ATIS-0100038

ANALYSIS OF LARGE DS3 FCC REPORTABLE OUTAGES

TECHNICAL REPORT

As a leading technology and solutions development organization, ATIS brings together the top global ICT companies to advance the industry's most-pressing business priorities. Through ATIS committees and forums, nearly 200 companies address cloud services, device solutions, emergency services, M2M communications, cyber security, ehealth, network evolution, quality of service, billing support, operations, and more. These priorities follow a fast-track development lifecycle — from design and innovation through solutions that include standards, specifications, requirements, business use cases, software toolkits, and interoperability testing.

ATIS is accredited by the American National Standards Institute (ANSI). ATIS is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding Partner of oneM2M, a member and major U.S. contributor to the International Telecommunication Union (ITU) Radio and Telecommunications sectors, and a member of the Inter-American Telecommunication Commission (CITEL). For more information, visit < www.atis.org >.

ATIS-0100038, *Analysis of Large DS3 FCC Reportable Outages*

Is an ATIS Standard developed by the **DS3 Outage Analysis Subteam** of the **ATIS Network Reliability Steering Committee (NRSC)**.

Published by

Alliance for Telecommunications Industry Solutions
1200 G Street, NW, Suite 500
Washington, DC 20005

Printed in the United States of America.

ATIS-0100038

ATIS Technical Report on

Analysis of Large DS3 FCC Reportable Outages

Alliance for Telecommunications Industry Solutions

Approved April 2013

Abstract

This paper discusses the investigation process and findings of the NRSC from its examination of large DS3 outages as identified in NORS reports for which the reason reportable was 1,350 DS3 minutes from January 2010 through September 2012.

Foreword

The Alliance for Telecommunication Industry Solutions (ATIS) serves the public through improved understanding between carriers, customers, and manufacturers. The Network Reliability Steering Committee (NRSC) strives to improve network reliability by providing timely consensus-based technical and operational expert guidance to all segments of the public communications industry. As a trusted expert, the NRSC addresses network reliability improvement opportunities in an open, noncompetitive environment. The NRSC advises the communications industry through developing and issuing standards, technical requirements, technical reports, bulletins, best practices, and annual reports.

The mandatory requirements are designated by the word *shall* and recommendations by the word *should*. Where both a mandatory requirement and a recommendation are specified for the same criterion, the recommendation represents a goal currently identifiable as having distinct compatibility or performance advantages. The word *may* denotes a optional capability that could augment the standard. The standard is fully functional without the incorporation of this optional capability.

Suggestions for improvement of this document are welcome. They should be sent to the Alliance for Telecommunications Industry Solutions, NRSC, 1200 G Street NW, Suite 500, Washington, DC 20005.

At the time of consensus on this document, NRSC, which was responsible for its development, had the following leadership:

R. Krock, Alcatel-Lucent, NRSC Co-Chair

S. Hartman, CenturyLink, NRSC Co-Chair

C. Underkoffler, ATIS Chief Edior

The DS3 Outage Analysis Subteam was responsible for the development of this document.

R. Howard, Verizon, DS3 Outage Analysis Subteam Co-Lead

M. Linnell, Applied Communication Sciences, DS3 Outage Analysis Subteam Co-Lead

R. Canaday, AT&T

E. Lawrence, AT&T

M. Peay, Cox Communications

B. Wormsley, Ericsson Services representing Sprint

R. Fiala, T-Mobile

H. Salters, T-Mobile

T. Collier, Sprint

K. Dausy, Verizon

S. Wolff, Verizon

Table of Contents

Table of Figures

ATIS Technical Report on –

Analysis of Large DS3 FCC Reportable Outages

1 Overview

In January 2012, the Alliance for Telecommunication Industry Solutions (ATIS) Network Reliability Steering Committee (NRSC) established a subteam to investigate an apparent upward trend in the number of large DS3 outages, where 1,000 or more DS3s were reported to the Federal Communications Commission (FCC) through the Network Outage Reporting System (NORS) based on thresholds found in the FCC Part 4 Disruptions to Communications; Final Rule (FCC Outage Rules).[1]

The NRSC launched an investigation by opening Issue Statement 21 entitled *Large DS3 Outage Investigation* to address this concern. The Issue Statement defines the business need as:

> *Quarterly reports presented to the NRSC and industry by the FCC Public and Homeland Security Bureau (PSHSB) indicated there was an upward trend in large DS3 outages, diminishing network reliability and raising questions regarding capacity and diversity. The NRSC, as part of its mission, agreed to analyze this trend and provide guidance to the industry to mitigate these outages.*

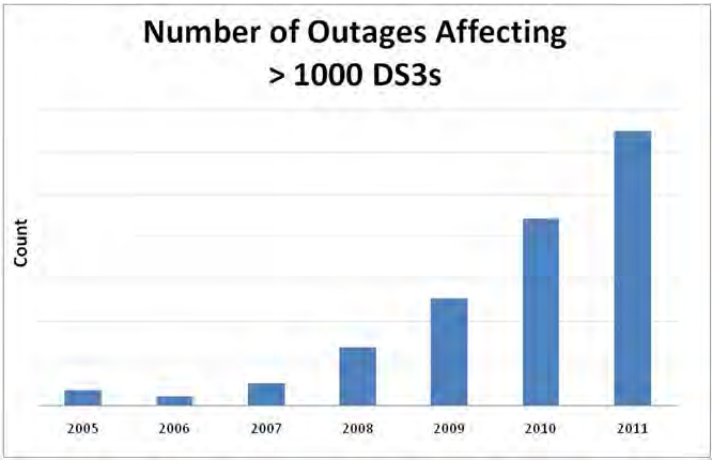

Figure 1 - Big DS3 Outages[2]

During the August 17, 2011, NRSC meeting, the FCC PSHSB noted that the number of these events appeared to be on the rise. They speculated that the cause could be that facilities are getting very large, which would mean that the overall capacity of traffic on these facilities is also increasing. During the December 7, 2011, NRSC meeting, the FCC PSHSB noted their data indicated that Big DS3 outages appeared to be increasing at a significant rate. In addition to asking the NRSC to investigate these types of outages, it was also noted that this upward trend resulted in the development of a number of questions the FCC raised in FCC Docket #11-60, *In the matter of reliability and continuity of Communications Networks, Including Broadband technologies effects on Broadband Communications Networks of Damage or Failure of Network equipment or severe overload Notice of*

[1] Part II Federal Communications Commission 47 CFR Parts 0, 4, and 63 Disruptions to Communications; Final Rule December 3, 2004.

[2] FCC NORS Analysis presented at NRSC Public Meeting on December 7, 2011, Slide 15.

Inquiry. Specifically, the FCC noted that the numbers of large DS3 events were causing them to question whether enough diversity is built into networks. Major points that the NRSC considered were:

1. Is the apparent increase due to network re-designs and larger capacity systems or is there a reliability issue?
2. Are these types of outages identifying a lack of diversity in portions of the network that are designed to have redundancy?
3. Is the number of large DS3 outages a significant percentage of the total number of DS3 outages?
4. Are the requirements of the existing Part 4 outage reporting rules adequate for DS3 failures given the evolution that has taken place in communications providers' networks, (e.g., increasing capacity of transport facilities)?
5. Is the standardized methodology for calculating the outage index (i.e., the level of customer impact), relevant for Large DS3 events?

These major points are addressed below.

2 Introduction

Communication providers are required by Part 4 Rules to report outages of at least 30 minutes duration that affect at least 1,350 DS3 minutes. "DS3 minutes" are defined as the mathematical result of multiplying the duration of an outage, expressed in minutes, by the number of previously operating DS3 circuits that were affected by the outage.[3] The NORS report form contains a field for the Number of Potentially Affected DS3s.

This paper discusses the investigation process and findings of the NRSC from its examination of large DS3 outages as identified in NORS reports for which the reason reportable was 1,350 DS3 minutes from January 2010 through November 30, 2011. Large DS3 outages are described by the FCC as affecting greater than 1,000 DS3s. The FCC's concern about the high number of large DS3 outages occurring stems from the assumption that 666,000 customers are potentially affected, per the Outage Index equation described in ATIS-0100021.2012, *Analysis of FCC-Reportable Service Data.* With the apparent increase in the number of large DS3 outage reports filed and the assumed customer impact, the NRSC understands that this would be of concern to the FCC. The NRSC, however, also considered these outages from a broader perspective, with consideration being given to today's network realities when assessing customer impact and significance of the events.

