This indicated that throughput using pooled connections is almost six times faster than non pooled connections and web applications realize significant performance improvements by using connection pooling over no connection pooling.
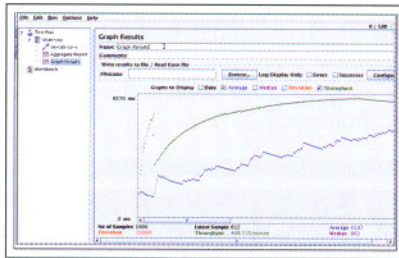

Figure I.2.7: Pooled connections throughput

Figure I.2.8: Non pooled connections throughput

D) Oracle Certifying Authority 10g setup for Digital Certificate based Applications:

Infrastructure for Oracle 10g OCA (Oracle Certifying Authority) has been setup for issuing and managing Digital Certificates. This PKI (Public Key Infrastructure) setup will be used for management of Digital Certificates that provide digital identities required to automate Digital Signature based processes.

Oracle 10g platform provides tightly integrated Oracle Certifying Authority (OCA) and Oracle Single Sign-on. The integration of Single Sign-On with OCA enables less time consuming setup for SSL communication between client, application server and database server. Oracle PKI setup needs combination of robust infrastructure for managing and distributing digital certificates and also for enforcing policies related to certificate strength and validity period.

We have configured OCA end-user interface to obtain a certificate which can be imported into user's internet browser using Single Sign-on credentials. We have imposed 1024 bits RSA key length for employees and 2048 bits RSA key length for servers/ PCs. The certificate validity period can also be defined. Unique certificate constraint has also been enabled to prevent OCA from issuing multiple certificates to the same employee.

Using this OCA PKI setup, Digital Certificates have been tested as proof-of-concept for:

- Reliable two factor user authentication - the first factor is proof of possession of private key and second factor is validation of public key belonging to specific identity by OCA.

- SSL communication for web server - client browser validates identity of a web server and encrypts data flow between browser and web server.

OCA PKI setup will be used for deployment of workflow based applications in near future.

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

I.3: Development in Networking and Communication at RRCAT

A) Email service enhancements:

In our endeavor to improve and secure the emails services at RRCAT, following enhancements were made to the email services setup:

1) Enhancements to LDAP (Lightweight Directory Access Protocol) setup:

Email accounts at RRCAT are being managed using LDAP based directory service with "ou=People,o=cat,c=in" as the base Distinguished Name (DN). This setup was upgraded by adding "Account Validity", "Account Status", "Description" and "Internet Access" attributes to each account record. Proper values of these attributes for every account (1800) were verified and then inserted in the existing database using PHP and shell scripts. Figure I.3.1 depicts email account details view showing newly added attributes.

Figure I.3.1: Email account details view

The email account request form is modified to have these fields for newly created accounts. The addition of these attributes has allowed development of necessary applications for automatic weeding out of expired accounts, thus enhancing security. The account validity for the employee accounts is taken as the superannuation date, while for non employee accounts it is to be specified by the account holder and approved by the division head with whom the person is working. The above procedure is fully implemented as an automated system for which necessary application has been developed and commissioned. Figure I.3.2 depicts the account validity expiry reminder and deletion alerts generated by the application for weeding out expired accounts. The email alerts are sent to the administrator's inbox.
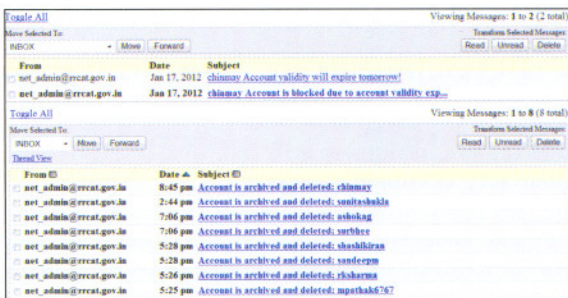

Fig. I.3.2: Account validity expiry reminder and deletion alert

2) Development of Web interfaces for Email account administration:

For creation of email accounts the open-source package - PHPLDAP Admin (version 0.9.3) - is being used at RRCAT. The package has been enhanced and account creation plugin has been modified to make it work as per our account creation policy. Figure I.3.3 depicts the web based email account creation interface, listing all the attributes required to be filled up at the time of account creation.

