

Oracle Communications EAGLE Release 46.3 Feature Guide

ORACLE WHITE PAPER | AUGUST 2016





Table of Contents

Table of Contents	0
List of Terms	1
Introduction	8
About this Manual	8
About the Oracle Communications EAGLE	8
Oracle Communications EAGLE Product Overview & Benefits	9
Benefits	9
Go Forward Product Model	10
Operations, Administration, and Maintenance	13
General	13
Operations	13
Upgrade	13
Remote Upgrade	14
Controlled Features	14
Feature Bit Control	14
Feature Access Key Control	14
Administration and Provisioning	14
EAGLE Command Classes	15
EAGLE Security	15
FTP Retrieve and Replace	16
EAGLE OA&M IP Security Enhancements	17
EAGLE OA&M Password Security Enhancements	18

SEAS over IP	18
Maintenance	19
Alarms	19
Disk/Database Maintenance	20
IMT Fault Isolation	22
Link Maintenance	23
SNMP V2 Traps on E5-OAM	26
MTP-SCCP FUNCTIONALITY	27
GENERAL	27
NRC FEATURES	27
Signaling Message Handling Congestion Control - ANSI	28
Procedure to Eliminate False Link Congestion - ANSI	28
Prevention of Congestion on Newly Available Linksets - ANSI	29
Prevention of Congestion from Rerouted Traffic - ANSI/ITU	29
MTP Circular Route Detection - ANSI	29
Prevention of Link Oscillation - ANSI	30
MTP Restart - ANSI/ITU	30
Procedures for Recovery from Processor Outages - ANSI/ITU	30
Cluster Routing and Management Diversity - ANSI	30
SCCP Routing in Response to MTP Congestion - ANSI	31
Prevention of SCCP Circular Routes	31
Prevention of Trunk Looping Caused by ISUP	32
Improved Signaling Link Test (SLT) Procedures - ANSI	32
Backup Procedures Against Loss of TFR/TCR - ANSI	33

MTP User Flow Control - ANSI	33
Optional TFP Broadcast across Network Boundaries - ANSI	33
ADVANCED MTP CAPABILITIES	33
Advanced MTP Routing Functions	33
Multiple Point Code - ANSI/ITU	39
ITU-N Duplicate Point Code	41
ITU-I/ITU-N Spare Point Code Support	42
ITU SLS Enhancements	42
Random SLS Generation	44
SLS Bit Rotation on Incoming Linkset	46
SLS Bit Rotation using 8 bits for ANSI links	49
Miscellaneous Protocol Features	49
Proxy Point Code	50
Multiple Linksets to Single Adjacent Point Code	50
Network Indicator Mapping	51
Point Code and CIC Translation	52
GATEWAY SCREENING - ANSI/ITU	53
General	53
GWS Functionality	53
Allowed OPC	55
Allowed DPC	55
Allowed SIO	56
Allowed ISUP Message Type	56
Allowed TUP Message Type	56

Blocked OPC	56
Blocked DPC	56
Allowed SCCP Called/Calling Party Addresses (PC/SSN)	56
Allowed SCMG Affected Point Code	57
Allowed Affected Destination Field Screen	57
Provisioning Ranges for Gateway Screening	57
GWS Stop Action for MTP Routed Messages	57
GWS Stop Action – De-encapsulate	57
GWS Stop Action – Duplicate and Route	57
NETWORK SECURITY ENHANCEMENTS	58
SS7 Firewall	58
GSM MAP SCREENING – ITU	59
General	59
GSM MAP Screening Process	59
GSM MAP Screening Duplicate/Forward	61
GSM MAP Screening Limitations	63
ENHANCED GSM MAP SCREENING - ITU/ANSI	63
Introduction	63
Enhanced GSM MAP Screening Example	64
Enhanced GSM MAP Screening Limitations	64
SCCP-GLOBAL TITLE TRANSLATIONS (GTT) - ANSI/ITU	64
General	64
Basic Global Title Translation Functionality	64

Advanced Global Title Translation Functionality	67
SCCP XUDT MESSAGE SUPPORT - ITU/ANSI	79
Introduction	79
Available Support	79
XUDT Limitations	80
GUARANTEED IN-SEQUENCE DELIVERY OF SCCP PROTOCOL CLASS 1 MESSAGES	80
Introduction	80
Available Support	80
Considerations/Limitations	81
TRANSACTION-BASED GTT LOADSHARING	81
Introduction	81
Considerations and Limitations	82
WEIGHTED GTT LOADSHARING	83
Introduction	83
Considerations and Limitations	84
GTT LOAD SHARING TO 32 DESTINATIONS	85
HEX DIGIT SUPPORT FOR GTT	85
Description	85
Limitations	86
FALL-BACK TO GTT AFTER LNP MR SERVICE	86
Fallback to GTT	86

GTA/GTII/GTIN/GTIN24	86
Translation Type	86
Numbering Plan	86
Nature of Address Indicator	86
Fall-back to GTT Description	86
Exceptions to Fall-back to GTT	87
Pre-LNP QS and Post LNP MR GTT	88
SUPPORT FOR J7 (JAPAN SS7)	89
Support for J7 (Japan SS7)	89
DATABASE SERVICES	90
120M DN AND 120M IMSI VIA SPLIT DATABASE AND DUAL EXAP	
CONFIGURATION	91
EPAP Database Expansion to 480M	91
QUERY-BASED NUMBER PORTABILITY SOLUTIONS (FIXED OR MOBILE)	91
NA LNP - North American Local Number Portability	91
INP (INAP-based Number Portability) - ITU	97
ANSI-41 INP Query (AINPQ)	101
LOCREQ Query Response	102
ENUM Query Response	102
MOBILE NUMBER PORTABILITY SOLUTIONS	102
MNP GSM Mobile Number Portability	103
MNP Message Flow	103
MNP Database	107



MNP Assumptions/Limitations	108
ANSI-41 Mobile Number Portability	108
ANSI-41 MNP Service Selection	109
IS-41 GSM Migration	110
Service Portability (S-Port)	119
Relay to HLR	121
Relay to HLR	121
Intra Network Number Portability	122
NUMBER PORTABILITY SOLUTIONS FOR PREPAID/SERVICE NODE ACCESS	
	122
GSM SRI Query	122
GSM ATI Query	123
Prepaid IDP Query Relay	124
IDP Relay for SMS	129
IDP Screening for Prepaid	129
Info Analyzed Relay	130
Analyzed Information query with no EPAP/ELAP	130
SIP Number Portability	130
ISUP-INTERCEPTION-BASED ROUTING AND NUMBER PORTABILITY SOLUTIONS	
	131
Triggerless ISUP Framework (TIF)	131
TIF Blacklisting	133
TIF CdPN EPAP-based Selective Screening: SELSCR	134



TIF ASD and TIF GRN support	135
TIF GRN use case for TIF CgPN service	136
TIF ASD use case for TIF CgPN service using ASDOTHER	137
MESSAGE FLOWS	138
TIF NP - Triggerless ISUP Framework Number Portability	140
TIF Simple Number Substitution	144
TIF Number Substitution using Numbering Plan Processor	145
TIF Enhancements including IAM/SAM Splitting based on DPC	145
SMS NUMBER PORTABILITY AND ROUTING SOLUTIONS	146
GSM Prepaid SMS Intercept	146
Loadsharing between Multiple IN Platforms	149
SMS Number Portability for GSM and IS41	151
MO SMS IS41-to-GSM Migration	156
MO SMS B Party Routing	157
MO SMS NPP	157
HLR ROUTER	157
General	157
HLR Router Overview	158
MGT (E.214) and IMSI (E.212) Routing	159
DN (E.164) Routing	160
HLR Router Architecture	161
HLR Router Assumptions/Limitations	165
HLR Router MAP Layer Routing	166



VOICEMAIL ROUTER	167
Background	167
Voicemail Router Overview	167
EQUIPMENT IDENTITY REGISTER (EIR)	168
Background	169
Feature Overview	169
Architecture and Database	171
Measurements and Logs	171
Assumptions and Limitations	172
SUPPORTING FUNCTIONALITIES	172
SCCP Service Re-Route	172
MTP Messages for SCCP Applications	175
Multiple Local SCCP Subsystems	175
Additional Subscriber Data (ASD)	175
Numbering Plan Processor (NPP)	176
HomeSMSC “Match with Digits” Option	180
TCAP-Segmented SMS Support Phase 1	180
ORACLE COMMUNICATIONS LOCAL SERVICE MANAGEMENT SYSTEM (LSMS)	
(NORTH AMERICAN)	182
LSMS OVERVIEW	182
LSMS HARDWARE OVERVIEW	183
APP-B Card Components	183
LSMS ARCHITECTURE	184



Hot Swap Capability, Critical Hardware Components	184
Data Redundancy	184
Segmented Network Configuration Support	184
Network Interfaces	184
LSMS FUNCTIONS	184
Data Administration	185
Data Auditing	186
LSMS User Interfaces	186
Local Data Security	187
Local Data SPID Security	188
Outage Recovery	188
Support for Multiple EAGLE LNPs	188
Enhanced LSMS Filters	189
Support for Multiple NPAC SMSs	189
Multiple Supported Service Providers	189
System Surveillance	189
Remote Monitoring	189
Reports	189
Report Generator	190
Logs	190
LSMS Query Server Package	191
File Transfers	191
Automatic File Transfer	192
Backup	192

IP SIGNALING	192
OVERVIEW	192
EAGLE as Signaling Gateway	193
IPLIMx, IPGWx, and IPSG Applications	193
PERFORMANCE	195
PROTOCOLS AND APPLICATIONS	195
SCTP/IP	195
SCTP vs. TCP	196
M3UA on IPGWx	200
SUA DAUD with SSN Support	202
Routing Key Registration	202
Q.BICC Routing	204
M2PA on IPLIMx	205
SNMP	206
Large BICC MSU Support for IP Signaling	207
EAGLE Fast Copy	208
IPSG Link Capacity Sharing	209
Support of 1M System (SIGTRAN + ATM) TPS	209
Configurable SCTP Heartbeat Timer	209
GATEWAY FUNCTIONALITY	210
ANSI/ITU MTP GATEWAY	210
Level 3 MSU Discrimination	210
MSU Routing	210

Administering Point Codes	211
Local Link Congestion	211
Remote Link Congestion	212
X.25/SS7 GATEWAY FEATURE	213
DATA TRANSPORT ACCESS	213
GWS Redirect Table	213
MSU Encapsulation	214
MEASUREMENTS	216
GENERAL	216
BASIC MEASUREMENT COLLECTION	216
Report Parameters	217
SIGTRAN Measurements	217
ADVANCED MEASUREMENTS	218
MEASUREMENTS PLATFORM	218
Measurement Platform Limitations	220
E5-OAM Integrated Measurements	220
STPLAN FEATURE	220
Addendum	222
Go Forward Product Descriptions and Mapping to Legacy Part Numbers	222

Table of Figures

Figure 1: Oracle Communications EAGLE Functional Overview	10
Figure 2: Functional OAM Diagram	13
Figure 3: High Level Data Flow for FTP Retrieve and Replace Feature	16
Figure 4: SEAS Architecture/Deployment using IP	18
Figure 5: Alarm Diagram	19
Figure 6: EAGLE Database Operations	21
Figure 7: Link LBPs for Latching Test	24
Figure 8: DS0 Link LBPs for Non-Latching Test	25
Figure 9: Link Diagnostic Diagram	26
Figure 10: Cluster Routing	34
Figure 11: Nested Cluster Routing	36
Figure 12: Network Routing	37
Figure 13: Origin-based MTP Usage Example	38
Figure 14: Origin-based MTP Routing Route Selection Example	39
Figure 15: Typical International Deployment of MPC Feature	40
Figure 16: Typical International Deployment of ITU-N Duplicate Point Code Feature	41
Figure 17: ITU-T ISUP Routing Label with CIC	42
Figure 18: Example of Bit Rotation	43
Figure 19: SLS Creation Using Other CIC Bit	43
Figure 20: Random SLS Generation in a Combined Link	45
Figure 21: Random SLS Generation in a Single Linkset	46
Figure 22: Bit Rotation Example	47
Figure 23: SLS Bit Rotation Example	47
Figure 24: Example with Standard Bit Rotation Applied	48
Figure 25: Example Applying SLS Bit Rotation on Incoming Linkset	48
Figure 26: Multiple Linksets to Single Adjacent Point Codes	51
Figure 27: Network Indicator Mapping Example	52
Figure 28: GWS Functional Diagram	54
Figure 29: GWS Provisioning Structure	55
Figure 30: GSM-MAP Screening Process	60
Figure 31: MAP Message Forward Example - SMS	61
Figure 32: MAP Message Duplicate Example - SMS	62
Figure 33: Enhanced GSM MAP Screening Example	64
Figure 34: Structure of GTT Provisioning Table	65
Figure 35: Origin-based SCCP Routing Example	71
Figure 36: Flexible GTT Example	73
Figure 37: ANSI<->ITU SCCP Conversion - MTP Routed	77
Figure 38: ANSI<->ITU SCCP Conversion - GT Routed	78
Figure 39: ANSI-ITU SMS conversion process	79
Figure 40: Weighted Load Sharing Based on MAPGROUP	84
Figure 41: Origin based LNP QS call flow with Pre-LNP GTT processing	88
Figure 42: LNP MR with fall-back to GTT post processing	89
Figure 43: EAGLE LNP Architecture	92
Figure 44: LNP Data Flow	93
Figure 45: INP Call to a Non-ported Number	98
Figure 46: INP Call to a Ported Number	98
Figure 47: Non-Call Related Message for Ported Number Flow	99
Figure 48: INP Circular Route Prevention	101
Figure 49: MT Call to Non-ported or Imported Number - Indirect Routing	103
Figure 50: MO/MT Call to Exported Number - Direct Routing	104
Figure 51: MO/MT Call to Foreign Number Not Known to Be Ported - Direct Routing	105
Figure 52: Non-CR Message for Non-ported Number - Indirect Routing	105
Figure 53: Non-CR Message for Ported Number - Indirect Routing	106
Figure 54: Non-CR Message for Ported or Non-ported Number - Direct Routing	107
Figure 55: IS-41->GSM Migration Network View	111
Figure 56: Call Originated from IS-41 MSC for GSM-Migrated Subscriber	112
Figure 57: Originated from GSM MSC for GSM-Migrated/GSM-Only Subscriber	113
Figure 58: Call Originated from IS-41 MSC for Non-GSM-Migrated Subscriber	114
Figure 59: Call Originated from GSM MSC for Non-GSM-Migrated Subscriber	115
Figure 60: MT SMS Delivery for Non-Migrated IS-41 Subscriber SRI-for-SM First	116

Figure 61: MT SMS Delivery for GSM-Migrated/GSM Only Subscriber: SRI-for-SM First.....	117
Figure 62: SRI Re-Direct to serving HLR.....	122
Figure 63: Example of ATI Query/Response to MNP Database Node.....	123
Figure 64: Prepaid Mobile Voice Call Terminating to Ported-Out Subscribers.....	125
Figure 65: Prepaid Mobile Voice Calls Terminating to Ported-In Subscribers.....	126
Figure 66: System Architecture for SIP Number Portability.....	131
Figure 67: TIF Overview.....	132
Figure 68: Basic Message Flow of TIF BlackList.....	134
Figure 69: Basic Operation of TIF ASD for TIF CdPN Service.....	136
Figure 70: Basic Operation of TIF GRN for TIF CgPN Service.....	137
Figure 71: Basic Operation of TIF ASD for TIF CgPN service using ASDOTHER.....	138
Figure 72: ISUP IAM Message Flows for TIF ASD for TIF CdPN service.....	138
Figure 73: ISUP REL Message Flow for TIF ASD for TIF CdPN service.....	139
Figure 74: ISUP Message Flows for TIF GRN for TIF CdPN service.....	139
Figure 75: ISUP REL Message Flow for TIF GRN for TIF CdPN service.....	139
Figure 76: ISUP IAM Message Flows for TIF ASD for TIF CgPN service.....	139
Figure 77: ISUP IAM Message Flows for TIF GRN for TIF CgPN service.....	140
Figure 78: Call to Ported Subscriber with IAM Relay and NP Flags.....	141
Figure 79: Call to Ported Subscriber with REL Message and NP Flags.....	142
Figure 80: Delivery of MO_FSM from Postpaid Subscriber.....	147
Figure 81: Successful Delivery of MO_FSM from Prepaid Subscriber.....	147
Figure 82: Unsuccessful Delivery of MO_FSM from Prepaid Subscriber.....	148
Figure 83: PPSMS IN Platform Loadsharing.....	149
Figure 84: MO-based GSM SMS NP - Called subscriber is another network subscriber.....	152
Figure 85: MO-based IS41 SMS NP - Called subscriber is in-network subscriber.....	153
Figure 86: MT-based GSM SMS/MMS NP- called party for other network subscriber.....	154
Figure 87: MT-based IS41 SMS NP - called subscriber from other network subscriber.....	155
Figure 88: Integrated STP/HLR Router Node in a Mobile Network.....	158
Figure 89: Stand-alone HLR Router Node in a Mobile Network.....	159
Figure 90: HLR Router E.214(E.212) Routing Example.....	160
Figure 91: MSISDN-Mobile Terminated Call Example.....	161
Figure 92: HLR Router Architecture.....	162
Figure 93: HLR Router Provisioning Hierarchy.....	162
Figure 94: Support for Provisioning Multiple EPAPs.....	164
Figure 95: Voicemail Router Message Flow.....	168
Figure 96: EAGLE EIR Call Flows.....	170
Figure 97: HLR Router and GTT Traffic.....	174
Figure 98: Action Set <-> Action Relationship.....	178
Figure 99: Rule/Filter/Action Set Relationship.....	179
Figure 100: Service Rule Set and Rule Relationship.....	180
Figure 101: Example of TCAP Segmented SMS Support Phase.....	181
Figure 102: Sample LNP Network.....	183
Figure 103: LSMS Query Server Overview.....	191
Figure 104: Oracle SIGTRAN Protocols.....	193
Figure 105: Typical EAGLE IP Signaling Deployment.....	195
Figure 106: SCTP Overview Diagram.....	196
Figure 107: Associations vs. TCP Sockets.....	197
Figure 108: SCTP Protocol Handshake.....	198
Figure 109: SCTP Retransmission Control.....	199
Figure 110: IPGWx Overview Diagram.....	200
Figure 111: IPGWx Protocol Diagram.....	201
Figure 112: IPGWx Network View.....	201
Figure 113: BICC Message Format.....	204
Figure 114: IPLIMx Network View.....	205
Figure 115: IPLIMx Overview Diagram.....	206
Figure 116: IPLIMx Protocol Diagram.....	206
Figure 117: Sample Gateway STP Network.....	211
Figure 118: Traffic to and from a Congested Link.....	212
Figure 119: Congestion Levels.....	212
Figure 120: MSU Encapsulation.....	215
Figure 121: DTA Message Flow.....	216
Figure 122: Measurements Platform Functional Diagram.....	219

Figure 123: STPLAN Functional Diagram.....	221
--	-----

Table of Tables

Table 1: Go Forward Product Model.....	10
Table 2: Number of Components to Inspect Under Various Conditions	23
Table 3: Link Fault Sectionalization Tests Remote Link Element (RLE) Types	25
Table 4: Link Fault Sectionalization Test Types.....	25
Table 5: Global Title Translation.....	66
Table 6: GTT Messages	68
Table 7: Available User-Selectable SCCP Routing Hierarchies	70
Table 8: Flexible GTT Routing.....	73
Table 9: Transaction-based GTT Provisioning Options	82
Table 10: Message Relay Services and GTT Actions.....	86
Table 11: Service Name and Corresponding Feature which may relay MSU	86
Table 12: Exceptions to Fall-Back to GTT functionality.....	87
Table 13: J7 Features and Support	89
Table 14: Measurement Counters for A Port	110
Table 15: Network Prefix To Be Appended to SRI_ACK.....	121
Table 16: TON to NAI Mapping	128
Table 17: OFNAI to TON Mapping	129
Table 18: Example of Complex Filtering Rules for ISUP NP - Relay	143
Table 19: Example of Complex Filtering Rules for ISUP NP – Release.....	144
Table 20: IMEI Treatment.....	170
Table 21: LSMS Functions	184
Table 22: SNMP Traps Supported.....	207
Table 23: Additional Link Component Peg Counts	208
Table 24: Remote Congestion Response	212
Table 25: DTA CgPA SSN Mapping Table	214
Table 26: IPVSHL Linkset Registers.....	218
Table 27: Oracle Communications EAGLE (base-fee).....	222
Table 28: Oracle Communications EAGLE	224
Table 29: Oracle Communications EAGLE LNP Advanced Service Module Enabler	224
Table 30: Oracle Communications EAGLE LNP.....	225
Table 31: Oracle Communications EAGLE Advanced Service Module Enabler	225
Table 32: Oracle Communications EAGLE Mobile Number Portability	226
Table 33: Oracle Communications EAGLE SS7 Firewall.....	227
Table 34: Oracle Communications EAGLE HLR Router	228
Table 35: Oracle Communications EAGLE Equipment Identity Register	228
Table 36: Oracle Communications EAGLE Global Title Translation Routing	228
Table 37: Oracle Communications EAGLE Triggerless ISUP Framework Routing	229
Table 38: Oracle Communications EAGLE Origin Based Routing	230
Table 39: Oracle Communications EAGLE Prepaid Routing	230
Table 40: Oracle Communications EAGLE SMS Routing.....	231
Table 41: Oracle Communications EAGLE Service Handler 8GB	231
Table 42: Oracle Communications EAGLE Ethernet B Traffic Handler.....	232
Table 43: Oracle Communications EAGLE Asynchronous Transfer Mode B Traffic Handler	233
Table 44: Oracle Communications EAGLE E1T1 B Traffic Handler.....	234
Table 45: Oracle Communications EAGLE Application Processor Provisioning	235
Table 46: Oracle Communications EAGLE Application Processor NonProvisioning.....	235
Table 47: Oracle Communications EAGLE Application Processor Database Capacity.....	236
Table 48: Oracle Communications EAGLE LNP Application Processor.....	236
Table 49: Oracle Communications EAGLE LNP Application Processor Database Capacity	236
Table 50: Oracle Communications LSMS	238
Table 51: Oracle Communications LSMS Query Server	239
Table 52: Oracle Communications EAGLE FTP Table Base Retrieval	239

List of Terms

Acronym	Meaning
A-Port	ANSI-41 Mobile Number Portability
ACG	Automatic Call Gapping
ACM	Address Complete Message
ACSE	Association Control Service Element
ADL	Application Data Loader
ADU	Application Defined UAM
AE	Application Engine
AIN	Advanced Intelligent Network
AINPQ	ANSI-41 INP Query
ANSI	American National Standards Institute
AOPS	Area of Portability Service
API	Application Programming Interface
APLI	ACSE Presentation Layer Interface
AS	Application Server
ASP	Application Server Process
ASL8	Adjacent SLS 8-bit Indicator
ATH	Application Trouble Handler
ATM	Asynchronous Transfer Mode
AuC	Authentication Center
BICC	Bearer Independent Call Control
Capability	Term used interchangeably with function
CC	Country Code
CEIR	Central EIR
CIC	Circuit Identification Code
CLASS	Custom Local Area Signaling Services
CM	Cluster Manager
CNAM	Calling Name Delivery
CNCF	Calling Name Conversion Facility
CNIP	Calling Name Identification Presentation
CS	Control Shelf
CF	Control Frame
CPA	Customer Provisioning Application
CPC	Capability Point Code

CSPC	Concerned Signaling Point Code; Oracle term for Affected Point Code
DAF	Data Acquisition Function
DCB	Device Control Block
Default GTTs	GTTs used for non-ported numbers
DMS	Disk Management Subsystem
DN	Directory Number or Telephone Number
DS0A	Digital Signal Level 0 Applique
DSGRT	DSG Runtime
DSM	Database Service Module
DSU	Data Service Unit
DTA	Database Transport Access
E5-E1T1	EAGLE E1/T1 Interface Card. Note: This card is replaced by the Oracle Communications E1T1 B Card.
E5-ENET	EAGLE Ethernet Interface Card. Note: This card is replaced by the Oracle Communications EAGLE Ethernet B Card
E5-IPSM	EAGLE IP Services Module
E5-SLAN	E5-ENET card with STPLAN functionality. Note: This card is replaced by the Oracle Communications EAGLE Ethernet B Card
E5-SM4G	EAGLE 4 GB Service Module. Note: This card is replaced by the Oracle Communications EAGLE 8 GB B card.
E5-STC	E5-ENET card with Signaling Transport functionality- used for sending MSU data to the IMFs
ECAP	EAGLE Collector Application Processor
EF	Extension Frame
EIR	Equipment Identity Register
ELAP	EAGLE LNP Application Processor
EMS	Element Management System
ENUM	E.164 Number Mapping
EO	End Office
EOAP	Embedded OAP
EOT	End of Table
EPAP	EAGLE Provisioning Application Processor
ETSI	European Technical Standards Institute
FAT	File Access Table
FCI	Forward Call Indicator
FTP RR	FTP Retrieve and Replace

FTRA	FTP Table Base Retrieval Application
MNP	GSM Mobile Number Portability; A feature that provides mobile subscribers the ability to change the GSM subscription network within a portability cluster, while retaining their original MSISDN(s)
GAP	Generic Address Parameter
GGSN	Gateway GPRS Support Node
GLS	Gateway Loading Services
GMLC	Gateway Mobile Location Center
GMSC	Gateway Mobile Switching Center
GN	Generic Name
GPL	Generic Program Load
GPRS	General Packet Radio Service
GPSM	General Purpose Service Module
GSM	Global System for Mobile Communication
GT	Global Title
GTT	Global Title Translation
GWS	Gateway Screening
HC-MIM	High Capacity Multi-channel Interface Module
HDD	Hard Disk Drive
HIPR	High Speed IMT Packet Router
HLR	Home Location Register
HMI	Human-to-Machine Interface
HMUX	High Speed Multiplexer
HSL	High Speed Link (T1 or E1)
IAM	Initial Address Message
IAS	Integrated Application Solution
IDPR	Prepaid IDP Query Relay
IETF	Internet Engineering Task Force
IGM	IS41 GSM Migration
IMEI	International Mobile Equipment Identity
IMF	Integrated Message Feeder
IMSI	International Mobile Subscriber Identity
IMT	Interprocessor Message Transport
IN	Intelligent Network
INAP	Intelligent Network Application Protocol
INP	INAP-based Number Portability

IPGW	IP Gateway
IPLIM	IP Link Interface Module
IPS	IP Signaling
IPSG	IP Signaling Gateway
IPSM	IP Services Module
IPSP	IP Server Process
ISDN	Integrated Services Digital Network
ISUP	ISDN User Part
ITU	International Telecommunications Union
ITU-I	ITU International
ITU-N	ITU National
JIP	Jurisdiction Indicator Parameter
LIM	Link Interface Module
LNP	Local Number Portability
LNP database	Realtime database
LNPQS	LNP Query Service
LRN	Location Routing Number
LSB	Least Significant Bit
LSL	Low Speed Link
LSMS	Local Service Management System
LU	Location_Update [message]
M2PA	SS7 MTP2-User Peer-to-Peer Adaptation Layer
M3UA	SS7 MTP3-User Adaptation Layer
MCC	Mobile Country Code
MCPM	Measurement Collection and Polling Module
MDAL	Maintenance Disk and Alarm
MDB	Main Memory Database
MDS	Maintenance Disk Service
MGT	Mobile Global Title
MIM	Multi-Channel Interface Module
MNC	Mobile Network Code
MNP	Mobile Number Portability
MPL	Multi-Port Link Interface Module
MPS	Multi-Purpose Server
MR	Message Relay

MRN	Message Reference Number
MSB	Most Significant Bit
MSC	Mobile Switching Center
MSIN	Mobile Subscriber Identity Number
MSISDN	Mobile Station ISDN Number
MSRN	Mobile Station Routing Number
MSU	Message Signal Unit
MTRG	Maintenance Task Report Generator
NAK	Negative Acknowledgment
NAPTR	Naming Authority Pointer
NEBS	Network Equipment Building System
NDC	Network Destination Code
NP	Number Portability
NPA	Numbering Plan Area
NPANXX	Numbering Plan Area and Exchange
NPAC	Number Portability Administration Center
NPDB	Number Portability Database and industry-generic term for Oracle's Real-Time Database (RTDB).
NPF	Number Portability Function
NPREQ	Number Portability Request Query
NRC	Network Reliability Council
NSAP	Network Service Provider Access Point
NSFI	Next Screening Function Indicator
NSR	Next Screen Reference
OAM	Operations, Administration, and Maintenance processor
OAP	OSS Application Processor
OPC	Originating Point Code
OSI	Open System Interconnections
OSS	Operations Support System
Override GTTs	Global title translations provisioned on a per LRN basis that take precedence over the GTTs in the subscription version (TN record) from the NPAC/LSMS
PCS	Personal Communication Service
PDB	Provisioning Database
PDBA	Provisioning DB Application
PDBI	Provisioning Database Interface
PIP	Party Information Parameter

PLMN	Public Land Mobility Network
PLNP	PCS 1900 LNP
Q3	Q.3 Protocol
RMS	RAM Management Services
RTDB	Real Time Database
SAI	Send_Authentication_Information [message]
SAF	Service Application Function
SAS	Signaling Application System
SCB	Storage Control Block
SCCP	Signaling Connection Control Part
SCCS	Switching Control Center System
SCM	System Configuration Manager
SCRC	SCCP Routing Control
SCTP	Stream Control Transmission Protocol
SEAS	Signaling Engineering and Administration System
SGSN	Serving GPRS Support Node
SOIP	SEAS over IP
SE-HSL	Synchronous E1 High Speed Link
SGF	Signaling Gateway Function
SID	Self-Identification
SIGTRAN	Signaling Transport (IETF)
SIH	System Information Handler
SLAN	STP LAN
SLDR	System Loader
SLIC	Service and Link Interface Card
SLS	Signaling Link Selector
SLSCI	SLS Conversion Indicator
SLTM	Signaling Link Test Messages
SMS	Short Message Service
SMS	Storage Management Services
SNAM	Signaling Network Activation Manager. Telcordia® Signaling Network Activation Manager is a robust, user-friendly OSS that simplifies the provisioning of routing and configuration data into a wide array of core network elements, including STPs, MSCs, and HLRs.
SPID	Service Provider ID
SRI	SendRoutingInfo

SRST	Signaling Route Set Test
SS7	Signaling System No. 7
SS7oIP	SS7 over IP
SSEDCM	Single Slot Enhanced Data Communication Module
SSEL	Session Selector
SSP	Service Switching Point
STC	Signaling Transport Card
STF	Signaling Transfer Function
STH	System Trouble Handler
STP	Signal Transfer Point
SUA	SCCP User Adaptation Layer
TCAP	Transaction Capability Application Part
TCU	Table Creation Utility
TDM	Terminal Disk Module
TFC	Transfer Controlled
TFP	Transfer Prohibited
TFR	Transfer Restricted
TLNP	Triggerless LNP
TN	10 Digit Telephone Number
TPS	Transactions Per Second
TSM	Translation Services Module
TVG	Ticket Voucher Group Usage
TT	Translation Type
TTT	Trouble Text Table
TU	Transaction Unit
UAM	Unsolicited Alarm Message
UIM	Unsolicited Information Message
VLR	Visitor Location Register
WLNP	Wireless LNP



Introduction

About this Manual

The Oracle Communications EAGLE (EAGLE) Feature Guide provides a high-level overview of the EAGLE with its most important features including these related products:

- » Oracle Communications EAGLE Application Processor Provisioning (EPAP)
- » Oracle Communications EAGLE LNP Application Processor (ELAP)
- » Oracle Communications EAGLE FTP Table Base Retrieval (FTRA)
- » Oracle Communications Local Service Management System (LSMS)

The Feature Guide complements the OC EAGLE user documentation by emphasizing new features and hardware used in new deployments. See also the EAGLE Planning Guide to help plan for deployment and configuration of the EAGLE and LSMS.

The revision of this Feature Guide reflects these releases: EAGLE 46.3, EPAP 16.1, ELAP 10.1, FTRA 4.5, and LSMS 13.2.

For detailed product information or for requirements of earlier releases, always refer to the user documentation for the respective release. Contact your Oracle Communications Sales representative to obtain any of the listed documentation.

About the Oracle Communications EAGLE

The EAGLE is the world's leading signaling platform and a future-proof solution for operators migrating to next-generation IP connectivity. From a single platform, the EAGLE performs key functions such as signal transfer point (STP), signaling gateway, intelligent routing, screening services, number portability (NP) and integrated performance and service management. Service providers can optimize the use of network resources, manage subscribers and migrate them to new technologies, control fraud, and interoperate between networks with disparate technologies. The EAGLE delivers impressive database size, signaling capacity and transaction speed. These advanced features, coupled with high-performance IP connectivity, optimize today's core telecommunications network with scalability, reliability, security, and flexibility, while providing investment protection. The following products are supported on the EAGLE platform.

- 
- » SS7 Signal Transfer Point (STP) - The STP delivers ANSI/ITU National or International Gateway functionality, centralized signaling routing, and bridges the existing circuit switched and packet networks.
 - » Signaling Gateway - offers proven and robust IP signaling solutions to fit a variety of networking needs and boasts some of the largest deployments in all regions of the world.
 - » Number Portability - a broad portfolio of number portability solutions covering GSM, CDMA and fixed networks, as well as intra-carrier number retention. Provides number portability solutions to over 115 operators in 42 countries.
 - » HLR Selection - Home Location Register (HLR) routing solution provides a cost-effective, turnkey solution to more efficiently distribute subscribers and services across multiple HLRs in the network or across multi-technology networks (mixing Legacy HLR, Next Generation HLR...)
 - » Equipment Identity Register - The Equipment Identity Register (EIR) effectively renders a stolen handset useless and helps deter handset theft.
 - » Integrated Applications - The EAGLE platform supports a variety of network services and value-added applications, including:
 - » Intelligent routing services such as subscriber management, access screening, GSM equipment identity register, least cost routing, number translation, managed roaming, bridge/migration gateway and more.
 - » Triggerless services for the deployment of services without expensive intelligent network (IN) switch upgrades, such as number screening for fraud control, NP and number substitution.
 - » Applications to efficiently manage the transition from 2G/3G to 4G technologies, such as Voice over LTE.
 - » Integrated monitoring supporting network applications for revenue protection, service assurance and market intelligence.

Oracle Communications EAGLE Product Overview & Benefits

The EAGLE is the world's leading signaling platform and a future-proof solution for operators migrating to next-generation IP connectivity.

Benefits

- » **Single Platform:** a unique platform supporting key functions such as integrated monitoring, signal transfer, signaling gateway, advanced routing applications, screening and security, and number portability.
- » **Scalability:** Operators can purchase the capacity and connectivity needed to meet existing or planned network requirements.
- » **Reliability:** 99.99999+>% field-proven reliability in wireless/wireline networks worldwide.
- » **Flexibility:** Supports an extended variety of link interface types and industry standards for flexible configuration and connection of network devices.
- » **Network security:** Signaling connectivity to other service providers is centralized at the EAGLE.

» Investment protection: Protects original investment by providing a migration path to next-gen networks for both core and advanced features.

*Reliability calculated using accepted industry methods of measuring STP population availability in a mated pair configuration.

OC EAGLE
Functional Overview

Signaling Gateway	<ul style="list-style-type: none"> Supports M2PA, M3UA and SUA interfaces Seamless migration from TDM to IP Deployed in both in the Core and Edge Vast customer experience & vendor interoperability
Number Portability	<ul style="list-style-type: none"> Integrated NP solution supporting many services Deployed throughout the world both in Wireline and Wireless market - >100 operators in >40 countries Support Voice, Prepaid, SMS and MMS messages
SS7 Signal Transfer Point	<ul style="list-style-type: none"> Provides core SS7 functionality and inter-connectivity throughout the SS7 network LSL, HSL or SIGTRAN support 2 to 2,800 signaling links Integrated Monitoring
Security and Fraud	<ul style="list-style-type: none"> Supports multi-layer screening and filtering: Gateway Screening of MTP routed messages
Advanced Routing	<ul style="list-style-type: none"> Provides advanced and flexibility routing capabilities for variety of applications HLR Router - Flexible routing of message to HLR

ORACLE

Copyright © 2013 Oracle and/or its affiliates. All rights reserved.

Figure 1: Oracle Communications EAGLE Functional Overview

Go Forward Product Model

The Go Forward Product Model lists the software licenses available and the unit by which the licenses are sold.

Table 1: Go Forward Product Model

Product Grouping	Product Name/Description	Metric	Classifications
Base	Oracle Communications EAGLE (base fee)	Per Node	ISO
	Oracle Communications EAGLE (capacity)	Per 250K TPS	ISO
Number Portability (North America)	Oracle Communications EAGLE LNP Advanced Service Module Enabler	Per Card	ISO
	Oracle Communications EAGLE LNP	Per Node	ISO
Number Portability (Rest of World)	Oracle Communications EAGLE Advanced Service Module Enabler	Per Card	ISO
	Oracle Communications EAGLE Mobile Number	Per Node	ISO

	Portability		
Software Features	Oracle Communications EAGLE SS7 Firewall	Per Node	ISO
	Oracle Communications EAGLE Suspicious Call Identification	Per Node	ISO
	Oracle Communications EAGLE Service Actions Portability and Flexibility	Per Node	ISO
	Oracle Communications EAGLE Intra Network number Portability	Per node	ISO
	Oracle Communications EAGLE HLR Router	Per Node	ISO
	Oracle Communications EAGLE Equipment Identity Register	Per Node	ISO
	Oracle Communications EAGLE Global Title Translation Routing	Per Node	ISO
	Oracle Communications EAGLE Triggerless ISUP Framework Routing	Per Node	ISO
	Oracle Communications EAGLE Origin Based Routing	Per Node	ISO
	Oracle Communications EAGLE Prepaid Routing	Per Node	ISO
Oracle Communications EAGLE SMS Routing	Per Node	ISO	
Card Licenses	Oracle Communications EAGLE Service Handler 8 GB	Per Card	ISO
	Oracle Communications EAGLE Ethernet B Traffic Handler	Per Card	ISO
	Oracle Communications EAGLE Asynchronous Transfer Mode B Traffic Handler	Per Card	ISO
	Oracle Communications EAGLE E1T1 B Traffic Handler	Per Card	ISO
	Oracle Communications EAGLE Service and Link Interface Card Handler	Per Card	ISO
Oracle Communications EAGLE Application Processor Software:	Oracle Communications EAGLE Application Processor Provisioning (base fee)	Per Card	ISO
	Oracle Communications EAGLE Application Processor Database Capacity (capacity)	Per 500K DB Entries	ISO
	Oracle Communications EAGLE Application Processor Nonprovisioning (base fee)	Per Card	ISO
Oracle Communications EAGLE LNP Application Processor Software:	Oracle Communications EAGLE LNP Application Processor (base fee)	Per Card	ISO
	Oracle Communications EAGLE LNP Application DB Capacity (capacity)	Per 12M LNP Entries	ISO
Oracle Communications EAGLE LSMS Software:	Oracle Communications LSMS	Per Card	ISO
Product Options	Oracle Communications LSMS Query Server	Per Server	SW
Oracle Communications EAGLE Element Management System Software:	Oracle Communications EAGLE Element Management System	Per Server	SW



	Oracle Communications EAGLE Element Management System	Per Node	SW
Product Options	Oracle Communications EAGLE Element Management System Reporting Studio	Per Server	SW
Oracle Communications EAGLE FTP Table Base Retrieval Software:	Oracle Communications EAGLE FTP Table Base Retrieval	Per Server	SW

Operations, Administration, and Maintenance

General

The Operations, Administration, and Maintenance functions provided by the EAGLE are as follows:

- » Operations
 - » Upgrade
 - » Feature Bit and Feature Activation
- » Administration and Provisioning
 - » Terminals
 - » Command Classes
 - » Security
 - » FTP Retrieve and Replace
- » Maintenance
 - » Alarms
 - » Disk Operations (Backup/Restore/Repair)
 - » IMT Fault Isolation
 - » Link Maintenance (LFS, SLTMs)
 - » Device Configuration and Control (covered under the Maintenance subsections and the Administration and Provisioning section)

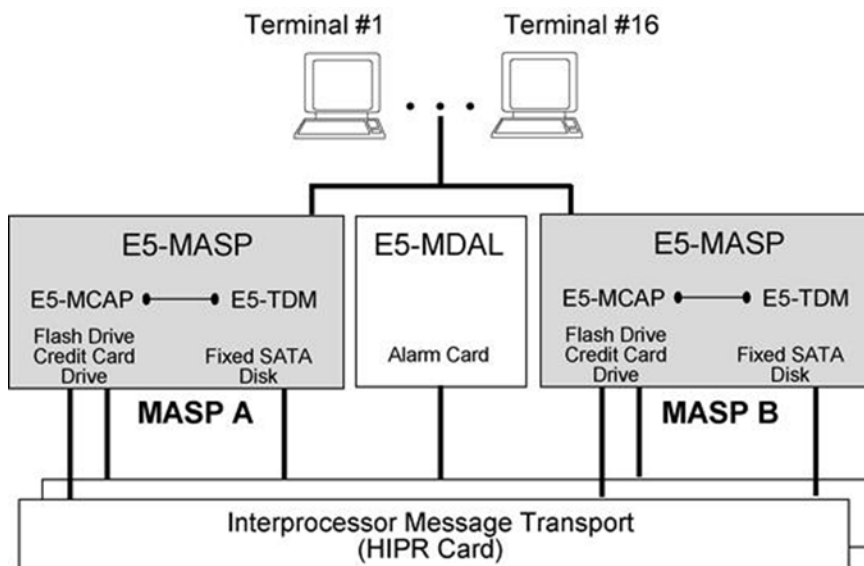



Figure 2: Functional OAM Diagram

Operations

One interesting attribute of the EAGLE is that application cards do not use the OAM cards' functionality for message processing. Hence, OAM operations primarily involve upgrades to the software.

Upgrade



The software upgrades for the EAGLE are executed in accordance to an upgrade procedure. The procedure describes the step-by-step process to perform the upgrade execution as well as pre- and post-upgrade activities required to ensure a successful upgrade. The upgrade execution is accomplished by the use of one command. This command has been developed to determine the current configuration and determine which automatic steps are required to accomplish the upgrade. There are several types of upgrade. The most common upgrade is from a source release to a target release that requires a full database conversion. The second type is going from one release to a maintenance release.

Upgrades can be performed either on site or remotely. This data link is a secure link with password protection. Typically, upgrades take 4-6 hours depending on the size of the system and features involved. The EAGLE can gracefully back out and restore the previous software versions. Should any emergency situation occur during upgrade, recovery procedures can be used to restore the EAGLE without incurring reportable downtime.

Remote Upgrade

As of Release 39.2, the EAGLE supports the ability to transfer an EAGLE software upgrade file via FTP/SFTP from a remote server. A software upgrade can be accomplished without the need for inserting an MO disk locally on site. Check the Planning Guide for hardware dependencies.

Controlled Features

The EAGLE contains a wide variety of optional features that a customer can purchase. The features are controlled either through a system-wide feature bit or through feature activation.

Feature Bit Control

The EAGLE controls some features with a feature bit. To turn on the feature, the user enters a command with the feature parameter set to On. When a feature is turned on, it cannot be turned off.

Feature Activation


Features are activated through configuration instructions or commands. Feature Access Key control is removed. Bandwidth control may still be used, if chosen. Unless specifically designed to do so, once a feature is turned on, it cannot be turned off by the customer. We trust that our customers only activate those features they have licensed.

Administration and Provisioning

Administration of the EAGLE can be accomplished via one of the 16 serial connections, 24 telnet connections, or via the SNAM interface. Each serial terminal can be configured in a variety of modes:

- » VT320 - normally used as a full-service terminal for personnel.
- » Keyboard Send Receive (KSR) - allows faster throughput since the control characters associated with the VT320 mode of terminal operation need not be transmitted.
- » Printer - provides output to a printer. No input is accepted.
- » SCCS - provides a non-printable ASCII 0x01 character to the beginning of the EAGLE output headers which allows the SCCS to identify the beginning of a new output from the EAGLE. SCCS uses KSR mode for presentation.
- » Management (MGMT) - provides a modified KSR style terminal to better interface with OSS equipment

For those customers who desire to administer and provision the EAGLE via IP, the EAGLE supports IP-based connections to the EAGLE user interface (UI) via a telnet client. The IP User Interface feature adds up to 8 connections via a single IPSM card, up to 3 cards per system (total 24 telnet access ports), in addition to the existing 16 RS-232 terminal ports.



Some key benefits of an IP connection are that a Dial-up connection is not required, additional EAGLE UI access points are provided, allows access to the EAGLE UI from an IP network, improved UI speed and data throughput, enhanced output buffering (vs. serial terminals) and provides for a robust platform for future IPUI development.

The additional ports are accessible from any existing LAN or WAN connection along a customer's IP-based network. Craftspersons only need access to a standard telnet client to connect to and work on the EAGLE.

Other OAM items of note:

- » Each EAGLE terminal connection can support retrieval of up to 10 serial connections or 20 telnet terminal connections.
- » The EAGLE can also be configured to support most commonly used timezones.

EAGLE Command Classes

The EAGLE provides the following non-configurable command classes that can be assigned to different users of the system:

- » Basic
- » Debug
- » Link Maintenance
- » Program Update
- » Security Administration
- » Database Administration
- » System Maintenance
- » LNP Basic
- » LNP Database Administration
- » LNP Subscription

Additionally, the Command Class Management feature allows the user to place Oracle Communications EAGLE commands into 32 new configurable command classes, which are in addition to the non-configurable command classes. The craftsperson can provision any of these configurable command classes to contain any EAGLE commands. The command classes can then be assigned to a user and/or terminal, thus allowing the user or terminal the privilege of executing any command in the class. This allows users and terminals to fully configure custom command classes.

EAGLE Security

The EAGLE has many features to maintain the security of the system by enforcing specific requirements for logging onto the EAGLE, specific management actions for user IDs and terminals, and requirements for creating and managing passwords. The specific EAGLE security features are listed below:

- » Unauthorized Use Warning Message
- » Login Success or Failure Tracking
- » Disallow Simultaneous Login Sessions with the Same User ID
- » Idle Terminal Port Lockout
- » Logout on Communications Failures
- » Revoking a User ID
- » Management of Unused User IDs
- » Password Requirements and Encryption
- » Clearing Passwords from RAM

- » Locking a Terminal's Keyboard
- » 50,000 entry (rolling) Security Log
- » Secure Shell on IP User Interface

FTP Retrieve and Replace

When the IP User Interface feature is on, the FTP Retrieve and Replace feature is available and provides expanded retrieve and replace capability.

FTP Retrieve and Replace uses EAGLE FTP commands to transfer portions of the EAGLE OA&M database to a customer Windows-based PC or UNIX FTP Server or Client.

FTP Table Base Retrieval Application

The EAGLE FTP Table Base Retrieval Application (FTRA), a Java-based application running on a Windows-based PC or UNIX FTP Server, uses IPUI terminals and FTP Retrieve and Replace to retrieve EAGLE table data for supported rtrv commands. FTRA can be used to manipulate the table data and send subsequent changes (replace) to the Oracle Communications EAGLE OAM.

The FTP Retrieve and Replace capability provides the following capabilities:

- » Enhanced retrieve capabilities of EAGLE table data, whereby the application retrieves table data transparently upon request by the user and converts the data to a comma-separated variable (.csv) file.
- » Enhanced input (replace) capabilities of EAGLE table data, supporting input of script files containing commands created by the user. The transfer of data to the EAGLE is transparent to the user.
- » A much faster and more reliable retrieval and input capability.
- » Validating data prior to input and identifying the data at issue.
- » Automated scheduling of data retrieval
- » Connection up to 100 STPs
- » Command Line capability in addition to GUI capability
- » Logging of all retrieve activity
- » Filtering
- » Secure Shell capability (secure shell and SFTP) concurrent with the EAGLE OA&M IP Security Enhancements feature.

FTP is used to quickly retrieve large provisioning tables from the EAGLE in an easy, reliable manner. FTP allows easy connectivity over an IP network and provides a fast, reliable transfer protocol. By speeding up and facilitating the retrieval of provisioning tables, it becomes easier to manage database table data.

The figure below shows the high-level data flow for the FTP Retrieve and Replace capability.

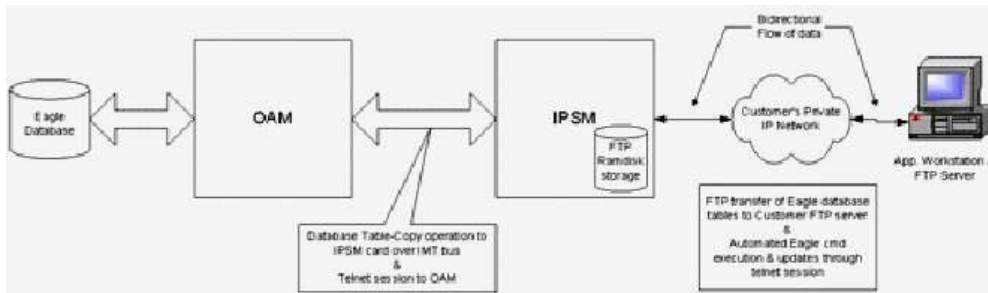



Figure 3: High Level Data Flow for FTP Retrieve and Replace Feature



For data output, EAGLE table data is transferred from the EAGLE OAM through the IPSM card and then by FTP to a customer's workstation to create an offline copy of the database. FTRA is then used to convert EAGLE table data into CSV file output.

For data input, EAGLE command files can be used to send commands back to the EAGLE OAM. An EAGLE command file is an ASCII text file, which contains only supported EAGLE commands. Once an EAGLE command file is ready for input, the file must be validated against the offline EAGLE database prior to sending the commands to the EAGLE OAM. FTRA allows the user to visually validate the commands prior to sending the file to the EAGLE. Once offline database validation and visual validation are complete, the user can use FTRA to send the validated commands back to the EAGLE through a telnet session at an IPUI telnet terminal.

During replace operations, there is no synchronization of databases with the live EAGLE database. The lack of database synchronization may cause problems with conflicting provisioning performed on the EAGLE during the interim.

CSVGEN Upgrade from EAGLE TDM

Starting in EAGLE Release 32.0 and later, a single installation of FTRA can provide support to multiple systems running different Oracle Communications EAGLE releases. The CSVGen components will be transferred along with the EAGLE table data during all transfers. The transfer will be done automatically and ensures that the FTRA is always current and up-to-date with every connection to the EAGLE.

FTRA Dependencies on EAGLE

As of release 46.0, the FTRA dependencies on EAGLE are removed, including, validation of rtrv-gpl in FTRA and generation of stp.csv by FTRA.

EAGLE OA&M IP Security Enhancements

The basic Telnet and FTP protocols used by the optional IP User Interface (IPUI) feature and the FTP Retrieve and Replace feature should be used only in a private network. Telnet passwords are transmitted unencrypted as plain text, and FTP file transfers are sent in the clear. Public networks require a more secure transmission.

The EAGLE OA&M IP Security Enhancements feature adds protection of password transmission and data communications between the EAGLE and the user's management system and/or terminal equipment, and strengthens the authentication of users.

For the Measurements Platform feature and FTRA, the Secure FTP (SFTP) function of the EAGLE OA&M IP Security Enhancements feature provides IP security over the connection between the EAGLE and the remote FTP server or client. SFTP supports strong data encryption using widely accepted cipher routines. SFTP guarantees data integrity, which ensures data cannot be tampered with, even while in transit over the network. A 32 MB MCPM card must be used for the Measurements Platform when the EAGLE OA&M IP Security Enhancements feature is used for secure measurements data transfer.

The EAGLE OA&M IP Security Enhancements feature can be turned on and off in the system. The feature is on or off for both IPUI and Measurements platform. It cannot be on for one feature and off for the other feature at the same time.

Secure Shell (SSH)

Secure Shell (SSH) is the protocol for secure remote login and other network services over a non-secure network. The EAGLE OA&M IP Security Enhancements feature uses SSH to encrypt and authenticate all incoming and outgoing transmissions, including passwords, for incoming and outgoing transmission of EAGLE IPUI traffic,

including passwords, to effectively eliminate eavesdropping, connection hijacking, and other network-level attacks. For the EAGLE OA&M IP Security Enhancements feature to operate correctly, all SSH clients and SFTP servers supported for this feature must be compatible with OpenSSH Version 3.7.1.

EAGLE OA&M Password Security Enhancements

The EAGLE OA&M Password Security Enhancements feature increases the security measures used by the EAGLE Password Management facility.

New Security Measures:

- » • More restrictive password measures
- » • Prevention of password re-use
- » • Prevention of bypassing password re-use rules
- » • Prevention of a common password pattern
- » • Access to the EAGLE for a specified period without requiring a password change
- » • Enhanced notification to the user that passwords have expired or are about to expire

SEAS over IP

- » The SEAS-over-IP (SOIP) feature provides a TCP/IP-based interface for SEAS. The SEAS interface constitutes the path between the EAGLE and a Common Channel Signaling Message Router (CCS MR). The EAGLE acts as a client and connects to the CCS MR, which acts as the server. Data is passed between the EAGLE and the CCS MR using the SR-5129 protocol.

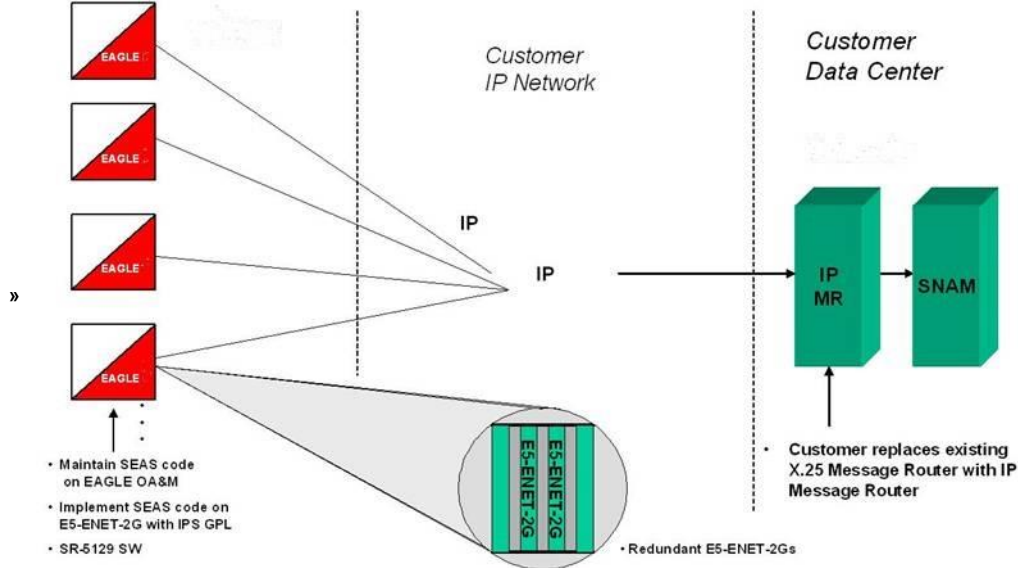


Figure 4: SEAS Architecture/Deployment using IP

The SEAS-over-IP feature has the following limitations:

- » MMI messages are not supported.
- » The CCS MR node name is not configurable by the EAGLE. The CCS MR must be assigned a name by Telcordia.
- » The only supported Authentication Mode in Oracle Communications EAGLE for Client Authentication for communication with the CCS MR with the Security Feature for Password Authentication.

Maintenance

EAGLE maintenance uses commands and test procedures to ensure database preservation and to troubleshoot different EAGLE components. Maintenance functions include:

- » Alarms
- » Disk/Database Maintenance
- » IMT troubleshooting
- » Link Maintenance

Alarms

The EAGLE provides a wide variety of alarm indications to allow easy identification and acknowledgment of a system alarm.

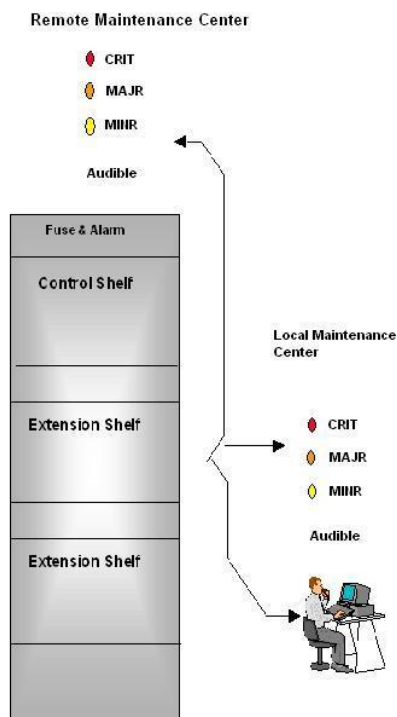



Figure 5: Alarm Diagram

Alarm status region of the VT320 display terminal shows how many alarms are pending in the following four categories:

- » **CRIT** – critical alarms
- » **MAJR** - major alarms
- » **MINR** - minor alarms



» **INH** - number of devices that have alarms inhibited

The EAGLE allows the connection of up to 16 external devices for alarm reporting. These devices are defined in the EAGLE database as customer-defined troubles. The devices are monitored and report state changes to the user through an unsolicited alarm message (UAM).

Alarms can also be inhibited. Alarm inhibiting allows the user to inhibit critical, major, and minor alarms for specific devices. There are two types of inhibits for alarms - temporary and permanent.

A temporary alarm inhibit will inhibit the specific device alarm until the condition that caused the alarm is no longer present. When the alarmed condition is no longer present, the alarm inhibit will be automatically cleared.

A permanent alarm inhibit will also inhibit the specific device alarm but will keep the alarm inhibited even if the alarming condition clears. Removing a permanent alarm inhibit requires manual intervention to clear the inhibit.

Alarms can be turned off for these devices or entities:

- » Cards
- » Signaling links
- » Linksets
- » Routes
- » EAGLE terminals
- » System clock
- » TCP/IP data links
- » Customer defined troubles
- » Signaling Engineering and Administration System (SEAS)/X.25 links
- » IP Gateway application sockets
- » IP link between the LSMS and MPS

Disk/Database Maintenance

Each TDM (fixed disk) contains the "master" set of data and programs for an EAGLE. The EAGLE provides redundant storage (active and standby) of the system data. The order of operations on the active and standby fixed disks on the TDMs is that the active TDM is executed first, followed by the standby TDM.

A logical view of the different EAGLE database partitions is shown below.

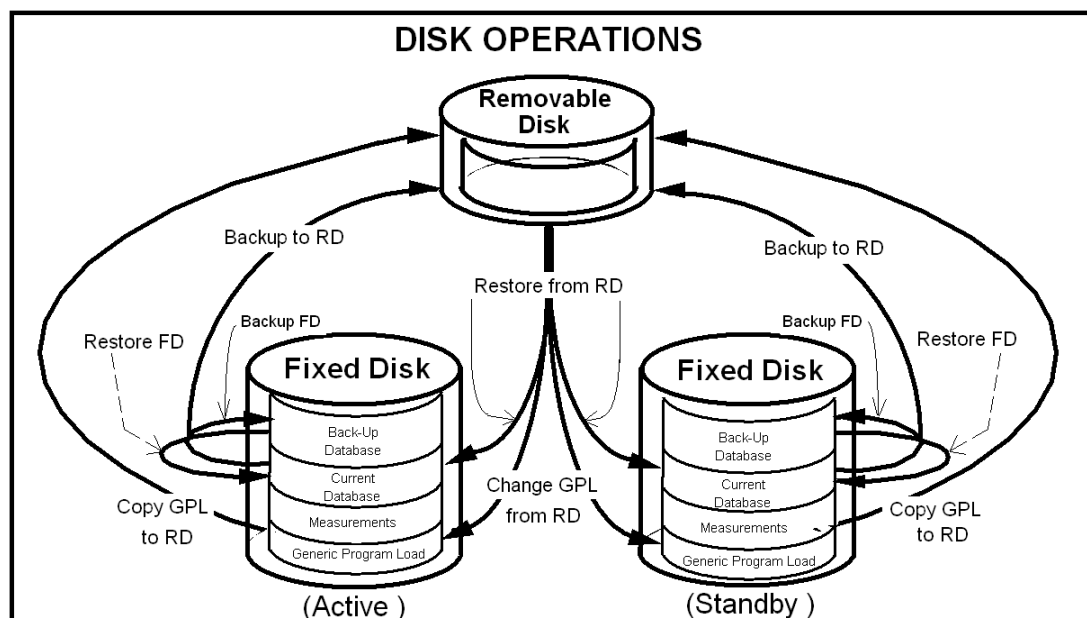


Figure 6: EAGLE Database Operations

Active/Standby Fixed Disks

The active and the standby disks each contain 5 partitions. A partition is a logical grouping of related tables. The types of partitions are the current database partition (usually called the current partition), the backup database partition (usually called the backup partition), the measurements partition, the GPL partition, and the common partition (not shown in the figure above).

The data that can be administered by users is stored in two partitions on the fixed disk - a current database partition that has the tables that are changed by online administration and a backup database partition that is a user-controlled copy of the current partition. All of the online data administration commands work on the data in the current partition. The purpose of the backup partition is to provide the users with a means of rapidly restoring the database to a known good state if there has been a problem while changing the current partition.

A full set of Generic Program Loads (GPLs) is stored on the fixed disk in the GPL partition. There is an approved GPL and a trial GPL for each type of GPL (except for the GPLs for the OAM and a test GPL named CDU, both of which have only an approved version).


Measurement tables are organized as a single partition on the fixed disk. These tables are used as holding areas for the measurement counts and are rewritten every 24 hours.

The common partition (not shown in the figure above) has only a few tables. The most important table is the DMS configuration table, which contains information about the size of all tables.

Some of the routine database management functions are listed below.

- » Database Backup/Restore/Repair
- » Database Copy (Fixed Disk to Fixed Disk)
- » Disk Coherency Tests
- » Online Disk Formatting

Removable Cartridge



A removable cartridge can be used for four purposes:

- » To hold an offline backup copy of the administered data
- » To hold an offline copy of the set of GPLs installed on a system
- » To hold a copy of the measurement tables so they can be processed by an offline PC-based program
- » To hold an offline copy of the security log.

A single removable cartridge cannot store data, GPLs and measurements. A removable cartridge can be formatted and initialized for use either for storage of data and GPLs, or for storage of measurement tables, but not for both.

The two types of removable cartridges are referred to as:

- » System removables (Data and GPLs)
- » Measurements removables

Disk Maintenance Operations

» Database Backup

Database backups are made to the backup partition of the fixed disks or onto the removable cartridge. The original data is taken from the current partition on the fixed disk. Only the administered database tables are included in the backup. GPLs and measurement tables are not part of the backup. Note this is not the EPAP/ELAP databases, which are backed up separately from the EPAP/ELAP systems. This backup is only for the EAGLE OAM database.

» Remote Backup

As of Release 39.2, the EAGLE supports the ability to backup the EAGLE OAM database to a remote server, without the requirement of inserting an MO disk locally on site. Check the Planning Guide for hardware dependencies. The backup data is transmitted to a remote server via FTP or SFTP. The entire database is backed up in a single file.

» Database Restore

Database restores are made from the backup partition of the fixed disks or from the removable cartridge. Database restores only restores the administered data tables, not the GPLs or measurement tables.

» Remote Restore

Along with the R39.2 Remote Backup capability, the EAGLE also offers database restore from a remote server. Check the Planning Guide for hardware dependencies.

» Database Repair

Database repair copies the current and backup partition from either the active or the standby fixed disk to the other.

» Copy GPL

This command copies the set of approved GPLs from the active fixed disk on the TDM or the removable cartridge onto the standby fixed disk on the TDM or the removable cartridge. This is typically done after the installation of a new GPL on the system, when the GPLs have been approved, and will allow the user to keep one removable cartridge with a copy of all the approved GPLs in use on the system.

» Copy Measurements

When there is a need to perform offline analysis of the raw measurements data, this command copies that data onto the removable cartridge. The data is copied from the active fixed disk on the TDM to the removable cartridge.

IMT Fault Isolation

Interprocessor Message Transport (IMT) subsystem fault isolation procedures are designed to isolate non-transient IMT problems that have been detected on an IMT bus or a card attached to that bus. The IMT bus needs to be out of service in order to perform this procedure.

This places the EAGLE in IMT simplex mode.

These procedures can be used to:

- » Detect non-transient IMT faults
- » Isolate IMT bus failures to the bus segment or individual card

IMT fault isolation procedures can dramatically reduce the amount of time and effort needed to find and solve IMT-related problems. The table below shows what would be required to find a particular fault on the IMT bus with and without the IMT fault isolation feature. The data in this table is based on the EAGLE containing the maximum 16 shelves, with each shelf fully populated with cards.

Table 2: Number of Components to Inspect Under Various Conditions

Component Type	Without IMT Fault Isolation	If Fault is Isolated to the Card Level	If Fault is Isolated to the Bus Segment Level
Intershelf cables	16	0	0 or 1
HIPR2	32	0	1 or 2
Backplanes	16	0	1 or 2
Cards	252	1	2
All components	316	1	4 to 7

Note the All components row. In this example, without the IMT fault isolation procedures, there are 316 possible failure points to investigate. With IMT Fault isolation, potential failure points are narrowed down to one component (best case) or 4 to 7 components, depending on the number of cards in the suspect IMT bus segment.

IMT bus errors can be either transient or non-transient. Transient errors cause packet loss or data corruption, but the cards remain connected to the IMT bus. Non-transient errors cause the cards to be disconnected from the IMT bus. The IMT Fault Isolation procedures detect non-transient errors.

Non-transient errors fall into two categories:

1. Errors that cause all cards to be isolated from one of the IMT buses (the IMT bus is out of service)
2. Errors that cause a subset of the cards (typically a single card) to be isolated from one of the IMT buses (the IMT bus remains in service)

When an IMT bus is out of service, IMT fault isolation can determine the location and probable cause of the failure. Those faults that are card-specific are isolated to the card. Faults that cannot be isolated to a specific card are isolated to the segment of the IMT bus on which they occur. No attempt is made to isolate a particular component below the card level since cards are a field replaceable unit.

Link Maintenance

The EAGLE supports the following link maintenance procedures:

- » Administrable SLTMs
- » Link Fault Sectionalization
- » Loopback testing for ATM links

- » Remote Loopback Testing for DS0A
- » Command Driven Loopback
- » Link Diagnostics

Administrable SLTMs

This function allows the user to configure signaling link test messages (SLTMs). To test the coherency of a particular link, two signaling points can transmit periodic test messages. The signaling point initiating the test selects a link to test and then transmits an SLTM containing a test pattern. The other signaling point responds with an echo of the test pattern contained in the SLTM. The intervals between transmission of SLTMs are controlled by the *sltm_enabled* field in a corresponding SLTM table record. The SLTM table record also controls the following:

- » Length of the test pattern in the SLTM
- » Automatic generation of SLTMs
- » Generation of periodic SLTMs when a link is put in service

The SLTMs can be sent to a signaling link that is in service whenever desired.

Link Fault Sectionalization

The EAGLE supports up to 1024 Link Fault Sectionalization (LFS) tests at one time and a maximum of 32 remote link elements for each LFS Test while being able to display real time results of the tests in progress. Link Fault Sectionalization is not specified nor supported on ATM based High Speed Links but alternative loopback tests are provided as described in **Loopback Testing for ATM Links**. LFS is only supported for DS0 56 Kbps links. The E1/T1 MIM (in T1 mode) and MPL-T cards support up to 8 simultaneous LFS tests.

Link Fault Sectionalization allows maintenance personnel, using industry standard error patterns, to perform DS0 fault sectionalization tests, a series of far-end loopback tests from the local EAGLE or to a remote EAGLE, and to identify faulty segments of an SS7 transmission path up to and including the remote network element.

The SS7 LIM must be powered up and provisioned with the signaling link deactivated before starting the link fault sectionalization tests. No messages are transferred to or from the signaling link by the SS7 LIM while the link is performing a Link Fault Sectionalization test.

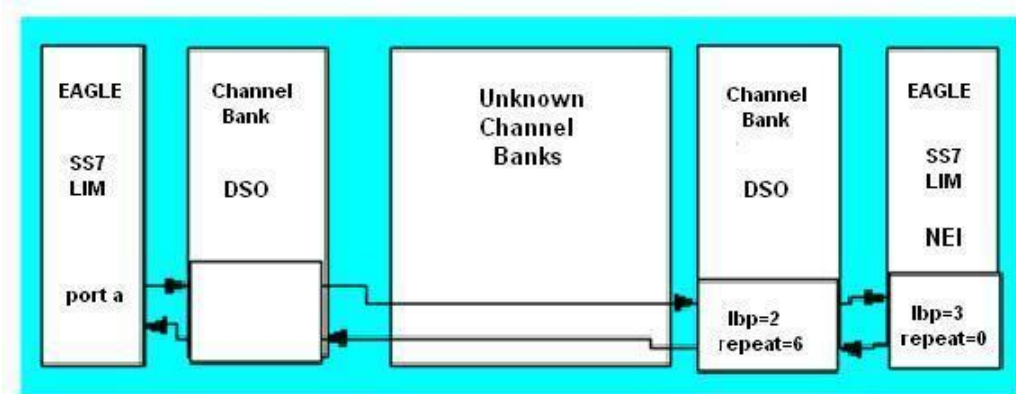


Figure 7: Link LBPs for Latching Test

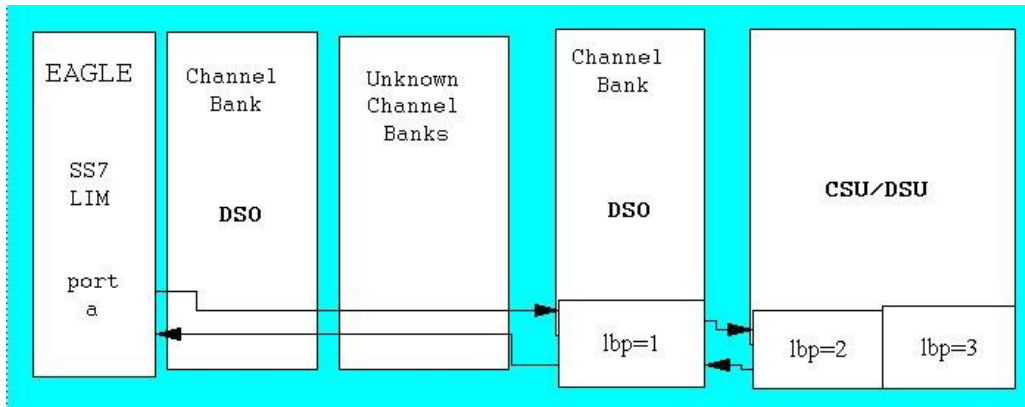


Figure 8: DS0 Link LBPs for Non-Latching Test

The point on the signaling link at which each loopback test ends is called the far-end loopback point. A far-end loopback point (LBP) is achieved when the remote link element (RLE) sends the received data back to the transmitter, allowing the transmitter to verify the received data.

Table 3: Link Fault Sectionalization Tests Remote Link Element (RLE) Types

Element	RLE Description	Latching	Nonlatching
DSO	DSO Dataport	Yes	No
CSU	CSU Dataport	Yes*	Yes
DSU	DSU Dataport	Yes*	Yes
NEI	Network Element Interface	Yes	No

* The CSU and DSU must be strapped or optioned to support latching link fault sectionalization loopback.

The LBP is moved along the signaling link path until the LBP is in the far-end network element. Therefore, each LBP along the link requires the initiation of one link fault sectionalization test on the SS7 LIM.

Table 4: Link Fault Sectionalization Test Types

Link Fault Sectionalization Test Types	Description
Latching link fault sectionalization test (LLT-auto)	A loopback point is established using signaling commands and remains until it is removed by signaling commands.
Latching link fault sectionalization test (LLT-man)	A loopback point is established by manual means and remains until it is removed by manual means.
Nonlatching link fault sectionalization test (NLT)	A loopback command is interleaved with the test data.

Loopback Testing for ATM Links

The `tst-slk` command allows the operator to run ATM loopback tests for up to 24 hours. This functionality is similar to Link Fault Sectionalization for standard DS0 loopbacks. This functionality allows the customer to verify intermittent ATM link problems. The `tst-slk` command tests can be grouped into two categories, message-based tests and hardware-based tests. The SLTC and OAM tests are message-based tests. These tests involve sending a message

to the far end and expecting an appropriate reply. All ATM cards support these tests. The LXVR, LINE, and PAYLOAD tests are hardware-based tests. The E1-ATM card does not support LINE and PAYLOAD tests.

Remote Loopback Testing for DS0A

This function is provided for signaling links connected to a LIM card running the *ss7ansi* application. This capability allows the signaling link to be placed in loopback automatically when it receives a valid latching loopback code sequence from the network (when a test pattern is detected). This allows the signaling link to be tested from another far-end network element or maintenance test unit. While in loopback mode, the signaling link is out of service.

Command Driven Loopback

Command Driven Loopback allows the operator to force a link into a loopback to the far end. This feature is similar in functionality to a remote initiated loopback except that the operator manually puts a signaling link into loopback to the far end. A signaling link may go in and out of loopback as determined by loopback codes sent by the far end, however, a link placed in Command Driven Loopback will remain in loopback until removed from loopback via a command. Command Driven Loopback allows loopback testing of a signaling link when either far-end-initiated loopbacks are prevented or when a constant loopback state is desired. IPLIMx and IPGWx cards do not support this capability.

Link Diagnostics

Link Diagnostics provides detailed status information of link failures. This capability either confirms or eliminates a portion of the near-end node as the reason for the link failure.

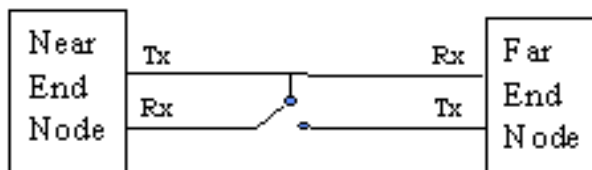


Figure 9: Link Diagnostic Diagram

SS7 Level 2 status information is buffered before and after a link failure has occurred. This feature provides the capability to loop the internal transmit and receive data on the LIM card. Link failures can occur on the near-end node, far-end node, or the cable connecting the two nodes.

Link Failure Status Information


The Level 2 SS7 data is divided into two groups: service data and alignment data.

Service data is a running history of when the link comes in service and goes out of service. The history contains the reason the link fails from the perspective of Level 2 along with the timestamp. This information can be used to help solve whether the near-end or far-end node is responsible for causing the link to fail.

Alignment data is a running history of Level 2 alignment events with timestamps. This information can be used to help determine why the link does not realign.

The service and alignment data buffer and the service data buffer can each hold 69 events.

SNMP V2 Traps on E5-OAM



The current SNMP northbound interface for faults provided by the EAGLE requires an EMS to convert those faults/alarms to SNMP traps for northbound delivery to an NMS. A new SNMP interface will be added to the EAGLE to allow the EAGLE to directly send SNMP traps northbound to an NMS, or up to 2 NMSs.

Prior to this feature, there was no direct SNMP northbound interface from the EAGLE to an EMS or NMS. This causes the need for a separate EMS to serve as an intermediary between the EAGLE and an NMS. This intermediary EMS reads the EAGLE alarms based on textual output (in ASCII format) from the EAGLE and translates those alarms into SNMP traps sent northbound to the NMS.

This feature allows the EAGLE to directly communicate with an NMS, without requiring the intermediary EMS. There are some constraints, in that the data stream of SNMP traps for alarms will not provide the configurable pre-filtering of alarm data. The NMSs will receive SNMP traps for all devices being alarmed/alarm cleared. The NMSs may also receive UIM data in the form of SNMP traps as well.

With the current EAGLE EMS methodology, an NMS sends an SNMP SET variable to the EAGLE EMS when a resynchronization is required. The EMS front-end provides facilities for filtering of the alarms.

This SNMP implementation is a FAK controlled feature (893-0404-01) that will allow for EAGLE Traps, to provide for both UAM and UIMs. This FAK can only be activated and turned “on” or “off” for the Oracle Communications EAGLE Maintenance and Administration Subsystem Processor Card with SSD Locking and the Oracle Communications EAGLE Maintenance Disk and Alarm cards ONLY. Once activated and turned on, these traps will be sent to an NMS or set of NMSs specified by the “ent/chg/trv-snmpp-host” commands. It will also allow configured NMSs to request a resync for all of the existing UAMs. And each provisioned NMS will receive a heartbeat Trap at a rate determined by the NMS declaration so the NMS will know it is connected in low periods of UAM/UIM activity.

EAGLE Eyes OAM Friendly Commands

Introduced in release 46.0, the Eagle Eyes OAM Friendly Commands feature allows users to configure and perform Eagle Eyes traffic captures using OAM commands.

MTP-SCCP FUNCTIONALITY

GENERAL


The EAGLE implements the ANSI SS7 protocol in accordance with applicable sections of ANSI Standard T1.111-112 and T1.114. The EAGLE implements the ITU SS7 protocol in accordance with applicable sections of Q.7XX.

This section is not intended to describe basic SS7 functionality but rather to highlight specific MTP and SCCP protocol features supported in the EAGLE as follows:

- NRC Features
- Advanced MTP Capabilities
- Gateway Screening
- GSM MAP Screening
- Global Title Translations
- Support for J7 (Japan SS7)

Database services provided by the Oracle Communications EAGLE are covered in Chapter 5.0.

NRC FEATURES



An extensive study of SS7 procedures was performed by the industry and standards bodies to identify the requirements to improve the reliability of the signaling network. The study resulted in 17 recommendations which were later prioritized and published by the Network Reliability Council (NRC). These 17 NRC items have been incorporated in the ANSI and Telcordia standards. Some of these features are also applicable to the ITU network and are noted as such. The implementation of these NRC items will result in a significant improvement of network reliability. To meet the NRC objectives, the EAGLE contains all 17 NRC features, as applicable to an STP and network implementation of these features:

1. Signaling Message Handling Congestion Control
2. Procedure to Eliminate False Link Congestion
3. Prevention of Congestion on Newly Available Linksets
4. Prevention of Congestion from Rerouted Traffic
5. TP Circular Route Detection
6. Prevention of Link Oscillation
7. MTP Restart
8. Procedures for Recovery from Processor Outages
9. Cluster Routing and Management Diversity
10. SCCP Routing in Response to MTP Congestion
11. Prevention of SCCP Circular Routes
12. Prevention of Trunk Looping caused by ISUP
Not Applicable to the EAGLE
13. 8-Bit SLS Support
14. Improved Signaling Link Test (SLT) Procedures
15. Backup Procedures Against Loss of TFR/TCR
16. MTP User Flow Control
17. Optional TFP Broadcast across Network Boundaries

Signaling Message Handling Congestion Control - ANSI


Procedures were added to the EAGLE MTP protocol to control STP signaling message congestion handling. If the STP has an internal failure that causes a reduction in the STP's signaling message handling capacity, an option exists for the EAGLE to request traffic to be rerouted by sending TFR messages to adjacent SPs with the destinations of discarded messages indicated. Message-congestion handling also includes provisions for the discard of messages by priority.

Procedure to Eliminate False Link Congestion - ANSI

It is possible that some problems on a link in a linkset will cause that link to go into congestion, even though the traffic on the linkset is not high enough to cause congestion. For example, if a link has a large number of retransmissions, the traffic on the link could increase enough to cause congestion on that link.

To correct this condition, EAGLE will start a T31 timer whenever a link goes into congestion. If the link remains in the same congestion state until T31 expires, the link will be removed from service. The link will become unaligned, and then the alignment procedure will be started.

The congestion level that starts the T31 timer is also provisionable to either congestion level 1 or congestion level 2. T31 is started for a link anytime it reaches this congestion level or a higher level. An increase in congestion level or abatement to a lower congestion level restarts the timer. Abatement below the provisioned congestion level stops the timer.



For example, if T31 is 60 seconds and a link goes into congestion level 1, a 60-second T31 timer is started. If after 45 seconds the link's congestion increases to level 2, the timer is restarted. If the link remains at congestion level for 60 seconds, the link is taken out of service and it becomes unaligned. Then the alignment procedure is started, and the EAGLE attempts to realign the link.

This procedure and the T31 timer are only defined in ANSI networks.

Prevention of Congestion on Newly Available Linksets - ANSI

When a large linkset first becomes available, there may not be enough links up to carry the normal amount of traffic on the linkset. Without this procedure, multiple-link linksets have a high probability of recongesting if all traffic is resumed and a sufficient number of links in the link set are not available (e.g., if TFA is sent). In effect, a single link within a link set could be burdened with the entire load of traffic destined for the link set if this procedure is not instituted. Thus, the EAGLE will not broadcast TFAs when there are not enough links available in a linkset. This feature only affects linksets or combined linksets with 3 or more links equipped.

When a linkset that was previously unavailable becomes available and if the number of links available is less than the required number of links, the EAGLE will not broadcast TFAs. For point codes that were previously prohibited that use the linkset as the least cost route, the EAGLE will broadcast TFRs. For point codes that were previously restricted that use the linkset as a least cost route, the EAGLE will not broadcast any TFx message.

Prevention of Congestion from Rerouted Traffic - ANSI/ITU

This procedure eliminates the possibility of congestion resulting from a burst of rerouted traffic emanating from the failure of other signaling routes by pacing the broadcast of TFx/TCx messages. This regulation of broadcast will have the net effect of dealing with congestion much more effectively.

Controlled rerouting is performed by a signaling point upon receipt of a transfer allowed or transfer restricted message, which results in traffic being diverted from a less efficient route to a more efficient route. During controlled rerouting, the signaling point stops traffic toward the concerned destination on the current route. It then buffers messages for a time period before routing them on the new route. This is done to minimize message mis-sequencing by allowing time for the traffic already on the less efficient route to reach its destination.

After the EAGLE broadcasts TFA/TCA or TFR/TCR messages announcing the change in status, multiple signaling points may perform controlled rerouting and release messages on the new route nearly simultaneously. This burst of rerouted traffic is a potential source of congestion.


This is available for both ANSI and ITU Networks. If TFA/TFRs are sent for affected X.25 pseudo point codes, they are also paced.

MTP Circular Route Detection - ANSI

If routing data were provisioned incorrectly, or were corrupted, MSUs could be routed in an endless circular route. With the addition of cluster routing and E links, there is an increased danger of circular routing.

If the EAGLE detects circular routing, a flag is set, showing that circular routing was detected for this destination. The destination is prohibited and a critical alarm is raised. The destination will remain prohibited as long as the circular routing flag is set. After network operations personnel correct the routing data, they can manually allow the route by using the `rst-dstn` command, which clears the circular routing flag. The flag is also cleared at node restart.

Changing the routing data using the `chg-rte`, `ent-rte`, or `dlt-rte` command does not clear the flag for circular routing (except for deleting all routes to a destination, then re-entering the routes).



The EAGLE checks for circular routing on a linkset basis. That is, a test may be run on linkset A while another test is run on linkset B. But only one test will be run at a time for linkset A. Also, only one test will be run per destination. If a destination uses linkset A and linkset B as combined linksets, and linkset A is testing the destination, linkset B will not start another test for the destination.

The EAGLE also checks for circular routing on C linksets.

Prevention of Link Oscillation - ANSI

When signaling links oscillate in and out of service, the EAGLE and the link's adjacent node will generate frequent changeovers and changebacks and excessive network management messages. To prevent this from happening, the EAGLE will implement a procedure to prevent link oscillation. GR-82 CORE specifies that one of two procedures should be used to control link oscillation. The EAGLE uses the preferred procedure.

- » When a LIM card first attempts to align a failed link, the LIM card will start a T32 timer. If the link fails before the timer expires, the LIM card will not attempt to align the link again until the timer expires. Once the timer expires, the LIM card will again attempt to align the link.
- » T32 is only started after a link fails, not when a link is manually deactivated.

