Mission Critical MPLS in Public Safety Microwave Systems

The Technology to Support Evolving Networks

Application Note

February 2017

Mission Critical MPLS in Public Safety Microwave Systems

The Technology to Support Evolving Networks

Abstract

This application note explains why MPLS (multi-protocol label switching) is one of the most suitable advanced networking technologies to support public safety communications networks that use point-to-point microwave systems. This paper is intended for state and local public safety chiefs, deputy chiefs, government executives, commissioners, administrators, network managers, and policy makers who are responsible for public safety and government communications systems.

Table of Contents

Microwave Networks, Inc.
4000 Greenbriar Dr.
Stafford, TX 77477

1-281-263-6500
www.microwavenetworks.com

Executive Overview

Public safety communications networks are transitioning and converging. **LMR (land mobile radio)** systems are transitioning from legacy to digital IP systems. In addition, LMR and mobile **LTE (long term evolution)** broadband networks are converging. As a result, new voice, data, and video services are transforming public safety communications networks. These new networks and services are based on **IP (Internet Protocol)** frameworks and standards.

To backhaul new IP networks and services, state and local governments are turning to **MPLS (multi-protocol label switching)** to support existing and future LMR and public safety broadband networks.

MPLS is the right technology to support the transition of legacy LMR systems to digital IP and the convergence of LMR with mobile LTE networks. MPLS solves the problem of transporting multiple technologies and protocols over a single medium, while ensuring guaranteed delivery of high priority communications. By supporting multiple transport technologies, MPLS enables network transition and convergence, with improved network security and mission critical reliability.

MPLS provides the redundancy and priority for mission critical reliability to support network availability for critical voice, data, and video communications. Operating over a variety of backbone transport networks including fiber and microwave, MPLS achieves several mission critical goals by using features that ensure network availability for first responders, chiefs, commanders, and government directors and managers.

MPLS supports,

- Network redundancy
- Prioritization of communications traffic
- High bandwidth capacity
- Performance guarantees
- Virtual Private Networks (VPN)
- Interoperability of multiagency and interagency communications
- Security governing user access controls and end-to-end encryption
- Scalability to grow as networks transition from legacy to digital IP networks

In summary, state and local governments are utilizing MPLS to handle the transition and convergence of public safety LMR and broadband network technologies including microwave networks. When deploying MPLS in microwave systems, government can use **hybrid microwave** radios to efficiently support the transition of mission critical legacy networks to modern IP networks.

Overview of MPLS

MPLS is a standard based framework and proven technology based on the work of the **IETF** (**Internet Engineering Task Force**), a community of network engineers, designers, developers, operators, and vendors focused on the development of Internet standards.

MPLS is a mature and widely deployed carrier-grade packet technology used in core, aggregation, and transport packet networks.[i] IETF established the MPLS framework in 1998. Carriers have utilized MPLS for almost two decades and enterprise has utilized it for over one decade. Large statewide mission critical utilities have deployed enterprise MPLS in their converged microwave, fiber, SCADA, and LMR networks. For example, South Mississippi Electric Power Association is a mission critical utility that utilizes MPLS in its microwave and fiber backhaul network, which covers large portions of the state. In addition, small and large municipalities and county governments utilize MPLS. As an example, Pinal County, Arizona is implementing MPLS in its LMR and communications networks.

MPLS can transport IP and non IP traffic. By connecting different technologies that normally would be incompatible, MPLS unifies legacy and new network technologies.[ii] Examples of legacy technologies include T1/E1, ATM, Frame Relay, DSL, and SONET, while examples of modern technologies include **Ethernet** and IP protocols. MPLS separates service delivery from transport, remaining independent of transport protocols, fostering the transition and convergence of networks. MPLS enables network migration strategies including LTE IP radio access network architectures and IP based P-25 land mobile radio networks. [iii]

Mission Critical MPLS

Most importantly, network engineers can design and control mission critical features into a modern Ethernet IP network by utilizing **MPLS-Traffic Engineering**. IP networks alone are not mission critical grade because IP networks deliver communications data on a best efforts basis. Performance is not guaranteed and can vary with congestion. That's not good enough for public safety. IP best efforts is like regular mail service; eventually mail will arrive at its destination but can vary in the time it takes to arrive and delivery is not guaranteed. In contrast, MPLS is like priority express mail with guaranteed delivery for high priority communications. Using traffic engineering features, MPLS raises IP networking to mission critical standards of reliability, ensuring network availability.

