COMMDEX

IP/MPLS Whitepaper

Benefits of Converged Networking in a Public Safety Environment

Table of Contents

Introduction

Present day public safety agencies are continually called upon to protect and serve their communities with increasing responsibilities. These agencies are most effective in performing their mission when their personnel are able to efficiently communicate, share information, and are aided in decision making in a fast-paced situational environment.

Traditionally, the systems utilized for each agency's first responder communications, 911 dispatch, traffic management, video surveillance, and machine-to-machine communications have been separate and standalone, or separate with defined interconnection points. In the case of the former, there is no communication between agencies or subsystems. In the case of the latter, these interconnection points are the hinges upon which interoperability rely and are often bottlenecked.

As has been evidenced in many high-profile emergencies, multiple first responder agencies will convene upon a scene for disaster recovery after a hurricane or tornado, or upon an area as a result of an amber alert, only to learn that they cannot communicate with one another to provide a coordinated response. They are unable to be aided by anyone who wants to communicate but is not using pre-authenticated devices such a specific radios, and specific wireless channels. Dispatchers begin to play an overarching role for relaying communications. Critical messages can be lost or modified in a fast-paced response.

As some time passes, responders become equipped with multiple devices to communicate on multiple networks. Mutual-aid wireless channels begin to be used on a regional or state-wide level to provide some level of coordinated response. At this same time, the responder is still shut out of cross-agency data systems. He or she is most likely unable to see mobile surveillance video deployed by his or her home agency while communicating with a visiting agency. Communications become fragmented, the responders are frustrated, the response is slow, and victims adversely impacted.

These types of scenarios continue to dominate the day-to-day operations of the first-responder due to a lack of a unifying set of networking standards and protocols. Until recently, the amount of information transmitted was small and the need was not evident to have a single individual accessing multiple systems and then relay new information across agencies.

To solve these inter and intra-jurisdictional subsystem communications challenges and leverage high speed, low latency technologies, public safety agencies need to consider converged backbone networks. In a converged backbone network, a single, hardened network in a given geographic area carries all public safety traffic, with various agency subsystems sharing traffic paths. The argument is that the need for interoperation transcends public safety radio traffic and requires the use of various Internet Protocol and Networking standards to implement robust, seamless, data-driven networks with hierarchical priority.

Current Public Safety Network Landscape

The primary use of a public safety communications network in the past has been two-way Land Mobile Radio (LMR) traffic amongst first responders. These users communicate with their command to provide coordinated incident response on the ground in a speedy manner. 911 Dispatch also utilizes this network to direct the responders to specified locations. Prior to the need for data services, or external agency resources, this type of network was quite suitable for emergency response. Individual macro radio frequency (RF) sites would broadcast signals to communicate with the hand-held radios. These sites utilized T1 based backhaul at a line rate of 1.544 megabits per second. Multiple T1s could be connected for additional throughput as needed. In many cases, these T1 uplinks would aggregate over a microwave network that interconnected the sites to the dispatch core. This microwave network would support a DS3 or OC-3, as the TDM interface over SONET to carry the traffic.

Prior to the rise of higher bandwidth data networks, a pure TDM network met the capacity and system interoperability needs of the end users. T1 capacity truly comes into question when a first responder needs to call up a data file, or transmit or view video from his or her vehicle, while communicating with other users and other agency members are doing the same. Additionally, each T1 dedicated in a system is a fixed allocation regardless of use. From an efficiency standpoint an improvement stood to be made where a system was only burdened by the traffic of its users at any instantaneous moment in time.

