MISSION-CRITICAL COMMUNICATIONS NETWORKS FOR PUBLIC SAFETY

HIGHLY RELIABLE CONVERGED IP/MPLS-BASED BACKHAUL

APPLICATION NOTE

Alcatel·Lucent

ABSTRACT

Public Safety personnel rely on communications to keep connected, maintain security, enhance safety, and gain situational awareness. New broadband applications and the need for greater efficiency are changing the requirements for public safety backhaul networks. Dedicated backhaul networks have become restrictive and are being replaced with converged wide area networks (WAN). Alcatel-Lucent delivers a converged IP/Multiprotocol Label Switching (MPLS)-based communications network for public safety using next-generation products and advanced management tools. The Alcatel-Lucent IP/MPLS, microwave, and optics products support network resiliency, quality of service (QoS), virtualization, accurate synchronization, convergence, and a management platform that automates and simplifies operations. Deploying a modern, reliable, and flexible Alcatel-Lucent IP/MPLS network will enable a public safety agency to migrate to a converged network that can effectively support performance guarantees on new IP and packet based and traditional time division multiplexing (TDM) based applications such as land mobile radio/professional mobile radio/terrestrial truck radio (LMR/PMR/TETRA), video surveillance, sensors, remote download, and long term evolution (LTE) mobile broadband. Reliable communication is essential to meeting key objectives of providing “always on” services, increasing security, and improving network efficiency and staff responsiveness while serving the public. A transformation to converged IP/MPLS and packet microwave backhaul optimizes performance, reduces both capital expenditures (CAPEX) and operating expenses (OPEX), and provides a foundation for LTE deployment.

TABLE OF CONTENTS

INTRODUCTION

A secure, reliable communications network is critical to the operation of public safety agency. Their responsiveness depends heavily on maintaining emergency communication and the access to and sharing of information. With continued security threats and the demands for greater efficiency with more effective cross agency coverage, the modernization of public safety communications networks is a priority for many public safety agencies.

A traditional public safety communications network uses plesiochronous digital hierarchy (PDH) and /or synchronous digital hierarchy (SDH)/synchronous optical network (SONET) based TDM technologies. As technologies have evolved, IP-based voice, video, and data systems provide superior performance over traditional approaches to mission-critical communications. Many public safety communications networks are evolving to broadband solutions which utilize an IP WAN for first responder radio networks, video surveillance, LTE, improved interoperability, and better integration with growing IT applications. Many of these applications are resource intensive and require substantially more bandwidth than existing mission-critical voice and sensor traffic. Agencies can effectively address public safety IP communications requirements and control costs by deploying a converged IP/MPLS-based network.

Alcatel-Lucent has state-of-the-art, highly reliable and secure, IP-MPLS-based communications equipment that can form a single converged network, with integrated optical and microwave packet transport, providing a reliable infrastructure to support mission critical voice, video, and data communications. This approach expands broadband to first responders while transforming traditional backhaul and site-to-site communications to a converged network that enables true multi-agency interoperability with enhanced safety and efficiency. An IP/MPLS network improves the bandwidth efficiency of a public safety network, saves costs, enables easier access to existing government databases, and enhances the safety of the general public as well as the safety of personnel delivering these services. Performance guarantees for critical applications such as LMR/PMR/TETRA and video surveillance are enabled with an IP/MPLS converged network. Alcatel-Lucent's management platform improves efficiency by automating and simplifying operations management for communications services, thus reducing any barriers of introducing IP/MPLS-based technologies and services.

PUBLIC SAFETY COMMUNICATIONS CHALLENGES

The primary purpose of a public safety network is to carry mission-critical LMR/PMR/TETRA traffic. The communications network must provide services that can be shared among agencies, expandable into new areas, and easily managed end to end. The emergence of new applications such as mobile broadband and video surveillance, and the growing need for resiliency and interoperability between agencies are important reasons for change. Better communications and interoperability are now possible with the introduction of IP communication. TDM technology is limited in efficient bandwidth usage when handling IP-based traffic which is bursty and dynamic in nature. With a growing need to increase the efficiency and bandwidth of networks and allow more centralized high impact applications on the network, many agencies are modernizing their communications infrastructures by replacing legacy LMR/PMR/TETRA and microwave backhaul networks from the current TDM-based backhaul to IP-based converged WAN networks.

Moving to IP and packet based solutions

IP-based solutions offer many benefits. For example, IP-based LMR voice messages can be sent in compressed and encrypted IP packets end-to-end, providing a high level of security while maintaining voice quality. IP-based communication allows easier interoperability between agencies. For example, connecting a county's emergency center to the state police can help reduce isolated islands of communications. Other benefits include the integration of the network with off-the-shelf IP data applications and interconnection of peripherals such as scanners and video devices. This means first responders will have higher speed access to many databases of critical information such as video archives, building plans, and GPS coordinates. Video surveillance is being deployed in extended areas. A large agency that uses video surveillance extensively could easily have hundreds or even thousands of video sources requiring packet traffic to be sent to multiple viewing sites and storage areas. Another advantage is the integration with LTE mobile broadband to provide higher bandwidth for applications over a large footprint. A successful implementation of IP-based solutions requires a highly reliable IP backbone network that can support a broad range of new applications from broadband data and video to voice interoperability.