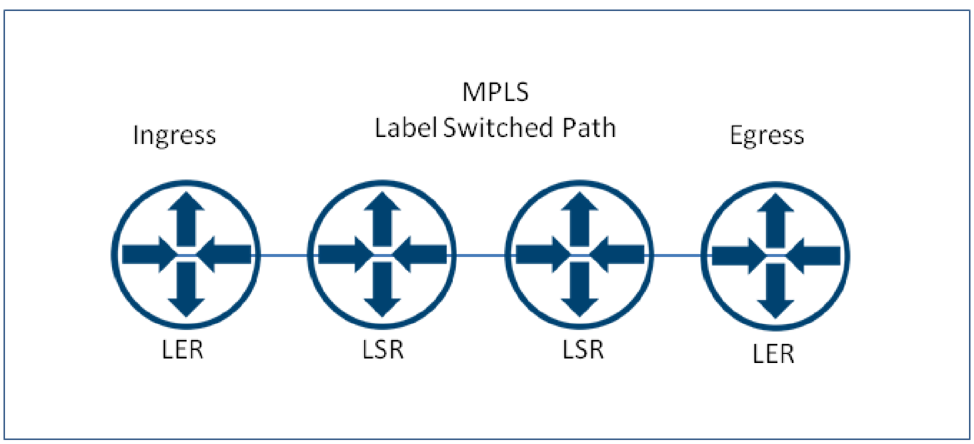
MPLS -Traffic Engineering offers key features such as preplanned alternate routing and prioritization to achieve several mission critical objectives. MPLS is a protocol that uses labels rather than IP addresses to route data communication packets over preplanned paths. It's like placing a shipping label on a package for express guaranteed delivery. In many instances, MPLS can transport labeled traffic faster than IP addressed traffic.

MPLS uses three types of switch/routers:

- **Ingress Label Edge Router (LER)**
- **Label Switch Routers (LSR)**
- **Egress Label Edge Router (LER)**

The ingress Label Edge Router is the entry point into the MPLS network. It receives a packet, analyzes it, places an MPLS label onto it, and forwards the packet to a Label Switch Router. The Label Switch Router is a transit router and forwards labeled packets along predefined paths. The egress Label Edge Router removes the last label before packets leave the MPLS network.

Simplified MPLS Router Diagram



MPLS switches and routes voice, data, and video over predefined paths, known as **Label Switched Paths.** Network managers control where and how data flows on a network over predictable paths and can provide performance guarantees. Paths are preplanned, often based on best paths for speed and capacity. Path routes, speed, and capacity are defined by user rules. Managers can also specify the bandwidth and capacity of label switched paths, over large capacity microwave and fiber networks. For example, video traffic consumes several thousand times more bandwidth than voice. Ample bandwidth capacity is required for video transport. So managers need to optimize bandwidth capacity for peak performance loads and ensure that paths are fast and big enough for time sensitive video and voice applications.

Utilizing another important MPLS feature, network managers can configure preplanned label switched paths as primary paths and alternative back-up paths. If a primary path fails, MPLS switch-routers can switch to alternative back-up paths very quickly, providing network redundancy, reliability, and availability. This is known as **Fast Reroute** and its redundancy is a fundamental mission critical concept. Fast Reroute protects against any single point of failure in the MPLS network. Fast Reroute is automatic and switches and restores path availability quickly.

