Public Safety Communications Resiliency

Ten Keys to Obtaining a Resilient Local Access Network

SAFECOM NCSWIC

Homeland Security

EXECUTIVE SUMMARY

Federal, state, local, tribal, and territorial public safety entities rely on voice and data communications networks to achieve their missions. Yet, communications continuity planning often overlooks one of the most critical and vulnerable parts of these networks: the local access network. The local access network is the "last mile" connection between an organization's communications infrastructure and the commercial service provider's network. An incident such as a cable cut, flood, or damage to the commercial service provider's facility or tower, can completely disrupt the local access network, leaving a public safety organization unable to perform its critical functions.

Communications resiliency means a network is able to withstand damages, thereby minimizing the likelihood of a service outage. Resiliency is the result of three key elements: route diversity, redundancy, and protective/restorative measures.

The Department of Homeland Security Office of Emergency Communications (OEC) helps organizations mitigate threats to communications continuity and supports resilient, "always available communications." This document focuses on the resiliency of the local access because this area of the network typically has the least diversity, while metro and national networks tend to have much greater diversity. This document presents an introduction to resiliency concepts and ten keys to obtaining and maintaining resiliency in a local access network. OEC developed these ten keys as recommendations to help organizations maintain critical communications in emergency situations:

- Understand Communications Resiliency
- Document Current Network Implementation
- Identify Current Network Implementations within Organization Control
- Interface with Service Providers
- Check for Shared Facilities and Communications Links Among Service Providers
- Evaluate the Need for Alternative Path Solutions
- Check for Eligibility for OEC Priority Services
- Seek Partner Organizations and Campus Environments
- Maintain Vigilance
- Stay Up-to-Date with Alternate and Emerging Technologies

This document details important aspects of communications resiliency, such as knowing the exact network infrastructure in the local loop, interfacing with commercial service providers, and properly maintaining alternative path solutions. While these recommendations can mitigate a number of challenges, they should not be considered a comprehensive methodology for maintaining critical communications.

TABLE OF CONTENTS

INTRODUCTION

Communication is critical for the operation of all government organizations, especially during natural or manmade disasters. To maintain critical communications during such events, an organization should carefully plan, implement and review resiliency within its local access network before an event occurs. The local access network is the "last mile" connection between an organization's communications infrastructure and the commercial service provider's network. An incident such as a cable cut, flood, or damage to the commercial service provider's facility or tower, can completely disrupt the local access network, leaving an organization unable to perform its critical functions.

The Department of Homeland Security (DHS) Office of Emergency Communications (OEC) helps organizations mitigate threats to communications continuity and supports resilient, "always available communications." This document presents ten key steps that organizations can follow to determine if local network infrastructure communication paths are sufficiently diverse to minimize communications outages.

1 Understand Communications Resiliency

The first step in achieving communications resiliency is to understand the concept. Communications resiliency means a network is able to withstand damage, thereby minimizing the likelihood of a service outage. Resiliency is the result of three key elements[1]:

- **Route Diversity.** Route diversity is defined as routing communications between two points over more than one physical path with no common points.
- **Redundancy.** Redundancy means that additional or duplicate communications assets share the load or provide back-up to the primary asset.
- **Protective/Restorative Measures.** Protective measures decrease the likelihood that a threat will affect the network, while restorative measures, such as OEC's Priority Services, enable rapid restoration if commercial services are lost or congested.

While the successful implementation of these three elements combined will provide optimal communications resilience, this document focuses primarily on presenting key actions an organization can take to achieve diversity in its various communications networks. Figure 1 illustrates a route diverse communications network between an organization's facility and a telecommunications Central Office (CO) that includes physically separate points of entry or exit at the organization's facility, two physically separate cabling paths to the CO, and physically separate points of entry or exit at the CO. Although the definition of route diversity does not include a standard for route separation distance, actual implementation of route diversity

[1] Route diversity should not be confused with redundancy or resiliency. Redundancy is simply duplicate communications assets. Redundancy combined with route diversity increases resiliency, which is a network's ability to recover from or withstand potential threats. This document presents keys for achieving route diversity.

suggests the greater the distance of separation, the greater the benefit. For example, if the separate points of entry are next to each other, route diversity still exists (see Example 2 in Figure 1 below); however, this may not be the best implementation of route diversity in practice. A better implementation of route diversity is shown in Example 2 where the cabling paths have significant physical separation. The best example of route diversity in Figure 1 is demonstrated by Example 3, as the routes are both physically separate and a choice can be made between two central offices for routing.

