



Post-PSTN Public Communications Resiliency

FCC Technological Advisory Council: Communications Resiliency Working Group

ABSTRACT :

The purpose of this paper is to provide a detailed overview of the communications network, as it relates to resiliency. The paper identifies areas of concern, and related recommendations.

Post-PSTN Public Communications Resiliency:

*Technological Advisory Council: Communications Resiliency Working Group
Presented to the TAC December 2013*

Committee Members and Contributors:

Russ Gyurek, Cisco Systems (Chair)

Henning Schulzrinne, FCC (Advisor)

John Barnhill, GENBAND

Mark Bayliss, Visual Link Internet

Nomi Bergman, Bright House Networks

Mark Bregman, Neustar

Ralph Brown, CableLabs

Ed Chan, Verizon

David Clark, MIT

Brian Daly, AT&T

Saikumar Devulapalli, Ericsson

Adam Drobot, OpenTechworks

Brian Fontes, NENA

Dale Hatfield, Silicon Flatirons

Doug Jones, Verizon

Greg Lapin, American Radio Relay League

Mark Linsner, Cisco Systems

Tom McGarry, Neustar

Mike McNamara, TW Telecom

Vish Nandlall, Ericsson

Jack Nasielski, Qualcomm

Katherine O'Hara, Verizon

Brian Rosen, Neustar

Jim Shortal, Cox Communications

Marvin Sirbu, Carnegie Mellon

Paul Steinberg, Motorola

Harold Teets, TW Telecom

Glen Tindal, Juniper Networks

Joe Wetzel, Earthlink

Table of Contents

Executive Summary – The network in Transition.....	5
Recommendation Summary.....	9
Overview of Network Events.....	11
Overview of communications resiliency.....	17
The Wireline Circuit Switched Network.....	19
Future Evolution of Communications Networks.....	29
Disaster Planning and Response.....	37
Resiliency for Public Safety Communications.....	41
Reporting and Metrics.....	43
Policy: Regulatory and Agency Cooperation.....	49
Conclusions and Summary.....	51

Table of Figures

Figure 1. Wireline Residential Voice Trend.....	6
Figure 2. Household Voice Usage Trends.....	6
Figure 3. Voice Usage, Ages 18-34.....	7
Figure 4. Hurricane Sandy Rebuilding Strategy Report.....	14
Figure 5. Consumer Power Impacts by Technology.....	15
Figure 6. Simplified TDM Switch Block Layout.....	17
Figure 7. Access Technology Transition.....	20
Figure 8. Voice Technology Transitions.....	21
Figure 9. Generic Multi-site Architecture for Communication Systems.....	22
Figure 10. PacketCable 1.x Reference Architecture.....	24
Figure 11. OpenSource IMS Architecture.....	25
Figure 12. Voice over LTE Architecture.....	26
Figure 13. LTE Core Example Fallover Scenarios.....	27
Figure 14. Packet Optical Convergence.....	29
Figure 15. Packet-Optical Convergence.....	30
Figure 16. Converged IP and Optical Network.....	30
Figure 17. Software Defined Networking.....	31
Figure 18. Increased Virtualization and SDN Functionality.....	32
Figure 19. ETSI Network Function Virtualization.....	32
Figure 20. IMS in the Cloud: Example Architecture.....	34
Figure 21. M2M connection platform reference architecture.....	35
Figure 22. Pocketnow provides an inside view of AT&Ts Q22013 Disaster planning exercise.....	38
Figure 23. Verizon Emergency Communications Center.....	39
Figure 24. NERC State of Reliability Report - 2012.....	48

TAC Resiliency WG



How can we ensure networks are more resilient in 5, 10 & 15 years than they are today?



High Level Presentation of this paper was presented to the FCC Technological Advisory Council on December 9, 2013. A full copy of the presentation can be downloaded at <http://transition.fcc.gov/bureaus/oet/tac/tacdocs/meeting12913/TAC-Presentation-12-9-13.pdf>

EXECUTIVE SUMMARY – THE NETWORK IN TRANSITION

Communications network users are driving the transition away from wireline, circuit switched voice services, sometimes called the Public Telephone Switched Network (PSTN), at a rapid rate. For many years, this network set the standard for reliability and universal reach and became known as the “system of record” on which many devices and services were built. The PSTN is also the network where the majority of regulation, policy and guidelines are anchored.

The communications industry is undergoing a dramatic transformation that began with the introduction of IP-based data networks in the early 1990s and then with Voice over Internet Protocol (VoIP) in the late 1990s, and it now includes all forms of voice, video, and messaging communications. In fact, while generically referred to as the “IP transition”, the industry is actively managing three simultaneous transitions: the transition of voice from circuit-switched to packet; the rapid evolution of consumer access from wired to wireless; and the transition from copper to fiber. Implicit in this is the move from TDM to IP and the evolution from narrowband services to broadband services.

The emergence of smartphones, combined with high-speed mobile broadband and fixed mobile broadband have all been key catalysts in this transformation.

Gone are the days when all communications services were tightly integrated with the physical plant like telephone lines and central office switches. The internet has become the great equalizer in many respects, lowering historical barriers to service delivery. Communications now encompasses many brands, service providers, devices, networks, and technologies, many of which were not in existence just a decade ago. While the communications landscape is rapidly changing, the Internet itself is growing and evolving, such that it may eventually encompass and surround much of a person’s daily life at work, home, or on the road.

The last two years in particular have seen a dramatic shift in the telecommunications industry where enterprises and consumers are rapidly substituting wired and wireless services with broadband-based VoIP and mobility. While the reasons behind this transition are many, ultimately we are now a fully connected society where “always on” telecommunications infrastructure has become the expected norm from people from all walks of life. The challenge is to transition to new technologies and provide services that will be either as or more resilient than the services they replace.

Today, the trend is clear. Consumers are rapidly substituting traditional wired services with more advanced wireless offerings. Businesses and remaining wireline consumers are rapidly adopting broadband-based VoIP technology, leaving fewer and fewer subscribers on the legacy PSTN network. In fact, the latest Local Competition Report published in November 2013 shows that the wired residential voice subscribers dropped 14 percent in just three years¹.

1 FCC Local Telephone Competition: Status as of December 31, 2012 available at http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-324413A1.pdf

Residential Wired Voice Lines (000)

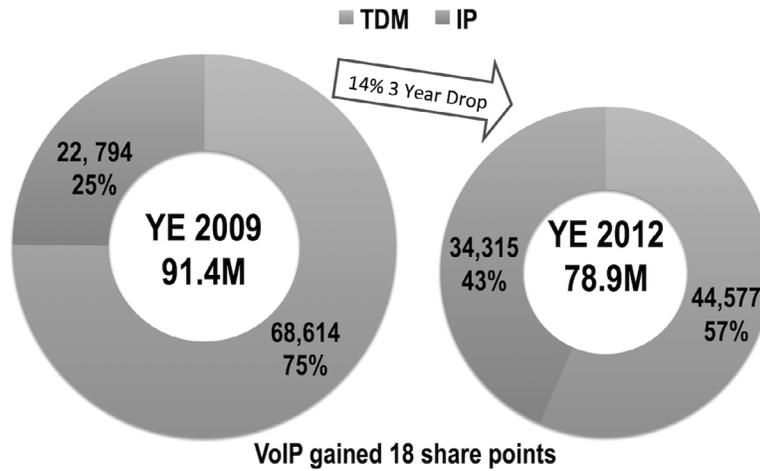


Figure 1. Wireline Residential Voice Trend

In data collected and published by the Center for Disease Control (CDC)² in Figure 2 below, only 8.6 percent of U.S. Households continue to rely solely on a landline while more than 38 percent rely solely on a wireless voice service. Note: The CDC collects this data in order to communicate to US households in the case of health-related emergencies and to conduct health-related telephone surveys.

Household Voice Technology

% of US Households by Communications (Voice) Modality

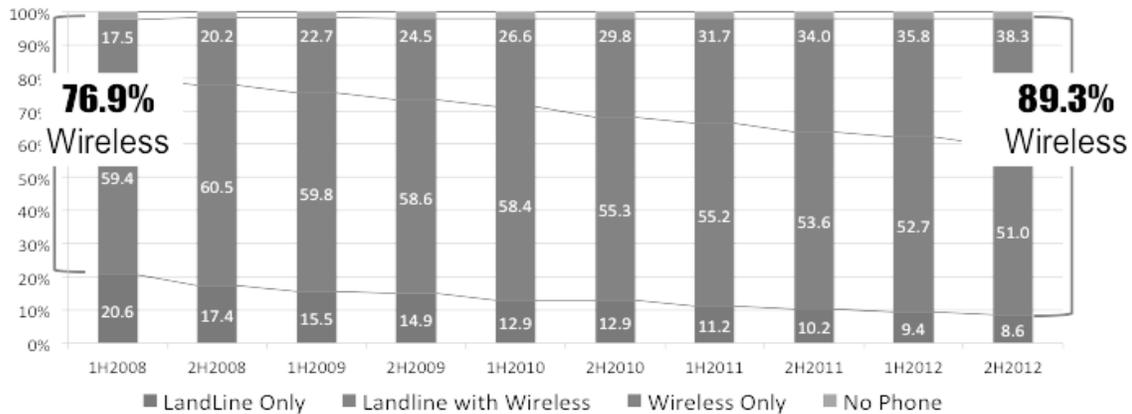


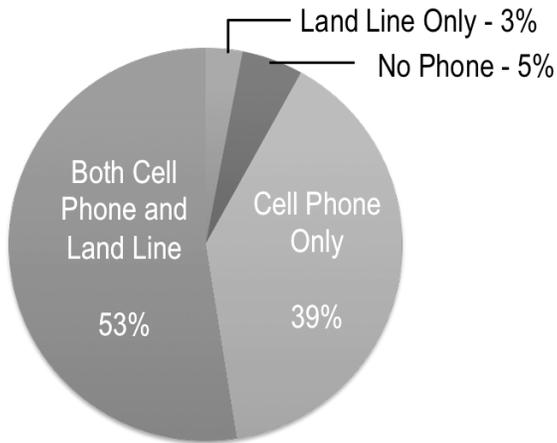
Figure 2. Household Voice Usage Trends

Further analysis by Mediarmark Research and Intelligence demonstrates the generational aspects of this trend by showing that only three percent of Americans ages 18-34 live in landline-only households (Figure 3)³. With the substitution of technology come changes in performance, both good and potentially bad.

2 Blumberg SJ, Luke JV. Wireless substitution: Early release of estimates from the National Health Interview Survey, July – December 2012. National Center for Health Statistics. June 2013. Available from: <http://www.cdc.gov/nchs/nhis.htm>.

3 Quoted in news releases. Full Data available: http://codebook.mriplusonline.com/TM13/cb_TM13_SecAll.pdf

Americans age 18-34



SOURCE: Mediamark Research & Intelligence

Figure 3. Voice Usage, Ages 18-34

- Network Events
- Circuited Switched Infrastructure
- Emerging Network Trends
- Natural and Man-made Disaster Planning and Response
- Public Safety Implications
- Metrics and Reporting
- Regulatory Actions and Agency Cooperation

The Technical Advisory Committee (TAC) understands that the Federal Communications Commission has clear direction to ensure public safety and that communications services are reliable and available to all citizens consistent with its statutory obligations. The Commission also has expressed their ongoing interest in continuing to promote competition and protecting consumers. For these and other public interest obligations, all stakeholders want to ensure that the public communications network continues to provide a high level of resiliency and reliability that accounts for the unique engineering, network configurations and consumer uses of these evolving networks.

With this in mind, the TAC created a Resiliency Working Group intended to characterize how the resiliency of the current telecommunications infrastructure can be maintained, while evolving to a future mode of operations intended to leverage brisk technical and standards evolution. Therefore the guidance and recommendations reflected in this paper are intended to cover the following technology and policy areas:

Ultimately, our Working Group's goal is to address the key underlying elements that contribute to resiliency, offering recommendations intended to support a future network that is resilient and service-rich.

RECOMMENDATIONS

RECOMMENDATION SUMMARY

1. **RECOMMENDATION:** FCC sponsored industry collaboration to create educational material/guidelines for consumer backup power associated with their broadband communication services.
 - a. Explore leveraging DHS, FEMA, and the Ad Council to establish a fund to create and promote consumer awareness.
 - b. Collaborate with service providers and consumer electronics manufacturers to document power consumption for devices in the communications chain.
 - c. FCC to promote the development of a CPE efficiency and “plug” program to create a common power plug for back up power.
 - d. Establish a challenge.gov challenge to develop creative solutions to maintain customer communication services for at least 24 hours during power outages.
 - e. FCC to recognize there is an existing and evolving voluntary telecommunications industry agreement focused on energy efficiency (<http://www.ncta.com/news-and-events/media-room/article/2453>).

2. **RECOMMENDATION:** Optimize the current restoration process: FCC creates national program on a collaborative restoration approach in response to outages or natural disasters to increase resiliency and long-term reliability. Additionally, this program would help reduce damage to communications networks during the restoration process post natural disasters.
 - a. Explore creating a “data exchange” for various utility/communication providers to share data with each other for greater efficiency and optimization of restoration process.
 - b. Provide estimated time to restore electrical service, by area, to communications companies.
 - c. Provide communications companies with power crew work locations so that efforts can be coordinated.
 - d. Instruct clearing and tree removal power crews not to cut any communications cables; call providers for quick removal of any cables.
 - e. Place communications technical facilities at risk, and outside plant locations critical to public and private sector entities on priority restoration lists.

3. **RECOMMENDATION:** Reliability/Resiliency: The FCC act as a catalyst and work closely with the power industry to encourage continued improvements to reliable commercial power architectures to assist the communications service providers in developing resilient industry-related strategies for critical network infrastructure.
 - a. FCC to work with FERC and other power industry agencies.
 - i. Explore the impact of long-term use of back-up and diverse power sources.

4. **RECOMMENDATION:** “Dig Once Policy”: Building on the 2011 Executive Order – Accelerating Broadband Infrastructure Deployment, FCC to Encourage Dig Once policies be enacted at local, state and federal levels to facilitate co-installation of communications networks during public works and utility construction
 - a. “Dig Once” policy would minimize the disruption to citizens by consolidating utility work among different companies. Potential to reduce facility cuts. Longer term greater reliability of network through underground installations of physical plant.
 - b. Collaborate with the FCC Inter-Governmental Advisory council to jointly address how to get more voluntary cooperation.

5. **RECOMMENDATION:** Data collection and Metrics: Use network data sources to better track, predict, and plan network resili-

ency for disaster preparedness. To baseline and measure resiliency improvement over time.

- a. FCC to work collaboratively with providers to establish a data analytic ability to use existing data sources, including existing NORS and DIRS data, for greater predictability and analysis of resiliency, and creation of a “Reliability Baseline” as a reference for future comparisons and metrics, working voluntarily with industry.
- b. FCC to partner with CDC to update current data gathering process to get more specific information relating to availability of multi-modal communication options, clarifications between VoIP, OTT VoIP, and traditional wireline voice services for better reliability reporting and planning capability.
- c. Leverage MBA data sets: Determine what data could be of value for reliability in the long-term goals of the MBA program.
- d. FCC to work with providers, determine what additional data is a meaningful indicator of reliability; develop a voluntary “crowd sourcing” data collection model to gather data in a manner that protects provider and consumer privacy and proprietary needs.
- e. Create annual network reliability baseline update.

6. **RECOMMENDATION:** FCC Sponsored Workshops:

- a. Workshop: Consumer Awareness: The FCC host consumer awareness workshops to foster and create educational material on guidelines for consumers addressing power back up and services impact.
- b. Establish a challenge.gov contest to design a low-power (< 0.5 W standby, say) DSL or cable modem that can survive on battery power for at least 24 hours. Right now, cable/DSL modems require ~5W.
- c. Consider adopting battery strategies that utilize readily available sizes such as D Cells.

Other Items:

- The team has discussed the critical nature of cyber-security related recommendations as the network is fully transitioned to IP. However, recommendations that have been discussed seem to overlap with the Cyber-Security work group, so we will defer to them for formal recommendations to the TAC.
- Metrics: The collection of metrics is a point on which the TAC WG did not reach consensus. States are exploring ways to continue to require a subset of statistical reporting in order to fulfill the mission to protect consumers and ensure public safety. Others prefer for service providers to manage their own networks and only report issues when unusual events occur that would require an outage report. As many new communications technologies require a broadband connection, the working group has discussed the value of application statistical reporting when there is no reporting on the underlying broadband network that enables the communications service on several occasions.