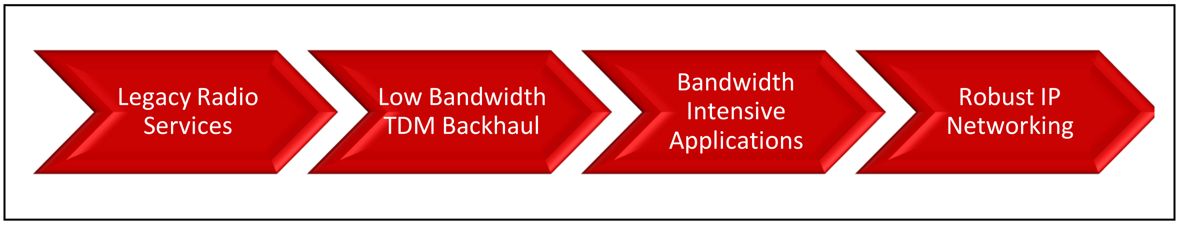

Figure 1. Evolution of TDM Radio Networks to IP Networking

The need of public safety users to access Ethernet services continues to create a dilemma in communication networks that are not converged. Access to digital surveillance cameras, digital files, records, databases, are not readily available to users of a traditional LMR network. This problem is further compounded when additional agencies arrive and are using separate carrier-based networks. In an ideal situation, a responder crew arriving at a large structure fire would be able to quickly coordinate a response, download building plans showing critical stairways and water lines, and simultaneously radio another agency in the next jurisdiction for relief. As public safety broadband networks become available in the next few years via FirstNet, agencies will finally have access to private broadband networks to fill this gap. However, this also means that the traditional TDM and SONET networks that have interconnected legacy systems for years will be inadequate to support this new need. A migration to converged IP networks is the answer to allow these agencies to merge the voice and data traffic from their various networks, which allows users to perform at their very best in their missions to save and protect lives.

The Migration to All-IP

Modern day IP networks offer a set of new features and standards that make them less costly to deploy and easier to implement, while offering all of the redundancy and security capabilities of legacy TDM systems. As an added bonus, higher capacities are the norm, bringing in a much lower cost per bit in operating expenses. These networks are "future-proofed" for a much longer period of time, requiring less expense for public safety agencies that are procuring new communications technologies.

A major agency concern is that bandwidth may not be allocated for essential services such as two-way radio traffic, resulting in service affecting congestion. Implementing Multi-protocol Label Switching (MPLS) allows for individual traffic streams to be segregated while utilizing the same “pipe” and alleviating those concerns (Figure 2). In the IP networking world, bandwidth is only constrained by the capacity of the digital fiber or microwave backhaul. Capacities routinely exceed several hundred megabits and can reach up to 10 gigabits per second.