MTP Restart - ANSI/ITU

MTP restart procedures enable an STP that is restarting to bring a sufficient number of signaling links into the available state and to update its routing tables before user signaling traffic is restarted. ANSI and ITU MTP restart procedure can be provisioned to be enabled or disabled on a per-STP basis. MTP restart capability is administered on a per linkset basis. MTP procedures are also used by an STP when an adjacent node becomes accessible via a direct link set. MTP restart is a network management function and occurs at level 3 of the MTP.

MTP Restart is supported for both ANSI and ITU networks. In case of an X.25/ITU- ANSI gateway, the X.25 links are treated as though they are not equipped with the Restart capability. TRA messages received over an X.25 link are ignored.

If the MTP Restart procedure is enabled, the EAGLE will attempt to bring links up in the following order:

- » Links to the EAGLE that are equipped with MTP Restart capability
- » All other links

Procedures for Recovery from Processor Outages - ANSI/ITU

The EAGLE used to send SIPOS (Link Status Signal Units (LSSUs) with status of processor outage) to the adjacent signaling point, when a link is remotely or locally inhibited. The EAGLE also used to perform a sequence controlled changeover by sending a changeover order to the remote end. Sending a changeover order under these conditions results in the remote node taking the link out of service.


The EAGLE now performs a time-controlled changeover instead of a sequence-controlled changeover when the signaling link gets locally or remotely inhibited, or when a local or remote processor outage condition is entered under these conditions.

Using this capability, the Oracle Communications EAGLE behaves in the following manner:

- » When the signaling link is inhibited locally or remotely, the EAGLE does not send SIPOs. Instead, a time diversion changeover procedure is started for the inhibited signaling link.
- » When the signaling link is unavailable because of a remote or local processor outage, a time-controlled changeover is performed instead of a sequence-controlled changeover.

This feature applies to both ANSI and ITU signaling links.

Cluster Routing and Management Diversity - ANSI



When an STP is switching traffic to remote (non-adjacent) nodes, it is possible that an STP is using the same route set for multiple destinations. Cluster routing allows the STP to provision one route set to an entire cluster of destinations. This is possible when a number of non-adjacent destinations, which share the same routeset, can be converted to a cluster entry with a single cluster route set. Cluster routing allows the STP to switch traffic to more destinations while minimizing network management traffic in the event of network failures. The EAGLE' capability of managing clusters will significantly increase its capability to manage and switch traffic to more end nodes. Also note that the EAGLE supports nested clusters and network routing. See *Advanced MTP Routing Functions* for more detail.

SCCP Routing in Response to MTP Congestion - ANSI

The EAGLE provides an option to route traffic to a backup node/subsystem when the primary node/subsystem is congested.

Without this option to reroute, additional messages would continue to be funneled to the congested node/subsystem contributing to the congested state and hampering message load recovery.

Prevention of SCCP Circular Routes

Auto Point Code Recovery

Circular Route Detection is intended to identify destinations affected by Direct or Indirect Routing Loopbacks. However, it can be invoked due to a Far End Loopback that causes congestion, thus marking point codes as permanently prohibited (until user intervention) when the network automatically detected and corrected the event (physical loopback) that caused the circular routing. Manual intervention is required by the network operator to reset the prohibited destination. This causes the affected destinations to be out-of-service for longer than necessary, and the operator incurs additional expense for investigation of the problem.

The Auto Point Code Recovery feature enhances the ability of the EAGLE to handle circular routing that is caused by far-end loopback. The feature also automatically resets a destination point code (DPC) that has been marked as prohibited due to circular route detection (CRD). The EAGLE detects far-end loopback in a link through the signaling link test control (SLTC) procedure. The originating point code (OPC) sends a signaling link test message (SLTM) across a link to the STP and expects a signaling link test acknowledgement (SLTA) from the STP. If far-end loopback occurs in the connecting link, then the OPC receives the same SLTM instead of an SLTA. The OPC marks the link as failed as soon as it receives the SLTM.

The circular route caused by the loopback can cause multiple MSUs to be returned to the OPC, which can increase the congestion level on the link and invoke CRD processing. CRD marks the link as failed and marks the DPCs as CRD-prohibited. After a link has been marked, the link cannot be used until the DPC is cleared.

The Auto Point Code Recovery feature consists of two separate features. Each feature addresses an aspect of far - end loopback and CRD.

- » **Enhanced Far-End Loopback Detection:** The Enhanced Far-End Loopback Detection feature significantly decreases the time required to take a link out of service by failing a link as quickly as possible when an SLTM is received. The rapid failure prevents the EAGLE from marking DPCs as CRD-prohibited.
- » **Circular Route Auto-Recovery:** The Circular Route Auto-Recovery feature automatically clears CRD when far-end loopback is detected, and the failing link is part of the linkset that detected the circular route. If the Circular Route Auto-Recovery feature is not enabled, the user must clear CRD manually by a user command.

ITU does not support Circular Route Detection; Circular Route Auto-Recovery will only apply to ANSI Point Codes

SCCP Loop Detection (ANSI/ITU)

The implementation of OMAP and XU DT as a network wide-solution to SCCP looping issues can cost operators many millions of dollars to implement. The SCCP Loop Detection feature, which is applicable for ANSI and ITU networks, allows operators to detect SCCP Looping and prevent link outages due to this type of condition as well providing an alternative solution to the NRC's (Network Reliability Council) requirement of network-wide implementation of the hop counter in XU DTs messages. This alternative will give operators a more cost-effective solution to this problem.

The SCCP Loop Detection feature allows the EAGLE to detect SCCP looping of UDT/XU DT and U DTs/ XU DTs messages for all concerned signaling transfer points (STPs). An STP sends GTT messages to the capability point codes (CPCs) of mated nodes for loadsharing; however, SCCP looping can result if the destination point code (DPC) is the same as either the originating point code (OPC) or the point code of any intermediate in the network. The CPC cannot be omitted because it is used in other functionality. The SCCP Loop Detection feature allows a correlation to be made between true/secondary point codes and CPCs for all concerned STPs. This correlation allows the EAGLE to compare the OPC of an incoming MSU to the post-GTT DPC to determine the possibility of looping.

A Loopset table is provisioned to define the correlation between the true/secondary point codes and the CPCs.

The SCCP Loop Detection feature operates in the Notify and Discard modes. In the Notify (default) mode, the SCCP Loop Detection feature generates a UIM when it detects SCCP looping and does not discard the MSU. This UIM allows the user to capture and verify MSUs throughout the system for SCCP looping. In the Discard mode, the SCCP Loop Detection feature generates the same UIM when it detects SCCP looping and discards the MSU.

Prevention of Trunk Looping Caused by ISUP

This feature is not applicable for the EAGLE.

8-Bit SLS Support - ANSI

The SLS (signaling link selection) is a field in the routing label of the MSU. It is set by the originator of the MSU to a random value. It is used by the EAGLE to pick which outgoing linkset and signaling link to use. MSUs with the same destination and the same SLS take the same path through the network, which guarantees arrival at the destination in sequence.

The value of the SLS is used by the EAGLE to distribute traffic over the available signaling links in a linkset. The EAGLE uses an 8-bit SLS code, which provides the EAGLE with 256 SLS codes, of which 128 SLS codes are used for signaling link selection. The additional SLS codes allow traffic to be distributed more evenly.


Because some signaling points may still be generating messages with a 5-bit SLS, the EAGLE provides an option to convert 5-bit SLSs in messages to 8-bit SLSs. This option is set on an outgoing linkset basis.

ITU messages continue to use 4 bit SLSs. Messages that go from ITU to ANSI are converted from a 4 bit SLS to a 5-bit SLS. If the outgoing linkset uses 5- to 8-bit conversion, the ITU messages are converted to 8-bit SLSs. If the linkset does not use 5- to 8-bit conversion, the ITU messages are converted from 4-bit to 5-bit SLS.

MSUs generated by the EAGLE (MTP management, SCCP management, LNP query response and messages received from X.25) have an 8-bit SLS.

Improved Signaling Link Test (SLT) Procedures - ANSI

The SLT verifies link assignments and can detect looped links and other link irregularities. This test was enhanced to lessen the probability of test failure during link processing delays or congestion. Under current procedures, if the



SLT is initiated and not acknowledged before time out, the link is taken out of service. The new procedure initiates a second SLT (same test pattern as the first) in an effort to retain the service of the link in the event the first SLT was merely delayed due to congestion.

This capability applies only to ANSI links.

Backup Procedures Against Loss of TFR/TCR - ANSI

TFR/TCR messages may be lost or not processed at a node because of signaling link failure, congestion, or other error conditions. Because of lost or unprocessed messages, other nodes continue to send traffic over a restricted route and results in C-link congestion. To help prevent this problem, after the first TFR/TCR is sent in response to the error condition, the level 3 timer T18 is started. If the error condition is still present when the level 3 timer T18 expires, the EAGLE sends a second, backup TFR/TCR once per linkset in response to messages received after the first TFR/TCR.

This feature applies only to ANSI signaling links.

MTP User Flow Control - ANSI

When a route set is unavailable or a change occurs in the congestion status of a route set, the EAGLE takes flow control actions as described in section 11.2 of ANSI T1.111.4.

Optional TFP Broadcast across Network Boundaries - ANSI

The EAGLE allows a user to disable the broadcast of TFP/TCP/TFA/TCA messages per affected cluster to preserve STP resources in broadcasting. For each cluster destination provisioned, the user can set Broadcast Exception Indicator (BEI) to 'yes' or 'no'. When BEI is set to 'yes', broadcast of messages regarding the cluster and its members are disabled.

ADVANCED MTP CAPABILITIES

The EAGLE provides a rich suite of advanced MTP capabilities for both ANSI and ITU networks:

- » Advanced MTP Routing (ANSI/ITU)
- » Multiple Point Code (ANSI/ITU)
- » ITU-N Duplicate Point Code (ITU)
- » ITU-SLS Enhancements (ITU)
- » Random SLS Generation (ITU)
- » Proxy Point Code (ANSI/ ITU)
- » Multiple Linksets to Single Adjacent Point Code

The 10,000 Routesets feature allows up to 10,000 routesets or destinations to be provisioned on the EAGLE. The maximum number of supported aliases and exception list entries are also increased to 10,000, each.

An additional 500 entries continue to be supported for dynamically created exception list entries. These entries are available only if the Cluster Routing feature is turned on.

Advanced MTP Routing Functions

The EAGLE contains these functions to enhance its basic routing functions. Least Cost Routing - ANSI/ITU:

The Least Cost Routing function allows the assignment of a weighting factor to a route. The weighting factor is used by MTP routing to determine the primary route (available route with the lowest cost), and the alternate routes. By using this feature, multiple routes may be assigned to one destination, with a primary route selected for all routing unless congestion or some other condition should be encountered, at which point the next most preferred route would be chosen.

Each routeset (combination of routes) may be assigned six routes, with each route assigned a different cost factor. The range for cost factors is 0 to 99, with 99 being the least favorable route (highest cost).

Combined linksets may be assigned the same cost factor, allowing equal loadsharing over the two linksets.

Cluster Routing, Nested Cluster Routing, and Network Routing – ANSI:

The Cluster Routing, Nested Cluster Routing, and Network Routing capabilities allow for more generalized routing capabilities thus reducing the number of route table entries for a given number of destinations. Cluster Routing allows routing by network cluster (10-10-*). Nested Cluster Routing allows cluster routing with full point codes provisioned on a separate route. Network routing allows routing by network indicator (10-*-*).

Full point code entries, cluster entries, and network entries can be provisioned for members of the same network. Any overlaps in the routing strategies are handled by a specific searching hierarchy.

For example, all of these route-table entries can coexist:

1. 10-10-10 full point code entry
2. 10-10-* cluster entry
3. 10-*-* network entry

The searching hierarchy will try to match against a full point code entry first followed by a cluster entry and finally by a network entry. In the example, when the EAGLE routes an MSU destined for 10-10-10, it would use the full point code entry. When the EAGLE routes an MSU destined for 10-10-2, it would use the cluster entry. When the EAGLE routes an MSU destined for 10-11-2, it would use the network entry.

» Cluster Routing - ANSI

The cluster routing capability contains 2 separate cluster routing functions - cluster and nested cluster routing.

Cluster routing eliminates the need for a full point code entry in the routing table to route to every signaling point in every network. Cluster routing allows the EAGLE to configure one route set to an entire cluster of destinations.

This function also allows the EAGLE to manage and switch traffic to more end nodes. Cluster routing allows provisioning of clusters as well as full point codes that belong to the same cluster as destination point codes. The point codes 10-10-* and 10-10-10 entries can be provisioned as long as they are on the same route with the same cost.

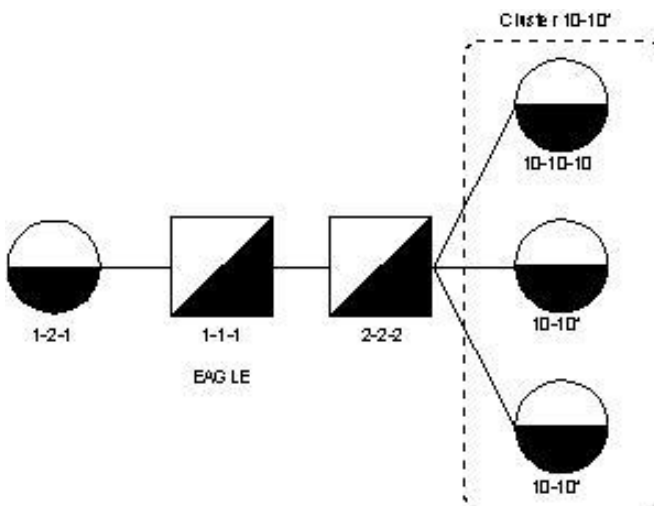


Figure 10: Cluster Routing

Restrictions for cluster routing

- » A full point code route within a cluster route must be on the same route as the cluster route with the same cost.
- » Cluster entries can be provisioned only as ANSI destination point codes.

The ANSI alias point code for an ITU international or ITU national destination point code must be a full point code. Measurements for messages that are received on a cluster route are pegged to that cluster route entry, but not by full point code.

» Exception List (X-Lists)

An exception list for a cluster is a list of point codes in a cluster whose routes are more restricted than other routes to that cluster. The term “more restricted” is used when comparing the route status of a cluster member to the route status of the cluster. A PROHIBITED status is more restrictive than a RESTRICTED status, and a RESTRICTED status is more restrictive than an ALLOWED status. This list contains point codes that are not assigned to any individual routeset and are the only routeset to that node. The exception list is a dynamic list that changes when the status of the cluster routesets changes.

The EAGLE allows users to specify whether exception list entries need to be created on a per-cluster basis. An exception list exclusion indicator can be specified for each cluster. If the exception list exclusion indicator is specified, the EAGLE does not maintain exception list entries. If it is not specified, the EAGLE maintains exception list entries for the cluster.

The Exception List entry capacity is configurable by the customer from 500 minimum (default) to 2000 xlist entries. Note that adding additional xlist entries beyond 500 will reduce the number of available routes.

Compatibility with Non-Cluster-Routing STPs

If some STPs in the network in which the EAGLE is operating are not cluster-routing STPs, those STPs not doing cluster routing will interpret TCx messages and apply them to each individual point code belonging to the concerned cluster. This may cause an inconsistency in the status records for exception listed point codes in different STPs. To avoid this situation, the EAGLE takes the following steps:

- » After broadcasting a TCR message for a cluster, the EAGLE stops any level 3 T8 timers running for exception-listed members of the cluster to enable TFPs for the cluster’s exception-listed (prohibited) member point codes. This allows TFPs to be sent for prohibited members immediately after a TCR is broadcast.
- » After broadcasting a TCA message for a cluster, the EAGLE enables a one-time TFR for the cluster’s exception-listed (restricted) member point codes by stopping the level 3 T18 timer, and enables the TFPs for the cluster’s exception listed (prohibited) member point codes by stopping the level 3 T8 timer. This allows TFPs to be sent for prohibited members and TFRs for restricted members immediately after a TCA is broadcast.

» Nested Cluster Routing

Nested Cluster Routing removes the restriction of having the full point code route on the same route as the cluster route. The EAGLE supports up to 500 nested cluster entries.

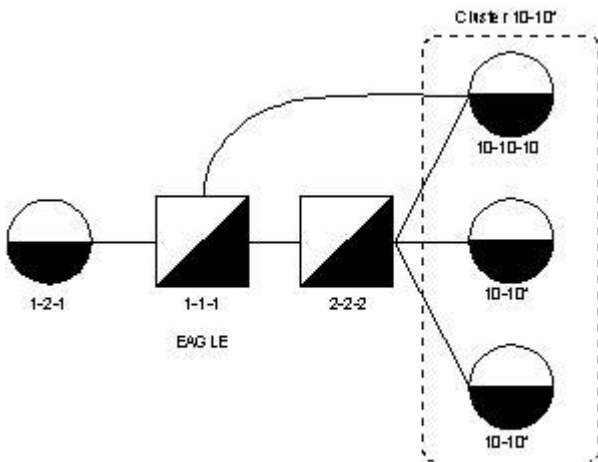


Figure 11: Nested Cluster Routing

Restrictions:

- » A maximum of 500 Nested Clusters entries (regardless of the number of full point code routes within the cluster) are supported per node.
 - » Nested Cluster entries can be provisioned only as ANSI destination point codes.
 - » The ANSI alias point code for an ITU international or ITU national destination point code must be a full point code.
 - » If a cluster is more restricted than a member, the EAGLE will broadcast the status of the least restricted member and rely on the response method for members of the cluster that do not have a full point code entry.
 - » The EAGLE will not broadcast preventive TCPs for nested cluster destinations. Because the EAGLE will not send preventive TCPs when it begins routing towards a nested cluster, circular routing can occur. The EAGLE will send response method TFPs if it receives an MSU when there is danger of circular routing.
 - » Measurements for messages that are received on a cluster route are pegged to that cluster route entry, not by full point code.
- » Network Routing-ANSI

Network routing is a higher level of routing than cluster routing and allows the user to provision a single routeset that will be used for all MSUs destined to members of a network. The advantages of network routing are:

- » Further reduces the number of entries in the route table
- » Allows routing to members of a network without having to add those members to the route table

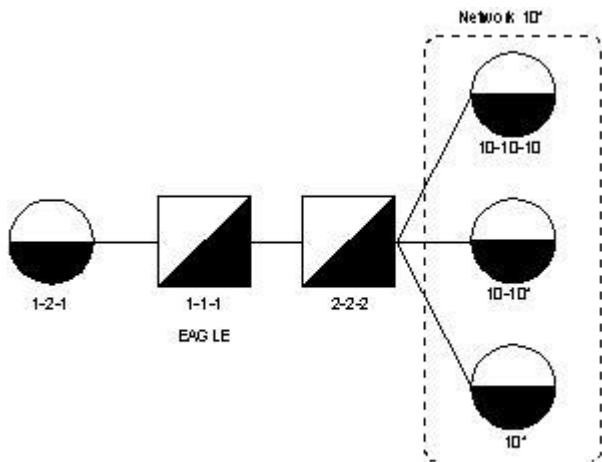


Figure 12: Network Routing

An EAGLE user can connect to a remote network by provisioning a single route table element. As the remote network grows, the EAGLE user would not have to add new route table entries for each new point code in the remote network.

Restrictions:

- » Limited network management functionality is provided with network routing. The EAGLE will not broadcast TFP/TCP messages for network routes but will pace response method TFP/TCP messages to avoid network management overload.
- » Measurements for messages that are received on a network route are pegged to that network route entry, not by cluster or full point code.

Origin-based MTP Routing

The Origin-based MTP Routing feature allows greater flexibility and control over EAGLE SS7 message routing. This feature allows selective routing of messages based on a combination of the MTP origination and destination information in the message. Standard EAGLE MTP routing is based only on the MTP destination information.

Standard MTP routing in the EAGLE uses a combination of the SLS, DPC, and Network Indicator fields in the MTP layer to determine the next routing destination for the message. Origin-based MTP Routing makes use of the SLS, DPC, OPC, SI, and Network Indicator fields in the MTP layer to determine the next routing destination for the message. Origin-based MTP Routing allows greater flexibility over routing of messages, based on both Origination and Destination information.

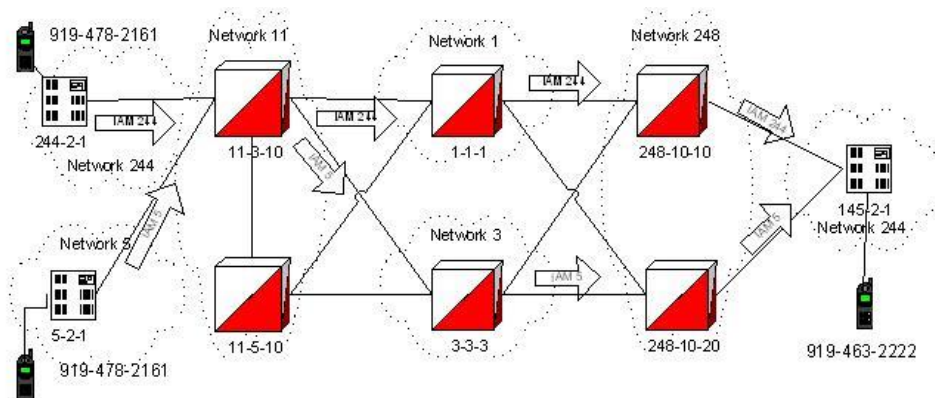


Figure 13: Origin-based MTP Usage Example

The EAGLE with point code 11-3-10 in Network 11 has the Origin-based MTP Routing feature active. Caller (919-478-2161) originates a call from network 244 (MSU 244) via MSC 244-2-1. This MSU has a final destination (DPC) of 145-2-1, where the called subscriber resides. Network 244 has a routing agreement with Network 11, and has requested a preferred route via Network 1 for messages from its network. Thus, IAM 244 is sent via STP 1-1-1 in Network 1.

Later, the caller 919-478-2161 flies to another location that is served by Network 5 instead of Network 244. Again, caller 919-478-2161 originates a call to 919-463-2222. Now the IAM message originates at MSC 5-2-1 instead of MSC 244-2-1. Network 5 also has an agreement with Network 11, but has requested routing via Network 3 for messages from its network. Thus, STP 11-3-10 routes the IAM message through STP 3-3-3 in Network 3.

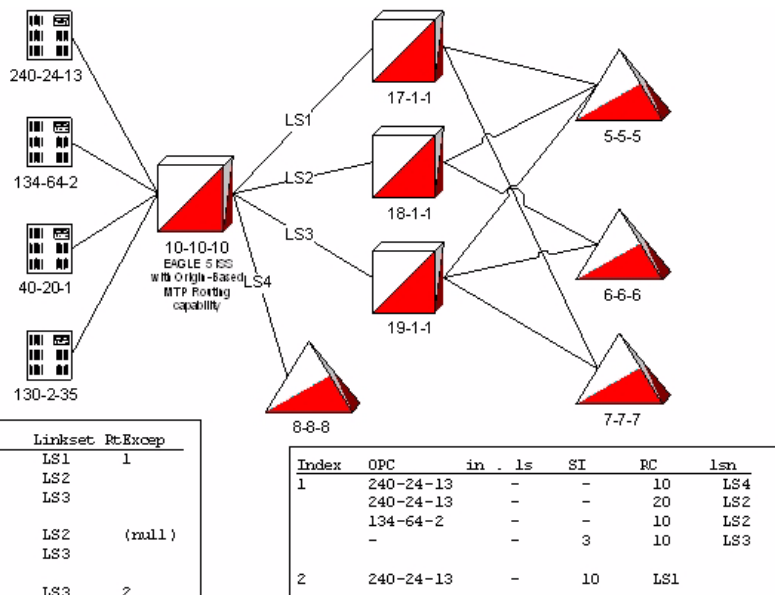
Both message are destined for 145-2-1, but can be sent via different routes based on the originating network.

With Origin-based MTP Routing, the following routing options are available:

- » DPC + OPC (most preferred)
- » DPC + Incoming Linkset
- » DPC + CIC (valid for ISUP messages only)
- » DPC + SI
- » DPC (least preferred)

The EAGLE will always use the most preferred route type, as long as that route is available. Route cost is used to choose amongst routes of the same type. Therefore, a DPC + OPC route with route cost of 20 will be chosen ahead of a DPC + SI route with the route cost of 10, and a DPC + OPC route with a cost of 10 will be chosen over a DPC + OPC route with a cost of 20.

Network management events (TFPs, TFAs, and TFRs) are still driven by the DPC-only routes. The new route types are considered exception routes and do not factor into the availability status of a destination. If all of a destination's DPC-only routes become unavailable, the destination is considered unreachable by the EAGLE, even if an exception route to that specific destination is still capable of carrying traffic.



Routing Table
(a new pointer field (RtExcep) that points to set of routing exceptions applicable to this destination)

Exception Routes Table
This table contains additional qualifiers for MTP route selection .
Additional optional qualifiers will include OPC from MTP Routing Label, incoming linkset , or SI from MTP Routing Label

Figure 14: Origin-based MTP Routing Route Selection Example

In the figure above, STP 10-10-10 has 3 DPC-only routes for end node DPC 5-5-5: LS1, LS2, and LS3, in that order of preference. 5-5-5 also has a set of exception routes. Exception routes (if available) are preferred over standard DPC-only routes, as described below:

- » OPC=240-24-13: LS4 will be the most preferred route, followed by LS2. If neither of those routes are available, the system will use LS3 (all SCCP (SI=3) messages without matching OPC), and then LS1 (DPC-only route) for all other messages.

Note: LS4 is not one of DPC 5-5-5's original route-set. Also, LS4 will deliver the message to an end node with PC of 8-8-8, rather than to a transit node with connection to 5-5-5. This can be useful for re-direction application, etc. The 8-8-8 end node needs to be able to process a received message with a DPC different than its own in this case.

- » OPC=134-64-2: LS2 will be the most preferred route, followed by LS3 for all SCCP (SI=3) messages without matching OPC. LS1 will be the least preferred option
- » OPC=40-20-1 and 130-2-35: LS3 will be the most preferred route for all SCCP (SI=3) messages, as there are no matching OPCs, followed by LS1 for non-SI=3 messages.

DPC 6-6-6 is configured with 2 DPC-only routes, LS2 and LS3, and does not have any exception routes.

DPC 7-7-7 is configured with 2 DPC-only routes, LS3 and LS1. DPC 7-7-7 has 1 exception route for OPC 240-24-13, which prefers LS1 over LS3. Messages from all other OPCs will follow the DPC-only routes.

Multiple Point Code - ANSI/ITU

The Multiple Point Code (MPC) feature allows expanded capability for routing in both domestic and international networks.

MPC Description

Some North American customers desire to collapse multiple existing STPs into one EAGLE. Without the Multiple Point Code feature, collapsing multiple STPs into one STP can present problems because end offices and other nodes may not be controlled by the carrier, therefore making reprovisioning of these network elements difficult. MPC support is designed to allow the EAGLE to assume more than one point code for SS7 routing. MPC support is different in concept from capability point codes in that MTP functions will use secondary point codes as if they were the actual point code of the EAGLE.

International customers may want to deploy a single STP pair in multiple national (ITU-N) networks. This deployment may not be possible without the MPC feature because these operators are often forced to use a unique point code assigned by each national regulator of these target countries. For example, in the network shown in the figure below, both Country 1 and Country 2 need to route to the EAGLE using different ITU-N point codes. The Multiple Point Code feature allows the EAGLE to assume both point codes and allow proper routing for Country 1 and Country 2.

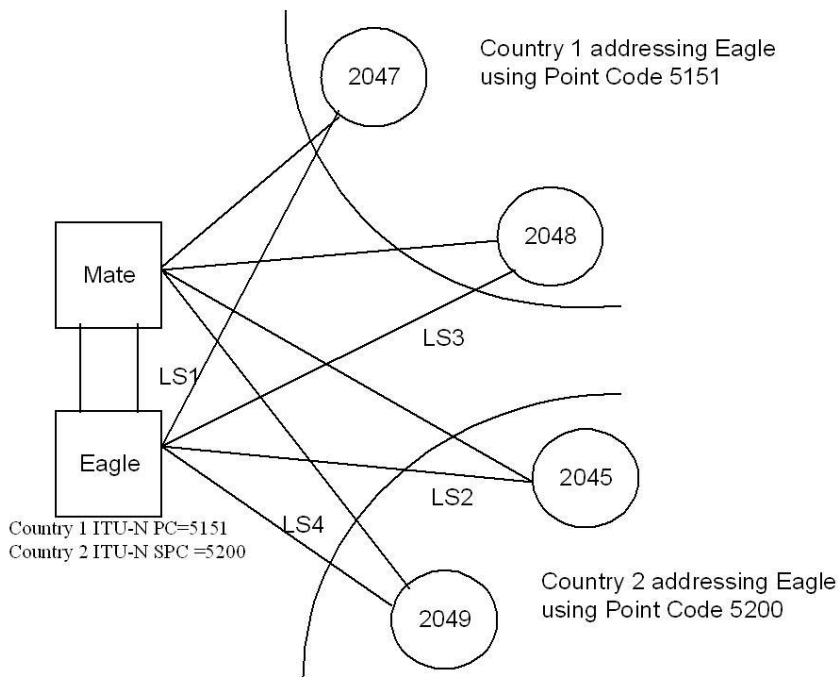


Figure 15: Typical International Deployment of MPC Feature

Both North American and international customers may need additional links between two nodes beyond the number of links permitted by the protocol. For example, the maximum number of links between two nodes in an ITU network is 16. The Multiple Point Code feature can allow for additional linksets between these nodes, increasing the number of links that can be used.

The EAGLE supports three True Point Codes (TPCs), one for each of the ANSI, ITU-National, and ITU-International network type domains. The EAGLE also supports 40 Secondary Point Codes (SPCs). The 40 SPCs can be assigned as either ANSI, ITU-I, or ITU-N in any combination. For each destination that uses an SPC, the user must specify which SPC type is used.

With the Multiple Point Code feature, customers can configure multiple linksets between two nodes if the adjacent node also supports Multiple Point Codes. The EAGLE continues to enforce the rule that each linkset must have a different adjacent point code.

MPC Limitations

The Multiple Point Code feature has the following limitations:

- » The same adjacent point code cannot be used for two different linksets.
- » Local EAGLE subsystems (e.g., LNP) must use the True Point Code.

ITU-N Duplicate Point Code

The ITU-N Duplicate Point Code (ITUDUPPC) feature allows the EAGLE to be placed in multiple ITU-N networks of the same type when there is the same national point code used in two or more of these networks. This feature requires the Multiple Point Code (MPC) feature to be on.

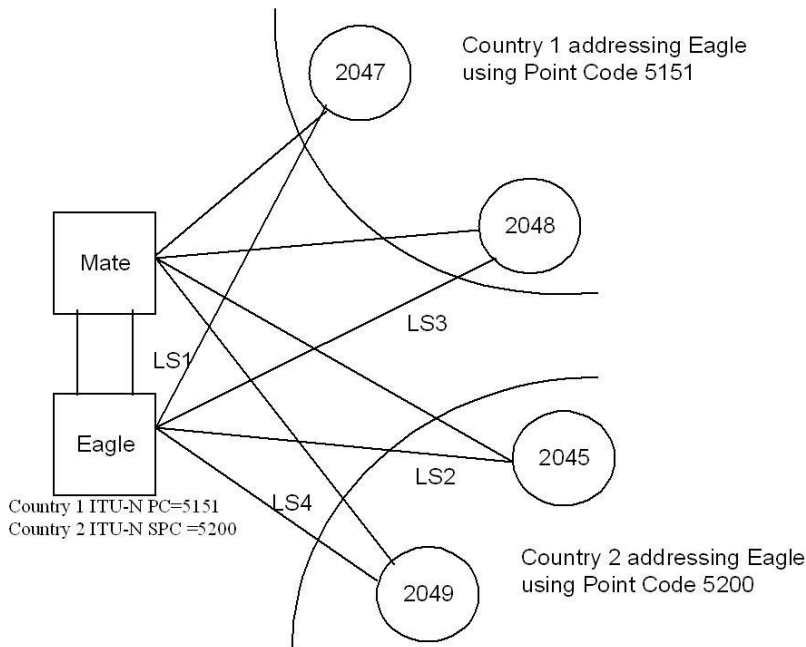


Figure 16: Typical International Deployment of ITU-N Duplicate Point Code Feature

The ITU-N Duplicate Point Code feature allows an EAGLE mated pair to route traffic for two or more countries that may have overlapping point code values. For example, in the network shown above, both Country 1 and Country 2 have SSPs with a point code value of 2047. The ITU-N Duplicate Point Code feature allows the EAGLE to properly route to both of these nodes by using groups.

The user must divide their ITU-National destinations into groups. These groups would likely be based on country. However, one group could include multiple countries, or a single country could be divided into multiple groups.

The ITU-N Duplicate Point Code feature has the following limitations:

- » No duplicate point codes are allowed within a group
- » ITU-National traffic from a group must be destined for a PC within the same group.

- » The user must assign a unique two-letter group code to each group. For example, in the network shown above, Country 1 can have only one point code with a value of 2047. Traffic coming from SSP 2047 in Country 1 can be destined only to other nodes within Country 1. In this example, the user assigns a group code of AA to Country 1 and a group code of BB to Country 2.
- » When an EAGLE pair is deployed in multiple national networks, one C-linkset per national network may be required between the EAGLE pair.
- » When an EAGLE is deployed in multiple national networks and using the ANSI/ITU Gateway feature, each ANSI or ITU-I node can only send and receive messages from one ITU-N group. Also, the ITU-N alias of the sending node must have the same group code as the destination group code.
- » If the ITU-N Duplicate Point Code feature is used to deploy an EAGLE in two or more networks, then those networks cannot have overlapping (duplicate) GTT entries because the EAGLE has only a single set of GTT tables.

ITU-I/ITU-N Spare Point Code Support

The EAGLE ITU International/National Spare Point Code feature allows a network operator to use the same Point Codes across two networks (either ITU-I or ITU-N). The feature also enables National and National Spare traffic to be routed over the same linkset.

The EAGLE uses the MSU Network Indicator (NI) to differentiate the same point code of one network from the other. In accordance with the SS7 standard, unique Network Indicator (NI) values are defined for Point Code types ITU-I, ITU-N, ITU-I Spare, and ITU-N Spare:

- » ITU-International NI=00
- » ITU International Spare NI=01
- » ITU-National NI=10
- » ITU National Spare NI=11

ITU SLS Enhancements

The ITU SLS Enhancements feature provides the ability to modify the method the EAGLE distributes traffic across ITU SS7 links.

The EAGLE uses the LSB of the SLS to load-share between linksets of a combined linkset. ITU-T ISUP messages use an SLS that is obtained from the lower 4 bits of the CIC field representing the circuit being used. Refer to the figure below for an ITU-T routing label with CIC.

16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	Bit Location
DPC																Routing Label word 1
SLS (CIC)				OPC												Routing Label word 2
Spare				"Other" CIC bits (bits 5-16)												ISUP CIC (cont.)

Figure 17: ITU-T ISUP Routing Label with CIC

CIC selection can be determined based on an odd/even method where an SSP uses either all odd CICs, or all even CICs, to help prevent "glaring" (e.g., 2 SSPs attempting to seize the same trunk at the same time). This causes the LSB of the SLS to be fixed; if the LSB is fixed, inadequate loadsharing occurs for the SS7 network. This situation can also occur within a single linkset (international), since the EAGLE also uses the SLS (containing a fixed LSB) to select a link within a linkset.

ITU SLS Enhancements provide the user two options for addressing the problem:

- » Bit Rotation - The customer can have the EAGLE rotate the 4 bits of the SLS, thus changing the least significant bit (LSB) of the SLS. If selected, this option is applied to all ITU messages.

1) Customer has selected bit 2 as the "Rotated LSB"

2) Received CIC contains the following bits, with SLS = 1001:

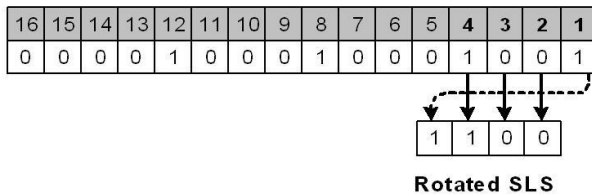


Figure 18: Example of Bit Rotation

» Use of Other CIC Bit - The customer can have the EAGLE derive the SLS from bits 2 to 4 of the CIC to serve as the three lower bits of SLS, and one other bit of the CIC to serve as the most significant bit (MSB) of the SLS. If selected, this option is only applied to ITU ISUP messages.

1) Customer has selected bit 9 as the "other CIC bit"

2) Received CIC contains the following bits:

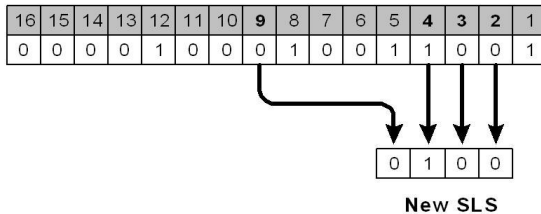


Figure 19: SLS Creation Using Other CIC Bit

Only the link selection algorithm is modified by this feature, not the actual SLS field of the message (i.e., the SLS value received by the EAGLE is the SLS value sent by the EAGLE).

» Combining "Bit Rotation" and "Use of Other CIC Bit"

Both the Bit Rotation option and the Other CIC Bit option can be applied to provide an even distribution of ITU-ISUP messages sent by the EAGLE. If the customer has activated the options for a given linkset, the SLS field will be processed in the following order:

1. The SLS is modified using the Other CIC Bit option.
2. The modified SLS is modified again using the Bit Rotation option.
3. The modified SLS is used by the existing linkset and link selection algorithms to select a link.
4. The ISUP message is sent out the link containing the original, unmodified SLS field.

» ITU SLS Enhancement Limitations

ITU SLS Enhancements have the following limitations:

- » When two linksets are used as a combined linkset, they should have the same Other CIC Bit and Bit Rotation settings. This is not enforced in the EAGLE, and there is no warning mechanism for incorrectly provisioned linksets and routes.
- » Bit Rotation functionality is not compatible with the Random SLS Generation feature.

Random SLS Generation

The Random SLS Generation feature allows operators to overcome some of the ITU protocol limitations by ignoring the SLS value in the incoming SS7 message when selecting an outgoing link for the message. Overcoming the limitations is accomplished by generating a new 8-bit SLS value that is used internally by the EAGLE to randomly select an outgoing link to the destination. Without this feature, ITU customers can experience link load-balancing problems attributable to several factors. The ITU protocol uses a 4-bit Signaling Link Selection (SLS) field with no modification of SLS values by intermediate nodes, and a one-to-one mapping of SLS values to signaling links. These rules can be overly restrictive in situations where they are not necessary. The Random SLS Generation feature addresses some of these shortcomings.

The Random SLS Generation feature does not alter the SLS value in the outgoing message; it is the SLS value received in the message. The newly-generated SLS is used for link selection only.

In any situation where a link is failed, SLS values that were mapped to that link will be remapped to other links of the linkset or combined linkset. Remapping will be done in the reverse order that the SLS values were originally mapped to links, of course skipping the failed link. Subsequent link failures will have their SLS values, along with SLS values from the prior failure(s), remapped in the same way. The odd/even mapping rule for combined linksets will not apply to the remapped SLS values under failure conditions. This is to continue to achieve the best possible load balance across all links. No MSUs should be discarded in any case.

Oracle recommends that the Random SLS Generation feature be performed at a single site and monitored before being rolled out to an entire network. Any negative effects of the feature can be rolled back by simply disabling the feature at the node with a single command

The figure below shows a combined linkset from node A to nodes B and C, with 8 links per linkset. Since 8 bits allows for values 0 - 255 (decimal), the figure shows how these values will get internally mapped to the links of the combined linkset. For ease of reading, not all values are shown. Similarly, Figure 21: Random SLS Generation in a Single Linkset shows the mapping for a 4-link single linkset between nodes D and E.

In a non-failure condition, the process for mapping the internally generated SLS values to SLC (Signaling Link Code) values for specific links is as follows:

- » A "random" 8-bit SLS value is "generated". In reality, a single table of 256 unique SLS values, initially generated in random order, exists in the system. A counter is maintained for each linkset in the system that will cause the linkset to cycle through the random values in the table as messages are routed out that linkset. For a combined linkset (CLS), the counter for the first linkset in the Random SLS Generation feature linkset table will be used.
- » For a CLS, the first bit is used to select the LS and then is ignored when selecting the SLC. For a single LS, the first bit is used when selecting the SLC. In all cases, the fifth bit is ignored when selecting the SLC. This is due to internal ANSI-based processing in the EAGLE.

» The adjusted SLS value (with fifth and possibly also first bits ignored) is then divided by the number of links in the LS (not CLS) and the remainder gives the SLC value. For example, in the figure below the SLS value 78 is mapped to SLC 7 in LS 1 as follows:

1. 78 decimal = 01001110 binary
2. the fifth bit is ignored leaving 0101110
3. the least significant bit is used to select LS1 and is then ignored, leaving 010111
4. $010111 (= 23) \text{ MOD } 8$ leaves a remainder of 7, hence $\text{SLC} = 7$

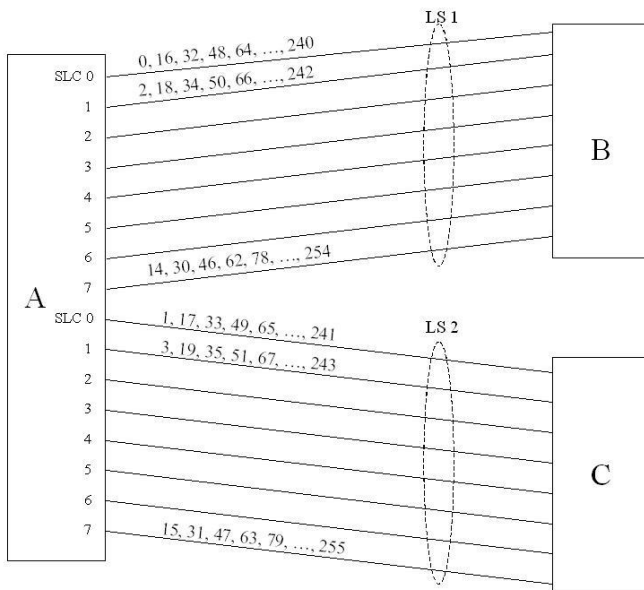


Figure 20: Random SLS Generation in a Combined Link

In another example, in the figure below, the SLS value 78 is mapped to SLC 2 in LS1 (the only linkset) as follows:

1. 78 decimal = 01001110 binary
2. the fifth bit is ignored leaving 0101110
3. $0101110 (= 46) \text{ MOD } 4$ leaves a remainder of 2, hence $\text{SLC} = 2$

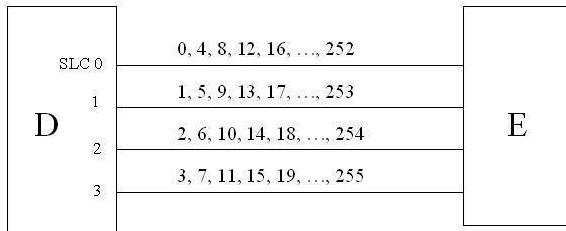


Figure 21: Random SLS Generation in a Single Linkset

Random SLS Generation Limitations

The Random SLS Generation feature is compatible with the Other CIC Bit portion of the ITU SLS Enhancements feature but is not compatible with the Bit Rotation SLS Bit portion.

Per-Linkset Random SLS

The Per-Linkset Random SLS (Signaling Link Selection) feature is an enhancement of the existing Random SLS Generation feature, to allow an operator to apply Random SLS generation on selected linksets instead of system-wide to all linksets. The Per Linkset Random SLS feature provides an STP option that can help to resolve load balancing problems on specific linksets without affecting the entire routing scheme of the EAGLE.

Linkset provisioning is enhanced to allow configuration of specific linksets for Random SLS generation. The Per Linkset Random SLS feature can operate on both ITU SCCP Class 0 and Class 1 traffic or only ITU SCCP Class 0 traffic for a specific linkset. Oracle recommends when provisioning two linksets that are in a combined linkset that the Random SLS values are the same for both linksets to avoid undesirable SLS distribution of traffic.

SLS Bit Rotation on Incoming Linkset

The ITU SLS Bit Rotation feature described previously solves many problems related to inadequate distribution of SLS values from other network nodes. However, there are cases for which the current solution does not solve the issue. Consider the example (assuming 4 SLS bits).

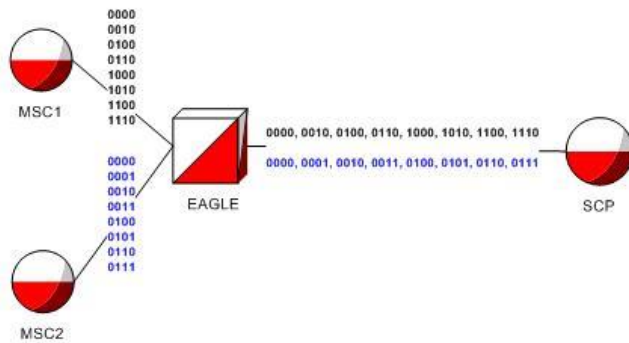


Figure 22: Bit Rotation Example

In the example above, MSC1 is sending 8 SLS values, all even (i.e. 0,2,4,6,8,10,12,14), and MSC2 is sending 8 SLS values, sequentially from 0-7 (i.e. 0,1,2,3,4,5,6,7). The linkset to the SCP from the EAGLE contains 8 links. Without any additional processing at the EAGLE, the SLS distribution for messages going to the SCP would appear as shown in the SLS Bit Rotation Example.

SLS	Outgoing SLS Usage Factor
0	2
1	1
2	2
3	1
4	2
5	1
6	2
7	1
8	1
9	0
10	1
11	0
12	1
13	0
14	1
15	0

Figure 23: SLS Bit Rotation Example

As seen in the figure, some SLS values for the outgoing traffic distribution will be over-utilized by a factor of 2, while others are not used at all. This will result in uneven traffic distribution on the outgoing linkset.

If the existing SLS Bit Rotation feature were used to try and remedy this scenario, it would not give optimum results because the SLS rotation is based upon the SLSBR setting provisioned against the outgoing linkset, and thus all traffic which is to be routed out of that linkset will have the same bit rotation applied, regardless of where the traffic originated from. This would result in an SLS distribution as shown in the following figure.

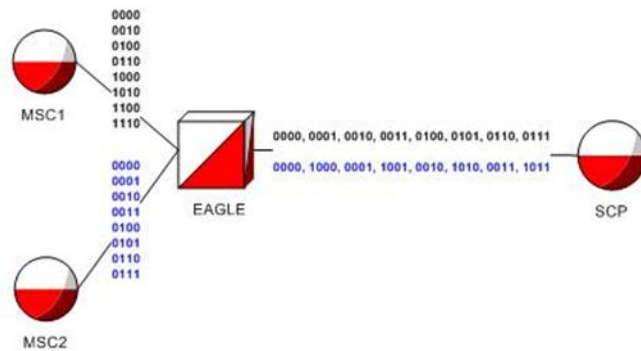


Figure 24: Example with Standard Bit Rotation Applied

As can be seen, this still results in several SLS values being over-utilized in comparison to other values, and hence, uneven traffic distribution on the links within the linkset.

The SLS Bit Rotation on Incoming Linkset feature provides an alternative solution by allowing the bit rotation to be applied only on the incoming linkset. Thus, when traffic is being routed from multiple sources to the same destination, the SLS values from one source can be rotated while SLS values from another source are left intact. Applying this principle to the previous example results in the SLS distribution shown below.

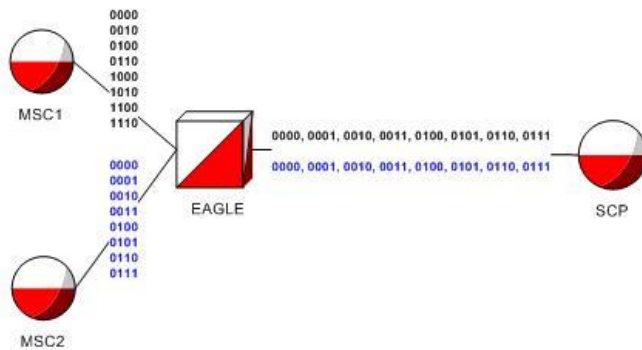



Figure 25: Example Applying SLS Bit Rotation on Incoming Linkset

As seen in this example, bit rotation is only applied to the messages arriving on the linkset from MSC1, while rotation is not applied to message arriving on the linkset from MSC2. The result is a perfectly even distribution of SLS values on the outgoing linkset, result in even traffic distribution across all links within the linkset.

The SLS Bit Rotation on Incoming Linkset feature provides support for both ANSI and ITU protocols (something the standard Bit Rotation feature does not).

The SIS Bit Rotation on Incoming Linkset feature and the standard Bit Rotation feature may co-exist on the same node. In fact, it is possible to provision incoming and outgoing bit rotation on both sides of a MSU's path. However, if this occurs, the EAGLE will only apply incoming bit rotation. If EAGLE applies bit rotation to an MSU on the incoming side, it will ignore any outgoing bit rotation setting on the linkset which is transmitting that MSU. Other MSUs being transmitted out of that linkset that did not receive rotation on the incoming linkset will continue to be rotated.



As with the standard Bit Rotation feature, the EAGLE only uses the modified SLS value for routing decisions. The original SLS in the message is not modified, and is transmitted just as it was received.

SLS Bit Rotation using 8 bits for ANSI links

The SLS Bit Rotation on Incoming Linkset feature has been enhanced to allow the rotation algorithm to support 5 or 8 bits for ANSI links. The value supported by the algorithm is based on the incoming linkset. ITU links continue to support 4 links. The Least Significant Bit (LSB) for rotation can have a value of 1 - 8.

Miscellaneous Protocol Features

Preventive Cyclic Retransmission (PCR)

PCR and basic error correction are the two forms of error correction for the SS7 protocol. PCR is a forward error correction scheme that uses positive acknowledgments to support the forward error correction. Negative acknowledgments are not used for retransmission. PCR is used when the one-way delay on a link is greater than or equal to 15 milliseconds. A typical use of PCR is a satellite link.

Manual Deactivation of SRST Message

When a destination for a route becomes restricted or prohibited, the EAGLE starts sending signaling route set test (SRST) messages for that destination. This capability allows a user to manually stop sending signaling route set test messages for a specific destination on a specific route. The destination of the route must be either the DPC of the route, a cluster point code of a route, or an entry on the cluster routing exception list.

Priority Processing of Network Management Messages - ANSI

During normal operation, the network management functions are processed with equal priority, but the EAGLE closely monitors for excessive unexpected events, which may result in a network management processor overload. The prioritization of network management functions is triggered when the network management processor overload is experienced. The EAGLE provides the capability to prioritize the network management functions to make sure that critical network management functions receive high processing priority under such overload conditions.

This feature is applicable only for the ANSI network. Network Management events triggered due to change in status of ITU network elements (links, routes, linksets, destination) are processed on a first come first serve basis.

Setting the Frequency of RST Messages on Low Priority Routes


The EAGLE allows the configuring of a timer to specify the frequency of SRST messages for routes of lower priority than the current route.

Linkset Restricted Support

The Linkset Restricted Support feature introduces route selection algorithm that reduces the potential for congestion by diverting traffic from lower routes with insufficient capacity to higher cost routes with the needed capacity.

Every destination provisioned in the EAGLE is allowed up to six independent routes in its routeset. Each route is a path to a destination over a single linkset. Routing has always selected the least cost Available route, regardless if that route is Allowed or Restricted. This routing path algorithm can increase the likelihood of congestion because Restricted routes (due to number of available links) of lower cost are always preferred to Allowed routes of a higher cost.

The Linkset Restricted Support feature will provide an optional alternative routing algorithm that is more tolerant during linkset transitions and will reduce the likelihood of experiencing congestion on linksets that do not have a sufficient quantity of available links to carry normal traffic loads. Routes are considered Allowed or Restricted based



on the number of available links compared to the number of provisioned links. Route selection algorithm chooses the least cost Allowed route, which may or may not be the least cost Available route. If there is no Allowed route, then the route selection algorithm chooses the least cost Restricted route.

Proxy Point Code

The introduction of an EAGLE into a home network and the replacement of direct connect links into a foreign network, a method must be available for seamless migration. Currently, if the home network migrates links from direct connect to the EAGLE, the foreign network must change the adjacent point code from the original node to the EAGLE self point code. In many cases, the foreign network is resistant to change, and this may impact the rollout of the EAGLE.

The Proxy Point Code (PPC) feature allows the EAGLE to assume the point codes of adjacent nodes to ease the migration of deploying an STP for SS7 links interconnect in a network. For example, if a foreign-network SS7 node is directly connected to an SS7 node in the home network, an EAGLE can be deployed, in a transparent way to the foreign network, which would still behave as if it was directly connected to the end node. The EAGLE would route the SS7 messages coming from this foreign-network SS7 node into the home network based on destination PC.

The proxy point code is used as the originating point code for all EAGLE generated messages that are routed to the adjacent node of the linkset (referred to as the proxy linkset). The proxy point code can be reached by all nodes in the home network and can access all STP routing functionality in the foreign network. The EAGLE routes SS7 messages coming from the foreign-network SS7 node into the home network based on the destination point code. The EAGLE can support up to 100 point codes that can be designated as proxy point codes. The proxy point code must be a full point code and can be any of the following network types; ANSI, ITU-N, ITU-I, ITU-N Spare, ITU-I Spare and ITU-N24.

The PPC feature supports three configurations;

1. Adjacent point code and proxy point code.
2. Many adjacent point codes and many proxy point codes
3. Multiple adjacent point codes and single proxy point code

The PPC feature has the following limitations:

- » Only 'A' link types are supported on a linkset using a proxy point code.
- » Secondary adjacent point codes are not supported on a proxy linkset.
- » M3UA links and SUA links are excluded for proxy point codes.
- » If the routeset from the EAGLE to the proxy node is prohibited, then all links in any proxy linkset using the proxy point code are unavailable for traffic.
- » If more than 50% of the links in the linkset are down, then congestion may occur.
- » Only one linkset to an adjacent point code is supported by the EAGLE unless the Multiple Linksets to Single Adjacent PC feature is used.
- » Configurations where the same proxy point code is a member of both the foreign and home networks are not supported.
- » Global title translation (GTT) to a proxy node is not supported.

Multiple Linksets to Single Adjacent Point Code

The EAGLE existing Multiple Point Code (MPC) feature (see Multiple Point Code - ANSI/ITU) allows multiple linksets to be established between an EAGLE and an adjacent node. This is typically needed in situations where a single 16-link E1/T1 TDM SS7 linkset does not provide enough bandwidth to carry the traffic involved, and where

high speed link options (i.e., E1/T1 ATM HSL, SE-HSL or SIGTRAN IP links) are not feasible or not supported by the adjacent node

The use of the MPC feature for this purpose carries the limitation that both the EAGLE and the adjacent node must support multiple-point-code functionality because linksets are typically defined solely based on the adjacent point code. Therefore, no more than one linkset can be established between the EAGLE and an adjacent node that does not support multiple point codes; the EAGLE would have no way to distinguish between the two linksets for routing and network management purposes. Even if multiple point codes are used on the EAGLE, the two linksets would carry the exact same internal definition because they are defined by adjacent point codes only.

The Multiple Linksets to Single Adjacent PC (MLS) feature is intended to solve this problem and allow multiple linksets to be established between the EAGLE and an adjacent node, even if that node supports only a single self point code.

In the example shown below, the EAGLE still uses multiple self point codes and associates a self point code to each of the linksets going to SSP2. However, SSP2 is now required to support only a single self point code. Thus, LS1, LS2, and LS3 are connected between one EAGLE and one destination point code. 2-2-2 is still the TPC for the EAGLE; 3-3-3 and 4-4-4 are still SPCs.

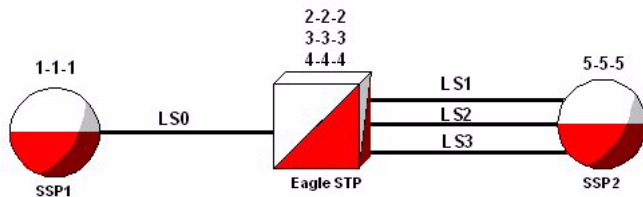


Figure 26: Multiple Linksets to Single Adjacent Point Codes

The MLS feature has the following limitations:

- » The MLS feature does not support multiple IPGW linksets to the same adjacent point code.
- » The EAGLE allows up to 6 routes to be established to a single destination in the routing tables. However, the EAGLE currently allows loadsharing on only 2 of these 6 routes.

Network Indicator Mapping

In some network routing scenarios, it is desirable to make MTP-level routing decisions based on the linkset on which the message is received. The Network Indicator Mapping feature is intended to provide a method for achieving this. The NI Mapping feature provides a mechanism to temporarily map the NI from an incoming message to a different value for use by the EAGLE's message processing algorithms.

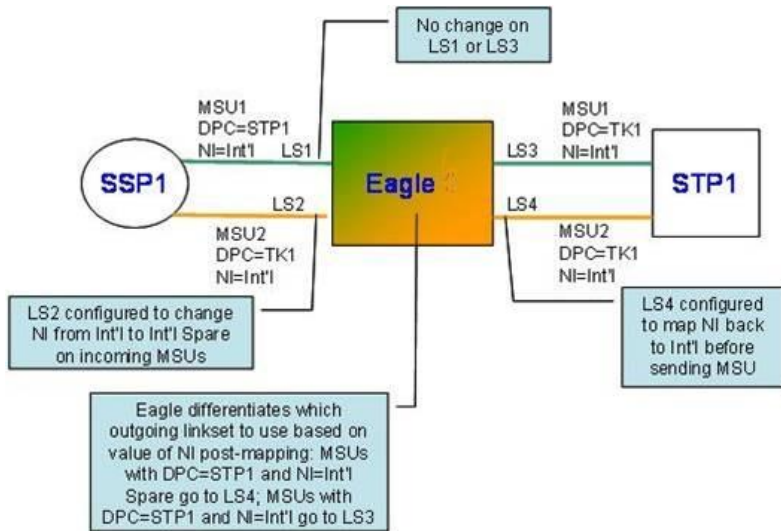


Figure 27: Network Indicator Mapping Example

As shown in the figure, LS2 uses the NI Mapping feature and is configured such that the NI of incoming MSUs is mapped from International to International Spare, while LS1 does not use the NI Mapping feature. Thus, in this example, EAGLE will internally see two types of MSUs from SSP1 destined for STP1: MSUs routed to STP1 with NI=International and MSUs routed to STP1 with NI=International Spare. Based on the different NI, the EAGLE can choose a different outgoing linkset toward STP1.

NOTE: In order to satisfy the use case noted in the figure above, both the NI Mapping feature and the Multiple Linksets to Single Adjacent Point Code (MLS) feature are required. However, MLS is NOT a prerequisite for the NI Mapping feature in general - i.e. NI Mapping can be used on a single linkset going to an APC, without requiring MLS.

The incoming NI Mapping value and the outgoing NI Mapping value are independently configured and are not correlated. The customer must insure through provisioning that the values are compatible, or as desired. e.g. it would be possible via provisioning to set NI mapping on an incoming linkset such that a particular MSU has NI changed from ITU-I >> ITU-IS. The logical setting for the outgoing linkset that will carry this MSU would be ITU-IS >> ITU-I. However, if the user forgets to set NI Mapping on the outgoing linkset, or intentionally sets it to ITU-I >> ITU-IS for example, the modified MSU would be routed with NI=ITU-IS, rather than ITU-I. This is similar to how the TT Mapping feature operates in the EAGLE today.


Point Code and CIC Translation

The Point Code and CIC Translation (PCT) feature allows the EAGLE to change the destination point code (DPC) and originating point code (OPC) of an MTP-routed MSU to previously configured values. This functionality allows external networks to continue using the old point codes by emulating and mapping them to the new real point codes within the networks. The feature can also be used to change the circuit identifier code (CIC) for the MSU.

Note: ITUN24 point codes, spare point codes, and private point codes are not supported by PCTtranslations.

A new PCT table is used to define translations between real and emulated point codes.

Network nodes can send and receive traffic to and from the emulated point code (EPC) without 'knowing' the real point code (Real PC) that is being emulated by the EPC. This ability allows the Real PC to be changed transparently from the rest of the network, which can continue using the EPC to route traffic.



For each incoming MTP-routed MSU, a DPC lookup and an OPC lookup are performed. If a translation is found during the DPC lookup, then the DPC of the MSU is replaced by the Real PC as the MSU is received by the EAGLE. If a Real CIC was provisioned in the translation, then the CIC of the MSU is changed to the value from the Real CIC range.

If a translation is found during the OPC lookup, then the OPC of the MSU is replaced by the EPC as the MSU leaves the EAGLE. If an Emulated CIC was provisioned in the translation, then the CIC of the MSU is changed to the value from the Emulated CIC range

Features and functionalities in the EAGLE use the real point code in provisioning.

The PCT feature is a quantity feature. The quantity is used to define the maximum number of allowed translations.

GATEWAY SCREENING - ANSI/ITU

General

Gateway Screening is used at gateway STPs to limit access into the network to authorized users. A gateway STP performs inter-network routing and gateway screening functions. The Gateway Screening feature (GWS) is provided on the EAGLE to control access to non-home SS7 networks. The feature includes both inbound and outbound message screening. The EAGLE implementation of gateway screening adheres to the requirements stated in GR-82-CORE.

The EAGLE current implementation of gateway screening supports this process on as many as 255 linksets, and each linkset can be allowed one of 1024 screen sets. Each screen set can contain up to 8000 entries (rules). There are no translation table limits or interdependencies among these screening tables. To support rapid access and download following a processor restart, all GWS tables are also stored on at least two dedicated GLS (Generic Loading Service) cards.

GWS Functionality

Gateway screening provides two levels of screening:

- » MTP screening
- » SCCP screening

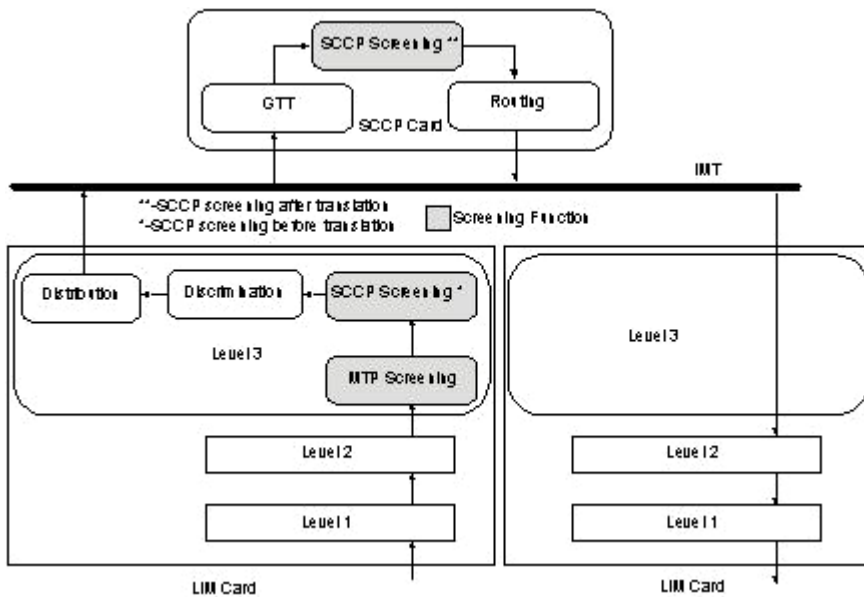


Figure 28: GWS Functional Diagram

MTP screening allows the user to screen based on the following:

- » Allowed OPC (OPC)
- » Blocked OPC (BLKOPC)
- » Allowed SIO (SIO)
- » Allowed ISUP Message Type (ISUP)
- » Allowed TUP Message Type (TUP)
- » Allowed DPC (DPC)
- » Blocked DPC (BLKDPC)
- » Allowed priority values per SI value
- » Allowed HO-HI fields (SI=0,1,2)
- » Affected Destination Field for Network Management.

SCCP screening allows the user to screen based on the following:

- » Allowed Calling Party Address (CgPA)
- » Allowed Translation Type (TT)1
- » Allowed Called Party Address (CdPA)2.
- » Affected Point Code and Subsystem (AFTPC)

Screening functions are defined through the use of gateway screening administration commands. Administration of gateway screening tables is via the standard EAGLE interface or SNAM.

A screening table contains the screening rules. The size of these tables may vary from table to table depending on the number of screening rules defined in the screening table. Each rule within a screening table consists of a pattern followed by the next screen to reference as indicated by the next screening reference identifier if a match occurs.

A screen set is formed by linking together a group of screening tables. These screen sets are then applied to the linksets. The incoming SS7 messages are then screened against the rules in the tables. A screen set is associated with a linkset.

For example, a condition in an OPC Allowed table may point to a subsequent condition in a DPC Allowed table. Each screening table contains a unique list of conditions for a particular non-home signaling network. Once constructed and entered into system memory, a table may be reused by other screen sets. All screening tables are user administrable.

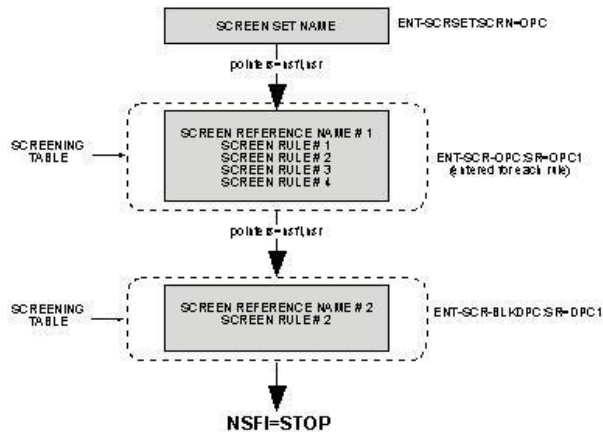


Figure 29: GWS Provisioning Structure

Gateway Screening on a particular linkset can be set to function in one of four states:

- » NO SCREENING – Screening is not performed. All message signaling units (MSUs) are passed.
- » SCREEN AND REPORT – Screening is performed. When an MSU fails screening, it is discarded, an output message is generated, and measurements are pegged.
- » SCREEN AND DON'T REPORT – Screening is performed. When an MSU fails screening, it is discarded and measurements are pegged, but no output message is generated.
- » SCREEN TEST MODE – Screening is performed but all MSUs are passed. When an MSU fails screening, an output message is generated, but the MSU is still passed.

For easy access and review, the EAGLE screening databases may be retrieved for display or printout at the user interface via another simple set of commands. Screening verification is accomplished on the Oracle Communications EAGLE through a test mode command that automatically produces printouts of all incoming messages that will be screened before the screening option is activated.

Eleven screening tables are defined for EAGLE Gateway Screening data. Depending on the values present in the selected field of the SS7 message, different messages may undergo different screening checks. To reduce the size and number of screening tables, each rule can represent a range of point codes by means of “wild card” character fields.

Allowed OPC

Allowed OPC screens are used to screen all SS7 messages transported on an incoming linkset configured for gateway screening containing the specified originating point code (OPC).

Allowed DPC

Allowed DPC screens are used to screen all SS7 messages transported on an incoming linkset configured for gateway screening containing the specified destination point code (DPC).

Allowed SIO

The allowed SIO screen set is used to screen all SS7 messages transported on an incoming linkset from another network for allowed combinations of service indicator, network indicator, and message priority.

The allowed SIO screen allows for different next screening values depending on the value of the service indicator (si) parameter.

Allowed ISUP Message Type

Allowed ISUP Message Type screens are used to screen all ISUP messages transported on an incoming linkset configured for gateway screening containing the specified ISUP message type.

Allowed TUP Message Type

Allowed TUP Message Type screens are used to screen all TUP messages transported on an incoming linkset configured for gateway screening containing the specified TUP message type.

Blocked OPC

Blocked OPC screening can be used in place of, or along with allowed OPC screening. This method of screening allows blocking a small number of point codes, rather than entering a large number of individual point codes in an allowed OPC screen set.

Blocked DPC

Blocked DPC screening can be used in place of, or along with allowed DPC screening. This method of screening allows blocking a small number of point codes, rather than entering in a large number of individual point codes in an allowed OPC screen set.

Allowed SCCP Called/Calling Party Addresses (PC/SSN)

The message type of the message being screened for the SCCP message format ID must be either a UDT, UDTS, XUUDT or XUUDTS message. All other message types are passed.

Screens can be created to allow specific called or calling party addresses (PC/SSN) within an SCCP message. Ranges can also be specified. This provides screening of messages destined to SCPs in the host network, or adjacent networks.

The allowed calling party address (CgPA) screen can screen messages for these SCCP message types: UDT, UDTS, XUUDT, and XUUDTS.

The allowed CgPA screen allows for different next screening values depending on the value of the CdPA routing indicator (ri) parameter.

The allowed called party address (CdPA) screen can screen messages for the SCMG format ID (SCCP Management Format ID).

The wildcard value for the subsystem parameter (ssn=*) indicates the range of values from 2 to 255. The SCMG format ID does not apply because messages with a subsystem of 2 to 255 are not SCCP management messages.

If the value of the ssn parameter is not a wildcard (1 - 255), the NSFI for the Allowed CdPA screen can be either the allowed affected point code screen (aftpc) or stop.

4.4.11 Allowed Translation Type

Translation type screening provides screening of the translation type field in the called party address of SCCP messages. MSUs requiring global title translation are passed without screening.

Allowed SCMG Affected Point Code

Affected point code screening applies to subsystem prohibited (SSP), subsystem allowed (SSA), and subsystem test (SST) SCMG messages. All other SCMG messages are passed. Both the point code and the subsystem number are checked by the screen.

Allowed Affected Destination Field Screen

The Allowed Affected Destination field contains the affected destination point code of incoming MTP network management messages. This is also referred to as the concerned signaling point code.

Other methods of screening the affected point code in network management messages involve a check for the point code in the routing table, self point codes, and capability point codes. This check is applied after the MSU has passed all other screening tables.

Screening by the Allowed Affected Destination field allows the network management message to be screened with gateway screening screen sets. Using the Allowed Affected Destination field screening table instead of the routing table makes it possible to reject messages containing point codes in the routing table. This keeps interconnecting networks from either accidentally or maliciously sending a network management message for a destination in the home network.

Provisioning Ranges for Gateway Screening

The values for certain parameters used to configure gateway screening can be entered as a range of values. Allowing a range of values for these parameters reduces the number of entries in the gateway screening tables required to support a particular configuration. Ranges are supported for the following parameters:

- » si – the service indicator for the SIO screening reference
- » ni – the network identifier for an ANSI point code
- » nc – the network cluster for an ANSI point code
- » ncm – the network cluster member for an ANSI point code
- » pri – the message priority in the SIO field of an MSU
- » h0 – the H0 heading code in the SIF field of an MSU
- » h1 – the H1 heading code in the SIF field of an MSU
- » type – the translation type in the called party address field of an MSU

A range of values for these parameters can be specified for gateway screening commands entered on an EAGLE terminal or on the SNAM interface.


GWS Stop Action for MTP Routed Messages

The GWS Stop Action for MTP Routed Messages feature provides a new sccp Gateway Screening (GWS) stop action. This stop action allows IS41-based features to process MTP-routed traffic. GWS rules are used to filter MTP-routed SCCP messages on a per linkset basis. UDT, UDTS, XU DT, and XU DTS messages are then forwarded to Service Module cards for processing.

GWS Stop Action – De-encapsulate

The GWS Stop Action – De-encapsulate feature adds the capability to de-encapsulate a re-directed message from a remote EAGLE and provide all of the features and functionality to the encapsulated MSU as if the MSU were received without any SCCP encapsulation.

GWS Stop Action – Duplicate and Route



The GWS Stop Action – Duplicate and Route feature allows users to duplicate and forward ISUP messages selectively to another monitoring system where analysis can be performed to identify potential spam or robo-call scenarios. This feature provides the capability of selective forwarding of the MSUs to another network element.

NETWORK SECURITY ENHANCEMENTS

The Network Security Enhancements feature enhances the EAGLE network security by discarding messages that should not be received by the EAGLE. This feature is designed to allow maximum flexibility to the user, so that different network implementations can still use the applicable functionalities provided by this feature.

The Network Security Enhancements feature is controlled by feature activation and has four different STP command options to control activation of the three major aspects of this feature:

MTP message SID verification (Enhanced MTP Security)

1. Option #1: Mate SID verification - SECMTPMATE-EAGLE should not receive a message with the True, Secondary, or Capability Point Code of the Mate STP other than across the C link.
2. Option #2: Self SID verification - SECMTPSID-EAGLE should not receive a message with its own point code as the OPC except for circular route tests and SLTM's during maintenance.
3. Option #3: MTP Network management message OPC verification (Enhanced MTP Management Protection) - SECMTPSNM-EAGLE should not receive an MTP network management message unless:
 - Rule #1 - The OPC is an adjacent point code
 - Rule #2 - The EAGLE has a route to the OPC of the MTP network management message on the linkset which the message was received.
 - Rule #3 - The EAGLE has a route to the destination field in the message (if applicable to the concerned message) on the linkset which the message was received.

For all link types, the following additions or exceptions apply:

- » Rule #3 would not apply to RSM messages.
 - » Rule #1 would not apply to UPU, TFC and RCT messages.
4. Option #4: SCMG AFTPC verification (Enhanced SCCP Management Protection) - SECSCCPSCMG-EAGLE should not receive a SCCP network management message unless:
 - Rule #1 - The EAGLE has a route to the OPC of the SCMG message on the linkset, on which the message was received.
 - Rule #2 - The EAGLE has a route to the Affected Point Code in the message on the linkset on which the message was received.

The Affected Point Code (industry term) and the Concerned Signaling Point Code (EAGLE term) are synonymous. This option will only apply to SSP and SOR messages. This feature will not affect the following messages: SSA, SST, SOG, SBR, SNR and SRT.

The four STP options can be turned on or off independently. Network Security Enhancements capabilities are independent of Gateway Screening and are performed before Gateway Screening occurs on the MSU.

SS7 Firewall & Origin Based Routing Enhancements

Mobility by its nature relies on Service Providers ability to exchange information. This need to provide ubiquitous services creates opportunities for network abuse such as fraud, call interception and spam. The EAGLE 46.3 release extends the translation and filtering capabilities, enabling Service Providers to utilize parameters within the Operation Code (OPCODE) when defining policies. To receive the full benefit of the security enhancements offered in this release, the Origin Based Routing and SS7 Firewall features should be licensed along with any prerequisites. Release 46.3 adds the following new filters and capabilities:

Origin Based Routing

» OPCODE Parameter Filters

- IMSI
- MSISDN
- VLRNb
- SM RP OA
- SM RP DA

The existing FLOBR / TOBR Framework is enhanced to allow these additional 'MAP Components' to be used in the routing selection process.

» Validate MAP SCCP

- A new validate GTT action is added to mitigate the risk of SMS fraud by validating the parameters within the SCCP used for transport with the parameter within the MAP.

SS7 Firewall

The enhancements offered in this release provide a set of capabilities to log or throttle a message. This includes the following new capabilities:

» Logging

A new logging GTT action is added. An SCCP card is allowed to log up to 100 log events / second. The resulting benefits are that fraudulent MSUs can be identified and that messages are filtered properly.

» Egress Throttling

A new throttle GTT action is added to mitigate the risk of a denial of service attack. This allows the user to provision a maximum threshold of MSUs allowed to hit the GTT action during a 30 second period. If that maximum threshold is reached, then messages will be discarded.

GSM MAP SCREENING – ITU

General

The GSM MAP Screening feature allows an extension of the EAGLE message screening capabilities beyond the MTP and SCCP levels to the MAP level. Advanced network capabilities, proliferating roaming agreements, and the advent of mobile number portability are placing increasing demands on limited network resources such as Home Location Registers (HLRs). As a result, many GSM network operators have a need to screen messages at the MAP level to prevent unauthorized access to their resources.

GSM MAP Screening Process

The Any Time Interrogation (ATI) feature, defined in MAP Version 3, is an example of an enhanced capability driving the need for screening. ATI allows external entities to query the operator's HLR regarding a mobile subscriber's locations or state (idle or busy). MAP Screening enables operators to screen incoming messages based on the identity of the requestor, the destination queried, and the specific information requested.

GSM MAP Screening can be combined with other EAGLE-based features, such as Mobile Number Portability and HLR Router, to further address the GSM operator's specific needs. Refer to the following figure GSM-MAP Screening Process.

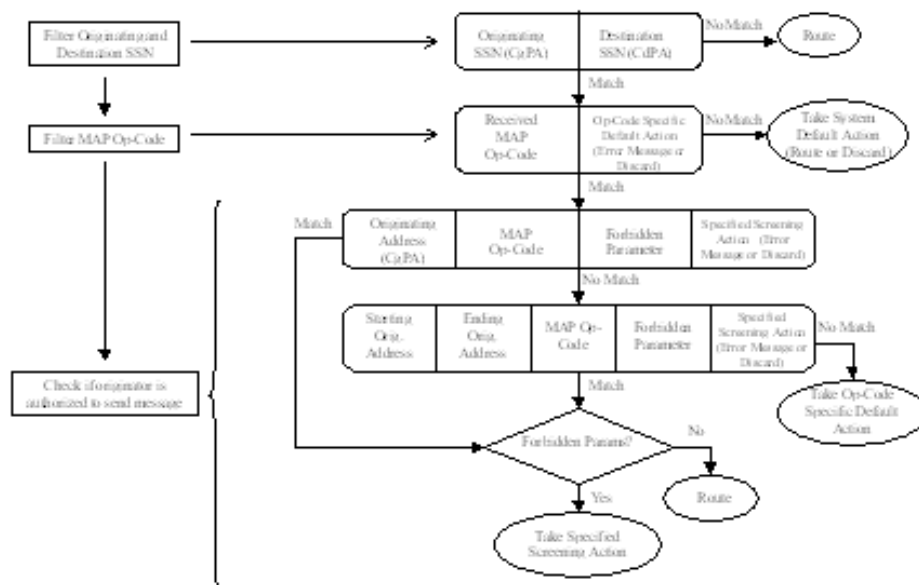


Figure 30: GSM-MAP Screening Process

When a message arrives at the EAGLE with a routing indicator of Route-on-GT, it is first subjected to Gateway Screening (GWS). If the message is not screened by GWS, GTT-based message relay services, such as GTT, MNP, or HLR Router, are performed. Lastly, if the GSM MAP Screening feature is turned on, the message will then be screened at the MAP level prior to routing.

The originating SSN is examined to determine if it is one of the target originating SSNs that require further screening. If the originating SSN is a target SSN, the destination SSN will be examined to determine if it is a target destination SSN. If either the originating SSN or the destination SSN is not target SSNs, the message will be immediately routed. The target originating and destination SSNs are provisioned by the user prior to putting the feature into service.

If both the originating and destination SSNs are found to be target SSNs, the MAP Opcode and its parameters are decoded from the TCAP portion of the message. The MAP Opcode is examined; if it is determined not to be a target Opcode as provisioned by the user, the message is either routed or discarded, depending upon the STP System Default Action for unknown Opcodes. This action is user-provisionable.

If the message contains an Opcode targeted for screening, the feature searches the MAP Screening database using the calling party (CgPA) and MAP Opcode. If a match is found, then the EAGLE will take the appropriate action based on the forbidden parameter value associated with this CgPA/Opcode combination. Possible values for forbidden parameter are Location, State, All, or None. If the message contains a parameter that has been defined as forbidden for a particular CgPA and MAP Opcode, then the message will either be discarded or returned with an error message, depending upon the Specified Screening Action provisioned by the user.

If a match is not found on a single entry CgPA, the CgPA range table will be searched. If a match is found for the CgPA range and the MAP Opcode, the appropriate action will be taken as described for a single entry match. If no match is found in the CgPA single entry or range tables, the message will either be discarded or returned with an error message, depending upon the Opcode Specific Default Action provisioned by the user. This may be different than the Specified Screening Action.

If an error is encountered while decoding the MAP/TCAP portion of the message, the EAGLE will either route or discard the message, depending upon the default action provisioned by the user.

GSM MAP Screening Duplicate/Forward

The GSM MAP Message Duplicate/Forward option extends the capabilities of GSM MAP Screening by allowing MAP messages to be routed, discarded, duplicated, or forwarded based on the provisioned screening criteria. This gives the EAGLE the ability to offload or copy certain types of MAP messages to an attached processor (such as an SCP) based on the MAP Opcode or Calling Party Address or both.

For these advanced services on MAP messages, targeting specific MAP messages based on SSN and MAP Opcode as shown below, allows for a finer granularity in message selection.

GSM MAP Screening Forward Function

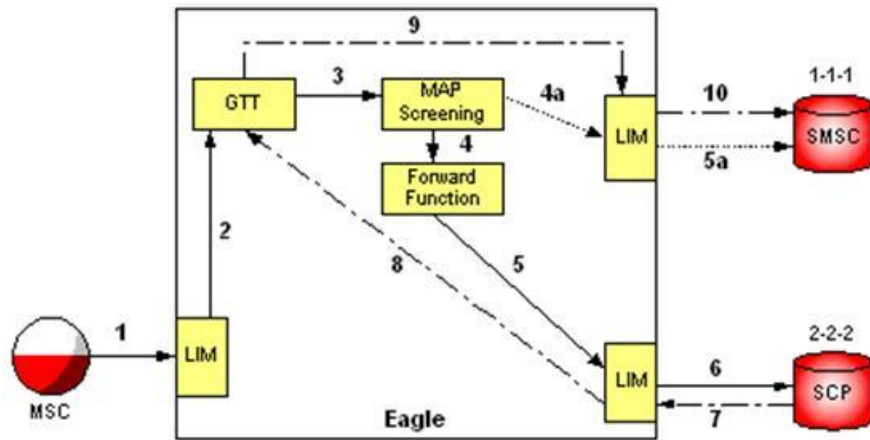


Figure 31: MAP Message Forward Example - SMS

Key:

-▶ Path normally taken by MSU not subject to MAP screening forward/duplicate
- ▶ Path taken by MSU subject to MAP screening on way to SCP 2-2-2
- - - - -▶ Path taken by MSU after processing at SCP and returned to Eagle for routing

Legend:

1. An MSU containing a MAP SMS message arrives at the EAGLE. The message is Route-on-GT with a CdPA GT corresponding to the SMSC. This linkset has the GSM MAP Screening option turned ON.
2. Since the message requires GTT, the LIM forwards it to the GTT function on the SCCP card.
3. GTT is performed and the resulting message contains a DPC of 1-1-1 in the routing label, corresponding to the SMSC. The CdPA GT is unaffected and is still present in the message. This represents the "normal" Global Title Translation for this GT.
4. GSM MAP Screening is performed and determines that the message should be forwarded to the SCP for further processing instead of being sent to the original destination.
If GSM MAP Screening determines that the message should not be forwarded, the message may be sent to a LIM for routing to the SMSC based on the results of GTT, and the provisioned default action.

- GSM MAP Screening determines the DPC and SSN for the SCP, provisioned in the MAP Opcode or GSM MAP Screening table. The message is modified by placing these values in the MTP and SCCP layers. The resulting message contains a DPC of 2-2-2 in the routing label and CdPA PC. A new CdPA SSN may also be in the message. The CdPA GT is unaffected and is still present in the message. The mated application table is consulted, and the message is sent to a LIM for routing to the SCP.

The non-forwarded message from 4a is routed directly to the SMSC, if the provisioned default action was ROUTE.

- The forwarded message from 5 is routed to the SCP.

Note: Steps 7, 8, 9 and 10 are for explanatory purposes only; they do not impose any new functionality on the EAGLE or the GSM MAP Screening function itself.

- The SCP may be the terminating node, or it may be performing some intermediate processing and needs to send the message on to the originally intended node. If so, it sets the routing indicator to Route-on-GT and returns the message (possibly modified) to the EAGLE. For this example, this linkset has the GSM MAP Screening option turned OFF, so after GTT, the message is simply routed to the SMSC without being screened again.
- The message is forwarded to an SCCP card for GTT. GTT is performed using the CdPA GT (which is still the GT of the SMSC).
- Since the GSM MAP Screening option is not turned on for linksets coming from the SCP, the message is sent directly to a LIM for routing to the SMSC.
- The message is delivered to the SMSC. Note the SCP may have modified this message.