Alcatel-Lucent has a highly reliable, secure IP/MPLS-based converged network that enables public safety agencies to meet the performance requirements of all their mission-critical services and applications. An IP/MPLS implementation offers advantages and savings such as:

- Optimizing the bandwidth available in the network to make possible the introduction of new applications
- Reducing the dependency on leased lines
- Satisfying the growing bandwidth demands and IT functions
- Enabling LTE backhaul for mobile broadband
- Reducing network complexity and improving efficiency with integrated IP/MPLS and packet microwave functionality over a single infrastructure

These not only enhance the safety of the general public but also expand the use of the network and the investment of the agencies.

THE ALCATEL-LUCENT IP/MPLS NETWORK

Many public safety agencies have deployed or are deploying IP-based core networks to support all of their backhaul and WAN communications needs. Not all IP-based solutions are appropriate for public safety agencies. To simultaneously support all levels of mission-critical and non-mission-critical traffic of a public safety operation, an IP/MPLS-based communications network is needed. Non-MPLS-based IP networks have grown significantly in recent years, but they often lack the necessary scalability to support traffic that requires QoS levels for mission-critical operations. Traditional IP and Ethernet networks also lack the ability to optimize the use of network resources and the capability to react to network events fast enough to guarantee end-to-end QoS per application.

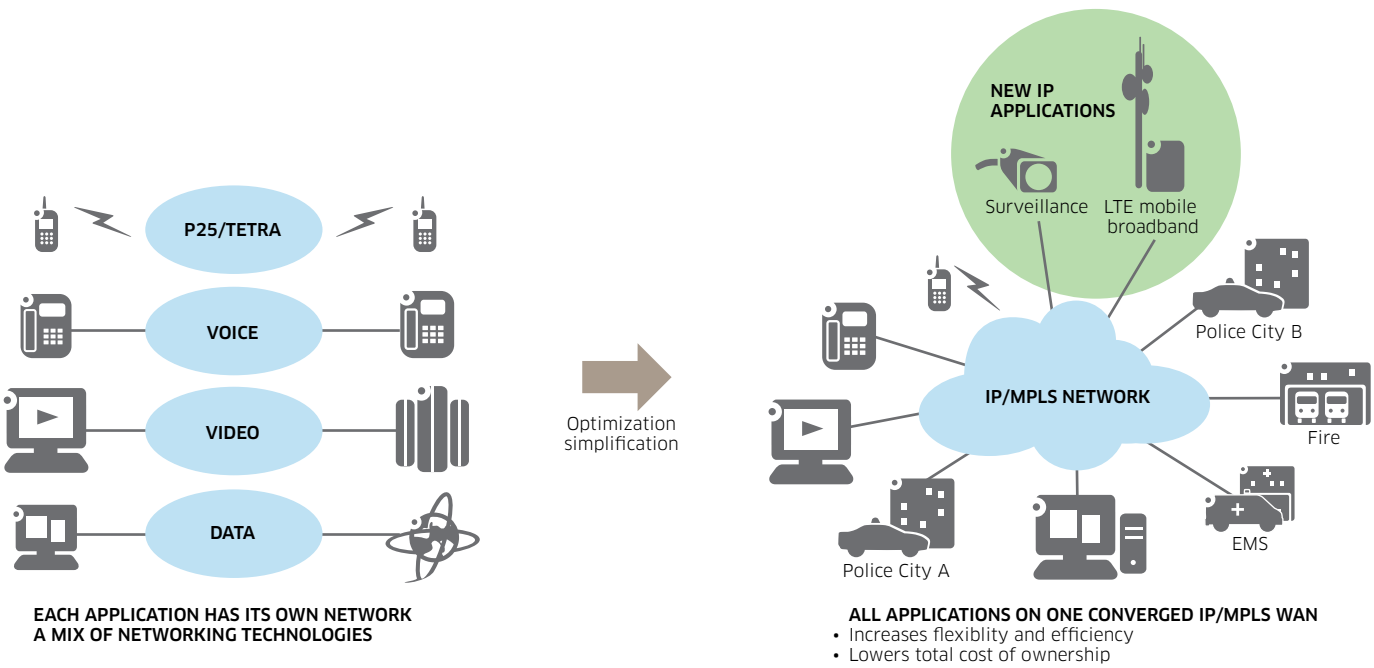
By using IP/MPLS, the public safety agency gets the best of both worlds — an IP network that has the robustness and predictability of a circuit-based network along with high capacity and support for bursty traffic. The IP/MPLS network enables the deployment of new IP/Ethernet applications as well as support of existing TDM-based applications, allowing the agency to improve services to its users. With an IP/MPLS network, the agency has a secure network with the following features:

- Highly scalable and reliable with redundancy and Fast Reroute (FRR) capabilities
- Addresses a range of QoS and service level agreement (SLA) requirements
- Optimizes bandwidth usage and avoids common modes through traffic engineering
- Extensive operations, administration, and maintenance (OAM) tools for troubleshooting and maintenance
- Advanced network and service management to simplify operations
- Supports future LTE deployments

Each application on the network has unique requirements for bandwidth, QoS, and availability. The IP/MPLS network enables the public safety agency to set service parameters for each service and traffic type (for example, multiple types of voice, video and data traffic) according to operational requirements. This network is also capable of supporting low jitter and delay to handle all traffic types effectively and reliably in real time. In addition, the Alcatel-Lucent IP/MPLS network supports advanced capabilities, including non-stop routing, non-stop services and FRR, to maintain high network resiliency.

