iDEN System Integration

Major Project Report

Submitted in partial fulfillment of the requirements

For the degree of

Master of Technology

In

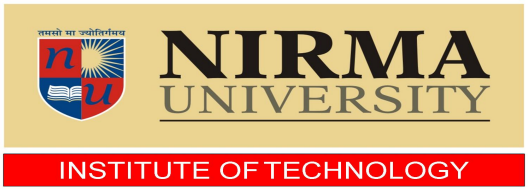
Electronics & Communication Engineering

(Communication Engineering)

By

Parth Sharma

(09MECC11)



Department of Electronics & Communication Engineering

Institute of Technology

Nirma University

Ahmedabad-382 481

May 2011

iDEN System Integration

Major Project Report

Submitted in partial fulfillment of the requirements

For the degree of

Master of Technology

In

Electronics & Communication Engineering

(Communication Engineering)

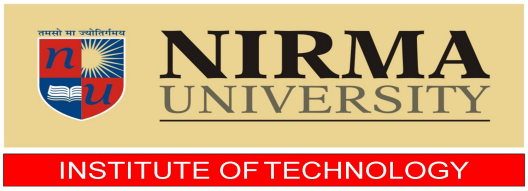
By

Parth Sharma

(09MECC11)

Under the Guidance of

Prof. M. R. Naik



Department of Electronics & Communication Engineering

Institute of Technology

Nirma University

Ahmedabad-382 481

May 2011

Declaration

This is to certify that

i) The thesis comprises my original work towards the degree of Master of Technology in Communication Engineering at Nirma University and has not been submitted elsewhere for a degree.

ii) Due acknowledgement has been made in the text to all other material used.

Parth Sharma

Certificate

This is to certify that the Major Project entitled **"iDEN System Integration"** submitted by **Parth Sharma (09MECC11)**, towards the partial fulfillment of the requirements for the degree of Master of Technology in Communication Engineering of Nirma University, Ahmedabad is the record of work carried out by him under our supervision and guidance. In our opinion, the submitted work has reached a level required for being accepted for examination. The results embodied in this major project, to the best of our knowledge, haven't been submitted to any other university or institution for award of any degree or diploma.

Date: Place: Ahmedabad

Guide	HOD
(Prof. M. R. Naik) Assistant Professor, EC	(Prof. A. S. Ranade) Professor, EC
Director	Program Coordinator
(Dr. K. Kotecha) Director, IT, NU	(Dr. D. K. Kothari) Professor, EC

Abstract

The Integrated Digital Enhanced Network is a well renowned communication network. In any communication system, the testing of the system is an important phase without which the system cannot be launched in the real world. Similarly, the network elements of the iDEN system have to be first tested rigorously under several scenarios to check whether the element responds as per the expectations in such scenarios or not. This thesis explains the basics of the iDEN (Integrated Digital Enhanced Network) and it explains the need for developing the test cases for different network elements individually and for the entire system as a whole. This thesis includes the approaches adopted for the test case development. These approaches include several scripting tools and automation tools used to create scenarios for testing of the network elements and also for the end-to-end system testing. This thesis explains several call scenarios created using the above mentioned approaches. The results include the findings as the end results of the test case developments. The conclusions included in the thesis indicate the behavior of the network elements under different call scenarios. The future scope of the project includes the further testing of different network elements of the system. It also throws some light on the possible future expansion of the system testing by upgrading the system version to the Melody Based iDEN System.

Acknowledgements

First and foremost I would like to thank Prof. A. S. Ranade, Head of the Electrical Engineering department and Dr. D. K. Kothari, coordinator of M.Tech Communication Engineering program to give me this opportunity to undertake this thesis work.

I would like to thank my Thesis Supervisor Prof. Mehul R. Naik and my Project Manager Mr. Varadarajulu Kolamala for giving me this opportunity to be a part of such a dignified organization to carry out my thesis work.

I would like to thank Prof. Mehul R. Naik for guiding me through the thick and thin of this journey. I would like to thank Papu, Chandra, Leena, Chetan, Pramod, Samal, Sheetal, Anita, Mahesh, Rupesh, Srinivas, Jisha, Deepa, Shailesh, Pooja, Sinduja and Reshma for their guidance at Motorola throughout the tenure of the thesis work.

I would like to show my deep regards and sincere thanks to all my friends for their support.

I am indebted to my parents who stood by my side through tough times and became my strength. It is because of them I am able to successfully complete the journey of this thesis.

- Parth Sharma

09MECC11

Contents

List of Tables

List of Figures

Chapter 1

Introduction

Today, the world and the technology in the field of wireless communication are growing by leaps and bounds. In such scenario it becomes very important for the service providers and the technological experts to keep up to the pace of the ever-growing technology. Moreover, the customers are becoming more aware in the matter of what kind of services they require and what kind of facilities they want in a single handset or a mobile device. On the other hand the service providers have to keep in mind the limitation of the availability of the wireless resources which are always in less quantity as is known since years. In such scenario, technological advancement is required which can serve the customers with all the possible facilities in one mobile handset. The technology should be able to serve the ever-growing demands of the services of the customers and also it should use the wireless resources available wisely and effectively. Motorola's iDEN is the answer to all the above needs from the point of view of both the customers and the service providers. iDEN is the Integrated Digital Enhanced Network. It provides the customers with the facilities of a cellular network, a trunked radio device, and packet data services. The mode of communication that is being used can be divided into two major parts namely half duplex and full duplex.

- Half Duplex: This is a communication technique in which the communication takes place from only one end at a given time. That means that a person can

either send the message or can receive the message but not both at the same time.

- Full Duplex: This is a communication technique in which the person can send and receive the messages at the same time.

Generally in most of the communications it is not required to use the full duplex mode of communication and can use the half duplex mode of communication to efficiently convey the message required. For example the communications like text messages and paging service does not require full duplex mode of communication. Only half duplex mode is enough to successfully complete the communication. Moreover, in the traditional telephone services like mobile to landline or vice versa, the full duplex mode of communication is required to be implemented.

In these cases iDEN can be the best suitable network to support both the modes of communication. The iDEN system provides both full and half-duplex operations. This melding of communication methods allow much of the voice traffic to be run in half-duplex mode, while providing full-duplex functionality when required. Thus, iDEN can be viewed as the integration of the traditional Push-to-Talk (PTT), packet data services and the full duplex traditional cellular services. Hence the first requirement of the need of the hour i.e. to satisfy the customers with the most possible facilities is thus achieved by the iDEN network.

Growth in wireless communications products has accelerated as people are becoming more mobile. Requirements have also grown beyond the traditional limited feature, single function, communications units of the past. In addition to increased feature/functionality requirements, users are looking for services to be offered by a single service provider. For the iDEN operator such services can easily and quickly be provisioned and made available to the end user ahead of traditional deployment approaches.

Motorola recognized the finite availability of Radio Frequency (RF) spectrum and the pressure for efficient usage of that resource. With this in mind, Motorola created

the iDEN (integrated Dispatch Enhanced Network) technology that increases the efficiency of a single 25 KHz RF channel up to six times that of an AMPS Cellular RF channel. In addition to the increased channel efficiency, iDEN, when deployed to support Roaming, allows interconnect users to roam seamlessly throughout linked service areas placing and receiving calls as easily as if the MS was on its home system. For the service provider, the iDEN nationwide network capability allows the offering of more services, such as nation wide SMS delivery while roaming, than current analog cellular.

Beyond the additional integrated features that iDEN provides to the end user, the iDEN system, using digital technology provides clearer voice quality with fewer dropped calls and improved security. iDEN provides an operator with the ability to offer an integrated service that includes Short Message Service, Local and Wide Area Dispatch Service (both Private Two-way and Group Call), Cellular Telephony Service, Voice Mail Service and Circuit Switched Data with Packet Data a planned future feature [1][2][3][4][5].

1.1 Summary of iDEN Features

- Fully featured compact Hand-held portables or vehicular Mobile Stations (MS)
- Full Duplex cellular like service
- Short Messaging Service similar to digital paging
- Circuit Switched Data for digital connections to base computer systems
- Dispatch capability for Private, Local and Wide Area Group calling
- Digital technology for reliable and secure communication
- Flexible Network Scaling
- Spectrally Efficient RF Channel usage.

1.2 Geographical Organization

In order to support the increasing demands of the telecommunication services, the iDEN network is divided into several divisions or areas for the sake of simplicity. These kinds of division are based upon the geographical locations and hence it is called the geographical organization of the network. Figure 1.1 represents the Geographical Organization used in the iDEN network [1]. The following are the geographical divisions in which the network is being divided.

- Global
- Region
- Domain
- Service Area
- Location Area
- Cell

1.2.1 Global

Global means the world as a whole. The worldwide Public Switched Telephone Network (PSTN) is a part of the global geographical region of iDEN. A mobile unit of the iDEN network must be able to communicate with the PSTN. When the iDEN system uses the PSTN (Interconnect) system, the rules and procedures of the PSTN are used. Interconnect calling is the access to land-line systems and the services available and emerging in the public switched environment. Global Two-Way (Dispatch) communications, while currently not available, is emerging technology.

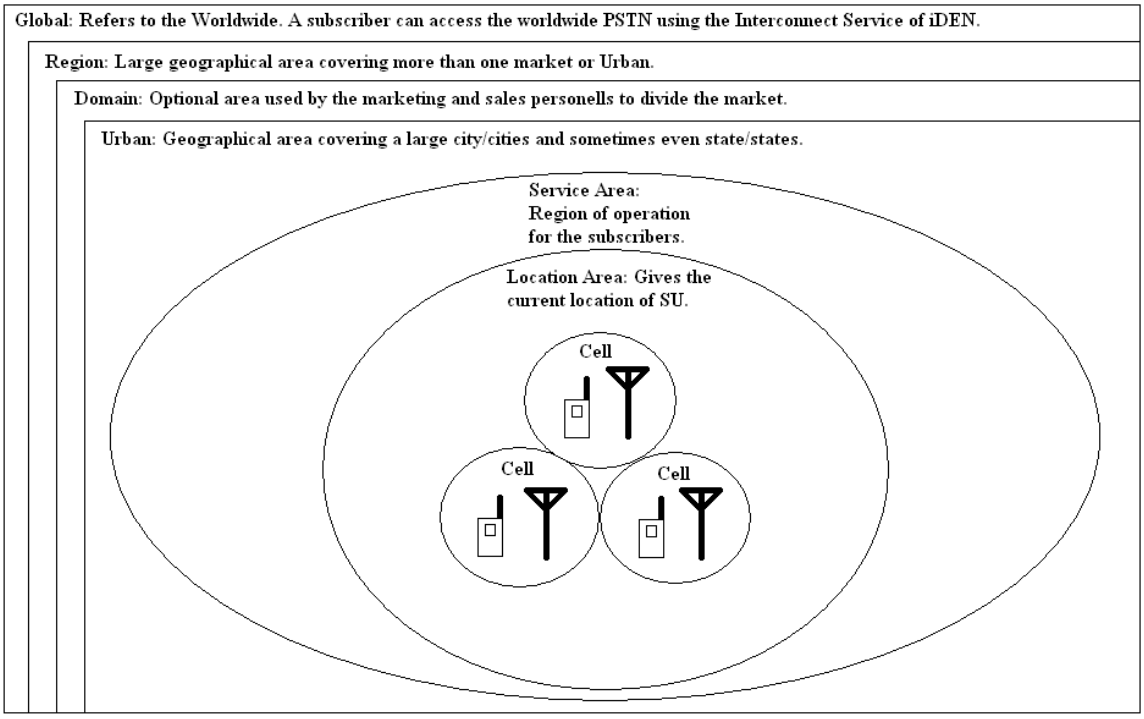


Figure 1.1: Geographical Organization

1.2.2 Region

A region is a geographical area which is used by the service providers to provide the services to the users. A single service provider will provide service in one region. These regions are also known as markets and these markets may or may not overlap depending upon the need for the continuity of the service between the different regions. Regions may be covered by either Interconnect or Dispatch calling.

1.2.3 Domain

Domain is an optional geographical area used by the sales and marketing personals in order to divide the market for the sales purpose.

1.2.4 Urban

Urban is generally centered on a large city. An urban can also span the area of more than one city or even more than one state.

1.2.5 Service Area

A service area is a geographical division solely for the purpose of the dispatch service. This area is used for the provisioning of the user databases. This area determines the region where the dispatch service for that particular subscriber is authorized.

1.2.6 Location Area

A location area is a geographical area decided based on the present or the most recent known location of the MS (Mobile Station). Each MS while moving from one location area to another has got their Location Area Identifier with the help of which the current location of the MS can be found for paging and call setup purpose. The location areas for the dispatch services are different in sizes from that of the interconnect services.

1.2.7 Cell

A cell is the area serviced by the RF propagation pattern of the antennas and a radio of a remote tower (cell site). The area is the effective size of a cell. An EBTS cell site may be either Omni-directional or sectored. An Omni site will have 1 cell. Sectored sites have 2, to 12 sectors (cells). Sectored sites most commonly have three cells. An

MS is located by radio link integrity between 1 or more cells. One cell acts as host serving cell until a better radio link is detected from another cell.

1.3 Logical Organization

Most communication systems can be divided into logical groups and hence iDEN is also divided into the logical groups as follows. The Figure 1.2 represents the Logical Organization of the iDEN Network [1].

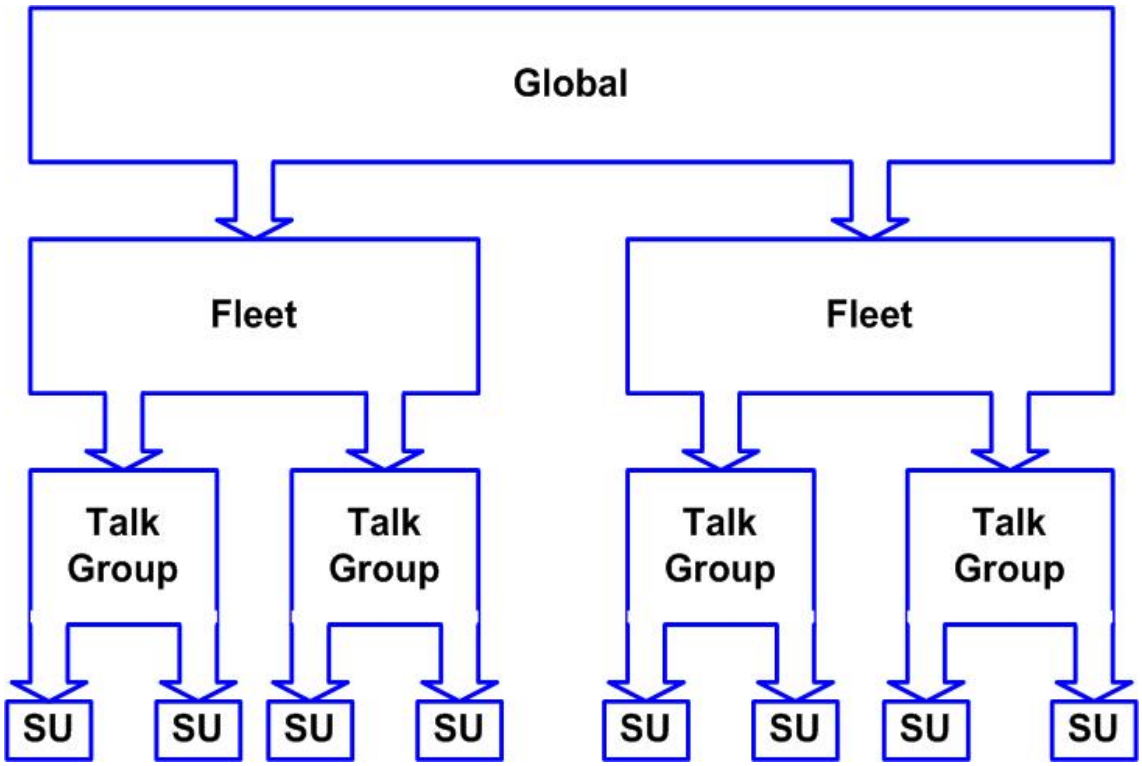


Figure 1.2: Logical Organization

1.3.1 Global

Global is the logical division which may contain all the potential users of the network which uses the Global System for Mobile Communications which is compatible with

the Public Switched Telephone Network.

1.3.2 Fleet

Fleet is a logical group that can be considered as an organization in which the members of the organization are the part of this group. For example, a fleet of trucks or in institute can be seen as fleets. In the case of the fleet of trucks, the owner of the trucks may wish to be in constant touch with all the member trucks of the fleet. For this purpose the owner may register his group of trucks as a fleet with all the members recognized individually using a fleet ID.

1.3.3 Talk Groups

A talk group can be seen as a subsection of a fleet. For example if an organization is considered as fleet then the organization may have different departments like the security department, the IT department, the drivers group and so on. More often the members of these subsection need to communicate with the members of their own subsection only and in that case the these subsection form what is called talk groups and the members of these talk groups are assigned group IDs for their clear distinction and identification.

1.3.4 Users

The smallest possible unit of the logical organization is the user itself. The user is the subscriber unit that avails the iDEN services and is a member of some talk group or some fleet or some urban and is definitely a member of the global group of the logical organization hierarchy.

1.4 Services provided by the iDEN network

1.4.1 Interconnect service

iDEN provides the users with the interconnect services which allows the subscribers to make calls to other mobile devices in the GSM network and also the mobile devices in the land based PSTN. Also while roaming i.e. when the mobile device is in the extended network the users can make and/or receive calls and if the users have the privilege then they could also send and/or receive data [1][2][3][4]. The major network elements which are required to provide and maintain the interconnect service are as follows:

- **EBTS (Enhanced Base Transceiver Station):** It provides the radio resources to the mobile stations.
- **iBSC (iDEN Base Site Controller):** It routes the interconnect packets between the EBTS and the MSC.
- **MSC (Mobile Switching Center):** It is the most important network element for the interconnect services and it acts as the major router to route the interconnect packets to the final destination i.e. iDEN MS, GSM MS or PSTN telephone.
- **SMS (Short Message Service):** It provides the facility of text messaging to the users.
- **VMS (Voice Mail Server):** It acts as an answering machine for the voice mails and stores the messages for the users and also notifies whenever there is a voice mail available to the users.
- **SDM-FT (Super node Data Manager-Fault Tolerant):** This element allows the law enforcement agencies to intercept an interconnect call for legal activities. It also provides the call records and data to the legal agencies.

1.4.2 Dispatch Service

Dispatch services allow the users to make half-duplex calls which incorporates the traditional Push-to-Talk (PTT) mode of communication using the iDEN network to make local area, selected area or wide area calls [1][2][3][4]. The important network elements used for the functioning of dispatch service are as follows:

- **HA-DAP (High Availability Dispatch Application Processor):** This network element is responsible for the overall coordination of the dispatch call. It sets up the dispatch call and maintains the call during its life time.
- **HA-iHLR (High Availability iDEN Home Location Register):** This element stores the database which contains the information about the home location of any MS. Also, this element helps the HA-DAP to page the destination MS while making a dispatch call.
- **iSG (iDEN surveillance Gateway):** This element plays the role of SDM-FT for the dispatch service. It allows the law enforcement agencies the access to the call records and interception of the dispatch calls for legal purposes.

1.4.3 Packet Data Service

The packet data service provided by the iDEN network is a non-voice communication service that helps the MS to get directly connected to Internet, Intranet, Extranet and VPN (Virtual Private Network) [1]. The following are the major network elements that are responsible for the coordination of the packet data service.

- **MDG (Mobile Data Gateway):** This network element acts as n interface between the SU and the Internet. It converts the protocols of the SU to the protocols of the Internet and vice versa. MDG also acts as a Foreign Agent (FA) for the SUs.

- **HA (Home Agent):** HA route the data packets to the correct MDG/FA in order to ensure correct delivery to the destination SU.
- **BA (Billing Accumulator):** It maintains the billing information for the packet data services and provides the billing records as and when required.
- **AAA server (Authentication, Authorization and Accounting server):** It performs the tasks of verification and identification of SU, SU level of service and tracks the call sessions and records for the accounting purpose.

1.4.4 Network Management

iDEN provides the most important portion of the network i.e. the network management. This service manages all the network elements and takes proper measures in case of faults or alarms. The most important network element for the network management is the OMC-R (Operation and Maintenance Center Radio). This NE tracks the performances of each and every network element and takes proper steps to cure the faults that arise. It establishes, maintains, collects information about the network and presents it to the system operator [1].

1.5 Key Technical Aspects

The services that the iDEN system provides to the customers make the users available with a fully fledged mobile device. At the same time the iDEN system incorporates such cutting edge technologies that make the maximum and efficient utilization of the radio spectrum available with the service providers. Some of those technological aspects are being discussed in this chapter. These technologies include the use of VSELP compression technique along with the Time Division Multiplexing techniques. The combination of all the technologies helps the service providers to accommodate as many users in to the available spectrum. Thus the iDEN network provides the subscriber with the fully fledged mobile device with all the facilities and also the

service provider can have the leisure of an efficient utilization of the radio spectrum available and thus providing the best of both the worlds [4].

The frequency bands supported by the iDEN system are as shown in Table 1.1.

Range (MHz)	Channel Spacing (KHz)	Carrier Pairs (MHz)	Link	Spacing (MHz)
806-821	25	806-821 851-866	Uplink Downlink	45
821-825	25	821-825 866-870	Uplink Downlink	45
896-901	25	896-901 935-940	Uplink Downlink	39
1453-1465	25	1453-1465 1501-1513	Uplink Downlink	48

Table 1.1: Frequency Bands

1.5.1 Radio Carrier Characteristics

The allotment of the frequency channel definition is clear and distinct in case of iDEN network. This is made possible because of the superior out of the band rejection and the narrow in band frequency sensitivity at a precise frequency center. The iDEN system provides better carrier sensitivity, a good Carrier-to-Interference Ratio trade-offs, along with sufficiently low adjacent channel interference [4].

1.5.2 Vector Sum Excited Linear Predicting (VSELP)

VSELP is the linear predicting technique that is used to compress the digital voice packets at the transmitter end and it decompresses the data at the receiver end. It first converts the analog voice data into digital data and then performs the functions of compression. The compression ratios available in the case of VSELP come in two versions that are 3 and 6. If the requirement of the hour is to have a better sound quality and the radio resources are available in plenty then the compression ratio of

3 can be used. And if the need is to have the maximum utilization of the spectrum then the voice quality can be compromised a bit and the compression ratio can be selected to be 6 [4][6].

1.5.3 Radio Carrier Access Method

In order to make the maximum utilization of the spectral resources, the iDEN system incorporates the Time Division Multiple Access (TDMA) to access the radio carrier. The data of the conversations in the system is in the form of digital data stream. This data stream generally runs much faster than required during a conversation. Due to this reason, the digital stream of data can be divided by time and more than one user can be interleaved to share one radio resource. This can be made possible using TDMA without the loss of data or without the adjacent users interfering in each other. This increases the possible number of users for a given radio resource. The number of slots required for one radio is shown as follows:

- 3 per radio (Interconnect)
- 4 per radio (2-Dispatch and 2-Interconnect)
- 6 per radio (Dispatch only)

This provides several benefits:

- Reduced base station costs as compared to analog transmissions
- Full-duplex support - allowing the MS to switch between transmit and receive.
- No incremental hardware to support dispatch, interconnect, and messages.

And for the full duplex application of the iDEN system, Time Division Duplexer is used along with the TDMA radio access scheme.

Thus the second requirement of the system i.e. to make the effective use of the RF spectrum available is done using the above mentioned techniques. Thus the users

can get the full fledged mobile station and the service providers can accommodate the maximum number of users in the available RF spectrum [4].

1.6 Thesis Organization

Chapter 2 explains about the evolution of the iDEN system during the course of the time. It also gives the details of the functions of each Network Element at each stage of system evolution.

Chapter 3 talks about the various interface and the protocols running at those interface in the NGD iDEN system. Detailed descriptions of all the protocols used are being covered in this particular chapter.

Chapter 4 explains the Dispatch Application Processor as the heart of the Dispatch subsystem of iDEN. It explains the system achitecture of the DAP and the tasks that DAP performs.

Chapter 5 explains about the development of the test cases for the box/component testing phase of system integration. It talks about the tools used to develop the test cases and the results pertaining to the tests.

Chapter 6 gives the details of the system testing phase as the final phase of the system integration. It gives the details of the tools and the test cases developed using these tools to perform the system testing.

Chapter 7 finally concludes the thesis and throws some light on the possible future scope and expansions possible in the project.

The Appendices at the end gives a bird's eye view of the functions of all the NEs in the system. Also it gives detailed descriptions of the dispatch calls and call flows whose khowledge plays the most important part in the process of developing and running the test cases at both the box level and at the system level.

Chapter 2

iDEN Subsystems

The iDEN system has been around the communication world since a long period now and has it seen several changes and modifications. From the very introduction of the concept, there has been a change in each and every Software Release that happens. But all in all the iDEN system can be classified into three generations of key technological progression. These three generations are called the Legacy iDEN, the Next Generation Dispatch (NGD) and the Melody based iDEN System.

This chapter gives a brief introduction regarding each of the generation and its network elements. In all of these generations, the system is divided into three major subsystems namely Interconnect Subsystem, Dispatch Subsystem and the Packet Data Subsystem.

2.1 Legacy iDEN System

The Figure 2.1 shows the block diagram of a typical MSO in the Legacy iDEN System. The Legacy iDEN system was based on the dedicated T1/E1 lines and the Frame Relay protocols throughout the network [1].

The network elements of the Legacy iDEN System are as shown in the Figure.

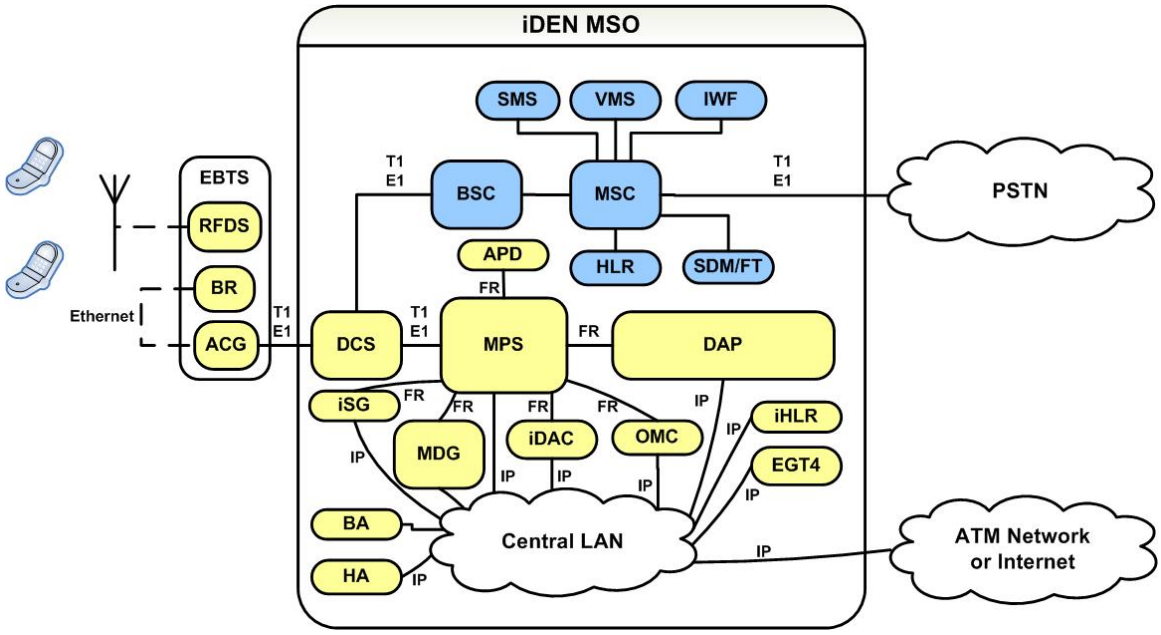


Figure 2.1: Legacy iDEN System

2.1.1 Interconnect Subsystem

The Interconnect subsystem of iDEN system allows the users to roam freely in the entire iDEN system and it also allows the users to make and receive interconnect calls to the other iDEN subscribers, subscribers of other roaming partners and also to PSTN telephones.

