Reliable communications are fundamentally important for public-safety first responders, who must keep connected with each other and the control center as well as acquire situational awareness in real time when responding to emergencies. On the one hand, requirements for public safety communications networks are rapidly changing with the adoption of new broadband-based multimedia applications, IP-based Land Mobile Radio/Private Mobile Radio (LMR/PMR) and Long Term Evolution (LTE), as well as robotic technology such as unmanned aerial vehicle (UAV). On the other hand, the TDM-based backhaul networks in use are approaching end of life. As a result, public safety agencies are replacing their dedicated TDM-based backhaul networks with converged IP/MPLS WANs in preparation for such transitions. This paper discusses the advantages offered by this new converged backhaul network.
Public safety communications networks modernization

The Detroit police department in the U.S. first started to use Land Mobile Radio (LMR), also known as Private/Professional Mobile Radio (PMR), in 1928\(^1\). Since then, secure and reliable communications networks for backhaul of radio traffic have been critical for the operations of public safety agencies worldwide. Their responsiveness and effectiveness depend on the maintenance of emergency communications to share in real-time tactical field information with dispatch or command center, as well as access to applications such as a geographic information system (GIS) and unmanned aerial vehicle (UAV). With increasing security threats and demands for greater efficiency, better information sharing and cross-agency coordination, the modernization of public safety communications networks has become a top government priority.

Public safety backhaul challenges

This modernization efforts brings about a whole set of challenges, compelling public safety agencies to re-imagine their backhaul networks.

**LMR/PMR evolution**

Many public safety network operators are upgrading their current LMR/PMR systems to support a new generation of radio standards (P25 phase 2 and TETRA Plus, also known as TETRA Enhanced Data Service or simply TEDS) in order to take advantage of increased channel capacity and improved spectrum efficiency, as well as more efficient voice encoding. These IP-based radio system upgrades, together with new adoption bandwidth-intensive data applications, require packet-based backhaul networks to provide communication between radio sites, switching sites and the command center. The adoption of IP-based communications also makes establishing connectivity among agencies and jurisdictions easier, facilitating seamless collaborations. For example, connectivity between a city’s emergency center and a national disaster center can be established using inter-domain IP routing via a national IP backbone network. Furthermore, new IP-based peripherals such as scanners and video devices such as body-worn camera can now be used. New IP-based applications can also enable first responders to have quick access to critical information databases including video archives, a GIS and all-time protection under an automatic person location system (APLS).

---

\(^1\) T.A. Peters & L. Bell, eds., The Handheld Library: Mobile Technology and the Librarian (Santa Barbara: Libraries Unlimited, 2013) p. xi.
Despite the LMR upgrade to packet, many legacy TDM-based systems (for example, order wire communications between radio sites and cross-agency communications over UHF/VHF such as mutual aid communications in the U.S.) will remain in use in the foreseeable future. These established applications still require the use of TDM T1/E1 interfaces, as well as analog voice interfaces such as E&M and FSX/FSO. Therefore, the new packet-based backhaul network needs to do the following:

- Support legacy interfaces
- Carry the packetized traffic with the TDM-like quality of service (QoS)
- Distribute frequency synchronization end-to-end for legacy applications via line timing or other synchronization technologies such as IEEE 1588v2

**Adopting LTE for public safety mobile communications**

Today, there are two separate technology families for mobile communications:

- 2G, 3G and 4G LTE (abbreviated as LTE below) for commercial cellular networks that serve consumers and businesses
- Dedicated LMR, including P25 and TETRA, for public safety organizations

With the phenomenal market acceptance of next-generation LTE mobile services\(^2\), the public has been enjoying enhanced multimedia capabilities and instant access to a plethora of information on the Internet, enabled by high-bandwidth LTE data services and innovative personal devices and applications that are not available to LMR/PMR users. Recognizing that the real-time sharing of multimedia information and instant access to databases can greatly enable public safety agencies to more quickly respond and provide critical help, major public safety associations have endorsed\(^3\) or are looking to LTE as the successor technology of existing LMR/PMR systems. Consequently, many public safety organizations are now studying how to augment their existing system with LTE.

