18 June 2014

Standard Operating Procedure (SOP) and Workflow for IP Address Management at TIFR LAN

To enhance the IT security and enable systematic and smooth functioning of IP address management at TIFR LAN, policy and SOP governing this service, approved by implementation team is given below.

A. Objective of IPAM service

1. To make available online the IP addresses in use and trace the end usage of the IP.

2. To maintain online records of network incidents to help analyze the incidents and take corrective measures to avoid recurrence.

3. To block unused IPs at the gateway level to avoid misuse of floating IPs and unblock IP's on request when requested through IPAM application.

4. To help department administrators / IT representatives to maintain online records of IP distribution.

The SOP is categorized to highlight the role of each entity in the workflow.

B. Role of the Department IT representative: Department administrators / IT representatives are the vital link between users and Computer Center (CC) to maintain the services and help users to carry out their work without any hurdle. They have to take lead in all IT matters of the department and suggest Dean / Chairperson keeping in mind the importance of IT services.

1. Department administrators / IT representatives have to furnish the required end user / end usage information through the IPAM application for any IP request to block or unblock.

2. When more than 90% of the IP pool assigned to the department is utilized, the IPAM system will alert the department IT representative by e-mail to request for release of additional IP's to the pool used by his / her department. The IT representative has to act on this email by logging in to the IPAM system and request for additional IP's to pool.

3. All the network incidents violating the CCCF usage policy are now logged in the IPAM with date and incident details. IT representative has to co-operate with the network administrator in case the incident is pertaining to his / her department by providing the necessary incident details.

4. Ensure that the DHCP (Dynamic Host Configuration Protocol) clients are on private IP address range and not in the LAN range of IP's.

5. Department administrators / IT representatives to segregate the IP’s used for common facility and IP’s allotted to end users. Details pertaining to each class should be entered while requesting IP blocking / unblocking.

6. Inform the CC in case of change / delegation of IT department representative responsibility to a person other than that registered in the IPAM system and ensure proper transfer of know-how in operating the IPAM system to the new entrant.

7. Ensure prior arrangements are made to draw IP to handle requests which may arise beyond the service window of SRS (Service Request System) like handling weekend requirements of visitors.

8. Some fields in IPAM application forms are made mandatory to collect minimum data to unblock the IP on firewall. If department administrator / IT representative do not have complete information, they can take assistance from available CCCF technical staff.

Note: All the above points are the minimum requirements to be met by the IT department representative. IPAM service cannot be guaranteed if the above requirements are not complied.

C: Role of the CCCF network administrator

1. IP block / unblock request submitted by the department IT representative has to be examined and appropriate action through the IPAM system should be initiated. This request should be serviced within the SRS service window of two (2) hours.

2. Attend on high priority any service tickets raised for this service.

3. When the IT representative request for additional IP pool, CC network administrator has to judiciously allocate the IP pool for the department at the requested block. However IP’s in pool will be assigned only on specific request for IP address allocation which come through the IPAM system from the respective department with necessary detail of end usage.

4. All the network incidents violating the CCCF usage policy are now logged in the IPAM with date and incident details. It is the primary responsibility of the CC network administrator to log such incidents with full detail at the IPAM system. However, CC network administrator can seek the help of the department IT representative for gathering the necessary incident details.

5. Ensure that there is no free and floating IP’s in the TIFR LAN open to internet which could be a point of misuse / attack.

6. Associate the IP and usage of common department facilities to roles like department administrator rather than to any individual. Such IP’s should be audited once a year for confirming their continual usage.

7. Reassign the role of IT department representative on receiving the information on role change with proper communication to the concerned department and also registering at the IPAM system.

8. When a particular end user retires / resigns from TIFR, act on the SRS ticket generated for blocking the user IP based on the trigger generated from the People finder. The user IP will be blocked and IP released to the pool for reuse.

D: Role of the end user

1. End users have to comply with the TIFR network usage policy listed at CCCF website. Non-complied users will face disconnection and face disciplinary action.

2. In case a particular user is unable to get the IP address for his / her system, (s)he has to approach the department IT representative with the necessary details and get the IP allocated through the IPAM system.

3. In case a particular user is away from the institute for more than six months and is in possession of an IP, which (s)he may not require during this period, (s)he has to inform the department IT representative and CC network administrator over email to block the IP. On user resuming office IT representative will request to unblock the blocked IP allotted initially.