
December, 2014

# WORKING GROUP 9

## Infrastructure Sharing During Emergencies

## Transport Subcommittee

## Shared Services

Table of Contents

# 1. RESULTS IN BRIEF

## 1.1. Executive Summary

The Transport Sub-Committee of CSRIC WG 9 was tasked to review and assess various methods to acquire, or share TRANSPORT infrastructure in the aftermath of a major event, to compensate for the loss of transport assets. The scope of this initiative focused solely on creating or refining best practices for the Wireline, Wireless and Cable infrastructure segments. The scope of this initiative does NOT focus on transport failures due to lack of power, nor does it focus on non-disaster, transport failures (e.g. backhoe incidents).

The sub-committee found that the most common point of transport failure during a disaster is the "unprotected" connection between the End-User (customer) and the Network or Service Provider (wireless, wireline or cable). As such, the subcommittee chose to focus on determining whether there were alternate transport options that could be shared or leveraged in the immediate aftermath of a disaster to replace that "last-mile" portion.

The sub-committee found that there is little or no shared, last-mile transport infrastructure that access providers could share or provision dynamically (within hours). There are opportunities however, for the End User and/or Service Provider to utilize alternate transport modes to augment or create redundant last-mile segments, but these alternate transport options do not lend themselves to on-the-fly provisioning. These alternate transport options are briefly reviewed within this document. Instead, these alternate transport modes must be considered and planned in advance to ensure sufficient capacity, and an optimized cut-over protocol is in place, if needed.

Many end users with critical services take advantage of the Telecommunications Service Priority (TSP) Program[1] to ensure that restoration of their critical circuits is prioritized before other restoration efforts. For some users, however, prioritized restoration of circuits may not provide the degree of reliability required. Clear communication by the end user to the network or service provider will provide the means to mutually develop plans and protocols that will meet the end user's requirements. Unfortunately, the sub-committee also learned that "customer demand for unprotected services is increasing"[2], and it is not clear that these customers fully understand the implications of buying services in this manner.

*The sub-committee endorses recommendations previously made by the Network Reliability Steering Committee[3] specifically:*

- *Customers purchasing protected or unprotected lightpaths, circuits or other transport services should consider reviewing the ATIS Network Diversity Assurance Initiative (NDAI) report regarding bilateral contractual arrangements to manage diversity for critical services.*

*The subcommittee continues to endorse the outreach efforts of the Federal Communications Commission (FCC) and Department of Homeland Security (DHS) to build awareness of the TSP Program, for the prioritized restoration afforded by this program may meet some end user needs.*

[1] http://www.dhs.gov/telecommunications-service-priority-tsp
[2] *ATIS-0100038, Analysis of Large DS3 FCC Reportable Outages"*, 2013, Alliance for Telecommunications Industry Solutions (ATIS), Network Reliability Steering Committee (ATIS-0100038)
[3] ibid

# 2. Introduction and Background

## 2.1 Working Group 9 – Transport Subgroup Team Members

| Company | Name | Company | Name |
|---|---|---|---|
| **AT&T** | Steven E. Martin | **Ericsson-ATIS** | Ernie Gallo |
| **Battery Corp** | Tom Cooleen | **HHS** | Ingrid Caples |
| **Battery Corp** | Dick Scott | **Federal Reserve** | Wayne Pacine |
| **Cat5 Resources** | Cindy Perez | **Federal Reserve Bank - NY** | Lola Judge |
| **Cat5 Resources** | K Catalano | **FS-ISAC** | Denise Anderson |
| **CenturyLink** | Kathryn Condello | **Level 3** | Jeff Ary |
| **Comcast** | Lynette Van Someren | **Pacific Power Rentals** | Richard Qualey |
| **Commscope** | Anil Trehan | **T-Mobile** | Jay Naillon |
| **Cox Communications** | Jim Shortal | **T-Mobile** | Harold Salters |
| **Cox Communications** | Mark Peay | **T-Mobile** | Joan Vaughn |
| **CTIA** | Rick Kemper | **US Treasury** | Kate Kingberger |
| **ENP** | Robert Oenning | **FEMA** | Jarrett Devine |

# 3. Objective, Scope, and Methodology

### *3.1. Objective*

The Transport Sub-Committee of CSRIC WG 9 was tasked to assess various methods to acquire or share TRANSPORT infrastructure in the aftermath of a major event in order to compensate for the loss of transport assets. This working group will examine various options and recommend a set of best practices Network Operators, Service Providers and End Users could adopt to sustain critical communications in future emergencies.

### *3.2. Scope*

The scope of this initiative is focused solely on creating or refining best practices for the Wireline, Wireless and Cable infrastructure segments. The scope of this initiative does NOT focus on transport failures due to lack of power (being addressed separately), nor does it focus on transport failures (ex. backhoe incidents) not associated with major events. The scope of this initiative will incorporate as appropriate, Best Practice considerations for Network Operators, Service Providers and End Users relying on transport for critical communications (Critical Users)

### *3.3. Methodology*

To address the questions posed to the Transport sub-committee, members reviewed existing documentation and received briefings from subject matter experts to better understand the following:

- Root Causes of Transport Outages
- Current Best Practices Associated with Transport Outages
- Viability of "Sharing" Excess Transport Among or Between Access Segments
- Viability of Alternate Transport Modes for "Stand-by" Transport Capacity

The assessments, analysis and resulting recommendations outlined within this document were based on these efforts, generated through a cooperative effort and by majority consensus of subject matter experts belonging to the CSRIC Working Group 9– Transport sub-committee.

# 4. Analysis, Findings, and Recommendations

## *4.1. Analysis*

### 4.1.1. Root Cause Analysis

The sub-committee reviewed the most predominant Root Cause of disaster-related, transport failure, the transport failure points, by access segment (wireline, wireless, cable), and whether existing best practices would have mitigated these root causes.

**Most predominant Root Cause of Transport Failure.** For the purposes of this tasking, the sub-committee was interested in assessing how often major transport failures could be attributed to disaster-related events. In the nomenclature of the Network Outage Reporting Systems (NORS), the most applicable, root causes associated with storms falls under "Environment (External) category. The subcategories within this grouping include:

- **Animal Damage** - Component destruction associated with damage caused by animals (e.g., squirrel/rodent chewing of cables, insect infestation, bird droppings, bird nests, etc.).
- **Earthquake**** - Component destruction or fault associated directly or indirectly with seismic shock. However, if damage was the result of inadequate earthquake bracing, consider the fault to be a hardware design.
- **Fire**** - Component destruction or fault associated with a fire occurring/starting outside the service provider plant. This includes brush fires, pole fires, etc.
- **Flood****
- **Ice/Storm****
- **Lightning/Transient Voltage**** - Component destruction or fault associated with surges and over-voltages caused by (electrical) atmospheric disturbances.
- **Other**
- **Storm -Water/Ice**** - Component destruction or fault associated with fog, rain, hail, sleet, snow, or the accumulation of water/ice (flooding, collapse under weight of snow, etc.).
- **Storm -Wind/Trees**** - Component destruction or fault associated with wind-borne debris or falling trees/limbs.
- **Vandalism/Theft** - Component loss, destruction, or fault associated with larceny, mischief, or other malicious acts.
- **Vehicular Accident** - Component destruction or fault associated with vehicle (car, truck, train, etc.) collision.