Example 1
Route Diversity with Cabling in Close Proximity

Example 2
Route Diversity with Physically Separate Cabling

Example 3
Route Diversity with Physically Separate Cabling and Separate Central Offices

Figure 1: Route Diversity Examples[2]

As shown in Figure 2, land mobile radio (LMR) network route diversity involves at least two unique paths between the console and the base station(s)/repeater sites, and/or the central controller and the geographically dispersed repeater/tower sites whether provided through leased circuits or an Internet protocol (IP) network. The same concepts for diversity demonstrated in the figures throughout this paper between an agency facility and central office apply also to the communication paths of land mobile networks.

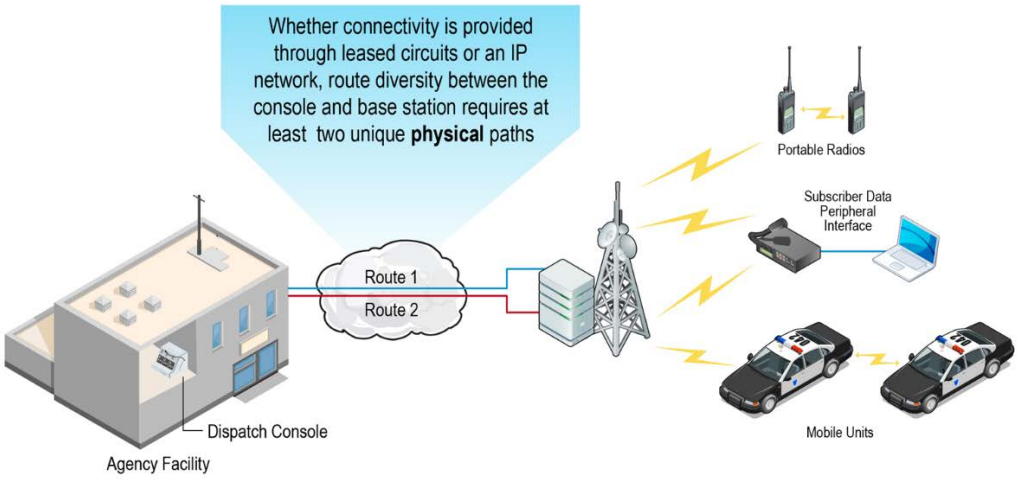


Figure 2: Route Diversity for a Land Mobile Radio Architecture

[2] The graphics in this document are for illustrative purposes only and actual communications network routing will vary by network.

Though this document focuses only on communications network diversity, following Project 25 (P25) standards[3] for LMR systems can improve resiliency. P25 standards encourage use of enhanced features, capabilities, and services designed specifically for the rigors of the public safety environment. The standards articulate requirements for reliable software implementation, ruggedized hardware platforms, and systems designed for high resiliency and redundancy.

2 Document Current Network Implementation

Researching how communication systems are implemented and identifying the supporting network's physical infrastructure is the second step in achieving communications resiliency. An organization should gather and update this information as the initial activity in the analysis of a communications system. A diagram of the physical connectivity and layout of the network will help to identify network assets and their connection points.