For any interconnect call the iDEN system first pages/tracks the target subscriber. Once the destination is reached it will check for the availability of the services for both the originator and the target. If the subscribers in the call are authorized to make the call then sufficient radio resources are being assigned to the units. Once the resources are assigned, the system is then responsible for the routing of the voice packets to the destination and from the originator.

The process of call setup and call maintenance occurs in the same manner when the user is moving around in the network. The roaming user can initiate and receive the calls even when in the extended network in the same manner as if the user is in its

home network. The references for the Interconnect subsystem and the Interconnect calls are [1], [2] and [3].

The major Network Elements involved in an Interconnect call are:

- SU (Subscriber Unit) - sends and receives voice data
- EBTS (Enhanced Base Transceiver System) - converts the radio link to the land link and discriminates between interconnect and dispatch calls
- BSC/iBSC (Base Site Controller / iDEN Base Site Controller) - routes interconnect packets between the EBTS and the MSC
- MSC (Mobile Switching Center) - determines Interconnect services and location information and also controls and routes the calls to other providers
- IWF (Inter-working Function) - provides circuit switched data services
- SMS (Short Message Service) - provides text message services
- VMS (Voice Mail Server) - serves as an answering machine and stores messages for the SU. It also indicates when voice mail is present.
- SDM/FT (SuperNode Data Manager/Fault Tolerant) - part of the Call Intercept System (CIS) that allows law enforcement agencies to obtain call data records as well as intercept audio in an Interconnect phone call for court authorized monitoring.

Enhanced Base Transceiver System

The Radio Access Network of the iDEN system contains the EBTS which provides the SU an interface between the SU and the rest of the land based network. The EBTS converts the radio signal from the subscriber to the land based signal for the rest of the Network Elements.

An EBTS consists of three main Network Elements namely, RFDS (Radio Frequency Distribution System), BR (Base Radio) and iSC/ACG (iDEN site Controller/ Access Control Gateway).

Base Radio

Base Radio is responsible to allocate the channels to the SU. There can be more than one BR in one EBTS. Each BR can allocate a single 25 KHz channel to the SU. Alternatively, if the BR is functioning in Quad BR mode, then it can allocate up to 4 25 KHz channels to the SU. BRs send both the control information and the compressed speech over a radio channel and packet data translations. The Base Radio is the Network Element which can communicate with the SU [7].

Radio Frequency Distribution System

RFDS consists of 3 antennas per Omni or per sector. These antennas can be used both for transmitting and for receiving. And hence set of 3 duplexers are also provided with the RFDS. RFDS allows several BRs to share a common antenna system. Another major function of the RFDS is to amplify and distribute the receive signal to the BRs [8].

iDEN Site Controller/Access Control Gateway

The iSC controls the routing of information to/from the Base Radios, performs resource allocation and satellite tracking. iSC controls the functioning of RFDS and BR [9].

iDEN Base Site Controller (iBSC)

The Network elements other than the SU and the EBTS are categorized into a section called the Mobile Switching Office (MSO). The iBSC is a network element of the interconnect portion of the MSO of iDEN system. iBSC routes the voice and control

signals between the EBTS and the MSC [10]. iBSC consists of two major components namely, iCP (iDEN Call Processor) and iVPU (iDEN Voice Processor Unit). The functions of iDEN Call Processor are as follows:

- It manages the processes of setting up a call, maintaining the call and tearing down the interconnect calls.
- While the Mobile Station is in motion, iCP provides the provisioning of handing over the controls to the other cell sites and hence helps in the mobility management of the system.
- It helps in converting the wireless radio links into the land based links for the rest of the system elements.

The functions of the iDEN Voice Processor Unit are as follows:

- The formats of voice data used for the wireless links are different than the formats used by the land based PSTN system. The formats supported by iDEN are VSELP and AMBE++, while the format for the PSTN is Pulse Code Modulation (PCM). Hence iVPU helps in converting the VSELP and AMBE++ voice packets into PCM voice packets for PSTN.
- Since the network element iVPU is performing the tasks for the interconnect portion of the system it is here called iVPUi where i stands for Interconnect.

Mobile Switching Center (MSC)

The Mobile Switching Center does almost the same tasks as it does in a GSM network. The main function of MSC is to provide an interface between the iDEN Mobile Stations and the PSTN network. It also provides the interface between the iDEN network and other cellular networks as well. The area of service of one MSC depends upon the coverage area of the MSC. Generally, in one urban one or more MSCs may serve the functionalities. MSC in general can be treated as a generic switch which

can perform several tasks such as roles of landline switch, a wireless switch, a gateway, etc. The functionality of MSC is dependent on the software that is used in the element which decides which of the above mentioned functions will be performed by the MSC. The MSC has basic functionality as well as specific functions in the iDEN. These include:

- Speech - the information sent by the customer from one location to another. The information is only passed through a peripheral module and the network.
- Message - the internal information sent by the entire DMS (Digital Multiplexing Switch) switch for call setup. It is often referred to as message links.
- Signaling - the information sent between Central Offices and the BSC/iBSC and EBTS for digit transmission and call details for billing.

The other functions of MSC are as follows:

- Controlling and interfacing the iDEN network with the PSTN network.
- It handles the entire call processing for the interconnect calls.
- It helps the process of echo cancelling, provided that the necessary supporting equipments are also available to the MSC.
- It provides the subscribers with the supplementary services along with the interconnect services.
- At the time of call processing it makes sure that the MS initiating the call is authorized to make that particular call and hence does the task of subscriber authorization and authentication.
- It performs the task of intra system roaming between the iBSCs and/or between the MSCs.
- It maintains and controls the database for the billing purpose.

- It also provides an interface for the customer supplied billing system.
- It controls the Inter Working Funtion (IWF). IWF is mainly responsible for the controlling of circuit switched data in iDEN system.
- One more feature that is supported by the interconnect portion of the iDEN system is the voice mail facility. The MSC is also responsible to control the Voice Mail System.

A major function of any network is to constantly track the location of the mobile station in the network. For the same purpose, MSC has got two network elements namely Home Location Register (HLR) and Visited Location Register (VLR).

Home Location Register (HLR)

The Home Location Register (HLR) is the location where every Subscriber Unit's permanent subscriber records are stored. The HLR may be implemented as part of the MSC or as a separate computing system. All SU identities and the various supplementary services are provisioned in the HLR. The HLR performs Subscriber Access Control. It is queried each time an interconnect call is initiated or interconnect call features are requested and the VLR does not contain an entry. The MSC manages access to the system by verifying requests for service against a database of subscriber privileges. The HLR database also contains Mobile Station Identification data and Fixed Network Data.

Visited Location Register (VLR)

The Visitor Location Register (VLR) is the location and activity database of the MSC, containing the IDs and the most recent location information on each iDEN Subscriber Unit (SU). The core processor reads this location register database to check SU authorization and location information it requires for call setup. The VLR is a fast-access database storing data about the SU units that are now or have been

recently active. It is a fast look up for Interconnect calls, permissions, and services. The VLR speeds call setup because the entire HLR subscriber database that is located on disk is not searched.

Inter Working Function (IWF)

The Inter-Working Function basically performs the task of providing an interface between the PSTN network and the iDEN network for the transfer of data packets. It provides a data rate adaptation between the PSTN and the iDEN network. With the help of the hardware and the software the IWF performs the following major functions in the iDEN system.

- Provides circuit switched data services.
- Serves as a translation and conversion point.
- Allows an end-to-end connection between an SU and a remote device such as a dial-up modem.
- Provides required rate adaptation between the SU and PSTN or between two SUs.
- This allows subscribers to connect a laptop computer or fax machine directly to an iDEN SU to provide wireless modem and fax data capabilities.

Super Node Data Manager/ Fault Tolerant

For legal purposes it is generally required to intercept several calls in any mobile network. In iDEN system also the provisioning of interconnect call tracking and surveillance is available in the form of SDM/FT. SDM/FT manages the formatting of the data and provides an access to the Mobile Switching Center of the interconnect portion. This access to the switch enables the system to maintain the surveillance records, customer provisioning and billing records. The surveillance of any call includes the following functions:

- Call identifying- In order to ensure that the call being traced is the same call it has to be first identified and verified as a valid user.
- Call content information- Once the call is being identified the voice packets have to be intercepted by the system in order to know what conversation is going on.
- Also the location of the SU has to be known in order to tracks the mobile station.

There are three primary elements used to provide this service:

- SuperNode Data Manager (SDM) - provides the point of access for a law enforcement agency to log into the system and obtain interconnect voice data.
- Call Intercept Provisioning Center (CIPC) - provides a web interface to provision surveillance information. Once the information has been submitted, the CIPC informs the SDMs of the presence of the new warrant. Also as a part of the warrant provisioning, the CIPC provides the surveillance ID and password for the law enforcement agency to gain access to the surveillance.
- Law Enforcement Monitor (LEM) - provides the ability to log into the SDM/FT with a surveillance ID and password, then collect and store the audio and data about the calls under surveillance. Once those are stored, the LEM must be able to decode the audio and data into some format usable by the agency in court.

2.1.2 Dispatch Subsystem

Dispatch subsystem manages the facility provided by iDEN called the dispatch calling facility. Dispatch calling facility allows the subscribers to make the voice communication which uses half-duplex traditional push-to-talk mode of communication. When a SU initiates the dispatch call, the system searches the destination and then routes the voice packets to the destination. Once the call has been activated the user can

receive whatever the other caller transmits and when the user wants to transmit the voice data, he has to push the talk button and the voice data can be transmitted. The iDEN system allows the users to make several types of dispatch calls some of which are default and for some external hardware and/or software are required. The references for the Dispatch Subsystem of iDEN are being taken from [1], [2], [3] and [4]. The following are the different types of dispatch calls that the users can make using this facility provided by iDEN:

Private Call

- A private dispatch call is the call that can be made between two parties out of which one party may initialize the call and the another one accepts the request of the initiator.
- To initiate a private call, the caller has to enter the destination's fleet member identification number and then has to press the talk button.
- Once the talk button is pressed, the system validates and authenticates the caller subscriber.
- The system also checks whether the caller is authorized to make this particular call or not.
- If the caller is successful in validating itself then the system starts the paging process in order to find the called subscriber unit.
- After finding the called mobile, the system allocates radio resources.
- If resources are available and the called party is available, a call establishment indicates to the originator that the called party has been located and is ready for the call.
- The called MS activates the audio. The caller's Fleet Member ID is sent to the called MS during the set-up process for display on the called user's MS or for

returning another call. The called MS may display the caller's alias if it has the feature and is programmed to display the alias.

- During the conversation, a hang time is provided so that the two parties may exchange transmissions. After each transmission, the Fixed Network Equipment (FNE) maintains the call for the hang time to allow either user time to respond. If at any time during the process, the called or caller MS does not respond in a programmable timeframe, the FNE disconnects all the channels and tears down the call. The call hang timer is reset by each new transmission.

Group Call

Dispatch Group Calls allow MSs which are members of predefined groups to communicate in half-duplex (one person talking at a time and the others listening) among themselves. Only members of the group can participate in the conversation and any authorized group member can either set-up or participate in the call. The call can be set up without all group members being available and can involve members being served at different sites. Any group member can leave the group at any time. After one MS makes the request, the Fixed Network Equipment (FNE):

- Validates the Dispatch Group Call request
- Determines the Dispatch Location Areas (DLAs) of the group's members
- Pages members (sends a Location Request) in those DLAs
- On Page response, assigns a channel at each site that needs to be added and have resources available.

Three types of Dispatch Group Calls (DGC):

- Local Area Call - Communications between MS in the "Home" or "Local" service area.

- Selected Area Call - Communications between a caller and a group in different service areas.
- Wide Area Call - Communications between a caller and a group anywhere in the network.

Call Alert

- A Call Alert is a dispatch call request.
- It used to notify the called party that voice communication is desired.
- The calling party selects call alert on the MS (Call Alert mode) and then enters the Called MSs Fleet Member ID, or, selects an alias for the pre-programmed list.
- The calling MS receives an acknowledgment (ACK) if the request is successfully delivered.
- An audio tone and a visual indicator on the called MS informs the user of Call Alert.
- The Call Alert displays and stores the calling MSs Fleet Member ID (or alias) on the called MS.
- This can be used to simplify call back.
- The called MS may then select the alert on the MS and initiate a callback.
- The called MS may also delete the alert. Deleting the call alert does not stop the returned Acknowledgement.
- The entire Call Alert procedure takes place on the control channels so no talk channel resources are used.

Emergency Calls

- An Emergency Call is an option. This is a special situation of a Wide Area Dispatch Group Call that is given the highest priority.
- The priority allocates resources for the call, as well as preempts existing calls and call requests.
- An Emergency Call is used to alert all members of the group of an emergency initiated by a user.
- An emergency call is handled before any other call and is intended to announce and open a line of communication in a dangerous situation.
- For users with an Advanced Feature Unit (AFU) MS, a button on the MS generates an Emergency Call. This option is provisioned in the DAP.
- The request triggers a new call, or causes an in-progress call to be elevated to Emergency status.
- Except for the priority, the FNE processes an Emergency call like a Dispatch Group Call. An Emergency Call can also be terminated at any time by the initiator or another user with an MS provisioned override the status.
- An optional advanced feature package is required for the Infrastructure to process Emergency Calls.

MS Status

- Status Code (an 8 bit number) to another MS in the same fleet.
- The meaning of the Status Code is user defined.
- Some MSs can translate the status code into a character string on the MS display.

- The Status Code is transparent to the iDEN system.
- It is not examined, defined or recorded by the iDEN system.
- The MS Status is similar to Call Alert and is controlled by the MSs user interface.
- Like Call Alert, the MS Status returns an acknowledgement when the status is delivered or the MS returns a failure reason.
- MS Status also saves the calling MS fleet ID so a call back can be selected on the MS display.
- The difference between MS Status and Call Alert is the definition in provisioning:
  - A Call Alert may be activated as send, receive, or neither by MS.
  - MS Status can be activated for just send, just receive, both, or neither.
- MS Status is also sent over the control channels and does not use any talk channel resources.

The next sections describe the functions of the major network elements used in the Dispatch Subsystem.

Dispatch Application Processor

The DAP is the processing entity responsible for the overall coordination and control of Dispatch and Packet Data services. The DAP has been optimized to support rapid response time for services, which include but are not limited to: Group calls, Private calls, Call Alerts, Emergency calls and Packet Data networking [11][12]. The DAP provides the following functionality in the iDEN network:

- Overall coordination and control of Dispatch and Packet Data functions.

  - The DAP assigns the signaling and routing paths for Dispatch calls and Packet Data. When the MS requests service the DAP verifies the mobile, confirms the services availability to the MS, and processes the request.

- Tracks and maintains Dispatch and Packet Data mobility.
  - The DAP maintains the last known dispatch location area for all active and recently active MSs. This is used by the DAP to route calls.
- Provides the Visitor Location Register (VLR) for subscriber information.
- Provides first-time registration for Dispatch and Interconnect subscribers.
  - When an MS is powered-on, the MS sends a service request. If the mobile's identification is not valid in the system, service is denied.
- Tracks Subscriber Unit (SU) deactivation.
- Sets up Dispatch group calls.
- Collects alarms and performance statistics.

Dispatch Subscriber Parameters

In order to make the functioning of dispatch call smooth, there are several parameters defined for the users to make themselves identified to the system whenever it is required. The following are those parameters.

Urban ID

The Urban ID parameter defines the home region for a particular SU. This parameter allows an SU to roam outside the home region and maintain a unique ID that is used to confirm service, and permit inter-region and horizontal Dispatch (cross fleet) calling. The Dispatch-Home Location Register (D-HLR) and Dispatch-Visitor Location Register (D-VLR) maintain the Urban ID information in its databases.

Fleet ID

The Fleet ID parameter is an identification number assigned to major corporate or municipal subscribers by the service provider. A fleet is comprised of different groups, users, or members and those groups are defined and managed by the HLRs and VLRs of the dispatch subsystem. The Fleet ID parameter is the largest functional unit of a Dispatch call.

Fleet Member ID

The Fleet Member ID parameter is a number assigned by the service provider to uniquely identify an SU as a member of a particular fleet. This parameter is used to identify the originator or target SU during a Private Dispatch call.

Talk Group ID

The Talk Group ID parameter is a number given by the service provider to divide fleets into groups or logical units. The type of fleet and the number of groups in a fleet vary with the requirements of each fleet. Members of the fleet are assigned to different groups based on task, function, organization, or another method. A SU may be part of more than one talk group, and can change the default talk group, as long as the change is allowed in provisioning by the service provider.

Multiple Simultaneous Talk Group ID

An AFU SU is required to support the MST optional feature. The MST feature allows a SU to belong to up to four groups in the same fleet. This optional feature allows a user to monitor and participate with other groups. The user operates a mode switch to change to the associated group from the current selected group. The original group is called the selected group, and the other 3 potential groups are called associated groups. There is only one selected group allowed per mode switch setting. And the capability to select different associated talk-groups for all modes can be toggled on

or off.

iDEN Home Location Register

The Home Location Register of the Dispatch Subsystem is a network element that stores the information regarding the subscriber provisioning and the services that the subscribers are allowed to access. It also stores the ISDN addresses of the serving DAPs corresponding to the SUs in its Urban. Whenever a dispatch or packet data call has to be initiated, the DAP needs to query the iHLR in order to find the destination's current location [15][16].

iDEN Data Access Controller

The iDAC provides the routing of voice for Inter-Urban Dispatch calls across different Urbans. The iDAC communicates with DAPs, APDs and the OMC-R in the same Urban, and with remote iDACs in other Urbans. An iDEN subscriber in one Urban area can make a Dispatch call to another iDEN subscriber in another Urban. When a DAP sets up an Inter-Urban Dispatch call, it specifies the local APD and the remote iDAC to route the voice. When the APD receives voice for a call, it routes the voice to the iDAC. When the voice reaches the remote iDAC, the iDAC converts and sends the voice to its local APD. The following are the functions that iDAC performs in the iDEN system:

- Sends and receives voice and control traffic to APDs and remote iDACs.
- Reports alarms, state changes, and statistics to the OMC-R.
- Maintains performance statistics and uploads the statistics when requested by the OMC-R.

Advanced Packet Duplicator

The APD provides the duplication and routing of voice packets for the iDEN network. When a Dispatch call is initiated, the DAP sends the APD a routing table that

contains all of the targeted subscriber IDs and EBTS sites associated with each mobile subscriber. When a Dispatch voice packet is received, the APD looks up the call ID in the routing table and performs the necessary duplication and routing. The APD after receiving voice packets from one site on a call, duplicates and routes them to the other sites on the call. The APD provides the following functionality in the iDEN network:

- Duplicates and routes voice packets to each site on the call.
- Reports alarm and state information to the OMC-R.
- Provides the MMI (Man Machine Interface) interface to operate and maintain the APD.

iDEN Surveillance Gateway

The iSG of Dispatch subsystem performs almost the same function of SDM/FT of the interconnect subsystem. The iSG provides law enforcement surveillance capability for the iDEN Dispatch and Packet Data subsystems. When provisioning surveillance in the iDEN network, each Urban has one or more pairs of iSG for redundancy. The iSG provides the following functionality in the iDEN network:

- Provides surveillance capability for Dispatch and Packet Data subsystems.
- Retrieves surveillance information and forwards it to the LEA (Law Enforcement Agency).
- Filters dispatch call data streams received from DAPs and APDs, duplicates as necessary, and routes to one or more LEMs (Law Enforcement Monitors).
- Maintains an IMSI listing for surveillance activities.
- Reports alarms, state changes, and statistics to the OMC-R.

Metro Packet Switch

The MPS manipulates the paths used by Dispatch voice packets during a Dispatch call, and the data packet paths used during Packet Data networking. The DAP controls the source and definitions for routing and movement of voice and data packets. The MPS is implemented in a tiered architecture and routes signaling and control information between the DAP, MDG and the EBTS sites. The MPS provides the following functionality in the iDEN network:

- The main function of MPS is to provide interfaces between the DAP, APD, and MDG by performing the necessary conversion of frame relay to IP.
- Controls the overhead and manages the flow of voice and data packets between the Dispatch Network Elements.
- Routes voice and data packets for group Dispatch calls and network multicasts to and from the APDs to the correct destination.

2.1.3 Packet Data Subsystem

Packet data is a non-voice communication service provided by Motorola that helps connect the Mobile Station to any network, may it be Internet, Extranet, VPN, etc. the packet data networking allows the service providers to be a point-of-presence for the Mobile Users to use the Internet.

The following are the network elements that take part in a normal packet data session and call flow:

- **Subscriber Unit (SU):** SU is a network element that will act as a modem when it is connected to the terminal or workstation. This network element is used to directly receive and send the data to and from the network with which it is connected.

- **Enhanced Base Transceiver System (EBTS):** EBTS determines that the particular call is a packet data call and it assigns radio resources to the Mobile Station for that call.

- **Mobile Data Gateway (MDG):** MDG is the main network element of the packet data subsystem. It routes the data packets to and from the network with which the device would be connected be it the Internet or any extranet. MDG also acts as a Foreign Agent (FA) for the mobile IP communication. MDG converts the protocols from iDEN to Internet and vice versa [13][14].

- **Home Agent (HA):** HA routes the data packets to the correct MDG which is serving the Subscriber Unit (SU).

- **Billing Accumulator (BA):** BA keeps the track of the time for which the data transfer took place and also the data rate and the amount of data transfer for billing requirements of the service providers.

2.1.4 Packet Channel Assignment

This subsection describes the organization of how a Packet Channel is assigned to the subscribers and what all Network Elements are involved in this procedure.

PDR

In order to provide packet data services to the users, a geographical location is being assumed known as the PDR or the Packet Data Region. This is a region made up of the cluster of MDGs and their associated sited used to provide services to the user.

MDG

Mobile Data Gateway is the main network element of the packet data subsystem. It manages the subscriber units and does the cluster management without the intervention of the OMC-R. It routes the data packets to and from the SUs. In one PDR

there can be as many MDGs as we want to but due to the limitations of the available IP addresses and the present subnet mask formats a maximum of 4 MDGs can be allowed in one PDR [13][14].

RAG

RAG is the Resource Allocation Group. There are a maximum of 32 RAGs in each packet data region. All mobile subscribers within a regional network are assigned to one of the RAGs. Each RAG is associated with a mobile IP Care of Address. RAG mappings are used to assign a mobile subscriber to a packet channel, to route packets within the packet data region, and to assign mobile subscriber to a serving MDG node.

Each RAG has got the capacity to manage a maximum of 128000 users at a time. There can be a maximum of 32 RAGs in one PDR. All the RAGs are evenly distributed among the available MDGs. If the number of RAGs are more than the MDGs then they need to be distributed among the MDGs in such a way that the difference between the number of RAGs between any two MDG nodes should not exceed more than 1.

PCH

Packet Channels are used to transfer the packet data over the air. Out of the available channels some of the channels can be assigned as PCH to the users. As per SR9.8 onwards versions there can be a maximum of 9 PCH in an omni cell and there can be 3 PCH per sector in a sectored cell.

The available PCH and the RAGs will map with each other. The mapping can be in such a way that more than one RAGs will map itself to one PCH. This mapping is also done so that the load is divided equally among all the PCHs.

Now whenever an SU wants to have a packet data service, it will query the DAP for the same. DAP will find the available MDGs in the SU's home PDR and will

assign one MDG to the SU using the round-robbin method in order to have equal load among all the MDGs.

Once an MDG is selected, the MDG will select on RAG out of the available RAGs with it. The RAGs in turn will find their mapping with the PCHs and will assign the PCH to the users.

One PCH can accommodate more than one SU because the size of PCH can be set as per the requirement as 3:1, 6:1, 12:1 and even 1 which means the PCH can occupy entire BR.

Since one RAG can serve 128000 users and there can be 32 RAGs per PDR, the current capacity of the PDR is 4.096 million users. This capacity has to be double to 8 million users by installing the new feature of 8 Million Packet Data Users in the SR 20.0 phase 2. This feature increases the capacity of the PDR by allowing 64 RAGs per urban and 32 RAGs per MDG (which was 32 RAGs per urban and 4 RAGs per MDG node in SR 20.0 phase 1 and previous releases).

2.2 Next Generation Dispatch

The Next Generation Dispatch Architecture introduced a phased migration with the introduction of feature functionality and enhancements which eventually increased the capacity, performance and management of the system.

The most important feature of the NGD is the introduction of the Highly-Available feature for the NEs. This feature allows the NE to have a high level of redundancy which eventually allows the system to serve the capacity even in the time of outage and the down time can be handsomely reduced. There are a few new NEs introduced in this generation and a few are being discarded as well.

The North-Bound NEs i.e. the NEs from the iVPU and onwards communicate with each other using the high speed Ethernet networks. And this particular generation of iDEN is currently being serving the subscribers and hence the discussion in the following chapters will be based with the NGD as a reference [1].

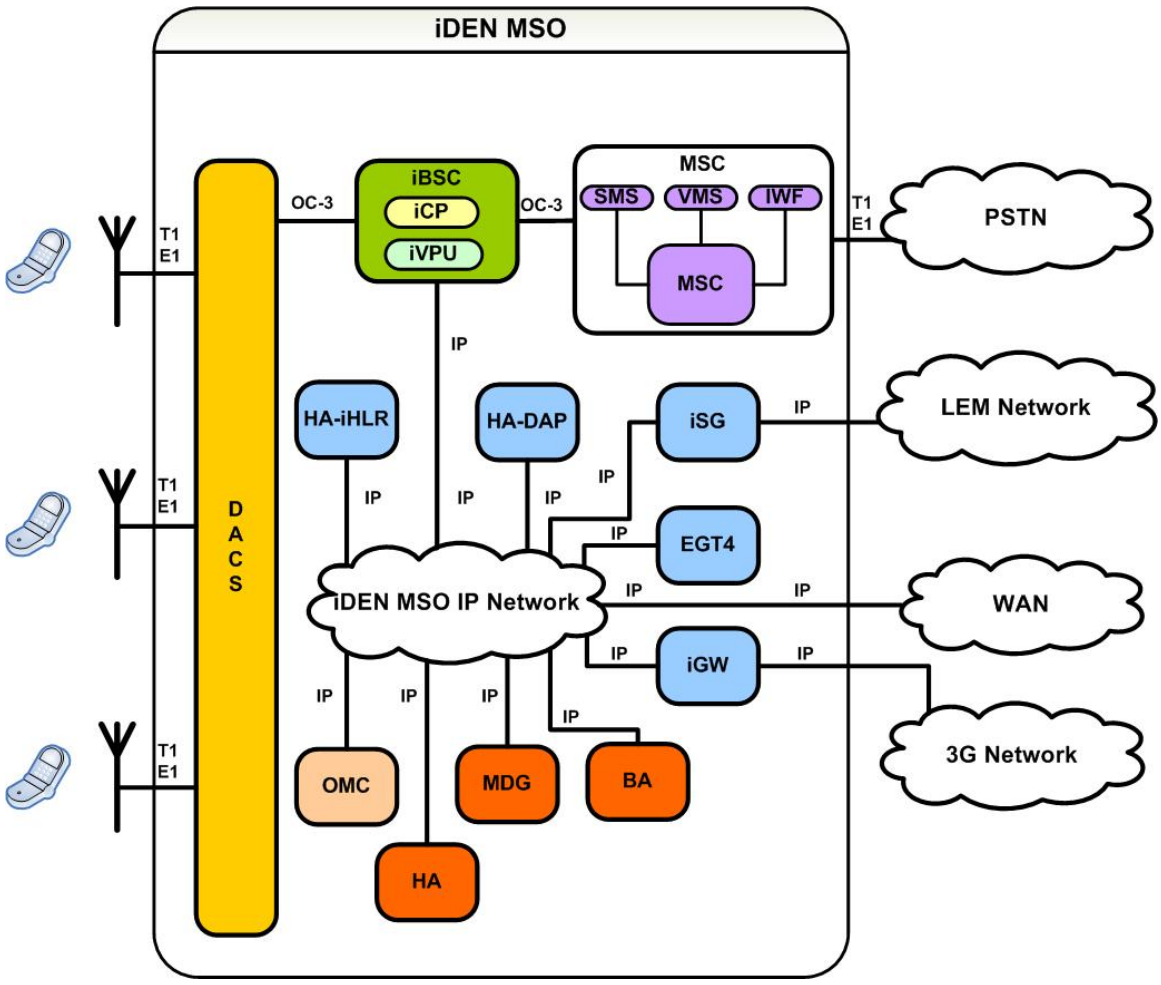


Figure 2.2: Next Generation Dispatch

From the Figure 2.2, it can be said that as the system has progressed into the next generation the distinction between the individual subsystems is slowly diminishing. There are a few network elements that play roles in more than one subsystem like the iVPU. The following are the details of the subsystems in this generation of the iDEN system [1].