Figure 1 shows the concept of a converged IP/MPLS network. With a converged network model, an agency no longer needs to deploy separate dedicated networks for individual applications and can support all applications on a single physical infrastructure with network virtualization – resulting in greater overall network capacity, efficiency, performance and availability in an environment of strained agency budgets.

Figure 1. Converged network model



Virtualization

The Alcatel-Lucent IP/MPLS network provides for the virtual isolation of various traffic types on a single infrastructure using virtual private networks (VPNs). These VPNs enable the full separation of traffic from different applications or agencies sharing the single network, allowing for a secure environment and effective bandwidth allocation. Advanced IP/MPLS VPNs — such as Circuit Emulation Service (CES), virtual private LAN service (VPLS), and IP VPNs — are supported which can then be used to provide different applications to agencies in an environment that is private and unaffected by other traffic. One service is carried across one VPN while the traffic of different services is securely separated in their own VPN, effectively providing separate private networks.

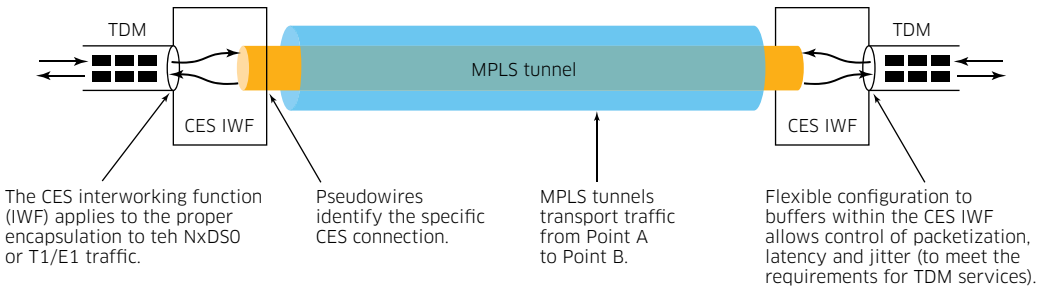
Circuit Emulation Service

Public safety agencies need to consider that they can leverage new IP/MPLS network technologies when migrating legacy TDM systems and services. Public safety agencies can take advantage of the IP/MPLS CES functionality and transition their legacy applications gradually. CES delivers the same quality of service as the existing TDM network infrastructure, with the same level of predictability. The Alcatel-Lucent IP/MPLS network has a circuit emulation interworking function that ensures all information required by a TDM circuit is maintained across the packet network. This provides a full transition to a packet network over time while providing TDM service continuity.

Two principal types of circuit emulation can be used: Circuit Emulation Service over Packet Switched Network (CESoPSN) and Structure Agnostic TDM over Packet (SAToP). CESoPSN allows NxDS0 service, including full T1/E1 capability. SAToP provides the ability to carry unstructured T1/E1 circuits across the IP/MPLS network.

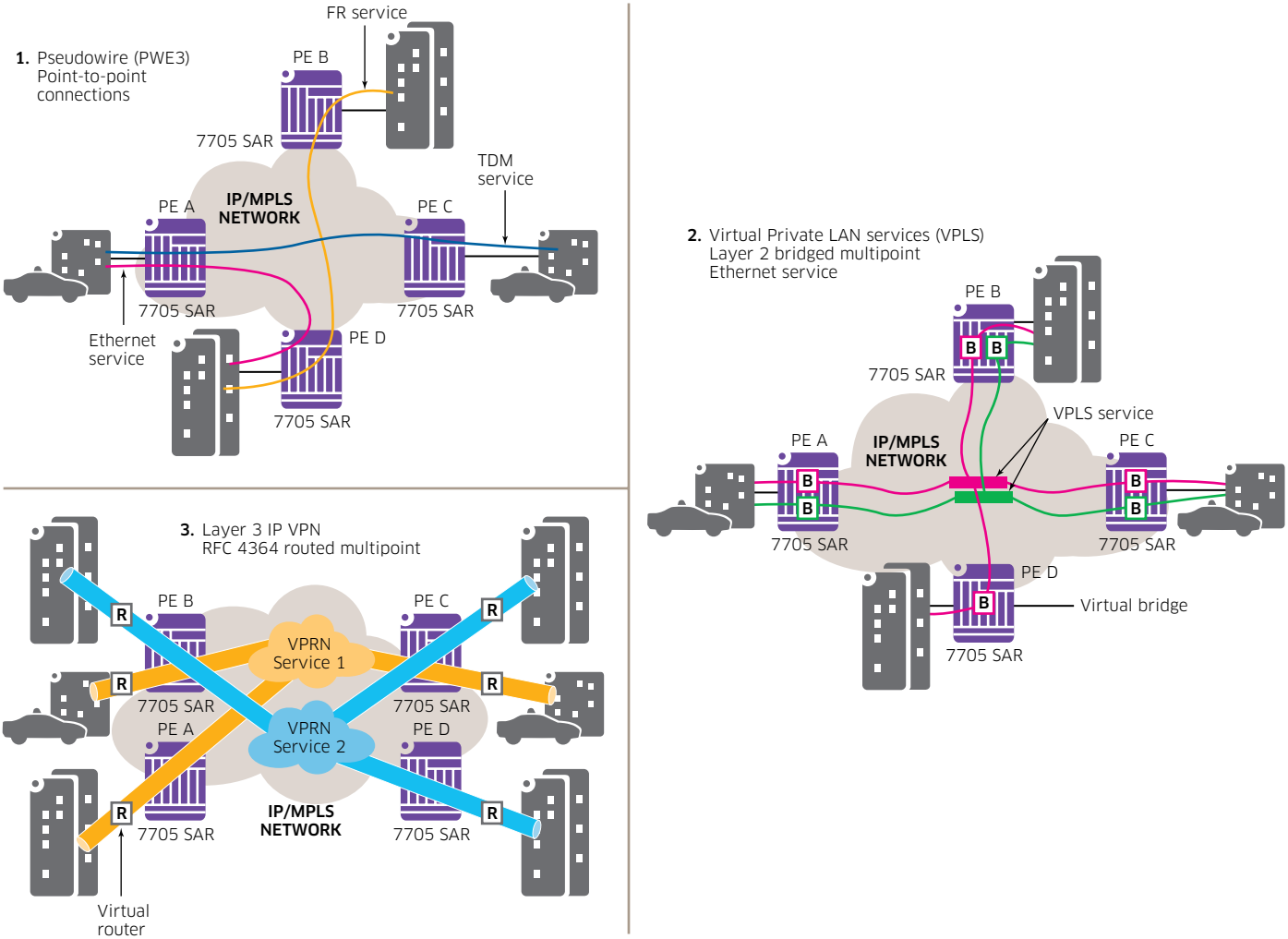
In an IP/MPLS network, the MPLS tunnel is used as the transport layer (Figure 2). A pseudowire is created to identify the specific TDM circuit within the MPLS tunnel. The circuit emulation service interworking function (CES IWF) ensures that all information required by the TDM circuit is maintained across the packet network. This function provides a transparent service to the end devices.