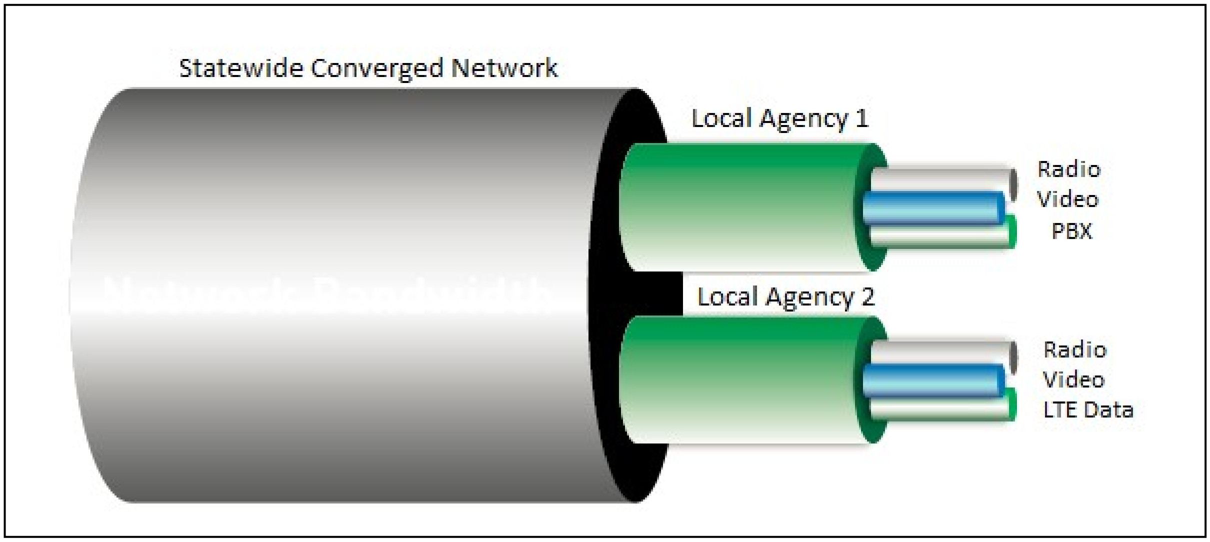

Figure 2. Converged Network with Multiple Traffic Streams

To allow for seamless migration, IP infrastructure can be provisioned to allow for native TDM operation during the migration. That is to say, the legacy devices such as radio systems or analog cameras can continue operation on the new IP network, by carving out bandwidth reserved for them. As systems are upgraded, this bandwidth is dynamically allocated to new packet Ethernet services and devices. As networks grow, new MPLS services are nearly “plug and play” and allow for rapid scaling, enabling those networks to be utilized to their full potential and yield greater communications efficiencies. The following section outlines basic operation of IP/MPLS networks.

MPLS Functionality for Public Safety

In an MPLS network, Label Switched Paths are established, creating a virtual network for each device that is connected to the backbone. This allows for multiple types of traffic from multiple applications and from multiple agencies to share the same physical infrastructure, simultaneously (Figure 2). Individual networks can be kept logically separate, while sharing data between them through MPLS switching devices, in a truly interoperable fashion. If interoperability is required across multiple jurisdictions or states, this can be accomplished by crossing the network “border” and “speaking” to the target network. Since both networks ideally utilize MPLS, they speak the same language and also interoperate.

The three key features of MPLS public safety networks that preserve network quality are Fast Reroute, Bandwidth Efficiency, and Quality of Service (QoS). New MPLS networks should be designed in ring node configurations that will allow for the leveraging of the Fast Reroute feature of MPLS. This is akin to legacy 50 millisecond SONET protection switching, in the event of link or node failure. All nodes are aware of best paths through Open Shortest Path First (OSPF) protocol and Interior Gateway Protocol (IGP), and can reroute traffic rapidly, preserving system uptime for critical traffic.

A new IP based network should be able to accommodate multiple services and applications for first responder use, beyond radio communications traffic. MPLS routers at each site node ensure that bandwidth is only consumed if traffic is transmitted, as previously mentioned. What this does is allow for multiple services to be simultaneously deployed and available for use on the single network.

To preserve the most critical traffic, QoS is implemented on the network. For example, a network may transport radio communication traffic, video surveillance from mobile command centers, and traffic cameras. The network will have different priority QoS settings for each type of traffic, in this case, with radio communications as highest priority and traffic cameras as lowest priority. During times of network congestion, this ensures that radio communications for mission critical personnel remains uninterrupted. Without QoS, various traffic streams compete for available bandwidth under network loading and the end result is delay, jitter, and service outages for the user. Fortunately, implementation of these traffic classes is straightforward and defined in a tabular format within the network.

Because MPLS by definition is Multi-Protocol, expansion of services into a backbone is categorized as plug-and-play. If the network in the previous example is on-air and carrying radio traffic and two types of video traffic, it is relatively easy to add in a database of real-time GPS locations of each vehicle in a patrol fleet. This allows a fleet manager to use the same network a dispatcher is using to schedule vehicles for maintenance. If the dispatcher needs to know the location of the closest officer, that same information is available through the converged network. If the users decide, this database traffic may have second to last priority. To expand upon an earlier example, if the building commission of the municipality wants to add its databases of building plans, that can similarly be added to this same network, and a first responder can access this while on a service call.