2.2.1 Interconnect Subsystem

The Interconnect Subsystem of the NGD contains the following network elements

- Subscriber Unit (SU)
- Enhanced Base Transceiver System (EBTS)
- iDEN Base Station Controller (iBSC)
- Mobile Switching Center (MSC) and its corresponding subnetwork elements

The SU, EBTS, MSC and its supporting subnetwork elements perform the same functions as described in the Legacy iDEN System. The noteworthy difference is the introduction of the iBSC.

iDEN Base Station Controller (iBSC)

The iBSC comprises of two NEs namely iCP (iDEN Call Processor) and the iVPU (iDEN Vocoder/Voice Processing Unit). The iBSC as a unit performs the same funtions as the Legacy BSC used to perform but the internal functions are being divided among the iCP and the iVPU.

The iCP performs the task protocol conversion that is related to the signaling part of the messages. The iDEN network in general uses the SNMP protocol for the Network Management. The signaling protocol of MOBIS for over the air signalling is used in the iDEN portion of the system. MOBIS is Motorola's version of Abis protocol used in the GSM. This modification is being made based upon the difference in the protocols and interfaces used in iDEN that differs from the GSM network. iCP converts this MOBIS messages into the SS7 signaling messages compatible with the further NEs of the Interconnect Subsystem.

The iVPU's job in the Interconnect Subsystem is to convert the VSELP voice packets from the iDEN portion of the network to PCM data compatible with the GSM based MSC. The major fuctionalities of iVPU can be seen in the Dispatch Subsystem more than the Interconnect Subsystem.

2.2.2 Dispatch Subsystem

The following lists the Network Elements of the Dispatch Subsystem of the NGD.

- Subscriber Unit (SU)
- Enhanced Base Transceiver System (EBTS)
- iDEN Base Station Controller (iBSC)
- Highly Available Dispatch Application Processor (HA-DAP)
- Highly Available iDEN Home Location Register (HA-iHLR)
- iDEN Site Controller (iSG)

The Highly Availability feature that is introduced in the NGD is distinctly visible in the names of the NEs that support this feature. The NEs namely SU, EBTS and iSG has got the same functionalities as in the previous generation of iDEN.

The HA-DAP has also got the same functions of overall management of the Dispatch calls. The only difference is that HA-DAP is a bi-nodal NE with two nodes namely the active node and the standby node. At all time the active node will be serving the total capacity of SUs and it will always have a redundant standby node with all the databases replicated and ready to take over the entire capacity of the system in case the active node goes down due to some reason.

HA-iHLR

The Highly Available iDEN Home Location Register (HA-iHLR) is responsible for dispatch authentication, and dispatch and packet data registration in the iDEN network. The HA-iHLR is comprised of two redundant iHLR nodes that provide increased reliability and an active/standby configuration. The active node processes a full load of all mobility, call processing, and provisioning operations, while the standby node is available when needed. The active node contains a standalone database that stores

subscriber information. The subscriber information includes the types of Dispatch calls that the subscribers are provisioned for, fleet assignments, and talkgroup and individual subscriber identification numbers [15][16].

iVPU

iDEN's iVPU supports Dispatch, Interconnect and Packet data subsystem in one way or the another. It is responsible for the audio routing and duplication in the latest version of the dispatch subsystem. The latest versions of the dispatch subsystem are known as the Next Generation Dispatch. In this NGD, the following are the functions of an iVPU in general:

- Performs audio routing and duplication for the NGD.
- Supports the Horizontal Function for Inter Urban calls.
- Interfaces with the HA-DAP and MDGs to provide Dispatch and Packet Data service.
- Manages control links from the HA-DAPs and MDGs.
- Provides pass-through connectivity between the HA-DAP - EBTS, the MDG - EBTS, and the MPS.

From the above mentioned functions it is clear that iVPU performs the functions of protocol conversion of Frame Relay to IP done by MPS. It does the functions of data duplication performed by APD. And also iVPU is capable of routing the voice and data packets to the correct NE that too in the Horizontal Networking which was the function if iDAC previously. Hence, the three NEs namely MPS, APD and iDAC are being replaced by a single NE of iVPU.

The iVPU has got three different kinds of software configurations. These features and benefits are based upon the concepts that the network has one set of hardware and multiple sets of software. The iVPU has following three different kinds of software configurations:

- iVPUi - This kind of software configuration makes the iVPU to work only for the Interconnect portion of the network.
- iVPUd - This software configuration works only for the Dispatch and Packet data portion of the system (i.e. no Interconnect).
- iVPUdi - This software configuration works for all the three subsystems i.e. Interconnect, Dispatch and the Packet Data Subsystem.

The iVPU software load supports the following major functions:

- Interconnect Transcoding
- Dispatch Intra Urban Dispatch Audio Routing and Duplication. Thus iVPU performs the tasks of MPS and APD of the previous versions of Dispatch.
- Dispatch Inter Urban Dispatch Audio Routing and Duplication, thus performing the tasks of iDAC and MPS.
- It also does the function of Frame Relay and IP Inter-working which was the major task done by the MPS.

2.2.3 Packet Data Subsystem

The network elements of the Packet Data Subsystem of NGD and their functions are same as that of the previous generation of iDEN system.

2.3 Melody Based iDEN System

The main difference between the Melody based iDEN system and the other generations of the system is the introduction of a hardware chassis named the Melody Controller Shelf (MCS) [1].

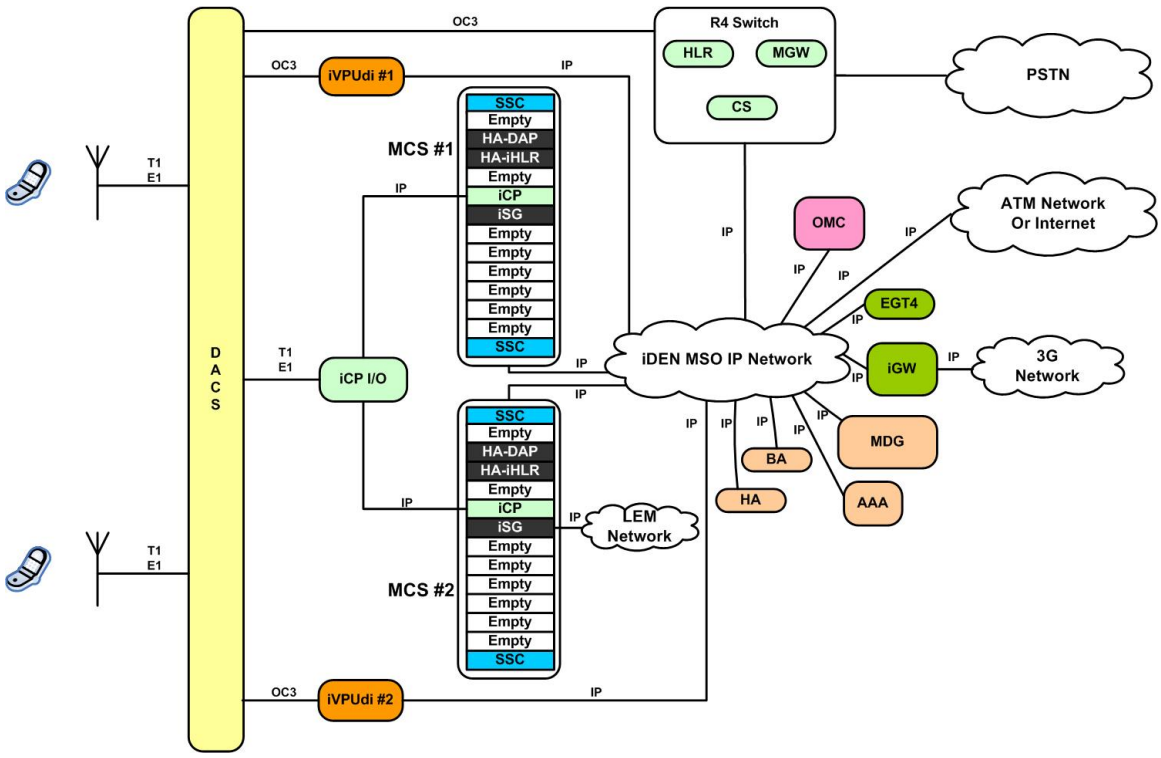


Figure 2.3: Melody Based iDEN System

Melody Controller Shelf

The Melody Controller Shelf (MCS) is an Advanced Telecommunications Computing Architecture (ATCA) based communications server that is specifically designed to address the unique carrier-grade requirements of the telecommunications industry. This particular hardware chassis can act as a network element and also can house up to 14 Payload Processing blades where each blade can be configured to act as a stand-alone network element.

The MCS can house different network elements such as HA-DAP, HA-iHLR, iCP and the iSG. The migration of the NGD to the Melody based iDEN system can lead to even higher scalability and cost effectiveness.

The MCS has been installed in a dual shelf configuration each one uniquely identified by MCS-1 and MCS-2 respectively [1].

Shelf Switch Controller (SSC)

There are two Shelf Switch Controllers per Melody Controller Shelf in active/standby configuration. It is located at the 1st and the 14th slots of the MCS [1]. The following are the features and functionalities of SSC.

- The SSC is considered as a new Network Element all together within the Melody based iDEN System.
- The SSC provides IP interface between the Network Elements configured in the MCS and the rest of the iDEN MSO.
- SSC provides internal IP switching between the NEs in the MCS.
- It also provides a user interface in the form of Local Maintenance Terminal (LMT).

SSC blades are a mated pair that ALWAYS exists in the SAME Melody Controller Shelf. Two SSC blades will exist within each shelf, bringing the overall total to four.

The Shelf Switch Controller (SSC) operates in an active/standby configuration. That is, if the active SSC were to fail, the standby SSC will take over all responsibilities of the failed blade.

However, inter-nodal communication by the SSC is only conducted with its mate in the SAME shelf.

This means that switchover of an Active SSC will only transfer control to its mate residing within the SAME shelf.

2.3.1 Interconnect Subsystem

The Interconnect subsystem here, is comprised of the following network elements.

- iBSC - iBSC, here, is not a separate entity. But iCP and iVPU combinely acts as iBSC.

- iCP - iCP does the same functions as in the case of the previous versions. iCP has a redundancy with its redundant node present on the other MCS.
- iVPU - iVPU also does the same job as it did for the previous versions.
- iCP I/O - This particular entity is required to terminate the SNMP and the SS7 message links. Since the MCS talks to the rest of the MSO through IP, the protocols need to be converted into IP before forwarding the messages to the iCP.
- Nortel R4 Switch - This particular switch is an IP based ATCA switch which is used to route and switch the data packets to the PSTN. It consists subsections named, HLR, Call Server (CS) and Media Gateway.
  - HLR is the central database where every SU's permanent Interconnect records are stored. These records may comprise of MS IDs, IMSIs and the ISDNs.
  - The Call Server (CS) provides the Interconnect call control functions such as setting-up, maintaining, and tearing down Interconnect calls.
  - The Media Gateway (MGW) provides the voice and data path between the Melody-based iDEN System and other telecommunications networks such as Public Switched Telephone Network (PSTN).

2.3.2 Dispatch Subsystem

The Dispatch subsystem of Melody based iDEN System comprises of iVPUdi, HA-DAP, HA-iHLR, iSG and Enhanced Global Title Translation Table Tool (EGT4).

Out of these NEs, iVPUdi, HA-DAP, HA-iHLR and iSG does the same job as in the previous versions. HA-DAP, HA-iHLR and iSG has got redundancy with their redundant node present in the other MCS.

It is good to note that the capacity of HA-DAP in this version is almost three times less than HA-DAP of NGD. But at the same time the space occupied by Melody

DAP as compared to HA-DAP of NGD is drastically reduced and since there are several empty slots available in the MCS, more slots can be configured to act as DAP and hence the capacity of the Urban can be increased with a very little space to compromise. This is the major reason and motivation for the development of the Melody based iDEN System.

EGT4 was also used in the previous versions. The following subsection describes its functions.

EGT4

The Enhanced Global Title Translation Tool (EGT4) is a centrally located workstation that supplies information about ALL iVPUdi's, HA-DAPs, and HAiHLRs to ALL iVPUdi's, HA-DAPs, and HA-iHLRs in the Urban/HN1C network [17].

This allows communication between the Network Elements as well as making possible Horizontal Networking or Dispatch Roaming (Urban-to-Urban Dispatch Communication).

2.3.3 Packet Data Subsystem

The Packet Data Subsystem includes MDG4, HA, BA and AAA which performs the same functionsas the previous versions.

2.4 Summary

This chapter explains about the evolution of the iDEN system and its corresponding changes in each stage of evolution. The chapter also gives the details regarding each and every Network Element and their functionalities.

Chapter 3

System Interfaces

This chapter includes the detailed description regarding the interfaces and the protocols that are being used in the different layers of each and every link.

The details shown in the Figure 3.1 reveals the protocols that are being used in the iDEN system. The following are the major interfaces in the system.

- RF interface between the Mobile Station (MS) and the Access Control Gateway (ACG)/Base Radio (BR) of the Enhanced Base Transceiver System (EBTS).
- T1/E1 interface between the ACG and the Digital Access Cross-connect Switch (DACS).
- The optical communication between the DACS and the iDEN Vocoder/Voice Processing Unit (iVPU).
- The Ethernet interface between the northbound Network Elements.
- And an important interface between the Dispatch Visited Location Register (D-VLR) present in the Dispatch Application Processor (DAP) and the iDEN Home Location Register (iHLR).

The following subsections present a brief introduction regarding each of the above mentioned interfaces.

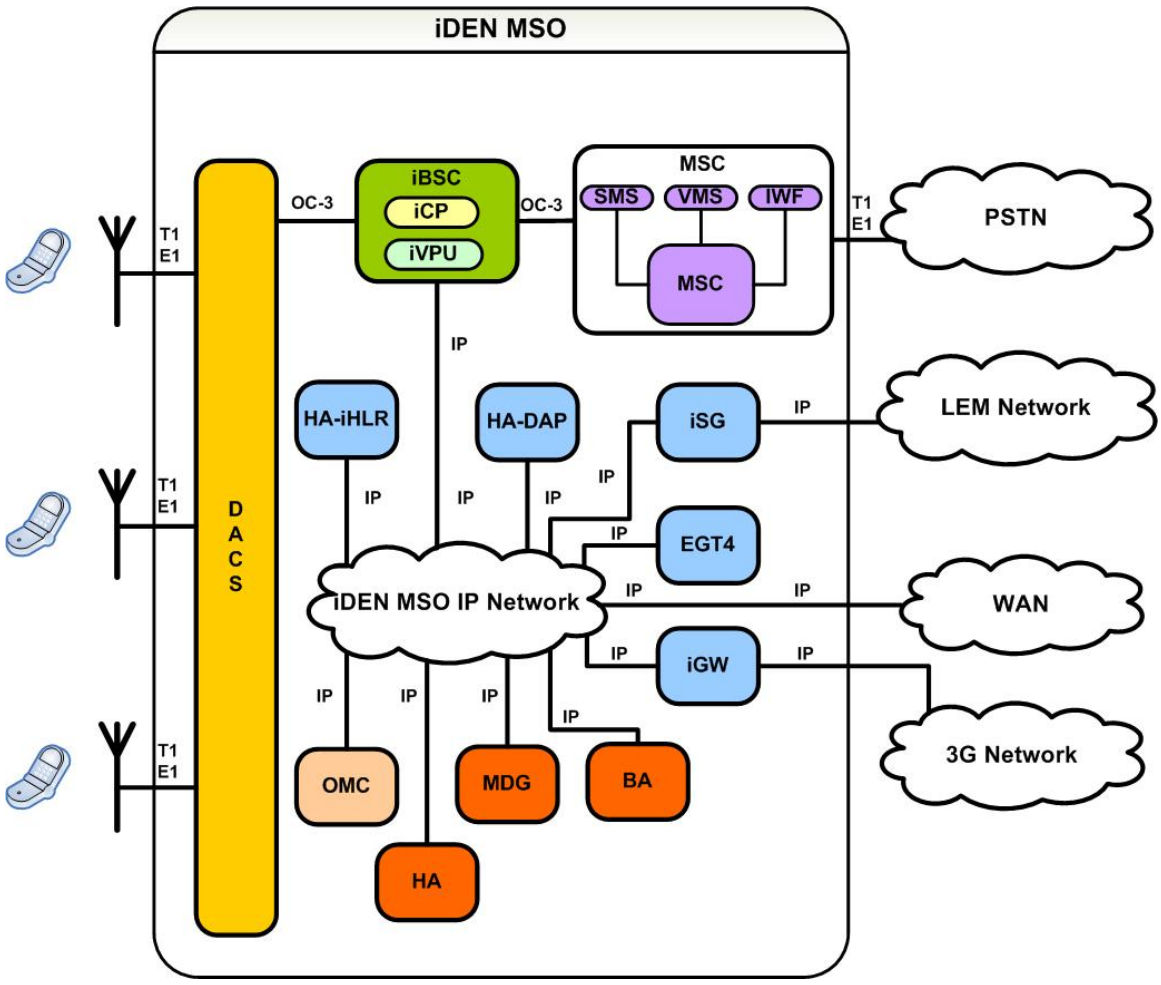


Figure 3.1: Next Generation Dispatch based iDEN System

3.1 RF Interfaces

This section describes the protocols used for the over-the-air interfaces.

3.1.1 Physical Layer

The first layer of the RF interface is the physical layer and the digital data is modulated using the modulation technique of Multiple carrier 16 Quadrature Amplitude Modulation technique [20].

In a 16 QAM signal, there are 16 points in the constellation. Each point represents

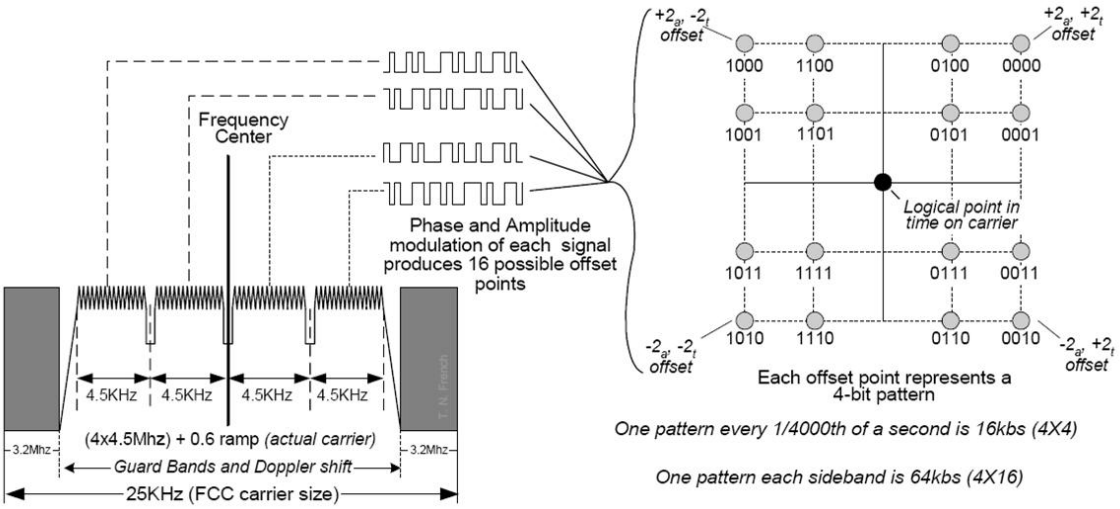


Figure 3.2: RF Interface: Multiple Carrier 16-QAM [20]

a symbol of 4 bits. Now the symbol rate at which the symbol is transmitted is 4000 symbols per second. Hence the data rate will be 16000 bits per second. Now to further enhance the data rate, the complete carrier is not used but the entire carrier is divided into 4 sub-carriers as shown in the Figure 3.2. Each sub-carrier now has the capacity of transmitting at the rate of 16000 bits per second which gives us a total bit rate of 64Kbps. This is the basic concept of Multiple Carrier 16 QAM that 4 sub-carriers each having 16 QAM modulated signals at different frequencies are Frequency Division Multiplexed to form the original big carrier. This approach is used to reduce the adjacent channel interference and power management which eventually enhances the overall data rate of transmission.

The power management can be done in such a way that in a situation when the channel is noisy and the data requires more power to be transmitted, at that time instead of using all the 4 sub-channels only one sub-channel can be used with all the power allotted to only one sub-channel which will allow reliable transmission even in the noisy communication channel.

This particular approach is ideal for the Mobile Stations because the MSs are

battery operated and such power saving techniques can save much power [20].

3.1.2 Link Layer

The procedures of the layer 2 of the RF interface are used for the transmission of the layer 3 messages. There are two major procedures namely, Random Access Procedure and the Associated Control Procedure [21].

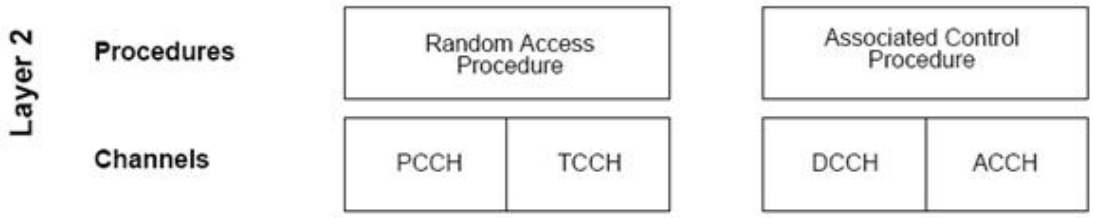


Figure 3.3: RF Interface: Layer 2 [21]

The RAP supports unreliable transmission of short fixed-length messages using the Primary Control Channels (PCCH) and the Temporary Control Channels (TCCH).

The ACP supports reliable point-to-point transmission of arbitrary-length messages using Dedicated Control Channels (DCCH) and the Associated Control Channels (ACCH).

Primary Control Channel

The PCCH is used to transfer important call control and mobility management information between the SU and the EBTS. The system uses the PCCH to contact the SU and the SU uses the PCCH to measure the signal quality and stay in contact with the system. There are 3 types of PCCH.

a. **Broadcast Control Channel (BCCH):** Refers to the outbound part of the primary control channel (PCCH). Carries cell parameters and other system

information.

b. **Common Control Channel (CCCH):** Refers to the outbound part of the PCCH. Transmits channel assignments, pages, etc. to the MS population.

c. **Random Access Channel (RACH):** Refers to the inbound part of the PCCH. Used by MSs to obtain access to the system.

Temporary Control Channel

TCCH provides for inbound random access to support functions such as channel re-assignment and handover access.

Dedicated Control Channel

DCCH is used to maintain constant control contact with the SU.

Associated Control Channel

ACCH is used for the imbedded signaling needs during an active interconnect voice call. It is used for the handovers and allows the SMS delivery of text messages.

3.1.3 Network Layer

Layer 3 is divided into three sublayers:

Radio Resource Management (RR) sublayer - Responsible for control of Layer 1 and Layer 2. Provides connection management for the MM-sublayer. To do so, it controls various RF-specific functions such as cell selection, channel allocation, and handover.

Mobility Management (MM) sublayer - Responsible for registration, location reporting, and security. Also provides connection management for the CM-sublayer.

Connections Management (CM) sublayer - Provides the interface to the next higher layer. Entities in this sublayer provide support for circuit-switched calls,

supplementary services, short message service, dispatch calls, and message alert.

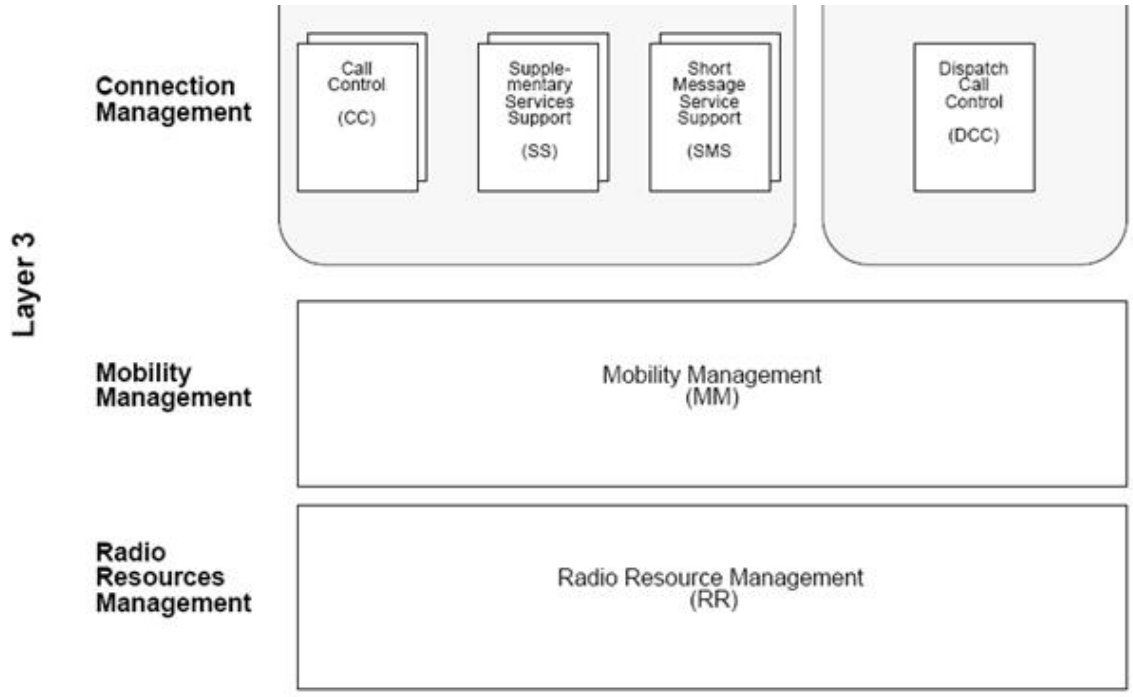


Figure 3.4: RF Interface: Layer 3 [22]

The CM sub-layer is populated by a set of protocol entities, each responsible for specific Layer 3 operations. The functions performed by these entities are generally divided into telephone and dispatch services.

The Call Control (CC) entity controls establishment, maintenance, and release of circuit-switched connections for telephone and data. It also provides for call-related supplementary services.

The Supplementary Services Support (SS) entity provides for call-independent supplementary services.

The Short Message Service Support (SMS) entity provides for transfer of short messages over the RF interface.

The Dispatch Call Control (DCC) entity controls establishment, maintenance, and release of dispatch calls (although, for reasons of efficiency, most of the signaling

for dispatch calls is done by the RR sub-layer) [22].

3.1.4 Application Layer

The application layer will contain the messages related to the connection management and the messages related to the interconnect, dispatch and packet data call processes.

3.2 ACG-DACS Link

The link between the ACG and the DACS is used to transmit voice, data, and control and network management messages necessary to provide communication services to the DACS.

Out of the 7 layers of the OSI model, this particular link has got 4 layers namely the physical layer, data link layer, network layer and the application layer i.e. layers 1,2,3 and 7 [23][24][25][29].

3.2.1 Physical Layer

The layer 1 of this link is the T1/E1 link. T1 is the standard used in the US and some other parts of the world. Rest of all the countries in the world including India uses E1 as a replacement to this T1 standard. The only difference between the two standards is the number of channels multiplexed and hence the bandwidth allowed using these protocols.

T1

To improve signal/noise ratio on multi-line phone trunks, Bell began converting some frequency division multiplexing (FDM) lines to time division multiplexing (TDM) back in the 1960's.

The digitization technique chosen was pulse code modulation (PCM), taking 8000 samples/second of the analog waveform and quantizing it to 8 bit precision with an

analog to digital (A/D) converter. When the bits are serially shifted out, the signal source is called a "DS0" by the phone company.