Fig. I.3.3: Email Account creation interface

For modification and deletion of email accounts, web based interfaces have been developed in-house - using LDAP APIs (Application Programming Interfaces) and PHP language- and packaged as a software. The software has an administrative and a guest interface. The administrative interface has different modules - a) Email account modification module: It is used to modify account attributes like "Account validity", "Account status", "Description" and "Internet status". Figure I.3.4 depicts the web based email account modification interface.
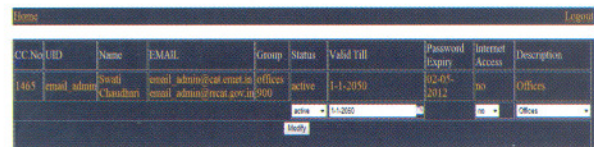

Fig. I.3.4: Email Account modification web interface

b) *Email account deletion module:* It is used to archive and delete inactive accounts. Figure I.3.5 depicts email account deletion web interface.
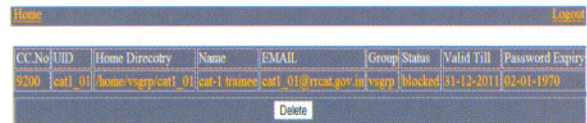

Fig. I.3.5: Email Account deletion web interface

c) *Email account search module:* It is used to search for email accounts based on various attributes of LDAP, like UID (User Identifier), ccno, group, description and account status. Various reporting options have also been developed to generate list of email accounts based on search options. Guest Interface is available to view various account reports. This development helps in better email administration by providing convenient and user friendly web interfaces for email account administration and management. Figure I.3.6 depicts search module interface.
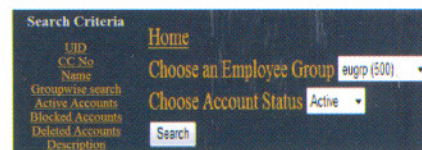

Fig. I.3.6: Email Account data search web interface

3) Development of unlock overquota email account application:

For smooth functioning of the email services, RRCAT has an overquota account locking policy. A fixed disk quota has been assigned to every user account and user email accounts are automatically locked in case of over quota. In earlier system, users were required to contact the email administrator to unlock such email accounts. A new

application has been developed which empowers users to unlock their accounts without email administrator's intervention. The users then have to prune the account till 4:00 AM on the next day and bring the account disk usage within limits. After that the account starts to operate normally. The application uses the concept of allowing temporary increase in user quota for a defined period. To avoid misuse, necessary checks have been incorporated in the application. The application has been deployed on mail server and is only accessible after successful authentication. Figure I.3.7 depicts the webpage of this application.

Fig. I.3.7: Unlock email account page

4) Development of Password change reminder application:

RRCAT has an email password policy. As per the policy users are required to change password of their single sign-on id (to access email, Internet, RRCATInfonet services) at least once in six months. If users do not change password for six months, it will expire at the end of six months, after the last change. Users can change their password by using the option available on the email login page. To help the user to remember the requirement to change password, first reminder mail will be sent one month prior to the date of password expiry. Second and third reminders will be sent fifteen days and one day prior to the date of expiry of your password. In case user still fails to change the password, though the access to email and other services will be blocked, user can still change the password by using the change password option. The password policy is available for reference at: http://cati.cat.ernet.in/catintra/nhtml/chpass.html.