This paper also provides an analysis of NRSC member data which provides a significant, albeit partial, subset of the total number of outage reports filed by industry under the FCC's Outage Rules and, where appropriate, makes recommendations to reduce or mitigate these types of outages. The NRSC considered relevant industry work related to capacity and diversity issues, changes in customer needs and purchasing decisions, and network evolution including large DS3 capacity systems.

[3] Historically, the earliest capacity calculation of a single Digital Signal 3 (DS3) was defined as 672 unique voice or data customers that are impacted by a failure of a DS3. This definition carries over the paradigm from the Outage Reporting rules prior to 2005 that focused on 30,000 potentially affected customers. The current calculation describes a situation where each customer is allotted 64 Kilobits per second (Kbps) capacity on one of the 672 channels of available payload on the DS3.The result of this historical view of the usage of a DS3 overestimates the number of customers affected by the failed capacity of a single DS3 (i.e., 1 DS3 represents 672 customers). When this calculation is applied to a failure of 1,000 DS3s, the potential customer impact is implied to be 672,000 unique voice or data customers with a combined rate capacity of 5.333 GB.

3 References

At the time of publication, the editions indicated were valid. All standards are subject to revision, and the reader is encouraged to investigate the possibility of applying the most recent editions of the standards indicated below.

[1] Part II Federal Communications Commission 47 CFR Parts 0, 4, and 63 Disruptions to Communications; Final Rule December 3, 2004.[4]

[2] ATIS-0100021. 0100021, *Analysis of FCC-Reportable Service Data,* December 2012.[5]

[3] *FCC Network Outage Reporting System User Manual,* Version 7, December 17, 2012.[6]

[4] ATIS-I-0000041, *National Diversity Assurance Initiative*, February 2006.[7]

4 Definitions & Acronyms

4.1 Definitions

Application Diversity	This type of diversity is the diversity that the service provider's customer provides to their customers. This level of diversity is exclusively within the responsibility of the customer and is independent of the service provider. Customers develop their own diversity plan for applications that run over their physical networks
Channelized	The use of a single wideband (i.e., high-capacity) facility to create many relatively narrowband (i.e., lower capacity) channels by subdividing the wideband facility.
Contributing Factor	FCC NORS cause code that describes problems or causes that are closely linked to the outage.
Direct Cause	FCC NORS cause code that describes the immediate event that results in an outage and as the event, action, or procedure that triggered the outage.
Diversity Services	This type of diversity references what a service provider sells to their customers. The level of diversity is based on design, cost, and needs of the individual customer. The customer is responsible for deciding what level of diversity is utilized and/or built. The overall diversity is based on the customer's decision to purchase or not purchase a certain service, decision to utilize service from multiple providers, or to build a portion of the network themselves.
Network Diversity	This type of diversity references the practice of ensuring there are multiple physically diverse circuit routes to a critical facility. This level of diversity is exclusively within the responsibility of the service provider to manage and maintain. It refers to the network elements and facilities within the service provider's span of control and ends at the demarcation point with other provider networks.
Root Cause	FCC NORS cause code that describes the underlying reason why the outage occurred or why the outage was reportable and that the Root Cause is the key problem which once identified and corrected will prevent the same or a similar problem from recurring.
Unchannelized	Not using channels. An unchannelized network typically refers to a packet switching network

[4] This document is available from the U.S. Government Printing Office. < http://www.gpo.gov >

[5] This document is available from the Alliance for Telecommunications Industry Solutions (ATIS), 1200 G Street N.W., Suite 500, Washington, DC 20005 < https://www.atis.org/docstore/product.aspx?id=27898 >.

[6] This document is available from the FCC Public Safety and Homeland Security Bureau. < https://www.fcc.gov >

[7] This document is available from the Alliance for Telecommunications Industry Solutions (ATIS), 1200 G Street N.W., Suite 500, Washington, DC 20005 < https://www.atis.org/docstore/product.aspx?id=27923 >.

	such as IP.
Sympathy Reports	Outage reports that are filed under Part 4 rules when an outage in one service provider's network results in an FCC reportable condition for another service provider.

4.2 Acronyms & Abbreviations

ATIS	Alliance for Telecommunications Industry Solutions
FCC	Federal Communications Commission
FCC Outage Rules or Part 4	FCC Part 4 Disruptions to Communications; Final Rule
DS0	Digital Signal 0
DS3	Digital Signal 3
Gbps	Gigabit per second
GB	Gigabyte
Kbps	Kilobit per second
Mbps	Megabit per second
NDAI	National Diversity Assurance Initiative
NORS	Network Outage Reporting System
NRSC	Network Reliability Steering Committee
OC3	Optical Carrier 3
PSHSB	Public Safety and Homeland Security Bureau
TDM	Time Division Multiplexing

5 Objective, Scope, & Methodology

5.1 Objective

The objectives of this study were to perform a thorough and expert analysis of available data from NRSC member companies and, based on that examination, determine if a similar upward trend existed in large DS3 outages as seen in the FCC's December 7, 2011, quarterly report. In addition, the Subteam sought to identify through this internal data collection process and analyses any immediate causes that could potentially be mitigated through the use of existing industry Best Practices or through firsthand recommendations developed by the team.

The objectives were accomplished using a consensus based approach whereby NRSC member companies agreed, under a Non-Disclosure Agreement, to voluntarily provide highly sensitive outage reports to a third party to analyze and summarize the data. The information was then aggregated and reported back to the Subteam with the company identifying information removed. This data was used to create charts and tables, to research the data points available in the FCC NORS reports, as well as to examine the quantity, frequency, direct causes, root causes, and contributing factors of qualifying events.

The team also analyzed data tables created from member data that expressed the types of direct and root causes chosen at the time Final Reports were filed into the NORS system. This data was presented in percentage based format to rank highest to lowest percentages of cause codes used to describe the findings of each outage report by member companies.

As the team reviewed the data analysis it became apparent that additional major points were being discovered that would need to be addressed. Additional objectives were appended to the original list to revise the approach to include the five major points previously described:

1. Is the apparent increase due to network re-designs and larger capacity systems or is there a reliability issue?
2. Are these types of outages identifying a lack of diversity in portions of the network that are designed to have redundancy?
3. Is the number of large DS3 outages a significant percentage of the total number of DS3 outages?
4. Are the requirements of the existing Part 4 outage reporting rules adequate for DS3 failures given the evolution that has taken place in communications providers' networks (e.g., increasing capacity of transport facilities)?
5. Is the standardized methodology for calculating the outage index (i.e., the level of customer impact), relevant for Large DS3 events?

The team also recognized that an opportunity existed to educate readers on the modernization of transport technology to larger capacity systems and how that modernization may have unintentionally altered the perception of user impact during a qualifying outage. There was also an opportunity identified to discuss the current methodology of determining the amount of "pain" customers experience during a large DS3 outage event.

5.2 Scope

The scope of the effort was to analyze network outages reported to the FCC under Part 4, specifically the 1,350 DS3 reporting threshold that impacted 1,000 or more DS3s as was presented by the FCC during the NRSC's December 7, 2011, quarterly meeting. The initial data set collection consisted of the following criteria:

- Data range January 2010 through November 30, 2011;
- If possible, member companies were asked to provide a complete data set of all 1,350 DS3 events regardless of the number of DS3s impacted; or
- Where complete data sets were not available, a subset of outages where:
    - Reason Reportable was 1,350 DS3s Minutes; and
    - DS3s reported equaled 1,000 or more.

This data set was provided to the trusted third party entity under Non-Disclosure Agreement for analysis. This scope was adjusted later to include a month by month extension of the data range of January 2010 through July 2012 to continue investigation of ongoing trends in reporting related to the large DS3 events.

5.3 Methodology

The team began work by using collected data to confirm a trend existed within NRSC member companies and to determine whether the trend aligned with the FCC's trend. Outage data filed by service providers into the NORS system is protected and unavailable to the NRSC for routine evaluation. To perform any meaningful evaluation regarding these failures, member companies agree to provide their individual NORS filings to a trusted entity to preserve the protection of the reports and any sensitive information contained within the reports. The aggregated data was then used to develop the theories the team would explore and to further narrow the focus to the most prospective leads.

Following the initial data review, each company performed an internal deep dive into the top 80% of root and direct cause areas. This step in the investigation was essential in expanding on the details and trends behind the NORS reports to formulate the findings and recommendations. The deep dive was also used to discern if there was a specific product line, specific hardware element, or activity during a certain time of day that could support the causes of large DS3 outages.