Network infrastructure documentation may already exist, and should be updated regularly. This documentation of different components, equipment, and a mapping of all critical network elements is sometimes known as a Reference Architecture. More advanced Reference Architectures may include detailed information such as hardware assets (e.g., routers, gateways, servers), software assets, licenses, circuits, Internet Protocol (IP) addresses, power requirements, and roles associated with each piece of network infrastructure. For a land mobile radio system, physical assets and connections may include console equipment, repeaters, network interconnect equipment, transmitter combiners, receiver multi-couplers, filtering equipment, base stations, antennas, towers, enclosures, microwave equipment, commercial services networks/circuit offerings, backhaul implementation equipment, radio frequency (RF) site infrastructure, transmission lines, subscriber equipment, monitoring equipment, and commercial and backup power equipment. Reference architecture documentation should also include any ancillary or other connected integrated systems. Accurate network diagrams are the foundation of communications resiliency analysis.

3 Identify Current Network Implementations within Organization Control

As part of the network infrastructure documentation process, the organization should include an inventory of on-site communications equipment, entry and exit points in buildings, and key communication distribution points immediately outside the facilities.

[3] The latest list of P25 standard documents available can be found at http://www.project25.org/. Copies of the Standards are free to Government Agencies in the United States. Follow this link for an application form: http://www.tiaonline.org/all-standards/p25-downloads-application

Personnel familiar with an organization's voice and data communications likely can provide information on both government-owned and commercial service provider-owned on-site communications equipment. Such equipment is often located at critical termination points within the facility including telecommunication closets, centralized data centers, and storage locations. These personnel may also be able to provide information on the specific entry and exit points for communications into and out of the building as well as demarcation points. Demarcation points, where service provider equipment transfers service to the organization's equipment, are typically located in a telephone closet. Figure 3 provides a sample graphical depiction of where these points could be located. A visual inspection of the area immediately outside a facility is often adequate to detect communications distribution points. These points are typically the location where lines running to the facility connect to a bigger local loop.

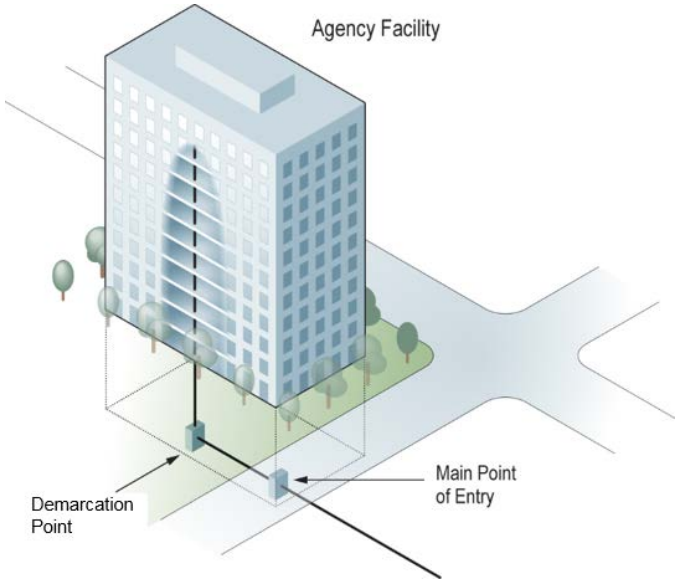


Figure 3: Identify Current Network Configuration

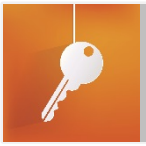
4 Interface with Commercial Service Providers

Identifying and interfacing with an organization's voice and data commercial service providers furthers the understanding of an organization's communications network. For example, organizations may procure unique service terms with commercial communications service providers in the form of service level agreements (SLA) based on specific requirements, including service availability, circuit diversity and service restoration response times. All SLAs should be collected by a single organization point-of-contact and included in the organization's communications infrastructure knowledge base.

Beyond information contained in SLAs, service providers themselves can provide valuable and accurate information regarding physical connectivity and locational intelligence for the

organization's network. A provider's network diagrams offer the most precise information. By combining information from all the commercial services providers an organization should be able to create a physical topology and document it as part of their Reference Architecture. This information would include the number of lines, as opposed to the number of circuits, serving the organization; the redundancy of these lines; and the subsequent locations where these lines terminate (for example, COs and points of presence). When considering redundancy, an organization must account for the connections to the organization's equipment and facilities rather than different providers, as some providers may utilize the same lines and the same physical paths. Lines of transmission will ideally terminate at different facilities, as lines terminating at the same facility share the same risk, if the facility is rendered inoperable. To verify this data, the organization can periodically request validation of route diversity status, as providers often "groom" circuits to balance network traffic.