An additional fundamental mission critical concept is the prioritization of communications. Network managers can prioritize communications traffic using **Class of Service.** For example, real-time command and control voice traffic receives a higher priority than e-mail, ensuring that the essential voice traffic is communicated in real-time even during times of busy traffic or congestion such as large scale emergencies or events.

Network managers can organize government departments so that each department has its own private secure network. This is known as **L3-VPN** (**Layer Three Virtual Private Network**). Operating at layer three of the OSI (Open Standards Interface) computer networking model, Virtual Private Networks can create scalable virtual routing domains and provide end-to-end encryption. Communications remains private and secure from hackers and eavesdroppers, ensuring communications confidentiality and integrity. Cybersecurity access control and end-to-end encryption help protect IP networks and organizations from cyber threats.

Furthermore network managers can separate traffic into logical groups, by departments or agencies. For example, in a municipality or county government, police, fire, emergency management, public works, government administration etc. can have their own Virtual Private Network, while sharing the common municipality or county network. With MPLS, managers can utilize **VPLS** (**Virtual Private Local Area**

Network Service) to link a large number of users or end-points in a common domain or **LAN (local area network).**

VPLS is an Ethernet-based multipoint-to-multipoint layer two VPN.[iv] It allows network managers to connect geographically dispersed organizations and personnel across an MPLS backbone. A virtual local area network is a way to logically segregate networks at the layer two switching or data link level. In MPLS networks, VPLS operates like local area networks but with the added quality and reliability of MPLS. In Public Safety P25 applications, network managers can use VPLS to connect primary and backup LMR communication systems for quick switchover in the case of a primary LMR system outage, ensuring continuity of operations. Another benefit is cost savings. A state or local government department can operate as a private service provider for other government departments, allowing different government departments to share the network while conserving budgets.

Managers can transition and scale their networks using MPLS. Microwave radios and fiber optic cable are the physical transport layers that connect LMR base stations, LTE base stations, computer networks, telephone networks, and end-user devices. As these network elements transition, converge, and grow, MPLS has the scalability to support the transformation and growth. Scalability is important in evolving LTE networks.

Mission Critical Hybrid Microwave Radios and MPLS

Microwave radio plays an important role in linking and transporting LMR and LTE data from base stations or nodes, as well as computer, telephony, and video systems. Microwave radio is a viable high capacity transport system when fiber cable is not available or financially or physically viable. Microwave radio can provide large bandwidth capacity of one Gigabit of data or even greater when aggregated, transporting dynamic voice, data, and video.

In public safety, point-to-point microwave systems are designed with redundancy to protect against failure, ensuring high network reliability and availability. Typically, mission critical microwave paths are designed for at least **five nines** (99.999%) or better availability, which means about five minutes of outage per year. To protect against path failure, microwave radios are configured in a ring topology that provides circuit redundancy. In a spur topology, hot standby radios protect against path failure.

As LMR networks transition from legacy to modern IP networks, the networks that still use legacy **TDM (time division multiplexing)** circuits and devices are best served with hybrid microwave radios. Legacy networks are based on TDM telephony technology. Modern IP networks are based on Ethernet technology. A hybrid microwave radio supports both native TDM and native Ethernet communications traffic, allowing the TDM traffic to be transported without conversion to IP.

Native TDM microwave radios are faster, more efficient, and less likely to cause jitter than emulated TDM, known as **pseudowire** which is method to convert TDM to IP. Furthermore native TDM radios are easy to configure and maintain. However TDM only radios cannot support Ethernet and IP services. So a hybrid radio with native Ethernet is needed too.

Ethernet is the foundation for building IP networks over microwave and fiber transport. Native Ethernet microwave radios include powerful features: layer two switching, virtual local area networks, ring protection, encryption, space diversity, and hot-standby switching.

