Technical Report

CenturyLink Communications, LLC

UT-181051

Staff Consultant

Jeffrey Wheeler, Technical Architect

April 2021

Introduction

Washington state experienced a state-wide outage of its enhanced 911 (E911) emergency services lasting from the early morning of December 27, 2018 to December 29, 2018. At the time of the outage, CenturyLink Communications, LLC (CenturyLink or company)[1] was the incumbent Washington state E911 service provider.

The December 2018 outage intermittently disrupted E911 emergency service in Washington for 49 hours and 32-minutes and impacted the entire state. The outage impaired several modes of connecting with E911, including wireline, wireless, and Voice over Internet Protocol (VoIP) calls. Washington residents attempting to access E911 service during the outage encountered fast busy signals, no dial tone, and silent calls.

The root cause analysis determined that the outage was caused by the generation of malformed packets and a subsequent broadcast storm that was exacerbated by CenturyLink's management and communications processes internally and externally. The root cause was a broadcast storm[2] triggered by an incorrect configuration in the CenturyLink network nodes supplied by its vendor, Infinera Intelligent Transport Networks (Infinera).[3] As a result of the broadcast storm, the network failed, and services were impacted intermittently over the course of the outage.

Additionally, the analysis finds CenturyLink did not comply with industry guidelines and best practices as put forth by the Federal Communication Commission (FCC), the FCC's Communications Security, Reliability, and Interoperability Council (CSRIC), and other standard bodies.

Washington State E911 Overview

In Washington state when a customer dials 911, the call is carried to a local switching office and is then transported to a network gateway switch in either Spokane or Seattle, the call queries a database to gain location information associated with the calling party that originated the 911 call, and the 911 call is then delivered to the designated Primary Safety Answering Point (PSAP).

Generally, E911 calls originating from locations in western Washington are directed to the Seattle gateway network switch and E911 calls originating in eastern Washington are directed to the Spokane gateway network switch. Each gateway provides alternate call routing services for

[1] All Commission registered names are as follows: CenturyLink Communications, LLC, CenturyLink, CenturyTel of Washington, Inc., CenturyTel of Inter Island, Inc., CenturyTel of Cowiche, Inc., United Telephone Company of the Northwest, Qwest Corporation dba CenturyLink QC.

[2] A broadcast storm is a pathological condition that may occur in a TCP/IP network that can cause broadcast packets to be propagated unnecessarily across an enterprise-wide network, causing network overload. A chain reaction can produce so many broadcast messages that the network can shut down. Newton's Telecom Dictionary, 28th ed. (2014).

[3] Infinera Intelligent Transport Networks (Infinera), a vendor that provides equipment and professional services to CenturyLink, including nodes and cards.

the other and contains a primary and secondary switch, thereby providing high availability and redundancy should one of the gateways fail.

When a E911 emergency call is made, that call is routed to the appropriate PSAP using Automatic Location Identifier (ALI) data associated with the telephone number used by a caller. ALI data contains data used to identify a caller's location and subscriber information.[4] Without ALI data, a call will not, in most cases, be delivered to a PSAP. At the time of the Washington December 2018 service outage, [redacted].[6]

Three-Phase PSAP Migration Project Snapshot Prior to the Outage

The Washington Military Department (WMD) implemented a three-phase migration approach to transition Washington's 62 PSAPs from CenturyLink's ESInet to Comtech's ESInet 2. At the time of the December outage, Washington's E911 services were in the process of being transferred from CenturyLink to another service provider, TeleCommunication Systems, Inc., d/b/a Comtech Telecommunications Corp. (Comtech). The service migration from CenturyLink to Comtech was divided into three separate phases.[7] The goal of the three-phase migration project was to transfer all 62 primary Washington PSAPs from CenturyLink's ESInet to the Comtech's ESInet 2, after which Comtech would act as the E911 service provider to Washington PSAPs.[8]

Migration Project Status at Time of Outage (Phase One)

The service migration was in phase one of the network migration project when the December outage occurred.[9] Phase one of the migration project involved moving PSAPs using the CenturyLink's ESInet to the Comtech's Next Generation 911 (NG911) ESInet 2.[10] Once completely implemented, the ESInet 2 network that Comtech develops and manages would be substantially different from the CenturyLink ESInet in that it is an end-to-end internet protocol (IP) network configuration platform.

