G) Enhancements and re-vamping of RRCAT Website:

RRCAT website has been enhanced with new look and feel. The web pages have been re-designed and re-arranged with updated contents. The look and feel has been changed using smart drop down menus and cascading style sheets for easy and quick navigation of the website. The contents for Immovable Property Returns of Group A employees have been deployed in PDF format for the calendar year 2012. The website has been regularly updated by deploying scientific contents of various divisions and documents related to recruitment, tenders, conference/ workshop etc.

A 'Website Update Notification System' with automated voice calls and email alerts has been developed and integrated with website updating mechanism. The automated system generates email alerts for web site administrators, whenever website is updated. The alert contains listing of modified files after every updation of the website. This facility will be very useful to monitor unauthorized website updates, in case the website gets updated or changed by un-authorized persons.

Reported by:
Alpana Rajan (alpana@rrcat.gov.in) and Anil Rawat

I.3: Developments in Networking and Communication at RRCAT

(A) Commissioning of new 10G Ethernet Network Core Switch:

New chassis based core switch (Black Diamond BD8810) has been commissioned in place of the aging core switch in IT building, so as to upgrade RRCATNet backbone and server connectivity from the existing 1 Gbps to 10 Gbps. The new core switch has aggregate switching capacity of 3872 Gbps (full duplex), backplane switching capacity of 1320 Gbps (full duplex) and aggregate throughput of 2840 Mpps. It has 24 nos. of 10Gbps optical fiber ports, 48 nos. of 1Gbps optical fiber ports and 192 nos. of 1 Gbps copper ports.

The new switch has been configured in failover, redundant mode with another core switch in IT Extension building. Critical network services have been configured in load balance and failover mode, for providing uninterrupted services to users, on round the clock basis. All building rings (08 nos.) have been migrated to the new core switch. Firewall and routing configurations have also been migrated from the replaced core switch to the new core switch.

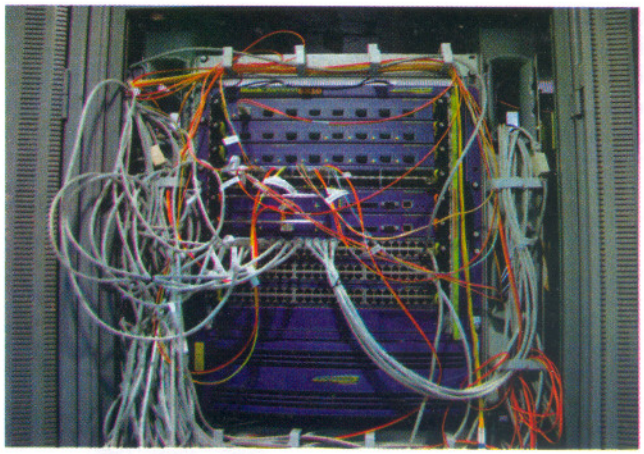

Figure I.3.1: Rack view of newly commissioned core switch BD8810

Figure I.3.1, illustrates rack view of new BD8810 core switch, installed in IT building. The commissioning of the new core switch with zero network downtime was achieved by utilizing the failover configurations of the existing core switches.

(B) Design, Development and Deployment of Network Node Life Cycle Management System (NNLMS):

Network Node Life Cycle Management System is designed, developed and deployed on RRCATNet, to record and manage information related to various network activities performed on various network nodes attached to RRCATNet. Information related to every network node's physical location, connectivity status at different times, details of Internet accesses and email transactions performed from a node, throughout its entire life cycle is managed in this system. This helps in performing forensic analysis of network nodes. The system uses connection logs stored in Network Access Control (NAC) server, Dynamic Host Configuration Protocol (DHCP) server logs, mail server logs and proxy server logs stored in various servers, converts the flat log files into database and provides intuitive interfaces for performing correlational analysis and report generation. The system is developed using PHP, java scripts and MYSQL is used as backend data store.