It became important to distinguish between interconnected and non-interconnect VoIP service, and address fixed and nomadic within the domain of interconnected VoIP. There is agreement that there is tremendous variability in interconnected VoIP (nomadic and fixed) quality of service that could be tied to a number of different factors, most of which could include non-service provider related items. It was also clear that a nomadic extension of a fixed service would have additional issues based on the type and speed of broadband access available.

There was some agreement that new complexities of service delivery would benefit from a fresh look at gathering performance information on various voice services. There was a proposal for the FCC to seek a third way by exploring leveraging a crowd-sourced data-gathering model. Most Interconnected VoIP traffic today is carried over private managed IP networks that would not be measured by the MBA initiative, which points towards a new methodology for reporting performance, specifically a user-reported series of statistics enabled by technology. Similar to crowd-sourcing, the FCC could work with service providers and equipment manufacturers to leverage various embedded device technologies to determine the performance characteristics of the network elements. This would include monitoring of network events that impact reliability and resiliency.

OVERVIEW OF NETWORK EVENTS

A number of natural and man-made disasters over the past decade demonstrate the critical nature of the communications infrastructure.

The Derecho

“In June 2012, portions of the Midwest and Mid-Atlantic regions of the United States experienced a destructive windstorm called a derecho⁴, resulting in 22 deaths and leaving millions without electrical power.

The 2012 derecho severely disrupted 9-1-1-related communications. Seventy-seven 9-1-1 call centers serving more than 3.6 million people in six states lost some degree of connectivity, including vital information on the location of 9-1-1 calls, mostly due to service provider network problems. From isolated breakdowns in Ohio, New Jersey, Maryland, and Indiana, to systemic failures in northern Virginia and West Virginia, 9-1-1 systems and services were partially or completely down for up to several days. Seventeen PSAPs⁵ in three states lost service completely, affecting the ability of more than 2 million people to reach 9-1-1 at all.⁶”

The greatest impacts occurred in northern Virginia as a result of power failures and the failure of back up generators to take the load. The resulting loss of the SS7⁷ signaling capability isolated several 9-1-1 switches. This, coupled with losses in transport equipment, created communications problems that lingered days after the event.

Hurricane Sandy

In 2012, Hurricane Sandy uncovered significant exposures to the resiliency of our telecommunications infrastructure. Hurricane Sandy was a Category 1 Hurricane with sustained winds of 80 mph; nowhere near a catastrophic Category 4 or 5 hurricane with sustained winds of 150 mph or more typically associated with far-reaching damage potential, but there was catastrophic flooding and the impact to the US economy was severe.

It is estimated that 8.5 million people in 15 states lost power. The storm affected personal and business services which impacted millions more. Making matters worse, fuel distribution was also disrupted, which left portable generators unused in some cases. As a result, communications and broadband access were compromised for millions of individuals and thousands of businesses.

The FCC recently summarized the impact to communications service during Hurricane Sandy as follows: “Superstorm Sandy disabled at its peak more than twenty-five percent of cell sites in 158 counties in all or part of ten states and the District of Columbia.⁸ The most extensive wireless service impairments from Superstorm Sandy were heavily concentrated in New Jersey and in the New York City metropolitan area, where millions of residents found themselves without reliable and continuous access to mobile wireless communications throughout the storm and its aftermath.⁹ Several counties had outages more than double the

4 The National Weather Service defines a derecho as “a widespread, long-lived wind storm that is associated with a band of rapidly moving showers or thunderstorms. Although a derecho can produce destruction similar to that of tornadoes, the damage typically is directed in one direction along a relatively straight swath. As a result, the term ‘straight-line wind damage’ sometimes is used to describe derecho damage. By definition, if the wind damage swath extends more than 240 miles (about 400 kilometers) and includes wind gusts of at least 58 mph (93 km/h) or greater along most of its length, then the event may be classified as a derecho.” See <http://www.spc.noaa.gov/misc/AbtDerechos/derechofacts.htm>.

5 Public Safety Answering Point

6 Impact of the June 2012 Derecho on Communications Networks and Services, Report and Recommendations, A Report of the Public Safety and Homeland Security Bureau, Federal Communications Commission, January 2013, <http://www.fcc.gov/document/derecho-report-and-recommendations>

7 Signaling System 7

8 See Statement of FCC Chairman Julius Genachowski, Superstorm Sandy Field Hearing, New York, NY, and Hoboken, NJ (Feb. 5, 2013), available at http://transition.fcc.gov/Daily_Releases/Daily_Business/2013/db0205/DOC-318754A1.pdf.

9 See, e.g., Kevin McCoy, et al., Wireless Service Improves in Sandy-affected Areas, USA Today (Nov. 1, 2012), available at <http://www.usatoday.com/story/tech/2012/11/01/sandy-cellphones-service-charging/1675189/> (“Wireless coverage is gradually recovering in the areas affected by Hurricane Sandy, but millions of Northeasterners are still grappling with spotty or no cellular connections.”).

twenty-five-percent figure for the larger area—some much more—and for the state of New Jersey, all of which was included in the reporting area, aggregated cell site outages were on the order of forty percent. However, within a few days, cellular coverage improved dramatically, despite significant challenges in replenishing fuel supplies, part through diligent deployment of generators, cell-towers-on-wheels (COWS) and cell towers on light trucks (COLTs).

Boston Marathon Bombing

On April 15, 2013, near the densely packed finish line of the Boston Marathon, two bombs exploded killing three people and injuring 176 others. Instantly, chaos ensued and the area was turned into a “war zone” as described by ABC News.

Local government officials used social media including Twitter to notify citizens of the incident and later to solicit video footage of the area near the finish line.

While wireless networks operated as designed and did not suffer outages as a result of the bombing, the sudden surge in traffic and resulting congestion made it difficult for participants and spectators to connect with their family members. Also, as police began the manhunt for the bombers, first responders sought to share high volumes of data, primarily citizen captured video, with other law enforcement agencies and the public at large. Collecting mobile phone video and sharing it for analysis reportedly helped with the identification and capture of the bombers.

Suzanne Spaulding, deputy undersecretary of the U.S. Department of Homeland Security, acknowledged there were other communications failures during the response to the bombings. “Significant problems really arose ... with that essential delivery of big data packages, particularly the videos that proved to be so significant and important in the resolution of this event.”¹⁰

Colorado Floods

After wildfires and droughts earlier in the year, residents of Colorado were hoping for some rain. What they got was more than a year’s worth of rain in just four days. The flooding created widespread problems with power outages and road washouts. Communications service providers experienced the effects of the floods, losing fiber backhaul in some cases that isolated facilities and created service outages. In other cases, power loss and restoral times exceeded the battery capabilities to provide back up power. While not as severe as other storms, local officials reported that communications problems did impact search and rescue efforts.

Hurricane Katrina

The panel investigating Hurricane Katrina found that though the coastal areas along the Gulf of Mexico suffered substantial damage, the region’s communications infrastructure as a whole performed fairly well in the face of the extreme winds and rain from the storm. They cited unique conditions, such as substantial flooding, widespread and extended power outages and security issues as being largely responsible for the significant communications disruptions that affected much of the region for an extended period. In addition, failure of redundant pathways for communications traffic, and inadvertent line cuts during restoration were named as issues contributing to network failures or delays in restoration.

While not specifically our focus here, the potential for man-made communications outages, whether accidental or intentional also represents significant resiliency challenges. The TAC cyber-security working group is addressing many of these items. However, the physical security of the power grid, communications infrastructure, and particularly top-tier interconnection facilities should be considered as critical infrastructure on which the nation’s ability to communicate and conduct commerce depends. Not all man-made events affecting communications networks are large, well-planned occurrences. For example, as service providers seek to add back up power deeper in the outside plant, thieves targeting generators, batteries and heavy metals are creating an outage potential where the provider has actually taken steps to guarantee service¹¹.

10 <http://www.pewstates.org/projects/stateline/headlines/after-boston-bombings-a-failure-of-communications-85899471750>

11 <http://www.khou.com/news/crime/khou-89547597.html>

The actual reliability and resiliency of the network direction is difficult to ascertain without a clearly defined baseline. To date, such a baseline does not exist and therefore it is difficult to determine resiliency trends. This paper addresses some of these issues in more detail by recommending data use and sources.

Dependency on the Power Grid

Natural disasters, similar to the examples above, demonstrate the essential nature of the power grid to communications.

- In the Derecho example, the largest impact was actually to the wireline switch and SS7 outages due to power loss and generator failure.
- In Hurricane Sandy, wireless towers were out of service due to various factors, but it should be noted that some wireline infrastructure was flooded and required complete replacement.
- Even though Hurricane Katrina occurred a number of years ago, many of the recommendations still apply. They are listed below.
- The Colorado floods created problems in two primary areas, flooding of facilities isolating offices and towers and power outages.

Whether caused through overload, natural disaster, or man-made events, the nation's power supply is critical to the performance of its communications network. This becomes even more relevant as the network of record moves away from wireline. While many of the key facilities such as cellular towers, central offices, and data centers maintain generators or battery back up, these are typically designed for limited coverage pending restoral of commercial power. At the premise level, the average home¹² doesn't have a generator or back up power supply that will maintain fixed communication or Internet service during an outage.

Major recommendations¹³ made by the Hurricane Katrina Panel to promote efficient and effective disaster planning and recovery efforts centered around four areas:

- Pre-position the communications industry and government to achieve greater network reliability and resiliency in the event of natural disasters;
- Improve recovery coordination;
- Improve the operability and interoperability of public safety and 911 communications
- Improve disaster-related emergency communications to the public.

Major recommendations¹⁴ coming from the Derecho report include ensuring that service providers:

- Conduct periodic audits of 9-1-1 circuits
- Maintain adequate backup power at central offices
- Follow regular maintenance and testing procedures
- Have adequate network monitoring links
- Have a more specific obligation to notify 9-1-1 call centers of breakdowns of 9-1-1 communications.

As the Derecho report was issued after Hurricane Sandy hit, the report included two additional areas of focus based on this event:

- The ability of consumers to originate successful calls for help in emergencies, including the availability of wireless networks
- Power for consumers' devices and equipment

¹² The 21st century does not have a CO powered phone, but several active devices that require power to provide communications across multiple protocol layers.

¹³ <http://transition.fcc.gov/pshs/docs/advisory/hkip/karrp.pdf> pages iii-v

¹⁴ http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-318331A1.pdf starting page 39

In the Hurricane Sandy report, the analysis led to the following statement:

“DOE and the National Telecommunications Information Administration (NTIA, part of DOC), should work with FCC to promote a programmatic approach to ensure that cellular towers (antennas), data centers, and other critical communications infrastructure are able to function regardless of the status of the electrical grid. In addition, encouraging stored power (i.e., batteries) for consumer level broadband equipment, through funding or other means, will improve impacted individuals’ ability to seek information, help with recovery needs, communicate with family members, and even work from home when transportation or business facilities are significantly compromised.¹⁵”

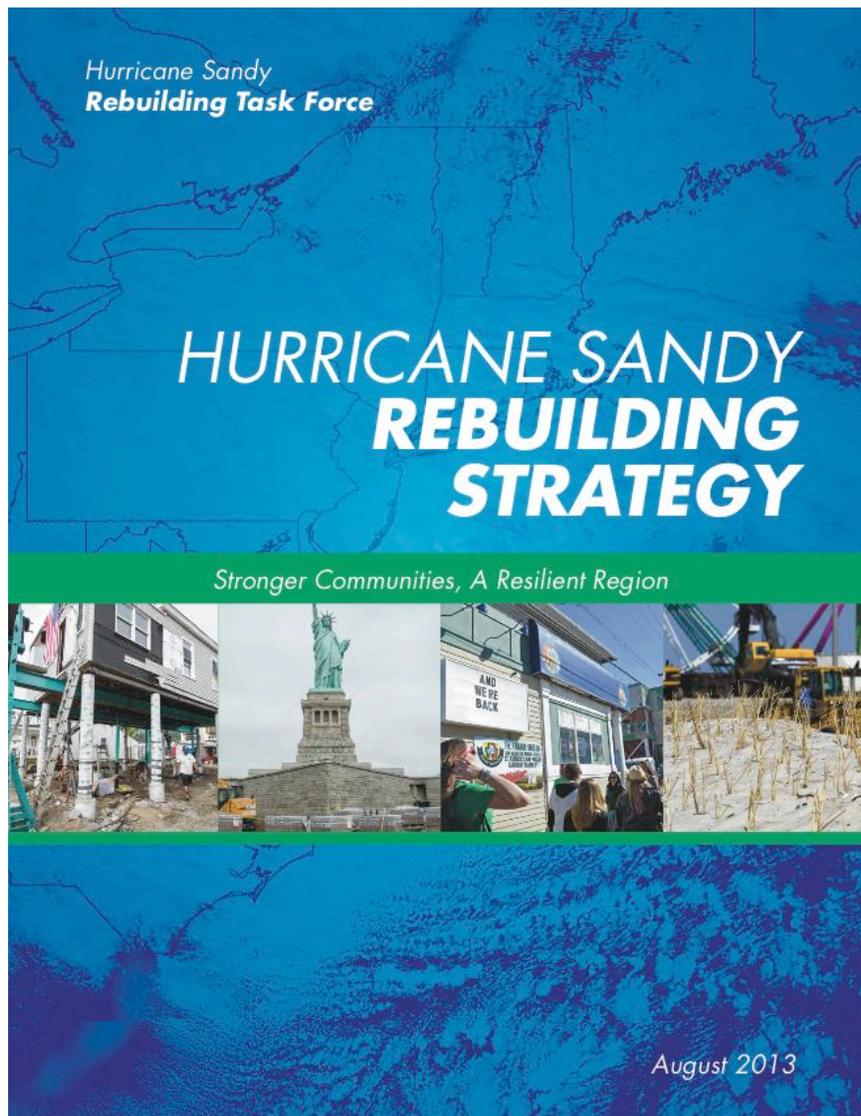


Figure 4. Hurricane Sandy Rebuilding Strategy Report

15 <http://portal.hud.gov/hudportal/documents/huddoc?id=HSRebuildingStrategy.pdf> page 69, recommendation 16

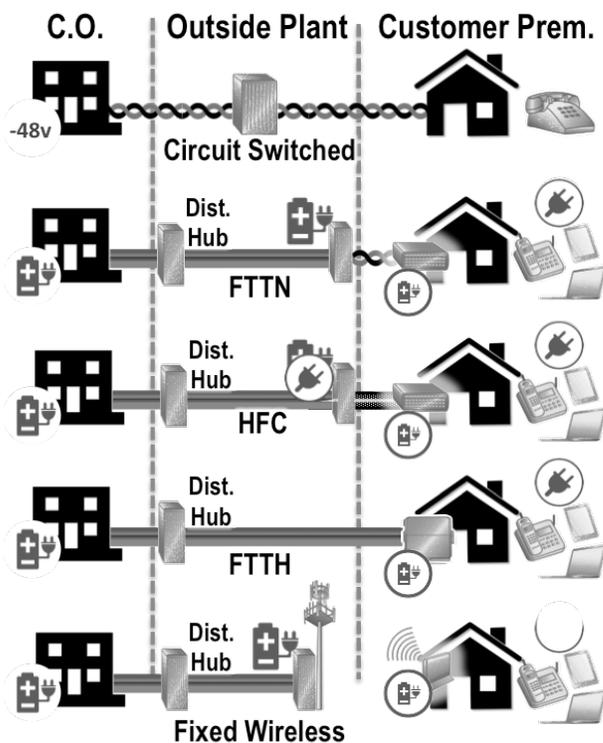
RECOMMENDATION: Reliability/Resiliency: The FCC act as a catalyst and work closely with the power industry to encourage continued improvements to reliable commercial power architectures to assist the communications service providers in developing resilient industry-related strategies for critical network infrastructure.

- a. FCC to work with FERC and other power industry agencies.
 - i. Explore the impact of long-term use of back up and diverse power sources.

Subsequent to the Hurricane Sandy report, the FCC studied the reported data and subsequently conducted hearings and interviews to gather a more complete record on the actual scope of service failures. The Commission found that performance varied between service providers in ways not easily explainable by the event.

In the 2011 report from CSRIC on the transition to next-generation 911 (NG911), power supply dependencies were noted in specific recommendations at the Federal, State, and PSAP levels¹⁶.