When deploying MPLS in microwave systems, network and telecom managers can use hybrid microwave radios to efficiently support TDM circuits and devices. As the use of TDM circuits and devices wanes over time, managers can use greater portions of the hybrid radios' Ethernet bandwidth for Ethernet and IP services, gracefully retiring TDM circuits and devices while augmenting Ethernet capacity. Software defined hybrid microwave radios can evolve as the networks evolve.

Furthermore, software defined radios provide cybersecurity solutions that include **FIPS 140-2** compliance and identity management access control. FirstNet requires FIPS 140-2, which is a U.S. government standard for protecting cryptographic encryption modules. Identity management access controls are security controls that authenticate, authorize, and account for technical personnel who configure radios.

Combined with MPLS-Traffic Engineering, hybrid microwave radios provide the access and backhaul transportation network that can support network transition and convergence, while providing mission critical reliability and network availability.

Conclusion

MPLS is the future of multiple converged public safety networks. And that future is now. MPLS provides mission critical reliability and redundancy to support network availability for critical voice, data, and video communications on converging networks. Microwave radio integrates well with MPLS-Traffic Engineering to provide mission critical network reliability and availability.

Successful implementation of MPLS and microwave systems starts with system design based on a detailed understanding of mission critical microwave radios, TDM and Ethernet/IP technologies, and MPLS-Traffic Engineering.

About Microwave Networks

Microwave Networks has MPLS network integration experience. It has integrated MPLS switch-routers with microwave radios for statewide and local networks. It has also partnered with Juniper Networks, a global leader in advanced networking and MPLS.

Microwave Networks has a qualified team of trained and experienced microwave and networking engineers, technicians, trainers, program managers, and administrators, who know how to build, design, integrate, implement, and support reliable microwave networks integrated with MPLS.

With its headquarters and manufacturing facility in Stafford, Texas, Microwave Networks is a trusted global provider of customized microwave and cybersecurity solutions. The company designs, provides, installs, and services licensed and unlicensed, point-to-point and point-to-multipoint microwave systems in the 4–80 GHz bands. Cybersecurity solutions for microwave radio include FIPS 140-2 compliance and identity management access controls. For over 47 years, Microwave Networks has provided reliable microwave communications products and services to public safety, government, utilities, and industrial customers.

Please contact a Microwave Networks Regional Director to learn more about mission critical microwave and MPLS for public safety networks.

Glossary

3GPP	3rd Generation Partnership Project is a group of organizations that define the standards for broadband mobile networks including LTE. Also see LTE
Band 14	The 10 + 10 MHz of spectrum in the 700 MHz band specifically allocated for the public safety LTE Nationwide Public Safety Broadband Network (NPSBN). 788 – 798 MHz is for the base station uplink (receive) and 758 – 768 MHz is for the base station down link (transmit).
Class of Service (CoS)	Prioritizes communications traffic in an IP/MPLS network. CoS groups similar types of communications traffic (for example, voice, video, e-mail, etc.) into classes with each class having its own level of service priority.
Ethernet	Computer networking technology used to structure local area networks typically at layer two. The basis for building IP networks.
Fast Reroute	Fast reroute is a MPLS (Multiprotocol Label Switching) technology that provides fast traffic recovery of path or router failures for mission critical services. Fast reroute provides redundancy for an LSP path.
FIPS 140-2	The Federal Information Processing Standard (FIPS) Publication 140-2, (FIPS PUB 140-2), is a U.S. government computer security standard used to accredit cryptographic modules. FirstNet requires FIPS 140-2.
Hybrid Microwave	Microwave radios that provide native TDM and native Ethernet services. Hybrid microwave supports the transition of legacy TDM to Ethernet IP networks.
Internet Protocol (IP)	The Internet standard protocol is a set of rules and methods by which data is sent over communications networks on the Internet.
Local Area Network (LAN)	A group of electronic devices connected together usually in a limited geographical area, typically the Data link layer or layer two. Also see VLAN.
Layer Three	The Network layer or IP layer of the OSI network model.
Layer Two	The Data Link layer of the OSI network model. Typically the the switching layer.
LMR	Land mobile radio systems commonly known as two-way radios.
Label Edge Router (LER)	An ingress or egress router that places or removes a label on a packet in an MPLS network. The LER is usually placed on the edge of a network.
Label Switch Path (LSP)	A preplanned path in an MPLS network.
Label Switch Router (LSR)	An MPLS router that switches the labeled packets. Also know as a transit router in an MPLS network.
Long-Term Evolution (LTE)	A standard for high-speed wireless communication for mobile phones and data terminals. Commonly referred to as 4G (fourth generation).

