The bandwidth file name will be determined by whether the outlet is using the PSTN modem, in which case Connection Type will be MODM. Normally it will be ADSL.
14) The bandwidth file will have the filename:

    QOS_BNDWDTH_<fad_code>_<yyyymmdd>_<Connection Type>.new

CNIM creates and maintains a new log file which will record the bandwidth available at the outlet. The available bandwidth log will only be maintained for the new ADSL network type.

A registry item will declare the frequency this information is collected, it is anticipated it will be collected multiple times per hour.

Record format

Each line in the log file will include two comma separated fields: the timestamp when the bandwidth check was run and the available network bandwidth, in bits per second, from the gateway counter to the data centre, as below:

<date>, <time>, <bandwidth>, <fail code>

All timestamps will be recorded in UTC time. An example record is shown below:

24/10/2003, 14:25:00:00, 0000033660, 00

Filename format

The filename format will include a prefix, indicating the file contents, the fad code of the outlet, a date stamp and the network connection type (allowing for future extension) and a .new or .old suffix, i.e.

QOS_BNDWDTH_<fad code>_<yyyymmdd>_<ADSL>.new

These files will be stored in the same directory as the call summary files.

FUJ00171956

A new file will be generated each day at midnight, with a .new suffix. The old file will be renamed with an .old suffix – CASQOS will process all .old files since the last time it executed. CASQOS will be responsible for housekeeping old files.

2.2.10 Dial Back Requirement

Design Overview: See section 5.8

CNIM is required to cause the line to connect out from the outlet to the Data Centre, should it detect an incoming call whilst the line is down. Usually this would occur during a Connection Type of Metered on Demand (MOD) or Voice on Demand (VOD) - see Table 13 for a description of Connection Types.

CNIM will switch on Keep Alive for a period of 2 minutes; - see section 2.2.11 for a more detailed description of Keep Alive.

2.2.11 Keep Alive Requirement

Design Overview: See section 5.14

The Keep Alive requirement comprises two components:

1) Keep Alive during "Nailed Up" Periods.
2) Keep Alive during Dial Back - see 2.2.10

Nailed Up periods comprise those connection types for which the connection should be continuous, e.g. FRIACO Fixed, Metered Fixed and ADSL Fixed. It also comprises any time of day for a Satellite outlet.

In either case the mechanism of Keep Alive is to "ping" one or more of the VPN Servers [Ref 9], available to the outlet at either Data Centre.

The frequency of pinging will such as to maintain line connectivity whilst keeping network traffic to a minimum.

The Eicon card Shorthold Timer and MCDT values will be modified as to reduce the ping frequency required whilst not keeping the line open unduly in the event of CNIM Keep Alive being terminated. See 2.2.7.a for the timer values used.

At the conclusion of Keep Alive the card will be reconfigured.

2.2.11.a Ping Sequence

This section is part of the requirements for version 2 of CNIM.

With the “ping” process employed to maintain a connection to the Data Centre, there are three issues to be considered:

1. Ping failure – an allowance of a 1% failure rate to be made.
2. All pings can fail for 1 or 2 seconds under certain network conditions.
3. VPN session establishment can impact the ability of the ping to work.

To overcome the issues above, CNIM utilises a sequence of “pings”, “n” seconds apart in order to ascertain whether or not the call had worked. As soon as a ping succeeds, then the call is deemed to be a success and the rest of the sequence is not done. In addition, on an ISDN/FRIACO outlet, if the Eicon card reports that the call had closed before a ping had succeeded then the call is deemed to have failed. The remaining “pings” in the sequence are not done, as they would cause additional calls to be made to the Data Centre. If all the “pings” in the sequence are deemed to have failed, then the last “ping” will time-out after “n” seconds.

FUJ00171956

2.2.11.a.1 Methodology

The time between "pings" is a Registry Entry and initially will be set to 4 seconds.

1. CNIM selects 4 out of the 8 VPN servers; The VPN servers selected are the first from each of the 4 IP Subnets.
2. The order to use the 4 VPN servers is randomised on starting CNIM.
3. With each call, CNIM starts with the first VPN server on the list, "pings" the server and waits for X seconds.
4. If no response from the "ping" **and** the call is still open, CNIM "pings" the next server on the list.
5. This repeats until all 4 servers have been "pinged" **or** the call has been dropped.
6. If **no** reply, then the call is deemed to have failed.
7. On the next call, CNIM will commence with the VPN server that responded the previous time, after the ping interval timer of Y seconds.
8. For "Fixed" connections, CNIM will "ping" the VPN server that responded the previous time. If this fails, CNIM tries the other 3 VPN servers, in sequence, 4 seconds apart, prior to declaring the call dead. As with other "pings", it will check the call is up before doing each "ping".
9. This means that at most 4 "pings" are used to determine whether or not a call has failed. See Figure 9.
10. Note that "X" and "Y" seconds differ between ISDN, VSAT and ADSL outlets. The values used are set in registry in section 5.13.3.b

FUJ00171956

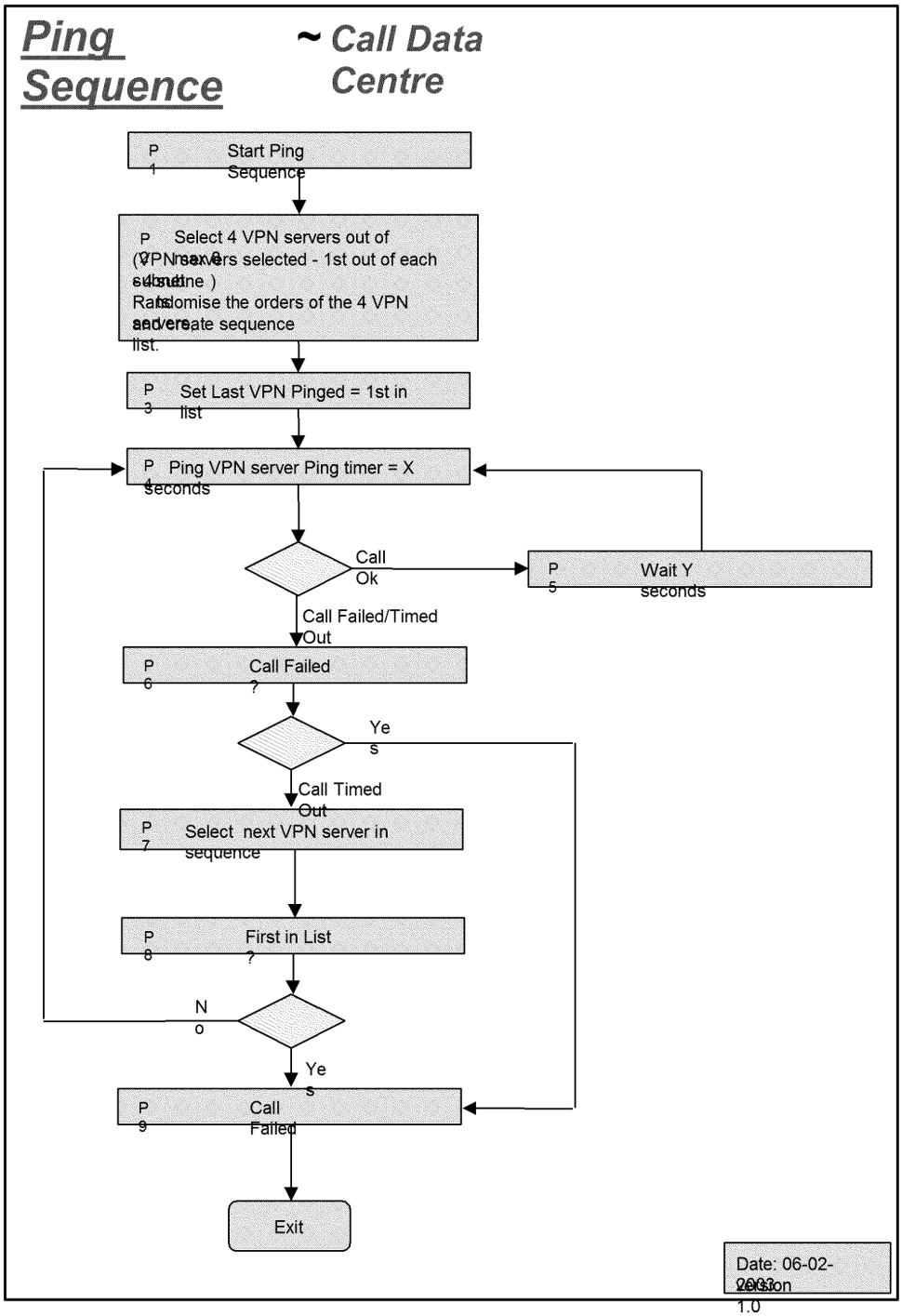

Figure 9 Ping Sequence (call to Data Centre)

2.2.12 Time Format Requirement

Design Overview: See section 5.15

FUJ00171956

CNIM will use U.T.C. throughout except in the case of the Call Plan file - see Appendix A1 where the start and end times given are considered to be in local time. This means the same Call Plan can be used throughout the year provided no call plan period ends/starts between 2 a.m. and 3 a.m. UTC on the days of the clock change. This is because 2:15 a.m. (say) local time does not exist during the Spring switch to B.S.T whilst 2:15 a.m. local time occurs twice during the Autumn switch to GMT (U.T.C.).

2.2.13 GetStatus Query Requirement

Design Overview: See section 5.16

The requirement for the GetStatus functionality is specified in [Ref 5] and [Ref 6] and is repeated below.

CNIM provides a CNIM Client DLL for use by components on the Counter that require information on the current network connection, if any. It provides a CNIM Get Status function, whereby the Counter Call Scheduler (CCS) can poll for changes in the network connection.

There are three aspects that might change:

- *The Network Connection Status. The possible values of this 'CNIM Status' are given in Table 18.*
- *A number of QOS Flags. The QOS flags are given in Table 19.*
- *The Current Connection Type: One of Satellite, Metered, FRIACO, Voice, ADSL, ISDN,GSM. CCS will not use the actual type, but will notice that the type has changed and react accordingly.*

The time (i.e. tick count) of the last 'material change' is returned by the function. Changes in this time also count as a change and are to be reported by the function.

The function can also return the (static) Connection Type: FRIACO 24-hour (Silver), Metered 'dial-in' (Bronze), etc. However, CCS does not make use of this information.

Network Connection Status (from CNIM)	Description	Time of last material change
OK_Connected	Currently connected	Start of current connection
OK_Disconnected	Not currently connected, last call succeeded	End of last connection
Call Lost	Connection in progress was dropped	End of last connection
First Failure	First attempt to connect has failed	Time of first failure

FUJ00171956

Temporarily Unavailable	More than one attempt to connect has failed. The time when it is anticipated that it will become Permanently Unavailable is also returned	Time of first failure
Permanently Unavailable	More than 15 minutes (configurable in CNIM) since First Failure; or CNIM has deemed, by other means, that the fault is permanent	Time of first failure
Unknown[1,2]	Most likely cause is the CNIM service has failed	–

Table 18 – Network Connection Status from CNIM

[1] The CNIM Client DLL will return Unknown when it cannot communicate with CNIM, the most likely cause of which is that the CNIM service has failed. As Tivoli will be monitoring and restarting CNIM, there is no requirement for CCS to raise an alert. However. if the fault persists for a long time (maybe 1 hour), CCS will raise an alert by writing an Error to the NT Event Log.

[2] Other failures returned by this DLL will be treated in the same way.

FUJ00171956

QOS Flag (from CNIM)	Description	Used by CCS
Network connection nailed up	The time until when it is nailed up is also returned. This applies during FRIACO Fixed and Metered Fixed periods. This also applies during ADSL Fixed	For scheduling Riposte connections
Fixed connection	Set during the periods when Riposte is to nail up the connection. Only relevant if the network connection is nailed up. (This applies to FRIACO Fixed and Metered Fixed network behaviours.) This also applies during ADSL Fixed and ADSL Establish.	For scheduling Riposte connections
Emergency connection	Set when the current connection is of an emergency nature. (This applies to a connection over a Voice network) This flag prevents Riposte nailing up the line itself.	For monitoring the Online Status
Contracted Silver	The Outlet is contracted to receive Silver network service.	For monitoring the Online Status, and then only in controlling the message displayed to the Clerk.

Table 19 – QOS Flags from CNIM

The Contracted Silver flag is used to indicate those outlets which have the silver service as opposed to bronze. The reason being different messages can be displayed at a silver outlet in the event that a different level of service is offered. The flag is set on service types 7 through to 12.

The table below shows Connection Type flags for certain connection types.

Period\ Connection Type	Mode 1	Mode 2	Mode 3	GSM	Day D Mode
FRIACO Establish	Fixed=0 NailedUp=1 Emergency=0	Fixed=0 NailedUp=0 Emergency=0	Fixed=0 NailedUp=0 Emergency=1	As Mode 1	As Mode 1
FRIACO Fixed	Fixed=1	Fixed=1	Fixed=1	As Mode 1	As Mode 1

FUJ00171956

	NailedUp=1 Emergency=0	NailedUp=1 Emergency=0	NailedUp=0 Emergency=1		
Metered Fixed	Fixed=1 NailedUp=1 Emergency=0	Fixed=1 NailedUp=1 Emergency=0	Fixed=1 NailedUp=0 Emergency=1	As Mode 1	As Mode 1
Metered on Demand	Fixed=0 NailedUp=0 Emergency=0	Fixed=0 NailedUp=0 Emergency=0	Fixed=0 NailedUp=0 Emergency=1	As Mode 1	As Mode 1
Voice on Demand	Fixed=0 NailedUp=0 Emergency=0	Fixed=0 NailedUp=0 Emergency=0	Fixed=0 NailedUp=0 Emergency=1	As Mode 1	As Mode 1

Table 20 QOS Flags for Connection Types

1) Other bits are ignored if Emergency set.
3) CNIM will only set the "Contracted Silver Outlet" flag for 24 hr silver outlets, not part-time Silvers (NST 7).
4) The Emergency flag is only set when at voice (Mode 3) and the line is up.

2.2.13.a GetStatus Query Requirement for ADSL

The following details are taken from [Ref 14]

CNIM makes information available to the counter call scheduler on the availability of the outlet to data centre network. This will continue, and will apply to the new ADSL network. Where the network is permanently unavailable, information regarding the failure, in the form of an error code, is passed to the Post Office clerk along with a request to raise a call with the Horizon helpdesk. Permanent unavailability is defined as being unable to connect to the data centre for a 15 minute period. The current isdn network has certain constraints on the number of call attempts across the whole network per second. CNIM is limited to making on average (across all outlets) 1 call attempt per 15 minutes, hence the 15 minute period before declaring the network as permanently unavailable, ensuring at least one additional call attempt is made following the failure.

In the majority of cases the error code passed back will be the same as that recorded in the last record in the call summary file. There is a failure state where the ADSL call remains intact however IP communications is not possible to the data centre. This failure condition will be detected by CNIM pinging data centre components whilst an ADSL connection is outstanding. Where the ping continues to fail for greater than the period used to determine the network has become permanently unavailable (currently set at 15 minutes), CNIM will mark the gateway communications as permanently unavailable to the CCS, which in-turn will make this information available to the Horizon online applications / online service indicator. This error code will be overridden if at a later stage the call state does change.

2.2.13.b GetStatus Flag Settings for ADSL with ISDN and GSM Backup

Period\Connection Type	ADSL	ISDN (RAS)	GSM
RA	Fixed=0 NailedUp=0	Fixed=0 NailedUp=0	Fixed=0 NailedUp=0

FUJ00171956

	Emergency=0	Emergency=0	Emergency=0
RAIG	Fixed=1 NailedUp=1 Emergency=0	Fixed=1 NailedUp=1 Emergency=0	Fixed=1 NailedUp=1 Emergency=0

Table 21 Flag Settings for Resilient Network

2.2.13.c GetStatus Flag Settings for ADSL with GSM Backup

Period\Connection Type	ADSL	GSM
RA	Fixed=0 NailedUp=0 Emergency=0	Fixed=0 NailedUp=0 Emergency=0
RAG	Fixed=1 NailedUp=1 Emergency=0	Fixed=1 NailedUp=1 Emergency=0

Table 22 Flag Settings for Resilient Network

2.2.14 Satellite Requirements

The fundamental difference between a satellite gateway and any other, from the point of view of CNIM, is the absence of the Eicon card. CNIM is unable to configure the means of communication on the gateway and is used only to monitor and log calls and to return failure information to the CCS via the GetStatus mechanism.

2.2.15 Tracing Requirements

Version 2 of CNIM will use the TuneableTrace mechanism. See NB/LLD/025.

From version 2 onwards the trace file will contain which “ping” in the sequence has worked, in order to give some indication as to the quality of the network at the time.

2.2.16 Static Test Requirements

There are two CNIM function calls that are test scenarios.

2.2.16.a CNIM Test – Implementation

When CNIM has been installed at an Outlet, it has to ascertain whether or not the metered service is available. CNIM will only attempt to connect to the Data Centre via the metered service as this is available 24 hours a day, seven days a week. If the metered call fails the installation will be rolled back.

2.2.16.a.1 Implementation Test at S60

From S60 the Implementation Test will merely comprise updating registry to say that the process has been completed and that CNIM is installed.

FUJ00171956

2.2.16.b CNIM Test – normal running

During normal running if the CNIM test function is invoked it will attempt Data Centre calls through the primary number in Mode 1 and Mode 2. A file is generated within the CNIM folder on the Gateway PC with the results of the Data Centre calls.

2.2.16.b.1 Normal Test at S60

From S60 the Normal Test has been removed.

2.2.17 BNR - CP4097 CNIM to send reset to Connection Manager every 20 minutes.

Design Overview: See section 5.23

For ADSL connected outlets (NST13 and NST14) CNIM will issue a reset request to Connection Manager at 20 minute intervals during periods of ADSL network failure. The first reset will occur immediately following the first ping failure.

2.2.17.a Service Type 13 - ADSL only Outlets

On NST 13 outlets the connection type will remain as ADSL throughout the reset cycle unless the user manually switches to GSM backup. In any event the reset cycle will continue until network connectivity is restored.

On first ping failure CNIM will set the Connection Manager reset flag to be set to 1 and will start a 20 minute "Blackhole" timer which, on expiry, will alsocause the Connection Manager reset flag to be set to 1. Connection Manager will then reset the RAS connection each time the reset flag is set to 1.

If during the 20 minute wait period, CNIM detects a change of RAS connection state by Connection Manager then the "Blackhole" timer will be reset and a new ping test will be initiated. If the ping test fails then the timer will be reinitiated.

2.2.17.b Service Type 14 - ADSL Outlets with ISDN Backup

On NST 14 outlets during core hours the connection will switch to ISDN after 10 minutes in the event of network failure. This is done by CNIM requesting an ISDN connection type from Connection Manager. The change of connection type will cause CNIM to retest the connection and, if it succeeds, the "Blackhole" timer will be terminated. If the test fails then CNIM will enter the 20 minute reset cycle as for an ADSL connection.

2.2.18 BNR - CP4103 GSM Network gives Received Signal Strength Information

Design Overview: See section 5.24

CNIM will be required to log the received signal strength, obtained by Connection Manager, to TuneableTrace. CNIM will monitor Connection Manager registry and log each change of RSSI value.

2.2.19 Event Logging of Network Switching for BNR

Design Overview: See section 5.25

The following requirements are taken from [Ref 20].

FUJ00171956

CNIM is responsible for controlling the switch between network types. On switch to a new network type CNIM will raise an event. CNIM will include the following information specifically within the event text:

- *The network type before the switch;*
- *The network type following the switch;*
- *The time and date the switch was attempted.*

CNIM will raise an information event where the switch was successful and an error event where the switch was not successful. A unique, to CNIM, event ID will be recorded against the event allowing Tivoli to filter the events to be forwarded to the data centre.

The following additional information will be gleaned from the event itself:

- *The time the event was raised and therefore the switch was complete, i.e. when the event was written;*
- *The Gateway counter machine name, which includes the FAD code of the Branch.*

CNIM is also responsible for testing the ISDN backup network connection at strategic outlets once per week. The event raised to record a successful test will include the information document above against the standard network type switch event plus the following additional information / changes:

- *The percentage of successful ping attempts made across the 10 minute test period.*

A different event ID will be used to allow the event to be distinguished from events relating to a switch required following a failure.

FUJ00171956

3 ARCHITECTURE

3.1 System Diagram

The relationship of the CNIM to other system components is shown in Figure 10.

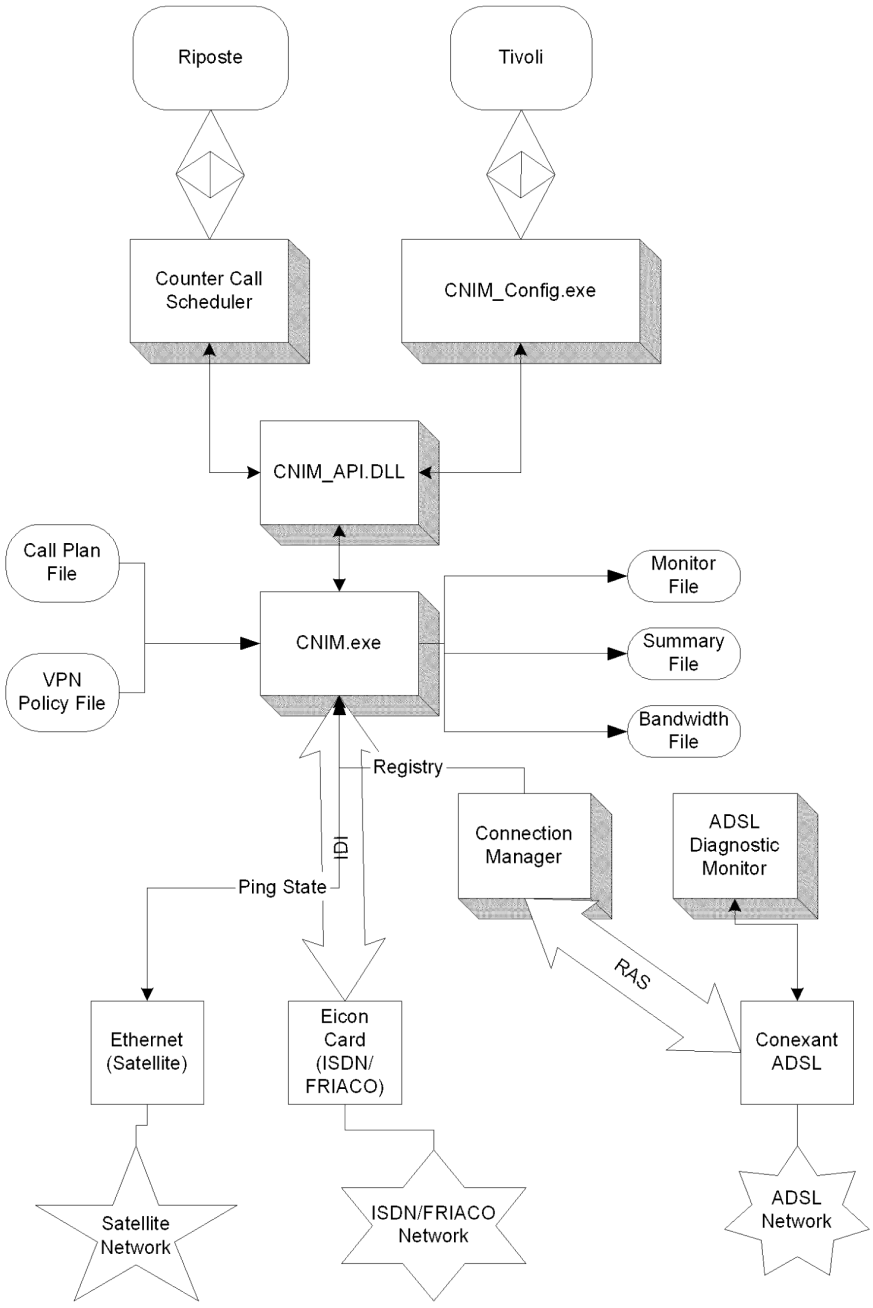

Figure 10: System Diagram

FUJ00171956

3.2 Operational Overview

One of the roles of CNIM is to manage the Eicon card if one is present and to provide call logging and diagnostic information.

For a satellite or ADSL outlet no Eicon card is used. On VSAT outlets CNIM relies on ping success/fail information, whilst on an ADSL outlet CNIM uses line status data from Connection Manager.

Call logging takes place by providing a one-line record for each call made or received by the outlet. Each record is placed in a "Monitor" file specific to that 24-hour period, i.e. each “UTC” day. In addition a summary of the day’s calls will be placed in a "Period" file as a one line record. The file names of the Monitor and Period files will be specific to the date for which that file applies.

Current diagnostic information will be available via the CNIM_API.dll. This provides a "GetStatus" function, which may be used to query the current connection type and whether a line test is pending. The API also provides functionality to test all available numbers during installation and to provide a reset mode such that updated registry input will be incorporated into the existing run mode.

CNIM also incorporates a "Call Reversal (Dial Back)" facility such that on closure of in inbound call to the outlet CNIM will initiate a connection to the data centre.

FUJ00171956

4 EXTERNAL INTERFACES

4.1 Interfaces Provided

4.1.1 NT Service Interface

- CNIM provides the standard ServiceMain() and Handler() functions to support an NT service.
- The CNIM starts automatically. Subsequent control is via the Control Service API (OpenService(), StartService(), ControlService(). Start and stop controls are supported. Pause and resume controls are not supported.

4.1.2 GetStatus Interface to Counter Call Scheduler

CNIM is required to provide network status information to Counter Call Scheduler (CCS) on demand. CCS may request information immediately or request to be notified of network changes within a certain period. At the end of that period CNIM will return the current network state.

More detail for this is given in section 5.16.

4.1.3 Operational Control Interface

4.1.3.a Call Plan Registry

The NT registry key [HKEY_LOCAL_MACHINE\SOFTWARE\ICL\Pathway Configuration\CNIM\CallPlan] is used to control the operational state of CNIM. The following key values are defined:

Name	Type	Max size	Default value	Description
Call_Plan_Dir	String	64	"C:\CNIM\"	Call plan directory
Call_Plan_Prefix	String	64	"CALL_PLAN_"	Call Plan file prefix
Call_Plan_Output	String	64	"CP_Out.txt"	Call Plan output file

Table 23 Registry Entries - Call Plan

4.1.3.b Connection Modes Registry

The NT registry key:

[HKEY_LOCAL_MACHINE\SOFTWARE\ICL\Pathway Configuration\CNIM\Connection\ConnectionModes] contains a set of subkeys, one for each connection type.

The value name is the CNIM mode and contains the connection type for that mode, the corresponding Branch Resilient Network mode as input from the engineers buttons and the Test Range. A BNR mode of 0 essentially means that that mode of connection cannot be initiated from the "Connect" button on the engineers screen. In the case of "Idle" it would be initiated from the "Drop" button.

Conventional CNIM using NDIS with the Eicon card would use CNIM modes 1,2 and 3. There would be no mapping of CNIM modes 2 and 3 to the engineers buttons. Generally the buttons map to RAS modes, which for an NDIS outlet would be CNIM mode 4 (BNR mode 2). On an NDIS outlet then NDIS Primary would be BNR mode 1.

FUJ00171956

The values used are described below:

FUJ00171956

4.1.3.b.1 FRIACO Establish Connection Types

[HKLM\SOFTWARE\ICL\Pathway Configuration\CNIM\Connection\ConnectionModes\NDIS_FE]					
Name	**Type**	**Max size**	**Default value**	**Contents**	**Description**
0	String	64	N/A	IDLE_RAS,0,RID_Range	Network Type "Idle", BNR Mode 0, RAS Idle Test range
1	String	64	N/A	FP,1,F_Range	FRIACO Primary, BNR Mode 1, NDIS Fixed range
2	String	64	N/A	MS,9,F_Range	Metered Secondary, BNR Mode 1
3	String	64	N/A	VP,9,F_Range	Voice Primary, BNR Mode 1
4	String	64	N/A	IDLE,0,RID_Range	Idle, BNR Mode 2, RAS Idle Test range

Table 24 CNIM and BNR Modes for Connection Types - FRIACO Establish

4.1.3.b.2 FRIACO Fixed Connection Types

[HKLM\SOFTWARE\ICL\Pathway Configuration\CNIM\Connection\ConnectionModes\NDIS_FF]					
Name	**Type**	**Max size**	**Default value**	**Example**	**Description**
0	String	64	N/A	IDLE_RAS,0,RID_Range	Network Type "Idle", BNR Mode 0
1	String	64	N/A	FP,1,F_Range	FRIACO Primary, BNR Mode 1
2	String	64	N/A	MS,1,F_Range	Metered Secondary, BNR Mode 1
3	String	64	N/A	VP,1,F_Range	Voice Primary, BNR Mode 1
4	String	64	N/A	IDLE_RAS,0,RID_Range	Idle, BNR Mode 2, RAS Idle Test range

Table 25 CNIM and BNR Modes for Connection Types - FRIACO Fixed

4.1.3.b.3 FRIACO Fixed With GSM - Connection Types

[HKLM\SOFTWARE\ICL\Pathway Configuration\CNIM\Connection\ConnectionModes\NDIS_FFG]					
Name	**Type**	**Max size**	**Default value**	**Example**	**Description**
0	String	64	N/A	IDLE_RAS,0,RG_Range	Network Type "Idle", BNR Mode 0
1	String	64	N/A	FP,1,F_Range	FRIACO Primary, BNR Mode 1
2	String	64	N/A	MS,1,F_Range	Metered Secondary, BNR Mode 1
3	String	64	N/A	VP,1,F_Range	Voice Primary, BNR Mode 1
4	String	64	N/A	GSM,2,RG_Range	GSM, BNR Mode 2, RAS GSM Test range

Table 26 CNIM and BNR Modes for Connection Types - FRIACO Fixed with GSM

4.1.3.b.4 Metered Fixed Connection Types

[HKLM\SOFTWARE\ICL\Pathway Configuration\CNIM\Connection\ConnectionModes\NDIS_MF]					
Name	**Type**	**Max**	**Default**	**Contents**	**Description**

FUJ00171956

		size	value		
0	String	64	N/A	IDLE_RAS,0,RID_Range	Network Type "Idle", BNR Mode 0
1	String	64	N/A	MP,1,F_Range	Metered Primary, BNR Mode 1
2	String	64	N/A	MS,1,F_Range	Metered Secondary, BNR Mode 1
3	String	64	N/A	VP,1,F_Range	Voice Primary, BNR Mode 1
4	String	64	N/A	IDLE_RAS,0,RID_Range	Idle, BNR Mode 0

Table 27 CNIM and BNR Modes for Connection Types - Metered Fixed

4.1.3.b.5 Metered Fixed with GSM Connection Types

[HKLM\SOFTWARE\ICL\Pathway Configuration\CNIM\Connection\ConnectionModes\ NDIS_MFG]					
Name	**Type**	**Max size**	**Default value**	**Contents**	**Description**
0	String	64	N/A	IDLE_RAS,0,RG_Range	Network Type "Idle", BNR Mode 0
1	String	64	N/A	MP,1,F_Range	Metered Primary, BNR Mode 1
2	String	64	N/A	MS,1,F_Range	Metered Secondary, BNR Mode 1
3	String	64	N/A	VP,1,F_Range	Voice Primary, BNR Mode 1
4	String	64	N/A	GSM,2,RG_Range	GSM, BNR Mode 2, RAS GSM range

Table 28 CNIM and BNR Modes for Connection Types - Metered Fixed with GSM

4.1.3.b.6 Metered On Demand Connection Types

[HKLM\SOFTWARE\ICL\Pathway Configuration\CNIM\Connection\ConnectionModes\NDIS_MOD]					
Name	**Type**	**Max size**	**Default value**	**Example**	**Description**
0	String	64	N/A	IDLE_RAS,0,RID_Range	Network Type "Idle", BNR Mode 0
1	String	64	N/A	MP,1,D_Range	Metered Primary, BNR Mode 1
2	String	64	N/A	VP,1,D_Range	Voice Primary, BNR Mode 1
3	String	64	N/A	VS,1,D_Range	Voice Secondary, BNR Mode 1
4	String	64	N/A	IDLE_RAS,0,RID_Range	Idle, BNR Mode 0

Table 29 CNIM and BNR Modes for Connection Types - Metered On Demand

4.1.3.b.7 Metered On Demand with GSM Connection Types

FUJ00171956

[HKLM\SOFTWARE\ICL\Pathway Configuration\CNIM\Connection\ConnectionModes\NDIS_MODG]					
Name	**Type**	**Max size**	**Default value**	**Example**	**Description**
0	String	64	N/A	IDLE_RAS,0,RG_Range	Network Type "Idle", BNR Mode 0
1	String	64	N/A	MP,1,D_Range	Metered Primary, BNR Mode 1
2	String	64	N/A	VP,1,D_Range	Voice Primary, BNR Mode 1
3	String	64	N/A	VS,1,D_Range	Voice Secondary, BNR Mode 1
4	String	64	N/A	GSM,2,RG_Range	GSM, BNR Mode 2, RAS GSM range

Table 30 CNIM and BNR Modes for Connection Types – MOD with GSM

4.1.3.b.8 Voice Connection Types

[HKLM\SOFTWARE\ICL\Pathway Configuration\CNIM\Connection\ConnectionModes\NDIS_VOD]					
Name	**Type**	**Max size**	**Default value**	**Example**	**Description**
0	String	64	N/A	IDLE_RAS,0,RID_Range	Network Type "Idle", BNR Mode 0
1	String	64	N/A	VP,1,I_Range	Voice Primary, BNR Mode 1
2	String	64	N/A	VS,1,I_Range	Voice Secondary, BNR Mode 1
3	String	64	N/A	VT,1,I_Range	Voice Tertiary, BNR Mode 1
4	String	64	N/A	IDLE_RAS,0,RID_Range	Idle, BNR Mode 0

Table 31 CNIM and BNR Modes for Connection Types – Voice

4.1.3.b.9 Voice with GSM Connection Types

[HKLM\SOFTWARE\ICL\Pathway Configuration\CNIM\Connection\ConnectionModes\NDIS_VODG]					
Name	**Type**	**Max size**	**Default value**	**Example**	**Description**
0	String	64	N/A	IDLE_RAS,0,RID_Range	Network Type "Idle", BNR Mode 0
1	String	64	N/A	VP,1,I_Range	Voice Primary, BNR Mode 1
2	String	64	N/A	VS,1,I_Range	Voice Secondary, BNR Mode 1
3	String	64	N/A	VT,1,I_Range	Voice Tertiary, BNR Mode 1
4	String	64	N/A	GSM,2,RG_Range	GSM, BNR Mode 2

Table 32 CNIM and BNR Modes for Connection Types - Voice with GSM

4.1.3.b.10 RAS ADSL Connection Types

FUJ00171956

[HKLM\SOFTWARE\ICL\Pathway Configuration\CNIM\Connection\ConnectionModes\RAS_A]					
Name	**Type**	**Max size**	**Default value**	**Contents**	**Description**
0	String	64	N/A	IDLE_RAS,0,RA_Range	Network Type "Idle", BNR Mode 0
1	String	64	N/A	ADSL,1,RA_Range	ADSL, BNR Mode 1
2	String	64	N/A	IDLE_RAS,0,RA_RANGE	Idle, BNR Mode 0
3	String	64	N/A	IDLE_RAS,0,RA_RANGE	Idle, BNR Mode 0
4	String	64	N/A	IDLE_RAS,0,RA_RANGE	Idle, BNR Mode 0

Table 33 CNIM and BNR Modes for Connection Types - ADSL only

4.1.3.b.11 RAS ADSL-GSM Connection Types

[HKLM\SOFTWARE\ICL\Pathway Configuration\CNIM\Connection\ConnectionModes\RAS_AG]					
Name	**Type**	**Max size**	**Default value**	**Contents**	**Description**
0	String	64	N/A	IDLE_RAS,0,RAG_Range	Network Type "Idle", BNR Mode 0
1	String	64	N/A	ADSL,1,RAG_Range	ADSL, BNR Mode 1
2	String	64	N/A	GSM,2,RAG_Range	GSM, BNR Mode 2
3	String	64	N/A	IDLE_RAS,0,RA_Range	Idle, BNR Mode 0
4	String	64	N/A	IDLE_RAS,0,RA_Range	Idle, BNR Mode 0

Table 34 CNIM and BNR Modes for Connection Types - ADSL with GSM

4.1.3.b.12 RAS ADSL-ISDN-GSM Connection Types

[HKLM\SOFTWARE\ICL\Pathway Configuration\CNIM\Connection\ConnectionModes\RAS_AIG]					
Name	**Type**	**Max size**	**Default value**	**Example**	**Description**
0	String	64	N/A	IDLE_RAS,0,RAIG_Range	Network Type "Idle", BNR Mode 0
1	String	64	N/A	ADSL,1,RAIG_Range	ADSL, BNR Mode 1
2	String	64	N/A	ISDN,2,RAIG_Range	ISDN, BNR Mode 2
3	String	64	N/A	GSM,3,RAIG_Range	GSM, BNR Mode 3
4	String	64	N/A	IDLE_RAS,0,RA_Range	Idle, BNR Mode 0

Table 35 CNIM and BNR Modes for Connection Types - ADSL with ISDN and GSM

4.1.3.b.13 RAS ISDN Only Connection Types

[HKLM\SOFTWARE\ICL\Pathway Configuration\CNIM\Connection\ConnectionModes\RAS_IT]					
Name	**Type**	**Max**	**Default**	**Example**	**Description**

FUJ00171956

		size	value		
0	String	64	N/A	IDLE_RAS,0,RIT_ Range	Network Type "Idle", BNR Mode 0
1	String	64	N/A	ISDN,1,RIT_Range	ISDN, BNR Mode 1
2	String	64	N/A	IDLE_RAS,0,RIT_ Range	Network Type "Idle", BNR Mode 0
3	String	64	N/A	IDLE_RAS,0,RIT_ Range	Network Type "Idle", BNR Mode 0
4	String	64	N/A	IDLE_RAS,0,RIT_ Range	Network Type "Idle", BNR Mode 0

Table 36 CNIM and BNR Modes for Connection Types - ISDN Only

4.1.3.b.14 VSAT Connection Types

[HKLM\SOFTWARE\ICL\Pathway Configuration\CNIM\Connection\ConnectionModes\VSAT_PC]					
Name	**Type**	**Max size**	**Default value**	**Example**	**Description**
0	String	64	N/A	PC,0,P_Range	Permanent Connection, BNR Mode 0
1	String	64	N/A	PC,1,P_Range	Permanent Connection, BNR Mode 1
2	String	64	N/A	PC,2,P_Range	Permanent Connection, BNR Mode 2
3	String	64	N/A	PC,3,P_Range	Permanent Connection, BNR Mode 3
4	String	64	N/A	PC,4,P_Range	Permanent Connection, BNR Mode 4

Table 37 CNIM and BNR Modes for Connection Types – VSAT

4.1.3.b.15 Frame Relay Establish Connection Types

[HKLM\SOFTWARE\ICL\Pathway Configuration\CNIM\Connection\ConnectionModes\FR_FRE]					
Name	**Type**	**Max size**	**Default value**	**Example**	**Description**
0	String	64	N/A	FRE,0,FR_Range	Frame Relay Establish, BNR Mode 0
1	String	64	N/A	FRE,1,FR_Range	Frame Relay Establish, BNR Mode 1
2	String	64	N/A	Empty	Empty
3	String	64	N/A	Empty	Empty
4	String	64	N/A	Empty	Empty

Table 38 CNIM and BNR Modes for Connection Types – Frame Relay Establish

4.1.3.b.16 Frame Relay Fixed Connection Types

FUJ00171956

[HKLM\SOFTWARE\ICL\Pathway Configuration\CNIM\Connection\ConnectionModes\FR_FRF]					
Name	**Type**	**Max size**	**Default value**	**Example**	**Description**
0	String	64	N/A	FRF,0,FR_Range	Frame Relay Fixed, BNR Mode 0
1	String	64	N/A	FRF,1,FR_Range	Frame Relay Fixed, BNR Mode 1
2	String	64	N/A	Empty	Empty
3	String	64	N/A	Empty	Empty
4	String	64	N/A	Empty	Empty

Table 39 CNIM and BNR Modes for Connection Types – Frame Relay Fixed

FUJ00171956

4.1.3.c Service Mode Registry

The Service Mode registry is used to map Connection types to secondary names which relate either to phone number names or RAS connection types.