As the transition to VoIP and wireless continues, the ability to rely on network powered communications declines. In diagram below (Figure 5), we illustrate how this transition also transfers responsibility for power from centralized locations to customer premise. Note that in all cases except for the first scenario for central office powered service, it will be up to the consumer or the enterprise to provide backup power for their own communications. While some network access devices provide for a battery backup, most service providers are not providing or monitoring battery life at the customer premise.



In recent comments on network resiliency, Commissioner Rosenworcel recounts some of these same events and also observed that new wireless and IP services are dependent on commercial power, and these events raise important questions concerning not only the availability of back up power but the need to ensure “that consumers understand not just the benefits, but also the limitations, of new technologies when they reach out for assistance” and to be prepared for such events¹⁷.

For more information on this topic, we refer the reader to the paper authored by Professor David Gabel and Steven Burns published by the National Regulatory Research Institute (NRRRI). This paper, entitled “The Transition from the Legacy Public Switched Telephone Network to Modern Technologies” provides a detailed look at the impact of commercial power on communications¹⁸.

Figure 5. Consumer Power Impacts by Technology

16 <http://transition.fcc.gov/pshs/docs/csric/CSRIC-WG4B-Final-Report.pdf>

17 See FCC 13-125, page 38 http://transition.fcc.gov/Daily_Releases/Daily_Business/2013/db0927/FCC-13-125A1.pdf

18 Available at <https://prodnet.www.neca.org/publicationsdocs/wwpdf/111212nrri.pdf>

It is important to point out that the Consumer Electronics Association (CEA) has been actively working with service providers and electronics manufacturers to improve the power performance of key elements in the communications chain. They have been pushing for market-oriented programs and initiatives, including industry-led standards and market research driving towards increased energy efficiency. They are working with governments in the development of energy efficiency initiatives that complement and support the voluntary approach and continued innovation, expanded consumer choice, and enhanced product functionality. They coordinate their efforts with other stakeholders including advocacy groups and regulators such as the Department of Energy, Environmental Protection Agency, Federal Trade Commission, and the California Energy Commission, among others. As an example, CEA, the National Cable & Telecommunications Association (NCTA) and 15 industry-leading video providers and device manufacturers signed an unprecedented Set-Top Box Energy Conservation Agreement that will result in annual residential electricity savings of \$1.5 billion or more.

RECOMMENDATION: The FCC sponsor industry collaboration to create educational material and guidelines for consumer back-up power associated with their broadband communication services.

- a. Explore leveraging DHS, FEMA, and the Ad Council to establish a fund to create and promote consumer awareness.
- b. Collaborate with service providers and consumer electronics manufacturers to document power consumption for devices in the communications chain.
- c. FCC to promote the development of a CPE efficiency and “plug” program to create a common power plug for back up power.
- d. Establish a challenge.gov challenge to develop creative solutions to maintain customer communication services for at least 24 hours during power outages.
- d. Establish a challenge.gov challenge to develop creative solutions to maintain customer communication services for at least 24 hours during power outages.

RECOMMENDATION: FCC Sponsored Workshops:

- a. Workshop: Consumer Awareness: The FCC host consumer awareness workshops to foster and create educational material on guidelines for consumers in relation to power back up and services impact.
- b. Workshop: CEA and other relevant parties: FCC to promote labeling, efficiency, ease-of-use for CPE. Attendees to include: CEA, CPE vendors, SP's and consumer advocacy groups.
- c. Physical Infrastructure Reliability Summit/Workshop: This workshop would be designed to leverage the Hurricane Sandy Rebuilding Strategy Action Report. FCC would lead collaboration efforts with other government entities in relation to power reliability and restoration.

OVERVIEW OF COMMUNICATIONS RESILIENCY

The Wireline Circuit Switched Network

Resiliency is a key attribute of the Public Switched Telephone Network. The customer premise, the access, the switch, the tandem and interconnection, power and the transport were all built with reliability in mind.

The Switch

In the TDM network, resiliency was developed over a long period of time through design, performance analysis, standards and root cause failure analysis. One of the frequent expressions of PSTN service performance has been the characterization that the network service is available 99.999% of the time. This standard of “5 nines” continues to drive the performance expectation of the network. This, in turn, has driven vendors and service providers to develop products and procedures to meet these standards.

For example, digital switches were designed to have essentially no unplanned downtime. Many digital switches have traditionally been built to specifications that ensure they are only out-of-service for unplanned purposes no more than a few minutes in a forty year period.

This level of reliability was accomplished in the digital switch by having all essential components duplicated, spared or backed-up. Equipment vendors developed proprietary hardware and software that was fully redundant and fault tolerant in that no single failure could cause a switch outage. This strategy created a resilient network by interconnecting multiple individual switches, all designed to be fully redundant and to survive failures and disruptions.

At the call level, any given call was simultaneously processed by a primary (or hot) and standby processor. If the primary component failed, the standby unit instantly took over the call with no perceivable loss of service. Routine automated diagnostic and

maintenance programs in the switch software identified and corrected problems before they affected service, and a sophisticated automated system of alarms and logs keep the central office staff informed of any potential trouble areas within the switching system.

In addition, most large providers provisioned network-wide operations systems (OSs) that gave them a real-time view of all their switching systems. The OSS provided a centralized place to anticipate and preempt problems that might span multiple network nodes.

While each switch had redundancy built-in, external events are accounted for as well. For example, in the event of a power failure, switching sites and remotes are provisioned with battery back up power supply. Central offices are typically equipped with large battery arsenals and diesel generators that could power the facility as long as fuel was maintained. Trunks to a given office are designed to provide multiple routes to access other switches. In cases where switch connectivity is

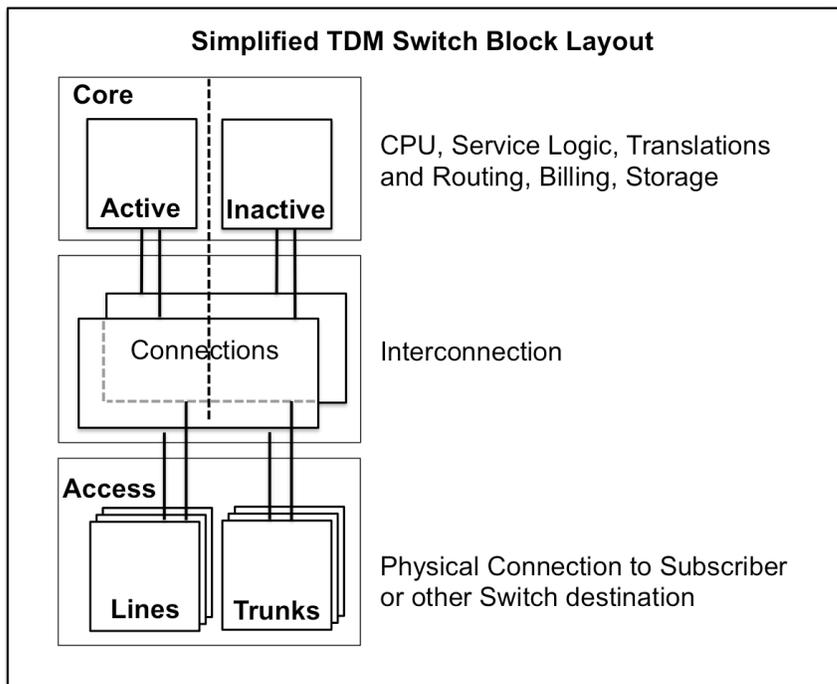


Figure 6. Simplified TDM Switch Block Layout

lost, the ability for users to place switch with emergency standalone support. Switches were originally developed to support approximately 100,000 subscribers or 50,000 trunks, depending on the office type. However, more than 80 percent of TDM offices never had more than 20,000 subscribers, thereby limiting the impact of a specific switch failure.

This view of network resiliency was built switch by switch under the requirement that each switch would be meeting the 99.999% objective and that the network would as well. Maintenance procedures were developed to upgrade hardware and software without creating an outage. That is, upgrades were performed on the inactive side of the redundant processor. If there was a problem when switching to the new software, the original load was still there and ready to perform.

However, this increased costs: TDM hardware was manufactured in relatively low volumes. Vendors developed millions of lines of software, hardened to support the same “no downtime” mindset for patching and upgrades. These vendors also developed rigorous maintenance procedures to prevent outages. In addition, TDM equipment consumed significant energy.

Access to emergency operators (Public Safety Answering Points) were ensured through a combination of switch reliability and dedicated trunks connecting to PSAP’s that weren’t impacted when other trunks were in overload.

In the late 1990s, improvements in commercial off-the-shelf (COTS) hardware and software (UNIX, Linux etc.) created an opportunity for vendors to transition their software to run on new platforms and new operating systems. Redundancy schemes began to change as well as 1:1 redundancy in hardware processing transitioned to a 1:n scheme with a single processor backing up several active processors. New types of service providers were also emerging. Voice over Internet Protocol (VoIP) was being rolled out in boutique, purpose-built applications, intended initially to bypass high toll charges being incurred on international calls. The success of these use cases allowed enterprises and carriers to leverage VoIP as well. In fact, service providers providing facilities-based VoIP via GR303¹⁹ or H.323²⁰ deployments built many of the competitive services in the US.

The migration of the PSTN over to the Next-generation IP networks that provide for voice services results in a shift from this ultra-reliable simplex network elements (“PSTN style” engineering) to what may appear as a less resilient architecture. However, geo-redundant network elements combined with protocols to detect a failed element and re-distribute the traffic (“Internet style” engineering) will result in equivalent or better resilient networks supporting basic voice communications. There have been numerous studies to evaluate the overall reliability of Next-generations Networks that are IP and or IMS-based networks. Continued competition will further incent service providers to develop and deploy the latest and best architectures to ensure more reliable and resilient networks in the future (see CableLabs whitepaper²¹).

Access

Today, the outside plant continues to be made up of twisted copper pair wire carrying both lines and trunk traffic as well as high-capacity fiber-optic cable or HFC networks that usually carry multiplexed traffic from many lines or trunks. A variety of technologies and devices are deployed today that constitute the “local loop”. Twisted copper pair, coaxial cables via a Hybrid Fiber Coax (HFC) network,

To make a traditional telephone ring, power was provided from the central office or a Remote Digital terminal (RDT). An effect of this architecture was that phone service continued to work through most power outages. This has been one of the strengths of the PSTN. In most cases, the voice network continued to work if power to the central office or the RDT (line concentrator) was maintained. Over time, line concentration equipment, signal repeaters, and a host of other outside plant equipment evolved to extend the loop length and quality of voice service over the loop.

19 <http://www.telcordia.com/services/testing/integrated-access/ss/>

20 <http://www.itu.int/rec/T-REC-H.323/en/>

21 <http://www.cablelabs.com/specification/voip-availability-and-reliability-model-for-the-packetcable-architecture/>

The next-generation of physical (non-radio) access in the last mile is based on Passive Optical Network (PON) architecture. The PON typically consists of Optical Link Termination (OLT) located at a central office exchange (1:N passive splitter/aggregator located near the access region connecting to typically 64 Optical Network Units (ONUs)). These entities are linked by fiber connections. For fiber to the curb deployment, ONU functions are located in roadside cabinets and users are connected to the network using DSL over twisted copper pair connections. The main fiber runs on a PON network that can operate at 2.5 to 10 Gbps. There are no power requirements on the fiber outside plant, however, power at the premise to drive the lasers and premise equipment is required. In the case of HFC networks power is provided for the active network elements, the electrical/optical conversion node and amplifiers in the RF coax network. Cable operators typically provide back up power systems for these network elements. Multiple services are carried over the HFC network, including VoIP using DOCSIS transport.

Interconnection

The trunking between a central office and the tandem or the interexchange carrier office was typically completed with more than one trunk and more than one route. The IXC switches were each connected to every other switch via physical trunk connections. Over time, analog trunks were replaced by optical interfaces and the network of physical trunks is being by an IP network.

Service providers have traditionally ensured the reliability of their transmission networks by configuring and engineering alternate routes for traffic. One route—the working path—between City A and City B, for instance, might be placed along a major highway while the alternate route—the protection path—might be placed along a utility right-of-way. Microwave transmission is another widely used way to provide alternate routing.

Optical deployment coupled with the (synchronous Optical Network) SONET standard—dramatically improved reliability of transmission networks through self-healing fiber ring technologies. With a bidirectional line-switched SONET ring, for instance, multiple offices were linked by pairs of fiber rings, each of which was provisioned to carry half the traffic on the system during normal operation. SONET systems often have diverse physical routes to mitigate the impact of a fiber cut due to construction or other unexpected intrusion (note, most distribution fiber rings, in the access part of the plant, are “collapsed rings” and not diverse rings). The remaining bandwidth is held in reserve for protection. In the event of a cable cut or degradation of optical signal, the transmission equipment automatically places the affected traffic on the alternate route and sends it around the ring in the opposite direction, routing around the point of failure. Since the reroute is accomplished in milliseconds, service outages are prevented.

Service providers have built extremely reliable networks with automatic failover systems. However, this is part of the circuit switched network that had at least 100% spare capacity in place.

Next Generation or IMS Network Resiliency

Technology advancements in data networks, and hardware and software platforms have enabled higher capacity, high-quality multiservice networks to replace those of a single purpose nature. This evolution has enabled a single converged edge network element to support a large number of ports across multiple technologies, including LTE, Wi-Fi and FTTH.

The figures below show the evolution of data networks in the wireless, wireline and cable technology segments.

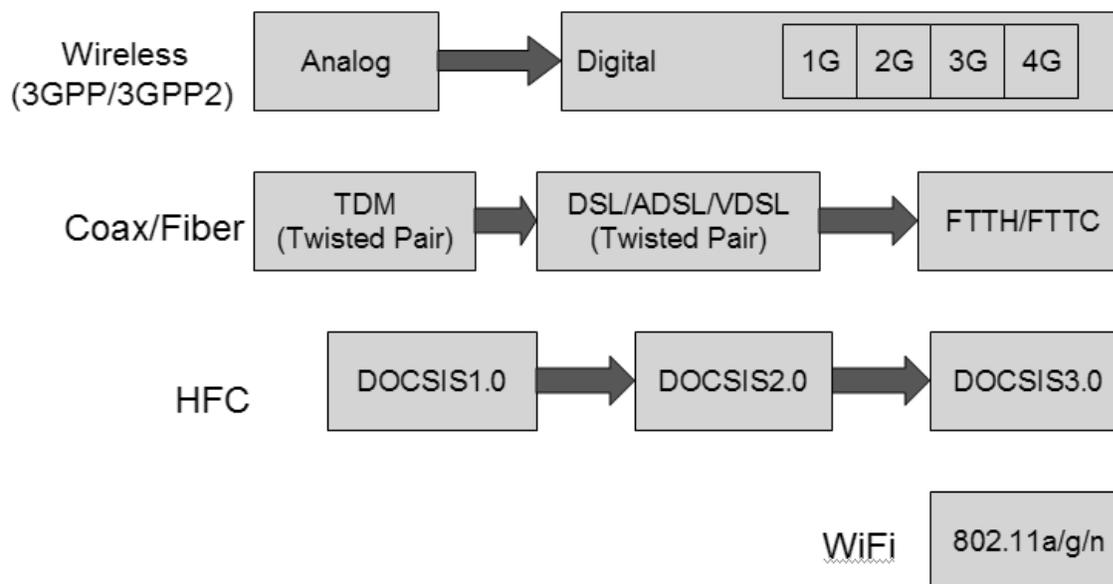


Figure 7. Access Technology Transition

A similar evolution has occurred for voice networks. Circuit-switched networks are giving way to packet-switched VoIP networks in wireline and cable segments. The Radio Access Network (RAN) interface is already packetized, while the wireless networks are now adopting a packet-switched core network based on IMS architecture. The first generation VoIP networks such as PacketCable1.0 and DSL/ADSL networks supported a soft-switch architecture and required switches to be deployed in network locations such as central offices, albeit fewer locations due to capacity, and leveraged cost and efficiency advantages afforded by all-IP networks.

