Roadmap for Railnet in Indian Railways

By Western Railway

Drivers for RAILNET

- With plans for increased Digitalization/paperless working Railnet network becomes very vital and important.
- Railway Board has already issued guidelines for Railnet architecture in Zonal Headquarter and Division.
- Approximate 2 lakhs Railnet connections are working on date in Indian Railways.
- With the coming up of various on line departmental applications, Railnet network should be robust, reliable, efficient and available up to technician level/Every station.

Drivers for RAILNET

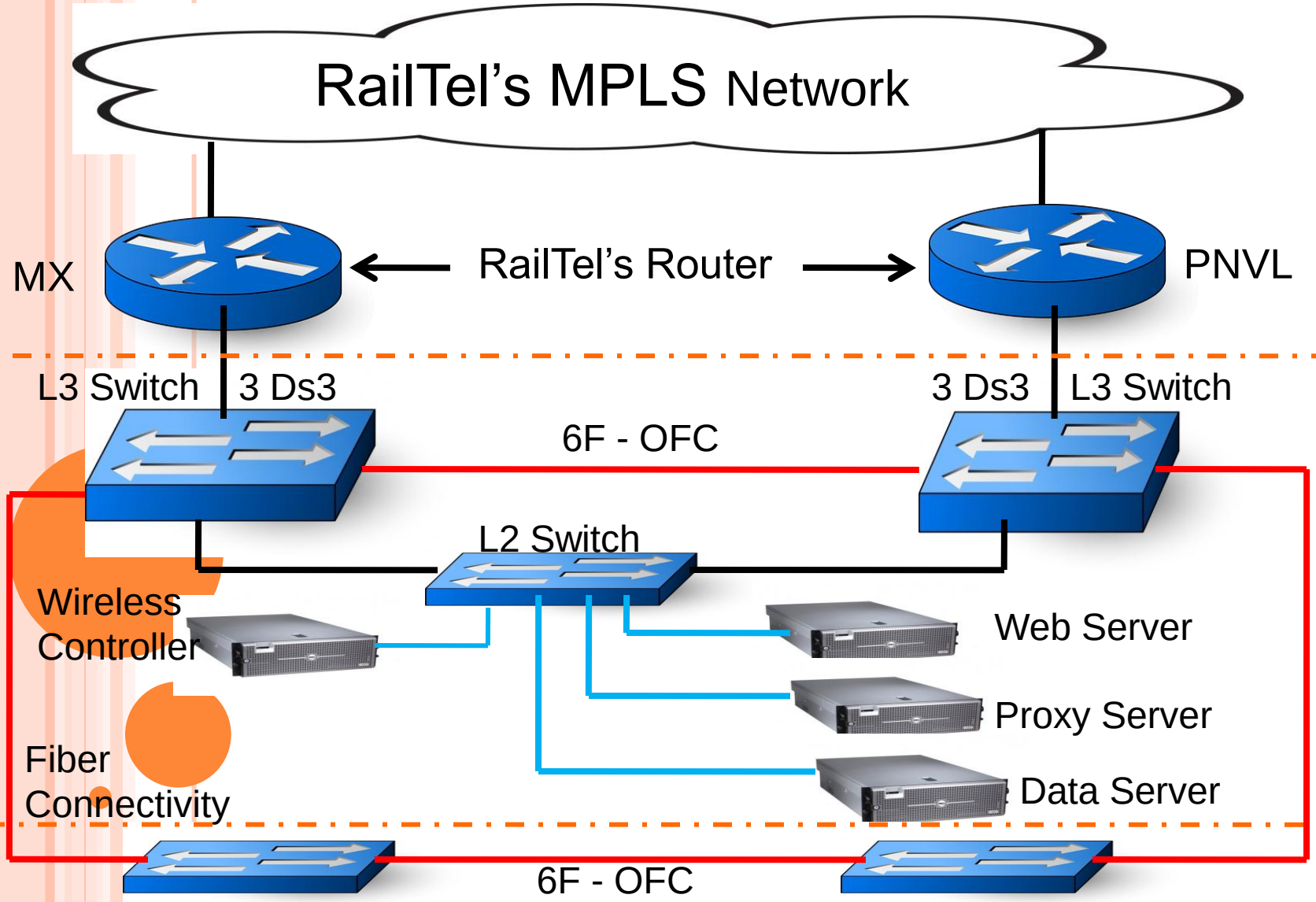
- Introduction of Various other services on Railnet like Video Conferencing etc.
- Provision of Instant Messaging Applications in day to day office working.
- Creation of our own Cloud for sharing of information from Any where/Any time
- Railnet network after migration from SDH based network to Carrier Ethernet base network.