Service providers are often reluctant to divulge such information as providers fear the exposed plans could pose a threat to the safety of their networks. The following can help alleviate a provider's fears when requesting sensitive information: (1) A letter outlining the intent of the data's use and listing individuals who will have access, (2) A non-disclosure agreement (NDA) signed by those granted access to the data, (3) A documented procedure for use, storage, and access of information for anyone granted access and (4) a policy for the return of information should it be deemed necessary by the provider (The third and fourth items may or may not be included in the NDA).



5 Check for Shared Facilities and Communication Links among Service Providers

Organizations often procure contracts with multiple communication service providers to ensure route diversity exists in last-mile circuits. However, many organizations do not realize that contracting with multiple service providers generally does not guarantee resilient connections. Often, one provider will lease lines from another commercial services provider's infrastructure rather than installing its own circuits. As shown in Figure 4, this could mean that an organization is employing service from two carriers but only using one physical path (running in the same conduit) for all services. Organizations should have conversations with service providers to gather accurate information on the locations and routes of communication service pathways outside of the facility's campus and between architecture elements, such as console to base station communication paths. Organizations should also determine how each provider handles routing within its network; separate communications services may converge on single network devices in common locations, which would result in a non-route diverse path.

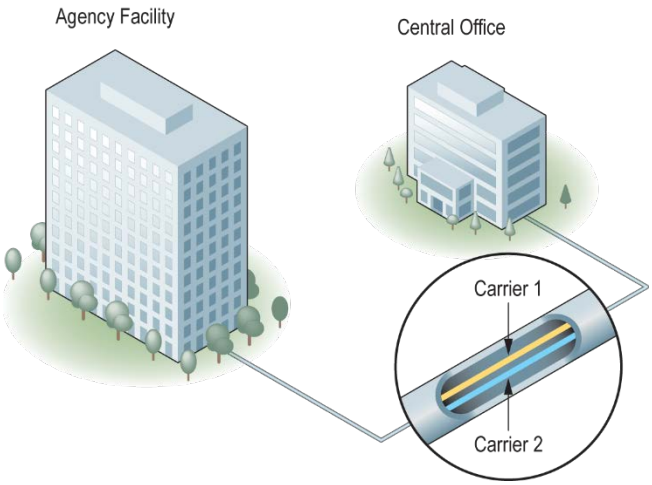


Figure 4: Non-Route Diverse Path Due to Shared Link

6 Evaluate the Need for Alternative Path Solutions

Once an organization understands its existing asset inventory and infrastructure configuration, the organization should determine if its communications systems provide sufficient resiliency. If not, the organization should develop a plan to address areas of concern. A typical solution is the use of backup systems. Backup systems, whether operational (hot standby) or non-operational (cold standby), provide redundancy support and may, if procured and configured correctly, drastically increase the diversity of an organization's communications systems.

Redundancy is available in every area of the communications system. Circuit redundancy provides alternate communication links from the organization's facility to the service provider's network. Redundant links – configured to reside along separate pathways, terminate at separate provider locations, or both – provide additional diversity. Secondary circuits can serve as standbys, inactive circuits or dark fiber, or operational links providing existing services. These connections may consist of alternative technologies to traditional copper and fiber, such as optical beams, microwave transmission, radio frequency transmission, or satellite uplinks.

Organizations can also easily implement redundancy in support of on-site communications equipment. Many organizations house communications equipment to handle various localized communication functions and provide outbound connectivity. Public branch exchange systems provide various telephone functions including voicemail, caller identification, voice conferencing, and local/long distance calling. Access routers enable local data communications functions and external information exchange functions including electronic mail, Internet connectivity, and file transfer protocol. Organizations may also have additional customer premise equipment, such as multiplexers or patch panels. All of these assets can be supported by backups. Redundancy increases the resiliency of the overall communications connections by greatly reducing recovery time from days to hours or minutes.