**3GPP LTE standards and spectrum allocation for public safety**

While LTE holds immense potential for public safety mobile broadband data communications, it will also have to fulfill requirements of some niche public safety applications, particularly critical voice communications\(^4\), before it can completely replace current LMR/PMR systems. Key features of critical voice communications include direct communications and group communications\(^5\).

---

\(^2\) According to GSA, there are 480 LTE networks launched in 157 countries as of Jan, 2016 (http://gsacom.com/paper/gsa-evolution-to-lte-report-january-25-2016-480-lte-networks-launched-in-157-countries/)

\(^3\) Both the Association of Public-Safety Communications (APCO) and the TETRA and Critical Communications Association (TCCA) have endorsed LTE as standard for emergency communications broadband network http://apcoalliance.org/4g.html; http://www.tetraday.com/news/tcca-signs-lte-agreement


The 3rd Generation Partnership Project (3GPP) telecommunications association, which has developed cellular radio network technology standards, including 3G and 4G LTE, has taken on the challenge. First, 3GPP Release 11 LTE\(^6\) extends the Use Equipment (UE) power class to include class 1 to improve the uplink for extended coverage performance for the North and South American region (also known as region 2). Subsequently 3GPP Release 12 LTE\(^7\) standardizes enhanced LTE to meet public safety application requirements; it includes the first step of proximity services that facilitate discovery and communications between nearby users over a radio connection and a group call system that enables one-to-many calling as well as dispatcher communications. 3GPP Release 13 LTE further incorporates mission-critical push-to-talk (MCPTT), E-UTRAN isolated operation to strengthen resiliency, as well as additional proximity services enhancements.\(^8\) Continuing the development momentum, 3GPP Release 14 LTE is targeting to complete work on mission-critical data and video services, as well as pursue new study items including proximity services for wearable devices.\(^9\)

Complementing the standardization works are worldwide efforts in allocating private LTE spectrum. In 2012, the United States spearheaded the efforts by passing a federal legislation to allocate band 14 in the 700 MHz spectrum, commonly known as LTE band 14, for public safety communications. The First Responder Network Authority (FirstNet\(^{10}\)) was subsequently formed “to provide emergency responders with the first high-speed, nationwide network dedicated to public safety”.\(^{10}\) Various state and local agencies, together with Nokia, have successfully conducted multiple trials, including New Jersey and Las Vegas. Besides, public safety agencies in South Korea and Qatar\(^{11}\) have also deployed their private LTE networks with the 700 MHz and 800 MHz spectrum correspondingly. Other potential candidates includes 400 MHz, 900 MHz and higher such as 1.4 GHz, 1.8 GHz and 2.1 GHz.

### 4G LTE E-UTRAN architecture

LTE, with an evolved UMTS Terrestrial Radio Network (UTRAN), briefly known as E-UTRAN (see Figure 1), introduces new requirements for public safety backhaul networks. E-UTRAN comprises of a set of eNBs connecting among themselves via X2 interfaces, to a Serving Gateway (SGW) via S1-U interfaces, and to a Mobility Management Entity (MME) via S1-MME interfaces. It is a flat any-to-any, all-IP network as described in 3GPP standard TS 36.300\(^{12}\), instead of a hub-and-spoke network found in LMR or older 2G and 3G technology. The eNB communicates not just with the centralized SGW and MME, but also

---

\(^6\) [3GPP Release 11 LTE](http://www.3gpp.org/specifications/releases/69-release-11)

\(^7\) [3GPP Release 12 LTE](http://www.3gpp.org/specifications/releases/68-release-12)

\(^8\) [3GPP Release 13 LTE](http://www.3gpp.org/release-13)

\(^9\) [3GPP Release 14 LTE](http://www.3gpp.org/release-14)

\(^10\) [National Telecommunications and Information Administration, FirstNet](http://www.ntia.doc.gov/category/firstnet)


\(^12\) [http://www.3gpp.org/DynaReport/36300.htm](http://www.3gpp.org/DynaReport/36300.htm)
dynamically with neighboring eNBs as LTE user equipment roams. The direct inter-eNB communications enables more efficient handover during roaming 3GPP Release 13 LTE and better subscriber load management. To support E-UTRAN load-balancing 3GPP Release 12 LTE and high availability, LTE’s S1-flex function allows for eNBs to connect with multiple SGWs and MMEs.