The system has five major modules – a) *Log file parser module* – In this module parsers have been developed to process huge log files and extract meaningful data, and store it in database for faster analysis. b) *Data updating module* - This module is developed to update the log database automatically on daily basis. c) *Comprehensive report generation module* – In this module user friendly web based application is developed to provide single point access to multiple server logs stored in database format. This module has options for generating reports related to Internet Accesses, Email transactions and network connections made by nodes on network. Query preprocessing and optimization has been

done for faster data retrieval d) *Analysis module* - This module is developed for analysis purpose. It generates pie charts, illustrating top 10 frequently accessed websites and regular mail senders/receivers (overall as well as for specific time duration) on RRCATNet.

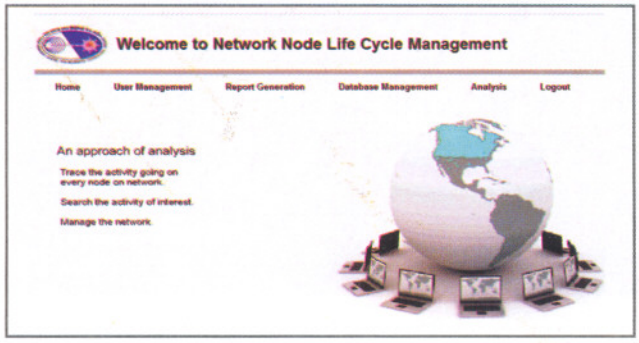

Figure I.3.2: Snapshot of administrator interface of NNLMS

Figure I.3.2 is a snapshot of administrator interface of NNLMS, showing different available options. Figure I.3.3 illustrates snapshot of Internet access report generated from NNLMS.

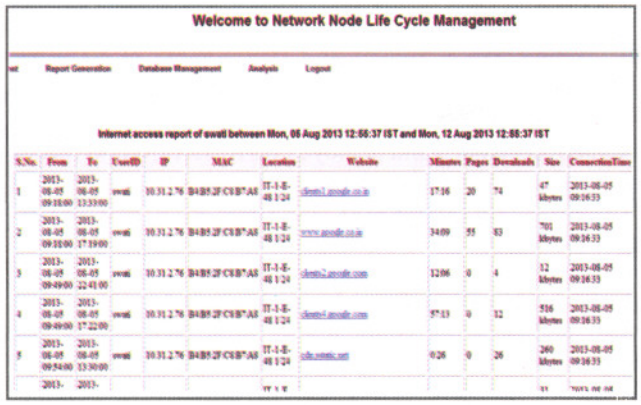

Figure I.3.3: Internet access report generated using NNLMS

Figure I.3.4, is a snapshot of email transactions report, with Date/Time, From, To, Subject, Mode, IP address, MAC address, connection time and location details.

