



Providing highly dependable 9-1-1 emergency response services

With an ESN® of utmost resiliency

Application note

Abstract

9-1-1 is a lifeline to citizens who need emergency assistance. Migration to next generation 9-1-1 (NG9-1-1) improves emergency response and heightens citizen safety — but dependable NG9-1-1 mandates Emergency Services IP networks (ESInets) with utmost resiliency. This application note explains how to harness the resiliency and robustness of MPLS technology to build an IP/MPLS-based ESInet with the utmost reliability, one that can still deliver emergency communications services even during extreme events.

Contents

Abstract	2
The advent of NG9-1-1	4
ESInet architecture overview	4
Building an ESInet with the utmost resiliency	5
PSAP access router redundancy protection	6
ESInet communications path redundancy protection	7
Host site georedundancy protection	9
Protection from adverse environmental conditions	9
Conclusion	10
Abbreviations	10

The advent of NG9-1-1

The first emergency 9-1-1 service went live in 1968 in Haleyville, Alabama, heralding a dependable way for citizens to dial for emergency rescue services. Society has since relied on this service to ensure public safety every day. With the introduction of automatic number identification (ANI) and automatic location information (ALI) technologies as well as the adoption of wireless communications service and voice over Internet Protocol (VoIP), the original 9-1-1 service has subsequently undergone different phases of evolution to enhanced 9-1-1 (E9-1-1), wireless E9-1-1 and VoIP E9-1-1.

The 21st century has seen the rise of the internet and new communications technologies, including real-time texting, instant messaging, picture sharing and social media feeds, which are fully embraced by the public. In addition, innovative digital technologies such as unmanned aerial vehicles (UAVs), wearable devices (e.g., smart watches and fitness trackers) and CCTV have become so prevalent that they can be harnessed to widen situational awareness. As a result of these innovations, it's imperative that telecommunicators working in public safety answering points (PSAPs, also called emergency communications centers), have the capabilities to seamlessly accept new digital information from any networked device, process and analyze the multimedia data, and transfer the information to first responders as well as other PSAPs and public safety agencies.

Accordingly, PSAPs need to upgrade to support next generation 9-1-1 (NG9-1-1) while maintaining interoperability with legacy systems. NG9-1-1 employs new IP-based digital systems for call processing and call dispatch; therefore, the network that connects NG9-1-1 PSAPs and NG9-1-1 core services (NGCS) systems and applications is an IP network commonly known as an Emergency Services IP network (ESInet).

IP technology was initially designed to offer non-critical, best-effort services that have no reliability requirements — and this is not acceptable for an ESInet. As a result, there have been a lot of efforts in the National Emergency Number Association (NENA) to formulate a set of ESInet design considerations¹ that ensure reliable transport of emergency communications services traffic, particularly during major incidents or severe weather events. Based on those design considerations, this application note explains how to harness the resiliency and robustness of MPLS technology to build an IP/MPLS-based ESInet with the utmost reliability, one that can still deliver emergency communications services even when multiple network faults occur.