Road Ahead……

- There should be only one ubiquitous network, **Railnet** as a bearer for all services viz Train traffic control, UTS/ PRS,FOIS etc.

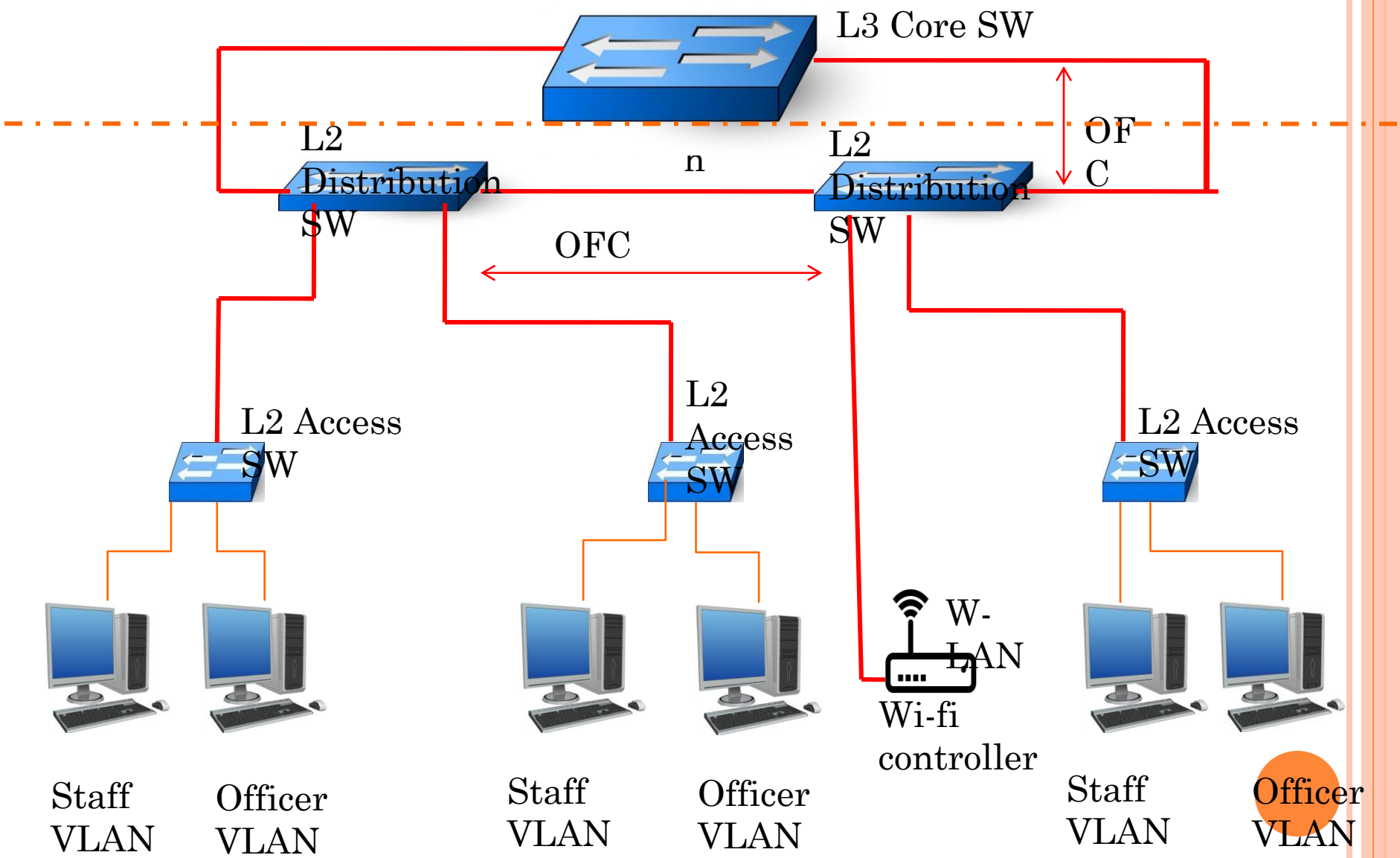
- Prerequisites:
  - Network shall be with proper design and capacity with hardware redundancy.
  - Adequate bandwidth capacity with redundancy.
  - Migration from SDH based network to Carrier Ethernet base network.