With the immense degree of connectivity required among all E-UTRAN components, it is crucial to have a flexible backhaul network that is highly resilient and can enable operators to flexibly deploy MPLS-based and Carrier Ethernet-based any-to-any services with the precision of traffic engineering in a scalable manner. The use of the X2 interface, which requires minimum latency, calls for routing capability at the edge. Furthermore, with the future introduction of eMBMS-based mission-critical services, multicast capability and delivery of precise time and phase synchronization in the network are also pivotal.

Figure 1. LTE E-UTRAN network

Network infrastructure sharing

As government are under sustained pressure to improve effectiveness and efficiency, it is imperative to maximize return on any infrastructure investment. Therefore, the proposition of network infrastructure sharing has become very attractive. While the degree and method of infrastructure sharing will vary in different countries depending on local regulatory frameworks, it is generally a paradigm that the backhaul network can also be used to serve other government departments, public communities and public utilities in order to improve network use. This model can yield tremendous savings for all participating parties.
To support infrastructure sharing, the new public safety network must be a highly robust multiservice network with an architecture that is poised to grow and expand. It needs to be able to scale in size and grow in capacity, fully utilizing available transmission assets, including microwave spectrum, optical fiber, and even leased lines if necessary. It also needs to support a flexible range of point-to-point and multipoint virtual private networks (VPNs) for TDM, Ethernet and IP services to meet the need for different organizations’ applications. At the same time the network must maintain complete virtualization in the control plane and data plane among all the VPNs to ensure security, and service-aware traffic management to maintain agreed quality of service (QoS) for all user groups, particularly first responders, since it is crucial that the quality level not be compromised at any time.

Deploying backhaul networks for LTE and beyond

To tackle the trends and associated requirements discussed above, many public safety agencies have already adopted a converged IP/MPLS backhaul network. A network blueprint is shown in Fig. 2. This converged network offers the following advantages:

- Readiness to scale and expand
- Versatile and efficient use of transmission media and topologies
- Advanced traffic management and QoS
- Strong network resiliency and rapid recovery
- Graceful legacy TDM migration
- Multiservice backhaul for infrastructure sharing
- Rigorous security protection
- Precise synchronization distribution
- Efficient end-to-end network management
- Future communications readiness
**Scalable network size and capacity**

The backhaul network must scale seamlessly to support increasing numbers of locations and devices at higher capacities. The network platform needs to accommodate different interface speed and capacity requirements depending on their locations in the network. It should also render installation versatility for small enclosures and full outdoor environments if required. In addition, to reduce OPEX and training requirements, all nodes should be based on the same operating system and be managed by a unified network manager and command line interface.

**Versatile and efficient use of transmission media and topologies**

Because backhaul network coverage spans dense urban areas to remote terrain, operators must be resourceful in using the means of transmission, such as microwave, fiber, copper and even third-party leased lines if necessary. The backhaul equipment must therefore support transmission layer integration (see Figure 3) to consolidate and simplify network design and operations, and ensure consistent commissioning and operations procedures for all network sites, regardless of the medium.

**Figure 2. A converged IP/MPLS backhaul network blueprint**

**Figure 3. Transmission Integration in an IP/MPLS router**
The most common transmission medium is packet microwave complemented by optical fiber when available. For microwave, depending on geographic practice and site setting, either outdoor or indoor microwave radios can be deployed. The following microwave capabilities are key to fully utilize the spectrum acquired:

- **Service-driven adaptive modulation**: This feature optimizes overall microwave channel throughput, even in adverse weather conditions. Critical traffic is always transmitted with priority using advanced QoS prioritization and scheduling techniques if modulation levels need to drop to deliver capacity during severe weather.

- **Cross-polar interference cancelation (XPIC)**: This capability doubles the capacity of a single frequency by using both horizontal and vertical electromagnetic polarizations. This increases capacity while also saving spectrum and antenna costs.

- **Higher order quadrature amplitude modulation (H-QAM)**: Higher QAM levels up to 2048 QAM increase the number of transported symbols per hertz to help squeeze more bandwidth out of scarce microwave spectrum.

- **Multi-channel link scaling**: When a high-capacity link is required, multiple radio channels need to bond together into a bigger link, particularly between large aggregation sites.

