GOVERNMENT OF INDIA(BHARAT SARKAR)
MINISTRY OF RAILWAYS(RAIL MANTRALAYA)
(RAILWAY BOARD)

No. 2000/Tele/TW/1/Railnet works/Pt. **New Delhi, dt.30.04.2007.**

The General Managers (S&T),
All Indian Railways.

The Managing Director/
Railtel Corporation of India Ltd.

The Chief Project Manager,
IRPMU.

Sub:- Guidelines for Railnet network.

1.0 Railway Board undertook Security and Network Architecture Review & Audit of Railnet to assess adequacy of present security architecture as well as auditing the configuration and design of network architecture for optimum utilization and efficiency. The purpose of conducting this audit was to treat the Railway Board as pilot site so that recommendations can be replicated at all other locations also.

Following points emerged from this:

a) Network Architecture Review

- Rail Bhawan network is in a single Broadcast Domain
- IP Addressing used is flat 10.1.0.0/16
- No segmentation of Networks
- No Access List configured in any Switch
- HUBS are used at Access Level and at Core Level Switches
- Network Devices are scattered
- Cabling is not in healthy condition and Cat5 cables are used.
- Sub optimal Design
- No Automatic IP Assignment
- No Structured Cabling
- ARP traffic is about 70% of total traffic.
- Lot of Collisions in the network
- CPU utilization of Core Switch Cisco 2924 is more than 75%. This is very high and shows the stress on the networking devices.
- IOS in Switches and Routers is not updated.
- Security is not configured in Switches and Routers
- Software Based Firewall is used at the Perimeter but is not configured tightly because of unclear security policy.
- Firewall Policies are configured to allow services like "e-Donkey", "Messenger", "Real Audio and Streaming".
- Software Based IDS is used in Internet Gateway but the same is not protecting the perimeter.

- IDS is not configured for Critical Signatures like "Probes"
- IDS is not configured for "TCP Reset" for Attack Signatures like "Buffer Overflow", "Backdoors", "DOS Attacks"
- No Patch Management System in place

b) Network Security Review

- No Password Policy
- No E-Mail Policy
- No DMZ Security Policy
- No Remote Access Security Policy
- No Anti Virus Policy
- No Internet Usage Policy
- No Backup and Recovery Policy

(c) Internet Gateway

- No Internet Gateway planning is done
- Every Railway and some Divisions/PUs/CTIs etc. have taken their own Internet gateway breaching the security of the network.

2.0 A Committee consisting of CCE/CR, CCE/WCR, GM/RailTel and Director/Tele was constituted to examine the existing Railnet architecture on Indian Railways taking into account Security Audit Report as stated above and Security Audit of some other Railways like WCR which have already been conducted and suggest measures to improve functioning of Railnet on IR. Based on the Committee's recommendations following broad guidelines are issued:-

(i) There is a need for central monitoring of the Railnet functioning to ensure uniformity of practices, uniform architecture, central management of e-mail and web-servers and monitoring. Till a separate organisation is set up for this purpose, this job would be undertaken by IRPMU directly under the guidance of Railway Board. IRPMU will coordinate with RailTel to provide/decide under the guidance of Board issues such as Internet Gateway, adequate bandwidth regarding network upgradation, e-mail & web-server locations, disaster server locations, network monitoring etc.

(ii) To ensure the uniformity of network across IR, it has been decided that Railnet will be set up on MPLS network of RailTel as an MPLS based VPN. All the Railnet locations viz., Zonal Railways, Divisions, CTIs, PUs etc. will be connected to the MPLS network of RailTel using 2 MBPS links preferably on Ethernet with a provision of upgrading it in near future. Railway Board will be connected to the MPLS network with 10MBPS link to start with.

(iii) There will be four Internet Gateways at Delhi, Mumbai, Kolkata, & Chennai provided by RailTel. The distribution of Zonal Railways which will be served by these Gateways will be as follows:-

(a) Northern region – Delhi – NR, NCR, NWR, NER, RDSO, CORE, DLW, RCF
(b) Western region – Mumbai – WR, CR, WCR,
(c) Eastern region – Kolkata – ER, SER, ECR, NFR, ECoR, SECR, CLW
(d) Southern region – Chennai- SR, SWR, SCR., ICF, WAP

RailTel will ensure that the Internet traffic is automatically routed through other gateways in case of failure of the any of the gateway.