For the purposes of this assessment, the categories annotated with an "**" were considered appropriate for this analysis.

**Large-Capacity Transport Failure.** Upon review of the April 2013 ATIS "*Analysis of Large DS3 FCC Reportable Outages"*[4], report, the sub-committee found that weather, or disaster-related causes are not significant contributors to large transport outages. Indeed, the largest applicable Environmental-External subcategory cited as "direct cause" to transport outages was "Lightning-transient voltage" at 1.1%.

This same report also reviewed major storm activity between January 2010 and June 2012 to assess how these factors might have impacted the resiliency of larger DS3 capacity systems.[5] The data showed "that environmental conditions were not a significant contributor in the causes of large DS3 events. In fact, a small number of outages that exceeded the 1,000 DS3 thresholds were the result of storm summarization by providers. In other words, several smaller DS3 systems were combined into a single NORS report due to a common event (i.e., storm activity) driving the total DS3 impact over 1,000 DS3s."

**Last-Mile Transport failure.** In contrast, the transport segment between the End User and Network Provider infrastructure (the "last mile") is vulnerable to weather-related failures.

What is the "last mile?" In the context of this report, the subcommittee considers "last mile" to be the connection between the customer (end user) and the telephone company, cable company or ISP. The last mile has traditionally used copper-based telephone wire, coaxial cable, or Ethernet, and wireless technologies offer alternative options in some locations. The specific infrastructure constituting the "last mile" varies by access segment:

- Wireline: Customer Premise and Serving End Office
- Cable: Head End to the distribution node closest to the subscriber's physical location (leaves out going from the pole underground or by aerial to the subscriber (home/business location.)
- Wireless: Base Station (providing RF coverage to the end-user subscriber) and the final transport link from a distribution node (serving end office for a Local Exchange Carrier (LEC) T1), OR the final Ethernet gigabit fiber hop connecting the wireless base station with the Mobile Switching Center (MSC).

While disruption of "last mile" segments does not constitute a major service outage to the Network Provider, the sub-committee recognized this same "last mile" can be key to the resilience of the End User's service. The impact experienced by the End User can be significant, if the End User relied on that segment for critical purposes and did not request or arrange to protect that segment, thus creating a Single Point of Failure (SPOF). Indeed, any End User with more than one route into the Provider's network more than doubles its survivability. "While the provider's network has a high level of built in resilience, the last mile connection to the customer is usually a single point of failure, often because there is no alternative route. It is the most exposed part of the network to external interference or disruption."[6]

**Identifying "Last Mile" Criticality.** End Users have historically communicated the criticality of circuits to their Network Providers by requesting Telecommunications Service Priority (TSP) restoration codes from the Department of Homeland Security (DHS)[7]. If the End User's TSP request

[4] (ATIS-0100038) Figure 9 Top 80% of Root Causes – Non Sympathy
[5] (ATIS-0100038) Figure 18 Direct and Root Causes – Environmental Impact
[6] *Telecommunications Resilience Good Practice Guide Version* 4 March 2006 Centre for the Protection of National Infrastructure
[7] The TSP program authorizes national security and emergency preparedness (NS/EP) organizations to receive priority treatment for vital voice and data circuits or other telecommunications services. The TSP program supports a

meets criteria within the national security/ emergency preparedness continuum, is approved by the DHS TSP Program Office, and submitted to the Network Provider, the Network Provider tags those circuits (virtually) within their systems, and these circuits are prioritized for restoration.

As of March 2014, DHS Office of Emergency Communications has assigned 279,000 priority restoration codes. Of those 279K codes, 44% (>124,000) were assigned to private sector entities. Of note, approximately 70,000 of the private sector codes are assigned to wireless service providers, to ensure their "last mile" (the backhaul between the wireless base station and serving end office) received priority for restoration. Wireless service providers are the single largest user class in the TSP Program and constitute 25% of all assigned codes.

The importance of End Users communicating the criticality of their circuits to the Network Service Providers cannot be overstated. Many times, it is only when the End User submits their TSP Code to the Network Service provider, that there is any awareness that there is a critical function running on that circuit. These lessons have been affirmed in a number of resilience guides directed at End Users, such as the United Kingdom (UK) Center for the Protection of National Infrastructure "*Telecommunications Resilience Good Practice Guide*"[8] and the ATIS Network Diversity Assurance Initiative (NDAI)[9]. "The customer (end user) must be knowledgeable and able to articulate the risk it is willing to tolerate, and also translate this risk tolerance into terms that the (network) provider understands. It is also important that the provider has knowledge of the customer's business continuity objectives so the provider can communicate how technical alternatives address business risk. This would create a partnership among the parties and commitment on both sides to ensure that technical diversity approaches satisfy functional requirements and mitigate potential risks. "[10].

The Financial Sector has clear understanding of how to communicate the criticality of their services, as does the Public Safety community. Best Practice 9-9-0580 addresses the issue in the following manner: "*Network Operators and Public Safety Authorities should apply redundancy and diversity where feasible, to all network links considered vital to a community's ability to respond to emergencies."* Despite the applicability of both the Financial Sector and Public Safety best practices to other Sectors or End Users that provide critical services, it is not clear this same level of communication is being conveyed to the Network or Service Providers.

In the ATIS report cited above, the Network Reliability Steering Committee (NRSC) analyzed the mixed use of protected services (i.e., transport diversity) and unprotected services (i.e., no alternate transport diversity) by corporations and government entities purchasing bandwidth from service providers. The NRSC determined that "customer demand for unprotected services is increasing".[11] The report went on to state that "the NRSC believes that most communication service providers currently offer unprotected circuit terminations or lightpaths to provide affordable, dedicated bandwidth. Unprotected bandwidth is typically used when guaranteed path diversity is not needed, quality of services is not critical, or other means of a diverse path are engineered into the architecture by the consumer." The network providers within the subcommittee concurred with this assessment of current practices.

---

Federal Communications Commission mandate to prioritize requests by identifying those services critical to NS/EP. A TSP assignment ensures that it will receive priority attention by the service vendor before any non-TSP service.

[8] United Kingdom (UK) Center for the Protection of National Infrastructure "*Telecommunications Resilience Good Practice Guide* March 2006.