Figure 2. Circuit Emulation Service functionality overview



A pseudowire, also known as virtual leased line (VLL), encapsulates traffic over label switched paths (LSPs) to create a point-to-point service. An MPLS pseudowire is analogous to a private line within the IP/MPLS network. It offers a point-to-point connection between any two end devices. Figure 3-1 depicts three different types of pseudowires — TDM, frame relay (FR), and Ethernet. The pseudowire can be used for applications that require dedicated point-to-point connectivity. For example, pseudowires support the transport of legacy voice, data, and alarm applications, along with LMR/TERTA traffic backhaul using T1/E1, serial, and, E&M interfaces to enable the migration of SDH/SONET networks to IP without impacting the long life cycle of traditional applications.

Figure 3. IP/MPLS-based VPN services



Virtual private LAN service

VPLS is a bridged multipoint service that forwards traffic based on the media access control (MAC) address. A VPLS is protocol-independent and enables multipoint connectivity at Layer 2 within the IP/MPLS network. Figure 3-2 depicts two VPLS instances within a network. VPLS is composed of virtual bridges at each node. Each virtual bridge performs MAC learning and constructs a table that maps MAC addresses and corresponding MPLS paths. The VPLS concept is similar to a logical LAN connection where all end devices connected to the VPLS appear as if they are within the same LAN segment.

IP VPN

An IP VPN is a Layer 3 VPN, a routed service that forwards traffic based on the IP address and is implemented specifically for IP traffic only. An IP VPN enables multipoint connectivity at Layer 3 within the IP/MPLS infrastructure (Figure 3-3), with each IP/MPLS node supporting virtual routing and forwarding (VRF) instances.

The Alcatel-Lucent solution

The Alcatel-Lucent IP/MPLS implementation provides a service-oriented approach that focuses on service scalability and quality, as well as per-service OAM. With a service-aware infrastructure, the agency has the ability to tailor services such as mission-critical applications so that it has the guaranteed bandwidth to meet peak requirements. The Alcatel-Lucent service routers support IP routing and switching, which enables the agency to support real-time Layer 2 and Layer 3 applications.

The Alcatel-Lucent converged IP/MPLS network leverages multiple state-of-the-art technologies. The network extends IP/MPLS capabilities from the core to access and can include the following main components:

- Alcatel-Lucent 7750 Service Router (SR)
- Alcatel-Lucent 7705 Service Aggregation Router (SAR)
- Alcatel-Lucent 9500 Microwave Packet Radio (MPR)
- Alcatel-Lucent 7450 Ethernet Service Switch (ESS)
- Alcatel-Lucent 7210 Service Access Switch (SAS)
- Alcatel-Lucent 1830 Photonic Service Switch (PSS)
- Alcatel-Lucent 5620 Service Aware Manager (SAM)

The Alcatel-Lucent IP/MPLS products provide routing, switching and multiservice capabilities, enabling the public safety agencies to support real-time applications across the full extent of the network. The Alcatel-Lucent IP/MPLS implementation includes non-stop routing and non-stop service capabilities that provide unparalleled reliability.