- **MPLS-aware packet throughput booster**: Uses advanced packet compression to reduce Ethernet and IPv4/IPv6 protocol header, increasing radio link throughput over the air interface by as much as 300 percent. With the associated MPLS label awareness, the compression is the perfect companion to the MPLS network.

When fiber is available, the operators should be able to utilize it fully by using wavelength division multiplexing (WDM) technology. Coarse WDM (CWDM), with its compelling economics, can allow up to eight 1 Gb/s and/or 10 Gb/s wavelengths to be carried in the same strand of fiber.

Operators should also be able to mix and match transmission media seamlessly when building a network. For example, in Figure 4, a microwave link is deployed to complete a fiber ring for enhanced network resiliency.

*Figure 4. Hybrid ring topology*
**Strong Backhaul QoS**

Supporting mission-critical services such as mission-critical push-to-talk (MCPTT) and mission-critical data services is pivotal to support first responder field activities. Such services have high performance requirements resulting in stringent delay budget. For example, MCPTT access time needs to come under 300 ms for 95% of the time\(^{13}\). Mission-critical data service controlling unmanned aerial vehicle, or drone, has an end-to-end delay budget of only 50 ms\(^{14}\).

Therefore a strong backhaul network QoS undergirded by advanced traffic management capabilities is essential. The backhaul network must incorporate extensive traffic management mechanisms such as advanced hierarchical rate scheduling and custom per interface QoS policy. Through proper network design and the use of multiple levels and instances of hardware-based shaping, queuing and priority scheduling, the network can manage traffic flows to ensure high priority transmission of critical traffic and equitable network bandwidth consumption by non-critical traffic according as required.

Even with advanced traffic scheduling, it is sometimes unavoidable for a high-priority packet to wait for its turn when a jumbo best-effort packet has started transmission. This phenomenon is commonly known as head-of-line blocking, which causes high jitter. While its impact on jitter is negligible on optical Ethernet as the transmission bit rate is in the order of 1 Gb/s or higher, it becomes significant for lower speed links like microwave whose bandwidth is in the order of hundreds of bits per second or lower. Packet fragmentation and interleave, a technique that fragments all packets before queuing and scheduling, can bring down the time high-priority packets have to wait to the value of one segment of transmission, thus minimizing jitter, which is key to the high quality of real-time applications and packet synchronization technology such as IEEE 1588v2.

The essence of the technique is described below (see Figure 5):

1. As long, low-priority frames arrive, they are fragmented into multiple shorter fragments, and subsequently placed in the appropriate lower priority queue.
2. If there are no higher priority frames, the first low-priority fragment starts the transmission process.
3. If a subsequent high-priority frame arrives, it is placed in a high-priority queue to wait for transmission. If the frame length is shorter than that of a fragment, no fragmentation is required for these higher priority frames.
4. When the transmission of the first low-priority fragment has finished, the transmitter serves the high-priority frames, interleaving with the previously sent low-priority fragments.
5. After the high-priority frames are served, the transmitter switches back to service the low-priority frame fragments.

\(^{13}\) For a more detailed discussion, please refer to 3GPP TS 22.179 Mission Critical Push To Talk (MCPTT) over LTE (http://www.3gpp.org/ftp/specs/archive/22_series/22.179/)

\(^{14}\) For a more detailed discussion, please refer to 3GPP TS22.289 Mission Critical Data services over LTE (http://www.3gpp.org/ftp/specs/archive/22_series/22.282/)
**Strong network resiliency and rapid recovery**

Strong resiliency is essential for a public safety communications network, which carries mission-critical voice, video and data information. The network should have high reliability levels for uninterrupted operations. Platform protection is a key step in achieving that. Deploying a fully redundant platform that supports hitless control/fabric protection is a significant improvement from adopting a two-node architecture, which effectively doubles the size of the network. Complementary to platform redundancy are the high-availability features of Non-Stop Routing (NSR) and Non-Stop Services (NSS). The benefits of NSR and NSS are unparalleled availability and reliability, which are essential for aggregation sites. NSR ensures that a control card failure has no service impact. MPLS signaling adjacencies and sessions, as well as the Label Information Base, remain intact if there is a switchover. NSR also ensures that VPN services are not affected in a control-fabric module switchover.