[9] **"***National Diversity Assurance Initiative",* February 2006 Alliance for Telecommunications Industry Solutions (ATIS)

[10] **"***National Diversity Assurance Initiative",* February 2006 Alliance for Telecommunications Industry Solutions (ATIS)

[11] Briefing by Robin Howard from ATIS/NRSC Analysis of Large DS3 FCC Reportable Outages (ATIS-0100038)

As such, the subcommittee chose to focus on assessing whether there were alternate means to share, or provision dynamically ("on-the-fly") transport in the aftermath of a major event for those critical-service end users whose arrangements either failed, or that may not have otherwise made arrangements in advance?

#### 4.1.2. REVIEW CURRENT BEST PRACTICES ASSOCIATED WITH EXTERNAL-ENVIRONMENT (WEATHER) WHICH MIGHT MITIGATE LAST-MILE PROVISIONING/RESTORATION POST-DISASTER

**General Best Practice Review**. In the context of the root cause assessment conducted above, the subcommittee considered the following Best Practices as potential starting-points for preventing last-mile outages or alternatively, promoting faster provisioning or restoration post-disaster.

| Number | Description |
|---|---|
| 9/6/5249 | Network Operators should consider geographic separation of network redundancy during restoration, and address losses of redundancy and geographic separation following restoration. |
| 9-7-1049 | Service Providers should consider utilizing multiple network carriers for internet backbone connectivity to prevent isolation of service nodes. |
| 9-7-1050 | Network Operators and Service Providers should consider tertiary carrier/transport methods such as satellite, microwave or wireless to further reduce point of failures or as "hot transport" backup facilities. |
| 9/7/5075 | Network Diversity: Network Operators and Service Providers should ensure that networks built with redundancy are also built with geographic separation where feasible (e.g., avoid placing mated pairs in the same location and redundant logical facilities in the same physical path). |
| 9/7/5079 | Network Operators and Service Providers should, where feasible, provide both physical and logical diversity of critical facilities links (e.g., nodal, network element). Particular attention should be paid to telecom hotels and other concentration points. |
| 9/7/5107 | Network Operators, Service Providers and Equipment Suppliers should evaluate and manage risks (e.g., alternate routing, rapid response to emergencies) associated with a concentration of infrastructure components. |
| 9/7/5261 | Network Operators, Service Providers and Property Managers should identify carrier interconnection points and coordinate restoral plans, as appropriate. |
| 9-8-0731 | Network Operators and Service Providers should provide physical diversity on critical inter-office and wireless backhaul routes when justified by a risk or value analysis. |
| 9-9-0402 | Network Operators, Service Providers, and Public Safety should, where appropriate, design networks (e.g., Time Division Multiplexing (TDM) or Internet Protocol (IP)) to minimize the impact of a single point of failure (SPOF). |
| 9-9-0580 | Network Operators and Public Safety Authorities should apply redundancy and diversity where feasible, to all network links considered vital to a community's ability to respond to emergencies. |

| | |
|---|---|
| 9-9-0736 | Network Operators should develop and implement a rapid restoration program for cables and facilities. |
| **9-9-1031** | **Network Operators, Public Safety and Service Providers should consider entering into Mutual Aid agreements with partners best able to assist them in a disaster situation using the templates provided on the NRIC and NCS websites. These efforts could include provisions to share spectrum, fiber facilities, switching, and/or technician resources.** |

In general, the subcommittee felt that the best practices outlined above, were implemented by the Network Providers, and credit many of these practices to the high reliability their networks. However, certain Best Practices suggest collaboration with End Users Many of the best practices, and the subcommittee re-affirmed the necessity for End Users to communicate to the Network Providers any critical services that might not otherwise be known.

**Sharing of Transport-Related Hardware Components:**

Network hardware components fail for many reasons; some may be weather-related. When this occurs, service continuation may come in the form of a redundant failover, or via load sharing. In other cases, replacement of the failed component(s) is required to restore vital communications services. Often, this replacement equipment is on site, and can quickly be put into service. In other cases, a maintenance agreement is in place for the equipment, and a vendor provides this replacement equipment. In other cases, equipment may come from another location from within the service provider's enterprise, and in others, the equipment may be provided by the equipment manufacturer.

There will be cases however, where a critical component may not be available via any of the above methods. Some of the equipment in question can be very specialized, with unique configurations. In certain cases, this equipment is manufactured to order, or is only periodically produced, and an off-the-shelf or off-the-assembly-line unit may not be available. In these cases, it is possible that another service provider may have equipment that could be used at this time of need.

Several existing best practices support sharing of resources and/or restoration plans between service providers:

| Number | Description |
|---|---|
| 9-9-1031 | Network Operators, Public Safety and Service Providers should consider entering into Mutual Aid agreements with partners best able to assist them in a disaster situation using the templates provided on the NRIC and NCS websites. These efforts could include provisions to share spectrum, fiber facilities, switching, and/or technician resources. |
| 9-7-5261 | Network Operators, Service Providers and Property Managers should identify carrier interconnection points and coordinate restoral plans, as appropriate |

While there are numerous steady-state forums where service providers can exchange information on planning initiatives, the subcommittee felt the most effective forum for post-incident support

and resources is the DHS National Coordinating Center (NCC)/Communications Information Sharing and Analysis Center (ISAC)[12].

The twelve (12) Best Practices above all play a role in ensuring the reliability of the networks, and the lack of weather-related causes associated with large-scale outages is a testament to use of these practices. Since the analysis suggested that it was the last-mile component that needed to be reviewed, the subcommittee turned its focus to on assessing the viability of "sharing" excess transport among or between the Access Segments (wireline, wireless, cable), and the viability of utilizing alternate transport modes as a means to replace or augment last-mile transport in the aftermath of a disaster. In all cases, the subcommittee was focused on determining whether there were options that might prove faster than the time associated with a prioritized restoration.

#### 4.1.3. *Assess Viability of "Sharing" Excess Transport Among or Between Segments*

Recognizing that the most predominant transport failure was within the "last mile" of the networks, the subcommittee reviewed network topologies by segment to assess points between segment carriers. The most common intersection point between the access segments (wireline, wireless, cable) were at higher levels of interconnection such as tandem locations and telecomm hotels, which would not serve to mitigate the last-mile transport failures.

Since there were virtually no common access points suitable for providing alternate, last-mile transport, it was the subcommittees view that sharing of transport facilities was not feasible.

#### 4.1.4. *Assess Viability of "Stand-by" or "On-the-Fly" Transport Services*

The subcommittee received a number of briefings on the viability of alternate transport modes and assessed whether these modes could potentially be accessed in the immediate aftermath of a disaster related outage. In particular, the subcommittee reviewed the capabilities of accessing dark (unlit) fiber, microwave connections, Very Small Aperture Terminal (VSAT) and passive optical network capabilities. The subcommittee was interested in the bandwidth these options might provide, and whether these options could be provisioned "on-the-fly" (within hours), or whether these options could be available on some stand-by (pre-arranged, but in reserve) capacity. Without exception, the options briefed did not lend themselves to dynamic (within hours) provisioning. Under optimal circumstances the VSAT and Microwave options can be provisioned within one-two days, which might prove faster (under certain circumstances) than prioritized restoration intervals.