Figure I.3.4: Email transaction report generated using NNLMS

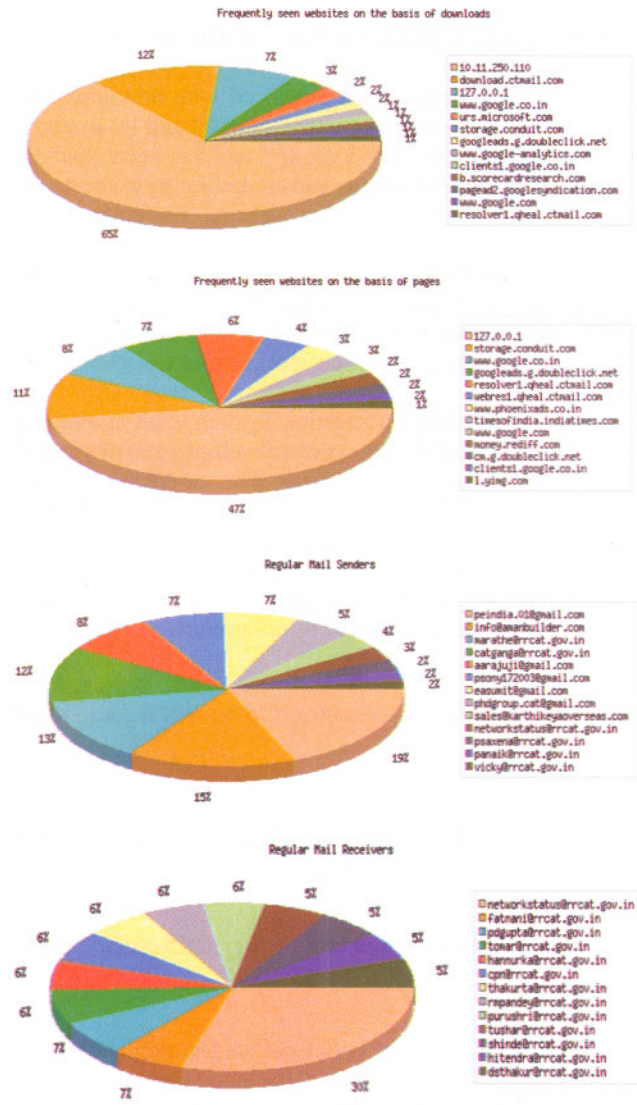

Figure I.3.5: Pie Charts illustrating detailed analysis.

Figure I.3.5 illustrates snapshot of pie charts generated using NNLMS. It shows top 10 frequently visited websites on page number wise and download size basis and top 10 mail senders and receivers on RRCATNet.

C) Design, Development and Deployment of proactive Website Intrusion Detection System (WIDS):

Message Digest (MD5) checksum based Intrusion Detection and Prevention System is designed and developed for strengthening security of RRCAT official website. It works on the concept of checksum calculation for the entire set of static pages of the website. Whenever website contents are modified by authorized persons, changed checksum is calculated and stored. This stored checksum is compared with the checksum calculated on the fly by a background process, executing on a different server. This system plays a key role in ensuring the integrity of the website which can be caused by any unauthorized

modification. If somehow, integrity of the website is compromised, WIDS automatically blocks the website and sends an unauthorized modification alert to the system administrators in the form of voice and email alerts. WIDS has provisions for performing authorized website updates. WIDS is successfully deployed on three number of web servers placed in Internet De Militarized Zone (DMZ) of RRCATNet.

(D) Design, Development and Deployment of proactive network administration system using voice and email alerts:

This system is designed, developed and deployed for performing proactive administration of RRCATNet. This application generates voice and email alerts in case of unauthorized modifications to RRCAT website, change of status of network switches, crossing of temperature of switches above a defined threshold and change in status of Internet links attached to RRCATNet. Open Source based Asterisk server is configured for generating voice call alerts. The major benefit of this system is that the network administrator gets immediate alerts about change in status of various devices and services, which substantially reduces their response time for attending a problem and rectifying the problem.

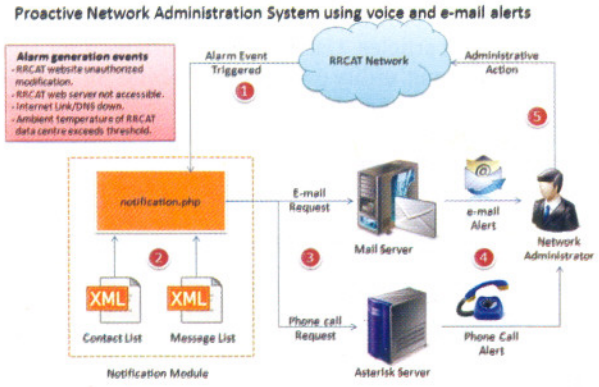

Figure I.3.6: Block diagram of Proactive Network Administration System using voice and e-mail alerts

Figure I.3.6 depicts complete block diagram of the deployed proactive network administration system on RRCATNet. Simple Network Management Protocol (SNMP), Simple Mail Transfer Protocol (SMTP) along with PHP and BASH scripting languages have been used in the development of the system.