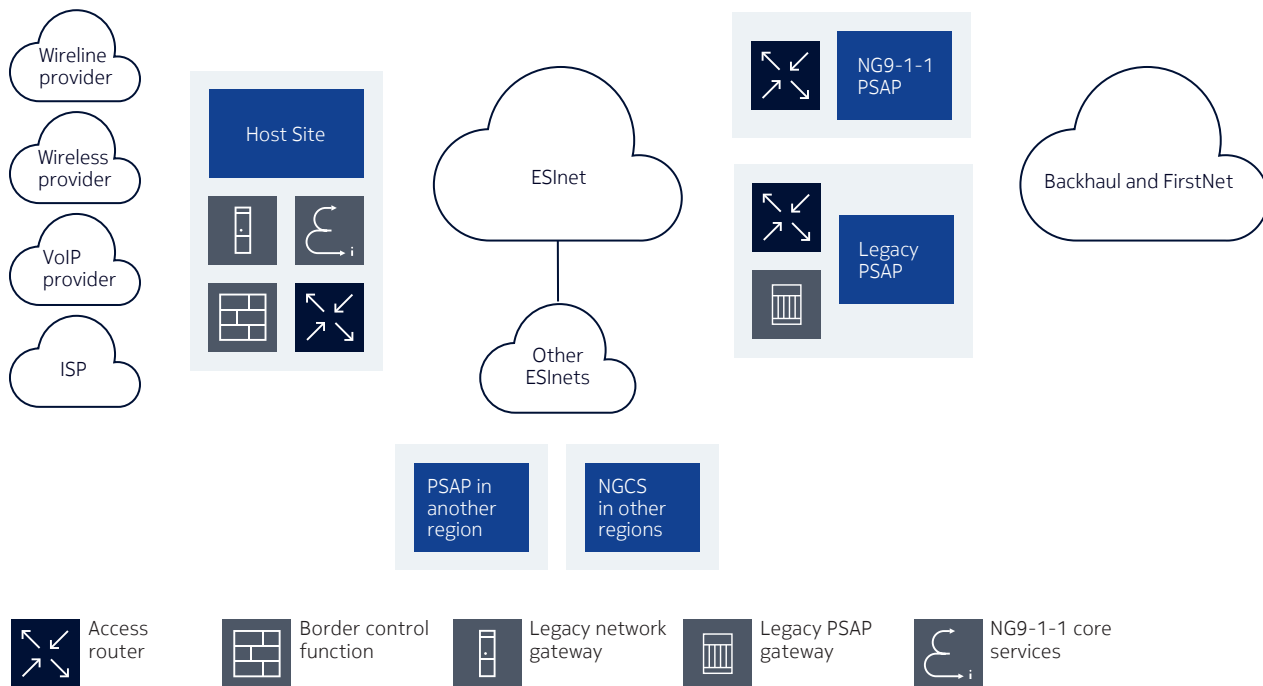
ESInet architecture overview

ESInet is the underpinning of the NENA i3 architecture. In essence, it is a private IP transport network shared by all public-safety agencies responding to an emergency. It connects PSAPs, NGCS systems and other applications such as CAD. ESInet also interconnects with communications service providers — wireline, wireless, VoIP and internet service providers (ISPs) — to receive 9-1-1 calls. And ESInet interconnects with public safety networks such as FirstNet that dispatch and support first responders.

Figure 1 shows an ESInet architecture blueprint where NGCS systems are centrally installed in host sites that serve all PSAPs in a region.

¹ The ESInet design document is available [here](#).

Figure 1. An ESInet architecture blueprint



With ESInets, unlike the legacy 9-1-1 systems, PSAPs in different domains are no longer segregated². As a result of the dynamic IP routing capability, ESInets can be interconnected to establish PSAP-to-PSAP connectivity. Firewall and routing policies can be deployed at the border to ensure network security. Together with the use of a common signaling protocol, Session Initiation Protocol (SIP), PSAPs in different domains can seamlessly communicate with each other when necessary. By interconnecting ESInets, telecommunications can transfer misrouted 9-1-1 calls or access specific resources to provide a more effective response if needed.

Building an ESInet with the utmost resiliency

Faults happen in any network. However, when an ESInet experiences network faults and cannot recover, PSAPs become unreachable and emergency communications services stop, potentially resulting in loss of property or even loss of life. To avoid this situation, strong ESInet resiliency is of utmost importance to withstand not only the impact of regular network faults but also multiple faults resulting from disaster situations such as severe weather events. The following three capabilities are key:

- Early network fault detection
- Rapid failover switching (hitless or at the speed of SONET technology)
- Multi-fault resiliency

² In the traditional E9-1-1 architecture, PSAPs in different domains are connected to different selective routers (a traditional telephone switch or a softswitch). Routing 9-1-1 calls to a PSAP in another domain is not possible.