For NDIS outlets these secondary names are stored in the Eicon section of registry as described in section 4.1.3.o

4.1.3.c.1 Service Mode – FRIACO 1

[HKLM\SOFTWARE\ICL\Pathway Configuration\CNIM\Connection\ServiceMode\FRIACO1]					
Name	**Type**	**Max size**	**Default value**	**Example of Secondary Name**	**Description of connection to use**
FP	String	64	N/A	FC1P	FRIACO 1 Primary
FS	String	64	N/A	FC1S	FRIACO 1 Secondary
MP	String	64	N/A	DP	Dialaround Primary
MS	String	64	N/A	DS	Dialaround Secondary
VP	String	64	N/A	VP	Voice Primary
VS	String	64	N/A	VS	Voice Secondary
VT	String	64	N/A	VT	Voice Tertiary
GSM	String	64	N/A	GSM	GSM
IDLE	String	64	N/A	IDLE	Idle

Table 40 Service Mode – FRIACO 1

4.1.3.c.2 Service Mode – FRIACO 2

[HKLM\SOFTWARE\ICL\Pathway Configuration\CNIM\Connection\ServiceMode\FRIACO2]					
Name	**Type**	**Max size**	**Default value**	**Example of Secondary Name**	**Description of connection to use**
FP	String	64	N/A	FC2P	FRIACO 2 Primary
FS	String	64	N/A	FC2S	FRIACO 2 Secondary
MP	String	64	N/A	DP	Dialaround Primary
MS	String	64	N/A	DS	Dialaround Secondary
VP	String	64	N/A	VP	Voice Primary
VS	String	64	N/A	VS	Voice Secondary
VT	String	64	N/A	VT	Voice Tertiary
GSM	String	64	N/A	GSM	GSM
IDLE	String	64	N/A	IDLE	Idle

Table 41 Service Mode – FRIACO 2

4.1.3.c.3 Service Mode - Metered

FUJ00171956

[HKLM\SOFTWARE\ICL\Pathway Configuration\CNIM\Connection\ServiceMode\Metered]					
Name	**Type**	**Max size**	**Default value**	**Example of Secondary Name**	**Description of connection to use**
MP	String	64	N/A	DP	Dialaround Primary
MS	String	64	N/A	DS	Dialaround Secondary
VP	String	64	N/A	VP	Voice Primary
VS	String	64	N/A	VS	Voice Secondary
VT	String	64	N/A	VT	Voice Tertiary
GSM	String	64	N/A	GSM	GSM
IDLE	String	64	N/A	IDLE	Idle

Table 42 Service Mode - Metered

4.1.3.c.4 Service Mode - RAS

[HKLM\SOFTWARE\ICL\Pathway Configuration\CNIM\Connection\ServiceMode\RAS]					
Name	**Type**	**Max size**	**Default value**	**Example of Secondary Name**	**Description of connection to use**
ADSL	String	64	N/A	ADSL	ADSL
ISDN	String	64	N/A	ISDN	ISDN
GSM	String	64	N/A	GSM	GSM
IDLE	String	64	N/A	IDLE	Idle

Table 43 Service Mode - RAS

4.1.3.c.5 Service Mode - Voice

[HKLM\SOFTWARE\ICL\Pathway Configuration\CNIM\Connection\ServiceMode\Voice]					
Name	**Type**	**Max size**	**Default value**	**Example of Secondary Name**	**Description of connection to use**
VP	String	64	N/A	VP	Voice Primary
VS	String	64	N/A	VS	Voice Secondary
VT	String	64	N/A	VT	Voice Tertiary
GSM	String	64	N/A	GSM	GSM
IDLE	String	64	N/A	IDLE	Idle

Table 44 Service Mode - Voice

4.1.3.c.6 Service Mode - VSAT

[HKLM\SOFTWARE\ICL\Pathway Configuration\CNIM\Connection\ServiceMode\VSAT]					
Name	**Type**	**Max size**	**Default value**	**Example of Secondary Name**	**Description of connection to use**
PC	String	64	N/A	PC	Permanent Connection

Table 45 Service Mode - VSAT

4.1.3.c.7 Service Mode – Frame Relay

FUJ00171956

[HKLM\SOFTWARE\ICL\Pathway Configuration\CNIM\Connection\ServiceMode\FrameRelay]					
Name	**Type**	**Max size**	**Default value**	**Example of Secondary Name**	**Description of connection to use**
FRE	String	64	N/A	FRE	Frame Relay Establish
FRF	String	64	N/A	FRF	Frame Relay Fixed

Table 46 Service Mode – Frame Relay

4.1.3.d Mapping Service Type to Service Mode

The following registry table is used to map standard service types to service modes.

[HKLM\SOFTWARE\ICL\Pathway Configuration\CNIM\Connection\NST_To_Mode]					
Name	**Type**	**Max size**	**Default value**	**Contents**	**Description of connection to use**
ST_ADSL	String	64	N/A	RAS	RAS Service Mode
ST_ADSL_ISDN	String	64	N/A	RAS	RAS Service Mode
ST_BRONZE	String	64	N/A	Metered	Metered Service Mode
ST_FRAME_RELAY	String	64	N/A	FrameRelay	Frame Relay Service Mode
ST_FRIACO_SILVER_24HR_C1	String	64	N/A	FRIACO1	FRIACO 1 Service Mode
ST_FRIACO_SILVER_24HR_C2	String	64	N/A	FRIACO2	FRIACO 2 Service Mode
ST_FRIACO_SILVER_DAYTIME_C1	String	64	N/A	FRIACO1	FRIACO 1 Service Mode
ST_FRIACO_SILVER_DAYTIME_C2	String	64	N/A	FRIACO2	FRIACO 2 Service Mode
ST_NON_FRIACO_SILVER_24HR	String	64	N/A	Metered	Metered Service Mode
ST_NON_FRIACO_SILVER_DAYTIME	String	64	N/A	Metered	Metered Service Mode
ST_SATELLITE	String	64	N/A	VSAT	Satellite Service Mode
ST_SILVER_PARTTIME_A	String	64	N/A	Metered	Metered Service Mode
ST_SILVER_PARTTIME_B	String	64	N/A	Metered	Metered Service Mode
ST_VOICE	String	64	N/A	Voice	Voice Service Mode

Table 47 Mapping Service Type to Service Mode

4.1.3.e Live Registry

The NT registry key [HKEY_LOCAL_MACHINE\SOFTWARE\ICL\Pathway Configuration\CNIM\Live] is used to control the operational state of CNIM. The following key values are defined:

Name	**Type**	**Max size**	**Default value**	**Description**
CAUSE_CODE	String	64	N/A	The last disconnection cause code.
CUR_DAY	String	64	N/A	"MON", "TUE", "WED", THU, "FRI", "SAT", "SUN"
CUR_NET_TYPE	String	64	N/A	"VP", "VS", "VT", "FC1P",

FUJ00171956

CUR_NET_TYPE_INTERNAL	String	64	N/A	"FC2P", "FC1S", "FC2S", "MP", "MS", "DP", or "DS" "F" = FRIACO "M" = Metered "D" = Dialaround "P" = Permanent

FUJ00171956

DFND_END_TIME	String	64	N/A	Defined end time for the "Nailed Up" period. Of the form - "23:00:00"
DFND_NET_TYPE	String	64	N/A	Defined network type: "01" to "14"
DFND_START_TIME	String	64	N/A	Defined start time for the "Nailed Up" period. Of the form - "08:00:00"
DIRECTORY_MONITOR_FILES	String	64	"C:\CNIM\MONITOR\"	Monitor files directory
DIRECTORY_PERIOD_FILES	String	64	"C:\CNIM\SUMMARY\"	Summary files directory
DIRECTORY_TEST_FILES	String	64	"C:\CNIM\TEST\"	Test files directory
DISABLE_ON_TEMP_FAIL	DWORD	N/A	1	
Disabled_Channel	DWORD	N/A	2	Comms channel not used
Eicon_Num_1	String	64	N/A	1st Eicon number
Eicon_Num_2	String	64	N/A	2nd Eicon number
Eicon_Num_3	String	64	N/A	3rd Eicon number
Eicon_Num_4	String	64	N/A	4th Eicon number
Eicon_Num_5	String	64	N/A	5th Eicon number
Eicon_Num_6	String	64	N/A	6th Eicon number
ErrorExtension	String	64	"ERR"	Filename extension for Error files
Est_End_Time	String	64	N/A	Time at which CNIM will terminate the "Nailed Up" period.
FAIL_NET_TIME	String	64	N/A	Time at which the network was deemed to have permanently failed.
FRIACO_PRIME_NUMBER	String	64	N/A	The primary FRIACO number for this outlet.
FRIACO_SECONDARY_NUMBER	String	64	N/A	The secondary FRIACO number for this outlet.
KEEP_ALIVE_STATE	String	64	N/A	Current Keep Alive State: "UP" or "DOWN"
METERED_PRIME_NUMBER	String	64	N/A	The primary metered number for this outlet.
METERED_SECONDARY_NUMBER	String	64	**N/A**	The secondary metered number for this outlet.
Migration_State	String	**64**	**"WITHIN_MIGRATION"**	**EITHER "WITHIN_MIGRATION" OR "POST_MIGRATION"**
Monitor_Dial_Prefix	String	64	"QOS_MON_D_"	Monitor File name prefix - dialled
Monitor_Metd_Prefix	String	64	"QOS_MON_M_"	Monitor File name prefix - metered
Monitor_Perm_Prefix	String	64	"QOS_MON_P_"	Monitor File name prefix - permanent
Monitor_Prefix	String	64	"QOS_MON_"	Monitor File name prefix
NET_DOWN	String	64	N/A	Network Up/Down flag:

FUJ00171956

				"YES" or "NO"
NewFileExtension	String	64	"NEW"	Name of extension used at end of the current call plan filename
OldFileExtension	String	64	"OLD"	Name of extension used at end of older call plan filenames
Period_Prefix	String	64	"QOS_P_"	Period File name prefix
Ping_State_List_Length	DWORD	N/A	10	Maximum number of ping states to store
STATE_NET	String	64	N/A	Network state: "SNET_UNKNOWN"; "SNET_FAILED" or "SNET_OK";
Subordinated_CM_Codes	String	64	""	Codes from Connection Manager that are subordinate to the ADSL Diagnostic Monitor code. None currently used at S60.
Successful_Cause_Codes	String	64	Typical values, these may vary: "0x0000,0x0080, 0x0090"	Cause codes that indicate a successful call closure.
Test_Prefix	String	64	"TEST_RESULT_"	Prefix for test result files.
TickLineChanged	DWORD	N/A	0	Tick count when the line last changed
TickNextTest	DWORD	N/A	0	Tick count when the next test will be performed. Indicates permanent failure.
USE_SINGLE_PING_FOR_KA	DWORD	N/A	1	
VOICE_PRIME_NUMBER	String	64	N/A	The primary 'voice' number for this outlet.
VOICE_SECONDARY_NUMBER	String	64	N/A	The secondary 'voice' number for this outlet.
VOICE_TERTIARY_NUMBER	String	64	N/A	The tertiary 'voice' number for this outlet.
VPN_SERVER_PINGED	String	64	N/A	IP Address for the VPN Server being pinged.
VPN1_ADDR	String	64	N/A	IP Address of the 1st VPN server listed in the policy file.
VPN2_ADDR	String	64	N/A	IP Address of the 2nd VPN server listed in the policy file.
VPN3_ADDR	String	64	N/A	IP Address of the 3rd VPN server listed in the policy file.
VPN4_ADDR	String	64	N/A	IP Address of the 4th VPN server listed in the policy file.
VPN5_ADDR	String	64	N/A	IP Address of the 5th VPN server listed in the policy file.
VPN6_ADDR	String	64	N/A	IP Address of the 6th VPN server listed in the policy file.
VPN7_ADDR	String	64	N/A	IP Address of the 7th VPN server

FUJ00171956

				listed in the policy file.
VPN8_ADDR	String	64	N/A	IP Address of the 8th VPN server listed in the policy file.

Table 48 Registry Entries - Live

4.1.3.f Period Registry

The NT registry key [HKEY_LOCAL_MACHINE\SOFTWARE\ICL\Pathway Configuration\CNIM\ Period] is used to store data for the "Period" file. The following key values are defined:

Name	Type	Max size	Default value	Description
FRIACO_Time_Secs	**DWORD**	N/A	0	Total number of FRIACO seconds in 'Nailed Up' period
Metered_Call_Count	DWORD	N/A	0	Total number of metered calls in 'Nailed Up' period
Metered_Time_Secs	DWORD	N/A	0	Total number of metered seconds in 'Nailed Up' period
Start_Date	String	N/A	N/A	Date at which CNIM started monitoring – format "11/09/2002"
Start_Time	String	N/A	N/A	Time at which CNIM started monitoring. – format "14:26:36:986"
Total_Time_Secs	DWORD	N/A	0	Total number of FRIACO and metered seconds in 'Nailed Up' period

Table 49 Registry Entries - Period

4.1.3.g RPC Registry

The NT registry key [HKEY_LOCAL_MACHINE\SOFTWARE\ICL\Pathway Configuration\ CNIM\RPC] is used to set the maximum number of RPC connections that CNIM will accept. The following key value is defined:

Name	Type	Max size	Default value	Description
Max_Connections	DWORD	N/A	000000c8	Max number of threads

Table 50 Registry Entries - RPC

4.1.3.h Test Results Registry

The NT registry key [HKEY_LOCAL_MACHINE\SOFTWARE\ICL\PathwayConfiguration\CNIM\TestResults] is used to store the test results. The following key values are defined:

Name	Type	Max size	Default value	Description
CNIM_Result_Path	String	64	**"C:\TEMP\CNIM_RES**ult.BAT"	Location of CNIM Results
dwImpTestResult	DWORD	N/A	0	0 = Fail 1 = Pass
ImpTestResult	String	64	N/A	Test result:

FUJ00171956

				"PASS" or "FAIL"
Number_1	String	64	N/A	1st Number tested
Number_1_dwResult	DWORD	N/A	0	0 = Unknown 1 = Layer 1 Fail 2 = Num. Not Tested 3 = Num. Fail 4 = Num. OK
Number_1_Result	String	64	N/A	Test result for Number 1: "UNKNOWN" "LAYER1_FAIL" "NUM_NOT_TESTED" "NUM_FAIL" "NUM_OK"
Number_2	String	64	N/A	2nd Number tested
Number_2_dwResult	DWORD	N/A	0	As for 1 above.
Number_2_Result	String	64	N/A	As for 1 above.
Number_3	String	64	N/A	3rd Number tested
Number_3_dwResult	DWORD	N/A	0	As for 1 above.
Number_3_Result	String	64	N/A	As for 1 above.
Number_4	String	64	N/A	4th Number tested
Number_4_dwResult	DWORD	N/A	0	As for 1 above.
Number_4_Result	String	64	N/A	As for 1 above.
Number_5	String	64		5th Number tested
Number_5_dwResult	DWORD	N/A	0	As for 1 above.
Number_5_Result	String	64		As for 1 above.
Number_6	String	64		6th Number tested
Number_6_dwResult	DWORD	N/A	0	As for 1 above.
Number_6_Result	String	64		As for 1 above.
RunnerTrigger_Path	String	64	"C:\Autoconfig\RunnerTrigger.exe"	Location of RunnerTrigger executable.
Test_Date	String	64	N/A	Date of Test e.g. "2002/12/31"
Test_Time	String	64	N/A	Time of Test e.g. "13:40:50"

Table 51 Registry Entries - Test Results

4.1.3.i Times Registry

The NT registry key [HKEY_LOCAL_MACHINE\SOFTWARE\ICL\Pathway Configuration\CNIM\ Times] is used to control the operational state of CNIM. The following key values are defined:

Name	Type	Max size	Default value (DWORD in Hex)	Description
OFFSET_RIT	STRING		160	Offset in minutes
CM_Reset_Timeout	DWORD		0000ea60	60000 milliseconds for Connection Manager to

FUJ00171956

				respond
CM_Reread_Delay	DWORD		000003e8	1000 milliseconds before checking if Connection Manager has updated registry
Dial_Back_KA_Max	DWORD	N/A	000000078	120 sec dial back max. time
Actual_Overhang	DWORD	N/A	0	Actual time in seconds beyond the nominal call plan time at which the connection type is changed.
CHAP_Interval_ISDN	DWORD	N/A	00000000a	Challenge Handshake Authentication Protocol interval – in ISDN mode. The interval in seconds, between authentications.
CHAP_Interval_Non_ISDN	DWORD	N/A	0	Challenge Handshake Authentication Protocol interval – in non ISDN mode. The interval in seconds, between authentications.
Dial_Back_Idle_Timeout	DWORD	N/A	000004b0	Maximum time to wait for the line to go idle before dialling back.
FRIACO_Metered_Time_Max	DWORD	N/A	00000384	Maximum time for Keep Alive when FRIACO is at Dialaround.(Sec.)
FRIACO_Metered_Time_Min	DWORD	N/A	0000012c	Minimum time for Keep Alive when FRIACO is at Dialaround. (Sec.)
Line_Test_Timeout	DWORD	N/A	78	Timeout (sec.) when doing an implementation test.
Max_Overhang	DWORD	N/A	0000003c	Maximum time in seconds beyond the nominal call plan time at which the connection type is changed.
Min_Overhang	DWORD	N/A	1	Minimum time in seconds beyond the nominal call plan time at which the connection type is changed.
Max_Tick_Deviation	DWORD	N/A	000003e8	Variation in tick count which is ignored between GetStatus calls.
MCDT_Fixed	DWORD	N/A	00000000a	Minimum Call Duration Time - Fixed Period
MCDT_MOD	DWORD	N/A	000000000	Minimum Call Duration Time – Dialled Period
MCDT_VOD	DWORD	N/A	000000014	Minimum Call Duration Time – Voice on Demand
OFFSET_FE_FF	String	64	"-15"	Maximum offset of boundary in minutes between FRIACO-Establish and FRIACO-Fixed.

FUJ00171956

OFFSET_FE_MOD	String	64	"10"	Maximum offset of boundary in minutes between FRIACO-Establish and Metered-On-Demand.
OFFSET_FF_MF	String	64	"15"	Maximum offset of boundary in minutes between FRIACO-Fixed and FRIACO-Fixed.
OFFSET_FF_MOD	String	64	"10"	Maximum offset of boundary in minutes between FRIACO-Fixed and Metered-On-Demand.
OFFSET_MF_FF	String	64	"-15"	Maximum offset of boundary in minutes between Metered-Fixed and FRIACO-Fixed.
OFFSET_MF_MOD	String	64	"10"	Maximum offset of boundary in minutes between Metered-Fixed and Metered-On-Demand.
OFFSET_MOD_FE	String	64	"15"	Maximum offset of boundary in minutes between Metered-Fixed and FRIACO-Fixed.
OFFSET_MOD_MF	String	64	"-15"	Maximum offset of boundary in minutes between Metered-On-Demand and Metered-Fixed.
Permanent_Fail_Counter	DWORD	N/A	0xfff	Maximum number of failed call attempts before permanent fail flag is set. Effectively no longer used.
Permanent_Fail_Timer	DWORD	N/A	384	After trying to connect using Mode 1 & 2 numbers for this time period, Mode 3 numbers are attempted.
Ping_Timeout_Seconds_Satellite	DWORD	N/A	28	Satellite Ping Timeout. (Sec.)
Ping_Timeout_Microseconds	DWORD	N/A	0	Ping microsecond Timeout
Ping_Timeout_Seconds	DWORD	N/A	5	Ping Timeout. (Sec.)
Shorthold_Fixed	DWORD	N/A	28	Time that the line is held open for – Fixed period
Shorthold_MOD	DWORD	N/A	5	Time that the line is held open for – Metered On Demand
Shorthold_VOD	DWORD	N/A	5	Time that the line is held open for – Voice On Demand
Test_Thread_Shutdown_Timeout	DWORD	N/A	0000000f	Maximum time to spend waiting for test thread to stop. (Sec.)
Test_Timer_Max	DWORD	N/A	384	Maximum time between tests (sec.).
Test_Timer_Min	DWORD	N/A	258	Minimum time between tests (sec.).

FUJ00171956

Table 52 Registry Entries - Times

The NT registry key [HKEY_LOCAL_MACHINE\SOFTWARE\ICL\Pathway Configuration\ CNIM\Users] is used to control the users ID's and passwords to connect via data or ISDN (voice). The following key values are defined:

Name	Type	Max size	Default value	Description
Inbound_Stored	DWORD	N/A	N/A	
PW_Inbound_Data	String	64	**"F5J3TS5"**	Password for data
PW_Inbound_ISDN	String	64	N/A	**PASSWORD FOR ISDN (VOICE)**
UID_Inbound_Data	String	64	**"ENERGISCVX"**	User ID for data
UID_Inbound_ISDN	String	64	N/A	User ID for ISDN (voice)

Table 53 Registry Entries - Users

4.1.3.j SubAddressing Registry

The NT registry key [HKEY_LOCAL_MACHINE\SOFTWARE\ICL\PathwayConfiguration\CNIM\SubAddressing] is used to control incoming calls and prevent the call being accepted, thereby saving the cost of accepting the call. This facility is not used at present.

Name	Type	Max size	Default value	Description
MSN	String	N/A	N/A	
Subaddress	String	N/A	N/A	

Table 54 Registry Entries - Sub Addressing

4.1.3.k Trace Registry

The NT registry key [HKEY_LOCAL_MACHINE\SOFTWARE\ICL\Pathway Configuration\ Trace\CNIM] is used to control trace logging. The following key values are defined:

Name	Type	Max size	Default value	Description
NumMaxLines	DWORD	N/A	000007d0	Maximum number of lines in log file.
TraceFile	String	64	"C:\CNIM\Trace\CNIM.log"	Location of the trace file
TraceLevel	DWORD	N/A	0xff	Trace level for normal use.
WriteInterval	DWORD	N/A	1	Number of lines to cache between writes.

Table 55 Registry Entries - Tracing

FUJ00171956

4.1.3.l TuneableTrace Registry

The NT registry key [HKEY_LOCAL_MACHINE\SOFTWARE\ICL\Pathway Configuration\CNIM\TuneableTrace] is used to control logging to TuneableTrace. The following key values are defined:

Name	Type	Max size	Default value	Description
ID	String	64	"NULL"	Top level ID
Name1	String	64	"cnim"	1st level name
Name2	String	64	"service"	2nd level name

Table 56 Registry Entries - TuneableTrace

A hierarchy of names is used to map onto the 'Name1, Name2, Instance' structure of the client table used by TuneableTrace. For VB clients the 'Instance name' used should be NULL. The Instance key has one mandatory value entry, 'TraceLevel' the value of which is a 32 bit trace level. Optionally, a value named 'Expiration' can be used which will prevent the unique set of keys identifying a particular client being deleted once used. The 'TraceLevel' and 'Expiration' value names are case sensitive. The value takes the format of a six digit date string in the format YYMMDD.

The NT registry key [HKEY_LOCAL_MACHINE\SOFTWARE\ICL\Pathway Configuration\CNIM\TuneableTrace\cnim\service\null] is used to control logging to TuneableTrace. The following key values are defined:

Name	Type	Max size	Default value	Description
Expiration	String	64	"991231"	Keep this trace level until the date shown
TraceLevel	DWORD	N/A	0x2f0ff	Normal level of Tracing

Table 57 Registry Entries - CNIM TuneableTrace

4.1.3.m Service Event Registry

The NT registry key [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Application\CNIM] is used to specify the message path. The following key values are defined:

Name	Type	Max size	Default value	Description
TypesSupported	DWORD	N/A	7	Eventlog
EventMessageFile	String	64	"c:\cnim\cnim_msg.dll"	Event Message File location

Table 58 Registry Entries - Message Path

4.1.3.n Service Dependency Registry

The NT registry key [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CNIM] is used to specify the dependency on the RPC service.

Name	Type	Max size	Default value	Description

FUJ00171956

DEPENDONSERVICE	HEX(7)	N/A	52,70,63,53,73,00,00	RPC
DEPENDONGROUP	HEX(7)	N/A	00	

Table 59 Registry Entries - CNIM Service Dependency on RPC

4.1.3.o Eicon Registry

The NT registry key [HKEY_LOCAL_MACHINE\SOFTWARE\ICL\Pathway Configuration\Eicon] is used to control the input data to CNIM. The following key values are defined:

Name	Type	Max size	Default value	Description
DP	String	64	N/A	Dialaround Primary
DS	String	64	N/A	Dialaround Secondary
FC1P	String	64	N/A	FRIACO 1 Primary
FC1S	String	64	N/A	FRIACO 1 Secondary
FC2P	String	64	**N/A**	FRIACO 2 Primary
FC2S	String	64	N/A	FRIACO 2 Secondary
MP	String	64	N/A	Metered Primary
MS	String	64	N/A	Metered Secondary
SERVICETYPE	String	64	N/A	Service Type
VP	String	64	N/A	Voice Primary
VS	String	64	N/A	Voice Secondary
VT	String	64	N/A	Voice Tertiary

Table 60 CDF Data Storage in Registry

4.1.3.p User Registry

The NT registry key [HKEY_LOCAL_MACHINE\SOFTWARE\ICL\Pathway Configuration\CNIM\Users] is used to control the input data to CNIM. The following key values are defined:

Name	Type	Max size	Default value	Description
PW_Inbound_ISDN	String	64	N/A	Extracted from the Eicon card when CNIM first installed, and stored in registry.
PW_Inbound_Data	String	64	"f5j3ts5"	Password expected to be received when using the Data network.
UID_Inbound_Data	String	64	"energiscvx"	User ID expected to be received when using the Data network.
Inbound_Stored	dword	N/A	00000000	Set to 1 on CNIM installation when the ISDN Inbound password has been stored.

Table 61 User Data Storage in Registry

FUJ00171956

4.1.3.q Connection Manager Registry

The NT registry key [HKLM\Software\Fujitsu\POA\ConnectionManager\State] is used to display service and connection state information. The following key values are defined:

Name	Type	Max size	Default value	Description
DayD	DWORD	N/A	0	Set to 1 when Connection Manager enters DayD dialling mode, set to 0 otherwise.
HeartBeat	DWORD	N/A	N/A	Unless the service is Idle or Suspended, this registry value is updated to the value of GetTickCount at a rate determined by the ConnectionManager\HeartBeat value.
Status	String	N/A	N/A	Reports a change of dialling state, as a comma-separated set of fields. Eaxample: D,Data_Centre,210,01/12/2005 00:02:37.571
Suspended	String	N/A	N/A	This value is set to non-null if the Connection Manager service has entered a suspended state. It is set back to null on entry to a non-suspended state or when the service stops. Values defined are N The Network type is undefined or is not one of VSAT, ISDN or ADSL X The network type is indeterminate following an incomplete switch operation S The main Service configuration is invalid D The current Dial mode configuration is invalid
CurrentDialParams	String	N/A	N/A	This is a comma separated string holding: Call ID, username, phone number, device type, device name and Port. Example: 49, h2000610010100A,01344123456,isdn,ISDN,ADSL1
LastConnection	String	N/A	N/A	This is a comma separated string holding: username, phone number, device type, device name, port, phonebook entry name, call ID and timestamp. Example: h2000610010100A,01234 567890,isdn,ISDN,ADSL,Data Centre,001,04/08/2005 06:31:01.001
LastDisconnection	String	N/A	N/A	This is a comma separated string holding the same data as Status but remains unchanged until the next disconenction. Example: X,Data_Centre,209,01/12/2005 00:02:37.261,C,R
RASConnectionState	String	N/A	N/A	Holds entries like: "Dialling" "Authenticating" "Connected" "Disconnected"

Table 62 Connection Manager Registry

4.1.3.r Interface with ADSL Diagnostic Monitor

The NT registry key [HKLM\Software\Fujitsu\POA\ADSLDiagnosticMonitor] is used to request connection state information. The following key value is defined:

FUJ00171956

Name	Type	Max size	Default value	Description
GetConnectionStatusFlag	DWORD	N/A	N/A	Flag set to 1 by CNIM to request data and to 0 by ADM when data available

Table 63 ADSL Diagnostic Monitor Registry

The NT registry key [HKLM\Software\Pathway Configuration\ CNIM\ADSLDiagnosticMonitor] is used to store connection state information. The following key values are defined:

Name	Type	Max size	Default value	Description
ConnectionState	DWORD	N/A	N/A	Connection state as an integer value
StatusTickCount	DWORD	N/A	N/A	Tick count when status data set
TimeOut	DWORD	N/A	5000	Timeout in milliseconds waiting for data from ADM

Table 64 CNIM ADSL Diagnostic Monitor Data

4.1.3.s CNIM NST Groups

These values are used by CNIM to determine its mode of operation.

[HKEY_LOCAL_MACHINE\SOFTWARE\ICL\Pathway Configuration\ CNIM\ NST_Groups]

Value	Type	Entry	Description
ADSL	String	"13"	ADSL Service type
FMRY	String	"03"	Frame Relay Service Type
ISDN	String	"01,04,05,06,07,08,09,10,11,12"	ISDN/Data Service Types
VSAT	String	"02"	VSAT Service Type

Table 65 CNIM NST Groupings

4.1.3.t CNIM Network Settings

These values are used by CNIM to display current network type

[HKEY_LOCAL_MACHINE\SOFTWARE\ICL\Pathway Configuration\ CNIM\ Network]

Value	Type	Entry	Description
"Type"	String	"ADSL" | "FMRY" | "ISDN" | "VSAT"	Network Type

Table 66 CNIM Network Settings

4.1.3.u Bandwidth Configuration Settings

Detailed bandwidth design is shown in 5.7.3.c

The bandwidth configuration settings shown below are used to set the payload sizes for the large and small pings. CNIM will use these values to set the payload for the two bandwidth pings.

The overall difference in the ping size is also stored in registry and CNIM will use this value in determining the bandwidth value.

[HKEY_LOCAL_MACHINE\SOFTWARE\ICL\Pathway Configuration\CNIM\Bandwidth]

FUJ00171956

Value	Type	Entry	Description
LargePayload_Bytes	DWORD	966	Payload in bytes for large ping
SmallPayload_Bytes	DWORD	32	Payload in bytes for small ping
PingDifference_Bits	DWORD	7680	Difference in ping size
MaxValue	DWORD	512000	Cutoff value to prevent excessive values being produced

Table 67 Bandwidth Configuration Settings

Related result codes are shown below.

[HKEY_LOCAL_MACHINE\SOFTWARE\ICL\Pathway Configuration\CNIM\Bandwidth\ResultCodes]

Value	Type	Entry	Description
P1<P2	DWORD	0	Ping 1 Round Trip Time(RTT) less than that for Ping 2 - Success.
P1_Failed	DWORD	1	Ping 1 failed
P2_Failed	DWORD	2	Ping 2 failed
P1_And_P2_Failed	DWORD	3	Both pings failed
MaxValueExceeded	DWORD	4	The calculated value exceeds the maximum possible bandwidth.
P2<P1	DWORD	10	Ping 2 Round Trip Time(RTT) less than that for Ping 1 - Fail.

Table 68 Bandwidth Result Codes

4.2 Interfaces Used

The following interfaces will be used:

- The NT Service Control Manager, SCM, will control the service.
- Win32 API is used to access NT resources, e.g. the NT registry.
- Eicon IDI gives direct access to the Eicon driver and may be used to monitor line state and to request indications of line events.
- Eicon DIAPI is used to manage Eicon card parameters
- Connection Manager registry data

FUJ00171956

5 DESIGN OVERVIEW

5.1 Service Definition

CNIM is an NT service with the following properties:

1) The service name is 'CNIM', and the display name is "CNIM".
2) The service is self-configuring. That is it can be created and deleted using a command line parameter, not a separate utility.
3) The service is run under the LocalSystem account on the outlet's gateway PC.
4) The service reports any errors and significant activity using the NT event log. The event log source name is "CNIM".
5) The service will be configured to start automatically.
6) It can be stopped and started using Service Control API functions (OpenService(), StartService(), ControlService()). It does not support pause and resume.
7) The service executable file will have an embedded version number resource to identify itself.

5.2 CNIM Service Design Overview

Requirement: See section 2.2.1

CNIM will be compiled as a single executable which will run as a service.

CNIM will link to the IDI interface using its own library comprising source code supplied by Eicon.

CNIM will link to the DIAPI interface and the DIAPI DLL will be installed with the service.

CNIM will link to the TuneableTrace DLL which is installed as part of the BI3 upgrade

5.2.1 Service Dependencies

CNIM is dependent on the RPC service for communication with the CNIM_API.dll. CNIM is also dependent on the VPN service in that WAN communication to the Data Centre is not possible without VPN running. On start up CNIM will check the status of both services and will not proceed until both are running.

CNIM is also dependent on the ADSL Diagnostic Monitor service and the Connection Manager service, whilst running in ADSL mode, to supply diagnostic data. CNIM may continue to run without these two services but will display a red error event.

5.3 Eicon Card Configuration Design Overview

Requirement: See section 2.2.7.

5.3.1 Card Parameter Storage

Eicon card parameters will be stored in registry. The parameters to be stored are explained in section 2.2.7.

5.3.1.a Phone Numbers and Network Service Type

Phone numbers and the Network Service Type, are supplied to the outlet via a CDF file. The file contents are processed by EiconConfig and placed in registry as shown in section 4.1.3.o., for use by CNIM.

FUJ00171956

5.3.1.b CHAP Passwords and User Ids

CHAP password and UID information is held in registry as shown in section 4.1.3.p.

The data network Inbound User ID and Password is configured into registry before CNIM is installed. It is the responsibility of CNIM to extract the existing ISDN inbound password from the card during installation. It is assumed at installation, that the card is configured to use the ISDN network. CNIM will store this password in registry and set the registry flag "Inbound_Stored" to 1 after storage.

CNIM will add the User ID stored in registry under "UID_Inbound_Data", to the set of inbound user Ids that the card will accept.

5.3.1.c Shorthold, Minimum Call Duration and CHAP Interval Times

These parameters are shown in section 2.2.7.a. These are supplied to CNIM during installation and CNIM uses them to modify the behaviour of the card, depending on the connection type required.

5.3.2 Card Parameter Application

Eicon card parameters will be applied via the DIAPI interface. This is a set of functions contained within the DIAPI DLL. CNIM will statically link to this DLL and so it must be present on all gateway platforms including satellite gateways, even though it can perform no function in the latter instance.

The Diapi ISDN interface for Windows NT allows a user to communicate with the ISDN network through a set of language functions via the Eicon communications adapter.

More detail on this is given in Appendix A9.

5.4 Network Service Type Design Overview

Requirement: See section 2.2.7.b

The network service type (NST) is passed to the outlet as part of the CDF file and is stored in registry. CNIM uses the NST to determine which table within the Call Plan applies to the outlet.

CNIM will run in one of three modes, ADSL, ISDN or VSAT. It will only react to those events that are appropriate for its current mode.

CNIM will retrieve the mode of operation from the Network Service Type and the NST_Groupings sections of registry.

When in ISDN mode CNIM will react to network events from those objects that receive indications from the IDI. These are described below.

When in ADSL mode CNIM will listen for registry notification of network status updates from Connection Manager.

In VSAT mode CNIM will simply rely on pinging the VPN Servers at regular intervals to determine network status.

5.5 CDF Data Storage Design Overview

Requirement: See section 2.2.8.

CDF data in this context applies to phone numbers only. These are stored in the map shown on the right (Phone Number from Registry) in the diagram below.

FUJ00171956

Four further maps are created for the four main service type groupings, namely FRIACO 1 and 2, Metered and Voice. These map the original numbers onto the FRIACO, metered and voice numbers for a particular outlet. Finally three Connection Type maps are created which map the Service Type maps to the Modes 1, 2 and 3 numbers required for each connection type.

CNIM will attempt to use the Mode 1 number at all times. Failing that it will move to Mode 2 temporarily. Should Mode 2 fail to work then the card will be configured with Mode 3 numbers

FUJ00171956

which, in practise, will be ISDN numbers.

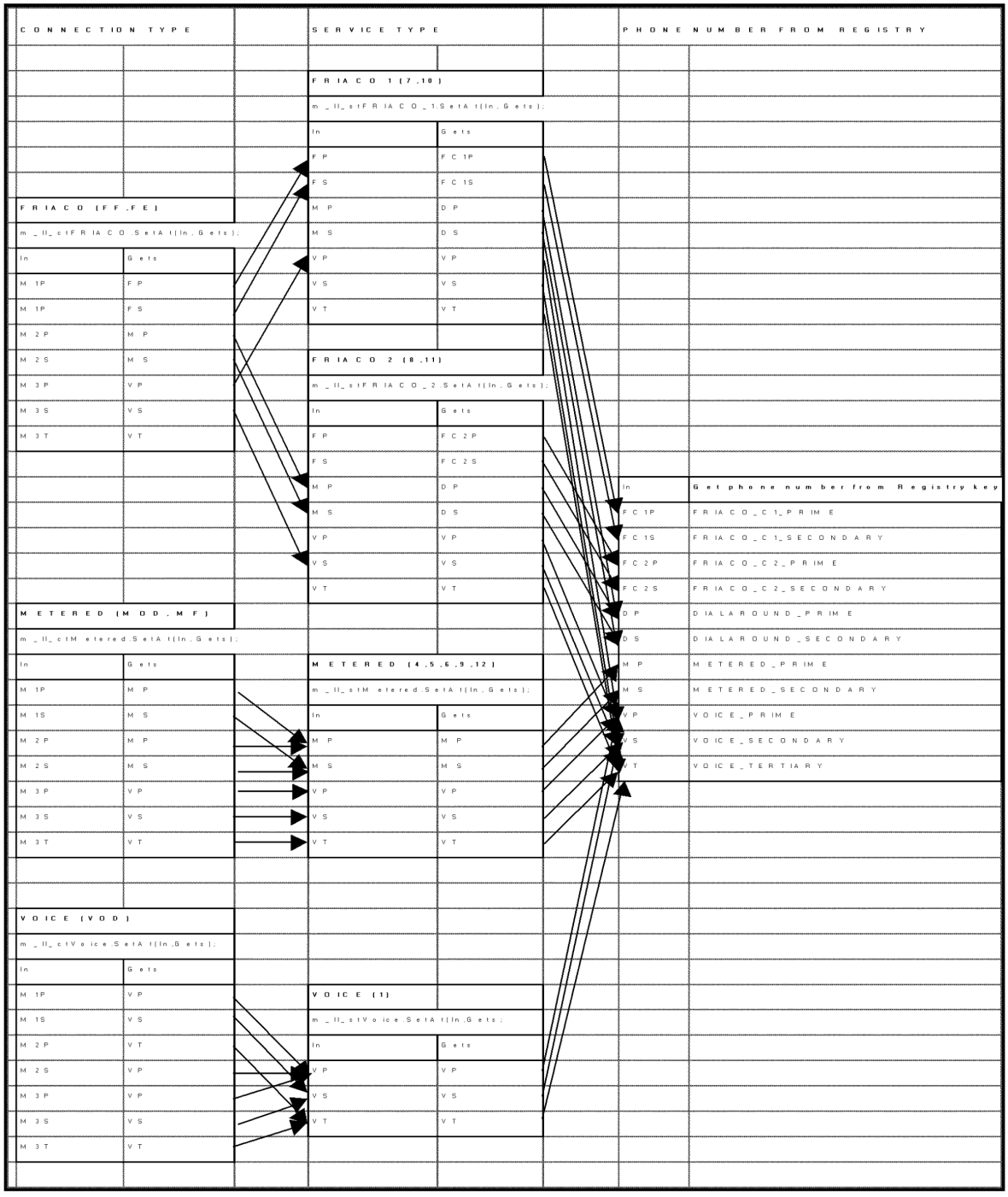

Figure 11 Telephone number mapping from Registry

Each connection type (FRIACO, Metered and Voice) has a maximum of six 7 telephone numbers which it can try to establish a connection to the data centre. These numbers are

FUJ00171956

grouped in order of priority into Mode 1 (M1P and M1S), the numbers to be tried first, Mode 2 (M2P and M2S), and Mode 3 (M3P, M3S and M3T) as is illustrated in the above diagram.

The above diagram is simplified in CNIM Version 2, in that only one number is applied per mode. Therefore the concept of a primary and secondary number per mode is not used. This is covered in section 5.13.1 and means that for the purposes of the above diagram only M1P, M2P and M3P numbers will be used.

5.6 Call Plan Design Overview

Requirement: See section 2.2.7.c

The Call Plan comprises a number of tables within a file, each table comprising one record for each day of the week. Each record comprises a number of elements which give the connection type required for a given period of the day. The time span of the element is given to the nearest minute.

CNIM creates a set of linked lists where the top most list comprises a set of tables. Each table comprises a list of days and each day contains a list of elements.

Call Plan management requires that for a given Network Service Type, date and time the appropriate element can be retrieved and from that element the required connection type determined. The Network Service Type is used as the index to the first list to determine the table in question. The day of the week determines which record in the table is required and the time of day is used to determine which element in the record is required.

Call Plan maps are created on service start up and when the Reset function is called.

The Call Plan file name contains a date and time as shown in section 2.2.7.c.4. CNIM is capable of determining which is the newer file should more than one Call Plan file be present in the directory. Older files will be renamed with the suffix ".OLD"

5.7 QOS Logging Design Overview

Requirement: See section 2.2.9

Call logging is required in order to ensure that SLA's are met and to help diagnose problems on the network.

5.7.1 Call Logging - ISDN

In order to create the call logs, CNIM must be aware of the state of the line at all times. For ISDN/Data network, this is done via the IDI interface.

5.7.1.a The IDI Interface

The IDI is kernel mode interface used by drivers to access the ISDN adapter cards. Within the IDI several adapter cards of the same or different type can be registered at the same time.

On top of the IDI other drivers as NDIS, CAPI or ECBIOS can be loaded.

All communication between the application and the IDI is related to 8-bit Ids. The Ids identify the entity within the ISDN protocol the application is using. When a new ID is assigned the related entity is configured at the same time. The global ID defines what type of entity shall be assigned.

Three global Ids are currently defined:

0x00 Signalling entity

FUJ00171956

0x20 Network Layer entity

0xe0 Management entity

A simple application using a network layer protocol on one B-channel typically assigns two Ids. A signalling entity to control call establishment and release and a network layer entity for the network layer protocol. The network layer entity is typically assigned as soon as a call is established. As part of the configuration the network layer protocol is selected and the related signalling entity is specified at this time.

CNIM is primarily concerned with using the IDI at the management level although future work may involve the use of signalling entities.