Phase two of the migration was scheduled later in the process and involved [redacted] Phase three of the project was intended to [redacted].[11]

---

[4] All records or other information relating to customers or subscribers of a service provider of the type referred to and accessible subject to procedures specified in 18 U.S.C. § 2703(c) or (d) or 18 U.S.C. § 2709.
[5] West Telecom Services, LLC changed its name to Intrado Communications, LLC, with the Commission effective May 1, 2020.
[6] UT-181051, Staff Investigation Report, Appendix D (C).
[7] UT-181051, Staff Investigation Report, Appendix D (C).
[8] As of Feb. 2021, there are 83 PSAPs, including 51 primary, 27 secondary, 3 back-up, and 2 test PSAPS.
[9] *See*, UT-181051, Staff Investigation Report, Appendix D (C).
[10] ESInet 2 is an ASCI standard certified Internet Protocol platform. For more information, *NENA i3 NG911 architecture STA-010.3*, *available at* https://www.nena.org/general/custom.asp?page=FuncIntrface_NG911
[11] UT-181051, Staff Investigation Report, Appendix D (C).

[redacted][13] [redacted][14] On Dec. 27, 2018, CenturyLink had successfully transferred 47 of the 62 Washington state PSAPs from its ESInet to Comtech's ESInet 2.[15] At the time of the December 2018 outage, E911 calls in Washington were processed as follows:[16]

[redacted]

December 2018 Outage

[12] UT-181051, Staff Investigation Report, Appendix D (C).
[13] Public telecommunications transport network means infrastructure which permits communications between and among defined network termination points. Newton's Telecom Dictionary, 28th ed. (2014), pg. 1245.
[14] UT-181051, Staff Investigation Report, Appendix D (C). See also, CenturyLink WMD Contract, E09-196, Amendment M ([redacted])("[redacted]").
[15] UT-181051, Staff Investigation Report, Appendix E.
[16] UT-181051, Staff Investigation Report, Appendix D (C).

CenturyLink informed commission staff of the following information pertaining to the outage by email on December 28, 2018:[17]

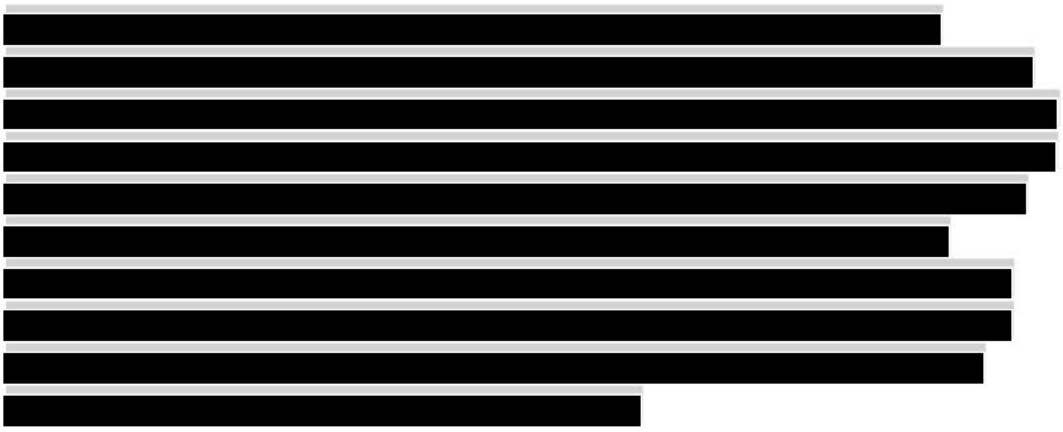
[redacted]

[17] UT-181051, Staff Investigation Report, Appendix T (C).

The CenturyLink network outage report filed with the commission on December 31, 2018 includes detailed network information related to the outage that began on December 27, 2018.[18] In its report Century Link stated:[19]

[redacted]

[18] UT-170042, CenturyLink Reason for Outage Report, December 31, 2018, attached as Appendix B (C).
[19] Id.



FCC Network Outage Report

On August 19, 2019, the FCC published a report regarding the December 28, 2018 outage. The report stated in part that on the "morning of December 27, 2018, CenturyLink experienced a nationwide outage on its fiber network that lasted for almost 37 hours." [20] The FCC observed:[21]

> In the affected network, network traffic transits across nodes, where data enters and exits the network. At the time of the outage, the affected network used nodes supplied by Infinera Intelligent Transport Networks (Infinera). Each node provides optical fiber switching, a process that ensures that network traffic is directed towards the intended network path, between networks components called line modules. Line modules provide the connection points between nodes across the country. Internal to each node, a component called a switching module transfers packets from inbound line modules to outbound line modules. The switching module directs traffic that arrives on a particular port and stream of an inbound line module to the correct port on the correct outbound line module.