While these options did not lend themselves to on-the-fly availability, access to unlit metro fiber, VSAT and microwave transport options can be incorporated into an End User's business continuity plan or used by the Network Provider to provide a "stand-by," diverse pathway requested by End Users with critical needs. The specifics, however, on which option to use and how to ensure it met the end user's needs would be subject to cost, advance planning and engineering by both parties.

In the opinion of the subcommittee, the use of Passive Optical Networks (PON) did not meet the objectives sought for alternate stand-by transport in the aftermath of an event. End Users with sufficient scale, however, may want to consider converting their enterprise architecture to one leveraging PON technologies given the advantages of reduced power requirements for the enterprise as a whole and an architecture that might lend itself to simplified provisioning of alternative, back-up power.

[12] http://www.dhs.gov/national-coordinating-center-communications

Appendix D provides brief summaries of the microwave, VSAT, dark fiber, and PON options as conveyed through subcommittee briefings.

### 4.2. FINDINGS

4.2.1. The subcommittee found that External Environment (weather) was not a predominant root cause for large scale outages.

4.2.2. The sub-committee found that External Environment (weather) was the predominant root cause for failure, of an "unprotected" transport connection between the End-User and the Service Provider (wireless, wireline or cable).

4.2.3. The sub-committee found that there may be some opportunity to share common transport hardware among Network or Service providers through mutual aide agreements or coordination forums such as the NCC/COMM-ISAC.

4.2.4. The sub-committee found that wireless providers have conveyed the criticality of approximately 70K circuits by placing a TSP code on their "last-mile" circuit.

4.2.5. The sub-committee found that customer demand for unprotected "last mile" services is increasing.

4.2.6. The sub-committee found that there is little or no common, last-mile transport infrastructure that access providers could share.

4.2.7. The sub-committee found there are no alternate transport options that can be provisioned "on the fly" for immediate transport access without advance planning.

4.2.8. The sub-committee found there are alternate transport options, most notably satellite and microwave options that might be provisioned (within 1-2 days) sooner than restoration intervals.

4.2.9. The sub-committee found that dark fiber, satellite and microwave options can be provisioned for stand-by access provided engineering and arrangements have been made in advance.

4.2.10. With foreknowledge, it may be possible for the Network Provider, Service Provider and End User to make the appropriate plans to assure that critical services are assured to the degree required by the End User. It is not clear that this level of communication is occurring between all End Users with Critical Services and the Network or Service Providers.

## 5. *RECOMMENDATIONS*

In summary, the sub-committee found that there is little or no common last-mile transport infrastructure that access providers could share dynamically. Furthermore, the sub-committee found that there are no alternate transport options that can be provisioned "on the fly" for immediate transport access without advanced planning. With foreknowledge, it may be possible for the Network Provider, Service Provider, and End User to make the appropriate plans to assure that critical services are secured to the degree required by the End User. For instance, the sub-committee found there are alternate transport options, most notably satellite and microwave options, which might be provisioned (within 1-2 days) sooner than restoration intervals. The sub-committee also found that dark fiber, satellite, and microwave options can be provisioned for stand-by access provided engineering and arrangements have been made in advance. It is not clear, however, that this level of communication is occurring between all End Users with Critical Services and the Network/Service Providers so that these advance plans and arrangements can be made. It is important for the End Users to articulate their business continuity objectives to the Network or Service provider so that arrangements to address the End User needs are accommodated.

In the context of continued assurance for last-mile segments, it is the Transport Subcommittees recommendation that the FCC continue to promote and encourage Network Providers, Service Providers and Critical Users to review these current Best Practices:

| Number | Description |
|---|---|
| 9-7-1049 | Service Providers should consider utilizing multiple network carriers for internet backbone connectivity to prevent isolation of service nodes. |
| 9-7-1050 | Network Operators and Service Providers should consider tertiary carrier/transport methods such as satellite, microwave or wireless to further reduce point of failures or as "hot transport" backup facilities. |
| 9/7/5075 | Network Diversity: Network Operators and Service Providers should ensure that networks built with redundancy are also built with geographic separation where feasible (e.g., avoid placing mated pairs in the same location and redundant logical facilities in the same physical path). |
| 9/7/5079 | Network Operators and Service Providers should, where feasible, provide both physical and logical diversity of critical facilities links (e.g., nodal, network element). Particular attention should be paid to telecom hotels and other concentration points. |
| 9/7/5107 | Network Operators, Service Providers and Equipment Suppliers should evaluate and manage risks (e.g., alternate routing, rapid response to emergencies) associated with a concentration of infrastructure components. |
| 9-8-0731 | Network Operators and Service Providers should provide physical diversity on critical inter-office and wireless backhaul routes when justified by a risk or value analysis. |
| 9-9-0402 | Network Operators, Service Providers, and Public Safety should, where appropriate, design networks (e.g., Time Division Multiplexing (TDM) or Internet Protocol (IP)) to minimize the impact of a single point of failure (SPOF). |
| 9-9-0532 | Network Operators and Public Safety should periodically audit the physical and logical diversity called for by network design of their network segment(s) and take appropriate measures as needed. |
| 9-9-0566 | Network Operators, Service Providers and Public Safety should consider placing and maintaining 9-1-1 TDM or IP based networks over diverse interoffice transport facilities (e.g., geographically diverse facility routes, automatically invoked standby routing, diverse digital cross-connect system services, self-healing fiber ring topologies, or any combination thereof). |
| 9-9-0580 | Network Operators and Public Safety Authorities should apply redundancy and diversity where feasible, to all network links considered vital to a community's ability to respond to emergencies. |
| 9-9-0736 | Network Operators should develop and implement a rapid restoration program for cables and facilities. |
| 9/9/5113 | Network Operators, Service Providers, Public Safety and Property Managers, when feasible, should provide multiple cable entry points at critical facilities (e.g., copper or fiber conduit) avoiding single points of failure (SPOF). |

*The sub-committee endorses recommendations previously made by the Network Reliability Steering Committee[13] specifically:*

- *Customers purchasing protected or unprotected lightpaths, circuits or other transport services should consider reviewing the ATIS Network Diversity Assurance Initiative (NDAI) report regarding bilateral contractual arrangements to manage diversity for critical services.*

*The subcommittee recommends that the FCC continue to support outreach efforts of the Federal Communications Commission (FCC) and Department of Homeland Security (DHS) to build awareness of the TSP Program, for the prioritized restoration afforded by this program may meet some end user needs.*

