TEC
TELECOMMUNICATION ENGINEERING CENTRE

NEWSLETTER

VOL 6 JULY 2002 ISSUE 3

OPERATIONS SUPPORT SYSTEMS

IN THIS ISSUE

Foreword

Opening up of the telecom market has brought in a competitive environment wherein the operators have to tailor their networks to meet the demands of customers varying from plain telephone to high-speed interactive multi-media mobile services, in a cost effective manner. Next Generation Networks are envisaged to facilitate convergence based on packet technologies.

In an open and competitive scenario, network operators look towards providing the services with an excellent quality, reducing the costs and increasing revenues. Operations Support Systems for Network Management, Billing & Customer care, Fraud Management etc., play an important role in improving the network performance, enhancing the customer satisfaction and increasing the return on investment.

I am happy to note that Telecom Engineering Centre has been disseminating information on various technological developments related to telecom, through TEC Newsletter.

Dr. D.P.S. Seth
Member (Services)
Telecom Commission

CDOT NMS

CDOT has developed a Network Management System (CNMS) which supports the functionality of Performance Management, Configuration Management and Fault Management in the network. The system collects traffic, alarms and other data from network elements; analyses the data; provides tools through application software for better management of traffic and faults. It is an effective management tool for network performance analysis and also dimensioning of the network. The system is also capable of generating reports on performance analysis and other management reports.

The system has been field-tried at Kolkata, Goa and Bangalore by interfacing to E10B, OCB-283, AXE-10, EWSD, 5ESS and C-DOT exchanges. BSNL is in the process of implementing it in their network.

System Description

The architecture of the CNMS is schematically shown on the next page. The OMC ports of the exchanges are connected to NMS through leased lines terminated in the modem rack. The connectivity is possible through RS232 or X.25 protocols. The data is obtained on-line from exchanges through Mediation Devices by automatically issuing exchange commands for periodic collection of data. The periodicity of monitoring is minimum 5 minutes; however, this value may vary depending on the speed of OMC of exchange. The data collected from the OMC ports (on the flow or through file transfer) is stored in a data base server. The operator terminals, which are connected to server via LAN, can run application programs and generate different reports.

Different components of CNMS are explained below:

(i) **Network Server:** This is a SUN ULTRA I Workstation installed with SOLARIS 2.6 Operating system (ULTRA II Workstation or a Pentium PC can be used depending on the number of exchanges to be monitored). It handles the Mediation Device for Data Collection from various exchanges, maintains database of collected information by the Mediation Device. It also supplies the information from the Data Base to the operator terminal on demand.

(ii) **LAN Terminal Server (LTS):** It is a Serial Port Multiplexer where individual port can be accessed over LAN using TCP/IP.

(iii) **Modem Rack:** It consists of a set of Modems connected with single power supply and provides interface to MODEMS at exchanges.

(iv) **8 Port UTP Hub:** It provides terminating points for all the elements on the Ethernet

LAN and Networking facility to all the elements of the NMS.

(v) **Admin Control Terminal:** It is a PENTIUM P3 CPU 400 MHZ with 64 MB RAM and at least 6GB HDD, which acts as, an Administrative Control terminal. It is also used as an operator terminal. This terminal also runs PAGING Application.

(vi) **Operator Terminals:** These are PENTIUM P3 CPU 400 MHZ with 64 MB RAM. The terminals run CNMS applications and allow monitoring of exchanges. Printer is connected to one of the terminal.