The FCC further stated:[22]

> The nodes in the affected network possess a proprietary internode management channel. This proprietary management channel is designed to allow for very fast, automatic rerouting of traffic to avoid a loss of traffic during a failure in the network. It does this by enabling line modules to send packets directly to other connected nodes without receiving network management instructions about how to route traffic. To prevent management instructions from being sent to other nodes, the proprietary management channel has a filter that prevents packets that are 64 bytes or fewer from using the channel. As the supplier of these nodes, Infinera provides its customers – including CenturyLink in this case – with the

[20] UT-181051, Staff Investigation Report, Appendix C at 3, ¶ 1.
[21] UT-181051, Staff Investigation Report, Appendix C at 5, ¶ 8.
[22] UT-181051, Staff Investigation Report, Appendix C at 6, ¶ 9.

primary management channel enabled by default. CenturyLink was aware of this channel but neither configured it nor used it.

Duration and Impact of Outage in Washington

On Dec. 27, 2018, Washington began experiencing a statewide outage of its E911 emergency system. Once it became aware of the outage, CenturyLink began attempting to diagnose and resolve the outage. Nearly 37 hours after the outage began, CenturyLink resolved the network impairment.[23] Other carriers that relied on CenturyLink service, including Comtech, did not achieve full service restoral until 49 hours, 32 minutes after the outage began.[24] Comtech further reported that it received no NG911 or wireless E911 calls during three periods of time during the outage:[25]

Dec. 27, 2018, 3:48 a.m. – Dec. 27, 2018, 4:16 a.m.

Dec. 27, 2018, 11:00 p.m. – Dec. 28, 2018, 6:26 a.m.

Dec. 28, 2018, 9:05 a.m. – Dec. 28, 2018, 9:57 a.m.

The outage affected 22 million customers across 39 states, including approximately 17 million customers across 29 states who lacked reliable access to E911.[26]

Findings

CenturyLink's network consists of six primary long-haul transports. [redacted][27] The December 2018 outage was caused by a network error on that transport network that led to the network's impairment and inability to properly route calls.

Specifically, the December 2018 outage was caused by CenturyLink's failure to properly configure its management channel in the network infrastructure.[28] This misconfiguration of Infinera nodes led to a broadcast storm, which impaired the ability to forward IP packets across the transport network.

Best Practices and Industry Recommendations

[23] UT-181051, Staff Investigation Report, Appendix C at 8, fn. 25 ("While the nodes had been restored, other services that had been negatively affected did not automatically come back online, necessitating further restoration work by CenturyLink and its vendors. For example, CenturyLink's own cloud services remained unavailable for over 20 hours after the network was restored.").
[24] UT-181051, Staff Investigation Report, Appendix C at 9-10, ¶ 19.
[25] UT-181051, Staff Investigation Report, Appendix C at 10, ¶ 20.
[26] UT-181051, Staff Investigation Report, Appendix C at 3, ¶ 1.
[27] UT-181051, Staff Investigation Report, Appendix U (C).
[28] UT-181051, Staff Investigation Report, Appendix C at 6-9.

Industry recommendations and best practices applicable to emergency services and 911 are put forth by several organizations, including the FCC, CSRIC, and the National Emergency Number Association (NENA).[29]

The FCC regulates 911 for communications services including VoIP, mobile satellite services, telematics, and Text Telephone Devices (TTYs). These are important parts of FCC programs to apply modern communications technologies to public safety. In the FCC's 911 Reliability Order, 911 service providers are required to provide reliable 911 service using circuit diversity, central office backup power, and diverse network monitoring.[30] The FCC 911 Reliability Order identifies critical actions for 911 services including auditing for circuit diversity and identifying transport paths.[31] The FCC states that "because IP-based NG911 networks may not employ circuit-switched technologies, we intend the auditing obligation to extend to data transport paths for the core 911 capabilities . . . regardless of whether they are technically 'circuits'."[32]

