NG9-1-1 Resiliency Matters

WHITE PAPER

www.gdit.com

The importance of reliability in emergency services communications systems cannot be overstated; lives depend on it. When it comes to crime, medical emergencies, fire or accidents, the impacted and witnesses who dial for help need 9-1-1 calls to go through. Factors affecting resiliency of 9-1-1 services include telecommunications systems, signaling and media transport mechanisms, IP network design, software, monitoring and cyber security. A holistic view of resiliency in a Next Generation 9-1-1 (NG9-1-1) solution is important to help limit or eliminate single points of failure. Factors adding resiliency to a NG9-1-1 solution include:

- Standards-based resiliency
- Redundant components
- Resilient Internet Protocol (IP) networks
- Resilient signaling, voice and data paths
- Redundant applications
- Routing policies and agreements
- Cyber security

This white paper describes the importance of resiliency for a Next Generation 9-1-1 solution and provides recommendations on achieving it.

A Centralized Core Enhances Resiliency for NG9-1-1 Solutions

A NG9-1-1 solution is based on Internet Protocol (IP), enabling functional elements to be deployed in a centralized manner. The critical functional elements within a NG9-1-1 Core Services (NGCS) solution provide border control and location-based call routing services using the Session Initiation Protocol (SIP) for a set of public service answering points (PSAPs). In a NG9-1-1 solution, these services are deployed on servers operating inside of at least two data centers used to house the applications, servers, gateways and other components. For NG9-1-1 solution core resiliency, it is recommended the data centers be geographically separated by at least 50 miles, have multiple independent paths for all signaling and media, have redundant power and cooling, and limited access with video monitoring and biometric security.

There are four tiers measuring data center resiliency described in ANSI/TIA-942, which specifies the minimum requirements for telecommunications infrastructure in data centers. It is recommended data centers be a minimum of Tier 2, but a desired solution would be a Tier 3+ data center that would meet both availability and cost requirements. Another key attribute of a viable data center is the number of carrier connections available for both legacy and IP network transport and signaling. This becomes more important as the NG9-1-1 solution evolves from the transitional phase into an i3 end-state phase, where the selective router (SR) is no longer used and each individual carrier provides 9-1-1 calls using SIP including location information.

Geographic diversity is important to help ensure connectivity is redundant to different physical locations so a problem at one location does not affect the other. Similarly, network diversity involves multiple carriers to ensure there is no common communication link or facility in the path for the redundant connectivity. The same attributes apply for connectivity of PSAPs to the Emergency Services IP network (ESInet), except for lower bandwidth requirements.

The ESInet provides the backbone of the communications network for routing NG9-1-1 calls from the NGCS applications in the data center, to call takers at PSAPs, sharing their information. The key resiliency attributes for the ESInet include geographically-separated data centers that communicate with PSAPs across a redundant IP network design with geographic and network diversity. An ESInet for a particular NG9-1-1 solution is more than just the wide area network; it is the end-to-end emergency services IP network for NG9-1-1 core services connecting to a number of PSAPs. An ESInet includes the NG9-1-1 IP network at the data centers, the wide area network and local area networks at the PSAPs. An ESInet is comprised of a network of networks with a core providing geographic and network diversity, end-to-end traffic engineering for bandwidth and quality service, security with private communication tunnels and high levels of encryption, and high performance with fast speeds and maximum up-time.

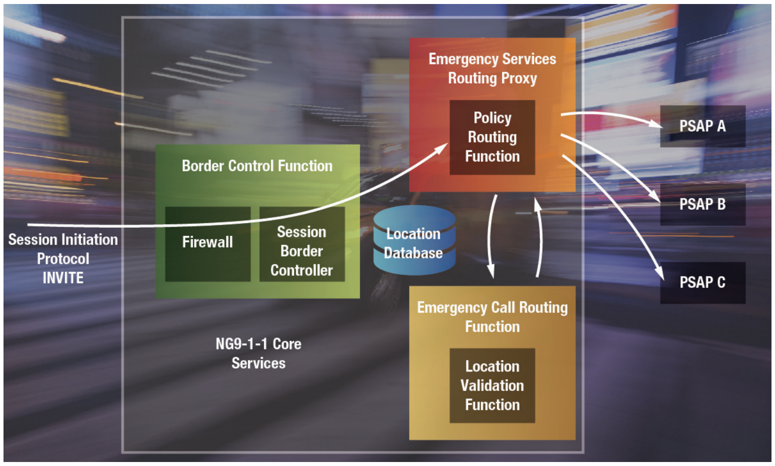
Emergency Services Routing Proxy
Policy Routing Function
PSAP A
PSAP B
PSAP C
Border Control Function
Session Initiation Protocol INVITE
Firewall
Session Border Controller
Location Database
Emergency Call Routing Function
Location Validation Function
NG9-1-1 Core Services

Figure 1. Routing Policies Enhance Resiliency

It is recommended an ESInet be built on a standards-based wide area network (WAN) core, using IP layer 3 protocols like Multiprotocol Label Switching (MPLS) and Border Gateway Protocol (BGP). MPLS provides fast re-routing, enables quality of service and control of bandwidth for different customers over the same physical network path. BGP provides a dynamic private WAN overlay across the MPLS core for IP communications among the data centers and PSAPs.