The above procedure is fully implemented as an automated system. Figure I.3.8 depicts a typical password expiry email alert.
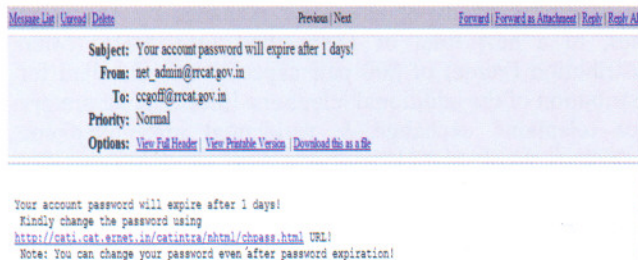

Figure I.3.8: Password expiry reminder alert

B) Commissioning of a new Failover and load balanced proxy server setup:

The new proxy server setup at RRCAT has been implemented to provide a high speed, authenticated and redundant internet proxy service to the users at RRCAT. The main objective of the implemented scheme is to maximize the utilization of two number of load balanced internet links of 34 Mbps (1:4 shared) capacity each, with uninterrupted operation, without any performance degradation and with minimal administrative intervention. The access log files generated by the SQUID proxy servers are used for generating graphical pages using squint-0.3.18 package for analysis of internet usage and utilization.

Two servers have been configured with Centos 6.0 and latest SQUID proxy software (Version 3.2.0.13). Each server has been configured to run four number of squid processes to serve proxy requests for achieving maximized response time. Each squid process uses its own cache memory and generates individual log file. Multiple log files generated in the process are sorted and merged together for storing consolidated access log. Ultra Monkey based load balancing package of the linux OS has been used for failover and load balanced operation. Figures I.3.9 and I.3.10 depict typical log processing performed on actual proxy server after the new setup deployment.

Figure I.3.9: Users daily, weekly and monthly Internet access reports

Figure I.3.10: User's hourly Internet access statistics

In order to monitor the performance of squid servers, Multi Router Traffic Grapher (MRTG) has been configured. Figure I.3.11 depicts daily graph generated for HTTP Hits/Requests being served by the four proxy server processes running on a server. Figure I.3.12 depicts typical graphs showing server traffic on the four proxy processes after the new setup deployment.
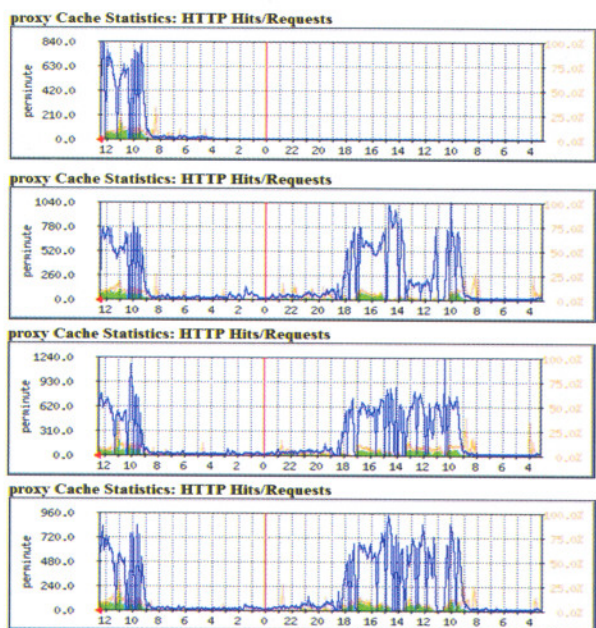
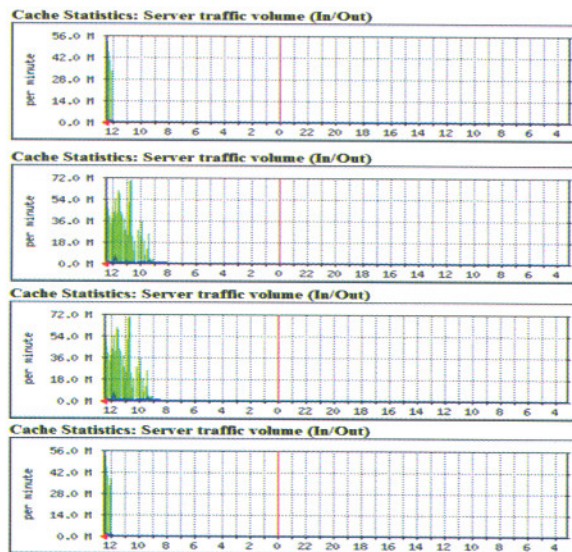*Figure I.3.11: HTTP Hits/Requests statistics per squid process in a server*