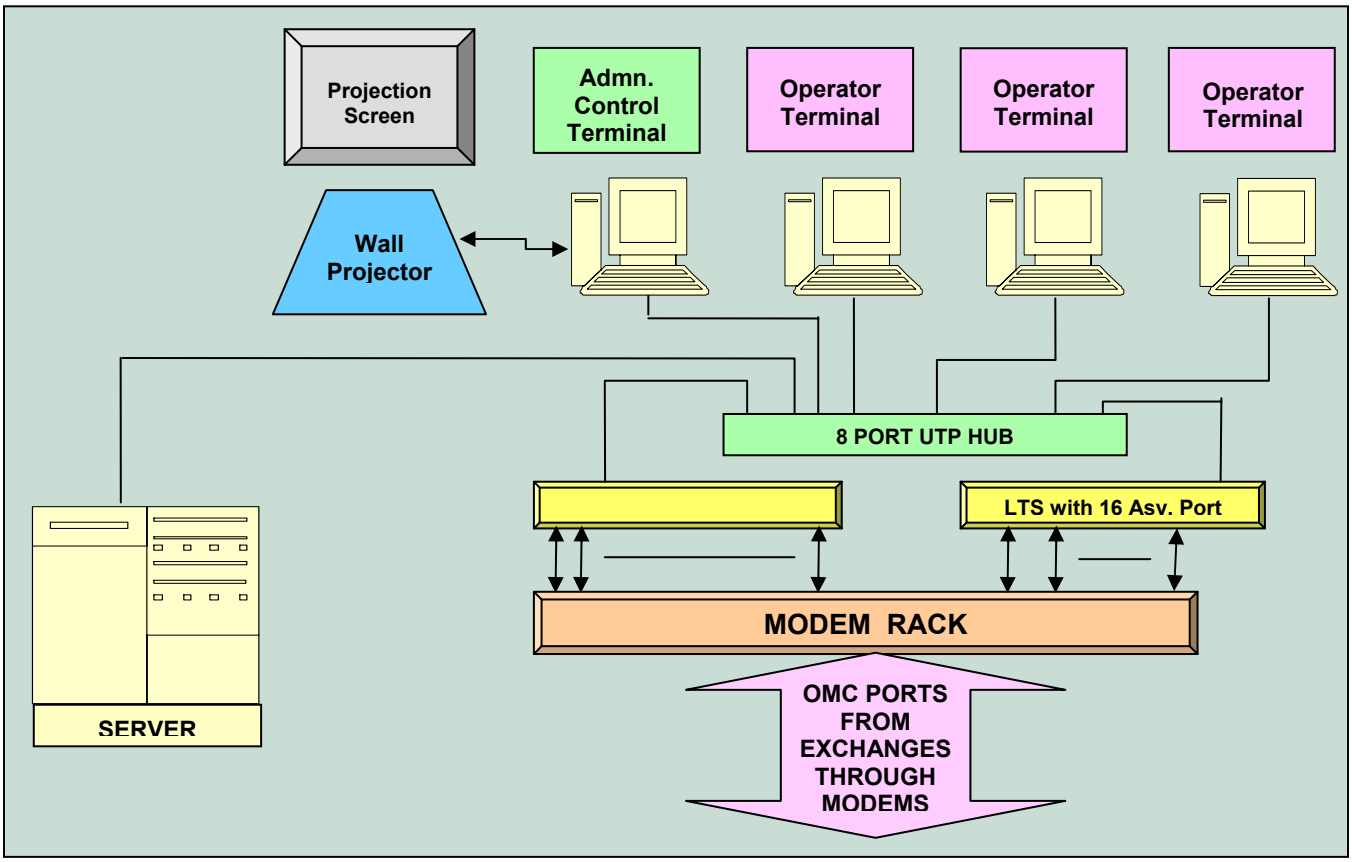
(vii) **Wall Projection System:** A Projection system is used to project the data from one of the Operator terminal.