Redundancy can also be implemented to ensure reliable and continuous operation of the support systems used to allow the communications networks to function. Communication assets are electronic devices that require safe operation environments to run effectively. The most obvious and possibly vulnerable support system is the commercial electric power supply system. Organizations are often affected by local and regional losses of electric power. Although this is beyond an organization's control, the addition of battery backups, uninterruptible power systems (UPS) and backup power generators ensure the survivability of communications during intermittent power surges, losses of power, or extended blackouts. The availability of backup power systems greatly increases the resiliency of the communication functions and supports critical operations.

Check for Enrollment and Eligibility for OEC Priority Telecommunications Services

Once an organization has identified critical circuits within their network, OEC's Telecommunications Service Priority (TSP) [4] should be considered for those circuits. As a result of hurricanes, floods, earthquakes, and other natural or man-made disasters, commercial service providers frequently experience a surge in requests for new services and requirements to restore existing services. The TSP program provides service vendors a Federal Communications Commission (FCC) mandate to prioritize requests by identifying those services critical to national security and emergency preparedness (NS/EP). A TSP assignment ensures that it will receive priority attention by the service vendor before any non-TSP service.

TSP provides priority in both circuit *provisioning* and *restoration* situations. When circumstances require installation of a new telecommunications service faster than a service vendor's normal processes allow, an organization may request *provisioning priority*. This can be an immediate installation following an emergency or an installation by a specific date, also known as an essential provisioning. *Restoration priority* is for new or existing telecommunication services and requires that service vendors restore them before non-TSP services. Restoration priority helps minimize service interruptions that may have a serious, adverse effect on the supported NS/EP functions. Organizations must request TSP restoration priority on its circuits before a service outage.

There are five broad categories that serve as guidelines for determining whether a circuit or telecommunications service is eligible for priority provisioning or restoration. Eligible services must meet at least one of the following criteria:

- Serves our national security leadership;
- Supports the national security posture and U.S. population attack warning systems;
- Supports public health, safety, and maintenance of law and order activities;

[4] Additional information can be found at www.dhs.gov/tsp.

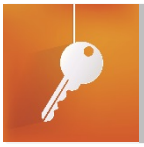
- Maintains the public welfare and the national economic system; or
- Is critical to the protection of life and property or to NS/EP activities during an emergency.

Telecommunications Service Priority (TSP) service user organizations may be in the federal, state, local, or tribal governments; critical infrastructure sectors in industry; non-profit organizations that perform critical national security and emergency preparedness (NS/EP) functions; or foreign governments. Typical TSP service users are responsible for the command and control functions critical to management of and response to NS/EP situations, particularly during the first 24 to 72 hours following an event.

In addition, during times of extreme telecommunications network congestion, qualified organizations benefit from priority access treatment. OEC provides priority access for NS/EP personnel in federal, state, local, tribal and territorial organizations and private entities in critical sectors. OEC recommends that qualified organizations participate in the following programs to ensure continuity of communications during times of network congestion, whether congestion is in the local network, larger networks within the immediate area, or in destination networks:

- Government Emergency Telecommunications Service (GETS) – GETS is a no cost service providing emergency access and priority processing in the local and long distance segments of the public switched network. Public and private organizations use GETS in crisis situations when the network is congested and the probability of completing a call over normal or other alternate telecommunication means has significantly decreased.[5]
- Wireless Priority Service (WPS) – WPS is a low cost service providing priority treatment of phone calls made from cellular telephones by NS/EP personnel during emergency situations when cellular networks can experience congestion due to increased call volumes or damage to network facilities.[6]

For information on TSP and all Priority Telecommunications programs, visit https://www.dhs.gov/topic/emergency-communications, contact the DHS Priority Telecommunications Service Center at 866-627-2255, or email support@priority-info.com.