Note: The SCP may route the message to a node other than the originally intended SMSC. In this case, the SCP is responsible for placing the new routing information (new GT or new DPC/SSN) in the routing label and sending the message back to the EAGLE.

GSM MAP Screening Duplicate Function

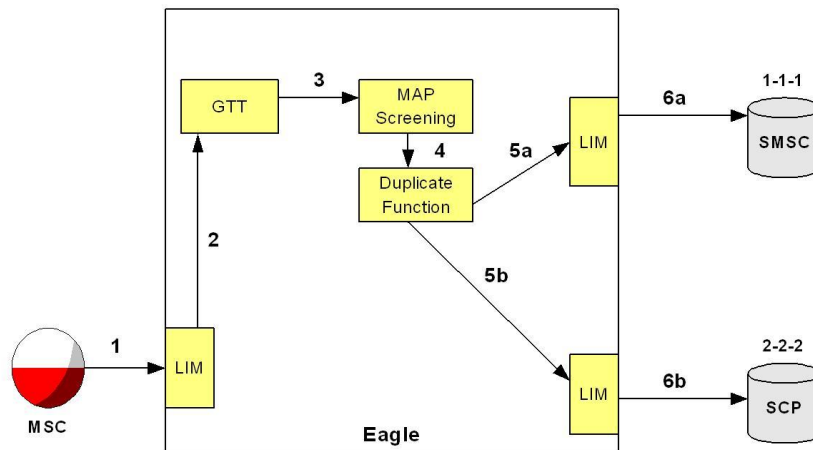


Figure 32: MAP Message Duplicate Example - SMS

- An MSU containing a MAP SMS message arrives at the EAGLE. The message is Route-on-GT with a CdPA GT corresponding to the SMSC. This linkset has the GSM MAP Screening option turned ON.
- Since the message requires GTT, the LIM forwards it to the GTT function on the SCCP card.
- GTT is performed and the resulting message contains a DPC of 1-1-1 in the routing label, corresponding to the SMSC. The CdPA GT is unaffected and is still present in the message. This represents the "normal" Global Title Translation for this GT.
- GSM MAP Screening is performed and determines that the message should be duplicated to the SCP for further processing.

5. a: A copy of the MSU is made. The original MSU is sent to a LIM for routing to the intended destination, based on the results of GTT.
b: GSM MAP Screening determines the DPC and SSN for the duplicate node, provisioned in the MAP Opcode or MAP Screening table. The copied MSU is modified to contain the PC/SSN of the SCP in the routing label (e.g., a DPC of 2-2-2 is now in the routing label). The mated application table is consulted, and the duplicate message is sent to a LIM for routing to the SCP.
6. a: The original MSU is sent to its intended destination (1-1-1).
b: The duplicated MSU is sent to the SCP (2-2-2).

GSM MAP Screening Limitations

GSM MAP Screening has the following limitations:

- » Overlapping range entries cannot be provisioned.
- » There is no cross-checking between the individual entry table and the range table when numbers are provisioned. The individual table entries are exceptions to the range table. So, if an individual number is provisioned that is already part of a range, automatic splitting of the range entry will not occur. This may or may not be considered a limitation.
- » Per-server measurements are not provided for range table entries, and no per-server measurement will be pegged when a match occurs in the range table.
- » This feature is applicable only for ITU implementations.
- » A given Global Title Address (GTA) may be entered in the GSM MAP Screening table only once.

ENHANCED GSM MAP SCREENING - ITU/ANSI

Introduction

The Enhanced GSM MAP Screening feature allows implementation and enforcement of many complex interconnect policies in real time and the flexibility in routing decisions based on combinations of the message origin and destination nodes.

Enhanced GSM MAP Screening builds on the existing functionality present in the GSM MAP Screening feature, which is detailed in GSM MAP Screening – ITU. The existing feature is retained for ITU GSM operators who only need screening on the combination of SCCP CgPA GTA digits and MAP Operation Code. The Enhanced feature is available for both ANSI and ITU GSM operators who need the ability to screen on the combination of SCCP CgPA GTA digits and NP/NAI, SCCP CdPA GTA digits and NP/NAI, and MAP Operation Code.

Enhanced GSM MAP Screening adds the following:

- » Allows implementation and enforcement of complex interconnect policies
- » Works in conjunction with GSM MAP Screening Forward and Duplicate actions to provide both message screening and routing decisions based on combinations of origination and destination nodes and type of message
- » Rules are defined based on combinations of SCCP Calling and Called Party Address Digits, NP/NAI, and MAP Operation Code
- » "Wild Carding" is allowed for all fields in a rule for complete flexibility
- » Actions include: Discard, Route, Forward, Duplicate, and Duplicate and Discard
- » Can perform advanced functionality such as origin-based routing, origin destination-based routing, or message type-based routing.
- » As of Release 39.2, the Forward and Duplicate actions allow network domain crossings - e.g. messages may be forwarded from ITU-N to ITU-I, etc.
- » Also as of Release 39.2, the Enhanced GSM MAP Screening feature provides support for non-segmented XUDT messages. Segmented XUDT continues to be unsupported.

Enhanced GSM MAP Screening Example

The figure below illustrates the enforcement of an interconnect policy between three mobile operators. This scenario is just one example of what can be accomplished using Enhanced GSM MAP Screening.

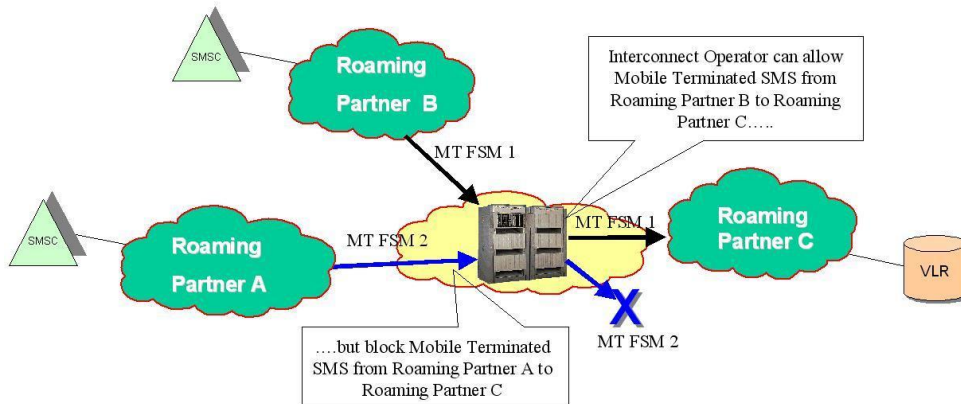


Figure 33: Enhanced GSM MAP Screening Example

The EAGLE with Enhanced GSM MAP Screening is serving as the policy enforcement node. By configuring the blocked/allowed rules in Enhanced GSM MAP Screening, the EAGLE can be configured to allow Roaming Partner B to send Mobile Terminated SMS messages to Roaming Partner C, but to block the same messages to Roaming Partner C if they come from Roaming Partner A. With standard GSM MAP Screening, it is only possible to block a message based on the originating network, regardless of the terminating network.

This example also shows that the existing Forward action of MAP Screening can be combined with the extended rule set of Enhanced MAP Screening to perform tasks such as sending messages to different destinations depending upon the CgPA GTA, CdPA GTA, and MAP Operation Code. This is in contrast to simple GTT, which only factors the CdPA GTA into the routing decision.

Enhanced GSM MAP Screening Limitations

Enhanced GSM MAP Screening is applicable for both ITU and ANSI implementations. Otherwise it carries the same limitations as standard GSM MAP Screening; see GSM MAP Screening Limitations.

SCCP-GLOBAL TITLE TRANSLATIONS (GTT) - ANSI/ITU

General

The SCCP Global Title Translations (GTT) feature uses the signaling connection control part (SCCP) to translate addresses (Global Titles) from signaling messages that do not contain explicit information allowing the message transfer part (MTP) to route the message.

Basic Global Title Translation Functionality

- » Basic global title translation functionality provides the following:
- » 270,000 to 1,000,000 GTT entries
- » 65,536 to 200,000 GTT per Translation Type (TT)
- » 1,024 to 3000 Mated Applications
- » 96 Capability Point Codes
- » SCCP Class 0 and 1 connectionless services
- » Online administration of Global Title data

- » Traffic reporting capability
- » Operational measurements

The EAGLE SCCP subsystem conforms to ANSI T1.112 and ITU Q.7XX1.

Global Title Translation Provisioning

The EAGLE uses tables for performing global title translations. Each table points to another table. The following tables are used for SCCP routing and management.

- » Translation Type (TT) Table
- » Global Title Translation (GTT) Table
- » MAP Table
- » Concerned Signaling Point Code (CSPC) Table

Translation Type Table
Translation Type (TT)
TT Name
Number of Digits
Alias TT

GTT Table
TT
TT Name
GTA
EGTA
XLAT
RI
Point Code
NGT
SSN

MAP Table
Point Code
SSN
Relative Cost
Mated Point Code ^a
Mate SSN ¹
Mate Relative Cost ¹
CSPC Group Name
Message Routing in Cong
Sub System Messages

^a EAGLE 5 ISS supports up to 7 mated point codes

Concerned Signaling PC Table
CSPC Group Name
CSPC

Figure 34: Structure of GTT Provisioning Table

Note: The figure above is only a representation of the actual table structures within the EAGLE.

Translation Type Table

The Translation Type (TT) table is used to direct the translation process to the proper GTT tables for translation and further routing or processing. The Translation Type table supports translation values from 0 to 255.

The EAGLE also provides the capability to map both on a system-wide basis (translation type aliasing) and linkset basis (translation type mapping).

- » Translation Type Aliasing - ANSI/ITU: The EAGLE allows the user to define an alias for Translation Type. When a global title translation is performed involving an alias, the translation type is “mapped” by the alias. The mapping provides the ability to access one GTT table with different TT values. The EAGLE supports one alias per Translation Type.
- » Translation Type Mapping - ANSI/ITU: Translation Type mapping in the EAGLE can take place on an incoming linkset, outgoing linkset, or both. Mapping performed on an incoming linkset is performed before global title translation and gateway screening. Mapping performed on an outgoing linkset is performed after global title translation and gateway screening. The EAGLE supports 256 translation type mappings for each linkset. Since the EAGLE supports a total of 255 linksets, the total number of translation type mappings that can be provisioned in the EAGLE system wide is 65,280.

Global Title Translation Table

The Global Title Translation (GTT) Table contains the digits or ranges of digits that are used to translate the inbound MSU to either another node for additional global title translation (intermediate GTT) or the MSU’s final destination (final GTT). The EAGLE GTT table allows up to 1,000,000 total GTT entries with a performance restriction of up to 200,000 GTT entries per TT. Each entry may be a single value or a range of values.

The EAGLE supports translations when the CdPA has more digits than the GTT range provisioned.


For example, an inbound MSU that arrives with a translation type of 253 and the digits 3038258000 in the CdPA would be translated by the range 3038258-3038259.

Table 5: Global Title Translation

TT	GTA	EGTA	PC	XLAT	RI
253	3137070	3137080	1-1-3	DPC	GT
253	3137254	3137258	1-1-4	DPC	GT
253	3038258	3038259	1-1-1	DPCSSN	SSN

There are five possible results to a global title translation:

1. DPC only, route on GT – This result indicates that the DPC should be altered with the new translated point code, and the message will be routed to that node for further translation. The address indicator routing flag remains set to “route on GT.” If the called party address contains a point code then it is also replaced with the new point code.
2. DPC only, route on SSN – This result indicates that the final destination SSN is already in the called party address and, with the addition of the new translated DPC, the final destination of the message is known. The address indicator routing flag is set to “route on SSN.” The new point code becomes the DPC of the message. If the called party address contains a point code then it is also replaced with the new point code.
3. DPC and SSN, route on GT – This result indicates that the final destination SSN should be determined by translation and be placed in the called party address. Further translation is required at the new node to determine the final DPC. The address indicator routing flag remains set to “route on GT.”
4. DPC and SSN, route on SSN – This result indicates that the final destination SSN and DPC should be determined by translation. No further translation is required, and the message can be routed to its final destination. The translated point code is placed into the DPC, and the SSN should be placed in the called party address. The address indicator routing flag is set to “route on SSN.”
5. New GT – This result indicates that the translation type in the called party address should be replaced with the new translation type from the translation. This also indicates that the DPC in the message should be



altered with the new translated point code and routed to that node for further translation. The routing indicator flag should remain set at “route on GT.”

In all cases, the message is passed to the MTP application to be routed to the new destination.

MAP Table

The MAP table provides the set of remote subsystems associated to a particular remote point code - see Figure 34: Structure of GTT Provisioning Table. Each table contains up to ten subsystems assigned to a particular point code. This table also provides timers used for the subsystem status test (SST) procedure and information for locating the replicated point code and subsystem for any particular SSN. An option is provided on a per point code basis to send an SST upon receipt of an MTP-RESUME to ensure the subsystem is indeed available

The MAP table supports:

- » 3000 full point code entries
- » 8 point codes per MAP group
- » 10 subsystems per point code

Global Title Translations may result in a choice of up to eight node/subsystems (replicated subsystems). Routing between the replicated pairs is based upon the global title translation results, which are provisioned in the database. There are four routing possibilities:

1. Solitary – the GTT has a single node subsystem.
2. Dominant – all traffic is routed to the primary node/subsystem(s) if it is available. If the primary becomes unavailable, the traffic is routed to the backup subsystem(s). If the primary subsequently becomes available again, traffic is then routed back to the primary node/subsystem(s).
3. Load sharing – the load is shared equally between replicated subsystems.
4. Combination Load Share/Dominant - allows a group of primary node/subsystem(s) to loadshare as a dominant group while having the flexibility to form secondary, tertiary, etc. node/subsystem groups.

SCCP routing and subsystem management are handled according to the mated application parameters srm (subsystem routing messages) and mrc (message routing under congestion).

Concerned Signaling Point Code Table

The Concerned Signaling Point Code table consists of a group of point codes that are notified via a broadcast TFP/TFA when the EAGLE receives an SSP/SSA from a subsystem.

The Concerned Signaling Point Code table supports:

- » 2,550 total entries
- » 96 entries per group

Advanced Global Title Translation Functionality

The EAGLE provides advanced Global Title Translation functionality to meet specific network needs. The EAGLE provides the following advanced Global Title Translation capabilities:

- » Enhanced Global Title Translation (EGTT)
- » Variable Length Global Title Translation (VGTT)
- » Modified Global Title Translation (MGTT)
- » Advanced Global Title Modification (AMGTT)
- » Intermediate GTT Loadsharing (IGTTLS)
- » Origin-based SCCP Routing

- » Flexible GTT Loadsharing
- » GTT Loadsharing between ITU network types
- » GTT Loadsharing with Alternate Routing Indicator
- » 6-way Loadsharing on Routesets
- » Flexible Linkset Optional Based Routing (FLOBR)
- » TCAP Opcode Based Routing
- » GTT Actions
- » ANSI<-> ITU SCCP Conversion
- » ITU-N - ANSI SMS Conversion

Enhanced Global Title Translation

Enhanced Global Title Translation (EGTT) broadens the translation mechanism used to perform GTT table selection beyond using the translation type for both ITU and ANSI messages. Typically, EGTT would be necessary for Global Title Translation functionality in ITU environments.

EGTT provides the following capabilities:

- » Global Title Translation by a combination of domain (ANSI or ITU), Global Title Indicator (GTI), Translation Type (TT), Numbering Plan (NP), and Nature of Address Indicator (NAI) selectors.
- » Supports multiple selector entries (ANSI or ITU)
- » Provides an option to delete the CdPA global title after the translation if the result of translation is RI=0 (rt-on-ssn) and PC-SSN is not equal to the EAGLE point code and local SSN.
- » Performs global title translation on ITU messages without an SSN in the CdPA. (ANSI messages are discarded when no SSN is present in the CdPA)
- » Inserts the SSN in the CdPA (when not present) with the SSN obtained from the translation data for ITU Messages.
- » Inserts the PC in the CgPA when an ITU message does not have a PC present in the CgPA and the CgPA RI is "route on SSN". The OPC from the MTP portion is copied over to the CgPA PC.
- » Allows canceling of a called global title and is provisionable per global title address (GTA).

Note: The default GTT functionality for LNP Message Relay messages will ignore this option, if provisioned.

Variable Length Global Title Translation

Variable Length Global Title Translation (VGTT) allows different global title lengths within a Translation Type/GTT Set.


VGTT provides the following capabilities:

- » A total of 16 different GTT lengths are supported per TT or GTT set.
- » Ability to "best fit" route the message by allowing default/nested ranges.

For example, if a customer wanted to use default routing for all route-on-gtt messages and use final global title translation on a few GTT ranges, the GTT table may look as shown below:

Table 6: GTT Messages

TT	GTA	EGTA	PC	XLAT	RI
253	0	9	1-1-3	DPC	GT
253	313	314	1-1-4	DPC	GT
253	3038258	3038259	1-1-1	DPCSSN	SSN



The EAGLE will search, based upon the CdPA, the range of digits equal to or the best match number of digits less than the number contained in the CdPA. In the example above, an MSU with 3134654 in the CdPA of the inbound MSU would first search the 7-digit ranges, find no match, and subsequently search the 3-digit tree and be translated on the range 313-314.

Modified Global Title Translation (ITU)

The EAGLE GTT feature allows the Called Party Translation Type (TT), Point Code (PC), Subsystem Number (SSN), and Routing Indicator (RI) to be modified in the outgoing message. Some networks need the ability to modify more fields in an outbound MSU to be compatible with the node the MSU is destined for. The Modified Global Title Translation feature allows users to customize the GTT information in the MSU to ensure correct routing.

Modified Global Title Translation allows the user to modify any part of the Called Party Global Title in the outgoing message, other than Encoding Scheme, after GTT has been performed. In addition to the TT, PC, SSN, and RI, a user can specify a new value for the Numbering Plan (NP) and Network Address Indicator (NAI). Also, a specified number of prefix or suffix digits of the CdPA Global Title Address (GTA) can be added, deleted, or replaced. This is all defined on a per-entry (i.e., GTA) basis via the EAGLE MMI.

Advanced Global Title Modification

The Advanced GT Modification feature (AMGTT) allows information in the SCCP calling party address (CgPA) to be modified as part of global title translation (GTT). This information includes the global title address (GTA), translation type (TT), numbering plan (NP), and network address indicator (NAI) parameters.

AMGTT extends the functionality of the Modified Global Title Translation feature, which allows modification of Called Party Address (CdPA) information.

Intermediate GTT Loadsharing (ITU)

The EAGLE allows loadsharing between multiple nodes when the EAGLE is performing final GTT. Final GTT means the result of the EAGLE translation is a point code (PC) and subsystem number (SSN), and the routing indicator in the outgoing message is set to Route-on-SSN. The loadsharing is accomplished by accessing a mated application (MAP) table, which specifies the PC, SSN and load-sharing relationship (via relative cost) of up to 8 mated nodes. This loadsharing mechanism is not allowed if the EAGLE is performing intermediate GTT, where the routing indicator in the outgoing message is set to Route-on-GT.

Some international customers have a need to load-share between nodes even when the STP is performing intermediate GTT. This may occur in a network that does not use capability point codes (CPCs). This generally occurs in a quad-STP configuration where the first STP pair performs an intermediate GTT and then must load-share to the second STP pair, which will then perform the final GTT. If a CPC is not available for routing to the second STP pair, there is currently no way for the EAGLE to perform loadsharing.

The Intermediate GTT Loadsharing feature provides the ability to load-share between up to 8 nodes after global title translation, when the outgoing message is Route-on GT. For outgoing messages that are Route-on-SSN (final GTT), the existing Weighted SCP Loadsharing feature will be used.

The Intermediate GTT Loadsharing feature supports a minimum of 1700 GTT transactions per second per DSM card or 850 GTT transactions per second per TSM card while running GTT, VGTT, EGTT, and Modified Global Title Translation.

The Intermediate GTT Loadsharing feature makes use of a Mated Relay Node (MRN) table, which is new to the EAGLE platform. This table holds up to 3000 point codes, with a capacity of up to 7 alternate point codes for each.

The loadsharing relationship between the point codes is specified by assigning each PC a relative cost in relation to its mate PCs. (This is the same method used for final GTT loadsharing via the Weighted SCP Loadsharing feature). The MRN table supports ITU-I and ITU-N point codes and is provisioned via the EAGLE MMI.

If Intermediate GTT Loadsharing is activated, any GTT performed that results in an outgoing message with RI=route-on-GT, triggers an entry into the MRN table. From this table, the EAGLE determines whether the translated PC has any mate PCs and the relative cost of those PCs. If some of the mate PCs have the same relative cost as the translated PC, messages are load-shared equally among all the PCs with equal cost. If a message is destined for a PC that is currently out-of-service, the message will be delivered to the mate PC with the next lowest cost. If the translated PC is available, messages will always be delivered to that PC, even if a mate PC exists with a lower cost, or unless the mate PCs are at equal cost with the translated PC. The only time a message will not be delivered to the translated PC is if it is unavailable, or if it is in an equal-cost loadsharing relationship with another PC, in which case messages will alternate among all the PCs with the same cost to achieve an even load distribution, regardless of the specified translated PC.

Origin-based SCCP Routing

The Origin-based SCCP Routing feature allows greater flexibility and control over their EAGLE SS7 message routing. This feature allows selective routing of messages based on a combination of the SCCP origination and destination information in the message. EAGLE normal SCCP routing is based only on the SCCP destination information - that is, CdPA GTA translation.

Normal SCCP routing/GT translation in the EAGLE uses a combination of the GTA, TT, NAI, NP and GTI fields in the SCCP CdPA parameter to translate and determine the GTT destination for the message. Origin-based SCCP Routing makes use of a combination of the GTA, TT, NAI, NP and GTI fields in the SCCP CdPA parameter as well as the GTA, TT, NAI, NP, GTI and PC/SSN in the SCCP CgPA parameter to determine the GTT destination for the message. The MTP OPC may also be used as a qualifier in the routing decision. This allows greater flexibility over routing of messages, based on both Origination and Destination information.

With Origin-based SCCP Routing, the user has 3 modes of operation for GT translation or SCCP routing: CdPA only (current GTT mechanism), Advanced CdPA, which incorporates both CdPA and CgPA parameters into the routing decision, and CgPA only, which uses only CgPA information and no CdPA information to make the routing or translation determination.

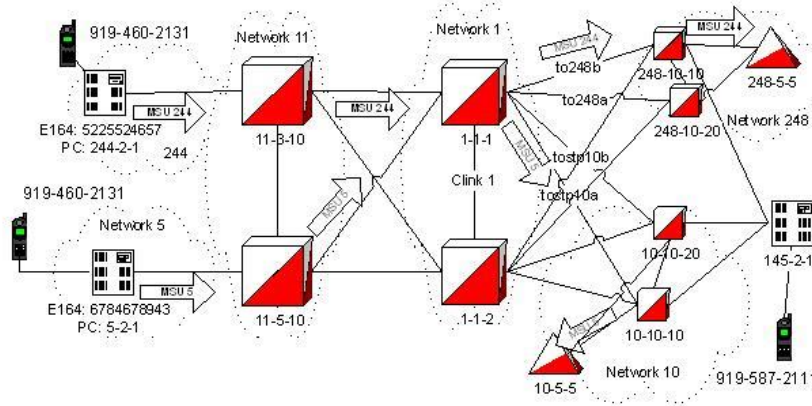
The EAGLE provides 8 user-selectable hierarchies to determine the order in which GTT modes are used. The system will allow a user to specify, on each individual incoming linkset basis, the GTT mode hierarchy that the EAGLE will follow when performing global title translation. The hierarchies are summarized below. For hierarchies containing multiple modes, the table lists the priority order used by the EAGLE in finding a match. If a matching translation cannot be found in the higher priority mode, the EAGLE will search again using the next highest priority mode, and so forth.

For example, if the user has selected Hierarchy #5: Advanced CdPA, CdPA only, and CgPA only and a matching entry is not found using Advanced CdPA mode, the EAGLE will search again using CdPA only mode. If a match is not found in this mode, the EAGLE will search again using CgPA only mode.

Table 7: Available User-Selectable SCCP Routing Hierarchies

Available GTT Modes Hierarchies	
1	CdPA only
2	Adv. CdPA, CdPA

3.	CgPA, Adv. CdPA, CdPA
4.	Adv. CdPA, CgPA, CdPA
5.	Adv. CdPA, CdPA, CgPA
6.	CgPA, CdPA
7.	CdPA, CgPA
8.	CgPA only



Start GTA	End GTA	XLAT	RI	PC	SSN	idx (Adv. CdPA GTT)
9195872000	9195872999	DPCSSN	SSN	248-5-5	5	1
5483526	5483527	DPC	GT	10-10-10		-
...						

GTT Table

a newindex field pointing to a set of Advanced CdPA GTTs

idx	S. CgPA GTA	E. CgPA GTA	CgPA PC	OPC	CgPA SSN	XLAT	RI	PC	SSN
1	6784678943	6784678943	-	-	-	DPCSSN	SSN	10-5-5	5
1	-	-	5-2-1	-	-	DPCSSN	SSN	10-5-5	5
...									

Advanced CdPA GTT Table

a newset of translations using the newoptional message fields as qualifiers

Figure 35: Origin-based SCCP Routing Example

In the figure above, the EAGLE with point code 1-1-1 is performing Origin-based SCCP Routing. Its GTT table and Advanced CdPA GTT table are shown for clarity. The examples below show use cases for a network requesting CgPA Route-on-GT and for a network requesting CgPA Route-on-PC. The difference in the two scenarios is primarily whether a GTA or PC/SSN is present in the CgPA to be used by the CgPA only or Advanced CdPA modes of Origin Based Routing.

Both examples assume that Caller 919-460-2131 originates a call requiring an SCP database lookup from network 244 (MSU 244) via MSC 244-2-1. MSU 244 is intermediate GTT'd at STP 11-3-10 and sent to EAGLE 1-1-1. The network operator who owns 1-1-1 has a business arrangement between network 244 and network 248, and wants to send the query to the SCP of network 248. This linkset is using an Advanced CdPA followed by CdPA-only hierarchy. Thus, the EAGLE searches the Advanced CdPA GTT table. An applicable match is not found, thus the EAGLE searches next the CdPA only criteria, finds a match, and sends the query to 248-5-5 based on the translation data in the GTT Table

1. CgPA Route-on-GT Example

Subsequently, Caller 919-460-2131 flies to a location that is served by network operator 5 instead of Network 244. Again, caller 919-460-2131 originates a call that requires the same database lookup. Now the message originates at MSC 5-2-1 instead of MSC 244-2-1. MSC 5-2-1 requests response routing based on GT, and thus puts its own E.164 number (6784678943) inside the GTA field of the CgPA parameter of the query message and sets the RI to Route-on-GT. This message receives an intermediate GT translation in Network 11, and is then routed to EAGLE 1-1-1. This linkset also has an Advanced CdPA followed by CdPA-only hierarchy.

When query message MSU 5 arrives at EAGLE 1-1-1, the EAGLE first searches the Advanced CdPA Table and finds a match on MSC 5-2-1's CgPA GTA (6784678943). Because of the hierarchy selected, the translation in the Advanced CdPA table takes precedence over the CdPA-only translation in the standard GTT table. Thus, the EAGLE forwards the query to Network 10's SCP (10-5-5) instead of Network 244, which would be the chosen network if CdPA-only mode were used.

2. CgPA Route-on-PC Example

Alternatively, assume the same situation as described in section 0.00, except that this time MSC 5-2-1 requests response routing based on PC, and thus puts its own point code (5-2-1) inside the CgPA PC field of the query message. The message again receives an intermediate GT translation in Network 11, and is then routed to EAGLE 1-1-1. This linkset has an Advanced CdPA followed by CdPA-only hierarchy.

When query message MSU 5 arrives at EAGLE 1-1-1, the EAGLE again searches the Advanced CdPA first and finds a match on CgPA PC (5-2-1). Because of the hierarchy selected, the translation in the Advanced CdPA table takes precedence over the CdPA-only translation in the standard GTT table. Thus, the EAGLE will forward the query to Network 10's CNAM SCP (10-5-5).

Flexible GTT Loadsharing

The EAGLE loadshares post-GTT destinations through the use of either the Mated Application (MAP) table for final GTT or the Mated Relay Node (MRN) table for intermediate GTT. When a group of point codes are entered into the MAP or MRN tables as mates, the EAGLE will loadshare messages for that GT translation between the PCs based on the relative cost assigned to each PC. PCs may be in primary/backup relationships, or loadsharing relationships, depending on the relative costs assigned to each.

Based on the current architecture, the EAGLE does not allow the user to define different GT translations which use different loadsharing relationships between the same set of destination point codes in the MAP or MRN tables. The EAGLE also does not allow the user to define different sets of destinations containing overlapping point codes. The load-sharing relationships established between a group of point codes in the MAP or MRN table are global across all translations.

For example, assume a user defines GTA=9194605500 in the GTT tables with a final GT translation to PC/SSN=1-1-1/10. The user then defines a relationship in the MAP table between destination point code/SSNs 1-1-1/10 and 2-2-2/10. The relative costs between the two PCs are equal, meaning all traffic routed using GTA=9194605500 will be divided equally between the two destinations. Next assume the user defines another GTA=9194611000 in the GTT tables, also with a translation to PC/SSN=1-1-1/10. Because of the previously defined relationship between 1-1-1/10 and 2-2-2/10, all traffic routed using this GTA will also be divided equally between those two destinations. Because the EAGLE currently only allows one set of relationships to be defined between a GTT destination and any other PC(s), all GTAs in the GTT table that translate to 1-1-1/10 will have the same set of load-sharing rules applied.

The Flexible GTT Load-Sharing feature is designed to provide more flexibility by allowing different relationships to be established between the same set (or subset) of destinations. For example, in the scenario above, GTA=9194605500 could translate to PC/SSN=1-1-1/10 and indicate a load-sharing relationship with PC/SSN=2-2-2/10, while GTA=9194611000 could also translate to PC/SSN=1-1-1/10, but indicate there is no load-sharing with any other destination. Furthermore, GTA=9193881416 could also translate to destination 1-1-1/10, but indicate a load-shared relationship with destinations 2-2-2/10 and 3-3-3/10. Thus, traffic routed to GTA=9194605500 would be

divided equally between 1-1-1/10 and 2-2-2/10, traffic routed to GTA=9194611000 would be sent only to 1-1-1/10, and traffic routed to GTA=9193881416 would be divided equally between 1-1-1/10, 2-2-2/10, and 3-3-3/10.

Flexible GTT Loadsharing applies to both the MAP and MRN tables, and thus is applicable for both final and intermediate GT translations.

As an example, consider the network shown below.

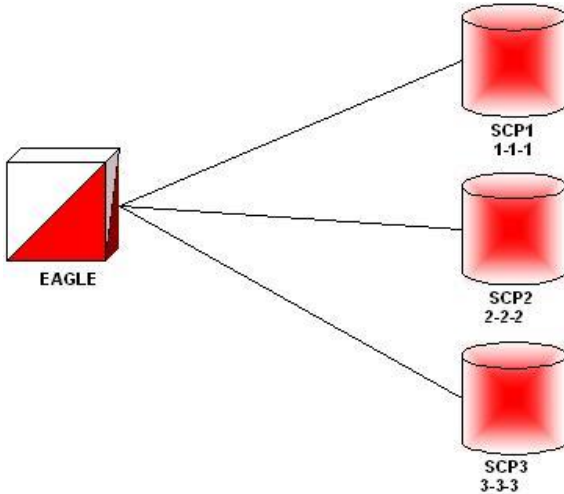


Figure 36: Flexible GTT Example

Without Flexible GTT Loadsharing, any GTA that translates to either PC 1-1-1, 2-2-2 or 3-3-3 will result in traffic being routed to those three destinations based on a single mate relationship. However, with Flexible GTT Loadsharing, it is possible to have different mate relationship depending on which GTA is used for the translation:

Table 8: Flexible GTT Routing

Flexible GTT routing to SCP1, SCP2, and SCP3:

GTA Used	Loadsharing Relationship
GTA1	Traffic equally divided between SCP1, SCP2 and SCP3
GTA2	Traffic equally divided between SCP1 and SCP3 only
GTA3	All traffic routed to SCP1 only, with backup to SCP2
GTA4	All traffic routed to SCP2 only. No backup.

GTT Loadsharing between ITU Network Types

The GTT Loadsharing between ITU Network Types feature allows GTT loadsharing to occur between ITUNational (ITU-N), ITU-N spare, ITU-International (ITU-I), and ITU-I spare point codes within the same MAP or MRN set.

It also allows different alias combinations to be provisioned, such as an ITU-N spare alias for an ITUN destination point code. It supports the current maximum of two alias point codes per destination point code.

The feature adds support for provisioning additional alias combinations for ITU-I, ITU-N, ITU-I spare, and ITUN spare true point codes and their spare types, including:

- » ITU-N spare alias for ITU-N true point code

- » ITU-N alias for ITU-N spare true point code
- » ITU-I spare alias for ITU-I true point code
- » ITU-I alias for ITU-I spare true point code
- » the ability to provision an ITU-I and an ITU-I spare alias for an ITU-N/ITU-N spare point code
- » the ability to provision an ITU-N and an ITU-N spare alias for an ITU-I/ITU-I spare point code.

These new alias combinations allow MTP-routed and GT-routed messages to cross spare-non spare network boundaries. SCCP conversion of CgPA point code, conversion of concerned point code (network management messages) and affected point code (SCMG messages) are also supported for the new alias combinations.

GTT Loadsharing with Alternate Routing Indicator

The GTT Loadsharing with Alternate Routing Indicator (GTT LS ARI) feature allows the routing indicator (RI) in the outgoing message to be provisioned without depending on whether the primary GT translation resulted in Final or Intermediary GTT. This feature provides a backup SCCP loadsharing mechanism if the primary SCCP loadsharing mechanism does not route the message.

This feature allows loadsharing relationships to be established between the MAP and MRN table in that the MAP set and MRN sets allow provisioning of MRN and MAP sets, respectively, as the Alternate Mate RI if the point codes in the MAP or MRN table are unavailable.

If the feature is enabled, then the MRN table allows access to the MAP table to perform a secondary mate search if all point codes in a given MRN set are unavailable. The MAP table also allows access to the MRN table to perform a secondary mate search if all point codes provisioned in a given MRN set are unavailable. If a point code or a point code/subsystem number combination is specified, but an MRN set or MAP set is not specified, then the default MRN set or MAP set is used. Only one secondary mate search can be performed per translation.

6-Way Loadsharing on Routesets

The 6-Way Loadsharing on Routesets feature allows loadsharing across all 6 routes to a destination or exception route.

Flexible Link set Optional Based Routing

The Flexible Link set Optional Based Routing (FLOBR) feature allows GTT routing to be based on the incoming linkset. Messages that encounter GTT are routed based on the incoming linkset of the original MSU.

The FLOBR feature also allows full customization of the GTT routing hierarchy. If flexible routing is used, then a predetermined routing hierarchy is not necessary. The GTT routing translation can link to any GTT set as long as the GTT set has a different set type. The capacity of the GTT selector table is increased to support 100,000 GTT selectors.

The following additional functionality is provided:

- » Fall-back to GTT after EPAP-based Relay Services: Global Title Translation (GTT) can be performed on an MSU that is relayed to another destination based on routing data obtained from the EPAP database/PPSOPTS table by an EPAP-based service. GTT for Service Related MSUs is performed on a service selector basis. Each supported service selector can be configured to indicate whether GTT is required after service execution is complete. The MNP, HLR ROUTER, SMSMR, IDPR, INPMR, and TTR service selectors are supported.
- » GTT/TT Commands allowed with EGTT: The ent/dlt/rtrv-tt and ent/chg/dlt/rtrv-gtt commands are supported for GTT simple entries (entries that have not been modified by enhanced GTT processes) independently of the enabled GTT features.

- » CdPA SSN for GTT Routing: GTT routing can be performed based on Called Party (CdPA) Subsystem Number (SSN) translations when the FLOBR feature is turned on.
- » DPC for GTT Routing: The MTP Destination Point Code (DPC) can be considered as part of the routing criteria for GTT Routing.
- » Use of the same GTT set types in a Translation Search: When performing a translation using FLOBR processing, lookup can occur in the same GTT set type up to 7 times during a search. The same set name cannot be repeated in a single GTT search.

Feature independence of the TST-MSG tool: The TST-MSG tool can be used when any GTT feature is turned on.

TCAP Opcode Based Routing

The TCAP Opcode Based Routing (TOBR) feature allows GTT routing to be based on information in the TCAP portion of ANSI or ITU messages or on the SCCP Called Party Subsystem Number (CdPA SSN).

For ITU messages, the information in the TCAP portion includes ITU TCAP package type, application context name, and operation code. For ANSI messages, the information includes ANSI TCAP package type, family, and operation code specifier.

All UDT, UDTS, Unsegmented XUDT, and Unsegmented XUDTS queries are supported. Segmented XUDT messages are supported for SSN routing. The TOBR feature allows all segmented TCAP SMS messages within a transaction to be routed to the same destination. The messages are routed based on the TCAP OpCode and Dialogue portion of the message.

GTT Actions

The GTT Actions framework increases the functionality of the Global Title Translation (GTT) and Flexible Linkset Optional Based Routing (FLOBR) features. GTT Actions supports all functionality provided by the Enhanced GSM MAP Screening (EGMS) feature except for screening based on Forbidden Parameters in ATI messages.

Note: Both GTT Actions and EGMS are supported and can co-exist in the system.

The GTT Actions framework consists of three separate features:

1. GTT Action - DISCARD – there are three types of discard:
 - Discard – discard message with no return error
 - UDTS – discard message and send UDTS/XUDTS independently of the value of the Message Handling flag in the MSU
 - TCAP Error – return a specified TCAP Error for the opcode

The functionality performed by the GTT Action - DISCARD feature was originally performed by the Origin-based SCCP Routing (OBSR) feature. All entries that were previously provisioned using the OBSR feature will be converted to a GTT Action and Action Set.
 2. GTT Action - DUPLICATE
 3. GTT Action – FORWARD
- Routes a copy of the message to a specified duplicate node. The original message is always routed based on GTT/DB data. A copy of the message is routed to a specified duplicate node if the node is available.
- Routes the original message to a specified forward node instead of the destination indicated by the GTT/DB data. If the Forward node is not available, a configurable default action can be used. This action could result in an error response (TCAP Error or UDTS), silent discard, or routing based on default GTT/DB data.

The GTT Actions framework allows the creation of a GTT Action Set, which is a list of actions that are performed on a message. A GTT Action ID is used to define the action and its characteristics.

The GTT Actions framework also provides the following capabilities:

- » **Advanced GTT Modification Enhancements:** Data, including Calling Party data, used to configure the Advanced GTT Modification (AMGTT) feature is maintained in a new GT Modification (GTMOD) table.
The AMGTT feature is also enhanced to allow deletion of a trailing 0 in the Global Title Address (GTA) during GTT modification if the conversion from GTI(x)=2 to GTI(x)=4 occurs. Encoding scheme (ES) calculations are performed on the remaining digits after the 0 is deleted.
- » **Non-overlapped GTT Selectors:** ITU GTT selectors (i.e ITU-I, ITU-N, ITU-N24, ITU-I Spare and ITU-N Spare) with different domains can be provisioned for the same GTI value and translation type (TT) independently.
- » **Per-Path Measurements:** Per-Path measurements, the equivalent of the EGMS Per-Path measurements, can be performed by GTT. These measurements provide counts for GTT Actions that match a pre-defined combination of CgPA GTA, CdPA GTA, and Opcode values. This functionality is not specific to FLOBR or GTT Actions, but can be specified for any GT translation. If CdPA-only GTT is the only service turned on, having per-path measurements is not applicable, since there is no searching on CgPA or Opcode.
- » **Reference Count for GTTSETs:** The response of the dlt-gttset command is enhanced by maintaining an internal reference count for each GTTSET. When a GTTSET is referenced or de-referenced, the reference count for that GTTSET is incremented or decremented by 1.
- » **Support of xlat=none Translations:** A GT entry containing GTT Action or GT Modification data can be provisioned when translation data is not present. This ability also allows loadsharing of message-relayed EPAP-based features. If xlat=none is provisioned, then both an MRN set and a MAP set can be provisioned against the translation.
- » **Unique GTT Selectors:** GTT Selectors with ITU-I Spare and ITU-N Spare domains can be provisioned using the ent/chg/dlt/rtrv-tt and ent/chg/dlt/rtrv-gttset commands.
The MTP Routed GTT feature allows Global Title Translation (GTT) and GTT Actions functionality to be performed on MTP-routed SCCP messages. This feature is provisioned using options in the chg-sccpopts command.

GTT Actions to Trigger Services

Introduced in EAGLE release 46.0, the GTT Actions to Trigger Services feature provides new GTT Actions to allow triggering EAGLE services such as HLR Router or MNP. This feature allows a service to be triggered as a GTT Action based on either the usual GTT rules or after FLOBR/TOBR execution. The GTT Actions to Trigger Services feature is useful when combining advanced routing features with Number Portability lookup or with HLR Router lookups.

ANSI->ITU-SCCP Conversion

Since some ANSI and ITU SCCP parameters are incompatible in format or coding, this feature provides a method for the EAGLE to convert these SCCP parameters in UDT and UDTS messages. Other types of SCCP messages (for example, XUDTS) are not supported and are discarded.

The ANSI-ITU-China SCCP Conversion feature provides a generic capability to correctly format and decode/encode these SCCP messages:

- » UDT and UDTS messages - includes SCMG messages, which are a specialized form of UDT messages
- » MTP routed SCCP messages
- » GT routed SCCP messages.

ANSI->ITU SCCP conversion also provides SCCP management (SCMG) across network type boundaries, i.e., Concerned Signaling Point Codes for a mated application may be of a different network type than the mated application.

UDTS message return is controlled inherently by the SCCP layer protocol within the protocol class byte. If bits 5-8 indicate return message on error, a UDTS message will be sent when there is an error. Otherwise, no UDTS is returned to the originator.

For point code conversion to take place, alias point codes must be provisioned to allow for translation of different point code formats.

MTP-routed UDT/UDTS (SCCP) messages are converted on the LIM card. If the message carries Global Title information, but the current EAGLE is not the Destination Point Code, conversion of that Global Title information is also performed on the LIM card. The figure below illustrates ANSI->ITU SCCP conversion for MTP routed messages.

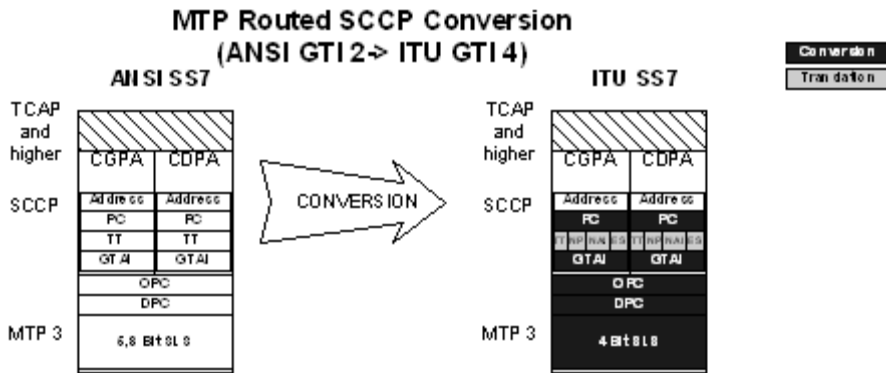


Figure 37: ANSI->ITU SCCP Conversion - MTP Routed

GT-routed UDT/UDTS (SCCP) messages are converted on the SCCP card. An important difference between MTP-routed and GT-routed SCCP conversion is that for MTP-routed conversion, the CDPA point code is actually converted while for GT-routed messages, the CDPA point code is a result of the GTT translation and not a conversion. Another difference is that for GT-routed messages, the CDPA point code is inserted as the MTP DPC as well, so neither the CDPA nor the MTP DPC in a converted GT-routed message undergoes conversion but rather is replaced as a result of GT. Finally, as is the case for all GT-routed messages, the MTP OPC will be the EAGLE point code for the outbound network. The figure below illustrates ANSI->ITU SCCP conversion for GT-routed messages.

GT Routed SCCP Conversion (ANSI GTI 2-> ITU GTI 4)

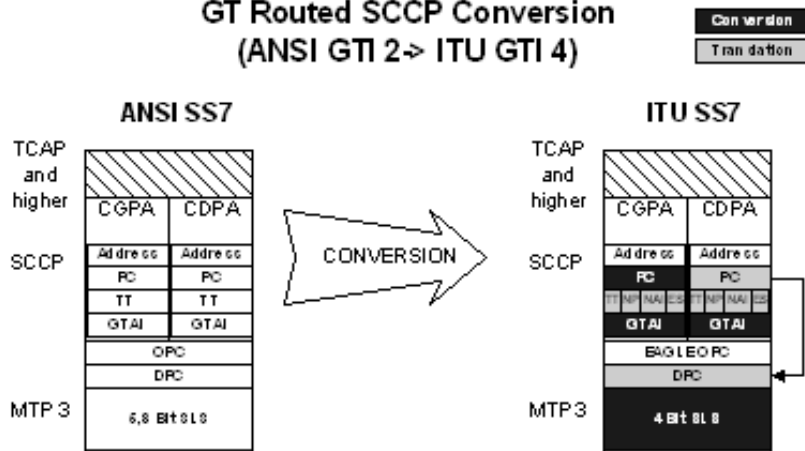


Figure 38: ANSI->ITU SCCP Conversion - GT Routed

An SCCP message may be converted using 3 different conversion methods:

- » GTA Specific SCCP Conversion - GT-Routed Messages only
 - » Allows for per GTA specific SCCP conversions
 - » Same functionality as Default SCCP Conversion
- » Default SCCP Conversion
 - » Performed on all MTP routed SCCP messages
 - » Performed on all GT routed messages if no GTA specific conversion exists.
 - » Supports ANSI GTI 2 and ITU GTI 2 and 4
 - » Allows for digit manipulation and changing TT, NP and NAI parameters
- » System Default Conversion
 - » Allows for a system default conversion when no conversion parameters are found either in GTA Specific SCCP and Default SCCP Conversion.

ITU-N - ANSI SMS Conversion

Operators that handle SMS traffic traveling from ITU to ANSI networks and vice-versa require a solution to convert their text-based traffic.

The ITU National-ANSI SMS Conversion feature fulfills this need and modifies the SMS Address parameter in the TCAP/IS41 layer of the Registration Notification (RegNot), SMS Request Return Result (SMS Req RR), and SMS Notification (SMS Not) messages that cross the ITUN-ANSI network boundary.

The below figure illustrates the ANSI-ITU SMS conversion process:

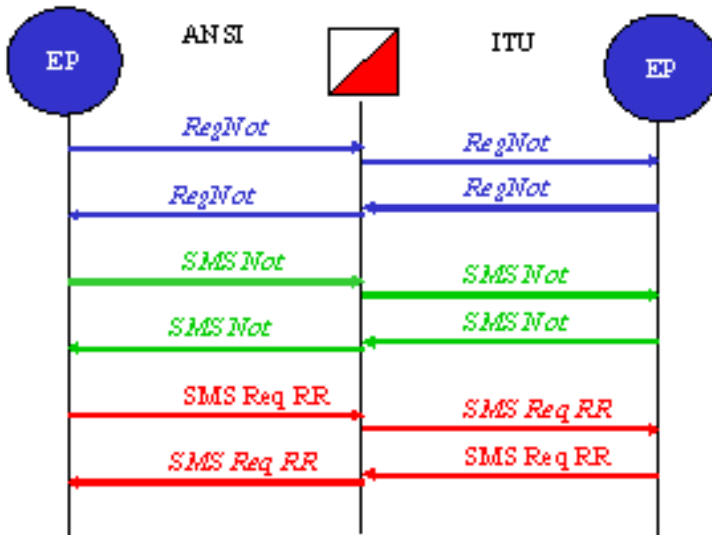


Figure 39: ANSI-ITU SMS conversion process

The EAGLE determines whether the message is sent from an ITU to an ANSI destination (or vice versa) and accordingly converts the Point Code of the SMS Address parameter in the TCAP/MAP layer. The SMS Address parameter in the identified messages must contain an ANSI or ITU-N point code value to enable the ITU-N -ANSI SMS Conversion feature to process the messages. Finally, the EAGLE routes the messages to the original destination based on the MTP DPC, whether they have been converted or not.

This feature has the following limitations:

- » ITU-N 24 Bit and ITU International point codes are not supported
- » Point Code clusters are not supported

SCCP XUDT MESSAGE SUPPORT - ITU/ANSI

Introduction

XUDT is a defined SCCP message format in both ANSI and ITU SS7 recommendations. UDT has been the predominant format for SCCP messages, and few networks have had a need to utilize XUDT. However, with increasing use of SMS and GPRS in next generation networks, the use of the XUDT format is starting to become a requirement, both in ITU and ANSI networks. The EAGLE supports MTP routing on XUDT messages, but does not support GTT and other SCCP processing on XUDT messages. With this feature, the EAGLE will support processing of XUDT messages under certain conditions.

Available Support

SCCP XUDT Message Support includes the following:

- » Allows EAGLE to interoperate in ANSI and ITU networks using XUDT messages.
- » Provides support for the following features and functions in relation to XUDT messages:
 - » MTP routing for Protocol Class 0 and Protocol Class 1 ANSI and ITU XUDT messages
 - » GTT/EGTT/VGTT routing to a primary destination with backup for Protocol Class 1
 - » GTT routing with equal cost loadsharing to 8 destinations for Protocol Class 0
 - » MTP and SCCP (pre- and post-GTT) Gateway Screening
 - » SCCP Hop Counter

- » HLR Router
- » XUPTS transfer and generation
- » INAP-based Number Portability (INP) Message Relay
- » INAP-based Number Portability (INP) Query/Response (non-segmented XUPT only)
- » MNP Message Relay
- » Enhanced GSM MAP Screening (non-segmented XUPT only)

XUPT Limitations

The following limitations exist in the deployment of XUPT support. This section will be revised as enhancements are made in future EAGLE releases.


- » Protocol Class 1 messages cannot be equally loadshared among all available GTT destinations as can Protocol Class 0. Protocol Class 1 will be routed to a primary destination with backup
- » INAP InitialDP messages requesting INP Query Service cannot be sent in segmented XUPT or LUPT format (INP Message Relay on XUPT messages and Query/Response for non-segmented XUPT is supported.)
A new XUPT UDT Conversion feature in R 43.0 allows XUPT(S) < - > UDT(S) conversion to occur based on the Destination Point Code (DPC) for MTP-routed and EAGLE-generated SCCP messages. Format conversions for both segmented and non-segmented messages are supported; however, the system does not perform segmentation or reassembly. For GT-routed messages and MTP-Routed SCCP messages that are processed on Service Module cards, XUPT UDT conversion is applied after the ANSI/ITU SCCP Conversion feature processes the messages.
- » GSM_MAP_Send_Routing_Info (SRI) messages destined for EAGLE MNP Query Service cannot be in XUPT format (MNP Message Relay on XUPT/LUPT messages is supported.)
- » Message destined for processing by the EAGLE IS41 to GSM Migration feature cannot be in XUPT format.
- » North American LNP queries cannot be sent in XUPT format. Also, North American LNP Message Relay is not supported on XUPT messages)
- » XUPT messages cannot be subjected to (standard) GSM MAP Screening. Enhanced GSM MAP Screening does support non-segmented XUPT messages.
- » XUPT messages cannot be subjected to ANSI <=> ITU <=> China SCCP conversion (MTP conversion is supported).
- » GSM_MAP_Check_IMEI message queries to the EAGLE Equipment Identity Register (EIR) feature cannot be in XUPT format.
- » XUPT Support does not offer unique measurements pegs for XUPT messages separate from UDT messages. Existing EAGLE measurements will be pegged for all message types.

GUARANTEED IN-SEQUENCE DELIVERY OF SCCP PROTOCOL CLASS 1 MESSAGES

Introduction

Many networks utilize SCCP Protocol Class 1 for messages that are required to arrive at their destination in sequential order. Typically, Class 1 messages are used in dialogues with intelligent network or application database nodes such as IN, AIN, or CAMEL SCPs. Today, the EAGLE can process and route Protocol Class 1 messages, and in most cases will deliver these messages to the destination in the correct sequential order (as received from the originating node). However, the EAGLE does not have an active mechanism to completely guarantee that these messages will stay in sequence as they are routed through the EAGLE node. As a result, there may be extreme cases in which Class 1 messages may get out of order and may be delivered to the destination node out of sequence. This feature will implement an active algorithm within the EAGLE to insure that Class 1 messages are delivered out of the EAGLE in the same order that they were received.

Available Support



The Guaranteed In-Sequence Delivery of SCCP Protocol Class 1 Messages feature provides an active mechanism to insure that SCCP Protocol Class 1 messages (UDT, and XUDT) will be delivered in the same order they were received by the EAGLE from the originating node. Support is provided for the following:

- » GTT routing to a primary destination with backup
- » ANSI and ITU Protocol Class 1 - UDT/XUDT message types
- » Protocol Class 1 UDT supported for all EAGLE features and functionalities, with the exception of equal cost GTT loadsharing to multiple destinations
- » Protocol Class 1 XUDT support provide except as indicated in XUDT Limitations of this document.

Considerations/Limitations

- » Incoming Traffic Volume Limitation: With In-Sequence Delivery of SCCP Class 1 message functionality active, all EAGLE SS7 link types, TDM or IP, will continue to perform at maximum capacity if only 50 percent of the incoming traffic are SCCP Class 1 messages. A higher mix of SCCP Class 1 message could potentially result in congestion at the LIM card.
- » GTT Loadsharing Limitations: As related to Protocol Class 1 messages, the EAGLE provides GTT routing to a primary destination with backup only. Equal cost loadsharing to multiple GTT destinations is not possible for Class 1 messages in this phase. In most respects, this is not a concern because the nature of Class 1 messaging means that the same sequence of messages must arrive at the same destination node. Therefore, it is unlikely that equal cost loadsharing would be desirable on these messages because this could cause messages within the same sequence to arrive at different destinations.
- » Message Sequencing Considerations: The Guaranteed In-Sequence Delivery of SCCP Protocol Class 1 Messages feature guarantees that the EAGLE will deliver all Protocol Class 1 UDT/XUDT messages to the destination node (or next node in the route) in the same order that they were received from the originating node (or previous node in the route). As long as the messages are in the correct sequence when they arrive at the EAGLE, they will be delivered by the EAGLE to the next node in the correct sequence. If the messages are not in the correct sequence when they arrive at the EAGLE, they will not be delivered to the next node in the correct sequence. The EAGLE will not perform message re-sequencing for messages that are received out of sequence. Because the EAGLE is a transit node, and the originating and destination nodes are responsible for re-sequencing, the EAGLE is only required to maintain the sequence that it received.

This feature assumes that the Class 1 option of the EAGLE Random SLS feature is not activated for the linkset in question. If it is, the messages will not be delivered in sequence even with the Class 1 sequencing algorithm active. This is not a limitation - this is the intended behavior of the Random SLS feature.

TRANSACTION-BASED GTT LOADSHARING

Introduction

Today, Global-Title-routed messages coming into the EAGLE are routed using the SCCP information. When loadsharing gt-routed messages, there is no way to guarantee messages of the same transaction are load-shared to the same destination in MAPGROUP/MRNGROUP. This is because the EAGLE load-shares the messages based on SCCP parameters. For applications like Prepaid services, various gt-routed messages belonging to the same call need to go to the same load-shared PC in the MAPGROUP/MRNGROUP.

The Transaction-based GTT Load Sharing (TBGTTL) feature uses the transaction parameter to control load-sharing for Class 0 and Class 1 SCCP messages. The Transaction-based GTT Load sharing feature also controls load-sharing for unit data (UDT) and extended unit data (XUDT) messages.

EAGLE generates a unique key for each MSU when transaction-based GTT load-sharing is performed. This key, called the MSU Key, is a unique 4-byte number. The value of the MSU Key depends on the selected transaction parameter. The transaction-based GTT loadsharing algorithm ensures that message signal units (MSUs) that have the same MSU Key value are routed to the same destination within the Entity Set.

For UDT messages, the key is based on MTP, SCCP, or TCAP transaction parameters. For XUDT messages, the key is based on MTP or SCCP parameters.

Table 9: Transaction-based GTT Provisioning Options

Protocol	MSU Key Value
TCAP	TCAP ID
SCCP	For XUDT(S) & UDT(S) messages – last 4 bytes of GTA field of CdPA inbound MSU
MTP	For XUDT(S) & UDT(S) messages – last 3 bytes of incoming OPC & 1 byte of SLS combined. This structure applies to both ANSI and ITU point codes. This is the default parameter for performing TBGTTLS

The EAGLE provides multiple forms of Intermediate and Final GTT loadsharing. These load-sharing modes are determined by the relative cost of each entity in the Entity Set.

The possible configurations are

1. Solitary
2. Dominant
3. Load-Shared
4. Combined Load-Shared/Dominant

TBGTTLS affects only entities that work in the Load-Shared and Combined Load-Shared/Dominant loadsharing modes.


- » In Load-Shared mode, the entire Entity Set is a part of one Relative Cost (RC) group and MSUs are load-shared based on the transaction parameter within the entities in the Entity Set. If none of the entities in the Entity Set are available for routing, the message is dropped and a UDTS/XUDTS message is generated if “return on error” is set in the SCCP message. A UIM (internal error report) is generated to notify the user that the MSU has been dropped.
- » In Combined Load-Shared/Dominant mode, TBGTTLS is initially applied to the RC group, where the PC/PC+SSN belong, that is obtained as a result of GTT.
 - » If none of the entities are available for routing within that particular RC group, the next higher cost RC group shall be chosen and TBGTTLS is applied to the new RC group. This process is repeated until there is no available entity in the Entity Set for routing.
 - » If none of the entities are available for routing, the message shall be dropped and a UDTS/XUDTS message is generated if “return on error” is set in the SCCP message together with a UIM is generated to notify the user that the MSU has been dropped.

Considerations and Limitations

For Transaction-based GTT loadsharing, Intermediate GTT loadsharing (IGTTLS) for MRN and GTT (for MRN or MAP) is required.

If the Transaction-based Load Sharing and Weighted GTT Load Sharing features are both enabled, then transaction-based loadsharing has higher priority. This guarantees that messages of a single transaction are loadsharing to the same entity within the MAP group or MRN group.

For transaction-based routing, loadsharing can be guaranteed only when incoming messages are well distributed over MTP/SCCP/TCAP parameters. When the incoming traffic is well distributed using the MTP/SCCP/TCAP parameters, then EAGLE will distribute traffic (at least 1,000 messages) in accordance with loadsharing applicable to the MAPSET/MRNSET with an allowed deviation of $\pm 5\%$. If a new entry is added or an existing entry is deleted



from an RC group within an Entity Set while MSUs are getting routed to one of the entities in that particular RC group, the EAGLE might not be able to maintain the loadsharing distribution and allowed deviation for the load-shared traffic:

- » When the Transaction-based GTT Loadsharing feature and the Weighted GTT Loadsharing feature are both on, the following scenario can occur:
 - » An RC group (for example, RC1) becomes prohibited and all of its traffic is rerouted to an alternate RC group (for example, RC2).
 - » A node comes up in RC1 (which was the initial destination for an MSU routed base on TBGTTLS), but the weight percentage of RC1 is still below the in-service weight threshold. RC1 is still considered prohibited and traffic is not sent to the node in RC1.
- » If the number of available entities within the RC group differs between successive MSU transmissions, all the MSUs that are getting routed to alternate destination (because the primary destination was not available) get rerouted, even if the entity that has become unavailable is not the destination entity for those MSUs.
- » When the Primary Destination is inhibited and the traffic is failed over, the node state might not be maintained if other nodes also fail.
- » When an entity is added to a group or deleted from a group, so that the number of entities in the group changes, the assignments within the group could all change.
- » The Transaction-based GTT Loadsharing feature uses only the first TCAP ID that it encounters in a message and does not distinguish between Origination (OTID) or Destination (DTID). This behavior may cause the TCAP ID method not to function in all scenarios. Before implementing the Transaction-based GTT Loadsharing feature, the user must fully understand call flows to insure that use of the TCAP ID method will operate as intended for the particular call flows.

WEIGHTED GTT LOADSHARING

Introduction

The EAGLE load-shares post-GTT PC plus SSN through the use of the Mated Application (MAP) table for final GTT and Mated Relay Node (MRN) table for intermediate GTT. Based on the current architecture, EAGLE does not allow the user to define different weighted load-sharing relationships between point codes in the MRN/MAP table. The EAGLE only supports equal loadsharing between point codes with same relative cost in the MRN Group or MAP Group.

When a node with higher capacity is added in the network, then there is a need for weighted GTT load-sharing (WGTTLS). This feature allows different load-sharing relationships to be established between point codes with the same relative cost within a MAP Group or MRN Group. The Weighted GTT Loadsharing feature controls loadsharing through the MAP and MRN entities within a MAP group or MRN group. MAP entities distribute MTP-routed GTT traffic to the final destination. MRN entities relay MTP-routed GTT traffic to other nodes for further GTT processing.

The Weighted GTT Loadsharing feature provides the following two methods to control the distribution of GTT traffic through MAP or MRN groups:

- » Individual weighting for each RC group entity: Individual weighting assigns different load capacities, in the range of 1 to 99, to the entities of an RC group. Each entity receives a percentage of the network traffic proportionate with its weight relative to the total weight of the RC group.
- » In-service threshold of each RC group: The in-service threshold is the minimum percentage of the total of the provisioned weights of an RC group that must be available for the RC group to receive network traffic. An in-service threshold of 1% means that the group will be used if any member is available. The entire RC group is considered unavailable for network traffic if the percentage of the available weights is less than the in-service threshold. The RC group is considered available if the percentage of the available weights is greater than or equal



to the in-service threshold. If an RC group is available, network traffic can be sent to any available entity in the RC group.

WGTTLS adds two new modes for loadsharing:

- » Weighted Load-Share
- » Weighted Combined Load-Share

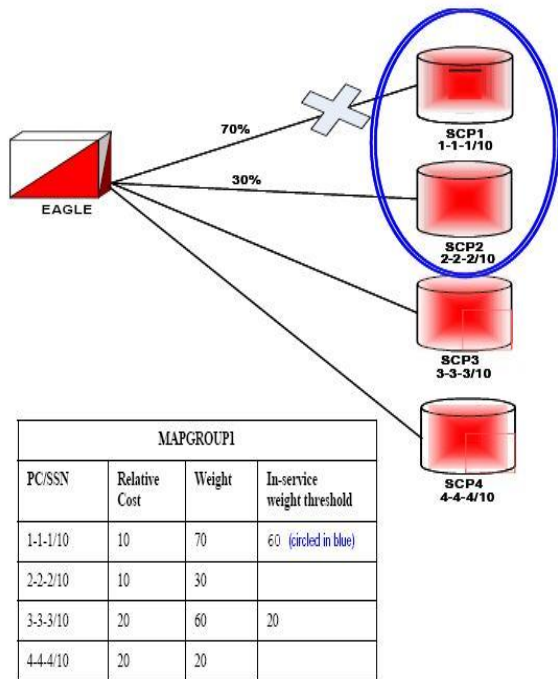


Figure 40: Weighted Load Sharing Based on MAPGROUP

As shown above, when MAPGROUP1 is selected, the traffic will be distributed between PC/SSN=1-1-1/10 and PC/SSN=2-2-2/10, when both are available. Based on the configured weighted loadsharing, PC/SSN=1-1-1/10 will receive 70% (70/100) of the traffic and PC/SSN=2-2-2/10 will receive the remaining 30%(30/100).


When the PC/SSN=1-1-1-1/10 becomes unavailable, the combined “in-service weight threshold” drops to only 30% so it is below its 60% threshold. In this case 3-3-3-3/10 and 4-4-4-4/10 PC/SSNs with relative cost (RC) of 20 becomes available where PC/SSN 3-3-3-3/10 receives 60% of the traffic and 4-4-4-4/10 receives 20% of the traffic.

When PC=1-1-1/10 becomes available, the available weight percentage of relative cost group 10 is now 100%. This is over the in-service weight threshold of 60%. In this case, the traffic is redistributed back 70/30 between PC=1-1-1 and PC=2-2-2 when all these PC’s are available.

Considerations and Limitations

For Weighted GTT loadsharing, Intermediate GTT loadsharing (IGTTLS) for MRN and GTT (for MRN or MAP) are required.

Outbound traffic distribution is affected by incoming traffic distribution. If the OPC, SLS, and incoming Link ID do not span a diverse range, then weighted distribution may not be able to be maintained. Maintaining the same DPC for the transaction is given priority. This affects SCCP Class 1 Sequenced traffic only. It does not affect Class 0, or Class 1 when Class 1 sequencing is turned off, which are balanced regardless of OPC, SLS, and incoming Link ID.



When weights are assigned or changed in an MRN or MAP group that is handling transaction-based traffic, the destination assignment of some transactions will change. This may cause some MSUs of the transaction to be directed to one destination and some to another destination.

If all RC groups in a MAP or MRN Group are Threshold-Prohibited, traffic loss will occur, even though some entities within the group are available. The decision to avoid congestion takes precedence over the routing all traffic.

GTT LOAD SHARING TO 32 DESTINATIONS

The GTT Load Sharing to 32 Destinations feature increases loadsharing destinations for intermediate and final GTT from 8 to 32 destinations. The feature allows each Mated Application Table (MAP) set or Mated Relay Node (MRN) set that is used for loadsharing to be associated with up to 32 destination point codes in the EAGLE Destination table. The support of 32 destination point codes does not increase the maximum number of supported entries in the MAP table or MRN table.

HEX DIGIT SUPPORT FOR GTT

Description

The Hex Digit Support for GTT feature enables the EAGLE to process both ANSI and ITU Message Signaling Units (MSUs) that contain either decimal or hexadecimal Global Title digits (0-9, a-f, A-F) in the Called Party Address (CdPA) field.

When the Hex Digit Support for GTT feature is enabled and turned on, any of the following three scenarios are possible:

- » Incoming MSUs whose digits equal 10 are matched to a global title translation that contains a single GTT table entry of GTA=10.
- » Incoming MSUs whose digits equal 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30 are matched to GTT table entries with a range of GTA=20 and EGTA=30.
- » Incoming MSUs whose hexadecimal digits equal 2A, 2B, 2C, 2D, 2E, 2F are matched to GTT table entries with a hexadecimal range of GTA=20 and EGTA=30.

If desired, the user can then split the hexadecimal range into three separate GTT table entries and specify translation data for hexadecimal digits as follows:

- » GTA=20 EGTA=29 with existing translation data
- » GTA=2A EGTA=2F with user specified translation data
- » GTA=30 with existing translation data

Before the Hex Digit Support for GTT can be enabled and turned on, the GTT feature must be turned on.

When enabled and turned on, the Hex Digit Support for GTT feature enhances the functionality of the following features:

- » ANSI-ITU-China SCCP Conversion: When the Hex Digit Support for GTT and the ANSI-ITU-China SCCP Conversion features are enabled and turned ON, the values specified for the npds and nsds parameters can be either decimal digits (0-9) or hexadecimal digits (0-9, a-f, A-F).
- » Enhanced Global Title Translation (EGTT): When the Hex Digit Support for GTT and the EGTT features are enabled and turned ON, the values specified for the gta, egta parameters in the gta command, can be either decimal digits (0-9) or hexadecimal digits (0-9, a-f, A-F).
- » Global Title Translation (GTT): When the Hex Digit Support for GTT and the GTT features are enabled and turned ON, the values specified for the gta and egta parameters in the gtt commands, can be either decimal digits (0-9) or hexadecimal digits (0-9, a-f, A-F).

- » Modified Global Title Translation (MGTT): When the Hex Digit Support for GTT and the MGTT features are enabled and turned ON, the values specified for the npds, and nsds parameters in the gta/gtt commands, can be either decimal digits (0-9) or hexadecimal digits (0-9, a-f, A-F).
- » Origin-based SCCP Routing (OBSR): When the Hex Digit Support for GTT feature and the OBSR features are enabled and turned ON, the values specified for the cdpa gta/egta and cgpa gta/egta parameters can be either decimal digits (0-9) or hexadecimal digits (0-9, a-f, A-F).

For more information about how to configure the EAGLE and its database to implement the above listed features, refer to the Database Administration Manual – Global Title Translation for this release.

Limitations

The configuration of the Hex Digit Support for GTT feature may exceed the 150-character command-length limit per entry. Configure the feature in stages as necessary.

FALL-BACK TO GTT AFTER LNP MR SERVICE

Fallback to GTT

To take advantage of screening functionality provided by GTT Actions feature for non-GTT Message Relay Services, user is allowed to provision GTT Required, GTT Selector ID (SELID) and Default Action parameters for corresponding Service Selector entry in the database, as shown below.

Table 10: Message Relay Services and GTT Actions

GTA/GTII/GTI N/GTIN24	Translation Type	Numbering Plan	Nature of Address Indicator	SSN Number	Service	GTT Req'd	SELID	Default Action
4	1	1	2	4	HLR Router	YES	100	Fall through GTT or Discard/UDTS/TCAP Error GTT Action Id or Fallback to EPAP/PPSOPTS Routing data

The “GTT Required” option indicates whether GTT needs to be performed after successfully finding the routing data from RTDB or PPSOPTS database for non-GTT Message Relay Services. If the routing data is not found for non-GTT Relay Services from RTDB or PPSOPTS database, the standard “Fall through GTT” procedure shall be executed.

Fall-back to GTT Description

Fall-back to GTT after non-GTT Message Relay Services functionality (hereafter referred to as Fall-back to GTT) provides a generic mechanism to perform GTT on the Service Relayed MSU. Fall-back to GTT functionality is achieved by providing support to provision a new optional parameter ‘GTT Required’ on per Service Selector basis for non-GTT Message Relay Services. ‘GTT Required’ option in the Service Selector can be provisioned to indicate if GTT shall be performed on the Service Relayed MSU after the successful execution of non-GTT Message Relay Services.

Table 11: Service Name and Corresponding Feature which may relay MSU

Service Name	Corresponding Feature which may relay MSU based on RTDB/PPSOPTS data
MNP	GSM MNP (Part Number: 893-0172-01) ANSI41 MNP (Part Number: 893-0166-01) IS41 GSM Migration (Part Number: 893-0173-01)

SMSMR	Prepaid SMS Intercept Ph1 (Part Number: 893-0067-01)
HLR Router	HLR Router MAP Layer Routing (Part Number: 893-0217-01) HLR Router (Part Number: 893-0219-01)
INPMR	INP (Part Number: 893-0179-01)
IDPR	IDP A-Party Routing (Part Number: 893-0333-01) IDP Service Key Routing (Part Number: 893-0336-01)
TTR	For IS41 (ANSI TCAP) messages selected for this service, the 'GTT Required' option shall have no effect. For GSM (ITU TCAP) messages selected for this service, the 'GTT Required' option shall have same effect as for IDPR service.

The 'GTT Required' parameter shall be examined only if message is required to be relayed based on routing data from RTDB/PPSOPTS table after the successful execution of a non-GTT Message Relay Service. lists the non-GTT Message Relay Services and the corresponding feature(s) which may result in message relay based on routing data from RTDB/PPSOPTS table. Existing behavior of the service shall remain unchanged if 'GTT Required' parameter in the concerned Service Selector indicates that GTT is not required on the Service Relayed MSU. If 'GTT Required' parameter indicates that GTT is required on Service Relayed MSU, then GTT shall be performed on the MSU modified by Relay Service according to GTT hierarchy of the incoming link set. The default value of 'GTT Required' shall be set to indicate that GTT is not required on Service Relayed MSU. If GTT performed on the Service Relayed MSU is successful then all the GTT features including GTTMOD, GTT Action, ANSI/ITU/CHINA SCCP Conversion and EGMS shall be performed on the message.

Note: Fall-back to GTT functionality is applicable only to the Service Relayed MSU. Query/Response and standard Fall Through to GTT procedures are not in the scope of Fall-back to GTT functionality.

Exceptions to Fall-back to GTT

If a service performs GTT on service specific parameters to obtain information required for message routing (for example "MO SMS B-Party routing" in SMSMR Service finds routing information by performing GTT on CDPN) then Fall-back to GTT functionality shall not be applied on those messages. These exceptions to Fall-back to GTT functionality are listed below.

Table 12: Exceptions to Fall-Back to GTT functionality

Service Name	Feature Name	Exception Description
MNP	IS41 GSM Migration (Part Number: 893-0173-01)	IGM SRI_SM Relay to Default IS41 SMSC functionality relays the message to the default IS41 SMSC based on GTT translation of GTA defined by GSMOPTS:DEFIS41SMSC.
	MT-Based GSM SMS NP (Part Number: 893-0200-01)	MT SMS SRI_SM Relay to Default IP SMSC functionality relays the SRI_SM message to the default IP SMSC based on GTT translation of GTA defined by GSMSMSOPTS:DEFIPSMSC.
	All features under MNP service.	MNP service allows re-routing of messages when the service is OFFLINE. In such case, a GTT parameter is already present that specifies whether GTT is required when the service is OFFLINE.
HLR Router	All features under HLR Router service.	HLR Router service allows re-routing of messages when HLR ROUTER service is OFFLINE. In such case, a GTT parameter is already present that specifies whether GTT is

		required when the service is OFFLINE.
SMSMR	MO SMS B-Party Routing (Part Number: 893-0246-01)	MO SMS B-Party Routing performs GTT on TCAP B-Party digits (TCAP CDPN) and routes the message based on the GTT translation results.

Service Selector search is not performed for the MTP-routed messages with CDPA GTI=0. Therefore, the parameters required to perform Fall-back to GTT functionality are not available for MTP-routed messages with GTI=0. The Fall-back to GTT on Service Relayed MSUs shall not be applicable on messages with GTI=0 i.e. if a message with GTI=0 is relayed by EPAP-related service, then GTT shall not be performed on the message.

Pre-LNP QS and Post LNP MR GTT

Currently there is no option to do GTT prior to LNP QS lookup or fall-back to GTT after successful completion of the LNP MR service. There is a need to do Pre-LNP lookup GTT based screening for LNP QS and the ability to fall-back to GTT after LNP MR. Two use-cases are shown below one for Pre-LNP GTT based screening (PR# 128288) and the other for Post-LNP GTT based screening (PR# 128289).

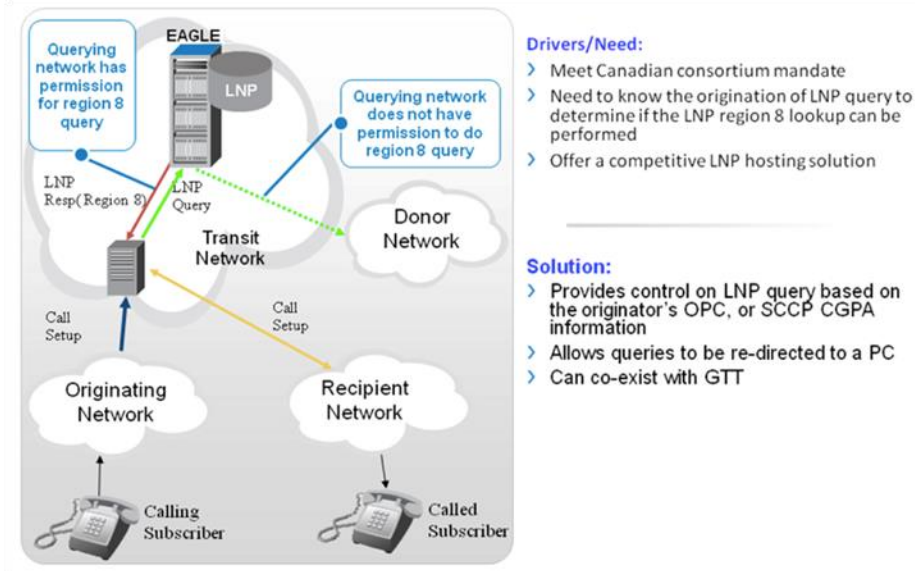
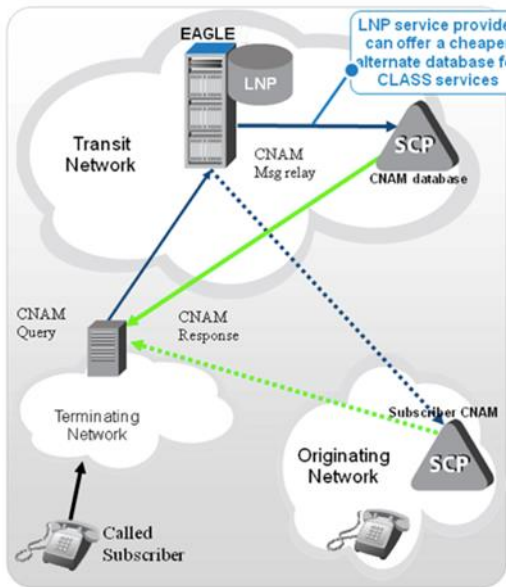


Figure 41: Origin based LNP QS call flow with Pre-LNP GTT processing

In the case of QS, we would potentially need to do Calling party based GTT prior to doing the LNP RTDB lookup. In the use case cited above, if a calling party has an agreement with the LNP provider, the region 8 LNP RTDB lookup is performed. Else the query gets forwarded to the donor network for the LNP lookup.



Drivers/Need:

- > Need to know the origination of LNP query to determine alternative database or optimal routing to destination
- > Offer a competitive LNP hosting solution

Solution:

- > Provides control on LNP message based on the originator's OPC, or SCCP CGPA information
- > Capability to fall-back to GTT post LNP Message Relay processing

Figure 42: LNP MR with fall-back to GTT post processing

The figure above shows the use case for LNP MR with fall-back to GTT processing. For example the initial message selection can be done using FLOBR after which this enhancement adds the capability to fall-back to GTT post processing.

SUPPORT FOR J7 (JAPAN SS7)

Support for J7 (Japan SS7)

SS7 networks in Japan are not using the standard ITU-N formats and procedures - the Japanese Telecom authority (TTC) has modified the ITU specifications to suit the Japanese telecom signaling needs. For example the 16-bit point code format and 48 bits (or 40 bits based on SI value) MTP3 routing label is used in Japanese telecom network signaling. Currently the EAGLE product doesn't support the modifications standardized by TTC.

The initial software release (R45.1) supporting J7 over Sigtran transport on the EAGLE will have conformance as detailed in this document, to the MTP3 layer (JT Q.704) and SCCP layer (JT Q.711), protocols. The next software release adds supporting J7 over E1/T1 transport (J1), as detailed in this document, to the MTP1/MTP2 layers (JT Q.703/JT G.703/JT G.704).

A new on-only PN: 893-0408-01 will be used to control "J7 support" feature".

The following table lists signaling layers/protocols supported and not supported for J7 feature:

Table 13: J7 Features and Support

From (i/c)	To (o/g)	'To' Details	Supported?
ITU-T TDM	TTC TDM	TTC SCCP, TTC MTP3, MTP2, J1-64 Kbps	Yes
ITU-T TDM	Sigtran (w/16 bit PC support)	TTC SCCP, M3UA (16 bit PC), SCTP	Yes
		TTC SCCP, TTC MTP3,	Yes

		M2PA(16 bit PC), SCTP	
ITU-T Sigtran	Sigtran (w/ 16 bit PC support)	TTC SCCP, M3UA (16 bit PC), SCTP	Yes
		TTC SCCP, TTC MTP3, M2PA (16 bit PC), SCTP	Yes
ITU-T Sigtran	TTC TDM	TTC SCCP , TTC MTP3, MTP2, J1-64 Kbps	Yes

DATABASE SERVICES

The EAGLE is capable of providing integrated database services typically associated with a SCP or standalone application server. The integration of these applications with the core EAGLE infrastructure and STP functionality allows database services to run at high transaction rates with very high reliability. EAGLE supports the following database services:

- » Query-based Number Portability Solutions (Fixed or Mobile)
 - » NA LNP - North American Local Number Portability
 - » INP - INAP-based Number Portability
 - » AINPQ ANSI-41 NP Query
- » Mobile Number Portability Solutions
 - » GSM Mobile Number Portability
 - » ANSI-41 Mobile Number Portability
 - » IS-41 GSM Migration
- » Number Portability Solutions for Prepaid/Service Node Access
 - » GSM SRI Query
 - » GSM ATI Query
 - » IDP Relay
 - » IDP Relay for SMS
 - » IDP Screening
- » ISUP-interception-based Routing and Number Portability Solutions
 - » Triggerless ISUP Number Portability (TINP)
 - » TIF NP - Triggerless ISUP Framework Number Portability
 - » TIF Number Substitution
- » SMS Number Portability and Routing Solutions
 - » Prepaid SMS Intercept
 - » SMS Number Portability for GSM and IS41
 - » MO SMS IS41-to-GSM Migration
- » HLR Router
- » Voicemail Router
- » Equipment Identity Register
- » Supporting Functionalities
 - » SCCP Service Reroute
 - » MTP Messages for SCCP Applications

- » Multiple Local Subsystems
- » Additional Subscriber Data (ASD)
- » Numbering Plan Processor (NPP)
- » HomeSMSC "Match with Digits" Option
- » TCAP-Segmented SMS Phase 1

120M DN AND 120M IMSI VIA SPLIT DATABASE AND DUAL EXAP CONFIGURATION

EPAP and ELAP provide separate database for various features on EAGLE. Features like HLR ROUTER, MNP, EIR and TIF use the EPAP database. Features like LNP use ELAP DB. With the Dual ExAP Configuration feature, the EPAP-based features and ELAP-based features can be turned on (and process traffic) simultaneously on the same EAGLE.

Furthermore, customers using EPAP based features with subscription growth over 120M entries may expand EPAP data up to 240 million.

EAGLE supports the feature "EPAP Data Split" to control the RTDB split mechanism. Once the feature is turned ON, the service module card can be provisioned as either a DN card or IMSI card. On the DN card, DN, DN Block, ASD, and Entity data will be loaded, while on the IMSI card, IMSI, IMEI, IMEI Block, and Entity data will be loaded. The maximum of 120 million of DN data can be loaded on the DN cards while maximum of 120 million of IMSI on IMSI cards. Therefore the total maximum capacity of 240 million data can be supported system wide.

LIM cards will be responsible to determine which Service Module should process each MSU, requiring SCCP processing. This feature supports a maximum of 120 million of DN and 120 million of IMSI entries.

EPAP Database Expansion to 480M

The EPAP database expansion to 480M feature enhances the EPAP database capacity to allow configuring up to 240 million individual DN entries, 240 million individual IMSI entries and 48 million individual IMEI entries. Prior to EPAP release 16.1, the maximum number of individual DN and individual IMSI entries allowed was 120 million.

QUERY-BASED NUMBER PORTABILITY SOLUTIONS (FIXED OR MOBILE)

NA LNP - North American Local Number Portability

Local Number Portability (LNP) allows telephone subscribers to receive their telephone services from different switches belonging to different local exchange carriers within a rate center without having to change their telephone numbers. Oracle's LNP solution provides all the core functions of an STP, in addition to hosting local subsystems to support TCAP query/responses. The EAGLE LNP solution provides the appearance of a service control point (SCP) to other SCCP and TCAP applications residing in other network elements. This includes local SCCP subsystem management, automatic call gapping, and TCAP error handling procedures.

The two primary functions of LNP supported by the EAGLE are Location Routing Number (LRN) query and Message Relay (MR) function.

The LRN query function is required when a call is placed to a ported telephone number. A query is sent to the LNP database to obtain the LRN. The LRN gives the location of the new office switch on which the telephone number resides. When a response to the query is returned, the call is completed using the LRN to route the call to the new switch. LRN query processing services LRN queries in real time and generates the appropriate LRN response.