The management interface is used to access (read and write) internally available information by a client registered with the IDI. Additionally, specific actions or commands can be executed. The internally available information can be divided into the following categories:

- Version information about the driver
- Configuration information (Configured ISDN numbers, MAC addresses...)
- Statistics information (Number of packets sent/received, error counters, ...)
- Status information (State variables, number of active calls, ...)
- XLOG Trace information

Standard IDI mechanisms (REQUESTs, INDICATIONs, Information Elements) are defined to access the management information. Due to this IDI access mechanism, a generic tool can be used to handle the management information structures. Within this tool, no knowledge of any driver/protocol specifics is required.

The management information is structured like a directory tree. Each variable or node is identified by its path and name. A path contains node names (separated by a backslash '\'), followed by the specific variable or node name (similar to a file system). Each node can contain further nodes or variables.

A node can be read and returns the next deeper level of the directory tree. A variable can be read, written or marked as 'Notify on change' depending on its attribute. Actions or commands appear as 'Executable Variables' without a value that can be started with a specific request.

CNIM uses the three parameters shown in Table 69 to monitor the line state. CNIM is able to request notification of changes to Line State and Layer 2 State. CNIM must proactively request the latest value of Cause Code and may request the latest value of any other parameter.

Parameter	Change Notification Possible	State	Description
Line State	Yes	Unknown	Line State is Unknown
Line State	Yes	Idle	Line State is Idle
Line State	Yes	Connected Out	Line State is Connected Out
Line State	Yes	Connected In	Line State is Connected In
Layer 2 State	Yes	Unknown	Layer 2 State is Unknown
Layer 2 State	Yes	Idle	Layer 2 is Idle

FUJ00171956

Layer 2 State	Yes	Up	Layer 2 is Up
Cause Code	No	String Value	Reason for Call Closure

Table 69 IDI Parameter Description

5.7.1.b Call Activation and Closure

In order to determine that a call has been initiated CNIM requests notification of the Layer 2 State. Layer 2 State will always change on a call attempt, even if the network cable has been disconnected from the Eicon card.

On receiving this notification CNIM stores the initial time of the call. It will then request the Line State which will give the call direction. This information determines which monitor file will be used to store this call record. If a monitor file of the correct type does not exist for that day, CNIM will create one and store the initial record which will show the call as being "open". If the required monitor file does exist CNIM will parse the file to check that a previous record has not been left "open". If any record has been left open it will be changed to "unknown". This record should be disregarded for the purposes of QOS analysis.

CNIM will use the notification of Line State going Idle to determine when the call is closed. The call record in memory will be updated with the time of call closure, call duration and call result. The relevant monitor file will be parsed to find the equivalent open record and the record will be overwritten with the updated record.

In the event that the call has gone over midnight (UTC) then CNIM will record the call closure in the Monitor file for the day of call closure. Therefore this file will contain a record for a call that started on the previous day. The original open record in the previous days file will be left unchanged. This means that a monitor file may only have one open record and, if present, it must be the last record in the file.

CNIM will use the same mechanism to create and update the summary file for each day, although each summary file will only contains data for the day of that file.

5.7.2 Call Logging - VSAT

In order to determine the connection state, CNIM is only able to ping the data centre. Successful return of the ping indicates that the call is open, whilst ping failure indicates that the call is closed.

5.7.3 Call Logging - ADSL

Call logging under ADSL primarily will use the same technique as VSAT of periodically pinging the data centre to determine that comms are available. However CNIM may also determine the connection state using the following interfaces:

1) ADSL Diagnostic Monitor Registry
2) Connection Manager Registry

These are described in the following sections

FUJ00171956

5.7.3.a ADSL Diagnostic Monitor Interface

CNIM 3 will interface to the Conexant card via the ADSL Diagnostic Monitor service. This will allow CNIM to extract low level diagnostic connection data from the card for QOS record purposes.

In the event that CNIM receives notification from Connection Manager that the ADSL connection has been dropped it will request the latest connection status information from the ADM service. This will be done by setting a registry flag, in the ADM area of registry, that will cause the ADM to place the latest low level connection state in the CNIM area of registry. After setting the ADM "GetConnectionStatusFlag" to 1, CNIM will wait to receive notification that the connection state has been updated. It will check that the "GetConnectionStatusFlag" has been reset to 0 by ADM as a sign that the data has indeed been updated. CNIM will incorporate a timeout in its wait loop in the event that the ADM does not respond to the request.

The registry areas used for this process are described in section 4.1.3.r

5.7.3.b Connection Manager Interface

These details are taken from Connection Manager detailed design, [Ref 15]

Registry details are given in section 4.1.3.q

The State\DayD registry value is set to one on entry to Day D dialling mode, and to zero on exit from that mode. This flag is intended to allow CNIM to distinguish normal connections from modem recovery connections.

The State\Suspended registry value is updated whenever the service leaves or enters the Suspended state. It indicates whether or not the service is suspended, and if so, the reason for suspension.

The State\Status registry value is updated each time the connection state changes, allowing CNIM to determine the connection state. Note that there is a configured "settling" delay between RAS reporting "connected" and the Connection Manager reporting "connected".

Other components in the system need to know the current connection state. Connection Manager writes status information to the Status value under the key HKLM\SOFTWARE\Fujitsu\POA\ConnectionManager\State, which other applications can monitor using the Win32 registry change notification API.

The status information is provided as a comma-separated list. The first field of the list identifies a particular state and the remaining fields give extra information appropriate to the state. These fields are described in detail below.

Where status information relates to a particular connection, the phonebook entry name is given. Since it is likely that consecutive connection attempts will use the same phonebook entry, a sequence number is associated with each connection attempt, and that number is included in the state information. The sequence number is held in the registry, and is therefore persistent across service instances. It is initialised to zero when Connection Manager is installed, and is incremented before each dial attempt[3].

The State key has three other values under it: a flag that indicates Day D dialling, a flag that indicates suspension of the service, and a heartbeat value which is updated periodically. Note

[3] This value is a DWORD, so is unlikely to wrap in the lifetime of any particular Gateway.

FUJ00171956

that an application can only monitor a registry key and not individual values, so a change to any of the values under the State key can cause a change notification. Monitoring applications may need to keep previous values to determine what has changed. The heartbeat value allows an application to notice if Connection Manager is not in its normal dialling cycle.

The Suspended flag can have one of the following string values:

Suspended Value	Description
null	The service is not suspended
D	The default dial mode configuration is invalid
N	The Network Type is invalid or undefined
S	The service configuration is invalid
X	The last network type switch has not completed

The first field of the Status value is a single letter, indicating a connection state, as shown in the following table.

Connection State	Description
N	Not connected. There is no additional information with this status. *Not Connected* is set when: - the service enters the idle state - the service enters the suspended state at start-up because of an invalid or indeterminate network type - the service enters the suspended state on the first attempt to read the top-level configuration data - the dial mode configuration is invalid on the first entry to *PrepareToDial* and the service is suspended - no existing connection is adopted on the first entry to *PrepareToDial* In other words, *Not Connected* is only set as an initial state. Once the Connection Manager has attempted a connection, the status will not show *Not Connected* until the service is restarted, but will always be one of *Dialling, Failed to connect, Connected* or *Disconnected*. Example: N
D	Dialling. The dialling state is set just before dialling starts. The second field names the phonebook entry being dialled. The third field is a sequence number. The fourth field is the UTC time that dialling started. Example: D,Data_Centre,397,04/08/03 15:28:37.292
C	Connected. The connected state is set after a RAS connection has been established for the configured Settle time. The second field names the phonebook entry. The third field is

FUJ00171956

	the sequence number. The fourth field is the UTC time at which this state was reported i.e. the end of the settle period. Example: C,Data_Centre,397,04/08/03 15:28:52.177
F	Failed to connect. The failed to connect is set if a dial attempt fails. The second field names the phonebook entry. The third field is the sequence number. The fourth field is the UTC time that the failure was detected. The fifth field may be R, indicating an error returned from RasDial, or C, indicating that Connection Manager hung-up the connection. If the fifth field is R, the sixth field gives the RAS error as an 8-digit hexadecimal number. If the fifth field is C, The sixth field can be one of T = timed out D = interrupted by Day D dial request R = interrupted by a Reset request S = interrupted by Service Stop request B = interrupted by Black Hole error Examples: F,Data_Centre,502,12/08/2003 13:03:07.953,R,00000279 F,Data_Centre,503,12/08/2003 13:05:43.288,C,S
X	Disconnected. The disconnected state is entered if an established connection becomes disconnected. The second field names the phonebook entry. The third field is the sequence number. The fourth field is the UTC time that the disconnection was detected. The fifth field may be R, indicating an error returned from RAS via RasGetConnectStatus, or C, indicating that Connection Manager hung-up the connection. If the fifth field is R, the sixth field gives the RAS error as an 8-digit hexadecimal number. If no error is associated with the disconnection, this field will be 00000000. If the fifth field is C, The sixth field can be one of D = disconnected by Day D dial request R = disconnected by a Reset request S = disconnected by Service Stop request B = disconnected by Black Hole error Examples: X,Data_Centre,397,04/08/03 15:37:19.361,R,00000276 X,Data_Centre,398,04/08/03 15:44:21.498,C,S

5.7.3.c Bandwidth Calculation - ADSL Only

Bandwidth measure

Bandwidth will only be measured at ADSL connected outlets whilst there is an ADSL connection to the data centre. This data will be used to ensure that sufficient bandwidth is

FUJ00171956

available from the ADSL network for Post Office requirements and to determine if any particular outlet has too little bandwidth available.

The standard ping command will be used by CNIM to determine the bandwidth available to the data centre. In order to ensure meaningful results from the ping command, which by definition has a small payload, a number of factors need to be considered within the calculation:

- Latency

The available bandwidth will be determined by measuring the responses times of two ping commands, of different sizes, targeted at the data centre, submitted consecutively. As the ping requests are submitted consecutively the latency element of the two response times will be the same, allowing it to be removed from the final bandwidth calculation.

- Comms headers

A ping request is made up of the payload (as defined on the command line) and a number of headers:

  - ICMP
  - IP
  - VPN
  - VPN IP
  - PPP frame
  - VCMUX

In order to calculate the available bandwidth CNIM will need to take these headers into account, therefore along with the configuration information detailing the two ping payload sizes (in bits) a further value will be supplied which will define the actual difference in ping sizes in bits, again including headers.

- ATM cell mapping

The ping request will be split up into a number of ATM cells, 53 bytes in size. Of the 53 bytes, 5 bytes hold ATM header information, leaving 48 bytes to hold the payload, including higher level protocol headers. It will be necessary to ensure that the ping payload size plus comms headers, aligns as close as possible to an ATM cell boundary.

The frequency and sizing information will be included as registry parameters. The frequency of the bandwidth test will randomised, so as to avoid all outlets checking the bandwidth at the same time. The following table defines the ping sizes and frequency parameters that will be included in the NT registry, see section 4.1.3.u

These need to be confirmed (they will change as they do not include all the overheads).	
Small ping size	32 bytes
Large ping size	922 bytes
Difference in bits	7680 bits
Average time between	5 minutes

FUJ00171956

bandwidth checks

Due to the very small ping round trip times being measured it will be necessary to use the NT high resolution timer. The high resolution timer return 64 bit values therefore all calculations will need to take this into account. The bandwidth can be calculated as follows:

FUJ00171956

$$\frac{\text{Time difference in milliseconds}}{\text{Ping size difference in bits X 1,000,000}}$$

Proof of formula:

Size(small) = VPN Header + IP Header + Size small ping + ATM Cell Overheads

Size(large) = VPN Header + IP Header + Size small ping + ATM Cell Overheads + Extra Size for large (including ATM overhead)

Size(diff) = Size(large)-Size(small) = Extra Size for large

Elapsed(small) = Latency + Size(small)/Bandwidth

Elapsed(large) = Latency + Size(large)/Bandwidth

Elapsed(diff) = Elapsed(large)-Elapsed(small) = (Latency + Size(large)/Bandwidth) - (Latency + Size(large)/Bandwidth)

Elapsed(diff) = (Size(large)-Size(small))/Bandwidth = Size(diff) / Bandwidth

Bandwidth = Elapsed(diff) / Size(diff)

5.7.1.a.1 Bandwidth Pinging

CNIM uses the test thread to create the test ping. This same thread will carry out the bandwidth ping and the bandwidth calculation and pass the result to the logger thread.

The logger thread will be responsible for inputting that data into the bandwidth file.

5.7.1.a.2 Bandwidth Return Codes

CNIM is required to provide a set of codes as the last field in the bandwidth record. These codes are defined in Table 68. Note that a success code of "0" will only be given if the round trip time for ping 1 is less than that for ping 2 and the resultant calculated bandwidth value does not exceed the threshold specified in registry. If the threshold value is exceeded then CNIM will set the bandwidth to 0 and output the appropriate code as specified in registry.

5.8 Dial Back Design Overview

Requirement: See section 2.2.10

If the call into CNIM is an external call, i.e. from the Data Centre (via the ISDN Eicon card), the Eicon card is pre-configured to 'Reject' the call. The Eicon IDI interface will notify CNIM that a call occurred. On receipt of this notification, CNIM logs the reject call information, and initiates a call to the Data Centre, i.e. 'pings' to the VPN servers.

CNIM is unaware of who called the Outlet, (Riposte, Tivoli or Support), therefore it is the responsibility of the calling function to 'wait' and 'try again'. If the call from CNIM to the Data Centre has been successful, a tunnel will have been established to the appropriate LNS router, and the Summary router notified of the 'route' to the Outlet. The calling function on attempting the call again, will utilise this route/ tunnel established by the in-bound call from the Eicon card.

A 'Call Reversal' will only be sent to PO Outlets that are currently not connected to the Data Centre. This may include Outlets that are deemed to be on a permanent connection (FRIACO or Metered) but where the connection is currently down for whatever reason. The CNIM ascertains the outlets network service type by reading the appropriate Registry entry. The

FUJ00171956

number to be dialled in order to establish a call to the Data Centre is dependent on the day of the week, time of day, and what connection type should be invoked for the outlet at this time of day.

If the call to the Data Centre is successful, and the defined network connection type, is defined as a permanent connection for FRIACO or Metered access, then the 'Current' network connection type [CNET2], will be set to 'P' (permanent connection). Whereas if the first two FRIACO calls fail but the third call (Dial–Around), by the Eicon driver is successful or that the Outlet is deemed to be Metered Outlet then [CNET2] is set to 'M' (metered connection). CNIM will only update the Registry entries after the Eicon card has successfully established a call or failed in the attempt. CNIM will ascertain the outcome of the attempted call, by the fact that the IDI reports the status of the attempted call, i.e. the successful number 'called' or the Error code on a failed call. See Figure 12:

FUJ00171956

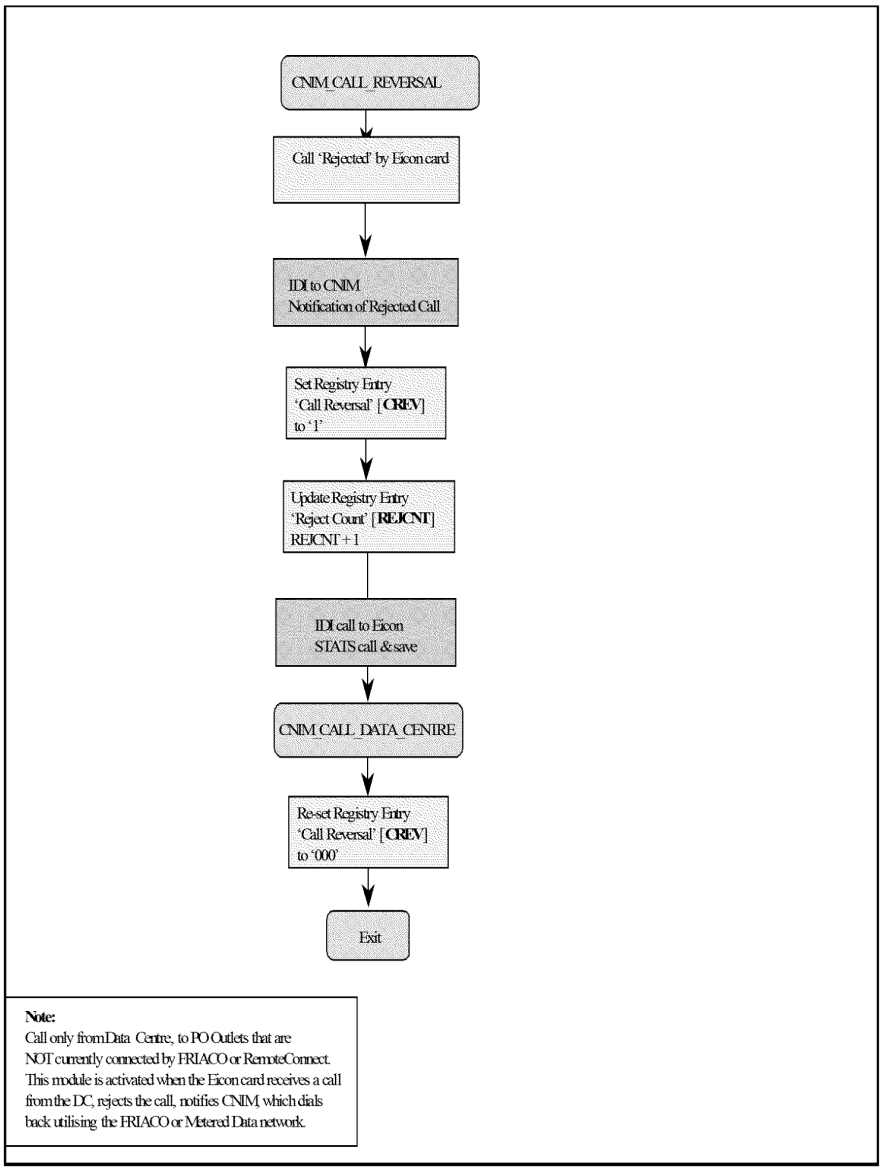

Figure 12 Call Reversal

FUJ00171956

5.9 Branch Resilient Network ISDN/GSM Switch Process

The Switch Network Use command is invoked by CNIM when a change between normal and fallback network use involves a reboot i.e. when the primary network type is NDIS ISDN. Reconfiguration is necessary because the Gateway's IP address is the same for both primary and fallback networks. When the primary network and fallback network(s) are using RAS the remote server provides the IP address, so there is no conflict. When NDIS ISDN is in use the IP address is set locally, and would conflict with the fallback RAS connection if not changed. Changing the IP address on the Eicon card requires a reboot.

The command syntax is

```
CmCmd SWITCH_NETWORK_USE TO=(NORMAL|FALLBACK)
```

It updates the platform configuration so that, on reboot, the platform uses either its normal or fallback network, and then signals the Desktop application to initiate the reboot.

Success or failure of the command, as for all the CLI functions, is indicated by ERRORLEVEL. However, the command is designed to be called from CNIM, and part of the command's functionality is to stop the CNIM service. The result is therefore also recorded in the registry value SwitchNetworkUseResult for CNIM to check after the reboot.

The table below shows Switch process parameters that are relevant to CNIM.

[HKEY_LOCAL_MACHINE\SOFTWARE\Fujitsu\POA\ConnectionManager\Switch]		
Value	**Type**	**Contents**
SwitchNetworkUseResult	DWORD	0 = Success 999 = Failure
IpDummy	String	0.0.0.0
IpLive	String	IP address set by SYSMAN or CNIM
EiconIpAddressRef	String	Registry key and value in which to set the IP address for the Eicon card. HKLM\SYSTEM\CurrentControlSet\Services\Diehl_DINDIS7\Parameters\Tcpip,IPAddress

Table 70 Connection Manager Switch Registry

The failover process on an ISDN outlet (FRIACO, Metered or Voice) whereby the gateway switches to GSM will be as follows:

1) CNIM will detect that the GSM command button has been pressed.
2) CNIM will determine that the outlet is an ISDN outlet.
3) CNIM will set a persistent flag in registry indicating that the switch to GSM is required. This is done by setting the "Connection_Type_Required" flag to GSM together with a timestamp.

FUJ00171956

5.10 Branch Resilient Network Interface with Connection Manager

CNIM will set the required RAS connection type within Connection Manager registry using the DialMode value:

[HKEY_LOCAL_MACHINE\SOFTWARE\Fujitsu\POA\ConnectionManager]
DialMode = string

Where the value of DialMode is taken from the following table

DialMode	Description
"Normal"	Connect using normal behaviour for the Network Type i.e. dialling on ADSL and idling on NDIS
"Idle"	Stop dialling even when the Network Type is ADSL
"Fallback_ISDN"	Connect using ISDN over RAS
"Fallback_GSM"	Connect using GSM over RAS

Table 71 DialMode Description

These strings will be stored in CNIM registry under the following key and values:

[HKEY_LOCAL_MACHINE\SOFTWARE\ICL\Pathway Configuration\CNIM\Connection]	
Value	**Contents**
RAS_ADSL	"Normal"
RAS_ISDN	"Fallback_ISDN"
RAS_GSM	"Fallback_GSM"
RAS_DROP	"Idle"

Table 72 DialMode Strings in CNIM Registry

Note that the heartbeat only runs when dialling or connected - it doesn't run in the idle state and that changing the dial mode always hangs up any current connection.

Use of the Reset flag below will cause Connection Manager to attempt to connect with the required connection type.

[HKEY_LOCAL_MACHINE\SOFTWARE\Fujitsu\POA\ConnectionManager\Triggers]
Reset = dword 00000001

The underlying network type for Connection Manager, is set using the NetworkType value below, this value will not change even in the event of a different connection type being required.

[HKLM\SOFTWARE\Fujitsu\POA\ConnectionManager]
NetworkType = string

Where the value of NetworkType is taken from the table below:

FUJ00171956

NetworkType	Description
"ADSL"	ADSL Gateway.
"VSAT"	VSAT Gateway.
"ISDN"	ISDN Gateway.
"indeterminate"	Gateway failed to switch correctly

Table 73 Connection Manager Network Types

Note that CNIM will be responsible to determining that any changes to network connectivity as registered by Connection Manager, are indeed of the right connection type as requested by CNIM. It will do this by determining that any change in connectivity occurred after the new connectivity was requested by CNIM. At present Connection Manager inputs the number of the phonebook entry in use, into registry.

Currently on ADSL outlets CNIM uses Connection Manager registry data as input to the QOS records related to each call. However as far as Counter Call Scheduler is concerned CNIM uses its current ping status of success or fail, to determine whether comms are available or not. To this end CNIM will not request Connection Manager to change connection type unless all test pings have failed.

5.10.1 RAS Connection Type Information

CNIM can determine the type of RAS connection in use currently, by Connection Manager, by use of the registry value **CurrentDialParams** which is a comma separated string holding:

call id, username, device type, device name, and port.

CNIM can determine the last connected type using the registry value **LastConnection** which is the same as CurrentDialParams but with a timestamp, phonebook entry name and phone number, added.

These values are also described in Table 62 and examples are shown below:

CurrentDialParams=49,h2000610010100A,0000,isdn,ISDN,ADSL1,
LastConnection=h2000610010100A,0000,isdn,ISDN,ADSL1,Data_Centre,48,04/08/03 15:28:37.292

Table 75 gives details of the phonebook entries to be used. In particular CNIM requires the entry for the port value in order to determine the connection type in use. The values these will be compared against will be stored in registry using the values shown in Table 74.

CNIM will check whether the string for the port value from Connection Manager contains one of the strings shown in Table 74.

[HKEY_LOCAL_MACHINE\SOFTWARE\ICL\Pathway Configuration\CNIM\Connection]		
Value	**Type**	**Contents**
Con_Man_Port_ADSL	String	ADSL1
Con_Man_Port_ISDN	String	ISDN2
Con_Man_Port_GSM	String	COM11

FUJ00171956

Con_Man_Port_PSTN	String	COM10

Table 74 Port Contents for Connection Types

Phonebook Entry	Device Type	Device Name	Port	UserName	Phone Number as issued
Bootle_Boot_ISDN	isdn	DIWAN	ISDN2	hFAD0010199	GRO
Bootle_Boot_PSTN	modem	Courier V.Everything External	COM10	hFAD0010199	
Wigan_Boot_ISDN	isdn	DIWAN	ISDN2	hFAD0010199	
Wigan_Boot_PSTN	modem	Courier V.Everything External	COM10	hFAD0010199	
Bootle_Day_D	modem	Courier V.Everything External	COM10	hFAD0010100B	
Bootle_GSM	modem	Standard 19200 bps Modem	COM11	hFAD0010100B	
Wigan_Day_D	modem	Courier V.Everything External	COM10	hFAD0010100B	
Wigan_GSM	modem	Standard 19200 bps Modem	COM11	hFAD0010100B	
Data_Centre	isdn	ISDN	ADSL1	hFAD0010100A	
Bootle_Fallback_GSM	modem	T-ModemCOM	COM11	hFAD0010100C	tbs
Bootle_Fallback_ISDN	isdn	DIWAN	ISDN2	hFAD0010100C	tbs
Wigan_Fallback_GSM	modem	T-ModemCOM	COM11	hFAD0010100C	tbs
Wigan_Fallback_ISDN	isdn	DIWAN	ISDN2	hFAD0010100C	tbs

Table 75 Connection Manager Phonebook Details

5.11 Determination of Failure Code

A failure code will be associated with each failed call. This code will be output to the relevant QOS record and to Counter Call Scheduler. When running in VSAT mode CNIM can only use codes defined for ping failure. In ISDN mode CNIM will use network cause codes primarily and will revert to Fujitsu defined codes of no error cause code is received.

When running as ADSL, CNIM will use error values from Connection Manager if any are available. If Connection Manager indicates no error and CNIM will query ADSL Diagnostic Monitor for an error value. If no error is found and the ping has failed CNIM will use the Fujitsu error codes.

Mode	Primary Source	Secondary Source	Tertiary Source

FUJ00171956

VSAT	Fujitsu Defined Error Codes	None	None
ISDN	Network Codes Via Eicon API	Fujitsu Defined Error Codes	None
ADSL	Connection Manager Registry	Conexant via ADM Registry	Fujitsu Defined Error Codes

Table 76 Determination of Failure Code

ISDN cause codes are shown in Appendix A4, RAS codes in Appendix A5, Connection Manager codes are given in Appendix A6, Fujitsu codes are given in Appendix A7 and CNIM codes are given in Appendix A8

5.11.1 Cause Code Ranges

Interface	Code Range	Description
Eicon	0x00nn	ISDN Cause Codes in 2 byte format. See Appendix A4
Defined	0x01nn	Fujitsu defined codes.
RAS	0x02nn	Codes mapped from the Win32 RAS API
Conexant	0x03nn	Codes mapped from data returned by ADSL Diagnostic Monitor
Connection Manager	0x04nn	Codes mapped from data returned by Connection Manager
CNIM Defined	0x05nn	CNIM State Codes
RAS	0x06nn	RAS specific error codes from Microsoft

Table 77 Cause Code Ranges

5.11.2 Eicon Cause Codes

Cause Codes are returned to the Eicon card on call closure and are a numeric indication of the reason for the call closure.

ISDN cause codes 0x00, 0x80 and 0x90 are considered successful codes in that no communication failure has occurred. These successful codes are stored in registry under the key and variable shown below:

For CNIM version 3, single byte ISDN cause codes will be mapped to 2 byte codes for consistency with other codes being output.

[HKEY_LOCAL_MACHINE\SOFTWARE\ICL\Pathway Configuration\CNIM\Live]

"Successful_Cause_Codes"="0000,0080,0090,0100,0200,0300,0400,0412,0413,0422,0423,0500,0600"

Any other cause code value will cause CNIM to consider that the call has failed.

FUJ00171956

5.12 Engineers Button, Design Overview

An Engineers screen will be available to both the Engineer and the Post Master. It will contain three buttons as well as connection status information. The three buttons are listed below:

1. Initiate Connection
2. Test Connection
3. Drop Connection

These buttons will map directly to three DWORD values within CNIM registry as shown below:

[HKEY_LOCAL_MACHINE\SOFTWARE\Fujitsu\POA\DesktopApplication\NetworkResilience\Triggers]			
Value	**Type**	**Possible Entries**	**Description**
Connection	DWORD	0, 1, 2, 3	Value is the mode number, 0 is idle.
Drop	DWORD	0, 1	1 = Drop
Test	DWORD	0, 1	1 = Test
RebootStatus	DWORD	0, 1,2,3,4,5,99	Values set by CNIM or the Engineers App, see the following table.
RebootNow	String	Any	"Y" = Reboot now

Table 78 Engineers Button Trigger Registry

The values Connection, Drop and Test are set by the Button App. and are transient in that any change in value will be read by CNIM and the value reset to zero. The Test button will be set to zero at the end of the test.

The "Initiate Connection" button will lead to further options allowing a choice of network type by the user. The user may choose Primary, Secondary or Tertiary modes and these will put the values 1, 2 or 3 in the Connection value.

If the user wishes to drop the connection then the value of DROP is set to 1.

The RebootStatus value is used in the following way.

1) The user requests a certain connection type.

2) If CNIM determines that a reboot would be required it will put the RebootStatus value to 1

3) If the Engineers App. see the value 1 it offers the user the option to continue with the reboot or to cancel the change of connection.

4) If the user chooses to continue with the reboot then RebootStatus is set to 3.

5) If the user cancels the reboot then RebootStatus is set to 4.

6) If RebootStatus goes to 3 CNIM will set it to 5 indicating that it is about to call the Switch process.

FUJ00171956

7) On reboot CNIM will check the value of RebootStatus to determine whether it last requested a reboot. It will then set it to zero.

8) If CNIM calls the Switch package then the RebootNow flag is set to "Y" by the Switch package to indicate that the Engineers App. should initiate a reboot.

FUJ00171956

5.12.1 BNR Static Data

The following table is used to store Reboot Static data for interaction with the Engineers App. and the parameters to be given to the Switch package when switching between NDIS and GSM backup.

It also contains the path to the Network Resilience area of registry.

[[HKEY_LOCAL_MACHINE\SOFTWARE\ICL\Pathway Configuration\CNIM\Branch_Network_Resilience]			
Value	**Type**	**Possible Entries**	**Description**
RebootRequired	DWORD	1	CNIM indicates that a reboot will be required
RebootNotRequired	DWORD	2	CNIM indicates that a reboot will not be required
RebootCancelled	DWORD	4	Engineers App indicates that the change of connection has been cancelled by user, (Cancel).
RebootAuthorised	DWORD	3	Engineers App indicates that the change of connection has been uathorised by user, (OK).
RebootingNow	DWORD	5	CNIM indicates that it is rebooting. This is for CNIM internal use
RebootCleared	DWORD	0	Default value, no action
RebootError	DWORD	99	An error has been detected following the reboot. Engineers App may indicate this to the user.
Switch_Command	String	"C:\\PathwayNetwork\\ConnectionManager\\CmCmd.exe"	Path to the Switch application.
Switch_To_ISDN_Parameters	String	"SWITCH_NETWORK_USE TO=NORMAL"	Parameters to give to the Switch application to switch to ISDN (NDIS).
Switch_To_GSM_Parameters	String	"SWITCH_NETWORK_USE TO=FALLBACK"	Parameters to give to the Switch application to switch to GSM(RAS).
ButtonAppRegRef	String	"SOFTWARE\\Fujitsu\\POA\\DesktopApplication\\NetworkResilience"	Path to the first part of the registry Key name used by the Desktop. This should contain the subkeys: ConnectionState History Modes State Triggers.

Table 79 BNR Static Configuration Data

FUJ00171956

5.12.2 Network Resilience State

In addition to the Trigger values the following State values are used by the Engineers App.

The DWORD CurrentMode will be set to 0,1,2 or 3 by CNIM to indicate the current mode. 0 means idle.

CNIM will check the time that the required mode was last set by a button press. In general if it was before the current Call Plan period then CNIM will revert to the default mode which would usually be ADSL. However this behaviour will vary for an NDIS outlet which has rebooted to GSM.

[HKEY_LOCAL_MACHINE\SOFTWARE\Fujitsu\POA\DesktopApplication\NetworkResilience\State]			
Value	**Type**	**Possible Entries**	**Description**
CurrentMode	DWORD	0,1,2,3	This is the current BNR mode of operation. 0 = Idle 1 = Mode 1 2 = Mode 2 3 = Mode 3 Set by CNIM when the DialMode string for Connection Manager is changed by CNIM or after a successful reboot.
RequiredMode	DWORD	0,1,2,3	Set by CNIM when an InitiateConnection button is pressed.
BootedNetworkType	String	NDIS | RAS	Set by CNIM on start up to store the network type on CNIM start based on Eicon card IP address.
ModeChangeTime	String	25/07/2005 09:00:24:039	UTC time for last change. Used by CNIM to determine if the last button press is still valid, i.e. within the current Call Plan period.
GsmSignalStrength	String	Monitor inactive Other strings, see Connection Manager LLD	Displays GSM signal strength.

Table 80 Branch Network Resilience - State Information

FUJ00171956

5.12.3 Network Resilience Modes

CNIM maintains the mode values for a particular outlet. The Engineers App. will use the values stored here to determine which connection types are possible. These will then be used to determine the content of the "Connect" page of the Engineers App.

[HKEY_LOCAL_MACHINE\SOFTWARE\Fujitsu\POA\DesktopApplication\NetworkResilience\Modes]			
Value	**Type**	**Possible Entries**	**Description**
1	String	"ADSL" "ISDN" "GSM" "NDIS" "VSAT"	This is set by CNIM for the particular outlet, Ie for NST 14, Mode 1 would be ADSL
2	String	"ADSL" "ISDN" "GSM" "NDIS" "VSAT"	This is set by CNIM for the particular outlet, Ie for NST 14, Mode 2 would be ISDN
3	String	"ADSL" "ISDN" "GSM" "NDIS" "VSAT"	This is set by CNIM for the particular outlet, Ie for NST 14, Mode 3 would be GSM

Table 81 Mapping Mode to Connection Type

FUJ00171956

5.12.4 Network Resilience History

CNIM maintains the History values for a particular outlet. The Engineers App. may incorporate the string held in these values, e.g. "ADSL" into the string used to open a particular registry key for example:

[HKEY_LOCAL_MACHINE\SOFTWARE\Fujitsu\POA\DesktopApplication\NetworkResilience\ConnectionState\ADSL]

which would hold state information for the ADSL connection type.

[HKEY_LOCAL_MACHINE\SOFTWARE\Fujitsu\POA\DesktopApplication\NetworkResilience\History]			
Value	**Type**	**Possible Entries**	**Description**
1	String	"ADSL" "ISDN" "GSM" "NDIS" "VSAT"	This is set by CNIM for the particular outlet, Ie for NST 14, Mode 1 would be ADSL
2	String	"ADSL" "ISDN" "GSM" "NDIS" "VSAT"	This is set by CNIM for the particular outlet, Ie for NST 14, Mode 2 would be ISDN during core hours.
3	String	"ADSL" "ISDN" "GSM" "NDIS" "VSAT"	This is set by CNIM for the particular outlet, Ie for NST 14, Mode 3 would be GSM during core hours.

Table 82 Mapping History to Connection Type

CNIM will only respond to the Drop and Test buttons where marked "yes" in the table below. It will not be possible to test or drop the ISDN connection on an ISDN outlet. Changing connection type on an ISDN outlet will lead to a visible warning that a reboot will be required.

Service Type	**NST 1,4,7,9 = ISDN**		**NST 2 = VSAT** **NST3 = Frame Relay**	**NST 13 = ADSL**		**NST 14 = ADSL + ISDN**		
Current Connection	**ISDN[1]**	**GSM**	**VSAT or Frame Relay**	**ADSL**	**GSM**	**ADSL**	**ISDN[3]**	**GSM**
Test Button Available	No	Yes	No	Yes	Yes	Yes	Yes	Yes
Drop Button Available	No	Yes	No	Yes	Yes	Yes	Yes	Yes
Initiate Connection of given Type	GSM[2]	ISDN/ GSM[2]	None	ADSL/ GSM	ADSL/ GSM	ADSL/ ISDN/ GSM	ADSL/ ISDN/ GSM	ADSL/ ISDN/ GSM

Table 83 Engineers Button Options

FUJ00171956

Note [1] ISDN under NDIS

Note [2] Warn that a reboot will be required.

Note [3] ISDN under RAS

The "Initiate Connection" button should only offer the appropriate options for the outlet service type. If the current connection type is selected when initiating a connection then Connection Manager will reset the connection.

CNIM must be able to respond to any order of button pressing.

The following assumptions are made:

1) Initiation of a connection implies the dropping of an existing connection.
2) A test may be interrupted by the dropping of a connection or the initiation of a new connection.
3) The test will comprise the normal CNIM pinging test of the data centre.
4) CNIM will return an error if an inappropriate command is given, i.e. attempting to drop or test an ISDN connection over NDIS or attempting to initiate an ISDN connection on an NST 13 outlet.
5) When a manual switch to a particular connection type is made, CNIM will not switch automatically to any other connection type during that Call Plan period. At the start of the next Call Plan period CNIM will initiate a new test sequence which may cause the connection type to change.

FUJ00171956

5.12.5 Returning Network State

The Engineers App will be responsible for displaying status information concerning each connection type, to the user. The three areas of registry, ADSL, ISDN and GSM, shown below will be updated by CNIM as and when a connection of the appropriate type is opened or closed.

As mentioned above the registry entry **ButtonAppRegRef** within the CNIM area of registry, will store a reference to the area of registry to be used to store the Engineers Button App. data. In the example below

ButtonAppRegRef = SOFTWARE\ICL\ButtonApplication\ResilientNetwork

[HKEY_LOCAL_MACHINE\SOFTWARE\Fujitsu\POA\DesktopApplication\NetworkResilience\ConnectionState\ADSL] **[HKEY_LOCAL_MACHINE\SOFTWARE\Fujitsu\POA\DesktopApplication\NetworkResilience\ConnectionState\ISDN]** **[HKEY_LOCAL_MACHINE\SOFTWARE\Fujitsu\POA\DesktopApplication\NetworkResilience\ConnectionState\GSM]** **[HKEY_LOCAL_MACHINE\SOFTWARE\Fujitsu\POA\DesktopApplication\NetworkResilience\ConnectionState\NDIS]** **[HKEY_LOCAL_MACHINE\SOFTWARE\Fujitsu\POA\DesktopApplication\NetworkResilience\ConnectionState\VSAT]**				
Value	**Type**	**Possible Entries**	**Format Example**	**Description**
TimeStamp	String	Date Time	"02/06/2005 14:10:00"	Date/Time stamp for last update
NetworkState	String	See Following Table	See Following Table	See Following Table
PhoneNumber	String	Any	GRO	Phone number dialled.
CallCode	String	Any		8 Alphanumeric character code
CallCodeDescription	String	Any	"Ping Failed"	Interpretation of Call Code. Limited to 40 characters.
PingState	String	Any	"22,10"	Number of pings for this connection type, Number of successful pings
EnableDrop	DWORD	0,1	0	Enable the Drop button for this connection type.
EnableTest	DWORD	0,1	0	Enable the Test button for this connection type.
TimeStamp	String	Any	"24/01/2006 13:44:29"	Time of last change
AllowConnect	DWORD	0,1	0	Allow a connection of this type.

Table 84 Resilient Network Status

The string descriptions to be used for Network State are shown in the table below. The state display will show both line state and ping state.

Note that the Ping State reverts to Unknown when a call opens.

Line State/Ping State	**Unknown**	**Ping Fail**	**Ping Success**

FUJ00171956

Line Unknown	"Call State Unknown, Ping State Unknown"	"Call State Unknown, Ping State Failed"	"Call State Unknown, Ping State Passed"
Line Closed	"Call State Closed, Ping State Unknown"	"Call State Closed, Ping State Failed"	"Call State Closed, Ping State Passed"
Line Opening	"Call State Attempting, Ping State Unknown"	"Call State Attempting, Ping State Failed"	"Call State Attempting, Ping State Passed"
Line Open	"Call State Open, Ping State Unknown"	"Call State Open, Ping State Failed"	"Call State Open, Ping State Passed"

Table 85 Network State Screen Information for BNR

The Engineers App. is responsible for monitoring this area of registry and displaying this information to the user.

5.12.6 ISDN/GSM Switch Process

The switch process between ISDN and GSM on an ISDN outlet is described below:

1. Engineers Button pressed to initiate GSM
2. Engineers App sets CONNECTION value in CNIM registry to 3.
3. CNIM notified of registry change
4. CNIM sets CONNECTION value in CNIM registry to 0.
5. CNIM sets Connection_Type_Required to "GSM" with timestamp.
6. CNIM checks the change required and sets its own flag REBOOT_REQUIRED, to 1.
7. The Engineers App is notified by registry that the REBOOT_REQUIRED flag is set.
8. The Engineers App warns the user that a reboot is required and offers the choice to continue or quit.
9. If the user chooses to continue the Engineers App updates the value of REBOOT_REQUIRED to 3.
10. If the user chooses to cancel the Engineers App updates the value of REBOOT_REQUIRED to 0.
11. CNIM is notified of the change and if the value is zero CNIM sets the Connection_Type_Required to "DEFAULT" with timestamp.
12. If the value of REBOOT_REQUIRED is 3 CNIM sets the value to 5 and spawns a new process which will run the switch command with the correct parameters to switch to GSM.