Over its history the cable industry has deployed three different network architectures to offer residential telephone services:

1. Proprietary Circuit-Switched TDM based digital voice
2. PacketCable™ 1.x – Network-Based Call Signaling (NCS) based VoIP
3. PacketCable™ 2.0/IMS – Session Initiation Protocol (SIP) based VoIP

As the cable industry first began offering residential telephone service, a small number of cable operators deployed proprietary solutions from Arris and Tellabs, such as the Arris Cornerstone® TDM, circuit-switched architecture²², which used traditional 5E/DMS 500 class switches and network power. The voice signal was carried in digital form over the cable HFC network between the head-end and the network interface module on the side of the residence, which converted the signal to/from analog form over twisted pairs into the residence. This infrastructure is being decommissioned in favor of the more cost-effective, vendor-supported, VoIP solutions based on soft-switches using NCS and SIP signaling.

22 "Trials of the ARRIS Cornerstone® Voice system began in late 1995, and commercial deployment began in 1996." Reference: <http://www.arrisi.com/solutions/voice/index.asp>

The figure below shows the evolution of wireline, wireless and cable networks to support voice over the past decade.

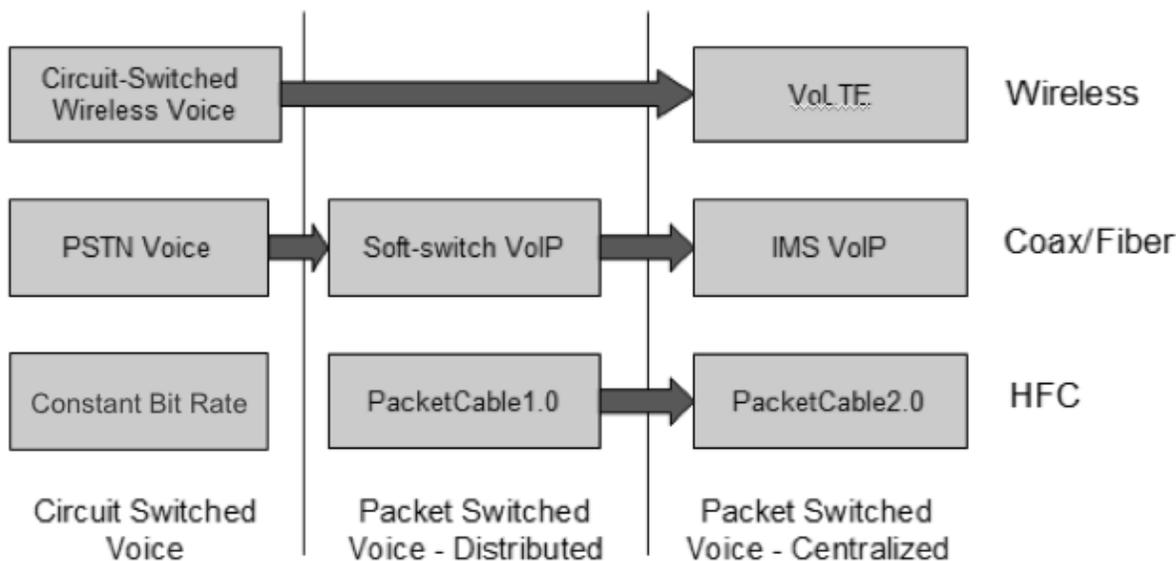


Figure 8. Voice Technology Transitions

The focus for the next-generation VoIP networks including PacketCable2.0, IMS VoIP and VoLTE technologies has primarily been on minimizing total cost of ownership by reducing the total number of soft-switches and voice applications servers in the network. Modern day IMS networks can typically support millions of voice subscribers on a given instance of the network at a particular site location. Therefore, it is not uncommon to find packet-core, IMS or PacketCable networks deployed at a handful of site locations (normally less than 10) supporting millions of voice and data services.

While increases in capacity have enabled core deployments into fewer locations, the resiliency risk is also concentrated into fewer locations, but with larger impacts. To mitigate this, the former practice of co-locating both the active and the backup processors in a single location is giving way to splitting the active and redundant processors into separate physical locations, connected via an IP network.

When a network or node at a given site fails in next-generation networks, a large number of ports, sessions or subscribers currently supported at the site are impacted. The service of these ports, sessions or subscribers needs to be rerouted to other sites to implement network resiliency. Furthermore, if a site or network node recovers, a failback mechanism needs to be implemented to resume site operation.

Most modern data switching and data routing platforms (for VoIP and data) manage failures using software-based algorithms. The good news is that such algorithms can be designed and deployed to address numerous scenarios including processor failures, network component failures, network connectivity failures, site failures, etc. Most network equipment vendors also reuse such failover mechanisms to implement zero-down-time updates of network components. The alternative is there are numerous considerations that can complicate the design and implementation, thereby affecting robustness of the overall network. The techniques described here include various cost, performance and robustness tradeoffs that next-generation communication networks providers must consider.

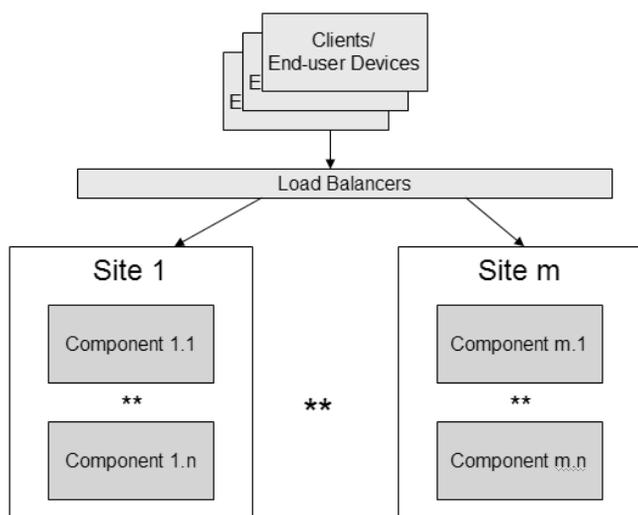


Figure 9. Generic Multi-site Architecture for Communications Systems

Figure 9 shows an abstracted architecture that can be applied to most next-generation communication systems across wireless, wire-line and cable segments. Later sections discuss specific examples of these networks for 4G LTE Packet Core and IMS VoIP networks.

Active-Active vs. Active-Standby

Two design paradigms are popular for reallocating workload upon failure: Active-Active and Active-Standby. In the Active-Active paradigm, all sites and network components manage traffic under normal working conditions. When one of the network components or site experiences failure, its workload is either allocated to another dedicated active element (called 1:1 redundancy) or spread across multiple active elements (called 1+N redundancy).

In the Active-Standby paradigm, standby sites or network components are idle under normal working conditions and take on workload upon the failure of its designated primary site/network components. There are various cost, performance and robustness tradeoffs in selecting Active-Active vs. Active-Standby configurations that this paper will not address. It is also possible to have certain network component types exhibit Active-Active redundancy while other component types exhibit Active-Standby, but it may complicate failover and failback design in such cases.

- Abrupt shift of workloads: When a network or node at a given site fails, a large number of ports, sessions or subscribers currently supported by the node have to be moved to another node. This has to be executed in such a way that the new target site(s) do not get overloaded due to abrupt shift in workloads that cause undesirable side effects. Throttling mechanisms such as exponential back-off or staggered requests need to be implemented to minimize errors in rebalancing the workload. Furthermore, if and when the site or network node recovers, failback mechanisms used to resume site operation need to take similar precautions against abrupt reallocation of workloads.
- Rebalancing network load to minimize transport hops, latency and cost: When workloads have to be reallocated upon failure, the network components and sites that will take on the new workload can be determined on a fine-grain level of port, session or subscriber basis or at a large-grain level (ex. Active-Standby paradigm, where the entire active network component's workload is transferred to the standby network component). Furthermore, the new network component/site that takes on the workload can be determined statically at design/configuration time or dynamically at time of failure. In making these design choices for rebalancing network load, careful attention must be paid to both technical and business requirements. Voice and data communications requires transport of voice and data packets from the customer device or terminal to the network components that service the particular session from the customer device. When rebalancing the workload as part of a failover, network components must be selected that optimize the number of transport hops, end-to-end latency and cost of transport.
- Toggling or fluttering: Time constants should be built for failback to avoid rapid sequence of failovers and failbacks that cause congestion problems, prolonged customer downtime and decreased overall robustness of the system. Time constants are rarely applied during failover to optimize service availability upon failure.
- Perceived customer experience and downtime: When network components and sites fail for various reasons, it may temporarily affect service and the customer experience. The total time from when the service becomes unavailable to when service is resumed after a failover is an important metric for measuring service availability. However, failover cannot be instantaneous for all ports, sessions or subscribers due to the "abrupt shift of workloads" issue described

above. Important voice and data services (such as emergency services) will have to be given priority over other services. Such requirements are typically enforced by individual customers, such as a public safety agency evaluating a VoIP and data network, and there are no industry-wide accepted best practices on how to prioritize downtime during failover for critical services. Important voice and data services (such as emergency services) will have to be given priority over other services. Such requirements are typically enforced by individual customers, such as a public safety agency evaluating a VoIP and data network, and there are no industry-wide accepted best practices on how to prioritize downtime during failover for critical services.

- Ambiguous designation of master node: Network connectivity failures in geo-redundant networks may present tricky situations where multiple network components may designate themselves as responsible for serving a single port, session or subscriber. This may be a transient situation where other synchronization mechanisms will correct the situation in a short period of time. Alternately, it may be a persistent situation during which the ownership of port, session or subscriber becomes ambiguous and can cause subsequent errors and service downtime at the port, session or subscriber level, often requiring other manual intervention to correct the situation. Design consideration should be given to avoid persistent ambiguities in ownership of user ports, sessions or subscribers, whereas transient ambiguities may be acceptable in favor of a simpler failover design of the end-to-end system.
- Large number of corner-cases: As described above, software-based failover design of next-generation communications systems can become fairly complicated very quickly and there are multiple design tradeoffs in relation to costs, performance and robustness of the system. As a result there is no one “ideal design for all communications networks.” Best practices should be followed based on accepted industry guidelines. This makes it challenging to quantify the robustness of communication systems and to test for all possible catastrophic failure scenarios. Most robustness testing frameworks and certification tests are vendor-specific. Given the varied number of ways in which next-generation networks can fail, it becomes difficult to validate high-level robustness requirements such as five 9’s availability. Consequently, service providers, government and public safety organizations are left to impose their own detailed robustness requirements in order to ensure compliance and positive user experiences.

As of 2013, there are approximated 35 million interconnected VoIP subscribers in service on various networks around the country and experience from deployment of these networks has shown that they perform well.

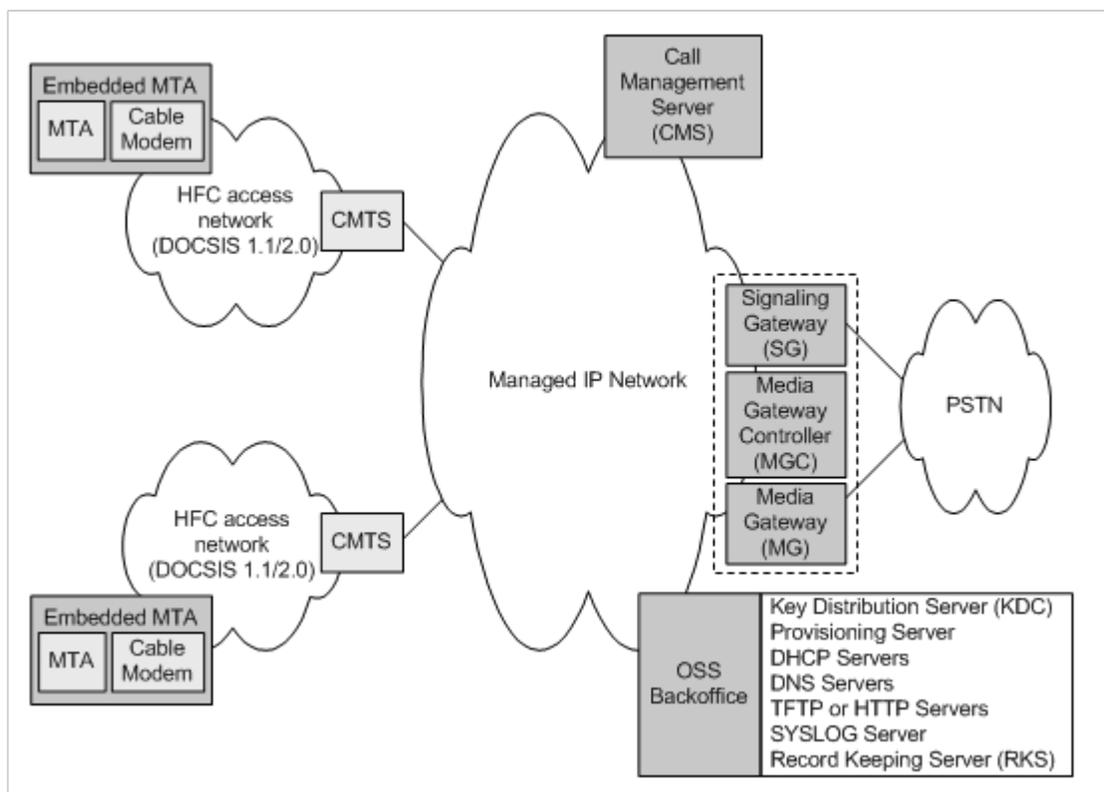


Figure 10. PacketCable 1.x Reference Architecture

PacketCable 1.x Architecture:

As shown in Figure 10, a PacketCable 1.x network is built around a centralized architecture in which the application logic plus the non-application-specific support functions, such as user authentication, service authorization and message routing, are all controlled by the Call Management Server (CMS). This application-centric approach works well for residential telephony, a well-defined service with simple endpoint devices.

In this architecture, the DOCSIS HFC access network provides high-speed, reliable, and secure transport between the customer premise and the cable headend. The access network provides DOCSIS capabilities, including Quality of Service. The DOCSIS HFC access network includes the following functional components: the Cable Modem (CM), the Multimedia Terminal Adapter (MTA), and the Cable Modem Termination System (CMTS).

The managed IP network serves several functions. First, it provides interconnection between the basic PacketCable functional components that are responsible for signaling, media, provisioning, and the establishment of Quality of Service on the access network. In addition, the managed IP network provides long-haul IP connectivity between other Managed IP and DOCSIS HFC networks. The Managed IP network includes the following functional components:

- Call Management Server (CMS) – The Call Management Server, or soft-switch, provides call control and signaling related services for the MTA, CMTS, and PSTN gateways in the PacketCable network. The CMS is a trusted network element that resides on the managed IP portion of the PacketCable network. The CMS consists of the Call Agent, the control component of the CMS that is responsible for providing signaling services using the NCS protocol to the MTA and the Gate Controller (CMS/GC) a logical QoS management component within the CMS that coordinates all Quality of Service authorization and control.

- There are several Operational Support System (OSS) back-office servers:
 - Key Distribution Server (KDS)
 - Provisioning Server
 - DHCP Servers
 - DNS Servers
 - TFTP or HTTP Servers
 - SYSLOG Server
 - Record Keeping Server (RKS)
- Signaling Gateway (SG) – The Signaling Gateway provides a signaling interconnection function between the PSTN SS7 signaling network and the IP network.
- Media Gateway (MG) – The Media Gateway terminates the bearer paths and transcodes media between the PSTN and IP network. The Media Gateway provides bearer connections between the PSTN and the PacketCable IP network. Each bearer is represented as an endpoint, and the MGC instructs the MG to set-up and control media connections to other endpoints on the PacketCable network. The MGC also instructs the MG to detect and generate events and signals relevant to the call state known to the MGC.
- Media Gateway Controller (MGC) – The Media Gateway Controller is a logical signaling management component used to control PSTN Media Gateways. The MGC maintains the call state and controls the overall behavior of the PSTN gateway.

PacketCable 1.x based systems represent the largest cable deployment of VoIP residential services. CableLabs has certified or qualified 116 eMTA products, 12 CMS products, 7 MG products, and 4 MGC products to date for PacketCable 1.x compliance.

Because the PacketCable 1.x architecture is built around a centralized architecture, resiliency of the VoIP system is dependent on the resiliency of the components of the architecture. Failover is often an aspect of the implementation of these components, rather than a feature of the network itself.