*The subcommittee recommends that the FCC coordinate with DHS to develop messaging appropriate for DHS Sector Outreach efforts, emphasizing the importance of communicating the criticality or business continuity objectives of Critical Infrastructure Key Resource Owner Operators to their Network or Service Providers.*

[13] ibid

# APPENDIX A: GLOSSARY

| Terminology | Description |
|---|---|
| **ATIS** | Alliance for Telecommunications Industry Solutions |
| **Base Station** | Cabinet and electronics for cell site |
| **CPNI** | Center for the Protection of National Infrastructure (UK) |
| **CSRIC** | Communications Security, Reliability and Interoperability Council |
| **Customer Premise** | Customer site, i.e. equipment is on the customer's premise |
| **DHS** | Department of Homeland Security |
| **DS3** | Digital Signal Level 3 |
| **End User** | A person who uses a product, i.e. Customer |
| **FCC** | Federal Communications Commission |
| **Head End** | Facility that houses electronic equipment to support in stream delivery of communications services |
| **ISP** | Internet Service Provider |
| **LEC** | Local Exchange Carrier |
| **MSC** | Mobile Switching Center |
| **NDAI** | ATIS Network Diversity Assurance Initiative |
| **Network Provider** | A business or organization that sells bandwidth or network access by providing direct Internet backbone access to the Internet and usually access to its network access points |
| **NORS** | Network Outage Reporting Systems |
| **NSRA** | National Sector Risk Assessment for Communications. |
| **Protected Services** | Network Diversity, Having multiple routes to a destination |
| **RF** | Radio Frequency – can be used as a synonym for radio to describe the use of wireless communication |
| **Segment** | Section of a communications network |
| **Service Nodes** | A physical entity that contains the service control function, service data function, specialized resource function and service switching/call control functions. A switch that is located at the meeting point between two networks, for instance between an end user's LAN to an ISP's network or an ISP's network to the Internet backbone. |
| **Service Provider** | A company that provides communications services to the end user |
| **Serving End Office** | The specific central office at which user lines and trunks are interconnected |
| **Subscriber** | A person or company that is authorized to receive or access communications services, i.e. customer |
| **Sympathy Reports** | Outage Reports that are filed under FCC Part 4 Rules when an outage reported in one service provider's network results in a FCC reportable condition for another service provider. |
| **T-1** | A full-duplex digital transmission facility that is composed of transmission media (optical or metallic) and regenerators that carry one DS1 signal. |
| **TSP** | Telecommunications Service Priority |
| **VSAT** | Very Small Aperture Terminal |
| **PON** | Passive Optical Networks |

# APPENDIX B: RESOURCE MATERIALS REVIEWED

## Publications

***"2012 National Sector Risk Assessment for Communications"***, U.S. Department of Homeland Security, September 27, 2012.

**"*Last Mile Bandwidth Task Force Report*",** National Security Telecommunications Advisory Committee (NSTAC) 2002

**"*ATIS-0100038, Analysis of Large DS3 FCC Reportable Outages*",** Alliance for Telecommunications Industry Solutions (ATIS). 2013

**"*National Diversity Assurance Initiative*"**, February 2006 Alliance for Telecommunications Industry Solutions (ATIS)

**"*Best Practices to Assure Telecommunications Continuity for Financial Institutions and the Payment & Settlements Utilities*"** Report by the Assuring Telecommunications Continuity Task Force, Payments Risk Committee, September 2004

***"Telecommunications Resilience Good Practice Guide Version 4"***, March 2006 Centre for the Protection of National Infrastructure

## Proceedings

**2013 FCC Network Resiliency Workshop**

Papers

http://edas.info/web/fcc-nr2013/program.html

*Leveraging Diversity for Resiliency,* Roch Guérin (Washington University in St. Louis, USA)
*Minimizing the Risk of Communication Failure,* John Thomas (Sprint, USA)
*FTTH technology in the Aftermath of Sandy,* Peter Vetter, Bell Labs, Alcatel-Lucent
*Network Adaptability from Disaster Disruptions and Cascading Failures*, Biswanath Mukherjee (University of California, Davis, USA)

Workshop Presentations:
http://www.youtube.com/playlist?list=PL4buVHalBRoPRqBvtphzmPN1k91l7vJYD

**ALTERNATE TRANSPORT BRIEFINGS**, March 19, 2014:

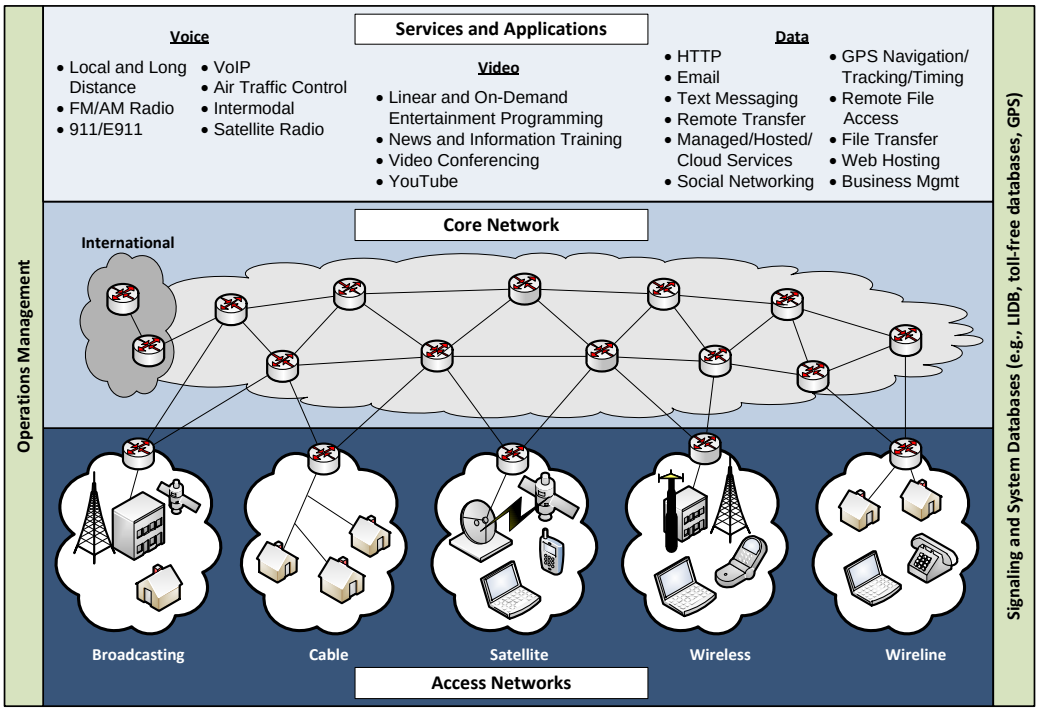
- Passive Optical Network Overview. Briefing provided by CenturyLink
- Satellite Communications and Network Transit. Briefing provided by Global VSAT Forum
- Dark Fiber Disaster Recover Considerations. Briefing provided by Level3
- Microwave Radio Transport. Briefing provided by Commsearch, a Commscope Company