The Message Relay function is required to perform 10-digit LNP GTT for various services while maintaining backward compatibility with existing non-LNP Operations Support Systems (OSSs). Currently, OSSs (and some switches) use 6-digit GTT for certain services. To minimize the impact of LNP on these systems, they continue to

route using 6-digit GTT. If the called party address does not include 10 digits, the 10 digits are extracted from the TCAP portion of the message and are used as a global title address (GTA).

The EAGLE LNP solution allows service providers a seamless growth path to meet industry requirements. LSMS sends data to the Real-time Database (RTDB) on the ELAP subsystem. The RTDB is then loaded to all SCCP service modules in the EAGLE. The figure below shows a high level architecture of the EAGLE LNP architecture.

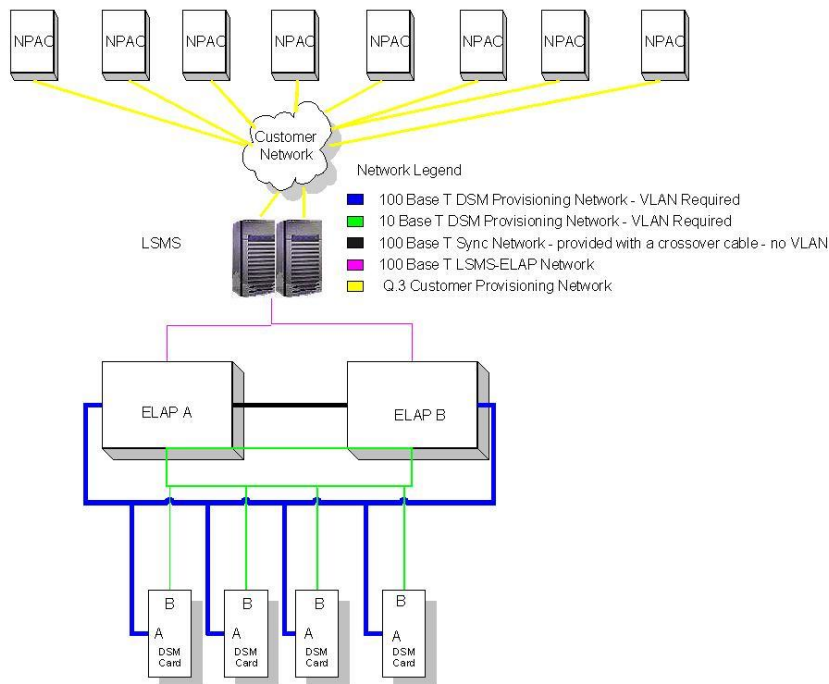


Figure 43: EAGLE LNP Architecture

The EAGLE with LNP functionality provides these capabilities:

- » Support for up to 504 million ported or pooled numbers.
- » Support for up to 40,800 transactions per second.
- » Support for up to 200,000 LNP override GTTs and 350,000 LNP Default GTTs.

Override GTTs are global title translations provisioned on a per LRN basis that take precedence over the GTTs in the subscription version (TN record) from the NPAC/LSMS. Default GTTs are GTTs used for non-ported numbers.
- » LNP Query processing functions required for call completion to ported numbers in either the AIN, IN, ANSI-41, or PCS 1900 query format.
- » AIN/IN node overload control using nodal based automatic call gapping (ACG-NOC) and manually initiated controls (ACG-MIC).
- » Enhanced GTT routing (LNP message relay) to support the five services associated with ported numbers (LIDB, CLASS, CNAM, ISVM, WSMSC).
- » 10-digit intermediate and final GTT.
- » 10-digit GTT services with only a 6-digit global title address included in the SCCP header
- » 6-digit default GTT for a non-ported directory number in a ported NPA-NXX
- » 2 methods of elimination of SCCP looping:
 - » using post-GTT gateway screening and capability point codes to prevent SCCP circular routing (preferred).
 - » replacing the translation type while routing to a gateway STP of an interconnecting network.

- » Replacing a global title address with a location routing number (LRN) to eliminate the need for 10-digit final GTT at the destination network
- » SSN management of remote applications for which a 6-digit or 10-digit final GTT is done
- » GTT for LNP queries and LNP query processing can be performed on the same node.
- » Non-LNP GTT and LNP GTT can both be performed by the EAGLE.
- » Query on release, originating, N-1, and terminating switch triggers are supported.

Database and Provisioning

There are several different types of data utilized in providing the LNP query and message relay functions. Most of this data is administered from the LSMS. System configuration and options related to the LNP function are administered at the EAGLE. LNP Data Flow shows the architecture of the data management system used to send the LNP data to the EAGLE from the NPAC SMS. The EAGLE LNP data is stored in the Real-Time Database (RTDB) on the ELAP and is downloaded to all SCCP service module cards on the EAGLE for data management. The ELAP provides an emergency provisioning interface in the event data cannot be received from the LSMS but is not shown in LNP Data Flow.

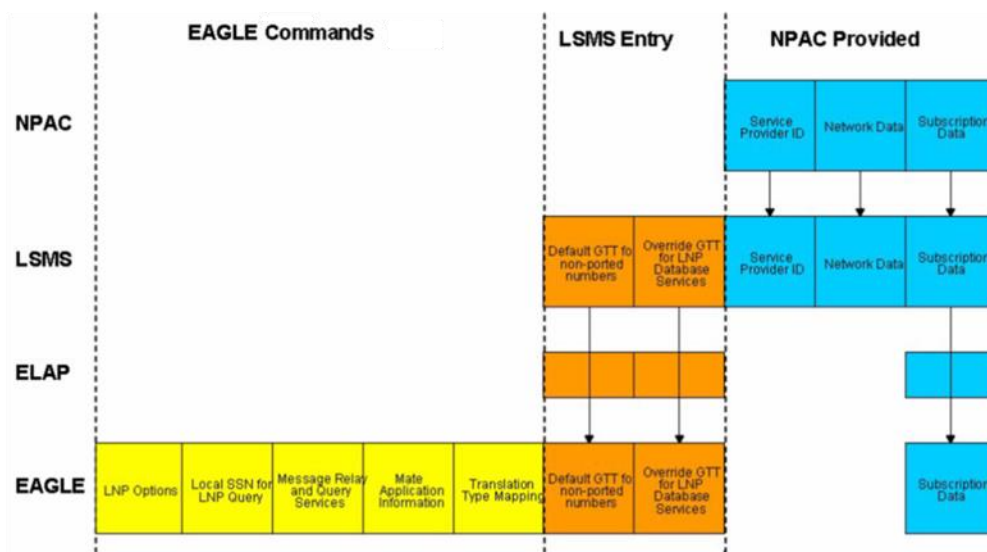


Figure 44: LNP Data Flow

The following provides a brief description of the LNP data that is contained in the EAGLE RTDB:

- » Subscription versions - These are the ported or pooled telephone numbers with related information that is sent from the NPAC to the LSMS and then to the EAGLE RTDB. Each subscription version at the EAGLE contains:
 - » 10-digit telephone number (TN)
 - » Location routing number (LRN)
 - » GTT data (DPC/SSN, routing indicator, etc.) for CLASS, LIDB, CNAM, ISVM, WSMSC
 - » Service provider ID-support for Mass Update of SPIDs which allows a bulk change of which service providers own which LRNs.
- » Default GTT for Message Relay for each portable NPA-NXX for CLASS, LIDB, CNAM, ISVM, and WSMSC - This data is used for GTT routing for non-ported numbers and is provisioned at the LSMS.
- » Default GTT for LRN queries for each portable NPA-NXX - Default GTT if the AIN/IN LRN query should be processed locally or routed to another node for processing. This data is provisioned at the LSMS.

- » LRN Override GTT for CLASS, LIDB, CNAM, ISVM and WSMSC - This data overrides the global title data in the subscription versions for the specified LRN. This allows gateway addresses to be provided to the NPAC for subscriptions, and allows the provider to override the gateway data for LRNs within their own network. If the GTT is a final GTT, then the mated application and related data (loadshare mode, concerned point code list, etc.) corresponding to the GTT data are provisioned at the EAGLE.
- » NPA-NXX requiring SCCP message relay service at the EAGLE - This data is provisioned at the LSMS.
- » An indication for each translation type (applicable for only ported NPA-NXXs requiring LIDB, CLASS, ISVM, WSMSC and CNAM message relay service) indicating whether the SCCP called party address (CdPA) includes 10-digits - This data is administered at the EAGLE.
- » NPA Split Data - This is used to identify the old NPA-NXX and new NPA-NXX so that calls are handled properly during the permissive dialing period. Splits are provisioned at the LSMS on a delayed order basis and forwarded to the EAGLE when the split becomes active.

Parameters required to customize LNP query and response processing are configured on each EAGLE and include:

- » AMAsIpID value
- » Indicator to include or exclude AMAsIpID parameter in the AIN response
- » Billing indicators (call type and feature ID) for the IN connection control response
- » 3- or 4-digit CIC for IN connection-control response

LSMS Interface

The service provider maintains and distributes LNP data to the EAGLE RTDB by using the Local Service Management System (LSMS). The LSMS provides the interface between the Number Portability Administration Center Service Management System (NPAC SMS) and the EAGLE RTDB. The data administered by the LSMS includes subscription, service provider, and network data (Override GTT, Default GTT, and NPA Splits).

LNP Data Audits/Reconcile/Loading

The Oracle LNP solution supports a variety of database audits/reconciles and loading the different modules for the LNP solution.

LSMS-ELAP Audit/Reconcile/Loading

Refer to ORACLE COMMUNICATIONS LOCAL SERVICE MANAGEMENT SYSTEM (LSMS) (NORTH AMERICAN).

ELAP-Service Module Audit/Reconcile/Loading


The ELAP-to-Service Module (SM) interface allows for rapid loading of the SM cards. Auditing and reconciling LNP data is automatic and does not require any user intervention.

The ELAP downloads LNP data to each SM card with a checksum. After receiving the LNP data, the SM card recomputes the checksum and, if the two checksums do not match, the SM card automatically requests a new update from the ELAP.

Each SM card can continue to receive updates from the MPS when a particular SM card needs to be reloaded. Each SM card can also retain its RAM-based data as long as power is not removed from the card (warm restart). Each SM card can reload LNP data rapidly if the SM card loses power (cold restart).

LNP Query

LNP Query functionality allows a call to be completed to a ported number, which is a telephone number that has been moved from one switch to another. When a call is placed to a portable telephone number, a trigger is set at the office switch and a query is sent to the LNP database to obtain the location routing number (LRN). The LRN gives



the location of the new switch on which the telephone number resides. When a response to the query is returned, the call is completed using the LRN to route the call to the new switch. To implement this capability, these features are required:

- » LRN query processing - services LRN queries in real time and generates the appropriate LRN response. Multiple query types are supported.
- » Automatic Call Gapping (ACG) control - Automatic call gapping is required for overload control when an excessive number of LRN queries are received on a nodal basis for a specific number of digits or for a specific set of dialed numbers. ACG controls are placed only on AIN and/or IN queries.

LRN Query Processing

The ELAP provides Location Routing Number (LRN) query services for wireline and wireless switches. AIN, IN, ANSI-41, and PCS query/responses formats are supported either by explicitly defining a translation type for the query or using the TT Independence for LNP Queries feature. The LRN query processing decodes the incoming query, performing appropriate TCAP error checking and return procedures. For a properly formatted query, the EAGLE locates the 10-digit TN and searches the LNP database for a match. If a match is found, the LRN is returned. Otherwise, the appropriate return for a non-ported TN is sent for the specific protocol.

Triggerless LNP

In addition to the mentioned LRN query formats supported, the EAGLE LNP solution also offers a triggerless LNP solution. For certain network configurations, triggerless LNP offers service providers a method to route calls to ported numbers without having to upgrade their switch (end office or mobile switching center) software to support LNP triggers. Triggerless LNP will selectively intercept IAM messages, via Gateway Screening, based on user configuration. For IAMs that have not had the LRN query performed, the LRN lookup is performed, and the IAM is modified appropriately for a ported or non-ported number based on the lookup results. Triggerless LNP requires the use of a Tandem Office switch in the call flow.

Automatic Call Gapping (ACG)

Automatic call gapping controls the rate at which location routing number (LRN) queries for a specified telephone number or a portion of a telephone number are received by the EAGLE when predefined thresholds are reached. ACG components are only defined for AIN and IN LRN responses. When conditions warrant, the LNP application will send ACGs as part of the AIN or IN LRN query response to throttle queries from the SSPs. The ACG component is appended to the outgoing TCAP Response Package. ACG controls are used under two conditions:

- » Node Overload - When a node overload condition is detected and an ACG control is configured for that overload level, the EAGLE sends an ACG component within each LRN query response it processes. The ACG control can be set based upon 6 or 10 digits.
- » Manually Initiated Controls - The EAGLE also may send a manually initiated ACG to control the rate of queries for a particular area code (3 digits), area code and prefix (6 digits), 10-digit telephone number, or part of a 10-digit telephone number (6 to 10 digits). The database can contain a maximum of 256 manually initiated ACG controls.

Message Relay Services

Message Relay differs from the LRN query functionality in that no response is sent back to an end office. Instead, Message Relay is an intercept of a TCAP query message, performing a 10 digit GTT for supported NPAC services, and forwarding the query to the correct service provider database containing the service.

The Message Relay functionality performs the global title translation using the appropriate default GTT for non-ported numbers or GTTs in the subscription data for ported numbers. To implement this capability, the following functions are required:

- » Ported NPA-NXX detection - The EAGLE maintains a list of all ported NPA-NXXs for which the node must perform 10-digit GTT. The first pass search shows whether the number belongs to a ported NPA-NXX. If the number does not belong to a ported NPA-NXX, normal GTT is performed on the number. If the number belongs to a ported NPA-NXX, two options are available for performing LNP GTT:
 - » The EAGLE is not responsible for performing 10-digit LNP GTT. The EAGLE performs normal GTT which results in routing the MSU to an external LNP database (for example, an LNP SCP) or another STP.
 - » The EAGLE is responsible for performing 10-digit LNP GTT. This routes the MSU to the RTDB on the EAGLE for performing 10-digit LNP GTT.
- » Prevention of SCCP looping - The complexity of LNP data administration across multiple carrier networks increases the chances of data inconsistencies and may result in SCCP circular looping. The GTT feature has been enhanced to allow modification of the translation type (TT) and global title address (GTA) as a result of translation. The GTA may be replaced by the location routing number to a gateway STP of an interconnecting network. This function is optional and can be configured by the user. The EAGLE LNP solution also offers post-GTT gateway screening options which may be used to prevent SCCP circular routing.
- » 10-digit final LNP GTT - The EAGLE supports final GTT performed on 10 digits. When the STP performs 10-digit final GTT, it will be capable of supporting routing and management of mated databases. All existing functions (loadsharing between databases, primary/backup relationship between databases, remote subsystem management, translation type mapping, translation aliasing, etc.) are performed with the 10-digit final LNP GTT.
- » 6-digit default LNP GTT - If the 10-digit GTT does not find a match (for example, when a number is not ported but belongs to a ported NPA-NXX); the EAGLE performs a 6digit default GTT.

SCCP and MTP Management to Support LNP

When the RTDB goes offline, the EAGLE sends SSPs that causes messages with the routing indicator set to SSN to be diverted to the mate subsystem. These will not cause messages with the routing indicator set to GT to be diverted. In order to make other nodes divert the messages with the routing indicator set to GT to the mate, the EAGLE sends response method TFPs for these messages that require either message relay or LNP query.

There are two cases in which the EAGLE generates a response method TFP:


- » While the RTDB is offline, a message arrives with the routing indicator set to GT for one of the EAGLE' LNP capability point codes and the result of the GTT is the EAGLE RTDB.
- » While the RTDB is offline, a message arrives with the routing indicator set to GT for one of the EAGLE' LNP capability point codes and the result of the GTT is that message relay is required on the EAGLE.

In both of these cases, the EAGLE generates a TFP concerning the LNP capability point code and sends the TFP to the OPC in the message. This TFP should cause the OPC to divert traffic to the mate. If a message arrives with the routing indicator set to GT for the EAGLE' true point code, the EAGLE does not generate a TFP. Nodes that send LNP traffic to the EAGLE with the routing indicator set to GT should use one of the EAGLE's LNP capability point codes, not the EAGLE's true point code or an STP capability point code. The STP capability point codes should be used for any nodes that send non-LNP GTT traffic.

If the EAGLE receives an RSP (Route Set Test Message - Prohibited) for a capability point code that is used for LNP and the RTDB is offline, the EAGLE does not reply. If the EAGLE receives an RSR (Route Set Test Message - Restricted) for a capability point code for LNP and the LNP subsystem is offline, the EAGLE replies with a TFP concerning the capability point code. When the RTDB is online, the EAGLE replies to both RSRs and RSPs for a capability point code that is used for an LNP with a TFA.

Reporting LNP Status and Measurements

The EAGLE LNP solution provides users on-demand status of the RTDB. The EAGLE displays a detailed status of LNP information for the LNP system as a whole or for a given SM. The system-wide detailed report includes



information for each of the GTT, LNP message relay (LNPMR), LNP query service (LNPQS), Wireless (ANSI-41) LNP query service (WNPQS), PCS 1900 LNP query service (PLNPQS) and automatic call gapping (ACG) functions.

The EAGLE also provides a set of measurements related to LNP query and message relay traffic. These measurements include queries for ported numbers per LRN, queries for non-ported numbers per NPA-NXX, and ported and non-ported message relay GTTs received for CLASS, LIDB, CNAM, ISVM and WSMSC. These measurements are available hourly and daily. Daily measurements are maintained for one week.

AIN LNP Message Support

Introduced in Release 46.0, the AIN LNP Message Support feature extends support of a Local Number Portability feature to allow processing AIN messages using a Mobile Number Portability database. The AIN message types are managed using Query/Response architecture.

INP (INAP-based Number Portability) - ITU

There are varying methods for network operators to introduce number portability. Wireline providers will generally use an IN (Intelligent Network)-based solution using the INAP (IN Application Part) protocol. In some cases, wireless operators are also choosing to use an INAP-based approach rather than the 3GPP-defined “SRF” method. Both ETSI and 3GPP standards for Number Portability allow for an IN-based solution to be used at the operator’s discretion.

The EAGLE INP feature satisfies the ETSI-defined INAP-based NP solution. The INP function can be deployed in a node that also performs the STP function or as a stand-alone INP node. INP and North American LNP are mutually exclusive on an EAGLE node. INP can be run on the same node as MNP and HLR Router. Some wireless operators use a combination of INP and MNP to satisfy all call flows.

For database provisioning, the INP feature (as well as the MNP and HLR Router features) require deployment of the EAGLE Provisioning Application Processor (EPAP). The EPAP provides a centralized database for provisioning with automatic replication to redundant systems.

As of Release 40.0, INP supports non-segmented XUDT messages for both Query/Response and Message Relay service. Segmented XUDT continues to be unsupported.

INP Message Flow

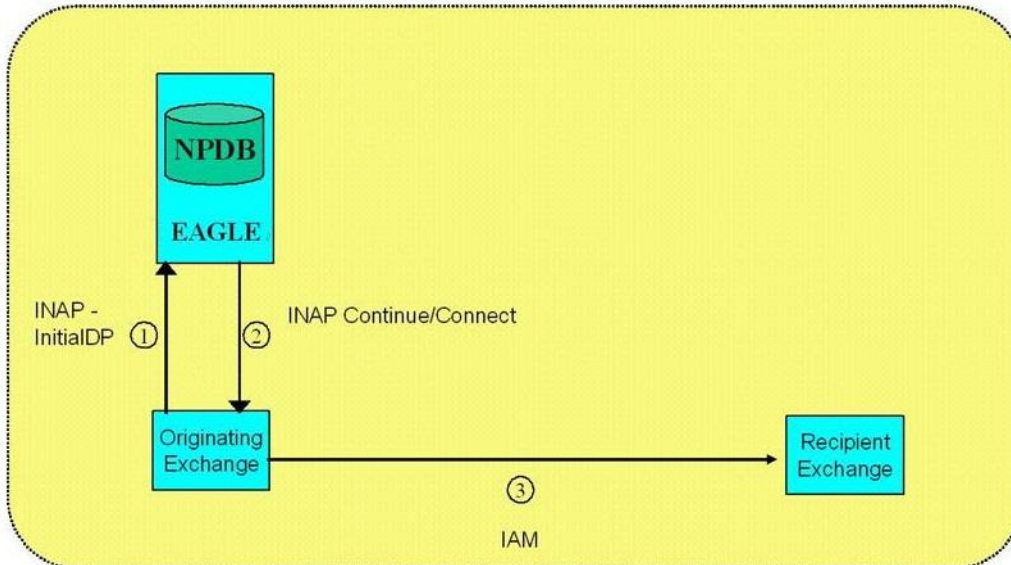


Figure 45: INP Call to a Non-ported Number

This figure shows an INP call to a non-ported or ported-in number:

- » The originating exchange sends an INAP InitialDP message to the EAGLE/INP. This message either comes into the EAGLE as route on SSN or GT information triggers INP call-related processing. The Called Party Number parameter contains the DN. The INP Number Normalization feature allows any unnecessary prefixes, for example, an access code 0 to be removed from the DN before the database is searched.
- » The EAGLE searches the NPDB with the DN and finds no match. The EAGLE either sends an INAP Continue message or an INAP Connect message to the originating exchange, depending upon the setting of the INP options within the EAGLE.
- » The originating exchange routes the call to the subscription network (which could be the originating network).

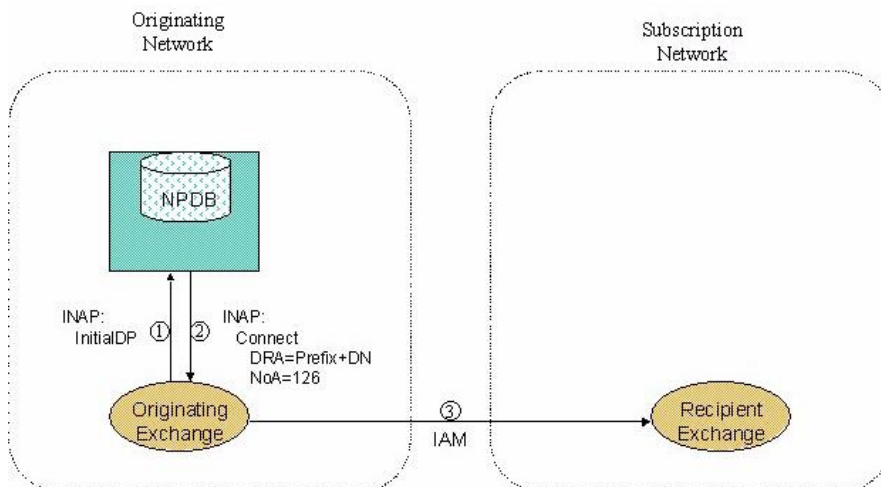


Figure 46: INP Call to a Ported Number

This figure shows an INP call to a ported number:

- » The originating exchange sends an INAP InitialDP message to the EAGLE/INP. This message either comes into the EAGLE as route on SSN or GT information triggers INP call related processing. The Called Party Number parameter contains the DN. The INP Number Normalization feature allows any unnecessary prefixes, for example, an access code 0 to be removed from the DN before the database is searched.
- » The EAGLE searches the NPDB with the DN and finds a match. An INAP Connect message is sent to the originating exchange with the Destination Routing Address = concatenated RN + DN, where the RN is found in the NPDB associated with the DN. The operator also has the option of sending the RN only. The nature of address (NoA) indicator will be set according to its provisioned value, which in this example is 126.
- » The originating exchange routes the call to the subscription network and/or exchange identified by the RN. In the case of an imported number, this would be in the same network as where the call was originated.

Note: In some cases, a two-step process could be used where the NP query in the originating network returns an RN that simply identifies an access point (e.g., gateway switch) in the subscription network. A subsequent NP query in the subscription network returns an RN that identifies the specific exchange of the subscriber. It is assumed that this second NP query in the subscription network does not include the RN (prefix) from the first query as part of the DN. Instead, the DN will contain the originally dialed number.

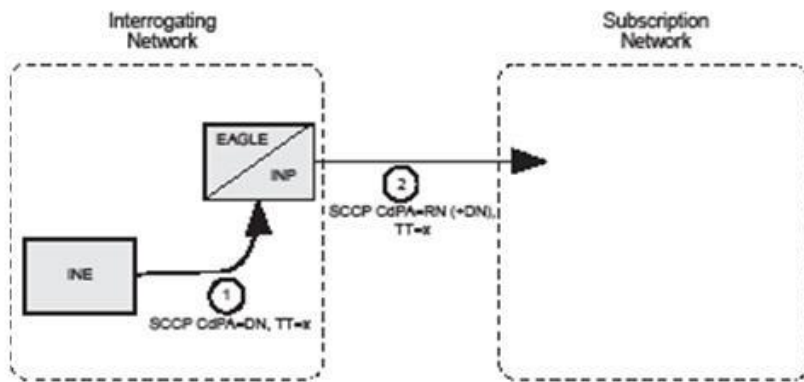


Figure 47: Non-Call Related Message for Ported Number Flow

The figure above shows a non-call related message for a ported number flow:

- » The Interrogating Network Entity (INE) sends the non-call related message to the EAGLE in the interrogating network. The SCCP CdPA contains the DN of the subscriber and the TT. The TT could be 0 or could have some other value depending upon the service, such as TT=17 for CCBS service.
- » Global title information triggers INP message relay processing. The EAGLE checks the leading digits of the SCCP CdPA to see if they contain the home network prefix if it has been provisioned. If so, the prefix is removed. The EAGLE then uses the DN from the SCCP CdPA to search the NPDB. A match is found, and the EAGLE uses the Message Relay GT address associated with the match to route the message to the designated node in the subscription network.

Although the figure above shows them as separate, the interrogating network could be the same as the subscription network.

INP Database

INP shares the same database features as MNP, HLR Router, EIR, and IS41 GSM Migration.

INP Assumptions/Limitations

The following assumptions and limitations apply to the INP feature:

- » The routing number (RN) found in the NP database will either be prefixed to the dialed number to form a new concatenated routing number to be returned to the switch, or will be sent on its own as the routing number.
- » The EAGLE will not send call gapping messages/components to the switch. In the event of EAGLE overload, some messages may be processed, while others are not (UDTS messages may be sent to switch). Call gapping is expected to be supported in a future release of INP.
- » The DN received in the INAP InitialDP message (Called Party Number) must be less than or equal to 15 digits.
- » INP will support only exact individual or range matches in the NPDB, based on the Called Party Number received in the query. Partial number matches with corresponding requests for additional digits by the EAGLE will not be supported.
- » INP will not support time activation of updates (e.g., for updates that are entered into the system along with a time value saying when they should go into effect).
- » INP will ignore the ServiceKey value in the INAP InitialDP message. It is assumed that queries received by the EAGLE addressed to the local INP subsystem are for INP, and there is no reason to look at ServiceKey.
- » The INAP Application Context Name (ACN) received by the EAGLE/INP from the SSP will be returned in the response. No checking for valid ACN values will be done.
- » In line with the ETSI standards, GSM operators who are using INP for call related messages will use the Signaling Relay Function (SRF) solution for non-call related messages. This feature will provide this non-call related message handling. MNP is not required.
- » Only one global title address per subscriber is needed for message relay.
- » The selector information in the SCCP CdPA that triggers INP call related processing is different than the information that triggers INP message relay processing.
- » When a selector combination points to INP call related, the EAGLE assumes the message is destined for the INP local subsystem and handles it accordingly. GTT is not actually performed on the message to derive the local subsystem.
- » INP responses (e.g., Connect) must be routed on subsystem number. They cannot be global title routed by the EAGLE.

INP Enhancements

INP allows a new option in the setting of the DRA parameter which is returned in INAP Connect messages. Prior, INP could return either the RN (for ported out) or SP (for ported in) from the RTDB in the IDP DRA parameter. Now, INP can return the RN for ported out, and one of two options for ported in: either the SP (HLR address) from the RTDB, or a HomeRN from the provisioned HomeRN list. If HomeRN is chosen, and if more than one HomeRN exists in the HomeRN table, INP will use the original HomeRN that was first provisioned in the table. Note that this refers to the first/original HomeRN that was provisioned in the HomeRN table, and not to the first HomeRN that is displayed in the output of the `rtv-homern` command. The EAGLE re-sorts the table each time a `rtv-homern` command is executed, and the first HomeRN displayed in this output may not necessarily correspond to the first HomeRN that was originally entered in the table.”

The Destination Routing Address (DRA) parameter (`chg-inpopts` command) has a new value (`homerndn`) that allows the return of the home routing number (HomeRN) in INP Connect Request messages. With this new value, INP allows the return of the routing number (RN) for ported-out numbers; and either the HLR address (SP) from the RTDB or the HomeRN from the provisioned HOMERN table for ported-in numbers.

If the HomeRN value is chosen, and if more than one HomeRN exists in the HOMERN table, INP will use the first HomeRN that was provisioned in the table. Note that this original HomeRN is not necessarily the first HomeRN that is displayed in the output of the `rtv-homern` command. The EAGLE re-sorts the table each time a `rtv-homern` command is executed.

```

rtrv-homern
rlghncxa03w 03-03-28 08:50:12 EST E
RN
-----
216780909087654 ----- first displayed
76345098
abc
abc1234
c10234567 ----- first provisioned
cabade

HOMERN table is (6 of 100) 6% full
;

```

Figure 48: INP Circular Route Prevention

5.1.2.5 INP Circular Route Prevention

The INP Circular Route Prevention feature detects and prevents circular routes for INPQ and INP MR Services. INPQ services are associated with received queries (InitialDP for INP-based queries or NPREQ for AINP-based queries) and the results are generated based on the RTDB lookup. INP MR services are associated with received INP queries that are related to the destination.

ANSI-41 INP Query (AINPQ)

ANSI-41 INAP Number Portability Query feature is an expansion of the INP Number portability solution. The AINPQ feature supports networks that require a number portability solution for a mix of ITU and ANSI-41 protocols in their network. This feature incorporates INP query (using inpq service selector or point code/subsystem) for ITU-N ANSI-41 NPREQ and additionally the existing INP queries for ITU-N and ITU-N24 INAP IDP message.

The addition of the AINPQ feature allows the INP message relay function to be invoked by either the INP or AINPQ feature. When the INP query is in operation it supports the following;

- » The handling of ITU national point code ANSI-41 NPREQ query encoded in ANSI-41 TCAP, ITU SCCP, and ITU MTP protocol stack.
- » ITU SCCP/MTP protocol validation and ANSI TCAP protocol validation for a received ANSI-41 NPREQ query.

The EAGLE performs number conditioning on the DGTSDIAL value in preparation for database lookup. The Called Party Prefix, National Escape Code, Service Nature of Address, Nature of Number, and Country Codes are used to condition the number as a National or International number. For a received ANSI-41 NPREQ query that requires INPQ processing, the EAGLE uses the digits encoded in the DGTSDIAL parameter for database lookup. Enhanced AINPQ and INP options for the Global Option for Connect on INP Query feature can be used to format information in the response that results from the database lookup.

Both INP and ANIPQ features use a common set of subsystem management, INP measurements, service selectors and INP options. The INP options in the EAGLE have been enhanced to support the AINPQ feature as follows;

- » A new INP option is provided to define the National Escape Code (NEC) value, up to 5 digits, for each EAGLE node.
- » Called Party Prefix has been increased to 40 entries from the original 5.
- » The destination routing address (DRA) options have been enhanced for INP and AINPQ for formatting the ROUTDGTGS parameter in the INP "Connect" message or AINPQ NPREQ "Return Result" response message, as follows:
 - » Support RN + [CDPNPFX] + DN in INP "Connect" or AINPQ "Return Result" response messages
 - » Support Routing Number in INP "Connect" or AINPQ "Return Result" response messages

Limitations and Considerations

- » The feature doesn't support NPREQ encoded in ANSI TCAP, SCCP and MTP protocol stack.
- » The EAGLE will discard ANSI-41 NPREQ queries encoded with ITU International point code in the MTP routing label.
- » AINPQ and EIR cannot be enabled in the system as the same time.

LOCREQ Query Response

The LOCREQ Query Response feature allows the EAGLE to respond to LOCREQ queries with a LOCREQ response message for both ported and non-porting subscribers.

The LOCREQ Query Response feature populates the RN of the ReturnResult message. Service Portability (S-Port) processing is used to control whether Generic Routing Number (GRN) or default RN digits are used for the RN in the ReturnResult message.

ENUM Query Response

The EAGLE is enhanced to support the ENUM interface to leverage the existing NP solution to provide Tier 1 lookup for ENUM queries. This can be positioned for operators looking for Tier1 lookup for supporting ENUM queries in their network to allow number portability in IMS networks.

The ENUM application supports an ENUM interface on UDP compliant to RFC 3403 and RFC 6166. This application supports:

- » Receiving ENUM queries from the ENUM client
- » Performing NP database lookups with the number in DNS format received in the ENUM query
 - » If a matching entry is found in the NP database, then a successful ENUM response is sent
 - » Otherwise, an error ENUM response message for cases with protocol errors

In addition a new database is created associating Tier 1 resource records and a destination number to a Tier2 name server. This overall solution provides the originating carrier only Tier 1 NAPTR records with the name of the Tier 2 ENUM server of the terminating carrier for a given destination number.

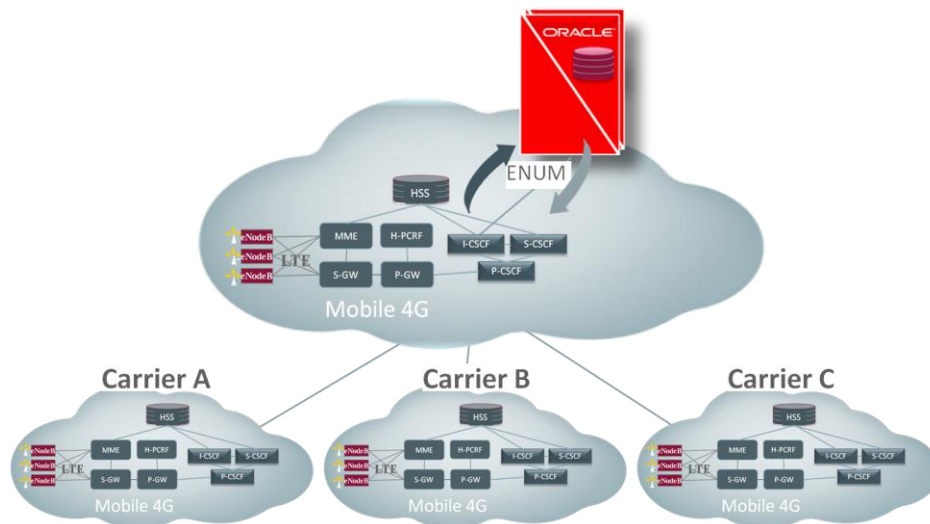


Figure 49 - ENUM Deployment Architecture

MOBILE NUMBER PORTABILITY SOLUTIONS

MNP GSM Mobile Number Portability

The Mobile Number Portability (MNP) feature implements number portability for GSM networks according to 3GPP 23.066, Signaling Relay Function (SRF) method. The focus is on service provider portability amongst GSM networks in a defined portability cluster, usually a country. With service provider portability, subscribers can change operators while retaining their MSISDN (Mobile Station international ISDN number) number. The MSISDN is the number dialed by someone trying to reach the subscriber. Their IMSI (International Mobile Subscriber Identifier) number is not portable. The IMSI identifies the SIM (Subscriber Identity Module) card which modularly plugs into the GSM handset.

The 3GPP standards have been defined so that GSM carriers can choose to implement IN-based (using INAP protocol) or SRF-based (using MAP protocol) MNP. SRF-based MNP processing involves the “intercepting” of existing MAP messages to check for ported numbers.

For call-related messages, MNP will act as an “NP HLR”, in the case where the number has been ported-out, by responding to the switch with a MAP SRI_ACK message. For calls to ported-in numbers and non-call related messages, MNP will perform message relay.

The 3GPP standards for SRF-based MNP define two routing options: direct routing and indirect routing. With direct routing, the network where the call is originated is responsible for determining whether the called party has ported and routed the call to the new subscription network. With indirect routing, this is the responsibility of the network that originally owned the number. MNP supports both direct routing and indirect routing.

The MNP feature incorporates a similar architecture to HLR Router. MNP is deployed in a node that is also performing the STP function. MNP, HLR Router, and INAP-based Number Portability (INP) can coexist on the same EAGLE node. MNP and North American LNP are mutually exclusive on an EAGLE node.

For database provisioning, the MNP feature (as well as the HLR Router and INP features) will require deployment of the EAGLE Provisioning Application Processor (EPAP). The EPAP performs function such as providing a centralized database for provisioning with automatic replication to redundant systems.

MNP Message Flow

Mobile Terminated Call to Non-Ported or Imported Number

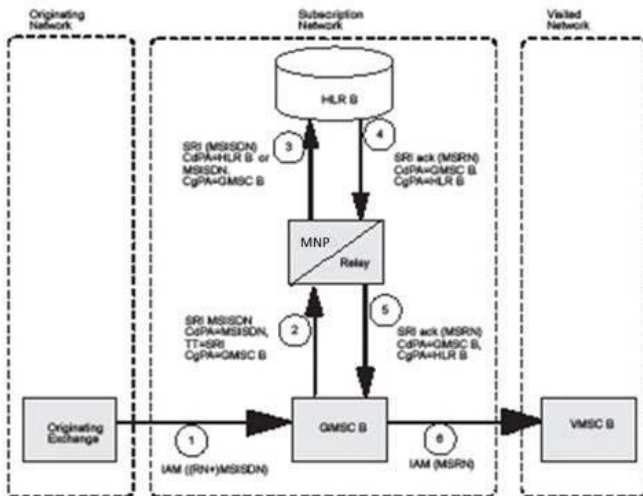


Figure 50: MT Call to Non-ported or Imported Number - Indirect Routing

This figure shows a mobile terminated call to a non-ported or imported number (indirect routing):

- » The originating exchange sends an IAM message to GMSC B in the subscription network. For the case where the number is imported, the original number range owner network would have performed an NP database lookup and determined the new subscription network (Routing Number - RN). As shown above, this could be sent in the IAM along with the MSISDN.
- » GMSC B sends an SRI request to MNP. Global title information triggers MNP processing. MNP determines that the message is an SRI and uses the MSISDN from the MAP message to search the MNP Database. A match is found with no Routing Number and an HLR GT address for HLR B; or no match is found and fall through to GTT produces routing to HLR B (another possibility is that GTT routes to some other node, possibly in a different network, which is outside the scope of this feature).
- » The message is routed to HLR B.
- » HLR B responds to GMSC B with an SR_ACK. This message can be GTT routed through the STP or MTP routed.
- » GMSC B sends an IAM with the roaming number to the visited network.

Mobile Call to Exported Number

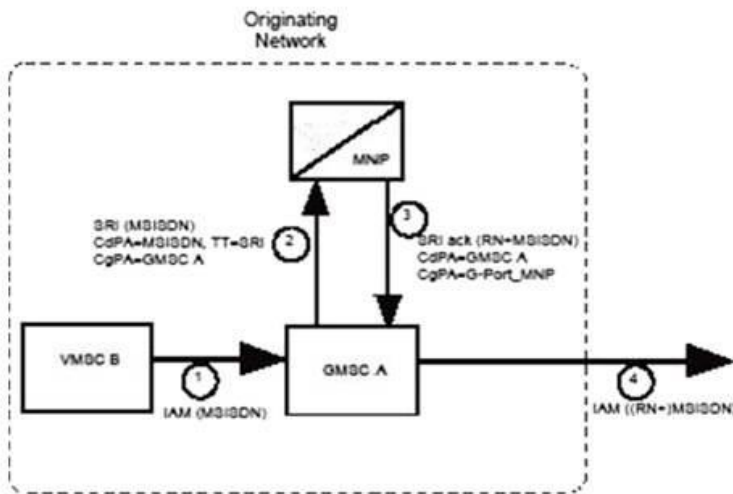


Figure 51: MO/MT Call to Exported Number - Direct Routing

This figure shows a mobile call to exported number (direct routing):

- » When the call is originated, VMSCB sends an IAM message to GMSC A.
- » GMSC A sends an SRI request to MNP. Global title information triggers MNP processing. MNP determines the message is an SRI and uses the MSISDN from the MAP message to search the MNP data base. A match is found with the Routing Number field populated.
- » MNP responds to GMSC A with an SRI_ACK message containing the Routing Number prefixed to the MSISDN number or the Roaming Number (shown as the Roaming Number above).
- » GMSC A sends an IAM with the roaming number to the subscription network. The Routing Number will be used by GMSC A, and possibly by transit exchanges, to route the call to the subscription network.

Note 1: This call flow assumes that the originating network does not equal the subscription network.

Note 2: If Indirect Routing was used in this case, the originating network would first route the call to the number range owner network (according to pre-portability rules), where MNP and NPDB would be accessed to find the Routing Number.

Mobile Call to Foreign Number Not Known to Be Ported

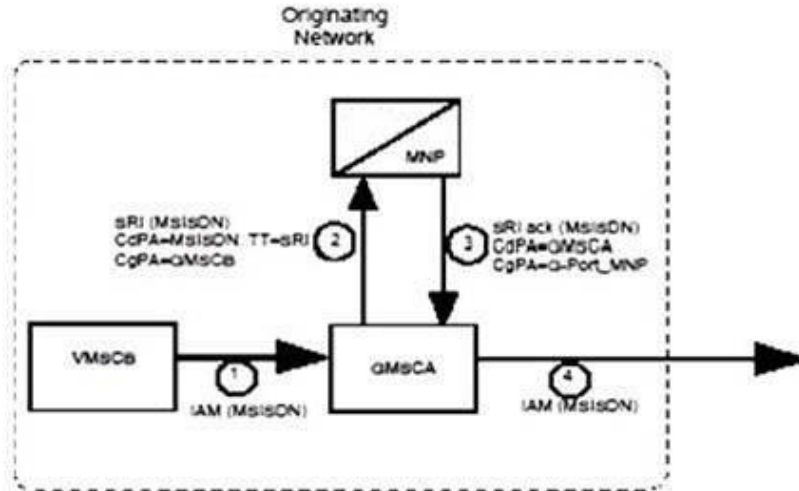


Figure 52: MO/MT Call to Foreign Number Not Known to Be Ported - Direct Routing

This figure shows a mobile terminated call to a foreign number not known to be ported (direct routing):

- » When the call is originated, VMSC B sends an IAM message to GMSC A.
- » GMSC A sends an SRI request to MNP. Global title information triggers MNP processing. MNP determines the message is an SRI and uses the MSISDN from the MAP message to search the MNP data base. A match is found, but the Routing Number and HLR Address fields are not populated.
- » MNP responds to GMSC A with an SRI_ACK message containing the MSISDN number with portability status associated with the MSISDN.
- » GMSC A sends an IAM with the roaming number to the subscription network.

Note: This call flow assumes that the originating network does not equal the subscription network.

Non-Call Related Message Flows

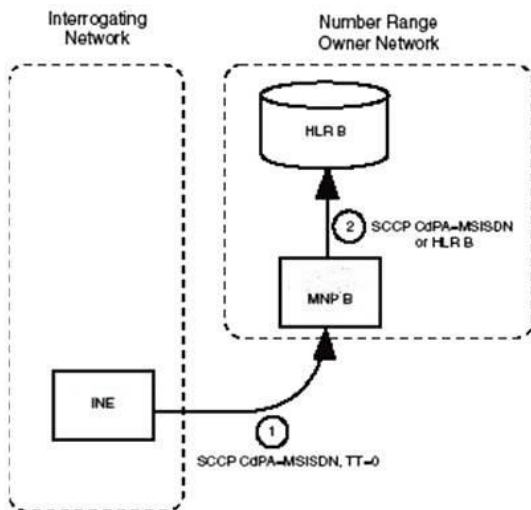


Figure 53: Non-CR Message for Non-ported Number - Indirect Routing

Above shows a non-call-related message for a non-ported number (direct routing):

- » The Interrogating Network Entity (INE) sends the non-call related message to MNP B in the number range owner network. The SCCP CdPA contains the MSISDN number of the subscriber and the TT. The TT could be 0, as shown above, or could have some other value depending upon the service, such as TT=17 for CCBS service.
- » Global title information triggers MNP processing. MNP B determines the message is non-call related (i.e., not an SRI that doesn't require Optimal Routing) and uses the MSISDN from the SCCP CdPA to search the MNP database. No match is found, so MNP B uses GTT to find the GT address associated with the MSISDN to route the message to HLR B.

The figure below shows a non-call-related message for a ported number (indirect routing):

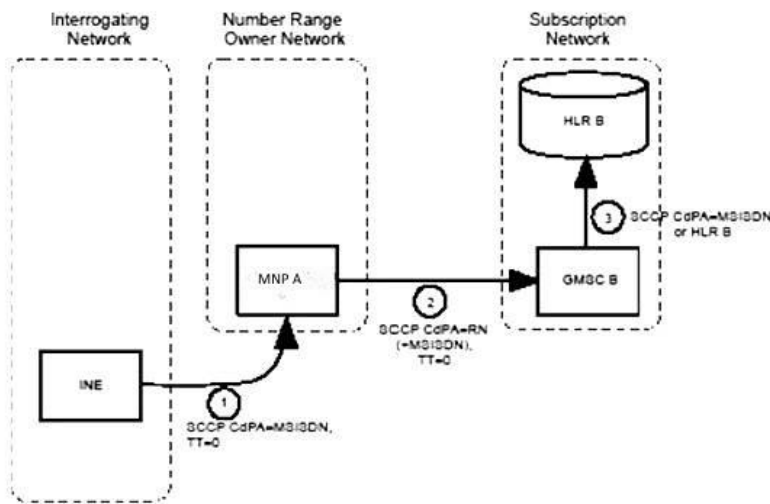


Figure 54: Non-CR Message for Ported Number - Indirect Routing

- » The Interrogating Network Entity (INE) sends the non-call related message to MNP A in the number range owner network. The SCCP CdPA contains the MSISDN number of the subscriber and the TT. The TT could be 0, as shown above, or could have some other value depending upon the service, such as TT=17 for CCBS service.
- » Global title information triggers MNP processing. MNP A determines the message is one requiring message relay (i.e., not an SRI that doesn't require Optimal Routing) and uses the MSISDN from the SCCP CdPA to search the MNP data base. A match is found and MNP A uses the Message Relay GT address associated with the match to route the message to the subscription network.
- » MNP B receives the message and determines the message is one requiring message relay (i.e., not an SRI that doesn't require Optimal Routing). It then checks to see if the SCCP CdPA begins with a Prefixed RN. If so, it removes the Prefix. Either way, it uses the MSISDN from the SCCP CdPA to search the MNP DATABASE. A match is found and MNP B uses the HLR GT address associated with the match to route the message to HLR B.

The figure below shows a non-call-related message for a ported or non-ported number (direct routing):

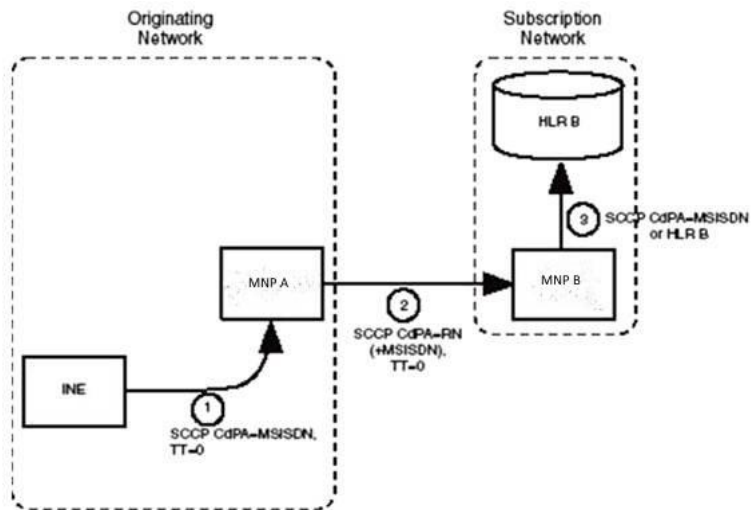


Figure 55: Non-CR Message for Ported or Non-ported Number - Direct Routing

- » The Interrogating Network Entity (INE) sends the non-call related message to MNP A in the interrogating network. The SCCP CdPA contains the MSISDN number of the subscriber and the TT. The TT could be 0, as shown above or could have some other value depending upon the service, such as TT=17 for CCBS service.
- » Global title information triggers MNP processing. MNP A determines the message is one requiring message relay (i.e., not an SRI that doesn't require Optimal Routing) and uses the MSISDN from the SCCP CdPA to search the MNP DATABASE.
- » If a match is found (ported case), then MNP A uses the Message Relay GT address associated with the match to route the message to the subscription network.
- » If no match is found (non-ported case), then MNP A uses GTT to route the message to MNP B.
- » MNP B receives the message and determines the message is one requiring message relay (i.e., not an SRI that doesn't require Optimal Routing). It then checks to see if the SCCP CdPA begins with a Prefixed RN. If so, it removes the Prefix. Either way, it uses the MSISDN from the SCCP CdPA to search the MNP DATABASE.

If a match is found (imported case), then MNP B uses the HLR GT address associated with the match to route the message to HLR B.

If no match is found, then MNP B uses GTT to route the message to HLR B.

Note: This call flow assumes the interrogating network does not equal the subscription network.

MNP Database

HLR Router and MNP utilize the same integrated database on the EAGLE (as do all of the EPAP-based Database Services features). Thus, MNP supports the following capacities, throughput, and functionality, similar to the HLR Router feature:

- » 120M individual DNs.
- » 50,000 DN ranges.
- » 5-15 digit hexadecimal DNs.
- » 1-5 digit hexadecimal Routing Numbers.
- » 5-15 digit hexadecimal "Signaling Point" (HLR) addresses.
- » Up to 75,000 TPS per node.

The MNP database is a feature-specific term for Oracle's Real-Time Database (RTDB), which is used by several number portability features.

- » Supports at least one message relay GT address (e.g., for Short Message Service (SMS), Support of Optimal Routing (SOR), Any Time Interrogation (ATI), Completed Call to Busy Subscriber (CCBS), etc.). This includes the ability to specify whether the RN should be prefixed onto the MSISDN in the SCCP CdPA of the outgoing message. The outgoing SCCP CdPA GTAI contents must be less than or equal to 21 digits.
- » Supports a portability status (0 - 255) for each subscriber record.

Note: Certain values have been assigned by ETSI. For example, 0 = not known to be ported; 1 = own number ported out; 2 = foreign number ported to foreign network.
- » Supports at least 256 ITU GTI 2 and 20480 ITU GTI 4 (5 unique values for NAI, 16 unique values for NP, and 256 unique values for TT) MNP selector combinations.
- » Provides control, via provisioning, for how non-international E.164 numbers will be converted to international numbers.
- » Provides, via provisioning, a new Nature of Address value and a new Numbering Plan value to be used for call-related responses (SRI ack) to the switch.
- » Provides, via provisioning, a new Nature of Address (NoA) value, a new Numbering Plan value, and a new TT to be used for non-call related message relay in the case where the number is ported. There must be one NoA value per Routing Number.
- » Scalable from 5000 to 75,000 queries per second.

MNP Assumptions/Limitations


The following assumptions and limitations apply to the MNP feature:

- » MNP as discussed in this document only applies within a single portability cluster. This is defined to be a set of networks in a country or multi-country region that has a common numbering plan and across which a subscriber, who is already inside the cluster, can port. Any individual MNP node is only required to support MNP within such a portability cluster.
- » It may be required for the EAGLE to look into the TCAP portion of the MAP message to determine the message type. Although 3GPP 23.066 defines a new Translation Type for SRI-MNP messages, MNP does not rely upon the use of this new TT.
- » The routing number found in the NP database will either be prefixed to the dialed number to form a new concatenated roaming number to be returned to the switch or will be sent on its own as the roaming number.
- » No MAP overload procedures, as defined in 3GPP 29.002, need to be supported by MNP.
- » No MAP messages other than those addressed in this document need to be handled by MNP in relation to Number Portability.
- » All non-call related messages impacted by MNP will contain the MSISDN number in the SCCP CdPA. In the case of the SRI message, it may be necessary to get the number from the MAP level.
- » TCAP op codes uniquely distinguish MAP SRI messages and do not change from one phase (or version) of MAP to another.
- » A routing number prefix could be required to be added to the SCCP CdPA contents for non-call related messages relayed by the MNP for ported subscribers. Such a prefix could also be received by the EAGLE in a message relayed from another operator. Such a prefix is shown by ETSI to be optional.

ANSI-41 Mobile Number Portability

This feature was developed for ANSI-41 markets (either in CDMA or TDMA) that have mobile number portability responsibilities in various regions around the world. As with MNP is for GSM networks, A-Port is the equivalent in the ANSI-41 domain. The ANSI-41 Mobile Number Portability (A-Port) feature enables an IS41 subscriber to change to a different service provider while retaining the same Mobile Dialed Number (MDN).

ANSI-41 MNP uses the EPAP (EAGLE Provisioning Application Processor) RTDB provisioning database to retrieve the subscriber portability status and provision directory numbers for exported and imported IS41 subscribers. This database maintains information related to subscriber portability in the international E.164 format. ANSI-41 MNP uses



RN (Routing Number) and Portability Type (PT) values to provision directory numbers (DNs) for exported subscribers. In addition, ANSI-41 MNP uses signaling point (SP) to provision DN for imported subscribers.

The ANSI-41 MNP message processing function mimics the MNP message processing function in that the EAGLE intercepts ANSI-41 LOCREQ and SMSREQ messages for the database lookup as opposed to SRI and SRI_SM for MNP. An IS41 LOCREQ message is initiated by a TDMA/CDMA MSC querying an HLR concerning terminating subscriber's subscription/location information for a voice call. An IS41 SMSREQ message is initiated by a TDMA/CDMA SMSC querying an HLR concerning terminating subscriber's subscription/current location information for delivering a short message.

ANSI-41 MNP Service Selection

Service selector lookup is performed using the MTP/SCCP data. If the selectors match and MNP service is assigned, A-Port handling is performed.

To manage number portability, ANSI-41 MNP uses the MNP SCCP Service Selector to process LOCREQ and SMSREQ SCCP messages. The EAGLE intercepts LOCREQ messages for the RTDB database lookup. An ANSI-41 LOCREQ message is initiated by a TDMA/CDMA MSC that queries the HLR for information regarding user subscription/location before terminating a voice call. ANSI-41 MNP supports both GT-routed and MTP-routed messages.

- » "GT-routed messages support UDT and non-segmented XUDT message types and perform service selector lookup after SCCP verification.
- » ANSI-41 MNP processes MTP-routed messages when used in conjunction with MTP Messages for SCCP Applications feature is turned on (see MTP Messages for SCCP Applications for further details).

ANSI-41 MNP begins TCAP/MAP verification if the message is ANSI TCAP and this verification is performed on all messages; only the ANSI TCAP format is supported.

The IGM, MNP CRP, and MT-based IS41 SMS NP features have been enhanced to support MTP-routed SMSREQ messages. If the SMSREQ message cannot be processed by any of these features, then the SMSREQ is MTP routed.

Database Lookup and Routing

The DN is used for database lookup.

- » For LOCREQ messages, the DN is derived based on the configured settings in the EAGLE "is41opts" options.
- » For non-LOCREQ messages, the DN is derived from the SCCP portion of the message.

ANSI-41 MNP performs number conditioning upon successful decode and verification of the message. HomeRN and IEC or NEC prefixes are removed. The DN is conditioned to international number format based on the service nature of address (SNAI or TCAPSNAI or MTPLOCREQNAI).

ANSI-41 MNP performs RTDB lookup on the conditioned number, and routes or relays the message based on the lookup result.

- » An SMSREQ message is relayed like any other non-LOCREQ message. No changes are performed to the TCAP/MAP portion of the message.
- » ANSI-41 MNP modifies the TCAP information for LOCREQ messages only when a HomeRN was deleted from the TCAP DN. Any gaps in the data caused by a change in field length will be resolved by shifting the remaining information up. Any IEC or NEC code is left.
- » ANSI-41 MNP falls through to GTT if number conditioning fails or does not find the DN in the RTDB database, or the DN is found with non-A-Port data.

- » If a HomeRN is detected in the Called Party and a matching DN with RN is found in the database, the EAGLE generates UIM (internal error message), indicating detection of circular routing, and routes the message using normal routing if both the MNP Circular Route Prevention feature and the IS41 GSM Migration feature are active.
- » Normal routing is performing GTT if the incoming message is sent to the EAGLE Self Point Code. Normal routing is routing the message to the MTP DPC if the incoming message is MTP-routed (the MTP DPC of the message is not the EAGLE Self Point Code).

ANSI-41 MNP shares the service state and re-route with the IS41 GSM Migration feature and the MNP feature, under one service called the MNP service state. (The MNP service state is used if only the MNP feature is on.) A-Port supports re-route functions as part of MNP service re-route. Alternate PCs are shared by all three features.

Measurements

The following enhancements support the collection and retrieval of measurements related to the A-Port feature. These measurement registers are supported with and without the Measurements Platform feature enabled.

New registers are added to the NP SSP reports; Hourly Maintenance Measurements on NP SSP (MTCH-SSP) and Daily Maintenance Measurements on NP SSP (MTCD-SSP).

Table 14: Measurement Counters for A Port

Peg Count Name	Description
APLRACK	Number of call related LOCREQ messages acknowledged.
APLRRLY	Number of call related LOCREQ messages relayed
APNOCL	Number of non-call non-LOCREQ related messages relayed.
APNOCLGT	Number of non-call Non LOCREQ related messages that fell through to GTT.

Feature Interactions

MNP and IS41 GSM Migration solve the problem of number portability from one network to another or number migration from one mobile protocol to another. One, two, or all three features could be active on a single EAGLE node at a given point. Because all of these features could have same type of MTP and SCCP layers (ITU or ANSI), it may look like same kind of message at service selection, which looks at the network domain and SCCP parameters. Therefore, all three features share one service. Because of this, existing functions like SRVSEL, Service, Re-route, CPC and status report for SCCP command service snapshot counts are affected.

Assumptions and Limitations

- » The SMSCs in the originating network and the SMSC in the terminating network are through SS7 and not via SMPP.
- » The feature does not support Number Portability across multiple countries.

A-Port Circular Route Prevention

The MNP Circular Route Prevention feature has been enhanced to provide the same functions for IS41 messages as it currently provides for GSM messages. Circular Route Prevention (A-Port CRP) detects and prevents circular routing for all messages that receive A-Port service, including LOCREQ and SMSREQ messages.

IS-41 GSM Migration

In many countries, wireless networks are undergoing a technology shift from networks based on the ANSI/IS-41 MAP protocol to a network based on the GSM MAP protocol. One reason for this shift is that GSM allows deployment of GPRS-based data services, which is a first step toward a 3G, or 3rd Generation wireless networks,

and GPRS is not compatible with an IS-41 network. Another reason is that GSM is more widely deployed world-wide than IS-41. Therefore, a migration to GSM provides for seamless international roaming.

When migrating to GSM, IS-41 subscribers will migrate gradually, one at a time, and they will want to retain their existing IS-41 phone number. This means that subscribers will have to be individually removed from the IS-41 HLRs and added to the GSM HLRs. This presents a routing problem because routing to HLRs is usually accomplished via GTT by grouping subscriber numbers into ranges, with each range having a translation to an HLR. This type of ranging is efficient because several million subscribers can be accounted for using only several thousand ranges. However, when an individual subscriber migrates to GSM, the GTT range that pointed that subscriber to the IS-41 HLR must be broken out into two ranges that point to the IS-41 HLR, and the migrated subscriber must be entered as a single entry that points to the GSM HLR. It is clear that the GTT tables will be quickly exhausted if all subscribers in a typical network (usually an average of 8 million subscribers or more) must be entered individually. This problem is addressed by the IS-41 to GSM Migration feature by treating the migrated customers as having ported to another network, in this case the GSM network.

IS-41 to GSM Migration requires the use of the EPAP application running on the OC EAGLE Application B card. IS-41 to GSM Migration is scalable from 850 to 75,000 queries per second.

For GSM Migration in general, four types of subscribers have been identified:

1. Non-Migrated- These are IS-41 subscribers who have not yet migrated to GSM.
2. Migrated with Two Handsets/GAIT Handset- These subscribers have migrated from IS-41 to GSM, and maintain two handsets, or a GAIT handset, in order to receive calls on the IS-41 network when GSM is not available. This capability is currently not supported.
3. Migrated with One Handset- These subscriber have migrated from IS-41 to GSM, but maintain only a single GSM handset. This category also includes new subscribers who sign up for GSM service only and have only one handset, but are given a number from the existing IS-41 number range.
4. GSM Only- These are new subscribers who sign up for GSM service only, have only one handset, and are given a number from a new "GSM only" number range.

Each type of subscriber is below.

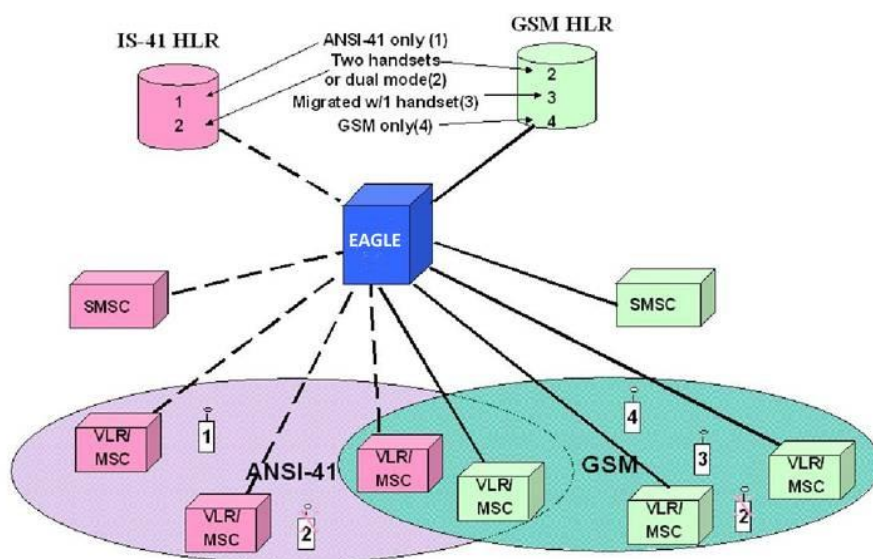


Figure 56: IS-41->GSM Migration Network View

The EAGLE can correctly handle calls to Non-Migrated subscribers via standard HLR Router or GTT routing schemes. Therefore, the only subscribers that are required to be provisioned in the GSM Migration database are the GSM-Migrated or GSM-Only subscribers, i.e. those who have migrated from IS-41 to GSM and have retained an "IS-41 number", or those who are new GSM only, but were given an "IS-41 number". In this scheme, messages received for Non-Migrated subscribers will result in no-match in the GSM Migration database, and will thus fall through to GTT and simply be routed per EAGLE' normal SCCP routing procedures. GSM-Migrated subscribers who use two handsets are not supported. Note that it is possible to also provision Non-Migrated subscriber in the GSM Migration database and thus be able to use standard HLR Router functionality to route messages for these subscribers instead of GTT. This is the customer's choice.

Message Flows

» Call Originated from IS-41 MSC for GSM-Migrated Subscriber

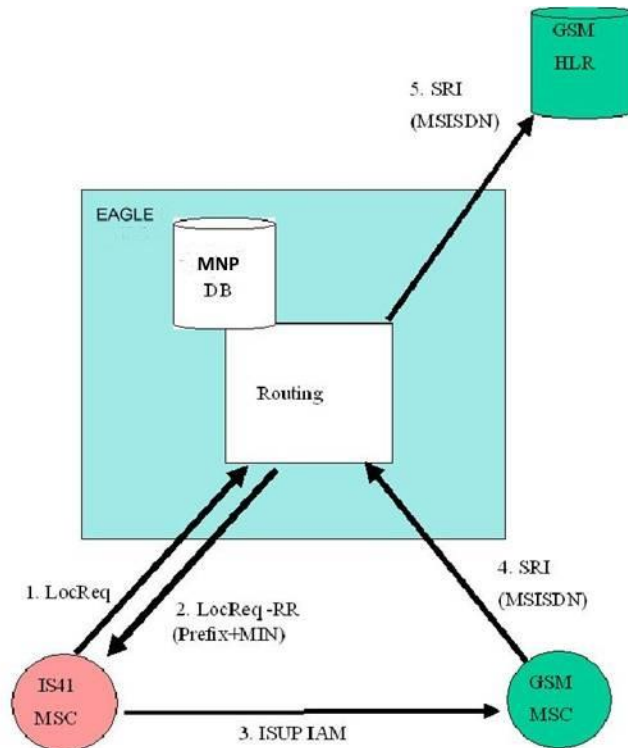


Figure 57: Call Originated from IS-41 MSC for GSM-Migrated Subscriber

1. When the IS-41 MSC receives the ISUP IAM, it sends a LocationRequest to the IS-41 HLR via the EAGLE. The EAGLE intercepts the Location Request message and uses the GTA in the SCCP CdPA to search the MNP DB to determine if this is a GSM-migrated subscriber.
2. Since the message is an IS-41 message, and the sub is GSM only, the EAGLE forms a LocationRequest - Return Result message and sends it to the IS-41 MSC using a special prefix added to the DN as the routing number. This prefix will be provisioned by the customer. The EAGLE switches the SCCP CdPA and CgPA information before sending the message so that the message appears to have come from the IS-41 HLR, not the EAGLE.
3. The special prefix causes the IS-41 MSC to route the ISUP IAM to a GSM MSC, after removing the prefix from the SCCP CdPA.
4. The GSM MSC sends a SendRoutingInformation message to the GSM HLR via the EAGLE.

5. EAGLE receives SRI message and selects it for MNP service. EAGLE' Service Selectors are provisioned such that SNP for this message is E.164. Thus, MNP uses the MSISDN number in the SCCP CdPA as an MSISDN to search the MNP database. This search indicates that this is a GSM-migrated subscriber. Since this is a GSM message, the relays message to the GSM HLR using the translation data in the MNP database.

» Originated from GSM MSC for GSM-Migrated/GSM-Only Subscriber

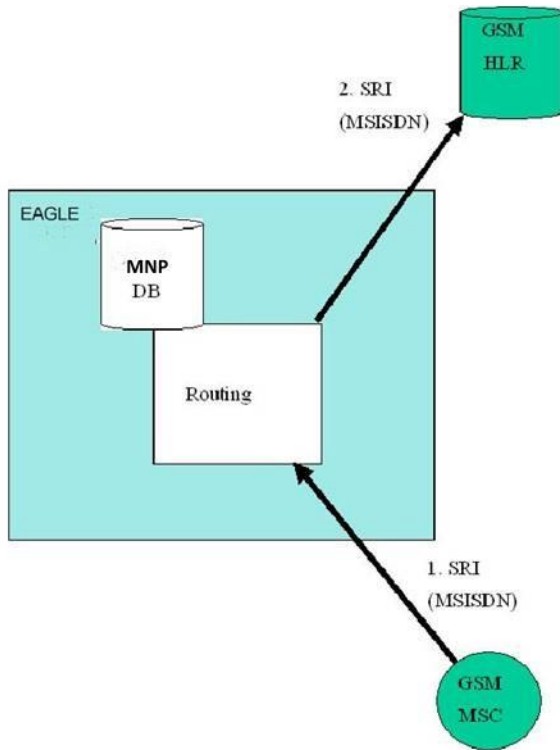


Figure 58: Originated from GSM MSC for GSM-Migrated/GSM-Only Subscriber

1. When the GSM MSC receives the ISUP IAM, it sends a SendRoutingInfo message to the GSM HLR via the EAGLE. The EAGLE intercepts the message and uses the digits populated in the SCCP CdPA GTA (or TCAP MSISDN) to search the MNP database to determine if this is a GSM-migrated subscriber.
2. Since the message is a GSM message, and the subscriber is GSM-migrated, the EAGLE routes the message to the GSM HLR, using the translation information from MNP database.

» Call Originated from IS-41 MSC for Non-GSM-Migrated Subscriber

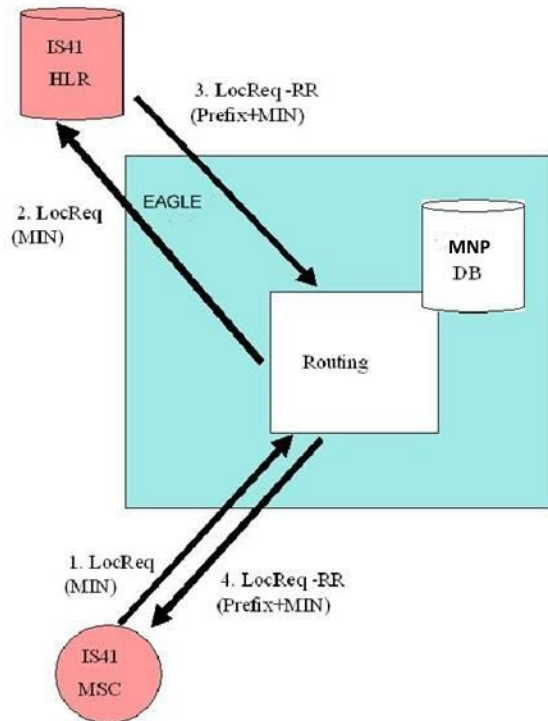


Figure 59: Call Originated from IS-41 MSC for Non-GSM-Migrated Subscriber

1. When the IS-41 MSC receives the ISUP IAM, it sends a LocationRequest message to the IS41 HLR via the EAGLE. The EAGLE uses the digits populated in the SCCP CdPA to search the MNP database. This search results in either: (1) A match in DB with migration type (portability type) of "none", and a translation to the IS-41 HLR, or (2) No match in DB, which will cause message to fall through to GTT.
2. In either case, since the message is an IS41 message, and the subscriber is IS41-only, the EAGLE routes the message to the IS41 HLR, using either the IS41 HLR translation information from MNP database, or the standard GTT translation.

» Call Originated from GSM MSC for Non-GSM-Migrated Subscriber

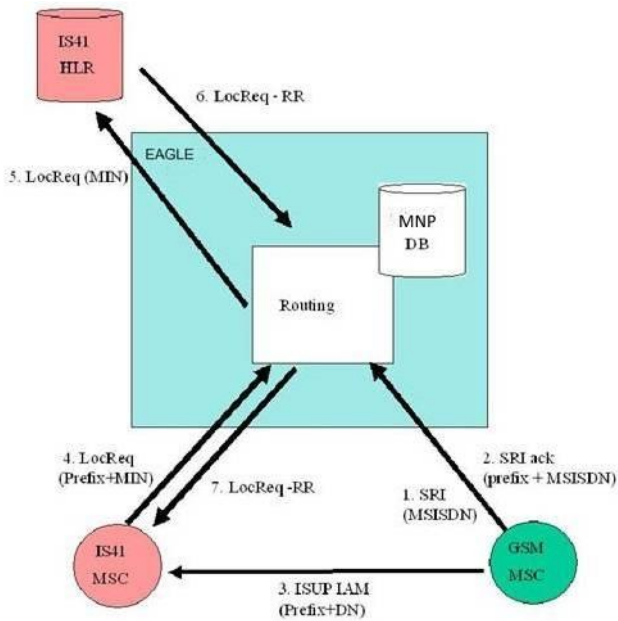


Figure 60: Call Originated from GSM MSC for Non-GSM-Migrated Subscriber

This call flow requires Non-Migrated subscribers to be provisioned in the GSM Migration/MNP database with an association to an RN which corresponds to the IS41 HLR

1. When the GSM MSC receives the ISUP IAM, it sends a SRI message to the GSM HLR via the EAGLE. The EAGLE intercepts the message and uses the digits populated in the SCCP CdPA GTA (or TCAP MSISDN) to perform database lookup. This search results in a match that indicates this is a non-migrated subscriber (portability type = "none").
2. Since the message is SRI, and the IS41 number is stored in the DB with an RN translation containing the Migration Prefix digits, the EAGLE returns an SRI-ack with the Migration Prefix as the routing number
3. The GSM MSC uses the routing prefix information returned in the SRI-ack to route the ISUP to the IS41 network.
4. When the IS-41 MSC receives the ISUP IAM, it sends a LocationRequest message to the IS41 HLR via the EAGLE. EAGLE removes the prefix and uses the MIN number in the SCCP CdPA as an MSISDN to search the MNP database. This search results a match in DB with migration type (portability type) of "none", and a RN translation to the IS-41 HLR.
5. Therefore, EAGLE message relays the LocReq to the IS41 HLR based on the PC/SSN information contained in the DB.

» MT SMS Delivery for Non-Migrated IS-41 Subscriber SRI-for-SM First

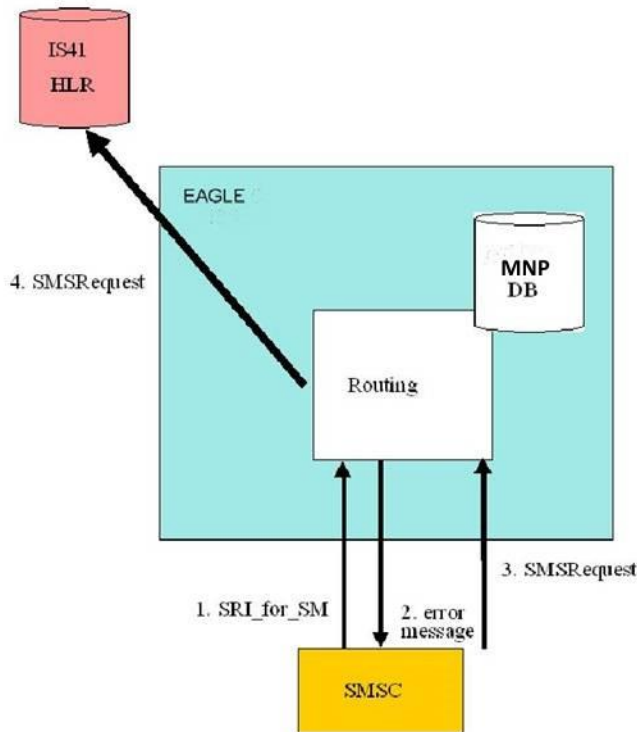


Figure 61: MT SMS Delivery for Non-Migrated IS-41 Subscriber SRI-for-SM First

1. The SMSC sends a SRI_SM to the GSM HLR via the EAGLE. The EAGLE intercepts the message and uses the digits populated in the SCCP CdPA GTA (or TCAP MSISDN) to search the MNP database. This search results in either 1 of 2 possibilities: The first possibility is a no match in DB (if non-migrated subs are not provisioned in DB). In this case, the message falls through to GTT. The GTT DB search would result in no match for this case (GTT tables for GSM TTs do not contain IS-41 only subs). The second possibility is a match is found in the DB (if both migrated and non-migrated subs are provisioned) with an RN translation to an ANSI Point Code for the IS-41 HLR, and a portability type of 0: "not known to be ported".
2. In the case of no match in MNP database, and no match in GTT DB, the EAGLE returns a UDTS error message to the SMSC per normal SCCP error handling. In the case a match is found with RN translation to the IS41 HLR and portability type = 0, the EAGLE returns a GSM SRI-for-SM error response with User Error = localValue 1 - "Unknown Subscriber".
3. The SMSC is programmed to formulate an IS-41 SMSRequest and send it to the IS-41 HLR via the EAGLE upon receiving the error message in 2.
4. EAGLE checks the migration DB. Since this is an IS-41 SMSRequest, and subscriber is not migrated, EAGLE relays the message to the IS-41 HLR, either by using an RN translation in the DB (if non-migrated subs are provisioned), or otherwise by GTT (if they are not provisioned).

» MT SMS for Non-GSM-Migrated IS-41 Subscriber: SMSRequest First

This case is the same as MT SMS Delivery for Non-Migrated IS-41 Subscriber SRI-for-SM First except the IS-41 SMSRequest is sent first instead of the GSM SRI-for-SM. Therefore, only steps 3 and 4 in the call flow above are performed: SMSRequest is received, EAGLE checks migration DB, and, since subscriber is not migrated, relays the message to the IS-41 HLR based on MNP translation data (if present) or GTT otherwise

» MT SMS for GSM-Migrated/GSM Only Subscriber: SRI-for-SM First

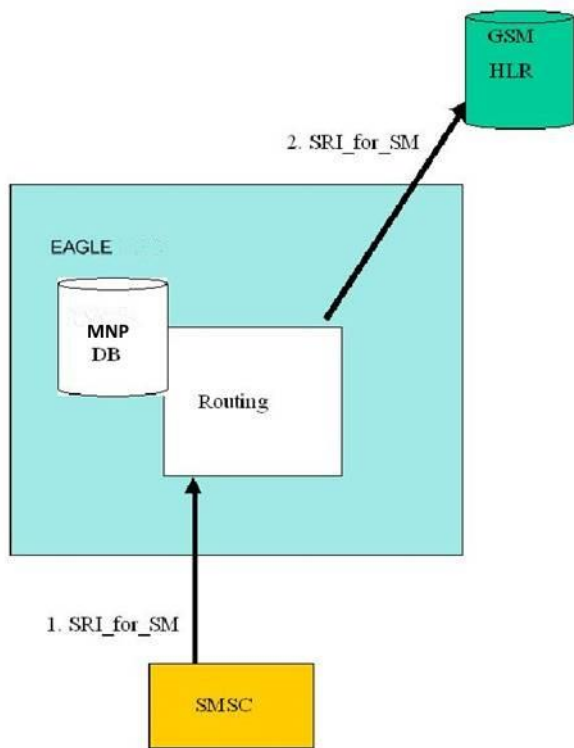


Figure 62: MT SMS Delivery for GSM-Migrated/GSM Only Subscriber: SRI-for-SM First

1. The SMSC sends a SRI_SM to the GSM HLR via the EAGLE. The EAGLE intercepts the message and uses the digits populated in the SCCP CdPA GTA (or TCAP MSISDN) to search the MNP database. Either this search results in a MNP database match (migrated/new sub with IS-41 number) or a no match in MNP (new sub with GSM number). If the MNP database results in no match, the GTT DB is searched, and a match will be found here (since the message contains a GSM TT and the sub is GSM).
2. In either case, since this is a GSM message and a GSM-migrated or GSM-only sub, the EAGLE relays the SRI_SM to the GSM HLR. If the match was found in MNP, the MNP translation data is used. Otherwise, GTT translation data is used.


» MT SMS for GSM-Migrated/GSM Only Subscriber: SMSReq First

This call flow is similar to that shown above, except the SMSRequest is delivered first. Steps are as follows:

1. IS-41 SMSRequest is received by EAGLE. EAGLE searches migration DB and finds a match with subscriber portability type = 5: "migrated".
2. Since this is an IS-41 message, and the subscriber is migrated, the EAGLE returns a SMSRequest Return Error response to the SMSC with SMS_Access Denied Reason = local value 5 - "Reserved value, treat as Denied"
3. The SMSC is programmed to formulate a GSM SRI-for-SM and send it to the GSM HLR via the EAGLE upon receiving the error message.
4. EAGLE checks the migration DB. Since this is an GSM SRI-for-SM, and the subscriber is migrated, EAGLE relays the message to the GSM HLR, based on the translation data in the MNP database.

IS41 GSM Migration

The IS41 GSM Migration (IGM) feature is an enhancement to the original IS-41 to GSM Migration feature. This feature adds the GSM-to-IS-41 migration functionality to the existing IS-41-to-GSM migration support of call termination for customers in migration from IS-41 to GSM wireless technology. This enhancement adds flexibility in



LOCREQ message decoding and encoding for number migration from one mobile protocol to another to the existing support of Loc_Req, SMS_Req, GSM SRI, and SRI_SM operation code processing.

The original IS-41 to GSM Migration feature functions support call termination for customers in migration from IS-41 to GSM wireless technology. The feature gives the wireless service provider a way to begin the migration of mobile subscribers from IS-41 to GSM, while allowing each subscriber to retain his or her existing phone number. The feature allows termination of calls to either an IS-41 handset or a GSM handset, based on the provisioned migration status of the subscriber.

The enhancement separates the IS41 GSM Migration feature from the MNP feature. The IS41 GSM Migration feature can exist as a standalone feature without depending on the MNP feature. When the IS41 GSM Migration feature is on, the MNP service selector is used instead of the MNP service selector.

The IGM feature uses the EPAP (EAGLE Provisioning Application Processor) RTDB to retrieve the subscriber portability status and provision directory numbers for exported and imported IS-41 subscribers. This database maintains information related to subscriber portability in the international E.164 format.

The IS41 GSM Migration feature supports both GT- and MTP-routed messages.

- » GT-routed messages support UDT and non-segmented XUDT message types and perform service selector lookup after SCCP verification.
- » A-Port processes MTP-routed messages if the MTP Messages for SCCP Applications feature (described in MTP is in operation).

The IS41 GSM Migration feature adds processing of LOCREQ and SMSREQ messages to the SRI and SRI_SM message processing provided by the original IS-41 to GSM Migration feature.

- » An ANSI-41 LOCREQ message is initiated by a TDMA/CDMA MSC that queries the HLR for information regarding user subscription/location before terminating a voice call.
- » An ANSI-41 SMSREQ message is initiated by a TDMA/CDMA SMSC that queries the HLR for information regarding user subscription/current location before delivering a short message.

If a data entry matching the conditioned Called Party is found and an NE (either RN or SP) is assigned to the entry, the EAGLE processes the SRI, SRI_SM, LOCREQ, and SMSREQ message based on the Network Entity (NE)/Portability Type (PT) value assigned.

This feature IGM shares the service state and re-route with the A-Port and MNP features, under one service called the MNP Service state. (The MNP service state is used if only the MNP feature is on.) The IS41 GSM Migration feature supports re-route functions as part of MNP service re-route. Alternate PCs are shared by all three features.

- » Database Lookup and Routing: The MSISDN is used for RTDB database lookup.
 - » The IS41 GSM Migration feature performs RTDB lookup on the conditioned number, and routes or relays the message based on the lookup result.
 - » The individual number database is searched first. If the number is not found, the number range database is searched.
 - » If a match is not found in the individual and range based databases, GTT is performed on the message.
 - » For LOCREQ messages, the DN is derived based on the setting of the LOCREQ DN option
 - » For non-LOCREQ messages, the DN is derived from the SCCP portion of the message.
 - » Upon successful decode and verification of the message, number conditioning is performed. The DN or SCCP CDPA digits might need to be conditioned to international number format based on the service nature of address (SNAI or TCAPSNAI or MTPLOCREQNAI). HomeRN and IEC or NEC prefixes are removed. The IS41 GSM Migration feature performs RTDB lookup on the conditioned number, and routes or relays the message based on the lookup result.

An SMSREQ message is relayed like any other non-LOCREQ message. No changes are performed to the TCAP/MAP portion of the message. If the general TCAP/MAP verification is successful, the TCAP Opcode is SMSREQ, and the IS412GSM option for bypass is set the message is processed as an SMSREQ message. Otherwise, message relay is performed using SCCP CDPA information.

The IS41 GSM Migration feature modifies the TCAP information for LOCREQ messages only when a HomeRN was deleted from the TCAP DN and the option of removal of the HomeRN is set. Any gaps in the data caused by a change in field length will be resolved by shifting the remaining information up. Any IEC or NEC code is left.

The IS41 GSM Migration feature falls through to GTT if number conditioning fails or does not find the DN in the RTDB database, or the DN is found with non-A-Port data

If a HomeRN is detected in the Called Party and a matching DN with RN is found in the database, the EAGLE generates UIM 1256, indicating detection of circular routing, and routes the message using normal routing if both the MNP Circular Route Prevention feature and the IS41 GSM Migration feature are turned on.

Note: Normal routing is performing GTT if the incoming message is sent to the EAGLE Self Point Code. Normal routing is routing the message to the MTP DPC if the incoming message is MTP-routed (the MTP DPC of the message is not the EAGLE Self Point Code).