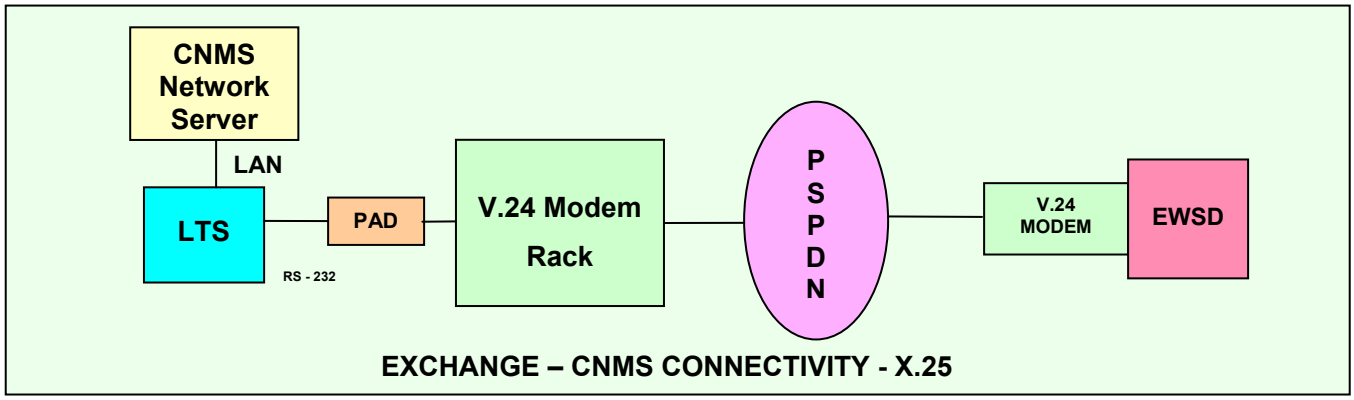
Application software

The system has the following application programs which can be run either through Administrative Control Terminal or Operator Terminals:

- *Net Analyser:* Responsible for preparation of graphs, reports based on the parameter collected.
- *Net Alarm:* Prepares the report on alarm.
- *Net Alert:* Details the list of Threshold Crossover Alarm.
- *Net Config:* Configures the Exchanges, circuit groups, RLUs, Destination, Alarm Severity and Category.
- *Net View:* Gives the Geographical view of the network along with the status of the exchanges.
- *Net Watch:* Gives the current details of traffic parameters of exchanges, circuit groups, RLUs and destination in tabular form.
- *Net Wizard:* Configures the control commands, demand reports and issue control commands.

With the help of above application programs, the system can generate different reports on traffic parameters, alarms etc.





EXCHANGE – CNMS CONNECTIVITY - X.25

Generation of Reports and Graphs

The system generates reports and graphs on the following data/ parameters:

Exchange

- Bids
- Total over flow
- Call Completion Ratio (CCR)

Circuit Groups

- Bids
- Mean holding Time in Seconds (MHTS)
- Seizures
- Out of service circuits
- Answer to Seizure Ratio (ASR)
- Over flows
- Answer to Bid Ratio (ABR)
- Equipped Circuits
- Outage
- Busy circuits
- Occupancy
- Traffic in Erlangs.

RLU

- PCM links out of service
- Outage
- O/G Rejection Call Blocking
- I/C Rejection Call Blocking