Railnet Network of Churchgate

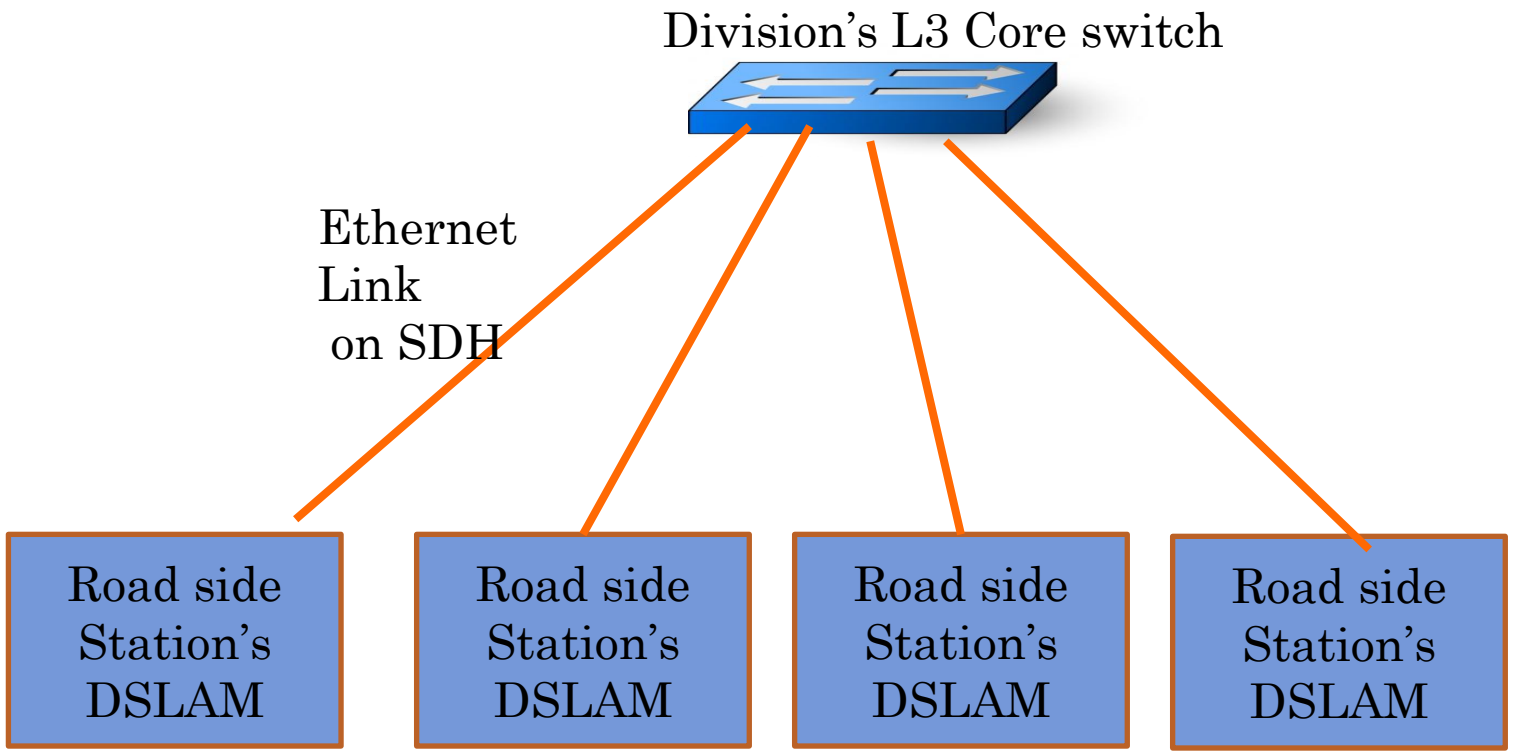


Floor wise extension of Railnet connectivity

Access Network



Extension of Railnet to Roadside station for Sr. Subordinate depot through DSLAM



Ethernet Link on SDH – 2/6 Mbps (Protected)
Total No. of DSLSMs over W.R – 65 Nos.
Railnet should be available upto the level of Techanicians

Factors to consider for future

- Security
- Uniformity among Railways
- Scalability
- Seamless features
- Quality of Service

Present Railnet Architecture

Indian Railways Railnet network has 3 components

1. Internet / Railnet bandwidth service provider (RailTel).
2. Railways internal Railnet network.
3. Various Applications running in the system.

Internet / Railnet bandwidth service provider (RailTel).

- There should be uniform cyber security policy to Indian Railway (as per current Govt. regulations).
- ISP for Indian Railways (Railtel) should provide secured VPN after following all security measures at their end.
- Railway's network design should ensure that no illegitimate traffic flows towards WAN link.

.

