MPLS Based Networks in Railway Deployments

Adam Oliver
Bachelor of Electronic Engineering
Calibre Global

SUMMARY
Safe and reliable communications are a critical component in operating modern railway networks. Voice radio, signalling, asset protection, CCTV, station services and alarms form the basis of a typical rail system, with telephony, data and internet connectivity between offices shaping corporate requirements. These services are traditionally provisioned through a combination of separate Synchronous Digital Hierarchy (SDH), Plesiochronous Digital Hierarchy (PDH), Ethernet and legacy analogue circuits, resulting in increased maintenance and support requirements. As more railways move towards Communications Based Signalling (CBS) systems bandwidth requirements increase, with a corresponding focus on reliability and resilience. Coupled with growing focus on Ethernet connectivity for hardware, an opportunity exists to explore alternate network arrangements that are more holistically encompassing of all supported technologies and their requirements.

Implementation of an IP/MPLS (Multi-Protocol Label Switched) network allows convergence of these disparate networks into a single unified system. Key infrastructure can be shared between different facets of an organisation on a single physical network, whilst maintaining completely independent circuits for the various services being transported. In contrast to an IP-only implementation, where scalability and traffic engineering can be challenging as network size increases, an IP/MPLS solution allows a network to grow as needed, while providing excellent load balancing to make better use of existing network infrastructure. This in turn can lead to savings in both OPEX and CAPEX, as both infrastructure and maintenance costs are reduced.

Ideally suited to both green and brown field rollouts, an IP/MPLS based network is a viable solution for any network rollout.

1. INTRODUCTION
Passengers of modern transport networks have high expectations for their journey. From basic services such as e-ticketing, timetabling and real-time scheduling information to on-board Wi-Fi and Video on Demand (VoD), customers are beginning to expect these services to be available. For the customer, provisioning of these services and overcoming technical hurdles associated with them is not a consideration.

Network operators, on the other hand, must consider both customer and operational needs. Safe and reliable communications are a critical component in operating modern railway networks. Services vital for railway operation – signalling systems, safety, voice radio, station services and asset protection – must be balanced against corporate and customer requirements, often contending for the same resources. Legacy equipment and systems must continue to operate in parallel with new deployments. On top of these operational requirements, unprecedented demand from customers for more services, with far greater bandwidth requirements, is forcing operators to re-evaluate their network architecture to best meet their needs moving forward.

Calibre Global has recently been involved in the deployment of an IP/MPLS network for a major rail system in Western Australia. Background and insight from the recent project are covered within this technical paper.
2. NOTATION

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>CBS</td>
<td>Communications Based Signalling</td>
</tr>
<tr>
<td>CE</td>
<td>Customer Edge</td>
</tr>
<tr>
<td>FEC</td>
<td>Forwarding Equivalence Class</td>
</tr>
<tr>
<td>HSRP</td>
<td>Hot Standby Router Protocol</td>
</tr>
<tr>
<td>LDP</td>
<td>Label Distribution Protocol</td>
</tr>
<tr>
<td>LSP</td>
<td>Label Switched Path</td>
</tr>
<tr>
<td>LSR</td>
<td>Label Switched Router</td>
</tr>
<tr>
<td>LTE</td>
<td>Long Term Evolution</td>
</tr>
<tr>
<td>MPLS</td>
<td>Multi-Protocol Label Switched</td>
</tr>
<tr>
<td>OAM</td>
<td>Operations Administration and Maintenance</td>
</tr>
<tr>
<td>P</td>
<td>Provider</td>
</tr>
<tr>
<td>PA</td>
<td>Public Address</td>
</tr>
<tr>
<td>PDH</td>
<td>Plesiochronous Digital Hierarchy</td>
</tr>
<tr>
<td>PE</td>
<td>Provider Edge</td>
</tr>
<tr>
<td>QoS</td>
<td>Quality of Service</td>
</tr>
<tr>
<td>SDH</td>
<td>Synchronous Digital Hierarchy</td>
</tr>
<tr>
<td>TDM</td>
<td>Time Division Multiplexing</td>
</tr>
<tr>
<td>TE</td>
<td>Traffic Engineering</td>
</tr>
<tr>
<td>VoD</td>
<td>Video on Demand</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
</tbody>
</table>

3. MPLS NETWORKS IN RAIL DEPLOYMENTS

3.1 Existing Network Architectures

Traditionally, operators have built and maintained discrete networks to support specific platforms. Functional requirements can vary significantly between services. Mission and safety critical services typically have very low bandwidth requirements, however timing and availability is of paramount importance. Less critical services such as voice and passenger information services have higher bandwidth requirements, but short interruptions will not necessarily impact train operation. Passenger services such as internet and video on demand will expand to fit any available bandwidth, however loss of these services – although inconvenient for the passenger – will not directly impact train operation. Table 1 provides indicative bandwidths for a selection of network applications, as well as their criticality for network operation.