The team evaluated the outages from the perspective of network and technological changes to gauge how these might interrelate to the increases detected by the FCC over time. The theory is that larger capacity systems can rapidly exceed FCC reporting thresholds mathematically due to equivalent bandwidth calculations performed by service providers as they determine the quantity of DS3s. The theory postulates that as the network moves

toward larger capacities, an increase in outages meeting FCC thresholds can be expected to some magnitude. With the changes to technology, the issue of reliability and resiliency and the use of diversity were debated along with the ability of sophisticated enterprise customers to understand network design and associated risks. Prior work completed by other industry groups was investigated to determine the relevance to this current issue and if that work could be incorporated into NRSC recommendations.

One concept involved the time of day outages occur in the network and that through assessment it may be possible to estimate the most likely times a provider could potentially expect a large DS3 event to occur. The methodology of calculating the level of customer impact, or pain felt, for large DS3 events was also studied as it relates to an outage index in use by industry and the FCC for several years. This calculation did not appear to scale correctly with these larger capacity systems and overemphasized the actual impact.

6 Analysis & Findings

6.1 Analysis

BANDWIDTH USAGE

The transport network is evolving in scope and capacity. As the network evolves, it is important to understand the transition from channelized DS3s to larger capacity data pipes and wavelengths. As technology improves, more data is transmitted across the same facilities. Originally, DS3s were intended to aggregate up to 28 T1 level circuits each with up to 24 DS0's, for a maximum of 672 basic DS0 level *channels* being transported. Each basic channel of 64 kbps can carry a single phone call or connection of traditional Time Division Multiplexing (TDM) services. Therefore, if the entire DS3 fails, you can reasonably estimate the potential impact is to all DS0 channels and calculate the maximum number of customers impacted.

Where customer's capacity needs go beyond traditional TDM, they will typically move up to an optical level circuit. Optical DS3s can transmit *unchannelized* data payloads using as little or as much bandwidth as required to move the payload up to the maximum available at high speeds. With the elimination of DS0 level channels, the ability to accurately estimate consumer impact during a failure is not as clear or easy to calculate. For example, if a channelized DS3 fails, you can reasonably estimate 672 DS0 level customers with voice or data connections being impacted. On the equivalent OC3 unchannelized circuit there may be just a few customers transmitting up to 155.52 Mbps of voice and/or data. As bandwidth has exponentially increased, the conceptual term DS3 continues to be recycled to describe an equivalent bandwidth of 45 Mbps, even though it is not in principle a correct term.

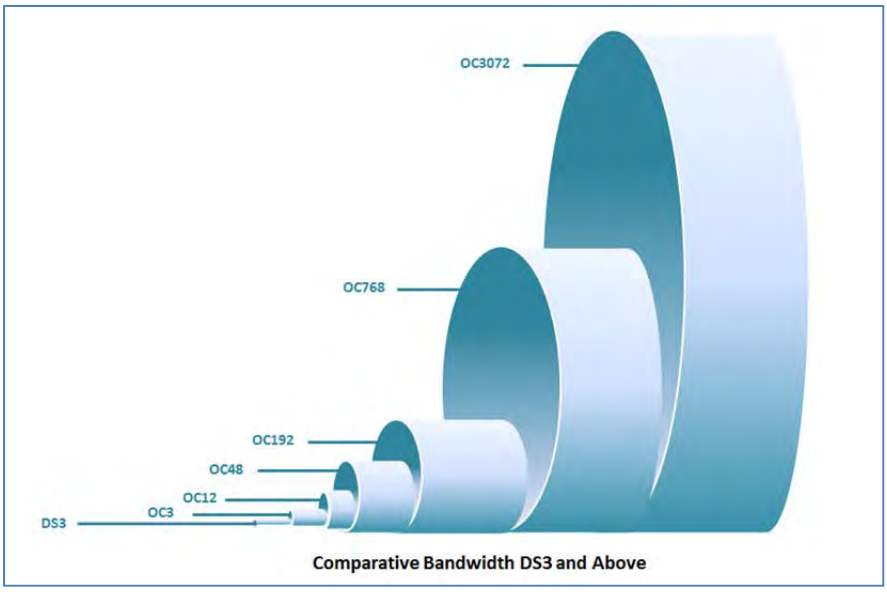

Figure 2 - Comparative Bandwidth

Figure 2 illustrates the evolution of capacity beginning with the original DS3 with a capacity of 44.736 Mbps through an OC3072 with a capacity of 160 Gbps. Above an OC48, transport system capacity effectively becomes a scalable product where data usage expands within the available bandwidth for one or more customers up to the maximum capacity. When multiple (or in some cases a single) large capacity circuit(s) or wavelength(s) are impacted, conversion of the bandwidth to DS3 equivalents results in an overestimate of customer impact. Therefore, if any combination of larger capacity systems fail (e.g., two OC768s or one OC3072) a 1,000 DS3 equivalency is exceeded. If you calculate the estimated customer impact as demonstrated earlier, a failure of 1,000 DS3s would represent 672,000 DS0 level customers, when in fact only one or two customers may actually be impacted. It is this calculation of "pain" that tends to overemphasize the impact of the specific outage.

So the next logical question to investigate is "Why use such large circuits then?" The simple answer is speed to transmit. The higher the capacity the faster the data will be transmitted to the other end. To illustrate, if we were to transmit a 100 Gigabyte (GB) file across an unchannelized DS3 it would take approximately four (4) hours and 56 minutes to complete the transfer. An OC192 circuit can transmit that same 100 GB in approximately one minute and 20 seconds[8]. These large payload types may not necessary be voice or other TDM services, but are more efficient when there is a mixture of enterprise and public type services. As consumer demand for high speed services increase, data consumption multiplies, driving the need to use these larger systems for economy of scale. In newer architectures, a failure of a large capacity system may have little to no impact on individual users when traffic is rerouted using diversity schemas or when the entire bandwidth is being used by an individual enterprise or government entity. In one test during the NRSC's investigation, a single large DS3 event was chosen at random using the date only. The team members were asked to review their company's outages for that single day looking for any significant outages. The investigation did not uncover any discernible impact nor did a general internet search seeking media coverage for any significant outages on that day.

CUSTOMER DEMAND FOR SERVICES

During the investigation, the NRSC determined that customer demand for unprotected services is increasing. Customers purchasing bandwidth from service providers are generally sophisticated corporations and government entities that understand complex networks. Their mixed use of protected services (i.e., network diversity) and unprotected services (i.e., no or alternate network diversity) was analyzed by the team.

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. Information regarding the diversity options is shared with customers in order to allow them to make informed decisions regarding their service.

An example of when unprotected wavelengths are used in an alternate diversity arrangement is in mesh architectures. In path-protected mesh networks, some connections can be unprotected; others can be protected against single or multiple failures in various ways. Figure 3 below illustrates a mesh network where unprotected lightpaths are used to provide diversity[9]. In this example, an unprotected optical path is reserved and shared (S/T) and provides failover protection for bandwidth demands for optical paths A/B and C/D. Each primary path A/B and C/D also utilize unprotected wavelengths with path protection being provided through the use of the reserved unprotected path.

[8] < http://www.numion.com/calculators/Time.html > using File Size 100 GB and 0% overhead.

[9] < http://upload.wikimedia.org/wikipedia/commons/8/8d/SBPP-before_failure.jpg >

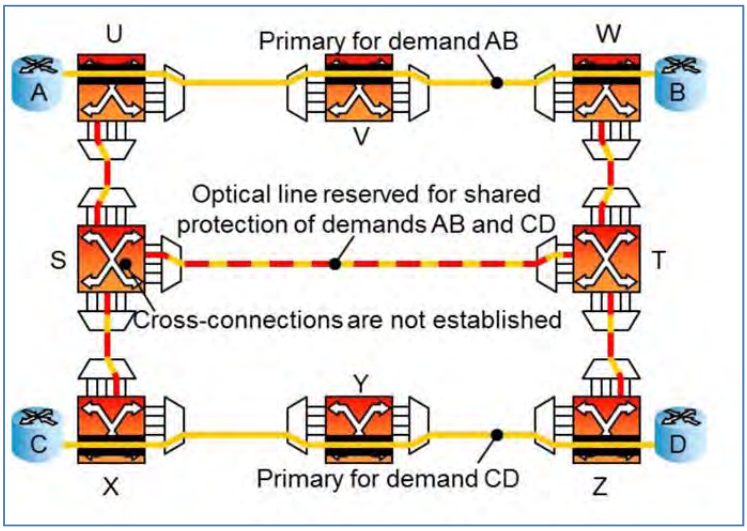

Figure 3 - Shared Backup Path Protection – Before Failure

Figure 4 illustrates the path diversity provided in the mesh arrangement if a failure occurs (C/D) and traffic is automatically rerouted across the reserved unprotected path (S/T)[10]. The mesh arrangement reduces overall costs for customers while providing resilient and reliable network diversity.