Additional Reports

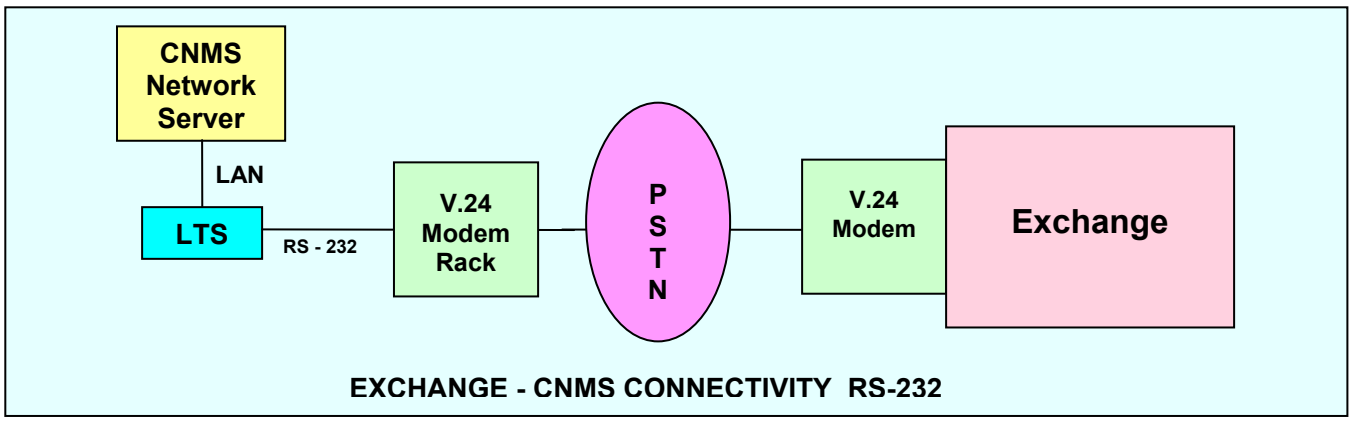
- Summary report on congestion
- Exchange performance report.

Presentation of alarms and data

CNMS supports a geographical navigation tool that shows the exchanges and their corresponding links with the geographical map as the background. It also provides the visual clue of the alarm status of the exchange with different colours, denoting the severity of the alarm. Links with critical alarms are shown. It provides the accessibility to invoke full alarm details display for the exchange, and to display the RLUs for the specified exchanges and to show the link details.

The system lists the current alarms for each exchange in a tabular form. The different alarms are categorised based on severity like critical, urgent and non-urgent and normal.

Traffic data can be presented in graphical form, which can be on Single parameter, multiple parameters, Maximum, Minimum & Average values. Single parameter can be for an interval on a day or range of days. Multiple parameters can be set for a particular hour on a day or over a range of days. All displays can be projected to a Wall Projection System.



EXCHANGE - CNMS CONNECTIVITY RS-232

FRAUD MANAGEMENT AND CONTROL CENTRE

Fraud in Telecom is an act committed to deprive the rightful revenue to the telecom service provider, which affects the profit margin of the service provider. Besides revenue loss, it spoils the reputation of a service provider and creates lack of confidence in the genuine subscribers. The objective of Fraud Management and Control Centre (FMCC) is to detect, analyse and control various frauds in a telecommunication network.

Frauds: some examples

Frauds in telecommunication network have different forms and can be broadly classified as 'non-technical' and 'technical' frauds.

- **Non-technical frauds**

Examples of non-technical frauds are:

Clip-on Fraud: fraudster accesses the DP/MDF and diverts the line and makes calls or sells calls to others.

Subscription Frauds: Fraudster registers for phone service, makes large number of calls (call selling) and runs away.

Premium Rate Service (PRS): Large number of calls will be made to the PRS and bills will not be paid but service provider collects revenue share from network operator.

- **Technical frauds**

They are committed by gaining access to the system. Some of such frauds are manipulation of databases (billing, charging, routing, etc.) through man-machine commands by authorised/unauthorised persons.

Frauds in cellular mobile networks are committed by cloning (duplication) of SIM cards.

Fraud detection techniques

The fraud detection is done in two ways namely 'real time' and 'near-real time'.

- **Real time detection**

It is based on the analysis of messages on the CCS7 signalling links. These links are monitored in a non-intrusive manner by connecting probes with high-impedance in parallel to the CCS7 signalling links. FMCC builds Call Detail Records (CDR) in real time by analysis of various call related parameters like calling number, called number etc. in CCS7 messages. Fraud detection is possible by analysis of usage profile, call patterns, calling trends derived from CDRs and correlation of certain user defined parameters using software models. The detection is achieved through various techniques:

(i) Thresholds

The FMCC can detect crossing of certain thresholds which are user programmable. Subscribers can be divided into groups like Home Group, Office Group, Business Group etc. Thresholds can be set separately for any subscriber group. Typically the Threshold values are:

- Maximum duration of a single Call (peak, off-peak period)
- Aggregate call duration
- Maximum metered units per call for STD/ISD,
- Aggregate call value in metered units
- Number of call attempts within a defined period.