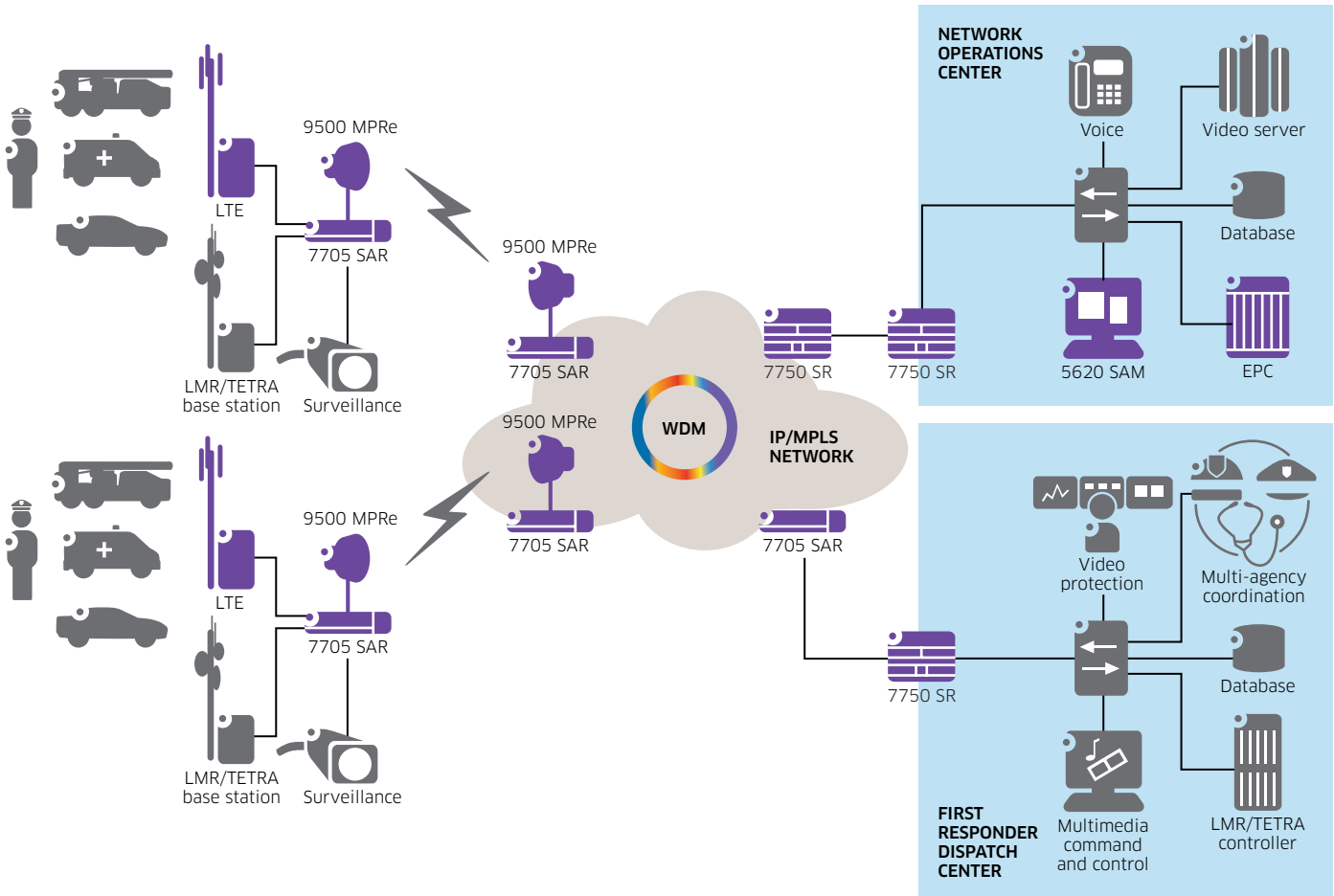
Microwave transmission systems are used extensively in public safety backhaul networks. Microwave provides great connectivity coverage where wireline connectivity is unavailable or impractical. Many public safety agencies used PDH and/or SDH/SONET microwave radio as a major part of their backhaul networks. In response to the need to support increasing packet application traffic, microwave systems have also evolved in recent years. In the Alcatel-Lucent converged network, the native packet microwave architecture of the Alcatel-Lucent 9500 MPR is optimized for a predominantly data-driven traffic mix by providing native packet transport over the radio link. Leveraging packet microwave, existing microwave licenses are maximized through applying packet techniques to optimize bandwidth and maximize payload capacity per radio link. Microwave packet radio introduces the ability to transport multimedia traffic efficiently while still supporting legacy TDM traffic. This combined packet and legacy traffic aggregation increases bandwidth utilization and optimizes Ethernet connectivity, which are critical for cost-effective broadband traffic support. Different redundancy mechanism can be configured or deployed on the 9500 MPR to ensure the availability over the wireless links. Simplified deployments are enabled through common outdoor units (ODUs) that can be deployed across all microwave applications including all-outdoor, split-mount and all-indoor applications.

An optical transport layer using coarse wavelength division multiplexing (CWDM) and/or dense wavelength division multi¬plexing (DWDM) can also be used for increasing backbone network capacity and for Data Center Connect. WDM enables public safety agencies to cost effectively scale their communications networks and services by maximizing fiber utilization and performance. As a highly integrated packet-optimized WDM solution, the Alcatel-Lucent 1830 PSS simplifies the aggregation and transport network by aggregating packet traffic efficiently, packing wavelengths to offer massive scalability and networking efficiency.