STANDARDIZATION OF BANDWIDTH DISTRIBUTION (SUGGESTION)

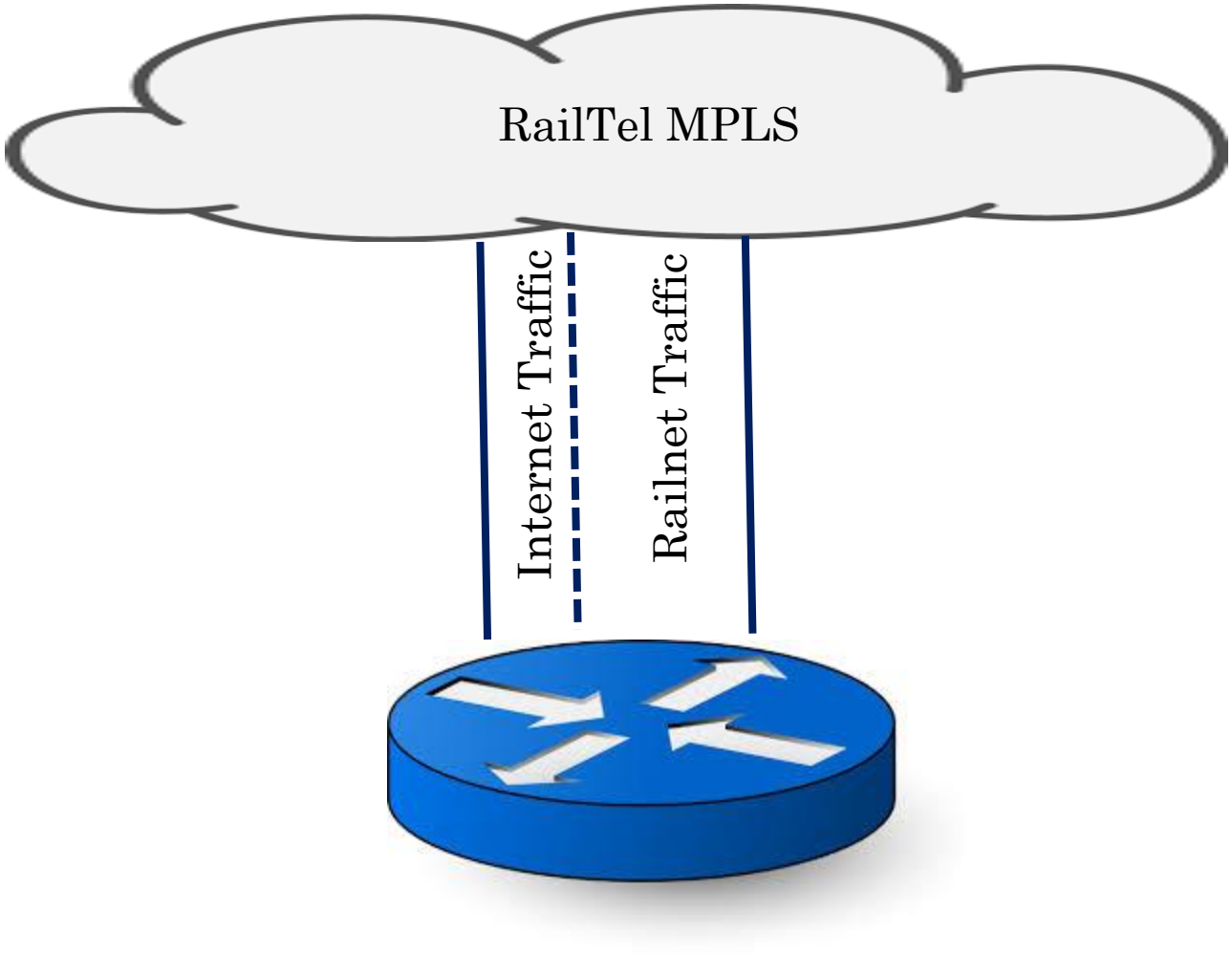
Assumption: The maximum requirement of Internet bandwidth per user is 256 Kbps concurrent user is 50% of total users			
Sr. No.	No. of users	Ideal condition	Practical condition
		Bandwidth requirement when 100% all the users are on line	Bandwidth requirement when 50 % users are on line
1	0 to 100	26 Mbps	13 Mbps
2	100 to 200	52 Mbps	26 Mbps
3	200 to 300	78 Mbps	39 Mbps
4	300 to 400	104 Mbps	52 Mbps
5	400 to 500	130 Mbps	65 Mbps
6	500 to 600	156 Mbps	78 Mbps
7	600 to 700	182 Mbps	91 Mbps
8	700 to 800	208 Mbps	104 Mbps
9	800 to 900	234 Mbps	117 Mbps
10	900 to 1000	260 Mbps	130 Mbps

Does not includes the Bandwidth requirement for online monitoring of CCTV footage.