Routing policies play a key role in resiliency of a centralized NG9-1-1 solution. As illustrated in Figure 1, policies for routing calls within and between jurisdictions need to be in place for when communication paths or functional elements are not available. In a NG9-1-1 solution, the emergency services routing proxy and the policy routing function can play this role of defining different routing policies.

Resilient Components of a NG9-1-1 Solution

The resiliency of NG9-1-1 applications is enhanced by operating them on servers located at two or more geographically-separated data centers. The application software runs natively or in virtual machines on commercial off-the-shelf servers. Each NG9-1-1 application operates in a high-availability configuration within each data center and synchronizes session state and other information between the data centers. By default, NG9-1-1 applications operate in a load-balanced manner across the data centers and can run in an isolated mode with capacity for 100% anticipated demand if needed.

Providing resilient power is mandatory, requiring redundant, independent paths and power sources. Using a universal power supply helps prevent damage from power surges, lightning strikes and provides battery-powered backup for a limited time. Generators can provide backup power for much longer durations than an uninterruptible power supply and powered equipment need dual power modules.

The resiliency of a NG9-1-1 solution is enhanced by keeping a watchful eye and analyzing the past history of the system. Logging, recording and monitoring play an important role. Real-time network performance allows you to observe behavior and make proactive changes. Logging and recording, monitoring and reporting for real-time network performance, user login and administrative action are important elements of ongoing maintenance of a NG9-1-1 solution. Availability and quality of service is maximized by analyzing historical conditions and being proactive in identifying conditions of congestion or failure.

In an IP-based architecture like NG9-1-1, security is critical. A holistic view includes security constructs built on defense-in-depth approaches and traffic monitoring with remediation. Security is defined for each component and at their interfaces. At the ESInet interfaces, there are stateful firewalls, IPS devices and the border control function. The latest security protocols are used to encrypt SIP signaling and media traffic – and the whole IP packet if needed. Application-aware stateful firewalls, intrusion prevention service devices and security certificates constantly monitor real-time traffic for secure access and data flow.

The NG9-1-1 architecture enables the ability to connect to an ESInet from any physical place using different devices, providing call taker mobility. For example, a PSAP could be unavailable due to building renovation or circuit changes, but call takers could log in from a different building or from any location.

The resiliency aspects of a NG9-1-1 solution help ensure the system's availability for 9-1-1 calls in an IP-based network with centralized applications. Design considerations and guidelines include:

- ✓ Standards-based NG9-1-1 architecture
- ✓ Redundancy and geographic diversity needed at all layers
- ✓ Flexible routing policies to improve scenario handling
- ✓ Cyber security from a holistic perspective

Delivering NG9-1-1 Solutions with an Experienced Systems Integrator

Since a one-size-fits-all approach is not viable across our diverse country, General Dynamics IT can help design, implement and maintain a NG9-1-1 solution with its role as a large system integrator, bringing best-of-breed solutions to bear for specific needs. Since 2009, the General Dynamics IT NG9-1-1 systems integration lab provides the ability to validate, integrate and test the different components of a complete i3-compliant NG9-1-1 solution. General Dynamics IT takes a very methodical and detailed approach to planning, implementing, monitoring and managing a complex solution such as NG9-1-1, which helps ensure components are correctly installed and the overall system is delivered within budget and time constraints.

A General Dynamics IT solution supports a standards-based approach to designing, implementing, managing, monitoring and maintaining a NG9-1-1 system. General Dynamics IT has more than 20 years of experience in communications and emergency services by implementing and managing U.S. Department of Defense 9-1-1 operations and the U.S. Federal Aviation Administration unified communications systems including voice, conferencing, call center, network security operations center and 9-1-1. In July 2014, General Dynamics IT successfully implemented and cutover an NG9-1-1 system for several counties in Ohio, and is currently deploying large NG9-1-1 systems for other state and local customers.

For more information on NG9-1-1 solutions from General Dynamics IT, visit our website at http://www.gdit.com/Capabilities/Enterprise-IT/Unified-Communications/ng9-1-1/.

About the Author

Tom Sammons serves as Principal Systems Engineer for Sales in the Global Solution Division of General Dynamics Information Technology. In this role, he is responsible for providing subject matter expertise of NG9-1-1 solutions and their components, meeting with customers, technical pre-sales systems engineering, writing white papers and speaking at industry events.

Tom is a member of the 9-1-1 community through his membership with APCO and NENA, his NENA Emergency Number Professional (ENP) certification and regular speaking engagements at conferences across the country. Tom holds a bachelor's degree in Computer Engineering from Florida Institute of Technology. Throughout his 30-year career in telecommunications and IP network engineering, he has been recognized by his leaders and peers for his passion and focus in leading teams, building quality solutions and for his technical writing and public speaking. Tom can be contacted at tom.sammons@gdit.com.

About General Dynamics Information Technology
As a trusted systems integrator for more than 50 years, General Dynamics Information Technology provides information technology (IT), systems engineering, professional services and simulation and training to customers in the defense, federal civilian government, health, homeland security, intelligence, state and local government and commercial sectors. Headquartered in Fairfax, Va., with major offices worldwide, the company delivers IT enterprise solutions, manages large-scale, mission-critical IT programs and provides mission support services. General Dynamics Information Technology is one of two business units that comprises the General Dynamics Information Systems and Technology business group.

7747 - 1/09/16