Including several DS0 channels in one TDM bit stream requires the addition of framing bits, so the individual channels can be identified on recovery. A "DS1" is composed of 24 byte-wise interleaved 8-bit samples (from 24 different DS0's) and one framing bit. The total bit rate is:

total rate = 8000 samples/sec * [(8 bits/sample * 24 samples) + 1 frame bit] = 1.544 Mbps

T1 is a channel that multiplexes 24 channels into one channel while E1 multiplexes 32 channels.

Split Backhaul and All Frame Relay Details

The Next Generation Dispatch (NGD) provides higher capacity and greater system reliability in a significantly smaller footprint. It is characterized by All Frame Relay (AFR), split backhaul, or a combination of configurations.

The T1/E1 link for Split Backhaul

The T1/E1 link is used to transport the system information, call control, coded voice and data traffic to and from the EBTS sites and the MSO. DS0s are used for interconnect, dispatch and packet data in accordance with the expected traffic requirements.

Subrate trunking refers to the process of multiplexing a DS0 into four 16 Kbps circuits. This technique is used to multiplex upto four interconnect conversations into one 64 Kbps timeslot (DS0).

Time slots allocated for Dispatch/Packet Data and Interconnect can be dynamically allocated. A typical T1 or E1 setup uses:

- One DS0 for Interconnect call setup and tear down (MOBIS).
- One DS0 for Operation and Maintenance Link (OML)

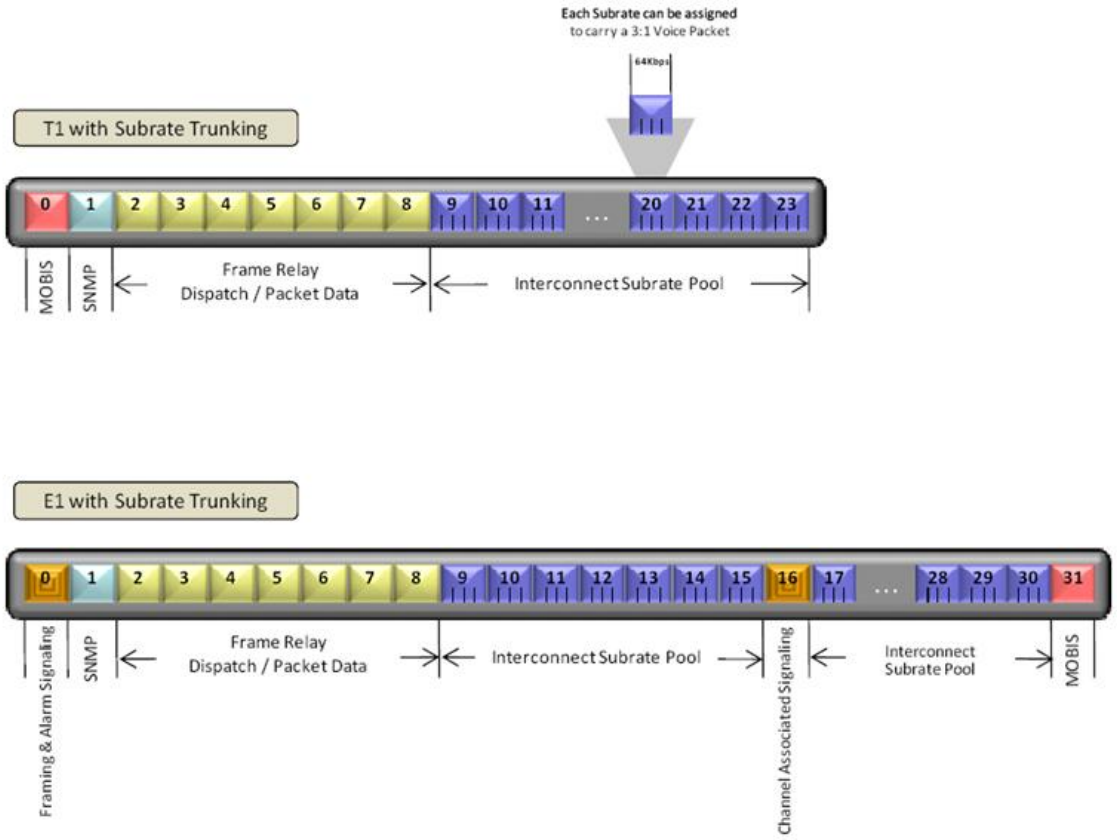


Figure 3.5: The T1/E1 link for Split Backhaul [24]

- One or more DS0s for Dispatch and Packet Data (Frame Relay)
- One or more DS0s for Interconnect and Circuit Data (VSELP)

All Frame Relay

Frame relay provides a packet switching technology used across the interface between the EBTS sites and the MSO. Frame relay provides a means for multiplexing many logical data packets over a single physical transmission link.

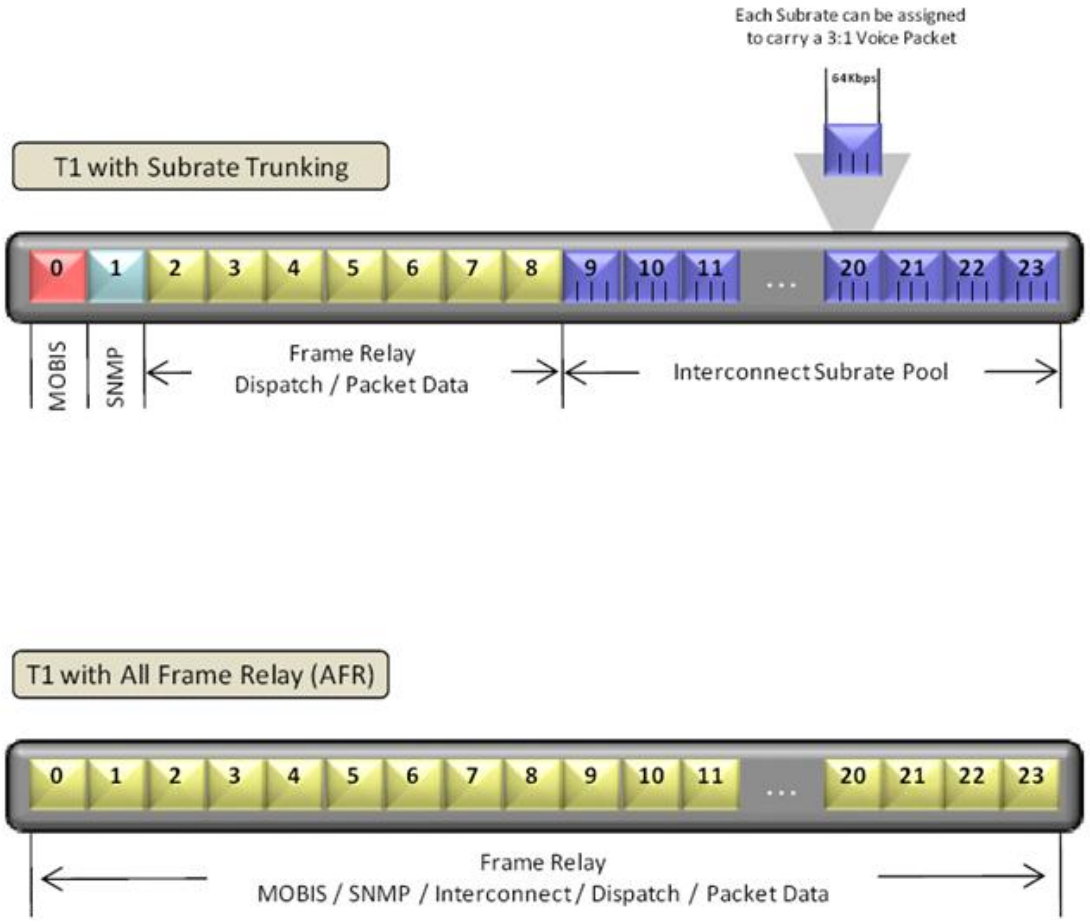


Figure 3.6: All Frame Relay [24]

T1 Link - Split Backhaul

The Digital Cross-connect Switch separates and re-aggregates as shown in the diagram

- MOBIS and SNMP channels terminates on an iCP
- Interconnect voice traffic terminates on the iVPUdi
- The Frame Relay traffic terminates on the iVPUdi

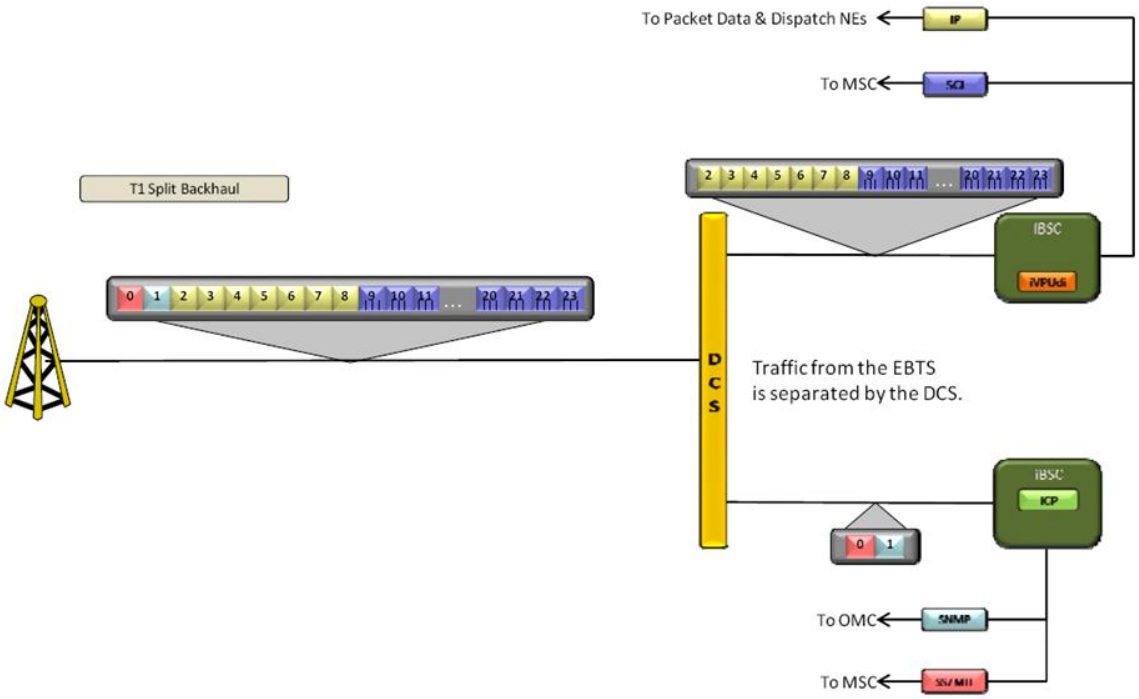


Figure 3.7: T1 Link - Split Backhaul [24]

T1 Link - All Frame Relay (AFR)

In All Frame Relay Mode, the EBTS supports combining all communication links onto a single frame relay pipe (superchannel). Or to put it in another way, a single frame relay channel carries all traffic: Dispatch, Packet Data, MOBIS, SNMP and Interconnect.

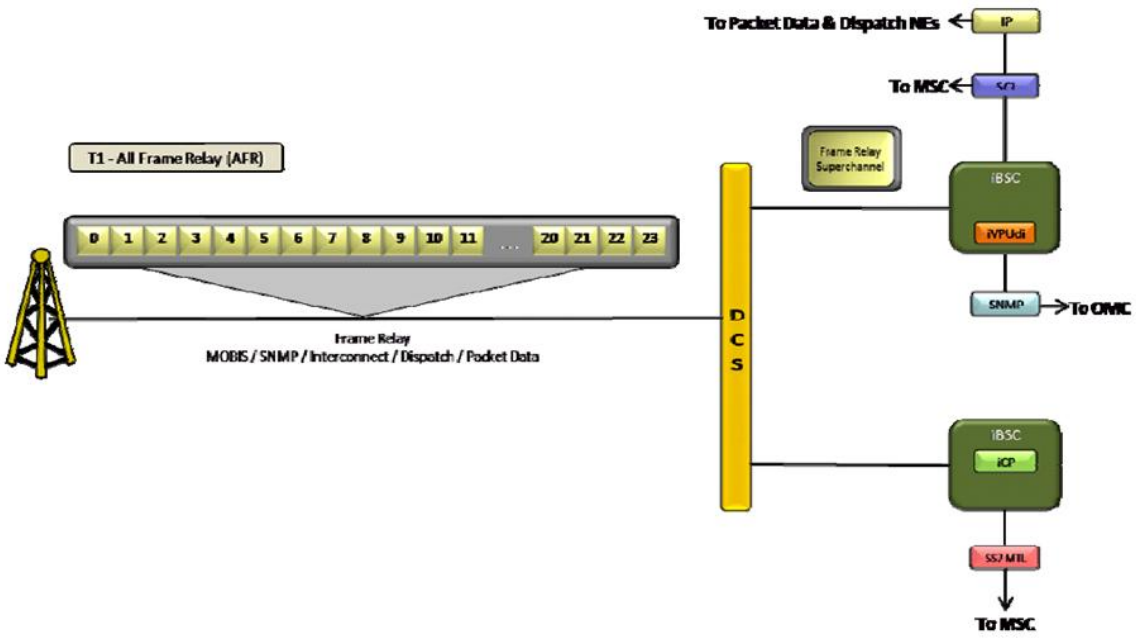


Figure 3.8: T1 Link - All Frame Relay (AFR) [24]

E1 Link - Split Backhaul

There is no such difference between the T1 and E1 links when employing Split Backhaul. The DCS will separate and re-aggregate the channels as shown in the figure.

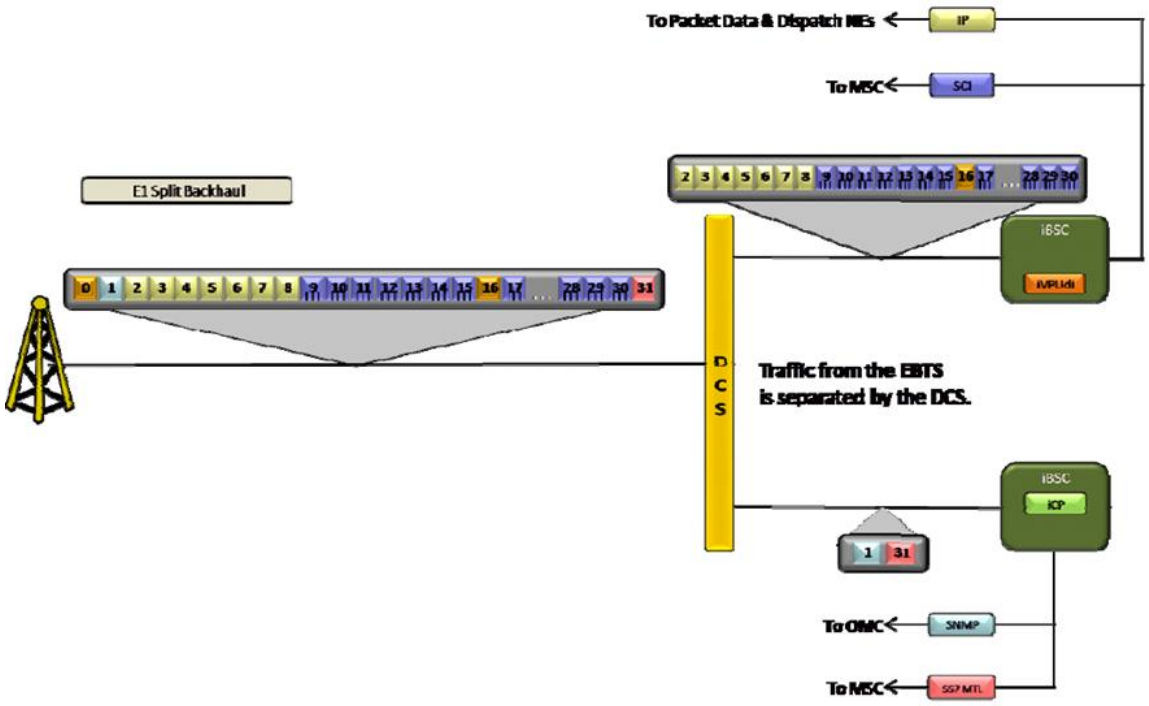


Figure 3.9: E1 Link - Split Backhaul [24]

E1 Link - All Frame relay (AFR)

The E1 All Frame Relay (AFR) link is again similar to that of the T1 AFR link.

3.2.2 Link Layer

This particular link of the network is the backhaul portion of the network and it holds a key position as it connects the cell sites i.e. the EBTS and the MSO in the field. There are two types of backhaul formats used in iDEN network namely split backhaul and All Frame Relay.

In the split backhaul network, the dispatch traffic is being routed using the frame relay protocol at the data link layer while the interconnect traffic follows the circuit switched protocols. In the AFR, all the traffic irrespective of its kind, i.e. voice, data or control are being transmitted using the frame relay protocols at the data link

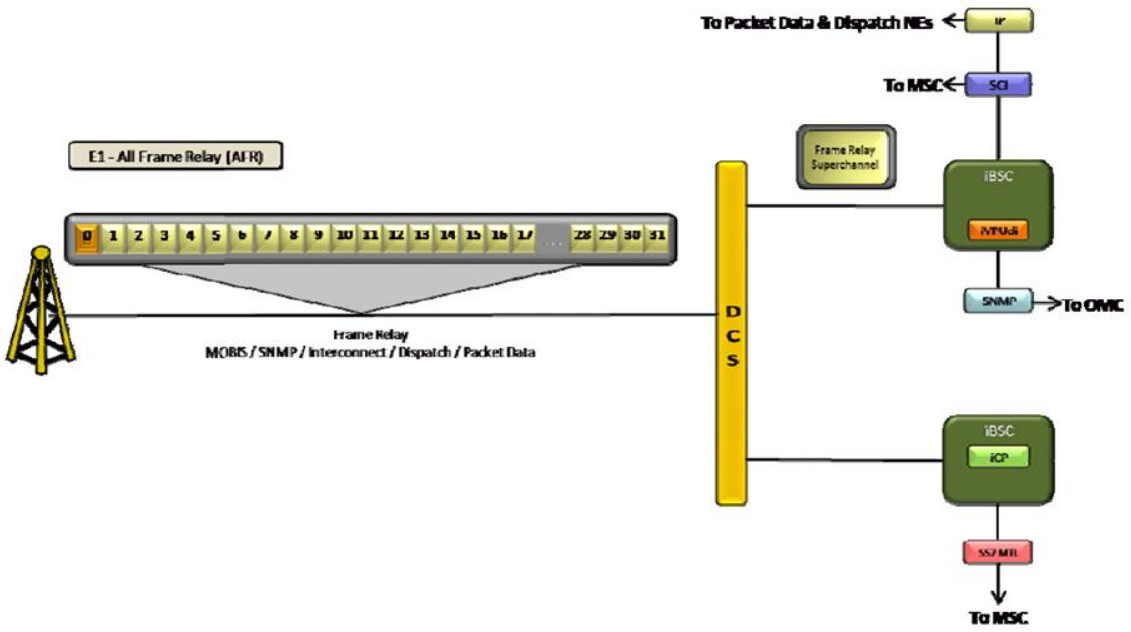


Figure 3.10: E1 Link - All Frame relay (AFR) [24]

layers.

Hence, the data link layers of this link consists of two protocols namely Frame relay and the Link Access Protocol for D channels used in ISDN. The details regarding Frame Relay and LAP-D can be found in the section B.1 and section B.2 respectively.

3.2.3 Network Layer

In GSM protocol stack, the call processing activities between the BTS and the BSC and their corresponding messages are defined by an interface called the "A-bis interface". In the iDEN system as well there is an important link between the ACG (which is a part of the EBTS) and the BSC. Now, since the protocols and the interfaces in iDEN system are different from that of the GSM protocol stack, Motorola has introduced its own version of A-bis interface named MOBIS for Motorola defined A-bis. Major portion of the protocol stack of MOBIS resembles that of the A-bis protocol and many message names are also common but the content of the messages

might be different for the iDEN system and a few new set of messages are also being introduced in MOBIS protocol stack.

The MOBIS protocol lies in the third layer of the ACG-BSC interface with the ITC header below it in the same layer containing the information regarding the routing tables. The major function of the MOBIS protocol is to handle the call processing and signaling for the interconnect portion of the iDEN system. It manages several processes like

- Paging processes
- Channel assignment processes
- Handover processes
- Audit processes

3.2.4 Application Layer

Finally at the application layer the messages are SNMP, MOBIS, Data and voice. The details regarding the SNMP protocol can be found in the section B.3.

3.3 DACS-iVPU Link

The interface between the DACS and the iVPU is the optical interface. The physical layer of the link is the OC3 connection while the link layer is a combination of frame relay and LAP-D protocol. The application layer contains the messages that are being exchanged between the DACS and the iVPU [26].

3.3.1 OC3

OC3 is the third degree of the optical carrier which is devoted to provide fast and reliable network connection. It runs on the standards set by SONET or Synchronous

Optical Network. An optical carrier has got an initial rate of 51.84 Mbps. And hence OC3 will be having the data rate of as high as 155.52 Mbps.

3.4 Northbound Interfces

The connections of the other network elements with the iVPU are through the high speed Ethernet of 1000T. The following are the protocols at each layers of the OSI model [27][28][29][30].

Application layer: this layer contains the corresponding messages between the two network elements.

Transport layer: this layer uses the TCP/UDP for connection oriented and reliable/connectionless transmission

Network layer: this layer uses the IP protocol

Data link and physical layer: these two layers use the Ethernet standards.

3.5 DAP (D-VLR)-iHLR Link

The interface between the DAP and the iHLR is a modified version of SS7 signaling protocol used for the telephone communications [31]. The following is a brief introduction of SS7 signaling.

Figure 3.11 shows a typical HLR connected to a VLR using MAP/SS7. Supporting a full SS7 stack on the DAP and iHLR platforms would have required porting of the MTP layer, including associated I/O controllers. Due in part to the high cost and schedule impact of this porting effort, as well as the ongoing maintenance burden on an obsolete platform, a decision was made not to use a complete SS7 stack. Instead, iDEN DAP-HLR communications will use TCP/IP in place of MTP and SCCP.

MAP (Mobile Application Part) is used to communicate between HLR's, VLR's, and MSC's. It has functionality for mobility management, provisioning, and authentication. Source and destination "addresses" at the MAP level are called Global Titles.

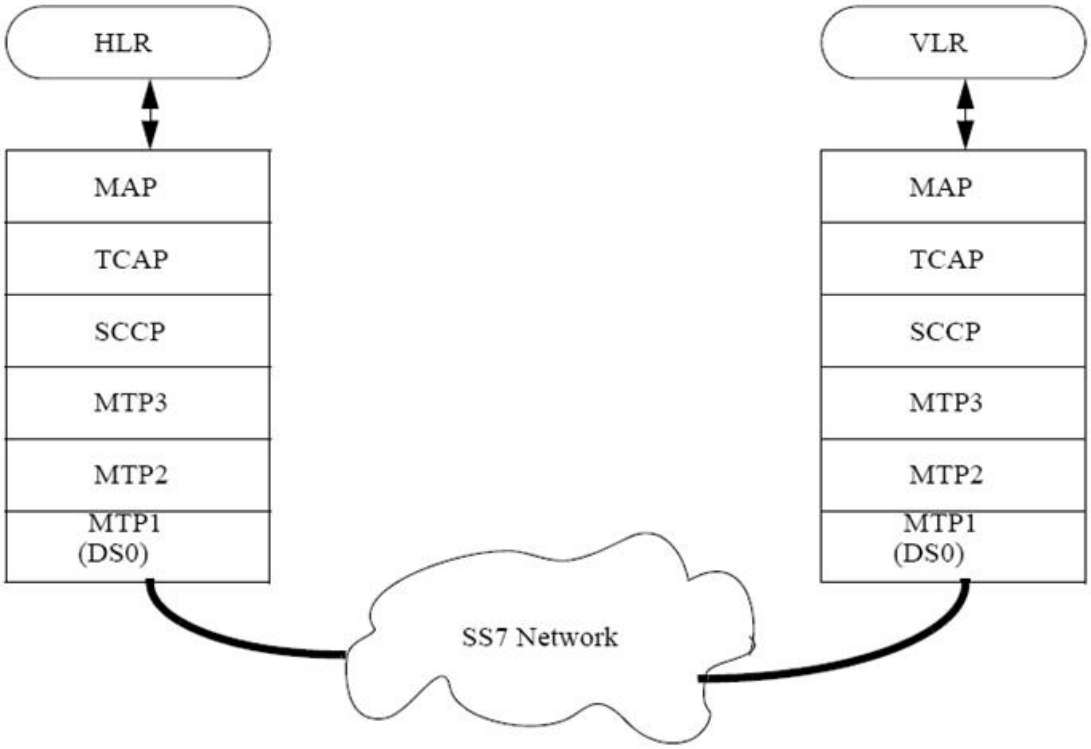


Figure 3.11: SS7 Protocol Stack [31]

They take many forms (such as 800 numbers), but DAP to iDEN HLR communications require IMSIs, ISDN addresses, and urban/fleet ids. IMSIs, urban/fleet ids, or ISDN addresses to identify HLRs, and just ISDN addresses to identify VLR's.

TCAP (Transaction Capabilities Application Part) provides an application such as MAP with the ability to conduct multiple simultaneous dialogs with a remote entity. Four distinct classes of service are available, which are differentiated by their level of reporting the outcome of operations to the requesting application. These range from Class 4 where neither success nor failure is reported, to Class 1, where both are reported. Communications are conducted using query/response exchanges using structured dialogs.

SCCP (Session Control Capabilities Part) provides routing and fault management. It keeps track of which destinations are reachable, and is able to route to an alternate

destination (if available) should the primary one becomes disabled. In performing this function, it translates a Global Title (GT-such as an ISDN address or an IMSI) to a point code, which identifies a destination SS7 network entity (each "box" in an SS7 network has one or more point codes assigned to it). Note that while an ISDN address has a direct mapping to a point code, many IMSIs (possibly in the hundreds of thousands) could map to a single point code. The point code that results from the GT translation (GTT) may not be the final destination of the message, it may only be an incremental step, so that another GTT would be done at this point code to refine the route further.

MTP3 (Message Transfer Part 3) provides link-level maintenance and routing. When a link fails, MTP3 takes it out of service and routes traffic around the failure while an attempt is made to automatically correct the problem. It only concerns itself with the next hop in the path to the destination, so this routing must be done at each node that the message traverses. If requested by the initiating user, packet sequencing is retained across each link. In the event of link failure, however, the sequence may be lost due to the messages traversing different links.

MTP2 provides the framing of messages across the physical link using HDLC (including CRC). It also provides link-level reliability by continuously testing link robustness and ensuring that each message transits the link without error. Because MAP is used with connectionless TCAP and SCCP, the link-level reliability provided by MTP2 is the only insurance that messages will successfully transit the network (there is no end-to-end reliability).

MTP1 provides the raw communication channel between adjacent nodes. It is responsible for aspects of data transfer related to the physical channel, such as bit synchronization.