- » IS41 GSM Migration Support for Relaying SRI_SM to Default SMSC: When an SRI_SM message is received for an own-network IS41 subscriber (NE=RN, PT=0), a configuration option specifies whether IGM responds with a Return Error message (existing function) or relays the SRI_SM message to the default IS41 Short Message Service Center (SMSC).

The IGM enhancement to relay an SRI_SM to a specified default SMSC is available if the IS41 GSM Migration feature (IGM) is on. The enhancement provides the following new GSMSMSOPTS configuration options:


- » IGMSMSRELAY— Select the existing function to send an SRI_SM with "unknown subscriber", or the new function to relay an SRI_SM to the default SMSC.
- » DEFIS41SMSC—Specify the default SMSC address.
- » IS41SMSCGTTSN—Specify the GTTSET where the translation for the default SMSC address is configured. If IGMSMSRELAY is NO, then IGM sends a Return Error message with error reason "Unknown Subscriber". If IGMSMSRELAY is YES, then IGM relays the SRI-SM message to the default IS41 SMSC by performing GTT translation (found in the GTTSET) on the default SMSC address digits.

Service Portability (S-Port)

"Service Portability" describes a special type of number portability that allows a subscriber to keep the same phone number when switching from one type of network or service technology to another within the same operator's network. Unlike traditional Number Portability, the subscriber does not move from one network operator or service provider to another. With Service Portability, the subscriber remains with the same operator, but receives service from a different network technology supported by that operator or moves from one physical network to another, with both networks operated by the same service provider.

Network nodes must be able to determine whether a message should use Service Portability or Number Portability. Operators offering Service Portability may need unique internal routing numbers (RNs) that can be used to indicate which network a subscriber belongs to, allowing network nodes to route calls and messages between the two networks.

Number Portability functions use the RN/SP Network Entity from the RTDB when formatting outgoing Called Party digits in a response or relayed message. The Service Portability (S-Port) feature allows RTDB GRN Entity digits to be used for own-network GSM and IS41 subscribers in response digit formats for any feature where Service Portability is performed. The GRN field in the RTDB is used to provision Service Portability prefixes on a per subscriber basis. A subscriber is considered an own-network GSM subscriber if the dialed number (DN) is



associated with an SP entity type in the RTDB. A subscriber is considered an own-network IS41 subscriber if the DN is associated with an RN entity type in the RTDB and the portability type (PT) is 0. EPAP-related features that use Number Portability processing can also use Service Portability processing, as described in the following sections:

- » AINPQ Service Portability
- » ATINP Service Portability
- » MNP SRI Query for Prepaid Service Portability
- » IAR NP Service Portability
- » INP Service Portability
- » Prepaid IDP Query Relay (IDP Relay) Service Portability
- » MO SMS Service Portability
- » TIF NP Service Portability

S-Port Subscriber Differentiation

The Service Portability (S-Port) Subscriber Differentiation feature allows multiple routing numbers to be provided for a subscriber. This functionality allows different processing to be performed on different groups of subscribers.

This feature uses the Additional Subscriber Data (ASD) as the subscriber's private routing number (for message relay features) and the Generic Routing Number (GRN) as the subscriber's public routing number (for query/response features). If ASD is not provisioned, then subscribers follow standard S-Port processing using the GRN.

The feature overrides the S-Port application of the GRN by using the ASD, if present, for call flows resulting in message relay.

GSM MAP SRI Redirect to Serving HLR

This feature provides the capability to resolve the incompatibility introduced by the proprietary implementation of the GSM MAP SRI message. This feature is an extension to the Mobile Number Portability (MNP) Protocol as described in Reference [5]. Therefore, the feature shall be compatible with other MNP enhancement features provided to date, including the "MNP Circular Route Prevention," "Portability Check for Mobile Originated SMS" and "Pre-paid SMS Intercept" features.

The feature supports up to 3 different vendor networks and up to 2 vendor types. For example

- » Vendor-Network 1: for example, Vendor Type 1, 2G Network
- » Vendor Network 2: for example, Vendor Type 2, 2G Network
- » Vendor Network 3: for example, Vendor Type 1, 3G Network

If the originating MSC (of the SRI) and the destination HLR are the same vendor type, the EAGLE MNP will relay the message to the HLR as noted by the SP in the NPDB. If not, the EAGLE checks to see if the vendor type is deployed in more than one network (where each network has its own vendor/network prefixes). If the vendor types of the originating MSC and destination HLR are different and the vendor type of destination HLR is deployed in more than one network the EAGLE MNP appends its respective vendor/network prefix that points to the network where the hosting HLR resides. If the vendor types of the originating MSC and destination HLR are different and the vendor type of destination HLR is deployed in only one network the EAGLE MNP appends the vendor/network prefix that assigned to the network.

- » Step 0: For a ported-in number, GMSC-Vendor 2 receives an IAM message with CdPN.
- » Step 1: The receiving GMSC interrogates the HLR for the subscriber's current location by issuing an SRI.

- » Step 2: When the EAGLE receives an SRI message that meets the MNP service selector criteria, HomeRN deletion and number conditioning are performed on the DN. The DN database is then searched. If the DN is found in the database with an SP (HLR entity address) associated with the called party MSISDN, the EAGLE then searches for the SP in the VendorID table. If the SP is found in the VendorID table, the EAGLE then checks if the CgPA has a valid length GTA. The EAGLE then searches the CgPA GTA in the VendorID table. If the CgPA GTA is found in the VendorID table, the EAGLE compares the two vendor numbers associated with the CgPA GTA and the SP. The EAGLE then determines whether the GMSC and the HLR are of the same vendor type. If they are of the same vendor type, go to Step 7. If they are different vendor types, go to Step 3.
- » Step 3: If the destination network belongs to a vendor type that is deployed in more than one network, the EAGLE will generate an SRI_ACK using the Vendor Prefix of the destination network as the RN. The MSRN is filled using various options provisioned in the GSMOPTS table as done currently for the MNP SRI_ACK. The SRI_ACK is then sent to the originating GMSC. The table below describes the prefix that should be appended if vendor types are different.

This feature was incidentally modified by PR 126584 in support of Additional Subscriber Data to include support for several new values of the GSMOPTS:MSRNDIG option.

PR 136590 (MNP Enhancements to support ROP) modified MNP feature to support several new values of GSMOPTS:MSRNDIG option. The GSM MAP SRI Redirect to Serving HLR feature inherits these new MNP modifications.

Table 15: Network Prefix To Be Appended to SRI_ACK

Originating GMSC (sending SRI)	Destination Network (HLR to Receive the SRI)	Actions to be Taken by EAGLE MNP	Network Prefix to be Appended to SRI_ACK, if returned.
Vendor 1 Network # 1	Vendor 1 Network # 1	Relay to HLR	N/A
	Vendor 2 Network # 2	Return SRI	SRI_ACK (Network #2 Vendor Network Prefix)
	Vendor 1 Network # 3	Relay to HLR	N/A
Vendor 2 Network # 2	Vendor 1 Network # 1	Return SRI	SRI_ACK (Network #1 Vendor Network Prefix)
	Vendor 2 Network # 2	Relay to HLR	N/A
	Vendor 1 Network # 3	Return SRI	SRI_ACK (Network #3 Vendor Network Prefix)
Vendor 1 Network # 3	Vendor 1 Network # 1	Relay to HLR	N/A
	Vendor 2 Network # 2	Return SRI	SRI_ACK (Network #2 Vendor Network Prefix)
	Vendor 1 Network # 3	Relay to HLR	N/A

- » Step 4: Based on the Vendor Prefix, the originating GMSC will route the call to the GMSC of the network associated with Vendor 1 via ISUP IAM.
- » Step 5: The subscription network GMSC formulates and sends an SRI message to the EAGLE to interrogate the subscriber's current location.
- » Step 6: The EAGLE MNP performs an NP database lookup based on the MSISDN in the SRI and determines that the number belongs to its network. It then compares the SP (HLR entity address) associated with the MSISDN and the CgPA GTA (GMSC/MSC) and finds that they are the same vendor type. Go to Step 7.
- » Step 7: The EAGLE MNP relays the SRI to the HLR as noted by the SP.
- » Step 8: The HLR returns an SRI_ACK to the GMSC via the EAGLE STP.

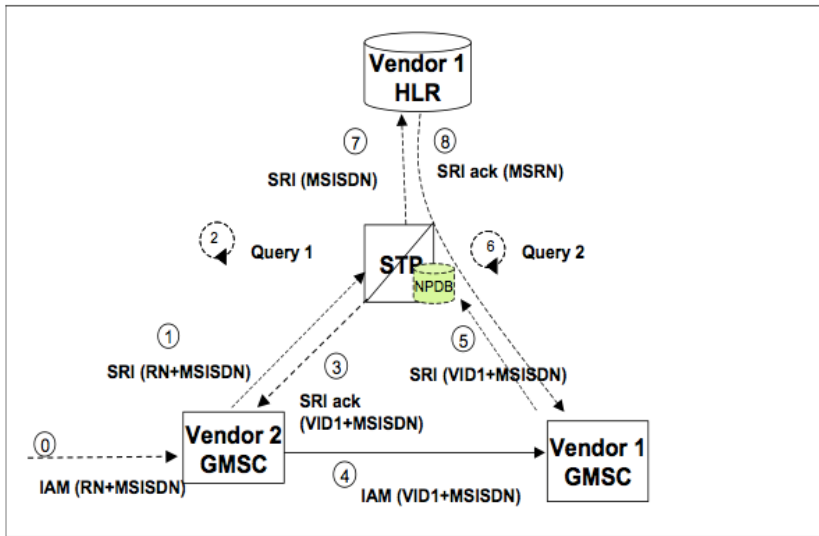


Figure 63: SRI Re-Direct to serving HLR

Intra Network Number Portability

Introduced in EAGLE release 46.1 the Intra Network Number Portability feature provides the enhanced ability to identify intra-circle and inter-circle calls. Before the Intra Network Number Portability feature, the GSM MAP SRI Redirect to Serving HLR feature identified the serving HLR based on the Circle Type and Circle Number for operators. With the Intra Network Number Portability feature, each Circle has a unique GRN, a unique Vendor Type, and a unique Vendor Number. The Intra Network Number Portability adds the new option GSMOPTS:SRIRDCTENT with two possible values: GRN, SP. The Intra Network Number Portability feature changes provide the MNP feature with the correct routing information for calls. Intra Network Number Portability and the GSM MAP SRI Redirect to Serving HLR feature cannot be used at the same time.

NUMBER PORTABILITY SOLUTIONS FOR PREPAID/SERVICE NODE ACCESS

GSM SRI Query

The MNP SRI Query for Prepaid feature enables the EAGLE to provide portability information to a Service Control Point (SCP) database. This information enables the database to determine the network used by a called subscriber.

The MNP SRI Query for Prepaid feature enables a user to provision the following Message Signaling Unit (MSU) values in the EAGLE GSERV table:

- » Translation type (TT)—The TT of the called party (CdPA)
- » Originating point code (OPC)—The OPC from the message transfer part (MTP) layer
- » Global title address (GTA)—The GTA of the calling party (CgPA)

These values are used to determine whether an SRI should receive MNP SRI Query for Prepaid service or normal MNP SRI service.

If the MNP SRI Query for Prepaid feature is enabled and turned on, an incoming SRI's TT, OPC, and GTA values are compared against the values in the GSERV table. If no match is found, or if no values are provisioned in the GSERV table, normal MNP SRI processing is performed on the message. If a match is found for one or more of the values, the message is treated as a Prepaid Query.

The MNP SRI Query for Prepaid feature affects only SRI messages. All other messages, including SRI-SM and SRI-GPRS messages, are processed by normal MNP service, even if the values in those messages match values in the GSERV table.

After an SRI message is identified as requiring MNP SRI Query for Prepaid service, the EAGLE performs a Mobile Number Portability (MNP) database lookup on the Mobile Station Integrated Services Digital Number (MSISDN). The results of the lookup are returned to the SCP that originated the query.

A TCAP/MAP error specifically related to a decoding error in the SRI MSISDN parameter causes an "Unsupported/Unexpected Data Value" MAP error. All other TCAP/MAP errors cause the message to be relayed to a Home Location Register (HLR), which then returns the appropriate MAP error based on the status of the subscriber (e.g., Unknown, Barred). The message relay is based on information in the MNP database. SCCP level errors cause the return on a UDTS message to the Prepaid SCP.

This feature requires activation and cannot be turned off once it is turned on.

The MNP SRI Query for Prepaid feature has the same hardware requirements as those required for the MNP feature.

GSM ATI Query

Like the GSM SRI Query feature, the GSM ATI Query feature allows an external service node, such as a prepaid SCP, etc., to directly query the EAGLE in order to obtain the Number Portability routing information for a particular subscriber number. Different nodes support different functionalities, and some nodes are unable to formulate SRI queries, but are able to formulate ATI queries. Furthermore, the use of the ATI query as a means for a node to directly query a number portability database on-demand and outside the strict confines of a call- or message flow-in-progress, has been standardized and is included in the 3GPP mobile number portability specification (23.066).

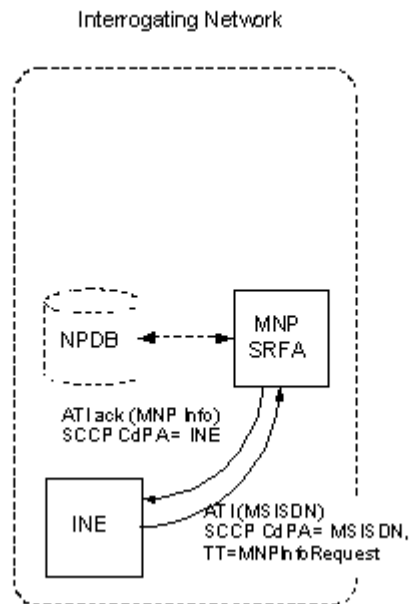



Figure 64: Example of ATI Query/Response to MNP Database Node

The figure above shows an example of the ATI query being used for a direct query to a number portability database.



The ATI query is intended to be routed directly to the node housing the number portability database - in this case, the EAGLE. Therefore, a new local subsystem is created on the EAGLE for the purpose of the ATI query. This new local subsystem can coexist with the other local subsystems for EPAP-based EAGLE features, including INP, EIR and Voicemail Router. (ATI query, and all other EPAP-based features cannot coexist with the ELAP-based North American LNP subsystem).

A node can route ATI NP queries to the EAGLE via one of three methods:

1. Using a set of SCCP message parameters (e.g. TT, NP, NAI, GTI, SSN) that will match a SCCP service selector combination provisioned in the EAGLE as uniquely identifying the ATI Query service.
2. Routing with SCCP CdPA RI=rt-on-gt to a set of GT Address digits which have been provisioned in the EAGLE to resolve to one of the EAGLE's point codes and the ATI Query local SSN.
3. Routing with SCCP CdPA RI=rt-on-ssn directly to one of the EAGLE's point codes and the ATI Query local SSN.

The ATI Query feature expects the number for DB search to be included in the RequestedInfo parameter of the ATI message. If this parameter is absent or a valid number is not present in this field, the EAGLE will terminate the service and return an ATI nack message.

The EAGLE performs an RTDB search using the digits from the RequestedInfo parameter, after conditioning the number per the provisioned setting for the ATI service. The EAGLE can be configured to define what constitutes a successful search. If a search is "not successful" per these criteria, the EAGLE will return an ATI nack. If the search is successful, the EAGLE will return an ATI ack, including the following parameters:

- » MNP_INFO: Includes the following:
 - » Routing Number found with the subscriber number in the MNP database, formatted per the configurable settings in the EAGLE.
 - » MSISDN used for the search, formatted per the configurable settings in the EAGLE.
 - » IMSI, formatted per the configurable settings in the EAGLE.
- » Number Portability Status

The ATI Query feature also allows the use of the new Additional Subscriber Data, or ASD, information from the EAGLE's RTDB in the formatting of the outgoing data fields in the ATI ack. See SUPPORTING FUNCTIONALITIES.

Prepaid IDP Query Relay

Prior to the implementation of number portability, correct charging of calls placed by prepaid mobile subscribers was relatively easy. Prior to completing call setup, the originating Mobile Switching Center (MSC) queries a prepaid database, commonly located in an SCP, using an INAP Initial Detection Point (IDP) message. The IDP message contains both the calling subscriber's phone number and the called subscriber's phone number (Called Party BCD Number). The prepaid SCP then sets the correct tariff for the call based both the calling and the called subscribers. The prepaid SCP may set different tariffs based on the destination of the call. For example, if a prepaid mobile call is to be terminated within the same network that serves the calling subscriber, the call may be free. If, however, the call is to be terminated to a foreign network, regardless of whether it is a fixed-line or competing mobile network, there may be a charge for the call.

Prior to number portability, the prepaid SCP could easily determine which network the called party belonged to simply based on the dialed digits (encoded in the INAP Called Party BCD Number parameter). However, with number portability, the dialed digits can no longer be relied upon to determine the current subscription network of the called party. Thus, the calling and called party information alone is no longer sufficient to determine the tariffs. The prepaid SCP needs also to know the portability status of the called party to set the correct tariffs.

The EAGLE with the Prepaid IDP Query Relay feature will intercept the IDP message, destined for a prepaid SCP, and perform number portability database lookup. If the called party is a ported-out number, the EAGLE will prepend the Routing Number (RN), which is associated with the called party and identified in the number portability database, to the INAP Called Party BCD Number parameter prior to forwarding the message to the prepaid SCP. If the called party is a ported-in number, the EAGLE will prepend the Home Location Register Identification (HLR-ID), which is associated with the called party and identified in the number portability database, to the INAP Called Party BCD Number parameter prior to forwarding the message to the prepaid SCP. The diagram below shows the call flows for prepaid mobile voice calls terminating to ported-out and ported-in subscribers.

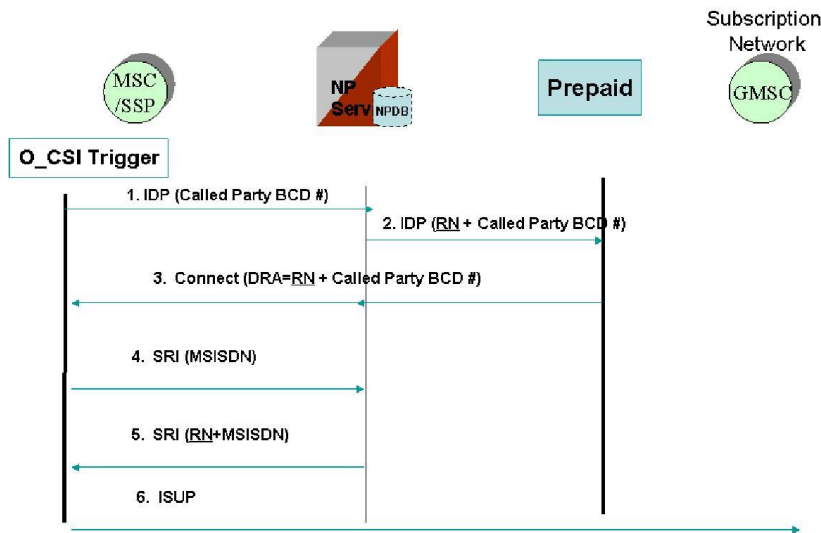


Figure 65: Prepaid Mobile Voice Call Terminating to Ported-Out Subscribers

1. The EAGLE performs the number portability database lookup based on the Called Party BCD Number parameter encoded in the IDP message. The EAGLE finds the DN entry in the number portability database as a ported-out subscriber.
2. The EAGLE prepends the Routing Number (RN) to the Called Party BCD Number and forwards the IDP message to the Prepaid SCP.
3. The Prepaid SCP returns an INAP Connect to MSC via the EAGLE.
4. The MSC sends SRI to an HLR. The EAGLE intercepts the message and performs number portability lookup.
5. The EAGLE finds the DN entry in the number portability database as a ported-out subscriber. The EAGLE returns SRI_ACK with MSRN assigned with RN (or the RN can be prepended to the MSISDN to form the MSRN).
6. The MSC performs call setup to the Subscription Network as noted by the RN.

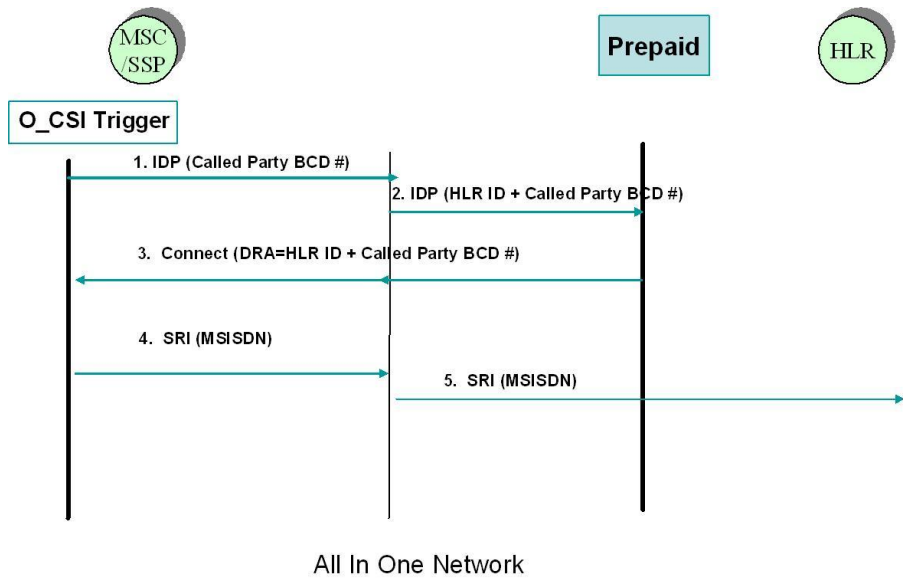


Figure 66: Prepaid Mobile Voice Calls Terminating to Ported-In Subscribers


1. The EAGLE performs number portability database lookup based on the digits encoded in the INAP Called Party BCD Number parameter. The EAGLE identifies the entry in the number portability database as a ported-in subscriber
2. The EAGLE prepends HLR ID to the INAP Called Party BCD Number parameter and forwards the IDP message to the Prepaid SCP.
3. The Prepaid SCP returns the INAP Connect (with HLR ID + Called Party BCD Number assigned to the INAP Directory Routing Address) to the MSC via the EAGLE. Alternatively, the prepaid SCP may choose to return an INAP Continue message to the MSC, via the EAGLE
4. The MSC sends the SRI to the serving HLR as noted in the HLR ID if returned from the Prepaid SCP via the EAGLE. If the HLR ID is not known, the MSC shall route the SRI message to the EAGLE for number portability database lookup.
5. The EAGLE relays the SRI to its serving HLR.

With the Prepaid IDP Query Relay feature, the Prepaid SCP will have all the information it needs, upon receipt of an IDP message, to determine the correct tariff to apply to the call. The Prepaid SCP does not need to launch a separate number portability query to obtain portability information to complete the call. The more stream-lined message-processing operations significantly reduce the signaling traffic required to traverse through the network. Without processing of the additional query, launched by the Prepaid SCP, the call can also be completed with shorter delay. The savings introduced by the elimination of the additional queries also allows the Prepaid SCP to have more processing capacity to handle prepaid calls.

The Prepaid IDP Query Relay feature is fully integrated with the Mobile Number Portability (MNP) and INAP-based Number Portability (INP) features. Namely, the Prepaid IDP Query Relay feature can be run simultaneously on the same node that runs MNP or INP. The feature uses the same MNP and/or INP database for database lookups, thus eliminating the need to maintain a separate database that would otherwise be required if stored by a separate SCP.

“Flexible” IDP Relay

A new infrastructure is introduced in Release 39.2, known as “NPP” or Numbering Plan Processor. See SUPPORTING FUNCTIONALITIES. In 39.2, the IDP Relay feature is adapted to make use of the NPP infrastructure. The feature, as adapted with the NPP infrastructure, is known in R39.2 as “Flexible IDP Relay”.



Flexible IDP Relay effectively replaces the existing Prepaid IDP Query Relay feature on upgrade. In future releases, the distinction between the two flavors of the feature will disappear, and it will simply be referred to as “IDP Relay”. For now, the two descriptions will be maintained for transition purposes.

The adaptation of the IDP Relay feature to use the NPP infrastructure was a response to many customers’ requirements for having more flexibility in the number conditioning and number formatting portions of the original IDP Relay feature, as well as the need to have CgPN lookup in addition to CdPN lookup in some use cases.

Due to the wide variety of numbering plans and numbering structures within those numbering plans, the previously semi-rigid options for number conditioning and formatting in the IDP Relay feature was not adequate for some operators. The Flexible IDP Relay feature addresses this requirement by linking a new internal infrastructure, the Numbering Plan Processor or NPP, into the IDP Relay message processing. See SUPPORTING FUNCTIONALITIES for more details on NPP specifically.

Through the use of the NPP infrastructure, IDP Relay now has a much greater flexibility in number conditioning and formatting, including the ability to remove multiple prefixes, access codes, escape codes, carrier selection prefixes, etc., from the incoming number before lookup. As these various digit strings are removed from the incoming number, they can be stored as “tokens”, and one or more of the tokens may be reused later in the number formatting stage. Furthermore, Flexible IDP Relay allows these tokens to be placed in the formatted number in any order required by the network.

Flexible IDP Relay also provides the ability to indicate a CgPN lookup and number prefixing is needed in conjunction with the CdPN lookup. This is useful for any case whereby the prepaid SCP requires portability information for both the calling and called parties. Flexible IDP Relay can perform a lookup on both numbers, and provide the NP information for both numbers to the SCP in the same message.

Other minor enhancements are also part of the Flexible IDP Relay feature, including the following:

- » Ability to select via configuration the number formatting options based on the Network Entity associated with a particular number in the RTDB. For example, some operators wish to prefix the RN for ported out numbers, but do not wish to prefix the SP (HLR ID) for ported in numbers.
- » Support for non-segmented XUDT messages.
- » Expansion of supported Service Key length from 1 byte to 4 bytes.
- » Support the ACCgPN Conditioning Action for extracting the Area Code from the Calling Party Number (CgPN). The length of the area code to be extracted is determined by global configuration. All action sets use this global value.

There are some customer networks where the area codes are of different lengths. Users do not dial the area code for intra-area code calls. For these cases, the variable length area code needs to be extracted from the CgPN (which always has the area code for this customer) in order to condition the CdPN prior to number portability database lookup. Starting with EAGLE release 44, there is an enhancement to extract variable length area codes from the CgPN by adding eight new CAs, ACCGPN1 - ACCGPN8, to specify the length of Area Code to be extracted from the CGPN of incoming MSU while processing IDPRCDPN(X) NPP service.

IDP A-Party Blacklist

The IDP A-Party Blacklist feature enhances the Prepaid IDP Query Relay feature to provide a generic framework to support subscriber blacklisting capability that works with either a query-based or relay-based method. The feature supports the blacklist check on the Calling Party (A-Party or CgPN) number in the IDP CAMEL or INAP message.

The EAGLE receives an IDP query message destined to the EAGLE Point Code or a prepaid IDP message sent to the EAGLE Point Code for translation to prepaid SCP. MSCs are configured with a trigger point to send an IDP

message for just post-paid or prepaid subscribers or for all subscribers in the network, depending on the use case for a particular operator.

The EAGLE receives the IDP message and performs the necessary discrimination and pre-processing using the current prepaid IDP Relay functions (SCCP CdPA check, CgPA check and Common Screening List SK BCSM filter). The EAGLE decodes the Calling Party Number (from the CgPN parameter) from the message. If the subscriber number is blacklisted, the number is entered with a blacklist flag and optional routing number information. If a match is found, EAGLE returns a Connect message with Routing Number (if provisioned). This Routing Number could be a service center number that receives the re-routed call and provides the necessary assistance. If the subscriber is not blacklisted, the IDP message continues normal processing (if it is prepaid IDP message), or a CONTINUE response is generated (if the blacklist query is received).

» IDP A-Party Routing

The IDP A-Party Routing feature allows routing for IDP or IDPSMS messages to be performed using the A-Party Calling Party Number (CgPN). This feature provides a routing alternative to the existing SCCP GTA routing. A-Party routing is performed using a new CGPN Service Action and invoking new algorithms during post-NPP processing.

If successful IDP A-Party routing occurs, then an IDP or IDPSMS message is routed to an available Prepaid Server from a list of provisioned servers in the MRNSET or MAPSET load share table. If routing failure occurs, then a UDTS is sent to the originator or the message is discarded. If all of the required data for IDP A-Party routing is not provisioned, then routing falls through to GTT routing.

» IDP Service Key Routing

The IDP Service Key Routing (IDP SK Routing) feature allows routing to occur based on the Service Key and EventType BCSM parameters in the incoming IDP or IPDSMS message. IDP SK routing can occur independently or can be used as a fall-through option for the IDP A-Party Routing feature.

If successful IDP SK routing occurs, then an IDP or IDPSMS message is routed to an available Prepaid Server from a list of provisioned servers in the MRNSET or MAPSET load share table. If routing failure occurs, then a UDTS is sent to the originator or the message is discarded.

If all of the required data for IDP SK routing is not provisioned, then routing falls through to GTT routing.

» Interaction between IDP A-Party Routing and IDP Service Key Routing

If the IDP Service Key Routing (IDP SK Routing) or IDP A-Party Routing feature is turned on, then the system behaves as if the routing provided by that feature was the only routing option.

If both features are turned on, and the A-Party Routing Service Action is provisioned, then both features are considered for processing. The IDP A-Party Routing option is checked first. If IDP A-Party Routing is not attempted, and the IDP SK Routing option is provisioned, then IDP SK Routing is considered.

If IDP A-Party Routing is not attempted, and the IDP SK Routing option is not provisioned, then GTT routing is performed.

Whether A-Party Routing or SK Routing is attempted, once a message attempts to route, the message does not attempt any other routing method, including SCCP GTA/GTT routing. If routing fails, then the attempt is considered an IDPR routing failure, a UDTS is sent, and the message is discarded.

Note: Post-processing network conversion for IDP A-Party Routing and IDP SK Routing can only be performed for ITU-I or ITU-N network types.

Configurable NAI to TON mapping

While decoding a CdPN or CgPN BCD parameter, the TON has to be mapped to a NAI value that can be used by NPP. This TON to NAI mapping is implemented as follows.

Table 16: TON to NAI Mapping

Decoding Mapping

TON	FNAI	
1	4	INTL
2	3	NATL
0	2	UNKN
All other values	2	

Similarly the OFNAI (from NPP) to TON mapping while encoding a CdPN or CgPN BCD parameter is implemented as follows

Table 17: OFNAI to TON Mapping

Encoding Mapping

OFNAI	TON	
4	1	INTL
3	2	NATL
2	0	UNKN
All other values	0	

This mapping will work for the standard (National and International) values, but for reserved values, this mapping is very restrictive.

Instead of the hard-coded mapping, starting with EAGLE release 44, the user shall be able to re-configure this mapping. The user will be able to change this mapping with the existing command `chg-ttropts`.

The default values in the configurable mappings will be as they were hard-coded before the implementation of this change so that it won't impact the customers who are already using IDPR and upgrade to the release with the implementation of this change.

IDP Relay for SMS

IDPs issued in the context of an SMS prepaid check using the CAP (CAMEL Application Part) protocol differ slightly from IDPs issued using the INAP protocol or CAP IDPs issued in the context of a voice call. The IDP Relay for SMS feature is a variant of the EAGLE's IDP Relay feature which allows processing of these CAP IDPs for SMS.


Differences from standard CAP/INAP IDP: The CAP IDP-SMS message uses a different opcode than a standard INAP or CAP IDP. The CAP IDP-SMS message also uses a "Destination Subscriber Number" parameter in place of "Called Party BCD Number" of CAP or "Called Party Number" in standard INAP. Lastly, IDP-SMS uses "Event Type SMS" in place of "Event Type BCSM".

In order to avoid potential duplication of Service Keys (SK for IDP-SMS maybe be the same as SK for IDP, making service selection difficult for EAGLE), the EAGLE allows an offset to be provisioned with the Service Key intended for IDP-SMS.

Functioning of the IDP Relay for SMS feature is otherwise identical to that of the IDP Relay feature.

IDP Screening for Prepaid

Network operators may use CAMEL (CAP) or INAP IDP messages to query prepaid engines to validate prepaid subscribers' credit status. The operators pay license fees for every prepaid status inquiry. With the IDP Screening capability, the operators can reduce the license fees as well as eliminate the unnecessary traffic resulting from prepaid status inquiries.



This feature allows the operator to designate some prepaid subscribers as premium service subscribers. These premium subscribers pay a special rate and thus calls or text messages originated from these subscribers do not require the typical per-call or per-message prepaid credit check at the SCP prior to completing the call or delivering the text message. Thus, for these messages, the EAGLE can respond directly to the IDP and avoid sending the IDP onward to the SCP, thus reducing the load on the SCP. Calls or messages from standard prepaid customers would still be relayed by the EAGLE to the SCP.

For voice calls or text messages originated by a prepaid subscriber, the serving MSC formulates an INAP or CAP IDP message, destined for a prepaid engine, to check the subscriber's credit status. The EAGLE intercepts the IDP message and examines whether checking credit status is required prior to routing the calls to the prepaid engine. If the message does not concern a premium prepaid subscriber, the EAGLE relays the IDP message to its intended destination, which would be the prepaid SCP.

Messages concerning a premium prepaid subscriber will be identified by a predefined ServiceKey value. The value assigned to ServiceKey is set by an originating MSC when the IDP is formulated. If a message concerns a premium prepaid subscriber, the EAGLE examines whether the call or text message is "in-network". An in-network call or text message refers to a call or text message from one of the network's own subscribers to another of the network's own subscribers. If it is "in-network", the EAGLE returns an INAP Continue message to instruct the MSC to continue the call (i.e. bypass the prepaid status check). For any other types of calls or messages, the EAGLE relays the IDP message to the prepaid SCP.

Info Analyzed Relay

Info Analyzed Relay (IAR) provides the ability to intercept AnalyzedInformation messages and apply Numbering Plan Processor (NPP) functionality. It consists of four features:

IAR Base

The IAR Base feature intercepts and processes AnalyzedInformation messages that are sent from a Mobile Switching Center (MSC) to a Service Control Point (SCP) or Services Node (SN). This feature supports the message processing functionality used by the IAR Additional Subscriber Data, IAR Generic Routing Number, and IAR Number Portability features.

IAR Additional Subscriber Data (IAR ASD)

The IAR ASD feature allows Additional Subscriber Data lookups to be performed on AnalyzedInformation messages.

IAR Generic Routing Number (IAR GRN)

The IAR GRN feature allows Generic Routing Number lookups to be performed on AnalyzedInformation messages.

IAR Number Portability (IAR NP)

The IAR NP feature allows the EAGLE to treat messages that relate to ported subscribers differently than non-ported subscribers. This feature provides support for IAR Service Portability.

Analyzed Information query with no EPAP/ELAP

This feature allows an AnalyzedInformation query to be responded to using an optional parameter that contains pre-configured response digits. These digits are configured to map to trigger type parameter values in the query. The Mobile Switching Center (MSC) that sent the AnalyzedInformation query interprets the response digits to route the call appropriately.

SIP Number Portability

The SIP Number Portability feature will provide SIP-based Number Portability using EAGLE's RxDDB. This feature adds a SIP interface to allow SIP NP requests to be received by an EAGLE card, processed by the EAGLE's RxDDB, and a response transmitted back to the requestor.

A new SIPHC GPL supporting a SIP stack over TCP/UDP has been added.

Figure below describes the overall system architecture

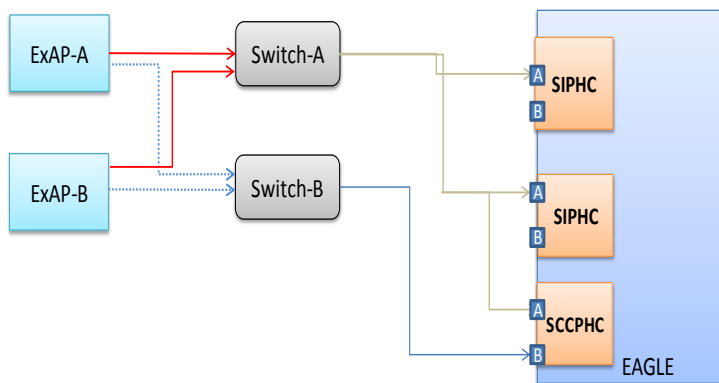


Figure 67: System Architecture for SIP Number Portability

SIP Application – FAX and MODEM URI Support and Configurable Thresholds

The SIP Application – FAX and MODEM URI Support and Configurable Thresholds feature adds support of FAX and MODEM as allowed schemes in SIP URI to perform Number Portability lookup on SIP INVITE message in the SIP application. The user can configure thresholds for the throughput limits. Alarms are raised based on the limits specified by the user.

ISUP-INTERCEPTION-BASED ROUTING AND NUMBER PORTABILITY SOLUTIONS

Triggerless ISUP Framework (TIF)

TIF Framework provides an overall structure for TIF features, which support ISUP messages. It allows the EAGLE to intercept messages that would normally be thru-switched and apply special processing to them. For example, an IAM could be intercepted and have the called number replaced based on portability information.

The flow of the TIF Framework is shown in Fig: xxx The TIF Framework consists of 2 main sections:

- » On the LIM, the TIF Framework uses gateway screening to select an MSU for processing, forwards it to Service Modules for processing.
- » On the Service Module cards, the TIF Framework decodes the MSU, invokes the Numbering Plan Processor, and encodes the results.

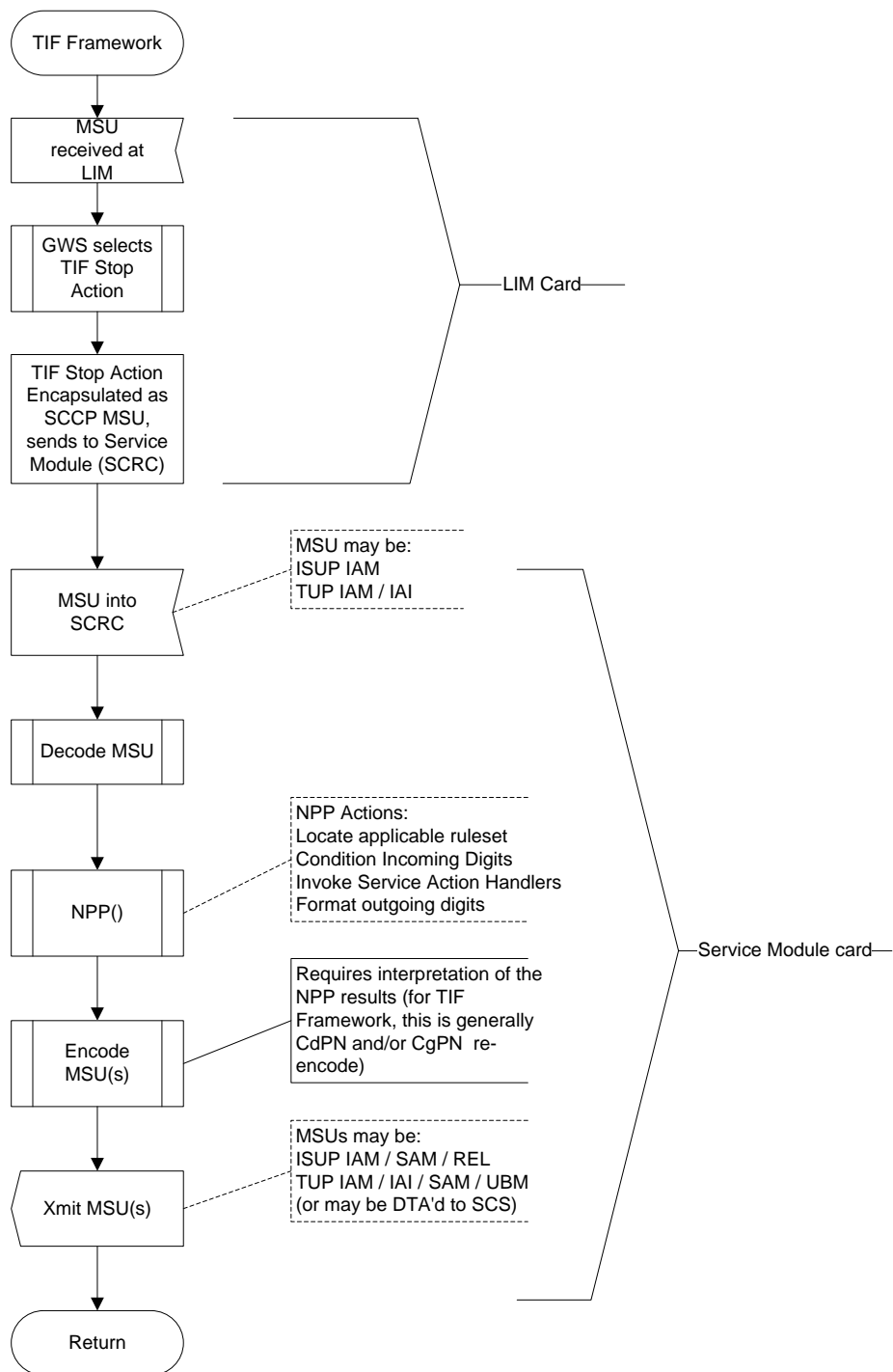


Figure 68: TIF Overview

TIF features are responsible for providing NPP with Service Action Handlers to perform database access, data evaluation, and any special handling for the MSU

TIF Calling Party Number Conditioning

There are 2 different methods for invoking the Calling Party within the TIF Framework:

1. Within CdPN NPP: The CdPN rule defined in NPP provides all instructions for handling the CgPN. Basic conditioning and formatting is supported via global TIFOPTS settings. This is the original design.
2. Separate CgPN NPP: the CgPN is processed via NPP rules, with access to all NPP Conditioning and Formatting controls. This is being added via PR 140600.

Prior to Release 44, there were 3 TIF NPP services – TIF, TIF2 and TIF3. These three services all do a lookup in the NPP Service Rule Set based upon data from the CdPN portion of the messages. These three CdPN services also do some minimal conditioning (controlled by TIFOPTS:CondCgPN) and formatting on the CgPN (controlled by TIFOPTS:IAMCGPN). This minimal conditioning and formatting is always done the same regardless of the CgPN's digits and NAI values. Service Actions concerning the CgPN are provisioned in the CdPN service, and use the minimally conditioned CgPN for their international form of the Calling Party.

In order to increase TIF CgPN functionality, the TIF framework is being enhanced to add TIF CgPN NPP services. The TIF CgPN NPP services will be invoked from the TIF CdPN NPP Service based upon the TIF CdPN Service Rule's INVKSERV value. Because TIF CgPN NPP services have full NPP processing, the user can use different conditioning and formatting for different CgPN and NAI values; thus giving the user more flexibility.

For this enhancement, three TIF CgPN NPP services are being added, which are TIFCGPN, TIFCGPN2 and TIFCGPN3. These services are tied to the TIF CdPN NPP services (TIF, TIF2, TIF3) in a one-to-one manner.. The TIF CdPN NPP Service Rules can have the INVKSERV value set to "NONE" or the associated TIF CgPN NPP Service name. If the INVKSERV parameter value is set to NONE, no additional NPP Services are invoked, so the old method processing is followed.

TIF Blacklisting

By allowing blocking ISUP IAM messages in different ways this feature provides EAGLE's TIF blacklist capabilities, which helps Network Operators to reduce significantly or even completely prevent spoofing their networks with illegal messages.

The existing TIF is not affected: new functionalities are added in addition to those already existing within TIF.

At this time 8 scenarios to generate ISUP RELEase MSU back to the originator of an incoming IAM based on Calling or Called Party Number are going to be implemented.

Following 4 TIF CgPN blacklist scenarios generate ISUP RELEase message back to the originator of processed ISUP IAM if:

1. the Calling Party number is found in RTDB and this found RTDB entry has CgBL flag = YES.
2. the Calling Party number is not found in RTDB.
3. the Calling Party begins with a specific prefix .
4. the Calling Party parameter is not present in the IAM or it is present with no digits in it.

The 4 scenarios of TIF CgPN blacklist functionality are controlled by FAKs: "TIF Subscr CgPN Blacklist" to turn ON/OFF two EPAP-based scenarios (1 & 2), and "TIF Range CgPN Blacklist" to turn ON/OFF two non-EPAP-based scenarios (3 & 4).

Following TIF CdPN blacklist scenarios generate ISUP RELEase message back to the originator of processed ISUP IAM if:

1. the Called Party number is found in RTDB and this found RTDB entry has CdBL flag = YES.
2. the Called Party number is not found in RTDB.

3. the Called Party begins with a specific prefix .
4. the Called Party is screened by TIF Selective Screening and the Release cause is not “NONE”.

The aforementioned scenarios of TIF CdPN blacklist functionality are controlled by FAK: “TIF Selective Screening” to turn ON/OFF 4 scenarios (5 – 8).

In order to provide configurable Release Cause values for the blacklist scenarios introduced with this feature, NPP is enhanced to associate 2 numeric values to each of the TIF BlackList and TIF Selective Screening Service Actions: first value to be used for ANSI ISUP and 2nd value – for ITU ISUP. These 2 values are enforced to be between 0 and 127. This new field in ent/chg/rtrv-npp-as commands will be called SAxVAL[1|2], where “x” is the same number as in appropriate SA, and this new parameter has 2 values assigned to it.

The figure below depicts the basic message-flow of TIF BlackList functionality:

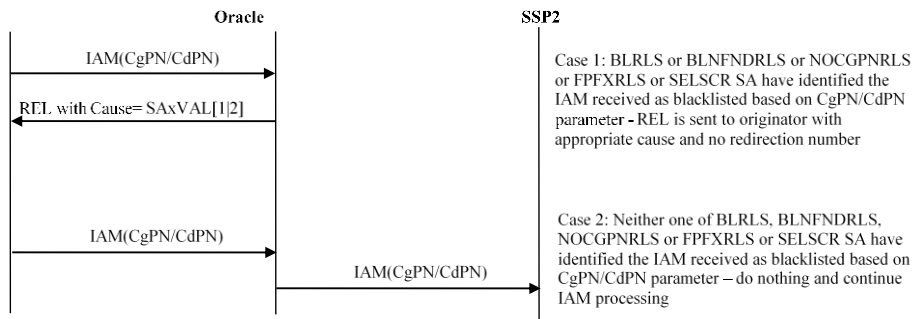


Figure 69: Basic Message Flow of TIF BlackList

TIF CdPN EPAP-based Selective Screening: SELSCR

A new CdPN Service Action is created: SELSCR. The SELSCR SAH indicates that the message is selectively screened based on CdPN and CgPN Call Types. The SELSCR SA also supports SAxVAL[1], SAxVAL[2] and SAxDGTS parameters. The SAxVAL[1] parameter indicates the Release cause for ANSI MSUs. The SAxVAL[2] parameter indicates the Release cause for ITU MSUs. The SAxDGTS parameter indicates the Call Type for CdPNs that match the associated NPP Rule.

If the SAxVAL parameter (Release Cause) for the SELSCR SA is configured in TIF NPP Service, it indicates that a RELEase should be generated. If the SAxVAL parameter (Release Cause) is not configured for the SELSCR SA, it indicates that the message should be RELAYed after modification as per FASCRCd and FASCRCG FA list configuration in the NPP Action Set associated with TIF NPP Service.

The following steps explain the TIF Selective Screening Process and how it performs selective screening:

1. Check if the TIF Selective Screening Feature ON? If “ON”, proceed to next step else continue to next SA.
2. Is the SAxDGTS field provisioned for the SELSCR SA? If yes, jump to step 5 else proceed to next step.
3. Perform RTDB lookup on CdPN. Is CdPN present in RTDB? If yes, proceed to next step else continue to next SA.
4. Are Call Types provisioned for CdPN? If yes, proceed to next step else continue to next SA.
NOTE: CdPN Call Types can be provisioned either in SAxDGTS parameter or in RTDB in ‘Number Substitution DN’ field. The SAxDGTS parameter holds preference over the RTDB ‘Number Substitution DN’ field for theCdPN.
5. Is the first Call Type provisioned for CdPN = ‘*’? If yes, the CdPN is screened else continue to next step.
6. Is valid CgPN present in Message? If yes, proceed to next step else continue to next SA.

7. Perform RTDB lookup on CgPN. Is CgPN present in RTDB? If yes, proceed to next step else continue to next SA.
8. Are Call Types provisioned for CgPN? If yes, proceed to next step else continue to next SA.
9. Is the first call type provisioned for CgPN = '*'? If yes, then CdPN is screened else continue to next step.
10. Match the first Call Type provisioned for the CdPN with the all the provisioned Call Type for the CgPN. Does first Call Type in the CdPN match with any Call Type in the CgPN? If yes, the CdPN is screened else continue to next SA

TIF ASD and TIF GRN support

This feature adds support for TIF ASD and TIF GRN. TIF ASD allows for the insertion of an ASD digit string into the CdPN or CgPN of an outgoing IAM or Redirection number of REL ISUP message. TIF GRN allows for the insertion of a GRN digit string into the CdPN or CgPN of an outgoing IAM or Redirection number of REL ISUP message. The values for both ASD and GRN are obtained from the RTDB. ASD/GRN are assigned against Individual or Range DN entry in RTDB.

TIF ASD and TIF GRN are built upon the services provided by the TIF framework and are considered to be “TIF applications” or “TIF services”. TIF ASD and TIF GRN allow retrieval of ASD/GRN from the RTDB based on the lookup of the CgPN and CdPN digits. In both cases of CdPN, CgPN or Redirection number (in case of NPRLS) is modified with ASD/GRN. ASDLKUP and GRNLKUP SAs for TIF CdPN service allows retrieval of ASD/GRN from CdPN of incoming IAM message to be inserted into the outgoing CdPN digits. CgPNASDRqd and CgPNGRNRqd SAs for the TIF CdPN service allows retrieval of ASD/GRN from CgPN of incoming IAM message to be inserted into the outgoing CdPN digits. ASDLKUP and GRNLKUP SAs for TIF CgPN service allows retrieval of ASD/GRN from CgPN of incoming IAM message to be inserted into the outgoing CgPN digits.

The TIF ASD/GRN feature introduces following additions to NPP:

- » Conditioning Action: No new conditioning Actions are defined by the feature.
- » Service Action:
 1. ASDLKUP, CgPNASDRqd introduced by TIF ASD
 2. GRNLKUP, CgPNGRNRqd introduced by TIF GRN.
- » Formatting Action: TIF ASD/GRN feature uses ASD and GRN formatting actions that are already being supported by the NPP framework.

Prior to PR 140600, the TIF ASD and GRN feature was only supported with the TIF CdPN service (TIF, TIF2, and TIF3). With the introduction of PR 140600, the TIF ASD and GRN feature is extended to allow support with the newly created TIF CgPN service (TIFCGPN, TIFCGPN2, and TIFCGPN3). The ASDLKUP and GRNLKUP SAs can be associated with a TIF CdPN service ruleset or a CgPN service ruleset. The CgPNASDRqd and CgPNGRNRqd SAs can only be associated with a TIF CdPN service ruleset.

With PR 140600, the ASDOTHER and GRNOTHER formatting actions are introduced. The ASDOTHER formatting action allows the ASD returned from a RTDB search in the ASDLKUP SA for TIF CgPN service to be used in CdPN formatting. The GRNOTHER formatting action allows the GRN returned from a RTDB search in the GRNLKUP SA for TIF CgPN service to be used in CdPN formatting.

The TIF CgPN service is invoked by the TIF CdPN service by setting the INVKSERV value in the ENT-NPP-SRS command to the appropriate TIF CgPN service (TIFCGPN, TIFCGPN2, or TIFCGPN3).

This section contains two basic use cases for TIF ASD and GRN. The first use case shows the TIF ASD for TIF CdPN service. The second use case shows the TIF GRN for TIF CgPN service.

TIF ASD use case for TIF CdPN Service

The following diagram shows the steps involved in a basic TIF CdPN ASD use case. In this case, the following TIF rules are assumed:

- » Filter FPFX=123
- » Filter FDL=13
- » Conditioning Action set=CC3+AC3+SN7
- » Service Action set=CgPNASDRqd
- » Formatting Action set= CC+ASD+AC+SN

An IAM message is received and an ASD value (a5d) from the database is inserted into the CdPN in the outgoing IAM message. The IAM message is then relayed.

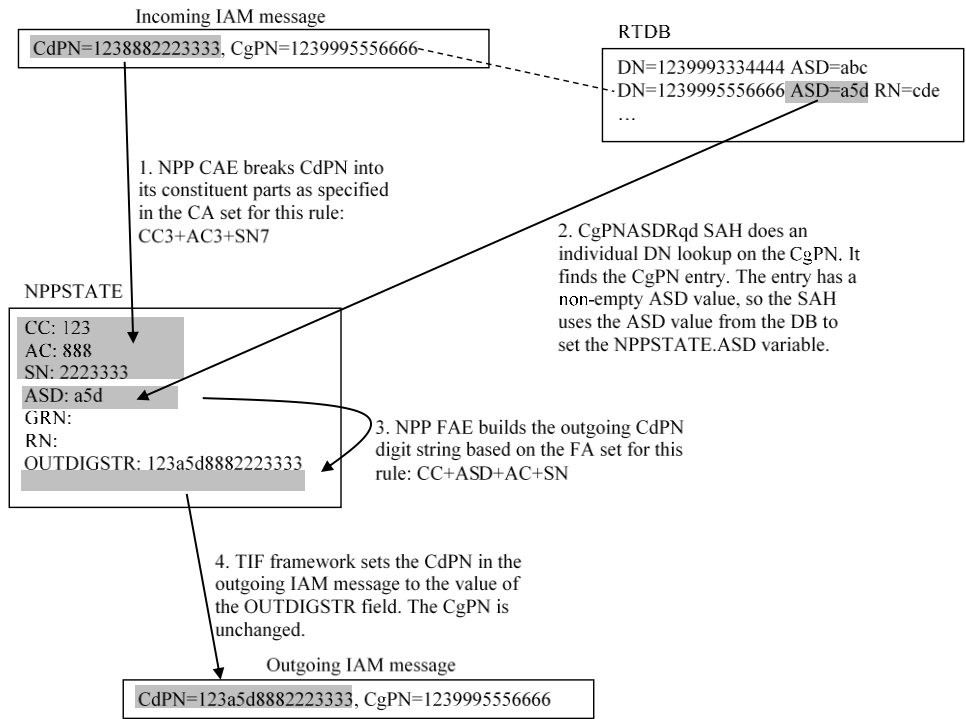


Figure 70: Basic Operation of TIF ASD for TIF CdPN Service

TIF GRN use case for TIF CgPN service

The following diagram shows the steps involved in a basic TIF CgPN GRN use case. In this case, the following TIFCGPN rules are assumed:

- » Filter FPFX=123
- » Filter FDL=13
- » Conditioning Action set=CC3+AC3+SN7
- » Service Action set=GRNLKUP
- » Formatting Action set= CC+GRN+AC+SN

An IAM message is received and an GRN value (a5d) from the database is inserted into the CgPN in the outgoing IAM message. The IAM message is then relayed.

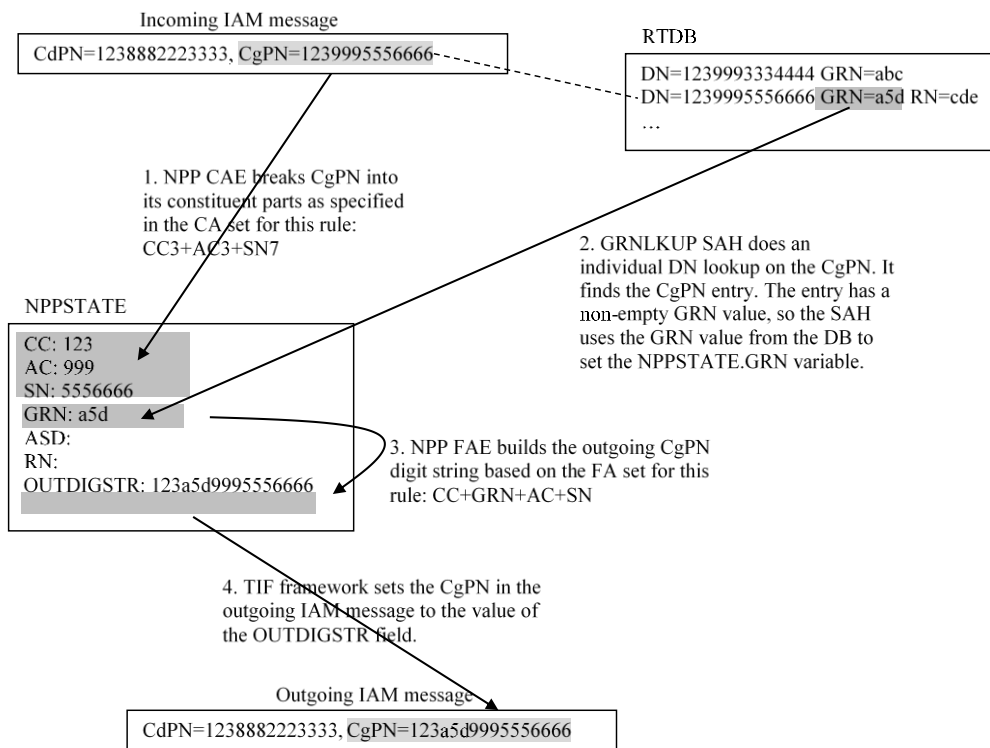


Figure 71: Basic Operation of TIF GRN for TIF CgPN Service

TIF ASD use case for TIF CgPN service using ASDOTHER

The following diagram shows the steps involved in a basic TIF CgPN ASD use case where ASDOTHER is specified as a TIF CdPN formatting action. In this case, the following TIF and TIFCGPN rules are assumed:

- » TIF rule:
 - » Filter PPFX=456
 - » Filter FDL=13
 - INVKSERV=TIFCGPN
 - » Conditioning Action set=CC3+AC3+SN7
 - » Service Action set=CDIAL
 - » Formatting Action set= CC+ASDOTHER+AC+SN
- » TIFCGPN rule:
 - » Filter PPFX=123
 - » Filter FDL=13
 - » Conditioning Action set=CC3+AC3+SN7
 - » Service Action set=ASDLKUP
 - » Formatting Action set= CC+AC+SN

An IAM message is received and an ASD value (a5d) from the database is inserted into the CdPN in the outgoing IAM message. The IAM message is then relayed.

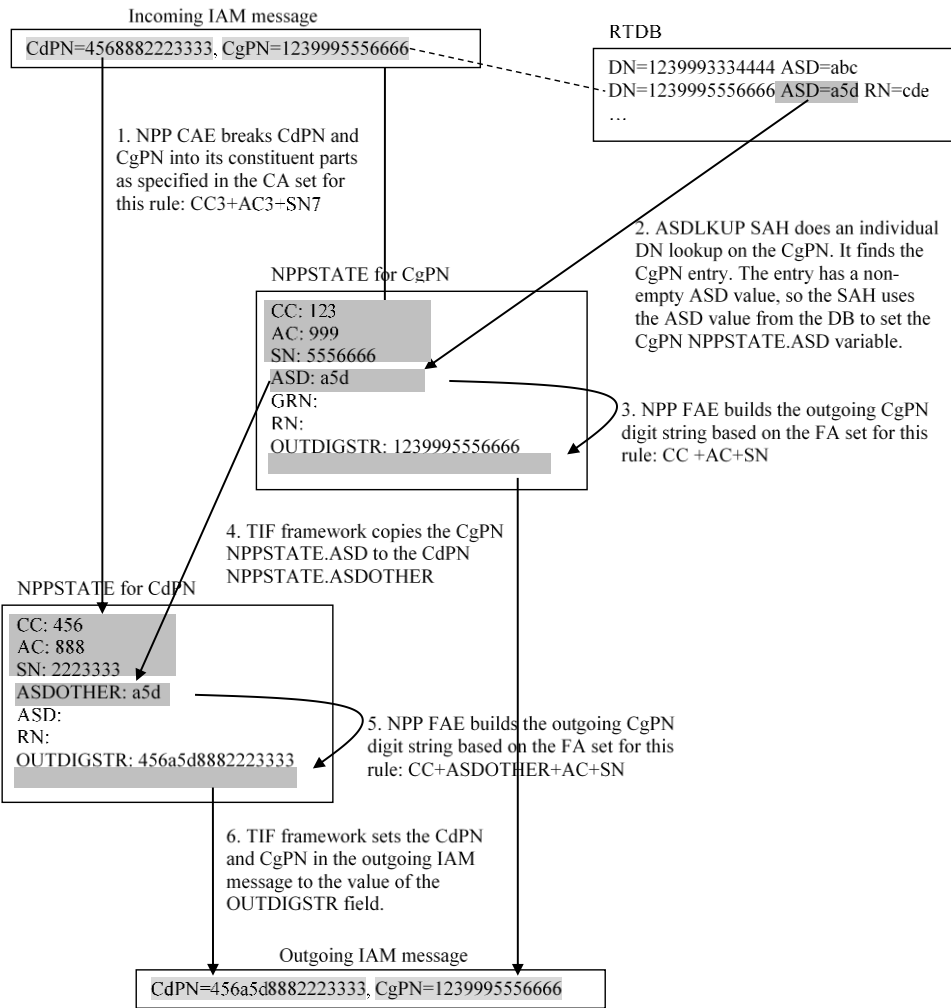


Figure 72: Basic Operation of TIF ASD for TIF CgPN service using ASDOTHER

MESSAGE FLOWS

The following figure shows TIF ASD use cases for TIF CdPN service.

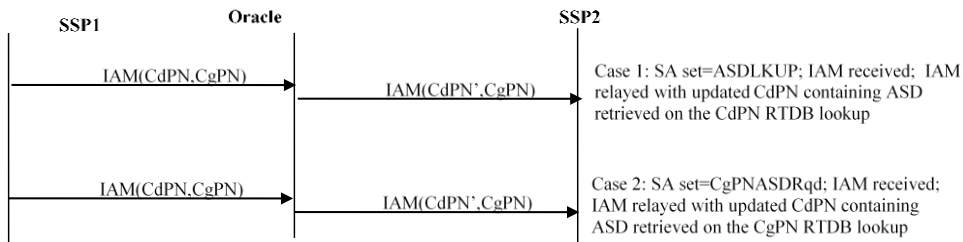


Figure 73: ISUP IAM Message Flows for TIF ASD for TIF CdPN service

The following figure shows TIF ASD use cases with NPRLS and NPNRLS for TIF CdPN service.

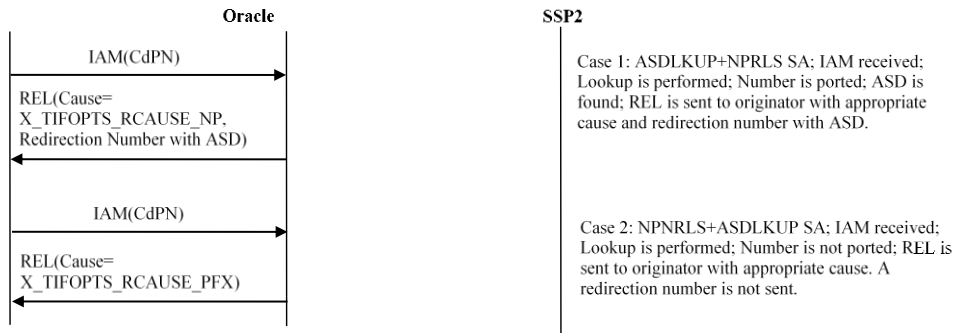


Figure 74: ISUP REL Message Flow for TIF ASD for TIF CdPN service

The following figure shows TIF GRN use cases for TIF CdPN service.

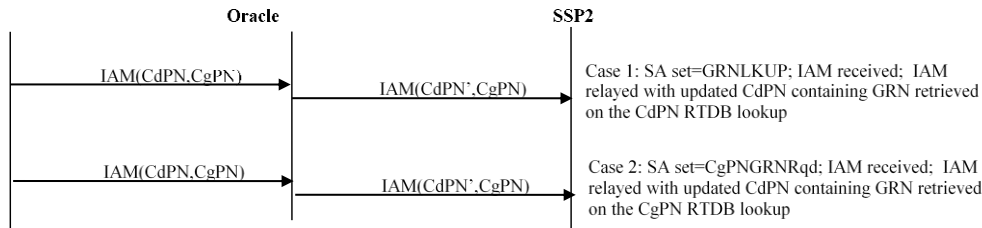


Figure 75: ISUP Message Flows for TIF GRN for TIF CdPN service

The following figure shows TIF GRN use cases with NPRLS and NPNRLS for TIF CdPN service.

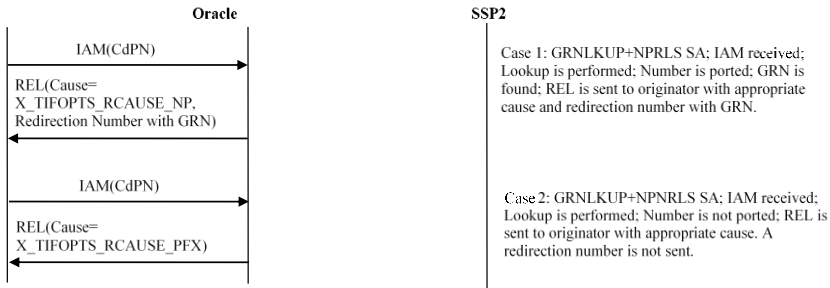


Figure 76: ISUP REL Message Flow for TIF GRN for TIF CdPN service

The following figure shows TIF ASD use cases for TIF CgPN service.

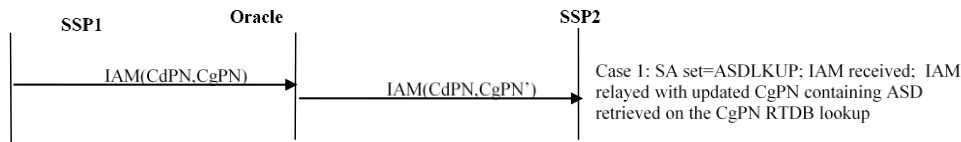


Figure 77: ISUP IAM Message Flows for TIF ASD for TIF CgPN service

The following figure shows TIF GRN use cases for TIF CgPN service.

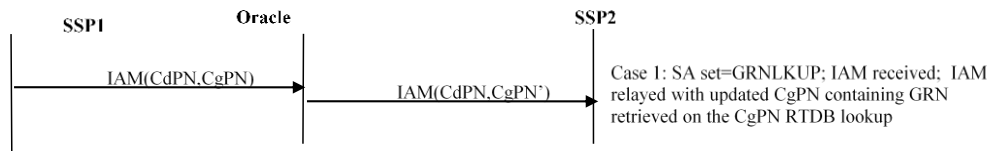


Figure 78: ISUP IAM Message Flows for TIF GRN for TIF CgPN service

TIF NP - Triggerless ISUP Framework Number Portability

TIF NP is the next evolution of the previous TINP feature set. In this present version of the Feature Guide, TINP is retained alongside TIF NP for transitional purposes, as TINP and TIF NP will both continue to be supported for the time being. However, it is expected that TIF NP would eventually replace existing installations of the TINP feature due to the much greater flexibility and usability of the TIF NP service in comparison with the previous TINP feature.

TIF NP essentially links the Numbering Plan Processor (NPP) infrastructure (see Numbering Plan Processor (NPP)) into the EAGLE's Triggerless ISUP NP functionality, making the feature far more flexible and usable across various operator implementations. This flexibility is especially needed in triggerless ISUP applications due to the wide variances of numbering plans and formats used in ISUP messaging in different operators' networks throughout the world.

TIF NP utilizes the configurable filters, conditioning actions, service actions, and formatting actions introduced by the NPP framework to provide several enhancements to the previous TINP feature. The capabilities and enhancements are detailed in the following subsections:

Relay Message

If the EAGLE is configured to send a relay message, and if the CDPN is a ported-out number, the EAGLE prepends the Routing Number that identifies the subscription network of the ported-out number to the CDPN before relaying the IAM message to its intended destination. If the CDPN is a ported-in or non-porting number, the EAGLE prepends a Network ID that identifies a sub-network within the operator network to the CDPN before relaying the IAM message to its intended destination. For other types of calls, such as international calls, or calls to a non-porting number, the EAGLE will simply relay the message to its intended destination.

The example in the figure below, shows a call to a ported subscriber with an EAGLE action set to generate a relay message. The portability information is encoded in the CDPN.

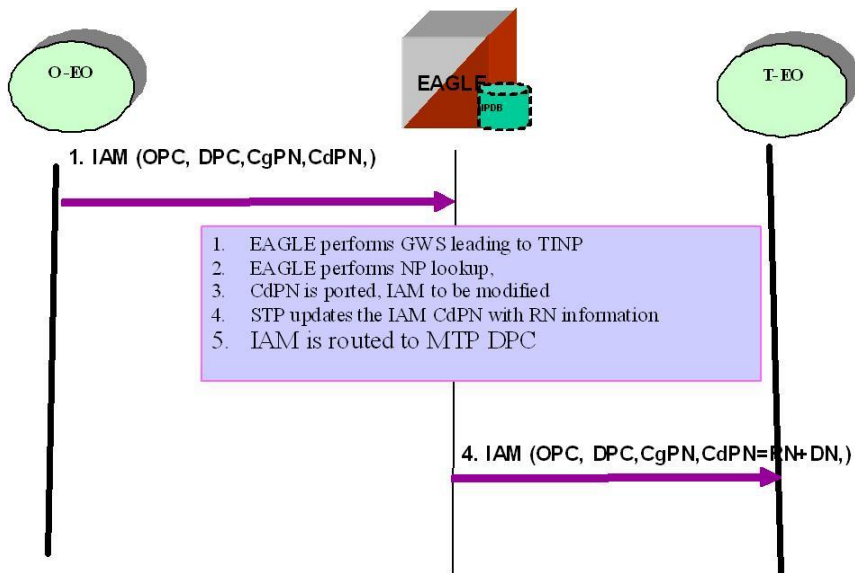


Figure 79: Call to Ported Subscriber with IAM Relay and NP Flags

The prefix or network ID prepended in the IAM message allows the destination switch to differentiate between an in-network call or an off-network call so that different billing rates or routing schemes can be applied to the call. For example:

- » Apply different charging rates to prepaid calls.
- » Reroute calls based on the network ID prepended to the CdPN of an IAM messages.
- » Segregate traffic based on the network ID prepended to the CdPN of an IAM messages.

Release Message

If the EAGLE is configured to send a release message, the EAGLE generates a release message with the Redirection Number before the call is eventually routed to the intended destination. The format of the Redirection Number can be configured to contain the RN (Routing Number information) and/or the DN (Dialed Number).

The example in the figure below shows a call to a ported subscriber with an EAGLE action set to generate a Release message (REL).

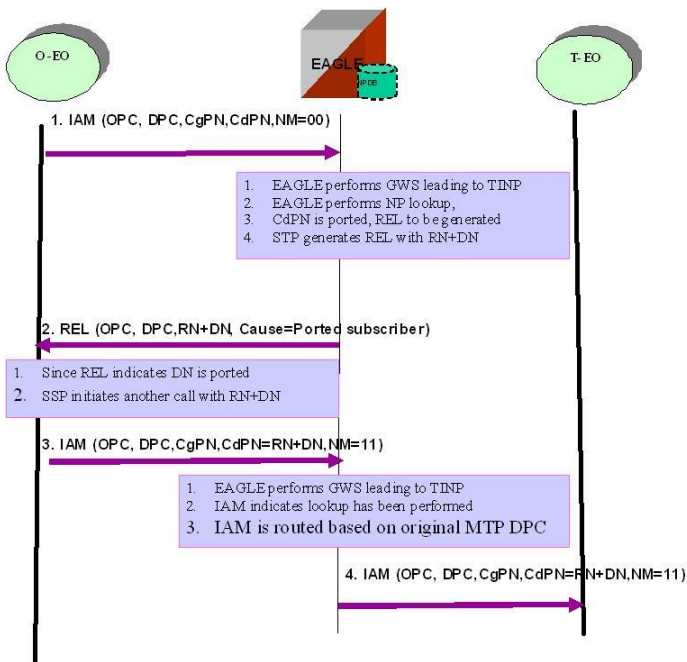


Figure 80: Call to Ported Subscriber with REL Message and NP Flags

Circular Route Prevention

The Circular Route Prevention (TINP CRP) function is an extension of the triggerless ISUP NP feature which helps in cases of circular routing caused by incorrect information in one or more networks' number portability databases. For example, a subscriber may have ported from network A to network B. Network A has the correct routing information, indicating the subscriber now belongs to network B. However, network B may have incorrect routing information, indicating that the subscriber still belongs to network A. In this case, network A will route the call to network B, based on its portability data, but network B will route the call back to network A, based on its incorrect data. This would result in a circular route. The TINP CRP function provides logic to prevent this scenario similar to the CRP logic used within the MNP and A-Port features, as follows:

- » If the routing number prefixed to the CdPN of an incoming IAM is a routing number of the network receiving the message (i.e. the RN prefixed to the incoming CdPN is found in the EAGLE's HomeRN list), and
- » If the result of the RTDB lookup is another RN, then a loop is detected and the call is released with ISUP REL message).
- » Else, normal processing continues.

Enhanced CgPN Lookup

TIF NP introduces Calling Party RTDB lookups into the triggerless ISUP NP feature set. TIF NP filtering rules (e.g. NPP) applies, such that CgPN lookups may be specified only for certain call types. For example: Imagine a customer that needs to determine if roaming calls are allowed to make the requested national long distance call. An important input into this decision is the current portability status of the caller. Thus, a CgPN (A party) NP check needs to be performed as part of the overall TIF NP service. However, the CgPN lookup only needs to be conducted for national long distance calls. The NPP filter rules can be provisioned in such a way that only digit strings denoted a national long distance call will trigger the CgPN NP lookup.

Number Portability Actions

Triggerless ISUP-based number portability can have one of two terminating actions:

1. Relay - a successful RTDB lookup indicates that the message should be relayed and formatted in a prescribed format (Usually with the RN prefixed to the called number).
2. Release - a successful RTDB lookup indicates that original message is discarded and that a release message is created, containing the routing information in a prescribed format.

Prior to TIF NP, the operator could only select these actions globally for messages processed by TINP. However, there are cases in which the service selection needs to be more precise. For example, IAMs originating at an in-network transit switch and terminating to a point code outside the local operator may require release functionality, while other IAMs require only relay handling.

TIF NP introduces the capability to tailor the number portability actions based on the characteristics of the incoming messages. Furthermore, TIF NP allows variations of release handling based on the configured rulesets. The following options are available:

This next requirement is fairly straight-forward. When using the release version of number portability, customers wish to specify:

1. Per-rule release cause value to be used in the release message.
2. Per-rule decision to include the RN or not in the release message.
3. Per-rule options for formatting of the RN in the release message.

Filtering for Number Portability

The term filters means a set of criteria that can be used to indicate a set of actions (rules) that need to be carried out. In the context of the TINP feature prior to TIF NP, the filters consist of Gateway Screening (GWS) rules, based on OPC, DPC, SIO and message type. However, experience has shown that service selection for ISUP-based number portability needs to be more specific and more flexible.

The figure below illustrates an example of a set of more complex filters that can be achieved with TIF NP.

Table 18: Example of Complex Filtering Rules for ISUP NP - Relay

Calltype	Incoming Format	3 Part Filter		
		NAI	Digit Prefix	Digit Length
Local Collect	b+AC+9090+DN		b	14
Local Call	b+AC+DN		b	10
Long distance call using BrT as LD operator	014+AC+DN		0	12
Long distance call using any operator as LD operator	0+CSC+AC+DN	Unknown	014	10
Local call	DN		*	8
Ported call from Other	060+CSC+AC+DN		060'	12

Operator	060+DN		060	8
	060+AC+DN		060'	10
Already ported	d+anything		D	*

The above set of filters would result in a relay action. The next figure shows an example of filters resulting in Release.

Table 19: Example of Complex Filtering Rules for ISUP NP – Release

Calltype	Incoming Format	3 Part Filter		
		NAI	Calltype	Incoming Format
Ported Iner-operator outgoing call	060 + anything		060	*
Already Ported	d+anything		D	*
Collect Call	9090+DN		9090	8
Local Call	DN	Unknown	*	8

Number Conditioning for TIF NP Lookups

TINP prior to TIF NP also has somewhat limited options for pre-RTDB number conditioning. TIF NP allows a much more flexible set of options for number conditioning prior to DB lookup.


Number Conditioning takes an incoming number string and processes so that it matches the internationally unique format (CC+AC+DN) in the EPAP database. Number conditioning applies to all TIF services using the EPAP database to perform a lookup. Take the digit string b+AC+ 9090 + DN from the preceding filtering example:

1. The 'b' prefix needs to be removed, which leaves: AC+ 9090 + DN.
2. The 'AC' is the area code ('NDC' is used in some network for the same purpose, and could be substituted here) and needs to be removed, but saved as a token for use in the RTDB query. This leaves 9090 + DN.
3. The '9090' prefix needs to be removed, but saved as a token for formatting the DN in the outgoing message. This leaves just DN.
4. The Area Code removed in step 2 needs to be prefixed to the result of step 3, resulting in AC+ DN.
5. The default country code (provisioned in the EAGLE) needs to be prefixed to the result of step 4, resulting in CC+AC+DN
6. Now the RTDB lookup can be performed using the digits CC+AC+DN.

This is just one example of the powerful use of TIF NP. As can be seen, TIF NP provides a much more powerful set of functionality as compared to the previous TINP feature.

TIF Simple Number Substitution

There are situations in some customers' networks whereby a set of switches cannot support the numbering ranges of ported numbers. For example: a customer's network may have owned the 4XXX number range, and its switches were programmed to support only 4XXX. However, after portability is introduced, the switches now need to support 5XXX and 6XXX number ranges as well. In some cases, older switches are not able to be programmed to handle



the new number ranges. In other cases, the operator may be seeking an alternative to re-programming all the switches in the network.

The TIF “Simple” Number Substitution feature in Release 39.2 takes a first step toward addressing this problem. TIF Simple Number Substitution allows the operator to select specific calls for which to provide CgPN substitution. Based on a matched CdPN filter and an action found in the rule, the CgPN will be replaced with one provisioned in the EAGLE.

The Simple Number Substitution feature allows only one provisioned CgPN to be exchanged with incoming CgPN, and is therefore limited in scope and application. A more flexible and thorough version of Number Substitution, which could allow substitution of both A and B number, as well as per-subscriber (as opposed to global) substitution digits, may be planned for a future release.

The TIF Simple Number Substitution feature does not require the EPAP provisioning. The substitution digits are provisioned via standard EAGLE commands.

TIF Number Substitution using Numbering Plan Processor

The Triggerless ISUP Framework (TIF) Number Substitution feature allows called party and/or calling party numbers on an incoming Initial Address Message (IAM) to be substituted with associated numbers from the RTDB on the outgoing IAM.

When an IAM is received, a lookup is performed on the called party number (CdPN) or calling party number (CgPN) in the RTDB database. If a successful retrieval of the called party directory number (DN) occurs, then the CdPN is substituted in the outgoing IAM. If a successful retrieval of the calling party DN occurs, the CgPN is substituted in the outgoing IAM.

The feature introduces the `nscdpn` and `nscgpn` Service Actions, which are used to perform a lookup for the incoming CdPN and CgPN, respectively. These Service Actions are used with the Numbering Plan Processor (NPP). For information on the Numbering Plan Processor and TIF, refer to the Numbering Plan Processor (NPP) Overview and the Feature Manual - TIF, respectively, of the latest EAGLE documentation set.

TIF Enhancements including IAM/SAM Splitting based on DPC

The TIF Enhancements including IAM/SAM Splitting based on DPC enhancement provides additional functionality for the EAGLE regarding ITU Incoming Address Messages (IAMs) that are processed by the Triggerless ISUP Framework (TIF). For additional information on TIF processing, refer to the Feature Manual - TIF. The new options are configured in the Destination and TIFOPTS tables.

IAM/SAM Splitting based on DPC

ITU IAMs can be split into an IAM message and an SAM message. Enabling of IAM/SAM splitting and the maximum length of the Called Party Number (CdPN) that triggers IAM/SAM splitting can be configured. Note: IAM/SAM splitting can be performed on all ITU IAMs that are processed by TIF. The message does not have to match a Numbering Plan Processor (NPP) rule or undergo digit modification.

Release Cause

Generation of a Release message based on the originating point code (OPC) of ANSI or ITU IAMs can be configured.

NM Bits Reset

The NM Bits for ITU IAMs can be configured to reset to 00.

SMS NUMBER PORTABILITY AND ROUTING SOLUTIONS

GSM Prepaid SMS Intercept

Mobile operators offering prepaid short message service (SMS) need an efficient way to perform credit checks on the subscriber sending or receiving the message prior to allowing the message to be delivered. Intelligent network (IN) databases are generally used to perform the actual credit check. However, these databases can become overloaded if messages are sent to them for evaluation unnecessarily. An example of such a case is when all short messages, including those from or to postpaid subscribers, are sent to the IN platform for evaluation. The messages from postpaid subscribers do not need a credit check, so this is additional traffic the IN platform must process unnecessarily.

Therefore, additional filtering and screening is needed in the SS7 network to provide a finer granularity in determining which messages actually need to be sent to the IN platform, and which may simply be routed.

The initial offering of the Prepaid SMS Intercept feature will deal only with non-segmented mobile originated SMS, i.e. those messages sent from a mobile handset through a Mobile Switching Center (MSC) to the Short Message Service Center (SMSC). Support for mobile terminated SMS, i.e. those messages sent from a SMSC through an MSC destined for a mobile handset, is under consideration for a future EAGLE release.

The Prepaid SMS Intercept feature will screen incoming messages from MSC based on the operation code contained in the Mobile Application Part (MAP) portion of the message. If the op-code indicates the message is a MAP_MO_FORWARD_SHORT_MESSAGE (MO_FSM), the sender's Mobile Station Integrated Service Digital Network (MSISDN) number will be retrieved from the MAP layer and a database lookup performed to determine if the subscriber is a prepaid or postpaid subscriber. If the MSISDN belongs to a postpaid subscriber, the message will be routed to the SMSC. If the MSISDN belongs to a prepaid subscriber, the message will be diverted to a third-party IN platform for a credit check before allowing the message to be delivered to the SMSC.

The MAP_FORWARD_SHORT_MESSAGE, referred to as FSM in this document is an SS7 message which is used to carry a text message (i.e. the "short message") being transmitted from the mobile handset of one subscriber to the mobile handset of another subscriber. In practice, the short message is delivered first to the SMSC belonging to the network of the sending subscriber. The SMSC is then responsible for sending the short message to the intended recipient, who may be in a different network. In MAP version 1, the FSM message is used for both legs of the delivery. In MAP versions 2 and 3, a MO_FSM (mobile originated) message is used to deliver the message from the sender to the SMSC, and a MT_FSM (mobile terminated) message is used to deliver the message from the SMSC to the recipient. This feature supports all MAP versions, but does not support segmented SMS, which may occur in MAP versions 2 and 3.

Message Flows

NOTE: The Prepaid SMS Intercept (PPSMS) feature uses a process of SSN discrimination to aid in message selection. In the remainder of this document, the entity "SMSC" will be used when referring to SCCP CdPA SSN discrimination. This is for clarity in the description of the function of PPSMS. In the ITU protocol, there is no specific SSN defined for SMSC. Thus, in practice, most operators use the SSN defined for MSC as the SMSC's SSN also. The PPSMS protocol uses this same implementation. Therefore, all commands will use MSC terminology and the SSN for MSC (8) when defining SMSC.