CableLabs published the “VoIP Availability and Reliability Model for the PacketCable™ Architecture”²³ technical report in November 2000. This technical report directly addressed the issue of availability using detailed end-to-end network models for both

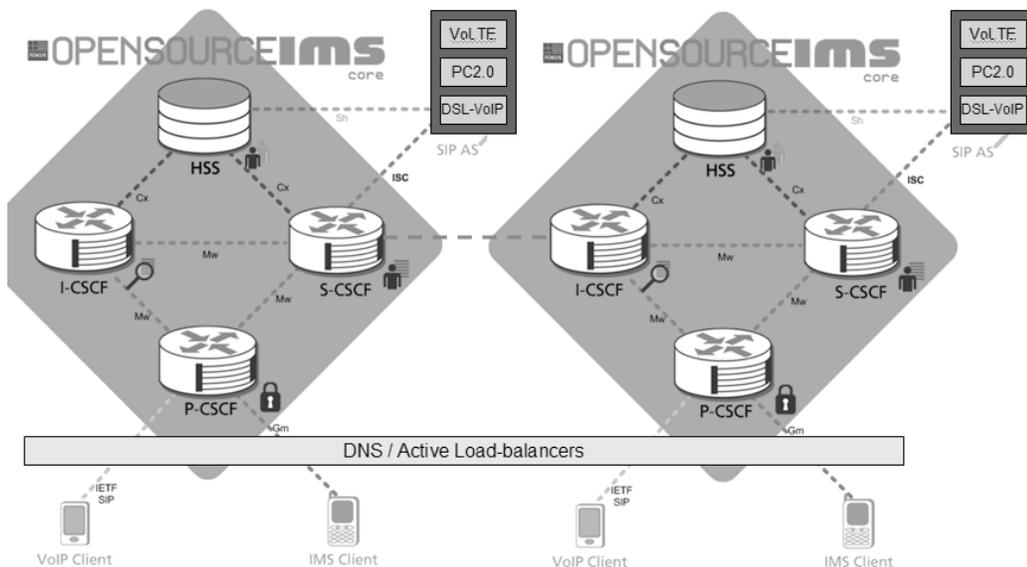


Figure 11. OpenSource IMS Architecture

23 “VoIP Availability and Reliability Model for the PacketCable™ Architecture”, Cable Television Laboratories, Inc., November 28, 2000.

the PacketCable 1.x and PSTN environments. The end-to-end availability objective of the PSTN network, based upon Telcordia documents, was 99.94 percent, with individual elements having the better-known value of 99.999 percent. The same end-to-end availability objective of 99.94 percent was set and achieved for the end-to-end PacketCable network.

Resilience in IMS VoIP network

IMS is a layered architecture that provides VoIP network capabilities across wireline (DSL-VoIP), Cable (PacketCable2.0) and 4G wireless (VoLTE) technologies. The layered architecture enables separation of concerns (switching vs. VoIP application vs. subscriber database etc.). This however results in multiple logical node types and adds heterogeneity to the network that increases the complexity of geo-redundant failover design. Figure 11 below shows a two-site geo-redundant IMS network that can support cable, wireless and wireline VoIP service. The major architectural difference across these three technology segments is the use of the appropriate Session Initiation Protocol Application Server (SIP AS) to address the technology specific requirements. IMS networks are typically implemented as Active-Active 1+N geo-redundant networks with DNS-based load-balancing and failure recovery with preconfigured primary and secondary sites to optimize transport costs and latency on signaling plane. Exponential or random back-off is often implemented when re-registering IMS clients upon a network component/site failure to avoid abrupt shift of workload as discussed above. A typical IMS site may be managing more than a million subscribers and moving them all to other sites upon a site and or node failure with back-off, may take 10s of minutes (depending on if the network is over-provisioned and other scalability considerations) and this would mean downtime in the order of tens of minutes for the

affected subscribers. This has real consequences for downtime and emergency services that need to be invoked during the failover period.

Resiliency in 4G LTE Core networks

LTE is a major step forward in mobile radio communications, and was introduced in 3GPP Release 8.

The packet core network is also evolving to a new flat IP-based multi-access core network. This new Evolved Packet Core (EPC) network is designed to optimize network performance, improve cost-efficiency and facilitate the uptake of mass-market multimedia services. Figure 12 shows the reference LTE architecture.

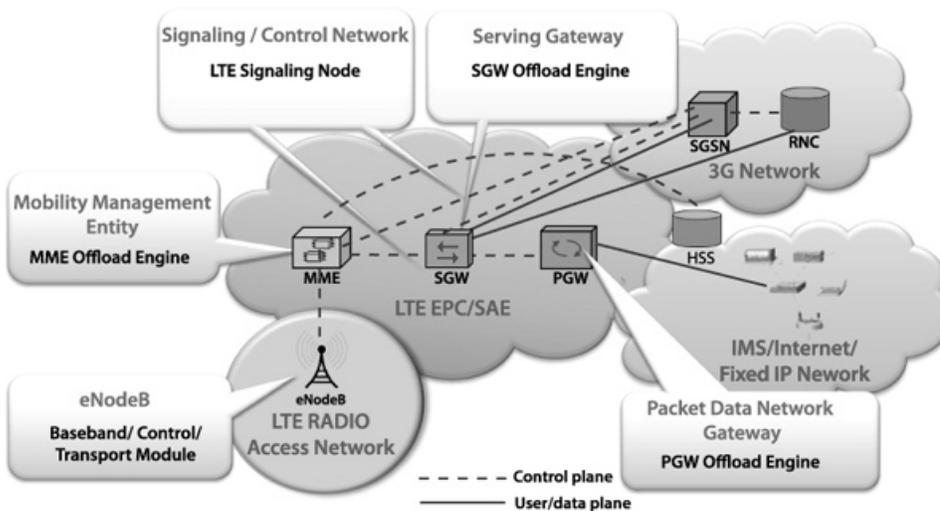


Figure 12. Voice Over LTE Architecture

eNodeB is the LTE radio base station. MME supports mobility management, SGW is the signaling plane gateway and PGW is the user plane gateway. The MME, SGW and PGM combined are referred to as the EPC.

The LTE base stations are connected to the Packet Gateway using the Core Network-RAN interface, S1. Existing 3GPP (GSM and WCDMA/HSPA) and 3GPP2 (CDMA2000 1xRTT, EV-DO) systems are integrated with the EPC network through standardized interfaces providing optimized mobility with LTE. For 3GPP systems this means a signaling interface between the existing Serving GPRS Support Node (SGSN) to the Mobility Management Entity (MME) in the EPC network; for 3GPP2 a control signaling interface between the CDMA RAN and the MME. This integration will support both dual and single radio handover, allowing for flexible migration to LTE.

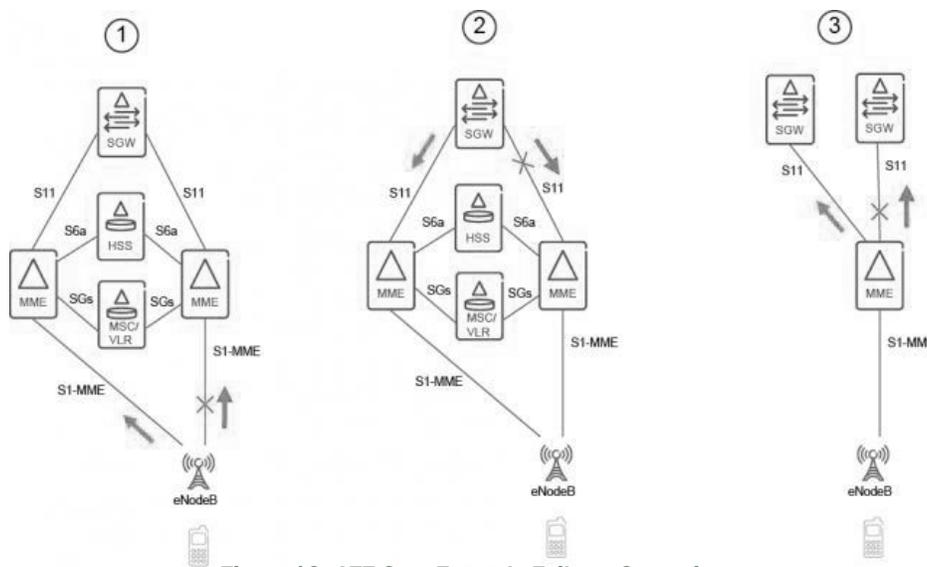


Figure 13. LTE Core Example Failover Scenarios

The concept of geo-redundant pools in the LTE network can be used to provide resiliency against MME and SGW failures, as well as link failures on the S1-MME and S11 interfaces, by preservation and service continuity of sessions. The basic idea is to duplicate UE contexts in a pool environment, to be used by MMEs in failure scenarios. The failover scenarios in Figure 13 are supported in the architecture:

1. An eNodeB cannot connect to the serving MME, due to MME or S1-MME failure, and selects a new MME. A UE with active PDN connections in the eNodeB experiences session continuity, since the new MME can reestablish the UE context.
2. An SGW cannot connect to the serving MME, due to MME or S11 failure, and Downlink Data Notifications with IMSI are sent to a new MME. By retrieving the UE context replica, it is possible to page the UE in its last TAI list area and at the subsequent Service Request to reconnect to an SGW.
3. An MME cannot connect to the serving SGW, due to SGW or S11 failure, and the MME relocates the PDN connections to another SGW.

A geo-redundant pool provides the following capabilities under the above failure conditions:

- Virtually no service impact on end users, even in outage scenarios
- Assures extremely high availability of services to end users and business partners. The precise operation of geo-redundant pool is vendor specific and beyond the scope of the current document.

Future Evolution of Communications Networks

This section discusses major trends occurring in the IT industry that will have significant impact on how communication networks of the future will evolve. It does not focus necessarily on resiliency issues in these future communications networks since these concepts are in a maturation phase.

Network Resiliency and Emerging Technologies

At an increasingly rapid pace, new trends emerge forcing the telecommunication's industry to re-think its networking paradigms. This especially has held true recently with three significant trends emerging: Converged Packet Optical, Software Defined Networking (SDN) plus Network Function Virtualization (NFV) and Cloud Computing.

Packet Optical Convergence

The first significant trend is Packet Optical convergence. Historically, telecommunications infrastructure has been viewed not as one network, but a grouping of networks each intended to address a specific technical need - be it wireline or wireless; or voice video or data, each riding over some underlying optical infrastructure. As the evolution to an all IP networking infrastructure reached full maturity, a transition to a network of network's approach solidified itself as the most common topology. Figure 14 highlights this concept showing where IP packets are transported from Point A to Point B and function as an overlay to an optical transport infrastructure.

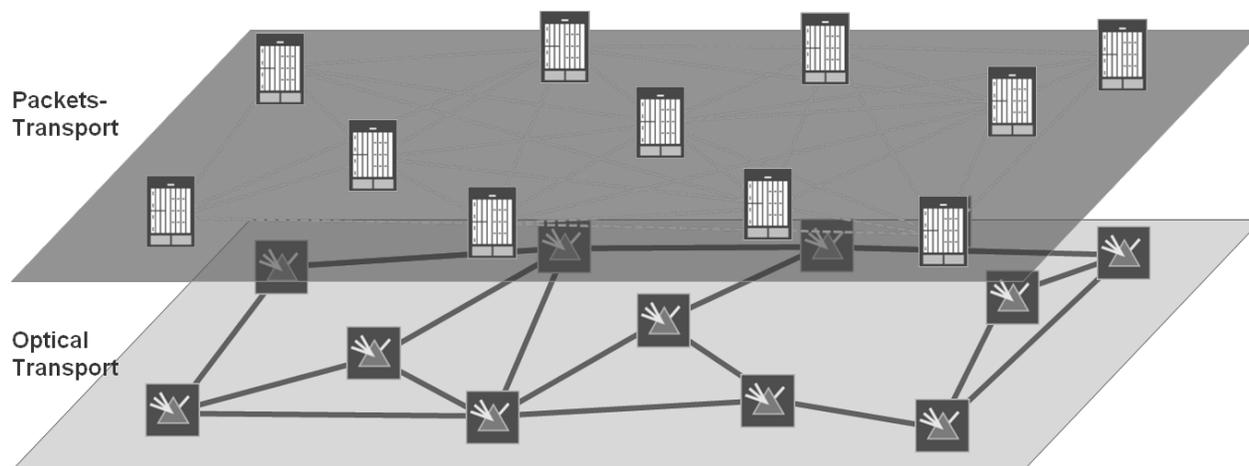


Figure 14. Packet Optical Convergence

This stacked network was sufficient as long as business and residential demand for IP connectivity services increased and the average retail prices was growing or at minimum flat. As with all maturing markets, the last two years have seen demand for IP transport services flatten and the competitive selling pressures have shifted the marketplace profitability curve impacting the financial bottom line.

In response, customers and equipment providers have started embracing an integrated Packet-Optical strategy, the ultimate goal being to eliminate the duplicative nature of the two networks and therefore converge them by moving optical capabilities into IP routers and switches. Obviously, the reverse can happen as well where IP routing and switching capabilities are moved into optical transport systems. In either case, the ramifications are significant, the economic and IT simplification benefits brought about, clear.



Figure 15. Packet-Optical Convergence

Of greater interest for this working group, however, are the ramifications to network resiliency. In a two-layer network (IP and optical), complexity is high as each requires their own traffic engineering and traffic planning processes. On the other hand, a single, converged network is intended to optimize both infrastructure costs and traffic optimization. Figure 16 suggests a simpler network resiliency proposition and the associated benefits derived when adding standard protocols and intended “map” traffic between these disparate networks. Using the combination of Dense Wave Division Multiplexing (DWDM) optical network and IP Routed paths, IP traffic can now be tunneled in colored wavelengths each with their own quality of experience. Previously duplicative operations and maintenance processes can now be either simplified if not eliminated and the potential programmability and resiliency of the network greatly improved.

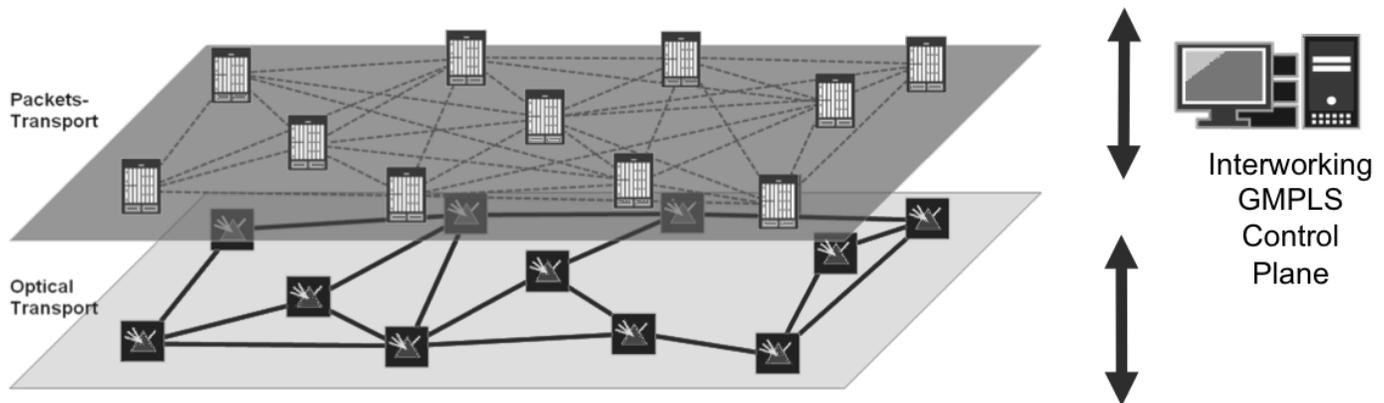


Figure 16. Converged IP and Optical Network

Software Defined Networking and Network Functions Virtualization

The second major telecommunication's revolution has been a parallel yet probably more critical trend intended to facilitate a world of network programmability known as Software Defined Networking (SDN). In tandem with SDN, Network Functions Virtualization (NFV) is an initiative to leverage the extensive benefits of software virtualization. SDN and NFV together introduce an entirely new network operations and maintenance paradigm where the Control Plane and the Data or Forwarding Plane are decoupled and a centralized and simplified management of IP network services deployed. Figure 17 depicts SDN and NFV.