FUJ00171956

13. Switch Package sets the SWITCH_RESULT flag to 1 in case of failure during switch
14. Switch Package disables SYSMAN
15. Switch Package stops CNIM and Connection Manager
16. Switch Package disables ISDN channels.
17. Switch Package sets dummy IP address on Eicon card
18. Switch Package disables ISDN monitoring.
19. Switch Package initiates a reboot.
20. ----------REBOOT----------
21. CNIM checks that the Connection_Type_Required was set during the current call plan period.
22. If the Connection_Type_Required was set before the current call plan period it is set to "DEFAULT"
23. CNIM notes Network Service Type and that Connection_Type_Required = GSM
24. CNIM checks that the SwitchNetworkUseResult is correct and that the Eicon card has a dummy IP address applied.
25. The Engineers App. will check that the SwitchNetworkUseResult is correct and will warn the user that the platform is in an indeterminate state if the SwitchNetworkUseResult displays an error.
26. If no switch error CNIM requests GSM connection from Connection Manager
27. CNIM waits for connection to be established and then does a test ping.
28. CNIM reports ping result.
29. CNIM does not change the connection type until the end of the call plan period.
30. If a switch error has occured CNIM will go to idle mode.
31. At the end of the call plan period CNIM sets the Connection_Type_Required to "DEFAULT"
32. CNIM moves to the default test plan sequence for the current call plan period.

5.13 Test Strategy, Design Overview

Requirement: See section 2.2.7.d

Line Failure is determined either by the receipt of an error cause code or by the fact that a ping initiated by CNIM fails to elicit a reply from its target.

CNIM will initiate a ping under the following circumstances:

- Outbound call is opened by an external source leading to a line check.
- Inbound call is received leading to CNIM initiating dial back.
- CNIM is within a "fixed" period and is required to keep the line up.
- When carrying out a test sequence following line failure.

The line test is done at the start of the call and is only done once per call. It comprises sending a ping to one or more of the four VPN servers with which the outlet is configured to test comms and waiting for a timeout period for a reply

FUJ00171956

CNIM will check the cause code each time the line goes idle to determine whether the call was successful as far as the telephone network is concerned. The code returned by the Eicon card is compared with a set of known good values.

If the line test should fail or the cause code is found to be an error code then the Test sequences shown in section 2.2.7.d will be initiated.

Test activity will be initiated by the line monitoring function within CNIM. When a call is opened an event will be sent to the test module which will decide if a line test is required. If a test is required then a ping will be sent to one or more VPN servers, depending on whether a reply was received from one of the VPN servers at the last ping attempt. Each ping attempt incorporates a timeout applicable to the network being used. Two timeout values are used, one for the satellite network and one for the ISDN/Data network.

When within test mode CNIM uses a set of timers to determine when the next test should take place. In general, on an ISDN outlet, each individual test will comprise a configuration of the Eicon card with the appropriate parameters followed by set of pings with a ping timeout period. In the event that the individual test fails then a timer will be set by the test module and acted upon by that module when the timer expires.

5.13.1 Run Mode – ISDN Outlet

5.13.1.a Pre Version 2.0

CNIM divides the phone numbers available to it into one of three modes, as shown in Table 86. See Table 14 for a description of the number types used in this table.

Mode 1 is considered normal running in that whilst running in this mode the test timer will not be set. Only one of the two available numbers is configured on the card at a time, in this mode.

Mode 2 is considered a failure mode in that both numbers in Mode 1 have failed. When in this mode the test timer will be set. As with Mode 1 only one number is configured on the card at a time.

Whilst in Mode 2 CNIM will not enter the Permanent Fail state as defined in Table 106.

Mode 3 is also considered a failure mode and if CNIM is unable to return to Mode 1 or 2 then it will enter the Permanent Fail state 15 minutes after the line first failed. The test timer will be set whilst in this mode.

Network\Mode	Mode 1 (One Number Used at a Time)	Mode 2 (One Number Used at a Time)	Mode 3 (All Numbers Configured on Card)
ISDN	VP, VS	VT, VP	VP, VS, VT, VP
Data	MP, MS	MP, MS	VP, VS, VT, VP
FRIACO (1)	FC1P, FC1S	DP, DS	VP, VS, VT, VP
FRIACO (2)	FC2P, FC2S	DP, DS	VP, VS, VT, VP

Table 86 Called Party Numbers per Mode - Version 1

5.13.1.b Version 2 Onward

FUJ00171956

The table below shows the revised mapping of phone numbers to Connection Type for CNIM Version 2.

Network\Mode Type	**Mode 1 Primary**	**Mode 2 Secondary**	**Mode 3 Tertiary**
ISDN voice (01)	VP	VS	VT
Bronze (04)	MP	VP	VS
Silver FRIACO (07) Fixed Period	FP	DS	VP
Silver FRIACO (07) Dialled Period	DP	VP	VS
Silver Metered (09) Fixed period	MP	MS	VP
Silver Metered (09) Dialled Period	MP	VP	VS
FRIACO 24 Hr (11) Metered period	DP	DS	VP
FRIACO 24 Hr (11) FRIACO Period	FP	DS	VP

Table 87 Called Party Numbers per Mode - Version 2

Note that Mode 2 numbers are directed to the same campus as the Mode 1 number for the outlet. This is because Energis will redirect a failed number on Mode 1 to the alternative campus. Therefore if CNIM deems that number to have failed then, in theory, a call to both campuses has been attempted.

5.13.1.a.1 Service Type 11 at Metered Fixed

For Network Service Type 11 during the metered period the connection type is Metered Fixed. Metered Fixed is also used by NST 09 during its fixed period and so for the two types the numbers used are:

Mode 1: NST 09 - MP, NST 11 - DP
Mode 2: NST 09 - MS, NST 11 - DS
Mode 3: NST 09 - VP, NST 11 - VP

5.13.1.a.2 Service Type 11 at FRIACO Fixed

For Network Service Type 11 during the FRIACO period the connection type is FRIACO Fixed. FRIACO Fixed is also used by NST 07 during its fixed period and so for the two types the numbers used are:

Mode 1: NST 07 - FP, NST 11 - FP
Mode 2: NST 07 - DS, NST 11 - DS
Mode 3: NST 07 - VP, NST 11 - VP

FUJ00171956

5.13.2 Ping Sequence

With the "ping" process employed to maintain a connection to the Data Centre, there are three issues to be considered:

1. Ping failure – an allowance of a 1% failure rate to be made.
2. All pings can fail for 1 or 2 seconds under certain network conditions.
3. VPN session establishment can impact the ability of the ping to work.

To overcome the issues above, CNIM utilises a sequence of "pings", "n" seconds apart in order to ascertain whether or not the call had worked. As soon as a ping succeeds, then the call is deemed to be a success and the rest of the sequence is not done. In addition if the Eicon card reports that the call had closed before a ping had succeeded then the call is deemed to have failed. The remaining "pings" in the sequence are not done, as they would cause additional calls to be made to the Data Centre. If all the "pings" in the sequence are deemed to have failed, then the last "ping" will time-out after "n" seconds.

Methodology

The time between "pings" is a Registry Entry and initially will be set to 4 seconds.

CNIM selects 4 out of the 8 VPN servers. The VPN servers selected are the first from each of the 4 IP Subnets.

A typical outlet Policy file is shown below:

[GENERAL]
Heartbeat=DEFERRED
HeartbeatResponseTime=60
HeartbeatDeferTime=900
EarlyAuthentication=1
KeyService=GSS
PacketEncapsulation=ESP
RequestDelay=60
KeyIdleTime=99999
LogDelay=1
AllowUserAccess=0
EncryptionSurvive=0
EncryptionOnStartup=1
UseCRYPTLogic=0
[ENCRYPTION]
EncryptionOnSend=USER1
KeyEncryption1=USER1
[DROP]
Ip1=IRRELEVANT-IRRELEVANT
Ip2=IRRELEVANT-IRRELEVANT
Ip3=IRRELEVANT

FUJ00171956

Ip4=IRRELEVANT
Ip5=IRRELEVANT
[PLAIN]
[CRYPT]
[TRY]
AcceptCryptAll=0
[CLUSTER]
Cluster1= IRRELEVANT
Cluster2= IRRELEVANT
Cluster3=IRRELEVANT
Cluster4= IRRELEVANT
Cluster5= IRRELEVANT
Cluster6= IRRELEVANT
Cluster7= Cluster5 + Cluster6

[TUNNEL]
Tunnel1=IRRELEVANT Cluster2
Tunnel2=IRRELEVANT Cluster7
Tunnel3=IRRELEVANT Cluster2
Tunnel4=IRRELEVANT Cluster1
Tunnel5=IRRELEVANT Cluster7
Tunnel6=IRRELEVANT Cluster1
Tunnel7=IRRELEVANT Cluster4
Tunnel8=IRRELEVANT Cluster7
Tunnel9=IRRELEVANT Cluster4
Tunnel10=IRRELEVANT Cluster3
Tunnel11=IRRELEVANT Cluster7
Tunnel12=IRRELEVANT Cluster3
[EXTAUTH]
ExtAuth1=IRRELEVANT /L=C
ExtAuth2=IRRELEVANT /L=P /CN=002001
ExtAuth3=IRRELEVANT /L=C
[SIGNATURE]
78f2e261f5b5d3e635432ee9eaad2048

In order to extract the VPN server IP addresses required the information in clusters 1 to 6 must be parsed. One server from each of the two VPN LANs at each Data Centre will be selected as a ping target. The LAN addresses are given below. Each outlet can connect to one or more VPN server on each LAN.

FUJ00171956

x.64.18.y

x.64.19.y

x.74.18.y

x.74.19.y

The file will be parsed so that one address from each LAN is chosen at random. In effect CNIM will ensure that the 2nd/3rd octet sequence is unique for each of the four VPN servers used as ping targets during the test cycle.

The order in which the chosen VPN servers are pinged is randomised on starting CNIM.

With each call, CNIM starts with the first VPN server on the list, "pings" the server and waits for 4 seconds.

If no response from the "ping" and the call is still open, CNIM "pings" the next server on the list.

This repeats until all 4 servers have been "pinged" or the call has been dropped.

If no reply, then the call is deemed to have failed.

On the next call, CNIM will commence with the VPN server that responded the previous time.

For "Fixed" connections, CNIM will "ping" the VPN server that responded the previous time. If this fails, CNIM tries the other 3 VPN servers, in sequence, 4 seconds apart, prior to declaring the call dead. As with other "pings", it will check the call is up before doing each "ping".

This means that at most 4 "pings" are used to determine whether or not a call has failed.

5.13.3 Test Strategy Design

The requirements for line testing, within CNIM, are given in section 2.2.7.d. These specifically refer to the requirements for CNIM version 2 onwards.

It may be seen that, within each test sequence, CNIM is required to move between certain states in a predefined manner and that these states share common features.

In order to facilitate the use of these test sequences a simple language has been developed, known as the CNIM Programming Language or CPL. The language is made up of a set of operations which may be grouped into elements, these elements being numbered and shown on the original test sequence diagrams.

Each operation is a discrete instruction or decision, for example:

Set Mode 1 number

Or

Determine next element on call failure.

Each element is stored in registry as a sequence of operation names and associated parameters. Each element has a two character name and is held in registry as a Multi String.

Operation types are shown in Table 88.

Type	No. Parameters	Parameter Length	Possible Value	Description
SET	1	1	1, 2 or 3	Set Mode 1, 2 or 3
TTP	0	N/A	N/A	Test Ping
KAP	0	N/A	N/A	KeepAlive Ping

FUJ00171956

BDP	0	N/A	N/A	Bandwidth Ping
STT	2	1 to 4	0 to 9999	Set Test Timer Min/Max in seconds. This will not affect the timer if it is already running.
CTT	0	N/A	N/A	Cancel Test Timer
ATT	1	2	00 to 99	Next Element after Timeout
LPS	2	1 to 4	0 to 9999	Loop Start for Min/Max sec's
LPE	1	2	00 to 99	Element address at start of loop
PGP	1	2	00 to 99	Next Element on Ping Pass
PGF	1	2	00 to 99	Next Element on Ping Fail
CLP	1	2	00 to 99	Next Element on Call Succeeds
CLF	1	2	00 to 99	Next Element on Call Fails
ENC	1	2	00 to 99	Next Element on No Call
GTO	1	2	00 to 99	Next Element to Go To
ALO	1	2	00 to 99	Next Element after Line Opening
ALC	1	2	00 to 99	Next Element after Line Closing
BRK	0	N/A	N/A	Break and go to wait state
END	0	N/A	N/A	End of test sequence
STM	0	N/A	N/A	Store current mode
RSM	0	N/A	N/A	Restore last stored mode to use
EIC	2	2	00 to 99	Set Shorthold Timer and MCDT Parameters on Eicon Card
ILD	1	2	00 to 99	Next Element if ISDN line down
ILI	1	2	00 to 99	Next Element if ISDN line is connected in.
ILO	1	2	00 to 99	Next Element if ISDN line is connected out.
BLU	1	1-4	0 - 9999	Break if the line is up (Before changing number) with timeout.
NTL	1	2	00 to 99	Goto address if timed out or line down
GES	0	N/A	N/A	Goto element start
SFF	1	1	0 or 1	Parameter 0 = Set fail flag to zero. Parameter 1 = Increment fail count
INT	0	N/A	N/A	Initialise Tester Thread
SBT	2	1 to 4	0 to 9999	Set Bandwidth Timer Min/Max in seconds. This will not affect the timer if it is already running.
CBT	0	N/A	N/A	Cancel Bandwidth Timer

FUJ00171956

BWT	1	2	00 to 99	Next Element after Bandwidth Timeout
DRP				Drop the connection
STE				Signal Test (Manual) Ended
MNT				Start a Manual Test
FNL	1	N/A	0 to 9999	Final Op, parameter is a mode number to control the action taken.
MD1				Go to Mode 1
MD2				Go to Mode 2
MD3				Go to Mode 3
ABT	1	2	00 to 99	Await bandwidth timer and branch
ABH	1	2	00 to 99	Await blackhole timer and branch
CBH	0	N/A	N/A	Cancel blackhole timer
SBH	1	1 to 4	0 to 9999	Set blackhole timer
SBT	1	1 to 4	0 to 9999	Set bandwidth timer
RCM	0	N/A	N/A	Reset Connection Manager
RCS	0	N/A	N/A	Reset Current Screen Statistics
SM1	2	1 to 4	0 to 9999	Set Mode 1 Timer
SM2	2	1 to 4	0 to 9999	Set Mode 2 Timer
CM1	0	N/A	N/A	Cancel Mode 1 Timer
CM2	0	N/A	N/A	Cancel Mode 2 Timer
GDD	0	N/A	N/A	Go to DayD Mode
LDD	0	N/A	N/A	Leave DayD Mode
CDD	0	N/A	N/A	Check if should be in DayD Mode

Table 88 CPL Operations

Test pings will be sent to N servers where N is stored in registry. KeepAlive pings will be sent to just 1 server.

The LPS loop operation will set a timer and carry out the operations between LPS and LPE until the timer expires.

Each element will parse its own registry entry and create a list of operations.

Following any BREAK operation the thread will wait and accept other events such as timer events signalling the end of the call plan period or service shutdown events.

The element will contain two state variables to store the test call state (TCS) and non test call state (NTCS). Initially both will be set to FALSE. If a ping succeeds the TCS is set to TRUE. If a non test call goes through successfully the NTCS is set to TRUE. This will be based on a line check following a Layer 2 Activated notification.

STM will store the current mode in a globally available variable. This would be done prior to changing mode to a different value and allows the stored value to be restored later using RSM.

FUJ00171956

Each ping operation, whether TTP or KAP would normally be followed by a PGF operation to determine the logical flow in the event of ping failure. It would not have to be followed by a PGP if no special action is required on ping success. The operations TTP and KAP are responsible for updating the failure state that would be returned to Counter Call Scheduler via the GetStatus mechanism.

5.13.3.a Diversion Operations

Diversion operations are those that divert the logical command flow to a new element and are described in more detail below.

In each case if the operation does not cause a diversion then control is passed to the next operation in sequence.

Type	Name	Description	Condition	Flag Type
ATT		Next Element after Timeout	Check input operation type is Test Timer	OperationType
LNE	Loop Not Ended	Element address at start of loop	Check if Loop Timer has gone off. If not go to address which is start of loop.	Timer Event
PGP		Next Element on Ping Pass	Go to the address given if the last ping passed.	BOOL Pass/Fail
PGF		Next Element on Ping Fail	Go to the address given if the last ping failed.	BOOL Pass/Fail
CLP		Next Element on Call Succeeds	Go to the address given if the last call succeeded.	BOOL Good/Bad Cause code
CLF		Next Element on Call Fails	Go to the address given if the last call failed.	BOOL Good/Bad Cause code
ENC		Next Element on No Call	No call has been made.	BOOL Call Made/Not Made.
GTO		Next Element to Go To	None	N/A
ALO		Next Element after Line Opening	Check input operation type is Line Event	OperationType
ALC		Next Element after Line Closing	Check input operation type is Line Event	OperationType

Table 89 Diversion Operation Conditions

Operations will be called continuously, each operation being responsible for retrieving the address of the next operation, until a BRK element is reached.

Following a BRK, CNIM Call Manager class will pass in the name of the event that has cause the operation test sequence to be restarted. This will have three possible values:

FUJ00171956

1. OT_ATT - Test Timer has expired.
2. OT_ALO - The line has been opened.
3. OT_ALC - The line has been closed.

The next operation following the break, which will only be of the type ATT, ALO or ALC, will run itself if it has received the right type of event. Otherwise it should retrieve the address of the next operation in sequence.

FUJ00171956

5.13.3.b Test Plan Details

5.13.3.b.1 Test Plan - FRIACO Establish

[HKEY_LOCAL_MACHINE\SOFTWARE\ICL\Pathway Configuration\CNIM\Test_Elements\E_Range]						
El't	**Op 1**	**Op 2**	**Op 3**	**Op 4**	**Op5**	**Op6**
00	ATT 11	GTO 01				
01	BRK	ATT 11	GES			
11	BLU	NTL 11	SET 1	CTT	STT 0 900	GTO 54
12	KAP	PGF 13	STT 32 32	GTO 55		
13	BLU	NTL 13	SET 2	GTO 14		
14	CTT	STT 210 810	GTO 51			
15	BLU	NTL 15	SET 1	TTP	PGP 12	GTO 16
16	BLU	NTL 16	SET 2	TTP	PGP 22	GTO 17
17	CTT	STT 450 1350	GTO 52			
18	BLU	NTL 18	SET 1	TTP	PGP 12	GTO 19
19	BLU	NTL 19	SET 3	CTT	STT 900 900	GTO 56
20	BLU	NTL 20	SET 2	TTP	PGP 22	GTO 21
21	BLU	NTL 21	SET 3	CTT	STT 900 900	GTO 57
22	CTT	STT 600 2400	GTO 53			
23	BLU	NTL 23	SET 1	TTP	PGP 12	GTO 13
35	TTP	PGP 22	GTO 51			
41	TTP	PGP 22	GTO 52			
45	TTP	PGF 14	GTO 53			
51	BRK	ALO 35	ATT 15	GES		
52	BRK	ALO 41	ATT 18	GES		
53	BRK	ALO 45	ATT 23	GES		
54	BRK	ATT 12	GES			
55	BRK	ATT 12	GES			
56	BRK	ATT 20	GES			
57	BRK	ATT 18	GES			

Table 90 E Range Test Elements - FRIACO Establish Period - S60

FUJ00171956

5.13.3.b.2 Test Plan - FRIACO or Metered Fixed

[HKEY_LOCAL_MACHINE\SOFTWARE\ICL\Pathway Configuration\CNIM\Test_Elements\F_Range]						
El't	**Op 1**	**Op 2**	**Op 3**	**Op 4**	**Op5**	**Op6**
00	ATT 11	GTO 01				
01	BRK	ATT 11	GES			
11	BLU	NTL 11	SET 1	CTT	STT 0 10	GTO 53
12	KAP 4	PGF 30	CTT	STT 32 32	GTO 54	
13	BLU	NTL 13	SET 2	GTO 14		
14	CTT	STT 210 810	GTO 51			
15	BLU	NTL 15	SET 1	TTP 4	PGP 12	GTO 16
16	BLU	NTL 16	SET 2	TTP 4	PGP 22	GTO 17
17	CTT	STT 450 1350	GTO 52			
18	BLU	NTL 18	SET 1	TTP 4	PGP 12	GTO 19
19	BLU	NTL 19	SET 3	CTT	STT 900 900	GTO 55
20	BLU	NTL 20	SET 2	TTP 4	PGP 22	GTO 21
21	BLU	NTL 21	SET 3	CTT	STT 900 900	GTO 56
22	LPS 300 900	EIC 40 10	GTO 45			
23	BLU	NTL 23	SET 1	TTP 4	PGP 12	GTO 13
30	TTP 4	PGP 12	GTO 13			
31	TTP 4	PGP 22	GTO 51			
41	TTP 4	PGP 22	GTO 52			
45	KAP 4	PGF 14	CTT	STT 30 30	GTO 57	
46	LNE 45	GTO 23				
51	BRK	ALO 31	ATT 15	GES		
52	BRK	ALO 41	ATT 18	GES		
53	BRK	ATT 12	GES			
54	BRK	ATT 12	GES			
55	BRK	ATT 20	GES			
56	BRK	ATT 18	GES			
57	BRK	ATT 46	GES			

Table 91 F Range Test Elements - FRIACO Fixed Period - S60

F01 uses a nominal randomisation time of 10 seconds, the requirement for a random 0-900 second delay being satisfied by the Call Plan modification that occurs at startup.

Element F35 sets the timer to 4 seconds because CNIM has set mode 2 Dialaround number and the card parameters will be:

MCDT = 0

Shorthold Timer = 5 seconds

FUJ00171956

5.13.3.b.3 Test Plan - FRIACO Fixed at S92

[HKEY_LOCAL_MACHINE\SOFTWARE\ICL\Pathway Configuration\CNIM\Test_Elements\F_Range]

El't	Op 1		Op 2	Op 3	Op 4	Op5	Op6			
00	STT 10 10	CDD J60	ATT 11	GTO 01						
01	BRK	CDD J60	ATT 11	GES						
11	BLU	GDD J60	NTL START	SET 1	CTT	STT 0 10	GTO 53			
12	KAP 4	PGF 30	CTT	STT 32 32	GTO 54					
13	BLU	GDD J60	NTL START	SET 2	GTO 14					
14	CTT	STT 210 810	GTO 51							
15	BLU	GDD J60	NTL START	SET 1	TTP 4	PGP 12	GTO 16			
16	BLU	GDD J60	NTL START	SET 2	TTP 4	PGP 22	GTO 17			
17	CTT	STT 450 1350	GTO 52							
18	BLU	GDD J60	NTL START	SET 1	TTP 4	PGP 12	GTO 19			
19	BLU	GDD J60	NTL START	SET 3	CTT	STT 900 900	GTO 55			
20	BLU	GDD J60	NTL START	SET 2	TTP 4	PGP 22	GTO 21			
21	BLU	GDD J60	NTL START	SET 3	CTT	STT 900 900	GTO 56			

FUJ00171956

22	LPS 300 900	EIC 40 10	GTO 45							
23	BLU	GDD J60	NTL START	SET 1	TTP 4	PGP 12	GTO 13			
30	TTP 4	PGP 12	GTO 13							
31	TTP 4	PGP 22	GTO 51							
41	TTP 4	PGP 22	GTO 52							
45	KAP 4	PGF 14	CTT	STT 30 30	GTO 57					
46	LNE 45	GTO 23								
51	BRK	ATT 15	GDD 60	ALO 31	GES					
52	BRK	ATT 18	GDD 60	ALO 41	GES					
53	BRK	ATT 12	GDD 60	GES						
54	BRK	ATT 12	GDD 60	GES						
55	BRK	ATT 20	GDD 60	GES						
56	BRK	ATT 18	GDD 60	GES						
57	BRK	ATT 46	GDD 60	GES						
60	CTT	STT 30 30								
61	BRK	ATT G62	ALO G62	ALC G62	ABH G72	PGP G71	PGF G70	CDD START	TTP 5	GTO 00
62	CTT	STT 30 30	TTP 10	RTN						
70	SBH 1200 1200	RTN								
71	CBH	RTN								
72	RCM	RTN								

Table 92 FRIACO Fixed Test Elements- S92

5.13.3.b.4 Test Plan - Dialled (MOD)

[HKEY_LOCAL_MACHINE\SOFTWARE\ICL\Pathway Configuration\CNIM\Test_Elements\D_Range]

FUJ00171956

El't	Op 1		Op 2	Op 3	Op4	Op5	Op6			
00	STT 10 10	CDD J90	ATT 02	GTO 01						
01	BRK	CDD J90	ATT 02	GES						
02	FCH 13	GTO 11								
11	BLU	GDD J90	NTL 11	SET 1	GTO 12					
12	BRK	ALO 31	GDD J90	GES						
13	CTT	STT 210 810	GTO 61							
14	BLU	GDD J90	NTL 14	SET 2	TTP 4	PGP 20	GTO 15			
15	BLU	GDD J90	NTL 15	SET 1	CTT	STT 450 1350	GTO 62			
16	BLU	GDD J90	NTL 16	SET 2	TTP 4	PGP 20	GTO 17			
17	BLU	GDD J90	NTL 17	SET 3	CTT	STT 900 900	GTO 66			
18	BLU	GDD J90	NTL 18	SET 1	TTP 4	PGP 12	GTO 19			
19	BLU	GDD J90	NTL 19	SET 3	CTT	STT 900 900	GTO 67			
20	TTP 4	CTT	STT 1800 5400	GTO 63						
21	CTT	STT 300 900	GTO 64							
22	BLU	GDD J90	NTL 22	SET 1	TTP 4	PGP 12	GTO 23			
23	BLU	GDD J90	NTL 23	SET 2	CTT	STT 450 1350	GTO 65			
24	BLU	GDD J90	NTL 24	SET 1	TTP 4	PGP 12	GTO 25			
25	BLU	GDD J90	NTL 25	SET 2	GTO 20					
31	TTP 4	PGP 12	GTO 13							
35	TTP 4	PGP 12	GTO 61							
41	TTP 4	PGP 12	GTO 62							
42	ENC 18	GTO 16								
45	TTP 4	PGF 21	GTO 63							
51	TTP 4	PGP 20	GTO 64							
55	TTP 4	PGP 20	GTO 65							
56	ENC 16	GTO 18								
61	BRK	ATT 14	GDD J90	ALO 35	GES					
62	BRK	ATT 42	GDD J90	ALO 41	GES					
63	BRK	ATT 24	GDD J90	ALO 45	GES					
64	BRK	ATT 22	GDD J90	ALO 51	GES					
65	BRK	ATT 56	GDD J90	ALO 55	GES					
66	BRK	ATT 18	GDD J90	GES						

67

FUJ00171956

BRK	ATT 16	GDD J90	GES							
70	SET 4									
71	TTP 5	GSB 80								
75	BRK	ATT 71	GES							
80	CTT	STT 30 30	RTN							
90	CTT	STT 30 30								
91	BRK	ATT G92	ALO G92	ALC G92	ABH 97	PGP G96	PGF G95	CDD START	TTP 10	GTO 00
92	TTP 10	CTT	STT 30 30	RTN						
95	SBH 1200 1200	RTN								
96	CBH	RTN								
97	RCM	RTN								

Table 93 D Range Test Elements - Dialled Period

FUJ00171956

5.13.3.b.5 Test Plan - Dialled (VOD)

[HKEY_LOCAL_MACHINE\SOFTWARE\ICL\Pathway Configuration\CNIM\Test_Elements\I_Range]

FUJ00171956

El't	Op 1		Op 2	Op 3	Op4	Op5	Op6			
00	STT 10 10	CDD J70	ATT 02	GTO 01						
01	BRK	CDD J70	ATT 02	GES						
02	FCH 13	GTO 11								
11	BLU	GDD J70	NTL 11	SET 1	GTO 12					
12	BRK	GDD J70	ALC 31	GTO 12						
13	CTT	STT 210 810	GTO 61							
14	BLU	GDD J70	NTL 14	SET 2	TTP 4	PGP 20	GTO 15			
15	BLU	GDD J70	NTL 15	SET 1	CTT	STT 450 1350	GTO 62			
16	BLU	GDD J70	NTL 16	SET 2	TTP 4	PGP 20	GTO 17			
17	BLU	GDD J70	NTL 17	SET 3	CTT	STT 900 900	GTO 66			
18	BLU	GDD J70	NTL 18	SET 1	TTP 4	PGP 12	GTO 19			
19	BLU	GDD J70	NTL 19	SET 3	CTT	STT 900 900	GTO 67			
20	CTT	STT 1800 5400	GTO 63							
21	CTT	STT 300 900	GTO 64							
22	BLU	GDD J70	NTL 22	SET 1	TTP 4	PGP 12	GTO 23			
23	BLU	GDD J70	NTL 23	SET 2	CTT	STT 450 1350	GTO 65			
24	BLU	GDD J70	NTL 24	SET 1	TTP 4	PGP 12	GTO 25			
25	BLU	GDD J70	NTL 25	SET 2	GTO 20					
31	CLP 12	GTO 13								
35	CLP 12	GTO 61								
41	CLP 12	GTO 62								
42	ENC 18	GTO 16								
45	CLF 21	GTO 63								
51	CLP 20	GTO 64								
55	CLP 20	GTO 65								
56	ENC 16	GTO 18								
61	BRK	ATT 14	GDD J70	ALC 35	GES					
62	BRK	ATT 42	GDD J70	ALC 41	GES					
63	BRK	ATT 24	GDD J70	ALC 45	GES					
64	BRK	ATT 22	GDD J70	ALC 51	GES					
65	BRK	ATT 56	GDD J70	ALC 55	GES					
66	BRK	ATT 18	GDD J70	GES						
67	BRK	ATT 16	GDD J70	GES						
70	CTT	STT 30 30								

71

FUJ00171956

BRK	ATT G72	ALO G72	ALC G72	ABH G82	PGP G81	PGF G80	CDD START	TTP 10	GTO 00	
72	TTP 10	CTT	STT 30 30	RTN						
80	SBH 1200 1200	RTN								
81	CBH	RTN								
82	RCM	RTN								

Table 94 I Range Test Elements - Dialled Period - ISDN

FUJ00171956

5.13.3.b.6 Test Plan - Dial Back S60.

In this plan the dial back sequence will start immediately that an inbound ISDN call is detected. The first thing it must do is determine whether the line is down.

[HKEY_LOCAL_MACHINE\SOFTWARE\ICL\Pathway Configuration\CNIM\Test_Elements\B_Range]					
El't	**Op 1**	**Op 2**	**Op 3**	**Op4**	**Op5**
00	STT 10 10	ATT 11	GTO 01		
01	BRK	ATT 11	GES		
11	ILD 21	ILO 21	GTO 12		
12	BRK	GTO 11			
21	LPS 120 120	GTO 22			
22	TTP 4	PGF 25	CTT	STT 32 32	GTO 24
23	LNE 22	GTO 30			
24	BRK	ATT 23	GES		
25	BLU	NTL 25	SET 3	EIC 40 10	GTO 27
26	TTP 4	PGF 30	CTT	STT 32 32	GTO 28
27	LNE 26	GTO 30			
28	BRK	ATT 27	GTO 28		
30	ILD 40	GTO 31			
31	BRK	GTO 30			
40	LPS 0 0	END			

Table 95 Dial Back

The test plans are stored in registry using the CNIM programming language. The dial back test plan has been modified such that, at the end of the 2 minute "pinging period" CNIM will wait within the dial back test plan until the line drops. CNIM will periodically (90 sec.) do a test ping and determine if the line changes status in response to that ping.

The LPS 0 0 step immediately before the end ensures that the loop timer is cancelled.

The following table of possible results shows CNIMs actions following each periodic test ping.

Ping Result	Line Status	Exit Dial Back
Success	No Change	No
Success	Does Change	Yes
Fail	No Change	Yes
Fail	Does Change	Yes

Table 96 Ping Result and Line Status

FUJ00171956

If the ping fails or the line does change status then CNIM will exit from the dial back test plan.

If the line does not change status and the ping succeeds then the line must be being held open by some external application. CNIM will not force the line to close but will continue looping until the line is allowed to close.

CNIM does not need to wait until the periodic ping before exiting the dial back plan. Once it has finished the 2 minute mandatory pinging period it will respond to a change in line status and exit the dial back plan. The periodic ping is used in the event of a "Layer 1" failure which may prevent the line changing status.

5.13.3.b.7 Test Plan - Satellite

Pinging is done once every 15 minutes.

The ping interval is reduced to 4 minutes and the ping sequence is altered to use keep alive pings in the first instance and test pings in the event of failure.

The KAP item was removed as it caused premature setting of the fail state.

El't	Op 1	Op 2	Op 3
00	STT 10 10	ATT 11	GTO 01
01	BRK	ATT 11	GES
11	TTP 40	GTO 13	
12	BRK	ATT 11	GES
13	CTT	STT 240 240	GTO 12

Table 97 P Range Test Elements - Permanent Connection (Satellite) - S60

5.13.3.b.8 Test Plan - ADSL

El't	Op 1	Op 2	Op 3	Op4	Op5
00	ATT 11	GTO 01			
01	BRK	ATT 11	GES		
11	TTP 5	GTO 30			
12	BDP 5	PGF 20	GTO 13		
13	BRK	ATT 30	ALO 20	ALC 20	GES
20	TTP 5	GTO 13			
30	CTT	STT 300 300	GTO 12		

Table 98 A Range Test Elements - ADSL - S60 - With Test On Line State Change

5.13.3.b.9 Test Plans for RAS at BNR - S92

FUJ00171956

5.13.3.b.9.1 Test Plans - ADSL Only

These elements are stored under the key:

[HKEY_LOCAL_MACHINE\SOFTWARE\ICL\Pathway Configuration\CNIM\Test_Elements\RA_Range]

The following elements are used overnight where no ISDN or ADSL backup is available outside core hours.

CNIM is expected to respond to the manual test button and does this via the MNT element. It must also respond to the Drop button and this is picked up by the DRP element.

When carrying out a manual test CNIM will use the LPS loop element with a time of 120 seconds. CNIM will carry out bandwidth pings during the test if required.

CNIM will reset the Test flag back to 0 at the end of the test via the STE element.

[HKEY_LOCAL_MACHINE\SOFTWARE\ICL\Pathway Configuration\CNIM\Test_Elements\RA_Range]

El't	Op 1	Op 2	Op 3	Op4	Op5	Op6	Op7	Op8	Op9	Op10	Op11	Op12	Op 13	Op 14
00	CDD J90	MD1 J11												
11	SET 1	SBT 300 300	STT 10 10	GTO 21										
21	BRK	GDD J90	ATT G31	ALO G31	ALC G31	ABT G41	ABH G80	MNT G50	MNT G61	DRP J85	MD1 J11	PGF G65	PGP G78	GES
31	TTP 5	RTN												
41	SBT 300 300	BDP 5	RTN											
50	RCS	LPS 120 120	CTT	STT 5 5	RTN									
61	BRK	GDD J90	ATT G31	STT 5 5	ABT G41	DRP J85	MD1 J11	LNE START	STE	RTN				
65	SBH 1200 1200	RTN												
78	CBH	RTN												
80	TTP 5	PGF G81	RTN											
81	RCM	GSB 78	GSB 65	RTN										
85	SET 0	GTO 86												
86	BRK	GDD	MD1	ALO	ALC	GES								

FUJ00171956

		J90	J11	G31	G31									
90	CTT	STT 30 30												
91	BRK	ATT G92	ALO G92	ALC G92	ABH G81	PGF G65	PGP G78	CDD STAR T	TTP 10	GTO 00				
92	TTP 10	CTT	STT 30 30	RTN										

Table 99 RA Range Elements - S92

FUJ00171956

5.13.3.b.9.2 Test Plan - ADSL with GSM Backup

These elements are stored under the key:

[HKEY_LOCAL_MACHINE\SOFTWARE\ICL\Pathway Configuration\CNIM\Test_Elements\RAG_Range]

El't	Op 1	Op 2	Op 3	Op4	Op5	Op6	Op7	Op8	Op9	Op10	Op11	Op12	Op 13	Op 14	Op 15
00	CDD G90	MD1 J11	MD2 J12												
11	SET 1	SBT 300 300	STT 10 10	GTO 21											
12	SET 2	SBT 300 300	STT 10 10	GTO 22											
21	BRK	GDD G90	ATT G31	ALO G31	ALC G31	ABT G41	ABH G80	MNT G50	MNT G61	DRP J85	MD1 J11	MD2 J12	PGF G65	PGP G78	GES
22	BRK	GDD G90	ATT G32	ALO G32	ALC G32	ABT G42	ABH G80	MNT G50	MNT G63	DRP J85	MD1 J11	MD2 J12	PGF G65	PGP G78	GES
31	TTP 5	RTN													
32	TTP 20	RTN													
41	SBT 300 300	BDP 5	RTN												
42	SBT 300 300	TTP 20	RTN												
50	RCS	LPS 120 120	CTT	STT 5 5	RTN										
61	BRK	GDD G90	ATT G31	STT 5 5	ABT G41	DRP J85	MD1 J11	MD2 J12	LNE START	STE	RTN				
62	BRK	GDD G90	ATT G32	STT 5 5	ABT G42	DRP J85	MD1 J11	MD2 J12	LNE START	STE	RTN				
65	SBH 1200 1200	RTN													
78	CBH	RTN													
80	TTP 5	PGF G81	RTN												
81	RCM	GSB 78	GSB 65	RTN											
85	SET 0	GTO 86													
86	BRK	GDD	MD1	MD2	ALO	ALC	GES								

FUJ00171956

		G90	J11	J12	G31	G31									
90	CTT	STT 30 30													
91	BRK	ATT G92	ALO G92	ALC G92	ABH G81	PGF G65	PGP G78	CDD START	TTP 10	RTN					
92	TTP 10	CTT	STT 30 30	RTN											

Table 100 RAG Range Elements - S92

FUJ00171956

5.13.3.b.9.3 Test Plan- RAS GSM Backup

These elements are stored under the key:

[HKEY_LOCAL_MACHINE\SOFTWARE\ICL\Pathway Configuration\CNIM\Test_Elements\RG_Range]

This is used by NDIS outlets running on GSM backup.

El't	Op 1	Op 2	Op 3	Op4	Op5	Op6	Op7	Op8	Op9	Op10	Op11			
00	STT 30 30	CDD J70	MD1 J30	MD2 J30	MD3 J30	MD4 J80	DRP J30							
10	BRK	GDD J70	ATT G12	MD1 J30	MD2 J30	MD3 J30	MD4 J80	GSB 20	DRP J30	MNT G50	ABH G60	PGF G65	PGP G66	GES
12	TTP 20	RTN												
20	CTT	STT 30 30	RTN											
30	GSB 20	SET 0	GTO 40											
40	BRK	GDD J70	MD4 J80	ATT G12	GSB 20	GES								
50	RCS	LPS 120 120	GSB 55											
51	BRK	GDD J70	ATT G12	MD4 J80	GSB 55	DRP J30	LNE START	STE	RTN					
55	CTT	STT 5 5	RTN											
60	RCM	GSB 66	GSB 65	RTN										
65	SBH 1200 1200	RTN												
66	CBH	RTN												
70	CTT	STT 30 30												
71	BRK	ATT G72	ALO G72	ALC G72	ABH G60	PGF G65	PGP G66	CDD STAR T	TTP 10	GTO 00				
72	TTP 10	CTT	STT 30 30	RTN										
80	SET 4	GTO 10												

Table 101 RG Range Elements - S92

FUJ00171956

5.13.3.b.9.4 Test Plan - ADSL with ISDN and GSM Backup

[HKEY_LOCAL_MACHINE\SOFTWARE\ICL\Pathway Configuration\CNIM\Test_Elements\RAIG_Range]

FUJ00171956

El't	Op 1	Op 2	Op 3	Op4	Op5	Op6	Op7	Op8	Op9	Op10	Op11	Op 12	Op 13	Op 14		Op 15	
00	CDD G90	MD1 J11	MD2 J12	MD3 J13													
11	SET 1	SBT 300 300	STT 10 10	GTO 21													
12	SET 2	SBT 300 300	STT 10 10	GTO 22													
13	SET 3	SBT 300 300	STT 10 10	GTO 23													
21	BRK	GDD G90	ATT G31	ALO G31	ALC G31	ABT G41	ABH G80	MNT G50	MN T G61	DRP J85	MD1 J11	MD2 J12	MD3 J13	PGF G64	PGP G78	GES	
22	BRK	GDD G90	ATT G31	ALO G31	ALC G31	ABT G42	ABH G80	MNT G50	MN T G62	DRP J85	MD1 J11	MD2 J12	MD3 J13	PGF G65	PGP G78	GES	
23	BRK	GDD G90	ATT G33	ALO G33	ALC G33	ABT G43	ABH G80	MNT G50	MN T G63	DRP J85	MD1 J11	MD2 J12	MD3 J13	PGF G65	PGP G78	GES	
31	TTP 5	RTN															
33	TTP 20	RTN															
41	SBT 300 300	BDP 5	RTN														
42	SBT 300 300	TTP 5	RTN														
43	SBT 300 300	TTP 20	RTN														
50	RCS	LPS 120 120	CTT	STT 5 5	RTN												
61	BRK	GDD G90	ATT G31	STT 5 5	ABT G41	DRP J85	MD1 J11	MD2 J12	MD3 J13	LNE STAR T	STE	RTN					
62	BRK	GDD G90	ATT G31	STT 5 5	ABT G42	DRP J85	MD1 J11	MD2 J12	MD3 J13	LNE STAR T	STE	RTN					
63	BRK	GDD G90	ATT G33	STT 5 5	ABT G43	DRP J85	MD1 J11	MD2 J12	MD3 J13	LNE STAR T	STE	RTN					
64	SBH 1200 1200	SM2 560 680	RTN														
65	SBH 1200 1200	CM2	RTN														

FUJ00171956

78	CBH	CM2	RTN														
80	TTP 5	PGF G81	RTN														
81	RCM	CBH	SBH 1200 1200	RTN													
85	SET 0	GTO 86															
86	BRK	GDD G90	MD1 J11	MD2 J12	MD3 J13	ALO G31	ALC G31	GES									
90	CTT	STT 30 30															
91	BRK	ATT G92	ALO G92	ALC G92	ABH G81	PGF G65	PGP G78	CDD START	TTP 10	RTN							
92	TTP 10	CTT	STT 30 30	RTN													

Table 102 Test Plan - ADSL/ISDN/GSM

FUJ00171956

5.13.3.b.9.5 Test Plan - ISDN Only

RAS outlets running on Service Type 14 are required to test the backup (ISDN) connection every Wednesday evening during the evening.