System generates an alert to the manager, whenever any of these thresholds are crossed.

(ii) *Call Patterns*

Any field (s) in the CDR can be predefined for generating a call pattern alert. The pattern may be calling number, called number, access code, country code etc., which is defined by the user. When the field in CDR matches with the predefined pattern, an alert is generated.

(iii) *Profile comparison*

Detection of fraudulent behaviour is done by comparing the profile with the normal usage of individual subscribers. The subscriber profile is

maintained for each subscriber (for working day as well as holiday) based on the usage and a calling pattern. The Subscriber profile contains data such as average metered units per call for STD/ISD, average number of call attempts, country codes and national areas dialled. Profile is updated by the system periodically based on the usage and calling pattern of each subscriber.

(iv) *Destination check*

Detection by checking whether the called number is figuring in the normally called destinations by individual subscribers.

(v) *Geography/velocity check*

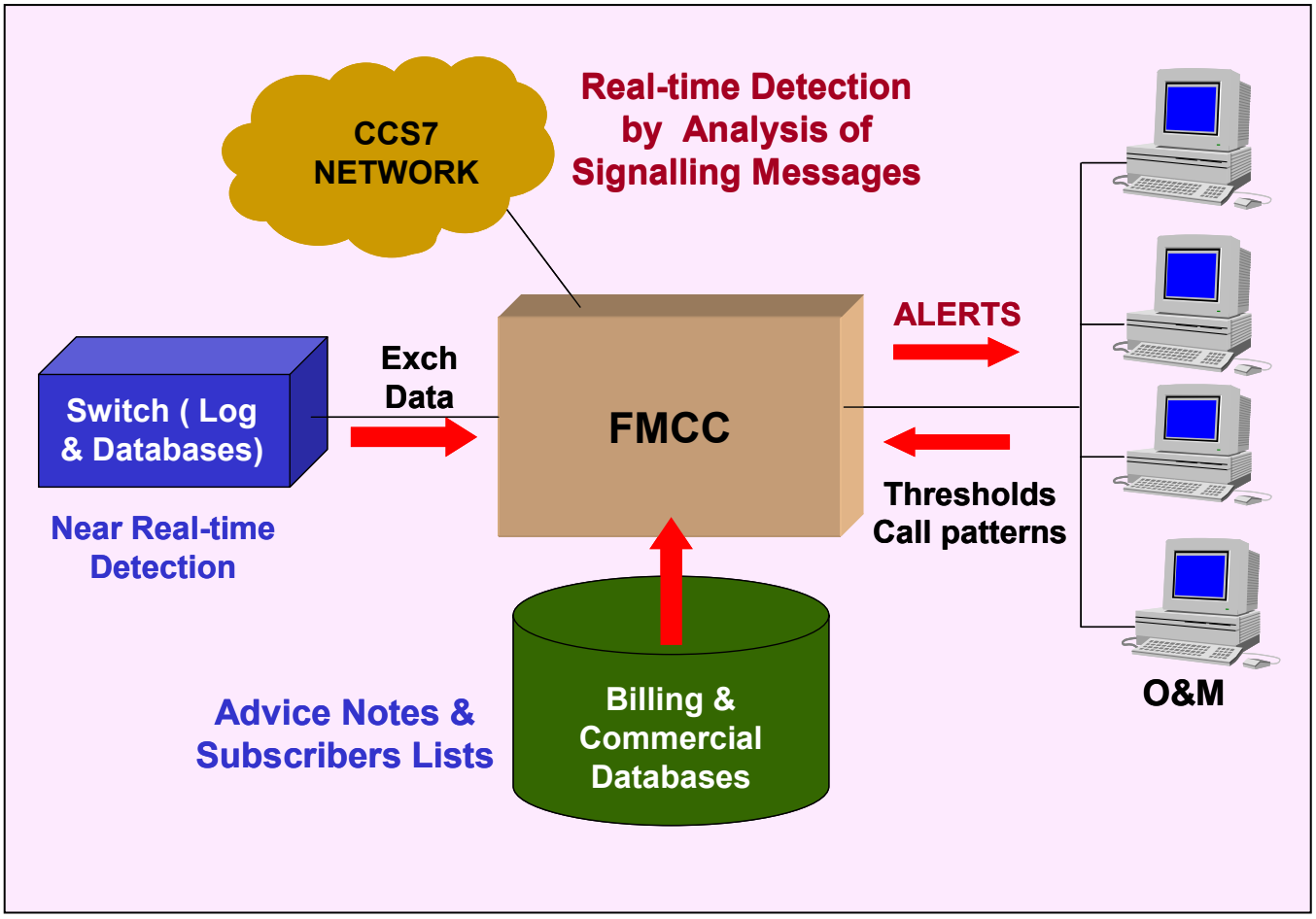
Detection of calls from geographically separated places with unlikely/unrealistic travel times, originated with a single telephone identification number (as in the case of mobile 'cloning').