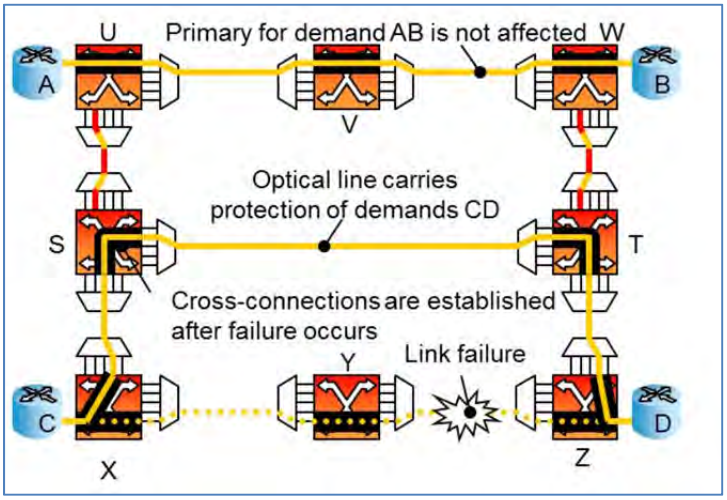

Figure 4 - Shared backup path protection after failure and recovery

In diverse arrangements such as above, the failure of a single lightpath due to a planned or unplanned event does not impact customers, but can qualify as a reportable condition under Part 4 rules. Without the understanding of this type of arrangement, the outage may appear to be significant in nature when in fact it is non-service affecting.

The NRSC supports the dissemination of information to customers who purchase unprotected lightpaths or circuits that outline risks and limitations related to network resiliency and diversity. A knowledgeable consumer is better able to evaluate their needs and risks for service and application diversity. The team also supports the view that customers with mission critical applications should have alternate or customer provided diversity and it is within their right to make the decision regarding the level of diversity deployed to support their services.

[10] < http://upload.wikimedia.org/wikipedia/commons/3/39/SBPP-after_failure_and_recovery.jpg >

DIVERSITY ISSUES

Part of the team's analysis focused on the discussion of diversity and whether the failure of a large capacity system was causing significant customer impact. Three types or levels of diversity were defined relevant to the use of large capacity systems:

- Network Diversity
- Diversity Services
- Application Diversity

The team reasoned that each type of diversity was distinctive and defined the responsibility for ensuring that specific type or level of diversity as follows:

- *Network Diversity* – This type of diversity references the practice of ensuring there are multiple physically diverse circuit routes to a critical facility. This level of diversity is exclusively within the responsibility of the service provider to manage and maintain. It refers to the network elements and facilities within the service provider's span of control and ends at the demarcation point with other provider networks.
- *Diversity Services* – This type of diversity references what a service provider sells to their customers. The level of diversity is based on design, cost, and needs of the individual customer. The customer is responsible for deciding what level of diversity is utilized and/or built. The overall diversity is based on the customer's decision to purchase or not purchase a certain service, decision to utilize service from multiple providers, or to build a portion of the network themselves.
- *Application Diversity* – This type of diversity is the diversity that the service provider's customer provides to their customers. This level of diversity is exclusively within the responsibility of the customer and is independent of the service provider. Customers develop their own diversity plan for applications that run over their physical networks.

The large capacity system outages analyzed by the team were consistent with network diversity and diversity services.

The team was also interested in reviewing the previous work by the ATIS National Diversity Assurance Initiative (NDAI) regarding their approach and recommendations for diversity. The NRSC was specifically interested in the following NDAI recommendation:

> "*This guidance will provide customers with the knowledge they need to identify the diversity risks that exist in their current telecommunications environment. It would also provide them with terminology that could be used to establish a common understanding with carriers when evaluating circuits for diversity assessment and assurance, as well as how circuits are engineered to address diversity concerns. Customers could then better determine the acceptable level of risk as it pertains to their telecommunications services."*[11]

This particular recommendation is relevant to our analysis in that the NRSC believes that customers should be provided with adequate information regarding the risks and limitations that are inherent in various diversity configurations. As well, the NRSC believes that service providers should continue to implement appropriate industry Best Practices regarding network diversity to provide the highest level of reliable and resilient service.

DATA ANALYSIS

The team completed an in-depth analysis of outage data that spanned a total of 31 months (January 2012-July 2012) and determined that primary causes of failure can be categorized in two areas: Hardware Circuit Packs and Cable Damage. The data also referenced a number of the reported events in the NORS system as involving

[11] ATIS-I-0000041, *National Diversity Assurance Initiative*, February 2006, Page 16.

unprotected wavelengths. A certain percentage of the outages were related to environmental events (e.g., storms) that when combined into a single report exceeded the 1,000 DS3 or more threshold that was investigated. The detailed analysis completed by the team can be found below.

Figure 5 represents the total number of large DS3 outages reported by NRSC member companies per month over the study period. The data shows that the reported number of NORS events began to rise in September 2011, and that the number of events dropped sharply in early 2012, followed by a sharp increase in April 2012. This trend confirmed that NRSC member companies are contributing to the increase seen in the FCC's data.

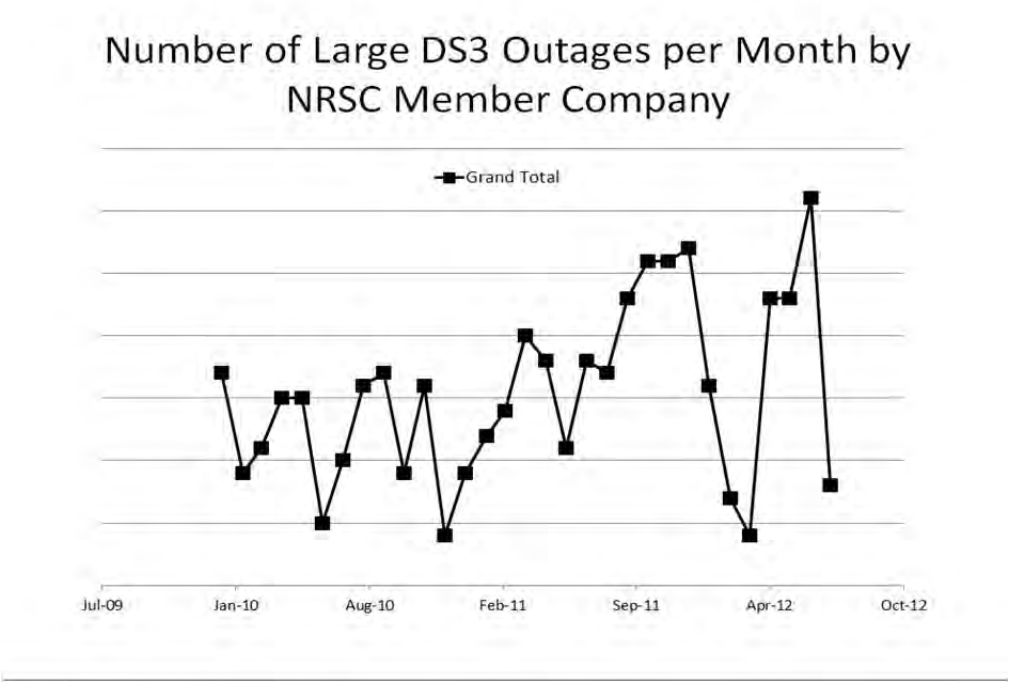

Figure 5 - Outages per Month – NRSC Member Companies

It should be noted that the data used for this study does not represent the industry as a whole, but does provide a significant view of the overall outages reported to the FCC. Figure 6 below presents the same data found above in Figure 5, but includes the control limits. The black line represents the standard which is the average number of reported outages from January 2010 to December 2010. The red lines represent being 99% within the contol lines. The yellow lines represent being 95% within the control lines. This translates to mean that about 1% of the time, there will be a data point outside (above or below) the red lines and that approximately 5% chance that a data point will appear above or below the yellow line.