Traditionally, Time Division Multiplexing (TDM) networks have formed the backbone for rail operations networks due to their predictable behaviour and well developed operations, administration and management (OAM) functions. SDH and PDH networks provide deterministic pathways with the high security for vital signalling railway operations and train control. Coupled with strong protection and restoration functionality, high availability networks can be deployed over large areas to support mission-critical services with a high degree of confidence.

Voice radio communications may be implemented as separate PDH networks, using TDM to multiplex multiple radio channels in single data streams. While effective, this is not necessarily efficient use of available bandwidth, particularly on infrequently utilised channels. Recent trends towards TETRA, GSM-R and P25 further reduce the requirement for TDM based voice services, instead requiring a reliable Ethernet backbone to interconnect base stations.

Isolation between each of these systems is assured, as each network operates independently. Those services requiring high availability have multiple transport paths provisioned, with protocols to ensure that any interruption to one path results in automatic changeover to the secondary path.

Each network requires its own training, maintenance and ongoing support requirements, which can lead to increased operating costs. As legacy equipment ages, so costs associated with support and replacement increase significantly. Furthermore, as legacy equipment approaches end-of-life, railway operators need to ensure that new equipment is implemented in the most cost-effective manner without interrupting services.

The current trend towards IP-based interfaces on new devices, coupled with the inherent flexibility of IP networks, provides a strong incentive to migrate towards a single communications network. However, strict IP-based networks may be unable to meet some of the stringent operating requirements, such as network reconvergence times and isolation between different traffic types. As such, any new
network implementation needs to meet the following criteria:

- High availability;
- Security and isolation between services;
- Support legacy services and interfaces; and
- Flexible and expandable to meet high bandwidth requirements.

An MPLS based network architecture meets these requirements, and is a viable solution for any a flexible, future-proof network rollout.

### 3.2 MPLS Overview

Multi-Protocol Label Switching (MPLS) is a packet-forwarding technology, using labels to make data forwarding decisions. Layer 3 header analysis is performed only upon the packet entering the MPLS domain, which reduces intermediate router processing overhead. Instead of packets being forwarded on a hop-by-hop basis, Label Switched Paths (LSPs) are established for particular source-destination Label Switched Router (LSR) pairs. Packets which are to be treated in the same manner are grouped into the same Forwarding Equivalence Class (FEC). This grouping method is flexible, and may be based on a combination of source or destination address, port, protocol or Virtual Private Network (VPN).

Control of LSPs within the MPLS network is dictated by a Label Distribution Protocol (LDP). Much as a routing protocol operates within a strictly IP-based network, the LDP is responsible for classification of FECs, distribution of label information within the network, and the establishment and maintenance of LSPs. Dedicated LSPs protocols exists, however many existing IP protocols have been extended to support label distribution in addition to IP routes.

When a packet enters an LSR router, the layer 3 header is interrogated to determine the required destination. Based on the received information, the ingress router assigns a label and FEC to the packet, and forwards it to the next hop in the core MPLS network. Upon receiving the packet, each intermediate LSR uses the label to forward the packet towards its destination, without the requirement for layer 3 processing. Within the core network, no IP information is visible to the routers beyond the label information assigned by the LSR. When the packet reaches the egress side of the MPLS network, the label is stripped from the packet and it is sent on its way using standard IP forwarding.

MPLS networks define three different equipment types:

1. Customer Edge (CE) Router – first device on the end-user (or customer) network prior to connecting to the MPLS network. It requires no knowledge of the MPLS network.

2. Provider Edge (PE) Router – first device on the MPLS network, and connects to one or more CE routers. All MPLS VPN processing occurs on the PE router.

3. Provider (P) Router – a backbone router within the core network equipped with MPLS forwarding capability.

A simplified MPLS network is illustrated in Figure 1. A packet from IP network A arrives at the ingress (or edge) router, where the header is interrogated to determine the required destination. The ingress router then applies a label, directing the packet to the egress router. Within the MPLS network, each router interrogates only the label to determine the next hop in the LSP, until the packet arrives at the end of the label switched journey. The egress router then removes the label and forward the packet into IP network B, where normal routing / switching behaviour directs the packet to the final destination.

MPLS has the advantage of being able to support a wide variety of network topologies through the use of MPLS Virtual Private Networks (VPNs). A VPN can be considered as a network-within-a-network, whereby connectivity to multiple sites is enabled over shared infrastructure, with the same routing table. Each VPN is completely isolated from all other VPNs within the network, which ensures isolation between applications and services is maintained at all times. Different VPNs may also implement completely different network topologies to meet the varying application requirements.