The RIT (RAS ISDN Test) Call Plan period will be given a nominal time of 21:00 - 21:10, i.e. a 10 time period. However a randomisation factor built into CNIM will move the start/end times back by a value between 0 and 160 minutes. The maximum offset (160) is stored in OFFSET_RIT under the CNIM\Times section of registry. Therefor the test will be carried out at any time between 21:00 and 23:40.

During this time period Fallback_ISDN will become mode 1 and CNIM will carry out a series of test pings until the end of the call plan period.

Alteration of the backup ISDN test timing would require updates to registry and/or the Call Plan file.

The test sequence is shown below.

[HKEY_LOCAL_MACHINE\SOFTWARE\ICL\Pathway Configuration\CNIM\Test_Elements\RIT_Range]

El't	Op 1	Op 2	Op 3	Op4	Op5	Op6	Op7	Op8	Op9	Op10
00	CDD J30	SET 1	RCS							
10	TTP 5	GSB 20								
11	BRK	ATT 10	FNL 1	GES						
20	CTT	STT 30 30	RTN							
30	CTT	STT 30 30								
31	BRK	ATT G32	ALO G32	ALC G32	ABH G40	PGF G45	PGP G46	CDD STAR T	TTP 10	GTO 00
32	TTP 10	CTT	STT 30 30	RTN						
40	RCM	CBH	SBH 1200 1200	RTN						
45	SBH 1200 1200	RTN								
46	CBH	RTN								

Table 103 RIT Range Test Elements - S92

CNIM will not carry out any bandwidth pings during this test phase.

The FNL element was added to ensure that the test results were logged before switching test sequences.

FUJ00171956

5.13.3.a.1.6 Test Plan - RAS at Idle

This is used by NDIS sites running on GSM at Idle, i.e. Mode 4 (BNR Mode 2). Connection Manager will have set the connection to idle. A test ping will be done every minute to update the network state.

[HKEY_LOCAL_MACHINE\SOFTWARE\ICL\Pathway Configuration\CNIM\Test_Elements\RID_Range]					
El't	**Op 1**	**Op 2**	**Op 3**	**Op4**	**Op5**
00	GSB 10	CDD J40	GSB 20	GTO 50	
10	CTT	STT 60 60	RTN		
20	SET 4	RTN			
30	TTP 20 20	GSB 10	RTN		
40	BRK	ATT G30	CDD START	GSB 20	GTO 50
50	BRK	ATT G30	GES		

Table 104 RID Range Test Elements - S92

Each Break operation is at the start of an element and that element is always terminated by a GoTo operation that takes control back to the start of the same element. The Break operation is followed by operations that allow branching under certain conditions, i.e. the test timer has expired or the line has opened or closed.

5.13.4 Code Character for Test Ranges

The character to be used to indicate in TuneableTrace which test range is in use, as from S92, will be stored within registry in the following location.

[HKEY_LOCAL_MACHINE\SOFTWARE\ICL\Pathway Configuration\CNIM\Test_Elements\All_Range_Letters]	
Value Name	**Value**
B_Range	'B'
D_Range	'D'
I_Range	'I'
E_Range	'E'
F_Range	'F'
P_Range	'P'
FR_Range	'R'
RIT_Range	'T'
RA_Range	'A'
RG_Range	'G'
RAIG_Range	'J'
RID_Range	'K'
RAG_Range	'H'

FUJ00171956

FR_Range	'R'

5.14 Keep Alive Strategy Overview

Requirement: See section 2.2.10

Keep Alive pings are required from CNIM in two situations.

- During Dial Back
- During Fixed Periods, e.g. FRIACO Fixed, Permanent Connection, etc.

Keep Alive will be carried out by sending "Pings" to one or more of the VPN servers with which the Gateway is configured to communicate. During Keep Alive periods the Eicon card will be configured with a suitable Shorthold Timer and Minimum Call Duration Time.

The interval between pings will be a configurable proportion of this time and will be optimised to reduce the load on the VPN servers.

A KeepAlive module will be used to control the frequency and target of each ping. This module will be responsible for parsing the VPN Policy file (SGVPN.INI) found on each gateway. Each policy file contains the IP addresses of the VPN servers with which the outlet may establish encrypted sessions.

At the first ping attempt CNIM will ping all eight VPN servers and store the address of the first VPN server to reply. Thereafter CNIM will only target that VPN server for its Keep Alive pings.

5.15 Time Format Overview

Requirement: See section 2.2.11.a

Time values are used within CNIM in a variety of ways. In particular input data from the Call Plan and output data to the Monitor, Summary and Bandwidth files.

Data written to the trace file is also time stamped.

Times within CNIM are considered to be in U.T.C. except for those specified in the Call Plan.

5.16 Design Overview: GetStatus Query

Requirement: See section 2.2.13

The CNIM_Get_Status function is implemented with the CNIM_API.dll. This in turn interfaces to the CNIM service using the RPC mechanism.

The CNIM_Get_Status function is called from the Counter Call Scheduler (CCS). The Get Status report provides the current status of a network connection to the caller. It specifies the defined connection type and the current mode of operation.

The function is called with a timeout parameter which defines the maximum length of time that the CCS wishes to wait for network state information. If the network state changes during that time period then CNIM will return the latest network state.

All parameters, with the exception of dwTimeout, are supplied as input/output parameters. This is because CNIM will compare its current network values with those supplied by CCS. If these differ CNIM will return immediately with the parameters updated to the latest values of network state.

The following parameters are used in this function call.

FUJ00171956


```
CNIM_DLL_API DWORD _stdcall CNIM_Get_Status(
DWORD       *iConnStatus,
DWORD       *iConnType,
DWORD       *dwTickNailedUp,
DWORD       *dwTickLastConnChange,
CHAR        *swFailCode,
DWORD       *dwTickPermanent
DWORD       dwTimeout);
```

Where

* Denotes return a value

The CNIM 'Get_Status' will return one of a set of values as shown in Table 105.

Any 'nailed-up' time reported by CNIM is from the start of the network connection up to the expected close of that connection. In the majority of cases this will include a period 'before' and 'after' the SLA period as CNIM will randomise both the 'start' and 'end' times. With a FRIACO connection type, the change from FRIACO-Establish to the FRIACO-Fixed will be reported to the Counter Call Scheduler as a change of connection. This change will be instigated by CNIM at a randomised time prior to the defined 'start' time.

Function Action	Return Value
Function Succeeded	0
Function Timed Out*	CNIM_GS_TIMEDOUT
Function Failed	CNIM_GS_FAIL

Table 105 GetStatus Return Values

*Note: Timed Out indicates the function returned valid data after a specified timeout value within which the line state did not change.

The Connection Status parameter supplied to the GetStatus call will be updated

5.16.1 Connection Status

FUJ00171956

Value	Defined Name	Description
0	CNIM_GS_UNKNOWN	Returned if the function call failed, e.g.the DLL could not communicate with the CNIM service.
1	CNIM_GS_CONNECTED	Connected – may or may not be nailed up
2	CNIM_GS_DISCONNECTED	NOT connected (last call attempt succeeded)
3	CNIM_GS_LOST_CONNECT	Connection was lost (cut) or disconnected
4	CNIM_GS_FAILED_ONCE	First connection attempt has failed (may be after a lost connection)
5	CNIM_GS_TEMP_UNAVAILABLE	More than one connection attempt has failed and not yet deemed to be a permanent failure
6	CNIM_GS_PERM_UNAVAILABLE	Connection has failed and needs attention to get it back

Table 106 Connection Status Values

5.16.2 Connection Type

***iConnType** - this indicates what type of connection is currently being used and is ignored if supplied as NULL. It is in 3 parts, i.e. 3 bytes, with 00 returned if the function call failed.

Outlet type (mask of 0xff)	
Value	**Meaning**
00	Function call failed
01	Voice (mobile)
02	Satellite
03	Frame Relay
04	Bronze (Metered-On-Demand)
05	Metered ‘nailed-up’ (Silver part time **A**)
06	Metered ‘nailed-up’ (Silver part time **B**)
07	FRIACO ‘nailed-up’ (Silver Daytime) (**C1**)
08	FRIACO ‘nailed-up’ (Silver Daytime) (**C2**)
09	Non-FRIACO (Metered) ‘nailed-up’ (Silver Daytime)
10	FRIACO 24hour (Silver) (**C1**)
11	FRIACO 24hour (Silver) (**C2**)
12	Non-FRIACO (Metered) 24hour (Silver)
13	ADSL
14	ADSL with ISDN

Table 107 Connection Type - First Byte

FUJ00171956

Current connection type (mask of 0x00ff)	
Value	**Meaning**
0x0100	Satellite
0x0200	Metered
0x0300	FRIACO
0x0400	Voice
0x0500	ADSL
0x0600	ISDN with RAS
0x0700	GSM
0x0800	Frame Relay
0x0900	PSTN

Table 108 Connection Type - Second Byte

Current QoS type may be one or more of the following bitmap values	
Value	**Meaning**
0x010000	Nailed up period
0x020000	'Fixed' connection
0x040000	Emergency connection
0x080000	Contracted Silver Outlet

Table 109 Connection Type - Third Byte

During a failed connection the current connection type and current QoS are those preferred for the current period.

5.16.3 TickNailedUp

***dwTickNailedUp** - this is a reference to a DWORD. When the function returns, the DWORD will be set to the TickCount for the time at which CNIM will no longer 'nail up' the connection. It is ignored if supplied as NULL.

This is used so that CCS knows when Riposte will no longer be nailed up.

5.16.4 TickLastConnectionChange

***dwTickLastConnChange** - returns the tickcount for the start of the current connection, the end of the last connection, or time a connection first failed as appropriate. This will change when there is a fast reconnection that caller may not otherwise have detected. It is ignored if supplied as NULL. The tickcount at the start of the service will be returned before the first connection attempt.

FUJ00171956

5.16.5 FailCode

***swFailCode** – supplied as an array of CNIM_GS_FCLEN bytes. A printable version of a failcode is returned in this field if the last connection attempt has failed (indicates what failure caused the primary connection to fail). It is "" for a successful connection (or disconnection) and ignored if supplied as NULL.

CNIM is expected to choose the most appropriate form of representation for the fail code.

5.16.6 TickPermanent

***dwTickPermanent** - returns the tickcount for when a failure is anticipated will become permanent and needing attention.

5.16.7 Timeout

***dwTimeout** - this indicates the timeout for the function in milli-seconds

If this value is (DWORD)-1 it will **not** timeout and will wait until it has something to return to the caller.

If this value is >= 0 then the function will return either, (a) when it has something to report to the caller, or (b) when the timer has expired (whichever occurs first).

If this value is 0 (zero) it will timeout immediately and 'return' the current status details.

5.17 Static Test Modes

There are two CNIM function calls that are test scenarios, initial testing at implementation when CNIM is first installed and activated, and secondly during normal running as a test facility.

5.17.1.a CNIM Test – Implementation

During CNIM installation the Implementation test is called by Tivoli. In version 1 of CNIM the metered numbers were tested to confirm network availability and then the registry flags shown below would be modified depending on whether the test has been passed or failed.

Flag	Pre Test Value	Post Test Value - Fail	Post Test Value - Pass
MIGRATION_STATE	WITHIN_MIGRATION	WITHIN_MIGRATION	POST_MIGRATION
ImpTestResult	-blank-	FAIL	PASS
dwImpTestResult	0	1	0
Service Start	Manual	Manual	Automatic

Table 110 Implementation Test Flags

In version 2 of CNIM the line is not tested and registry is updated to show that the test has passed. The "Fail" values above are no longer required.

5.17.1.b CNIM Test – normal running

During normal running if the CNIM test function is invoked (CNIMConfig –t) will attempt Data Centre calls using the Mode 1 Primary and Mode 2 Primary numbers.

A result file is created within the directory specified by the "Directory_Test_Files" entry in "Live" registry and the filename prefix is specified by the "Test_Prefix" entry, see Table 48.

The file name has the following naming structure:

TEST_RESULT_<fad code>_<yyyymmdd>_<hh-mm>

FUJ00171956

The file has the following format:

Date	Time (UTC)	Service Type	1st No.	OK ?	2nd No.	OK ?
dd/mm/yyyy	hh:mm:ss	1 - 12	11 digits	Yes or No	11 digits	Yes or No

For example:

24/10/2001, 15:00:33, 7, 12345678911, Yes, 12345678912, Yes

From S60 (CNIM 3) the Normal Test is removed.

5.18 CNIM Reset

To change the service type of an Outlet, the new type is put into the CNIM 'delivery' Registry. CNIM is then called with the 'r' option (CNIMConfig – r) that notifies CNIM that there has been a change in service type and to re-read the Registry and file entries into the 'live' Registry. This 'reset' function has the same effect as starting the CNIM service.

5.19 Service Installation and Configuration

CNIM is installed by the use of the command line instruction:

CNIM -install

And is removed by the use of:

CNIM -remove

On initial installation CNIM registry will contain certain default values.

During the migration phase of BI3 CNIM will be required to carry out an implementation test as described in section 5.17.1.a. If the test is passed then the relevant registry flags will be set such that CNIM will move to normal operation.

During the installation of a "spare" gateway the implementation test is not carried out and the installation script will make the necessary registry changes.

5.20 CNIM Trace

CNIM Tracing is controlled by a set of flags defined in Table 111. Each text message output by CNIM is assigned a low level trace flag.

Flag	Hex Value	Description
TL_MUST_LOG	0x00020000	Message must be logged.
TL_FN_ENTRY	0x00010000	Log function name on entry.
TL_LL_ERROR	0x00002000	Low level errors
TL_HL_ERROR	0x00001000	High level errors
TL_IDI_DATA	0x00000400	IDI data
TL_VL_DATA	0x00000200	Very Low level data
TL_LL_DATA	0x00000100	Low level data
TL_ML_DATA	0x00000010	Medium Level data
TL_TT_DATA	0x00000008	Test Timer data

FUJ00171956

TL_OP_DATA	0x00000004	Operation Element data
TL_HL_DATA	0x00000002	High level data
TL_EVENT_LOG	0x00000001	Log events to event log

Table 111 Trace Flags

CNIM Tracing module uses the following high level trace flags to determine whether messages should be sent to the event log and whether events should be logged to file.

Messages may be in the form of a text string within the source code or a message stored within the CNIM message DLL.

Messages are sent to one or more of the following outputs:

- CNIM log file
- TuneableTrace log file
- Event log
- Debugging output

5.20.1 Default Trace Levels

The default trace levels used by CNIM for both CNIM trace and TuneableTrace, are given in 4.1.3.k and 4.1.3.l. These levels are supplied in registry during installation.

5.20.2 CNIM Log File

The CNIM log file may only contain a maximum number of lines. The file name, location and maximum number of lines are specified in registry as shown in section 4.1.3.k. The level of trace for this file is also specified in the same location in registry.

The file wraps around when the max. line count is exceeded.

The old log file is overwritten when CNIM starts.

At S60 (CNIM 3) the CNIM log file is no longer used.

5.20.3 TuneableTrace File

The trace files for TuneableTrace are created in the directory "C:\TuneableTrace" and are archived automatically. The registry parameters controlling CNIM TuneableTrace are shown in section 4.1.3.l.and are ID, Name1 and Name2.

An application, TraceTune.exe is used to allow dynamic tuning of the trace entries in the registered with TuneableTrace.

In order to start tracing the following command should be used.

TraceTune ADD name1 name2 instance tracelevel

This call will adjust the tracelevel for the component identified by the name1, name2 and instance parameters. Tracelevel must be supplied as 8 hexadecimal digits. Empty string parameters, should be supplied as “”. A tracelevel value of 0 will disable tracing.

Note that the registry parameter ID is used as the "instance" parameter in the TraceTune ADD command.

CNIM may use the TuneableTrace function:

```
DWORD dwTraceLevel = TDTraceLevel(m_TuneableTraceHandle);
```

To determine the current tracelevel to which Tuneable Tracing for CNIM, is set.

FUJ00171956

5.20.4 Event Log

CNIM will register with the event log using the parameters shown in section 4.1.3.m. The service has the source name "CNIM".

5.20.5 Debugging Output

When run in debug mode CNIM will output messages to the screen to aid development.

5.21 Trace Logic

Tracing is required to be able to output trace information to any of the four output types mentioned above.

Tracing is controlled by the following parameters:

Parameter	Output	Description
Message Trace Level (MTL)	Any	Trace Level assigned to message. Any one of the low level trace levels.
Tuneable Trace Level (TTL)	TuneableTrace	Current Tuneable Trace Level. Combination of any low or high level trace level.
CNIM Trace Level (CTL)	CNIM Log	Current CNIM log Trace Level. Combination of any low or high level trace level.
DEBUG Flag	Debug Output	Flag set if running in debug mode.

Table 112 Tracing Parameters

The logic for tracing is shown below in Figure 13.

FUJ00171956

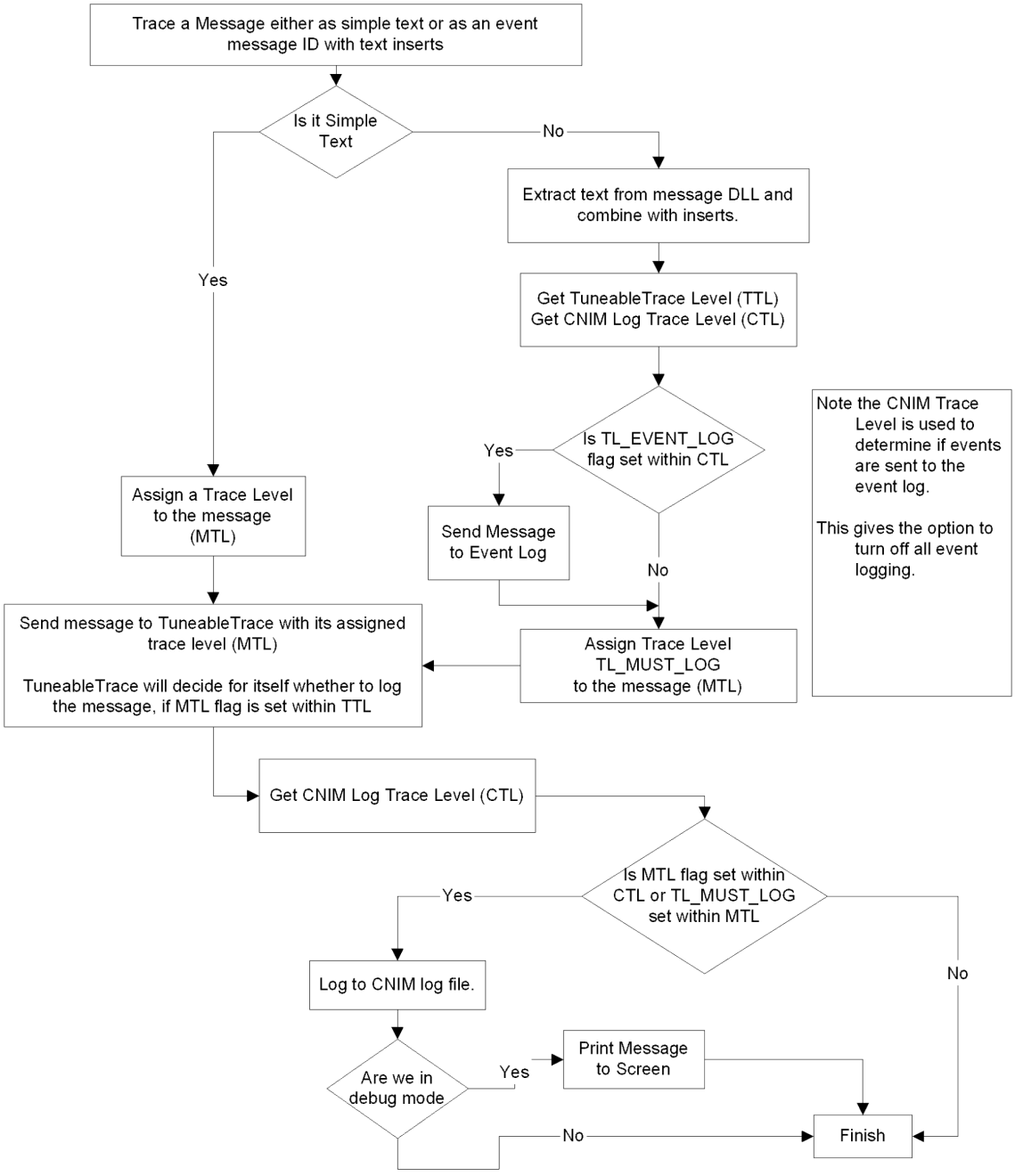

Figure 13 Trace Logic

FUJ00171956

5.22 Call Logging Logic

The logical interaction of the NetLevel objects, CNet, which waits for network events and CLogger which controls the logging of QOS data, is shown below.

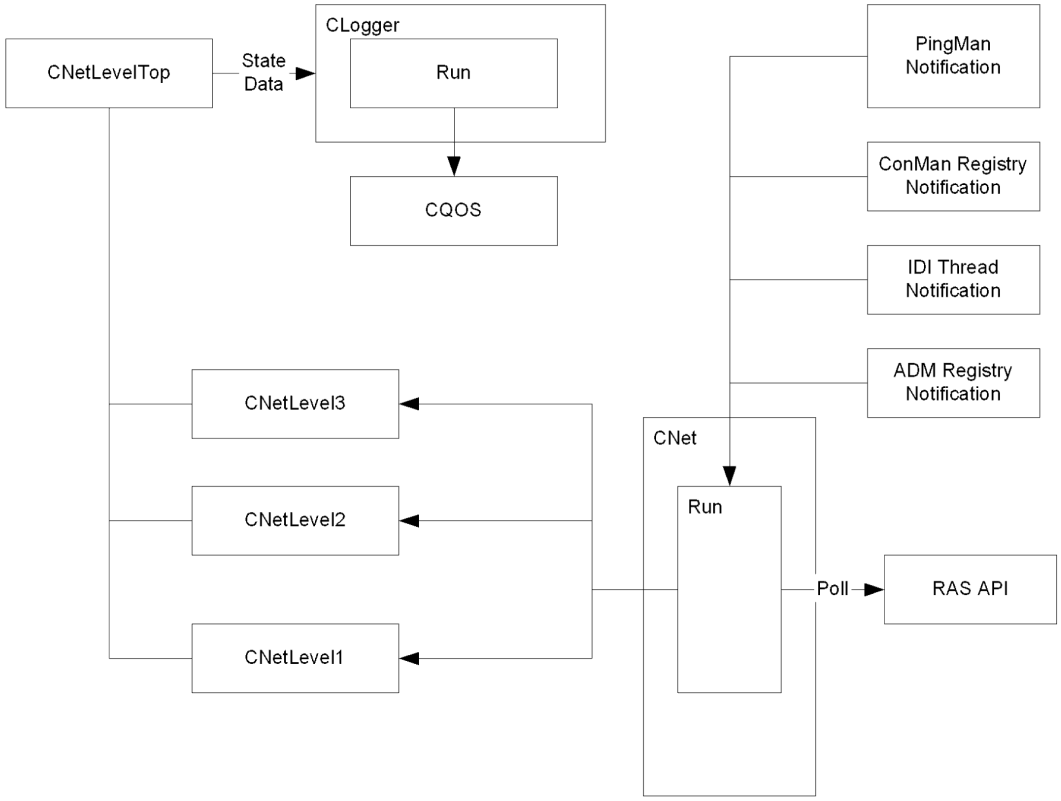

Figure 14 Call Logging Logic

5.23 CP4097 - 20 Minute Reset of Connection Manager

1. At initial ping failure CNIM will set a twenty minute "blackhole" timer.
2. CNIM will carry on doing bandwidth pings every 5 minutes, irrespective of the network condition.
3. CNIM will terminate the timer if a ping succeeds.
4. Upon expiry of the 20 minute "blackhole" timer CNIM will retest the connection and if the test fails it will request a connection reset. If the test succeeds then the test cycle will be aborted.
5. CNIM will use the Connection Manager registry interface as explained in section 5.10 to set the reset flag.

5.24 CP4103 - Logging of GSM Received Signal Strength to TuneableTrace

The Connection Manager registry area used by CNIM is explained in section 4.1.3.q.

FUJ00171956

As part of the Connection Management development, the registry value "CurrentDialParams" will be modified to have three further comma-separated variables appended when the GSM connection is in use. Three examples are shown below.

"49, h1234560010100A,0000,isdn,ISDN,ADSL1" *ADSL dial params*

"49, h1234560010100C,08081401224,modem,T-modemCOM,COM11,GSM,?,?" *GSM but info not available*

"49, h1234560010100C,08081401224,modem,T-modemCOM,COM11,GSM,+CSQ: 23 99,123….789" *GSM with rssi and imei*

CNIM will monitor the "CurrentDialParams" value in registry and will copy that entry to TuneableTrace each time it is changed. CNIM will not attempt to interpret the signal strength values.

FUJ00171956

5.25 Event Logging of Network Switch

CNIM will log the fact that it has succesfully changed or failed to change from one connection type to another and the time at which the change attempt occurred. The following table shows change of connectivity against event.

Start Network Type (SNT)	End Network Type (ENT)	Action	Event
Idle/NDIS/ADSL/ ISDN/GSM	NDIS/ADSL/ ISDN/GSM	Successful Connect	490 Network changed from (SNT) to (ENT) CNIM: Network changed from IDLE to ADSL at 22/01/2006 20:30:38
Idle/NDIS/ADSL/ ISDN/GSM	NDIS/ADSL/ ISDN/GSM	Failed Connect	491: Failed to change from (SNT) to (ENT) CNIM: Network failed to change from IDLE to GSM at 23/01/2006 11:56:07
Idle/NDIS/ADSL/ ISDN/GSM	Idle	Drop	490: Network changed from (SNT) to IDLE CNIM: Network changed from ADSL to IDLE at 22/01/2006 20:30:38
ADSL	ISDN	Successful automatic failover to ISDN	490: Network changed from ADSL to ISDN CNIM: Network changed from ADSL to IDLE at 22/01/2006 20:30:38 CNIM: Network changed from IDLE to ISDN at 22/01/2006 20:30:48
ADSL	No Connection	Failed automatic failover to ISDN	491: Failed change from ADSL to ISDN
ADSL/ISDN/GSM	No Connection	RAS connection dropped due to network failure.	No specific event required. Note that a call closure record with appropriate result, will be produced and a ping failure event.

Table 113 Network Switch Event Requirements

CNIM will also log the results of the backup (ISDN) test that occurs automatically and is marked in the Call Plan as an RIT period. CNIM will log the number of successful pings against the total number of pings and will also display the result as a percentage.

These event descriptions, IDs and event types are shown below. More detail is given in Appendix A3.

Event Description	Event ID	Event Type
Successful Change of Network	490	I
Unsuccessful Change of Network	491	E

FUJ00171956

Backup Test Result	492	I

Table 114 Events for Change of Connection Type

FUJ00171956

6 IMPLEMENTATION

6.1 Service

The service is implemented in C++. A base class is used to provide generic NT service functionality. A derived class provides functionality specific to the CNIM service.

6.1.1 Threading

The service is implemented as the following threads:

- A main thread, which receives service control notifications from the SCM and sends service status notifications to the SCM. It passes control requests to a watcher thread.
- A CCNIM thread that receives control requests from the main thread and implements these. This prevents the main thread from blocking waiting for the service to implement the control.
- A CallManager Test thread which controls testing of the line.
- An EiconManager Logging thread which monitors the line state using the IDI interface and logs call data.
- A KeepAlive thread which may be activated to continuously ping the VPN servers.
- An RPC thread which is used to monitor RPC connections from the CNIM_API DLL.
- API external thread for GetStatus.

The structure of the main threads is shown Figure 15.

The main thread handles the main() executable entry point, and also the service notification handler function.

The service thread contains ServiceMain(), the point of execution for the service. In turn, the service thread creates the logger and tester threads and then performs the main functionality of the service within its Run() function.

The logger and tester threads implements stop and shutdown control requests. They carry out the essential functionality of CNIM.

FUJ00171956

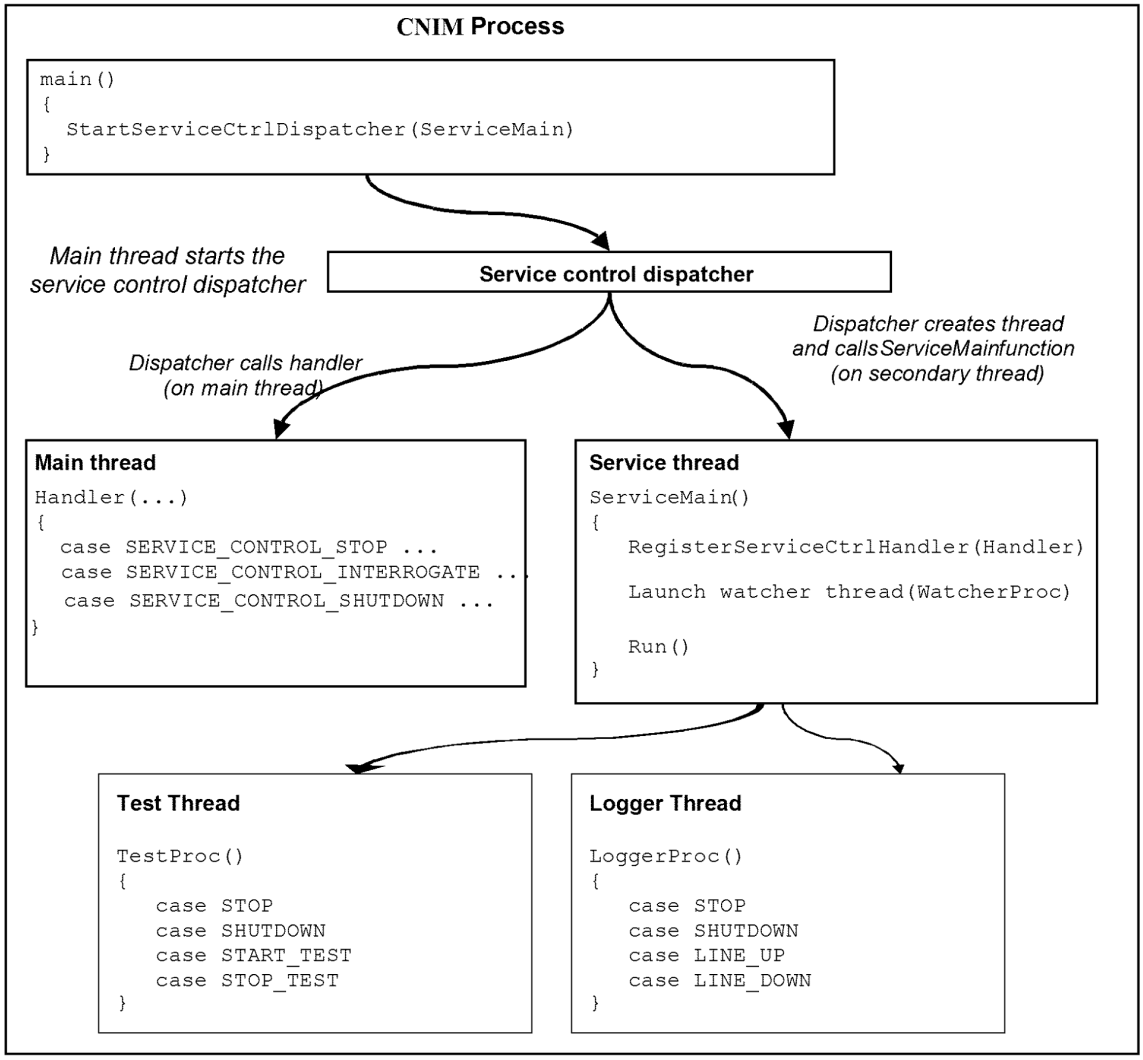

Figure 15: Service threading

6.1.2 Service control notifications

The SCM requests the service to change state by sending notifications to the service notification handler function:

Notification	Meaning	Comments
SERVICE_CONTROL_STOP	Requests the service to stop.	Supported
SERVICE_CONTROL_PAUSE	Requests the service to pause	Not supported
SERVICE_CONTROL_CONTINUE	Requests the paused service to resume.	Not supported
SERVICE_CONTROL_INTERROGATE		

FUJ00171956

	Requests the service to update immediately its current status information to the service control manager	Supported
SERVICE_CONTROL_SHUTDOWN	Requests the service to perform cleanup tasks, because the system is shutting down.	Supported
RANGE 128 TO 255	User defined notifications	Not supported

When a control notification is received, the service will report the appropriate status notification, see section 6.1.3.

6.1.3 Service status notifications

The service will report its state to the NT Service Control Manager using the usual SetServiceStatus() API:

State	Meaning	When reported
SERVICE_START_PENDING	The service is starting.	As soon as ServiceMain() is entered.
SERVICE_RUNNING	The service is running.	As soon as Run() is entered.
SERVICE_PAUSE_PENDING	The service pause is pending.	Not reported; pause and continue are not supported
SERVICE_PAUSED	The service is paused.	Not reported; pause and continue are not supported
SERVICE_CONTINUE_PENDING	The service is resuming.	Not reported; pause and continue are not supported
SERVICE_STOP_PENDING	The service is stopping.	As soon as SERVICE_CONTROL_STOP notification is received at Handler() and again after breaking out of main processing loop.
SERVICE_STOPPED	The service is not running.	When the service has broken out of its main processing loop and tidied up

Failure to respond to service control notifications in a prompt manner with the appropriate service status notification will cause the NT SCM to think that the service is no longer responding.

FUJ00171956

Service start-up:

Service initialisation is not a lengthy activity and consequently SERVICE_START_PENDING notifications with wait hints and periodic checkpoints are not required.

Service stop / shutdown:

Service stop/shutdown may be a lengthy activity and consequently SERVICE_STOP_PENDING notifications with wait hints and periodic checkpoints are required.

When a SERVICE_CONTROL_STOP or SERVICE_SHUTDOWN notification is received by the Watcher thread it issues a SERVICE_STOP_PENDING notification, signals the Service thread to stop and then exits. The Service thread on detecting the stop signal issues a further SERVICE_STOP_PENDING notification, tidies up and issues a SERVICE_STOPPED notification before exiting.

6.1.4 Inter-thread Communication

Communication between the Main thread and the Watcher thread is via events. The Main thread on receipt of service control notifications signals events from the SCM as follows:

EVENT	Service Control Notification	Comments
STOP	SERVICE_CONTROL_STOP	Supported
PAUSE	SERVICE_CONTROL_PAUSE	Not supported
CONTINUE	SERVICE_CONTROL_CONTINUE	Not supported
SHUTDOWN	SERVICE_CONTROL_SHUTDOWN	Supported

Communication between the Watcher thread and the Service thread is via events. The Watcher thread on detecting signals from the Main thread signals events as follows:

EVENT	Signal Detected	Comments
WO_STOP	STOP or SHUTDOWN	

6.1.5 Service Events

Whilst in its main processing loop the Service thread is waiting for one of a number of events to be signalled. The action taken upon notification of an event is dependent on the state. The following sections show for each state the events that can be signalled and the action that is taken.

6.1.5.a CCNIM

EVENT	Action
m_hStopEvent	service stop event
m_hPauseEvent	service pause event
m_hContinueEvent	service continue event

6.1.5.b CCallManager - Test Thread

FUJ00171956

EVENT	Action
m_hTesterShutdownEvent	Test Thread should return, service is shutting down
m_hStartTest	Start Test on Timer Expiry
m_hStartDialBack	Start a Dial Back
m_hNormalTest;	Start a Normal Test
m_hSetMode3	Set Mode 3 Parameters
m_hCallActivated	A Call has been Activated
m_hCallClosed	A Call has been Closed
m_hReset	Reset all CNIM Parameters
m_hStartCPTest	Start of Call Plan Period

Table 115 Test Thread Events

6.1.5.c CEiconManager - Logging Thread

EVENT	Action
m_hLogShutdownEvent	Stop thread, service stopping.
m_hPingOK_Satellite	Ping Succeeded on Satellite Service
m_hPingFailed_Satellite	Ping Failed on Satellite Service
m_hEndOfDay	End of Day, Update and Rename QOS Files
m_hLayer1_LineIdle	Line has gone Idle
m_hLayer1_LineOut	Line has connected out
m_hLayer1_LineIn	Line has connected in
m_hLayer2_Activating	Layer 2 is activating
m_hOpenSummaryRecord	Open a new Summary Record
m_hDropThrough	Go through wait loop
m_hIDI_Reset	Reset the IDI interface

Table 116 Eicon Manager Events

FUJ00171956

6.2 Classes

CNIM is constructed as a multithreaded service with the functionality to carry out three main tasks:

1) Log all calls made to and from the outlet.
2) Test and reconfigure the connection.
3) Provide connection status information to any application that requests it.

6.2.1 Class Overview

CNIM classes are shown within the boundary whilst external modules which provide an interface to which CNIM connects, are shown outside.

FUJ00171956

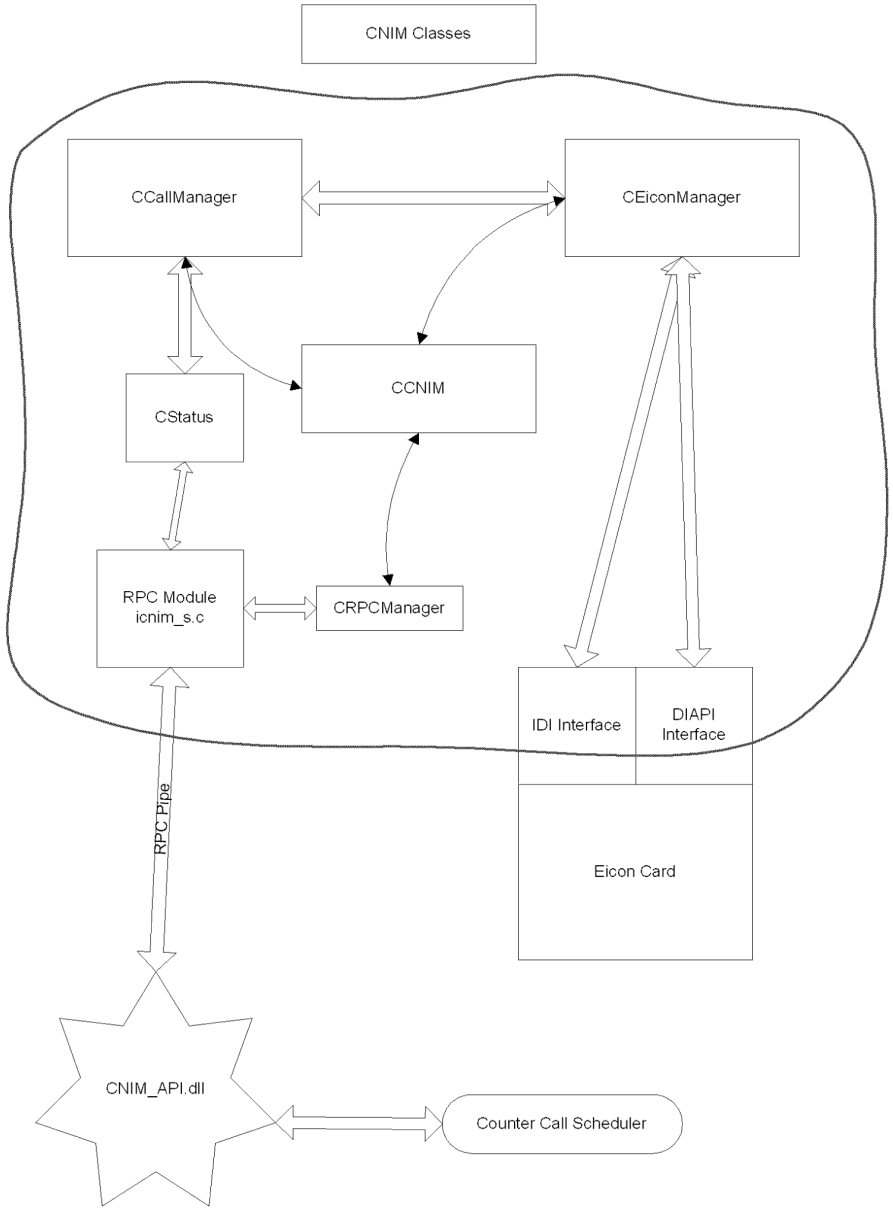

Figure 16 CNIM Class Overview

6.2.2 CService

The CService class provides a generic NT service capability.

6.2.3 CServiceInstall

The CServiceInstall class provides the functionality required to install and remove the service. The public methods Install () and Remove () are modified as follows:

- They return a bool value, TRUE indicating success and FALSE indicating failure.

FUJ00171956

- They output information and error messages to the Event Log.