(iv) Only one centralized e-mail server and one web & data based server shall be provided along with disaster recovery servers at different location. While authoritative DNA server would also be hosted centrally, caching DNS servers would be hosted on each Zone, Division, RDSO, PUS/CTIs. Decision regarding capacity of e-mail server/web/server, location and mode of operation of disaster recovery centre, utilization of single server or pool of servers for e-mail/web, storage capacity, other facilities to be provided and security infrastructure like fire wall, anti-virus/SPAM protection etc. would be decided by Railway Board separately and detailed directions would be issued in this regard. Decision as to how upgradation work would be carried out i.e. either centrally through RailTel or individually will also be taken shortly and advised.

(v) **LAN Infrastructure** – At present, most of the LAN infrastructure is based on CAT 5 Cable/Hubs & Layer 2 switches working at bandwidth of 10 /100 MBPS. It is decided that in all future upgradation work at Zonal& Divisional level, all backbone wiring of LAN should be on the fibre which is capable of working on 1GBPS. Manageable switches providing higher processing speed needs to be used. Network should be designed in such a way as to provide sufficient redundancy and the concept of V-LAN should be introduced for traffic segregation wherever required.

3.0 While further details will be firmed up by the central organisation/RailTel with the approval of Board and would be advised to the Railways shortly, proposed schematic set up for every level is enclosed as Annex. for guidance.

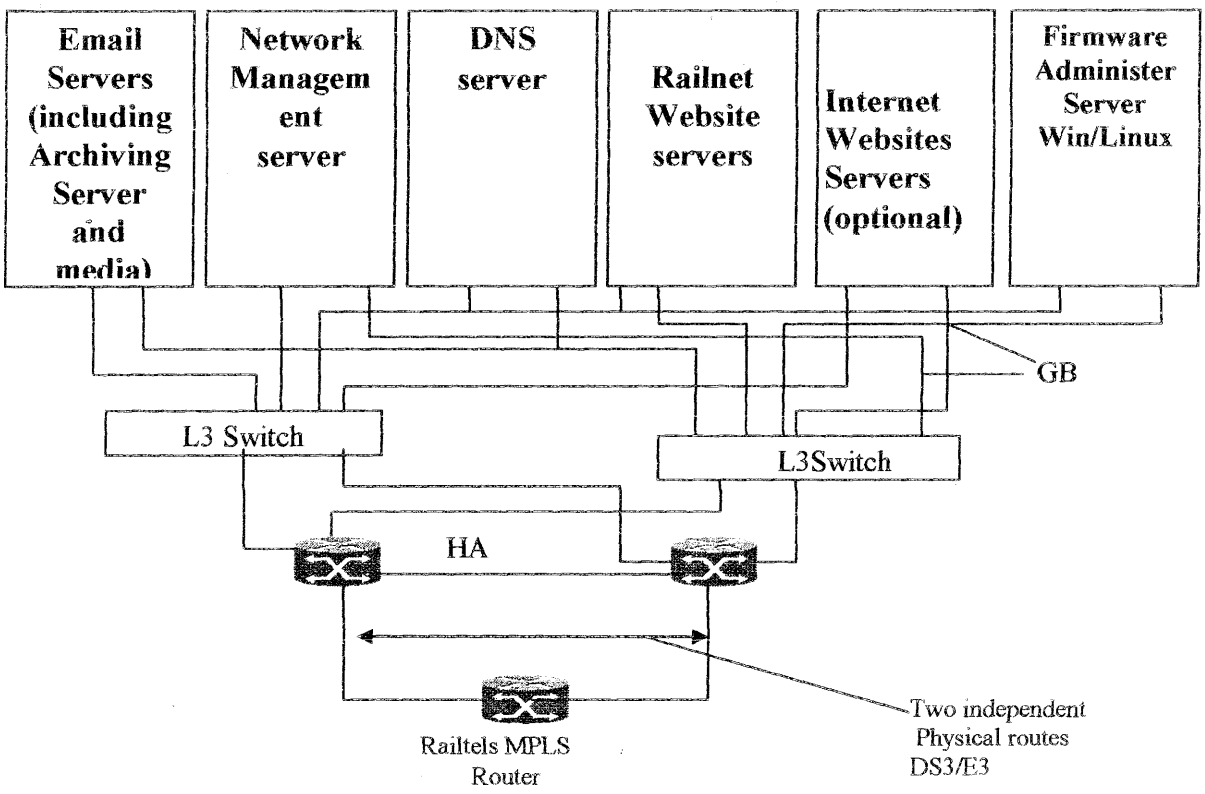
It is understood that a number of Railnet upgradation work have already been sanctioned on various Railways. Since most of the facilities would be provided centrally, Railways should not go ahead with this work till further directions from the Board excepting undertaking the LAN infrastructure work wherever required that too as per scheme enclosed and details enumerated in Para-2(v) above.