**RELATED TOPIC BRIEFINGS**:

- Priority Telecommunications Services. Briefing provided by DHS Office of Emergency Communications (3/19/2014)
- FEMA Resources and Capabilities in Disaster Recovery. Briefing provided by Region __ FEMA (2/26/2014)
- Review of Best Practices: Financial Sector participants, WG9 Transport Subcommittee (2/12/2014)
- "Assuring Telecommunications Continuity Task Force" report of the Payments Risk Committee

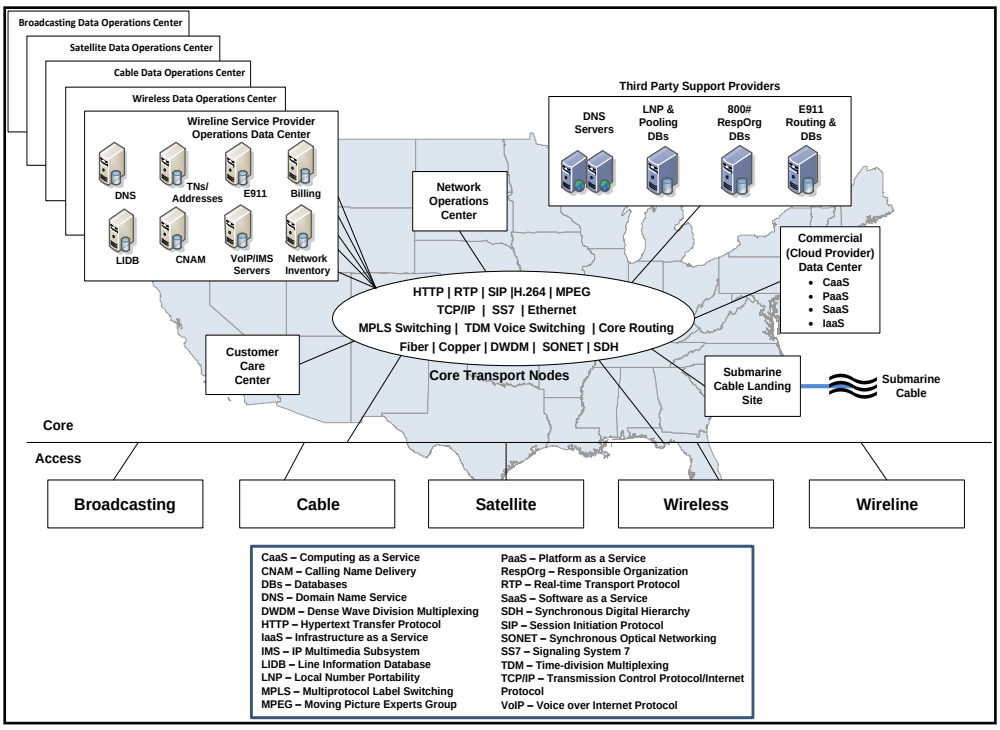
○ Alliance for Telecommunications Industry Solutions (ATIS) study entitled the "National Diversity Assurance Initiative".