8 Seek Partner Organizations and Considering Campus Environments

Organizations located in close proximity to one another may partner to share costs and explore new ways to achieve resiliency. If organizations are close enough together, backup wireless systems can connect the facilities and be used in emergency situations. An example of this setup is shown in Figure 5. The two organizations essentially become a campus. Each organization can

[5] Additional information can be found at www.dhs.gov/gets.
[6] Additional information can be found at www.dhs.gov/wps.

have one telecommunications service provider and still achieve resiliency, as long as each organization uses separate service providers with separate serving central offices. Under this arrangement, two organizations can share equipment expenses and contain costs. Each organization would need to buy extra bandwidth to support the added load in an emergency situation, but the overall savings could outweigh the cost.

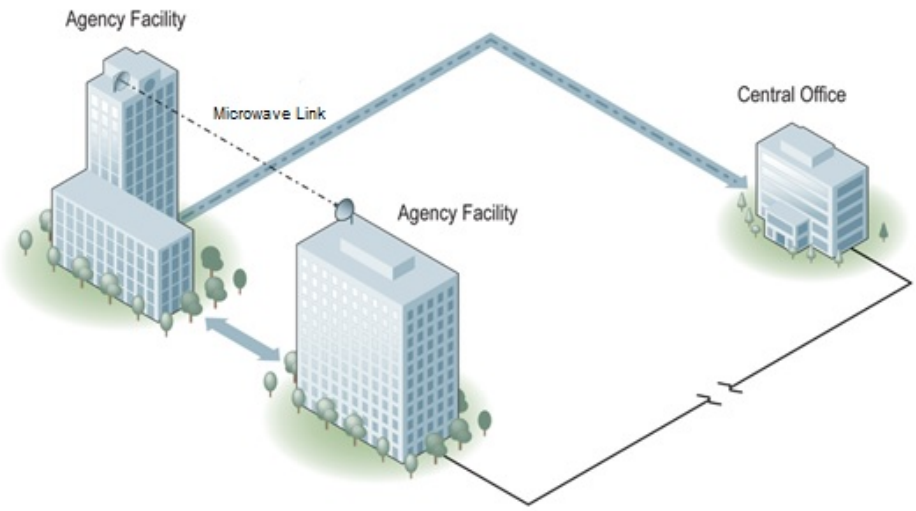
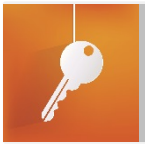


Figure 5: Seek Partner Organizations for a "Better" Solution

9 Maintain Vigilance

To ensure an organization's continuity of communications, organizations should regularly verify current communications resiliency. This is necessary because commercial service provider voice and data networks are routinely being changed and upgraded. A change may not be directly noticed or broadcast, thus OEC recommends that organizations conduct reevaluations at least annually, if not more frequently. Commercial service providers are not always obligated to notify clients of network changes, even if those changes may be detrimental to an organization's communications network.

In addition to keeping updated with service providers, organizations should collect internal organization information on a regular basis. OEC recommends that organizations identify representative(s) from related departments in the organization to meet at least quarterly to update communications-related information, such as network diagrams and location and operational status of all backup and emergency communications devices.



10 Stay Up-to-Date with Alternate and Emerging Technologies

In addition to purchasing secondary services from a commercial communications service provider, purchasing services from multiple providers, or enrolling critical circuits into the TSP, organizations should also consider using providers who deploy alternative transmission mediums for their communications services. Several wireless technologies are available that can enhance resiliency by providing redundant communication pathways or pathways that are inherently more resilient to vulnerabilities common among traditional lines.

Technologies are constantly maturing and emerging in the marketplace. Organizations should maintain knowledge of available options that may support their communication diversity and resiliency requirements.

Conclusion

Communications resiliency is an important aspect of an organization's mission-critical operations. Network redundancy and diversity can help organizations continue to function properly in emergency situations. Organizations must ensure that their networks are resilient in order to maintain operations and fulfill their missions. OEC is available to provide assistance to organizations throughout the process of improving network resiliency.

For additional information on public safety communications resiliency, please contact OEC at OEC-Routediversity@hq.dhs.gov.