CSRIC is a standards body with the purpose of providing recommendations for security, reliability, and interoperability of communications systems. CSRIC's recommendations focus on public safety, including reliability of communications systems and infrastructure and 911, E911, and NG911. CSRIC's recommends best practices to improve: 1) overall communications reliability; 2) the availability and performance of communications and the rapid restoration of communications services in the event of widespread or major disruptions, and; 3) the steps communications providers can take to help secure end-users and servers.[33] Further, CSRIC best practices advises network operators to "audit the physical and logical diversity called for by network design of their network segment(s) and take appropriate measures as needed."[34]

NENA publishes documents that are an information source for the industry. NENA has opined that network design and architecture supporting 911 service is increasingly populated with identifiable potential points of failure.[35] Although multiple points of failure present a greater potential risk of outages, this risk can be reduced if new and existing network features, coupled with physical route diversity, are employed. In fact, route diversity, network visibility, and remote troubleshooting, when properly implemented, can increase network reliability.

---

[29] NENA is accredited by the American National Standards Institute, which oversees standards and conformity assessment activities in the United States.

[30] *In re Improving 911 Reliability*¸ FCC 13-158, Report and Order, 17503, ¶ 81-82 (December 12, 2013) (911 Reliability Order), *available at* https://docs.fcc.gov/public/attachments/FCC-13-158A1_Rcd.pdf.

[31] 911 Reliability Order at 17503, ¶ 80. Diversity audits check for "single points of failure" in network configurations, while tagging ensures that changes to critical 911 assets cannot be made without rigorous review.

[32] 911 Reliability Order at 17503-04, ¶ 80-82.

[33] *See*, Communications Security, Reliability, and Interoperability Council, *available at https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council-0*

[34] CSRIC *Best Practice 12-9-0532*, *available at* https://opendata.fcc.gov/Public-Safety/CSRIC-Best-Practices/qb45-rw2t

[35] NENA, TID 03-501, Network Quality Assurance, Revised October 3, 2005, *available at https://www.NENA.org/general/custom.asp?page=ntwkqualityassurance*

As a network operator and service provider, CenturyLink should have utilized remote networking visibility features and alarms to monitor the status and functionality of its transport network.[redacted]

However, due to deficiencies in CenturyLink's network planning, visibility, and troubleshooting, the company experienced multiple points of network failure during the 2018 outage within the affected transport network. The affected CenturyLink transport network provided service for multiple carriers and [redacted] Had CenturyLink conformed to industry best practices regarding support of E911 services and identified potential points of failure, the outage may have been shorter in duration or entirely avoided.

Based on review of the outage, the Commission should find that CenturyLink failed to comply with multiple CSRIC best practices, as described in Appendix A to this report, and that this failure contributed to or prolonged the duration of the December 2018 outage.[39]

Conclusion

The root cause analysis identifies CenturyLink's failure to properly configure the management channel in its network infrastructure as the cause of the December 2018 statewide outage that occurred in Washington. Specifically, the outage was caused by the generation of malformed packets, which developed into a broadcast storm as a result of CenturyLink's management and communications processes. Analysis identifies CenturyLink deficiencies regarding network management and diagnostic ability to detect the cause of the outage that hindered a timely response.

[36] Appendix B (C); UT-181051, Staff Investigation Report, Appendix U (C).
[37] Appendix B (C).
[38] UT-181051, Staff Investigation Report, Appendix D (C).
[39] Appendix A (C).

APPENDIX A
IS REDACTED IN ITS ENTIRETY

APPENDIX B

Reason for Outage

CenturyLink

Date: December 31, 2018

Incident Start Time: December 27, 2018 08:40 GMT
Service Restore Time: December 28, 2018 21:36 GMT
While most services restored on December 28, 2018 at 21:36 GMT, all residual impact restored on or before December 29. Due to the nature of this event restoral times varied.

The information in this communication is confidential and may not be disclosed to third parties or shared further without the express permission of CenturyLink.

CenturyLink experienced a network event beginning on December 27 that impacted voice, IP, and transport services for some of our customers. The event also impacted CenturyLink's visibility to the management network, impairing our ability to troubleshoot and prolonging the duration of the outage. [redacted]

[redacted]

This letter is for informational purposes only and is not meant to be an admission of liability (or otherwise) on the part of CenturyLink. This letter does not amend or otherwise alter your contractual rights or those of CenturyLink. We hope that the information provided has been of assistance. Please do not hesitate to contact your account manager or your Repair Center if you have any further questions.

The information in this communication is confidential and may not be disclosed to third parties or shared further without the express permission of CenturyLink.