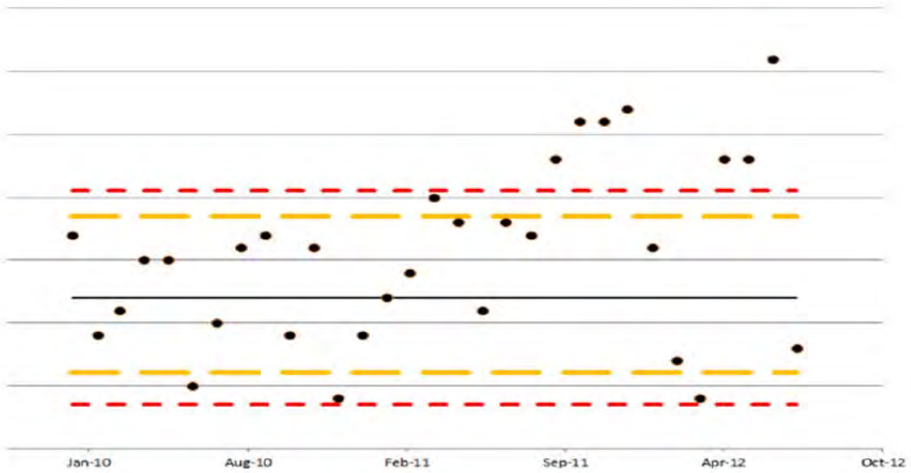

Figure 6 - Control Chart Outages per Month

Once the monthly data was plotted on the control chart a more stable depiction of the outage trend emerged. Although there are seven months beginning in 2011 where the outages fall outside the control limits, the data overall indicates the outages are mostly in control during the study period. The NRSC's review of the months outside of the control limits identified that there was a higher than average number of hardware failures from October through December 2011. Similarly, between April and June 2012, a higher than average number of fiber issues were identified as the driver for the increases.

Figure 7 is similar to Figure 5, however, this chart excludes "sympathy reports".

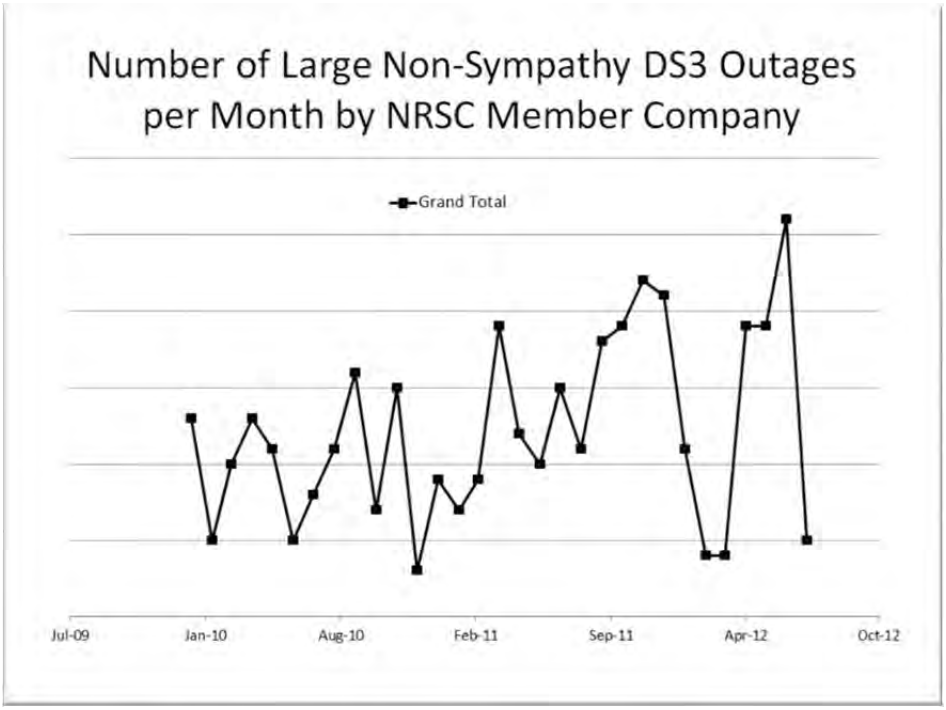

Figure 7 - Number of Large Non-Sympathy DS3 Outages

"Sympathy reports" is the industry term applied to FCC NORS outage reports that are filed under Part 4 rules when an outage in one service provider's network results in an FCC reportable condition for another service provider. Sympathy reports tend to over inflate the number of singular outage events occurring in the network that impact multiple providers. Although inclusion of sympathy reports can provide a picture of the interdependices between providers and overall impact, it can also skew the analysis results in a negative way.

In this analysis the exclusion of sympathy reports did not result in a major swing in the data. This lack of change indicates that the majority of large DS3 outages are reported by the circuit owner. It also indicates that failures in one service provider's network did not result in significant impact in other service provider's networks.

The next series of charts deal with the Direct Cause and Root Cause of outages. In order to properly interpret the data, a definition of each is provided below. These descriptions were provided to providers by the FCC for use when populating NORS outage reports.

The FCC NORS User Manual[12] defines Direct Cause as *the immediate event that results in an outage* and as *the event, action, or procedure that triggered the outage*. NORS users are provided a pick list of pre-designed choices. The service provider chooses the most accurate item from the list to describe the direct cause. The FCC NORS Manual defines Root Cause as *the underlying reason why the outage occurred or why the outage was reportable* and that the *Root Cause is the key problem which once identified and corrected will prevent the same or a similar problem from recurring*. *For any single incident there should be only one primary cause – the Root Cause*. As with Direct Cause, NORS users are provided a Root Cause pick list to choose from. It should be noted that the Direct and Root Causes and Contributing Factor choices consist of the same set of pre-designed choices.

Data illustrated on the following charts are based on the percentage related to how often a service provider chose a specific item from the drop down pick list as the most accurate Direct or Root Cause. These percentages are calculated against the total number of qualifying outage reports identified as impacting 1,000 or more DS3s or equivalents.

Top 80% of Root Causes - All Events

Root Cause	Percent
Hardware Failure - Circuit Pack-Card Failure-Other	31.2
Insufficient Data - Outside Owned Network	9.6
Cable Damage - Other	7.1
Cable Damage - Digging error	6.7
Cable Damage-Malfunction - Cable Malfunction	5.5
Procedural - Service Provider - Other	4.2
Hardware Failure - Other	3.4
Procedural - Other Vendor - Insufficient supervision-control	2.5
Environment (External) - Vandalism-theft	1.7
Procedural - Service Provider - Insufficient supervision-control	1.7
Environment (External) - Vehicular accident	1.5
Cable Damage-Malfunction - Aerial-Non-Buried	1.3
Environment (External) - Animal Damage	1.3
Environment (External) – Fire	1.3
Hardware Failure - Passive Devices	1.3

Figure 8 -Top 80% of Root Causes – All Events

[12] *FCC Network Outage Reporting System User Manual* Version 7, December 17, 2012.

Figure 8 illustrates the top 80% of root causes for qualifying outages. This chart includes all outage events including sympathy reports. The data indicates that within the top 80% hardware failure of circuit packs, passive devices, and other non specified incidents represents a total of 35.9%. Cable damage represents 20.6% of the total and the second highest root cause. Procedural (8.4%), Insufficent Data (9.6%), and Environmental (5.8%) complete the top 80%. Note that Insufficient Data – Outside Owned Network represents sympathy reports and the root cause would be determined on the triggering event.

Top 80% of Root Causes – Non Sympathy

Root Cause	Percent
Hardware Failure - Circuit Pack-Card Failure-Other	39.5
Cable Damage - Digging error	7.7
Cable Damage - Other	6.1
Cable Damage-Malfunction - Cable Malfunction	4.8
Procedural - Service Provider - Other	4.5
Hardware Failure - Other	4.2
Procedural - Other Vendor - Insufficient supervision-control	2.9
Environment (External) - Vandalism-theft	1.9
Environment (External) - Animal Damage	1.3
Hardware Failure - Passive Devices	1.3
Cable Damage - Cable unlocated	1.1
Design - Hardware - Poor card-frame mechanisms (latches, slots, jacks, etc.)	1.1
Design - Software - Ineffective fault recovery or re-initialization action	1.1
Environment (External) - Lightning-transient voltage	1.1
Environment (External) - Vandalism/theft	1.1
Environment (External) - Vehicular accident	1.1

Figure 9 - Top 80% of Root Causes – Non Sympathy

Figure 9 illustrates the top 80% of root causes for qualifying outages with sympathy reports excluded. By removing sympathy reports, the NRSC believes that the data represents a more accurate depiction of triggering events filed by service providers. Removing the sympathy reports alters the root causes and increases hardware failures to 45%, Cable Damage drops to 19.7%, Procedural events drop to 7.4%, Evironmental events increase to 6.5%, and Hardware/Software design events are added to the list (2.2%). The data shows that removing sympathy reports does not significantly change the overall root cause drivers for the outages.