Fast switching is one key pillar of rapid recovery. MPLS Fast Reroute (FRR) enables the network to consistently reroute connections around a failure at SDH/SONET speeds, regardless of the underlying network topology and size. FRR can distinguish and provide protection to applications depending on the MPLS tunnel priority. To protect the network against node or interconnection failures, end-to-end standby MPLS paths can also be provisioned. When Ethernet ring is deployed, the Ethernet Ring Protection (ERP) G.8032 technique is also an available option.

---

The other key pillar of rapid recovery is fast fault detection. In a common scenario of deploying microwave between backhaul equipment, the microwave link degradation condition (for example, high bit error rate condition or loss of signal) cannot be communicated quickly to backhaul equipment. The use of fault propagation mechanism backhaul equipment and the integrated microwave radio system for fast fault detection can reduce fault detection time from hundreds of milliseconds to very low tens of milliseconds. These two pillars are pivotal to enable network recovery with minimum application performance impact.

Other resiliency features, such as pseudowire redundancy for geodiversity protection,\textsuperscript{16} Multi-chassis Link Aggregation Group (MC-LAG) and automatic protection switching (APS) for core equipment nodal protection can also be deployed individually or together to further enhance end-to-end network resiliency.

For microwave links, 1+1 protection with hitless radio protection switching, space diversity and N+0 radio LAG are techniques that can render different levels of protection.

The network should also support advanced resilient topologies—such as multi-ring (also known as ladder), necklace and hybrid—to improve network robustness (see Figure 5). Particularly, the multi-ring’s rich path diversity, when fully capitalized by dynamic IP/MPLS, can provide the utmost redundancy protection even in multi-fault scenarios during a disaster.

Effective infrastructure sharing

Infrastructure sharing involves carrying traffic from other user groups in segregated VPNs and allow them to operate with a certain scope of autonomy.

The multiservice capability of an IP/MPLS network is ideal to carry traffic from different user groups. Its full range of MPLS-based VPN services has been deployed in many mission-critical and commercial networks in large scale under the most trying environments with no compromise (see Figure 7), regardless of whether the service type is TDM, Ethernet or IP.

Figure 7. Multiservice backhaul

1. Pseudowire (PWE3) Point-to-point connections
2. Virtual Private LAN services (VPLS) Layer 2 bridged multipoint Ethernet service
3. Layer 3 IP VPN RFC 4364 routed multipoint service
Some user groups may require a highly autonomous control of their VPNs. For example, they need to create new, modify or delete existing VPNs rapidly as operations evolve. An innovative network paradigm called network slicing is well-suited to accommodate this requirement. It segments the network assets (e.g. ports) into slices for different user groups. The user group could be given full administrative privilege to operate the network slice, without the concern of affecting other user groups, particularly critical radio applications (Fig. 8).

Figure 8. Network slicing provides highly autonomous infrastructure sharing capability

Graceful legacy TDM migration

From older generation of LMR/PMR system to UHF/VHF emergency communications (e.g. mutual aid communications used in the U.S.), legacy interface including E&M and T1/E1 are still commonly used. In public utilities, SCADA systems using serial V.24/RS-232 and operational voice systems with FSX/FSO systems are still prevalent. Up to now, they are typically carried over a TDM network. As TDM equipment and services are reaching end of life, there is a pressing need to migrate the traffic to the new backhaul network. Consequently the backhaul network also needs to support a wide portfolio of legacy interfaces. Complemented by the strong resiliency and deterministic network performance, such applications can be migrated gracefully.

17 For a detailed discussion on TDM migration, please read the paper “Migrating from SDH/SONET networks to IP/MPLS networks” (http://resources.alcatel-lucent.com/asset/145072)
Rigorous security protection\(^{18}\)

Cybersecurity is paramount for public safety agencies to safeguard their critical infrastructures. The network should have extensive integrated security features to defend against cybersecurity threats, ensure communications and data privacy, and deliver uninterrupted services. Strong mechanisms should protect the management, control and data planes against security threats from outside or inside the agency.

Access Control Lists (ACLs), network address translation (NAT) and stateful firewall can be used to thwart illegitimate senders and denial of service (DoS) attacks. Comprehensive user Authentication, Authorization and Accounting (AAA), strong password security provided by Simple Network Management Protocol version 3 (SNMPv3) confidentiality, integrity features, Secure Shell (SSH) encryption, and exponential backoff are used to stop illicit logins and dictionary attacks on the network. Hash-Based Message Authentication Code—Message Digest 5 (HMAC-MD5) is used to authenticate control plane packets.