30/11/07

(Sanjay Dungrakoti)
Director/Telecom

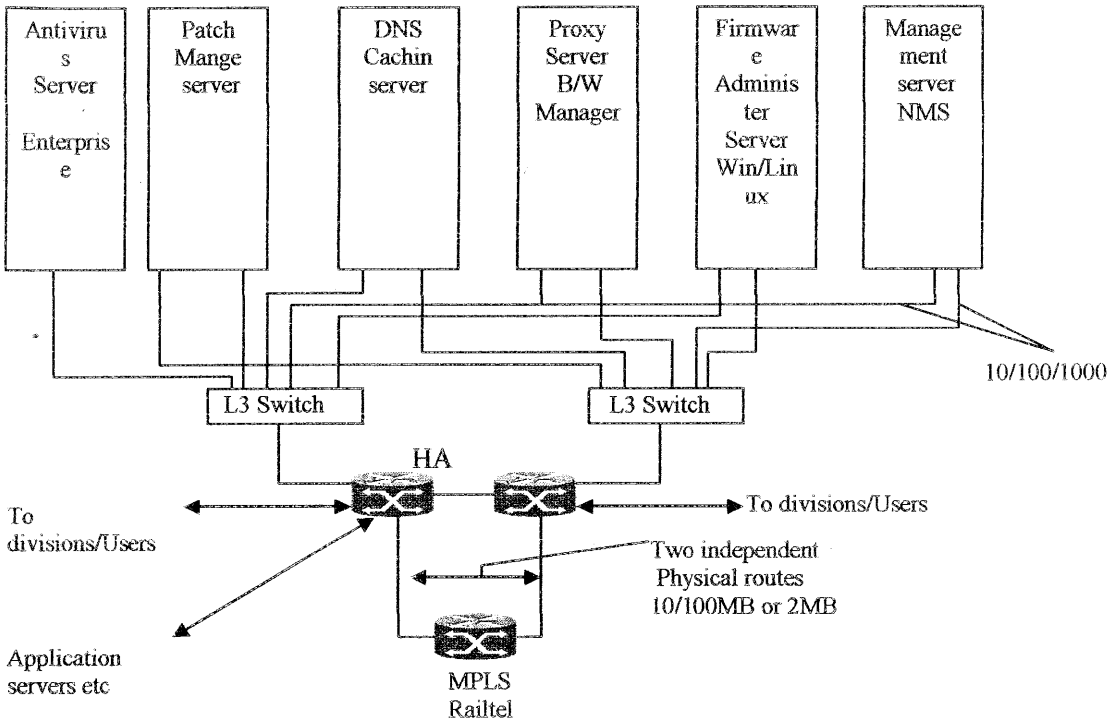
Annexure – I

Central Setup under Railway Board



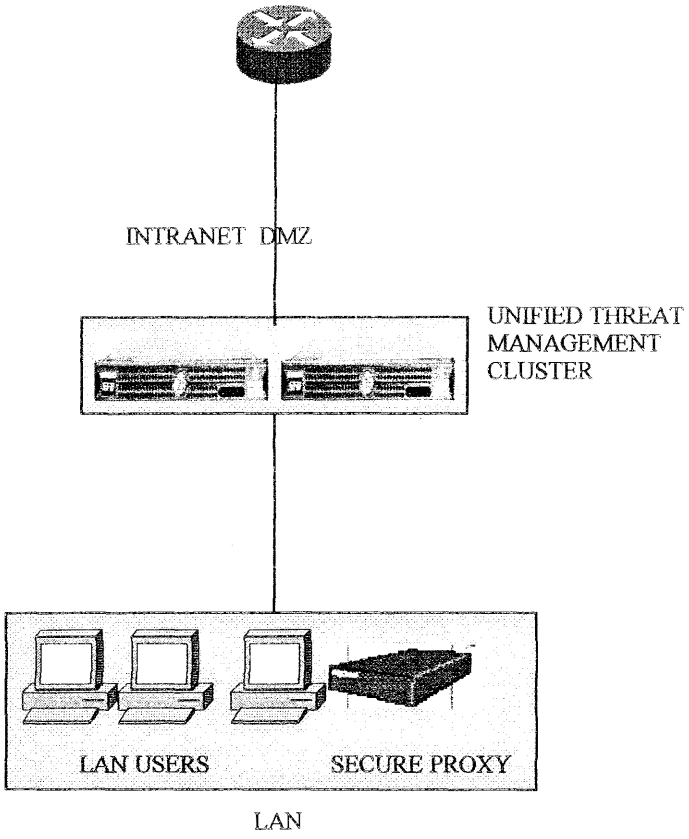
Annexure - II

Set up of
ZONAL HQ/RB/RDSO/RSC/PU's

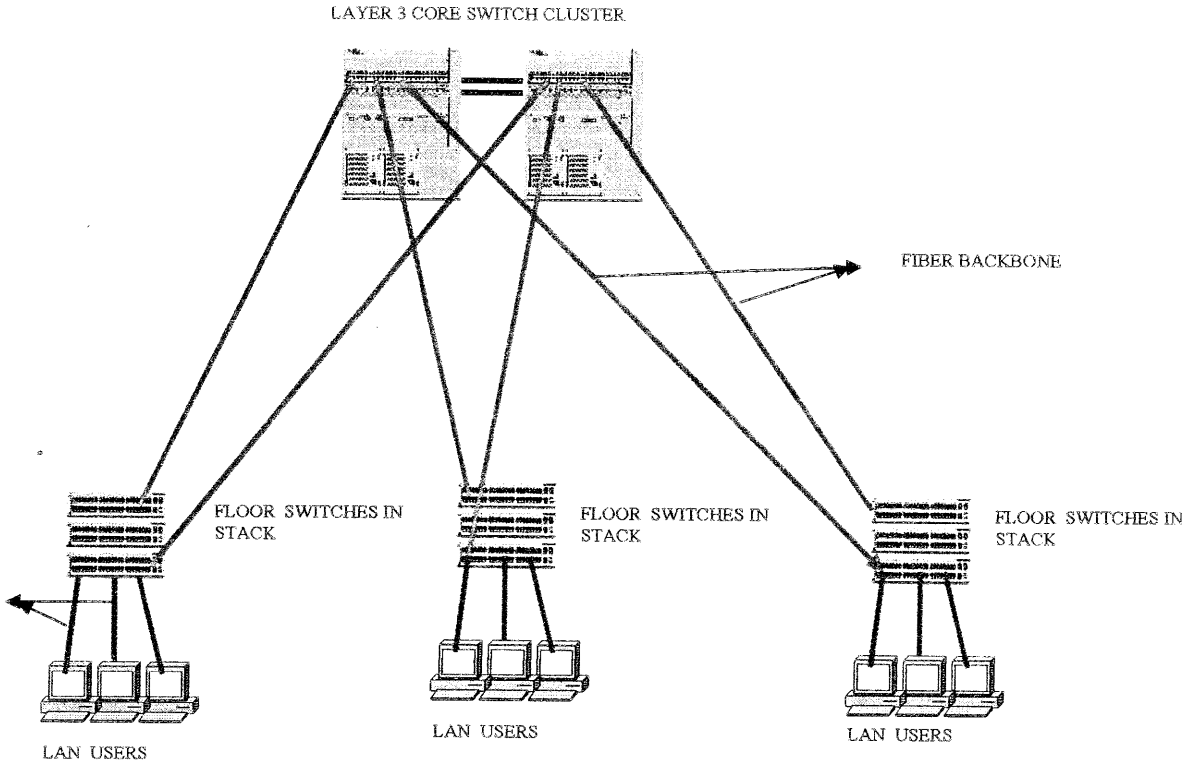


Annexure – III

Typical Setup at Divisions