» Successful Delivery of MO_FSM from Postpaid Subscriber

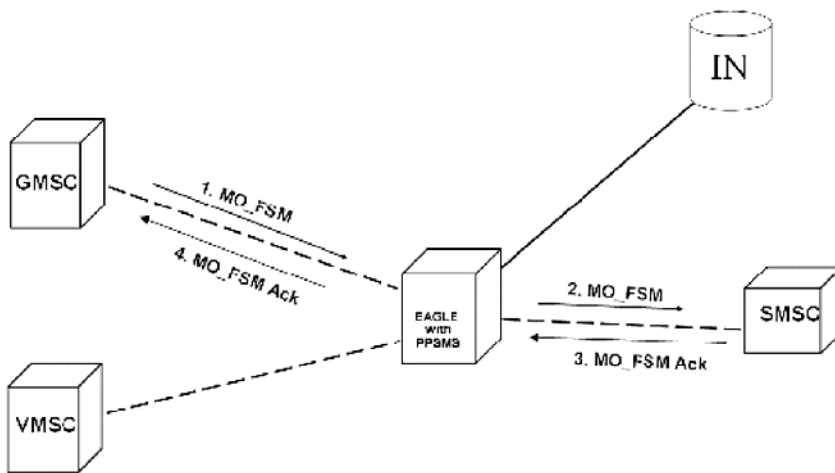


Figure 81: Delivery of MO_FSM from Postpaid Subscriber

1. GMSC sends MO_FSM to EAGLE with PPSMS.

Based on MTP DPC = The EAGLE point code and SCCP CdPA TT, NP, NAI, and GTI, the message is pre-selected for PPSMS service. EAGLE performs CdPA SSN discrimination. CdPA SSN = SMSC (8 - same as MSC), thus PPSMS service is selected. Otherwise, the message falls through to GTT.

Next, the MAP Opcode and SCCP CgPA GTA are examined. The Opcode is MO_FSM and the CgPA GTA is not from one of the IN platforms, therefore, PPSMS processing continues. (If Opcode is not MO_FSM, or if CgPA GTA is for one of the IN platforms, the message falls through to GTT).

The EAGLE queries the DB using sender's MSISDN from SM RP OA field in MAP portion of message. MSISDN is present in the database, but "Type" is neither "prepaid1" nor "prepaid2", meaning the sender is not a prepaid subscriber.

2. The EAGLE therefore GTT-routes the MO_FSM to the SMSC.
3. The SMSC returns the MO_FSM_ack.
4. The EAGLE either GTT- or MTP-routes the ack message to the GMSC.

» Successful Delivery of MO_FSM from Prepaid Subscriber

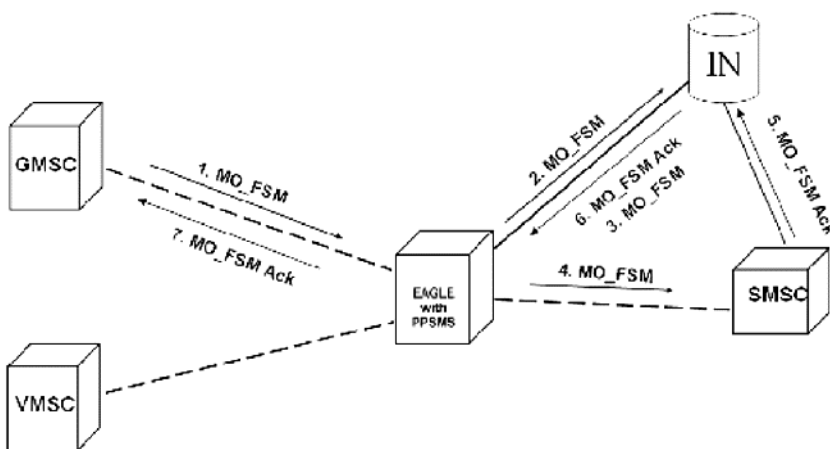


Figure 82: Successful Delivery of MO_FSM from Prepaid Subscriber

1. GMSC sends MO_FSM to EAGLE with PPSMS.

Based on MTP DPC = The EAGLE point code and SCCP CdPA TT, NP, NAI, and GTI, the message is pre-selected for PPSMS service. EAGLE performs CdPA SSN discrimination. CdPA SSN = SMSC (8 - same as MSC), thus PPSMS service is selected. Otherwise, the message falls through to GTT.

Next, the MAP Opcode and SCCP CgPA GTA are examined. The Opcode is MO_FSM and the CgPA GTA is not from one of the IN platforms, therefore, PPSMS processing continues. (If Opcode is not MO_FSM, or if CgPA GTA is for one of the IN platforms, the message falls through to GTT).

The EAGLE queries the DB using sender's MSISDN from SM RP OA field in MAP portion of message. MSISDN is present in the database, and the "Type" is "prepaid1", meaning the sender is a prepaid subscriber.

- The EAGLE forwards the MO_FSM to the IN Platform associated with "prepaid1", after checking mated application or mated relay node table for loadsharing information.

NOTE: the Portability Types "prepaid1" and "prepaid2" are used to select which of the two IN platforms the message should be sent to.

- The IN Platform checks the account, finds there is enough credit to send the message, and sends the MO_FSM to the SMSC via the EAGLE with PPSMS.
- Message arrives at EAGLE and is again pre-selected for PPSMS service based on CdPA TT, NP, NAI, GTI, and CdPA SSN = SMSC. Opcode is MO_FSM but the SCCP CgPA GTA is that of the IN platform, therefore, PPSMS service is not selected and message falls through to GTT and is routed to SMSC.
- The SMSC returns the MO_FSM_ack to the IN platform via the EAGLE, which either MTP- or GTT-routes the message to the IN platform.
- The IN Platform transfers the MO_FSM_ack to the first TCAP transaction and sends the MO_FSM_ack to the GMSC via the EAGLE, which either MTP- or GTT-routes the message to the GMSC.

» Unsuccessful Delivery of MO_FSM from Prepaid Subscriber

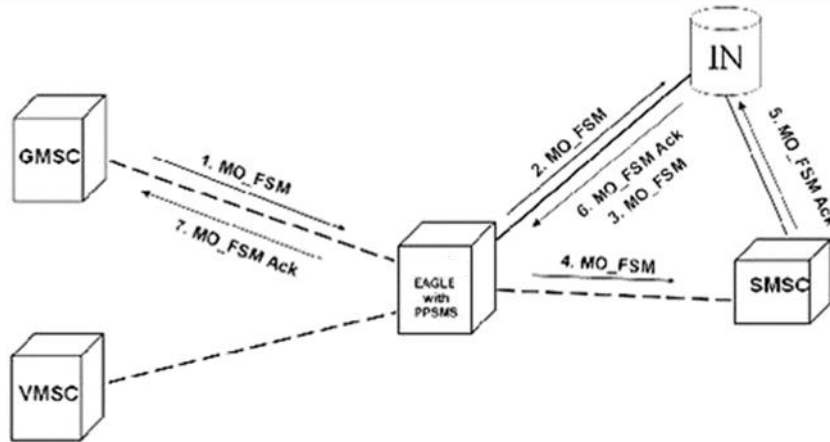


Figure 83: Unsuccessful Delivery of MO_FSM from Prepaid Subscriber

- GMSC sends MO_FSM to EAGLE with PPSMS.

Based on MTP DPC = The EAGLE point code and SCCP CdPA TT, NP, NAI, and GTI, the message is pre-selected for PPSMS service. EAGLE performs CdPA SSN discrimination. CdPA SSN = SMSC (8 - same as MSC), thus PPSMS service is selected. Otherwise, the message falls through to GTT.

Next, the MAP Opcode and SCCP CgPA GTA are examined. The Opcode is MO_FSM and the CgPA GTA is not from one of the IN platforms, therefore, PPSMS processing continues. (If Opcode is not MO_FSM, or if CgPA GTA is for one of the IN platforms, the message falls through to GTT).

The EAGLE queries the DB using sender's MSISDN from SM RP OA field in MAP portion of message. MSISDN is present in the database, and the "Type" is "prepaid1", meaning the sender is a prepaid subscriber.

2. The EAGLE forwards the MO_FSM to the IN Platform associated with "prepaid1".
3. The IN Platform checks the account, finds there is not enough credit to send the message, and rejects the message by returning a MO_FSM_Neg_Response to the GMSC via EAGLE.
4. The EAGLE either MTP- or GTT-routes the message to the GMSC

Loadsharing between Multiple IN Platforms

The PPSMS features allow SMS traffic to be loadshared between up to three external IN platforms. This is accomplished as follows:

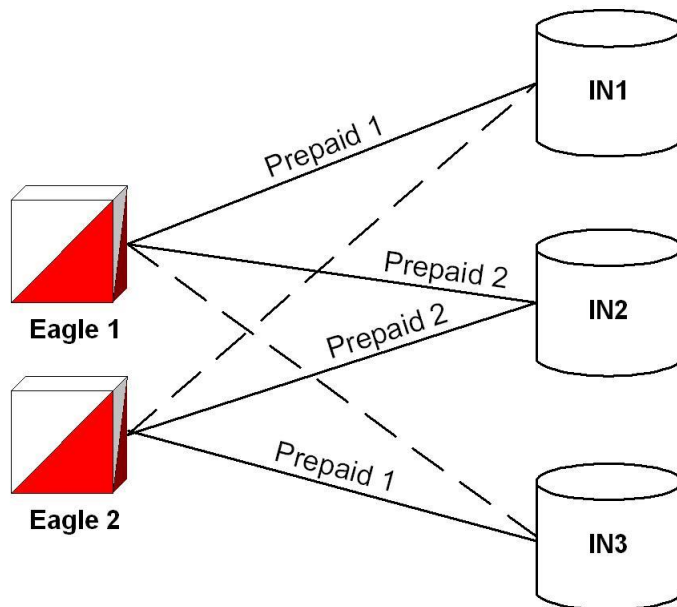


Figure 84: PPSMS IN Platform Loadsharing

In the figure above, three IN platforms are being used for handling of prepaid customers. Each EAGLE has the PPSMS feature turned on.

- » EAGLE 1 has translation information (PC and RI) provisioned in the GSMOPTS table for IN1 and IN2. It has been configured to send all MO_FSMs for prepaid type 1 subscribers to IN1 and all MO_FSMs for prepaid type 2 subscribers to IN2.
- » In its mated application (MAP) table and mated relay node (MRN) table, EAGLE 1 has IN3 provisioned as a mate point code for IN1 and the two are denoted as being in a loadsharing relationship. Note this is possible even though IN3 is not defined as a destination in GSMOPTS table for MO_FSMs. IN3 is simply an alternate destination for IN1 and does not have to be involved in the initial PPSMS decision.
- » IN2 is provisioned as a solitary node (i.e. no mated PC) in the MAP table of EAGLE 1. IN2 does not need to be present in the MRN table, since its absence will be interpreted as a solitary node.
- » EAGLE 2 has translation information (PC and RI) provisioned in GSMOPTS for IN2 and IN3. It has been configured to send all MO_FSMs for prepaid type 1 subscribers to IN3 and all MO_FSMs for prepaid type 2 subscribers to IN2.
- » Similar to EAGLE 1, EAGLE 2's MAP and MRN tables have provisioned IN1 as a mate point code for IN3. Again, this is possible even though IN1 is not defined in GSMOPTS as a destination for MO_FSMs.
- » IN2 is again provisioned as a solitary node in EAGLE 2's MAP table, and is not provisioned in the MRN table.
- » Both EAGLE 1 and EAGLE 2 have the global title addresses (GTAs) provisioned in GSMOPTS for IN1, IN2 and IN3. This allows both EAGLEs to perform CgPA filtering on incoming messages from all three platforms.

An example message flow follows:

1. A MO_FSM arrives at EAGLE 1. A PPSMS database search is performed and the message is determined to have originated from a prepaid type 1 subscriber.
2. Since the message is at EAGLE 1 and is prepaid type 1, the GSMOPTS will indicate the translation information for IN1. This information will be used to access either the MAP or MRN table (determined from translated RI), which will indicate that IN1 is in a loadsharing relationship with IN3.
3. For this example, assume the loadsharing algorithm indicates this message should be sent to IN3.
4. IN3 performs the database lookup, authorizes the message, and returns the MO_FSM to EAGLE 1. Since EAGLE 1 has IN3's GTA provisioned in GSMOPTS (note there is no translation information provisioned for IN3 in GSMOPTS of EAGLE 1), it can filter the message and pass it to GTT for routing to the SMSC instead of selecting it for PPSMS service again.
5. Later, another MO_FSM arrives at EAGLE 2. A PPSMS database search is performed and the message is determined to have originated from a prepaid type 2 subscriber.
6. Since the message is for prepaid type 2, GSMOPTS indicates the translation information for IN2. This information is used to access either the MAP or MRN table, which will indicate IN2 as solitary (no loadsharing relationship with another node).
7. The message is sent to IN2. IN2 authorizes the message and returns it to EAGLE 2, which sees the IN2 GTA and passes the message to GTT for routing to the SMSC.
8. Later, a MO_FSM arrives at EAGLE 2. A PPSMS database search indicates the message originated from a prepaid type 1 subscriber.
9. Since the message is at EAGLE 2 and is for prepaid type 1, GSMOPTS indicates the translation information for IN3. A MAP or MRN table search in EAGLE 2 reveals IN3 is in a loadsharing relationship with IN1.
10. Assume the loadsharing algorithm indicates the message is sent to IN1.
11. IN1 authorizes the message and returns it to EAGLE 2. Since GSMOPTS in EAGLE 2 has IN1's GTA provisioned (there is no translation information for IN1 in EAGLE 2's GSMOPTS), the message is passed to GTT.


Prepaid SMS Intercept Database

The PPSMS shares the same database as the MNP feature, and has the following attributes:

- » Supports up to 120 million individual MSISDN entries.
- » Supports at least 50,000 MSISDN range entries.
- » Supports individual and ranged 5 to 15 digit MSISDN numbers.
- » Supports up to three IN platforms, with loadsharing possible.
- » Supports two prepaid types which can be assigned to any MSISDN. (The portability status field from MNP is re-used in this capacity).
- » Supports at least 256 ITU GTI 2 and 20480 ITU GTI 4 (5 unique values for NAI, 16 unique values for NP, and 256 unique values for TT) service selector combinations.
- » Provides control, via provisioning, for how non-international E.164 numbers will be converted to international numbers.
- » Scalable from 850 to 75,000 queries per second.

Support for 32 Prepaid SMS Intercepts

The Support for 32 Prepaid SMS Intercepts feature increases the number of supported Prepaid SMS Intercepts to 32 (from 8 in previous releases of EPAP). Supported GTT (Global Title Translation) destinations have been expanded to 32, and IN SCP (Intelligent Network Service Control Point) platforms and EPAP portability types have been expanded to 32 from 8.



The PPSMS (Pre-paid Short Message Service) Phase 1 feature uses a MNP DN portability type (PT) field to identify the types of prepaid subscribers whose originated short messages (as part of SMS) need to be intercepted and forwarded to a corresponding intelligent network platform for verification. In EPAP 9.0, the PPSMS Phase 2 feature expands the PT range to support 32 types of prepaid subscribers.

MO SMS Prepaid Intercept on B Party

Some network operators have a need/desire to check if B party in the MO-SMS message is prepaid so that they can redirect prepaid SMS messages to a different SMSC than postpaid SMS messages. The current PPSMS Intercept feature does not check the status of the B party of the subscriber, only the A number. This feature is applicable to GSM messages only. GSM messages both over ANSI and ITU transport layers (MTP/SCCP) are supported.

The PPSMS B Party feature works in conjunction with the standard PPSMS feature. If the PPSMS Intercept feature and the B Party option are both on, the standard A-Party search is conducted first. If the A-Party is found to be a prepaid subscriber (i.e. associated to one of the 'prepaid' PT types in the EAGLE's RTDB), then the message is redirected to a prepaid SCP based on the A-Party information from the RTDB, and B-Party search is not conducted. If the A-Party is found to not be prepaid in the RTDB search, then another RTDB search is conducted using the B-Party from the MAP layer of the SMS. If the B-Party is found in the RTDB to be 'prepaid' (PT=one of the prepaid types), the EAGLE shall perform SMS redirection to the prepaid SCP indicated by the RTDB information found with the B-Party entry.

If the MO SMS Portability Check feature is also on, it will be done first. If the Portability Check feature results in a 'fraudulent subscriber' result, the message will be discarded, and PPSMS functionality (either A- or B-Party) will not be conducted.

SMS Number Portability for GSM and IS41

Many wireless operators SMSC use the called party number ranges to determine whether the called subscriber is its own subscriber or belongs to another operator. If the called party number belongs to the same operator, GSM or IS41 protocol is used to deliver the SMS. If the called party number belongs to another operator, SMPP protocol is used for delivery of SMS messages. Additionally, in some networks, SMSCs apply different charging for SMS sent to out-of-network subscribers. The SMSC needs the NP routing information as part of the MO SMS message.

When number portability is introduced, then the SMSC/MMSC can no longer use the called party number to determine whether the called subscriber is its own subscriber or belongs to another operator. If the SMSC cannot determine this, then the SMSC does not know when to use IS41 or GSM protocol and when to use the SMPP protocol to deliver the SMS message.

The SMS Number Portability (NP) features offer the SMSC/MMSC the required called subscriber's network information, so that the SMSC/MMSC can use the correct protocol and deliver the SMS to the called party.

The following sections describe the EAGLE features that apply to the Number Portability database lookup functionality:

- » Mobile Originated(MO)-based GSM SMS NP
- » Mobile Originated(MO)-based IS41 SMS NP
- » Mobile Terminated(MT)-based GSM SMS NP
- » Mobile Terminated(MT)-based GSM MMS NP
- » Mobile Terminated(MT)-based IS41 SMS NP

The Mobile Originated-based features have configurable options for controlling how the processing of SMS messages work. These include:

1. Specifying how to consider SMS destination address for processing (SNAI)
2. Selecting outbound digit format
3. Specifying when a NP DB lookup is considered to be successful
4. Specifying handling of sub address field in destination address (applicable to GSM only)

MO-based GSM SMS NP

In the example shown in the figure below, the MO-based GSM SMS NP feature

- » Intercepts SMS messages before they reach the SMSC.
- » Decodes the TCAP/MAP message destination address and performs lookup in the number portability (NP) Database
- » Modifies the destination address in the TCAP message with directory number (DN) porting information, and
- » Relays the message to the SMSC with the required information needed for delivery or off-net billing decisions.

As of Release 40.0, the HomeSMSC check portion of the MO-based GSM SMS NP feature processing (which is part of the determination of whether a message will receive MO SMS NP service) supports the HomeSMSC Match with Digits Option discussed in Numbering Plan Processor (NPP).

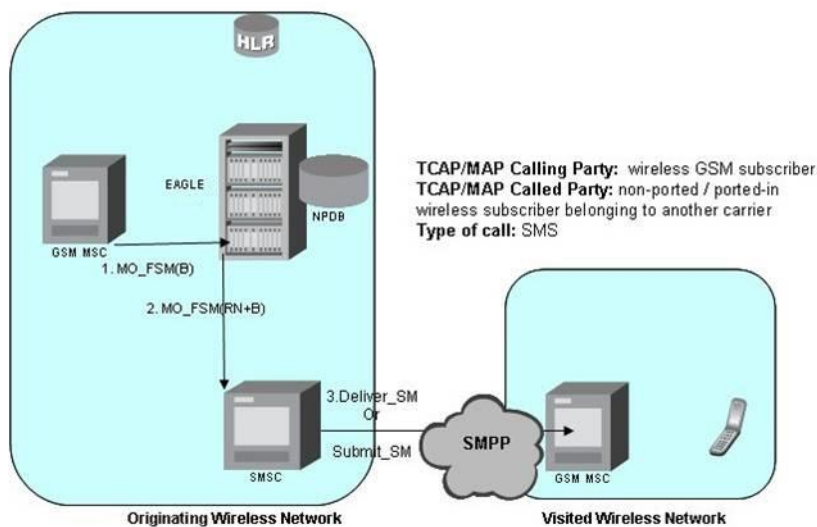


Figure 85: MO-based GSM SMS NP - Called subscriber is another network subscriber

MO-based IS41 SMS NP

The MO-based IS41 SMS NP feature provides network information to the short message service center (SMSC) for subscribers using the IS41 network. This information allows the SMSC to select a protocol to deliver Short Message Service Delivery Point-to-Point (SMDPP) messages to the called party.

In the example shown above, the MO-based IS41 SMS NP feature does the following:

- » Intercepts SMDPP messages before they reach the SMSC.
- » Decodes the TCAP/MAP message destination address and performs lookup in the number portability (NP) database
- » Modifies the destination address in the TCAP message with directory number (DN) porting information, and
- » Relays the message to the SMSC.

There are two options available with the MO-based IS41 SMS NP feature:

1. HomeSMSC Check Options

As of Release 40.0, the HomeSMSC check portion of the MO-based IS41 SMS NP feature processing (which is part of the determination of whether a message will receive MO SMS NP service) supports the HomeSMSC Match with Digits Option discussed in Sets.

Also, an option is added to completely bypass the HomeSMSC check.

The SMSC uses the DN porting information to determine whether to forward the message to other operators or to process the message for an in-network subscriber. The example shows delivery for an in-network subscriber. The MO-based IS41 SMS NP feature applies to messages using ANSI TCAP/MAP application layers, and either ANSI or ITU transport (MTP/SCCP) layers.

Note: As of Release 40.0, MO-based IS41 SMS NP supports ITU transport (MTP/SCCP) layers.

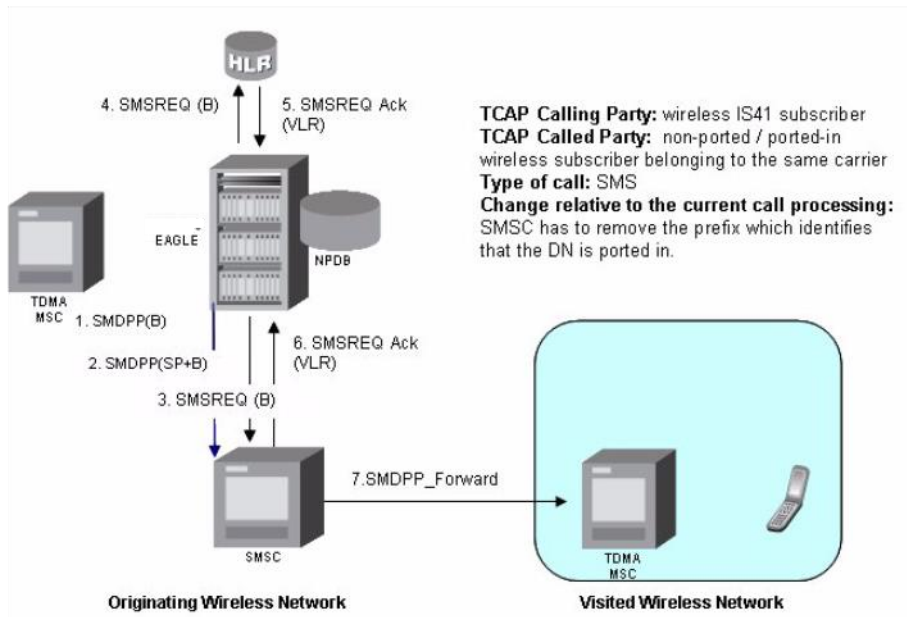


Figure 86: MO-based IS41 SMS NP - Called subscriber is in-network subscriber

2. B-Number Options

Prior to Release 40.0, the MO-based IS41 SMS NP feature always uses the Destination Address (DA) parameter in the IS41 MO SMDPP message for retrieval of the B-number to use for DB lookup, and outgoing message formatting. With Release 40.0, an option is added to allow the operator to choose either the DA or the Original Destination Address (ODA) parameter. Depending on the particular operator's message flows, one set of digits may be more appropriate than the other.

MT-based GSM SMS NP and MT-based GSM MMS NP

The Mobile Terminated (MT)-based GSM SMS/MMS NP feature allows number portability (NP) database lookup to be performed on Send Routing Information for Short Message (SRI_SM) messages. These messages are normally generated from the short message service center (SMSC) to determine the destination for a short message service (SMS) message.

The feature provides configurable options for controlling processing of SRI_SM messages and the content of the response:

- » Selecting the SMSC response message type and digit format
- » Specifying when an NP database lookup is considered to be successful
- » Specifying the format of digits encoded in the response message.

The MT-based GSM SMS/MMS NP feature allows the EAGLE to intercept non-call related messages and reply with routing information for out-of-network destination subscribers using the following process:

1. An SRI_SM message is intercepted from the SMSC before the message reaches the home location register (HLR).
2. The message destination address (SCCP Called Party GTA), is extracted, the digits are conditioned, and lookup is performed in the NP database.
3. If the destination address/subscribers belong to a foreign network, then a reply message is sent to the SMSC with routing information. If the destination address/subscribers belong to a local network, then the SRI_SM message is relayed to the HLR.

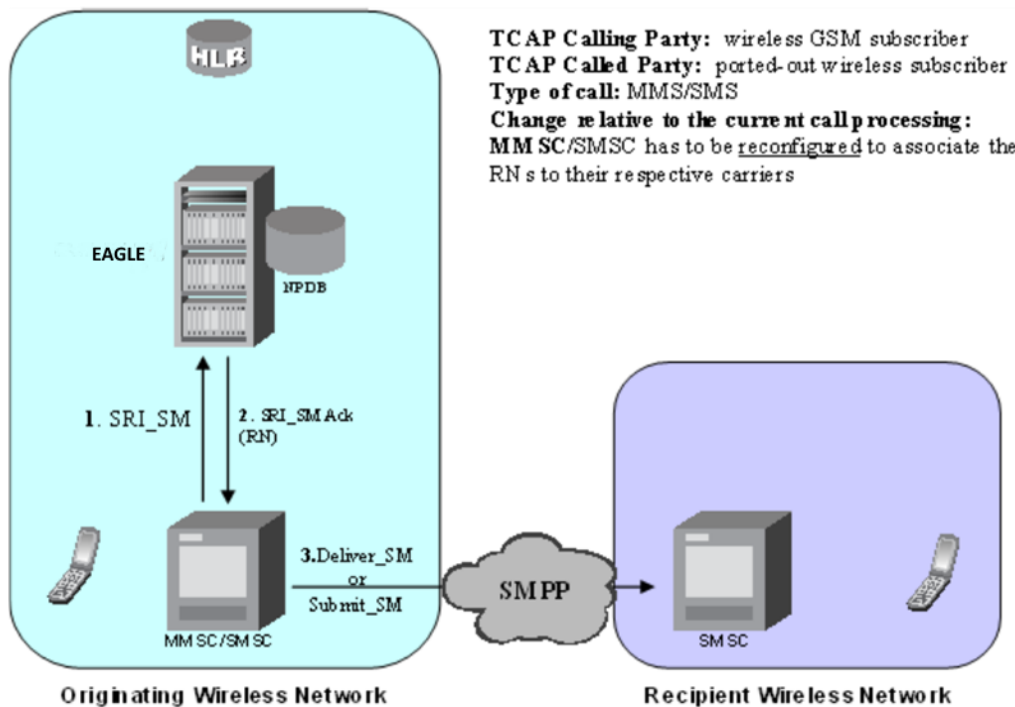


Figure 87: MT-based GSM SMS/MMS NP- called party for other network subscriber

MT-based IS41 SMS NP

The Mobile Terminated (MT)-based IS41 SMS NP feature enhances the A-Port feature to allow wireless operators to route short message service (SMS) messages within a number portability (NP) environment.

This feature provides the following configurable options for controlling processing of SMS routing request messages and the content of the response:

- » Selecting the short message service center (SMSC) response message type and digit format
- » Specifying when an NP database lookup is considered to be successful
- » Specifying the format of digits encoded in the response message.

In the example shown the MT-based IS41 SMS NP feature acts as follows:

1. Intercepts an SMSREQ message from the SMSC before the message reaches the home location register (HLR).
2. Extracts the message destination address (SCCP Called Party GTA), conditions the digits, and performs lookup in the NP database.
3. If the destination address/subscriber belongs to a foreign network, then a reply message is sent to the SMSC with routing information. If the destination address/subscribers belongs to a local network, then the SMSREQ message is relayed to the HLR.

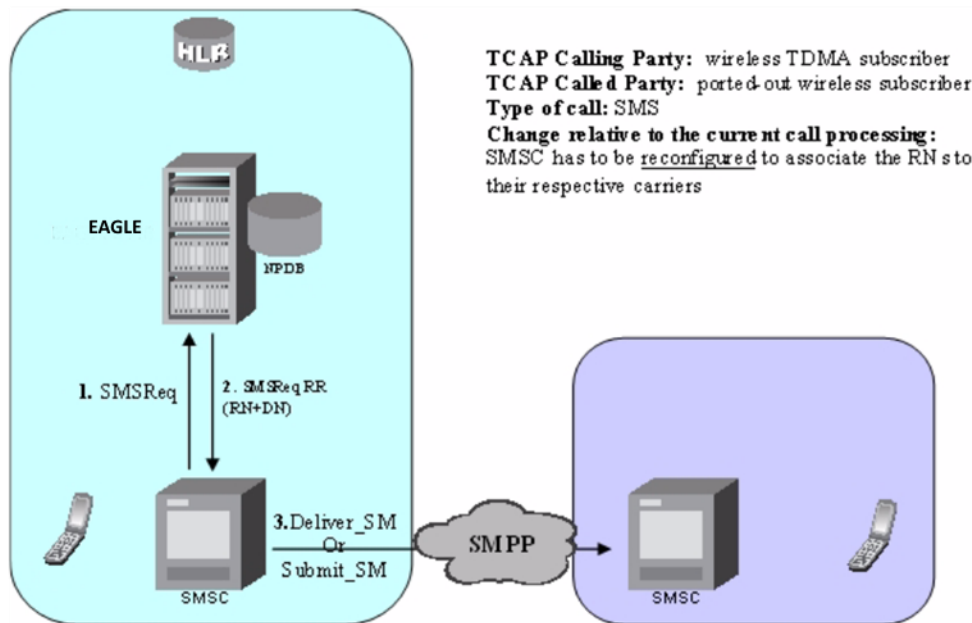


Figure 88: MT-based IS41 SMS NP - called subscriber from other network subscriber


The following is a list of feature considerations:

- » MO- and MT-based IS41 SMS Number Portability requires the A-Port feature. MO and MT-based GSM SMS Number Portability requires the MNP feature.
- » Mobile Terminated (MT)-based GSM MMS Number Portability requires the MT-based GSM SMS NP feature.
- » The five MO-based and MT-based SMS Number Portability features can co-exist with all EPAP-based features such as MNP, HLR Router, EIR, and INP except ELAP-based LNP.

Portability Check for Mobile Originated SMS

In GSM networks, when a mobile subscriber sends a short message or Mobile Originated Short Message Service message (MO SMS), using his or her handset, the message is first deposited in a Short Message Service Center (SMSC). This SMSC is then responsible for determining where the intended recipient, who is also a mobile subscriber, is located. The SMSC accomplishes this by querying the Home Location Register (HLR) of the recipient to determine which Mobile Switching Center (MSC) the subscriber is currently on. Once the location is determined, the SMSC sends the SMS to the recipient.

In a portability environment, this could lead to problems. The SMSC address to which a message is routed is programmed into the GSM mobile handset. When a subscriber ports to another network, the handset is reprogrammed with the SMSC address for the new network. However, the subscriber could then change this



address back to the address from his old network. This would cause SMS to be incorrectly sent to the subscriber's old network SMSC, rather than to the new network SMSC. Since the old network would not have billing records for the ported-out subscriber, the subscriber essentially would receive free SMS service.

The Portability Check for Mobile Originated SMS (MNP SMS) capability is designed to prevent such a possibility from occurring. With this feature, the EAGLE filters incoming messages based on MAP Operation Code. If the message is a MO Forward Short Message (MO FSM), the originating subscriber's Mobile Subscriber Integrated Services Digital Network (MSISDN) number (i.e. phone number) is used to search the Mobile Number Portability database.

If a match is found, indicating the subscriber has been ported-out, the EAGLE uses the destination SMSC address obtained from the SCCP CdPA to search a list of "home network" SMSC addresses. If a match is found, indicating the ported-out subscriber is attempting to send a short message using the old network's SMSC, the message is discarded. An error message is then generated and returned to the originating MSC.

The following are related features

» Segmented SMS

As of Release 39.0, the Portability Check feature provides support for TCAP-segmented SMS messages, as may be found in MAP versions 2 and 3. See SUPPORTING FUNCTIONALITIES.

» HomeSMSC "Match with Digits" option

Also as of Release 39.0, the Portability Check feature also supports the "match with digits" option for the HomeSMSC check. See also Numbering Plan Processor (NPP). Currently, the CdPA digits in the message must exactly match an entry in the HomeSMSC table, and the DN be an out-of-network subscriber, for the SMS to be discarded as fraudulent. This creates a case whereby a fraudulent subscriber can bypass the Portability Check by appending extraneous digits to the end of an otherwise valid SMSC address. The extraneous digits would result in a 'no match' in the HomeSMSC table, and thus the message would not be discarded, even though the subscriber is fraudulent. However, since GTT routing is range-based, a valid entry would be found in the GTT database for the SMSC address less the extraneous digits, and the fraudulent SMS would be successfully routed.


The new option in Release 39.0 allows the user to configure the EAGLE such that a match on longest string of digits in the CdPA is considered a match, even if extraneous digits exist at the end of the string. This effectively prevents the scenario described above.

MO SMS IS41-to-GSM Migration

The MO SMS IS41-to-GSM Migration feature provides a very similar functionality to the MO-based IS41 SMS NP feature discussed in MO-based IS41 SMS NP, but adapted for the specific message flows used in IS41-to-GSM Migration scenarios. Specifically, MO SMS IS41-to-GSM Migration allows the operator to configure which set of digits will be prefixed to the B number when a successful RTDB search is conducted. The feature allows the operator to prefix the RN/Network Entity found in the RTDB for the B number (which is basically the same behavior as the MO-based IS41 NP feature), or an option to prefix the provisioned "IS412GSM" migration prefix instead. This provides a global prefixing option for all SMS arriving for subscribers who have migrated from the IS41 network into the GSM network.

Like the MO-based IS41 SMS NP feature, the MO SMS IS41-to-GSM Migration feature allows the B number to be retrieved either from the Destination Address (DA) or Original Destination Address (ODA) parameter of the IS41 MO SMDPP message.

The MO SMS IS41-to-GSM Migration feature also provides a set of number formatting options for the outgoing digits which are separate from the MO-based IS41 SMS NP formatting options.



The HomeSMSC check portion of the MO SMS IS41-to-GSM Migration feature also supports the HomeSMSC Match with Digits Option discussed in Numbering Plan Processor (NPP). Furthermore, MO SMS IS41-to-GSM Migration also allows an option to completely bypass the HomeSMSC Check. The MO SMS IS41-to-GSM Migration feature can coexist with the other MO SMS NP features.

MO SMS B Party Routing

Some network operators have a need/desire to perform GTT routing based on the SMS B-party recipient digits found in the MAP layer rather than the digits from the SCCP CdPA. In the IS41 MO SMDPP and GSM MO_FSM messages, the SCCP CdPA digits generally correspond to a specific SMSC node, while the SMS B-party/recipient digits from the MAP layer correspond to either a SMS short code, or to the actual MSISDN/MDN of the subscriber receiving the SMS message.

The MO SMS B Party Routing feature allows the option of performing routing on the IS41 MO SMDPP or GSM MO_FSM messages based on the SMS B-party digits from the MAP layer rather than using the SCCP CdPA digits. When the B number is a short code, this option will allow the EAGLE to perform SMS Short Code routing, allowing an operator to direct an SMS to a specific SMSC based on the short code dialed by the SMS sender. When the B number is the MSISDN/MDN of the SMS recipient, this allows operators to direct an SMS to a specific SMSC based on subscriber groupings or types - i.e. "friends and family" type service, in-network/out-of-network, international, etc.

MO SMS B-Party Routing will perform all standard EAGLE GTT functionalities (e.g. EGTT, VGTT, AMGTT, etc.) using the B number, but will not perform SCCP Origin-Based Routing. If GTT fails on the B number, the EAGLE will then perform standard GTT using the SCCP CdPA. MO SMS B-Party Routing will only perform ITUI - ITUN14 SCCP conversion. It will not perform ANSI to ITU or ITUI/ITUN14 to ITUN24 SCCP Conversion - if a conversion scenario is encountered, the message will fall through to standard GTT.

MO SMS NPP

The MO SMS NPP feature applies comprehensive Numbering Plan Processor (NPP) number conditioning and service logic execution to the following existing features:

- » MO SMS B-Party Routing
- » MO SMS IS41-to-GSM Migration
- » MO SMS Prepaid Intercept on B-Party
- » MO-based GSM SMS NP
- » MO-based IS41 SMS NP
- » Portability Check for MO SMS
- » Prepaid SMS Intercept Phase 1 (PPSMS)

This feature also adds new MO SMS ASD and MO SMS GRN features, which are used to support Additional Subscriber Data and Generic Routing Number information, respectively. The MO SMS NPP feature supports GSM and IS41 protocols and IS41 SMDPP and GSM Forward SM Mobile Originated messages.

HLR ROUTER

General

This feature is applicable to any GSM or IS-41, ITU or ANSI mobile network. In the following text, the term Dialed Number (DN) is used to indicate Mobile Station International ISDN Number (MSISDN), Mobile Identification Number (MIN) or Mobile Dialed Number (MDN). Also, the term subscriber number is used to indicate DN and/or IMSI.

HLR Router optimizes the use of subscriber numbers and number ranges by providing a logical link between any DN and any IMSI, and also between any subscriber number and any Home Location Register (HLR). This feature allows subscribers to be easily moved from one HLR to another.

It also allows each HLR to be filled to 100% of its capacity by allowing subscriber number ranges to be split over different HLRs, and individual DNs/IMSI to be assigned to any HLR. Another benefit is that subscriber number routing data is not required to be maintained in all Mobile Switching Centers (MSCs) in the network.

There are two flavors of HLR Router: one for systems using ITU transport layers (MTP/SCCP), and one for systems using ANSI transport layers. Both flavors support either GSM or CDMA application layers (TCAP/MAP).

HLR Router Overview

HLR Router supports the following capacities, throughput, and functionality:

- » 120M individual subscriber numbers (any combination of IMSI and MSISDN, or MIN and MDN).
- » 50,000 DN ranges. (IMSI ranges supported via standard GTT).
- » 1 to 8 DNs per IMSI.
- » E.164 (DN), E.214 (MGT) or E.212 (IMSI) based routing.
- » 1-15 digit hexadecimal subscriber numbers
- » 5-15 digit hexadecimal "Signaling Point" (HLR) addresses.
- » Up to 75,000 TPS per node for ITU transport layer (MTP/SCCP) systems.
- » Up to 120,000 TPS per node for ANSI transport layer systems.

HLR Router can be deployed either as an integrated solution in an EAGLE also performing STP functions and/or other advanced database services or as a stand-alone solution in an EAGLE dedicated solely to the HLR routing functionality (see options below).

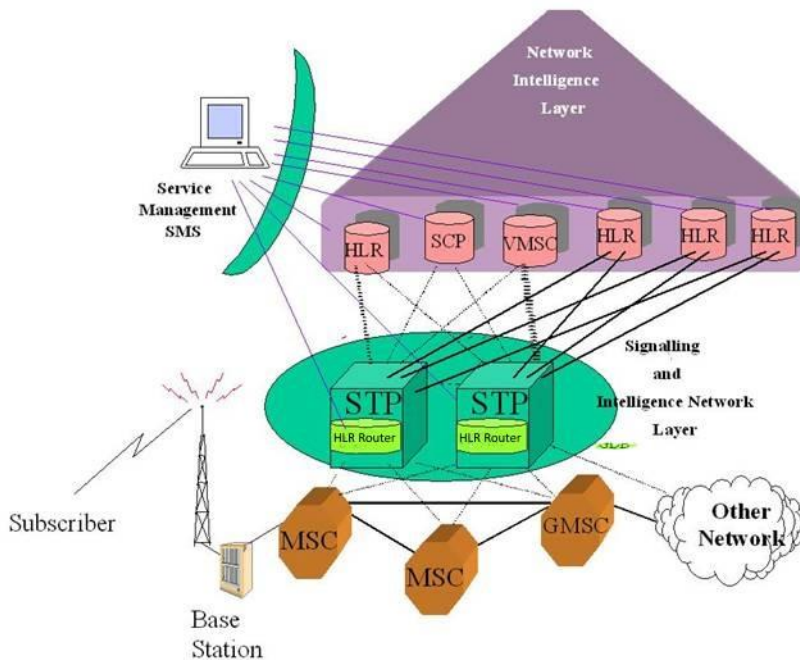


Figure 89: Integrated STP/HLR Router Node in a Mobile Network

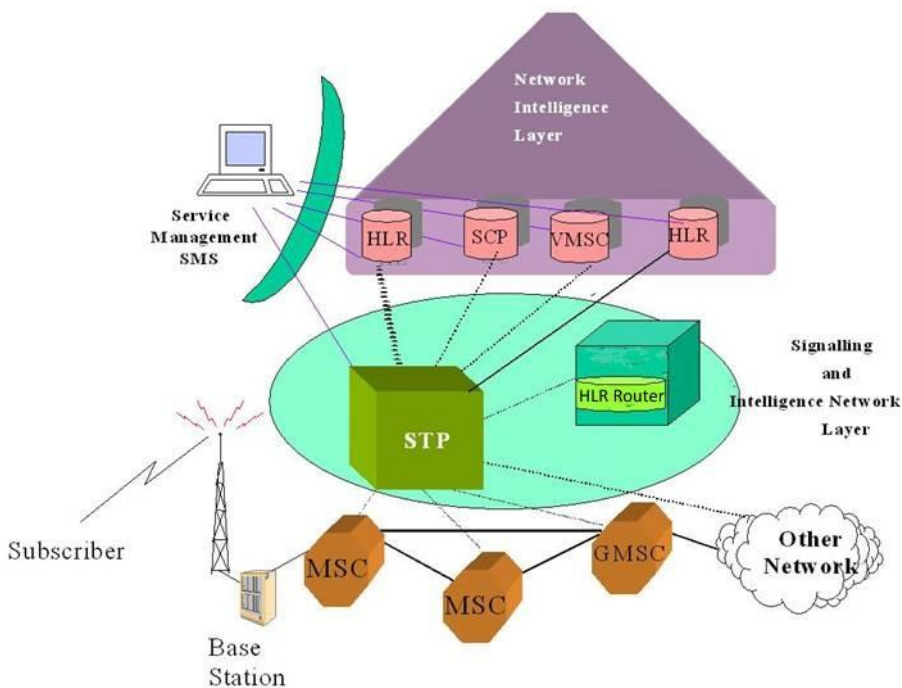


Figure 90: Stand-alone HLR Router Node in a Mobile Network

One advantage to the stand-alone setup is that the impact on the network due to the introduction of this new node is very minimal. The originating node(s) will still continue to route messages to the same STP. The existing STP will forward only HLR destined messages (or Authentication Center (AuC) destined messages if the HLR is an integrated HLR/AuC) to the HLR Router stand-alone node based on the subscriber number ranges. All HLR provisioned subscriber numbers must be provisioned in the GDB prior to bringing HLR Router into service.

Once in service, HLR Router, upon performing the HLR translations on incoming messages, will either MTP route the message through the STP directly to the end node, or forward the translated message back to the STP. If the STP is capable of broadcasting SCCP subsystem management messages (e.g., SSPs and SSAs to the HLR Router node), HLR Router could directly route the messages to the HLR (rt-on-ssn). Otherwise, HLR Router will replace the DN/IMSI/MGT GTA information with HLR entity numbers and forward the message to the STP so that the forwarded message can be easily translated to derive an HLR address.

MGT (E.214) and IMSI (E.212) Routing

The following HLR Router E.214/E.212 routing example and figure describe the call flow:

- » The message is received by the HLR Router feature. Global title information triggers HLR Router processing. Since the SCCP CdPA contains an E.214 number, HLR Router first converts the E.214 number to an international E.212 number before searching the HLR Router database with the E.212 number. (HLR Router also handles the case where an E.212 number is received in the SCCP CdPA. In this case, the database will be searched directly using the E.212 number.)
- » HLR Router finds a match with HLR global title information and routes the message to the designated DPC (HLR B).
- » HLR B responds to Visitor Location Register (VLR) A with an Update_Location ack message. This message has the E.164 address of VLR A in the SCCP CdPA and is routed by normal (or enhanced) GTT, not HLR Router.
- » The message is relayed to VLR A.

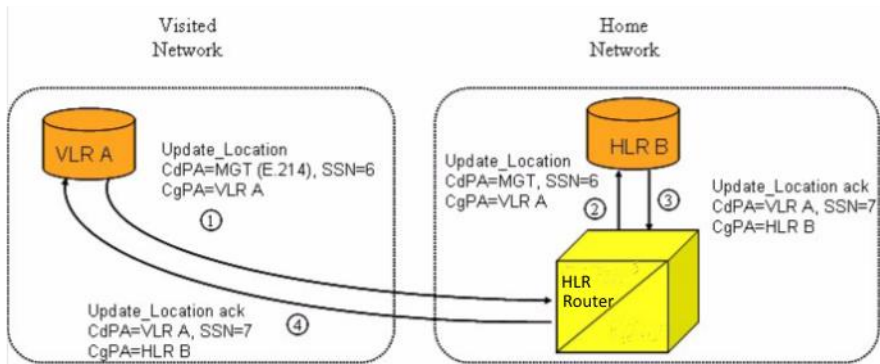


Figure 91: HLR Router E.214(E.212) Routing Example

DN (E.164) Routing

A mobile terminated call results in the Gateway MSC (GMSC) querying the HLR through the use of the called DN as a GTA. HLR Router is used to locate the appropriate HLR. The partial mobile terminated call procedure detailed below is an example of DN global title SCCP addressing:

- » A call is originated and an Initial Address Message (IAM) is sent from the originating network to the subscription network.
- » Digit analysis at GMSC B detects a mobile terminated call to a mobile station and generates a MAP Send_Routing_Info (SRI) message to the HLR Router.
- » The EAGLE receives the message. Global title information triggers HLR Router processing. Since the SCCP CdPA contains an E.164 number, HLR Router searches the HLR Router database with the E.164 number, which must be converted to an international number if not previously done. The HLR Router feature finds a match with HLR GT information and routes the message to the designated DPC (HLR B).
- » HLR B responds to GMSC B with an SRI acknowledgment (SRI ack). This message has the E.164 address of GMSC B in the SCCP CdPA and is routed by normal (or enhanced) GTT, not HLR Router.
- » The message is relayed to GMSC B.
- » GMSC B sends an IAM containing the MSRN to the visited network.

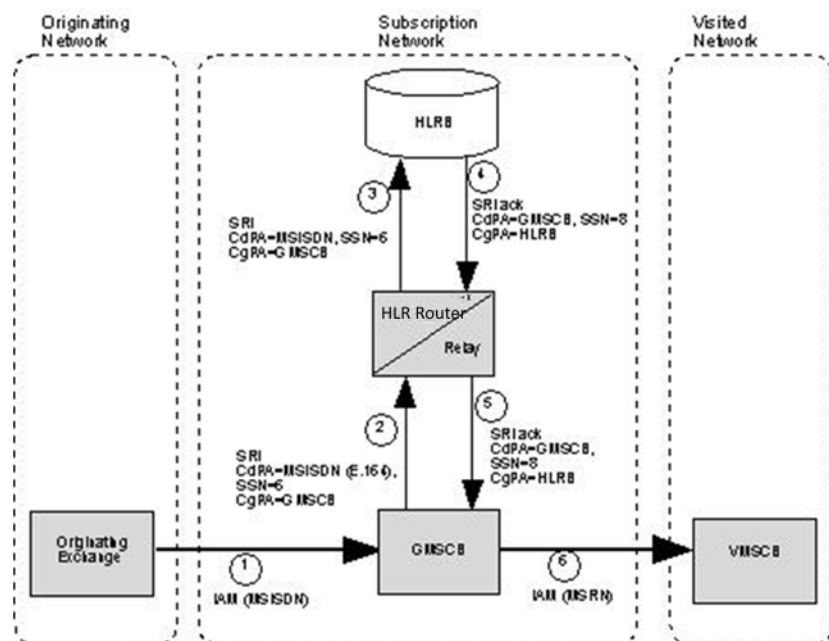
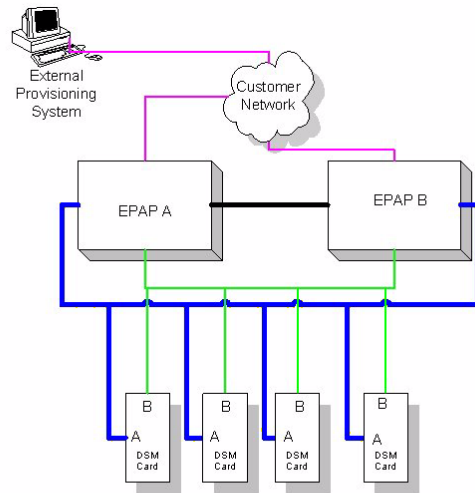


Figure 92: MSISDN-Mobile Terminated Call Example

Note: The GTT data should be set up carefully to prevent any looping between the STP and HLR Router node. The HLR Router relay function will return UDTS on GTT failures.

HLR Router Architecture

The HLR Router architecture contains a pair of active/standby EPAPs (EAGLE Provisioning Application Processors), which provide the interface between the real-time database (RTDB) of the EAGLE' SM cards (Database Service Modules) and the customer's provisioning system. Each EPAP is either equipped with both the Provisioning Database (PDB) and Real Time Database (RTDB) views of the database or just the RTDB view. An EPAP with just the RTDB view must be updated by an EPAP that has the PDB view. The EPAP utilizes the Multi-Purpose Server (MPS). Below depicts the HLR Router architecture and the provisioning hierarchy.



- Network Legend
- 100 Base T DSM Provisioning Network - VLAN Required
 - 10 Base T DSM Provisioning Network - VLAN Required
 - 100 Base T Sync Network - always provided with a crossover cable - no VLAN
 - 10 Base T Customer Provisioning Network

Figure 93: HLR Router Architecture

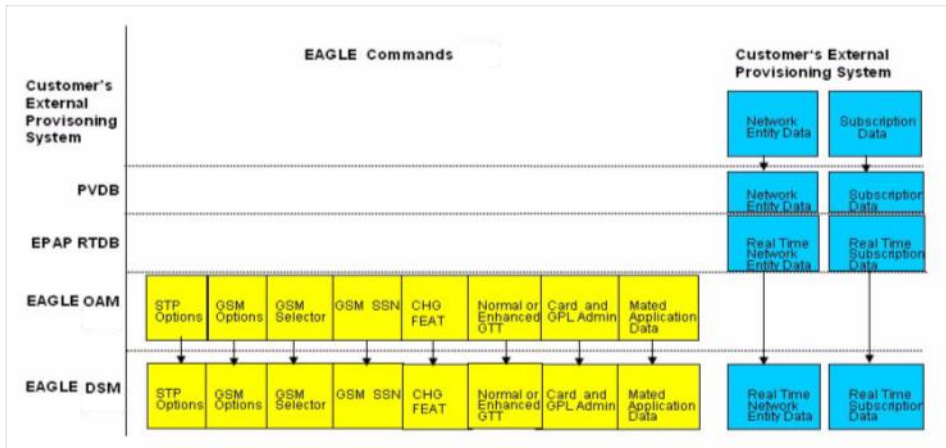



Figure 94: HLR Router Provisioning Hierarchy

The EPAP platform maintains an exact copy of the Real Time Database (RTDB) required by the EAGLE DSM cards, provisions the EAGLE DSM cards, and maintains redundant copies of both databases on mated EPAP hardware. The EPAP platform is a mated pair of processors contained in one shelf. The EPAP platform can be augmented with a RAID array, mass storage device for database backup if required. In this chapter, one half of the platform (i.e., the top or bottom side) is referred to as an "EPAP." "EPAP A" refers to the top side (facing); "EPAP B" refers to the bottom.

During normal operation, information flows through the PDDB/EPAP with no intervention. Subscriber data is generated at one or more operations centers and is delivered to the PDDB through a TCP socket interface, the Provisioning Database Interface (PDBI). The data is stored and replicated on both sides of the EPAP platform for



each mated EAGLE. The data is then transmitted across a private network to the DSM cards for use. Automated reports back to the customer's provisioning system reflecting the DSM card RTDB levels are provided.

Note that the primary interface to the PDBA is machine-to-machine messages via the PDBI. The interface is defined by Oracle and can be configured to update or create provisioning software compatible with the EPAP socket interface. Refer to the user documentation for configuration.

A direct user interface is provided on each EPAP to allow configuration, maintenance, debugging, and platform operations. A direct user interface is also provided by the PDBA for configuration and database maintenance. These interfaces can also be used for emergency provisioning of the PDB.

EPAP Features

» Backup Provisioning Network Interface

This capability allows for the configuring of a second interface to the customer network via an unused interface. This second interface must exist on a different subnet than the primary interface. The customer can then use either interface to communicate with the MPS (e.g., web UI, PDBI, telnet).

» EPAP Security Enhancements

The EPAP Security Enhancements capability implements a database table of authorized IP addresses that can be added to, deleted from, and retrieved by an authorized user via the EPAP GUI.

» Selective Homing of EPAP RTDBs

Under the default configuration, the RTDBs on an EPAP (A or B) will look for and receive updates from the local PDBA process on the local EPAP A (PDBA on the same MPS node as the RTDB), regardless of whether it is the active or standby PDB. An RTDB will only receive updates from the remote PDBA process on the mate MPS node if the local PDBA cannot be accessed.

Some customers would prefer to have all RTDBs within an "MPS System" (both nodes of a mated pair, or even multiple nodes within several mated pairs) always receiving updates from the active PDBA process, regardless of whether it is the local or remote PDBA.

The Selective Homing of EPAP RTDBs capability implements an EPAP configuration option that allows the customer to choose whether the RTDBs on a given MPS node will receive updates from a specific PDBA process (which may or may not be active), or from the active PDBA process (which may or may not be local). This option is selectable via the EPAP UI.

» Support for Provisioning Multiple EPAPs

The Support for Provisioning Multiple EPAPs capability provides the ability to add more MPSs without having to change the customer's provisioning system, or requiring provisioning from multiple sources. With Tekserver-based EPAPs, support for up to 24 RTDBs is provided.

This feature is transparent to the PDBI clients. Each client can provision data in the same manner, no matter if it is provisioning a single MPS pair, or multiple MPS pairs.

Customers may choose to add EAGLEs to their network without changing the way that they provision data. The provisionable PDBs will update the non-provisionable Real-time Databases at the additional sites. The two EPAPs that contain the PDB are called "provisionable" because these are the sites to which the customer provisioning application may connect. The additional EPAPs are called "non-provisionable." See the figure below.

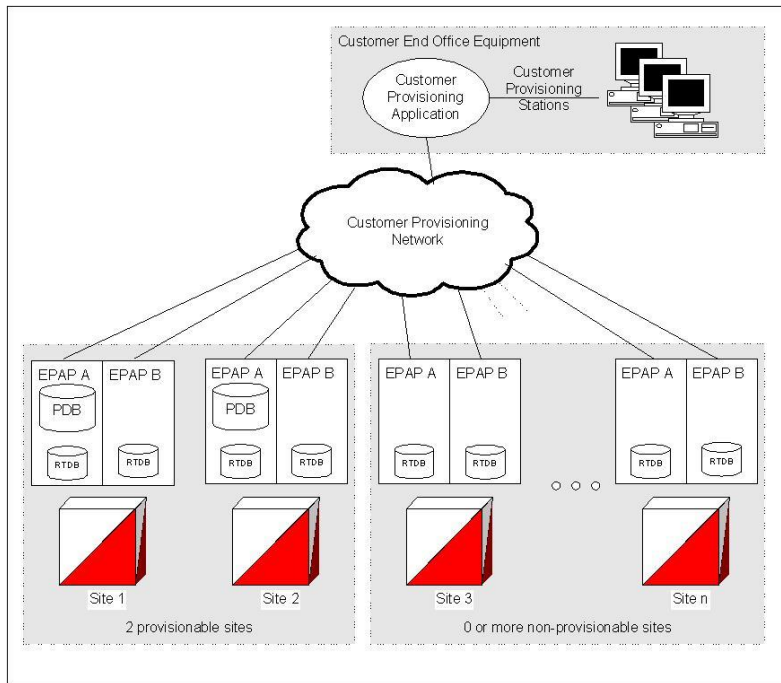


Figure 95: Support for Provisioning Multiple EPAPs

Newly added non-provisionable MPSs will use the Selective Homing of EPAP RTDBs feature to specify the PDB(s) from which to receive updates.

» Allow Write Commands on EPAP During Retrieve/Export

This feature allows an EPAP user to provision data via the GUI or PDBI while simultaneously performing a data export via the GUI or PDBI. There are three modes of operation:

1. Blocking mode - Blocks all write requests while an export is in progress.
2. Snapshot mode - Allows writes to continue during the export, and provides the export as a complete snapshot of the database at the time the export started. (Changes made to the DB after export has started are not reflected in the export file.) This mode provides a file that would be most applicable for importing back into the database later.
3. Real time mode - Allows writes to continue during export, but provides the export file in real-time fashion rather than as a snapshot. (Changes to the DB after the export has started may or may not be reflected in the export file, depending whether the changes are to an area of the DB that has already been exported.) This mode also provides a file that could be imported back into the database later, but is less than ideal, since it is not a complete snapshot of a given time.

» EPAP 30 Day Storage of Provisioning Logs

To allow greater flexibility of log files the EPAP 30 Day Storage of Provisioning Logs feature enables an EPAP to store provisioning, error, and debug EPAP PDB logs for a configurable period of time. The feature will allow for at least 30 days of storage, on the presumption that the disk partition does not become full. These time periods for logs can be configured through the EPAP GUI and consist of single day increments up to 30 days for provisioning and error logs and debug log files are configurable up to 7 days in daily increments.

The main limitation of this feature is it is dependent on partition capacity on the EPAP. This could result in less than the full 30 days of logs for the system but before the partition becomes full the EPAP will produce an alarm starting at 80%.

» EPAP Support for SSH on PDBI

The EPAP Support for SSH on PDBI feature provides support for SSH (secure shell) on the EPAP Provisioning Database Interface (PDBI) for customers who want additional security protection. SSH is a robust, commercial-

grade, and full-featured toolkit that implements security and network encryption. To make the data transfer between the CPA and the PDBA (Provisioning Database Application) machine secure, SSH tunneling (also called remote port forwarding) is used to securely connect the PDBA machine to the CPA machine.

» EPAP Support for HTTPS on GUI

The EPAP Support for HTTPS on GUI feature allows users to configure whether the GUI can be accessed only by standard HTTP (Hypertext Transfer Protocol) or only by HTTPS (Secure Hypertext Transfer Protocol) or by both. Secure HTTP (HTTPS) supports encryption of data exchanged between the web server and the browser. This facilitates data privacy.

» RTDB Retrieve

The RTDB Retrieve feature allows the user to query (from the web GUI) data that resides in the RTDB (Real-Time Database). This feature enables the user to compare data in the PDB (Provisioning Database) with data in the RTDB to verify that they are consistent.

» Automatic PDB Export Enhancement

The Automatic PDB Export Enhancement feature provides flexible scheduling for automatic PDB (Provisioning Database) exports. With more options to choose from, scheduling an automatic PDB export is now very similar to the way tasks or appointments can be scheduled in a calendar manager.

In addition to the previously available choices for export format (PDBI and Raw), mode, and data type (All, IMEI, IMEI block, IMSI, DN, DN block and Entity) these enhancements allow the user to:

- » View, modify, or delete existing reports
- » Choose from multiple options for the frequency of the export: Daily, Weekly, Monthly and Yearly
- » Choose the time of day to start the export
- » Add comments to describe the export

» Standalone PDB on EPAP

Introduced in EPAP Release 16.0, this enhancement allows the EPAP to operate in a standalone mode with only the Provisioning Database (PDB). An EPAP operating in standalone or PDB-only mode runs on a single OC EAGLE Application B card. Geographical redundancy is permitted, which allows the Active and Standby PDB in different locations. An EPAP can operate without a local mate. This enhancement also increases the PDBI performance.

» EPAP Feed to External Query Server

Introduced in EPAP Release 16.0, the EPAP Feed to External Query Server feature allows the EPAP to provide a copy of the EPAP Provisioning Database (PDB) to an External Query Server to allow offline query support of the Number Portability database. A Query Server can connect to only one EPAP. More than one Query Server can be deployed in the system as daisy-chained Query Servers.

» SNMP Interface on EPAP

Introduced in EPAP Release 16.0, the SNMP Interface on EPAP feature allows EPAP management directly by an Element Management System (EMS) in the standard SNMP interface. The SNMP Interface on EPAP feature supports the following:

- » Configuration of EMS is allowed with various parameters from the epapconfig utility.
- » The EPAP sends SNMPv2c trap messages to the configured EMS on the basis of the configurable parameter SNMP Alarm Feed. If SNMP Alarm Feed is set to on, the traps are sent to the EMS. If SNMP Alarm Feed is set to off, the traps are not sent to the EMS. SNMP trap messages can be sent to a maximum of five EMSs.
- » The EMS can receive and set the value of one MIB element resyncVar.
- » The EMS can resynchronize its alarm database with the active alarms on the EPAP by sending a SET request to the EPAP to set the object value of resyncVar to 1.

All alarms can be reported via this SNMP Northbound Interface. Visual alarms are allowed in the GUI, and also reported via the SNMP Northbound Interface.

HLR Router Assumptions/Limitations

The following HLR Router assumptions and limitations exist:

- » An E.214 number received by the HLR Router must first be converted to an E.212 number before searching the database. If the original E.212 number was truncated to form the E.214 number, as allowed by ITU-T Recommendation E.214, the full original E.212 number cannot be recovered, and HLR Router will not work properly.
- » No overload controls are required above and beyond existing EAGLE lower level mechanisms (e.g., for MTP congestion).
- » HLR Router only supports routing of messages to a single network node for a particular subscriber. For example, an individual subscriber cannot have some messages routed to his HLR, and other messages routed to a separate Authentication Center (AuC). In this example, if the AuC is co-located with the HLR, then this version of HLR Router will work. The HLR Router design allows for expansion to include routing to multiple network elements (corresponding to multiple services) for the same subscriber.
- » Messages routed by HLR Router cannot undergo ANSI/ITU MTP conversion.
- » HLR Router does not support ranges.

HLR Router MAP Layer Routing

The HLR Router MAP Layer Routing (MLR) feature allows subscriber digits to be obtained from either the SCCP layer or the MAP layer of a message during HLR Router database lookup. This ability resolves the issue of truncation of digits by the mobile switching center (MSC) that may occur in the SCCP layer.

In an ITU network, when a visited network entity (e.g., VLR, GGSN, SGSN, or GMLC) needs to contact a home network entity (e.g., AuC or HLR) with only the IMSI of a subscriber, the entity will convert the E.212 IMSI into an E.214 Mobile Global Title (MGT). This process applies only to the first message of a dialog.


An E.214 MGT number is in the format CC+NDC+MSIN (Country Code + Network Destination Code + Mobile Subscriber Identity Number). An E.212 IMSI number is in the format MCC+MNC+MSIN (Mobile Country Code + Mobile Network Code + Mobile Subscriber Identity Number). HLR Router performs E.214 MGT-to-E.212 IMSI conversion by replacing the CC+NDC digits at the beginning of the E.214 number with the corresponding MCC+MNC digits provisioned in the EAGLE.

When an E.212 IMSI number is converted into an E.214 MGT number for routing, the MCC+MNC digits in the IMSI number are replaced with the corresponding CC+NDC digits. In some cases, the MSIN portion of the IMSI digits may be truncated during this conversion when the resulting E.214 MGT number exceeds 15 digits. The truncation occurs when the IMSI number is already 15 digits long, and the number of digits in the CC+NDC used to construct the E.214 number exceeds the number of digits in the MCC+MNC, which were deleted from the E.212 number.

For example, if an IMSI number is 15 digits long, and the MCC+MNC portion is 5 digits long, the actual MSIN subscriber number is 10 digits. If the MSC converts to an E.214 number, and the CC+NDC is 6 digits, the resulting number (CC+NDC+MSIN) would be 16 digits. In this case, the MSC may truncate the last digit to keep the total number of digits at 15.

If this truncation occurs, the message sent to an EAGLE for HLR Router service would contain only 9 of the 10 MSIN digits. The EAGLE could convert the CC+NDC to MCC+MNC, but it cannot reconstruct the missing MSIN digit. Thus, HLR Router lookup may fail.

The HLR Router MAP Layer Routing feature enables the user to specify for certain MAP messages whether the subscriber digits should be obtained from the SCCP or MAP layer when performing HLR Router database lookup. The IMSI is not present in the MAP layer for all message types, and truncation can occur when converting. This issue affects only certain MAP message types. This feature only applies to the GSM MAP Location_Update (LU) message and GSM MAP Send_Authentication_Information (SAI) message. These two MAP messages commonly



encode the SCCP CdPA GTA in the E.214 format (MGT) where trailing IMSI digits may be truncated from MGT, and these two messages always include IMSI in the MAP layer.

IMSI is a mandatory parameter in both LU and SAI messages. An LU is a single message. However, an SAI dialog may consist of multiple service requests (e.g., the initial request is encoded in the TC_BEGIN message and the subsequent requests are encoded in TC_CONTINUE messages). For such multiple service requests, the IMSI is mandatory only in the initial service request (the TC_BEGIN message). The subsequent service requests (TC_CONTINUE messages) might not contain the IMSI parameter. Therefore, HLR Router only looks for IMSI in the MAP layer for SAI TC_Begin messages. For the subsequent SAI TC_Continue messages, the EAGLE will perform HLR Router database lookup using the SCCP CdPA GTA digits, which is an EAGLE existing service.

The HLR Router MAP Layer Routing support for ATI using MSISDN feature enhances the HLR Router MAP Layer Routing (HLR Router MLR) feature by providing the option to route AnyTimeInterrogation (ATI) messages using the Mobile Subscriber ISDN Number (MSISDN) from the MAP layer of the incoming message.

VOICEMAIL ROUTER

Background

Current voicemail routing schemes in mobile networks typically use a range-based mechanism whereby the voicemail calls are simply routed to any available Voicemail Server (VMS) platform in a loadsharing scheme. Either the subscriber numbers (MSISDNs in GSM networks) are divided into ranges and the MSCs route calls to the VMS associated with that particular number range, or a single "virtual" VMS routing number is used and the MSC routes via an STP node performing GTT to the individual VMS platform.

With the introduction of advanced and premium voicemail services such as video voicemail, multimedia voicemail, etc., operators have a need to deploy advanced voicemail platforms to handle these enhanced services. However, typically a minority of the operator's subscriber base will subscribe to these services. Therefore, it is desirable to deploy only a few advanced voicemail servers to service these subscribers, while maintaining the standard voicemail servers to service the majority of the subscribers. Another issue is that these multi-service VMS platforms sometimes use different Routing Numbers (RNs) to direct incoming messages to the correct service. This is similar to how an SCP might use different Subsystem Numbers (SSNs) to distinguish among services on the same platform.

With the existing routing scheme of simply dividing the subscriber<->VMS assignments by number range, or using a single virtual VMS number, it is not possible to achieve a specific assignment of premium subscriber to advanced VMS, nor to route to a specific RN service number within a VMS for that subscriber. Therefore, a flexible routing mechanism is required which will allow the operators to specify which subscribers are "premium" subscribers, and assign these subscribers to specific advanced VMS platforms on an individual MSISDN basis. The mechanism should also allow flexible assignment of Routing Numbers within a VMS platform based on call scenario and service being requested.

Voicemail Router Overview

The Voicemail Router feature builds on the EAGLE's suite of advanced database applications which includes the other features described within this chapter.

Voicemail Router will be a new local subsystem on the EAGLE, like EIR and INP. Queries from MSCs will be routed directly to the EAGLE as the Voicemail Router node. The MSC will have the option to send the message Route-on-GT using a GTA which corresponds to the EAGLE/Voicemail Router, which the EAGLE will then translate to its own PC and local Voicemail Router SSN, or the MSC may send the message Route-on-DPC/SSN directly to one of the EAGLE's True Point Codes and local Voicemail Router SSN.

NOTE: As of R39.2, the EAGLE supports multiple local subsystems, which allows the coexistence of EPAP-based database applications such as Voicemail Router, INP and EIR. EPAP-based applications and North American LNP continue to be mutually exclusive.

Voicemail Router supports ITU/ETSI INAP IDP or 3GPP CAMEL (CAP) IDP queries. AIN or WIN queries are not currently supported.

The subscriber (MSISDN/DN)<>VMS mappings will be provisioned via the EPAP in the same manner as MNP, HLR Router, etc., and will be maintained in the DSM RTDB like other EPAP DB application data.

The call decision criteria will be provisioned in tables in the EAGLE's OAM. These tables determine which specific routing number within the specific VMS platform will be used for the particular call based on the criteria of the call (each VMS platform may have up to 10 routing numbers for servicing different types of "voicemail" calls).

Upon receipt of the query, Voicemail Router will use the MSISDN<>VMS mapping table and the call decision criteria to determine a specific voicemail routing number which the MSC should use to route the call. This routing number is returned in an IDP response to the MSC.

The VMRN (Voicemail Routing Number) is a 1-15 digit hexadecimal number and generally corresponds to a type of mail service - for example, Voicemail Deposit, Voicemail Retrieval, etc. The Voicemail Router feature is not concerned with the practical purpose for each routing number, and the actual function they correspond to is transparent to Voicemail Router. Voicemail Router is only concerned with returning the appropriate routing number which corresponds to the subscriber and call scenario.

The figure below shows a general message flow for the Voicemail Router application.

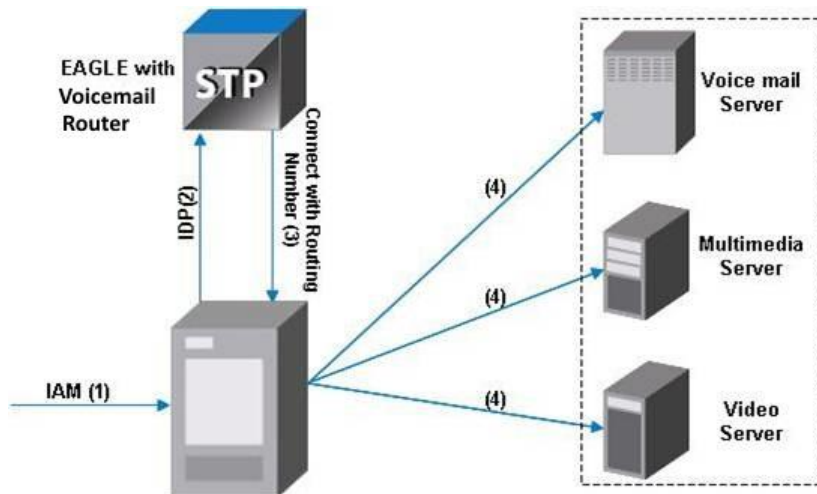


Figure 96: Voicemail Router Message Flow

1. MSC receives an IAM for a call being routed to a VMS
2. Instead of connecting directly to a VMS, the MSC is programmed to generate an IDP to the EAGLE, using subscriber information and call context information from the IAM
3. EAGLE will analyze the information provided in the IDP, perform appropriate database searches, and generate a CONNECT message to the MSC with routing information
4. The MSC can then connect to the correct VMS based on that routing information (4)

EQUIPMENT IDENTITY REGISTER (EIR)

Background

A handset theft problem exists in GSM networks in many countries. A person will obtain a legitimate subscription to a network, and will therefore obtain a legitimate International Mobile Subscriber Identity (IMSI), Mobile Station international ISDN number (MSISDN), and Subscriber Identity Module (SIM) card. (In GSM, the SIM card contains all of the subscriber's information.) The person will initially buy an inexpensive handset and then either steal a better handset from another subscriber, or purchase a stolen handset on the black market. Once the stolen handset is obtained, the thief replaces the stolen SIM card with his/her own legitimate SIM card. Since the SIM card and subscriber information contained therein (IMSI, MSISDN) point to a legitimate network subscription, and because most current network authentication methods are conducted on the subscriber information, and not the handset itself, the phone will operate and the network operator has no way to determine that the subscriber is using a stolen handset. In addition to individual handset theft, organized groups have begun stealing entire shipments of mobile handsets from warehouses, and then selling these handsets on the black market.

The Equipment Identity Register (EIR) is a network entity used in GSM networks, as defined in the 3GPP Specifications for mobile networks. The entity stores lists of International Mobile Equipment Identity (IMEI) numbers, which correspond to physical handsets (not subscribers). The IMEI is used to identify the actual handset, and is not dependent upon the IMSI, MSISDN, or SIM card. The IMSI, MSISDN, and SIM are all subscriber-specific, and move with the subscriber when he/she buys a new handset. The IMEI is handset specific.

The RTDB stores white, grey, and black lists of IMEI numbers. When a subscriber roams to a new MSC/VLR location, the handset attempts registration with the MSC/VLR. Before the MSC registers the subscriber on the new VLR, it may send a MAP_CHECK_IMEI query to the EIR. The EIR will return a response indicating whether the IMEI is allowed, disallowed, or invalid. If the IMEI is allowed, the MSC completes registration, otherwise, registration is rejected.

The EIR may also contain associations between individual IMEIs and IMSIs. This would provide a further level of screening by directly associating a particular IMEI with a particular IMSI. This association can be used in the following way: If an IMEI is found on a black list, an additional check of the IMSI could then be made. If the IMSI from the handset matches the IMSI provisioned with the IMEI, this would override the black list condition, and allow registration to continue. This could be used to protect against mistaken black list entries in the database, or to prevent unauthorized "handset sharing". Obviously, this association could be used in other ways. Additional options may be provided in a future version of EAGLE's GSM EIR, but are not provided in the initial release.

The EIR can be provisioned and maintained completely by the operator, or the operator may choose to deploy an interface between the network's EIR and the Central EIR (CEIR) database in Dublin, Ireland. The CEIR is maintained by the GSM Association and contains lists of authorized and unauthorized IMEIs from any GSM operator in the world who wishes to connect and upload their data. Operators may then connect to the CEIR and receive daily downloads directly into their EIRs. The CEIR allows any GSM operator in the world to connect and download either the entire database, or a subset of the database (i.e., only the data for a specific country or region). The initial offering of the EAGLE EIR does not support direct connection to the CEIR. However, the customer may develop and deploy a mediation device between the EAGLE EIR's open provisioning interface and the CEIR if they choose.

Use of the EIR can prevent the use of stolen handsets since the network operator can enter the IMEI of these handsets into a 'blacklist' and prevent them from being registered on the network, thus making them useless.

Prior to EAGLE release 44 the GSM MAP EIR support was only available to ITU networks. With EAGLE release 44, we support this feature on ANSI networks as well.

Feature Overview

The following shows the call flows for a network using the EAGLE EIR.

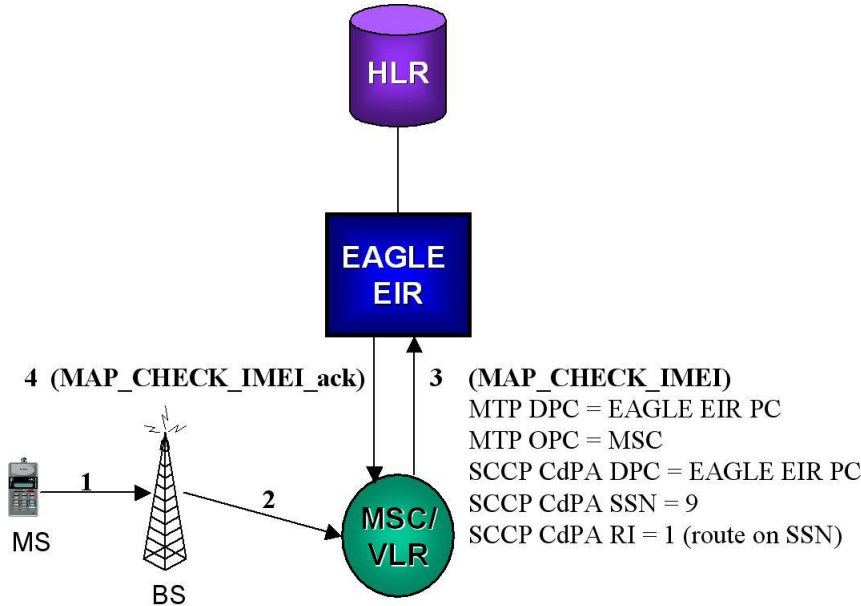


Figure 97: EAGLE EIR Call Flows

1. The Mobile Station (MS), i.e. handset, roams into new serving MSC/VLR area, and begins registration procedure with Base Station (BS).
2. BS begins registration procedure with MSC/VLR.
3. Before allowing the MS to register on the network, and prior to updating the HLR with the new MSC information, the MSC launches a MAP_CHECK_IMEI message to the EAGLE EIR. This message is either MTP-routed directly to the point code of the EAGLE and the EIR subsystem (SSN = "EIR"), or is GT-routed and the EAGLE GT-translates the message to its own point code and local EIR SSN = "EIR".
4. EAGLE EIR retrieves IMEI and/or IMSI from message and searches EIR tables for a match. This search may result in the IMEI being on the white, grey, and/or black lists, or it may result in an invalid or unknown IMEI (no match). It may also result in an invalid IMSI-IMEI combination. Based on the results of the search, the EAGLE EIR returns a MAP_CHECK_IMEI_ack containing either the Equipment Status (IMEI on allowed or not allowed), or a User Error (invalid or unknown IMEI).
5. (Not shown). The MSC either rejects or completes the registration attempt, depending on the information returned by the EIR.

The EAGLE EIR supports three "lists": white, grey, and black. The EIR allows a single IMEI to be on multiple "lists". When an IMEI is on more than one list, the EAGLE applies one of three different types of logic to determine which response should be delivered to the MSC. The logic, or "response type", is configurable by the operator by specifying "Type 1", "Type 2", or "Type 3". The following table indicates how an IMEI is treated based on the selected logic or response type.

Table 20: IMEI Treatment

Presence in List			EIR Response Type		
White	Grey	Black	Type 1	Type 2	Type 3
X			In white list	In white list	In white list

X	X		In grey list	In grey list	In grey list
X	X	X	In black list	In black list	In black list
X		X	In black list	In black list	In black list
	X		In grey list	In grey list	Unknown
	X	X	In black list	In black list	Unknown
		X	In black list	In black list	Unknown
			In white list	Unknown	Unknown

For example, if an IMEI is present on both the grey list and black list, and the Response Type is “Type 1”, then the EAGLE EIR returns a response of “black list”. However, if the Response Type is “Type 3”, then the same number will cause the EAGLE to return a response of “unknown”

The EAGLE also offers a Global Response Option which causes the EIR to return the same global response regardless of which list the IMEI is actually on. In this manner, all registrations are either allowed or disallowed as long as the option is set.

The EAGLE EIR complies with the relevant 3GPP specifications for the EIR entity.

Architecture and Database

The EAGLE EIR utilizes the same architecture and database as the MNP, HLR Router, and INP feature discussed earlier in this section. The EPAP and PDBI are the provisioning interface available to the network operator for provisioning list of IMEIs into the database with the associated list type. Numbers can either be provisioned individually or in groups via the PDBI API, or in bulk format via the EPAP GUI.

The total capacity of the database is 32 million IMEI numbers, and includes all numbers stored in the database, including MNP/HLR Router/INP MSISDNs and IMSIs as well as EIR IMEIs.

The RTDB supports both individual and ranged entries of IMEI numbers. The latter could be used in the instance where an entire shipment of handsets with consecutive IMEI numbers has been stolen, for example.

The EAGLE EIR is a new local subsystem on the EAGLE, similar to INP and LNP. Therefore, CHECK_IMEI queries may be MTP or GT routed to the EAGLE for EIR service. In the MTP routed case, the MSC would route the query to one of the EAGLE’s true point codes and the EIR local SSN (traditionally 9). In the GT routed case, the MSC would route the query to the E.164 address set up for the EIR entity. The EAGLE would perform GTT, which would translate to one of the EAGLE’s point codes and the EIR local SSN. Subsystem management is supported in the same manner as INP and LNP.

Currently, the EAGLE only supports a single local subsystem per node. Therefore, EIR, INP, and LNP are mutually exclusive on the same EAGLE node.

Measurements and Logs

The EAGLE EIR provides the following measurement pegs via the Measurements Platform (MP is required for the EIR feature):

- » Total number of MAP_CHECK_IMEI messages received
- » Total number of searches that resulted in a match with a "white listed" IMEI

- » Total number of searches that resulted in a match with a "grey listed" IMEI
- » Total number of searches that resulted in a match with a "black listed" IMEI
- » Total number of searches that resulted in a match with a "black listed" IMEI, but were allowed due to IMSI Check match
- » Total number of searches that resulted in a match with a "black listed" IMEI, and the IMSI in the database did not match the IMSI in the message
- » Total number of searches that resulted in a match with a "unknown" IMEI
- » Total number of searches that resulted in no match

The EAGLE EIR also provides a log file with an entry for each MAP_CHECK_IMEI received that resulted in a match with an IMEI or IMEI Range entry that is considered either grey- or black-listed. An entry is also created for an IMEI that was black-listed, but a match on IMSI allowed the subscriber to be treated as white-listed. This is captured as an "IMSI override" condition in the log. Each log entry contains the following information:

- » Time-of-day the message was received (in 24-hour format)
- » Date the message was received (in DD:MM:YYYY format)
- » The IMEI digits from the CHECK_IMEI message
- » The IMSI digits from the CHECK_IMEI message (if present)
- » Whether the IMEI was grey-listed, black-listed, or black-listed but allowed due to IMSI override.

This log is generated by the EPAP and is available via SFTP over the customer's provisioning network connected to the EPAP.


Assumptions and Limitations

- » Support is provided for GSM MAP only (The EIR mechanism is not defined in IS-41 MAP)
- » Not compatible with North American LNP on the same node
- » Not compatible with INAP-based Number Portability (INP) on the same node
- » Measurements Platform is required in order to receive the measurements for EIR
- » The EIR log is available via the EPAP only, and will not be available through the EAGLE OA&M.
- » Due to the above, if the connection between one of the EAGLE DSMs and the EPAP is lost, or if a DSM card boots, any logs currently in the buffer of the DSM will be lost. This is not considered a high risk. UDP is being used as the protocol for transfer of the logs, in order to boost performance versus a TCP implementation.
- » The logging capability is designed to handle a minimum of 100 black-list IMEI hits per second. If more hits are encountered, logging cannot be guaranteed.
- » The time stamp in the log is performed on the EPAP, not on the EAGLE DSM card. This should not present a problem as there is at most a 1 second delta between DSM and EPAP.
- » The total capacity of the EAGLE' advanced database services DB is 120 million subscriber number. The capacity of the RTDB is 32 million IMEI numbers. This encompasses EIR, MNP, HLR Router, PPSMS, and IS41 GSM Migration. MSISDNs entered for MNP, PPSMS and IS41 GSM Migration, and IMSIs entered for HLR Router reduce the available capacity for IMEI entries.

SUPPORTING FUNCTIONALITIES

SCCP Service Re-Route

The state of GTT and advanced SCCP services such as HLR Router and MNP goes hand in hand. HLR Router/MNP and GTT are always in an online state when the service module card is in normal service. This could pose an issue in cases when the HLR Router/MNP database is not in the process of full reload and is not in-sync with the EPAP database. In these cases, it may be desirable to temporarily halt HLR Router/MNP service entirely until enough service module cards have completed the reload. HLR Router/MNP service can only be halted by



bringing down the entire SCCP service. This not only halts the HLR Router service, but it also shuts down all the services hosted by the service module card, including GTT. This situation is not desirable.

This feature addresses both problems by providing a controlled way to take the HLR Router/MNP services offline and an option to reroute only HLR Router/MNP traffic to alternate nodes.