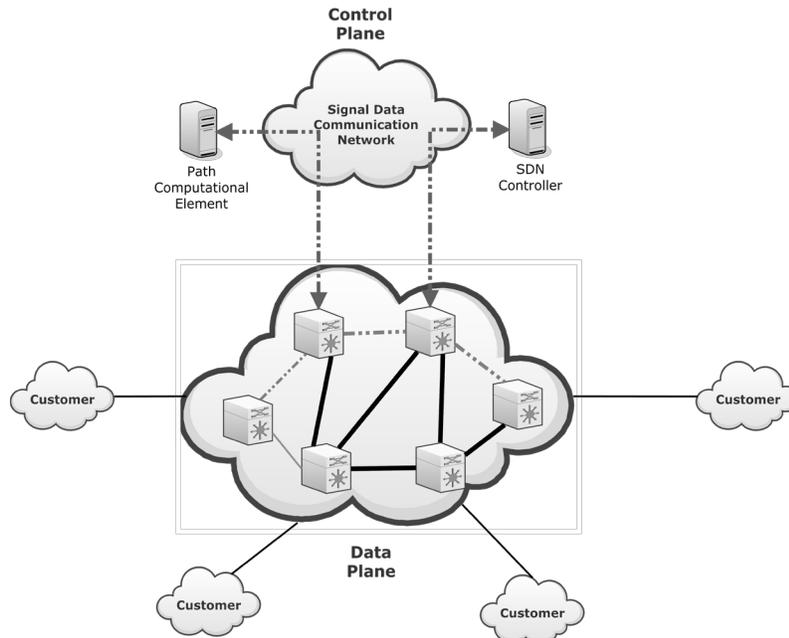


Figure 17. Software Defined Networking

To speed the adoption of SDN and NFV, the telecommunications industry has seen the rise of numerous standards bodies and committees such as the Open Networking Foundation intending to define, review or refine SDN concepts. Additionally, existing standards organizations such as the Alliance for Telecommunications Industry Solutions (ATIS) and the European Telecommunications Standards Institute (ETSI) are defining new network service specifications for virtualized network functions. However, broad standards initiatives alone do not ensure mass adoption, economics are also a critical enabler and here SDN and NFV are both making significant impact as pointed out by Strategy Analytics: “In addition, SNS Research recently forecast that SDN and NFV investments can save wireless and wireline service providers up to \$32 billion in annual capex by 2020.”** More importantly, Figure 18 points to an accelerating pace of economic impact and thereby equivalent speed of adoption.

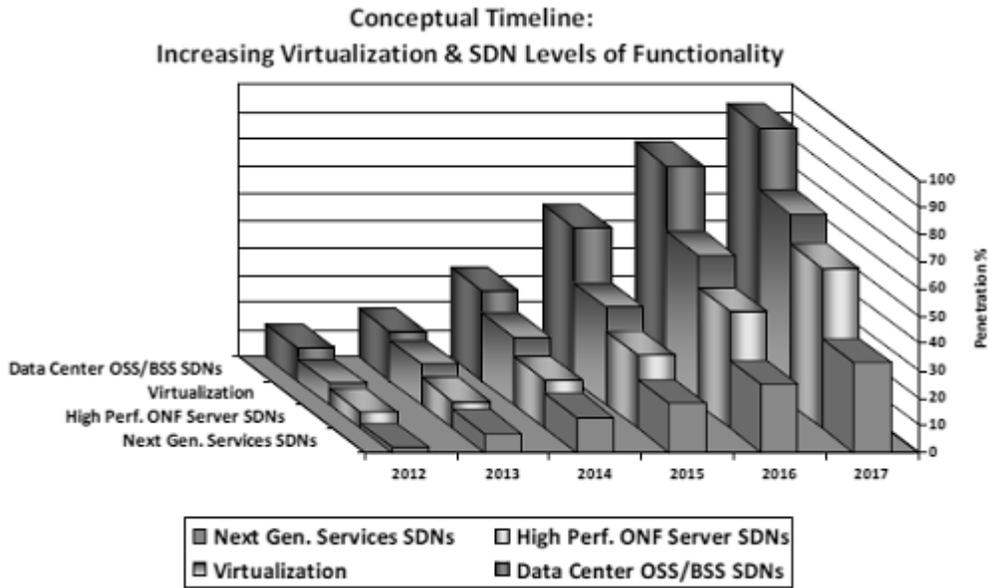


Figure 18. Increased Virtualization and SDN Functionality²⁴

In Figure 19 we see the ETSI (with significant input from ATIS, ETSI organizational partner) Network Functions Virtualization²⁵ block architectural framework and a number of critical components as required to enable the programmability of tomorrow’s telecommunications infrastructure. Business and operational support system integration combined with workflow orchestration will, over time, facilitate the transition from today’s present mode of operations to that of the future and a fully integrated IT and IP network will seamlessly function together, enabling a proactive, programmable network.

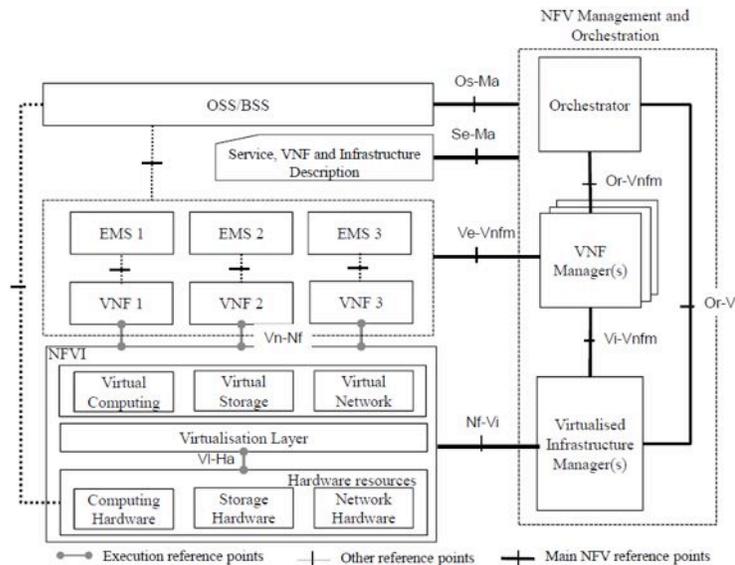


Figure 4: NfV reference architectural framework

Figure 19. ETSI Network Function Virtualization

24 **(*Source Strategy Analytics Wireless Networks and Platforms*) <http://www.fiercewireless.com/tech/story/sdn-will-be-2014s-biggest-network-trend-says-strategy-analytics/2013-11-14>

25 <http://www.etsi.org/technologies-clusters/technologies/nfv>

Cloud-based Communications Architecture

Cloud Computing is the third major technology trend, slightly more mature and now in wide adoption. Open Source organizations such as Open Daylight²⁶ and OpenStack²⁷ are defining API and Cloud Computing specifications intended to simplify the integration challenges in an infrastructure where compute, storage and data center networking are all readily accessible and rapidly provisioned. New automation workflows can now be created to fully provision blocks of Infrastructure (Compute, Storage, Network) allowing organizations to turn on or off virtualized network functions at a moment's notice. As a result, network management and analytics processing workloads can be proactively moved to IP traffic and programmatically re-routed where natural disasters are predictive such as Hurricane Sandy.

Resiliency in Cloud-based Communication Systems

Communications services providers are investing in cloud infrastructure such as IaaS (Infrastructure as a Service) to host their own communications service networks and to host back-office and front office applications for enterprise customers. The former investments are targeted to improve total cost of ownership and time-to-market on new communications services offerings. IaaS enables rapid deployment of applications (and more efficient use of hardware resources) because IaaS offers a pool of virtual machines with a specific set of requested compute, storage, memory and networking resources. This provides a level of detachment of communications service applications from physical servers enabling better hardware utilization, easier configuration and management of the communications service applications. Applications can also take advantage of auto-scaling features called "elasticity" where new virtual machines are created/destroyed and dynamically based on hitting certain thresholds of footprint for compute, memory and storage resources being consumed by applications.

Most communications services applications are being "ported" to run on virtual machines to afford the better cost-of-ownership economics. As of this writing most LTE vendors are porting their EPC to run on VMs and most IMS VoIP vendors are porting their IMS components to run on NFV architectures. Major progress by the vendor community is expected to be announced at major trade shows starting in February 2014.

Figure 20 shows example architecture for a cloud-based 1+1 Active-Active geo-redundant IMS VoIP network where the various components are running on virtualized IaaS infrastructure. The access-network and end user device are oblivious to whether the network components are running on bare-metal or virtual machines. Also, all the design tradeoffs and considerations mentioned in earlier sections of this chapter still apply to NFV-based implementations of communications networks because these design considerations apply at the application level (and not at the platform level). However, there are a few implications specific to NFV-based implementations of communications networks that is worth highlighting in this paper:

26 <http://www.opendaylight.org>

27 <http://www.openstack.org>

1. Centralized control plane and decentralized user plane: Centralized communications networks running on VMs can terminate the control plane for most data and voice communication services but the user plane may need to be closer to the edge of access (due to higher volumes of data in the user plane relative to the control plane). Figure 20 shows how the first access network can use the user plane collocated with the cloud data centers but the second access network needs a geo-redundant pair of data centers hosting the user plane closer to the access network. Latency, performance, cost and robustness are considerations for either collocating in or separating out the user plane from a cloud-based communications network.
2. An additional layer of failure: We have previously discussed processor failures, server failures, network component failures and site failures in the paper. The first three types of failures normally affect a logical network function mapped to that hardware and the site failure affects all the logical network functions at a given site. With the introduction of VMs, we increase the type of failures. If a server is hosting VMs for a few different types of network functions (say a PGW and MME), failure of the server will result in the failure of VMs, which result in failure of all the (potentially heterogeneous set of) applications running on those VMs. So a single hardware failure can cause failure of a combination of logical elements in a virtual environment. Testing for resiliency for NFV-based communications services should capture such failure scenarios to ensure proper function of the end-to-end network.
3. Most IaaS platforms provide built-in mechanisms for restarting VMs that were running on hardware that has failed. NFV-based network functions must utilize the underlying IaaS-based resiliency mechanisms to provide network function-level resiliency.
4. When NFV evolves in the future and network functions support elasticity, capacity planning and management should become significantly easier in communication networks.

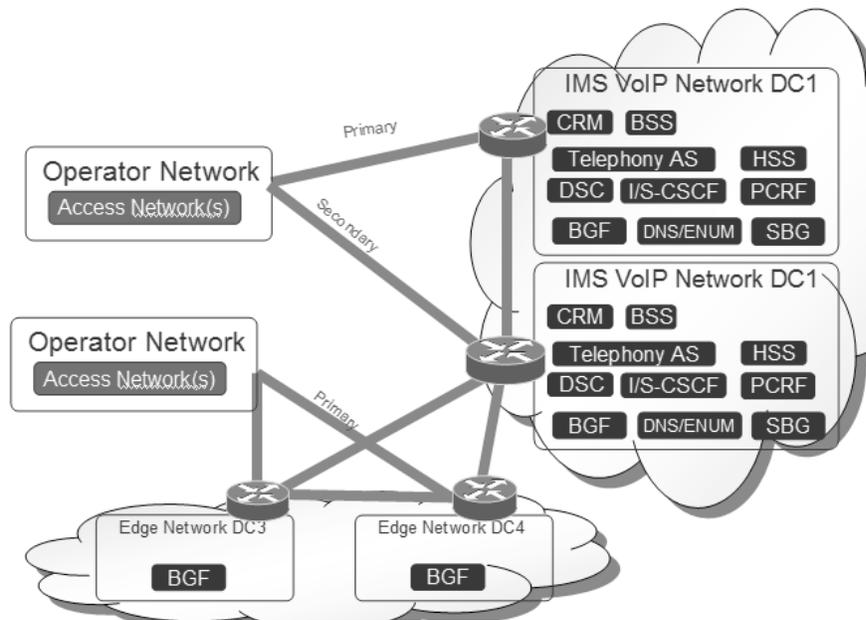


Figure 20. IMS in the Cloud: Example Architecture

Security in Cloud-based Communication Systems

The issue of cyber security for cloud-based communications systems grows in importance every day. For the purposes of the resiliency working group and this paper, we largely refer the reader to the white paper produced by the Cyber Security Working Group led by Paul Steinberg.

However, we will add that there is significant energy by communications providers to adopt cloud-based architectures, particularly by new entrants, but more and more as the target network architecture deployed by traditional service providers. The architecture will be built by the service providers themselves and by private, third-party providers who offer an infrastructure as a service. This outsourcing of the platform creates additional risks, and consequently additional responsibility to plan for deployments that protect the function of the network and protects the private information of end users.

Resiliency in M2M networks

Machine-to-Machine (M2M) networks are becoming an important aspect of communications networks given the proliferation of “Internet of things” (IoT). Most wireless operators offering M2M services include SIM (or soft-SIM) based M2M devices that are managed and monitored by operator network and the data collected from these devices and passed on to higher order IT and M2M analytics systems. M2M devices in the field can have embedded sensors or they can act like a hub for a handful of sensors that communicate using Zigbee, Wi-Fi or other near-range wireless communication protocols. M2M networks will play a vital role in the future for public safety, emergency, first response scenarios and should be resilient against failures at processor, server, network component and site levels.

Figure 21 shows the typical high-level architecture for a 1+1 Active-Active geo-redundant M2M connectivity network that supports configuration, life cycle management and health monitoring of SIM-based M2M devices and funnels the data from the M2M devices into vertical enterprise IT infrastructure. Most of the design principles and tradeoffs discussed in the earlier sections will apply to such a network.

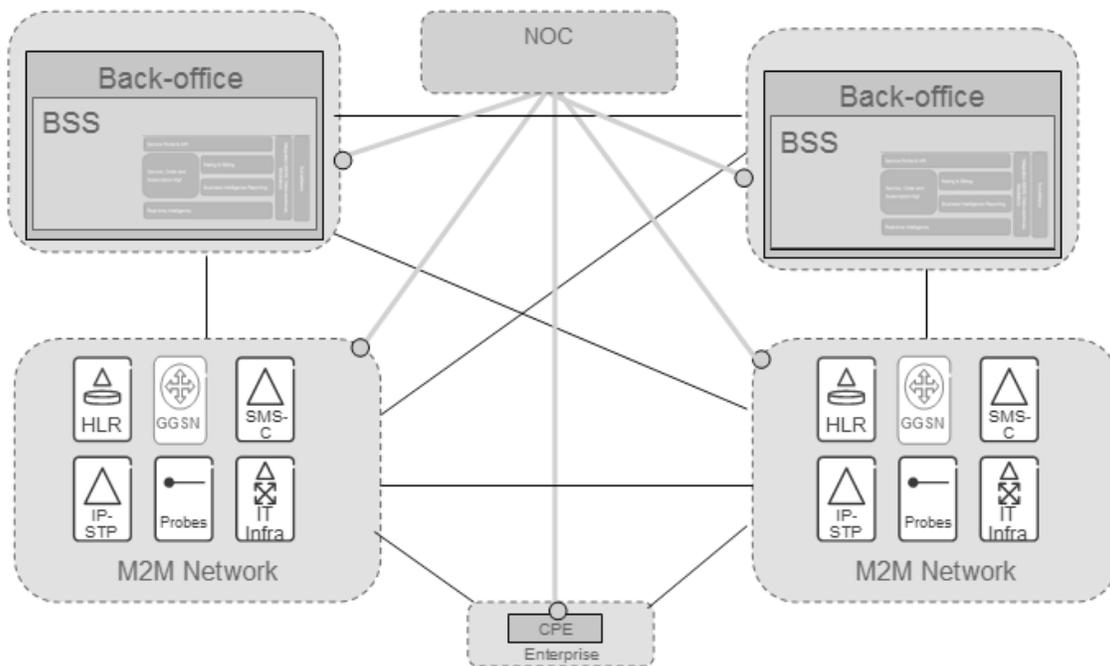


Figure 21. M2M connection platform reference architecture

WebRTC

WebRTC is an IETF and W3C standard for in-browser peer-to-peer voice and video communications and specifies the data plane behavior that is standardized across all browser types that support WebRTC. The control plane implementation is not standardized but mechanisms such as XMPP and SIP can be used with vendors providing gateways as needed. While some browser makers have been aggressively driving the WebRTC standardization, others have not converged on the standard. The resiliency of communications over a WebRTC client will depend heavily on the characteristics of the browser.

To summarize, while every five years the telecommunications industry undergoes dramatic changes, now more than ever three major trends are presenting themselves and their impact will be significant to the changing landscape of network resiliency. More importantly, these new trends in the form of converged Packet Optical, Software Defined Networking plus Network Functions Virtualization and Cloud Computing are forcing the telecommunication's industry to re-think its networking paradigms. Of significance will be the industry's ability to proactively move network function workloads, immediately steering IP traffic accordingly, especially where imminent natural disasters are a factor.