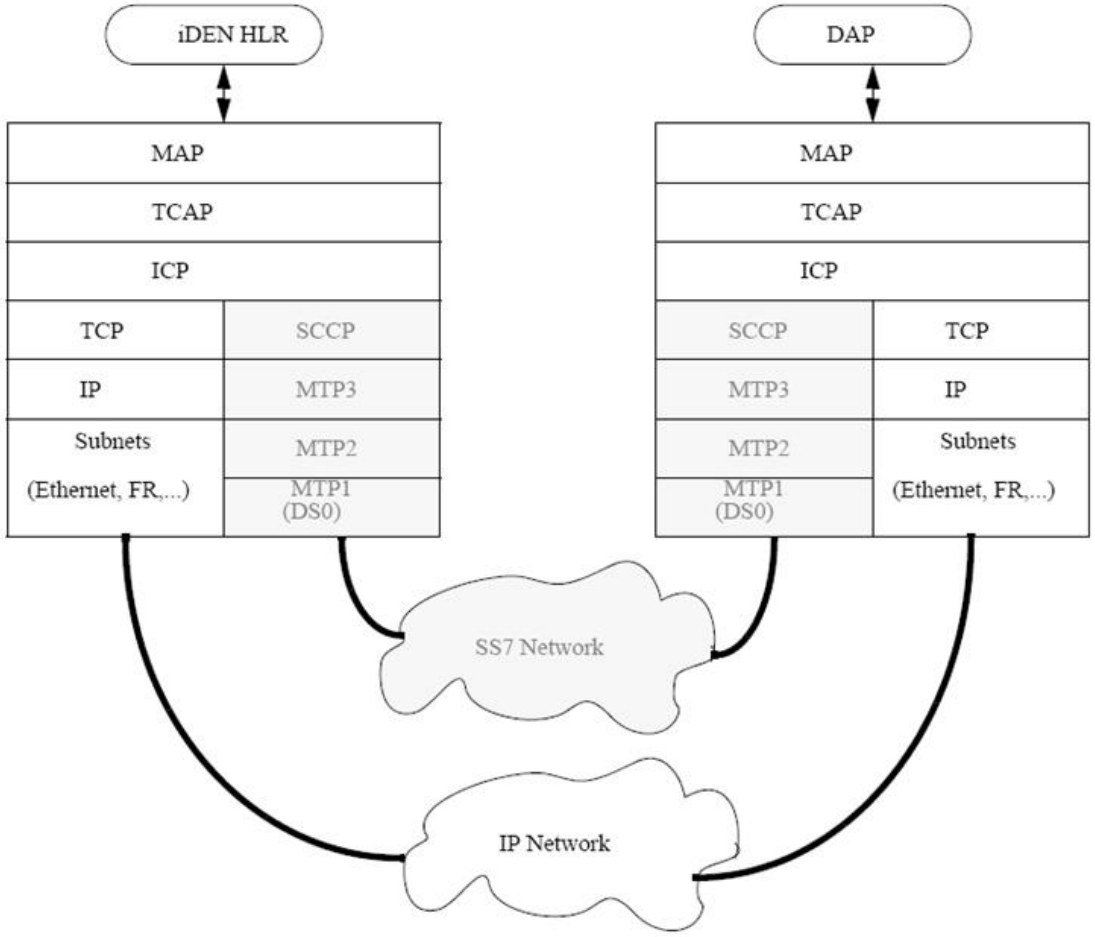


Figure 3.12: Hybrid Stack [31]

3.5.1 Hybrid MAP/TCAP/TCP/IP Stack

Figure 3.12 shows the communications protocol layering between the iDEN HLR and the DAP. The grayed areas of the diagram (depicting the lower layers of SS7) are shown in this diagram to clarify the eventual migration path to full SS7. This is because it may be necessary to communicate with SS7-only devices in the future, so the current solution must be upgradeable to support both SS7 and TCP/IP networks simultaneously.

The MAP layer deviates from GSM in several ways. First, MAP messages used in iDEN HLR communication will use a non-GSM application context and version.

Second, some of the messages will differ somewhat in structure from standard GSM messages due to differences in iDEN and GSM Packet Data implementations. Third, new MAP-like messages have been invented to handle iDEN's implementation of dispatch.

The TCAP layer will be standard ITU in the hybrid stack and, thus, requires no modification to support the DAP-HLR interface.

ICP (Internet Convergence Part) is an iDEN-specific layer designed to support MAP/TCAP over TCP/IP. It provides global title translation based on the IMSI/ISDN address / urban and fleet ids provided by the MAP user. The end result of the GTT is an IP address and port rather than a point code. This address is then used to identify a TCP connection over which to send the message. Should full SS7 be implemented in the future, a GTT for a device connected via SS7 would result in an indication that the message should be passed transparently to SCCP for transmission across the SS7 network (the upper service interface of ICP is by necessity the same as the upper service interface of SCCP, since they must both connect to TCAP).

TCP provides a sequenced, reliable facility between a source and destination. In this way, it is similar to MTP (2 and 3). However, TCP provides this service end-to-end, while MTP only provides it on a per-link basis. This makes the end-to-end reliability of TCP very high. The minus is that lost packets must be resent across the entire network, whereas with MTP they are resent only across the link. This requires that TCP networks be properly engineered for the maximum latency allowable of iDEN HLR communications. ICP will communicate with TCP via sockets. No modifications have been made to TCP for this protocol stack

IP is an unreliable network layer protocol that supports end-to-end addressing. Unlike the GTT of SS7, which may occur multiple times while a message transits the network, address determination in an IP network occurs at the source node. Once the IP address of the destination is determined, all nodes in the network route based on that address. IP addresses are 4 bytes in length, and are written and read by humans in a format known as "dotted decimal". Each byte is written in decimal,

and each byte is separated by a period. For example, the IP address given in hex as 0x0a0b0c0d would be written in dotted decimal as "10.11.12.13". No modifications have been made to IP for this protocol stack.

The data link layer for IP varies widely, consisting of various local and wide area network technologies such as Ethernet, FDDI, Frame Relay, SMDS, HPPI, HDLC, and X.25 (Although X.25 is considered a network level protocol, IP treats it as a data link protocol). As a message transits an IP network, it may encounter different technologies on each link it traverses. While the particular subnets used during iDEN HLR communications is not a concern in this document, it is expected that the platforms that the iDEN HLR and the DAP reside on will interface to the IP network using Ethernet. No modifications have been made to the datalink layer for this protocol stack.

3.5.2 Global Title Translation

iDEN MAP Address Structures

iDEN MAP uses three address formats in order to address HLRs and VLRs. These structures are IMSIs, iDEN ISDN-like Addresses, and urban/fleet ids.

IMSI

IMSIs are used to uniquely identify a subscriber, but a portion of the IMSI also identifies the HLR in which that subscriber's record is stored. IMSIs are used to identify a HLR when the DAP's D-VLR

- requests authentication sets (Send Authentication Information)
- requests a registering subscriber's D-VLR (Get Serving D-VLR)
- informs the HLR of a subscriber's location (Update Location)

ISDN

ISDN structures are used to identify DAPs and iDEN HLRs. Each DAP has its own ISDN and is referred to as the VLR Address; each iDEN HLR also has its own ISDN and is referred to as the HLR Address or HLR Number. A VLR Address is used to route messages when the iDEN HLR resets and when it provides the DAPs with subscriber data. A HLR Address is used to route messages after a DAP reset.

Urban and Fleet Ids

Urban IDs belong to the Highest Tier of UFMI Numbering Plan. An Urban ID, Fleet ID, and Member ID is entered by the operator at provisioning time to uniquely identify a particular Mobile Station. A UFMI is unambiguous and globally unique. A UFMI is made of three distinct values: an Urban ID, a Fleet ID, and a Member ID. The Urban ID/Fleet ID pair make up the unique identifier for each fleet in the HN. In order to facilitate split fleet data checking, the EGT4 will capture UFMI ranges by having the operator enter the Urban ID and Fleet IDs as separate 7-digit values.

3.5.3 TCP / IP Address Structures

This section describes their use in iDEN HLR communications.

IP Addresses and Port Numbers

The TCP / IP Addresses for the HLR and / or VLR's platform must be specified by a craftperson.

A Port Number identifies an application, so for this interface, one Port Number shall represent the HLR application and one shall represent the VLR. This value shall be defined by the service providers.

TCP uses local and remote IP Addresses and Port Numbers to establish a connection to a network entity when one doesn't currently exist. Establishment of a connection results in a socket number, which is then used to route messages.

Sockets

When a message must be delivered via IP between the iDEN HLR and the DAP, a socket is the address structure that is specified. A socket is an integer that is used to identify to an application the destination node's hardware platform and HLR or DAP application. In this DAP-HLR interface, after a TCP / IP connection is established between an iDEN HLR and DAP, the iDEN HLR uses its socket number to identify the connection to the DAP. Likewise, the DAP uses its socket number to identify the connection to the iDEN HLR.

Socket numbers are values that the application software understands ("application" is defined as iDEN HLR or DAP), but not the outside world. More specifically, a craftperson of the iDEN HLR or DAP shall not be cognizant of sockets.

3.5.4 Global Titling

After reading the above, the following should be evident:

- An IMSI associates with a specific iDEN HLR
- A VLR Address identifies a specific DAP
- A HLR Address (Number) identifies a specific iDEN HLR
- VLR Addresses and HLR Addresses are represented by ISDNs.
- IP Address and Port Numbers are used to identify a particular hardware box and its application when a connection is not established between an iDEN HLR and DAP
- Socket Numbers are used to identify a particular hardware box and its application (HLR or DAP) when a connection is established between an iDEN HLR and DAP

Given the above, the remaining must be specified:

- How are the MAP address structures converted to the TCP/IP Address structures?
- How does the craftperson enter this information?

These questions are answered by global titling, and this section begins with a logical description of the actual global titling translation process. This is followed by some suggestions as to how the service providers build the global title tables.

3.5.5 Global Titling Logical Description

When a message is delivered, translation using a number of database tables occurs. A logical description is provided below [32].

- MAP passes an IMSI, UFMI, or ISDN address down through TCAP to the Convergence layer.
- The Convergence layer uses the IMSI, UFMI, or ISDN number as an index into the Socket Table(s) to determine if a TCP / IP connection already exists to the destination node.
- One of two results can occur as a result of the database look-up. If a socket number is returned, the Convergence layer stores this information in its header and sends the message.
- If no entry exists in the socket table, then a connection between the iDEN HLR and DAP has not been established, so the message is discarded and TCAP is informed of the error. DAPs continuously attempt to establish failed connections, so no additional action is necessary.
- If a iDEN HLR is collocated with a DAP1, ICP will need to route messages between the local DAP and iDEN HLR. This routing will not require TCP connections, since the messaging is not leaving the DAP. Therefore, the global

titling may be handled differently in these cases, depending upon implementation. In any case, the locally destined messages are reflected back to TCAP for delivery.

3.5.6 Service Providers and Global Titling Tables

As mentioned above, the Convergence Layer must establish connections and to do so requires an IP Address and Port Number to the device. This information is stored in the DAP and iDEN HLR by a craftperson. The purpose of this section is to provide the information a craftperson must enter, and this information is that represented by the logical IP Tables. (The Socket Table entries are created by the software.) The information a craftperson must enter for the global titling to be used by a VLR to identify an HLR is

- a logical indication that the entry is for an HLR
- the IMSI range(s) that point to the HLR
- the UFI range(s) that point to the HLR
- the HLR's ISDN Address
- the urban area code (UANC) in which the HLR resides
- the IP Address to locate the HLR's hardware
- the Port Number to locate the HLR's protocol stack

Likewise, the information a craftperson must enter for the global titling to a DAP is

- a logical indication that the entry is for a VLR
- the VLR's ISDN Address

- the urban area code (UANC) in which the VLR resides
- the IP Address to locate the VLR's hardware
- the Port Number to locate the VLR's protocol stack

3.6 Summary

This chapter deals with the protocols and the interfaces between the network elements at each stage of the Next Generation Dispatch iDEN system. The links explained in this chapter are the RF interface links, ACG-DACS link, DACS-iVPU link, DAP-iHLR link and the links between the iVPU and the other north-bound NEs.

Chapter 4

DAP Architecture

The Dispatch Application Processor is the network element responsible for the overall coordination of the Dispatch and Packet Data Services. The architecture of the DAP can be divided into two major parts. The first part of the DAP architecture is the DAP core that handles the main functions and the other part contains the objects which supports the DAP core functionalities. The major reference for the DAP Architecture is being taken from [11].

The Figure 4.1 shows how the DAP architecture is being formed.

The supporting modules are the Mobile Application Part (MAP), Common Controller Platform (CCP) and Common Agent (CA).

4.1 Supporting Modules

4.1.1 Mobile Application Part (MAP)

- The Mobile Application Part contains various protocols pertaining to the various mobile applications.
- MAP provides a kind of interface for the communication between the Home Location Register and the Visited Location Register.

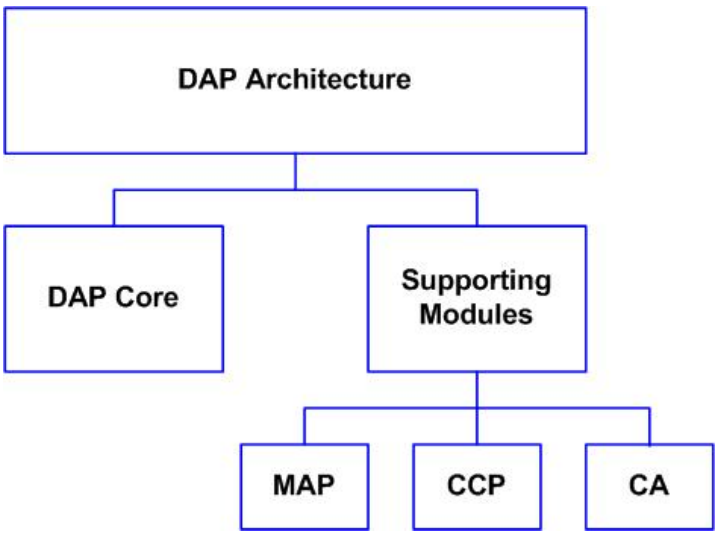


Figure 4.1: DAP Architecture

- MAP also provides different services to DAP such as authentication, location management, provisioning, etc.

4.1.2 Common Controller Platform (CCP)

- The Common Controller Platform provides an interface between the hardware or the operating system of the element and the application to be run on the element.
- The main advantage of using the CCP is that it makes the application platform independent to the hardware and the operating system.
- It acts as an emulator which emulates the hardware for the application and hence the application can be run on the element regardless of the OS and the hardware on the machine.
- The CCP module can perform similar tasks for other network elements as well such as DAP, iHLR, etc.

4.1.3 Common Agent (CA)

- Common Agent performs the tasks of the Operation and Maintenance Center for the DAP.
- It provides an interface between the DAP and the OMC.
- It also provides System Configuration data and Performance Management data of various DAP applications to OMC as and when asked by the OMC

4.2 DAP Core

The DAP core shown in Figure 4.2 can be divided into several architectural modules like Accounting and Performance Management, Resource Management, Configuration and State Management, System Control Management, Call Processing and Mobility Management, Availability Management and Database Management.

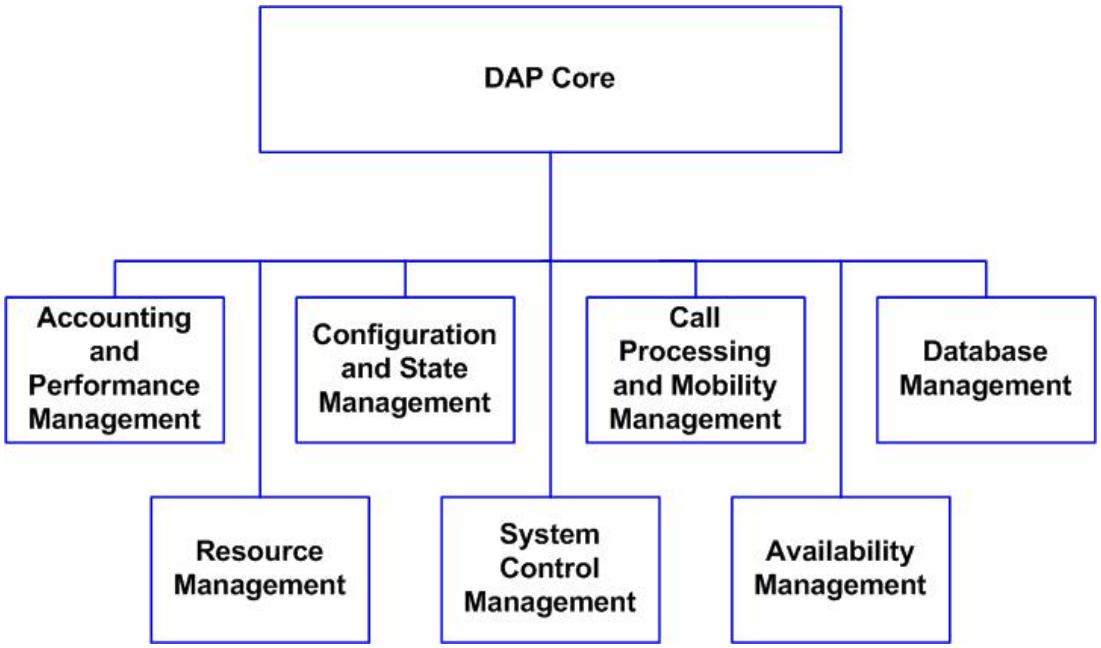


Figure 4.2: DAP Core

4.2.1 Accounting and Performance Management

This architectural module manages the call data records in the shared memory. This module retrieves the call data from shared memory as well as counter and distribution statistics from other tasks. From this data, at specified intervals, it creates billing files and sends raw statistics to the common agent.

4.2.2 Configuration and State Management

The Configuration and State Management AM provides integrated management of system configuration information such as a "hang timer" and a "wait for location response period" in the DAP. It also provides DAP's link state management functionality. The configuration management task of this module manages the system configuration for other tasks. The DAP link state management task of this module manages the links that DAP has got with other network elements. The following are the functions of this particular task:

- It performs link version check procedure for links of DAP-ACG, DAP-PD, DAP-MDG, DAP-iSG, DAP-iDAC and DAP-DAP.
- It performs link continuity check procedure for DAP-iSG, DAP-iDAC and DAP-DAP links.
- It instructs CCP to terminate the ACG, PD, MDG, iSG, iDAC and peer DAP links.
- It informs SPMT when a DAP-iSG link is terminated.
- For each link device type, inform corresponding resource management task on link status change, addition/deletion of links.

The watchdog management task of this module keeps track of system hangs. Whenever the system hangs or is about to hang, this task will perform the house

keeping and will reset the system so that graceful degradation of the system takes place and less time is required for the restart process of the system after a hang.

4.2.3 Call Processing and Mobility Management

This architectural module is responsible for the overall management of the call flows and the call processing tasks and also for the mobility management tasks.

The call processing management task of this module has got the responsibilities of setting up the dispatch and packet data calls, maintain the calls and then terminate the calls when over. The Call Processing Manager is responsible for the setup and maintenance of dispatch call functionality associated with the DAP. Its major function is to process dispatch calls and packet data calls. This task determines information about the state of the radios via the VLR database. It typically receives an external stimulus in the form of a "service request" and generates a sequence of actions, each predicated upon a response.

The Dispatch subsystem of iDEN system provides the users the facility of making a kind of call known as the selective dynamic group call. This particular facility is being managed by the selective dynamic group call task of this module. Managing a Selective Dynamic Group Call includes keeping track of the current state of each call and processing input messages for a call based on this state. This also involves preserving SDGC session records to handle callbacks after the call instance is terminated. This task provides surveillance information for surveillance subjects as well. This task assigns iSG(s) to the calls which involve surveilled MSs. For each of the surveillance subject involved in an SDGC, the task will forward necessary surveillance information to the iSG assigned to the call for that subject.

The Mobility Manager is responsible for tracking the location of MS's and handling authentication and registration issues. This includes dispatch registration (including Get IMSI, Get Serving D-VLR, Update Fleet Location, and Update Location), packet data registration, authentication, registration renewal, packet data de-registration,

de-activation, and forwarding group call reconnects to call processing task. The Mobility Manager is also responsible for applying the provisioning changes sent by the iHLR to the DAP and as the result of internal audits. This includes unsolicited Insert Fleet Data, Delete Fleet Data, Cancel Fleet Location, Cancel Location, unsolicited Insert Subscriber Data, Delete Subscriber Data, and Purge Fleet.

4.2.4 Database Management

The Database Management module of the DAP architecture manages the overall database so as to segregate different fleet/domain/urban boundary entities. It maintains the records of the subscriber call access records and dispatch group records. It also manages the back up data of the Mobile Data Gateway of the packet data subsystem. The information present in the Visited Location Register is maintained by this module. Also the surveillance information and the tracked call data is maintained by the database management module of the DAP core architecture.

4.2.5 System Control Management

The system control management module of the DAP core manages the initialization of the DAP and also manages the interface of DAP with the other Network Elements. The call dump data task of this module provides a man-machine interface to the DAP system for debugging purpose. The system administration management task of this module interprets the operator's requests for the system. The system maintenance terminal task of this module interprets the keyboard inputs of the operator for the system. Another task called the tracing task of this module keeps the track of various trace files that the log produces.

4.2.6 Resource Management

The Resource Management architectural module of DAP core tracks the state of external devices such as PDs and MDGs which the DAP utilizes as servers. The MDG

resource management task manages the availability of all the Mobile Data Gateways of the system using the DAP as servers. In the similar manner, the performance board manager task manages the status and availability of the Packet Duplicators and the iDEN Data Access Controllers using the DAP as servers. The iSG resource manager task manages the status and the availability of the iDEN Surveillance Gateways. And finally the DAP resource manages tasks manages the DAP which is being used as server by other network elements.

4.2.7 Availability Management

The availability management module of the DAP core is responsible to check the overall usage of the Dispatch Application Processor. This task is important in order to decide whether to delegate the task to the redundant DAPs or in severe conditions, whether to perform load shedding. The DAP Usability Reporting Task is responsible for determining the DAP's usability (i.e. utilization level) and notifying the ACGs of it. This measurement is used to distribute roaming MSs across the DAPs in an urban and to help prevent a DAP from becoming overloaded. Periodically, this task will be required to re-calculate the DAPs usability. This involves CPU utilization, D-VLR usage, etc. If this new value meets the reporting criteria, it will be transmitted to and acknowledged by all of the active ACGs. If the new value does not meet the reporting criteria, it will be discarded and the previous usability will be maintained until the next calculation cycle. When an ACG successfully completes Link Version Check, this task will inform it of the DAP's currently stored usability level in order to begin receiving MS registrations.

4.3 Summary

This chapter covers the details about the DAP architecture. The details of the DAP core and the supporting modules are being presented in this chapter. The DAP core containing MAP, CCP and CA is being explained. Also the seven supporting modules

of the DAP architecture are also being explained in detail in the later sections.

Chapter 5

Test Case Development

Before the implementation of any system in the real world it becomes very important to run rigorous tests on the system using several scenarios to check whether the system sustains in severe situations or not. In the same manner, for the iDEN system to be established it is necessary to check each and every network element individually so as to check its performance in several situations. The process of testing the network elements individually is called Box Testing. Once each of the network elements or the boxes is being tested individually, these boxes are then integrated well so as to form a system. This process of integration is called "iDEN System Integration". After the process of System Integration, it is then required to test the system as a whole both under simulations and also under real case scenarios.

Both the box tests and the system tests consist of what is called a test case. A test case can be thus defined as "a set of conditions which are transmitted to the Network Element and if the response is such that those conditions are satisfied, then the test is a success otherwise it's a failure". That means a test case consists of some messages which are to be transmitted to a particular network element. These messages have to be such that on receiving those messages the network element considers to have received those messages from some other network element or any such entity which is familiar to that particular network element. Since the network element considers the incoming message to be from a known network element, it would try to respond

to that message. And the response that is being sent by the network element under test will decide the success or failure of the test case. If the response is exactly the same as expected, then the test is said to have passed successfully. If the response is almost same, the results are said to be partially passed and if the response is totally bizarre, then the test is considered to have failed.

Both the box and the system tests are made up of one or more such test cases. And hence the major portion of the project consists of creating test cases and running the test cases for different network elements. There could be more than one means for writing the test cases namely, scripting tools, automation tools and the ultimate real case scenarios. Keeping in mind the entire project, all these three means of writing and running the test cases could be used and implemented but for time being only the first two of them are being explained since those means are only being used till date. The references for the test case development are being taken from [1] and [33].

5.1 Scripting Tools

The first means for writing and running the test cases is the scripting tools. Using this tool a small test case was being created and being run as an example of a simple test case scenario. The name of this test case is being given "Lab Monitor".

The function of this lab monitor is to monitor different lab machines which are running without human aid. The lab machines which could be the network elements just need the booting and the rest of the tasks are being performed by the machine by its own without the intervention of the humans. But since it runs on its own it becomes important to keep an eye on the status of these machines. This function of keeping an eye is being performed by the Lab Monitor. Since the tools used here is the scripting tool, the platform i.e. the operating system used for the test case development is the UNIX Operating System. Using this OS as a base several scripting languages are being used. The scripting languages used for the test case development are Perl and the Shell Scripting languages. In the Shell Scripting, different shells such

as Bourne Shell, C Shell, Korn Shell and Bourne Again Shell are being used.

A combination of these scripting languages is being used to develop several scripts whose combined job is to perform the task of the Lab Monitor. The following flow chart explains the working of the test case.

The main function of the Lab Monitor is to check the current status of different lab machines. The process of the test case is a request-response kind of process. The test case generates a set of predefined messages. These messages are being transmitted to the lab machine whose status has to be known. On receiving the messages, the machine responds accordingly and on the basis of the response, the conclusion is drawn about the status of the machine.

Figure 5.1 represents the flow of the Lab Monitor.

The following is the detailed description of the flow chart.

- The User can insert the ip address and the password of the desired machine
- Test Case connects the local machine to the desired machine
- A set of predefined messages are being sent to the desired machine
- The desired machine responds to the messages
- Response gets received by the local machine
- The Test Case extracts the useful information from the response given by the desired machine
- The information contains the current status of the desired machine in the form of the System Variables and the Ongoing Processes
- The information is then presented in the User Friendly XML (Extensible Markup Language) format
- Status of the information gives the details of the functionality of the machine

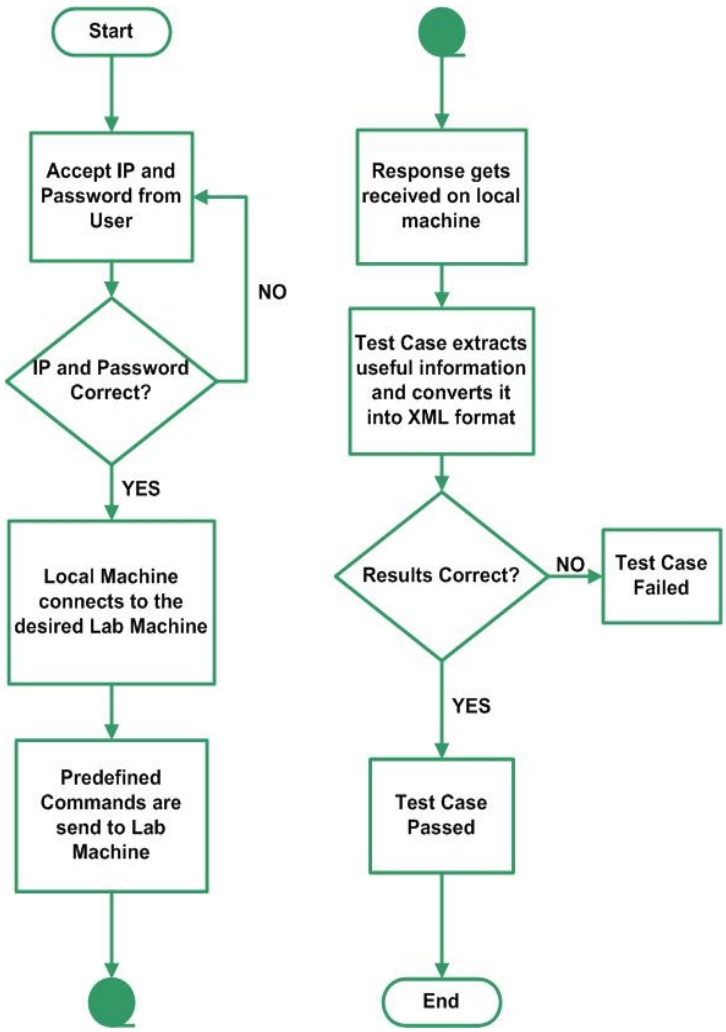


Figure 5.1: Lab Monitor Flow Chart

- And hence the response determines the success or failure of the test case
- The XML output file can be then merged with the GUI
- User can view the status of the desired machine using any web browser
- Thus making the test case and hence the application user friendly

5.2 Automation Tools

Another means for writing and testing the test cases is the automation tools. Automation tools are the tools which does the job of performing certain tasks on the basis of what response is available. In automation tools, a set of commands are predefined which can get executed on their own without the intervention of human aid provided that certain conditions are satisfied.

One such automation tool that is being used in the project is called the CTHA tool. CTHA is Componentized Test Harness Architecture. This particular tool is a one stop tool for box tests, where box test means testing a particular Network element individually under several extreme scenarios to check whether the Network element works according to the expectation or not. In this project CTHA has been used for the test case development and box test of one major Network element of the Dispatch subsystem namely Dispatch Application Processor.