# APPENDIX C: COMMUNICATIONS SECTOR NETWORK ARCHITECTURE DIAGRAMS [14]

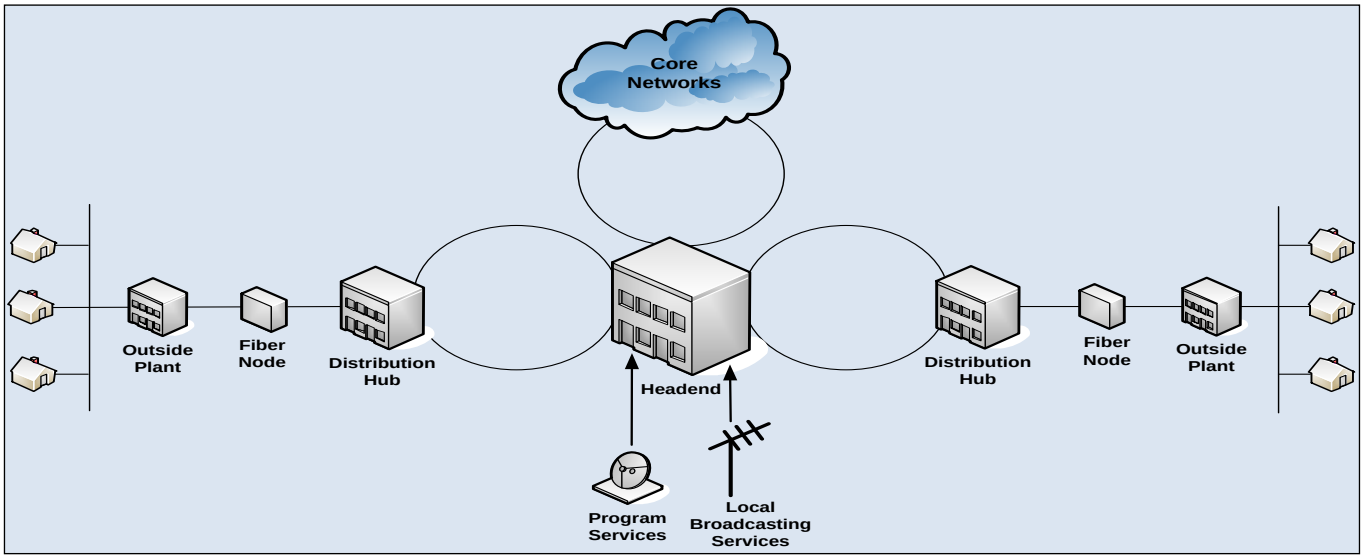



**High Level Communications Sector Architecture NSRA page 21**

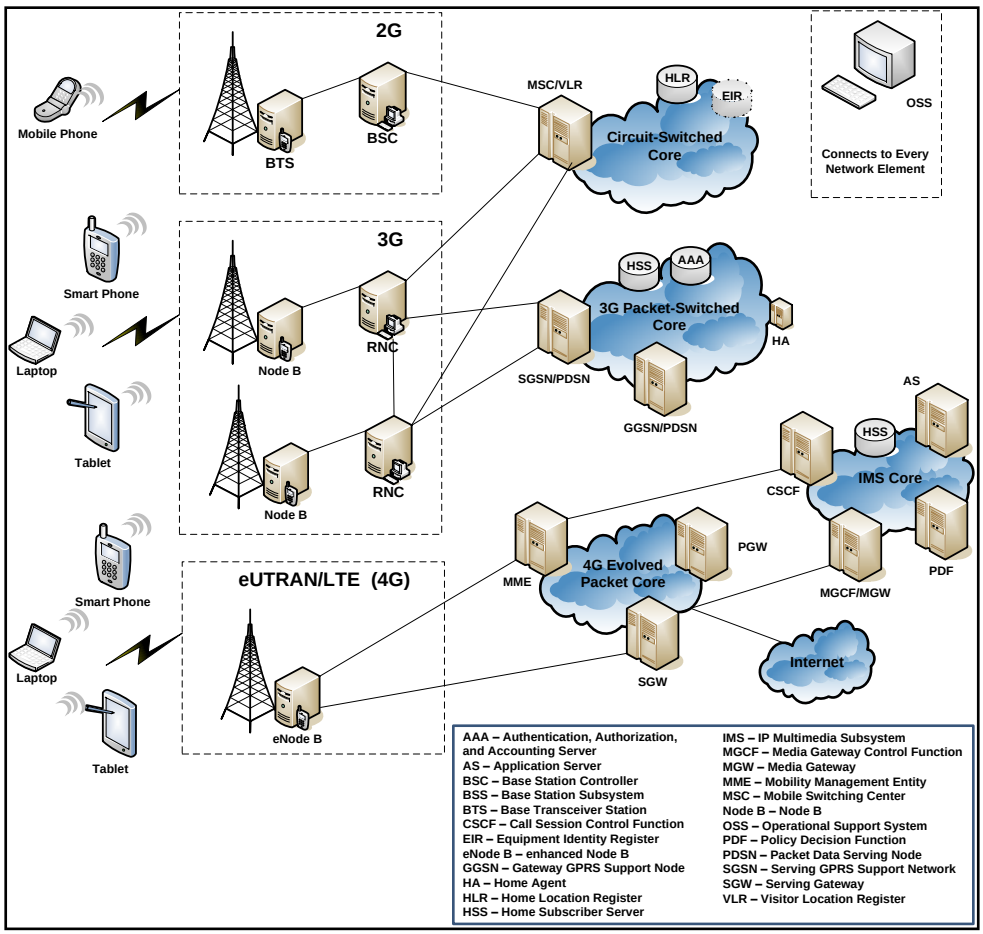
[14] ***"2012 National Sector Risk Assessment for Communications"***, U.S. Department of Homeland Security, September 27, 2012



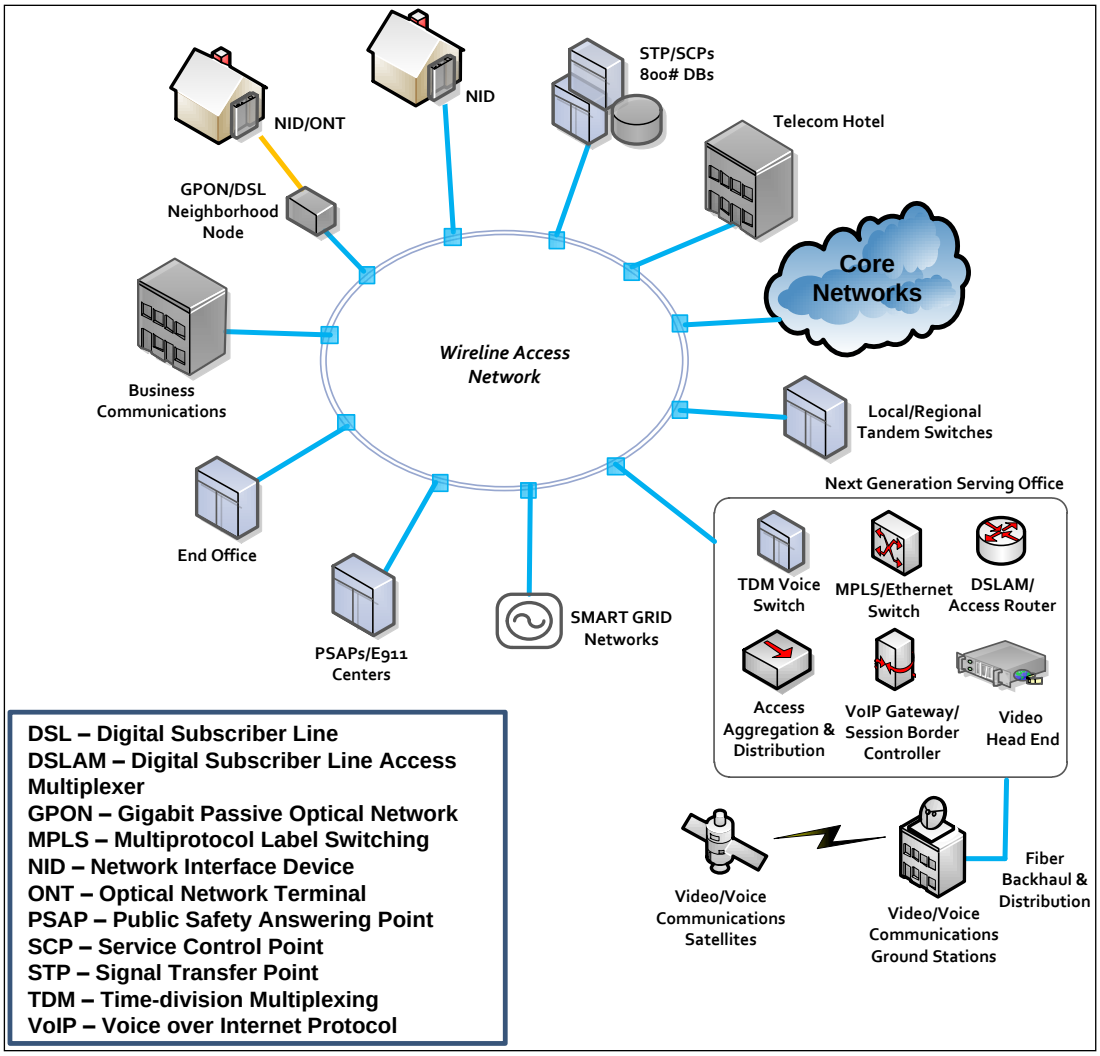

**Communications Sector "CORE" Architecture, NSRA page 23**




**Communications Sector "CABLE" Architecture, NSRA page 32**




**Communications Sector "WIRELESS" Architecture, NSRA, page 43**




**Communications Sector "WIRELINE" Architecture, NSRA page 48**

# APPENDIX D: MICROWAVE, VSAT, AND DARK FIBER DETAILED DISCUSSION

## Microwave

MW band selection comes in two forms;

- Licensed
  - Licensed microwave enables interference-free operation enabling a highly reliable link
  - Licensed links are protected from new entrants who need to work around existing links
  - Licensed links have a typical 10-year renewable term
- Un-Licensed
  - Unlicensed links can be implemented quickly (no frequency coordination or FCC licensing)
  - Unlicensed links typically have a lower initial equipment cost
  - Unlicensed links typically share the band with many other types of unlicensed devices that can cause harmful interference

Although, un-licensed links appear simple to implement there are considerations that will need to be evaluated before a plan can move forward. Additionally, this solution is not one that can be shared between service providers. Service providers would need to determine whether this solution is viable for each specific event for their network.