Inherent to IP/MPLS, Label Switched Paths (LSPs) behave as Virtual Leased Lines (VLLs), effectively stopping remote attackers from malignly injecting traffic in the middle of a tunnel. Complemented by encryption at MPLS layer with innovative technology Network Group Encryption (NGE), confidentiality and authentication of packet and TDM data are safeguarded while traversing the network.\(^{19}\)

Precise synchronization distribution

Precise frequency and time-of-day/phase synchronization is critical for maintaining operations and applications integrity in communications networks. In most TDM networks, synchronization is distributed within the network using SDH/SONET mechanisms built into the physical layer to distribute a reference clock, such as one obtained from a global positioning system (GPS) in a central location. To deliver TDM services over the new backhaul network, similar synchronization accuracy must be achieved.

To enable rapid and smooth migration as well as future LTE deployment, public-safety communications networks must support a wide range of synchronization technology options, including:

- External reference timing
- Line timing (from SDH/SONET, T1/E1)
- Adaptive clock recovery and differential clock recovery timing
- Synchronous Ethernet

\(^{18}\) For a detailed discussion on security, please read the paper “Impregnable network defense for mission-critical networks” (http://resources.alcatel-lucent.com/asset/194791)

\(^{19}\) Network Group Encryption (NGE), a standard-based innovative security solution, seamlessly protect multi-service MPLS traffic. For more information, please read the paper “Seamless encryption for mission-critical networks” (http://resources.alcatel-lucent.com/asset/187584)
• IEEE 1588v2-2008\textsuperscript{20} (also known as IEEE 1588v2) Precision Timing Protocol (PTP) (master, boundary clock, transparent clock and slave)

• Integrated GPS receiver

Synchronization requirements can sometimes be met by installing a local GPS—with an external receiver or an integrated receiver in the network node—at each site. However, because of growing concerns about the vulnerability of GPS to accidental or intentional interference, network-wide time-of-day synchronization distribution with IEEE 1588v2 as a backup source is becoming crucial.

**Unified end-to-end network management**

A backhaul network with unified end-to-end management by a network manager managing all MPLS services and the underlying optical and microwave transport domains can minimize operations complexity and staff technical training (Fig. 9). This cross-domain management capability maximizes management synergy by extending manage

Figure 9. Unified network and services management platform

Advanced management tools can greatly simplify network configuration and control, allow for effective problem isolation and resolution, and support new management applications. Operations, administration and maintenance (OAM) tools simplify the deployment and day-to-day operations of a public safety backhaul network. For example, connectivity tests at different layer enable rapid troubleshooting and proactive awareness of the state of traffic flows to help minimize service down time. Periodic OAM tests enable the continuous monitoring of packet loss, network delay and jitter conditions to facilitate preventive maintenance.

Network capability extensibility

It is essential the backhaul network architecture is extensible to support new and future applications. MPLS-based VPN services capability can continue to expand to support IP multicast and IP version 6 (IPv6). The network blueprint also facilitate the future adoption of software defined networking (SDN) and network functions virtualization (NFV) to fully capitalize on the advantages of cloud computing.

Nokia public safety IP/MPLS network solution

With the Nokia public safety IP/MPLS network solution, public safety agencies gain an IP/MPLS network that has all the architecture attributes described above. Solution highlights are:

- Scalable and flexible VPN services for TDM, Ethernet and IP
- Installation flexibility, which includes DIN mounting in small enclosures and outdoor mounting on a wall, pole or stand without cabinet
- Integration with versatile packet microwave
- Built-in CWDM networking
- Graceful transmission medium migration from microwave and optics
- Synchronization based on Bell Labs technology
- End-to-end multi-domain IP management, including MPLS, microwave, and optics

Solution components

The Nokia 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:

- Nokia 7750 Service Router (SR)
- Nokia 7705 Service Aggregation Routers (SAR)
- Nokia 7450 Ethernet Service Switch (ESS)
- Nokia 7210 Service Access Switch (SAS)
- Nokia 9500 Microwave Packet Radio (MPR), providing a packet microwave link to connect MPLS nodes
- Nokia 1830 Photonic Service Switch (PSS), the optical layer underlying the IP/MPLS network
- Nokia Network Services Platform for overall network services management
Blueprint backhaul network architecture

The Nokia IP/MPLS network solution helps public safety agencies to deploy converged networks for all applications while preserving QoS and reliability. This mission-critical design is ideal for public safety because it is capable of coping with LMR traffic now and scaling up for LTE traffic in the future. With strong solution components, network operators can design a network with a flexible architecture according to their unique set of requirements.