Top 80% of Direct Causes – All Events

Direct Cause	Percent
Cable Damage - Other	40.5
Hardware Failure - Circuit Pack-Card Failure-Other	21.4
Hardware Failure - Other	19.7

Figure 10 - Top 80% of Direct Causes – All Events

Figure 10 contains the top 80% of direct causes for qualifying outages including sympathy reports. The direct cause is the trigger that results in the outage. Hardware Failure involving circuit packs or other hardware issues were triggers for 41.1% of the reported events. Cable Damage was identifed on 40.5% of the large DS3 events. This data indicates a pattern of hardware and cable damage exists and becomes a objective for recommendations for outage mitigation.

Top 80% of Direct Causes – Non Sympathy

Direct Cause	Percent
Cable Damage - Other	31.8
Hardware Failure - Circuit Pack-Card Failure-Other	27.1
Hardware Failure - Other	24.7

Figure 11 - Top 80% of Direct Causes – Non Sympathy

Figure 11 contains the top 80% of direct causes for qualifying outages excluding sympathy reports. With the additional reports removed for clarity, the percentage of hardware trigger events increased to 51.8%. Cable damage goes down to 31.8% indicating other service providers identifed cable damage when reporting an other company caused event in NORS. However, even with sympathy reports excluded, the data continues to show the trend of hardware and cable damage as primary drivers for these larger DS3 events.

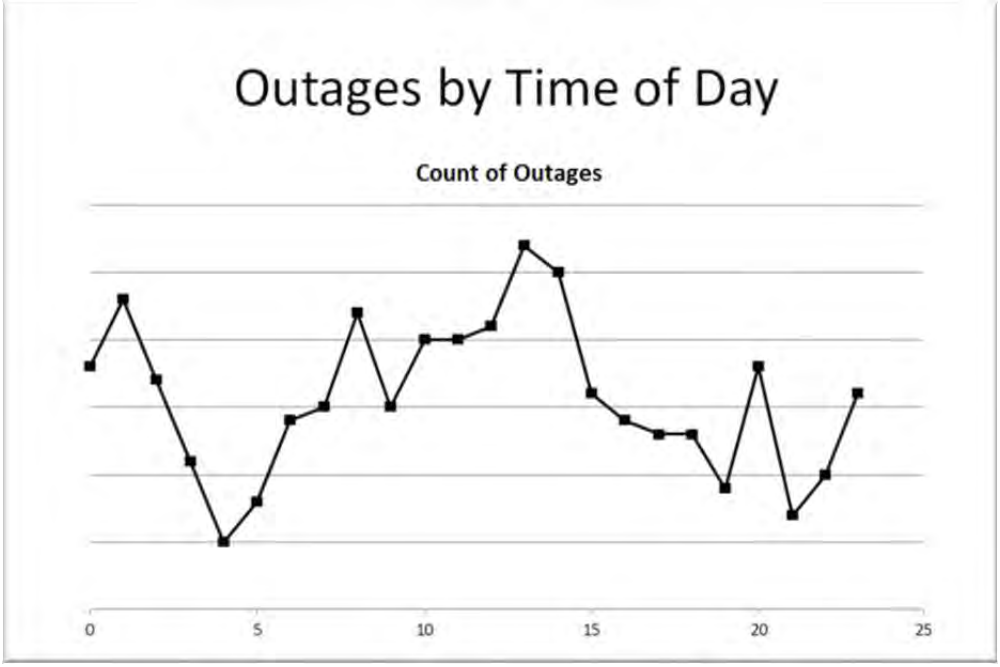

Figure 12 - Outages by Time of Day

Figure 12 illustrates a breakdown of all outage events by time of day. The team believed that plotting the outages across a chart in this fashion may suggest a trend related to scheduled maintenance or other time of day factors. On this chart, zero (0) represents any outage beginning at 12:00 a.m. – 12:59 a.m., one (1) representing outages beginning at 1:00 a.m. – 1:59 a.m., etc. up through 12:00 p.m. – 12:59 p.m. Data used for this chart includes all events, including sympathy reports. The data points to outage spikes trending during the maintenance window and mid-day hours. This is relevent when considering Hardware and Cable Damages are the primary drivers of these outages. When considering unprotected services, maintenance activity in the early hours can explain a percentage of failure because facilities often must be taken down to perform certain types of maintenance. Also, a higher spike in mid-day could be an indicator for when cable damage is most likely to occur.

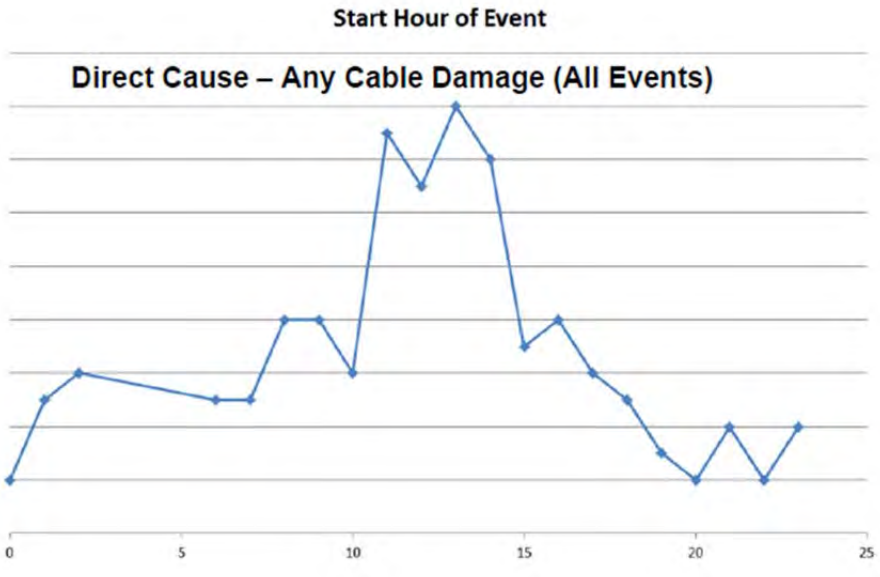

Figure 13 - Outages by Time of Day – Direct Cause – Any Cable Damage

Figure 13 is a further breakdown of all outage events by time of day where any cable damage was reported as the direct cause triggering event. On this chart, zero (0) represents any outage beginning at 12:00 a.m.– 12:59 a.m., one (1) representing outages beginning at 1:00 a.m. – 1:59 a.m., etc. up through 12:00 p.m. – 12:59 p.m. Cable damage during the mid-day hours is significant when compared to the earlier or later hours of the day. The data clearly shows a higher number of cable damage events between the hours of 10:00 a.m. – 4:00 p.m. regardless of the time zone the event occurred in.

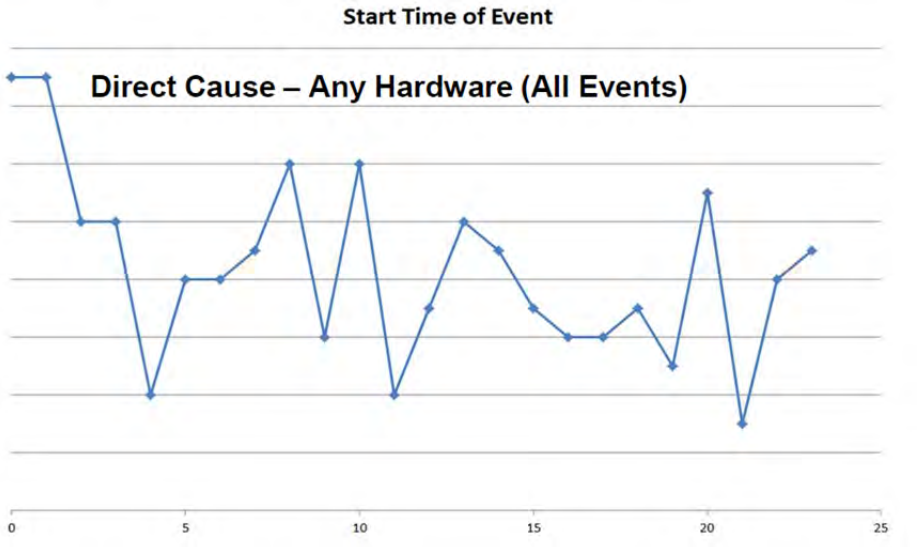

Figure 14 - Outages by Time of Day – Direct Cause – Any Hardware

Figure 14 is a further breakdown of all outage events by time of day where any hardware was reported as the direct cause triggering event. On this chart, zero (0) represents any outage beginning at 12:00 a.m.– 12:59 a.m., one (1) representing outages beginning at 1:00 a.m. – 1:59 a.m., etc. up through 12:00 p.m. – 12:59 p.m. Although not as pronounced as cable damage in the previous chart, the data confirms the idea that hardware failures in the maintenance window hours are higher than other times of day. The highest spikes are seen between the 12:00 a.m. and 3:00 a.m. time period regardless of time zone. However, the data also suggests that hardware failures are more spread out throughout the day based on NORS reports.