(E) Commissioning of centralized syslog and Open Source SECurity (OSSEC) log collection and analysis setup:

For consolidating logs, generated in internet DMZ servers and perimeter level routers, required for correlational analysis, a centralized syslog and OSSEC log collection cum analysis server has been commissioned on RRCATNet. Internet DMZ and perimeter routers related logs are sent to a syslog server which in turn transfers them to OSSEC server. Similarly proxy, authentication, firewall and mail servers send logs to OSSEC server. The OSSEC server raises an alert to the system administrator in the form of emails in case of any threat detected by parsing logs. The system generates automated alarms on occurrence of unusual log events. Open Source Software, Log Analyser (ver. 3.4.3), is installed on syslog server for graphical display of all the logs collected from different servers and routers.

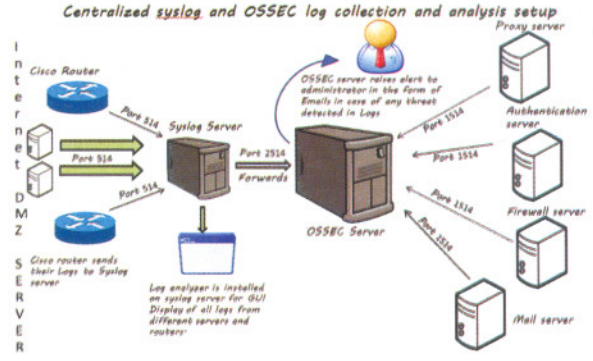

Figure I.3.7: Block diagram of centralized syslog and OSSEC log collection and analysis setup

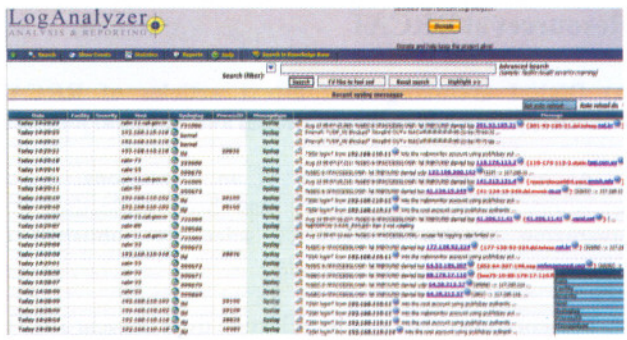

Figure I.3.8: Snapshot of GUI of centralized syslog and OSSEC log collection and analysis setup

Figure I.3.7 depicts block diagram of the centralized syslog and OSSEC log collection and analysis setup. Figure I.3.8 shows snapshot of Graphical User Interface (GUI) of the centralized syslog and OSSEC log collection and analysis setup.

F) RRCATNet Expansion and Upgradation:

Commissioning of five numbers of new OFC (Optical Fiber Cable) segments, providing 1 Gbps connectivity, between a) New CAP building and B-block building, b) LBAID building and CTL building, c) MDL and Ferrite building, d) UHV&MFL building and SCRF building and e) New CAP and User Hall building, has been completed.

Commissioning of building Local Area Network (LAN) is completed in 04 numbers of buildings comprising of (24-ports- IAM Ext. Building, 82-ports- User Hall, 90-ports – LBAID, 117-ports - UHV&MFL). Preventive maintenance work was carried out in all 58 numbers of network racks installed inside RRCAT premises. Limit learning has been configured on all edge switches for enhancing port level security.

(G) Expansion of communication network:

108 numbers of new telephone connections were provided at various locations in RRCAT campus (SSLD Extension, LBAID Lab., Optics Lab., UHV Lab.), 29 numbers of telephone connections were shifted to other locations as per user requirement, 21 number of Digital reflexes phones were provided with voice mail facility. Telephone lines have been commissioned in (User Lab. – 4 nos., Accelerator Magnet Technology Division – 08 nos., Physiotherapy Centre – 2 nos. and in Optical Workshop – 3 nos.). 02 number HOT Lines were commissioned between Indus and Main Gate security buildings.