Standards and Industry Advocacy

There are a number of groups working to ensure that the network developments and directions continue to function in a resilient manner. For example, ATIS Network Reliability Steering Committee (NRSC) addresses the topic and produces requirements, reports and best practices for service providers. As an organizational partner with ETSI, ATIS is actively participating with ETSI to shape the NFV architecture proposals. ²⁸

²⁸ <http://www.atis.org/bestpractices>

DISASTER PLANNING AND RESPONSE

The Federal Emergency Management Agency (FEMA) suggests that there are three major phases in disaster planning: planning, preparation and mitigation.²⁹

In the case of a communications network, the very engineering of the network and all of its connections and components must account for network resiliency. A well-designed network and a well-maintained network are fundamental to performing well during a crisis. The planning phase would also include the preparation of emergency plans and assembling equipment and personnel plans for a coordinated response. The mitigation phase would include the actual disaster recovery response along with analysis and determining improvements that could have avoided the failure or could have shortened the duration of the event.

By the time a service disruption occurs in the public communications network, service providers have been consistently preparing equipment and staff to maintain service during the event and to respond and recover in outage situations.

Before an event, the service provider designs the network to be resilient, following acknowledged best practices and company procedures. Additionally routine maintenance, monitoring and surveillance are performed. Key data including billing, translations and routing is typically backed up to a different facility so that necessary information is available to restore service. Additionally, service providers have worked to ensure that no single failure will create an outage.

As part of their emergency service plans, each service provider builds contingency plans for powering equipment, training employees and maintaining service. Some of these steps, such as monitoring network performance, providing battery back up and generator back up for critical infrastructure and proactive maintenance routine for testing of batteries and generators, generally create the likelihood that service will be maintained through many events, particularly weather related.

When an event occurs, service providers have plans in place to deploy people and equipment to affected areas and direct the recovery of service. Over time, portable command centers, temporary portable cellular towers and more are deployed to provide service for first responders and citizens to have a means of communications.

During an event, coordination between government authorities and other utility companies, particularly power providers, is critical to recovery of communications infrastructure.

While this is happening in the network, it is not as clear that consumers and businesses are aware that their own personal communications now depend on commercial power in ways not previously understood. Fixed VoIP providers typically do not provide batteries to power a terminal adapter during a power outage. While most US households have a wireless connection, typical device battery life is relatively short. Without a power supply, consumers often turn to their personal vehicles to charge mobile devices.

While we will discuss the consumer issues in more detail, it is clear that the commercial power will likely gate the communications of a household during an emergency.

²⁹ <http://www.fema.gov/plan-prepare-mitigate>

The following are examples from AT&T and Verizon on the extensive investment in Network Disaster Recovery.

From <http://www.corp.att.com/ndr/> we find the following:

“AT&T’s commitment to our customers doesn’t stop when a natural or a man-made disaster occurs. The mission of the Network Disaster Recovery (NDR) Team is to recover AT&T voice and data service network elements to an area affected by a disaster. Telecommunications is vital for our business and government customers following a disaster, both for the impacted area and for the rest of the country. NDR is responsible for the rapid recovery of service at AT&T network sites following catastrophic events.

AT&T’s Network Disaster Recovery plan has three primary goals:

- To route non-involved telecommunications traffic around an affected area.
- To give the affected area communications access to the rest of the world.
- To recover communications service to a normal condition as quickly as possible through restoration and repair.

AT&T has invested more than \$600 million in its U.S. NDR program and another \$15 million internationally. Team members have spent more than 125,000 working hours on field exercises and deployments over the last two decades. AT&T is the first company nationwide to receive United States Department of Homeland Security’s (DHS) Private Sector Preparedness Program (PS-Prep) certification.”



Figure 22. Pocketnow provides an inside view of AT&T’s Q22013 Disaster planning exercise³⁰

³⁰ <http://pocketnow.com/2013/05/21/att-disaster-recovery-video-tour>

Verizon has also invested extensively in their Business Continuity and Disaster Recovery Plans.



Figure 23. Verizon Emergency Communications Center.

“We have a cross-functional Business Continuity and Disaster Recovery (“BC/DR”) team responsible for minimizing the impact of a disruption to our customers, employees, infrastructure, and business operations. We accomplish this objective by focusing on the following activities:

- Identify critical functions, infrastructure and risks;
- Implement strategies to minimize the risk of a disruption;
- Develop Business Continuity, Disaster Recovery and Crisis Management plans to recover operations in the event of a disruption;
- Maintain BC/DR plans, with updates completed at least annually;
- Test our plans to validate our response capabilities.

We continue to refine our response and recovery capabilities due to the increasing variety of services we provide and the ever-changing level of potential threats to these services.”

Some of the technology available includes COWs (Cell On Wheels) and COLTs (Cell On Light Trucks) and CROWs (Cellular Repeater On Wheels) and GOATs (Generator On A Trailer). Additionally mobile command centers, power distribution trucks, and other required support are available from most larger service providers in order them to manage emergency communications in a series of self-contained solutions.

It is clear that extensive planning and investment is required to perform when disaster strikes, and the service providers have shown a dedication to this preparation.

OBSERVATION: As of December 2013, the FCC has an active proceeding on improving the Resiliency of Mobile Wireless Communications Networks, we recommend that the TAC defer any specific recommendations on power strategies for wireless equipment or provide recommendation on the preparedness efforts of service providers.

In the past, placement of electrical and communications cabling underground was limited. In many cases, underground installations were only found in situations where overhead placement was not practical, would create a safety issue, or where operating or maintenance conditions made aerial placement impractical. Improvements in the technical quality of both electrical and communications cabling has made underground placement much more attractive in recent years. Underground placement is desirable to many municipalities and private sector entities for aesthetic reasons, and such placement often also results in increased reliability, and lowered risk of disruption from weather-related events, car accidents, and lower wildfire threats.

RECOMMENDATION: “Dig Once Policy”: Building on the 2011 Executive Order – Accelerating Broadband Infrastructure Deployment, FCC to Encourage Dig Once policies be enacted at local, state and federal levels to facilitate co-installation of communications networks during public works and utility construction

- a. “Dig Once” policy would minimize the disruption to citizens by consolidating utility work among different companies. Potential to reduce facility cuts. Longer term greater reliability of network through UG installations of physical plan
- b. Collaborate with the FCC Inter-Governmental Advisory council to jointly address how to get more voluntary cooperation.

Higher costs for design and construction, a more intensive permitting process, and in some cases a lack of underground right-of-way access paths has limited the penetration of underground power and communications cabling. Adoption of open joint trenching, or “Dig Once” policies can help to remove many of these barriers through better coordination that enables the undergrounding of all utility and communications cables together. Hence access to underground construction initiatives should be open to communications providers when public works or utility projects are initiated. Though any given project may not be a candidate for joint location of services, the benefit gained where practical to all parties justifies the inclusion of communications providers when such projects are planned.

Many electrical utilities today encourage joint trenching with communications providers, even offering to serve as the overall project coordinator when such projects take place. In addition to these voluntary efforts, “Dig Once” on federal lands has been instituted via an Executive Order signed on June 13, 2012, and as part of the National Broadband Plan. A few states have adopted this practice, with the State of Illinois serving as a good example of being very active in this area. Finally, examples of local, municipal programs can be found in Boston, Massachusetts; Sandy, Oregon; and Mount Vernon, Washington.

RESILIENCY FOR PUBLIC SAFETY COMMUNICATIONS

Next-generation 9-1-1 (NG9-1-1) is the IP-based replacement for today's Enhanced 9-1-1 emergency calling system. It envisions a national (and beyond) interconnected overall system, capable of supporting and managing all types of multimedia 'calling' and public safety related data, including text, VoIP and video. The National Emergency Number Association (NENA) is the primary standards group for NG9-1-1, including its technology, databases, and operations aspects. NG9-1-1 will operate, along with other emergency services applications, on the emergency services IP network (ESInet), a private, managed IP transport network provisioned for public safety related entities.

In an all IP world, having broadband access, carrier, web, and private networks with extremely high uptime are critical to the emergency communications mission. Duplicated and redundant software functionality and databases running on resilient and duplicated servers, in turn running on multi-pathed and/or ring structured IP networks, is one way to provide that 24x7x365 dependability so necessary for 9-1-1 and other emergency services.

The resiliency of all facets of the above are of high interest to NENA, ATIS, the Association of Public-Safety Communications Officials (APCO), the FCC, and other state and federal agencies and parties dependent on emergency communications, especially in the worst of circumstances when other more general communications processes may be disrupted.

The nation's PSTN E9-1-1 networks today are considered to be resilient. The network was largely designed by, and maintained by the ILEC, who treats the E9-1-1 network as one of its major responsibilities. Each state develops regulation and policy for their E9-1-1 and PSAP centers. In some cases funding and implementation is pushed all the way down to the municipality level. IP-enabled NG9-1-1 technologies have the potential to make 9-1-1 networks more resilient. but also present new challenges to all stakeholders, including PSAPs and the state and local governments that support them, their vendors, originating service providers, and other service and application providers that NG9-1-1 networks may support.

Service providers should continue to ensure that the components of their 9-1-1 services comprise a true 5 nines service, with proper redundancy, power backup, management, and service priority.

The E9-1-1 system was designed in an age where deliberate attack on the network was not considered a credible threat, but overload by natural events (mass calling events) was considered likely. The network is deliberately designed to limit how many calls can come from a single switch, using standard network design principles. The trunk group is typically engineered to a P.01 Grade of Service, based on call volume in the busiest hour of the month, which effectively busies out in-mass calling events so as to spread calls among all sources fairly.

In today's environment, however, deliberate attack is a much more likely event, and controlling overload by limiting trunk group size can have an unfortunate side effect. Because the number of trunks from a given switch is small (very typically 2-4 trunks), it is easy to occupy all of them through various types of TDOS attacks, and then block any legitimate calls from coming to the PSAP. Attacks like this are feasible, and NG9-1-1 systems can help mitigate these risks by dynamically managing the connections between originating service providers and PSAPs, as discussed below.

9-1-1 networks will be transitioned to an IP infrastructure. This NG9-1-1 effort is just starting to be deployed at the state and local level, and in the current government funding situation, it will take years to fully deploy it. NG9-1-1 presents new challenges and new opportunities to all service providers. But similar to commercial services, IP in NG9-1-1 will have the ability to automatically route around failed portions of the network giving IP a self-healing feature that covers not only the backbone of the network, but can be implemented all the way to the end-devices, enabling highly resilient services.

Service providers who present calls to the new Emergency Services IP network (ESInet) will find that NG9-1-1 has all new databases, new SIP and HTTP based protocols, and supports a much wider range of devices and services, including most multimedia devices and services.

NG9-1-1 was designed to be inherently more capable to support sustained service availability in the event of disaster. While the legacy E9-1-1 system may be limited in its ability to recover from the failure of the local infrastructure and to handle a large number of calls, NG9-1-1 is designed to spread load widely, across the country if necessary, while providing the call taker not local to the caller with tools to effectively handle the call and arrange appropriate response. Such service requires that the local ESInet be highly redundant, and interconnected in multiple places to other ESInets. Since NG9-1-1 uses IP transport, the underlying physical facilities can include services from multiple providers, including wireline, cable, and wireless.

The Future:

As the build out of NG9-1-1 networks occurs, the caller will have choices in communicating with a PSAP. The NG9-1-1 architecture will support not only voice communication, but include 2-way video, text, telemetry data, automatic crash notification, etc. It also may include the ability to send pointers to additional relevant data such as medical records, building floor plans, and any contextual data deemed pertinent to the emergency.

Finally, to the extent consumers rely on pure over-the-top (OTT) services that do not have access to 9-1-1, they will need to be informed about the limitations of emergency communications for new IP-enabled communications methods.

REPORTING AND METRICS

Regulatory agencies at both the state and federal level have, as part of their mandate, a mission to ensure public safety and to protect consumers.³¹ The FCC and state regulators apply different types of network quality and outage-related information reporting requirements on different classes of service providers. There is no uniform method or metric of reporting such data.

At the request of the TAC working group, the FCC provided a proposed statement of intent for data collection that includes the following:

“Network performance measurements serve multiple complementary purposes:

- *Data that is gathered over extended periods of time can help industry, government and researchers identify **performance trends, root causes** and **correlations** of network outages, particularly as the underlying network technologies, operational practices and organizational structures change.*
- *Data collected in real-time during outages improves **situational awareness**, facilitates focusing on **critical needs** and identifies where **additional resources** or **alternative** means of **communications** are most urgently needed.*

*Long-term goals would include **better forecasting, predictive modeling and planning for various outages.**”*

Measuring Performance

The existing regulatory regime has followed an integrated service model resulting from congressional actions separately legislating requirements for different technologies. In this model, the service (voice) and the infrastructure (the wireline or wireless circuit-switched network) were integrated and regulated as a single service.

METRIC REPORTING: Current Reporting³²:

- NORS: Network Outage Reporting System.
 - *“The FCC requires communications providers, including wireline, wireless, paging, cable, satellite and Signaling System 7 service providers, to electronically report information about significant disruptions or outages to their communications systems that meet specified thresholds set forth in Part 4 of the FCC’s rules. Communications providers must also report information regarding communications disruptions affecting Enhanced 9-1-1 facilities and airports that meet the thresholds set forth in Part 4 of the FCC’s rules. Given the sensitive nature of this data to both national security and commercial competitiveness, the outage data is presumed to be confidential”*
 - In the past, NORS performance data could be obtained and analyzed with limited company specific information. Today, members of the TAC are unclear as to the value of this data because it isn’t widely available. The FCC and industry groups like ATIS have access to the information, but other availability is limited.
 - Some states require duplicative copies of FCC reports and other require annual reports based on service provider reporting to the FCC.
 - <http://transition.fcc.gov/pshs/services/cip/nors/nors.html>
- DIRS: Disaster Information Reporting System.
 - *“DIRS is a voluntary, web-based system that communications companies, including wireless, wireline, broadcast, and cable providers, can use to report communications infrastructure status and situational awareness information during times of crisis.*

31 *“What Can Be Measured Can Be Managed: An Approach to Maintaining Broadband Voice Service Quality” Sherry Lichtenberg, NRRI. Page v, <http://www.nrri.org/documents/317330/50a4687d-8a29-47aa-9f73-3336549b7bff>*

32 *Formerly, Incumbent LEC’s were required to report extensively on the performance of the public networks they operated. After 2010 most of these requirements ceased as forbearance stipulations approved in 2008 expired. A major reason ARMIS forbearance was granted was because it only applied to a specific subset of companies (Price-cap, Incumbent LEC’s) and only wireline TDM voice service. See <http://transition.fcc.gov/ccb/armis/descriptions.html>*

- DIRS is based on specific situations and events and provides a limited view of network resiliency.
- When activated, DIRS will collect information concerning:
 - Switches
 - Public Safety Answering Points (used for E9-1-1)
 - Interoffice facilities
 - Cell sites”
- <http://transition.fcc.gov/pshs/services/cip/dirs/dirs.html>

As we see above, the current application of reporting service performance creates only a partial picture of the range of services being offered.

The Critical importance of Broadband

As broadband (wired or wireless) becomes more essential to governments, citizens, and business, and voice increasingly becomes an application provided over broadband access, understanding broadband performance becomes more important.

The FCC began to report on broadband-based direction provided in Section 706 of Telecommunications Act of 1996. The Act required an annual report on the availability of advanced telecommunications services to all Americans. This resulted in ongoing reporting and tracking of broadband deployment, but not on the speed or performance characteristics of the broadband network. In the National Broadband Plan³³ several recommendations were made proposing the FCC establish a measurement regime for broadband service.

While not quoting the full detail here, section 4 of the plan includes the recommendation 4.3:

- “The FCC, in coordination with the National Institute of Standards and Technology (NIST), should establish technical broadband performance measurement standards and methodology and a process for updating them. The FCC should also encourage the formation of a partnership of industry and consumer groups to provide input on these standards and this methodology.
- The FCC should continue its efforts to measure and publish data on actual performance of fixed broadband services. The FCC should publish a formal report and make the data available online.
- The FCC should initiate a rulemaking proceeding by issuing a Notice of Proposed Rulemaking (NPRM) to determine performance disclosure requirements for broadband.
- The FCC should develop broadband performance standards for mobile services, multi-unit buildings and small business users.”