CTHA is mainly developed for the testing of DAP only. The current configuration of CTHA tool has been set to test the DAP, but it can be easily configured to test other Network Elements as well.

5.3 CTHA

CTHA as mentioned earlier is the Componentized Test Harness Architecture. This particular tool is used to test the DAP of the Dispatch subsystem. The main job of DAP is overall controlling of the dispatch calls i.e. call alerts, private calls, group calls and packet data calls. In order to test the functioning of a stand-alone DAP in the system it is required that the DAP should be used in the real call scenarios and tested whether the DAP is performing well or not.

But since this is an individual test, other network elements can not and in fact should not be used to create the call scenarios on the very first hand. The reason for this is that if there is some manufacturing defect in DAP itself and if it is directly

deployed with the other Network Elements, then it may lead to malfunctioning of not only DAP but other NEs as well. So instead of using the real NEs with the real DAP, some simulated NEs have to be deployed to perform the box test of DAP. This is when the CTHA tool comes into picture. CTHA tool helps the user to simulate many Network Elements into it and helps it to connect with the DAP.

The tool so simulates the NEs that when connected to the DAP, the DAP will consider it to be a real NE. That means the tool CTHA itself can act as an NE. In order to perform the box tests, it required to place the real DAP into the call scenarios and for that it is required that all the Network Elements needed in a dispatch call should be available. CTHA has got the capabilities of simulating the Network Elements such as iVPU, DAP, APD, iDAC, iSG, iDAC, D-VLR, etc.

A Sun machine is used to install this particular tool and it is configured to simulate the Network Elements that are required in the test cases. The ACGs are being simulated on a different machine called the Gcom Protocol Appliance (GPA) machine. The iHLR is being simulated on a different machine and the tool used for that is called the iHLRsim. The Operation and Maintenance Center (OMC) is also being simulated on a separate machine and the tool used for that is called OMCsim. Thus for a complete Dispatch subsystem the requirements will be

- Real DAP
- CTHA
- iHLRsim
- OMCsim

All these machines are then connected to each other to form the complete Dispatch subsystem as shown in Figure 5.2. The connections here are IP based. Once the system is virtually set up the DAP is ready to be box-tested.

In order to test the DAP it is required to simulate different call scenarios and see whether the DAP works according to the expectations or not. The following is an

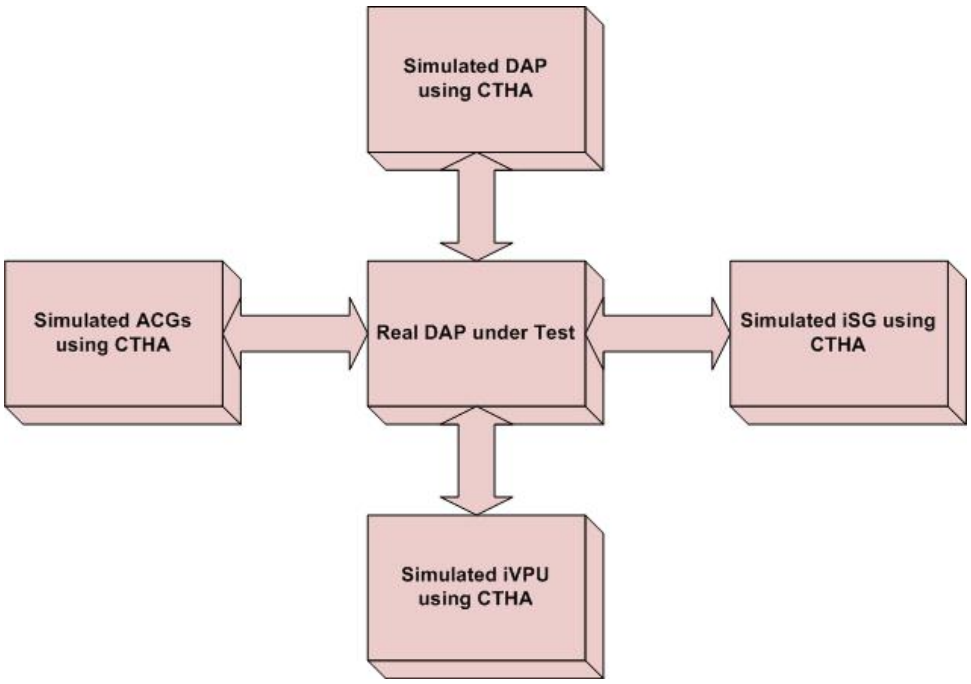


Figure 5.2: Test Case Organization using CTHA

example of such a call scenario created in CTHA. As shown in the figure, there are four network elements used for the call scenario/test case. Out of the four network elements, only one is real that is the real DAP under test. Other than that the Sim DAP Target, Sim ACG and the Sim iVPU are being simulated using the CTHA tools. These network elements are being added in the configuration files of CTHA tool and hence they are available in the Device Browser window of the CTHA tool. Which ever element is required can be dragged-dropped in the workspace and can be used.

After having all the network elements in the workspace, the messages have to be added to the workspace. All the messages are also being configured into CTHA tool and hence all the messages are available in the CTHA Message Browser window of the tool. In order to add the messages in correct order and sequence, it is required to have the detailed understanding of the dispatch call flows as described in the previous chapters.

The test case shown in the Figure 5.3 represents a simple "Dispatch Registration".

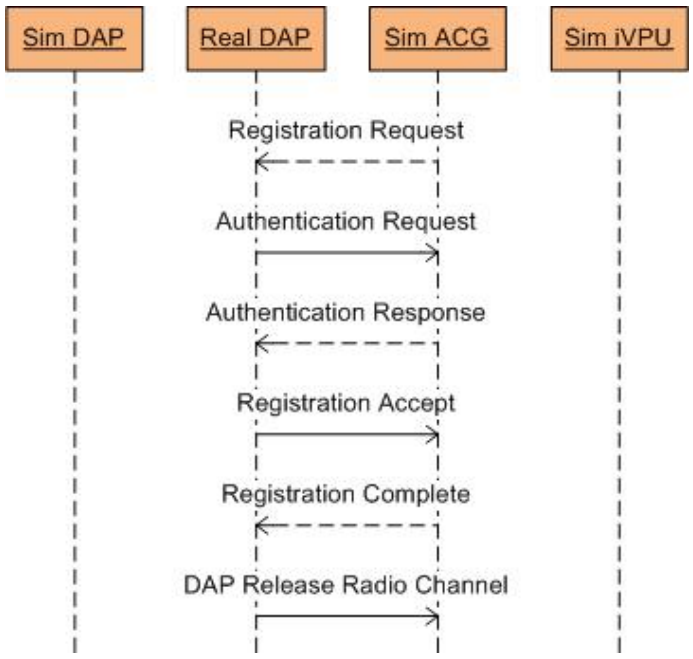


Figure 5.3: Call Scenario using CTHA

Now, the messages which are being placed directed from any other Sim network element towards the Real DAP are under the control of the user. The user can change the parameters of these messages and can create different scenarios. For example the very first message that is being directed from the Sim ACG towards the Real DAP is "Registration Request". In this particular message the user can set the values of the Mobile Station to be used, the ACG which will be serving it and what all permissions are being granted to the Mobile Station being used. Thus the messages that are directed from any Sim network element are under the control of the user.

But the messages which are being placed that are directed from the Real DAP towards any Sim network element represents the expectations of the user. For example, whenever the test case is being run the very first message "Registration Request" will be sent from our simulated ACG to the real DAP. On reception of the message, the real DAP will check for all the details that are being included in the message such as the MS identification numbers and the service provisioned to the MS. If all the

parameters are valid, the real DAP will reply to the simulated ACG some message. So as a user it is being expected that the real DAP will respond with an "Authentication Request" which is shown as the second message in the Figure 5.3. Thus while developing the test case the user needs to first know what all parameters are to be set in a particular message. After that the user should know the exact sequence of the messages that will be exchanged during the call flow.

Now at the time of running the test case if all the parameters of the first message are correct and the real DAP responds to the simulated ACG with an "Authentication Request" message, then CTHA tool compares the received actual message and the message specified in the test case. If both the messages are the same the tool considers that for time being the test case is OK and it will move further to the next message being specified in the test case. Again the third message in the test case is "Authentication Response". So if the details of this message are valid and if the real DAP responds with a "Registration Accept" message which is the next specified message then the CTHA tool will conclude that the "received" and the "specified" messages are same and hence the DAP responded well according to the expectations. And the same thing is applicable for the rest of the messages of the entire test case shown in the Figure 5.3. Further to simulate a call the other two Sim NEs namely Sim DAP and Sim iVPU can be also used. If all the messages are passed the test case is finally considered to have passed otherwise not. This is how test case have been created and tested to check the functionalities of the Real DAP under test.

5.4 Test Case Developed

There are several scenarios that can be tested using the CTHA tool. The following are the scenarios which have been tested on the real DAP using the CTHA tools

5.4.1 Perfect Case Call Flows

The first type of call scenarios been tested are the perfect case call flows. In this kind of scenarios four kinds of scenarios have been tested namely call alerts, intra DAP Private Calls, Inter DAP Private Calls and finally inter urban Private Calls. In all these scenarios the basic process is that first the Mobile Station needs to be registered into the DAP. Once the DAP accepts the registration requests, the call requests are sent to the DAP. DAP pages the ACGs to find the destination and call is established. After successful establishment of the calls the call is terminated successfully as well. Thus in these kinds of call scenarios, no additional features are added. The basic and normal call flows are used and the tests have been done and the results show that the request response technique used in the CTHA tool makes it clear that DAP functions according to our expectations and thus the test cases have been passed.

5.4.2 Reconnect Requests at Different Stages

The second kind of call scenarios that have been tested contains the scenarios of reconnect requests. Suppose while the call setup process is going on, the Mobile Station has first registered itself in one cell or under one ACG. Now while the other call setup messages are being executed, the Mobile Station moves from one cell to another cell. In that case the Mobile Station need to reconnect with the DAP by sending it the request for reconnection. And the DAP should be able to successfully reconnect the MS to sustain the call.

Now, this reconnect request can occur at any stage of the call setup. If it occurs after the call has been setup and the call is in progress, then iVPU has to handle the routing of the voice packets. But at the time of call setup, is at any stage the MS moves out of the home location, the reconnect requests have to be satisfied. Thus in these kind of call scenarios, such reconnect requests are being simulated at different stages of the call setup and expectations are made for the DAP to respond in a particular way.

Several different scenarios have been tested and that too in all kinds of calls namely intra DAP, inter DAP and inter urban calls and the test cases have been passed as well.

5.4.3 Different Bandwidth Allotment

This kind of call scenarios considers the allotment of different bandwidths for different Mobile Stations. Suppose the call scenario being considered is an intra DAP call. Then for this call the messages are simulated in such a manner that both the originator and the target Mobile Stations are being assigned different bandwidths as service provisioning. For example, the originator Mobile Station is being assigned the service provisioning to have extended 800 MHz of bandwidth and for the target the service provisioning for extended 800 MHz is kept off. That means the target can use only standard 800 MHz bandwidth.

In such a scenario if the originator initiates a call with the page request with extended 800 MHz bandwidth, the DAP will be knowing that the target that the originator wants to communicate with do not have the provisioning for extended 800 MHz bandwidth. Hence the DAP will send a messages to the ACG of the originator informing the originator that the call, for time being, has been queued because the originator needs to send a request with standard 800MHz bandwidth. And then if the originator MS sends the request accordingly, then only the call can be placed otherwise not.

These changes in bandwidth and the reconnect requests can be combined to create new kind of scenarios. For example, when the call setup started at that time the bandwidth allotments were correct but while the call is being setup the MS moves to a cell where the bandwidth allotment is not same as it was previously. In such scenarios the DAP should respond in a different manner so that the call setup becomes successful.

Thus combination of such scenarios have also been tested and the test cases have

been passed successfully notifying proper functioning of the DAP under test.

5.5 Summary

This chapter includes the major approaches taken for the development of test cases to test different Network Elements of the iDEN system. These approaches include the use of scripting tools and the automation tools. By using the scripting tools, the development of a test case named "lab monitor" has been explained in this chapter. In the later sections, the need for automation tools and the details of how automation tools work are being given. One of the sections deals with the automation tool CTHA which has been used as a major tool for testing the test cases on the DAP of Dispatch subsystem. Also the later sections cover the types of test cases being tested on DAP and also their corresponding results and responses given by DAP are also being discussed.

Chapter 6

Test Case Development: System Testing

The details regarding the box testing and the component testing were being covered in the previous chapters. This chapter describes the details regarding the system testing portion of the iDEN system integration.

System testing is the last step of the system integration. After the system testing phase is finished, the system becomes ready for launch commercially. As explained previously, the box testing procedures included that one of the network elements had to be tested rigorously. To do so, the NE under test was the only real NE. The rest of the NEs were being simulated and virtually connected to the NE under test. Now, in case of the system testing procedures, all the network elements after passing from the box testing phase are integrated to form an actual system. After the integration is done the system is ready to test. Several test cases are needed to be run to check the proper functionality of the system as a whole.

6.1 Approach

In order to be able to run the test cases a lab has been developed containing the real network elements to form the smallest possible geographical module i.e. Urban. A

small urban contains all the network elements that are included in an entire system and at the same time it does not contain the horizontal (inter-urban) call functionality of the original system.

Also, the urban, which is developed, contains only a few subscribers for testing purpose. So the generally, and in fact mostly, the problems of call drops due to load shedding will not come into picture. To test the load capacity of the system special loaders are used. Hence, all in all the urban that is developed for the testing purpose contains mostly the real network elements and a few simulators (the MSC is being simulated to test the interconnect portion of the system).

6.2 Tools

As explained earlier in the previous chapters, there are different interfaces being used at different links of the system. Hence, several different types of tools are being used to capture the live data packets that flow on the links during any call. This facilitates the test in-charge to clearly analyze the data packets and the messages flowing on the links.

6.2.1 iFTA

iFTA is the iDEN Field Test Application developed by Motorola. iFTA, in layman's terms is a packet sniffer that captures the packets passing through it while it is connected to that network.

In the system testing, iFTA is being used to capture the over-the-air messages. This tools captures the messages flowing between the Mobile Station (MS) and the Base Radio (BR) of the Enhanced Base Transceiver System (EBTS).

In order to capture the packets, the Mobile Station is connected to a workstation and the iFTA application is run on that machine. The application will make the terminal's capturing capability to promiscuous mode. This will allow the terminal to capture all the messages that are either transmitted or received by the Mobile

Station. The terminal duplicates the messages and displays them to the users for analysis. Since the terminal is in promiscuous mode, it will capture all the messages flowing on the wireless link even if the messages are not meant for that terminal.

6.2.2 Ethereal

Ethereal is another tool that is used to capture the packets. This tool has been developed specifically for the Ethernet links. This tool is run on a terminal that is connected to the system. It is also a packet sniffer and makes the terminal promiscuous one that will allow the terminal to capture all the messages that pass through it even if they are not addressed to that terminal. The links between the Base Radio and the Access Control Gateway of the EBTS are connected using the Ethernet links. ACG controls the functions of the BR and hence the messages exchanged between these two entities become important to analyze. Hence, this tool has being configured to capture the ACG-BR link Ethernet messages.

6.2.3 J2300 WAN Analyzer

This particular tool is being used in the Wide Area Networks to capture and analyze the end-to-end messages between different entities of the network.

As explained in the earlier chapters, the connection between the ACG to the Digital Access Cross-connect Switch is the traditional T1/E1 links. Now, the presence of this link makes the iDEN system a WAN system in which two LANs are connected with each other using the T1/E1 links. The first LAN is the internal Ethernet of the EBTS, while the second LAN is the network formed by the Ethernet links of the rest of the Northbound Network Elements. Hence, this WAN-like situation can be analyzed using the J2300 WAN analyzer. This tool is used to capture the messages between the ACG-DAP and/or ACG-MDG, etc. links.

6.2.4 Provtool

Provisioning Tools is a Graphical User Interface to access the database of the provisioned subscribers in the iDEN Home Location Register (iHLR). This particular tool is used to view and modify the details of the subscriber's information present in the database of the iHLR. The following are the parameters that can be viewed and modified using the Provtool.

- IMEI (International Mobile Equipment Identifier): This identifier is the SIM ID present on the SIM inserted in the MS.
- IMSI (International Mobile Subscriber Identifier): This particular identifier is what the system provides to the MS during the registration process.
- UFMI (Urban Fleet Member Identifier): This identifier uniquely identifies a mobile station. It also includes the Urban ID, Fleet ID and the member ID of the MS. The IMSI and UFMI are unique for an IMEI number.
- Group ID: This ID describes the group to which the MS is subscribed to for making the dispatch group calls.
- Mobile IP: During the packet data calls, the MS has to be assigned an IP in order to transmit the packet to the MS. Hence, the Mobile IP is assigned to the MS all it will be allotted to the MS during the packet data registration process.
- DAP ISDN: The Dispatch Application Processor (DAP) is uniquely identified using the ISDN number of the equipment. This number becomes crucial in case the MS roams outside the home location. The iHLR maintains an UFMI-DAP ISDN map and will use it whenever it is required to find the MS's serving DAP.
- Services: Provtool also maintains the records of what all services are being assigned to the MS. These services include, Dispatch Private and Group calls, interconnect calls and packet data calls. The assignment and restriction for these services can be done individually using the Provtool.

6.2.5 PDAT

PDAT is a Packet Data Application Tool used to perform the packet data calls. The packet data call service allows a workstation to get connected to the iDEN network or any other network such as extranet and Internet.

The iDEN MS is connected with the workstation and the MS is then made to act as a modem and hence the workstation gets connected with the iDEN network. PDAT is an application that has to be running on both the parties between whom the packet data call has to be made.

The PDAT allows the users to enter the IP and the port numbers of the other workstation. After successful entry of the parameters, the PDAT gives the users options to select the type of communication. PDAT allows the users to have two types of connections namely a connection-oriented connection and a connectionless connection.

In a connection-oriented connection, the originator of the call has to wait for the destination to acknowledge the connection after which the data transfer can start, while in connectionless connection, the data transfer can start without getting acknowledgment from the other workstation. After the data transfer is completed the call can then be terminated successfully.

6.2.6 DAP Local Maintenance Terminal

A DAP local maintenance terminal is an interface provided to the users to login to the DAP and check several system level information and modify those parameters as well. These parameters may include the load shedding parameters, hardware status and configuration, etc.

Since, the LMT is used to give access to some of the crucial informations to the users, there are five levels of user access available namely, Viewer, Technician, Engineer, Developer and System Administrator with the Viewer having the least priveledges and the Administrator having the most.

The following is the list of the categories and their parameters that can be viewed and modified using the LMT.

- Activity Log Management - This category contains the logs of the LMT activities such as logins logouts, etc. It also allows to backup these logs into a specific location.
- Billing - This category allows the users to
  - Backup the billing records generated by DAP
  - Congiure the ABFD (Automatic Billing File Deletion) start time. At this specifed time the processed billing files will be automatically deleted
  - configure the maintenance window - This time window will be used to do crucial maintenance.
  - Delete Billing Records
  - Enable/Disable ABFD
- Database Maintenance - This category allows the users to
  - Discard entire saved D-VLR
  - Synchronize Database between the active and stand by nodes
  - Enable/Disable Replication
- Database Query - The users can view individual D-VLR information
- Link Maintenance - The users can view the individual link status between the DAP and the other NEs. Also the links can be reset.
- Load Shedding - The users can view the current load shedding status.
- Parameter Maintenance - The users can view and modify individual parameters pertaining to different processes running on DAP.

- System Maintenance - The users, in this category can
  - Configure the OMC files
  - Perform the hardware tool diagnostics
  - Perform health checks and IP network management
  - Manage the nodes by starting, shutting or restarting the DAP application or DAP platform.
- Tools - The users get access to tools to view the GTT data and perform call traces.
- The users can also manage the session by modifiying the user previledges to access the LMT.

6.2.7 iHLR Local Maintenance Terminal

The iHLR LMT is also majorly similar to the DAP LMT. The main focus of this LMT is on the following functions:

- Maintenance of the Provtool
- Management of the provisioning
- Managing the records of the users.
- Perform GTT and maintain its database
- Tracing of the call in terms of provisioning and location updates.

6.3 Test Case Development

Now, in order to make sure that the system is functioning at its best, it becomes necessary to run several rigorous tests on the system and unusual scenarios are needed

to be created to know how the system reacts and to make sure the system reacts the same way as expected and not the any other way.

Another major reason for running the following test drills is the system upgradation. Initially, the system was in the Software Release 20.0 phase 1, which had to be upgraded to SR 20.0 phase 2 which includes the new improved packet data subsystem with increased number of served subscribers at a time. Initially, the system was capable of serving about 4 million packet data subscribers. But after the upgradation of the system, a new feature named the 8 Million Packet Data feature ensures about 8 million packet data SUs served at a time. Hence, test cycles are needed to be run both before and after the upgradation to make sure the system works normally. Also some of the test cases covered in the following sections cover the testing of the new 8 million packet data feature after upgrade as well. Mostly all the test cases covered below were being tested both before and after the upgradation.

The following sections of this chapter describe the different types of test cases that were developed and run on the system.

6.3.1 Registration Test Cases

Registration is a process that takes place every time the MS is powered ON. It also takes place when master reset of the MS is done or the MS is powered ON for the very first time. Before switching ON the MS, the provisioning has to be done to allocate various parameters to the MS using the Provtool. During the registration process, all these parameters allocated to the MS are then being assigned to the MS. To verify the assignment, Ethereal is used to capture the registration messages. These messages include the details of the parameters assigned. The following table shows the test suite and the included test cases for registration.

Events	**Description and Results**
IMEI Registration	The details regarding the MS are already provisioned in the iHLR and master reset is done in the MS. On Powering ON the MS, the IMEI will be assigned to the MS and the MS will be registered into the system. In order to check the IMEI registration, the MS needs to be reset because IMEI registration takes place only once at the time of first power ON.
New Unit Registration	The details of the MS are not present in the iHLR. Hence, a new entry for the MS with all the parameters is made in the iHLR. On powering ON, the MS will be registered in the system as a new subscriber and IMEI registration will be successful.
IMSI Registration	After the MS is powered ON for the first time, the IMEI will be assigned to the MS. For each and every subsequent power ONs, the IMSI will be used to register the MS in the system and not the IMEI. So at the time of first IMEI registration only, the IMSI will also be assigned to the MS so that for the subsequent registrations, IMSI is used and not the IMEI.

Table 6.1: Registration Test Cases:I

Events	Description and Results
Changed IMSI Registration	Once the IMEI and normal IMSI registrations are successful, the IMSI of the MS is changed using the Provtool. And in the next power ON the new IMSI should be assigned to the MS.
Changed UFMI Registration	At the time of IMEI registration, the UFMI is also assigned to the MS. So after normal assignment, if the UFMI is changed for that MS, then on next power ON, the new UFMI should be assigned to the MS.
Packet Data Registration	For all the services that are allowed to the MS, separated registrations will take place describing its parameters. Similarly, if the packet data service is allowed to the MS, then packet data registration should successfully take place at the time of IMEI registration and all the subsequent IMSI registrations.
Mobile IP Registration	For the packet data services, the MS has to be assigned a Mobile IP for the transfer of packets to and from the MS. This registration takes place ever time the MS is powered ON and the assigned Mobile IP can be seen in the packet data success messages captured on the Ethereal.

Table 6.2: Registration Test Cases:II

6.3.2 Normal and Secondary Calls Test Cases

This test suite contains the test cases of normal calls like the private calls, group calls, etc. also it contains the situations of a secondary call being made while a primary call is already going on either the originator or the target. The following describes the test cases.

Events	Description and Results
Private Call	A normal private call has to be established between two Mobile Stations and end to end messages are to be verified.
Group Call	A normal group call has to be established between a group of assigned MSs and their messages are to be verified.
Call Alert	A normal call alert has to be sent from one MS to another MS.
Cross-Fleet Call	A private call has to be established between two MSs of different fleets provided that both the MSs are allowed to make a cross-fleet PC (privileges can be changed using Provtool).

Table 6.3: Normal and Secondary Calls Test Cases:I

6.3.3 Channel Re-assignment Test Cases

The dispatch call services of the iDEN system are the improvised forms of the traditional Push-to-Talk services. In the dispatch calls, the parties have to push the PTT button to transmit the voice. Once the PTT button is released, the channels that were being allocated to the call are released. This feature of iDEN allows the released channels to be used for another call if they are required during the ideal period of the initial call. If no other call requires the channels, then the same channels need to be re-assigned to the call whenever any of the parties press the PTT button to talk. This test suite contains two scenarios to test this feature of re-assignment. It is shown in the following table.

Events	Description and Results
Primary PC, Secondary PC	A normal PC has to be established and has to be maintained. A secondary PC has to be established using a third MS with the target as any one of the two parties of the primary PC. The originator of the primary PC should get the target busy message. Also the paging requests will not be sent by the secondary call originator to the destination MS.
Primary PC, Secondary GC and vice versa	A normal PC (or GC) has to be established and maintained. A secondary PC (or GC) has to be originated from a different MS with target as any of the parties of the primary call. The originator of the secondary call should get the target busy message. Also in this case the paging messages will be sent by the originator of the secondary call but the target of secondary call will not respond to the pages.
Primary PC, Secondary CA and vice versa	A normal PC (or CA) has to be established and maintained. A secondary PC (or CA) has to be established with a different MS. The target of the secondary call will get a target busy message. Also the secondary call target will not respond to the paging requests of the secondary call originator.

Table 6.4: Normal and Secondary Calls Test Cases:II

6.3.4 Packet Data Test Cases

The system has to be upgraded to the second phase of the current software release in which the capacity of the MGD to handle the SUs will be increased. In the first phase of the system there were maximum of 32 RAGs allowed in one Urban area. And with each RAG capable of serving 128,000 users, the total capacity of the system was about 4.096 million users per Urban. While in the second phase of the system, there will be a maximum of 64 RAGs allowed in the Urban which increases the capacity to about 8 million users per Urban. In order to make this transition to the second phase several test cases need to be run first on the first phase to make the system ready for the second phase.

In order to run the packet data tests, a tool named PDAT was being used. This

Events	Description and Results
Normal Scenario of Private Call	A private call has to be established between two MSs and voice packets have to be exchanged one after another and each time the PTT is pressed the re-assignment of the traffic channels have to be examined.
Loss of signal during the conversation in PC	A private call has to be established and while the conversation is active, one of the MSs has to be taken away from the coverage area so that there occurs loss of signal. The channels, hence, will not be released and the call has to drop with the error message of "Loss of Transmission".

Table 6.5: Channel Re-assignment Test Cases

tool allows the users to establish a connection for a packet data session. This tool uses a socket based approach to establish connection hence the IP and the port of source and destination needs to be added. Also, this tool allows the users to establish a connectionless connection and a connection-oriented connection. The connectionless connection allows the users to transmit data without the recipient acknowledging the connection. While, the connection-oriented connection needs an acknowledgment from the recipient before the transmission can take place. The following are the packet data test cases.

Events	Description and Results
PD Registration	A normal packet data registration process has to be examined while power ON.
Mobile IP Registration	A normal Mobile IP registration has to be examined
TEI format	TEI is a Temporary Equipment Identifier which has a particular format and is assigned to the MS for each Packet data session. This number has a change in the second phase. So the initial format has to be verified.
Inbound PD session	A normal inbound packet data session has to be established with an MS as target.
Outbound PD session	A normal outbound packet data session has to be established with an MS as originator.
Secondary calls during PD session	A secondary call has to be attempted while a PD session is in progress with the target as one of the parties of the PD session. The originator of secondary call should get a target busy message.
SU out of power-No deactivation-PD registration of power ON	The MS's battery has to be drained out so that the MS switches OFF. Since, this is not a normal Power OFF process, the deactivation procedure will not initiate and the PD registration has to take place on power ON.
SU out of coverage-No deactivation-PD registration when MS back	The MS has to be made out of coverage. No deactivation procedure will initiate. And the PD registration has to take place when the MS returns back to the coverage.
Power cycle-Deactivation-PD registration of power ON	A normal power OFF process has to be done to switch OFF the MS. Since, this is a normal power OFF, the deactivation process has to initiate. Also, the MS has to do a PD registration on power ON.