The network and service administration of the Alcatel-Lucent converged IP/MPLS communications network is handled by the industry-leading Alcatel-Lucent 5620 SAM, an integrated application that covers all aspects of element, network and service management on one platform. It simplifies the provisioning and management of the network, including automating routine tasks, correlating alarms to problems, managing the assignment of end-to-end connections, and facilitating the introduction and administration of new services, all through a user-friendly point-and-click interface. The Alcatel-Lucent 5620 SAM not only manages the Alcatel-Lucent IP/MPLS, microwave, and optics equipment, but it also is capable of managing third-party elements within the network. In addition, the Alcatel-Lucent end-to-end LTE wireless mobile broadband solution, from access to backhaul to packet core, is also managed by the 5620 SAM to enhance and maximize the benefits of the multiservice IP/MPLS network.

Figure 4 shows a typical Alcatel-Lucent converged IP/MPLS communications network for Public Safety. Pseudowire, VPLS, and IP VPN are used to provide network virtualization. The Alcatel-Lucent IP/MPLS network has proven very successful in helping public safety agencies to deploy a converged network for all applications while maintaining QoS for each type of application. This mission-critical design is ideal for the public safety agencies because it is capable of coping with not just LMR/TERTA voice traffic but thousands of video streams, voice traffic, and various data services simultaneously.

Figure 4. Alcatel-Lucent IP/MPLS Communications Network for Public Safety

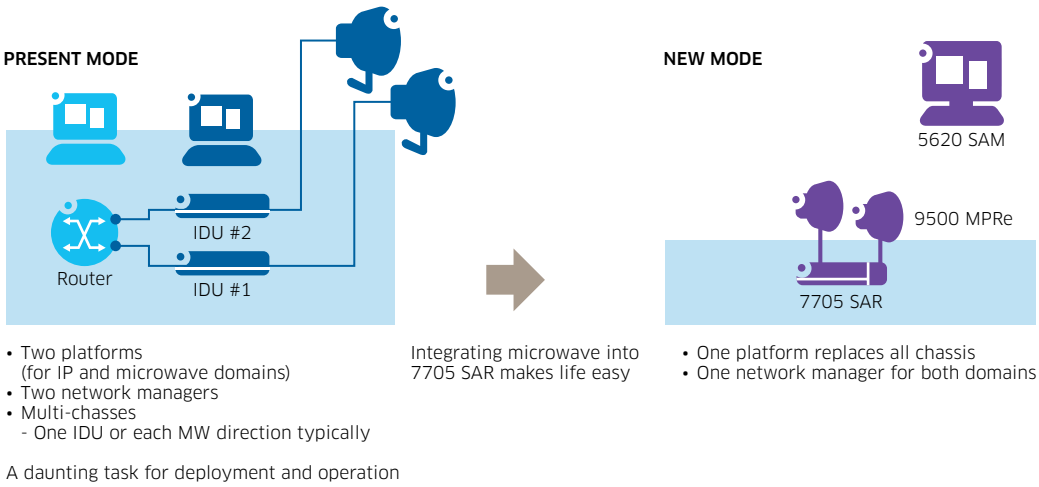


Land Mobile Radio Backhaul

A LMR/TETRA system communicates between the controller and the base stations, and the traffic is transported by the IP/MPLS-based microwave backhaul network. The IP/MPLS network provides the necessary network wide reliability, security, quality of service, and bandwidth optimization. Unlike traditional TDM implementation, an IP/MPLS based network allows microwave radio bandwidth to be used in a dynamic manner such that network bandwidth is only consumed if user traffic is present. This means more applications with higher bandwidth can be converged and carried over the same network.

Figure 5 shows the integrated 7705 SAR and 9500 MPRe configuration. Instead of a traditional architecture overlaying IP/MPLS over microwave transmission between two platforms, the 7705 SAR is fully integrated with the 9500 MPR for a single seamless platform across the IP and microwave domains. This tight integration provides many advantages including the elimination of multiple network managers, elimination of multiple indoor units (IDUs) for direct connections, rapid detection of fault, reduction of equipment space and sparing requirements, reducing power consumption and cooling needs, and streamlining installation and operations management.

Figure 5. Integrated IP/MPLS and Packet Microwave Transport



IP video surveillance

For a large agency that uses video surveillance extensively, hundreds or thousands of video sources may each require the support of Mb/s of bandwidth. This can add up to a substantial amount of IP traffic that needs to be cost effectively supported. Therefore, the public safety WAN communications network must be able to handle the massive amounts of video traffic generated by the surveillance cameras. Maintaining the flow of this video traffic from each camera toward the dispatch and operation centers is key to the safe and effective operation of the public safety agency.

Modern video surveillance systems are IP-based and are integrated with the WAN using a network-based architecture. Managing video traffic can be a challenge for agencies that are still using traditional networks. Adding surveillance video traffic onto an IP network unprepared for video traffic can adversely impact all services on the network.

The Alcatel-Lucent IP/MPLS network can address the video surveillance requirements for guaranteed delivery of mission-critical surveillance video traffic and concurrent support of other critical data and voice traffic on a single converged network. The network is capable of handling current video traffic levels and future growth, including significant increases in bandwidth.