Root Cause for Direct Cause - Cable Damage – Other (All Events)

Root Cause	Percent
Cable Damage - Digging error	20.0
Cable Damage - Other	16.7
Cable Damage-Malfunction - Cable Malfunction	12.5
Environment (External) - Vandalism-theft	5.8
Environment (External) - Animal Damage	4.2
Procedural - Other Vendor - Insufficient supervision-control	4.2
Environment (External) - Lightning-transient voltage	3.3
Environment (External) - Vandalism/theft	3.3
Cable Damage - Inadequate-no notification	2.5
Cable Damage-Malfunction - Aerial-Non-Buried	2.5
Environment (External) - Vehicular accident	2.5
Insufficient Data	2.5

Figure 15 - Root Cause for Direct Cause – Cable Damage - Other

Figure 15 provides an analysis on what Root Cause was chosen by service providers for the primary chosen Direct Cause for Cable Damage – Other including sympathy reports. In other words, what was the overall Root Cause of the outage once triggered by the Direct Cause. This breakout is important to better comprehend the types of cable damage being reported and to suggest a possible path for mitigation recommendations. The top three drivers for cable damage are digging errors (20%) (e.g., cables located but damaged or mislocated cables), other unspecified failures (16.7%), and cable malfunction (12.5%) (e.g., fiber cable microbends or breaks, connector failures). Another area of concern is Vandalism/Theft (9.1%) which is an indicator that fiber cables in some cases may have been mistaken for copper cables by criminals resulting in an outage to the tranport network.

Root Cause for Direct Cause - Hardware Failure - Circuit Pack-Card Failure-Other (All Events)

Root Cause	Percent
Hardware Failure - Circuit Pack-Card Failure-Other	88.2
Design - Software - Ineffective fault recovery or re-initialization action	3.9
Environment (Internal) - Other	2.0
Cable Damage - Other	1.0
Environment (Internal) - Environmental system failure (heat/humidity)	1.0
Hardware Failure - Circuit Pack/Card Failure-Processor	1.0
Hardware Failure - Other	1.0
Hardware Failure - Peripheral unit failure	1.0
Insufficient Data - Under Investigation	1.0

Figure 16 - Root Cause for Direct Cause – Hardware Failure – Pack/Card Failure - Other

Figure 16 provides an analysis on what Root Cause was chosen by service providers for the primary Direct Cause of Hardware Failure – Circuit Pack-Card Failure-Other including sympathy reports. The data indicates the most significant cause of failure to be circuit packs. In a dual path arrangement, the possibility of a single pack failure resulting in an outage is problematic. However, in an unprotected design, single pack failures would result in a loss of capacity. Similarly, a discovery of pack failure from a single product line or manufacturer would be more alarming than failures across all product lines in the network. In this investigation, the NRSC cannot attribute pack failures to a single vendor or product line. However, data revealed a moderate percentage of the pack failures attributable to system optics (e.g., lasers and ramen pumps).

Root Cause for Direct Cause - Hardware Failure – Other (All Events)

Root Cause	Percent
Hardware Failure - Circuit Pack-Card Failure-Other	61.3
Hardware Failure - Other	12.9
Hardware Failure - Passive Devices	4.3
Design - Hardware - Poor card-frame mechanisms (latches, slots, jacks, etc.)	3.2

Figure 17 - Root Cause for Direct Cause – Hardware Failure – Other

Figure 17 provides an analysis on what Root Cause was chosen by service providers for the primary chosen Direct Cause of Hardware Failure – Other including sympathy reports. This data also specifies pack failure as a top driver for large DS3 failures occurring in the study. Hardware Failure – Other (12.9%) indicates that not all

failure types can be categorized by the current FCC NORS Root and Direct cause categories. This analysis also identifed that a the small percentage (3.2%) of failures were the result of poor design, which was identifed by the specific service provider. Passive devices (i.e., non electronic) provide evidence that mechanical or non-active elements in a design can and do fail a small percentage of the time (4.3%).

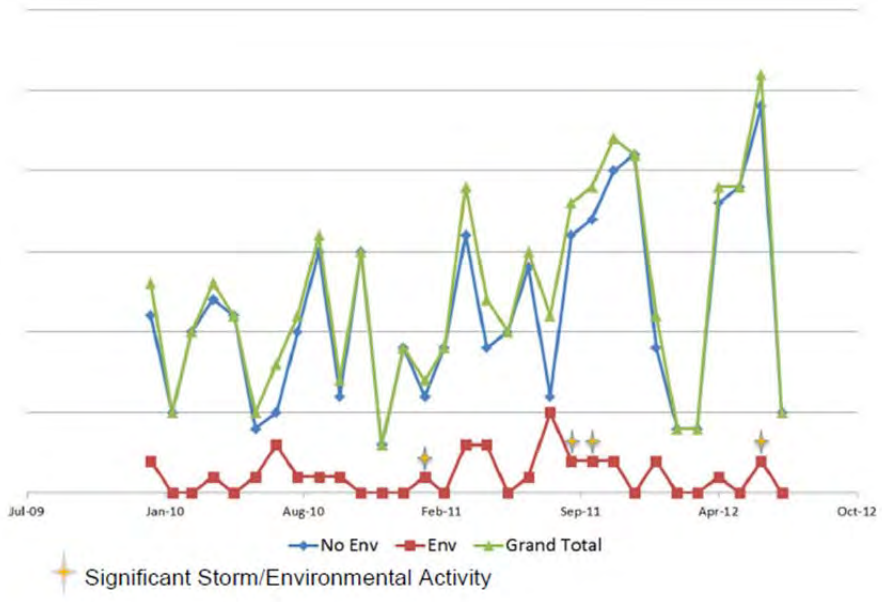

Figure 18 - Direct and Root Cause - Environmental Impact

The team also researched recent major storm activity and how the storms may have impacted the resiliency of larger DS3 capacity systems. Figure 18 plots the NORS reports where the direct or root cause was marked as Environmental, with the exception of vehicular damage and vandalism/theft or included one or more keywords describing a storm event. The “Env” line in the chart depicts the outages related to storm activity. Four recent events were identified:

- January 2010 snowstorm in the Washington, DC Metro area;
- September 2012 earthquake in the Northeast United States;
- October 2012 snowstorm in the Northeast United States; and
- June 2012 Derecho storm in the Midwest and Mid-Atlantic United States.

The data shows that enviromental 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 threshold 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.

6.2 Findings

Based on the NRSC analysis over a study period of 31 months, several issues and findings are presented below:

Reviewed Issue	Findings
Accuracy of Data	• Study data does not represent the industry as a whole, but does provide a significant view of the overall outages reported to the FCC. • When large capacity systems are impacted, providers must convert the bandwidth to DS3 equivalents for assessing outage reporting under the Part 4 rules.
Bandwidth Usage	• The transport network is evolving. • As bandwidth has exponentially increased, the conceptual term DS3 continues to be recycled to describe *equivalency,* even though it is not in principle a correct use of the term. • As consumer demand for high speed protected and unprotected services increase, data consumption multiplies, driving the need to use these larger systems for economy of scale. • In newer architectures a failure of a large capacity system may have little to no impact on individual users when traffic is rerouted using diversity schemas or when the entire bandwidth is being used by an individual enterprise or government entity.
Customer Demand	• Customer demand for unprotected services is increasing. • A mixed use of protected services and unprotected services could be detected in analyzed outage reports. • Most communication service providers currently offer unprotected circuit terminations or lightpaths to provide affordable dedicated bandwidth. • Customers who purchase unprotected lightpaths or circuits are typically aware of risks and limitations related to network resiliency and diversity. • A knowledgeable consumer is better able to evaluate their needs and risks for service and application diversity.
Diversity Issues	• Three types or levels of diversity were defined relevant to the use of large capacity systems: o *Network Diversity* – Within service provider's span and control and prior to the demarcation point with other provider networks. o *Diversity Services* – Customer shares the responsibility for the level of diversity built into their design. o *Application Diversity* – Exclusively within the responsibility of the customer independent of the service provider. • Large capacity system outages analyzed by the team were consistent with network diversity and diversity services. • Service providers should continue to implement appropriate industry Best Practices regarding network diversity to provide the highest level of reliable and resilient service.