Table 6.6: Packet Data Test Cases:I

6.3.5 Event and alarm Management Test Cases

The Operation and Maintenance Center (OMC) administers each and every network element of the system. It also generates various alarms in case any faults are detected with the NEs. These alarms are useful for the operator to notify the faults and rectify them. The following are the test suites and the test cases of certain scenarios that requires the OMC to generate particular alarms.

Events	Description and Results
Addition of new PDR	Successful attempt to add a new Packet Data Region in the Urban has to be made.
Additions of new MDG4	Successful attempt to add a new MDG4 in the PDR has to be made. With the system in first phase, a maximum of 8 logical MDG4s can be added per PDR.
Same RAG ID in same PDR	An attempt to add two RAGs with same RAG ID in the same PDR has to be made. The OMC won't allow it to happen.
Different RAG IDs in same PDR	RAGs with different RAG IDs will be allowed in the same PDR.
Same RAG ID in different PDR	RAG with same RAG IDs in two different PDRs will be allowed.
Multiple PDRs with Multiple RAGs	Successful attempts to add multiple PDRs with multiple RAGs in them have to be made. With the system in the first phase, 32 RAGs per PDR and 4 RAGs per MDG will be allowed.

Table 6.7: Packet Data Test Cases:II

Link Failures

In this test suite it is required to disable several links between the network elements and the corresponding alarms and its criticality has to be examined in the OMC console.

Triggered Events	Alarms Generated
Terminate DAP-DAP link	DAP-DAP TCP link down DAP peer to peer connection terminated
Terminate DAP-MDG link	DAP-MDG TCP link down
Terminate DAP-iVPU link	DAP-iVPU TCP link down
Terminate DAP-ACG link	DAP-ACG TCP link down

Table 6.8: Link Failure Test Cases

MS Registration

In this test suite some unusual scenarios have to be created and MS registration has to be attempted to get some specific alarms on the OMC.

Triggered Events	Alarms Generated
MS tries to register with invalid IMSI	DAP cannot map to iHLR for this IMSI
MS missing from iHLR and MS tries to register	iHLR claimed that IMSI is unknown

Table 6.9: MS Registration Test Cases

DAP Replication

As explained in the previous chapters, the DAP is a bi-nodal network element which means that there will be two DAP nodes, one active and other in standby mode. Both these nodes need to be in synchronization with each other and the D-VLR data of each node has to be replicated in from the active node to the stand by node. The following test cases shows the alarms generated on enabling and disabling the replication function.

Triggered Events	Alarms Generated
DAP Replication turned OFF	DAP Replication communication failure
DAP Replication turned OFF	DAP Replication suspended
DAP Replication turned ON	DAP Replication Synchronized

Table 6.10: DAP Replication Test Cases

DAP Shutting Down

There are some specific alarms that generate while the DAP application is shutting down or it is starting. DAP was made to restart to cover both the alarms of shutting

down and starting. The following test cases describe those critical alarms.

Triggered Events	**Alarms Generated**
Stop Standby DAP node	DAP Replication Failure
Stop Active DAP node	HA Recovery Initiated
Stop Active DAP node	DAP shutting down UEA-UDI Active-Maintenance Maintenance-Standby
Reboot DAP Application	DVLR initialize GTT initialize UDI-UEA Standby-Active

Table 6.11: DAP Shutting Down Test Cases

DAP Node States

UEA-Unlocked Enabled Active UEIm-Unlocked Enabled Impaired UDI-Unlocked Disabled Idle

Miscellaneous

This test suite contains come of the misc test cases and their corresponding alarms.

Triggered Events	**Alarms Generated**
Link version check failure between DAP-MDG	MDG did not send link version check request to DAP
IP address conflict	Invalid IP MDG did not send link version check request to DAP
Link version mismatch	ACG/iVPU did not send link version check request to DAP

Table 6.12: Misc. Test Cases

6.3.6 Daylight Saving Test Cases

The feature of daylight saving is used in the European countries in which the time is manually manipulated during the summer and spring seasons in order to have more hours to work with the daylight ON. Even though this feature is not used in the Asian continent, the parameters and its test cases are needed to be run to check its normal functionality. The following are the Daylight Saving Test Cases.

Events	**Description and Results**
Time Zone Offset parameters change	Successful modification to valid change to the parameter. Also denial has to be obtained for invalid value entered for this parameter
Daylight Saving start week, day and month	Successful modification to valid change to these parameters. Also denial has to be obtained for invalid values entered for these parameters
Daylight Saving stop week, day and month	Successful modification to valid change to these parameters. Also denial has to be obtained for invalid values entered for these parameters
Daylight Saving magnitude	Successful modification to valid change to the parameter. Also denial has to be obtained for invalid value entered for this parameter
Rollback	After successful modification of the above mentioned parameters, a successful attempt to rollback the system version to the previously running SV has to be made.

Table 6.13: Daylight Saving Test Cases

6.3.7 Online Configuration Change Test Cases

The online configuration of the system parameters allows the users to change those parameters without pushing a system load to the NE and let it download. These parameters can be changed on-the-go and doesnot require the lengthy procedures of system version download onto the Network Element. The following are the test cases pertaining to some of those parameters. In the test cases mentioned below there is required to change the configuration and notice the change in the state of the particular application in OMC's system status display (SSD).

Events	**Description and Results**
Ethernet connection disabling	The Ethernet connection of the DAP has to be disabled and SSD should show the Ethernet status as impaired.
Disabling one or more Misc. hardware	Misc. hardware includes DAP fans, CPU and power supply. One or all of these hardware has to be disabled and the hardware status in SSD has to be verified as impaired.
Disabling critical applications	Critical applications like Mobility management and Call processing management running on DAP have to be killed and their corresponding status in the SSD has to be verified as out-of-order.
Enabling/Disabling Replication Application	The database replication of DAP has to be enabled and disabled and the corresponding change on their status information in SSD has to be verified as running or out-of-order.

Table 6.14: Online Configuration Test Cases

6.3.8 Post upgrade PD test cases

After the upgrade of the system from SR 20.0 phase 1 to SR 20.0 phase 2, there are certain packet data test cases related to the encryption and compression of the packet data has to be checked. The provisioning of encryption and compression for a specific SU can be modified using the Provtool. Also, the requests related to the encryption and compression that the SU sends while PD and Mobile IP registration can also be

changed using the Hyperterminal. So a combination of these provisioning has to be made and the test cases have to be performed.

SU Provisioning Compression	**SU Provisioning Encryption**	**SU Request Compression**	**SU Request Encryption**	**Results**
Disabled	Enabled	Disabled	Disabled	The data compression and encryption algorithm details are not assigned to the SU at the time of PD Registration.
Disabled	Disabled	Enabled	Enabled	The data compression and encryption algorithm details are not assigned to the SU at the time of PD Registration.
Disabled	Disabled	Enabled	Disabled	The data compression and encryption algorithm details are not assigned to the SU at the time of PD Registration.
Disabled	Disabled	Disabled	Enabled	The data compression and encryption algorithm details are not assigned to the SU at the time of PD Registration.
Disabled	Disabled	Disabled	Disabled	The data compression encryption parameters and algorithm details are not assigned to the SU at the time of PD Registration.

Table 6.15: Packet data Compression and Encryption Test Cases

It has to be noted that in all the above test cases, there are three levels of parameter changes which will finally decide the encryption and compression services. The first level is the system parameter i.e. the MDG4 parameters related to encryption and compression has to be changed which ,in the above test cases, are changed to be enabled. The second level is the provisioning using the Provtool and the third is the

SU requests which can be modified using the Hyperterminal.

6.4 Summary

This chapter explains the importance of System Testing phase as the final stage in the process of System Integration. It then explains the tools which were being used to test the real system. At the end the chapter includes various kinds of test cases that were being run using those tools and the results that were being obtained.

Chapter 7

Conclusion and Future Scope

7.1 Conclusion

The call scenarios tested using the CTHA tool for the Dispatch Application Processor of the iDEN system pertains to different kinds of private dispatch calls such as Intra DAP calls, Inter DAP calls and Inter Urban calls. The results shows that the DAP behaves in its own different way for every new call scenario that has been tested. The test cases tested on DAP contains the call scenarios of reconnect requests at different stages of the call setup process. Also the tests include the scenarios of different bandwidth provisioning and different bandwidth allotment for different geographical locations and different subscriber units. In all the cases the DAP responds exactly the way as it should respond theoretically.

After the box testing phase the features of the system testing phase was also successfully tested. The major reason for running the test cycles in the System Test was to verify the proper functioning of the system before and after the upgradation from SR 20.0 phase 1 to SR 20.0 phase 2. Hence, a series of tests were run and proper functioning of the end-to-end system was being verified.

7.2 Future Scope

Since the test cases in case of the Box Testing phase have been limited to the private calls and call alerts in some cases, the thesis work can be extended for group dispatch calls with different call scenarios to test the DAP. Also other tools can be learned and used for further test case development and testing of the network elements other than DAP such as iDEN's Home Location Register (iHLR), the network element used for packed data services namely Mobile Data Gateway (MDG), the network element acting as gateway between the iDEN network and the 3G network namely iDEN Gateway (iGW), etc.

In case of System Testing phase the future expansion of the thesis can cover the integration and the testing of the Melody Based iDEN system. As described earlier, the description and the tests in this thesis are discussed keeping the NGD as current running version of iDEN. But future expansion of the system to the Melody Based system can be done and then the system testing of the latest version can be carried out. The testing of the Melody iDEN can cover a whole range of tests can a healthy progress can be achieved in that particular direction.

Appendix A

Abbreviations

Abbreviations	Description
BA	Billing Accumulator - gathers usage details from the MDG and stores the data for retrieval for billing purposes. Data is retrieved or forwarded to the customers Billing Accumulator for further processing.
BR	Base Radio - performs the RF communications with the SUs, sending both the control information and the compressed speech over a radio channel.
BSC	Base Site Controller - performs call processing, operations and maintenance, and provides the interface between the XCDR system and the EBTS.
DAP	Dispatch Application Processor responsible for the overall control and coordination of Dispatch and Packet Data services.
DCS	Digital Cross Connect Switch - central connecting point for ALL T1 and E1 links in the network and is used to separate the information on the T1 or E1 links and route the data to the correct network element.

Table A.1: Abbreviations I

Abbreviations	Description
EBTS	Enhanced Base Transceiver System - carries the radio signal from the SU to the system.
EGT4	Enhanced Global Title Translation Table Tool - It provides the following information to all DAPs, iHLRs and iDACs in the network: International Mobile Station Identifier (IMSI) ranges associated with a particular iHLR IP addresses of all iHLRs and D-VLRs
HA	Home Agent - routes packets from the Internet to the correct MDG for delivery to the SU.
BSC	Base Site Controller - performs call processing, operations and maintenance, and provides the interface between the iVPU system and the EBTS.
iCP	iDEN Call Processor controls the signaling necessary to set up, maintain, and tear down calls. It also provides handover support and control in Mobility Management.
iDAC	iDEN Dispatch Access Controller - provides Dispatch audio routing between horizontally networked iDEN systems. The iDAC provides the routing of the voice for inter-urban Dispatch calls across different urbans.
iGW	iDEN Gateway - interworks signaling and bearer paths between 3G networks and the iDEN Dispatch network. The iGW supports Selective Dynamic Group Calls (SDGC) which include iDEN and 3G subscribers.
iSG	iDEN Surveillance Gateway - provides an access point for law enforcement agencies to monitor Dispatch calls.
iVPU	iDEN Vocoder Processing Unit - converts the VSELP or AMBE++ voice packets used on the radio link to PCM used by local and Interconnected PSTNs.

Table A.2: Abbreviations II

Abbreviations	Description
iWF	Inter Working Function - performs the data-rate adaptation between the PSTN and the iDEN system.
MDG	Mobile Data Gateway - manages the overall process of Mobile IP. The MDG works in conjunction with the HA router to receive forwarded packets from its home address and distributes these packets to an SU.
MPS	Metro Packet Switch - routes Dispatch and Packet Data packets to the proper Dispatch subsystem element.
OMC-R	Operation and Maintenance Center-Radio - establishes, maintains, collects information about the network, and is available to the system operator.
PD	Packet Duplicator or Packet Data - allows a carrier to supply their subscribers Internet Protocol (IP)-based network access to either the Internet or their own networks.
RFDS	Radio Frequency Distribution System - connects the base radios to the RF antennas.
SDM/FT	Supernode Data Manager/Fault Tolerant - allows law enforcement agencies to obtain call data records as well as intercept audio in an Interconnect phone call for court authorized monitoring.
SMS	Short Messaging Service - provides the functionality of receiving short text messages.

Table A.3: Abbreviations III

Appendix B

Key Protocols

B.1 Frame Relay

Frame Relay is a protocol standard for LAN internetworking which provides a fast and efficient method of transmitting information from a user device to LAN bridges and routers. The Frame Relay protocol uses a frame structured similar to that of LAPD, except that the frame header is replaced by a 2-byte Frame Relay header field. The Frame Relay header contains the user-specified DLCI field, which is the destination address of the frame. It also contains congestion and status signals which the network sends to the user.

B.1.1 Virtual Circuits

The Frame Relay frame is transmitted to its destination by way of virtual circuits (logical paths from an originating point in the network) to a destination point. Virtual circuits may be permanent (PVCs) or switched (SVCs). PVCs are set up administratively by the network manager for a dedicated point-to-point connection; SVCs are set up on a call-by-call basis.

B.1.2 Advantages of Frame Relay

Frame Relay offers an attractive alternative to both dedicated lines and X.25 networks for connecting LANs to bridges and routers. The success of the Frame Relay protocol is based on the following two underlying factors:

- Because virtual circuits consume bandwidth only when they transport data, many virtual circuits can exist simultaneously across a given transmission line. In addition, each device can use more of the bandwidth as necessary, and thus operate at higher speeds.

- The improved reliability of communication lines and increased error-handling sophistication at end stations allows the Frame Relay protocol to discard erroneous frames and thus eliminate time-consuming error-handling processing.

These two factors make Frame Relay a desirable choice for data transmission; however, they also necessitate testing to determine that the system works properly and that data is not lost.

B.2 Link Access Protocol - D channel (LAP-D)

LAP-D is the Layer 2 protocol used. This is almost identical to the X.25 LAP-B protocol. Here is the structure of a LAP-D frame:

Flag	Address	Control	Information	CRC	Flag

Table B.1: LAP-D frame structure

Flag (1 octet) - This is always 7E(0111 1110)

Address (2 octets)							
1	2	3	4	5	6	7	8
SAPI (6 bits)						C/R	EA0
TEI (7 bits)							EA1

Table B.2: LAP-D frame

SAPI (Service access point identifier), 6-bits

C/R (Command/Response) bit indicates if the frame is a command or a response

EA0 (Address Extension) bit indicates whether this is the final octet of the address or not

TEI (Terminal Endpoint Identifier) 7-bit device identifier

EA1 (Address Extension) bit, same as EA0

Control (2 octets) - The frame level control field indicates the frame type (Information, Supervisory, or Unnumbered) and sequence numbers (N(r) and N(s)) as required.

Information - Layer 3 protocol information and User data

CRC (2 octets) - Cyclic Redundancy Check is a low-level test for bit errors on the user data.

Flag (1 octet) - This is always 7E(0111 1110)

B.2.1 SAPIs

The Service Access Point Identifier (SAPI) is a 6-bit field that identifies the point where Layer 2 provides a service to Layer 3.

SAPI	**Description**
0	Call control procedures
1	Packet Mode using Q.931 call procedures
16	Packet Mode communications procedures
32-47	Reserved for national use
63	Management Procedures
Others	Reserved for Future Use

Table B.3: SAPI

B.2.2 TEIs

Terminal Endpoint Identifiers (TEIs) are unique IDs given to each device (TE) on an ISDN S/T bus. This identifier can be dynamic; the value may be assigned statically

when the TE is installed, or dynamically when activated.

TEI	Description
0-63	Fixed TEI assignments
64-126	Dynamic TEI assignment (assigned by the switch)
127	Broadcast to all devices

Table B.4: TEI

B.3 SNMP

B.3.1 SNMP Based on Manager/Agent Model

SNMP is based on the manager/agent model consisting of a manager, an agent, a database of management information, managed objects and the network protocol. The manager provides the interface between the human network manager and the management system. The agent provides the interface between the manager and the physical device(s) being managed.

The manager and agent use a Management Information Base (MIB) and a relatively small set of commands to exchange information. The MIB is organized in a tree structure with individual variables, such as point status or description, being represented as leaves on the branches. A long numeric tag or object identifier (OID) is used to distinguish each variable uniquely in the MIB and in SNMP messages.

B.3.2 5 SNMP Command Messages

SNMP uses five basic messages (GET, GET-NEXT, GET-RESPONSE, SET, and TRAP) to communicate between the manager and the agent. The GET and GET-NEXT messages allow the manager to request information for a specific variable. The agent, upon receiving a GET or GET-NEXT message, will issue a GET-RESPONSE message to the manager with either the information requested or an error indication as to why the request cannot be processed. A SET message allows the manager

to request a change be made to the value of a specific variable in the case of an alarm remote that will operate a relay. The agent will then respond with a GET-RESPONSE message indicating the change has been made or an error indication as to why the change cannot be made. The TRAP message allows the agent to spontaneously inform the manager of an "important" event.

Most of the messages (GET, GET-NEXT, and SET) are only issued by the SNMP manager. Because the TRAP message is the only message capable of being initiated by an agent, it is the message used by DPS Remote Telemetry Units (RTUs) to report alarms. This notifies the SNMP manager as soon as an alarm condition occurs, instead of waiting for the SNMP manager to ask.

B.3.3 Simplicity of SNMP Leads to Widespread Use

The small number of commands used is only one of the reasons SNMP is "simple." The other simplifying factor is its reliance on an unsupervised or connectionless communication link. This simplicity has led directly to its widespread use, specifically in the Internet Network Management Framework. Within this framework, it is considered "robust" because of the independence of the managers from the agents, e.g. if an agent fails, the manager will continue to function, or vice versa.

B.3.4 The SNMP Management Information Base (MIB)

Each SNMP element manages specific objects with each object having specific characteristics. Each object / characteristic has a unique object identifier (OID) consisting of numbers separated by decimal points (i.e., 1.3.6.1.4.1.2682.1). These object identifiers naturally form a tree. The SNMP MIB associates each OID with a readable label (i.e., dpsRTUAState) and various other parameters related to the object. The MIB then serves as a data dictionary or code book that is used to assemble and interpret SNMP messages.

B.3.5 SNMP Packets Require OIDs

When an SNMP manager wants to know the value of an object / characteristic, such as the state of an alarm point, the system name, or the element uptime, it will assemble a GET packet that includes the OID for each object / characteristic of interest. The element receives the request and looks up each OID in its code book (MIB). If the OID is found (the SNMP object is managed by the element), a response packet is assembled and sent with the current value of the object / characteristic included. If the OID is not found, a special error response is sent that identifies the unmanaged object.

When an element sends an SNMP TRAP packet, it can include OID and value information (bindings) to clarify the event. DPS remote units send a comprehensive set of bindings with each TRAP to maintain traditional telemetry event visibility. Well-designed SNMP managers can use the bindings to correlate and manage the events. SNMP managers will also generally display the readable labels to facilitate user understanding and decision-making.

B.3.6 Understanding SNMP Packet Types and Structure

Basic serial telemetry protocols, like TBOS, are byte oriented with a single byte exchanged to communicate. Expanded serial telemetry protocols, like TABS, are packet oriented with packets of bytes exchanged to communicate. The packets contain header, data and checksum bytes. SNMP is also packet oriented with the following SNMP v1 packets (Protocol Data Units or PDUs) used to communicate:

a. Get

b. GetNext

c. Set

d. Trap

B.3.7 Set Requests Change Variables Within Managed SNMP Devices

The SNMP manager sends a Get or GetNext to read a variable or variables and the agent's response contains the requested information if managed. The manager sends a Set to change a variable or variables and the agent's response confirms the change if allowed. The agent sends a Trap when a specific event occurs.

Appendix C

Call Flows

This Appendix gives a detailed overview of the processes that go into the different kinds of call in all the types of iDEN subsystems.

C.1 Interconnect Call Flows

A typical mobile to land interconnect call has the following major processes included:

- Resource Request
- Call Setup
- Connecting Voice

The following are the steps of a typical interconnect call.

C.1.1 Resource Request

a. The user initiates the call.

b. The EBTS of the serving cell assigns a channel to the subscriber unit (SU).

c. If a channel is not available with the EBTS, it will not acknowledge the service request of the SU and will notify the SU with a message indicating that all the

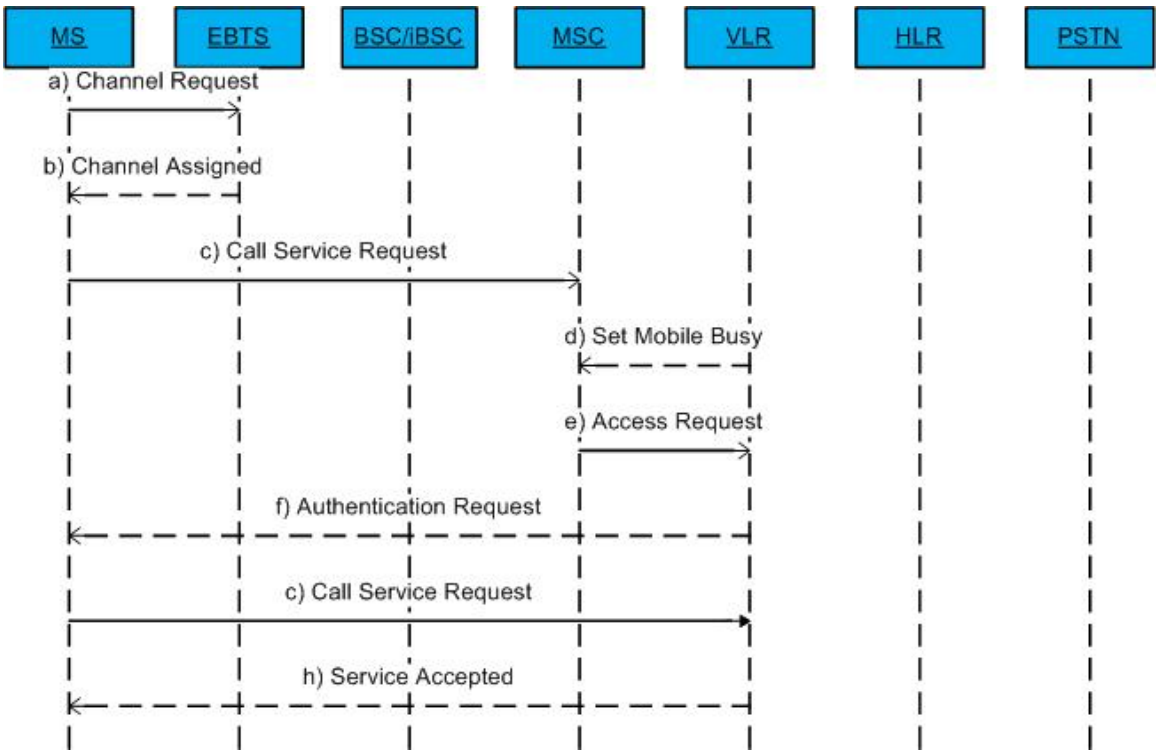


Figure C.1: Interconnect Call : Resource Request

channels are busy. But if a channel is available with the EBTS, the channel will be assigned to the SU and the service request containing the ID of the originating SU along with the type of service requested will be forwarded to the Mobile Switching Center (MSC).

d. On reception of the service request, the MSC will set the SU busy so that any other radio resource may not be assigned to that SU for any other call intended for the SU.

e. Then the MSC checks with the VLR so as to make sure that the SU is authorized for the service that it has requested.

f. If necessary, as an optional procedure, an authentication process runs between the VLR and the SU.

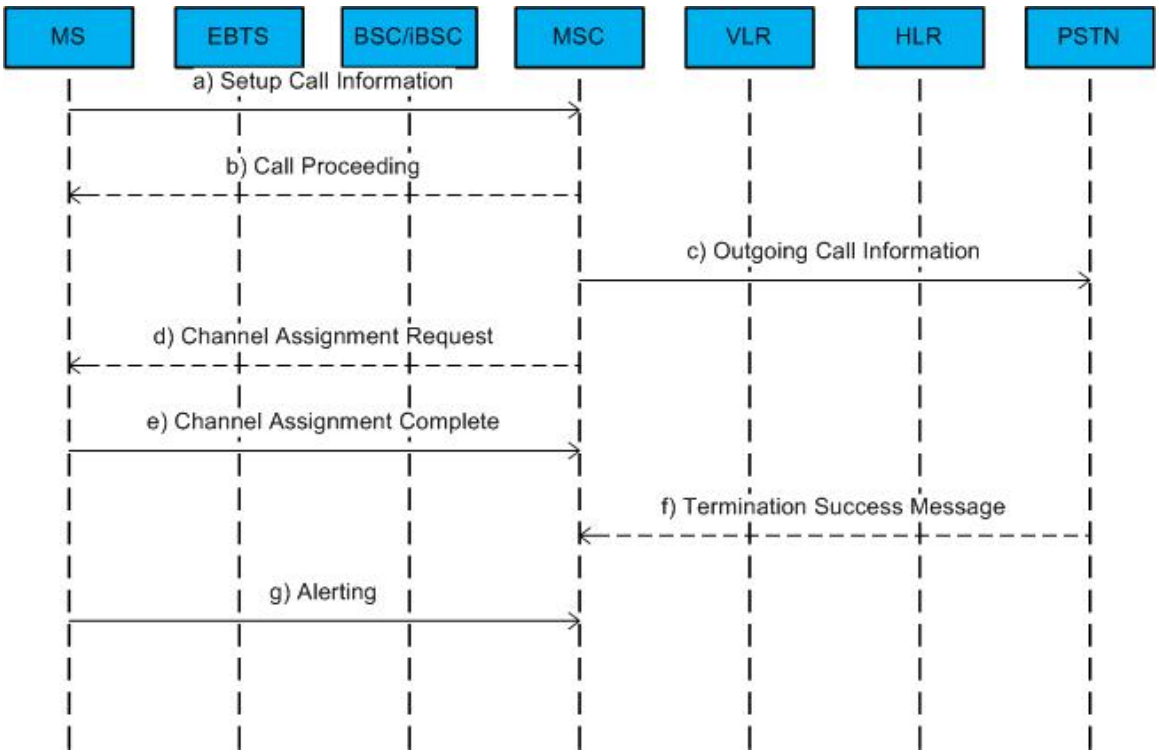


Figure C.2: Interconnect Call : Call Setup

g. The SU sends an authentication response to the authentication request sent to it by the VLR.

h. If the authentication is successful, the VLR sends an acknowledgement to the SU indicating that the service has been accepted.

C.1.2 Call Setup

a. After receiving the confirmation of the service request being accepted, the SU sends the dialed digits/telephone number to the MSC.

b. The MSC sends a call proceeding message to the SU and proceeds with the call setup with the information sent by the SU.

c. The MSC then captures a trunk and sends the call information to the PSTN.