Distributed video surveillance offers many advantages, including support for real-time video streaming in many locations and the flexibility to deploy video analytics software remotely. Because access and distribution of surveillance video streams can be very dynamic and mission-critical in nature, the highly scalable and reliable Alcatel-Lucent IP/MPLS network is ideal for handling thousands of video streams now required in modern surveillance applications.

Support for LTE

Many mobile operators worldwide have deployed the Alcatel-Lucent IP/MPLS network for LTE backhaul. The same IP/MPLS network that a public safety agency can deploy to support all the communications requirements including LMR/TERTA voice today is also ready to effectively support future LTE backhaul deployment.

CAPITALIZING ON IP/MPLS CAPABILITIES

Convergence of application traffic on a single network creates a need for high-capacity networks that support high bandwidth and flexible multipoint communications. Many public safety agencies have deployed their own IP/MPLS networks. IP/MPLS brings the advantages of a circuit-based network to an IP network, and enables network convergence, virtualization and resiliency.

CAPEX/OPEX and scalability

To meet public safety agencies' growing requirements for service deployment and bandwidth, the Alcatel-Lucent IP/MPLS network is extremely scalable, according to changing requirements. The IP/MPLS network can accommodate a growing number of applications and services. Minimal CAPEX requirements to deploy and scale this infrastructure are the result of the granularity in bandwidth, scaling options, and statistical multiplexing. The converged architecture and the ease of network management allow for optimized OPEX. A converged network also reduces the number of network elements required, thus also reducing costs.

Multiservice support

The Alcatel-Lucent IP/MPLS network offers a flexible network and service environment that enables the continuing support of existing TDM services while incorporating new IP and Ethernet applications. These packet applications are typically more efficient in bandwidth usage when deployed over an IP/MPLS network. All services converge at the access of the network, where the required packet handling, such as encapsulation and QoS capabilities, is executed. Different applications are transported through dedicated VPNs in a point-to-point, point-to-multipoint, or multipoint-to-multipoint manner.

High availability through IP/MPLS

High availability is essential to a public safety's communications network, which carries mission-critical voice, video and data information. With the Alcatel-Lucent IP/MPLS network, public safety agencies have the necessary reliability level to maintain uninterrupted operations. The MPLS FRR feature enables the network to reroute connections around a failure. Because the network is service aware, FRR can distinguish and prioritize traffic redirection according to priority. To protect the network against node or interconnection failures, end-to-end standby MPLS paths can also be provisioned.

The Alcatel-Lucent IP/MPLS implementation includes the unique additional high availability features of non-stop routing and non-stop services. The benefits are unparalleled availability and reliability:

- Non-stop routing ensures that a control card failure has no service impact. Label Distribution Protocol (LDP) adjacencies, sessions, and the database remain intact if there is a switchover.
- Non-stop service ensures that VPN services are not affected when there is a control fabric module switchover.

Other resiliency features such as pseudowire redundancy, multi-chassis link aggregation group (LAG), multi-chassis automatic protection switching (APS), and synchronization redundancy can also be implemented to maximize network resiliency.

Quality of service and traffic management

In a public safety communications environment where multiple services converge over a common infrastructure, QoS is essential. The Alcatel-Lucent IP/MPLS network can discriminate among various types of traffic, based on a rich set of classification attributes at Layer 1, Layer 2, Layer 2.5, or Layer 3, and prioritize transmission of higher priority traffic over lower priority. It utilizes extensive traffic management using an advanced scheduling mechanism to implement service hierarchies. These hierarchies provide maximum isolation and fairness across different traffic while optimizing uplink utilization. With multiple levels and instances of shaping, queuing and priority scheduling, the Alcatel-Lucent IP/MPLS network can manage traffic flows to ensure that performance parameters (such as bandwidth, delay and jitter) for each application are met.

Cybersecurity

Cybersecurity is paramount for public safety agencies to safeguard their critical infrastructures. The Alcatel-Lucent IP/MPLS network solutions have extensive integrated security features that help public safety agencies defend against cybersecurity threats, ensure communication and data privacy, and help deliver an 'always on' service.

The Alcatel-Lucent IP/MPLS products provide strong mechanisms to protect the management, control, and data planes to mitigate security threats. Access control lists (ACL) and traffic rate control and queuing can be used for all three planes to stop illegitimate senders and denial of service (DoS) attacks. Comprehensive user authentication, authorization, accounting (AAA), strong password security provided by SNMPv3 confidentiality, integrity features and Secure Shell (SSH) encryption, and exponential back-off is used to

stop illicit log-in and dictionary attack. HMAC-MD5 is used to authenticate control plane packets. 802.1x can help to prevent unauthorized device connection. Network address translation (NAT) is used to protect and hide private addressing space from external entities and encryption is used for data confidentiality and authentication. And, inherent to IP/MPLS, LSPs behave as virtual leased lines, effectively stopping remote attackers injecting traffic in the middle of a tunnel.

Network synchronization and timing

Accurate synchronization and microsecond timing is critical in communication networks to maintain network operational integrity. In most TDM networks, synchronization is distributed within the network using the SDH/SONET mechanisms built into the physical layer definition or by distributed global positioning system (GPS) clocks. To deliver the TDM service through a packet network, the same synchronization accuracy or better must be achieved.