Figure 10 shows a blueprint of an Nokia converged IP/MPLS communications network with microwave and optical integration for public safety. Packet microwave and optical assets are deployed to optimize connectivity and bandwidth. Pseudowires, VPLS and IP VPNs provide network virtualization for different applications.

Figure 10. Nokia public safety mission-critical backhaul solution
**Integrated IP/MPLS and microwave domains**

In a traditional architecture, IP/MPLS is overlaid over microwave transmission across two platforms. In the Nokia IP/MPLS network solution, the 9500 MPR is fully integrated with the 7705 SAR as a single, seamless, managed platform that converges the IP and microwave domains (see Figure 11).

Integration provides many benefits when microwave media are widely deployed:

- Elimination of multiple network managers
- Convergence of multiple indoor units (IDUs) and IP/MPLS router into one platform
- Rapid detection of microwave link degradation, including high bit error rate condition
- Reduced equipment space, sparing requirements, power consumption and cooling needs
- Streamlined installation and operations management
- Flexible microwave configurations with split-mount and all-indoor radios
- Redundant microwave link with 1+1, N+0 and space diversity

**Figure 11. Integrated 7705 SAR and 9500 MPR configuration**

- Two platforms (for IP and microwave domains)
- Two network managers
- Multi-chassis
  - One IDU or each microwave direction typically

Integrating microwave into 7705 SAR makes life easy

- One platform replaces all chassis
- One network manager for both domains

A daunting task for deployment and operation
Conclusion

Public safety agencies today are at a critical juncture. They are facing unprecedented challenge to protect the society and its citizens. With increasing levels of crime, terrorism, and natural disasters, they need to adopt new technologies to provide an agile, effective response swiftly and safely. A converged IP/MPLS backhaul network provides the foundational connectivity for dispatch, situational awareness and communications among first responders themselves and command center. It also has the potential to provide connectivity to other non-critical government agencies, expanding the network use and attaining high economic efficiency. As public safety agencies continue to strive to safeguard the public, the backhaul network will remain pivotal to accomplish their missions.