Figure I.3.12: Traffic In/Out statistics per squid process in a server

C) Commissioning of Virtual Private Network (VPN) setup for temporary access of XRD beam line (BL12) setup at Indus-2 over Internet:

VPN connectivity at RRCAT has been implemented for providing remote connectivity of RRCATNet resources over Internet. The VPN setup was used to provide VPN connectivity to the PC on which a Linux based software "SPEC" from M/s. Certified Scientific Software, Cambridge, MA., is installed. This software is being used on XRD beam line (BL12) at Indus-2. To enable the vendor, to upgrade the software and test its working with new x-ray detector module, remotely, over Internet, the VPN connectivity was provided.

D) Network threat analysis setup enhancements:

Network threat analysis setup, is helpful in analyzing network traffic and detecting intrusion attempts, including the zero day attacks and the virus attacks on a network. The existing network threat analysis setup at RRCAT was upgraded to 64bit Open Source Security Information Management (OSSIM version 3.1), being offered as Open Source Software by AlienVault. All existing servers and other network resources were migrated and new additional network servers and switch resources were added. After the recent additions the total number of network assets being monitored for their availability, totals to 135 which includes all network servers, switches and routers. Figure I.3.13 illustrates network assets availability status page after addition of assets.
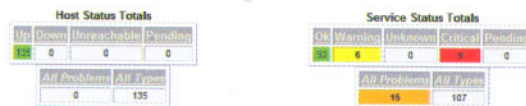

Fig. I.3.13: Network assets availability status page

E) Commissioning of a new firewall on Anunet and DAEGRID networks:

A new firewall (model: Fortinet FG-3016B) was commissioned to act as a firewall between the RRCAT Intranet, DAEGrid and Anunet networks. The new firewall was used to replace the old firewall (model: Fortinet FG-500A). The new firewall has provision for more number of 1Gbps optical fiber and 1 Gbps Ethernet interfaces, which will be used for future expansion of Anunet/DAEGrid network. All configurations related to failover operations of DAE Extranet connectivity based on multiple links, including NKN, DAEgrid and Anunet links have been completed.

F) Expansion of communication network:

A remote shelf of Laboratory area telephone exchange was commissioned at SCRF Lab, to provide voice communication facility to new buildings. This has increased the existing capacity of telephone exchange by 448 more lines, to a new total of 1886 lines. One MDF (Main Distribution Frame) of 800 pair capacity was installed for distribution of the additional telephone lines. The laboratory area telephone exchange & residential area telephone exchanges were upgraded to new OMNI PCX operating system Release 9.1. One VoIP (Voice over Internet Protocol) card was installed in laboratory area telephone exchange for providing VoIP services. New telephone connections were provided at various locations, including 5 in SCRF building, 9 in R&D G Block and 5 in Ferrite Lab buildings. 42 number of