6.2.4 CCNIM

The CNIM service class CCNIM is derived from CService.

The CCNIM class provides methods that support service specific functionality, namely:

- The processing logic within the Service thread required during service startup, running and closedown.

6.2.5 CEiconManager

The CEiconManager class controls the Eicon card configuration and monitors line state for logging purposes

The IDI interface is configured to notify CNIM when the line state changes. In addition the interface is used to retrieve the current connection status and the last disconnection Cause Code retrieved from the network.

The DIAPI interface is used to reconfigure the Eicon card with the appropriate telephone number(s) and parameters such as the Minimum Call Duration Time (MCDT).

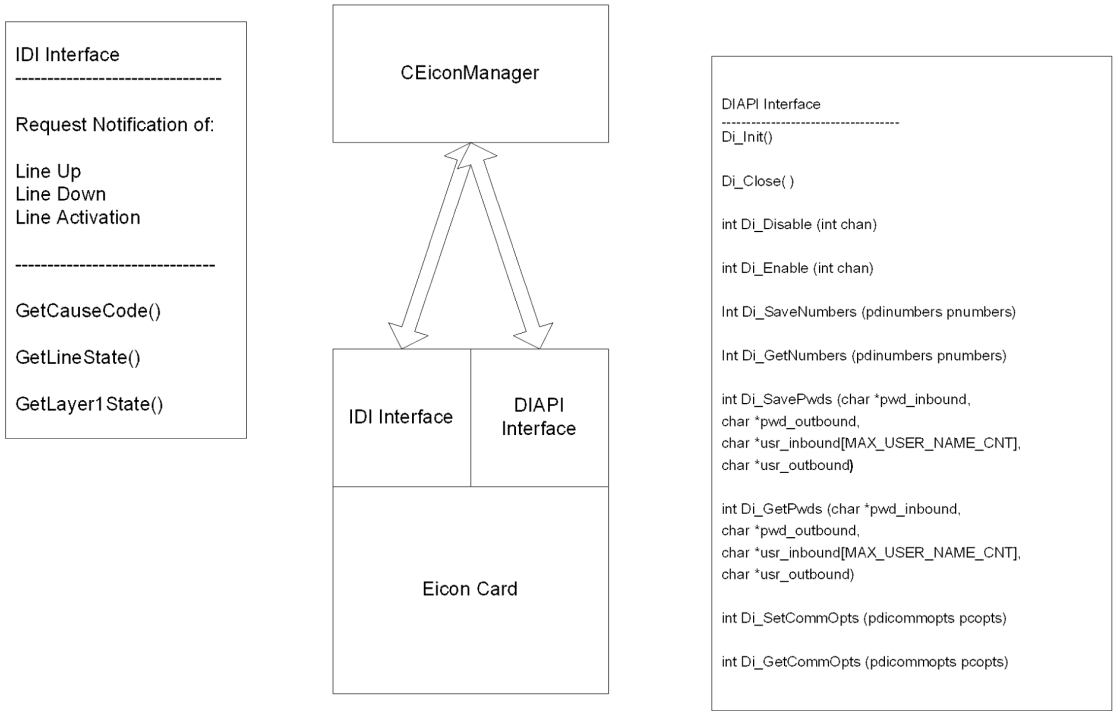

Figure 17 Eicon Interfaces

The EiconManager is responsible for controlling the CNIM Logger thread. Essentially this thread waits for line events and responds appropriately, for example to update the current Monitor and Summary files.

The logger thread will also interact with the test thread, so that when the line is activated by some external application the tester thread is aware of this event and may test the line if required.

FUJ00171956

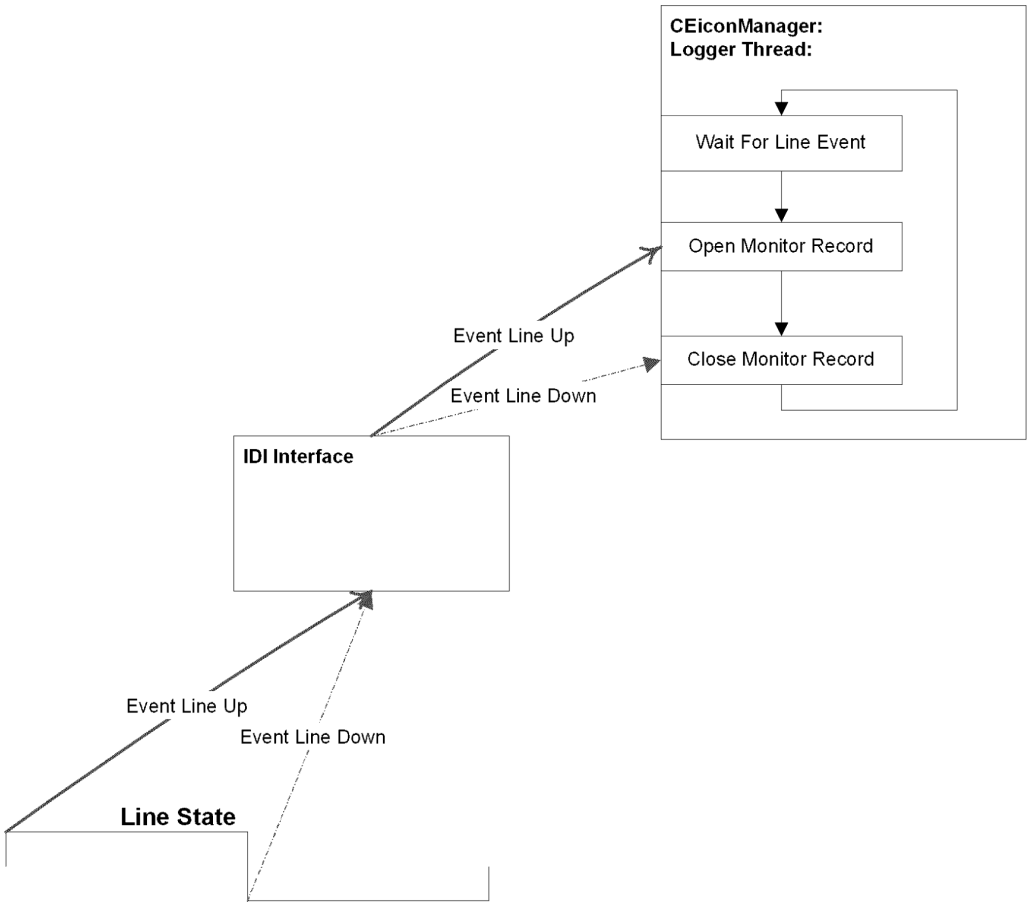

Figure 18 Logging Thread - IDI Interaction

6.2.5.a Protected Members

static CEiconManager*	_m_pThis	Static pointer to this
CDIAPI_Manager	m_DIAPI_Manager	DIAPI Interface Manager
CIDI_Manager	m_IDI_Manager	IDI Interface Manager
CRunMode	m_ModeCurrent	Current Run Mode
CRunMode	m_ModeRequired	Run mode required for new Call Plan period
CPeriodRecord	m_PeriodRecord	Current record in the summary file
CMonRecord	m_MonRecord	Current record in the monitor file
CEventList	m_lstLineEvents	List of line events received from IDI
CCallManager*	m_pCallManager	Pointer to the Call Manager
eCallResult	m_crLastResult	Result from last call closure
SYSTEMTIME	m_sysStartTime	Time at which call started
SYSTEMTIME	m_sysEndTime	Time at which call ended
DWORD	m_dwLogThreadId	ThreadID for the Log Thread
DWORD	m_dwLogExitCode	Exit code for the Log THread
DWORD	m_dwTickStart	Tick count at call started

FUJ00171956

DWORD	m_dwTickEnd	Tick count at call ended
BOOL	m_bSatelliteCallStarted	Has satellite call started
BOOL	m_bIsLogRunning	IsLog Thread running
BOOL	m_bPingOK	Did Last Ping Succeed
BOOL	m_bAwaitingNumberChange	Indicates if a number change is underway
eLineState	m_LastState	Last line state recorded from IDI
eLineMode	m_LineMode	Line mode is either ISDN or Data
eLayer1State	m_L1State	Layer 1 state
CString	m_csB1RemoteAddress	Channel B1 Remote Address
CString	m_csB2RemoteAddress	Channel B2 Remote Address
CString	m_csB1LineState	Channel B1 Line State
CString	m_csB2LineState	Channel B2 Line State
CString	m_csB1CauseCode	Channel B1 Cause Code
CString	m_csB2CauseCode	Channel B2 Cause Code
CString	m_csCallDate	Monitor Record Call Date
CString	m_csCallStartTime	Monitor Record Start Time
CString	m_csCallEndTime	Monitor Record End Time
CString	m_csCallDuration	Monitor Record Call Duration
CRITICAL_SECTION	m_CS_LineEvents;	Critical Section Guarding Line Events
CRITICAL_SECTION	m_CS_Codes	Critical Section Guarding Cause Codes
CRITICAL_SECTION	m_CS_GetLineData	Critical Section Guarding Line Data
CRITICAL_SECTION	m_csRunMode	Critical Section Guarding Run Mode
static CRITICAL_SECTION	_m_CS_IDI	Critical Section Guarding IDI Interface
HANDLE	m_hIDI_Reset	Event Handle for IDI Reset
HANDLE	m_hDropThrough	Event Handle for dropping through
HANDLE	m_hLayer1_LineIn	Event Handle for Line In
HANDLE	m_hLayer1_LineOut	Event Handle for Line Out
HANDLE	m_hLayer1_LineIdle	Event Handle for Line Idle
HANDLE	m_hEndOfDay	Event Handle for write the period file
HANDLE	m_hPingOK_Satellite	Event Handle for satellite ping succeeded
HANDLE	m_hPingFailed_Satellite	Event Handle for satellite ping failed
HANDLE	m_hOpenSummaryRecord	Event Handle for create a summary record
HANDLE	m_hLayer1_Up	Event Handle for Layer 1 up
HANDLE	m_hLayer1_Down	Event Handle for Layer 1 down
HANDLE	m_hLayer2_Activating	Event Handle for Layer 2 activating
HANDLE	m_hLayer2_Activated	Event Handle for Layer 2 activated
HANDLE	m_hLayer2_Closing	Event Handle for Layer 2 closing
HANDLE	m_hLayer2_Down	Event Handle for Layer 2 down
HANDLE	m_hLineDown	Event Handle to signal that line number can be changed
HANDLE	m_hLogThread	Event Handle for the Log THread
HANDLE	m_hAbandonSetCardNumber	Event Handle for Abandon Card Configuration
HANDLE	m_hLogShutdownEvent	Event Handle for Shutdown event
HANDLE	m_hLineOutForCheck	To signal that line is connected out

FUJ00171956

6.2.6 CCallManager

The CCallManager class controls the testing and choice of line numbers, depending on data from the Call Plan.

CallManager contains a member which is an instance of CCallPlan. This member is initialised at service start up and when a reset is requested.

CallManager is responsible for parsing the Call Plan file and creating a list of call plan elements which are logically grouped by Network Service Type and then by Day of the Week.

FUJ00171956

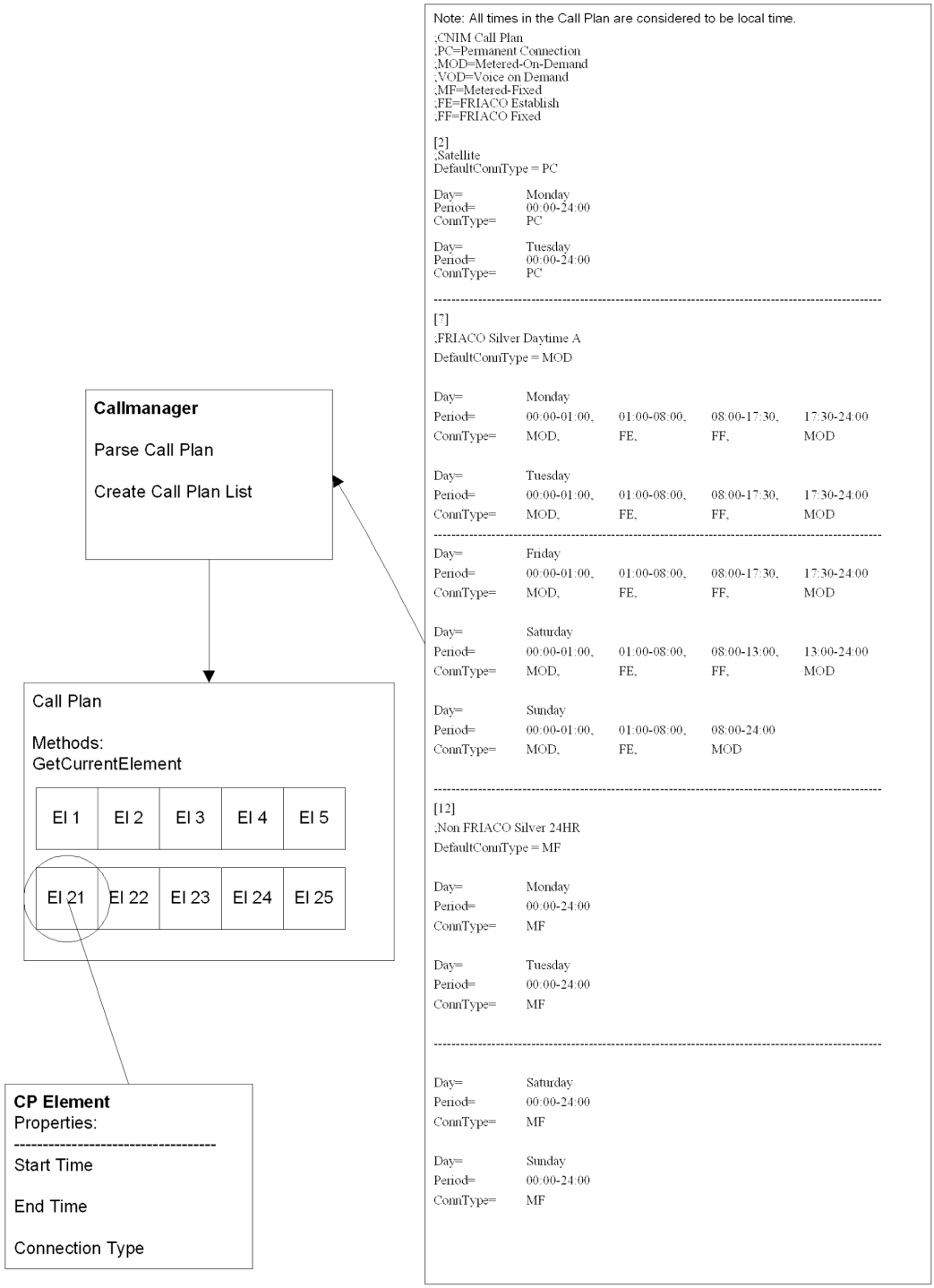

Figure 19 Call Plan Conversion to Element List

FUJ00171956

The CallManager is responsible for control of the TestManager which converts the CPL Elements in registry into a linked list of TestOperations, grouped into TestElements and stored by TestManager as a set of ElementLists, one list per connection type.

CallManager test thread is used to run each operation in turn, each operation being able to return the address of the next operation to run.

CCallManager contains a CPL interface comprising a number of class methods which may be called by the current test operation.

Each operation will call its own Run method which calls the appropriate CCallManager function within the CPL interface.

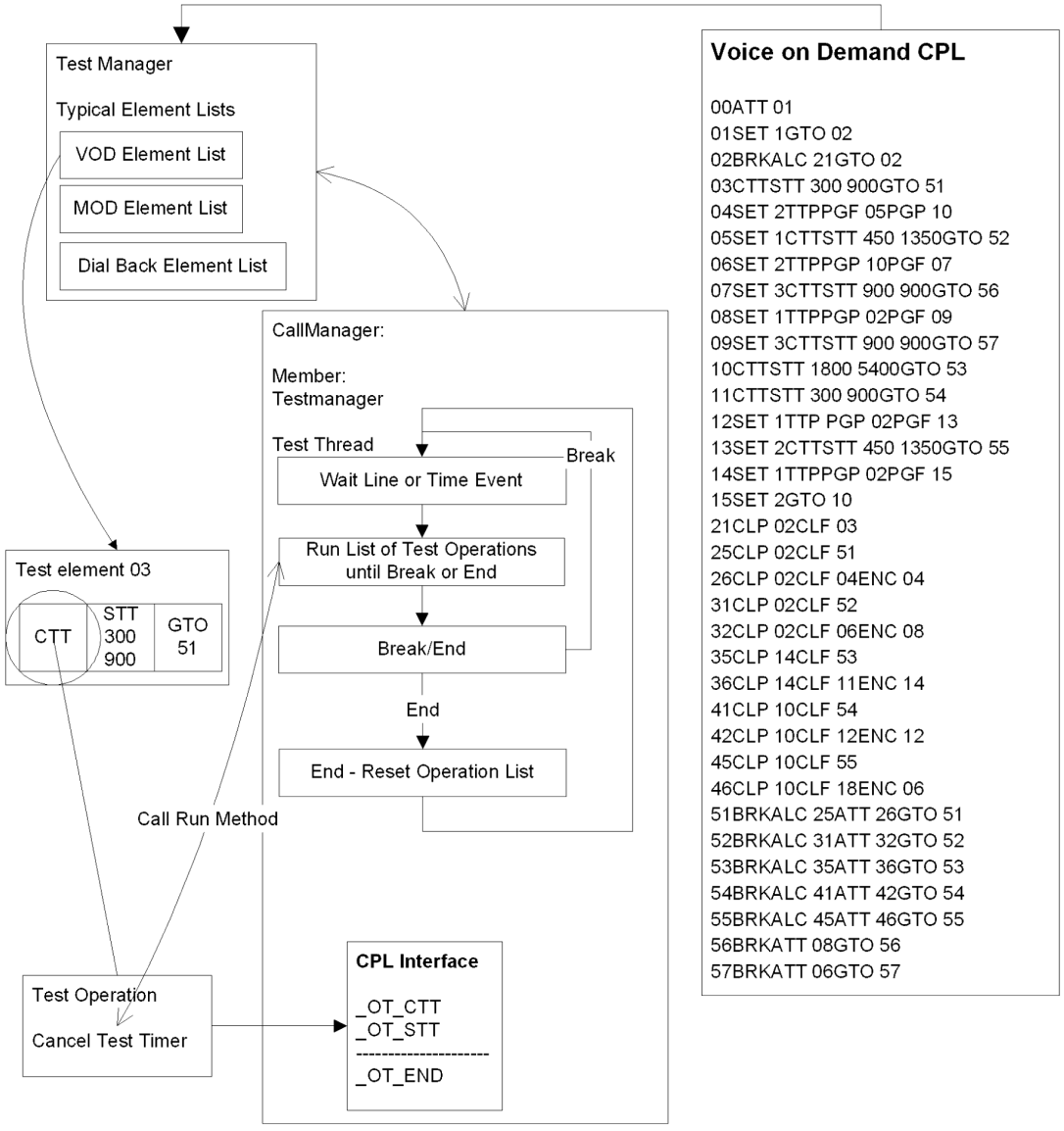

Figure 20 CPL to Test Sequence Schematic

FUJ00171956

6.2.6.a Protected Members

static CCallManager*	_m_pThis	Static pointer to this
CEiconManager*	m_pEiconManager	Pointer to the Eicon Manager instance
static eFailMode	_m_FailMode	Current fail mode status for CCS
CTestManager	m_TestManager	Test Manager member
CRegistryManager	m_RegistryManager	Registry Manager
CTestMode	m_TestMode	Current Failure Condition
CTimerManager*	m_pTimerManager	Timer Manager
CPingManager	m_PingManager	Ping Manager
eCallResult	m_crLastResult	Result of last call
CCallPlan	m_CallPlan	Call Plan
BOOL	m_bPingSucceeded	Did the last ping succeed
int	m_iLocalCallAttempts	Number of local call attempts
int	m_iSuccessfulCallAttempts	Number of successful local call attempts
int	m_iFailedCallAttempts	Number of failed local call attempts
int	m_iStoredMode	Store the last connection mode
static BOOL	_m_bCallPlanOK	Is Call Plan stored OK
BOOL	m_bIsEicon	Do we have Eicon available
DWORD	m_dwTesterThreadId	Tester Thread ID
DWORD	m_dwTesterExitCode	Test Exit Code
HANDLE	m_hTesterShutdownEvent	Handle to event for thread shutdown
HANDLE	m_hTesterThread	Handle to tester thread
HANDLE	m_hSetToLast	Handle to event to set return to previous test sequence.
HANDLE	m_hCallActivated	Event indicating call activated
HANDLE	m_hCallClosed	Event indicating call closed
HANDLE	m_hStartTest	Event indicating test started
HANDLE	m_hStartCPTest	Event indicating new Call Plan period
HANDLE	m_hSetMode3	Event to set Mode 3
HANDLE	m_hNormalTest	Event to run Normal Test
HANDLE	m_hImpTestComplete	Event indicating Implementation test complete
HANDLE	m_hReset	Reset CNIM parameters
HANDLE	m_hStartDialBack	Start dial back sequence
HANDLE	m_hLineUp	Line Up event handle
HANDLE	m_hLineDown	Line Down event handle
CRITICAL_SECTION	m_CS_ServiceType	Protect Get Service Type
static CRITICAL_SECTION	_m_CS_FailMode	Protect Get Fail Mode
static CRITICAL_SECTION	_m_CS_TestMode	Protect Test Mode
static CRITICAL_SECTION	_m_CS_RunMode	Protect Run Mode
static CRITICAL_SECTION	_m_CS	Protect Initialisation
static CRITICAL_SECTION	_m_CS_ConType	Protect Get Connection Type

6.2.7 CCallPlan

This class is responsible for reading the text file containing Call Plan information and storing it as a set of Call Plan elements.

FUJ00171956

6.1.8 CTestManager

A TestManager object is held by the Call Manager and controls the complete line test sequence. The Test Manager holds a set of test elements for each test scenario, where each test element comprises a set of test operations.

The Test Manager will be initialised at service start up to read in each range of elements from registry and to check that each element can be parsed and that the range is complete. There should be no missing links in the chain of elements.

The following test sequences must be provided:

E Range for FRIACO Establish

F Range for FRIACO Fixed

D Range for Metered (Dialled) Fixed

I Range for Voice on Demand

P Range for Permanent Connection (Satellite)

B Range for Dial Back

N Range for Normal Test

At any given time CNIM will be within one of the above sequences.

6.1.9 CIPAddress

The CIPAddress class supports the creation and manipulation of IP addresses. In general this class is used to convert a string read from text file, into an IP address capable of being recognised by the Win32 API.

6.1.10 CEventLog

The CEventLog class supports the output of events to the NT event log.

FUJ00171956

7 NON FUNCTIONAL REQUIREMENTS

7.1 Performance

Performance requirements are as yet undefined

- The CNIM will not have a significant impact on the performance of other processes.

7.1.1 Registry sizing

Section 4.1.3 specifies the size and number of Registry items used.

7.1.2 Event logging

Section 8.4 estimates the volume of information logged to the NT event log.

7.2 Resilience

This section describes how the CNIM is resilient to various types of failure. The following are discussed:

- Corrupt Policy File
- Terminal failure of the CNIM service

7.2.1 Corrupt Policy File

A corrupt Policy File will necessitate replacement of the gateway counter PC. It would not be possible for CNIM to determine the IP addresses of the VPN servers.

7.2.2 Failure of the CNIM service

A terminal failure of the CNIM service will require a reboot of the gateway counter PC.

7.3 Security

7.3.1 Event Logging

The event logging does not compromise security. It does reveal the state of the CNIM at various times.

7.4 Systems Manageability

7.4.1 Installation/Removal

The installation procedure for the CNIM service is as follows:

1. Enter installation registry entries from CNIM.reg file
2. Run CNIM.exe with a –install option from an appropriate batch file. CNIM makes the required Service Control Manager calls to register itself as a service. It returns a value of 0 in the event of success and non-zero if an error occurred.

Note that the service does not need to be started because the system will reboot following the installation.

When running the installation functionality CNIM detects which platform it is running on to ensure that it is only installed on the gateway counter (the installation command will be run on both gateways and slaves). This counter state is determined by examining the registry entry

[HKEY_LOCAL_MACHINE\SOFTWARE\ICL\Pathway\Fingerprint\Variables]

The _CType value is set to "Gateway", "Slave" or "Training"

FUJ00171956

If this value is not equal to "Gateway" then CNIM does not register with SCM and returns 0.

CNIM also supports an –uninstall option. This stops and de-registers the service by making the appropriate Service Control Manager calls. It returns a value of 0 in the event of success and non-zero if an error occurred.

7.4.2 Startup and Shutdown procedures

The Service Control Manager will manage the CNIM service by starting the service automatically. Subsequent control is via the Control Service API (OpenService(), StartService(), ControlService()).

For development testing, the CNIM can be controlled using the NT Control Panel Services applet, or the net start/stop console command.

7.4.3 Maintenance

No regular maintenance or housekeeping is required for the components described in this design. Error messages are logged using the NT event log, see section 8. The existing mechanisms for management of the NT event log will be used.

7.4.4 Software Distribution

The files identified in section 11.1 will be distributed by Tivoli.

The service will respond to requests to stop (SERVICE_CONROL_STOP in the service notification handler function). Tivoli can stop the service to undertake software distribution, and can then restart the service.

7.4.5 Year 2K compliance

The deliverables will be Year 2000 compliant.

7.4.6 Finite Date Limits

None.

7.5 Extensibility

There are no extensibility requirements at this time.

FUJ00171956

8 ERROR HANDLING AND EVENT LOGGING

8.1 Logging Requirements

Errors detected by the CNIM service will be logged to the NT event log.

8.2 Event Logging

A list of event log messages is available in Appendix A1.

The event log source name “CNIM” is used:

The event log message .dll is registered via a registry script

The service will make informational entries in the NT application event log when the service is ready to perform work and when it is closing down. Any errors will also be logged.

8.3 Auditing

There are no specific auditing requirements associated with this design.

8.4 Event Logging Estimates

This section estimates the volume of information logged to the NT event log.

Activity	Number of messages logged
Service startup	12
Service shut down	1
InitiateCrypt entries added to policy File	4

Table 117 Event Logging Estimates

FUJ00171956

9 TARGET ENVIRONMENT

Outlet Gateway PC.

FUJ00171956

10 TESTING REQUIREMENTS

See [Ref 21]

FUJ00171956

11 DELIVERABLES

11.1 Software

The following form the software deliverables:

File	Description
CNIM.exe	CNIM service
CNIM_msg.dll	CNIM message .dll
CNIM_API.dll	CNIM API .dll
CNIMConfig.exe	CNIM configuration executable
CNIM.reg	Initialise CNIM registry settings

These files will be installed/run on the gateway counter PC.

11.2 Documentation

A handover document gives instructions on how to install CNIM.

FUJ00171956

12 ASSUMPTIONS AND RISKS

12.1 ASSUMPTIONS

The following assumptions have been made concerning this development. The risk of these assumptions not being valid is discussed below:

ASS	DESCRIPTION
A1	The requirements identified in section 2 are complete and correct.

12.2 RISKS

The following risks are associated with this development:

RISK	SEVERITY	DESCRIPTION
R1	MEDIUM	All assumptions (see section 12.1) are valid

FUJ00171956

13 DESIGN CONFORMANCE

This table provides a measure of the compliance of the design against the requirements described in section 2.

The following syntax is used in the Conform column:

A * indicates that the requirement has been satisfied

A * followed by a reference number indicates that the requirement has been satisfied and specifies where in the design the requirement is satisfied

A * indicates a non-conformance

A **D** indicates a dependency on another development

The Comments column can be used to add any additional information (there should be no non conformances or dependencies without a description in the comments column]

Tag	Doc	Ref	Description	Conform	Comments
1		5.1	The CNIM shall run as an NT service under the LocalSystem account. The service shall start automatically.	*	
2		5.3	CNIM will configure the Eicon card in a manner which is consistent with the mode of operation required.	*	
3		5.4	CNIM configuration of the Eicon card and mode of operation will be within the concept of a Network Service Type that is assigned to the outlet.	*	
4		5.5	Outlet configuration data for phone numbers and Network Service Type is delivered via a CDF. See [Ref 21]. CNIM is required to retrieve CDF data from registry.	*	
5		5.6	CNIM configuration of the Eicon card and mode of operation will be within the concept of a Call Plan that is generic across all outlets.	*	
6		5.7	CNIM will log each call to a Monitor file and produce a Summary file of the calls for each day.	*	
7		5.8	If CNIM detects that the Data Centre has attempted to contact the outlet whilst the line is disconnected, it will go into KeepAlive mode to cause the line to connect.	*	
9		5.14	During certain periods of the day CNIM is required to maintain the line connection to eliminate the call setup time.	*	

FUJ00171956

			CNIM may also be required to maintain line connection if a call from the Data Centre to the outlet has been detected.		
10		5.15	All times used by CNIM will be in UTC with the exception of times specified within the Call Plan. Call Plan times will be in local time so that the same Call Plan can be used throughout the year.	*	
11		5.16	CNIM will accept a "GetStatus" query from an external source. CNIM will return data related to the current connection type and status.	*	
12		5.17	CNIM is required to supply two static test modes: Implementation Test Normal Test	*	

FUJ00171956

Appendix A1. CALL PLAN - CNIM 1,2,3

Note: All times in the Call Plan are considered to be local time.

```
;CNIM Call Plan
;PC=Permanent Connection
;MOD=Metered-On-Demand
;VOD=Voice on Demand
;MF=Metered-Fixed
;FE=FRIACO Establish
;FF=FRIACO Fixed

[2]
;Satellite
DefaultConnType = PC

Day=     Monday
Period=  00:00-24:00
ConnType=        PC

Day=     Tuesday
Period=  00:00-24:00
ConnType=        PC

Day=     Wednesday
Period=  00:00-24:00
ConnType=        PC

Day=     Thursday
Period=  00:00-24:00
ConnType=        PC

Day=     Friday
Period=  00:00-24:00
ConnType=        PC

Day=     Saturday
Period=  00:00-24:00
ConnType=        PC

Day=     Sunday
Period=  00:00-24:00
ConnType=        PC

[1]
;Voice
DefaultConnType = VOD

Day=     Monday
Period=  00:00-24:00
ConnType=        VOD

Day=     Tuesday
Period=  00:00-24:00
ConnType=        VOD

Day=     Wednesday
```

FUJ00171956


```
Period= 00:00-24:00
ConnType=       VOD

Day=    Thursday
Period= 00:00-24:00
ConnType=       VOD

Day=    Friday
Period= 00:00-24:00
ConnType=       VOD

Day=    Saturday
Period= 00:00-24:00
ConnType=       VOD

Day=    Sunday
Period= 00:00-24:00
ConnType=       VOD

[4]
;Bronze
DefaultConnType = MOD

Day=    Monday
Period= 00:00-24:00
ConnType=       MOD

Day=    Tuesday
Period= 00:00-24:00
ConnType=       MOD

Day=    Wednesday
Period= 00:00-24:00
ConnType=       MOD

Day=    Thursday
Period= 00:00-24:00
ConnType=       MOD

Day=    Friday
Period= 00:00-24:00
ConnType=       MOD

Day=    Saturday
Period= 00:00-24:00
ConnType=       MOD

Day=    Sunday
Period= 00:00-24:00
ConnType=       MOD

[5]
;Silver PartTime A (Metered)
DefaultConnType = MOD

Day=    Monday
```

FUJ00171956

Period= 00:00-08:30, 08:30-10:30, 10:30-24:00
ConnType= MOD, MF, MOD

Day= Tuesday
Period= 00:00-08:30, 08:30-09:30, 09:30-24:00
ConnType= MOD, MF, MOD

Day= Wednesday
Period= 00:00-24:00
ConnType= MOD

Day= Thursday
Period= 00:00-08:30, 08:30-09:30, 09:30-24:00
ConnType= MOD, MF, MOD

Day= Friday
Period= 00:00-24:00
ConnType= MOD

Day= Saturday
Period= 00:00-24:00
ConnType= MOD

Day= Sunday
Period= 00:00-24:00
ConnType= MOD

[6]
;Silver PartTime B (Metered)
DefaultConnType = MOD

Day= Monday
Period= 00:00-24:00
ConnType= MOD

Day= Tuesday
Period= 00:00-24:00
ConnType= MOD

Day= Wednesday
Period= 00:00-24:00
ConnType= MOD

Day= Thursday
Period= 00:00-24:00
ConnType= MOD

Day= Friday
Period= 00:00-24:00
ConnType= MOD

Day= Saturday
Period= 00:00-08:30, 08:30-12:30, 12:30-24:00
ConnType= MOD, MF, MOD

Day= Sunday

FUJ00171956


```
Period= 00:00-24:00
ConnType=       MOD

[7]
;FRIACO Silver Daytime A
DefaultConnType = MOD

Day=    Monday
Period= 00:00-01:00,    01:00-08:00,    08:00-17:30,    17:30-24:00
ConnType=       MOD,            FE,             FF,             MOD

Day=    Tuesday
Period= 00:00-01:00,    01:00-08:00,    08:00-17:30,    17:30-24:00
ConnType=       MOD,            FE,             FF,             MOD

Day=    Wednesday
Period= 00:00-01:00,    01:00-08:00,    08:00-17:30,    17:30-24:00
ConnType=       MOD,            FE,             FF,             MOD

Day=    Thursday
Period= 00:00-01:00,    01:00-08:00,    08:00-17:30,    17:30-24:00
ConnType=       MOD,            FE,             FF,             MOD

Day=    Friday
Period= 00:00-01:00,    01:00-08:00,    08:00-17:30,    17:30-24:00
ConnType=       MOD,            FE,             FF,             MOD

Day=    Saturday
Period= 00:00-01:00,    01:00-08:00,    08:00-13:00,    13:00-24:00
ConnType=       MOD,            FE,             FF,             MOD

Day=    Sunday
Period= 00:00-01:00,    01:00-08:00,    08:00-24:00
ConnType=       MOD,            FE,             MOD

[8]
;FRIACO Silver Daytime B
DefaultConnType = MOD

Day=    Monday
Period= 00:00-01:00,    01:00-08:00,    08:00-17:30,    17:30-24:00
ConnType=       MOD,            FE,             FF,             MOD

Day=    Tuesday
Period= 00:00-01:00,    01:00-08:00,    08:00-17:30,    17:30-24:00
ConnType=       MOD,            FE,             FF,             MOD

Day=    Wednesday
Period= 00:00-01:00,    01:00-08:00,    08:00-17:30,    17:30-24:00
ConnType=       MOD,            FE,             FF,             MOD

Day=    Thursday
Period= 00:00-01:00,    01:00-08:00,    08:00-17:30,    17:30-24:00
ConnType=       MOD,            FE,             FF,             MOD

Day=    Friday
```

FUJ00171956


```
Period= 00:00-01:00,    01:00-08:00,    08:00-17:30,    17:30-24:00
ConnType=       MOD,            FE,             FF,             MOD

Day=    Saturday
Period= 00:00-01:00,    01:00-08:00,    08:00-13:00,    13:00-24:00
ConnType=       MOD,            FE,             FF,             MOD

Day=    Sunday
Period= 00:00-01:00,    01:00-08:00,    08:00-24:00
ConnType=       MOD,            FE,             MOD


[9]
;Non FRIACO Silver Daytime
DefaultConnType = MOD

Day=    Monday
Period= 00:00-08:00,    08:00-17:30,    17:30-24:00
ConnType=       MOD,            MF,             MOD

Day=    Tuesday
Period= 00:00-08:00,    08:00-17:30,    17:30-24:00
ConnType=       MOD,            MF,             MOD

Day=    Wednesday
Period= 00:00-08:00,    08:00-17:30,    17:30-24:00
ConnType=       MOD,            MF,             MOD

Day=    Thursday
Period= 00:00-08:00,    08:00-17:30,    17:30-24:00
ConnType=       MOD,            MF,             MOD

Day=    Friday
Period= 00:00-08:00,    08:00-17:30,    17:30-24:00
ConnType=       MOD,            MF,             MOD

Day=    Saturday
Period= 00:00-08:00,    08:00-13:00,    13:00-24:00
ConnType=       MOD,            MF,             MOD

Day=    Sunday
Period= 00:00-24:00
ConnType=       MOD

[10]
;FRIACO 24HR C1
DefaultConnType = MF

Day=    Monday
Period= 00:00-01:00,    01:00-17:30,    17:30-24:00
ConnType=       MF,             FF,             MF

Day=    Tuesday
Period= 00:00-01:00,    01:00-17:30,    17:30-24:00
ConnType=       MF,             FF,             MF
```

FUJ00171956


```
Day=     Wednesday
Period= 00:00-01:00,     01:00-17:30,     17:30-24:00
ConnType=       MF,              FF,              MF

Day=     Thursday
Period= 00:00-01:00,     01:00-17:30,     17:30-24:00
ConnType=       MF,              FF,              MF

Day=     Friday
Period= 00:00-01:00,     01:00-17:30,     17:30-24:00
ConnType=       MF,              FF,              MF

Day=     Saturday
Period= 00:00-01:00,     01:00-13:00,     13:00-24:00
ConnType=       MF,              FF,              MF

Day=     Sunday
Period= 00:00-01:00,     01:00-08:00,     08:00-24:00
ConnType=       MF,              FF,              MF

[11]
;FRIACO 24HR C2
DefaultConnType = MF

Day=     Monday
Period= 00:00-01:00,     01:00-17:30,     17:30-24:00
ConnType=       MF,              FF,              MF

Day=     Tuesday
Period= 00:00-01:00,     01:00-17:30,     17:30-24:00
ConnType=       MF,              FF,              MF

Day=     Wednesday
Period= 00:00-01:00,     01:00-17:30,     17:30-24:00
ConnType=       MF,              FF,              MF

Day=     Thursday
Period= 00:00-01:00,     01:00-17:30,     17:30-24:00
ConnType=       MF,              FF,              MF

Day=     Friday
Period= 00:00-01:00,     01:00-17:30,     17:30-24:00
ConnType=       MF,              FF,              MF

Day=     Saturday
Period= 00:00-01:00,     01:00-13:00,     13:00-24:00
ConnType=       MF,              FF,              MF

Day=     Sunday
Period= 00:00-01:00,     01:00-08:00,     08:00-24:00
ConnType=       MF,              FF,              MF

[12]
;Non FRIACO Silver 24HR
DefaultConnType = MF
```

FUJ00171956

Day= Monday
Period= 00:00-24:00
ConnType= MF

Day= Tuesday
Period= 00:00-24:00
ConnType= MF

Day= Wednesday
Period= 00:00-24:00
ConnType= MF

Day= Thursday
Period= 00:00-24:00
ConnType= MF

Day= Friday
Period= 00:00-24:00
ConnType= MF

Day= Saturday
Period= 00:00-24:00
ConnType= MF

Day= Sunday
Period= 00:00-24:00
ConnType= MF

[13]
;ADSL

Day= Monday
Period= 00:00-08:00, 08:00-17:30, 17:30-24:00
ConnType= AE, AF, AE

Day= Tuesday
Period= 00:00-08:00, 08:00-17:30, 17:30-24:00
ConnType= AE, AF, AE

Day= Wednesday
Period= 00:00-08:00, 08:00-17:30, 17:30-24:00
ConnType= AE, AF, AE

Day= Thursday
Period= 00:00-08:00, 08:00-17:30, 17:30-24:00
ConnType= AE, AF, AE

Day= Friday
Period= 00:00-08:00, 08:00-17:30, 17:30-24:00
ConnType= AE, AF, AE

FUJ00171956

Day= Saturday
Period= 00:00-08:00, 08:00-13:00, 13:00-24:00
ConnType= AE, AF, AE

Day= Sunday
Period= 00:00-24:00
ConnType= AE

FUJ00171956

Appendix A2. CALL PLAN - CNIM 4 - S92 FOR BNR

The Call Plan for CNIM is as above with the exceptions of table13 which has new connection type names and a new table 14 for ADSL with ISDN automatic backup.

```
;CNIM Call Plan
;PC=Permanent Connection
;MOD=Metered on Demand
;VOD=Voice on Demand
;MF=Metered Fixed
;FE=FRIACO Establish
;FF=FRIACO Fixed

[2]
;Satellite
DefaultConnType = PC

Day=    Monday
Period=         00:00-24:00
ConnType=       PC

Day=    Tuesday
Period=         00:00-24:00
ConnType=       PC

Day=    Wednesday
Period=         00:00-24:00
ConnType=       PC

Day=    Thursday
Period=         00:00-24:00
ConnType=       PC

Day=    Friday
Period=         00:00-24:00
ConnType=       PC

Day=    Saturday
Period=         00:00-24:00
ConnType=       PC

Day=    Sunday
Period=         00:00-24:00
ConnType=       PC
```

FUJ00171956

[3]
;Frame Relay

Day= Monday
Period= 00:00-08:00, 08:00-17:30, 17:30-24:00
ConnType= FRE, FRF, FRE

Day= Tuesday
Period= 00:00-08:00, 08:00-17:30, 17:30-24:00
ConnType= FRE, FRF, FRE

Day= Wednesday
Period= 00:00-08:00, 08:00-17:30, 17:30-24:00
ConnType= FRE, FRF, FRE

Day= Thursday
Period= 00:00-08:00, 08:00-17:30, 17:30-24:00
ConnType= FRE, FRF, FRE

Day= Friday
Period= 00:00-08:00, 08:00-17:30, 17:30-24:00
ConnType= FRE, FRF, FRE

Day= Saturday
Period= 00:00-08:00, 08:00-13:00, 13:00-24:00
ConnType= FRE, FRF, FRE