- **Near real time detection**

To detect fraud in near real time, the system is interfaced to various switching systems to collect the office-data related to routing, charging and subscriber administration along with OMC log. It is also connected to commercial system for accessing data bases. The data is collected at pre-programmed intervals. The subscriber administration commands are audited against valid Advise Notes or disconnection/ reconnection orders. The data integrity of routing, analysis and charging is compared with the previously collected database and an error list is generated which can be analysed by the manager.

FMCC Architecture

FMCC consists of centralised equipment which controls several Remote equipment.



- **Remote site equipment**

It monitors the CCS7 signalling links in a non-intrusive manner, for building CDRs and interfaces with switching systems and commercial systems through mediation devices, for collecting relevant data. The data is filtered as per requirements and transferred to central site through Wide Area Network (WAN), for processing.

- **Central site equipment**

Central site equipment receives data from various remote equipments using WAN. The software algorithms for analysis of the data for detecting various frauds are available at central site. It supports multi-user work-stations for administration of the FMCC.

- **Wide Area Network**

WAN provides the communication between the Remote equipment and Central equipment using 2 Mbps E1 link or single/multiple links of 64 kbps as per requirements.

Reports of Alerts and Fraud cases

On detection of a suspected fraud, FMCC generates alerts to the manager. Based on the criteria defined by the manager, alerts are converted into detailed cases, which include all relevant information needed to facilitate investigation by manager, who can initiate manually initiated actions. Automatic actions by the system are also possible.

Pilot Project

A pilot project of FMCC is being implemented by BSNL at Hyderabad based on TEC GR No.G/FMC-01/01. July '99, to ascertain the efficacy and viability of such system. The project is meant for fixed network and envisages monitoring of sixteen CCS7 signalling links in OCB-283 for STD and ISD calls. CDRs are generated, filtered and transferred to the Central site using 2 Mbps OFC link. Twenty one exchanges are planned to be connected to FMCC for near-real time fraud detection and internal frauds. EWSD exchanges are interfaced on X.25 links while E10B, OCB-283 and 5ESS exchanges are connected using RS232. These exchanges are connected to FMCC using leased lines. Billing and commercial system based on DOTSOFT is also interfaced to FMCC for collection of commercial data. The equipment has been installed and the testing by TEC is nearing completion.

Emails @ TEC

Email addresses in TEC Head Quarter have been changed.