SCCP Service Re-Route is an optional feature that is supported for HLR Router/MNP service. This option can be enabled by defining a list of alternate PCs for the service, or by defining the GTT option for the service. Re-routing is activated by marking a service OFFLINE. When a service is OFFLINE, if alternate PCs are provisioned any messages destined to that service would be re-routed to available alternate PCs defined for that service. If alternate PCs are not provisioned or none of them are available, then the GTT option would be used. If the GTT option is YES, then messages destined to that service would fall through to GTT as part of re-routing procedure. SCCP Service Re-Route is applied to all messages destined to a service (based on the EAGLE SCCP Service Selectors).

Service Capability Point Code

Currently, the EAGLE supports capability point codes for STP, LNP, INP and EIR services/features. With this feature, a capability point code would also be supported for HLR Router and MNP services. All messages destined to a service are recommended to use Service Capability Point Codes (CPCs). The use of service capability point code aids the adjacent nodes in knowing about a possible service outage.

When a service using CPCs is offline, the EAGLE will generate response method TFP messages to the adjacent node about the service CPC. The TFP response to the adjacent node causes the traffic-originating nodes to stop sending service traffic to this node, and redirect traffic to the mate node. All service traffic coming into this node is sent to the alternate service nodes. Adjacent nodes will initiate route-set-test procedures after receipt of the TFP.

Conversely, if messages are routed to an EAGLE True PC rather than a CPC, then TFP messages are not generated when a service is offline, making it more difficult for the originator to determine the status of the service on a particular node.

Once the service is back online, the EAGLE will send a TFA to the adjacent nodes in response to any route-set-test messages. The traffic-originating nodes will then resume sending of service traffic to this node.

Refer to the following example:

1. HLR Router and GTT traffic originating from SSP_A, SSP_B and SSP_C will be distributed between STP_1 and STP_2. HLR Router traffic will be addressed to the HLR Router CPC (Service Capability Point Code) defined for STP_S1 and STP_S2. GTT traffic will be addressed to each EAGLE True PC, STP_1 and STP_2

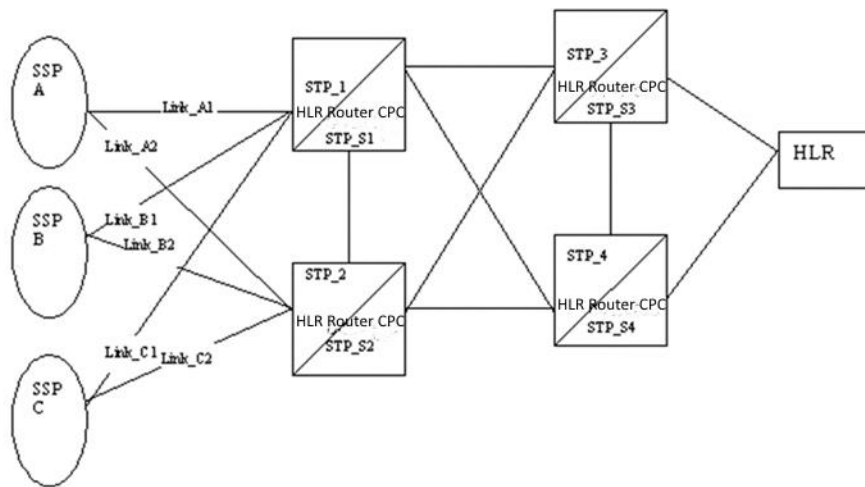


Figure 98: HLR Router and GTT Traffic

2. When HLR Router or MNP service is unavailable on STP_1, it will send a response method TFP message regarding point code STP_S1. This will cause SSP_A to stop using Link_A1 for HLR Router and MNP traffic. STP_1 could reroute all in-transit HLR Router and MNP traffic to STP_S2, STP_S3 and STP_S4 if provisioned as alternate PCs for the service. SSP_A will subsequently send all of its HLR Router and MNP traffic on link_A2 to STP_2. GTT traffic and MTP routed traffic will not be impacted. Other SSPs will perform similar rerouting.
3. When HLR Router or MNP service becomes available again on STP_1, STP_1 will respond with a TFA message (when route-set-test message is received from SSP_A) regarding point code STP_S1. This will cause SSP_A to again start sending its HLR Router and MNP traffic through link_A1. Other SSPs will perform similar rerouting.


With this feature, a new CPC Type pertaining to HLR Router/MNP service is added to the list of capability point code types supported by the EAGLE. HLR Router/MNP Capability point codes can be provisioned when the HLR Router or MNP feature is ON. There can be more than one Capability Point Code assigned to the HLR Router/MNP CPC Type. The EAGLE continues to support a total of 96 CPCs.

A new concept of “service state” is introduced with this feature. This concept is very similar to the EAGLE’ existing use of local subsystem state for LNP, INP, and EIR. When the HLR Router or MNP feature is turned ON for the first time, the service state is initially set to offline. The user can change the service to online at any point. Once the feature is brought online, HLR Router/MNP will start processing messages as soon as at least one service module card is in-service. In some cases, it may be desirable to wait until more service module cards are in-service before bringing HLR Router/MNP online. This decision is at the discretion of the operator.

The user can take the service offline at any point. This will cause the EAGLE to stop processing HLR Router/MNP traffic and SCCP Service Re-Route shall be performed.

HLR Router/MNP service state is persistent. Hence booting the OAM or all the service module cards with SCCP functionality would not change the service state from the current. The user must manually change the service state.

HLR Router and MNP will support up to 7 alternate PCs per domain for use as Service Re-Route destinations. All 6 domains (ANSI, ITU-I, ITU-N, ITU-N Spare, ITU-I Spare and ITU-N 24 bit) are supported. An entire set of alternate PCs are considered as a re-route set.



Instead of the alternate PC option, the operator may use the GTT option. If HLR Router/MNP service is offline when using the GTT option, all messages destined for the services will fall through to GTT based on the setting of the GTT option. This option is set to YES by default.

MTP Messages for SCCP Applications

The MTP Messages for SCCP Applications feature supports MTP-routed SCCP messages for the A-Port feature and the IS41 GSM Migration feature; LOCREQ messages and SMSREQ messages are supported. (The GSM messages are still not supported by the IS41 GSM Migration feature.) The MTP Messages for SCCP Applications feature can only be used if the A-Port feature, the IS41 GSM Migration feature, or the HLR Router feature are turned On.

Service Selection and Routing

All service selector options are not supported by the MTP Messages for SCCP Applications feature. Only MNP services for the A-Port and IS41 GSM Migration features and HLR Router services for the HLR Router feature are supported by this feature and service re-route is not performed on MTP-routed messages.

If the MTP Messages for SCCP Applications feature is active, all SCCP messages are routed to the service module cards. Service module cards perform SCCP decode and verification as they do for GTT today.

If the MTP-routed messages have CDPA GTI =0 and the IGM feature is turned on, a message is sent for MNP processing. If the MTP-routed messages have CDPA GTI not zero, service selector lookup is performed using the SCCP CDPA information.

- » "If the result of the lookup is for MNP service, a message shall be sent to MNP handling. MNP shall check if the TCAP portion of the message is ITU or ANSI. If the message has ITU TCAP, the message is forwarded to HLR Router processing. If the message has ANSI TCAP, A-Port general TCAP/MAP verification is performed if A-Port or IGM feature is active.
- » "If a service selector is not defined or does not match, or if the service is offline, MTP routing is performed on the messages. Service re-route is not performed on MTP-routed messages both for GTI is zero or none zero.
- » "Only LOCREQ messages are supported. See the ANSI-41 Mobile Number Portability and IS-41 GSM Migration feature descriptions for LOCREQ message handling.

HLR Router Feature Processing

If the result of service selector lookup is for HLR Router service, HLR Router message processing is performed. This feature supports HLR ROUTER service for MTP-routed TCAP/MAP messages. If the MTP Map Screening feature is on, MTP Map Screening is performed on post HLR Router messages and fall-through MTP-routed messages.


Considerations and Limitations

The use of the MTP Messages for SCCP Applications feature adversely affects the SCCP capacity, because all of the messages are counted under SCCP capacity.

Multiple Local SCCP Subsystems

As of Release 39.2, the EAGLE will support multiple local SCCP subsystems. Prior to this, only one local subsystem was allowed to be provisioned. In the EAGLE, features such as EIR, Voicemail Router, INP and North American LNP are local SCCP subsystems on the EAGLE, and could not coexist. After R39.2, an EAGLE node will be able to support simultaneously EIR, Voicemail Router and INP. North American LNP will continue to be mutually exclusive with these features due to the differences in ELAP and EPAP database schema.

Additional Subscriber Data (ASD)



Currently, EAGLE's EPAP database supports some data which can be associated with individual subscribers and ranges. Some examples of this data are:

- » Entities, e.g. RN/SP (which includes such information as entity type, entity value, etc.)
- » VMS - voicemail service center IDs
- » GRN - generic RNs

With new applications, and several applications co-existing on the same deployment, a need for more fields that can be associated with individual subscribers and ranges of subscribers grows. The Additional Subscriber Data (ASD) feature addresses the addition of a field into the EPAP and support of generic fields in the EAGLE.

One primary use case for the new field are requirements in certain number portability scenarios whereby additional pieces of information are used when porting. One such use case is the association of subscribers with geographical areas. Information is needed in the NP database to indicate which geographical area a subscriber is associated with. The ASD can be used to provide this information.

Another example use case for ASD is Triggerless Equal Access

Triggerless Equal Access using ASD

Triggerless Equal Access is used to allow subscriber access to all long distance carriers on equal terms. Equal access is intended to foster competition among long distance providers by providing all customer equal access to any of the carriers' services. Some countries require an equal access provider for national long distance and a different provider for international long distance.

Triggerless equal access allows a subscriber to indicate a preferred long distance provider/operator. The equal access code for the preferred providers is provisioned against the subscriber number (as additional subscriber data in the EPAP).


During call set-up, an IAM is intercepted by the EAGLE, and the equal access code associated with the calling party (A number lookup in the RTDB, insertion of the ASD for that subscriber) is inserted into the called party number of the outgoing IAM (for long distance calls). The network then uses the equal access code to correctly route the call to the appropriate long distance carrier.

Triggerless Equal Access and association to geographical area are just two examples of the use of ASD. Other use cases may arise. Depending on the particulars of the use case, the ASD field may be used as is in the EAGLE, or additional EAGLE feature development may be needed to make use of the ASD for the particular use case.

Numbering Plan Processor (NPP)

The Numbering Plan Processor, or NPP, is an infrastructural functionality built into the EAGLE as of Release 39.2, which is designed to eventually be available for use by all of the EAGLE's advanced database features. Each of the advanced database features requires additional work to "plug in" to the NPP functionality, so currently only a few features make use of its capabilities. The features which currently make use of NPP functionality include: IDP Relay, IDP Relay for SMS, Triggerless ISUP (TIF) Number Portability, and TIF Simple Number Substitution. Other features may be modified in future releases to also make use of NPP.

The NPP infrastructure changes the way service selection, number conditioning, action selection and number formatting is done for the features which have access to the infrastructure. The features (such as IDPR, TIF NP, etc.) which make use of NPP will "call" NPP from within the execution of the service. NPP will perform its duties (e.g. number conditioning, actions, and number formatting), then return the service control back to the requesting service.



NPP uses a filter to classify an incoming digit string. Each Filter classifies a digit string based on an FNAI (filter nature of address indicator) class, a FPFX (filter prefix), and a FDL (filter digit length). The combination of an FNAI-class, FDL and FPFX constitutes an NPP Filter. Customers can provision NPP filters that ignore FPFX and/or FDL. This is accomplished by allowing the FPFX and FDL values for a filter to be wild carded.

5NPP Filters

» Filter Nature of Address Indicator-Class (FNAI-Class)

Many protocols infer digit string formatting based on a protocol specific NAI value. NPP uses this same concept to help isolate digit strings. NPP defines NPP-specific FNAI-classes that services can map service-specific NAI values. The NPP-specific FNAI classes include NATL (national), INTL (international), NAI1(generic1), NAI2(generic2), NAI3(generic3) and UNKN.

» Filter Prefix (FPFX)

Many EAGLE features search for matching digit patterns that occur at the beginning of digit strings to determine further processing. NPP provides this functionality with Filter Prefixes (FPFX). An NPP filter prefix (FPFX) is a hexadecimal string of digits that may occur at the beginning of a digit string.

» Filter Digit Length (FDL)

In addition to FNAI-Class and Filter Prefixes, NPP provides additional digit string isolation criteria based on the incoming length of the digit string. An NPP filter digit length specifies how many digits the incoming digit string must have to match the filter.

» Action Sets

NPP allows customized EAGLE behavior to be provisioned as an Action Set. An Action Set consists of three subsets of Actions: Conditioning Actions, Service Actions and Formatting Actions. The figure below depicts graphically the relationship between Actions and Action Sets. Additionally, each Action Set contains an outgoing FNAI-Class that is communicated to the requesting Service.

» Conditioning Actions

Conditioning Actions (CAs) determine how a digit string is manipulated prior to applying services. CAs deal mainly with identifying a subscriber number in international format. The NPP allows up to twelve CAs per Action Set. The NPP executes CAs associated with an Action Set in the order provisioned.

» Service Actions

Service Actions (SAs) determine what EAGLE behavior to apply to a digit string. For example, all digit strings of a certain type might require a number portability check. To accomplish this, the NPP provides a number portability SA that can be associated with an Action Set. The NPP allows up to eight SAs to be associated with a single Action Set. The NPP executes Service Actions according to precedence defined by the calling Service. For example, number portability always executes prior to number substitution regardless of provisioning order, etc.

» Formatting Actions

Formatting Actions (FAs) are applied after Service Action execution. FAs determine how the outgoing digit string is formatted. For example, the customer may want a format of CC+RN+DN for certain message types and simply RN+DN for others. The NPP allows up to twelve FAs to be associated with a single Action Set. The outgoing digit string is constructed by inserting digits associated with each FA. Formatting Actions are executed in the order provisioned.

» Outgoing FNAI-Class

Each Action Set contains an outgoing FNAI-Class setting. This setting communicates the NAI of the outgoing digit string to requesting services. Additionally, NPP will map the outgoing FNAI-Class specified to a service-specific NAI value.

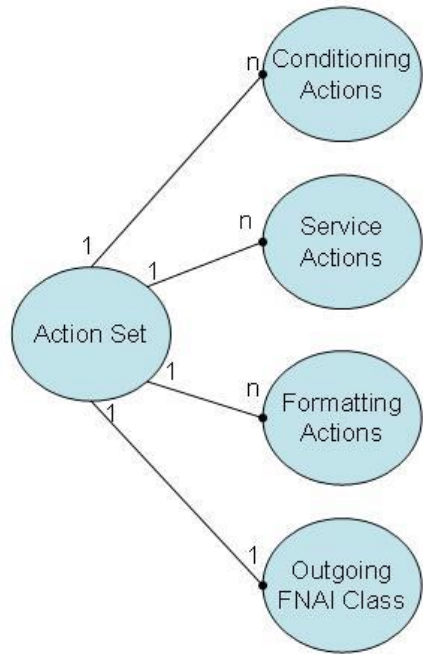


Figure 99: Action Set <-> Action Relationship

NPP Rules

An NPP Rule is an association between a single NPP Filter and a single NPP Action Set. An NPP Rule specifies the message type via the filter and what behavior to apply to each message via the Action Set. The figure below graphically depicts the relationships between Rules, Filters, Action Sets, and Actions.

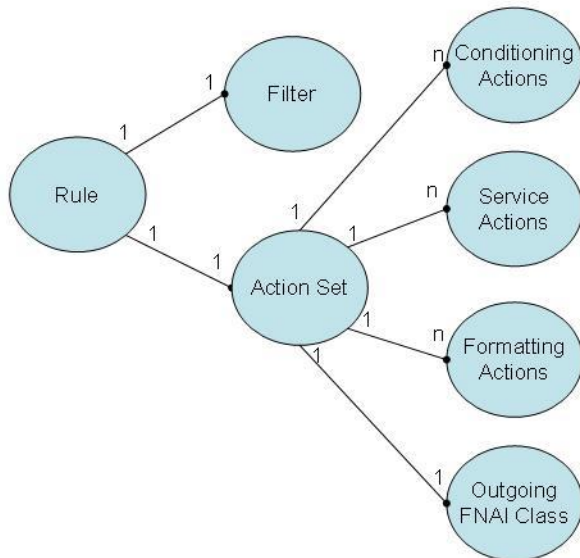


Figure 100: Rule/Filter/Action Set Relationship

Services and Service Rule Sets

“NPP Service” is a generic term that can be applied to any EAGLE application that has been modified (in the case of existing features) or designed (in the case of new features) to use the NPP infrastructure. Existing EAGLE features may be modified to use NPP infrastructure instead of their previous individual number conditioning/action/formatting rules. Such examples are IDPR and TINP. An “NPP Service Rule Set” is a collection of Rules that are associated with an NPP Service. The figure below graphically depicts the relationships between Services and Action Sets.

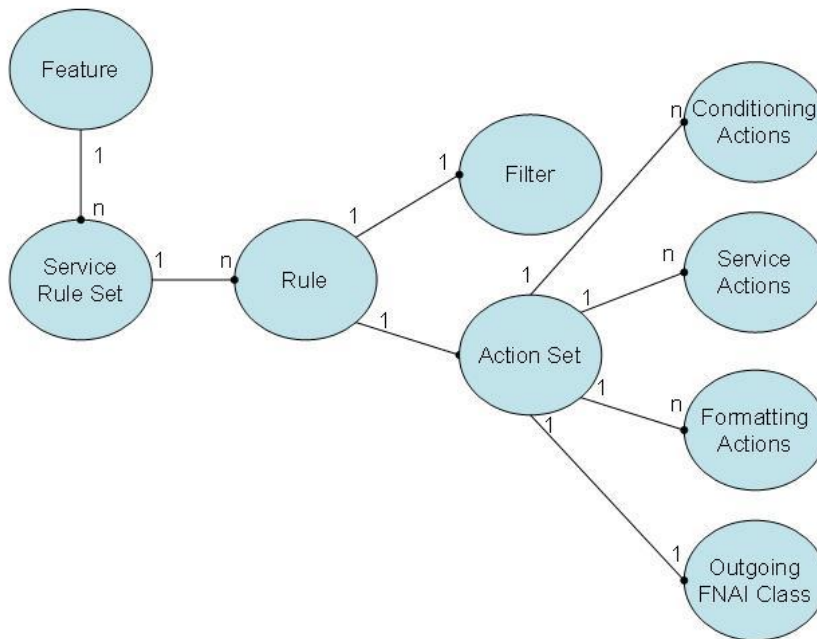


Figure 101: Service Rule Set and Rule Relationship

The overall purpose of the NPP infrastructure is to provide a common, highly flexible service execution environment which can eventually be accessed by all EAGLE advanced database applications. Rather than each feature having its own independent set of number conditioning rules, service actions and formatting rules (which may be overly limited in usefulness outside of a fairly small set of use cases), NPP provides a high degree of flexibility to the operator in how services are called, how numbers are conditioned prior to DB lookup, the actions that may be taken as a result of the DB lookup, and how the numbers are formatted after the service is completed.

Future EAGLE releases will see more of the existing advanced DB applications move into the NPP infrastructure.

HomeSMSC “Match with Digits” Option

A new “match with digits” option for the HomeSMSC check portion of the Portability Check for MO SMS, MO-based SMS NP (IS41 and GSM versions), and MO SMS IS41-to-GSM Migration features is now available in the EAGLE.

Without this option, when the EAGLE is conducting the HomeSMSC check portion of these features, the CdPA digits in the message must exactly match an entry in the HomeSMSC table.

This option allows the HomeSMSC check to be conducted with a longest match principle whereby a match on the longest number of digits will be considered a match, even if there are additional digits appended to the address in the incoming message.

TCAP-Segmented SMS Support Phase 1

In GSM MAP versions 2 and 3, SMS messages may be segmented into two TCAP payloads. The first payload is sent in a TCAP Begin message which contains no MAP operation information (e.g. no opcode, no subscriber digits, etc.). The second payload, which contains the pertinent MAP operation information, is sent in a TCAP Continue message. Both messages must be treated the same, and routed to the same destination. For EAGLE features which use MAP operation information for message treatment and routing decisions, segmented SMS messages

pose a problem. This is because there is not enough information in the first TCAP Begin for the EAGLE to make an appropriate decision.

As of Release 39.0, two such features (Portability Check for MO SMS and MO GSM SMS NP) are being modified to support segmented SMS messages. Other features which use MAP layer information (e.g. Enhanced GSM MAP Screening, Prepaid SMS Intercept, etc.) will continue to support only non-segmented SMS at this time. Segmentation support for these features may be provided in a future release. Hence, this feature is dubbed "Phase 1". Below is an example of the operation of the TCAP Segmented SMS Support Phase 1 feature.

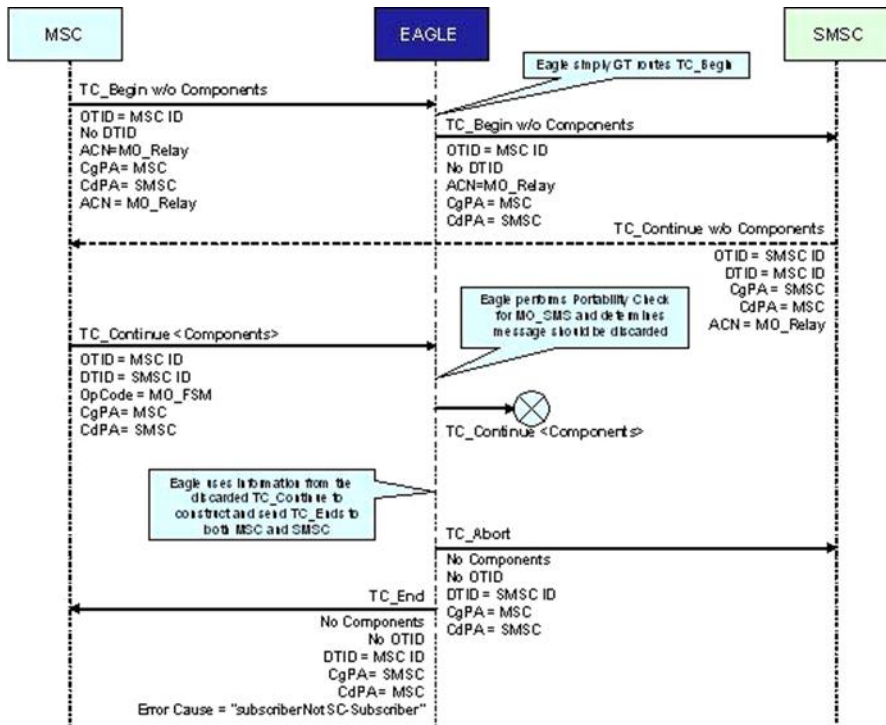


Figure 102: Example of TCAP Segmented SMS Support Phase

The Portability Check for MO SMS and MO SMS NP features support TCAP-segmented SMS messages as shown above, and as described below. (With one exception: the redirection option of the MO SMS NP feature is not supported for segmented SMS.) Both features do not alter the originally intended destination of the message, and this is the reason for the distinction between these features and the others. When the original destination is not being altered by the EAGLE based on MAP information, segmentation can be supported by the method described here. When a feature redirects a message to another destination based on MAP information (as is the case for Enhanced GSM MAP Screening Forward Action, Prepaid SMS Intercept, and the redirection action of MO SMS NP), a more complex solution is required.

The logic applied in the figure above is detailed below:

1. MSC routes a TC Begin without Components via EAGLE, indicating the opening message of a TCAP-segmented sequence. This message contains no actionable information for the Portability Check for MO SMS or MO GSM SMS NP features, so the EAGLE simply GT routes the message to the intended destination (i.e. SMSC).

2. After the SMSC confirms the dialogue, the MSC routes the TC_Continue with Components via the EAGLE. This message contains information needed for Portability Check and MO SMS NP to process the message. EAGLE intercepts the message and performs the appropriate service.
3. In the case of MO SMS NP, the EAGLE will modify the B-Party in the TC_Continue as needed, and then route the message to the SMSC (MO SMS NP does not have a discard option). The SCCP Called Party modification/re-route option of GSM MO SMS NP feature is not supported for segmented messages at this time...i.e. all segmented messages will be modified at the MAP B-Party, and then routed to the original SCCP CdPA, while non-segmented messages may continue to take advantage of the SCCP reroute option of the MO SMS NP feature.

In the case of Portability Check for MO SMS, the EAGLE will either decide to allow the TC_Continue to be routed to the SMSC, or it will decide to discard it based on the Portability Check algorithm. Because the dialogue has already been established between MSC and SMSC due to the delivery of the initial TC_Begin, the EAGLE cannot simply discard the message, but must properly close the dialogue on both sides (even though the EAGLE is technically not part of the dialogue). Thus, the EAGLE sends a TC_End to the MSC, serving as a proxy for the SMSC, with Error Cause of "subscriberNotSC-Subscriber", and it also sends a TC_Abort to the SMSC, serving as a proxy for the MSC. This properly closes the transaction and prevents the SMS from being delivered.

ORACLE COMMUNICATIONS LOCAL SERVICE MANAGEMENT SYSTEM (LSMS) (NORTH AMERICAN)

LSMS OVERVIEW

Oracle Communications Local Service Management System (LSMS) supports the administration of Oracle Communications (OC) North American Local number Portability (LNP) solution. The LSMS provides the interface between the NPAC SMS and the OC EAGLE Element Management System. It supports provisioning of the OC EAGLE with NPAC data as well as locally administered service provider specific data.

The LSMS is composed of hardware and software components that interact to create a secure and reliable LNP system.

The LNP data administered by the LSMS includes:

- » Subscription data
- » Number Pool Block data
- » Service provider data
- » Network data
- » NPA-NXX Default GTT data
- » LRN Override GTT data
- » NPA Split data

The OC LSMS provides these functions:

- » Receiving LNP data from NPAC SMS
- » Distributing data to the OC EAGLE LNP
- » Administering internal Service Provider LNP data to support the final global title translation for various services (LIDB, CNAM, CLASS, ISVM, WSMSC)
- » Storing NPAC LNP data and service provider LNP data on a persistent local database
- » Supporting data audit function between NPAC SMS and LSMS. The audit is initiated by NPAC SMS.
- » Initiating audits and reconciliation between LSMS and the OC EAGLE LNP
- » Supporting connection management for NPAC and OC EAGLE LNP communication

- » Handling local failures, NPAC communication failures, and OC EAGLE LNP communication failures and recovery
- » Event Logging
- » Providing internal data security using one-way encrypted passwords
- » Providing a secure interface to NPAC SMS using key list management
- » Reporting event notifications and alarms

The LSMS hardware and software components interact to create a secure and reliable LNP support system. The following sections discuss these components and their functions.

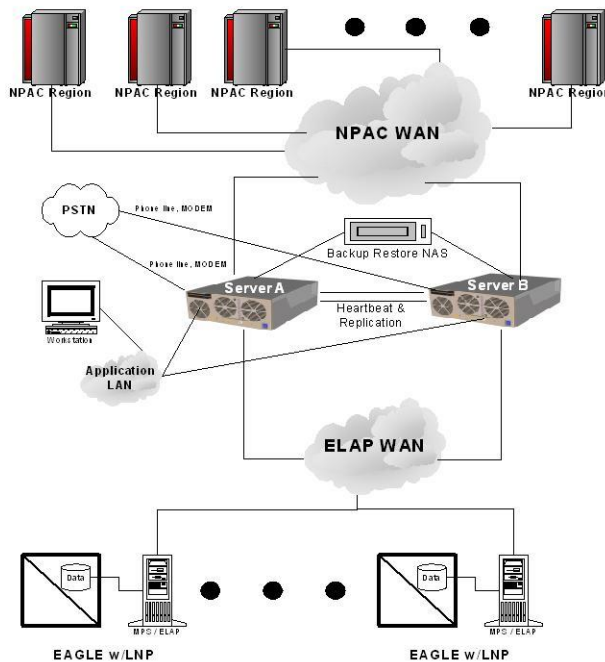


Figure 103: Sample LNP Network

LSMS HARDWARE OVERVIEW

The LSMS is comprised of two Oracle Communications EAGLE Application B Cards (APP-B) installed in an EAGLE heavy duty frame and deployed in a redundant, active/standby configuration. Data is replicated between the two servers as well as mirrored on dual drives within each server to provide failsafe data integrity. The LSMS system uses a Network Attached Storage (NAS) device to back up the system and application logs and the LSMS database. The NAS is also hosted on the APP-B Card.

APP-B Card Components

- » Dual Core 2.66 GHz 64-bit processor
- » Active / Trial BIOS architecture
- » 1333 MHz processor front side bus speed
- » 8 GB DDRs DRAM
- » LED status display
- » Hardware monitors that read and report:
 - » Supply and core voltages

- » Fan alarm inputs
- » Ambient and processor temperatures

LSMS ARCHITECTURE

Hot Swap Capability, Critical Hardware Components

The LSMS runs on redundant servers. If one server suffers a hardware failure, the other server will take over. This redundancy is carried to the component level. Some failed components can be replaced without interrupting the operation of their main assembly.

Data Redundancy

An LSMS primary set is comprised of one APP-B card and two removable drive modules. The secondary set comprised of the second APP-B card and two removable drive modules acts as a redundant system and fully mirrors the primary set. The two servers are configured in an active and standby configuration to support high availability. Data is replicated between the two servers as well as mirrored on the drive modules within each server to provide failsafe data integrity.

The primary set provides all system functions during operations unless it experiences a failure. If a failure occurs with the primary set, the secondary set can take over.

Segmented Network Configuration Support

The LSMS Segmented Network Configuration Support feature allows customers to have a segmented network architecture with the LSMS running on the APP-B cards. This feature allows the use of a segmented network to separate the Northbound (NPAC) and Southbound (ELAP, GUI, NAS) connections, where the eth0 port is used to connect to the NPAC. The eth1 port is used to connect to the EMS, Application and NAS. There is no functionality change of ports eth2 and eth3.

Network Interfaces

There are three primary protocols used in LSMS network connections. For the NPAC connections, the Q.3 protocol is used. The EMS connections use a proprietary High Speed Operations Protocol (HSOP). The Application and Admin network connections employ the standard TCP/IP stack.

LSMS FUNCTIONS

Table 21: LSMS Functions

Data Type	Default LSMS Capacity	Maximum LSMS Capacity
TNs/Number Pool Blocks	18 Million	504 Million
LRNs	100,000	200,000
NPA-NXXs	300,000	350,000
SPIDs	10,000	10,000
Supported Service Providers	32	512
Regional NPAC interfaces	3	8
Total number of EAGLEs and query servers supported	4 pair	8 pair
Users Supported	8	25

Data Administration

The main function of the LSMS is to receive, maintain, and distribute NPAC data and Locally Provisioned LNP data.

Administration of NPAC Data

The LSMS supports LNP data administration from up to eight regional NPACs. The NPAC data consists of:

- » Subscription versions (ported or pooled numbers with related data)
- » Number Pool Blocks (pooled numbers with related data)
- » Network Data (NPA-NXX, LRN, SPID, NPA-NXX-X)

Subscription versions include individual telephone numbers that are ported as well as numbers that are pooled. Number Pool Blocks are the Efficient Data Representation of pooled numbers.

The LSMS supports up to 504 million records. This capacity includes subscription versions and number pool blocks.

Number Pooling Efficient Data Representation (EDR)

This feature supports the Efficient Database Representation implementation of number pool blocks. A pool block, NPA-NXX-X, represents a 1000 block of numbers which are assigned to a block holder different from the code holder (NPA-NXX owner). Prior to EDR, each pooled TN is represented as an individual subscription version. The LSMS receives either pooled TNs or pool blocks depending on the Service Provider configuration at the NPAC. Conversion procedures are defined to migrate a region from individual TN pooling to EDR format.

Administration of Local LNP Data

The LSMS supports LNP data administration and distribution as defined in the following subsections.

» LRN Override GTT

When a telephone number is ported into the service provider's network, the final global title translation (GTT) for various services related to the ported-in number must be administered by the service provider. The LSMS supports administration and distribution of LRN override GTT data for the following services:

- » Custom Local Area Signaling Services (CLASS)
- » Line Information Database (LIDB)
- » Calling Name Delivery Service (CNAM)
- » Inter-Switch Voicemail (ISVM)
- » Wireless Short Message Service Center (WSMSC)


» NPA-NXX Default GTT

When an NPA-NXX is open for portability, default GTT may be provisioned for routing of non-ported numbers within that NPA-NXX. The LSMS supports administration and distribution of default GTT data for Message Relay for the following services:

- » Custom Local Area Subscriber Service (CLASS)
- » Line Information Data Base (LIDB)
- » Calling Name (CNAM)
- » Inter-switch Voice Messaging (ISVM)
- » Wireless Short Message Service Center (WSMSC)

» NPA Split Data

The LSMS supports administration of information regarding NPA splits. Users administer the old NPA, new NPA, NXX, and activation information. When the LSMS activates an NPA split, the LSMS changes all old NPA-NXX subscriptions to the new NPANXX and deletes the old information. The NPA split is forwarded to the EAGLE, where the EAGLE makes appropriate updates to its database.



NPAC updates its own records and does not automatically send the updated split information to the LSMS. The NPA splits are independently administered at the NPAC and LSMS.

» Migration of SPID Data

This function addresses the ability to migrate SV, NPB, network data, and related locally provisioned data from one Service Provider ID to another. This function does not occur over the NPAC/LSMS interface, but requires independent, coordinated activities at the NPAC and the LSMS.

The NPAC provides files with selection criteria that are used to determine which data objects need to be migrated from one SPID to another. Industry methods and procedures guide these independent updates at the NPAC and LSMSs (and other systems, such as SOAs) simultaneously across the country.

The LSMS uses these files to update the appropriate data at the LSMS. The LSMS also provides information to the Oracle Communications EAGLE over the LSMS/ELAP interface so that data at the EAGLE can be also migrated.

Since this function impacts data at the LSMS and the EAGLE, a corresponding EAGLE function is also required.

Data Auditing

As the facilitator of data provisioning between NPAC and the EAGLE LNP, the LSMS supports database auditing in both directions.

- » Supports data audit function between NPAC SMS and LSMS. This type of audit is initiated by NPAC SMS.
- » Initiates audits and reconciliation between LSMS and EAGLE LNP. This type of audit is initiated from the LSMS.

The LSMS responds to an NPAC SMS query request with the data in the LSMS database. The NPAC performs the comparison, and provides any corrections over the interface. The LSMS is not aware of the audit or its results.

An LSMS user can also initiate data audits from an LSMS workstation. The LSMS audits the LNP/STP database against the LSMS database. Audits may be performed with or without a reconcile. Results of the audit are provided to the user. Audit options are:

- » TN (range)
- » Audit TNs and Number Pool Blocks by time range
- » Number Pool Block (range)
- » Default GTT (range)
- » Override GTT (range)
- » NPA Splits (range)

For each type of audit, the LSMS identifies and reports the following types of discrepancies:

- » Different data - Data objects with different attributes or contents from the same data object stored on the LSMS
- » Missing data - LSMS data that does not exist in the EAGLE LNP database
- » Additional data - EAGLE LNP data objects that do not exist on the LSMS database


LSMS User Interfaces

Local Graphical User Interface (GUI)

The LSMS application allows direct administration and provisioning of the LNP data through an easy-to-use graphical user interface. Access to the local GUI is provided via the command line or via ssh or telnet.

The login message displayed may be optionally customized to meet local or corporate security guidelines.

The LSMS GUI uses a series of windows and menus to simplify the configuration and administration of the LSMS. Navigation through the GUI is accomplished by pointing and selecting menu choices using the mouse pointer. The command bar buttons can be clicked to activate a variety of functions:

- 
- » Configuring the LNP System (NPAC, LSMS, EAGLE RTDB) and service providers
 - » Administering NPAC and LSMS keys
 - » Managing NPAC functions
 - » Administering LSMS locally provisioned data (EMS List, default GTT, override GTT)
 - » Log file viewing

The GUI also provides monitoring capabilities to the users. Informational notifications, association status, and alarm data are displayed on the GUI.

IP Graphical User Interface (GUI)

The LSMS also supports a web-based access to the GUI. The web-based GUI is accessible from a workstation running the approved browsers on the same intranet as the LSMS. This is the same GUI as defined in the previous section, only the access method is changed. Traffic between the IP GUI and the LSMS is secured with SSL-3 encryption.

Command Line Database Administration

In addition to the Graphical User Interface, the LSMS also supports many functions via the optional command line interface.

Most LSMS functions are accessed through the GUI process, which requires users to have access to a local X-Windows server or web-browser. Some LSMS functions are also available by using a text-only local or remote interface using the command-line interface utility. Command line operations provide a limited, yet important, subset of the LSMS functionality to any authorized remote user. The command-line interface also allows the functionality to be accessible by using scripts, either locally or remotely.

Input Data by File

This feature provides an alternate method of provisioning new default GTT, override GTT, NPA Split entries, and EMS lists. New entries may be properly formatted in an input file and provisioned by importing the file, rather than individually entering the data via the GUI.

Service Assurance Interface

The Service Assurance feature allows an external system to access subscription version data from the LNP databases in the LSMS. This is limited to TN data only, Number Pool Block data is not supported. This information is useful in verifying correct porting of data, and helps in troubleshooting problems. There is one LNP database for each of the NPACs associated with the LSMS. The external system uses Service Assurance Manager (SAM) application to initiate service assurance data requests and associations. Single or multiple SAMs may exist on the external computer system. The SAM communicates with the LSMS through the Service Assurance Agent (SAA) application in the LSMS. The protocol used by the SAM/SAA is Q.3. The SAM application is not Oracle software and it resides only on the external system.

Local Data Security

The LSMS supports user account and password for login. The Service Provider ID may also be used for login verification.

Five non-configurable GUI user groups are available for various user authorization levels.

1. System Configuration User (Ismsadm)
2. Database Administration User (Ismsuser)
3. Viewer User (Ismsview)

4. External User (lsmsuext)
5. All Users (lsmsall)

Additional, configurable GUI user groups are also supported. Up to 128 configurable GUI user groups can be defined to ensure a customer specific and secure environment. After creating the new, configurable GUI user groups, the system administrator can assign users to the appropriate group.

The configurable GUI user groups control access to GUI commands, the CLAA (Command Line Administration Application) equivalent, or any UNIX command equivalent of the GUI functions, as well as defining access to a fixed set of UNIX commands.

The LSMS also supports an optional Automatic Inactivity Logout. This feature supports system level and user level timers. The timers are used to force a logout for inactive sessions. This is a security measure to prevent access to an abandoned user session.

Local Data SPID Security

The LSMS also supports SPID level security for user login. This allows the account administrator to grant access for each user to designated Supported Service Provider IDs only. Login verification in this case includes user account, password and SPID.

Outage Recovery

An outage can be caused by an LSMS internal error, an association failure (network failure), NPAC SMS downtime, or LSMS or NPAC SMS planned downtime.

Recovery with the NPAC

Each time the association is reestablished after an outage between the NPAC and the LSMS, the NPAC and the LSMS automatically resynchronize the LSMS database. The LSMS notifies NPAC SMS when the recovery mode finishes, and NPAC SMS then sends the LSMS any updates that occurred during the recovery.

If the NPAC and the LSMS are unable to complete automatic recovery, a bulk download from the NPAC to the LSMS may be performed to update the database.

The LSMS supports two different types of bulk data download (BDD) files from the NPAC.

1. Object based files provide all the data within a specified range. The LSMS uses this file to populate the data in the specified range.
2. Time range or delta BDD files provide transactions over a specified period of time. The LSMS uses this file to make updates, creations or deletions against its current database.


For either type of BDD file, the LSMS supports a response file, which can be used by the NPAC to update its TN status (e.g. remove a provider from the failed list).

Recovery with the EAGLE LNP

Each time the association is reestablished after an outage between the NPAC and the EAGLE, the LSMS and the EAGLE automatically resynchronize the EAGLE database. When recovery mode completes, the LSMS sends any queued updates that occurred during the recovery and continues sending normal traffic.

If the LSMS and the EAGLE are unable to perform an automatic recovery, due to the amount of data or duration of the outage, the condition will be flagged. A bulk download from the LSMS to the EAGLE may then be performed to update the database.

Support for Multiple EAGLE LNPs



The LSMS supports up to as many as eight EAGLE pairs. The LSMS supports association management, data distribution, and monitoring of all subtending EAGLEs.

The LSMS distributes ported Telephone Number records based on each EAGLE' area of portability service (AOPS). For each EAGLE LNP managed by the LSMS, the LSMS maintains a list of NPA-NXXs as its AOPS. The LSMS uses this list to determine which EAGLE should receive each ported record that is sent from the NPAC. This allows segregation of the LSMS ported number data onto multiple EAGLE pairs.

Enhanced LSMS Filters

The LSMS and EAGLE LNP databases may be deployed in a variety of network configurations. The Enhanced LSMS Filters function allows the user to administer locally provisioned data that may be unique to each Network Element. Whereas ported record data is distributed based on AOPS as described in Support for Multiple, this feature allows selective distribution of the Default GTT and LRN Override GTT data.

Support for Multiple NPAC SMSs

The OC LSMS receives and transmits NPAC LNP data from and to up to eight NPAC SMSs. The maximum number of NPAC SMS interfaces supported is configurable at installation time:

- » The LSMS maintains the logical separations of data belonging to each NPAC. Each NPAC SMS has access only to the data belonging to its domain and is prevented from modifying or retrieving other data.
- » A separate key file for secure association is used for each NPAC.

Multiple Supported Service Providers

The LSMS handles multiple supported service providers (Supported SPIDs). For each supported service provider, the LSMS maintains a service provider ID and supports locally provisioned data for that service provider ID. Supported Service providers are entities that buy access to the LNP service from the LSMS owner and use this functionality to support LNP in their own networks or the LSMS owner's network.

The LSMS system is configured with support for up to 32 Supported SPIDs. Additional Supported SPIDs may be optionally configured, up to a maximum of 512.

System Surveillance

This feature supports local and remote surveillance by reporting critical hardware messages, critical application messages, association failures, and other alarm and status information over a serial interface. Conditions requiring immediate action can be flagged to remote systems without requiring personnel on site. The first 8 characters of the message are the unique message ID.

Remote Monitoring

This feature provides an SNMP agent on the LSMS. A set of specific management information is provided to a remote location via the SNMP protocol over TCP/IP/Ethernet. Alarm, status and informational events are reported via SNMP traps and alarm resynchronization between LSMS and the NMS is supported. The three supported SNMP global modes include: SNMP v1 Only Mode, SNMP v3 Only Mode, or Both SNMP v1 and v3 Mode.

Reports

A variety of pre-defined reports are available on the LSMS. The LSMS supports generating, viewing, printing, and transferring these reports. Filter criteria are supported to allow the user to customize the report contents based on the need.

Report types are as follows:

- » Service provider administrative data - This is information, such as service provider ID and address, contained in the supported ServProvNetwork. Information regarding NPAC connections is also available in this report.
- » Supported service provider network data - This is information received from the NPAC, such as the service provider NPA-NXX list and LRN list.
- » Element management system configuration data - This information includes the element management system owner, ID, address, network element supported, and the area of service.
- » Message relay 6-digit default translations - These are the default global title translations.
- » Message relay 10-digit override translations - These are the override global title translations.
- » NPA Split Data
- » Subscriptions by LRN subscription data report
- » Subscriptions by Service Provider data report
- » LSMS Number Pool Blocks by LRN Data
- » LSMS Number Pool Blocks by Service Provider Data
- » Service Provider Data

Report Generator

The report generator uses a new LSMS Query Language (LQL) to enable the user to create reports that are not already available through the “Reports” menu item on the LSMS GUI. LQL is based on a subset of the American National Standards Institute (ANSI) Structured Query Language (SQL).

The report generator supports queries against Subscription versions, Number pool blocks, Default GTT, Override GTT, and NPA splits. Users may customize selection and output criteria for tailored reports. Interactive and batch mode are supported.

Logs

The LSMS maintains a set of logs for each NPAC associated with the LSMS, and another set for the LSMS supported agent, which is its interface to the network elements. All logs are viewable from all running GUI sessions. Logs are typically maintained on a daily basis, with up to seven days’ worth of logs stored on the system.

The LSMS logs include:

- » Security Log – This log records actions performed on the LSMS database which maintains LSMS user accounts.
- » NPAC Logs – These logs for each association with an NPAC include:
 - » Activity logs
 - » CMIP logs
 - » Transaction logs
 - » Event logs
- » EAGLE Agent Logs – These logs for each association with an EAGLE CLLI include:
 - » Transaction logs
 - » Exception logs
- » Common– These logs are common to the system
 - » Alarm
 - » Splits
 - » Trace
 - » Locally Entered Data
- » LSMS Usage Measurements – These logs record system run-time information, including:
 - » NPAC-initiated revisions to the LSMS data

- » NPAC-LSMS association and traffic measurement
- » LSMS-EMS association and traffic measurement
- » LSMS Evaluation Logs – These logs, which record system monitoring information, include:
 - » Audit and High-speed audit logs
 - » High-speed bulk load logs
 - » High-speed resynchronization logs
 - » Surveillance logs

LSMS Query Server Package

The LSMS Query Server Package enables customers to access real time LNP data using a standard API. Customers can perform customized, high volume automated data queries for use by internal office and support systems such as systems for service assurance, testing, service fulfillment, and customer care.

The query server resides on a separate platform from the LSMS, and maintains a separate and distinct copy of the LNP data. Customers provide their own hardware system that is consistent with the platform specifications provided by Oracle.

For purposes of quantifying the number of EAGLE nodes supported by the LSMS (so that the maximum number of supported EAGLE nodes is not exceeded), each query server supported must be counted as one EAGLE node.

As shown in the figure below, the query server system is provisioned from the OC LSMS using database replication techniques provided by MySQL.

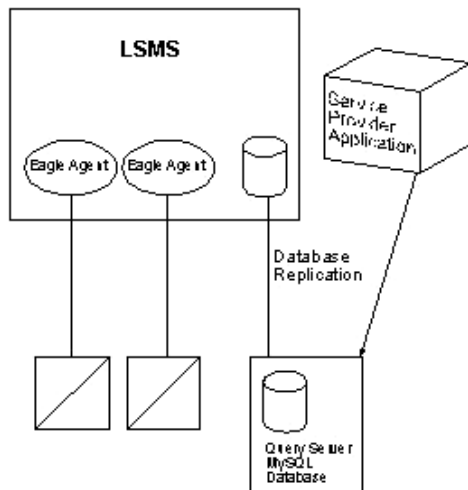


Figure 104: LSMS Query Server Overview

The LSMS Query Server supports automated database access using standard interfaces such as SQL, ODBC, and JDBC. This allows customers the flexibility to customize SQL queries in order to create queries to meet their specific business needs.

File Transfers

The LSMS has an FTP directory used for transferring files from the NPAC to the LSMS. Administration personnel can perform an SFTP-GET from the NPAC to the LSMS.

Automatic File Transfer

This feature offers the capability to schedule automatic transfers of files or logs generated at the LSMS to a remote FTP account. This reduces manual effort and potential errors which could result in missed data.

Backup

The LSMS automatically backs up the database and configuration data files onto the network attached storage device. The NAS provides additional data storage and recovery for up to five days of database updates. The backup data can be used to restore data after an outage.

IP SIGNALING

OVERVIEW

The telecommunications industry is moving from a traditional SS7 network to an all IP network to gain higher bandwidth at a lower cost, higher efficiency, and access to an exploding number of revenue-generating services. Oracle's goal is to use an SS7-over-IP or SIGTRAN converged network as the first step to make reliable signaling over IP possible without replacing the entire network.

An SS7-over-IP network consists of a traditional SS7 network that can integrate IP-enabled or all-IP devices with protocols defined by the Internet Engineering Task Force (IETF) standards organization. SS7-over-IP signaling primarily addresses the transport aspect of SS7. Call-control services and other types of services, therefore, can continue to be offered and deployed without concern for the method of interconnection. The method of service implementation, however, remains dependent on the particular network element chosen to support the service rather than the transport chosen.

SIGTRAN is a working group of the IETF, addressing packet-based Public Switched Telephone Network (PSTN) signaling over IP networks. The group's work resulted in a set of signaling transport protocols, which are called collectively "SIGTRAN" protocols or suite for the purpose of this document. The SIGTRAN) protocol suite is the protocol of choice to access IP networks.

The SIGTRAN architecture used by Oracle includes the following protocols:

- » Stream Control Transmission Protocol (SCTP); RFC 2960 - A reliable transport protocol operating on top of a connectionless packet network such as IP. Developed to eliminate deficiencies in TCP.
- » MTP2 User Peer-to-Peer Adaptation Layer (M2PA) protocol; RFC 4165 - Provides MTP3 with MTP2 equivalent service, over IP using the services of SCTP.
- » MTP3 User Adaptation Layer (M3UA) protocol; RFC 4666 - Designed for Signaling Gateways that enable a seamless inter-working between the SS7 and IP domain. This protocol supports the transport of any SS7 MTP3-User signaling (i.e. ISUP and SCCP) over IP using services of SCTP.
- » SCCP User Adaptation Layer (SUA) protocol; RFC 3868 - Supports the transport of SCCP-User signaling over IP using services of SCTP.

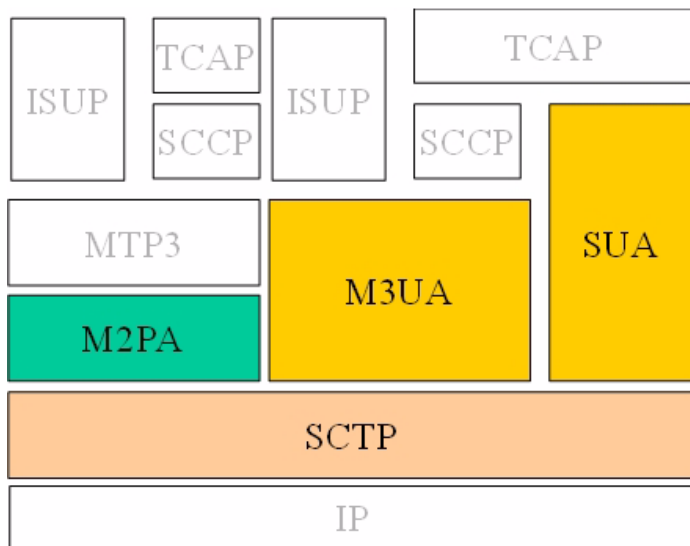


Figure 105: Oracle SIGTRAN Protocols

EAGLE as Signaling Gateway

The EAGLE is a robust SS7-over-IP solution that delivers centralized signaling routing, and bridges the legacy circuit-switched and packet networks. It provides seamless interworking between TDM resources such as Service Control Points and IP-enabled elements such as Media Gateway Controllers and next-generation databases. With its packet-based technology, the EAGLE can handle signaling requirements of the most complex networks, delivering dynamic bandwidth sharing to support increases in signaling traffic without additional nodes. The same platform delivers full Signal Transfer Point capabilities and a complete portfolio of integrated applications. Using the EAGLE to structure the network provides a predictable and reliable architecture with all required interfaces. The EAGLE is easily scalable to cover huge core networks, with an independent control layer that allows expansion on different parts of the network independent of each other. The EAGLE provides ease of database management for the SS7-over-IP architecture.

In general, IP Signaling functions provide:


- » Point code mapping between SS7 and IP
- » GTT and screening capability extended to IP
- » Protocol conversion for MTP, SCCP, and ISUP over IP
- » Point code consolidation (Carrier Identification Code [CIC] routing) for addressing multidiagonal-offload controllers to a single point code
- » Standard SCTP Association-based connection-oriented service.
- » Management control of the associations
- » Controlled flow of data across the association
- » Test and watchdog maintenance messages

IPLIMx, IPGWx, and IPSG Applications

The EAGLE implements SIGTRAN with three applications:

The IPGWx functionality provides Point to Multi-Point MTP-User signaling (e.g., ISUP, TCAP) over IP capability:

- » Supports M3UA and SUA protocols

- 
- » Typically used for A and E link connectivity
 - » Can host up to 50 IP logical connections per card
 - » Supports a SS7 signaling link, but this link terminates at a virtual SP, having a fake adjacent point code
 - » Supports routing keys (selects IP logical connection based on DPC/OPC/SI/CIC/SSN)
 - » Configured in a multi-card linkset configuration. A maximum of 8 cards per linkset and 64 cards per system is supported
 - » End Office mode (EAGLE shares its point codes with IP-remote-applications) is supported
 - » Implements Application Server procedures for M3UA and SUA
 - » Connects to IP-based User Parts. The peer does not need to implement MTP3

The IPLIMx functionality provides Point-to-Multi-Point MTP3 and MTP3-User signaling over IP capability:

- » Supports M2PA protocol
- » Typically used for B-C-D links but can be used for A links
- » Each IP logical connection is assigned to an SS7 signaling link
- » Can host up to 16 IP logical connections per E5-ENET card
- » Supports up to 16 SS7 signaling links per E5-ENET card; each link having an assigned IP logical connection
- » Does not support routing keys (MTP3 routing only). The connected IPSP must implement MTP3.
- » Up to 100 IPLIMs are supported in a system
- » End Office mode is not supported
- » Does not implement Application Server procedures

The IPSPG functionality provides Point to Multi-Point MTP3 and MTP-User signaling over IP capability:

- » Supports M3UA and M2PA protocols simultaneously on one card
- » Supports ANSI, ITU-N, ITU-24 or ITU-I on one card
- » Can host up to 32 IP logical connections per card and 16 links per linkset
- » Supports an SS7 signaling link
- » Supports routing keys using MTP origin based routing (selects IP logical connection based on DPC/OPC/SI, except adjacent PC)
- » Up to 100 IPSPG cards are supported in a system
- » Implements Application Server procedures for M3UA

The figure below shows a typical EAGLE IP signaling deployment.

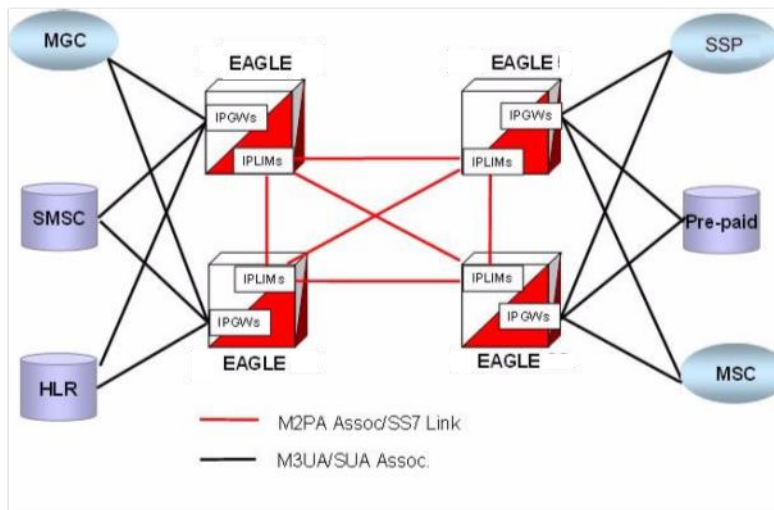


Figure 106: Typical EAGLE IP Signaling Deployment

PERFORMANCE

IP signaling throughput performance is determined by protocol, hardware, and feature set in use. Performance can be measured by considering the maximum throughput that can be sustained without congestion, the ability to increase total throughput under an increased load proportionally to added resources such as hardware or software (scalability), and the cost associated with each transaction per second (transaction unit model).

Please refer to the EAGLE Planning Guide for details regarding the various TU cost models and conversion to MSU/sec equivalents.

PROTOCOLS AND APPLICATIONS

SCTP/IP

TCP, the Transmission Control Protocol (IETF RFC 791), has been the primary means of reliable data transfer in IP networks around the world for several decades. Despite being ubiquitous, TCP has become limited in its use by new applications and has several security weaknesses. To overcome these limitations, the IETF Sigtran Working Group has developed a new, more reliable transport protocol and has named it the Stream Control Transmission Protocol (SCTP). SCTP (IETF RFC 2960) is the transport layer for all standard IETF-Sigtran protocols. SCTP is a reliable transport protocol designed to operate on top of IP.

SCTP offers the following services to its users:

- » acknowledged error-free non-duplicated transfer of user data.
- » data fragmentation to conform to discovered path MTU size.
- » sequenced delivery of user messages within multiple streams, with an option for out-of-order-of-arrival delivery of individual user messages. (option not supported)
- » bundling of multiple user messages into a single SCTP packet.
- » network-level fault tolerance through supporting of multi-homing at either or both ends of an association.

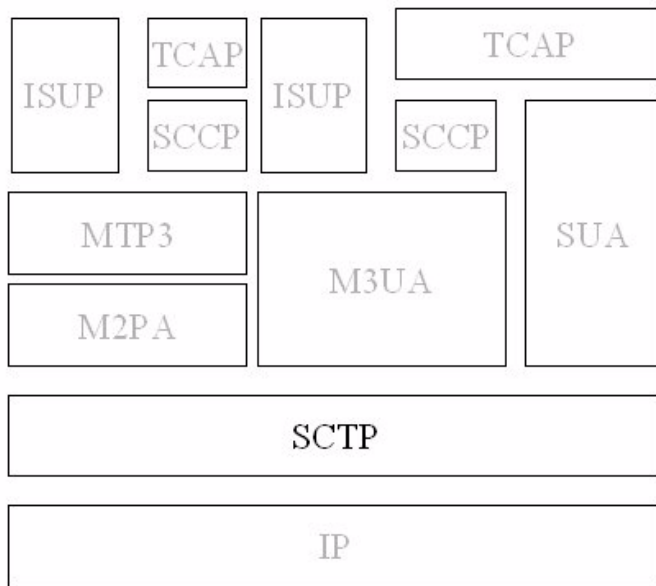


Figure 107: Sctp Overview Diagram

Sctp vs. TCP

Sctp is a connection-oriented transport protocol that uses logical connections called associations, which are similar to TCP sockets. However, an Sctp association is a much broader concept than the TCP connection. Although Sctp is similar in some respects to the Transport Control Protocol (TCP), it differs in several key areas. Sctp and TCP are similar in that they both provide a reliable data delivery over a non-reliable network protocol (IP). The Sctp protocol is intended to be a more robust and higher performance protocol than TCP in the following areas:

- » Broader definition of connection four-tuple via multi-homing (local IP address, local port, remote IP address, and remote port).
- » Multiple streams
- » Datagram stream
- » Selective Acknowledgements
- » Un-ordered delivery capability (not supported)
- » Enhanced security

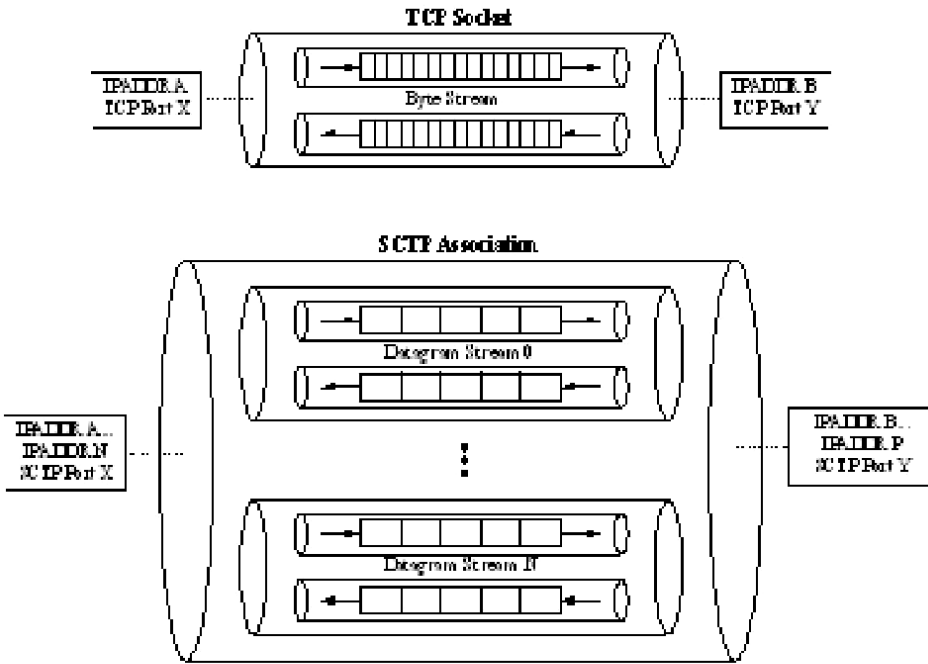


Figure 108: Associations vs. TCP Sockets

Broader Definition of Connection Four-Tuple (Multi-Homing)

The TCP protocol defines a connection via a four-tuple - a specific local IP address, local port, a specific remote host IP address and remote port. A TCP connection is point-to-point and once the session is established the four-tuple cannot change. SCTP uses a similar four-tuple concept, but provides for the local and remote IP address values to be a list of IP addresses. This feature allows a multi-homed host, with multiple network interfaces and more than one way to reach the far-end host. From a redundancy perspective the support of multi-homing session end-points can be viewed as a major advantage for SCTP.

Multiple Streams

TCP is a point-to-point byte stream oriented transport protocol. In such a protocol if a single byte is corrupted or lost, then all data that follows must be queued and delayed from delivery to the application until the missing data is retransmitted and received to make the stream valid. With the TCP protocol, all data being transmitted is affected due to the fact that there is only one path from end-to-end. The SCTP protocol addresses this limitation by providing the capability to specify more than one transport path between the two end-points. In SCTP, the four-tuple - with the multi-homing capability - defines what the SCTP protocol calls an association. The association is composed of one or more uni-directional transport paths called streams. The number of inbound and outbound streams is independent of one another and is determined at session initiation time (e.g., an association may be composed of 3 outbound and 1 inbound stream). In this scheme a data retransmission only affects a single stream. If an association is defined with multiple streams and a packet is lost on a specific stream, data transmissions on the other streams which form this association are not blocked. However, the application utilizing SCTP must take advantage of this capability.

Datagram Stream

Where TCP is implemented as a byte oriented stream protocol, SCTP is based on a datagram oriented protocol stream. In choosing the datagram as the smallest unit of transport, the SCTP protocol removes the need for the upper layer application to encode the length of a message as part of the message.

Selective Acknowledgements

TCP acknowledgements are specified as the last consecutive byte in the byte stream that has been received. If a byte is dropped, the TCP protocol on the receiving side cannot pass inbound data to the user until the sender retransmits the lost byte (i.e. the stream is blocked). SCTP uses a feature known as selective acknowledgement in which each data chunk is identified by a chunk number - Transmission Sequence Number (TSN) in SCTP terminology - and is explicitly acknowledged at a data chunk granularity. This means that if a data chunk is dropped, then only that one data chunk needs to be retransmitted. Also, with the concept of streams, a dropped data chunk only affects one stream due to the fact that ordered transmission of data is only enforced at the stream and not the association level.

Un-order Delivery Capability

Unlike TCP, the SCTP protocol provides a mechanism for un-ordered datagram delivery. This feature means that a datagram can be transmitted and received independent of datagram sequencing and thus not delayed in the presence of a retransmission. This capability is not currently supported.

Enhanced Security

The TCP protocol has a known and easily exploitable vulnerability to denial of service attacks (e.g., SYN attacks). This weakness is due to the three-way handshake utilized by the TCP session establishment protocol. The TCP session establishment method causes system resources to be committed prior to actually establishing the session. SCTP addresses this by utilizing a four-way handshake where resources are not committed by the host being contacted until the contacting host confirms that it is actually making a contact request to prevent such attacks. The SCTP handshake is shown in the figure below.

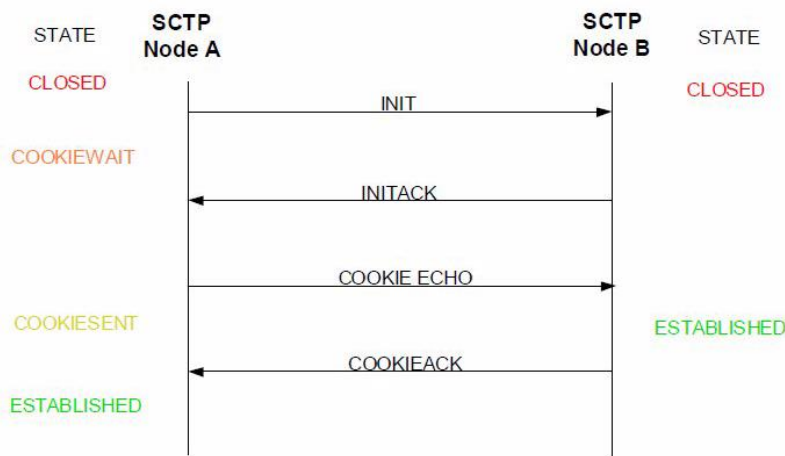


Figure 109: SCTP Protocol Handshake

SCTP Retransmission Control

The standard RFC definition of the SCTP protocol introduces several time-critical constraints that can have negative impacts on the delivery of SS7 data. For example, when back-to-back packet losses were suffered, the RFC standard does not provide for a rapid recovery mechanism. The RFC retransmission mechanism is better adapted to tolerate unstable networks exhibiting large amount of packet loss and varying network delays. These characteristics are not normal for stable networks exhibiting low packet loss and minimal delay variations.

SCTP retransmission control offers users a choice of two retransmission policies and enhanced control over the behavior of data retransmissions of SCTP associations in the IP Signaling function of the EAGLE as shown below. This functionality allows users to tailor retransmissions to their networks on an individual association basis to address these time critical protocol constraints.

- » RFC: Doubles the Timeout Value until Max Retries. Uses Slow Start and Congestion Avoidance algorithms per RFC 2960.
- » Linear: Same Timeout Used for Each retransmission. Only Slow Start Used for Congestion Avoidance

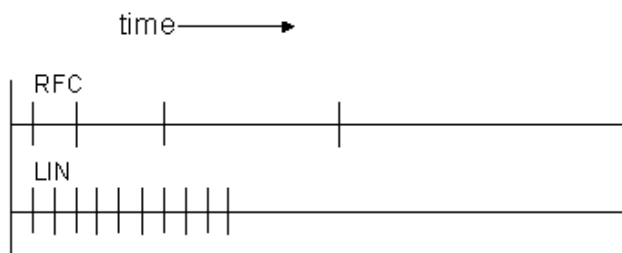


Figure 110: SCTP Retransmission Control

Note: Not all of the retransmissions are shown for RFC mode because of scale

Both the more aggressive linear algorithm and the RFC standard algorithm have fixed software limitations placed on the algorithms which are not appropriate for all network scenarios. Such limitations include boundaries on minimum and maximum retransmission delays, maximum number of retries, and minimum size of the congestion window.

It is important that the effect each parameter has on overall throughput be understood. When the upper bound of the retransmission timeout (RTO) is configured too low, an increased load caused by unnecessary data chunk retransmission can result in network congestion.

The overall effect will delay or prevent delivery of SS7 data, resulting in a negative impact on MSU throughput or even connections being lost. If the lower bound of the RTO is set too high, the SCTP protocol layer may not react quickly enough to network failures, resulting in the SS7 service being degraded.

In the "RFC" mode, the EAGLE implementation performs retransmissions and congestion control as specified in RFC 2960 with the following exceptions:

- » The calculated RTO is bounded by user-configurable upper and lower limits called RMIN and RMAX.
- » The Association.Max.Retrans value is specified by a user configurable parameter called RTIMES.
- » The minimum and initial value of the congestion window is a user configurable parameter called CWMIN.

In "Linear" mode, the Signaling implementation has the following differences from the RFC version:

- » Uses the current RTO value instead of exponential blocks for retransmission delay.
- » Uses the Slow Start algorithm at all times and does not use the Congestion Avoidance algorithm.

M3UA on IPGWx

The IP Signaling implementation of M3UA is based on IETF RFC 3332. According to the IETF's Architectural Framework for Signaling Transport (RFC 2719), IPGWx Signaling is signaling designed to support an Application Server (AS) that can communicate with up to 50 Application Server Processes (ASPs) connected to the AS per card via M3UA-enabled endpoints/SCTP associations.

The EAGLE M3UA implementation provides the following capabilities:

- » Support for the transfer of all SS7 MTP3-User Part messages (e.g., ISUP, SCCP, TUP, etc.)
- » Support for the seamless operation of MTP3-User protocol peers
- » Support for the management of SCTP transport associations and traffic between the EAGLE and up to 50 MGCs or IP-resident Databases per card.
- » Support for MGC or IP-resident Database process fail-over and load-sharing
- » Support for the asynchronous reporting of status changes to management
- » Support for between 64,000 to 112,000 TU/s (redundant) depending on configuration.
- » Support 64 point codes in M3UA DAUD message

The M3UA Layer at an ASP provides the equivalent set of primitives at its upper layer to the MTP3-Users as provided by the MTP Level 3 to its local users at an SS7 Signaling End Point (SEP). In this way, the ISUP and/or SCCP layer at an ASP is unaware that the expected MTP3 services are offered remotely from an MTP3 Layer at the EAGLE, and not by a local MTP3 layer. The MTP3 layer at the EAGLE may also be unaware that its local users are actually remote user parts over M3UA. In effect, M3UA extends access to the MTP3 layer services to a remote IP-based application.

The figure below shows a high-level view of the IPGWx protocols.

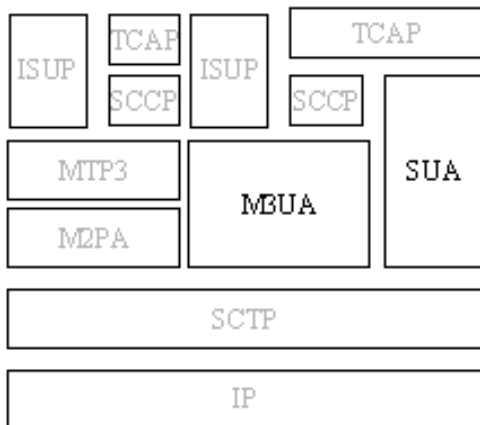


Figure 111: IPGWx Overview Diagram

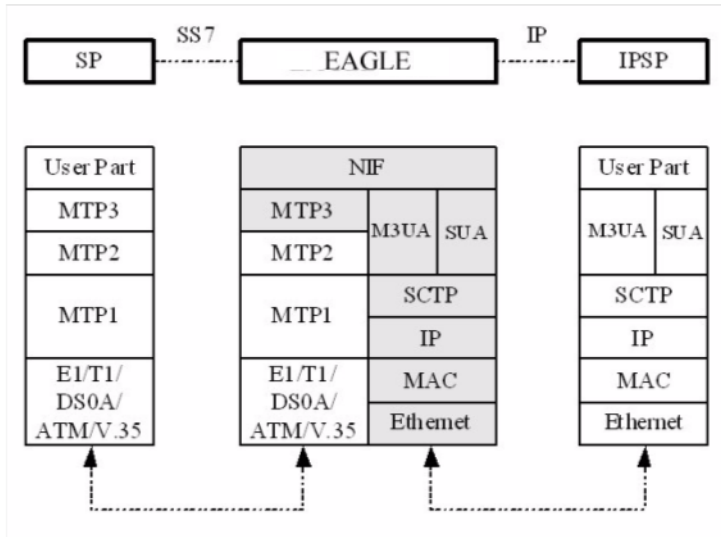


Figure 112: IPGWx Protocol Diagram

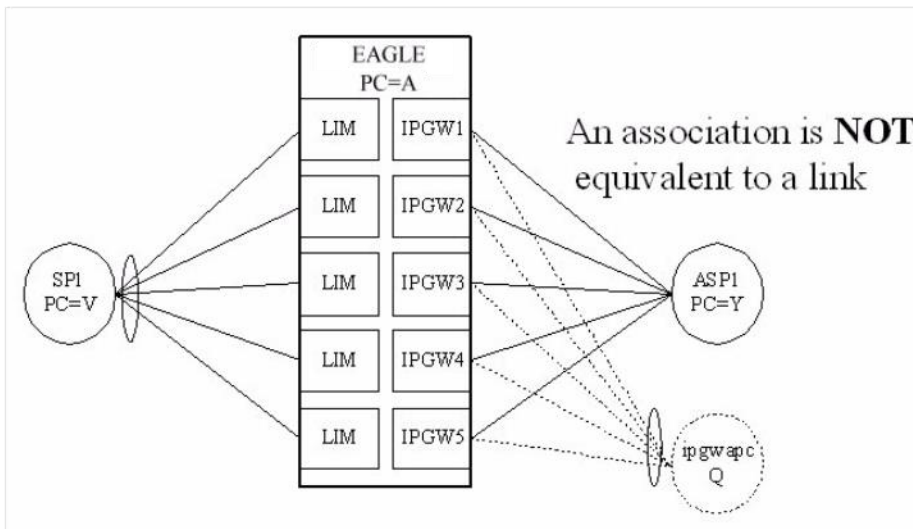


Figure 113: IPGWx Network View

M3UA Implementation Limitations

The EAGLE MTP3-User Adaptation Layer (M3UA) provides a protocol for supporting the transport of any SS7 MTP3-User signaling (e.g., ISUP and SCCP Messages) over IP using the services of the Stream Control Transmission Protocol. The main specification compliance items are summarized below. Note that this is not the entire list, just the main items:

1. The EAGLE implementation supports static routing key registration via OAM provisioning by associating an AS with a routing key. The ASPs that are working together to process SS7 traffic for one or more routing keys are logically grouped into an AS. Each routing key can be associated with a single AS. A single AS can be associated with multiple routing keys. Configuration is much simpler since there is no need to register each ASP for every key, only the AS needs to be registered. Since the EAGLE

implementation only supports static ASP/AS/Routing key configuration, ASP-ACTIVE is interpreted as applying to all of the routing keys associated with the ASP (through the AS).

2. The EAGLE implementation supports the LOADSHARE and OVERRIDE traffic mode types, but does not support the BROADCAST type.
3. The EAGLE implementation does not support the Info String parameter. This parameter is optional in all the messages it is defined in and will be ignored/disregarded in any message it is received in. The EAGLE never sends the info string parameter in an outgoing message.
4. The EAGLE implementation supports the Diagnostic Parameter but does not include the offending parameter for the case of Invalid Network Appearance, Traffic Handling Mode, Routing Context and Parameter Value. The EAGLE Diagnostic Parameter contains the 8 byte header of the invalid message.
5. The EAGLE implementation does not send HeartBeat Messages but will respond to BEAT Messages received from an ASP with Beat Acknowledge Messages.

IETF SUA for 'A' Link Connectivity

The SCCP User Adaptation Layer (SUA) is designed to fit the need for the delivery of SCCP-user messages (MAP & CAP over TCAP, RANAP, etc.) and new third generation network protocol messages over IP between two signaling endpoints. Consideration was given for the transport from an SS7 Signaling (e.g., the EAGLE) to an IP signaling node (such as an IP-resident Database). This protocol can also support transport of SCCP-user messages between two endpoints wholly contained within an IP network.

The EAGLE SUA implementation provides the following capability:

- » Support for transfer of SS7 SCCP-User Part messages (e.g., TCAP, RANAP, etc.)
- » Support for SCCP connection oriented service.
- » Support for the seamless operation of SCCP-User protocol peers
- » Support for the management of SCTP transport associations between the EAGLE and one or more IP-based signaling nodes).
- » Support for distributed IP-based signaling nodes.
- » Support for the asynchronous reporting of status changes to management

The IP Signaling implementation of SUA is based on IETF RFC 3868.

SUA DAUD with SSN Support

The SUA destination audit (DAUD) with SSN Support feature enables the EAGLE to update the SCCP cards with the status of remote subsystems to indicate whether the subsystems are allowed or prohibited. Additionally to determine the status of any subsystem using DAUD messages that contain the subsystem number (ssn) parameter.

When a node for a remote subsystem becomes available or unavailable, then the SUA DAUD with SSN Support feature allows the GSM MAP table, maintained on the EAGLE SCCP cards, to be updated with the new status.

When a DAUD message containing an ssn parameter is sent over an SUA association to the EAGLE, Gateway Screening is performed by a card that contains the SS7IPGW, IPGWI, or IPGHC GPLs. The message is then sent to the SCCP card to query the availability status of the subsystem. The EAGLE sends one of the following responses based on the subsystem status:

- » Status is available-Destination Available (DAVA) message
- » Status is unavailable-Destination Unavailable (DUNA) message
- » Status cannot be determined-Subsystem Status Unknown error message

Routing Key Registration

Routing Key Enhancements

To provide Signaling functions in Europe, IP Signaling must be able to route received ITU ISUP messages to devices on the IP network, such as MGCs.

The routing key enhancements feature provides routing to IP devices with an ITU National or International Point code. In addition, routing for TUP messages is also provided. The Routing Key Enhancements feature suite follows:

- » Q.BICC routing provides routing to SCTP/IP sockets for BICC messages. BICC messages are very similar to ISUP messages, except the CIC has been expanded to 32 bits. Routing for ANSI or ITU BICC messages is based on SI=13, OPC, DPC, and CIC. The point codes within the routing key must be ANSI, ITU National, or ITU International.
- » ITU routing key enhancements provide the following additional routing capabilities for international users:
 - » ITU ISUP CIC routing provides OPC/DPC/CIC routing to IP devices for ITU ISUP messages. Routing for ITU ISUP messages to an IP device is based on SI=5, OPC, DPC, and CIC. The point codes within the ITU ISUP routing key must be either ITU national or ITU international.
 - » ITU DPC-SSN routing provides DPC/SSN routing to IP devices for ITU SCCP messages. Routing for SCCP messages to an IP device is based on SI=3, DPC, and Subsystem. The point codes within the ITU SCCP routing key must be either ITU national or ITU international.
 - » ITU DPC-SI routing provides DPC/SI routing to IP devices for non-ISUP and non-SCCP ITU messages. A message with SI=4 bound for an ITU national or international point code is assumed to be a TUP message, and is routed as such. The point codes with the ITU DPC-SI routing key must be either ITU national or ITU international.
- » TUP routing provides OPC/DPC/CIC routing to IP devices for TUP messages. Routing TUP messages to an IP device with an ITU point code is based on SI=4, OPC, DPC, and CIC. The point codes within the routing key must be ITU national or ITU international. An MSU with SI=4 bound for an ANSI point code will continue to be routed on DPC-SI.

Unregistered Routing Key Treatment

The Unregistered Routing Key Treatment (URKT) feature provides improved methods of dealing with SS7 traffic that does not match a routing key entry in the IPGWx application routing key table. During transmit processing on each IPGWx card, the software attempts to find a routing key entry that exactly matches the MSU being processed. Prior to this feature, if a match could not be found, the MSU was silently discarded (in addition to the silent discard, if the MSU was an SCCP MSU we would generate a Sub System Prohibited (SSP) MSU and route it back to the originator). URKT provides several improved methods of dealing with these MSUs. Use of the URKT feature reduces SS7 message loss in an IP network.

The benefits of this feature include:

- » Addition of new types of routing keys to the IPGWx platform. For each MSU to be routed that does not exactly match a fully specified key, a hierarchy of lookups takes place which attempt to deliver the MSU to the best location (set of locations).
- » Ability for IPGWx cards to route MSUs to IP-NEs based on partial routing keys and default routing keys. Partial keys supported include: DPC+SI+OPC for CIC traffic, DPC+SI for CIC and SCCP traffic, DPC only, and SI only for CIC, SCCP, and MTP3-Other traffic.
- » Ability for IP-NEs to dynamically register and unregister partial and default routing keys.
- » Ability to provide a 'closest match' type of routing.
 - » Example #1 - if it is an ISUP MSU that we are trying to deliver, the normal ISUP key would be made up of DPC+SI+OPC+CIC. If no such match exists, try another lookup where we ignore the CIC. If that lookup fails, try another lookup where we ignore the CIC+OPC.

- » Example #2 – if it is an SCCP MSU that we are trying to deliver, the normal SCCP key would be made up of DPC+SI+SSN. If no such match exists, try another lookup where we ignore the SSN.

The user is required to perform provisioning to enable one or more of these URK Treatments. If no URK Treatment keys have been entered, the EAGLE will continue to silently discard (with peg + potential SSP) undeliverable MSUs.

Q.BICC Routing

Q.BICC provides routing to SCTP/IP sockets for BICC messages. Q.BICC routing does not convert ISUP to BICC messages and vice versa, but does provide the capability route BICC messages. Routing for ANSI or ITU BICC messages is based on SI=13, OPC, DPC, and CIC. Therefore, any message with the CIC in the position indicated in the figure below is routed on the key specified by SS7 Routing Key = (Message Type (SI=13) + OPC + DPC + CIC). The point codes within the routing key can be ANSI, ITU National, or ITU International.

Currently, the EAGLE can only route BICC messages that are 272 octets or less. For large BICC MSU support for IP signaling, see Large BICC MSU Support for IP Signaling.

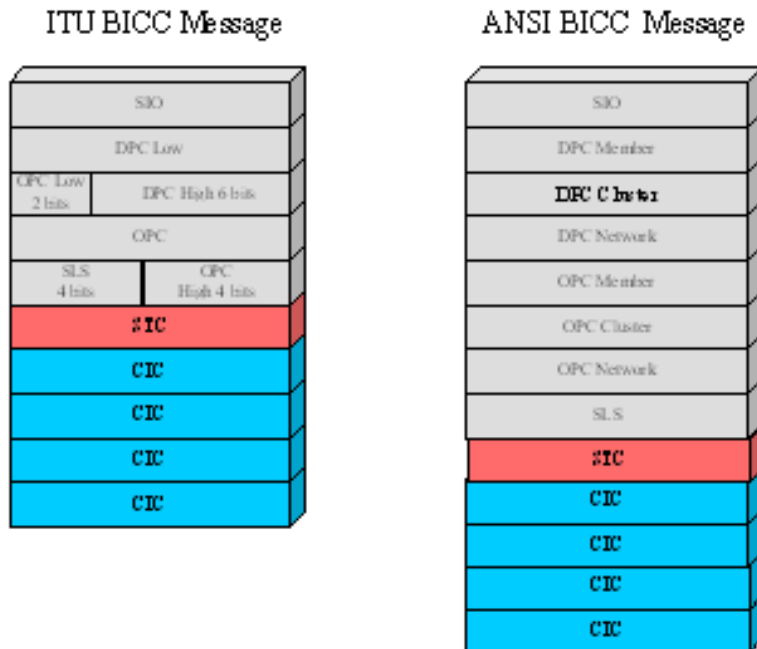


Figure 114: BICC Message Format

End Office Support

End Office Support enables the EAGLE to share its True Point Code (TPC) with an IP-based node connected via the IPGWx GPL without the need for a separate point code for the IP-node. When the End Office Support feature is in use, the EAGLE can share a point code for up to three network types with attached IP network elements.

Once a message arrives at the EAGLE destined for an end office node, routing key selection and socket/association selection allows multiple IP network elements to operate as a single end office node and be differentiated by using routing keys.

End office support is only deployed in single node configurations.

M2PA on IPLIMx

The MTP2-User Peer-to-Peer Adaptation Layer Protocol (M2PA) is designed for communications between peers (e.g., EAGLE to EAGLE), as well as IP enabled end points. The EAGLE supports the RFC version of the M2PA protocol, as well as draft version 6. M2PA is specifically designed to fully support the transport of SS7 Message Transfer Part (MTP) Layer 3 signaling messages over IP using the services of SCTP. This includes full MTP3 message handling and network management capabilities between any two SS7 nodes, communicating over an IP network. The M2PA protocol provides the following advantages over the M3UA and SUA protocols:

- » Greater support for MTP2 features such as link proving, processor outage, and blocking
- » Support for full retrieval due to link failure or processor outage (reduced message loss on failure)
- » Simple conversions of all SS7 messages into M2PA messages and vice versa (better gateway, higher performance)

The IPLIMx does not support routing keys, however, M2PA supports point-to-multi-point A-, B-, C-, D-, and E- SS7 link types. The addition of an M2PA/SCTP/IP protocol stack to the IPLIM application provides support for all of the SS7 link types using an industry standard protocol. This greatly increases the interoperability of the EAGLE in deployments involving these link types.