From the Customer Edge point of view, anything which occurs between PE routers is completely transparent. No knowledge of MPLS VPNs, FECs or the intermediate network topology is required on the CE equipment. MPLS VPNs allow CE equipment at remote locations to behave as though they are physically on the same network, without requiring knowledge of the underlying MPLS network topology. Importantly, when a layer 2 packet is encased in an MPLS header and transported across the network, the packet arrives at the destination unchanged. This allows the MPLS network to act as a transparent extender for any layer 2 service, allowing legacy network topologies to be migrated across without the requirement for GRE tunnelling or similar workarounds. In addition, MPLS layer 2 VPNs (L2VPN) offer better control over features...
such as Quality of Service (QoS) and Traffic Engineering (TE).

### 3.3 MPLS in the Transport Network

#### 3.3.1 Overview of Requirements

In order for MPLS to be a viable solution to creating a converged transport communications network, the implementation must address the key considerations of any rail communications infrastructure. The network must be safe, maintain a high availability, be secure, provide isolation between services, and be flexible enough to support legacy, existing and future equipment and systems. In particular, EN-50126 and EN50159 form the basis for safety-critical systems and must be adhered to, ensuring that any faults within the network do not lead to errors or failures in security.

The availability required of a network is a function of safety, cost, and productivity. Safety critical systems such as signalling and control systems may require an overall availability of 99.9999%, or 32 seconds of unavailable time per year. Less stringent requirements of 99.999% or 5 minutes of unavailable time per year may apply to passenger information systems, ticketing, and broadcast announcements. Any network implementation must be able to participate in the overall application calculation in such a way that the required availability can be met.

Security must be a key consideration, both from a physical access point of view, as well as within the various systems and applications. Proper steps must be taken to ensure that both human error and faults within the network do not result in breaches of security and put overall safety in question.

Support for legacy systems as well as existing and future requirements need to be considered. It is rare that a transportation network has the freedom for a complete Greenfields deployment. In most cases, existing applications, hardware and infrastructure need to be integrated into the new network, so legacy protocols and interfaces may need to be considered. Similarly, existing and future capacity must be taken into account – forward planning for bandwidth-hungry requirements of services such as Long Term Evolution (LTE), high bandwidth wireless systems, and other train-to-wayside services allows for a less painful upgrade path when considered in initial network design. This also extends to future expansion of the network – adding new stations, spur lines and applications should be as straightforward as possible.

#### 3.3.2 Network Topology

Figure 2 shows a simplified rail network utilising an MPLS backbone.

Each station is deployed with an MPLS-enabled router, which acts at the Provider Edge (PE) device, providing all mapping of services into the defined MPLS VPNs. One or more switches provide Customer Edge (CE) functionality, acting as the consolidating link between applications and the PE device.

Connectivity between stations may be modified to suit available transmission paths. MPLS is flexible – it can utilise existing Ethernet, SDH, ATM, Frame relay, microwave or leased line capacity that is available. The upshot of this is that existing infrastructure need not be immediately replaced, as existing network capacity can be transferred and reused as part of the MPLS core backbone. Existing dark fibre may also be utilised as bandwidth requirements increase, either through additional pipes between segments, or implementing multiple wavelengths on existing fibre links to increase capacity.

Adjacent stations are staggered on opposite sides of a ring to provide diverse paths on the main backbone, avoiding the need for high capacity alternate paths in the event of a single node failure. Physical implementation of these links can be optimised to suit the available resources. Ideally, each side of the ring would make use of fibres in separate cables for maximum protection against accidental damage. If dual fibre is not available, both sides of the ring can be implemented within a single fibre cable to create a “flat-ring” topology. This arrangement reduces infrastructure costs; however the trade-off is that an accidental fibre cut can impact both sides of the ring.

An added degree of protection can be provisioned through the use of end-to-end links over an alternate transmission medium. These links may consist of operator-owned point-to-point microwave links, dark fibre over diverse paths, or most commonly a public carrier-provided service. Placing these alternate paths at the end of the line provides a fully
redundant path for network traffic in the event that the primary paths are damaged.

3.3.3 Physical Station Infrastructure

For simplicity, Figure 2 is shown with a single CE and PE device at each station. To meet availability requirements, CE and PE devices may be fully or partially duplicated to provide protection in the event of equipment failure, as shown in Figure 3. In a duplicated scenario, Hot Standby Router Protocol (HSRP) configured on each device provides a virtual gateway for all traffic. In this way, failure of a single router, switch, or link at the station does not have a detrimental effect on traffic. The applications themselves will be unaware of a fault, as traffic will be maintained via the working router with minimal impact to the network.

An important consideration in selection of physical infrastructure is the matching of equipment to expected environmental conditions. An expectation at large stations is that a communications equipment room is available with suitable power and air conditioning to allow the operating environment to be reasonably controlled, avoiding the need for hardened equipment. Small stations, or wayside locations with a subset of the large station services, may not have environmentally controlled equipment rooms, which necessitate selection of equipment capable of withstanding a greater range of temperatures.

