Mission Critical MPLS in Utilities

The Technology to Support Evolving Networks

Application Note

February 2017

Mission Critical MPLS in Utilities

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 for utilities communications networks that use point-to-point microwave systems. This paper is intended for executives, administrators, network managers, and policy makers who are responsible for communications systems.

Table of Contents

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

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

Executive Overview

Utilities communications networks are transitioning and converging. Communications systems are transitioning from legacy TDM (time division multiplexing) to IP (Internet Protocol) systems. In addition, broadband networks are converging with narrowband networks. As a result, new voice, data, and video services are transforming utilities communications networks. These new networks and services are based on IP frameworks and standards.

To backhaul new IP networks and services, utilities are turning to **MPLS (multi-protocol label switching)** to support existing and future utilities broadband networks.

MPLS is the right technology to support the transition of legacy TDM to digital IP and the convergence of 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.

MPLS supports,

- Network redundancy
- Prioritization of communications traffic
- High bandwidth capacity
- Performance guarantees
- Virtual Private Networks (VPN)
- Interoperability of department 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, utilities are utilizing MPLS to handle the transition and convergence of narrowband and broadband network technologies including microwave networks. When deploying MPLS in microwave systems, utilities can use **hybrid microwave** radios to efficiently support the transition of mission critical legacy networks to modern IP networks.

MPLS is the data carrying networking and backhaul technology that supports the transition and convergence of communications 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. 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 utilities utilize MPLS. As an example, Pinal County, Arizona is implementing MPLS in its land mobile radio 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. 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.

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. IP 'best efforts' routing 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 **Label Switch-Routers** to label and forward traffic, providing end-to-end connectivity and communication.

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 utilities 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. Cyber security 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, public works utilities, police, fire, emergency management, 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. 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 utilities' LMR (land mobile radio) DMR (digital mobile radio) or P25 systems, 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. Different utilities departments can share the network while conserving overall budgets.

Managers can transition and scale their networks using MPLS. Microwave radios and fiber optic cable are the physical transport layers that connect nodes, 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.

Mission Critical Hybrid Microwave Radios and MPLS

Microwave radio plays an important role in linking and transporting 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 critical infrastructure networks, 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 TDM networks transition from legacy to modern IP networks, the networks that still use legacy TDM 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.

Cyber Security

Software defined radios provide cyber security solutions, providing network confidentiality, integrity, and availability. Cyber security controls include FIPS 140-2 encryption protections. Identity management access controls identify, authenticate, authorize, audit, and account for technical personnel who configure radios, providing integrity. NERC CIP v5/v6 standards specify identify management and access controls to protect cyber assets contained within electronic security perimeters in low, medium, or high impact systems.

MPLS-Traffic Engineering, hybrid microwave radios and their cyber security controls provide the access and backhaul transportation network that can support network transition and convergence, while providing mission critical reliability and network confidentiality, integrity, and availability.

Conclusion

MPLS is the future of multiple converged utilities 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, advanced networking, and cyber security 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, utilities, utilities, and industrial customers.

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

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

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