Need for 2 VPNs

- various departmental application have been made functional. All should work on Railnet as Railnet traffic pass form from our own network.
- 70% users in this Railway have Railnet with limited internet access and 30% users has the facility of Railnet with unlimited internet access.
- There for the it is proposed that Railtel may configure 2 VPNs of the total band width to carry Railnet and internet traffic separately, to avoid any type of congestion for Railnet Traffic.

- The total Internet / Railnet bandwidth shall be bifurcated in 2 VPNs as 1/3rd for Internet traffic and 2/3rd for Railnet traffic. There should not be any congestion for Railnet traffic :



QOS shall be applied for vital applications to give priority in Railnet traffic. Suggested priority levels

1. Accident communication through VSATs carrying video traffic.
2. Video conferencing between Railway Board and Zones carrying voice and video traffic.
3. Voice over data .
4. On line applications having time out criteria .
5. All other services

For reliable operations of Railnet it is further suggested that ;-

- Separate VLANs for 50 to 70 users on Department basis (to control Broadcast)
- Independent network for HQ, Division, workshops, stores depot, residential colonies etc., if number of users are more then 200.
- In Residential colonies, Railnet should be available on Fibre I.e. Fibre to Home. Initially fibre can be up to the building.
- Centralized NMS for monitoring of complete Railnet network at Zonal HQ and each Divisions.

Security

- Comprehensive Uniform security policy for Railnet to be developed
  - Access control to nodes to be well defined
  - Password policies
  - Access including programming rights to network elements to be defined
- Suggested to nominate a working group to develop security policy.
- Annual audit of security policies through CERT certified third party auditor.
- Availability of complete Syslog with at least 30 days backup.

WiFi penetration

- There is heavy demand for WiFi access
  - Need central authentication
  - Standardization of access points (RDSO may develop specification)

Security on Wi-fi network

- Wi-Fi Access points
  - MAC binding
  - Enabling SSID broadcast
  - Disabling DHCP server
  - WPA2/PSK encryption
- Wi-Fi Routers are secured by adopting
  - MAC binding
  - Disabling SSID broadcast
  - Disabling DHCP server
  - WPA2/PSK encryption

Provision of central authentication for Railways internal Wi-Fi network for seamless functioning of Internet and Railnet network during out of HQ movement of any Railway officials to any railway.

a. CUG mobile data of Indian Railways and their category can be used for authentication.

b. Using that data user can centrally authenticated for accessing Wi-Fi facility in all over India, within zones or within divisions. e.g. ‘A’ category CUG Nos. can be given all India Wi-Fi, ‘B’ category within zones and so on. It will avoid the cumbersome procedure of MAC binding.

Network Management

- Every Division should have NMS at least with viewing rights apart from Central NMS being planned through Railtel. It should have the facility of;-
- Failure management.
- Traffic and congestion management.
- Bandwidth management.
- Inventory Management.
- Reporting of failure as per escalating matrix through SMS and Email.

- RDSO should standardize the specifications of Datacom equipment based on the no. of users considering the utilization of any hardware resources not more then 50% even during the peak hours and approved the vendors for that.

- Railnet equipment room shall be dust free air-conditioned for reliable operation of vital Datacom equipment.
- All the connectivity shall be on fibre except the last mile up to users terminal. It should also be through CAT6 cable to extend the connectivity up to 1G to the users.
- Proliferation of Railnet/ Internet up to the Sr. Subordinate depot.
- Complete network shall be under comprehensive AMC with Round the clock availability of trained manpower of AMC for continuous monitoring.

Development and operational of various departmental applications (CRIS)

- CRIS has developed many departmental applications, keeping their servers in CRIS data centre and launched only on public network like I pass, IREPS, IRPSM,TMS, SIMS, RPF SMIS etc. Recently RRBs have also developed and launched their “Recruitment Indent Management system” www.rimsonline.in on public network.
- CRIS is also developing many more applications for each department for paperless working. All the applications, does not require public interface shall be launched only on Railnet network. The applications require, public interface shall be both on Railnet and public network.
  - It will save not only Railway revenue, but chances of hacking also will be reduced being our own intra network.
  - Necessary security if required can be implemented at server level.

Spin Offs:

- Ready for ERP implementation in Indian Railways.
- Free flow of information, any where , any time.
- Railway applications on intranet, less prone to hacking, effective security.
- Scalability and maintainability, being single network for all services.
- Inventory control.
- Suitable for integration of all services.

Thank you