Following is the list of email addresses for TEC Head Quarter and Regional TECs:

Designation	Email Address
Sr.DDG (TEC)	srddgtec@bol.net.in
DDG (E)	ddge@bol.net.in
DDG (I)	ddgi@bol.net.in
DDG (N)	ddgn@bol.net.in
DDG (R)	ddgr@bol.net.in
DDG (S)	ddgsw@bol.net.in
DDG (SAT)	ddgsat@bol.net.in
DDG (T)	ddgt@bol.net.in
DDG (V)	ddgv@bol.net.in
DDG (ER)	ddger@cal.vsnl.net.in
DDG (CR)	ddg.crtec@hd1.vsnl.in
DDG (NE)	ddgnetec@hd2.dot.net.in
DDG (NRC)	ddgnrc@del2.bol.net.in
DDG (RC)	ddgrc@bol.net.in
DDG (SR)	rtecsrbg@hotmail.com
DDG (WR)	ddgwrc@vsnl.net.in

Approvals issued by TEC during the period April 2002 to June 2002

Type Approvals.....	175
Interface Approvals.....	73
Service Test Certificates.....	41
Total	**289**

Approvals issued by TEC upto 31.06.2002

Type Approvals.....	5663
Interface Approvals.....	3346
Service Test Certificates.....	1458
Grand Total	**10467**

IMPORTANT ACTIVITIES OF TEC DURING THE 1st QUARTER OF 2002 - 2003

A. Preparation of GRs/IRs & Technical documents

Following GRs/IRs and Technical documents issued:

GRs for

- Frequency Counter (10 MHz to 40 GHz).
- Optical Router.
- RF Power Meter (50 MHz to 40 GHz).
- Spectrum Analyzer (50 MHz to 40 GHz).
- Synthesized Signal Generator (1GHz to 40 GHz).
- Tester for Gas Discharge Tube and Positive Temperature Coefficient Thermistor.
- Wireless LAN.

Revised GRs for

- 2GHz, 4 x 2 Mbps Digital Microwave Equipment (Hot standby configuration & Frequency Diversity configuration).
- 2 GHz, 2 Mbps Digital Microwave Equipment (Hot standby configuration).
- 2 Mbps Digital Echo canceller.
- Computerised Cable Record Management System.
- Cable Record Purification System.
- STM-1 Synchronous Multiplexer.

IR on

- Interchange of STM-1 signal at 155 Mb/s port between the networks.

Revised IR on

- Charge Indicator.
- Cordless Telephone Hand Set.
- System employing Computer Telephony.

Test Schedule for

- 2GHz, 4 x 2 Mbps Digital Microwave Equipment
- Buttinski Telephone Hand Set.
- Cable Record Maintenance system.
- Cable Record Purification System.
- Frequency Counter.
- Revised IR of integrated Media Gateway.

B. Tests and Field trials

Tests/field trials have been carried out for:

- 15 dBi and 17 dBi antenna of M/s Kaveri Telecom for CDMA WLL Base station.
- ATM Switch of CDOT.
- BNRC (Atomic Clock).
- Charging problems on VCC in CDOT IN system.
- CDOT call monitoring system for IMPCS additional features.
- CorDECT system with Internet Access of M/s ECIL.
- DWDM 32 chl of M/s ARM.
- Ericsson IN system of North Zone BSNL IMPCS project.
- IKON RAS model 4400.
- Lucent MSC & IN System of West zone BSNL IMPCS project.

C. Other Activities

- Manufacturer Forum conducted for:
  - 64 Kbps cross-connect with 2048 Kbps excess port.
  - 20m, 30m light weight towers, 40m narrow base tower and 15m self supporting mast.
  - ADSL Broad Band Network.
  - DCME with 16:1 and 20:1 gain.
  - Firewall.
  - IP Telephone.

TEC NEWSLETTER
Julyl 2002
Volume 6
Issue 3

Editor :
I. S. Sastry
DDG (S)
Phone : 3329540
Fax : 3723387
Email : ddgstec@del2.vsnl.net.in

Telecom. Engineering Centre
Khurshid Lal Bhavan
Janpath
New Delhi 110 001.