Reported by:
S. S. Tomar (tomar@rrcat.gov.in) and Anil Rawat

I.4: Development in Scientific Information Resources at RRCAT

A) Digital archiving of full-text articles of RRCAT scientists published in international and national journals

As a part of development of an institutional digital repository of RRCAT, library has been collecting and organizing articles of RRCAT scientists published in international and national journals.

Present archive has article collection from the year 1987 to 2013. Two thousand sixty six (2066) journal articles have been collected and organized in the library database. For building this digital archive, copies of articles are collected from online sources such as full-text databases, SCOPUS and websites of subscribed journals. Library also collects copies of articles (not accessible/subscribed by library) by requesting authors and other sources. Articles which are available only in print version have been digitized and 'pdf' copies of those articles are included in the archive. Library tries to include all articles published in journals to make the archive exhaustive. Bibliographical details of these articles are entered in LibSys 7 (web-centric library automation software) and its soft copy is hyperlinked.

Year wise number of articles added in the database is shown in the Figure I.4.1.

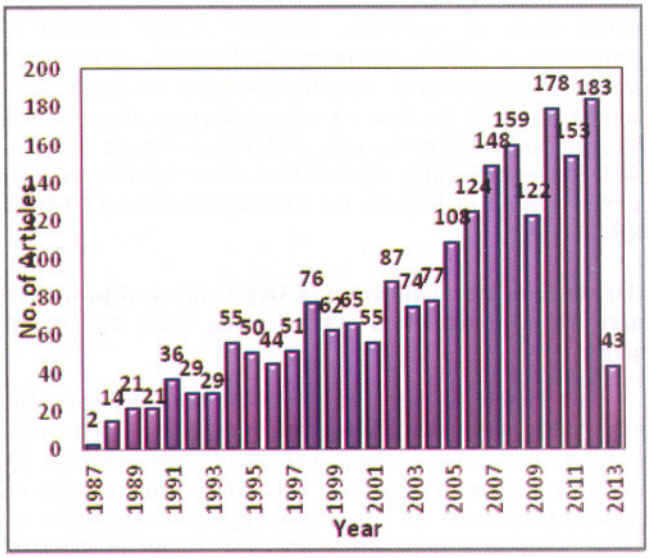

Figure I.4.1: Year wise journal articles archived in Web-OPAC.

Users can access full text of desired article through the Web based Online Public Access Catalog (Web-OPAC) on RRCATInfonet. One has to select "Article Data" database and enter the desired keywords to search articles on Web-OPAC. It is also possible to browse by author, title, journals, year wise and view full text articles. Users can save articles after login through 'My Account' utility provided in Web-OPAC. Default login and password is employee number with prefix 'cc', for example 'cc900'. Users can change password if they desire. Figure I.4.2 and I.4.3 depicts screen snap shots for searching articles and for full text view in Web-OPAC.

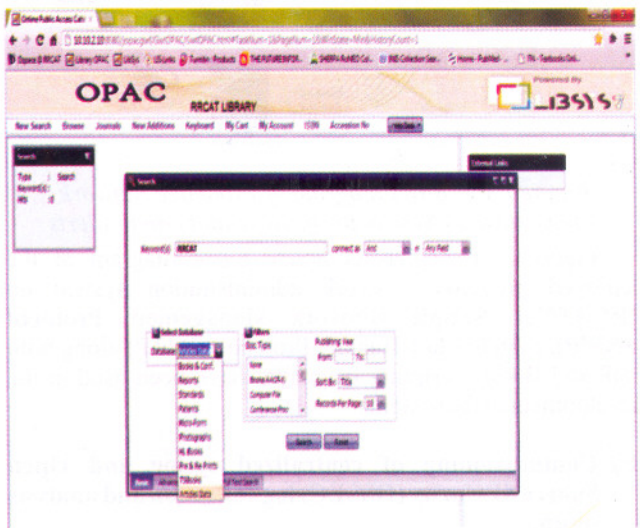

Figure I.4.2: Selection of 'Article Data' in Web-OPAC