To support such a network, MPLS nodes are constantly self-aware and they update their routing and forwarding tables in real-time. Deployed router configurations allow for redundant control modules, power supplies, and switch fabric. This allows for an always-on, always-optimized switching network that ensures the highest availability for public safety users.

The Converged Network

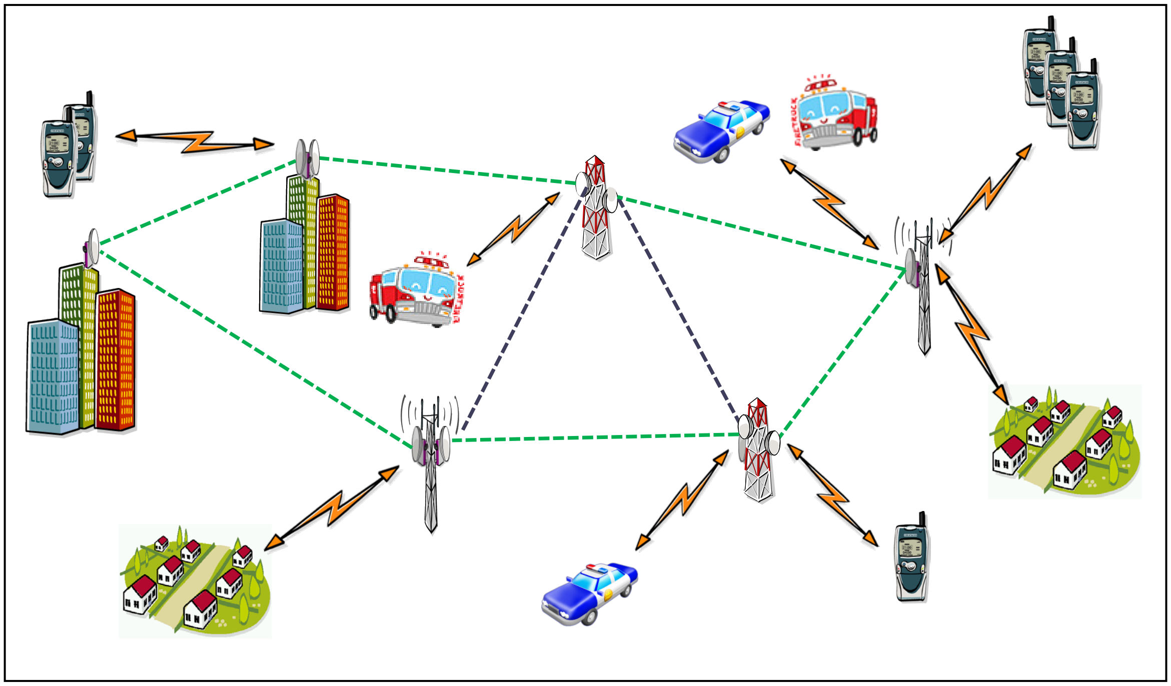

Figure 3. Sample Converged Network with Protected Ring Configuration

The network of today and the near future for public safety calls for convergence of voice, video, and data traffic on a single low-latency, high-throughput network in a secure manner. Different services must be managed with varying degrees of priority, while allowing interoperation between those services to efficiently allow first responders to collaborate, coordinate, and execute on their respective missions without delay. With the proper planning and sizing, the network can be "future-proofed" to allow for the addition of new services that further allow jurisdictions to save cost by utilizing a single shared, appropriately managed IP/MPLS converged backbone.

A standards-based integrated backhaul network is the best way to ensure that multiple agencies and jurisdictions can communicate to meet the needs of the communities they serve during first-response events. Given the backwards compatibility of today's networking technologies, municipalities can seamlessly transition from older public safety communications system to new, integrated networks. This allows new features to be implemented while retaining legacy functionality, ultimately leading to quicker response times and fewer interoperable communications failures.