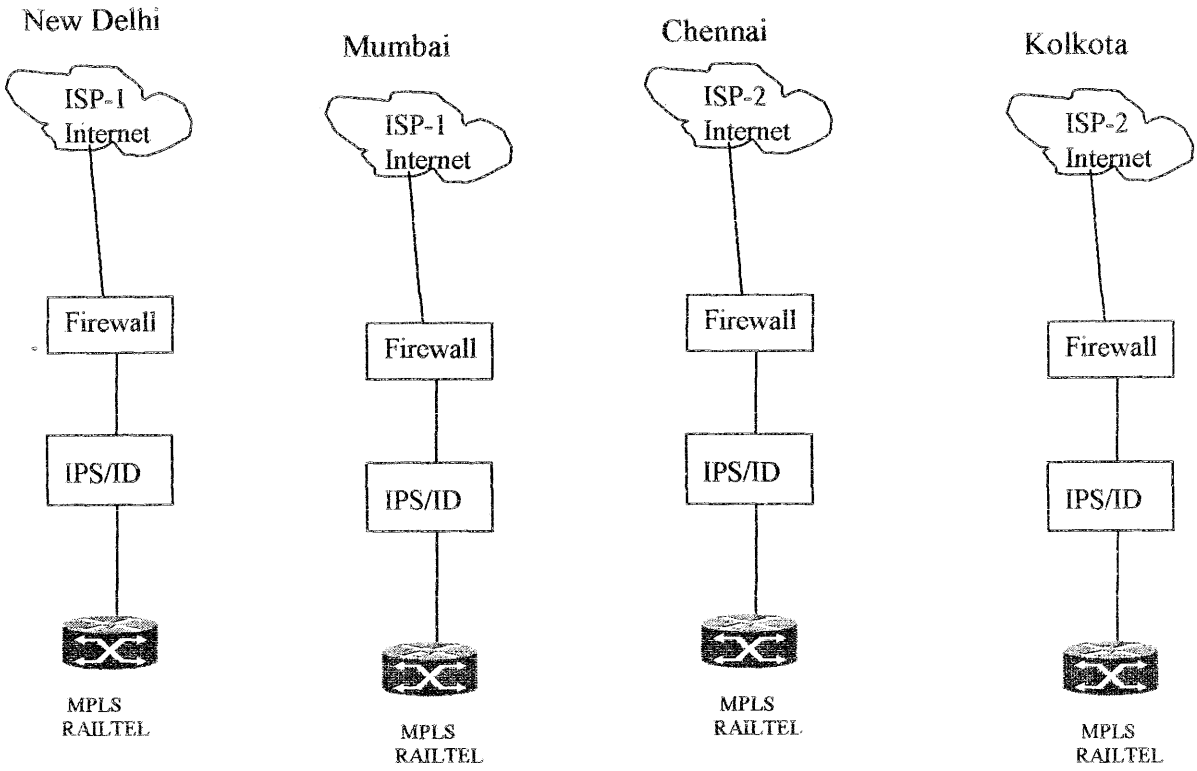


Typical Design for the LAN Core at each of the Railnet locations



Annexure - V

RAILNET INTERNET CONNECTION



Roles and Responsibilities of Railway Board/Central Organisation and Zonal Railways

Sr no	Activity	Sub-Activity	Agency Responsible
1	Network Admin	Permissions, Authentications, Access control etc	CO + HQ
1	Security Issues:	Policy + Control Implementation	CO HQ
2	IP - Addresses	Making Scheme Implementing	CO HQ [inform CO]
3	Antivirus	Loading & Updating	HQ
4	Patches/upgrades	Complete management	HQ
5	Internet	Internet permissions & B/W control	HQ, Division,