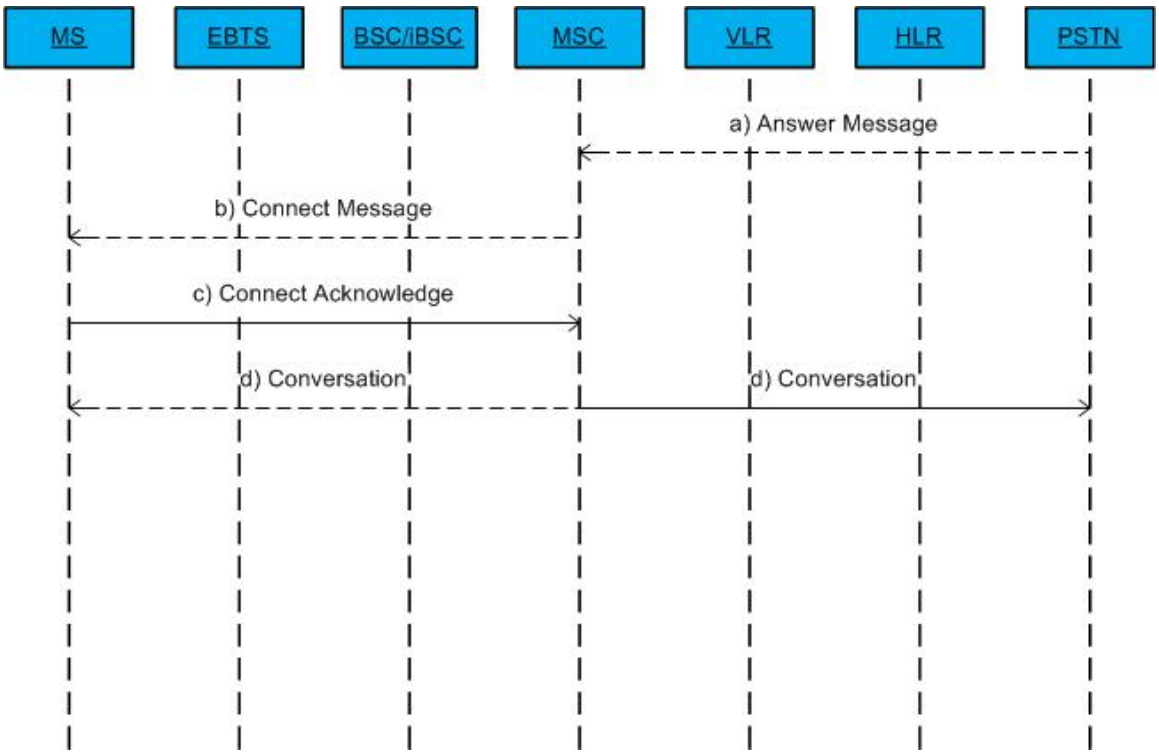


Figure C.3: Interconnect Call : Connecting Voice

d. The MSC then asks the BSC/iBSC to send a Dedicated Control Channel Request to the EBTS.

e. The EBTS assigns a channel to the SU which will then be used to complete the call setup procedure and to further carry the voice packets.

f. When the PSTN finds the destination landline telephone, it completes the connection and makes the telephone ring. It will then send a termination success message to the MSC.

g. The MSC in turn notifies the SU that the call has been connected by sending the ringing tone to the SU.

C.1.3 Connecting Voice

a. When the destination telephone answers the call, the PSTN sends answer message to the MSC.

b. The MSC then sends a connect message to the SU indicating that the connection has been established.

c. The SU in turn acknowledges the MSC for the connect message.

d. The MSC then opens a Traffic Channel between the SU and the PSTN and the voice traffic starts flowing between them. Ideally, the entire call setup process gets finished within 1 to 5 seconds from the point of call initiation.

C.2 Dispatch Call Flows

The test case development carried out in the project is carried out on the Dispatch Application Processor of the Dispatch subsystem. In order to perform the test case development it becomes necessary for the user to understand the detailed call flow of different kinds of dispatch calls. The Dispatch subsystem of the iDEN network supports two kinds of dispatch calls namely, private calls and the group calls. The major reference for the Dispatch call flows is taken from [33].

The private calls include only two parties namely the originator and the destination. It is a one-to-one conversation while a group call includes more than two members. It includes the members of the talk group in which the call has been initiated. It is a one-to-many-conversation.

The following section gives the details of different kinds of dispatch calls.

C.2.1 Private Calls

The private calls as explained earlier are one-to-one conversations. There can be three different kinds of private calls.

The first kind of private call is the "Intra DAP call". In this kind of call, both the originator and the destination are in the coverage area of the same DAP.

The second kind of private call is the "Inter DAP call". In this kind of call, the originator and the destination are under the coverage area of the same urban but under the coverage of two different DAPs.

The third kind of private call is the "Inter Urban call". In this kind of private call, the originator and the destination are under the coverage areas of two entirely different urbans. Although, most of the messages of the call flows of different calls are same, there are some vital changes that are required to be kept in mind for performing the test case development.

Intra DAP Private Call

Figures C.4 C.5 and C.6 represents the call flows of an Intra DAP Private call. As shown in the figure, there are network elements that take part in a call.

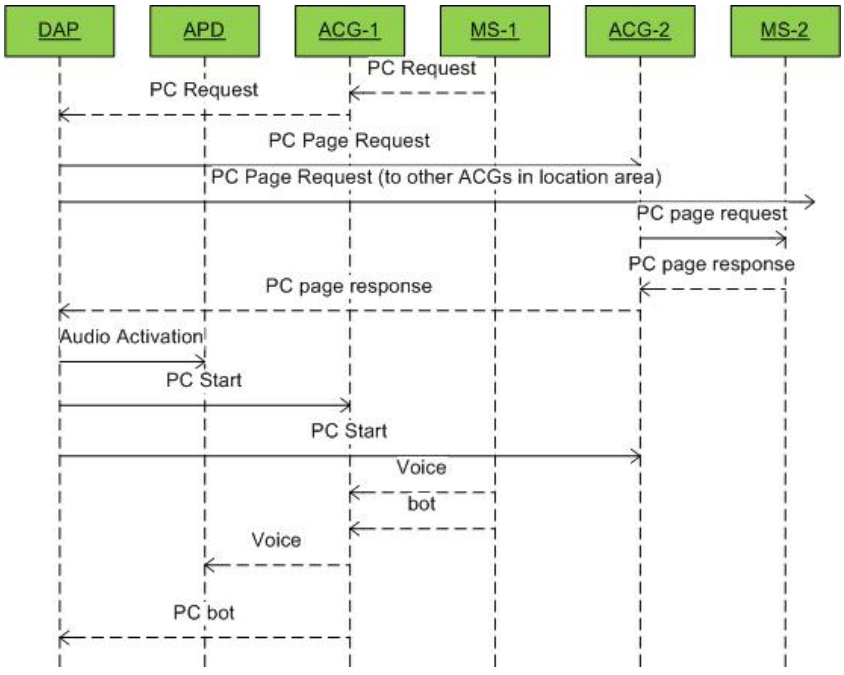


Figure C.4: Intra DAP Private Call : Part 1

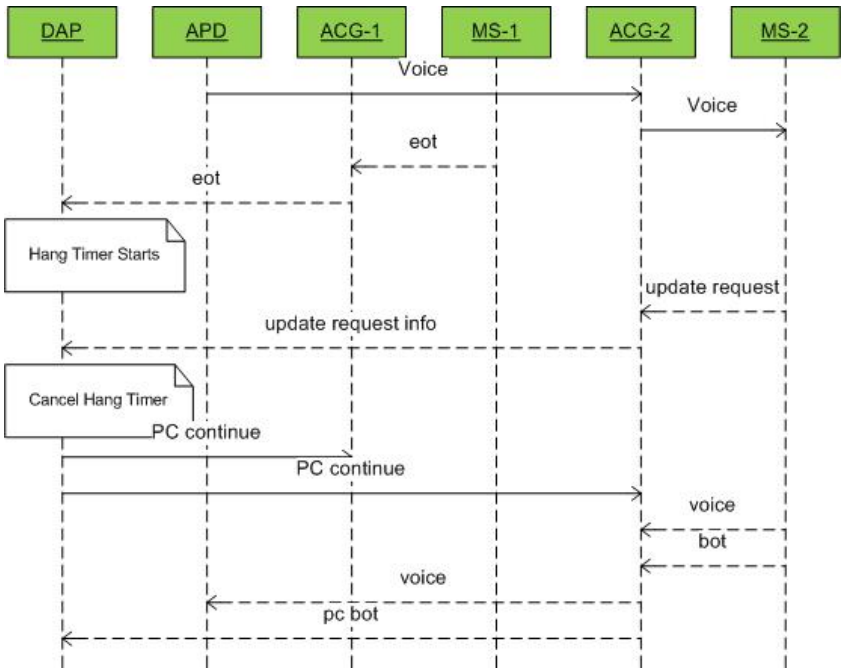


Figure C.5: Intra DAP Private Call : Part 2

The following are the steps explaining the flow of the call.

- The mobile station initiates a private call by sending a PC request to its serving ACG.
- The ACG in turn will inform the DAP about the request. The DAP will search its D-VLR and its Recent Call Records (RCR) to find the destination. If the destination is in the same DAP, the DAP will send page requests to all the ACGs under its location area.
- If the ACG identifies that the destination is under its coverage area, it will forward the page request to the destination.
- The destination MS will respond to the page request with a PC paging response to the ACG. The ACG will forward the response to the DAP.

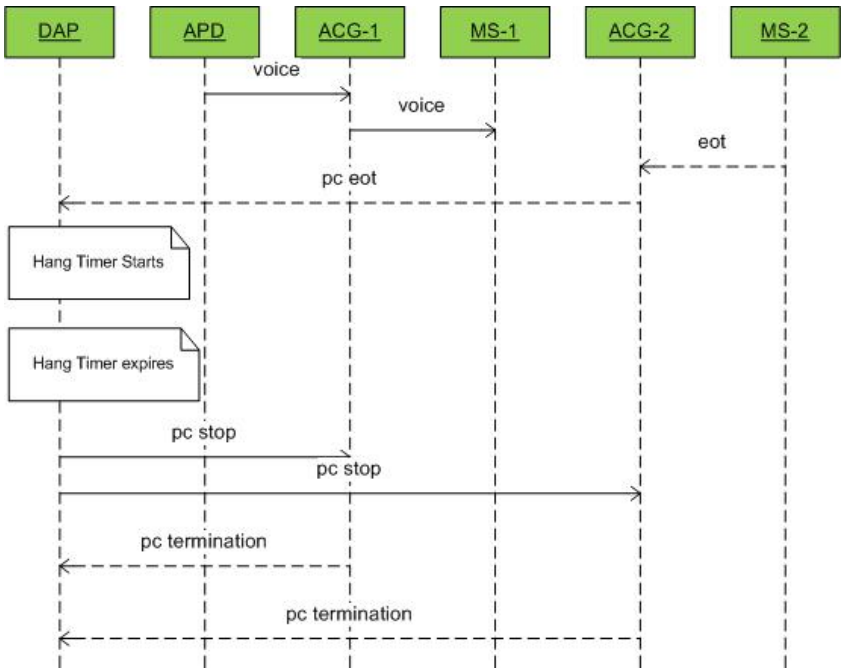


Figure C.6: Intra DAP Private Call : Part 3

- Once the DAP finds both the originator and the destination, it will send PC start messages to both the parties.
- The originator will then start transmitting voice packets to ACG along with a "bot (beginning of transmission)" message. The voice packets will be forwarded by the ACG to the APD and the bot will be sent to the DAP.
- The APD will route the voice packets to the destination ACG which in turn will forward the packets to the destination MS.
- Once the originator has finished with transmitting the voice packets, it will send an "eot (end of transmission)" message to the DAP via ACG.
- On reception of eot message, the DAP will indicate the ACGs to release the channels and will start a hang timer.
- Now if the destination wants to transmit voice packets, then it will send an

update request to the DAP via ACG before the hang timer expires.

- On reception of the update request, the DAP will cancel the hang timer and will indicate the ACGs to continue the call.
- In the similar manner, the destination will send voice packets with the help of ACG and APD.
- Once the transmission completes, the hang timer again starts and waits for an update request.
- If no update request comes, the hang timer expires and the DAP indicates the serving ACGs to stop the private call.
- The serving ACGs in turn acknowledges the instruction with a private call termination message to the DAP and the call ends.

Inter DAP Private Call

Figures C.7 and C.8 represent the Inter DAP private calls.

The following are the steps explaining the Inter DAP PC.

- In the Inter DAP call as well, the MS and then the ACG will send a Private Call request to the DAP.
- The DAP will search the location of the destination in its D-VLR and RCR. If the destination is not under its coverage area, the DAP sends a routing request to the iHLR. In turn the iHLR informs the location of the DAP that is serving the destination.
- The DAP then sends a target reserve request to the destination DAP in order to reserve the target. The destination DAP acknowledges the request by sending a response message back.

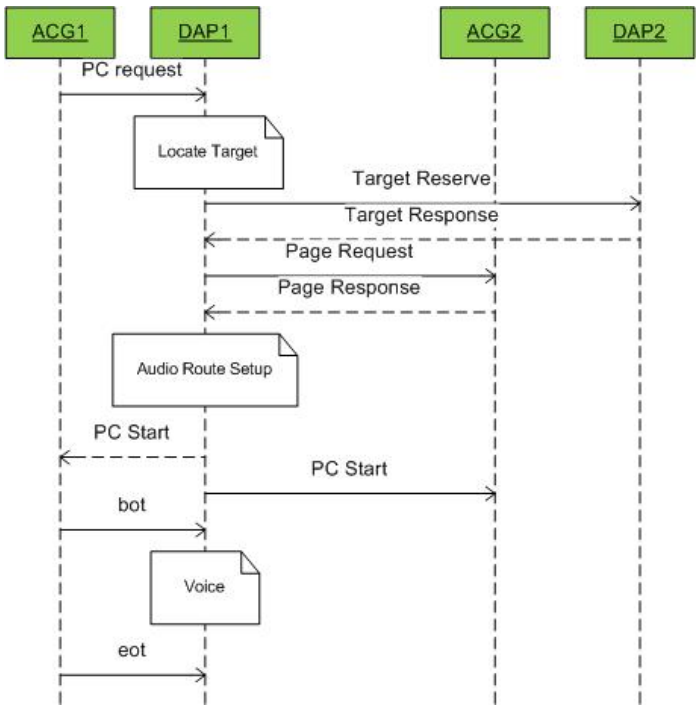


Figure C.7: Inter DAP Private Call : Part 1

- The DAP then sends the page request to the ACG to destination. On receiving the DAP does the audio route setup process and informs both ACGs to start the call.
- The originator then sends the bot, voice and eot. After receiving eot, the DAP indicates the ACGs to open channel and starts the hang timer.
- If the destination wants to transmit voice packets, it sends the update request to the DAP. On receiving the request, the DAP will stop the timer and tell the ACGs to continue the call.
- After the voice packets are being exchanged, and when the hang timer expires, the DAP indicates the ACGs to stop the call and the call ends.

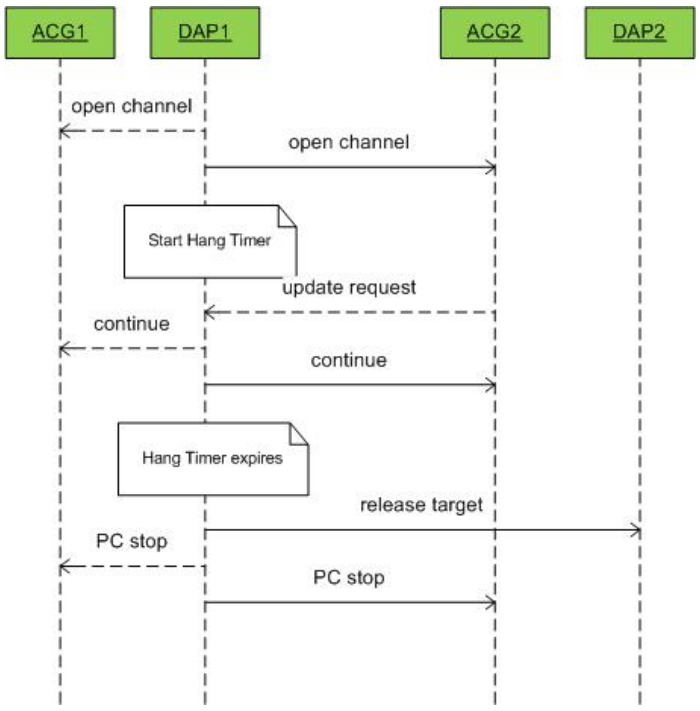


Figure C.8: Inter DAP Private Call : Part 2

Inter Urban Private Call

Figures C.9 and C.10 represent the flow of an Inter urban call.

The following are the steps explaining the flow of an Inter urban call.

- Since this is an Inter urban call the communication between the originator and the destination, as far as the call setup is concerned, will take place via DAPs only and not directly.
- The ACG of the originator will send private call request to its serving DAP.
- The DAP in turn will find the destination in its D-VLR and RCR. If the destination is not under the coverage of the DAP, it will send a routing request to the iHLR with the UFMI (Universal Fleet Member ID) of the destination. The iHLR in turn will send back the ISDN of the destination DAP.

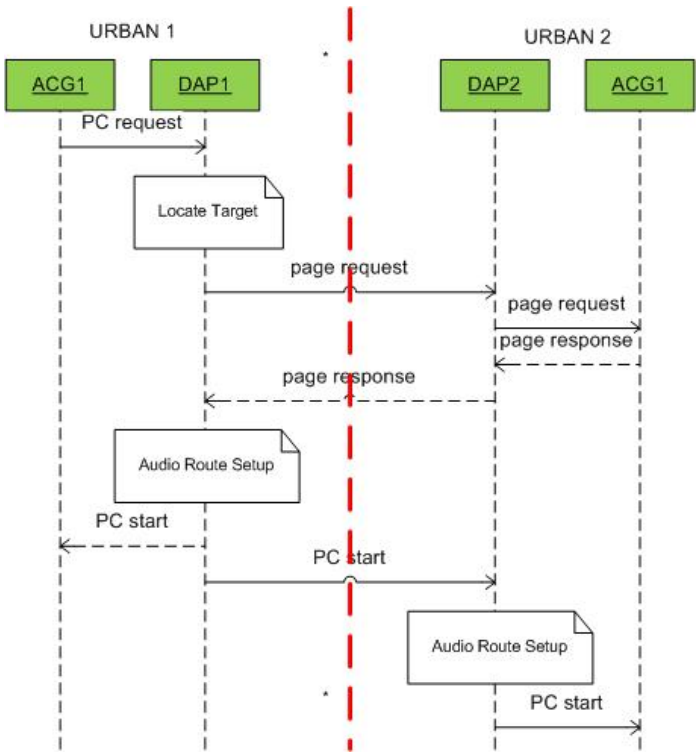


Figure C.9: Inter Urban Private Call : Part 1

- Once the destination DAP is found, the originator DAP will send page request to the destination DAP which will forward it to the destination ACG.
- On receiving the page response via the destination DAP, the originator DAP does the audio setup and informs its ACG to start the call.
- The destination DAP will setup the audio routes and will forward the PC start message sent by the originator DAP.
- The originator sends the bot. the voice packets will then be routed with the help of APD and the iDAC. Since this is an Inter urban call, the voice packets will first reach APD from ACG and then to iDAC of the originator.
- The originator iDAC will then forward the voice packets to the destination iDAC. The destination iDAC forwards it to its APD which finally routes the

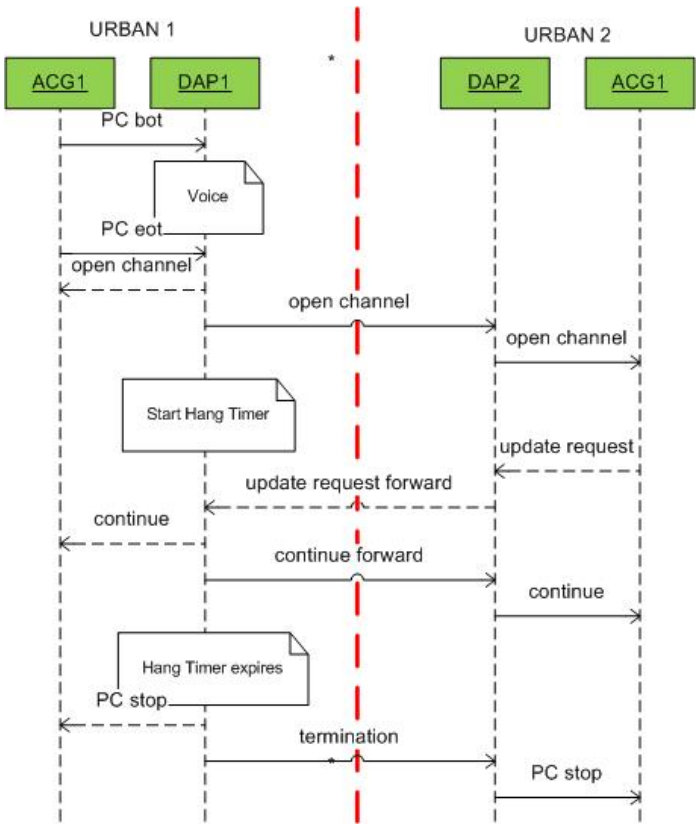


Figure C.10: Inter Urban Private Call : Part 2

voice packets to the destination ACG.

- After the originator has finished with the transmission, it will send the eot. The DAP will indicate the ACG to open channel and the destination ACG will receive the message via it's DAP.

- Then the same procedure of update request and then termination takes place. The only difference is that the communication will be through the DAPs where the originator's DAP will be in the commanding position and the destination DAP will just forward the messages to the destination ACG.

C.2.2 Group Call

As explained in the earlier chapters, the group call facility of iDEN allows a group of users to communicate with each other. The users of the group call have to be in the same talk group.

There are different kinds of group calls that a user can subscribe to. The main kinds of group calls are the local area group calls, selected area group calls and the wide area group calls.

The local area group call service allows the user to communicate with the group members present in the local or the home location area. The selected area group call, as the name suggests, allows the user to make a group call to the members present in its home and some selected location area. While the wide area group calls allows the users to communicate with the members in all the location areas.

The Figures C.11 and C.12 represents a typical group call scenario.

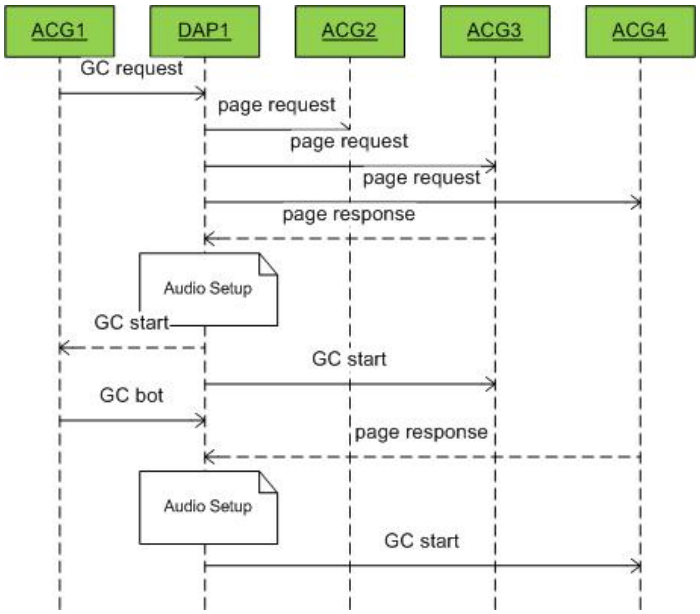


Figure C.11: Group Call : Part 1

The following are the steps explaining the flow of a group call.

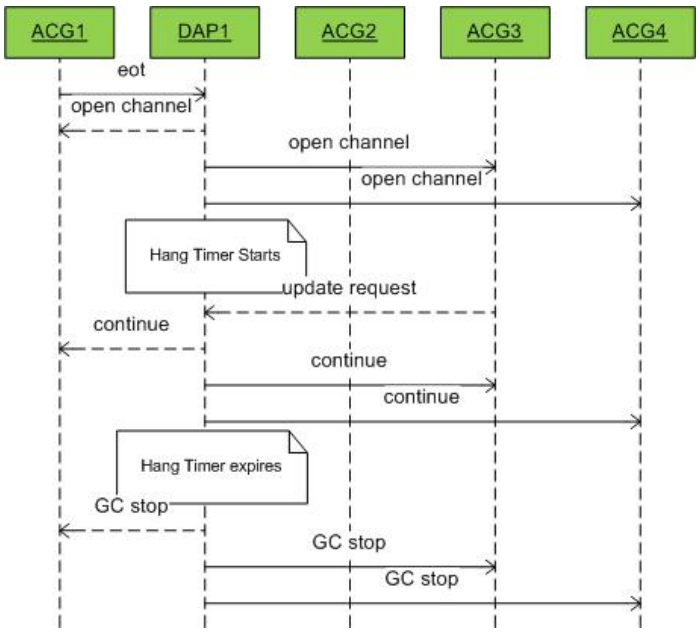


Figure C.12: Group Call : Part 2

- In the same way as in the private calls, here also the originating ACG will send a group call request to its serving DAP.
- The DAP in turn will send a page request to all the member ACGs on the basis of the type of the group call requested or allowed to the originator.
- Now in case of group call even if one of the group members respond to the page request the DAP setup the audio routes and will indicate the ACGs to start the group call.
- The originator sends the bot voice and the call starts.
- Now while the call is in progress, if any other group member responds to the page request, the DAP will setup the audio routes for that member and will indicate it to start the call.
- Then the end of transmission messages will trigger the DAP to send an open channel message to all the participating members and will start the hang timer.

- If any other member updates the call, then the call will continue otherwise the hang timer will expire and the DAP will send the Group Call Stop message to all the participating members and the call ends.

References

[1] Motorola Solutions Inc., *iDEN System Overview and Functional Description*, System Release 18.0, August, 2010.

[2] Motorola Solutions Inc., *iDEN System Overview and Functional Description*, System Release 17.0, September, 2008.

[3] Motorola Solutions Inc., *iDEN System Overview and Functional Description*, System Release 16.0, October, 2007.

[4] Motorola Solutions Inc., *iDEN Technical Overview*, August, 1996.

[5] Motorola Solutions Inc., *Guide to Motorola Acronyms and terms*, June, 2010.

[6] Motorola Solutions Inc., *Vector Sum Excited Linear Prediction 4200 bit per second voice coding algorithm for the Motorola Integrated Radio System*, September, 1994.

[7] Motorola Solutions Inc., *Technical Manual, iDEN EBTS, Base Radios*, January, 2010.

[8] Motorola Solutions Inc., *Technical Manual, iDEN EBTS, Radio Frequency Distribution System*, January, 2010.

[9] Motorola Solutions Inc., *Technical Manual, iDEN EBTS, Access Control Gateway*, October, 2010.

[10] Motorola Solutions Inc., *System Architecture Document for iDEN Base Site Controller*, June, 2004.

[11] Motorola Solutions Inc., *iDEN Tandem DAP Software Architecture*, System Release 13.0, November, 2009.

[12] Motorola Solutions Inc., *iDEN Dispatch Application Processor (DAP) User Manual*, July, 2010.

[13] Motorola Solutions Inc., *iDEN MDG4 System Manual*, July, 2010.

[14] Motorola Solutions Inc., *System Architecture Document for MDG4*, May, 2006.

[15] Motorola Solutions Inc., *System Architecture Document for Highly Available iHLR*, January, 2003.

[16] Motorola Solutions Inc., *iDEN Home Location Register User Manual*, September, 2009.

[17] Motorola Solutions Inc., *iDEN Enhanced Global Title Translation Table Tool (EGT4) User Manual*, October, 2009.

[18] Motorola Solutions Inc., *OMC-R System Overview*, March, 2010.

[19] Motorola Solutions Inc., *SAD for SR9.8 OMC-R Network Architecture*, March, 2010.

[20] Motorola Solutions Inc., *iDEN RF Interface Layer 1*, March, 1998.

[21] Motorola Solutions Inc., *iDEN RF Interface Layer 2*, June, 2004.

[22] Motorola Solutions Inc., *iDEN RF Interface Layer 3 General Aspects*, March, 1998.

[23] Motorola Solutions Inc., *iDEN ACG-BRC and ACG-ACG Interface Messages*, March, 1998.

[24] Motorola Solutions Inc., *iDEN MLC-EBTS Interface Messages and Procedures*, August, 2005.

[25] Motorola Solutions Inc., *EBTS Backhaul: Frame Relay DS0 Requirements*, September, 2004.

[26] Motorola Solutions Inc., *iVPU-ACG Interface Control Document*, June, 2007.

[27] Motorola Solutions Inc., *DAP-iVPU Interface Control Document*, October, 2005.

[28] Motorola Solutions Inc., *MDG-iVPU Interface Control Document*, October, 2005.

[29] Motorola Solutions Inc., *iDEN MDG-ACG Interface Messages and Procedures*, March, 2005.

[30] Motorola Solutions Inc., *iDEN DAP-MDG Interface Messages and Procedures*, August, 2010.

[31] Motorola Solutions Inc., *iDEN DAP-HLR Interface Messages and Procedures*, June, 2010.

[32] Motorola Solutions Inc., *GT4-iDEN-HLR/D-VLR Interface Control Document*, October, 2001.

[33] Motorola Solutions Inc., *Call Scenarios for Dispatch Calls*, May, 2004.