To implement the recommendations of the plan, the FCC enlisted the cooperation of 13 ISPs covering 86 percent of the US population to be part of a voluntary program to survey and measure broadband performance. The commission further enlisted vendors, trade groups, universities and consumer groups to come to an agreement on what to measure and how to measure it.³⁴

As a result, the study enrolled approximately 9,000 consumers as participants and collected data.

The results of these surveys were compiled and are found in the Measuring Broadband America reports.³⁵ The reports include standard statistical measures of all tests for all ISPs and speed tiers measured.

The measurements included sustained download, burst download, sustained upload, burst upload, web browsing download, UDP latency, UDP packet loss, Video streaming measure, VoIP measure, DNS resolution latency, DNS failures, ICMP latency, ICMP packet loss, latency under load, total bytes downloaded and total bytes uploaded.

33 “National Broadband Plan – Connecting America” recommendation 4.3, page 44-45, <http://www.broadband.gov/plan/>

34 Available at <http://www.fcc.gov/measuring-broadband-america/methodology>

35 Available at <http://www.fcc.gov/measuring-broadband-america>

QoS/VoIP

- Reach agreement on call quality metrics.
 - Many aspects: packet-level impairments (e.g. loss and jitter), application-level impairments (e.g. echo), and signaling (e.g. call completion failures). These require different treatment.
 - Work with industry and standards bodies—build on ongoing work.
 - Short term: convene a fact-finding workshop to inform FCC planning.
- Identify circumstances that call for a defined minimum acceptable quality.
 - Subsidized services, emergency services are possible examples.
 - Cannot expect a uniform definition to apply in all circumstances.
 - FCC should state an expectation that interconnection will not be a source of impairment or blocking.
- Initiate a high-level conversation about U.S. policy for voice communication.
 - Commission Should revisit 2011 TAC recommendations



Quality tracking

- Encourage and track industry efforts to develop systems that measure and report end-to-end call quality.
 - Should be an ongoing effort as part of VoIP transition.
 - FCC should state expectation that design of VoIP systems will permit associating problems with responsible actors.
 - Alternative is direct FCC measurement of call quality.
 - A possible undertaking, but for which technologies?
- FCC should continue to track service quality of public internet
 - Apply “Measuring Broadband America” (MBA)-like model to better capture measurements for VoIP Services
 - End-user QoE is the goal



We remind the committee that the 2012 TAC studied quality of service and made the following recommendations:³⁶

It appears that these recommendations remain appropriate for us today and that these issues could be further explored by the Technology Transitions Policy Task Force. In fact, it could be stated that the Task Force fulfills the recommendation above to initiate the conversation about U.S. policy for voice communications.

NO CONSENSUS ON RECOMMENDATION:

There are at least 2 positions in the working group. The first position is that market factors will drive service providers to deliver excellent service. A new requirement to report network performance would have little value in that other relevant service metrics would not be reported. The opposing view is that the FCC and state regulatory bodies cannot adequately fulfill their legislative mandate without accurate data on performance of the communications network as a whole is required to ensure consumer protection and public safety.

The FCC should consider requesting further input on this if IP Transition trials are undertaken.

Major providers who have direct interconnection facilities following best practices have procedures in place for measurements to assist the two peered companies in troubleshooting issues. Where the facilities are virtual or involve public access or public internet, diagnosing the problem will often be impossible. A facilities-based VoIP ILEC call to another facilities – based VoIP MSO can achieve extremely high call quality and can track performance between the two networks. A call originating over a Wi-Fi connection in a coffee house may connect with the appropriate SIP server, may complete the call, but fidelity of the audio and call drops/blocks will not be traced.

To illustrate this point, we have reviewed several boilerplate interconnection agreements from facilities- based service providers. Besides specifying the types and volume of traffic to be exchanged, there is also a responsibility built into the agreement for jointly diagnosing faults and maintaining network performance. These include the measurement of post-dial delay, the call success rate, the far end congestion ratio, the delay or latency, the packet loss ratio and the packet jitter. Maintaining these variables within contracted tolerances enable facilities-based providers to deliver TDM audio fidelity and as high definition codecs are implemented, will enable even more improved voice calling experiences.

Variables such as these are tracked by each company offering facilities-based VoIP today but there is no requirement or intent to share this information with any regulatory agency.

RECOMMENDATION: Data collection and Metrics: Use network data sources to better track, predict, and plan network resiliency for disaster preparedness. To baseline and measure resiliency improvement over time.

- a. FCC to work collaboratively with providers to establish a data/analytic ability and/or expertise to use existing data sources, including existing NORS/DIRS data, for greater predictability and analysis of resiliency, and creation of a “Reliability Baseline” as a reference for future comparisons and metrics, working voluntarily with industry.
- b. FCC to partner with CDC to update current data gathering process to get more specific information relating to availability of multi-modal communication options, clarifications between VoIP, VoIP OTT, and traditional wireline voice services for better reliability reporting and planning capability.
- c. Leverage MBA data sets. Determine what data could be of value for reliability in the long-term goals of the MBA program.
- d. FCC to work with providers, determine what additional data is a meaningful indicator of reliability; develop a voluntary “crowdsourcing” data collection model to gather data in a manner that protects provider and consumer privacy and proprietary needs.
- e. Create annual network reliability baseline update

New Direction for Data Collection

Crowdsourcing Network Events

As communications services move to IP it is becoming possible to monitor network performance and events without the participation of the service providers involved in delivering that service. Enlisting the participation of consumers and other volunteers to collect and share data through crowdsourcing programs can be easier and provide more reliable data.

The primary tool the FCC uses to monitor and encourage network reliability is their Network Outage Reporting Requirements³⁷ set forth in Part 4 of the FCC’s Rules (47 C.F.R. Part 4). There are two reporting systems³⁸; Network Outage Reporting System (NORS) and Disaster Outage Reporting System (DIRS). Currently wireline, wireless, paging, satellite, cable and interconnected VoIP providers are required to report network outages in NORS. Broadband providers are currently not required to report outages. DIRS is a voluntary system. The specific details of all reports are confidential. These systems provide important data to the FCC to understand and analyze outages to the nation’s communications infrastructure. They also serve to encourage reliability in the network by the entities that are being monitored.

37 Most recent major R&O on Network Outage Reporting; http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-04-188A1.pdf

38 NORS and DIRS; <http://transition.fcc.gov/pshs/services/cip/nors/nors.html>

In recent years the FCC has chosen a different tactic to collect monitoring data that has proved successful. In 2011 they rolled out the Measuring Broadband America (MBA) program³⁹. To measure fixed line broadband performance the FCC enlisted 11 volunteer broadband service providers and thousands of their customers. Customers were given routers that would periodically collect performance data and send them to a central collection point. The FCC created reports based on this data to determine the penetration and service quality of broadband in America.

On November 14, 2013, this program was augmented with a mobile speed test app⁴⁰. This is a true crowdsourced program that goes directly to the consumers and doesn't involve service providers. Android smartphone users can download the app from the Google Play or Apple app store. The app will collect mobile broadband performance data, which is then aggregated to a central collection point. The FCC analyzes the data and issues reports on America's mobile broadband performance. This application is one of several that consumers can download to verify their mobile broadband speeds.

Other examples of crowdsourced network monitoring include RIPE's Atlas project⁴¹ and CAIDA's Archipelago project⁴². RIPE is the European Regional Internet Registry and their project has more than 4,000 probes deployed around the world. CAIDA (Cooperative Association of Internet Data Analysis) is a nonprofit research organization located in the United States. Two of their four sponsors are the NSF and DHS. Both projects are similar in that they seek volunteers to host a probe that collects and reports performance data. The only things the volunteer needs to participate are an Internet connection and an available Ethernet port. The devices are small, simple and inexpensive and given to the volunteers for free.

Should the FCC wish to augment its existing Measuring Broadband America infrastructure to support network event monitoring or pursue a new effort, it will need to address several issues:

- Volunteer privacy
- Data to be collected
- Funding the effort
- Monitoring infrastructure, including outage reporting
- Timeliness of data
- Awareness campaign
- Distribution strategy

The FCC has proven to be a leader in crowdsourcing monitoring data. Network event monitoring is an excellent candidate for crowdsourcing. We recommend that the FCC leverage it's existing expertise in crowdsourcing programs to monitor network events that effect reliability and resiliency.

39 *Measuring Broadband America*; <http://www.fcc.gov/measuring-broadband-america>

40 *Mobile Broadband Speed Test*; <http://www.fcc.gov/document/fcc-unveils-mobile-broadband-speed-test-app-empower-consumers>

41 *RIPE's Atlas project*; <https://atlas.ripe.net/>

42 *CAIDA's Archipelago project*; <http://www.caida.org/data/monitors/monitor-map-ark.xml>

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

2012 State of Reliability

May 2012

RELIABILITY | ACCOUNTABILITY



3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Figure 24. NERC State of Reliability Report - 2012

POLICY: REGULATORY AND AGENCY COOPERATION

Collaboration During Emergency Restoration of Services

Many electrical utilities and communications providers work together on a frequent basis during normal operations. Small, very localized events, such as traffic accidents, construction incidents, or small storms result in the need to coordinate efforts. In most cases, the electricity crews first perform pole and/or power cable replacement, while the communications provider waits. Upon completion of the power work, the communications restoration can take place.

Many disaster-related events simultaneously disrupt electrical and communications capabilities, but on a much greater scale. As both essential services often share common poles or underground right of ways, and are trying to restore capabilities at the same time for their customers, it would seem to be intuitively obvious that close coordination of their efforts would take place. This is often not the case, however.

It is important to note that this relationship is not just one way; communications providers can provide valuable intelligence to assist power restoration. Several MSO's and service providers have network-monitoring tools that provide them with visibility on power outages that may assist the power utility. In addition, boots on the ground from communications providers can provide utility crews with reports on field conditions.

RECOMMENDATION: Optimize the current restoration process: FCC creates national program on a collaborative restoration approach in response to outages and or natural disasters to increase resiliency and long-term reliability. Additionally, this program would help reduce damage to communications networks during the restoration process post natural disasters.

- a. Explore creating a "data exchange" for various utility/communication providers to share data with each other for greater efficiency and optimization of restoration process.
- b. Provide estimated time to restore electrical service, by area, to communications companies
- c. Provide communications companies with power crew work locations so that efforts can be coordinated.
- d. Instruct clearing and tree removal power crews not to cut any communications cables; call providers for quick removal of any cables.
- e. Place communications technical facilities at risk, and outside plant locations critical to public and private sector entities on priority restoration lists.

There are many forums in which this information could be exchanged, and it need not be cumbersome to the electric utility. In some cases, the two organizations are already collaborating on smaller issues; they just need to expand the scope via a larger forum. This could be over the telephone via email, or face-to face. In some cases, communications providers are invited into electrical utility emergency operations centers when they are activated. In other cases, both utility and communications providers may physically be in a local, or state emergency management emergency operation center, or part of a private sector liaison arrangement, such as a Business Operations Center, and can exchange information in these forums.

There are several federal-level groups challenged to provide for the power infrastructure. Within the Department of Energy, ISER (Infrastructure Security and Energy Restoration) is the primary agency responsible for power restoration (Emergency Response Function #12). Within the Department of Homeland Security, FEMA (Federal Emergency Management Agency) develops and maintains a matrix of all government emergency responsibilities that they maintain in two documents:

1. Emergency Response Function Annex
2. Critical Infrastructure and Key Resource Support Annex

It could be useful for the FCC to begin or extend their dialog with important advocacy groups supporting electric utilities that deal with communications. Some of these organizations include:

- NRECA – National Rural Electric Cooperatives Association
- NRTC – National Rural Telecommunications Cooperative
- UTC – Utilities Telecommunications Council
- EPRI – Edison Power Research Institute
- NARUC – National Association of Regulatory Utilities Commissioners
- NERC – North American Electric Reliability Corporation

CONCLUSIONS AND SUMMARY

The telecommunications network has been in constant evolution for the past century. The pace of change has increased rapidly in the past two decades. The change is accelerating as technology advances and compute capabilities open new innovative possibilities. New technologies have led to fundamental changes in the architecture and design of telecommunications services. We are in the midst of the IP Transition of communications, including circuits transitioning to IP packets and twisted pair transitioning to coax, fiber optics, DSL and wireless technologies. These new technologies have moved us from a narrowband, mainly voice network, to a broadband, voice and data and video network. As a result the traditional system of record has migrated to this new services rich, multi-modal network. Consumers have embraced the transition through the adoption and use of mobile devices including smartphones, tablets and other portable devices. In the near future, there will be many more devices accessing services built on these architectures.

The goal in writing this paper is to provide a detailed overview of the traditional “system of record” and to explain the transition to IP and the resulting impact to resiliency, emergency services as well as future looking capabilities. Consumers and businesses are embracing the new IP transition, wireless technologies, and the many applications enabled on the new telecommunications platform. The paper explores technology options to ensure that this new public communications network has the important resiliency characteristics that users have come to expect from the PSTN services, and will continue to support emergency services. The transition is providing more options to consumers, which is providing greater individual and household communications resiliency based on the multiple methods to connect and communicate.

The transition to IP has changed the way in-home phone lines are powered. The move has been from a Central Office, battery back up system, to an in-home powered gateway that provides a Voice over IP (VoIP) service. Many consumers are not aware that they no longer have a traditional powered-voice line in their homes and a consumer education program should be developed to increase consumer awareness of the capabilities of their services and the options available to provide back up power. In addition, this paper recommends a multi-stakeholder process to engage with consumer electronics industry leaders to design equipment that would standardize consumer power back up and labeling. The industry is already developing more efficient next-generation equipment designs. This distributed power requirement can be problematic for users that do not have battery backup during environmental and manmade disasters. Many of the issues around powering are being addressed by service providers and industry groups. Some of the key findings and related recommendations included in this paper are focused on liaising and working with the commercial power industry to increase the resiliency of their networks.

Emergency services support is another area that is specifically called out in the paper. There has been great innovation in terms of how emergency PSAP networks and architectures continue to evolve and the types of communications from citizens they will be able to accept. The IP transition, along with mobility, has provided much greater capability for consumers to reach and access emergency services. There is an opportunity for innovation by utilizing alternate services such as texting, video, and other data related methods to access emergency services. Emergency Service stakeholders are embracing and driving the changes.

The TAC has been asked to explore ways to evaluate network resiliency. The goal is to determine whether resiliency is improving over time. As the IP transition moves forward, and we move away from the traditional PSTN the traditional measurements may not provide the data and information necessary to effectively evaluate resiliency. Metrics and reporting are a key part of measuring network resiliency. There are several systems in place today that (NORS, DIRS) measure outages without context to multi-modal impacts or other access capabilities. The recommendation on this topic is to work with the industry stakeholders and providers to determine what are the proper metrics in a multi-modal network. In addition, the establishment of a baseline is important in terms of the ability to determine net change. It is important to note that the FCC Advisor to our working group, Henning Schulzrinne, FCC CTO, has been designated as the leader of the FCC team that will be tasked with determining which metrics will be meaningful in the new competitive communications market place.

In conclusion, the rate of change in the communications industry will continue to accelerate. New technologies, new service providers, and an ever increasing number of connected devices and communications interfaces will continually expand and deepen our ability to communication. The dependency on the power grid and backup power for communications will increase. The impact of Internet of things and machine-to-machine communications will add billions of new devices connected to the network. It is important to understand these new technologies, and capabilities with an eye on the impact to the network.

It is critical that we encourage entrepreneurs, service providers, manufacturers and innovators to continue to invest their resources and creativity in communications solutions. To support this new world, there are few who believe that the provider landscape of tomorrow requires the full regulatory regime that supported a PSTN voice monopoly. In fact, most believe it would stifle investment in new and emerging solutions. As such, we encourage regulatory agencies to take a hard look at removing as much legacy regulation as possible and take a fresh look at encouraging competition and investment by supporting only those regulations necessary to support the statutory values inherited from the PSTN.

Finally, as the working group chairman, I thank the dedicated members of our working group for their efforts and contributions to the dialogue we have had on resiliency. In particular, I thank Henning Schulzrinne, Chief Technology Officer of the FCC for his leadership and guidance over the past year. Also, I thank those who have authored and edited the various sections of this paper and contributed to this important effort on resiliency. We look forward to the FCC utilizing the working group's recommendations as they focus on policy changes during the transition and beyond.