Day= Sunday
Period= 00:00-24:00
ConnType= FRE

[1]
;Voice
DefaultConnType = VOD

Day= Monday
Period= 00:00-08:00, 08:00-20:30, 20:30-24:00
ConnType= VOD, VODG, VOD

Day= Tuesday
Period= 00:00-08:00, 08:00-20:30, 20:30-24:00
ConnType= VOD, VODG, VOD

FUJ00171956

Day= Wednesday
Period= 00:00-08:00, 08:00-20:30, 20:30-24:00
ConnType= VOD, VODG, VOD

Day= Thursday
Period= 00:00-08:00, 08:00-20:30, 20:30-24:00
ConnType= VOD, VODG, VOD

Day= Friday
Period= 00:00-08:00, 08:00-20:30, 20:30-24:00
ConnType= VOD, VODG, VOD

Day= Saturday
Period= 00:00-08:00, 08:00-20:30, 20:30-24:00
ConnType= VOD, VODG, VOD

Day= Sunday
Period= 00:00-24:00
ConnType= VOD

[4]
;Bronze
DefaultConnType = MOD

Day= Monday
Period= 00:00-08:00, 08:00-20:30, 20:30-24:00
ConnType= MOD, MODG, MOD

Day= Tuesday
Period= 00:00-08:00, 08:00-20:30, 20:30-24:00
ConnType= MOD, MODG, MOD

Day= Wednesday
Period= 00:00-08:00, 08:00-20:30, 20:30-24:00
ConnType= MOD, MODG, MOD

Day= Thursday
Period= 00:00-08:00, 08:00-20:30, 20:30-24:00
ConnType= MOD, MODG, MOD

Day= Friday
Period= 00:00-08:00, 08:00-20:30, 20:30-24:00
ConnType= MOD, MODG, MOD

Day= Saturday

FUJ00171956


```
Period=      00:00-08:00,   08:00-20:30,   20:30-24:00
ConnType=    MOD,           MODG,          MOD

Day=   Sunday
Period=      00:00-24:00
ConnType=    MOD

[5]
;Silver PartTime A (Metered)
DefaultConnType = MOD

Day=   Monday
Period=      00:00-08:00,   08:00-08:30   08:30-10:30,   10:30-20:30,   20:30-24:00
ConnType=    MOD,           MODG,         MFG,           MODG,          MOD

Day=   Tuesday
Period=      00:00-08:00,   08:00-08:30   08:30-09:30,   09:30-20:30,   20:30-24:00
ConnType=    MOD,           MODG,         MFG,           MODG,          MOD

Day=   Wednesday
Period=      00:00-08:00,   08:00-20:30,   20:30-24:00
ConnType=    MOD,           MODG,          MOD

Day=   Thursday
Period=      00:00-08:00,   08:00-08:30   08:30-09:30,   09:30-20:30,   20:30-24:00
ConnType=    MOD,           MODG,         MFG,           MODG,          MOD

Day=   Friday
Period=      00:00-08:00,   08:00-20:30,   20:30-24:00
ConnType=    MOD,           MODG,          MOD

Day=   Saturday
Period=      00:00-08:00,   08:00-20:30,   20:30-24:00
ConnType=    MOD,           MODG,          MOD

Day=   Sunday
Period=      00:00-24:00
ConnType=    MOD

[6]
;Silver PartTime B (Metered)
DefaultConnType = MOD

Day=   Monday
Period=      00:00-08:00,   08:00-20:30,   20:30-24:00
```

FUJ00171956

ConnType= MOD, MODG, MOD

Day= Tuesday
Period= 00:00-08:00, 08:00-20:30, 20:30-24:00
ConnType= MOD, MODG, MOD

Day= Wednesday
Period= 00:00-08:00, 08:00-20:30, 20:30-24:00
ConnType= MOD, MODG, MOD

Day= Thursday
Period= 00:00-08:00, 08:00-20:30, 20:30-24:00
ConnType= MOD, MODG, MOD

Day= Friday
Period= 00:00-08:00, 08:00-20:30, 20:30-24:00
ConnType= MOD, MODG, MOD

Day= Saturday
Period= 00:00-08:00, 08:00-08:30 08:30-12:30, 12:30-20:30, 20:30-24:00
ConnType= MOD, MODG, MFG, MODG, MOD

Day= Sunday
Period= 00:00-24:00
ConnType= MOD

[7]
;FRIACO Silver Daytime A
DefaultConnType = MOD

Day= Monday
Period= 00:00-01:00, 01:00-08:00, 08:00-17:30, 17:30-20:30, 20:30-24:00
ConnType= MOD, FE, FFG, MODG, MOD

Day= Tuesday
Period= 00:00-01:00, 01:00-08:00, 08:00-17:30, 17:30-20:30, 20:30-24:00
ConnType= MOD, FE, FFG, MODG, MOD

Day= Wednesday
Period= 00:00-01:00, 01:00-08:00, 08:00-17:30, 17:30-20:30, 20:30-24:00
ConnType= MOD, FE, FFG, MODG, MOD

Day= Thursday
Period= 00:00-01:00, 01:00-08:00, 08:00-17:30, 17:30-20:30, 20:30-24:00
ConnType= MOD, FE, FFG, MODG, MOD

FUJ00171956

Day= Friday
Period= 00:00-01:00, 01:00-08:00, 08:00-17:30, 17:30-20:30, 20:30-24:00
ConnType= MOD, FE, FFG, MODG, MOD

Day= Saturday
Period= 00:00-01:00, 01:00-08:00, 08:00-13:00, 13:00-20:30, 20:30-24:00
ConnType= MOD, FE, FFG, MODG, MOD

Day= Sunday
Period= 00:00-01:00, 01:00-08:00, 08:00-24:00
ConnType= MOD, FE, MOD

[8]
;FRIACO Silver Daytime B
DefaultConnType = MOD

Day= Monday
Period= 00:00-01:00, 01:00-08:00, 08:00-17:30, 17:30-20:30, 20:30-24:00
ConnType= MOD, FE, FFG, MODG, MOD

Day= Tuesday
Period= 00:00-01:00, 01:00-08:00, 08:00-17:30, 17:30-20:30, 20:30-24:00
ConnType= MOD, FE, FFG, MODG, MOD

Day= Wednesday
Period= 00:00-01:00, 01:00-08:00, 08:00-17:30, 17:30-20:30, 20:30-24:00
ConnType= MOD, FE, FFG, MODG, MOD

Day= Thursday
Period= 00:00-01:00, 01:00-08:00, 08:00-17:30, 17:30-20:30, 20:30-24:00
ConnType= MOD, FE, FFG, MODG, MOD

Day= Friday
Period= 00:00-01:00, 01:00-08:00, 08:00-17:30, 17:30-20:30, 20:30-24:00
ConnType= MOD, FE, FFG, MODG, MOD

Day= Saturday
Period= 00:00-01:00, 01:00-08:00, 08:00-13:00, 13:00-20:30, 20:30-24:00
ConnType= MOD, FE, FFG, MODG, MOD

Day= Sunday
Period= 00:00-01:00, 01:00-08:00, 08:00-24:00
ConnType= MOD, FE, MOD

FUJ00171956

[9]
;Non FRIACO Silver Daytime
DefaultConnType = MOD

Day=	Monday				
Period=	00:00-08:00,	08:00-17:30,	17:30-20:30,	20:30-24:00	
ConnType=	MOD,	MFG,	MODG,	MOD	
Day=	Tuesday				
Period=	00:00-08:00,	08:00-17:30,	17:30-20:30,	20:30-24:00	
ConnType=	MOD,	MFG,	MODG,	MOD	
Day=	Wednesday				
Period=	00:00-08:00,	08:00-17:30,	17:30-20:30,	20:30-24:00	
ConnType=	MOD,	MFG,	MODG,	MOD	
Day=	Thursday				
Period=	00:00-08:00,	08:00-17:30,	17:30-20:30,	20:30-24:00	
ConnType=	MOD,	MFG,	MODG,	MOD	
Day=	Friday				
Period=	00:00-08:00,	08:00-17:30,	17:30-20:30,	20:30-24:00	
ConnType=	MOD,	MFG,	MODG,	MOD	
Day=	Saturday				
Period=	00:00-08:00,	08:00-13:00,	13:00-20:30,	20:30-24:00	
ConnType=	MOD,	MFG,	MODG,	MOD	
Day=	Sunday				
Period=	00:00-24:00				
ConnType=	MOD				

[10]
;FRIACO 24HR C1
DefaultConnType = MF

Day=	Monday				
Period=	00:00-01:00,	01:00-08:00,	08:00-17:30,	17:30-20:30,	20:30-24:00
ConnType=	MF,	FF,	FFG,	MFG,	MF
Day=	Tuesday				
Period=	00:00-01:00,	01:00-08:00,	08:00-17:30,	17:30-20:30,	20:30-24:00
ConnType=	MF,	FF,	FFG,	MFG,	MF

FUJ00171956

Day= Wednesday
Period= 00:00-01:00, 01:00-08:00, 08:00-17:30, 17:30-20:30, 20:30-24:00
ConnType= MF, FF, FFG, MFG, MF

Day= Thursday
Period= 00:00-01:00, 01:00-08:00, 08:00-17:30, 17:30-20:30, 20:30-24:00
ConnType= MF, FF, FFG, MFG, MF

Day= Friday
Period= 00:00-01:00, 01:00-08:00, 08:00-17:30, 17:30-20:30, 20:30-24:00
ConnType= MF, FF, FFG, MFG, MF

Day= Saturday
Period= 00:00-01:00, 01:00-08:00, 08:00-13:00, 13:00-20:30, 20:30-24:00
ConnType= MF, FF, FFG, MFG, MF

Day= Sunday
Period= 00:00-01:00, 01:00-08:00, 08:00-24:00
ConnType= MF, FF, MF

[11]
;FRIACO 24HR C2
DefaultConnType = MF

Day= Monday
Period= 00:00-01:00, 01:00-08:00, 08:00-17:30, 17:30-20:30, 20:30-24:00
ConnType= MF, FF, FFG, MFG, MF

Day= Tuesday
Period= 00:00-01:00, 01:00-08:00, 08:00-17:30, 17:30-20:30, 20:30-24:00
ConnType= MF, FF, FFG, MFG, MF

Day= Wednesday
Period= 00:00-01:00, 01:00-08:00, 08:00-17:30, 17:30-20:30, 20:30-24:00
ConnType= MF, FF, FFG, MFG, MF

Day= Thursday
Period= 00:00-01:00, 01:00-08:00, 08:00-17:30, 17:30-20:30, 20:30-24:00
ConnType= MF, FF, FFG, MFG, MF

Day= Friday
Period= 00:00-01:00, 01:00-08:00, 08:00-17:30, 17:30-20:30, 20:30-24:00
ConnType= MF, FF, FFG, MFG, MF

Day= Saturday

FUJ00171956

Period= 00:00-01:00, 01:00-08:00, 08:00-13:00, 13:00-20:30, 20:30-24:00
ConnType= MF, FF, FFG, MFG, MF

Day= Sunday
Period= 00:00-01:00, 01:00-08:00, 08:00-24:00
ConnType= MF, FF, MF

[12]
;Non FRIACO Silver 24HR
DefaultConnType = MF

Day= Monday
Period= 00:00-08:00, 08:00-20:30, 20:30-24:00
ConnType= MF, MFG, MF

Day= Tuesday
Period= 00:00-08:00, 08:00-20:30, 20:30-24:00
ConnType= MF, MFG, MF

Day= Wednesday
Period= 00:00-08:00, 08:00-20:30, 20:30-24:00
ConnType= MF, MFG, MF

Day= Thursday
Period= 00:00-08:00, 08:00-20:30, 20:30-24:00
ConnType= MF, MFG, MF

Day= Friday
Period= 00:00-08:00, 08:00-20:30, 20:30-24:00
ConnType= MF, MFG, MF

Day= Saturday
Period= 00:00-08:00, 08:00-20:30, 20:30-24:00
ConnType= MF, MFG, MF

Day= Sunday
Period= 00:00-24:00
ConnType= MF

[13]
;ADSL

Day= Monday
Period= 00:00-08:00, 08:00-20:30, 20:30-24:00
ConnType= RA, RAG, RA

FUJ00171956


```
Day=    Tuesday
Period=         00:00-08:00,    08:00-20:30,    20:30-24:00
ConnType=       RA,             RAG,            RA

Day=    Wednesday
Period=         00:00-08:00,    08:00-20:30,    20:30-24:00
ConnType=       RA,             RAG,            RA

Day=    Thursday
Period=         00:00-08:00,    08:00-20:30,    20:30-24:00
ConnType=       RA,             RAG,            RA

Day=    Friday
Period=         00:00-08:00,    08:00-20:30,    20:30-24:00
ConnType=       RA,             RAG,            RA

Day=    Saturday
Period=         00:00-08:00,    08:00-20:30,    20:30-24:00
ConnType=       RA,             RAG,            RA

Day=    Sunday
Period=         00:00-24:00
ConnType=       RA

[14]
;RAS = ADSL with ISDN backup

Day=    Monday
Period=         00:00-08:00,    08:00-20:30,    20:30-24:00
ConnType=       RA,             RAIG,           RA

Day=    Tuesday
Period=         00:00-08:00,    08:00-20:30,    20:30-24:00
ConnType=       RA,             RAIG,           RA

Day=    Wednesday
Period=         00:00-08:00,    08:00-21:00,    21:00-21:05,    21:05-24:00
ConnType=       RA,             RAIG,           RIT,            RA

Day=    Thursday
Period=         00:00-08:00,    08:00-20:30,    20:30-24:00
ConnType=       RA,             RAIG,           RA

Day=    Friday
```

FUJ00171956

Period=	00:00-08:00,	08:00-20:30,	20:30-24:00
ConnType=	RA,	RAIG,	RA

Day= Saturday

Period=	00:00-08:00,	08:00-20:30,	20:30-24:00
ConnType=	RA,	RAIG,	RA

Day= Sunday

Period=	00:00-24:00
ConnType=	RA

FUJ00171956

Appendix A3. EVENT LOG MESSAGES

Symbol	Id	Event Text	Type
INITIAL_ERROR	1	No Error	I
ERROR_GENERAL	2	General Error in CNIM:%r%n%1	E
ERROR_EXCEPTION	3	Exception Error in CNIM%r%n%1	E
ERROR_NULL_POINTER	4	Attempting to use a Null pointer%r%n%1	E
ERROR_EXTERNAL_FN	5	Error in another function%r%n%1	E
ERROR_PING_FAILED	6	Error: Ping failed%r%n%1	E
EVMSG_COPYRIGHT	300	%n%1 (%2) %r%nFile Version %3 %r%nCopyright 2002 Fujitsu Services Ltd.	I
EVMSG_CNIM_SERVICE_CREATED	301	Service created	I
EVMSG_CNIM_SERVICE_STOPPED	302	Service stopped	I
EVMSG_CNIM_SERVICE_REMOVED	303	Service removed	I
EVMSG_CNIM_SERVICE_RUNNING	304	Service running	I
EVMSG_CNIM_SERVICE_STOPPING	305	Service stopping	I
EVMSG_CNIM_ERROR_WIN32	306	%1	E
EVMSG_CNIM_STATE_CHANGED	307	Service state changed	I
EVMSG_NO_ERROR	308	Utimaco - No Error	I
EVMSG_USWERR_FILE_NOT_FOUND	309	Utimaco - File not found	E
EVMSG_USWERR_ITEM_ALREADY_EXISTS	310	Utimaco - Item already exists in policy file	I
EVMSG_USWERR_FIO	311	Utimaco - File IO error detected	E
EVMSG_USWERR_INVALID_CFG_FILE	312	Utimaco - Invalid Policy File	E
EVMSG_USWERR_INSUFFICIENT_PRIV	313	Utimaco - You currently do not have the rights to execute the requested action. Usually a password has to be presented in advance	E
EVMSG_USWERR_NOP	314	Utimaco - No operation done	E
EVMSG_USWERR_NOK	315	Utimaco - Function not executed	E
EVMSG_USWERR_FWBUG	316	Utimaco - Internal error detected	E
EVMSG_USWERR_INIT	317	Utimaco - Module not initialized	E
EVMSG_USWERR_ALLOC	318	Utimaco Message: Cannot allocate memory	E
EVMSG_USWERR_READ_FIO	319	Utimaco Message: File IO read error	E
EVMSG_USWERR_WRITE_FIO	320	Utimaco Message: File IO write error	E
EVMSG_USWERR_SESSION_ERR	321	Utimaco Message: General error	E
EVMSG_ACCESS_ERR	322	Utimaco Message: Access not allowed	E
EVMSG_USWERR_OPEN_FAILURE	323	Utimaco Message: An open command was not successful	E
EVMSG_USWERR_NOT_ENOUGH_MEMORY	324	Utimaco Message: Not enough memory	E
EVMSG_USWERR_IPC_FAULT	325	Utimaco Message: General failure of interprocess communication	E
EVMSG_USWERR_WAIT_AND_RETRY	326	Utimaco Message: The service currently does not take calls.	E
EVMSG_USWERR_COMMUNICATE	327	Utimaco Message: General communication failure	E
EVMSG_USWERR_UNEXPECTED_RET_VALUE	328	Utimaco Message: Unexpected return value	E
EVMSG_USWERR_NO_CARDREADER	329	Utimaco Message: No card reader attached	E
EVMSG_USWERR_BUFFER_OVERFLOW	330	Utimaco Message: Buffer overflow	E
EVMSG_USWERR_CARD_NOT_POWERED	331	Utimaco Message: Card is not powered	E
EVMSG_USWERR_TIMEOUT	332	Utimaco Message: A timeout has occurred	E
EVMSG_USWERR_ILLEGAL_CARDTYPE	333	Utimaco Message: Illegal card type	E
EVMSG_USWERR_NOT_SUPPORTED	334	Utimaco Message: The requested functionality is not supported at this time	E
EVMSG_USWERR_ILLEGAL_DRIVER	335	Utimaco Message: Illegal driver	E
EVMSG_USWERR_ILLEGAL_FW_RELEASE	336	Utimaco Message: The connected hardware whose firmware is not useable by this software	E
EVMSG_USWERR_OPEN_FILE	337	Utimaco Message: File opening failed	E
EVMSG_USWERR_CARD_NOT_INSERTED	338	Utimaco Message: Card not inserted	E
EVMSG_USWERR_ILLEGAL_ARGUMENT	339	Utimaco Message: Illegal argument	E
EVMSG_USWERR_SEM_USED	340	Utimaco Message: The semaphore is currently in use	E
EVMSG_USWERR_NO_DRIVER	341	Utimaco Message: No device driver installed	E
EVMSG_USWERR_GENERAL_FAILURE	342	Utimaco Message: General failure	E
EVMSG_USWERR_OUT_OF_SERVICE	343	Utimaco Message: The service is currently not available	E
EVMSG_USWERR_ITEM_NOT_FOUND	344	Utimaco Message: An item (e.g. a key of a specific name) could not be found	I
EVMSG_USWERR_PW_WRONG	345	Utimaco Message: The presented password is wrong	E
EVMSG_USWERR_PW_LOCKED	346	Utimaco Message: The password has been presented several times wrong and is therefore locked. Usually use some administrator tool to unblock it	E
EVMSG_USWERR_IDENTITY_MISMATCH	347	Utimaco Message: The identity does not match a defined cross-check identity	E
EVMSG_USWERR_MULTIPLE_ERRORS	348	Utimaco Message: Multiple errors have occurred. Use this if there is only the possibility to return one error code, but there happened different errors before (e.g. each thread returned a different error and the controlling thread may only report one	E
EVMSG_USWERR_ITEMS_LEFT	349	Utimaco Message: There are still items left, therefore e.g. the directory / structure etc. can't be deleted	E

FUJ00171956

EVMSG_USWERR_CONSISTENCY_CHECK	350	Utimaco Message: Error during consistency check	E
EVMSG_USWERR_ON_BLACKLIST	351	Utimaco Message: The ID is on a blacklist, the requested action is therefore not allowed	E
EVMSG_USWERR_INVALID_HANDLE	352	Utimaco Message: Invalid handle	E
EVMSG_USWERR_SECTION_NOT_FOUND	353	Utimaco Message: Section not found	I
EVMSG_USWERR_ENTRY_NOT_FOUND	354	Utimaco Message: Entry not found	I
EVMSG_USWERR_NO_MORE_SECTIONS	355	Utimaco Message: No more sections	I
EVMSG_USWERR_EOF_REACHED	356	Utimaco Message: End of file reached	I
EVMSG_USWERR_PW_TOO_SHORT	357	Utimaco Message: The length of the password was too short	E
EVMSG_USWERR_PW_TOO_LONG	358	Utimaco Message: The length of the password was too long	E
EVMSG_USWERR_ITEM_EXPIRED	359	Utimaco Message: Some item (e.g. a certificate) has expired.	E
EVMSG_UNKNOWN_UTIMACO_ERROR	360	Utimaco Message: Unknown error.	E
EVMSG_USWERR_SGVPN_DRIVER_NOP	361	Utimaco Message: No operations done in IP filter	I
EVMSG_USWERR_SGVPN_NO_VALID_YET	362	Utimaco Message: Certificate is not valid yet	E
EVMSG_USWERR_PARM1	363	Utimaco Message: The 1st parameter contained an illegal value	E
EVMSG_USWERR_PARM2	364	Utimaco Message: The 2nd parameter contained an illegal value	E
EVMSG_USWERR_PARM3	365	Utimaco Message: The 3rd parameter contained an illegal value	E
EVMSG_USWERR_PARM4	366	Utimaco Message: The 4th parameter contained an illegal value	E
EVMSG_USWERR_PARM5	367	Utimaco Message: The 5th parameter contained an illegal value	E
EVMSG_USWERR_PARM6	368	Utimaco Message: The 6th parameter contained an illegal value	E
EVMSG_USWERR_PARM7	369	Utimaco Message: The 7th parameter contained an illegal value	E
EVMSG_USWERR_NOMATCH	370	Utimaco code not recognised	E
EVMSG_FUNCTION_ENTERED	371	Function entered: %1	I
EVMSG_FUNCTION_LEAVING	372	Function left: %1	I
EVMSG_SGVPN_FAILURE	373	SGVPN Failure:%r%n%1	E
EVMSG_ERROR_FILE	374	File: %1%r%n Gave the error: %2%r%n	E
EVMSG_DEBUG_RUNNING	375	CNIM running in debug mode	I
EVMSG_WINSOCK_ERROR	376	Error %1 in Winsock function '%2'.%r%n%3	E
MSG_EXITING	377	%1 Agent terminated.	I
EVMSG_ERROR_INITIALISE_PORT_MONITOR	378	Cannot initialise port monitor	E
EVMSG_DEBUG	379	Message Text: %1	I
EVMSG_SERVICE_PAUSED	380	Service paused	I
EVMSG_SERVICE_RUNNING	381	Service running	I
EVMSG_ERROR_CANNOT_GET_REGISTRY_CHANGES	382	Error cannot get registry changes	E
EVMSG_ERROR_CREATE_EVENT	383	Error creating event: %1: Error: %2	E
EVMSG_ERROR_IN_CALL_REVERSAL	384	Call reversal has failed	E
EVMSG_ERROR_IN_PING_TIMEOUT	385	Pinger has timed out	E
EVMSG_ERROR_MESSAGE	386	%1	E
EVMSG_ERROR_UNABLE_KEEP_LINE_CLEAR	387	Unable to keep the line clear	E
EVMSG_INFO_RPC_THREAD_SIGNALLED	388	The RPC thread signal caught by CNIM	I
EVMSG_INFO_KEEP_ALIVE_THREAD_SIGNALLED	389	The Keep Alive thread signal caught by CNIM	I
EVMSG_INFO_LOGGER_THREAD_SIGNALLED	390	The Logger thread signal caught by CNIM	I
EVMSG_INFO_PORT_MON_THREAD_SIGNALLED	391	The Port Monitor thread signal caught by CNIM	I
EVMSG_INFO_CALLMON_THREAD_SIGNALLED	392	The Call Monitor thread signal caught by CNIM	I
EVMSG_INFO_EM_THREAD_SIGNALLED	393	The Eicon Manager thread signal caught by CNIM	I
EVMSG_CNIM_ERROR_FILE_NOT_OPENED	394	File: %1%r%n could not be opened. The cause is:%r%n%2	E
EVMSG_ERROR_INCORRECT_DOW_STRING	395	The string: %1%r%n is not a valid day of the week. Check STF File.	E
EVMSG_ERROR_ELEMENT_NOT_INITIALISED	396	Error: An element has not been initialised	E
EVMSG_ERROR_COMMA_MISMATCH	397	Error: The line:%r%n%1%r%n has a different number of entries from the line:%r%n%2	E
EVMSG_ERROR_INCORRECT_CONTYPE_STRING	398	The string: %1%r%n is not a valid connection type. Check STF File.	E
EVMSG_ERROR_INCORRECT_PERIOD_STRING	399	The string: %1%r%n is not a valid period. Check STF File.	E
EVMSG_ERROR_TABLE_NOT_FOUND	400	Table: %1 has not been found.	E
EVMSG_ERROR_DAY_NOT_FOUND	401	Day: %1 has not been found in table: %2	E
EVMSG_ERROR_ELEMENT_NOT_FOUND	402	Element not found for time: %1	E
EVMSG_ERROR_NULL_POINTER	403	Error - Null Pointer	E
EVMSG_ERROR_CANNOT_CREATE_EM_THREAD	404	Cannot create EiconManager thread: Error %1	E
EVMSG_ERROR_CANNOT_CREATE_CALLMON_THREAD	405	Cannot create Call Monitor thread: Error %1	E
EVMSG_ERROR_CANNOT_CREATE_CALLREV_THREAD	406	Cannot create Call Reversal thread: Error %1	E
EVMSG_ERROR_CANNOT_CREATE_PINGER_THREAD	407	Cannot create pinger thread: Error %1	E
EVMSG_ERROR_CANNOT_CREATE_RPC_THREAD	408	Cannot create RPC thread: Error %1	E

FUJ00171956

EVMSG_ERROR_CANNOT_CREATE_PORT_MONITOR_THREAD	409	Cannot create port monitor thread: Error %1	E
EVMSG_ERROR_IN_DATE_IN_FILENAME	410	The date\time stamp contains an invalid entry: %r%n%1	E
EVMSG_INFO_RENAMING_FILE	411	Renaming file:%r%n%1%r%nto%r%n%2	I
EVMSG_ERROR_CANNOT_SET_PROPS_FROM_NAME	412	Cannot set log file properties from name:%r%n%1	E
EVMSG_ERROR_CANNOT_CREATE_CALLMANAGER_THREAD	413	Cannot create the Call Manager thread	E
EVMSG_INFO_CALL_MANAGER_THREAD_SIGNALLED	414	The Call Manager thread signal caught by CNIM	I
EVMSG_ERROR_CAUSE_CODE	415	The call disconnected with the following error code:%r%n%1%r%nwith the following description:%r%n%2	W
EVMSG_ERROR_INVALID_IP_ADDRESS	416	Invalid IP Address:%r%n%1	E
EVMSG_ERROR_CANNOT_CREATE_KA_THREAD	417	Cannot create Keep Alive thread: Error %1	E
EVMSG_ERROR_CANNOT_CREATE_LOGGER_THREAD	418	Cannot create Logger thread: Error %1	E
CNIM_GS_TIMEDOUT_DO_NOT_USE	419	Get Status function timed out	I
CNIM_GS_LINE_EVENT	420	Get Status got a line event	I
CNIM_GS_SERVICE_STOP	421	Get Status got a stop event	I
CNIM_GS_INITIAL	422	Function status not set	I
CNIM_GS_FAIL	423	Get Status function has failed	E
EVMSG_INFO_RPC_MANAGER_INITIALISED	424	RPC Manager Initialised	I
EVMSG_INFO_CALL_MANAGER_INITIALISED	425	Call Manager Initialised	I
EVMSG_INFO_EICON_MANAGER_INITIALISED	426	Eicon Manager Initialised	I
EVMSG_INFO_MESSAGE	427	%1	I
EVMSG_ERROR_CANNOT_UPDATE_REGISTRY	428	Cannot update registry	E
EVMSG_INFO_EICON_INDEX	429	Eicon index set to: %1	I
EVMSG_ERROR_CANNOT_CREATE_CM_THREAD	430	Cannot create Call Manager thread	E
EVMSG_ERROR_CANNOT_CREATE_CM_TESTER_THREAD	431	Cannot create Call Manager Tester thread	E
EVMSG_INFO_TESTER_THREAD_SIGNALLED	432	The Tester thread signal caught by CNIM	I
EVMSG_ERROR_TESTING_CURRENT_NUMBER	433	Error testing current number	E
EVMSG_ERROR_LAYER1_FAIL	434	Layer 1 is down	E
EVMSG_ERROR_UNABLE_RAISE_LAYER_2	435	Unable to raise Layer 2 with Keep Alive	E
EVMSG_ERROR_B1_AT_IDLE_UNDER_TEST	436	B1 Remained Idle during test	E
EVMSG_ERROR_NUMBERS_DIFFER	437	Remote Address differs from Current Number	E
EVMSG_WARNING_FRIACO_AT_DIALAROUND	438	FRIACO is at Dial Around	W
EVMSG_ERROR_INVALID_NUMBER	439	The following number is invalid: %r%n%1	E
EVMSG_ERROR_ALL_NUMBERS_INVALID	440	All Eicon telephone numbers are invalid	E
EVMSG_WARNING_FAIL_MODE_TEMP	441	Failure mode is set to Temporary, Cause Code: %1, Description: %2	E
EVMSG_WARNING_FAIL_MODE_PERM	442	Failure mode is set to Permanent, Cause Code: %1, Description: %2	E
EVMSG_WARNING_FAIL_MODE_NONE	443	Failure mode is set to None	I
EVMSG_WARNING_FAIL_MODE_UNKNOWN	444	Failure mode is set to unknown, Cause Code: %1, Description: %2	I
EVMSG_WARNING_FAIL_MODE_LOST_CONNECTION	445	Failure mode is set to Lost Connection, Cause Code: %1, Description: %2	E
EVMSG_WARNING_FAIL_MODE_FAILED_ONCE	446	Failure mode is set to Failed Once, Cause Code: %1, Description: %2	E
EVMSG_ERROR_CANNOT_CREATE_KEEP_ALIVE_THREAD	447	Cannot create Keep Alive thread: Error %1	E
EVMSG_WARNING_IDI_MODULE_NOT_INITIALISED	448	IDI Module Not Initialised	I
EVMSG_WARNING_IDI_MODULE_INITIALISED	449	IDI Module Initialised	I
EVMSG_WARNING_DIAPI_MODULE_INITIALISED	450	DIAPI Module Initialised	I
EVMSG_WARNING_DIAPI_MODULE_NOT_INITIALISED	451	DIAPI Module Not Initialised	I
EVMSG_ERROR_NO_CALLPLAN	452	No Call Plan file found	E
EVMSG_ERROR_READING_CALLPLAN	453	Error reading Call Plan	E
EVMSG_INFO_NO_IMP_TEST_PASSED	454	The Implementation Test has not yet been passed	I
EVMSG_INFO_IMP_TEST_PASSED	455	The Implementation Test has been Passed	I
EVMSG_INFO_IMP_TEST_FAILED	456	The Implementation Test has been Failed	E
EVMSG_INFO_USING_ISDN	457	Using ISDN Numbers	I
EVMSG_INFO_LINE_CONNECTED_IN_DURING_TEST	458	The test timed out because the line was connected in	W
EVMSG_INFO_STARTING_IMP_TEST	459	Starting Implementation Test	I
EVMSG_INFO_APPLYING_NUMBER	460	Applying %1 To Eicon Card, %2, Type %3	I
EVMSG_INFO_WAITING_FOR_LINE_IDLE	461	Waiting for Line to go Idle	I
EVMSG_INFO_LINE_DID_NOT_GO_IDLE_AFTER_X_SECS	462	Line did not go Idle after %1 seconds	I
EVMSG_INFO_NUMBER_NOT_TESTED	463	Number %1 Not Tested	I
EVMSG_INFO_PINGING_VPN_SERVERS	464	Pinging VPN Servers	I
EVMSG_INFO_PING_REPLIED	465	The Ping Replied	I
EVMSG_INFO_PING_DID_NOT_REPLY	466	The Ping Did Not Reply	I
EVMSG_INFO_NUMBER_PASSED	467	Number %1 Passed	I

FUJ00171956

EVMSG_INFO_NUMBER_FAILED	468	Number %1 Failed	I
EVMSG_INFO_TEST_ABANDONED	469	Test Abandoned on Number: %1	I
EVMSG_INFO_LINE_IS_IDLE	470	Line is Idle	I
EVMSG_INFO_CHECKING_RPC_SERVICE_STARTED	471	Checking That RPC Service Has Started	I
EVMSG_INFO_RPC_SERVICE_HAS_STARTED	472	RPC Service Has Started	I
EVMSG_INFO_NUMBER_TIMED_OUT	473	Number %1 Timed Out	I
EVMSG_INFO_CHECKING_VPN_SERVICE_STARTED	474	Checking That VPN Service Has Started	I
EVMSG_INFO_VPN_SERVICE_HAS_STARTED	475	VPN Service Has Started	I
EVMSG_ERROR_LAYER1_OK	476	Layer 1 is Up	I
EVMSG_INFO_SECONDS_TILL_END_OF_PERIOD	477	Call Plan Period Will End In: %1 Seconds	I
EVMSG_INFO_PERM_FAILURE_SECONDS	478	Failure Mode Will Be Set To Permanent In: %1 Seconds	I
EVMSG_INFO_TEST_TIMER_LENGTH	479	Creating a Test Timer Of: %1 Seconds	I
EVMSG_INFO_KA_UP	480	Keep Alive is Up	I
EVMSG_INFO_KA_DOWN	481	Keep Alive is Down	I
EVMSG_ERROR_CANNOT_CREATE_TM_THREAD	482	Cannot create TimerManager thread: Error %1	E
EVMSG_WARNING_INVALID_CM_DATA	483	Warning: Invalid Data From Connection Manager: %1	W
EVMSG_WARNING_ADSL_ERROR_CODE	484	ADSL Disconnection Code :%1%r%nDescription: %2	W
EVMSG_WARNING_NO_CM_RESPONSE	485	Connection Manager did not respond to reset event	W
EVMSG_WARNING_NET_TYPE_ADSL	486	Network connection changing to ADSL	W
EVMSG_WARNING_NET_TYPE_ISDN	487	Network connection changing to ISDN	W
EVMSG_WARNING_NET_TYPE_GSM	488	Network connection changing to GSM	W
EVMSG_WARNING_NET_TYPE_NDIS	489	Network connection changing to NDIS	W
EVMSG_INFO_NET_CHANGE_SUCCESS	490	Network changed from %1 to %2 at %3	I
EVMSG_ERROR_NET_CHANGE_FAIL	491	Network failed to change from %1 to %2 at %3	E
EVMSG_INFO_BACKUP_TEST	492	Backup Test: %1 pings replied out of %2: Percentage %3	I
EVMSG_INFO_PERM_FAILURE_CANCELLED	493	Permanent Failure Timer Cancelled	I
EVMSG_WARNING_NET_TYPE_IDLE	494	Network connection changing to IDLE	W

FUJ00171956

Appendix A4. CAUSE CODE DESCRIPTIONS

Cause Code (Dec)	Cause Code Hex	CNIM Value	Description
128	80	00000080	0x80"Normal Disconnect"
129	81	00000081	0x81 "Unassigned (Unallocated number)"
130	82	00000082	0x82 "No route to specified transit network"
131	83	00000083	0x83 "No route to destination"
132	84	00000084	0x84 "Channel unacceptable (BT interim)"
133			
134	86	00000086	0x86 "Channel unacceptable"
135	87	00000087	0x87 "Call awarded and being delivered in an established channel"
136			
137			
138			
139			
140			
141			
142			
143			
144	90	00000090	0x90 "Normal call clearing"
145	91	00000091	0x91 "User busy"
146	92	00000092	0x92 "No user responding"
147	93	00000093	0x93 "User alerting, no answer"
148			
149	95	00000095	0x95 "Call rejected"
150	96	00000096	0x96 "Number changed"
151			
152			
153			
154	9A	0000009a	0x9A "Non-selected user clearing"
155	9B	0000009b	0x9B "Destination out of order"
156	9C	0000009c	0x9C "Invalid number format"
157	9D	0000009d	0x9D "Facility rejected"
158	9E	0000009e	0x9E "Response to STATUS ENQUIRY"
159	9F	0000009f	0x9F "Normal unspecified"
160			
161			
162	A2	000000a2	0xA2 "No circuit/channel available"
163			
164			
165			
166	A6	000000a6	0xA6 "Network out of order"
167			
168			
169	A9	000000a9	0xA9 "Temporary failure"
170	AA	000000aa	0xAA "Switching equipment congestion"
171	AB	000000ab	0xAB "Access information discarded"
172	AC	000000ac	0xAC "Requested circuit/channel not available"

FUJ00171956

173			
174			
175	AF	000000af	0xAF "Resource unavailable, unspecified"
176			
177	B1	000000b1	0xB1 "Quality of service unavailable"
178	B2	000000b2	0xB2 "Requested facility not subscribed"
179			
180			
181			
182			
183			
184			
185	B9	000000b9	0xB9 "Bearer capability not authorized"
186	BA	000000ba	0xBA "Bearer capability not authorized"
187			
188			
189			
190			
191	BF	000000bf	0xBF "Service or option not available, unspecified"
192			
193	C1	000000c1	0xC1 "Bearer capability not implemented"
194	C2	000000c2	0xC2 "Channel type not implemented"
195			
196			
197	C5	000000c5	0xC5 "Requested facility not implemented"
198	C6	000000c6	0xC6 "Only restricted information bearer capability available"
199			
200			
201			
202			
203			
204			
205			
206			
207	CF	000000cf	0xCF "Service or option not available, unspecified"
208			
209	D1	000000d1	0xD1 "Invalid call reference value"
210	D2	000000d2	0xD2 "Identified channel does not exist"
211	D3	000000d3	0xD3 "A suspended call exists, but this identity does not"
212	D4	000000d4	0xD4 "Call identity in use"
213	D5	000000d5	0xD5 "No call suspended"
214	D6	000000d6	0xD6 "Call having the requested call identity has been cleared"
215	D7	000000d7	0xD7 "Incompatible destination"
216			
217			
218	DA	000000da	0xDA "Destination address missing or incomplete"
219	DB	000000db	0xDB "Invalid transit network selection"
220			
221			

FUJ00171956

222			
223	DF	000000df	0xDF "Invalid message, unspecified"
224	E0	000000e0	0xE0 "Mandatory Information Element is missing"
225	E1	000000e1	0xE1 "Message type non-existent or not implemented"
226	E2	000000e2	0xE2 "Message not compatible with call state, or not implemented"
227	E3	000000e3	0xE3 "Information Element non-existent or not implemented"
228	E4	000000e4	0xE4 "Invalid Information Element contents"
229	E5	000000e5	0xE5 "Message not compatible with call state"
230	E6	000000e6	0xE6 "Recovery on time expiry"
231			
232			
233			
234			
235			
236			
237			
238			
239	EF	000000ef	0xEF "Protocol Error, unspecified"
240			
241			
242			
243			
244			
245			
246			
247			
248			
249			
250			
251			
252			
253			
254			
255	FF	000000ff	0xFF "Interworking, unspecified"

FUJ00171956

Appendix A5. RAS ERROR CODES

RAS error code are output by Connection Manager to registry and written directly to QOS output by CNIM.

See Appendix A10 for RAS codes prior to S92.