To enable rapid and smooth migration of these networks as well as the future deployment of LTE, the Alcatel-Lucent IP/MPLS products support a wide range of synchronization and timing options to ensure that the network is properly synchronized and to allow for deployment of new timing technologies such as Synchronous Ethernet (SyncE) and IEEE 1588v2 Precision Timing Protocol (PTP). The following features are supported:

- External reference timing
- Line timing
- Adaptive clock recovery (ACR) timing
- Synchronous Ethernet
- IEEE 1588v2 PTP

The Alcatel-Lucent implementation of high performance timing for packet solutions are accomplished by a combination of built-in architectural features, efficiently tuned algorithms, and powerful QoS mechanisms to minimize the delay experienced by synchronization traffic.

Effective management for easier day-to-day operations

A key element of reliable and flexible IP/MPLS-based networks is a set of effective, simplified management tools that provide easy configuration and control of the network, effective problem isolation and resolution, and support of new management applications. The Alcatel-Lucent IP/MPLS network includes OAM tools that simplify the deployment and day-to-day operation of a public safety agency's communications network. For example, service, interface, and tunnel tests allow for rapid troubleshooting and enable proactive awareness of the state of traffic flows to help minimize service downtime.

The Alcatel-Lucent IP/MPLS network is fully managed by the industry-leading Alcatel-Lucent 5620 Service Aware Manager. The Alcatel-Lucent 5620 SAM is an integrated application that covers all aspects of element, network and service management on one platform. It automates and simplifies operations management on a converged IP/MPLS network, driving network operations to a new level of efficiency. It also provides

simplified diagnosis and intuitive visualization of the relationship between services, the MPLS infrastructure and the routing plane. It enables public safety agencies to overlay Layer 2 and Layer 3 services, MPLS tunnels, and various OAM traces on the control plane map. This application simplifies problem resolution, reduces control plane configuration errors, and reduces troubleshooting time.

CONCLUSION

Public safety agencies are transitioning their backhaul networks from TDM to IP for efficient support of mission-critical LMR/TETRA voice, video surveillance, and LTE mobile broadband. Public safety agencies should ensure that their converged communications network transformation includes an IP/MPLS network, as only IP/MPLS can provide the reliability that is needed for mission-critical services. The Alcatel-Lucent IP/MPLS communications network can help a public safety agency extend and enhance its network with new technologies like IP, MPLS, and Ethernet while fully supporting existing TDM applications. These new technologies will enable the public safety agency to optimize its network flexibility and management in order to reduce both CAPEX and OPEX without jeopardizing safety, security or reliability. A service-aware IP/MPLS network provides the benefit of supporting converged voice, data and video applications that can be managed through configurable QoS levels. The Alcatel-Lucent IP/MPLS product portfolio leads the industry in reliability and OAM tools, key enablers for meeting the “always-on” requirement for mission-critical public safety operations. The Alcatel-Lucent IP/MPLS network can help address public safey communications challenges with:

- High network availability
- Network virtualization
- QoS guaranteed for priority traffic
- Support for existing mission-critical TDM services and new IP and Ethernet applications
- Flexible synchronization options
- Reduced operating and maintenance costs
- Improved first responder safety through effective, always-on communications
- Readiness for LTE deployment
- Multiple security technologies

ACRONYMS

AAA	Authentication Authorization Accounting
ACL	Access Control List
ACR	adaptive clock recovery
APS	automatic protection switching
CAPEX	capital expenditure
CES	Circuit Emulation Service
CES IWF	Circuit Emulation Service interworking function
CESoPSN	Circuit Emulation Service over Packet Switched Network
CWDM	coarse wavelength division multiplexing
DWDM	dense wavelength division multiplexing
E&M	Ear and Mouth

ESS	Ethernet Service Switch
FR	frame relay
FRR	Fast Reroute
GPS	Global Positioning System
HMAC-MD5	Hash-based Message Authentication Code - Message Digest 5
IDS	Intrusion Detection System
IDU	indoor unit
IP	Internet Protocol
IPS	Intrusion Protection System
IP VPN	IP virtual private network
IT	information technology
LAG	link aggregation group
LDP	Label Distribution Protocol
LMR	Land Mobile Radio
LSP	label switched path
LTE	Long Term Evolution
MAC	Media Access Control
MPLS	Multiprotocol Label Switching
MPR	Microwave Packet Radio
NAT	Network Address Translation
OAM	operations, administration and maintenance
ODU	outdoor unit
OPEX	operating expense
PDH	Plesiochronous Digital Hierarchy
PMR	Professional Mobile Radio
PSS	Photonic Service Switch
PTP	Precision Timing Protocol
QoS	Quality of Service
SAM	Service Aware Manager
SAR	Service Aggregation Router
SAS	Service Access Switch
SAToP	Structure Agnostic TDM over Packet
SDH	Synchronous Digital Hierarchy
SLA	service level agreement
SONET	Synchronous Optical Network
SSH	Secure Shell
SyncE	Synchronous Ethernet
TDM	Time Division Multiplexing
TETRA	Terrestrial Truck Radio
VPLS	Virtual Private LAN Services virtual private network
VPN	virtual private network
VRF	virtual routing and forwarding
WAN	wide area network

Alcatel·Lucent