![Figure 3: Typical Station Hardware Implementation](image)

3.3.4 Logical Infrastructure

MPLS Traffic Engineering (MPLS-TE) provides an effective method to make best use of available resources. MPLS-TE automatically establishes and maintains Label Switched Paths (LSPs) across the backbone, taking into account factors such as available bandwidth and link latency, creating optimal paths for traffic flow. Paths for LSPs are calculated at the LSP head end router, however in some fault conditions it may take longer than desirable for the head end router to calculate an alternate path. To avoid this situation, Fast Reroute is implemented on local routers. This feature enables all traffic carried by LSPs that traverse a failed link to be immediately rerouted around the failure using a backup LSP. The rerouting decision is locally controlled by the router with the failed link, while at the same time the fault is reported to the head end router by the routing protocol. Although the fast reroute link may not be the most efficient use of available resources, it will be held in place until an optimised LSP is calculated by the head end. By using MPLS-TE fast reroute feature, the MPLS core network can guarantee sub 50ms recovery in the event of node or link failure.

Quality of Service (QoS) allows preferential treatment to be given to key services, where factors such as bandwidth, latency and availability play a crucial role. Based on the each application’s performance requirements, operating characteristics and business criticality, services can be categorised and assigned to particular traffic priority classes. For example, train operation applications would be assigned a high priority, whereas passenger internet may be assigned a lower priority. If the MPLS network were to experience congestion or contention for bandwidth, QoS would prioritise the train operation traffic over and above any lower priority traffic. This may cause some loss to lower priority services; however train operations will not be impacted. QoS can be particularly useful where redundant path bandwidth capacity is limited – critical services are given highest priority to guarantee performance regardless of network condition, whereas less important services may suffer performance impact.

Safety and availability of the network is achieved with thorough network design in conjunction with ongoing audits and maintenance. Isolation between services is provided by segregating different traffic types into Virtual Private Networks (VPNs), which restrict communication between services unless explicitly allowed. When used in conjunction with QoS to prioritise critical traffic, fine control over traffic flow can be readily achieved.

3.4 Advantages and Disadvantages

The single most important advantage of MPLS is the ability to provision a single, converged network architecture. MPLS is highly scalable and adaptable, with the inherent ability to transport a wide variety of traffic, including Ethernet and SDH traffic. The flexibility and protocol agnostic nature of MPLS means that both existing and new applications can make use of the network, reducing operating costs associated with maintaining multiple independent networks. After initial setup, much of the diagnostics, fault finding and maintenance can be performed remotely from an operations centre, reducing the requirement for field staff.

A shortcoming of MPLS is that is considered time consuming and complex to set up, requiring specialist training to properly plan and implement the network. Well-developed Operations, Administration and Maintenance (OAM) tools which exist for SDH-
MPLS Based Networks in Railway Deployments

based networks are not yet available, limiting the ability for easy creation of new links and services from a Network Management System (NMS). The MPLS-TP standard being developed by IETF & ITU-T aims to extend the MPLS protocol to better meet transport network requirements, with a focus on well-developed, standardised OAM tools and the ability to automatically add routes to an entire network based on network end points.

3.5 How Does MPLS Benefit the Passenger?

The intricacies of a transport network design are of little interest to passengers. Redundancy, security, network availability and operational costs mean nothing. Passengers care about:

- Is my train on time?
- Can I buy my ticket, and top up my travel card?
- Is there entertainment / internet available on the platform and on the train?
- Will someone be available if I am in trouble?

Public address, passenger information displays, E-ticketing machines, emergency phones, CCTV security and information kiosks provide passengers with security, accurate timetable information and the ability to purchase or recharge tickets. Platform and rail-based intercoms, emergency phones and CCTV systems allow security to be maintained at all times, with knowledge that should an issue occur help is close at hand. The ability to provide continuous internet both on and off the platform, and the potential for video on demand or on-train movies all require fast, reliable backhaul to minimise potentially frustrating network bottlenecks.

The important factor then becomes ensuring the information is able to be quickly and reliably made available at stations and on the train for passenger use. An MPLS network has the ability to meet these requirements, while providing the flexibility and future proofing required by the operator.

4. CONCLUSION

The protocol-agnostic nature of MPLS networks means legacy services such as PDH/TDM and SDH services can be mapped into the MPLS network directly, allowing for transparent transportation and emulation of previous network infrastructure as required. At the same time, ample bandwidth can be provisioned on the same infrastructure to support essential passenger information services, as well as bandwidth-hungry applications such as internet and video on demand. Through network design, redundant paths and planning a highly available, resilient and secure network can be implemented as a basis for implementing a converged network fully capable of supporting the safety-critical applications required of a rail network.