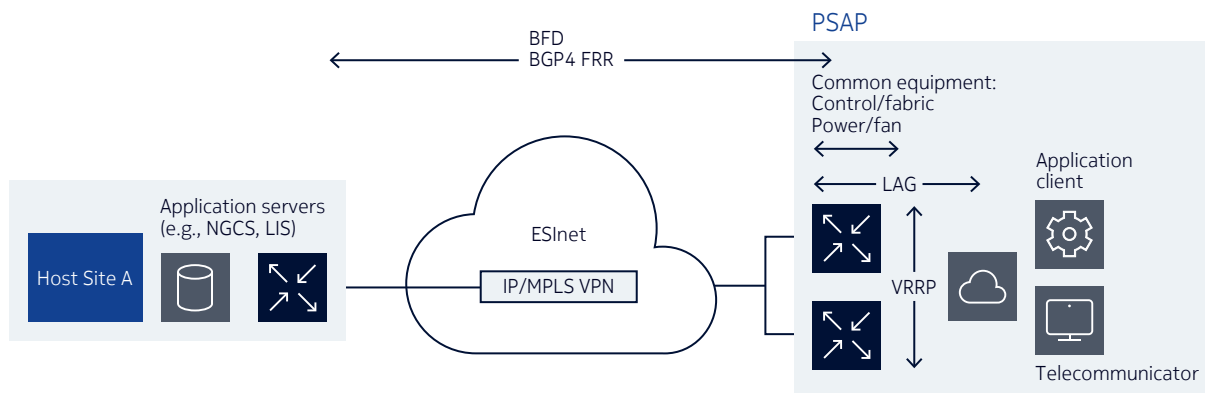
Today, IP networks built to carry mission-critical applications (public-safety LMR backhaul, high-voltage power grid protection and railway signaling) are very often deployed with MPLS. The rest of this application note discusses how to attain utmost resiliency by harnessing the following protection schemes available on an IP/MPLS platform:

- PSAP IP/MPLS access router redundancy protection
- ESI-net communication path redundancy protection
- Host site georedundancy protection
- Protection from adverse environmental conditions

PSAP access router redundancy protection

An IP/MPLS access router (abbreviated as “access router” hereafter) is the gateway for all communications by the application clients in the PSAPs. Therefore, full redundancy protection is paramount (see Figure 2).

Figure 2. Full access router redundancy protection



There are two types of access router protection: common equipment protection and nodal redundancy protection.

Common equipment protection

The access router needs hot redundancy protection for common equipment, including control card, switching fabric, power and fan. When the router switches to the backup component, emergency services communications should not be interrupted.

While the new generation of routers can accomplish hitless protection switching for fabric, power and fan, IP routing and MPLS signaling protocols (generally known as control protocols) need to reset. This brings down IP/MPLS VPN services, disrupting emergency communications services because PSAPs are no longer reachable until the network fully reconverges³, which can take up to several minutes.

An attempt to alleviate the impact was made with graceful restart (GR) mechanism to control protocols. When there is a control card switchover in an access router, its immediate neighbors do not report to other neighbors but wait a certain amount of time (called the grace period) for the access router to come back online.

However, if the access router completely fails instead of a simple control card fault, the grace period only further slows down the network reconvergence. Furthermore, if there is a second network failure

³ Reconvergence is when all routers in the network are notified that the latest topology changes have updated their forwarding tables.

(e.g., a broken link) somewhere else in the ESInet during the grace period, the graceful restart process on that access router terminates immediately and starts the reconvergence process by resetting the routing and MPLS signaling processes. This further lengthens the reconvergence time — and impacts emergency communications services. Therefore, graceful restart technology cannot render ESInet multi-fault resiliency.

The advent of nonstop routing and signaling technology on router control cards ushers in the concept of hitless switchover and eliminates any impact on emergency communications services even during a multi-fault scenario. Nonstop routing and signaling always keeps the active and standby control cards synchronous in the protocol processes.