Reviewed Issue	Findings
Data Analysis	• The data overall indicates the outages are mostly in control within the study period. • The trend indicates that NRSC member companies are contributing to the increase of these types of events. • The immediate causes of failure could be categorized in two areas: Hardware Circuit Packs and Cable Damage. • The vendor a service provider uses drives the card/element types being reported during hardware failures. • Data cannot attribute hardware pack failures to a single vendor or product line. • A certain number of >1000 DS3s are a summarization of storms where providers combined multiple elements. • Excluding sympathy reports does not significantly change the overall root cause drivers for the outages. • Failures in one service provider's network did not result in significant impact in other service providers' networks. • Outages trend up during maintenance window and mid-day hours. • Higher number of cable damage events occur between the hours of 10:00 a.m. – 4:00 p.m., regardless of the time zone. • Higher number of hardware events occur between the 12:00 a.m. and 3:00 a.m. time period regardless of time zone; however, more generally spread throughout the day. • Data shows that enviromental conditions are not a significant contributor in the causes of large DS3 events.
Network Reliability	• A number of the reported events involved unprotected wavelengths. • Data does not support a problem with repeat failures on the same circuits; impact is spread throughout the network. • Lack of repeat failures over the study period shows a level of reliability exists for unprotected services. • Unprotected service maintenance activity explains a percentage of failure since facilities often must be taken down to perform certain types of maintenance. • A moderate percentage of the hardware pack failures could be attributed to system optics (e.g., lasers and ramen pumps). • Passive devices (i.e., non electronic) can and do fail.

7 Conclusions

The NRSC does not believe that there is a network reliability issue associated with large bandwidth systems. With the exception of several months of higher than normal hardware failures and cable damage, the trend is generally stable. Several dynamics exist that help explain the direct and root causes of the outages, which are not different than those that affect smaller transport elements. While the NRSC agrees that the use of unprotected bandwidth is susceptible to singular failures, large scale impacts were not reported by multiple providers, customers using the transport capacity, or by local media. The NRSC's investigation concludes that a large bandwidth outage does not necessarily or directly equate to significant network or customer impact.

The NRSC also concludes that consumers purchasing large bandwidth services have a responsibility to design and purchase appropriate levels of diversity to protect critical communication services. Customer demand for unprotected high bandwidth services will continue to grow. The ATIS NDAI Report correctly warns customers to consider and take responsibility for their diversity. The NRSC supports this view and recommends that service providers and network operators follow industry Best Practices where appropriate to provide the highest level of reliability possible.

The NRSC concludes that additional research may be needed as networks grow and technology continues to change. This analysis may further assist in determining if NORS has appropriate thresholds to assess customer impact or adequate data fields to capture nuances associated with newer architectures. With reference to the high quantity of circuit pack failures, the NRSC suggests that service providers work closely with their vendors and hold them accountable for reliability and resiliency when their circuit packs have high failure rates. The NRSC also concludes that cable damage in some instances is preventable. However, it is not always within the service provider's or network operator's ability to prevent cable damage. That said, a robust cable damage prevention program can minimize risk.

8 Recommendations

The NRSC Large DS3 Outage team provides the following recommendations regarding the issue of outages where 1,000 or more DS3s or equivalents are involved:

INDUSTRY BEST PRACTICES

Providers should review the following industry Best Practices related to circuit pack failures and network reliability:

Number	Best Practice
8-7-0455	Equipment Suppliers should consider a program to remove cards or modules from circulation that have a history of failure even if tests indicate "No Trouble Found".
8-7-0404	*Network Performance*: Service Providers, Network Operators, and Equipment Suppliers should incorporate methodologies that continually improve network or equipment performance.
8-7-0406	*Spares and Inventory*: Network Operators and Service Providers should, where appropriate, establish a process to ensure that spares inventory is kept current to at least a minimum acceptable release (e.g., hardware, firmware or software version).
8-7-0501	Network Operators and Service Providers should report problems discovered from their operation of network equipment to the Equipment Supplier whose equipment was found to be the cause of problem.
8-7-0504	Network Operators and Service Providers, in order to facilitate asset management and increase the likelihood of having usable spares in emergency restorations, should consider maintaining "hot spares" (circuit packs electronically plugged in and interfacing with any element management system, as opposed to being stored in a cabinet) for mission critical elements.
8-7-0747	Network Operators, Service Providers, and Equipment Suppliers should work together to establish reliability and performance objectives in the field environment.
8-7-5080	Network Operators should identify and track critical network equipment, location of spares, and sources of spares to ensure the long term continuity and availability of communication service.
8-7-5083	Network Operators, Service Providers, and Equipment Suppliers should maintain the availability of spares for critical network systems.
8-7-0400	*Network Performance Measurements*: Network Operators and Service Providers should establish measurements to monitor their network performance.
8-7-0738	Network Operators and Service Providers should track and analyze facility outages taking action if any substantial negative trend arises or persists.

Providers should review the following industry Best Practices related to cable damage:

Number	Best Practice
8-7-0735	Network Operators should evaluate the performance of their contracted excavators and internal excavators to foster improved network reliability.
8-7-5263	Network Operators, Service Providers, and Equipment Suppliers should use cables with adequate reliability and cable signal integrity. Such properties as flammability, strain reliefs, and signal loss should be considered. If non-standard cables are used because of an emergency restoration, they should be marked as temporary and should be replaced with standard cables as soon as practical.
8-7-0705	Network Operators should use warning tape on buried facilities – place tape 12 in. above the cable system.
8-7-0706	Network Operators should use visible cable markings on buried facilities (unless prone to vandalism).
8-7-0709	Network Operators should compare outside plant drawings relative to marking cable route maps when locating buried facilities and resolve any discrepancies.
8-7-0722	Network Operators, Service Providers, and Property Managers should consider pest control measures to protect cables where appropriate.
8-7-0726	Network Operators should consider partnering with excavators, locators, and municipalities in a cable damage prevention program.
8-8-0784	*Cable Management*: Network Operators and Service Providers should utilize appropriate fiber/cable management equipment or racking systems to provide cable strain relief and ensure that bend radius is maintained to avoid micro-bends (e.g., pinched fibers).
8-7-0423	*Cable Management*: Equipment Suppliers should provide cable management features and installation instructions for network elements that maintain cable bend radius, provide strain relief to prevent cable damage, ensure adequate cable connector spacing for maintenance activities, and provide clear access for cable rearrangement (i.e., moves/add/deletes) and FRU (Field Replaceable Unit) swaps.
8-7-0733	Network Operators, when relocating buried facilities in a common right-of-way, should coordinate activities with other right-of-way occupants to minimize the potential for damage.
8-7-0741	Network Operators and Service Providers should review, and adopt as appropriate, best practices aimed at reducing damage to underground facilities that are maintained by the Common Ground Alliance (< http://www.commongroundalliance.com >).
8-7-0719	Network Operators should use “dig carefully” concepts and utilize guidance from industry sources when installing underground facilities.

Providers should review the following industry Best Practices related to network diversity:

Number	Best Practice
8-7-0532	*Diversity Audit*: Network Operators should periodically audit the physical and logical diversity called for by network design and take appropriate measures as needed.
8-7-0549	Network Operators should develop an engineering design for critical network elements and inter-office facilities that addresses diversity, and utilize management systems to provision, track, and maintain that inter-office and intra-office diversity.
8-7-1065	Network Operators and Service Providers should identify and manage critical network elements and architecture that are essential for network connectivity and subscriber services considering security, functional redundancy, and geographical diversity.
8-7-5075	*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).
8-7-5079	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.

Number	Best Practice
8-8-0731	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.

OTHER RECOMMENDATIONS

1. Service providers that sell unprotected services should ensure they have processes in place to appropriately provide customers who purchase unprotected lightpaths or circuits with information on the risks and limitations.
2. Customers purchasing protected or unprotected lightpaths or circuits should consider reviewing the ATIS Network Diversity Assurance Initiative (NDAI) Report regarding their diversity.