There are managed service organizations that specialize in design and implementation of MW systems. Service providers can set up service agreements, determine which amenities would be needed during a DR event and build a pricing catalog in advance. Then when an event occurs, the service provider only has to make a call to the managed service organization and give them the detailed instructions on the state of the network (i.e power is a requirement at the donor and receiving sites) for activating a link. Equipment can be either managed by the service provider or Network Operator.

## VSAT (Satellite)

Satellite like MW, can be managed on-the-fly, but does not lend itself to be shared between service providers. Services providers would need to determine whether this solution is viable for each specific event for their network. There are organizations that support enabling Satcom solutions and service delivery. These organizations will support the facilitation of emergency notifications and dialogue, training for VSAT installation, registry and installer database to support preparedness and task force to enable and monitor security of the link(s).

Satcom solutions have options for service providers to procure capacity on a satellite. Individual circuits are available to Network Providers and links are IP capable. Circuit types include Single Channel Per Carrier (SCPC) or Multiple Channels Per Carrier (MCPC).

VSAT services can be quick to deploy (2-3 days) at site locations convenient to the service provider. There are four "big" satellite provides worldwide and 8-10 smaller providers. Recently, satellite solutions have increased spectrum efficiency the latency that is seen in VSAT circuits and high-bandwidth options as well as bandwidth efficiency. Antennas and terminals are getting more compact allowing equipment to be more portable.

## Dark Fiber (Case Study)

**Dark Fiber Infrastructure**: Dark Fiber is unlit fiber on the intercity and metro networks. Intercity fiber is typically a point to point segment terminating in Tier 1 and Tier 2 cities with multiple regenerator sites in-between. Metro fiber is typically built in loops and segments connecting to multiple buildings

within a metro market. The dark fiber user is responsible for providing the optronics to make the dark fiber functional.

**Intercity dark fiber**: Intercity is optical fiber on the network that interconnects specific cities. Configurations may include fiber on point to point segments (typically ending at in Tier 1 and Tier 2 cities in controlled telecom locations sometimes called "Gateways"). Intercity fiber will typically pass thru multiple small facilities called In Line Amplifiers or Regenerators (ILA/3R) sites. Intercity Dark Fiber requires the purchase, installation, test, provisioning, and maintenance of optronics equipment for use at Gateway and ILA locations. Intercity Dark Fiber will require physical interconnects at the Gateway sites (or along the fiber right of way) to use the fiber. Interconnect locations are limited.

**Metro Fiber**: Metro dark fiber is optical fiber on the transport network contained within a particular metropolitan area. Typically configurations may include the fiber on metro loops and point to point segments. Metro fiber Loops typically are built with cable sizes from 12 count to 864 count cables. Metro fiber splice locations are typically more numerous due to the multiple buildings to be serviced. Metro fiber will typically support multiple metro buildings via laterals. Some laterals or routes are dedicated to a specific entity and are not available for other use.

## Disaster Recovery Considerations

### Intercity and Metro Recovery Routes:

- Potential recovery route(s) availability needs to be confirmed. Fiber may not be available on the route(s) required as well as total number of fibers required and timeframes needed.
- Potential handoff/interconnect locations from the impaired route to potential recovery routes need to be confirmed.
- Distances between fiber routes can be large. These interconnect distances can be longer than the portion of the route to be repaired. Interconnect locations on intercity fibers routes are extremely limited.
- If there is not an existing common fiber network handoff location between companies, build and permitting timeframes could be longer than the original network repair timeframes.
- Total scope needs to be confirmed before migration to the potential recovery route is contemplated.
- Equipment, space and power requirements needed for the duplicate route must be confirmed. Vendor lead timeframes or lack of space and power may not support the migration to a potential recovery route. Use of Intercity fiber will typically require deployment of new optronics equipment at multiple sites.

### Disaster Recovery Case Studies:

1. A Network Provider had an ILA site damaged by a hurricane near New Orleans. The Network Provider had access to intercity fibers on the nearby alternate carrier route. But given the complexity of locating equipment, space, power requirements, provisioning and installation, the Network Provider did not use the alternate carrier route fibers, but instead installed in a replacement ILA hut (on a trailer) for this recovery. The shared fiber solution with the alternate carrier would have taken much longer to turn-up than the ILA hut solution.
2. A Network Provider had a site damaged near New Orleans by a hurricane. The Network Provider ordered multiple 10G waves (lit capacity) for temporary capacity for one year (New Orleans to Houston) while the ILA site and damaged portion of the route was repaired.
3. During the recent floods in Northern Colorado, a telecom's intercity dark fiber route was damaged north of Denver. The Network Provider confirmed temporary fibers were available. The telecom's build timeframes to connect the Network Providers fiber was longer than the repair time on their damaged fiber. The telecom repaired their own route and did not use the Network Providers fiber.

4. A cable company asked a network Provider to confirm available fiber in Joplin, MO after their network was damaged by a tornado. The Network Provider dark fiber locations and the cable companies build timeframes did not support the use of any available dark fiber. The cable company repaired their own fiber routes and did not use the Network Provider fiber.

**Passive Optical Network Overview**

A **passive optical network (PON)** is a telecommunications network that uses point-to-multipoint fiber to the premises in which unpowered optical splitters are used to enable a single optical fiber to serve multiple premises. A PON consists of an optical line terminal (OLT) at the service provider's central office and a number of optical network units (ONUs) near end users. A PON reduces the amount of fiber and central office equipment required compared with point-to-point architectures. A passive optical network is a form of fiber-optic access network. Passive network utilizes unpowered optical splitters and shares fiber optic cables with multiple customers. Power is required at the source to manage traffic. These types of networks are conducive to closed campus type environment for a passive distribution using simplified wiring and reduced power.

"Fiber optic cables are more robust against floods than copper cables. The replacement of damaged copper cables and considerations to install utility cables underground in the aftermath of super storm Sandy provide an opportunity to roll out a future proof wireline infrastructure. A passive optical network (PON) does not require active equipment in the outside plant, which avoids the need for powering remote nodes and reduces the risk of failures… And improved energy efficiency of the customer premises equipment (CPE) enables new power back-up approaches, such as easy-to-replace consumer batteries or small solar cells."15

[15] FTTH technology in the Aftermath of Sandy, Petter Vetter, Alcatel Lucent, 2013 FCC Network Resiliency Workshop, http://edas.info/web/fcc-nr2013/program.html