When a switchover occurs, the standby card can immediately take over the control sessions without the immediate neighbors even noticing. Therefore, there is no impact on emergency communications services. A network change or fault somewhere else also will not affect the communications, thereby attaining the goal of multi-fault resiliency.

Nodal redundancy protection

Despite the protection discussed in the preceding section, there is still a scenario in which the router could fail completely due to some major site incident. To eliminate this single point of failure, access routers can be deployed in active/standby pairs running the Virtual Router Redundancy Protocol (VRRP) to attain nodal redundancy protection⁴. When the standby router detects failure of the active router, it takes over communications with the application clients and telecommunicators without disruption. Running the lightweight Bidirectional Forwarding Detection (BFD) Protocol can enable detection in tens of milliseconds.

However, when the nodal switchover occurs in the PSAP, other access routers, e.g. those in the host site, need to wait until routing reconvergence in the ESInet is completed, which can take up to several minutes before they can successfully send traffic to the backup access router in the PSAP. This brings down emergency communications. With the advent of MPLS fast-reroute technology merged with BGP4, other access routers no longer need to wait for reconvergence. Combining the use of BFD and BGP-4 fast reroute, when the host site router detects the PSAP router switchover through BFD, it immediately switches traffic to the newly active backup router without waiting for routing reconvergence in the ESInet. To further boost resiliency, the path between the host site and the PSAP backup access routers can be traffic engineered to use a different transmission path from the path between the host site and the active access router.

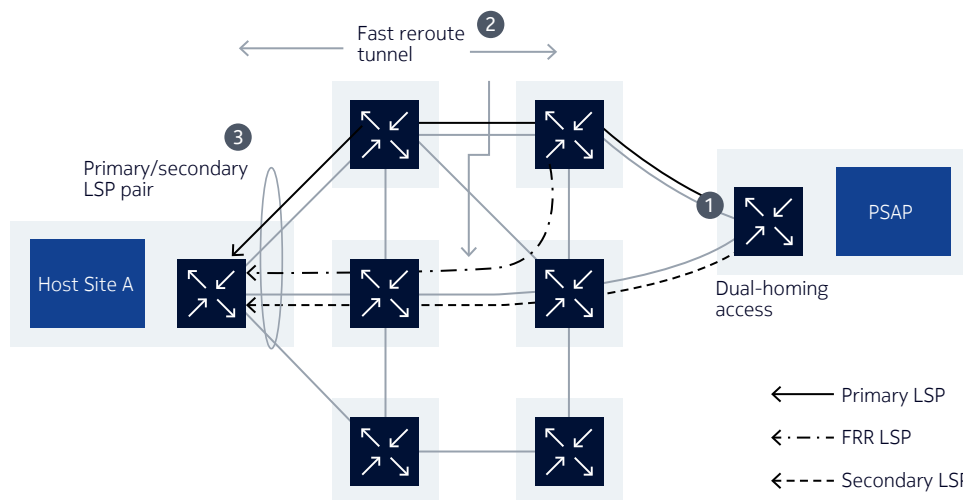
ESInet communications path redundancy protection

An IP/MPLS-based ESInet provides any-to-any communication paths with MPLS tunnels (technically known as label switched paths, [LSPs]). To provide highly reliable transport of emergency communications services traffic, it is important that LSPs have end-to-end redundancy protection along the path (see Figure 3).

- Access diversity (1 in Figure 3)
- Fast-reroute tunnel protection (2 in Figure 3)
- Primary/secondary LSP pair (3 in Figure 3)
- Multi-fault-resilient LSP

⁴ If required, VRRP can support more than one standby router.