MCPTT	Mission critical push-to-talk in LTE broadband networks, defined by LTE Release 13. Expected to be operational by late 2018 early 2019. Also see PTT.
Multi-Protocol Label Switching (MPLS)	MPLS transports multiple technologies and protocols over a single medium. MPLS can transport IP and non IP traffic, connecting different technologies that normally would incompatible. MPLS enables network transition and convergence and improved network security.
MPLS -Traffic Engineering	In the context of MPLS systems, traffic engineering defines several network parameters such as predefined paths, bandwidth, and priority. MPLS- Traffic Engineering designs redundancy, security, and priority into networks to meet mission critical network goals.
OSI Network Model	Open Systems Interconnection (OSI) is a model of seven network layer protocols, categorized by their model layers. Layer 1 is the physical layer; layer 2 is the data link layer commonly using Ethernet to switch frames; layer 3 is the networking layer using IP protocols to route packets; layer 4 is the transport layer which defines grades of delivery; layer 5 is the session management layer; layer 6 is the presentation layer; and layer 7 is the application layer.
P-25	Project 25 or APCO 25 is a suite of standards for land mobile digital radio communications used for public safety.
Protocol	A set of rules that specifies techniques and procedures used in electronic communications.
Pseudowire	A method to emulate various legacy networking or telecommunications technologies in Ethernet/IP, and MPLS networks. Emulated legacy technologies can include T1/E1, ATM, Frame Relay, DSL, and SONET.
PTT	Push-to-Talk enables radio transmission of an LMR handheld, mobile, or base station. Also see MCPTT.
Router	A router is an IP networking device that forwards data packets between computer communications networks. It sends a packet of data from source to destination at the layer three or networking layer, based on IP addresses.
SCADA	Supervisory control and data acquisition (SCADA) is a system used to monitor and control remote meters, sensors, valves, pumps, motors, etc. in telemetry or industrial control systems. Typically used by utilities and the oil and gas industries.
Switch	A networking device that filters and forwards frames of communications data. Switches connect end-point devices together in a network. Ethernet switches operate at the level two or Data Link layer of the OSI model.
TDM	Time Division Multiplexing is the method and process of frames carrying data in every frame and sent at regular intervals. It is a technology used in legacy telephony and data systems.
Virtual Local Area Network (VLAN)	A group of devices on one or more LANs that appear to communicate as if in one LAN, despite the devices being geographically dispersed. VLANs are software configured rather than hardware configured.

Virtual Private LAN Service (VPLS)	A method to organize Ethernet LANs and communicate over IP/MPLS networks.
Virtual Private Network (VPN)	A network technology that encrypts communications for a logical group of users, often over less secure networks or the Internet.

Sources

[i] *Enabling Next Generation Transport and Services Using Unified MPLS*, Broadband Forum, October 2010

[ii] *MPLS Feature Guide for EX4600 Switches*, Juniper Networks, 2016

[iii] *MMBI White Paper on Use of MPLS in LTE,* Broadband Forum, February 2010

[iv] *Introduction to VPLS*, Juniper Networks,
https://www.juniper.net/documentation/en_US/junos15.1/topics/concept/vpn-vpls-introduction.html

Microwave Networks, Inc.

4000 Greenbriar Dr.

Stafford, TX 77477

Tel. 1-281-263-6500
www.microwavenetworks.com