Acronyms

3GPP 3rd Generation Partnership Project
2G, 3G, 4G Second Generation, Third Generation, Fourth Generation
AAA Authentication, Authorization and Accounting
ACL Access Control List
AES Advanced Encryption Standard
APCO Association of Public-Safety Communications
APLS automatic person location system
CAPEX capital expenditures
CES Circuit Emulation Service
CESoPSN Circuit Emulation Service over Packet Switched Network
CLI command-line interface
CWDM Coarse Wavelength Division Multiplexing
DoS denial of service
EMS emergency medical services
eNB Evolved Node B
e-UTRAN Evolved UMTS Terrestrial Radio Access Network
EPC Evolved Packet Core
FirstNet™ First Responder Network Authority
FR Frame Relay
FRR Fast Reroute
GIS Geographic Information System
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GPS</td>
<td>Global Positioning System</td>
</tr>
<tr>
<td>H-QAM</td>
<td>Higher order quadrature amplitude modulation</td>
</tr>
<tr>
<td>HMAC-MD5</td>
<td>Hash-Based Message Authentication Code - Message Digest 5</td>
</tr>
<tr>
<td>HSS</td>
<td>Home Subscriber Server</td>
</tr>
<tr>
<td>IDU</td>
<td>indoor unit</td>
</tr>
<tr>
<td>IP VPN</td>
<td>IP virtual private network</td>
</tr>
<tr>
<td>IT</td>
<td>information technology</td>
</tr>
<tr>
<td>IWF</td>
<td>InterWorking Function</td>
</tr>
<tr>
<td>LAG</td>
<td>Link Aggregation Group</td>
</tr>
<tr>
<td>LMR</td>
<td>Land Mobile Radio</td>
</tr>
<tr>
<td>LSP</td>
<td>Label Switched Path</td>
</tr>
<tr>
<td>LTE</td>
<td>Long Term Evolution</td>
</tr>
<tr>
<td>MAC</td>
<td>Media Access Control</td>
</tr>
<tr>
<td>MC-LAG</td>
<td>Multi-chassis Link Aggregation Group</td>
</tr>
<tr>
<td>MCPTT</td>
<td>Mission Critical Push-to-talk</td>
</tr>
<tr>
<td>MME</td>
<td>Mobile Management Entity</td>
</tr>
<tr>
<td>MPLS</td>
<td>Multiprotocol Label Switching</td>
</tr>
<tr>
<td>NAT</td>
<td>Network Address Translation</td>
</tr>
<tr>
<td>NPSTC</td>
<td>National Public Safety Telecommunications Council</td>
</tr>
<tr>
<td>NSR</td>
<td>Non-Stop Routing</td>
</tr>
<tr>
<td>NSS</td>
<td>Non-Stop Services</td>
</tr>
<tr>
<td>OAM</td>
<td>operations, administration and maintenance</td>
</tr>
<tr>
<td>OPEX</td>
<td>operating expenditures</td>
</tr>
<tr>
<td>P25</td>
<td>Project 25</td>
</tr>
<tr>
<td>PCRF</td>
<td>Policy and Charging Rules Function</td>
</tr>
<tr>
<td>PDH</td>
<td>Plesiochronous Digital Hierarchy</td>
</tr>
<tr>
<td>PDN</td>
<td>packet data network</td>
</tr>
<tr>
<td>PE</td>
<td>provider edge</td>
</tr>
<tr>
<td>PGW</td>
<td>PDN Gateway</td>
</tr>
<tr>
<td>PMR</td>
<td>Private/Professional Mobile Radio</td>
</tr>
<tr>
<td>PTP</td>
<td>Precision Timing Protocol</td>
</tr>
<tr>
<td>PWE3</td>
<td>Pseudowire Emulation Edge-to-Edge</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>QoS</td>
<td>Quality of Service</td>
</tr>
<tr>
<td>RAN</td>
<td>Radio Access Network</td>
</tr>
<tr>
<td>SAToP</td>
<td>Structure-Agnostic TDM over Packet</td>
</tr>
<tr>
<td>SDH</td>
<td>Synchronous Digital Hierarchy</td>
</tr>
<tr>
<td>SGW</td>
<td>Serving Gateway</td>
</tr>
<tr>
<td>SNMPv3</td>
<td>Simple Network Management Protocol version 3</td>
</tr>
<tr>
<td>SONET</td>
<td>Synchronous Optical Network</td>
</tr>
<tr>
<td>SSH</td>
<td>Secure Shell</td>
</tr>
<tr>
<td>TCCA</td>
<td>TETRA and Critical Communications Association</td>
</tr>
<tr>
<td>TDM</td>
<td>Time Division Multiplexing</td>
</tr>
<tr>
<td>TEDS</td>
<td>TETRA Enhanced Data Services</td>
</tr>
<tr>
<td>TETRA</td>
<td>Terrestrial Trunked Radio</td>
</tr>
<tr>
<td>UTRAN</td>
<td>UMTS Terrestrial Radio Network</td>
</tr>
<tr>
<td>VLL</td>
<td>Virtual Leased Line</td>
</tr>
<tr>
<td>VPLS</td>
<td>Virtual Private LAN Service</td>
</tr>
<tr>
<td>VPN</td>
<td>virtual private network</td>
</tr>
<tr>
<td>VPRN</td>
<td>Virtual Private Routed Network</td>
</tr>
<tr>
<td>XPIC</td>
<td>Cross-polar interference cancellation</td>
</tr>
</tbody>
</table>

References

2. 3GPP Release 12 LTE. [http://www.3gpp.org/specifications/releases/68-release-12](http://www.3gpp.org/specifications/releases/68-release-12)
3. 3GPP Release 13 LTE. [http://www.3gpp.org/release-13](http://www.3gpp.org/release-13)
4. 3GPP Release 14 LTE. [http://www.3gpp.org/release-14](http://www.3gpp.org/release-14)