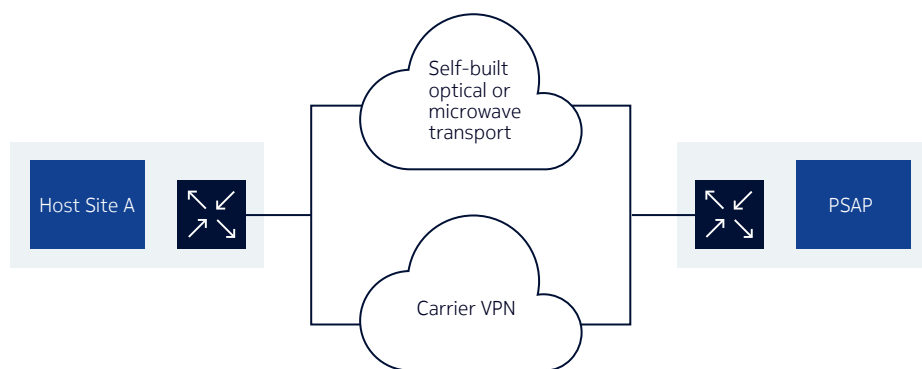
Figure 3. ESInet communications protected by path redundancy



Access diversity

To ensure PSAP reachability, it is critical to equip the access router with dual-homing network access using different transmission facilities along diverse paths in the self-built network or to even adopt a hybrid approach using a third-party carrier for the backup circuit (see Figure 4).

Figure 4. PSAP communications protected by access diversity



Fast reroute tunnel protection

Fast reroute (FRR) is an ultra-high-availability enabler for IP/MPLS, protecting traffic traveling inside the LSP from being discarded if any failure (nodal or link) occurs along the path. Operating at the speed of SONET 1+1 protection switching, it restores the traffic locally at the point of failure by switching the traffic onto a preset FRR tunnel (also known as bypass tunnel). FRR is highly scalable and easy to deploy because bypass tunnels are set up automatically by IP/MPLS routers without operator intervention.

Primary/secondary LSP pair

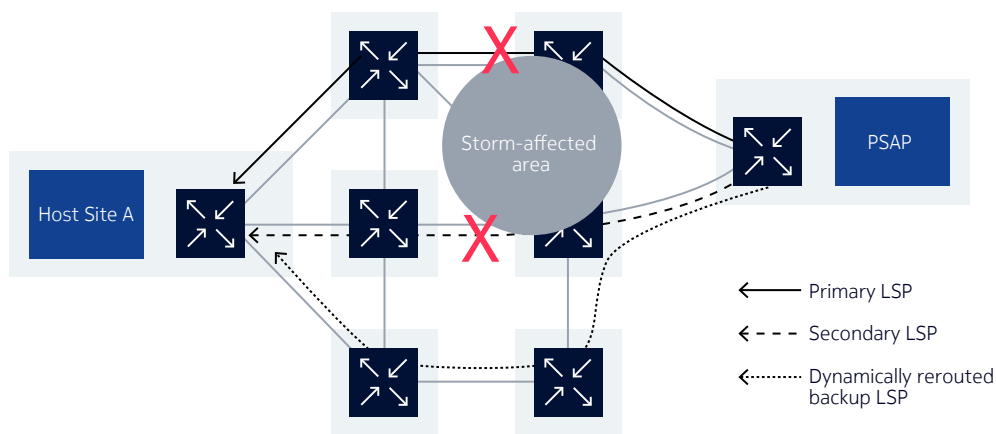
As a complementary protection mechanism to FRR, each LSP tunnel can be protected by a pre-established secondary LSP tunnel. While FRR restores traffic flow at SONET speed to ensure no disruption to emergency services as a temporary measure, secondary LSP with a diverse route serves as a protecting LSP with a traffic-engineered path for network optimization and quality of service. When the access router

learns that the primary LSP has invoked FRR, it switches traffic to the secondary LSP in a hitless manner, bringing no disruption to emergency communications services.

Multi-fault-resilient LSP

As severe weather events become more frequent and intense, multi-fault resiliency has become essential. LSP needs utmost resiliency to endure impacts from such events to continue to deliver emergency services at the time they are needed most. Capitalizing on the power of IP routing and intelligent path calculation, when links on the primary and secondary LSPs fail, IP/MPLS can still reroute affected LSPs around failures if physical reachability exists. As shown in Figure 5, a severe storm affects multiple links (the gray circle), bringing down both the primary and secondary LSP. Because there is rich path diversity in the core network, the access router can establish a dynamically rerouted LSP around the failures so that the PSAP can continue to provide emergency services.