telephone connections were provided at other locations as per user requirements. 22 number of new digital phones were provided and 31 number of new Digital Reflex Phones with voice mail facility were installed. Figure I.3.14 shows the view of the remote shelf installed at SCRF building. Figure I.3.15 shows the view of MDF commissioned at SCRF building.
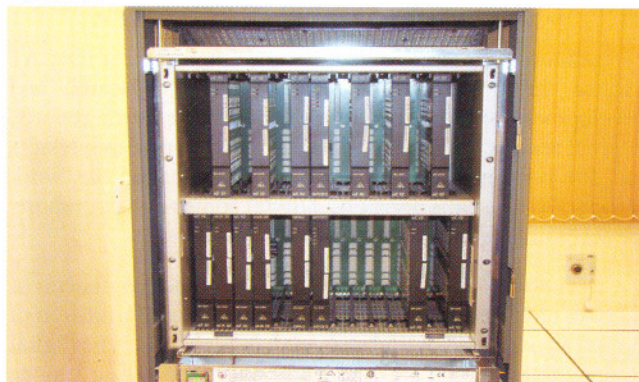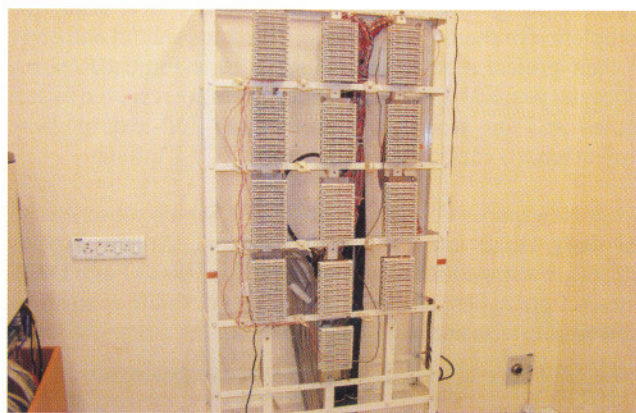

Fig. I.3.14: Remote shelf installed at SCRF building

Fig. I.3.15: MDF commissioned at SCRF building

G) RRCATNet Planning, Expansion and Upgradation:

Phase-V related Optical Fiber Cable (OFC termination) work was completed. Commissioning of 80 port SCRF building network, 72 port PG Hostel network and 48 port RTS Hostel building network was completed. Ferrite Lab building network of 12 points was connected to RRCATNet using OFC. Rack installation and rack end termination work at Fire Station Extension building was completed. In LFL, 24 newly laid network points have been connected and commissioned. In MIA building, 24-port switch was replaced with 48-port and newly laid points were commissioned. 05 number of new points were commissioned in Indus-I building for ISU users. A 10 Mbps connectivity was provided in new Civil Maintenance building. Total number of 105 new network points were added to RRCATNet. To strengthen the power backup setup at the IT building, the 200 KVA UPS setup was interconnected with the 80 KVA UPS setup to provide redundant main supply feed, in case of main supply failures.

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

I.4: Development in Library & Information Resources at RRCAT

A) Institutional Publications Productivity

Quantitative analysis of publications written by Scientists and Engineers of RRCAT and their citations was carried out in September 2011. 'Web of Science' an online citation database was searched to identify number of publications of RRCAT. It was found that total number of 1725 papers have been published since 1987 and these papers have been cited 11038 times. Earliest publication from RRCAT was in the year 1987. Publications have grown steadily over the last twenty four years. It was found that highest number of papers (172) were published in the year 2010.

During the period 1987-2011, average number of citations for a paper as per database is 6.40. Table I.4.1 & Figure I.4.1 show year wise number of publications and citations.

Publication Year	Number of Publications	Number of Citations	Average Citations/Pub.
1987	2	2	1.00
1988	3	15	5.00
1989	6	47	7.83
1990	8	34	4.25
1991	14	109	7.79
1992	25	243	9.72
1993	27	359	13.30
1994	50	477	9.54
1995	44	388	8.82
1996	44	341	7.75
1997	51	553	10.84
1998	72	480	6.67
1999	71	621	8.75
2000	64	558	8.72
2001	64	680	10.63
2002	89	648	7.28
2003	85	758	8.92
2004	83	757	9.12
2005	111	875	7.88
2006	126	1069	8.48
2007	144	852	5.92
2008	144	632	4.39
2009	120	346	2.88
2010	172	173	1.01
2011*	106	21	0.20
Total	**1725**	**11038**	**6.40**

* - till September 2011 only

Table I.4.1: *Year-wise Distribution of Publications and Citations of RRCAT*