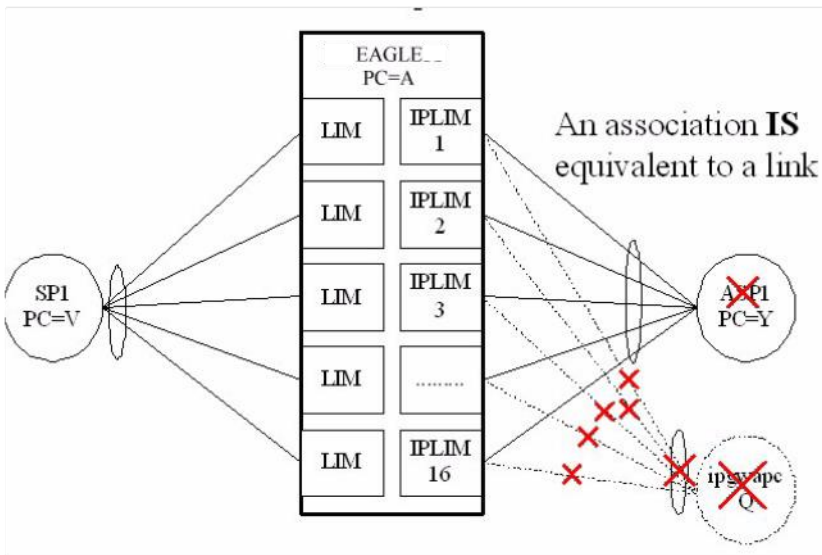


Figure 115: IPLIMx Network View

Below shows a high-level view of the IPLIMx protocols.

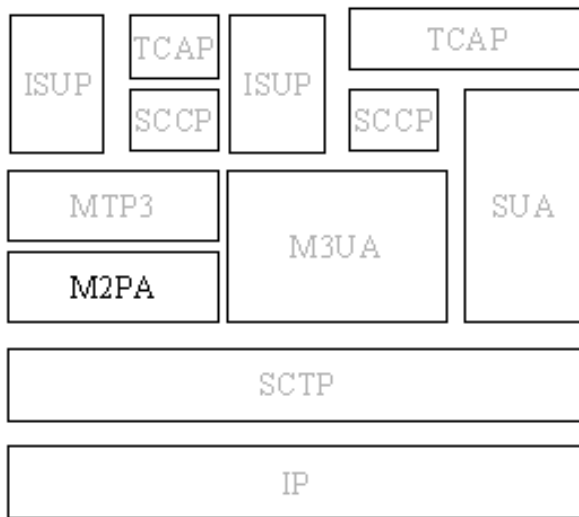


Figure 116: IPLIMx Overview Diagram

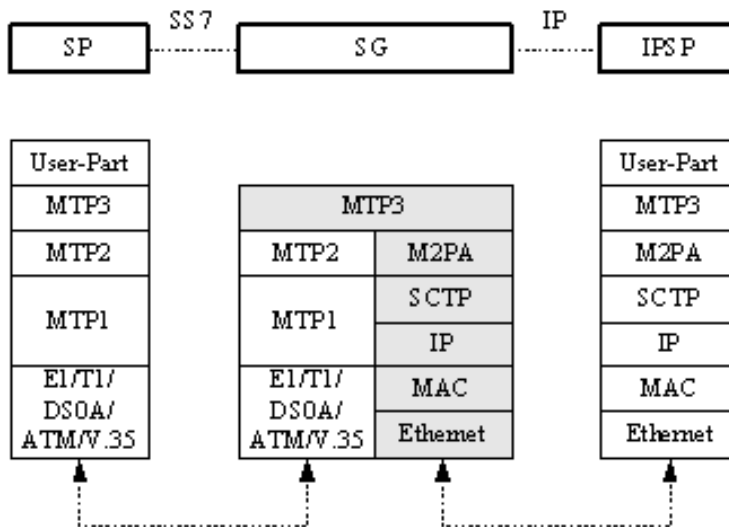


Figure 117: IPLIMx Protocol Diagram

SNMP

The SNMP Agent Implementation feature provides a Management Information Base (MIB) and SNMP traps for maintenance and monitoring of ethernet cards and IP objects. Requests (sets/gets) are supported at 5 per second.

The Simple Network Management Protocol (SNMP) is an industry-wide standard protocol used for network management. The SNMP Agent Implementation feature implements an SNMP agent on each IP card that runs the IPGWx or IPLIMx application. The SNMP Agent Implementation feature does not allow provisioning; the SNMP agent will run only on provisioned Ethernet cards. SNMP agents interact with network management applications called Network Management Systems (NMSs).

The SNMP agent maintains data variables that represent aspects of the IP card. These variables are called managed objects and are stored in the MIB. The SNMP protocol arranges managed objects into groups. There are five mandatory groups for any SNMP implementation: system, interfaces, at, ip, and icmp. Additionally, SNMP, TCP and UDP implementations must include the snmp, tcp, and udp groups.

The SNMP Agent Implementation feature supports all but the AT (Address Translation) group as defined in IETF RFC1213. The AT group is replaced by objects in other supported MIB groups.

An example of a system MIB is the sysUpTime object of the system group as follows:

```

SYSUPTIME OBJECT-TYPE
    SYNTAX TIMETICKS
    ACCESS READ-ONLY
    STATUS MANDATORY
    DESCRIPTION
        "THE TIME (IN HUNDREDTHS OF A SECOND) SINCE THE
        NETWORK MANAGEMENT PORTION OF THE SYSTEM WAS LAST
        RE-INITIALIZED."
 ::= { SYSTEM 3 }
    
```

The table below lists the supported traps and their compliance to the RFC.

Table 22: SNMP Traps Supported

TRAP TYPE	DESCRIPTION	Compliance
coldStart	A coldStart trap signifies that the sending protocol entity is reinitializing itself such that the agent's configuration or the protocol entity implementation may be altered	FC
warmStart	A warmStart trap signifies that the sending protocol entity is reinitializing itself such that neither the agent configuration nor the protocol entity implementation is altered	NC
linkDown	A linkDown trap signifies that the sending protocol entity recognizes a failure in one of the IP links represented in the agent's configuration	FC
linkUp	A linkUp trap signifies that the sending protocol entity recognizes that one of the IP links represented in the agent's configuration has come up	FC
authenticationFailure	An authenticationFailure trap signifies that the sending protocol entity is the addressee of a protocol message that is not properly authenticated. While implementations of the SNMP must be capable of generating this trap, they must also be capable of suppressing the emission of such traps via an implementation-specific mechanism	NC

FC = Fully Compliant

NC = Non Compliant

Large BICC MSU Support for IP Signaling

Feature Description

Bearer Independent Call Control (BICC) permits MSUs having a signaling information field (SIF) of greater than 272 bytes (up to 4095 bytes). The EAGLE software expects and enforces MSUs to have SIF less than or equal to 272

bytes. Large BICC MSU Support for IP Signaling features extends to allow up to 4095 bytes over the M2PA and M3UA protocols. This EAGLE feature is supported for ANSI, ITU National and ITU International.

Measurements have been improved to cater for this feature and following are the additional link component peg counts.

Table 23: Additional Link Component Peg Counts

Peg Count Name	Description
LMSURCV	Number of large MSUs received
LMSUTRN	Number of large MSUs transmitted
LMSUOCTRCV	Number of octets received in large MSUs
LMSUOCTTRN	Number of octets transmitted in large MSUs.
LMSURCVDSC	Number of large MSUs discarded in the receive path
LMSUTRNDSC	Number of large MSUs discarded in the transmit path

Considerations and Limitations

This feature allows a data feed for OC PIC of up to 272 bytes. If Large BICC MSU messages greater than 272 bytes invoke DTA or STPLAN processing, then the MSU is routed without copying, and an appropriate UIM is issued.

Large MSU Support for IP Signaling

The Large MSU Support for IP Signaling feature allows the Large BICC MSU Support for IP Signaling feature to support additional service indicator (SI) values. As part of this feature, the Large BICC MSU Support for IP Signaling feature is now referred to as the Large MSU Support for IP Signaling feature.

The Large MSU Support for IP Signaling feature supports MSUs with a SIF size of up to 4095 bytes for M2PA and M3UA protocols with SI values from 6 - 15.

The SI values are:


- » 6, 7—Data
- » 9—Broadband ISDN
- » 10—Satellite ISDN
- » 13—BICC
- » 14—H.248
- » 8, 11, 12, 15—Spare

The SLAN, Database Transport Access (DTA), and integrated monitoring features do not support Large MSUs.

EAGLE Fast Copy

The EAGLE Fast Copy (Fast Copy) feature uses a fast copy interface to the Integrated Message Feeder (IMF) to transport monitored SIGTRAN data while bypassing the Inter-Module Transport (IMT) and network stack. This ability allows data from the SIGTRAN network to be monitored in real time without impacting the EAGLE IMT bus, thereby eliminating EAGLE overhead.

The existing STC interface is used to transport configuration and link event data. Fast Copy architecture uses two separate networks for STC monitoring and Fast Copy monitoring.



The Fast Copy feature runs on Ethernet cards that are running the ipsg or ipgw application. The Fast Copy mode is a system-wide option. If the mode is set to fast copy, then all cards that are capable of supporting Fast Copy will switch to Fast Copy Monitoring.

FastCopy on IPGW provides support for monitoring M3UA and SUA traffic on Ethernet cards running the IPGHC GPL using Fast Copy-based or STC monitoring.

IPSG Link Capacity Sharing

The Support IPSG Link Capacity Sharing feature enhances the IPSG flow control by allowing all of the signaling links on an IPSG card to share in the Transactions per Second (TPS) of the card.

Each IPSG linkset is configured for the SLKTPS (also referred to as the Reserved SLKTPS) and the Maximum SLKTPS. The Reserved SLKTPS is the signaling link TPS capacity that is reserved or guaranteed for each link in an IPSG linkset. The Maximum SLKTPS is the maximum TPS capacity that a link is allowed if enough unused capacity is present on the host card. Linksets share available card capacity when presented with a load in excess of the Reserved SLKTPS up to the Maximum SLKTPS value.

During provisioning, the EAGLE verifies that neither the Reserved SLKTPS nor the Maximum SLKTPS exceed 5000 TPS and that the sum of the Reserved SLKTPS for all of the links hosted by an IPSG card does not exceed 5000 TPS for the card.

Operation of IPSG links when IPSG Link Capacity Sharing is used:

- » Links operate independently if their traffic load falls within their respective reserved capacity. The unconsumed portion is available to other links hosted by the same card.
- » If the traffic load exceeds the Reserved SLKTPS, then the link can draw from the card unused TPS. If the traffic load exceeds the Maximum SLKTPS for the card, then the link limits processing at the maximum SLKTPS and may enter congestion.
- » If the traffic load exceeds the Reserved SLKTPS, and enough card capacity originally existed to allow the link to process the load, but the available card capacity changes so that there is not enough available card capacity to process the load, then the link can enter congestion without affecting other links hosted by the card.
- » If multiple links hosted by an IPSG card exceed their Reserved SLKTPS, then the links compete for available capacity on a round-robin basis.

Support of 1M System (SIGTRAN + ATM) TPS

1M System TPS feature increases the allowed System TPS to 1M. This feature adds capacity to users who already have HIPR2 High Rate Mode feature ON and are running with any of the suggested system configuration and traffic pattern.

The maximum allowed System TPS value is 500,000, 750,000 or 1,000,000 depending on the HIPR2 High Rate Mode feature, MFC and 1M System TPS features:

- » If HIPR2 High Rate Mode feature is disabled or OFF, the maximum allowed system TPS will be 500,000.
- » If HIPR2 High Rate Mode feature is ON and 1M System TPS feature is disabled or OFF, the maximum allowed system TPS will be 750,000.
- » If HIPR2 High Rate Mode feature, the MFC feature and the 1M System TPS features are ON, the maximum allowed system TPS will be 1,000,000.

Configurable SCTP Heartbeat Timer

As of release 46.0, the SCTP Heartbeat Timer is configurable on a per association basis. The timer value is configurable from 500 milliseconds to 3000 milliseconds.

GATEWAY FUNCTIONALITY

ANSI/ITU MTP GATEWAY

The EAGLE provides the capability to act as a gateway STP between ANSI and ITU international, and ITU national networks. The EAGLE also continues to switch traffic that does not need to be converted when the origination network is the same network type as the destination network. In order to be able to perform these functions, the EAGLE does the following:

- » Discriminates between MSUs originating from each type of network
- » Converts MSUs to the appropriate format by converting the message transfer part (MTP)
- » Routes MSUs to the correct destinations

Level 3 MSU Discrimination

The EAGLE must determine whether an incoming MSU terminates at the STP or must be routed to another destination. To accomplish the discrimination task, the EAGLE does the following:

- » Compares the network indicator (NI) of an MSU to a database of valid NIs. If the network indicator is not valid, the MSU is discarded.
- » Extracts the network indicator and destination point code (DPC) information from the incoming MSU. If an MSU is transmitted to an ANSI linkset, the network indicator is forced to a binary pattern of "10" before being extracted.
- » Determines whether an incoming MSU terminates at the EAGLE or must be routed to another destination by joining the network indicator and DPC to a list of self point codes. The self point code is a combination of the true point code and capability point code. The capability point code identifies a group of nodes that have similar capabilities.

MSU Routing

MSU routing occurs after MSU discrimination and before MSU conversion (if conversion is necessary). The EAGLE selects an outgoing link on which to transmit the MSU. The MSU formats must be compatible with the linksets that transmit the MSUs.

EAGLEs are typically deployed in mated pairs. The EAGLE has a linkset for each supported network type. The EAGLE should have a unique adjacent point code. The EAGLE supports up to five self point codes - one for ANSI point codes, one for ITU international point codes, one for ITU national point codes, one for ITU National Spare, and one for ITU International Spare.

The figure below shows a sample network with mated gateway STPs. Note that there are different linksets for each network type. In the sample, STP (A) has an ANSI point code (007-001-001), an ITU National point code (09270), and an International point code (5-060-1).

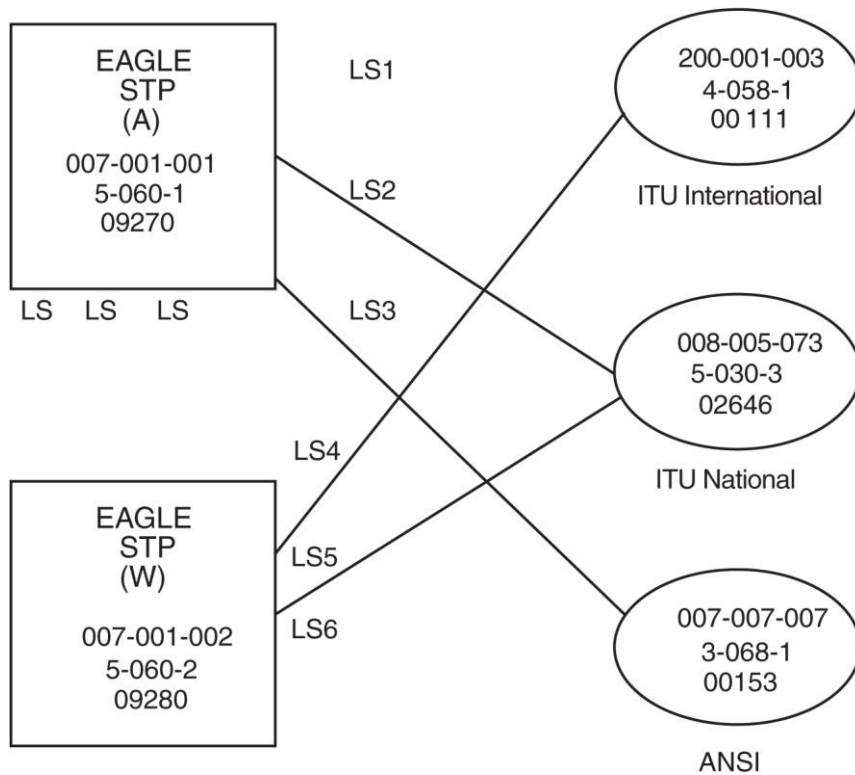


Figure 118: Sample Gateway STP Network

Administering Point Codes

The EAGLE can support multiple network types because each destination can be addressed by a true point code or by a list of alternate point codes. The list of alternate point codes contains from 0 to 2 alternates. The true point codes and alternate point codes are entered in the key table. For example, an ANSI destination could have both a true point code and an alternate point code that point to the same routing translation in the routing table.

Local Link Congestion

When a link is congested, the EAGLE sends ANSI TFCs to the ANSI origination point code (OPC) and ITU TFCs to the ITU origination point code (OPC). The figure below shows both an ANSI and an ITU network sending traffic to a congested link (the type of congested link does not matter). When an ANSI node is the source of the traffic to the congested link, the TFC contains a status. When an ITU node is the source of the traffic, the TFC does not contain a status.

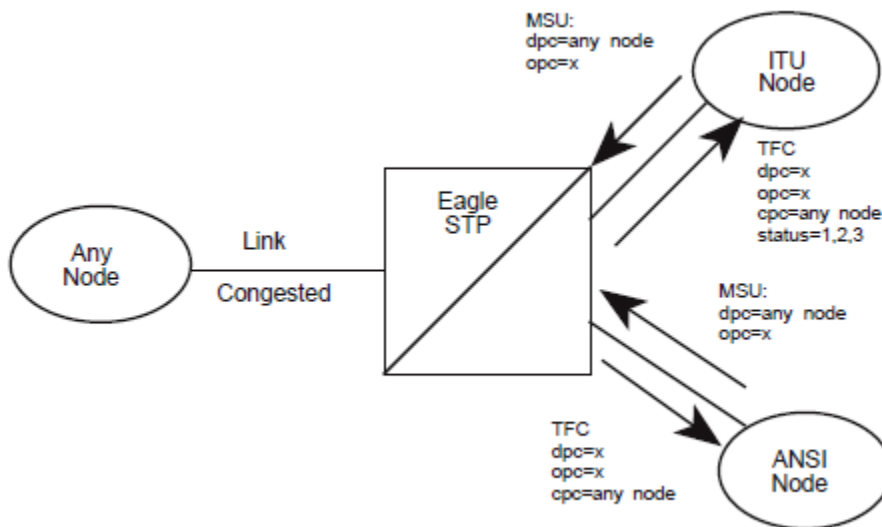


Figure 119: Traffic to and from a Congested Link

All links in the system operate with four levels of congestion. If the congestion level is "0", there is no congestion, the EAGLE does not transmit TFCs, and no MSUs are discarded. At level 3 (indicating a maximum level of congestion), the EAGLE transmits TFCs and discards MSUs.

Whenever the congestion onset status is above congestion onset level 1 and has not abated below congestion abatement level 1, the EAGLE generates a TFC. Whenever the congestion discard status is above discard level 1 and has not abated below discard level 1, the EAGLE discards the MSU per the figure below.

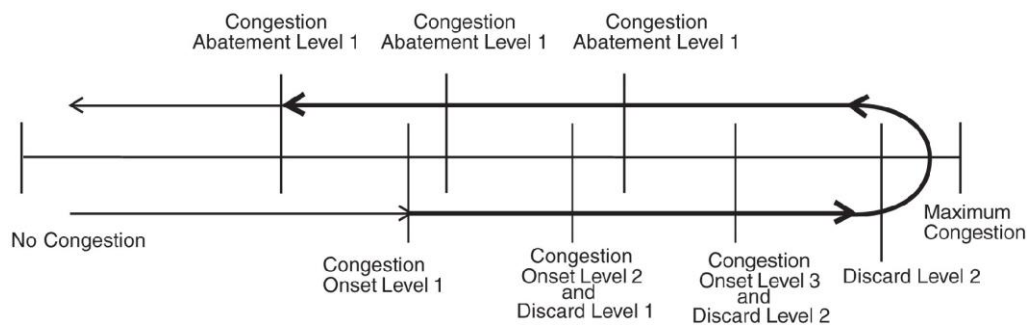


Figure 120: Congestion Levels

Remote Link Congestion

The table Remote Congestion Response shows the EAGLE response to remote congestion indicators.

Table 24: Remote Congestion Response

Event	EAGLE Response
-------	----------------

EAGLE receives an ANSI TFC	When the EAGLE receives an ANSI TFC, the routing table is modified to discard lower priority MSUs being routed to the concerned point code. The TFC contains the congestion status of the concerned point code. The routeset congestion test mechanism is used to abate the congestion.
EAGLE receives an ITU TFC	When the EAGLE receives an ITU TFC, the routing table is modified to discard the lower priority MSUs being routed to the concerned point code. The TFC does not contain the congestion status of the concerned point code. Instead, the congestion status is user-configurable using the <i>chg-isup-stp:status</i> command. Once the routeset is identified as congested, a timer is used to abate the congestion. The timer is similar to the ANSI routeset congestion test mechanism.
EAGLE receives an ANSI RCT	There is no change in the EAGLE response when the EAGLE receives ANSI routeset congestion test messages.
EAGLE receives an ITU RCT	The H0H1 message codes are not contained in the ITU environment. These codes generate an invalid H0H1 MRN, and the message is discarded. This has no impact on the ITU network because the EAGLE uses a timer to abate congestion and does not rely on a reply to the RCT message.

X.25/SS7 GATEWAY FEATURE

As of Release 42.0, X25 Gateway is no longer supported.

DATA TRANSPORT ACCESS

The Data Transport Access (DTA) feature intercepts MSUs that need further application processing and redirects the MSUs to an external processor for modification. The MSUs are selected for redirection by the gateway screening process, based on predefined OPC and DPC criteria. The external processor sends the processed MSU back to the EAGLE to be routed to the final destination. DTA is supported for ANSI and ITU destinations.

Two EAGLE features are required for the DTA feature to operate. The following features provide services to support the DTA feature:

- » Gateway screening
- » Global title translation (if SCCP subsystem management is to be supported)

Several applications would benefit from the Data Transport Access (DTA) feature. MSUs containing SCCP and proprietary data can be sent through the network to customer-specific databases. These MSUs may need additional processing, however, before being routed to their final destination.

The key attributes of the DTA feature are as follows:

- » Redirected MSUs are always encapsulated with the SCCP header
- » The redirected MSU is MTP routed using the Redirect DPC if the provisioned Redirect DPC is not the EAGLE point code.
- » The redirected MSU is GTT routed to the EAGLE SCCP subsystem if the provisioned Redirect DPC is the EAGLE point code.
- » If the redirect destination is unavailable or congested, DTA will send the message to the original destination without the DTA wrapper.

GWS Redirect Table

There is one table, the GWS Redirect table, in the EAGLE which governs the behavior of the DTA feature. The parameters of this table are as follows:

- » DPC - Determines the node that the MSU will be redirected to. If the MSU is to be redirected to an SCP, the DPC should be the EAGLE point code. Only one DPC is allowed to be provisioned. Currently only an ANSI DPC can be specified
- » GTA - Global Title Address that will be used in the SCCP header. Ignored if the DPC value is not the EAGLE point code.
- » SSN - Sub-System Number that will be used in the SCCP header. Ignored if the DPC value is not the EAGLE point code. SSN is use to let the destination know what type of network the encapsulated MSU is. Table 8 2 DTA CgPA SSN Mapping Table shows the SSN mappings.

Table 25: DTA CgPA SSN Mapping Table

Payload Type	CgPA SSN	Redirect MSU OPC
ANSI	0	Original OPC
ITU-I/ITU-N	250	EAGLE ANSI True PC
ITU-N 24 bit PC	251	EAGLE ANSI True PC

- » Routing Indicator- Route by GTT or SSN. Ignored if the DPC value is not the EAGLE point code. Ignored if the DPC value is not the EAGLE point code.
- » TT-Translation Type that will be used in the SCCP header. Ignored if the DPC value is not the EAGLE point code.
- » Enabled-On/Off toggle to turn the redirect function On and Off.

MSU Encapsulation

The redirect function encapsulates the original MSU in the SCCP data part of a new MSU.

The DPC and CDPA RI, SS, TT, Address fields, of the new MSU, are set according to the parameters that were entered in the GWS Redirect Table. There is no provision to use only a subset of the data in the GWS redirect table when encapsulating an MSU.

When the original MSU is too large to be encapsulated, it is discarded and an informational message is generated.

The figure below shows how the original MSU is encapsulated by the DTA feature.

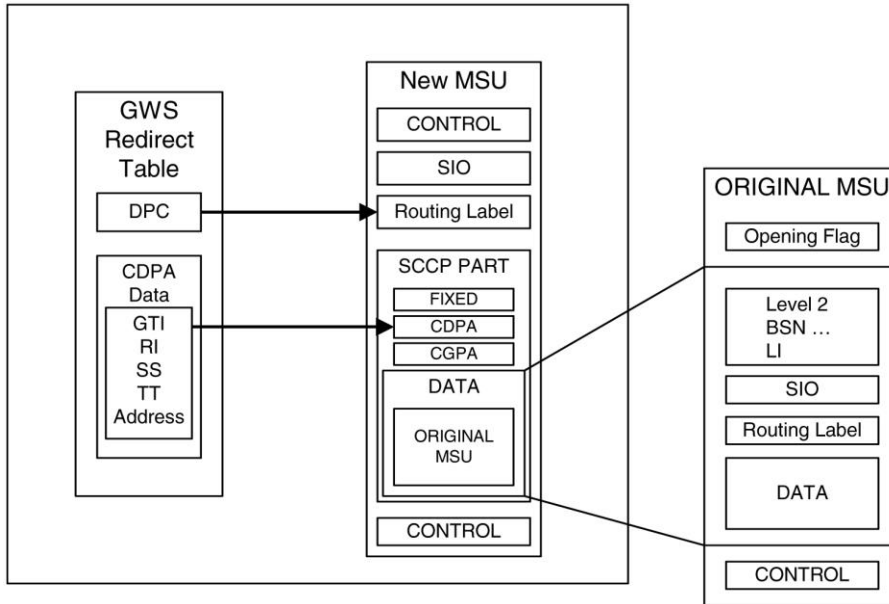


Figure 121: MSU Encapsulation

DTA Message Flow

The figure below shows the message flow of the DTA feature and is described below:

1. An MSU arrives and passes Gateway Screening. If the DTA redirect function is provisioned for that screening function, the EAGLE encapsulates the received MSU.
2. If the DPC provisioned in the redirect table is not the EAGLE point code, the MSU is MTP routed via the routing table and the encapsulated MSU is routed. The receiving node must be able to handle processing of the encapsulated MSU. If the redirect table has the EAGLE point code provisioned as the DPC, the encapsulated MSU is sent to the SCCP card where a Global Title is performed using the SCCP data that is contained in the encapsulated portion of the MSU (i/e. based on the data in redirect table).
3. The post GTT'd MSU is then routed to an external processor via normal routing methods.
4. The MSU arrives at the external processor, where the MSU is processed for a customized application. The host can identify the originator of the data by examining the MTP header included in the encapsulation.
5. Once the external processor has processed the user data and removed the encapsulation, it sends the MSU back to the EAGLE.
6. At the EAGLE, the MSU is routed to its final destination either in the SS7 network or in the X.25 network. The external processor determines the routing for the MSU, providing it in the routing label of the MTP portion of the MSU and in the SCCP called party address.
7. If the provisioned Redirect DPC was not the EAGLE point code, the encapsulated MSU is sent to the provisioned Redirect DPC. If the provisioned Redirect DPC was the EAGLE point code, the unencapsulated post-processed MSU is sent to the original DPC of the original MSU.

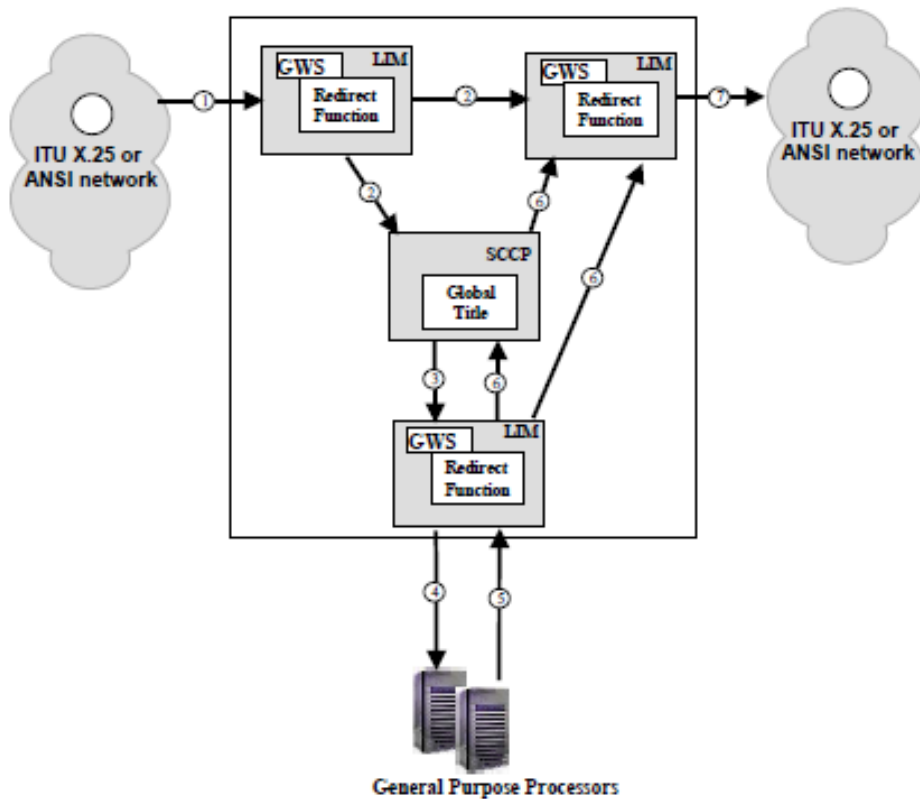


Figure 122: DTA Message Flow

MEASUREMENTS

GENERAL

The EAGLE provides a wide variety of measurements and measurement collection methods. The EAGLE provides both standard (basic) STP measurements and advanced measurements capability via various interfaces.


- » Basic Measurement Collection - provides required measurement collection for an STP per GR-82-CORE
- » Advanced Measurement Collection - allows customers to collect basic measurements over a variety of interfaces or perform advanced measurement operations by analyzing in detail the traffic switched by the EAGLE.

BASIC MEASUREMENT COLLECTION

This section describes the basic STP measurements generated by the EAGLE. Measurements provide operations and maintenance personnel with network performance and STP performance data in accordance with Telcordia GR-82-CORE

There are eleven types of basic measurements reports generated by the EAGLE, using the rept-meas or the rept-ftp-meas command:

- » STP system totals (SYSTOT)

- 
- » Component measurements (COMP)
 - » Daily maintenance measurements (MTCD)
 - » Day-to-hour maintenance measurements (MTCDTH)
 - » Measurement reports that apply to the LNP feature (MTCH)
 - » Network management (NM)
 - » Daily availability (AVLD)
 - » Day-to-hour availability (AVLDTH)
 - » Availability (AVL)
 - » Gateway (GTWY)
 - » Record Base (RBASE)

Report Parameters

Reports are available for the following entities:

- » Link
- » Linkset
- » STP
- » Translation Type (TT)
- » STPLAN
- » Origni
- » Origninc
- » Lsdestni
- » Lsorigni
- » Application (LNP, HLR Router, INP etc.)

There are four accessible periods for which measurements can be reported:

1. Last is used to access the previous collection interval.
2. Specific is used to access a specific interval (one of the previous 48 half-hour intervals).
3. Active is used to access measurements for the current collection interval.
4. All is used to access measurements for all collection intervals retained.

Measurements can also be backed up to a removable cartridge for storage. LNP measurements are placed in a File Transfer Area (FTA) for transport off the EAGLE via Kermit session or can be sent in comma delimited format via FTP.

SIGTRAN Measurements

The SIGTRAN Measurements (SIGTRAN) feature allows measurements for the IPGWx and IPLIMx cards to be obtained using the EAGLE commands or through EAGLE measurement collection and reporting mechanisms. The SIGTRAN feature also obtains measurements for the IPSG cards.

On-demand measurement reports can be obtained through the User Interface or the Measurements Platform (see description in **ADVANCED MEASUREMENTS**).

Scheduled measurement reports must be obtained through the Measurements Platform.

The SIGTRAN feature provides measurement capabilities for the following protocols:

- » UA

The UA protocol consists of a combination of the M3UA and SUA protocols. UA measurements are collected for IPGWx (SUA and M3UA) and IPSP (M3UA only) cards per association (ASSOC) on the application server (AS).

Measurements for UA messages that are received without a routing context or with multiple routing context values are pegged to the default AS value and the appropriate ASSOC. The RXMLRCMS register is used to indicate the number of messages received with multiple routing context values. This register is always pegged using the default AS value. The AS value can also be set to the default AS for all UA data.

All UA data for IPSP cards is pegged against the default AS.

» SCTP

SCTP measurements are collected for IPGWx, IPLIMx, and IPSP cards per CARD and ASSOC.

» M2PA

M2PA measurements are collected on IPLIMx and IPSP cards per LINK.

Link and Linkset Classes

The following new link classes are used to provide LINK measurements for the UA and M2PA protocols:

- » IPVHSL: M2PA links (IPLIMx and IPSP cards)
- » IPVLGW: M3UA and SUA links (IPGWx cards)
- » IPVL: M3UA links (IPSP cards)

These new link classes apply to the existing COMP-LINK, MTCD-LINK, and MTCDTH-LINK reports. Linkset class can be derived from the classes of the individual links contained within the linkset. Any linkset that contains IPVHSL class links (with or without classes of links) has linkset class IPVHSL. A linkset that contains IPVL or IPVLGW class links has linkset class IPVL. The additional linkset classes impact the register content of the COMP-LINKSET report.

The IPVL link class uses existing registers. New registers are provided for the IPVSHL link class. These registers are shown in the table below.

Table 26: IPVSHL Linkset Registers

Register Data	Description
ECLNKCB	Number of times the link performed ChangeBack procedures
ECLNKEXO	Number of times the link performed Extended ChangeOver
M2PLKNIS	Duration the link was not in the in-service state at the M2PA layer (in seconds)
M2PUDMRC	Number of M2PA UDMs received
M2PUDMTR	Number of M2PA User Data Messages transmitted
M2PUDOCR	Number of M2PA User Data Message octets received.
M2PUDOCT	Number of M2PA User Data Message octets transmitted

ADVANCED MEASUREMENTS

The EAGLE can provide a wide variety of message measurement capabilities. These capabilities include the following features:

- » Measurements Platform- provides comma delimited measurement data over TCP/IP.
- » IAS - provides integrated monitoring of links and high end application functions.
- » STPLAN - allows copying of MSUs to an off-board processor.
- » GR-310/778 (SEAS) - provides basic STP measurements over an X.25-serial interface.

MEASUREMENTS PLATFORM

The Measurements Platform supports the measurement peg-count-data growth path for systems beyond 700 links by providing a dedicated processor for collecting and reporting core STP, LNP, INP, HLR Router and MNP Measurements data. The Measurements Platform is required for customers with more than 700 links but can also be used by all customers who desire comma-delimited measurement data over secure TCP/IP. For more information on IP security over the Measurements Platform connection between the EAGLE and the remote FTP server, see EAGLE Security.

The Measurements Platform consists of multiple MCPM (Measurement Collection and Polling Module) cards in a primary/secondary configuration, in which a single primary MCPM performs all collection and reporting functions. The secondary MCPM card serves as backup for the primary MCPM. The figure below presents a functional diagram of the Measurements Platform and its interfaces to the customer's network.

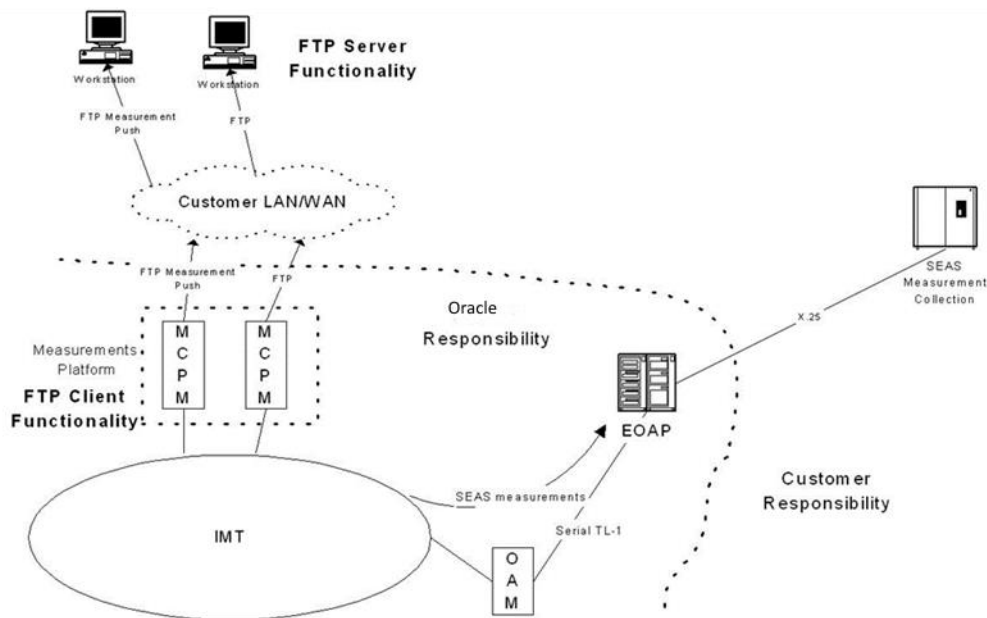


Figure 123: Measurements Platform Functional Diagram

The Measurements Platform is designed for future support of an N+1 architecture, in which multiple MCPM cards can be provisioned to share the measurement tasks. Currently, however, all secondary cards provide a redundant backup to the primary card. Secondary MCPM cards do not provide any collection performance benefit. Thus, there is no functional advantage to installing more than two MCPM cards. The primary MCPM monitors the status of all secondary MCPM cards. If the primary MCPM fails before or during collection, the secondary MCPM card assumes the primary role, and begins/continues collection. GR310/778 measurements are still supported, as shown in the figure above.

The primary benefit of the Measurements Platform is derived from the implementation of a dedicated processor for the collection of measurements. This provides increased bandwidth and performance compared with the measurements collection engine that currently resides in the OAM.

The Measurements Platform assumes the collection duties from the OAM and stores the collected data in MCPM RAM. Following collection, comma delimited scheduled reports are automatically generated and transferred to the customer's FTP server via the secure FTP interface. The reports are always transferred to the configured Primary FTP Server or, if the Primary server is down, to the configured Secondary FTP Server. The filename of the report contains the CLLI name of the EAGLE to easily identify the source of the data.



Measurement collection periods of 15 minute, 30 minute, hourly, and daily are provided.

On-demand report requests are also generated and transferred to the customer's FTP server, or output to the terminal. A command to enable the user to transfer missed scheduled reports is also available. Its purpose is to enable the customer to recover any scheduled reports within the last 24 hours that may not have transferred to the FTP Server.

Measurement Platform Limitations

Hard disk retention of measurement data is provided by the FTP server(s). Measurements data is stored locally in RAM on the MCPM cards, thus a loss of power will remove the measurements from that particular MCPM card. In the current Measurements Platform architecture, if a MCPM card losses power, its measurements data is lost. This is mitigated by hard disk retention provided by the FTP server(s) and the failover capabilities to the standby MCPM(s). For example, the data on a MCPM card is lost when it is removed from its slot, but as soon as the card is replaced, the data stored in the Data RAM Disk section of the Primary card is loaded to the newly inserted card.

E5-OAM Integrated Measurements

The E5-OAM Integrated Measurements (Integrated Measurements) feature allows the Measurements subsystem on the E5-OAM MASP to provide full support for the collection and reporting for all collectible measurement entities for nodes configured with up to 1200 links. Systems with more than 1200 links must install the Measurements Control Platform (MCP) for full measurement support.

The Integrated Measurements feature obsoletes the use of the File Transfer Area (FTA) for measurements, and replaces the FTA functionality with FTP functionality. The E5-OAM/IP Ethernet Support enhancement is used to provide Ethernet support for FTP.

This feature requires the Measurements Subsystem to transition to the Integrated Measurements. The transition is performed by provisioning the oamhcmeas option in the chg-measopts command. Provisioning this parameter also turns on the Integrated Measurements collection function.

Note: The Integrated Measurements collection function cannot be turned off after it has been turned on.

If the MCP is enabled prior to the transition, then the transition sequence transfers all historical measurements data from the MCP to the OAM. The MCP does not collect and report measurements during transition.

After the transition is complete, the OAM takes control of the Measurements Subsystem and is responsible for collection and reporting. The MCPM cards are set to IS-ANR - Restricted state, and the MCP is turned off.

STPLAN FEATURE

The STPLAN feature allows the EAGLE to support a TCP/IP connection from any interface shelf to external hosts. The STPLAN application allows the user to selectively copy outbound messages to a remote node for further processing. The messages that are copied to the external host are actually selected for copying on the inbound linkset by the Gateway Screening feature. The messages that pass the screening criteria set for that linkset are processed by the system, and are copied prior to being transmitted on the outbound link. The connection to the external host consists of several Ethernet cards using the TCP/IP protocol to communicate to an external processing device running software that receives and processes the messages. Each Ethernet card supports a single remote destination node. Each Ethernet card may also support a single default router.

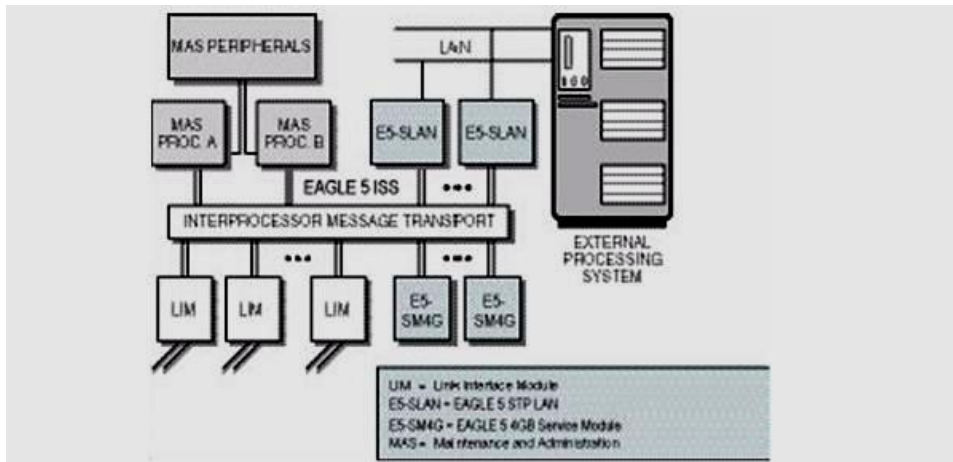


Figure 124: STPLAN Functional Diagram

The STPLAN feature is designed to provide an open system architecture, allowing third parties to design applications that can be attached as adjuncts to the EAGLE.

This feature requires an Ethernet card to provide an Ethernet interface at the interface shelf backplane and the processing power required to support message encapsulation and TCP/IP support.

The user may attach any compatible host system. The host system must be using TCP/IP as the higher layer protocol and must support 10/100 Base T Ethernet as the transmission method.

Messages are sent to the Ethernet card via Gateway Screening on the inbound LIM card. A flag is set on the inbound LIM card but the actual copy function occurs on the outbound LIM card. The EAGLE software on the Ethernet card receives SS7 MSUs from the LIMs and service module cards via Gateway Screening and copies those MSUs into memory on the Ethernet card. The copied MSU is encapsulated and transmitted using TCP/IP packets and Ethernet to the host computer. The host computer is responsible for reassembling the original message and processing the data.

The entire MSU is copied, including the MTP, which allows the host application to process the entire message. Total octet counts, including MTP level 2 and level 3, can be tallied and used for a variety of external measurements.

The IP addresses of adjacent hosts are entered into the EAGLE by using the EAGLE database administration commands.

Addendum

Go Forward Product Descriptions and Mapping to Legacy Part Numbers

Go Forward product descriptions are listed below in addition to the legacy part number composition. Please note, the Go Forward products are subject to prerequisites as indicated in the price list supplements and license user guides. The Go Forward product model shows the software licenses available for sale and reflects our current sales structure. If you possess legacy licenses, the following information shows you how those licenses are grouped in our current sales structure.

1. L99410 – Oracle Communications EAGLE (base fee) – ISO – Per Node: This product provides access to base Oracle Communications EAGLE functionality. This includes the basic operations, administration and maintenance features along with some basic routing and STP migration features. The legacy part numbers below are included in this Go Forward part number.

Table 27: Oracle Communications EAGLE (base-fee)

Part Number	Description
971-4221-01	Increased Linkset Capacity EAGLE
971-3020-01	Prevention Cyclic Retransmission Kernel EAGLE
971-4116-01	EAGLE Module Multiple Point Code Per 4 PCS
893-0187-02	EAGLE 11 To 20 Proxy Point Codes
893-0121-01	EAGLE 15 Minute Measurements
893-0187-03	EAGLE 21 To 30 Proxy Point Codes
971-4120-01	EAGLE 4001 To 5000 Routes
893-0356-01	EAGLE 41.1 Or Later GWS Stop Action For MTP Routed Messages
971-4013-01	EAGLE-8 BIT Sequencing Assurance
893-0198-01	EAGLE 6-Way Loadsharing on Routesets
893-0218-01	EAGLE Advanced Global Title Modification
893-0349-01	EAGLE Analyzed Info Query No DB
971-3019-01	EAGLE ANSI/ITU Gateway
893-0120-01	EAGLE ANSI/ITU SCCP Conversion
893-0176-01	EAGLE Auto Point Code Recovery
971-3021-01	EAGLE Base Software
971-3023-01	EAGLE Cluster Routing & Management Diversity
893-0058-01	EAGLE Command Class Management
971-1034-01	EAGLE DS0 Lookback
971-0253-01	EAGLE E5-OAM Card Set
893-0389-01	EAGLE E5-OAM Integrated Gateway Loading Services Per Node
893-0373-01	EAGLE E5-OAM Integrated Measurements Platform Per Node
893-0404-01	EAGLE E5-OAM SNMP Feed Per Node

971-4003-01	EAGLE Gateway Screening
971-4002-01	EAGLE Global Title Translation
893-0185-01	EAGLE Hex Digit Support For GTT
971-4061-01	EAGLE High Speed Master Clocking
893-0057-01	EAGLE IP User Interface
971-0092-01	EAGLE ITU Base Software
971-4119-01	EAGLE ITU Duplicate Point Code
893-0136-01	EAGLE ITU NATL/INTL Spare Point Code
971-4107-01	EAGLE ITU SLS
893-0184-01	EAGLE Large MSU Support For IP Signaling
893-0059-01	EAGLE Large Sys 1201 To 1500 Links
893-0059-10	EAGLE Large Sys 1501 To 2000 Links
893-0059-11	EAGLE Large SYS 2001 To 2800 Links
971-4143-01	EAGLE Large SYS 501 To 1200 Links
971-1035-01	EAGLE Link Fault Sectionalization
971-4198-01	EAGLE Measurements Platform
893-0197-01	EAGLE Multiple Linksets To Single Adjacent Point Code
971-4105-01	EAGLE Nested Cluster Routing
971-4125-01	EAGLE Network Routing
971-0109-[01, 02, 04, 05, -06, 07]	EAGLE Nodal Software Update (For releases 40.1, 41.x 42.x 43.x 44.x 45.x)
893-0393-01	EAGLE NPP Single WildCards UNLTD In 1ST 6 Positions
893-4000-01	EAGLE OA&M IP Security Enhancements
893-0372-04	EAGLE POINT CODE AND CIC TRANSLATION 100
893-0372-08	EAGLE POINT CODE AND CIC TRANSLATION 1000
893-0372-05	EAGLE POINT CODE AND CIC TRANSLATION 150
893-0372-06	EAGLE POINT CODE AND CIC TRANSLATION 200
893-0372-01	EAGLE POINT CODE AND CIC TRANSLATION 25
893-0372-07	EAGLE POINT CODE AND CIC TRANSLATION 250
893-0372-02	EAGLE POINT CODE AND CIC TRANSLATION 50
893-0372-03	EAGLE POINT CODE AND CIC TRANSLATION 75
971-4216-01	EAGLE Random SLS Generation
893-0165-01	EAGLE SCCP Loop Detection
893-0188-01	EAGLE SEAS Over IP Feature
971-0139-01	EAGLE SEAS Over IP
971-1037-01	EAGLE SEAS

893-0265-01	EAGLE SLS Bit Rotation On Incoming Linkset
893-0091-01	EAGLE System Security
893-0071-01	EAGLE System Software
971-0582-01	EAGLE TTC Base Software Per Node
893-0408-01	EAGLE TTC/ITU SCCP Conversion Per Node
893-0187-01	EAGLE UP To 10 Proxy Point Codes
893-0353-01	EAGLE XUDT UDT Conversion
893-0181-01	Enhanced Loopback Detection EAGLE
971-0139-02	EAGLE 37.5 Or Later License SEAS Over IP Upgrade
971-0377-01	EAGLE 39.2 Or Later License Network Indicator Mapping
971-4247-01	Network Surveillance Enhancements EAGLE

2. L99411 Oracle Communications EAGLE – ISO – per 250K Transactions per Second Metric: This product determines the maximum number of transaction per second (TPS) allowed per Oracle Communications EAGLE node. A minimum quantity of one is required per node. Depending on the quantity purchased, the following legacy part numbers may be activated.

Table 28: Oracle Communications EAGLE

Part Number	Description
893-0407-01	EAGLE 751K To 1M TPS Per Node
971-0252-01	EAGLE HIPR2 High Rate Mode Per HIPR2
893-0201-01	EAGLE HIPR2 High Rate Mode

3. L99412 Oracle Communications EAGLE LNP Advanced Service Module Enabler – ISO – per Card: This product enables the Oracle Communications EAGLE LNP solution and is required for each OC EAGLE Service Module 8 GB B Card utilized. This enables the maximum TPS for the card. The following list of legacy part numbers is included.

Table 29: Oracle Communications EAGLE LNP Advanced Service Module Enabler

Part Number	Description
971-0160-08	EAGLE 13,600 ANSI Database TPS Per E5-SM
971-0160-09	EAGLE 10,000 To 13,600 ANSI Database TPS Per E5-SM Upgrade
971-0160-06	EAGLE 10,000 ANSI Database TPS Per E5-SM
971-0160-07	EAGLE 6,800 To 10,000 ANSI Database TPS Per E5-SM Upgrade
971-0160-05	EAGLE 41.1 Or Later License 5,000 To 6,800 ANSI DB Transactions Per Second Per E5-SM Upgrade
971-0160-04	EAGLE 41.1 Or Later License 6,800 ANSI DB Transactions Per Second Per E5-SM
971-0160-03	EAGLE ANSI DB Transaction Upgrade To Maximum Transactions License Per E5-SM

971-0160-02	EAGLE Restricted ANSI DB Transactions License Per E5-SM
971-0160-01	EAGLE Version Independent License DB Transaction ANSI Per E5-SM

- L99413 Oracle Communications EAGLE LNP – ISO – per Node Metric: This product enables the Local Number Portability (LNP) features which must run on the EAGLE node and work in concert with the LNP functionality which execute on a separate LNP server hosted on the Oracle Communications EAGLE Application B Card. The following list of legacy part numbers is included.

Table 30: Oracle Communications EAGLE LNP

Part Number	Description
971-4064-01	POD Feature Module Number Pooling EDR EAGLE
893-0405-01	EAGLE Dual EXAP Support Per Node
971-0495-01	EAGLE GTT Post LNP Message Relay
971-0494-01	EAGLE GTT Pre LNP Message Relay
971-3025-01	EAGLE LNP Base Software
971-4032-01	EAGLE LNP Measurements
971-4117-01	EAGLE LNP Number Pooling/EDR
971-3030-01	EAGLE LNP Wireless Software
971-4087-01	EAGLE PCS Support
893-0406-01	EAGLE SIP Number Portability Per Node
971-0342-01	EAGLE 40.0 Or Later License ITU TCAP LRN Query
893-0263-01	EAGLE 40.0 Or Later License ACG For ITU TCAP LRN Query
971-0067-01	Enhanced LNP Architecture DSM Software EAGLE

- L99414 Oracle Communications EAGLE Advanced Service Module Enabler – ISO – per Card: This product enables any Oracle Communications EAGLE Application Processor based features which are processed on the EAGLE Service Module cards. The legacy part numbers listed below are included.

Table 31: Oracle Communications EAGLE Advanced Service Module Enabler

Part Number	Description
971-0161-10	EAGLE_13,600 ITU DATABASE TPS PER E5-SM_RTU_INVOICE ONLY
971-0161-11	EAGLE_10,000 TO 13,600 ITU DATABASE TPS PER E5-SM UPGRADE_RTU_INVOICE ONLY
971-0161-08	EAGLE_10,000 ITU DATABASE TPS PER E5-SM_RTU_INVOICE ONLY
971-0161-09	EAGLE_6,800 TO 10,000 ITU DATABASE TPS PER E5-SM UPGRADE_RTU_INVOICE ONLY

971-0366-01	EAGLE_E.164 BLACKLIST SUPPORT FOR 1000 ENTRIES_RTU_INVOICE ONLY
971-0161-07	RTU_EAGLE_41.1 OR LATER_6,800 ITU DB TRANSACTIONS PER SECOND_PER E5-SM IN >2000 LINK NODE_INVOICE ONLY
971-0161-06	RTU_EAGLE_41.1 OR LATER_LICENSE 3,125 TO 6,800 ITU DB TRANSACTIONS PER SECOND PER E5-SM UPGRADE_INVOICE ONLY
971-0161-05	RTU_EAGLE_41.1 OR LATER_LICENSE 6,800 ITU DB TRANSACTIONS PER SECOND PER E5-SM_INVOICE ONLY
971-0161-03	RTU_EAGLE_ITU DB TRANSACTION UPGRADE TO MAXIMUM TRANSACTIONS_LICENSE_ PER E5-SM
971-0161-02	RTU_EAGLE_RESTRICTED ITU DB TRANSACTIONS _LICENSE_ PER E5-SM

6. L99415 Oracle Communications EAGLE Mobile Number Portability – ISO – per Node: This product enables the Mobile Number Portability (MNP) features at the node level. The following legacy part numbers are included.

Table 32: Oracle Communications EAGLE Mobile Number Portability

Part Number	Description
Part Number	Description
893-0350-01	EAGLE 41.1 Or Later Info Analyzed Relay ASD
893-0178-01	EAGLE ANSI-41 INP Query
893-0166-01	EAGLE A-Port/ANSI-41 Mobile Number Portability
893-0221-01	EAGLE ATI Number Portability Query
893-0398-01	EAGLE EPAP 240M Support (120M DN + 120M IMSI) Per Node
971-0592-01	EAGLE EPAP PDBI Measurements Per Node
971-0505-01	EAGLE Mobile Number Portability DEL CC For SP Enhancement
893-0172-01	EAGLE Mobile Number Portability
893-0177-01	EAGLE Mobile Number Portability SRI Query For Prepaid
893-0140-01	EAGLE GSM MAP SRI Redirect To Serving HLR
893-0342-01	EAGLE Info Analyzed Relay Base
893-0261-01	EAGLE Info Analyzed Relay Number Portability
971-0395-01	EAGLE INP Additional Application
893-0285-01	EAGLE INP Circular Route Prevention
893-0173-01	EAGLE IS41 GSM Migration
893-0385-01	EAGLE LOCREQ Query Response
893-0070-01	EAGLE Mobile Number Portability Circular Route Prevention
893-0093-01	EAGLE Portability Check For Mobile Originated SMS
893-0244-01	EAGLE Proprietary ATI Number Portability Query

893-0343-01	EAGLE Service Portability
893-0406-01	EAGLE SIP Number Portability Per Node
893-0379-01	EAGLE S-Port Subscriber Differentiation
893-0167-01	EAGLE Voicemail Router
971-0359-01	EAGLE 41.1 Or Later License GRN For NP With INP ATI Mobile Number Portability
893-0179-01	EAGLE IDP Number Portability (INP)

7. L99416 Oracle Communications EAGLE SS7 Firewall – ISO – per Node Metric: This product enables a set of security and fraud detection features which allow for the screening, detection and analysis of suspect message parameters as well as the execution of various consequential actions. The following list of legacy part numbers is included.

Table 33: Oracle Communications EAGLE SS7 Firewall

Part Number	Description
Part Number	Description
971-0276-01	EAGLE EGMS Between ITUI/ITUN
971-0351-01	EAGLE EGMS Non-Segmented XUDT Support
971-0340-01	EAGLE EGMS RI GT For Outgoing Messages
971-0131-01	EAGLE EGMS TC Continue And End
893-0124-01	EAGLE Enhanced GSM MAP Screening
893-0132-01	EAGLE GSM MAP Screening
893-0275-01	EAGLE GTT Discard
893-0135-01	EAGLE MTP ROUTED GSM MAP Screening

8. L100139 Oracle Communications EAGLE Suspicious Call Identification – ISO – per Node: This product allows operators to detect and screen abusive, spam and fraudulent traffic. Enables selective copy and forward of ISUP messages based on configurable trigger parameters of the ISUP message.
9. L100140 Oracle Communications EAGLE Service Actions Portability and Flexibility – ISO – per Node: This product provides enhanced service selection capabilities for EAGLE Mobile Number Portability, HLR Router and SMS routing.
10. L100939 Oracle Communications EAGLE Intra Network Number Portability – ISO – per Node: This product allows enhancement to Mobile Number Portability allowing operators to route calls differently based on the origin of the call. For example, allows Indian operators to expand Regional Number Portability to National Number Portability. This feature can also serve 3G 4G migration scenarios.
11. L99417 Oracle Communications EAGLE HLR Router – ISO – per Node: This product is applicable to any ITU or ANSI mobile network. It optimizes the use of subscriber numbers and number ranges by providing a logical link between any DN and any IMSI and also between any subscriber number and any Home

Location Register (HLR). This feature allows subscribers to be easily moved from one HLR to another. The following legacy part numbers are included.

Table 34: Oracle Communications EAGLE HLR Router

Part Number	Description
Part Number	Description
893-0217-01	EAGLE HLR Router MAP Layer Routing
893-0219-01	EAGLE HLR Router
971-0453-01	EAGLE MAP Layer Routing Per 5 OPCODES

12. L99418 Oracle Communications EAGLE Equipment Identity Register – ISO – per Node: This product can prevent the use of stolen handsets by allowing the network operator to compare the handset's IMEI and/or IMSI to the blacklist of stolen handsets. If a match is encountered, the operator can prevent the handset from being registered on the network, thus rendering it useless. The following legacy part numbers are included.

Table 35: Oracle Communications EAGLE Equipment Identity Register

Part Number	Description
Part Number	Description
893-0123-01	EAGLE Equipment Identity Register
893-0424-01	EAGLE Diameter S13 Interface For EIR

13. L99419 Oracle Communications EAGLE Global Title Translation Routing – ISO – per Node: The SCCP Global Title Translations (GTT) feature uses the signaling connection control part (SCCP) to translate addresses (Global Titles) to final and / or intermediate routing destinations. The following legacy part numbers are included.

Table 36: Oracle Communications EAGLE Global Title Translation Routing

Part Number	Description
Part Number	Description
971-4077-01	GTT Measurements EAGLE
893-0077-01	EAGLE 1025 TO 2000 MAP Table Entries
893-0248-01	EAGLE 16 Different GTT Lengths In VGTT
893-0077-10	EAGLE 2001 TO 3000 MAP Table Entries
893-0064-01	EAGLE 5001 To 6000 Routes
893-0064-02	EAGLE 6001 To 7000 Routes
893-0064-03	EAGLE 7001 To 8000 Routes
893-0064-05	EAGLE 8001 To 10000 Routes

893-0218-03	EAGLE Advanced GT Modification, Calling Party Upgrade
893-0174-01	EAGLE Application Support For MTP Routed Messages
893-0154-01	EAGLE Flexible GTT Loadsharing
893-0061-10	EAGLE GTT >400K TO 1 Million Entries
893-0061-01	EAGLE GTT 270K TO 400K Entries
971-0425-01	EAGLE GTT After MNP For SRI SM
893-0276-01	EAGLE GTT Duplicate
893-0375-01	EAGLE GTT Forward
893-0274-01	EAGLE GTT Loadsharing With Alternate Routing Indicator
971-4259-01	EAGLE Increase GTT Entries To 200K Per TT
893-0069-01	EAGLE Intermediate Global Title Loadsharing
893-0171-01	EAGLE Transaction Based GTT Loadsharing
893-0170-01	EAGLE Weighted GTT Loadsharing

14. L99420 Oracle Communications EAGLE Triggerless ISUP Framework Routing – ISO – per Node: TIF (Triggerless ISUP Framework) provides an overall structure for ISUP traffic related features. It allows the EAGLE to intercept messages and apply special processing to them. For example, number portability, number substitution and blacklisting for called and calling party number. The following legacy part numbers are included.

Table 37: Oracle Communications EAGLE Triggerless ISUP Framework Routing

Part Number	Description
Part Number	Description
893-0245-01	EAGLE TIF ASD
971-0338-01	EAGLE TIF Base
893-0255-01	EAGLE TIF GRN
971-0337-01	EAGLE TIF IAM/SAM Split
971-0336-01	EAGLE TIF NP CRP
893-0189-01	EAGLE TIF Number Portability
893-0225-01	EAGLE TIF Number Substitution
893-0377-01	EAGLE TIF RANGE CGPN Blacklisting
893-0402-01	EAGLE TIF Selective Screening Per Node
893-0240-01	EAGLE TIF Simple Number Substitution
893-0376-01	EAGLE TIF SUBSCR CGPN Blacklisting
893-0222-01	EAGLE 39.2 Or Later License TIF SCS FWD

15. L99421 Oracle Communications EAGLE Origin Based Routing – ISO – per Node: The Origin-based MTP & SCCP Routing feature allows greater flexibility and control over the SS7 message routing. This feature allows selective routing based on a combination of the origination, destination and / or transaction type information in the message. The following legacy part numbers are included.

Table 38: Oracle Communications EAGLE Origin Based Routing

Part Number	Description
Part Number	Description
893-0279-07	EAGLE >96 TCAP OPCODES
893-0279-01	EAGLE 0 To 3 TCAP OPCODES
893-0279-06	EAGLE 49 To 96 TCAP OPCODES
893-0279-04	EAGLE 13 To 24 TCAP OPCODES
893-0279-05	EAGLE 25 To 48 TCAP OPCODES
893-0279-02	EAGLE 4 To 6 TCAP OPCODES
893-0279-03	EAGLE 7 To 12 TCAP OPCODES
893-0277-01	EAGLE Flexible Linkset Optional Based Routing
893-0142-01	EAGLE Origin-Based MTP Routing
893-0143-01	EAGLE Origin-Based SCCP Routing
893-0278-01	EAGLE TCAP OPCODE Based Routing

16. L99422 Oracle Communications EAGLE Prepaid Routing – ISO – per Node: Provides advanced routing mechanisms to ensure the correct routing and charging of signaling traffic related to prepaid customers and typically applied to number portability or SMS processing. For example, it enriches IDP messages with number portability information.

Table 39: Oracle Communications EAGLE Prepaid Routing

Part Number	Description
Part Number	Description
893-0332-01	EAGLE IDP A-Party Blacklist
893-0333-01	EAGLE IDP A-Party Routing
893-0155-01	EAGLE IDP Screening
893-0336-01	EAGLE IDP Service Key Routing
893-0257-01	EAGLE IDPR ASD
893-0256-01	EAGLE IDPR GRN
971-0311-01	EAGLE MO-SMS Prepaid Intercept On B-Party
971-0309-01	EAGLE Prepaid IDP Query Relay CGPN
893-0160-01	EAGLE Prepaid IDP Query Relay
893-0067-01	EAGLE Prepaid SMS Intercept

971-0354-01	EAGLE 40.0 Or Later License IDP-SMS Relay
971-0365-01	EAGLE 40.1 Or Later License Prepaid SMS Intercept Support For SSN Routing

17. L99423 Oracle Communications EAGLE SMS Routing – ISO – per NodeL: This product provides various Mobile Originated (MO) and Mobile Terminated (MT) SMS routing features including options such as B-Party routing and number portability related routing conditions. The following legacy part numbers are included.

Table 40: Oracle Communications EAGLE SMS Routing

Part Number	Description
Part Number	Description
971-0343-01	EAGLE MO SMS Interactions With IS41 GSM Migration
893-0194-01	EAGLE MO GSM SMS Number Portability
893-0195-01	EAGLE MO IS41 SMS Number Portability
893-0267-01	EAGLE MO SMS ASD
893-0246-01	EAGLE MO SMS B-Party Routing
893-0266-01	EAGLE MO SMS GRN
893-0241-01	EAGLE MT GSM MMS Number Portability
893-0200-01	EAGLE MT GSM SMS Number Portability
893-0199-01	EAGLE MT IS41 SMS Number Portability
971-0415-01	EAGLE SRI SM Circular Route Prevention

18. L99434 Oracle Communications EAGLE Service Handler 8 GB – ISO – per Card: This product is required for each Service Module 8 GB card purchased and entitles the maximum throughput capacity of the card. The legacy part numbers listed below are included.

Table 41: Oracle Communications EAGLE Service Handler 8GB

Part Number	Description
Part Number	Description
893-0191-01	EAGLE E5-SM4G 5000 TPS
893-0191-02	EAGLE E5-SM4G 6800 TPS
971-0076-01	EAGLE DSM Per 850 TPS
971-0136-01	EAGLE Version Independent License E5-SM4G Core SCCP Software
971-0278-01	EAGLE 5000 GTT TPS Per E5-SM
971-0278-05	EAGLE 10,000 GTT TPS Per E5-SM
971-0278-07	EAGLE 13,600 GTT TPS Per E5-SM

971-1171-01	DCM STC DCM Card 1000 TPS Functionality
971-0278-04	EAGLE 41.1 Or Later License 5,000 To 6,800 GTT Transactions Per Second Per E5-SM Upgrade
971-0278-06	EAGLE 6,800 To 10,000 GTT TPS Per E5-SM Upgrade
971-0278-08	EAGLE 10,000 To 13,600 GTT TPS Per E5-SM Upgrade
893-0191-03	EAGLE 10,000 TPS Per E5-SM8G-B Throughput Capacity Per Node
893-0191-04	EAGLE 13,600 TPS Per E5-SM8G-B Throughput Capacity Per Node
971-0278-02	EAGLE GTT Transactions Upgrade To Maximum Transactions License Per E5-SM
893-0191-01	EAGLE E5-SM4G 5000 TPS

19. L99436 Oracle Communications EAGLE Ethernet B Traffic Handler – ISO – per Card: This product is required for each Oracle Communications EAGLE Ethernet B (ENET-B) card purchased. These cards allow for SIGTRAN traffic or IP terminals or message copy capabilities and flow of SIGTRAN (IP Based) messages through the system. If used for SIGTRAN, entitles the maximum throughput capacity of the card. The legacy part numbers listed below are included.

Table 42: Oracle Communications EAGLE Ethernet B Traffic Handler

Part Number	Description
Part Number	Description
971-0085-01	EAGLE IP Gateway 1 TPS
971-0106-02	EAGLE IP Transport E5-ENET Core Software
971-0170-01	EAGLE Version Independent License IPLIM EDCM 2000 TU
971-0173-01	EAGLE IPGW 4000 TU
971-0287-01	EAGLE IPSG 5000 TUS
971-0287-03	EAGLE 38.0 Or Later License E5-ENET IPGW/IPLIM To IPSG Upgrade
971-0287-07	EAGLE 38.0 Or Later License E5-ENET IPGW To IPSG Upgrade M3UA Limited
971-0293-01	EAGLE Fast Copy 5000 TUS
971-3008-01	EAGLE STP LAN Per Link
893-0395-01	EAGLE E5-ENET-B IPSG High Throughput
971-0085-02	EAGLE IP Transport 1 TPS
971-0106-01	EAGLE IP Gateway E5-ENET Core Software
971-0119-01	Enhanced STC Performance Software License Up To 4800 TVG Grants Per EDCM/EDCM-A EAGLE
971-0172-01	EAGLE Version Independent License IPLIM E5-ENET 4000 TU
971-0217-01	EAGLE STC Per E5-ENET
971-0287-02	EAGLE IPSG 500 TUS
971-0287-05	EAGLE 38.0 Or Later License IPSG E5-ENET M3UA Limited
971-0287-08	EAGLE 41.1 Or Later License Per IPSG E5-ENET IN >2,000 Link Node

971-0293-02	EAGLE Fast Copy 500 TUS
971-3007-01	EAGLE STP LAN Per Node

20. L99438 Oracle Communications EAGLE Asynchronous Transfer Mode B Traffic Handler – ISO – per Card: This product is required for each Oracle Communications Asynchronous Transfer Mode B (ATM-B) card purchased and entitles the maximum throughput capacity of each card. These cards allow for traffic flow of ATM messages through the system. The legacy part numbers below are included.

Table 43: Oracle Communications EAGLE Asynchronous Transfer Mode B Traffic Handler

Part Number	Description
Part Number	Description
893-0391-01	EAGLE 1 to 5 3-Port E5-ATM Cards
893-0391-03	EAGLE 11 to 15 3-Port E5-ATM Cards
893-0391-05	EAGLE 21 to 25 3-Port E5-ATM Cards
893-0391-07	EAGLE 31 to 35 3-Port E5-ATM Cards
893-0391-09	EAGLE 41 to 45 3-Port E5-ATM Cards
893-0391-11	EAGLE 51 to 55 3-Port E5-ATM Cards
893-0391-13	EAGLE 61 to 65 3-Port E5-ATM Cards
893-0391-15	EAGLE 71 to 75 3-Port E5-ATM Cards
893-0391-17	EAGLE 81 to 85 3-Port E5-ATM Cards
893-0391-19	EAGLE 91 to 95 3-Port E5-ATM Cards
893-0391-21	EAGLE 101 to 105 3-Port E5-ATM Cards
893-0391-23	EAGLE 111 to 115 3-Port E5-ATM Cards
893-0391-25	EAGLE 121 to 125 3-Port E5-ATM Cards
893-0391-27	EAGLE 131 to 135 3-Port E5-ATM Cards
893-0391-29	EAGLE 141 to 145 3-Port E5-ATM Cards
893-0391-02	EAGLE 6 to 10 3-Port E5-ATM Cards
893-0391-04	EAGLE 16 to 20 3-Port E5-ATM Cards
893-0391-06	EAGLE 26 to 30 3-Port E5-ATM Cards
893-0391-08	EAGLE 36 to 40 3-Port E5-ATM Cards
893-0391-10	EAGLE 46 to 50 3-Port E5-ATM Cards
893-0391-12	EAGLE 56 to 60 3-Port E5-ATM Cards
893-0391-14	EAGLE 66 to 70 3-Port E5-ATM Cards
893-0391-16	EAGLE 76 to 80 3-Port E5-ATM Cards
893-0391-18	EAGLE 86 to 90 3-Port E5-ATM Cards
893-0391-20	EAGLE 96 to 100 3-Port E5-ATM Cards

893-0391-22	EAGLE 106 to 110 3-Port E5-ATM Cards
893-0391-24	EAGLE 116 to 120 3-Port E5-ATM Cards
893-0391-26	EAGLE 126 to 130 3-Port E5-ATM Cards
893-0391-28	EAGLE 136 to 140 3-Port E5-ATM Cards
893-0391-30	EAGLE 146 to 150 3-Port E5-ATM Cards
971-4188-01	EAGLE T1 ATM HSL 1/Link
971-4245-01	EAGLE E1 ATM HSL 1/Link

21. L99440 Oracle Communications EAGLE E1T1 B Traffic Handler – ISO – per Card: This product is required for each E1T1-B card purchased and entitles the maximum throughput capacity of the card. The legacy part numbers below are included.

Table 44: Oracle Communications EAGLE E1T1 B Traffic Handler

Part Number	Description
893-0130-02	EAGLE 5 To 8 Synchronous E1 High Speed Links
893-0130-04	EAGLE 17 To 24 Synchronous E1 High Speed Links
893-0130-06	EAGLE 33 To 40 Synchronous E1 High Speed Links
893-0130-08	EAGLE 49 To 56 Synchronous E1 High Speed Links
893-0130-10	EAGLE 65 To 72 Synchronous E1 High Speed Links
893-0273-04	EAGLE 41.0 Or Later Synchronous T1 High Speed Link A System Qty 24
971-0097-01	EAGLE E1 8 Low Speed Links
971-0097-02	EAGLE T1 8 Low Speed Links
971-0286-01	EAGLE Version Independent License Link Interface Module (HSL) T1 To E1 Capacity Increase
971-4177-01	Multi Port LIM EAGLE Module
971-4223-01	T1 MIM 8 Channel Per MIM EAGLE
971-4224-01	E1 MIM 8 Channel Per MIM EAGLE
893-0130-01	EAGLE 0 To 4 Synchronous E1 High Speed Links
893-0130-03	EAGLE 9 To 16 Synchronous E1 High Speed Links
893-0130-05	EAGLE 25 To 32 Synchronous E1 High Speed Links
893-0130-07	EAGLE 41 To 48 Synchronous E1 High Speed Links
893-0130-09	EAGLE 57 To 64 Synchronous E1 High Speed Links
893-0130-11	EAGLE 73 To 80 Synchronous E1 High Speed Links
893-0130-12	EAGLE 81 To 88 Synchronous E1 High Speed Links
893-0130-13	EAGLE 89 To 96 Synchronous E1 High Speed Links
893-0130-14	EAGLE 97 To 104 Synchronous E1 High Speed Links
893-0130-15	EAGLE 105 To 112 Synchronous E1 High Speed Links

893-0130-16	EAGLE 113 To 120 Synchronous E1 High Speed Links
893-0273-12	EAGLE 41.0 Or Later License Synchronous T1 High Speed Link A System Qty 88
893-0273-15	EAGLE 41.0 Or Later License Synchronous T1 High Speed Link A System Qty 112

22. L101180 Oracle Communications EAGLE Service and Link Interface Card Handler – ISO – per Card: This product is required for each Service and Link Interface card purchased and entitles the maximum throughput capacity of the card.
23. L99424 Oracle Communications EAGLE Application Processor Provisioning – ISO – per Card: This product provides the provisioning interface for MNP, HLR Router, INP/AINPQ, EIR, IGM, IDP, SMS related features and Network Bridge products. It also contains a separate database which stores Dialed Number (DN) and International Mobile Subscriber Identity (IMSI) entries used by number portability applications and applications which perform message analysis and re-routing based on a set of operator defined rules. The following legacy part numbers are included.

Table 45: Oracle Communications EAGLE Application Processor Provisioning

Part Number	Description
971-0441-01	EAGLE EPAP Lower PDBI Message Timeouts
971-0075-01	EAGLE EPAP Performance Software
971-0444-01	EPAP Enhanced Password Restrictions
971-0442-01	EPAP Enhanced PDBI Command Logging
971-0445-01	EPAP Restrict And Log Access
971-0260-01	EPAP 9.6 Or Later License PDBA Proxy Support For SOG
971-0277-01	EPAP Version Independent License 1000 Number Range Entries Per Each Increment
893-0161-01	SW Support OF 128 PDBI Connections

24. 99426 Oracle Communications EAGLE Application Processor NonProvisioning – ISO – per Card: This product offers similar functionality to part number L99424 however it is not provisioned directly from external data sources but rather from an Oracle Communications EAGLE Application Processor Provisioning node. The following legacy part is included.

Table 46: Oracle Communications EAGLE Application Processor NonProvisioning

Part Number	Description
971-3050-01	EAGLE Multiple EPAPS ON 1 Prov EPAP

25. L99425 Oracle Communications EAGLE Application Processor Database Capacity – ISO – per 500K DB Entries: This product provides database capacity for the Oracle Communications EAGLE Application Processor. Each unit of this part adds a database capacity of 500K. The maximum database capacity supported is 480M entries (240M for IMSIs and IMEI-based entries and another 240M for MSISDN based entries). The following legacy part is included.

Table 47: Oracle Communications EAGLE Application Processor Database Capacity

Part Number	Description
971-3055-01	EAGLE 500000 EPAP Entries

26. L99430 Oracle Communications EAGLE LNP Application Processor – ISO – per Card: This product is part of the Oracle Communications LNP solution. The Oracle Communications EAGLE LNP solution provides the appearance of a service control point (SCP) to other SCCP and TCAP applications residing in other network elements. This includes local SCCP subsystem management, automatic call gapping and TCAP error handling procedures. The two primary functions of LNP supported by the Oracle Communications EAGLE are: Location Routing Number (LRN) query and Message Relay (MR) function.

Table 48: Oracle Communications EAGLE LNP Application Processor

Part Number	Description
971-0068-11	EAGLE ELAP E5-APP-B Software
971-0077-01	EAGLE ELAP OS TPD Software
971-0078-01	EAGLE ELAP Performance Software

27. L99431 Oracle Communications EAGLE LNP Application Processor Database Capacity – ISO – per 12M LNP Entries: This product enables the database capacity for the required number of Local Number Portability (LNP) entries. Depending on the quantity purchased, the following legacy part numbers may be utilized.

Table 49: Oracle Communications EAGLE LNP Application Processor Database Capacity

Part Number	Description
971-4167-01	POD Feature Module 12-24M Numbers Upgrade LSMS
971-4168-01	POD Feature Module 24-36M Numbers Upgrade LSMSFEATURE MODULE 24-36M NUMBERS UPGRADE LSMS
971-4139-01	POD Feature Module 36-48M Numbers Upgrade LSMS
971-4017-01	Support 12 Million Ported Numbers EAGLE
971-4048-01	Support Up To 12 Million Records EAGLE
971-4171-01	POD Feature Module LNP 12M To 24M Record Upgrade Per Node EAGLE
971-4172-01	POD Feature Module LNP 24M To 36M Record Upgrade Per Node EAGLE
971-4173-01	POD Feature Module LNP 36M To 48M Record Upgrade Per Node EAGLE
893-0110-14	EAGLE >108M To 120M LNP Records
893-0110-15	EAGLE >120M To 132M LNP Records
893-0110-05	EAGLE Up To 12M LNP Records
893-0110-06	EAGLE >12M To 24M LNP Records
893-0110-16	EAGLE >132M To 144M LNP Records
893-0110-17	EAGLE >144M To 156M LNP Records

893-0110-18	EAGLE >156M To 168M LNP Records
893-0110-19	EAGLE >168M To 180M LNP Records
893-0110-20	EAGLE >180M to 192M LNP Records
893-0110-21	EAGLE >192M To 204M LNP Records
893-0110-22	EAGLE >204M To 216M LNP Records
893-0110-23	EAGLE >216M To 228M LNP Records
893-0110-24	EAGLE >228M To 240M LNP Records
893-0110-25	EAGLE >240M To 252M LNP Records
893-0110-07	EAGLE >24M To 36M LNP Records
893-0110-26	EAGLE >252M To 264M LNP Records
893-0110-27	EAGLE >264M To 276M LNP Records
893-0110-28	EAGLE >276M To 288M LNP Records
893-0110-29	EAGLE >288M To 300M LNP Records
893-0110-30	EAGLE >300M To 312M LNP Records
893-0110-31	EAGLE >312M To 324M LNP Records
893-0110-32	EAGLE >324M To 336M LNP Records
893-0110-33	EAGLE >336M To 348M LNP Records
893-0110-34	EAGLE >348M To 360M LNP Records
893-0110-35	EAGLE >360M To 372M LNP Records
893-0110-08	EAGLE >36M To 48M LNP Records
893-0110-36	EAGLE >372M To 384M LNP Records
893-0110-09	EAGLE >48M To 60M LNP Records
893-0110-10	EAGLE >60M To 72M LNP Records
893-0110-11	EAGLE >72M To 84M LNP Records
893-0110-12	EAGLE >84M To 96M LNP Records
893-0110-13	EAGLE >96M To 108M LNP Records
893-0094-02	EAGLE NPA-NXX Table Increase 300,000 Entries
971-4257-05	108 Million Numbers LSMS
971-4257-06	120 Million Numbers LSMS
971-4257-07	132 Million Numbers LSMS
971-4257-08	144 Million Numbers LSMS
971-4257-09	156 Million Numbers LSMS
971-4257-10	168 Million Numbers LSMS
971-4257-11	180 Million Numbers LSMS
971-4257-12	192 Million Numbers LSMS

971-4257-13	204 Million Numbers LSMS
971-4257-14	216 Million Numbers LSMS
971-4257-15	228 Million Numbers LSMS
971-4257-16	LSMS 11.0 Or Later License 240 Million Numbers
971-4257-17	LSMS 11.0 Or Later License 252 Million Numbers
971-4257-18	LSMS 11.0 Or Later License 264 Million Numbers
971-4257-19	LSMS 11.0 Or Later License 276 Million Numbers
971-4257-20	LSMS 11.0 Or Later License 288 Million Numbers
971-4257-21	LSMS 11.0 Or Later License 300 Million Numbers
971-4257-22	LSMS 11.0 Or Later License 312 Million Numbers
971-4257-23	LSMS 11.0 Or Later License 324 Million Numbers
971-4257-24	LSMS 11.0 Or Later License 336 Million Numbers
971-4257-25	LSMS 11.0 Or Later License 348 Million Numbers
971-4257-26	LSMS 11.0 Or Later License 360 Million Numbers
971-4257-27	LSMS 11.0 Or Later License 372 Million Numbers
971-4257-28	LSMS 11.0 Or Later License 384 Million Numbers
971-4257-01	Software Feature Module 60 Million Numbers LSMS
971-4257-02	Software Feature Module 72 Million Numbers LSMS
971-4257-03	Software Feature Module 84 Million Numbers LSMS
971-4257-04	Software Feature Module 96 Million Numbers LSMS
971-0073-01	SW DSM 4G 36 To 48M

28. L99428 Oracle Communications LSMS – ISO – per Card: This product provides the interface between the Number Portability Administration Center (NPAC) Service Management System (SMS) and the Oracle Communications EAGLE LNP Application Processor. It supports provisioning of the Oracle Communications EAGLE with NPAC data as well as locally administered service provider specific data. The following legacy part numbers are included.

Table 50: Oracle Communications LSMS

Part Number	Description
971-4070-01	Feature Module Remote Monitoring LSMS
971-4055-01	Increase Number Of Supported Service Provider IDS EAGLE
971-3024-02	LSMS BASE E5-APP-B LSMS SOFTWARE
971-0373-01	LSMS Security Enhancements
971-4265-01	NANC 3.2 Features LSMS
971-0083-01	NANC 3.3 Feature Set LSMS
971-0233-01	LSMS 10.0 or Later License NANC 399 SV Type Indicator and Alternative SPID

29. L99441 Oracle Communications LSMS Query Server – Server Perpetual: This product provides users with the ability to store a copy of the LSMS data on a separate, commercial off-the-shelf (COTS) hardware for off line data analysis and reporting. The following legacy part number is included.

Table 51: Oracle Communications LSMS Query Server

Part Number	Description
971-4263-01	Query Server Package LSMS

30. L99445 Oracle Communications EAGLE FTP Table Base Retrieval – per Server Perpetual: This product allows customers to provision table data of an Oracle Communications EAGLE node via FTP retrieval and script replacement. Oracle Communications EAGLE FTP Table Base Retrieval can be used to retrieve and manipulate the table data and send subsequent changes (replace) to the Oracle Communications EAGLE OA&M. The following legacy part number is included.

Table 52: Oracle Communications EAGLE FTP Table Base Retrieval

Part Number	Description
971-0638-01	EAGLE FTP Table Base Retrieval







Oracle Corporation, World Headquarters

500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries

Phone: +1.650.506.7000
Fax: +1.650.506.7200

CONNECT WITH US

-  blogs.oracle.com/oracle
-  facebook.com/oracle
-  twitter.com/oracle
-  oracle.com

Integrated Cloud Applications & Platform Services

Copyright © 2016, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. 0116

White Paper Oracle Communications EAGLE 46.3 Feature Guide
August 2016