Figure 5. A multi-fault-resilient ESInet



Host site georedundancy protection

The host site is the nexus of NG9-1-1 where all NGCS applications reside. It is crucial that there are multiple host sites in a geo-diverse arrangement. Each host site has its own NGCS applications and other associated equipment. With IP/MPLS VPNs, ESInet can seamlessly connect all PSAPs to the multiple host sites so that emergency services can continue even when a disaster brings down a host site.

Protection from adverse environmental conditions

It is important that the IP/MPLS router can withstand adverse environmental conditions and not be damaged. While PSAPs normally operate in a climate-controlled environment, during extreme weather events there can be overvoltages and overcurrents in the PSAP power systems and even power outages, affecting the climate control system. The voltage level in the backup power distribution system can also go down as outages continue. Consequently, it is important that the IP/MPLS router can continue to operate in extreme hot or cold temperatures as well as withstand the impacts of a voltage surge or a persistent low-voltage condition without damaging its electronics.

Even if the affected PSAP needs to cease operation for PSAP staff safety, the router can still function to support CCTV and other sensor applications to monitor the facility conditions. Moreover, when the weather events are over and power is restored, without having to replace damaged hardware, the router can immediately work normally and be ready to support PSAP communications. This shortens the time required to restore the affected PSAP to full operation.

Conclusion

9-1-1 is vital to citizens who need emergency assistance. With the rise of security threat level and more frequent extreme weather events, highly dependable 9-1-1 emergency response services have become more critical than ever. Migration to NG9-1-1 improves emergency response and heightens citizen safety, which is one of the key components of smart-city vision. Highly dependable NG9-1-1 mandates ESInets with utmost resiliency. If ESInets stop carrying data, emergency communications services stop assisting citizens in need. By harnessing the full redundancy protection capabilities of IP/MPLS platforms, ESInets can attain the utmost network resiliency to keep emergency communications services up and running, even under extreme weather conditions when emergency help from first responders is needed most.

To learn more about Nokia solutions for public safety, visit our [Public Safety](#) web page.

Abbreviations

BCF	Border Control Function
BFD	Bidirectional Forwarding Detection
BGP	Border Gateway Protocol
CAD	computer aided design
CCTV	closed circuit television
E9-1-1	enhanced 9-1-1
ESInet	Emergency Services IP network
FirstNet	First Responder Network Authority
FRR	fast reroute
IP	Internet Protocol
ISP	internet service provider
LAG	link aggregation group
LIS	location information server
LMR	land mobile radio
LNG	legacy network gateway
LPG	legacy PSAP gateway
LSP	label switched path
MPLS	Multiprotocol Label Switching
NENA	National Emergency Number Association
NG9-1-1	next-generation 9-1-1
NGCS	NG9-1-1 call services
PSAP	public safety answering point
SBC	session border control



SONET	synchronous optical network
VoIP	Voice over Internet Protocol
VPN	virtual private network
VRRP	Virtual Router Redundancy Protocol

About Nokia

We create the technology to connect the world. Powered by the research and innovation of Nokia Bell Labs, we serve communications service providers, governments, large enterprises and consumers, with the industry's most complete, end-to-end portfolio of products, services and licensing.

From the enabling infrastructure for 5G and the Internet of Things, to emerging applications in digital health, we are shaping the future of technology to transform the human experience. networks.nokia.com

Nokia is a registered trademark of Nokia Corporation. Other product and company names mentioned herein may be trademarks or trade names of their respective owners.

© 2019 Nokia

Nokia Oyj
Karakaari 7
FI-02610 Espoo, Finland
Tel. +358 (0) 10 44 88 000

Document code: SR1908037718EN (August) CID206543