Win 32 RAS Error ID	Connection Manager/ CNIM Value (Hex)	Description
PENDING	00000258	An operation is pending
ERROR_INVALID_PORT_HANDLE	00000259	The port handle is invalid
ERROR_PORT_ALREADY_OPEN	0000025A	The port is already open
ERROR_BUFFER_TOO_SMALL	0000025B	Caller's buffer is too small
ERROR_WRONG_INFO_SPECIFIED	0000025C	Wrong information specified
ERROR_CANNOT_SET_PORT_INFO	0000025D	Cannot set port information
ERROR_PORT_NOT_CONNECTED	0000025E	The port is not connected
ERROR_EVENT_INVALID	0000025F	The event is invalid
ERROR_DEVICE_DOES_NOT_EXIST	00000260	The device does not exist
ERROR_DEVICETYPE_DOES_NOT_EXIST	00000261	The device type does not exist
ERROR_BUFFER_INVALID	00000262	The buffer is invalid
ERROR_ROUTE_NOT_AVAILABLE	00000263	The route is not available
ERROR_ROUTE_NOT_ALLOCATED	00000264	The route is not allocated
ERROR_INVALID_COMPRESSION_SPECIFIED	00000265	Invalid compression specified
ERROR_OUT_OF_BUFFERS	00000266	Out of buffers
ERROR_PORT_NOT_FOUND	00000267	The port was not found
ERROR_ASYNC_REQUEST_PENDING	00000268	An asynchronous request is pending
ERROR_ALREADY_DISCONNECTING	00000269	The port or device is already disconnecting
ERROR_PORT_NOT_OPEN	0000026A	The port is not open
ERROR_PORT_DISCONNECTED	0000026B	The port is disconnected
ERROR_NO_ENDPOINTS	0000026C	There are no endpoints
ERROR_CANNOT_OPEN_PHONEBOOK	0000026D	Cannot open the phone book file.%
ERROR_CANNOT_LOAD_PHONEBOOK	0000026E	Cannot load the phone book file.%
ERROR_CANNOT_FIND_PHONEBOOK_ENTRY	0000026F	Cannot find the phone book entry.%
ERROR_CANNOT_WRITE_PHONEBOOK	00000270	Cannot write the phone book file.%
ERROR_CORRUPT_PHONEBOOK	00000271	Invalid information found in the phone book file.%
ERROR_CANNOT_LOAD_STRING	00000272	Cannot load a string.
ERROR_KEY_NOT_FOUND	00000273	Cannot find key
ERROR_DISCONNECTION	00000274	The port was disconnected.
ERROR_REMOTE_DISCONNECTION	00000275	The data link was terminated by the remote machine.
ERROR_HARDWARE_FAILURE	00000276	The port was disconnected due to hardware failure.
ERROR_USER_DISCONNECTION	00000277	The port was disconnected by the user
ERROR_INVALID_SIZE	00000278	The structure size is incorrect
ERROR_PORT_NOT_AVAILABLE	00000279	The port is already in use or is not configured for Remote Access dial out
ERROR_CANNOT_PROJECT_CLIENT	0000027A	Cannot register your computer on on the remote network.%
ERROR_UNKNOWN	0000027B	Unknown error
ERROR_WRONG_DEVICE_ATTACHED	0000027C	The wrong device is attached to the port

FUJ00171956

ERROR_BAD_STRING	0000027D	The string could not be converted.
ERROR_REQUEST_TIMEOUT	0000027E	The request has timed out.
ERROR_CANNOT_GET_LANA	0000027F	No asynchronous net available
ERROR_NETBIOS_ERROR	00000280	A NetBIOS error has occurred.%
ERROR_SERVER_OUT_OF_RESOURCES	00000281	The server cannot allocate NetBIOS resources needed to support the client
ERROR_NAME_EXISTS_ON_NET	00000282	One of your NetBIOS names is already registered on the remote network
ERROR_SERVER_GENERAL_NET_FAILURE	00000283	A network adapter at the server failed
WARNING_MSG_ALIAS_NOT_ADDED	00000284	You will not receive network message popups
ERROR_AUTH_INTERNAL	00000285	Internal authentication error
ERROR_RESTRICTED_LOGON_HOURS	00000286	The account is not permitted to logon at this time of day
ERROR_ACCT_DISABLED	00000287	The account is disabled
ERROR_PASSWD_EXPIRED	00000288	The password has expired.%
ERROR_NO_DIALIN_PERMISSION	00000289	The account does not have Remote Access permission
ERROR_SERVER_NOT_RESPONDING	0000028A	The Remote Access server is not responding
ERROR_FROM_DEVICE	0000028B	Your modem (or other connecting device) has reported an error
ERROR_UNRECOGNIZED_RESPONSE	0000028C	Unrecognized response from the device
ERROR_MACRO_NOT_FOUND	0000028D	A macro required by the device was not found in the device .INF file section
ERROR_MACRO_NOT_DEFINED	0000028E	A command or response in the device .INF file section refers to an undefined macro
ERROR_MESSAGE_MACRO_NOT_FOUND	0000028F	The <message> macro was not found in the device .INF file section
ERROR_DEFAULTOFF_MACRO_NOT_FOUND	00000290	The <defaultoff> macro in the device .INF file section contains an undefined macro
ERROR_FILE_COULD_NOT_BE_OPENED	00000291	The device .INF file could not be opened
ERROR_DEVICENAME_TOO_LONG	00000292	The device name in the device .INF or media .INI file is too long
ERROR_DEVICENAME_NOT_FOUND	00000293	The media .INI file refers to an unknown device name
ERROR_NO_RESPONSES	00000294	The device .INF file contains no responses for the command.%
ERROR_NO_COMMAND_FOUND	00000295	The device .INF file is missing a command.%
ERROR_WRONG_KEY_SPECIFIED	00000296	Attempted to set a macro not listed in device .INF file section
ERROR_UNKNOWN_DEVICE_TYPE	00000297	The media .INI file refers to an unknown device type
ERROR_ALLOCATING_MEMORY	00000298	Cannot allocate memory
ERROR_PORT_NOT_CONFIGURED	00000299	The port is not configured for Remote Access
ERROR_DEVICE_NOT_READY	0000029A	Your modem (or other connecting device) is not functioning
ERROR_READING_INI_FILE	0000029B	Cannot read the media .INI file
ERROR_NO_CONNECTION	0000029C	The connection dropped
ERROR_BAD_USAGE_IN_INI_FILE	0000029D	The usage parameter in the media .INI file is invalid
ERROR_READING_SECTIONNAME	0000029E	Cannot read the section name from the media .INI file
ERROR_READING_DEVICETYPE	0000029F	Cannot read the device type from the media .INI file
ERROR_READING_DEVICENAME	000002A0	Cannot read the device name from the media .INI file
ERROR_READING_USAGE	000002A1	Cannot read the usage from the media .INI file
ERROR_READING_MAXCONNECTBPS	000002A2	Cannot read the maximum connection BPS rate from the media .INI file
ERROR_READING_MAXCARRIERBPS	000002A3	Cannot read the maximum carrier BPS rate from the media .INI file
ERROR_LINE_BUSY	000002A4	The line is busy

FUJ00171956

ERROR_VOICE_ANSWER	000002A5	A person answered instead of a modem
ERROR_NO_ANSWER	000002A6	There is no answer.%
ERROR_NO_CARRIER	000002A7	Cannot detect carrier
ERROR_NO_DIALTONE	000002A8	There is no dial tone.%
ERROR_IN_COMMAND	000002A9	General error reported by device.%
ERROR_WRITING_SECTIONNAME	000002AA	ERROR_WRITING_SECTIONNAME
ERROR_WRITING_DEVICETYPE	000002AB	ERROR_WRITING_DEVICETYPE
ERROR_WRITING_DEVICENAME	000002AC	ERROR_WRITING_DEVICENAME
ERROR_WRITING_MAXCONNECTBPS	000002AD	ERROR_WRITING_MAXCONNECTBPS
ERROR_WRITING_MAXCARRIERBPS	000002AE	ERROR_WRITING_MAXCARRIERBPS
ERROR_WRITING_USAGE	000002AF	ERROR_WRITING_USAGE
ERROR_WRITING_DEFAULTOFF	000002B0	ERROR_WRITING_DEFAULTOFF
ERROR_READING_DEFAULTOFF	000002B1	ERROR_READING_DEFAULTOFF
ERROR_EMPTY_INI_FILE	000002B2	ERROR_EMPTY_INI_FILE
ERROR_AUTHENTICATION_FAILURE	000002B3	Access denied because username and/or password is invalid on the domain
ERROR_PORT_OR_DEVICE	000002B4	Hardware failure in port or attached device
ERROR_NOT_BINARY_MACRO	000002B5	ERROR_NOT_BINARY_MACRO
ERROR_DCB_NOT_FOUND	000002B6	ERROR_DCB_NOT_FOUND
ERROR_STATE_MACHINES_NOT_STARTED	000002B7	ERROR_STATE_MACHINES_NOT_STARTED
ERROR_STATE_MACHINES_ALREADY_STARTED	000002B8	ERROR_STATE_MACHINES_ALREADY_STARTED
ERROR_PARTIAL_RESPONSE_LOOPING	000002B9	ERROR_PARTIAL_RESPONSE_LOOPING
ERROR_UNKNOWN_RESPONSE_KEY	000002BA	A response keyname in the device .INF file is not in the expected format
ERROR_RECV_BUF_FULL	000002BB	The device response caused buffer overflow.%
ERROR_CMD_TOO_LONG	000002BC	The expanded command in the device .INF file is too long
ERROR_UNSUPPORTED_BPS	000002BD	The device moved to a BPS rate not supported by the COM driver
ERROR_UNEXPECTED_RESPONSE	000002BE	Device response received when none expected.%
ERROR_INTERACTIVE_MODE	000002BF	The Application does not allow user interaction. The connection requires interaction with the user to complete successfully.
ERROR_BAD_CALLBACK_NUMBER	000002C0	ERROR_BAD_CALLBACK_NUMBER
ERROR_INVALID_AUTH_STATE	000002C1	ERROR_INVALID_AUTH_STATE
ERROR_WRITING_INITBPS	000002C2	ERROR_WRITING_INITBPS
ERROR_X25_DIAGNOSTIC	000002C3	X.25 diagnostic indication.%
ERROR_ACCT_EXPIRED	000002C4	The account has expired
ERROR_CHANGING_PASSWORD	000002C5	Error changing password on domain. The password may be too short or may match a previously used password
ERROR_OVERRUN	000002C6	Serial overrun errors were detected while communicating with your modem
ERROR_RASMAN_CANNOT_INITIALIZE	000002C7	RasMan initialization failure. Check the event log
ERROR_BIPLEX_PORT_NOT_AVAILABLE	000002C8	Biplex port initializing. Wait a few seconds and redial
ERROR_NO_ACTIVE_ISDN_LINES	000002C9	No active ISDN lines are available
ERROR_NO_ISDN_CHANNELS_AVAILABLE	000002CA	No ISDN channels are available to make the call
ERROR_TOO_MANY_LINE_ERRORS	000002CB	Too many errors occurred because of poor phone line quality
ERROR_IP_CONFIGURATION	000002CC	The Remote Access IP configuration is unusable
ERROR_NO_IP_ADDRESSES	000002CD	No IP addresses are available in the static pool of Remote Access IP addresses

FUJ00171956

ERROR_PPP_TIMEOUT	000002CE	Timed out waiting for a valid response from the remote PPP peer
ERROR_PPP_REMOTE_TERMINATED	000002CF	PPP terminated by remote machine
ERROR_PPP_NO_PROTOCOLS_CONFIGURED	000002D0	No PPP control protocols configured
ERROR_PPP_NO_RESPONSE	000002D1	Remote PPP peer is not responding
ERROR_PPP_INVALID_PACKET	000002D2	The PPP packet is invalid
ERROR_PHONE_NUMBER_TOO_LONG	000002D3	The phone number including prefix and suffix is too long
ERROR_IPXCP_NO_DIALOUT_CONFIGURED	000002D4	The IPX protocol cannot dial-out on the port because the machine is an IPX router
ERROR_IPXCP_NO_DIALIN_CONFIGURED	000002D5	The IPX protocol cannot dial-in on the port because the IPX router is not installed
ERROR_IPXCP_DIALOUT_ALREADY_ACTIVE	000002D6	The IPX protocol cannot be used for dial-out on more than one port at a time
ERROR_ACCESSING_TCPCFGDLL	000002D7	Cannot access TCPCFG.DLL
ERROR_NO_IP_RAS_ADAPTER	000002D8	Cannot find an IP adapter bound to Remote Access
ERROR_SLIP_REQUIRES_IP	000002D9	SLIP cannot be used unless the IP protocol is installed
ERROR_PROJECTION_NOT_COMPLETE	000002DA	Computer registration is not complete
ERROR_PROTOCOL_NOT_CONFIGURED	000002DB	The protocol is not configured
ERROR_PPP_NOT_CONVERGING	000002DC	The PPP negotiation is not converging
ERROR_PPP_CP_REJECTED	000002DD	The PPP control protocol for this network protocol is not available on the server
ERROR_PPP_LCP_TERMINATED	000002DE	The PPP link control protocol terminated
ERROR_PPP_REQUIRED_ADDRESS_REJECTED	000002DF	The requested address was rejected by the server
ERROR_PPP_NCP_TERMINATED	000002E0	The remote computer terminated the control protocol
ERROR_PPP_LOOPBACK_DETECTED	000002E1	Loopback detected
ERROR_PPP_NO_ADDRESS_ASSIGNED	000002E2	The server did not assign an address
ERROR_CANNOT_USE_LOGON_CREDENTIALS	000002E3	The authentication protocol required by the remote server cannot use the Windows NT encrypted password. Redial, entering the password explicitly
ERROR_TAPI_CONFIGURATION	000002E4	Invalid TAPI configuration
ERROR_NO_LOCAL_ENCRYPTION	000002E5	The local computer does not support the required encryption type
ERROR_NO_REMOTE_ENCRYPTION	000002E6	The remote computer does not support the required encryption type
ERROR_REMOTE_REQUIRES_ENCRYPTION	000002E7	The remote computer requires encryption
ERROR_IPXCP_NET_NUMBER_CONFLICT	000002E8	Cannot use the IPX network number assigned by remote server. Check the event log
ERROR_INVALID_SMM	000002E9	ERROR_INVALID_SMM
ERROR_SMM_UNINITIALIZED	000002EA	ERROR_SMM_UNINITIALIZED
ERROR_NO_MAC_FOR_PORT	000002EB	ERROR_NO_MAC_FOR_PORT
ERROR_SMM_TIMEOUT	000002EC	ERROR_SMM_TIMEOUT
ERROR_BAD_PHONE_NUMBER	000002ED	ERROR_BAD_PHONE_NUMBER
ERROR_WRONG_MODULE	000002EE	ERROR_WRONG_MODULE
ERROR_INVALID_CALLBACK_NUMBER	000002EF	Invalid callback number. Only the characters 0 to 9, T, P, W, (,), -, @, and space are allowed in the number.
ERROR_SCRIPT_SYNTAX	000002F0	A syntax error was encountered while processing a script
ERROR_HANGUP_FAILED	000002F1	The connection could not be disconnected because it was created by the Multi-Protocol Router
INVALID RAS_HANDLE	00000000	The current RAS handle is invalid; Converted to **0x06ee**
UNKNOWN		Code not set; Converted to **0x06ff**

Table 118 RAS Error Codes and CNIM Equivalents

FUJ00171956

Appendix A6. CONNECTION MANAGER CAUSE CODES

The Connection Manager service will output the following two codes, State and Reason, into registry. CNIM will combine these codes to obtain the Cause Code given in the table.

State Code	Registry Abbreviation	Reason Code	Registry Abbreviation	CNIM Code
Connected	'C'	N/A	N/A	0x00000400
Not Connected	'N'	N/A	N/A	0x00000401
Dialling	'D'	N/A	N/A	0x00000402
Failed to Connect	'F'	Timed Out	'T'	0x00000410
Failed to Connect	'F'	Day D request	'D'	0x00000411
Failed to Connect	'F'	Reset request	'R'	0x00000412
Failed to Connect	'F'	Service Stop request	'S'	0x00000413
Failed to Connect	'F'	Blackhole	'B'	0x00000414
Disconnected	'X'	Day D request	'D'	0x00000421
Disconnected	'X	Reset request	'R'	0x00000422
Disconnected	'X	Service Stop request	'S'	0x00000423
Disconnected	'X	Blackhole	'B'	0x00000424

Table 119 Connection Manager Cause Codes

FUJ00171956

Appendix A7. FUJITSU DEFINED CAUSE CODES

These codes are defined within CNIM to cover those cases where a meaningful cause code is not returned to CNIM by the any other interface. This may occur for a number of reasons and includes Layer 1 failure that can be diagnosed and reported by the Eicon card.

User Defined Fault/ Network State	CNIM Value	Description
PING_SUCCESS_CODE	0x00000100	Ping Succeeded
LAYER1_DOWN_CODE	0x00000110	Layer 1 Down
PING_FAIL_CODE	0x00000111	Ping has Failed
L2_STILL_ACTIVATING_CODE	0x00000112	Layer 2 did not finish activating due to network fault
PING_UNKNOWN_CODE	0x00000113	Ping state is unknown
PING_WAITING_CODE	0x00000114	Ping state is waiting for ping reply (when call closed)
SHORT_CALL	0x00000115	Call length less than MCDT or Shorthold
UNKNOWN	0x000001ff	Default code, should not be seen in practise.

Table 120 Fujitsu Defined Cause Codes

FUJ00171956

Appendix A8. CNIM CAUSE CODES

If CNIM service changes state such that the call record is closed the value in the following table is placed in the QOS record.

State Code	Cause Code Hex Value
Service Shutdown	0x00000500

Table 121 CNIM Service State Codes

FUJ00171956

Appendix A9. DIAPI INTERFACE

The NDIS driver is not able to directly interface to user mode applications. Therefore, applications must be developed in user mode interfacing the DIAPI library. The diapi library is developed in Kernel mode. The DIAPI DLL interfaces directly with the NDIS driver. The NDIS driver interfaces with IDI (ISDN driver interface – Didd.sys) which contains the protocol stack. IDI interfaces directly with the ISDN card. This package is intended to work on an ISDN BRI line.

The table below shows the DIAPI functions available to CNIM.

Function	Description
Di_Init()	The Di_Init ( ) function initialises the internal data structures of the diapi library. Di_Init ( ) is the first command called. This function must be called before any other function of the Eicon diapi library can be used. Once called, any or many of the other functions may be called in any random sequence. The last function to be called, however, must be Di_Close ( ) before exiting the application. Calling Di_Init ( ) renders the line state as active (State = I_ACTIVE).
Di_Close( )	The Di_Close ( ) function is the last function to call. This function terminates Diapi. Once Di_Close ( ) is called, the only two options are to exit the application or re-initialise the diapi library. Calling Di_Init( ) is required to re-initialise the diapi library.
int Di_Disable (int chan)	The Di_Disable ( ) function completes after receiving a RELEASE and transmitting a RELEASE COMPLETE to the network layer Q.931. The Q.931 cause code for this function call is 80 90 - Normal Call Clearing. Subsequently, Di_Enable ( ) function must be called for data transfer to continue. During a call setup or a ping, this is seen as a “hardware error”. This is because calling Di_Disable ( ) renders the Eicon adapter inactive and unable to communicate with the ISDN switch. The line state for the Di_Disable ( ) function call is down (State = I_DOWN). Subsequent requests for call set-ups will be rejected unless Di_Enable ( ) is issued.
int Di_Enable (int chan)	The Di_Enable ( ) function completes when a Q931 call setup message SETUP is followed by a call proceeding of the channel id CALL PROC. The connection with the peer is established when we receive a connect RX CONN and then transmit a connect acknowledge CONN ACK. The DindisDiOut line state changes from I_INIT to I_CALLING (CALL PROC). During a call setup or a ping, assuming PPP has been negotiated successfully, a ping reply is the appropriate response. If the Eicon adapter is in an inactive state (Ditrace may indicate this), the adapter may be activated either through the diapi interface by calling Di_Enable ( ) and then choosing a B channel or using dcontrol by clicking on enable.
Int Di_SaveNumbers (pdinumbers pnumbers)	The Di_SaveNumbers ( ) function asks the user to enter the called party numbers, the destination subaddresses, the local origination address, and the local origination subaddress. The user is asked to enter up to 4 called party numbers and 4 destination subaddresses. This information is saved and written to the registry instantaneously. MSN stands for Multiple Subscriber Number, OAD for Origination address. This is the ISDN number of the line the NDIS is attached to. The NDIS driver uses this number to check that it is the destination for any incoming call. With ISDN you can have several devices on the same ISDN line

FUJ00171956

	and usually each is assigned a different number (MSN) so they can decide whether or not to pick up incoming calls. The default value of 0 would mean that incoming calls would only be picked up if the ISDN number of the line ended in a zero (NDIS does a comparison starting from the right digit). *In many installations this is not the case, and as the NDIS is the only device on the ISDN line setting the MSN to Nul means that it will not care what the destination number of an incoming call is, and so will pick the call up (subject to CLI information above).* For called party numbers, the primary number is tried first. If this number fails, then the second number is dialed. If the second number fails to connect then the third number is dialed. If the third number fails to connect the fourth number is dialed. If the fourth number fails to connect, the first number is retried and the process continues in a round robin fashion. Note: The fouth number entered should be the same as any one of the other 3 numbers, in order for the process to work in a round robin fashion.
Int Di_GetNumbers (pdinumbers pnumbers)	The Di_GetNumbers ( ) function retrieves the called party number(s), the destination subaddress(es), the local origination address, and the local origination subaddress. The Di_GetNumbers ( ) function will retrieve the most recent information that was stored in the registry using the Di_SaveNumbers ( ) function. The Di_SaveNumbers ( ) function is, therefore, called at least once for entering user data. Di_GetNumbers ( ) can then be called without having to call Di_SaveNumbers ( ) first.
int Di_SavePwds (char *pwd_inbound, char *pwd_outbound, char *usr_inbound[MAX_USER_NAME_CNT], char *usr_outbound)	The function Di_SavePwds ( ) prompts the user to enter an outbound user id and password, and an inbound user id and password. The outbound user id and password is used for authentication on the remote router. The Outbound User is the PPP username of the NDIS driver (and hence PO Counter). A user account must exist on the remote router. The inbound user id and password is used for authentication on the Eicon Diva adapter. The Inbound user array is a list of PPP usernames of the remote routers (each router can have a different name). The array size of MAX_USER_NAME_CNT is defined as 20 in diapi.h. This means that there could be up to 20 inbound user ids configured to dial into the Eicon NDIS adapter. In Pathway's case CHAP is used for PPP authentication so the Inbound and Outbound Password are set to the same value – usually known as the CHAP 'Secret'. If any of these values is changed it is used on the next time a connection is made or received When LCP is activated by a call, the password information is used to negotiate CHAP. CHAP requires that the same password (key) be used by both peers.
int Di_GetPwds (char *pwd_inbound, char *pwd_outbound, char *usr_inbound[MAX_USER_NAME_CNT], char *usr_outbound)	The function Di_GetPwds ( ) function retrieves both outbound and inbound userid and password information from the registry. The Di_GetPwds ( ) function will retrieve the most recent information that was stored in the registry using the Di_SavePwds ( ) function. The Di_SavePwds ( ) function is, therefore, called at least once for entering user data. Di_GetPwds ( ) can then be called without having to call Di_SavePwds ( ) first. The password information can only be obtained by calling Di_GetPwds ( ). The

FUJ00171956

	password information in the registry is stored in encrypted form, and no password information is present in the output of the Eicon supplied log file utilities such as Ditrace.exe.
int Di_SetCommOpts (pdicommopts pcopts)	The Di_SetCommOpts ( ) function prompts the user to turn broadcast on or off, to enter a values for each of the backoff parameters (Alpha, Beta , M) and to enter a reply timeout value. The broadcast filter is designed to stop any IP packets with a broadcast address from being transmitted over the ISDN line. The reason for this filter is that NT uses broadcast extensively to locate and monitor network resources such as PDC's, drive letter assignments, remote printers, etc. These broadcast packets are sent by NT on a regular basis over every available interface and will result in an ISDN call being initiated or if a call is up will result in the idle timer being reset so lengthening call times. Therefore if you leave the broadcast filter turned off for any length of time you will incur extra ISDN call charges but will also unnecessarily hold open the only ISDN channel you have available for use so preventing other PO locations from dialling in with configuration requests. Also, if a broadcast packet is sent by NT in the time between setting broadcast on and changing the number, a call will be initiated to the previously stored number which although the call will probably fail, CHAP authentication is not desirable. If you do need to leave the broadcast filter off for periods then an option would be to look at explicitly filtering out the ports that NT uses for network traffic - generally UDP port 137 and TCP port 139 and/or remove the bindings for WINS from the NDIS interface.' The alpha, beta and M backoff parameters are described in the algorithm below. a, b and m variables for back off algorithm Back off i.e. If the called number is busy at time T0 then it is retried at times T0 + b, T0 + ab, T0 + a2b,,....,T0 + am-1b, where a,b and m are supplied as profile parameters. The default action is to send all IP packets except those with a broadcast address – this is to prevent Windows Networking broadcasts bringing the ISDN line up unnecessarily. The Shorthold timer indicates that if there is no data traffic or if the line is idle for the amount of second specified, then issue a disconnect. The Shorthold timer is in seconds format. When the Shorthold timer expires, a disconnect DISC will be transmitted TX with a Q931 message of Normal call clearing with Cause 80 90. The reply timer indicates that if the remote peer does not reply to a request (ex. SETUP) then this timer will expire and a disconnect DISC will be transmitted TX with a Q931 message of Normal call clearing with Cause 80 90. The disconnect is issued because of a call time out.
int Di_GetCommOpts (pdicommopts pcopts)	The Di_GetCommOpts ( ) function will retrieve the most recent information that was stored in the registry using the Di_SetCommOpts ( ) function. The Di_SetCommOpts ( ) function is, therefore, called at least once for entering user data. Di_GetCommOpts ( ) can then be called without having to call Di_SetCommOpts ( ) first.

Table 122 DIAPI Functions

FUJ00171956

FUJ00171956

Appendix A10. RAS ERROR CODES - PRE S92

RAS error code are output by Connection Manager to registry and mapped to QOS output by CNIM.

Win 32 RAS Error ID	Win32 Value (Dec)	Connection Manager Value (Hex)	CNIM Value	Description
PENDING	600	00000258	0600	An operation is pending
ERROR_INVALID_PORT_HANDLE	601	00000259	0601	The port handle is invalid
ERROR_PORT_ALREADY_OPEN	602	0000025A	0602	The port is already open
ERROR_BUFFER_TOO_SMALL	603	0000025B	0603	Caller's buffer is too small
ERROR_WRONG_INFO_SPECIFIED	604	0000025C	0604	Wrong information specified
ERROR_CANNOT_SET_PORT_INFO	605	0000025D	0605	Cannot set port information
ERROR_PORT_NOT_CONNECTED	606	0000025E	0606	The port is not connected
ERROR_EVENT_INVALID	607	0000025F	0607	The event is invalid
ERROR_DEVICE_DOES_NOT_EXIST	608	00000260	0608	The device does not exist
ERROR_DEVICETYPE_DOES_NOT_EXIST	609	00000261	0609	The device type does not exist
ERROR_BUFFER_INVALID	610	00000262	060A	The buffer is invalid
ERROR_ROUTE_NOT_AVAILABLE	611	00000263	060B	The route is not available
ERROR_ROUTE_NOT_ALLOCATED	612	00000264	060C	The route is not allocated
ERROR_INVALID_COMPRESSION_SPECIFIED	613	00000265	060D	Invalid compression specified
ERROR_OUT_OF_BUFFERS	614	00000266	060E	Out of buffers
ERROR_PORT_NOT_FOUND	615	00000267	060F	The port was not found
ERROR_ASYNC_REQUEST_PENDING	616	00000268	0610	An asynchronous request is pending
ERROR_ALREADY_DISCONNECTING	617	00000269	0611	The port or device is already disconnecting
ERROR_PORT_NOT_OPEN	618	0000026A	0612	The port is not open
ERROR_PORT_DISCONNECTED	619	0000026B	0613	The port is disconnected
ERROR_NO_ENDPOINTS	620	0000026C	0614	There are no endpoints
ERROR_CANNOT_OPEN_PHONEBOOK	621	0000026D	0615	Cannot open the phone book file.%
ERROR_CANNOT_LOAD_PHONEBOOK	622	0000026E	0616	Cannot load the phone book file.%
ERROR_CANNOT_FIND_PHONEBOOK_ENTRY	623	0000026F	0617	Cannot find the phone book entry.%
ERROR_CANNOT_WRITE_PHONEBOOK	624	00000270	0618	Cannot write the phone book file.%
ERROR_CORRUPT_PHONEBOOK	625	00000271	0619	Invalid information found in the phone book file.%
ERROR_CANNOT_LOAD_STRING	626	00000272	061A	Cannot load a string.
ERROR_KEY_NOT_FOUND	627	00000273	061B	Cannot find key
ERROR_DISCONNECTION	628	00000274	061C	The port was disconnected.
ERROR_REMOTE_DISCONNECTION	629	00000275	061D	The data link was terminated by the remote machine.
ERROR_HARDWARE_FAILURE	630	00000276	061E	The port was disconnected due to hardware failure.
ERROR_USER_DISCONNECTION	631	00000277	061F	The port was disconnected by the user
ERROR_INVALID_SIZE	632	00000278	0620	The structure size is incorrect
ERROR_PORT_NOT_AVAILABLE	633	00000279	0621	The port is already in use or is not configured for Remote Access dial out
ERROR_CANNOT_PROJECT_CLIENT	634	0000027A	0622	Cannot register your computer on on the remote network.%
ERROR_UNKNOWN	635	0000027B	0623	Unknown error
ERROR_WRONG_DEVICE_ATTACHED	636	0000027C	0624	The wrong device is attached to the port
ERROR_BAD_STRING	637	0000027D	0625	The string could not be converted.
ERROR_REQUEST_TIMEOUT	638	0000027E	0626	The request has timed out.
ERROR_CANNOT_GET_LANA	639	0000027F	0627	No asynchronous net available

FUJ00171956

ERROR_NETBIOS_ERROR	640	00000280	0628	A NetBIOS error has occurred.%
ERROR_SERVER_OUT_OF_RESOURCES	641	00000281	0629	The server cannot allocate NetBIOS resources needed to support the client
ERROR_NAME_EXISTS_ON_NET	642	00000282	062A	One of your NetBIOS names is already registered on the remote network
ERROR_SERVER_GENERAL_NET_FAILURE	643	00000283	062B	A network adapter at the server failed
WARNING_MSG_ALIAS_NOT_ADDED	644	00000284	062C	You will not receive network message popups
ERROR_AUTH_INTERNAL	645	00000285	062D	Internal authentication error
ERROR_RESTRICTED_LOGON_HOURS	646	00000286	062E	The account is not permitted to logon at this time of day
ERROR_ACCT_DISABLED	647	00000287	062F	The account is disabled
ERROR_PASSWD_EXPIRED	648	00000288	0630	The password has expired.%
ERROR_NO_DIALIN_PERMISSION	649	00000289	0631	The account does not have Remote Access permission
ERROR_SERVER_NOT_RESPONDING	650	0000028A	0632	The Remote Access server is not responding
ERROR_FROM_DEVICE	651	0000028B	0633	Your modem (or other connecting device) has reported an error
ERROR_UNRECOGNIZED_RESPONSE	652	0000028C	0634	Unrecognized response from the device
ERROR_MACRO_NOT_FOUND	653	0000028D	0635	A macro required by the device was not found in the device .INF file section
ERROR_MACRO_NOT_DEFINED	654	0000028E	0636	A command or response in the device .INF file section refers to an undefined macro
ERROR_MESSAGE_MACRO_NOT_FOUND	655	0000028F	0637	The <message> macro was not found in the device .INF file section
ERROR_DEFAULTOFF_MACRO_NOT_FOUND	656	00000290	0638	The <defaultoff> macro in the device .INF file section contains an undefined macro
ERROR_FILE_COULD_NOT_BE_OPENED	657	00000291	0639	The device .INF file could not be opened
ERROR_DEVICENAME_TOO_LONG	658	00000292	063A	The device name in the device .INF or media .INI file is too long
ERROR_DEVICENAME_NOT_FOUND	659	00000293	063B	The media .INI file refers to an unknown device name
ERROR_NO_RESPONSES	660	00000294	063C	The device .INF file contains no responses for the command.%
ERROR_NO_COMMAND_FOUND	661	00000295	063D	The device .INF file is missing a command.%
ERROR_WRONG_KEY_SPECIFIED	662	00000296	063E	Attempted to set a macro not listed in device .INF file section
ERROR_UNKNOWN_DEVICE_TYPE	663	00000297	063F	The media .INI file refers to an unknown device type
ERROR_ALLOCATING_MEMORY	664	00000298	0640	Cannot allocate memory
ERROR_PORT_NOT_CONFIGURED	665	00000299	0641	The port is not configured for Remote Access
ERROR_DEVICE_NOT_READY	666	0000029A	0642	Your modem (or other connecting device) is not functioning
ERROR_READING_INI_FILE	667	0000029B	0643	Cannot read the media .INI file
ERROR_NO_CONNECTION	668	0000029C	0644	The connection dropped
ERROR_BAD_USAGE_IN_INI_FILE	669	0000029D	0645	The usage parameter in the media .INI file is invalid
ERROR_READING_SECTIONNAME	670	0000029E	0646	Cannot read the section name from the media .INI file
ERROR_READING_DEVICETYPE	671	0000029F	0647	Cannot read the device type from the media .INI file
ERROR_READING_DEVICENAME	672	000002A0	0648	Cannot read the device name from the media .INI file
ERROR_READING_USAGE	673	000002A1	0649	Cannot read the usage from the media .INI file
ERROR_READING_MAXCONNECTBPS	674	000002A2	064A	Cannot read the maximum connection BPS rate from the media .INI file
ERROR_READING_MAXCARRIERBPS	675	000002A3	064B	Cannot read the maximum carrier BPS rate from the media .INI file
ERROR_LINE_BUSY	676	000002A4	064C	The line is busy
ERROR_VOICE_ANSWER	677	000002A5	064D	A person answered instead of a modem
ERROR_NO_ANSWER	678	000002A6	064E	There is no answer.%
ERROR_NO_CARRIER	679	000002A7	064F	Cannot detect carrier

FUJ00171956

ERROR_NO_DIALTONE	680	000002A8	0650	There is no dial tone.%
ERROR_IN_COMMAND	681	000002A9	0651	General error reported by device.%
ERROR_WRITING_SECTIONNAME	682	000002AA	0652	ERROR_WRITING_SECTIONNAME
ERROR_WRITING_DEVICETYPE	683	000002AB	0653	ERROR_WRITING_DEVICETYPE
ERROR_WRITING_DEVICENAME	684	000002AC	0654	ERROR_WRITING_DEVICENAME
ERROR_WRITING_MAXCONNECTBPS	685	000002AD	0655	ERROR_WRITING_MAXCONNECTBPS
ERROR_WRITING_MAXCARRIERBPS	686	000002AE	0656	ERROR_WRITING_MAXCARRIERBPS
ERROR_WRITING_USAGE	687	000002AF	0657	ERROR_WRITING_USAGE
ERROR_WRITING_DEFAULTOFF	688	000002B0	0658	ERROR_WRITING_DEFAULTOFF
ERROR_READING_DEFAULTOFF	689	000002B1	0659	ERROR_READING_DEFAULTOFF
ERROR_EMPTY_INI_FILE	690	000002B2	065A	ERROR_EMPTY_INI_FILE
ERROR_AUTHENTICATION_FAILURE	691	000002B3	065B	Access denied because username and/or password is invalid on the domain
ERROR_PORT_OR_DEVICE	692	000002B4	065C	Hardware failure in port or attached device
ERROR_NOT_BINARY_MACRO	693	000002B5	065D	ERROR_NOT_BINARY_MACRO
ERROR_DCB_NOT_FOUND	694	000002B6	065E	ERROR_DCB_NOT_FOUND
ERROR_STATE_MACHINES_NOT_STARTED	695	000002B7	065F	ERROR_STATE_MACHINES_NOT_STARTED
ERROR_STATE_MACHINES_ALREADY_STARTED	696	000002B8	0660	ERROR_STATE_MACHINES_ALREADY_STARTED
ERROR_PARTIAL_RESPONSE_LOOPING	697	000002B9	0661	ERROR_PARTIAL_RESPONSE_LOOPING
ERROR_UNKNOWN_RESPONSE_KEY	698	000002BA	0662	A response keyname in the device .INF file is not in the expected format
ERROR_RECV_BUF_FULL	699	000002BB	0663	The device response caused buffer overflow.%
ERROR_CMD_TOO_LONG	700	000002BC	0664	The expanded command in the device .INF file is too long
ERROR_UNSUPPORTED_BPS	701	000002BD	0665	The device moved to a BPS rate not supported by the COM driver
ERROR_UNEXPECTED_RESPONSE	702	000002BE	0666	Device response received when none expected.%
ERROR_INTERACTIVE_MODE	703	000002BF	0667	The Application does not allow user interaction. The connection requires interaction with the user to complete successfully.
ERROR_BAD_CALLBACK_NUMBER	704	000002C0	0668	ERROR_BAD_CALLBACK_NUMBER
ERROR_INVALID_AUTH_STATE	705	000002C1	0669	ERROR_INVALID_AUTH_STATE
ERROR_WRITING_INITBPS	706	000002C2	066A	ERROR_WRITING_INITBPS
ERROR_X25_DIAGNOSTIC	707	000002C3	066B	X.25 diagnostic indication.%
ERROR_ACCT_EXPIRED	708	000002C4	066C	The account has expired
ERROR_CHANGING_PASSWORD	709	000002C5	066D	Error changing password on domain. The password may be too short or may match a previously used password
ERROR_OVERRUN	710	000002C6	066E	Serial overrun errors were detected while communicating with your modem
ERROR_RASMAN_CANNOT_INITIALIZE	711	000002C7	066F	RasMan initialization failure. Check the event log
ERROR_BIPLEX_PORT_NOT_AVAILABLE	712	000002C8	0670	Biplex port initializing. Wait a few seconds and redial
ERROR_NO_ACTIVE_ISDN_LINES	713	000002C9	0671	No active ISDN lines are available
ERROR_NO_ISDN_CHANNELS_AVAILABLE	714	000002CA	0672	No ISDN channels are available to make the call
ERROR_TOO_MANY_LINE_ERRORS	715	000002CB	0673	Too many errors occurred because of poor phone line quality
ERROR_IP_CONFIGURATION	716	000002CC	0674	The Remote Access IP configuration is unusable
ERROR_NO_IP_ADDRESSES	717	000002CD	0675	No IP addresses are available in the static pool of Remote Access IP addresses
ERROR_PPP_TIMEOUT	718	000002CE	0676	Timed out waiting for a valid response from the remote PPP peer
ERROR_PPP_REMOTE_TERMINATED	719	000002CF	0677	PPP terminated by remote machine
ERROR_PPP_NO_PROTOCOLS_CONFIGUR	720	000002D0	0678	No PPP control protocols configured

FUJ00171956

ED				
ERROR_PPP_NO_RESPONSE	721	000002D1	0679	Remote PPP peer is not responding
ERROR_PPP_INVALID_PACKET	722	000002D2	067A	The PPP packet is invalid
ERROR_PHONE_NUMBER_TOO_LONG	723	000002D3	067B	The phone number including prefix and suffix is too long
ERROR_IPXCP_NO_DIALOUT_CONFIGURED	724	000002D4	067C	The IPX protocol cannot dial-out on the port because the machine is an IPX router
ERROR_IPXCP_NO_DIALIN_CONFIGURED	725	000002D5	067D	The IPX protocol cannot dial-in on the port because the IPX router is not installed
ERROR_IPXCP_DIALOUT_ALREADY_ACTIVE	726	000002D6	067E	The IPX protocol cannot be used for dial-out on more than one port at a time
ERROR_ACCESSING_TCPCFGDLL	727	000002D7	067F	Cannot access TCPCFG.DLL
ERROR_NO_IP_RAS_ADAPTER	728	000002D8	0680	Cannot find an IP adapter bound to Remote Access
ERROR_SLIP_REQUIRES_IP	729	000002D9	0681	SLIP cannot be used unless the IP protocol is installed
ERROR_PROJECTION_NOT_COMPLETE	730	000002DA	0682	Computer registration is not complete
ERROR_PROTOCOL_NOT_CONFIGURED	731	000002DB	0683	The protocol is not configured
ERROR_PPP_NOT_CONVERGING	732	000002DC	0684	The PPP negotiation is not converging
ERROR_PPP_CP_REJECTED	733	000002DD	0685	The PPP control protocol for this network protocol is not available on the server
ERROR_PPP_LCP_TERMINATED	734	000002DE	0686	The PPP link control protocol terminated
ERROR_PPP_REQUIRED_ADDRESS_REJECTED	735	000002DF	0687	The requested address was rejected by the server
ERROR_PPP_NCP_TERMINATED	736	000002E0	0688	The remote computer terminated the control protocol
ERROR_PPP_LOOPBACK_DETECTED	737	000002E1	0689	Loopback detected
ERROR_PPP_NO_ADDRESS_ASSIGNED	738	000002E2	068A	The server did not assign an address
ERROR_CANNOT_USE_LOGON_CREDENTIALS	739	000002E3	068B	The authentication protocol required by the remote server cannot use the Windows NT encrypted password. Redial, entering the password explicitly
ERROR_TAPI_CONFIGURATION	740	000002E4	068C	Invalid TAPI configuration
ERROR_NO_LOCAL_ENCRYPTION	741	000002E5	068D	The local computer does not support the required encryption type
ERROR_NO_REMOTE_ENCRYPTION	742	000002E6	068E	The remote computer does not support the required encryption type
ERROR_REMOTE_REQUIRES_ENCRYPTION	743	000002E7	068F	The remote computer requires encryption
ERROR_IPXCP_NET_NUMBER_CONFLICT	744	000002E8	0690	Cannot use the IPX network number assigned by remote server. Check the event log
ERROR_INVALID_SMM	745	000002E9	0691	ERROR_INVALID_SMM
ERROR_SMM_UNINITIALIZED	746	000002EA	0692	ERROR_SMM_UNINITIALIZED
ERROR_NO_MAC_FOR_PORT	747	000002EB	0693	ERROR_NO_MAC_FOR_PORT
ERROR_SMM_TIMEOUT	748	000002EC	0694	ERROR_SMM_TIMEOUT
ERROR_BAD_PHONE_NUMBER	749	000002ED	0695	ERROR_BAD_PHONE_NUMBER
ERROR_WRONG_MODULE	750	000002EE	0696	ERROR_WRONG_MODULE
ERROR_INVALID_CALLBACK_NUMBER	751	000002EF	0697	Invalid callback number. Only the characters 0 to 9, T, P, W, (,), -, @, and space are allowed in the number.
ERROR_SCRIPT_SYNTAX	752	000002F0	0698	A syntax error was encountered while processing a script
ERROR_HANGUP_FAILED	753	000002F1	0699	The connection could not be disconnected because it was created by the Multi-Protocol Router
INVALID RAS_HANDLE	0	00000000	0x06ee	The current RAS handle is invalid
UNKNOWN			0x06ff	Code not set