BEFORE THE WASHINGTON
UTILITIES & TRANSPORTATION COMMISSION

WASHINGTON UTILITIES AND TRANSPORTATION COMMISSION

Complainant,

v.

CENTURYLINK COMMUNICATIONS, LLC, et al.,

Respondents.

DOCKET UT-181051

CROSS-ANSWERING TESTIMONY OF BRIAN ROSEN
ON BEHALF OF
WASHINGTON STATE OFFICE OF THE ATTORNEY GENERAL
PUBLIC COUNSEL UNIT

Exhibit BR-30CT

August 31, 2022

Shaded Information is Designated Confidential
per Protective Order in Docket UT-181051
TABLE OF CONTENTS

I. INTRODUCTION / OVERVIEW ....................................................................................... 1
II. TECHNOLOGY CHOICES ................................................................................................ 2
III. DIVERSITY .................................................................................................................... 8
IV. TRANSITION RESPONSIBILITIES ............................................................................... 19
V. FAILURES IN THE GREEN NETWORK ....................................................................... 29
VI. CONCLUSIONS ........................................................................................................... 31

FIGURES

Figure 1 - Trust IP Interconnect ....................................................................................... 28
Figure 2 - Untrusted IP Based Interconnect .................................................................... 28
Figure 3 - SS-7 Based Interconnect ................................................................................ 28
EXHIBITS LIST

Exhibit BR-31  Public Counsel Response to CenturyLink Data Request No. 17 with Attachments
Exhibit BR-32C  Comtech Response to Public Counsel Data Request No. 31 with Confidential Attachment
I. INTRODUCTION / OVERVIEW

Q. Please state your name and business address.
A. My name is Brian Rosen and my business address is 470 Conrad Drive, Mars, Pennsylvania 16046. I am the principal consultant for Brian Rosen Technologies LLC, where I provide guidance to states and local governments on deployment of Next Generation 9-1-1 (NG9-1-1) systems.

Q. On whose behalf are you testifying?
A. I am testifying on behalf of the Public Counsel Unit of the Washington Attorney General’s Office (Public Counsel).

Q. Have you previously provided testimony in this proceeding?
A. Yes, I provided testimony for Public Counsel Unit of the Washington State Attorney General’s Office (Public Counsel).

Q. What exhibits are you sponsoring in this proceeding?
A. I am sponsoring the following exhibits:

- Exhibit BR-31 Public Counsel Response to CenturyLink Data Request No. 17 with Attachments
- Exhibit BR-32C Comtech Response to Public Counsel Data Request No. 31 with Confidential Attachment

Q. What is the purpose of your cross-answering testimony?
A. In this testimony, I respond to CenturyLink witness testimony with regard to technology choices, diversity, transition responsibilities and Green Network failure.
II. TECHNOLOGY CHOICES

Q. Refer to Exhibit SET-1TC at 8:17–18. CenturyLink witness Steven E. Turner states: “SS7 technology is commonly used by the industry in 911 network architecture.” Is this true?

A. Yes, however Signaling System 7 (SS7) is not commonly used in Next Generation 9-1-1 (NG9-1-1) systems other than in the originating service provider (OSP) interconnect. SS7 was used in the older E9-1-1 system in two places: connecting to some originating service providers and in tandem-to-tandem connections where multiple selective routers were interconnected. In some NG9-1-1 systems, SS7 is still used to connect OSPs to NG9-1-1 because those OSPs have not converted to Session Initiation Protocol (SIP), not because SS7 is superior technology.

Q. At the time of the outage, was the Washington 9-1-1 system an older E9-1-1 system you just described?

A. No. At the time of the outage, the Washington 9-1-1 system was transitioning from an early, IP-based service, which was a migration step to a standards-based NG9-1-1 system. For the CenturyLink system, which was established prior to the NG9-1-1 standards, the contract states: “To accomplish this, there must be a switch from the antiquated legacy analog telephone system to a system as used in cellular and computer voice over internet (VoIP) protocols by telephone and communication
providers.” CenturyLink’s network (ESIet 1) and Comtech’s network (ESIet 2) were both IP networks.

Q. Is it common in the industry to use an SS7 interconnect between two IP networks?

A. No. Using an SS7 interconnect between two IP networks is highly unusual.

Q. Based upon your review of the record, did CenturyLink and Comtech discuss other options for interconnecting the two IP networks?

A. Yes. Emails in the record make clear that Comtech attempted to get CenturyLink to use an IP interconnect that closely resembles the current NG9-1-1 standards for interconnecting ESIets. Comtech’s proposal used SIP signaling which adhered closely to SIP signaling used within a standards-based NG9-1-1 system. While the current NG9-1-1 standards were published after the outage at issue here, the similarity to the standards shows that Comtech’s IP interconnect proposal was reasonable.

Although the details remain unclear, it appears that CenturyLink proposed an IP interconnect that was quite different from what Comtech (and the eventual NG9-1-1 standards) described. CenturyLink proposed to use protocols that are not used in NG9-1-1 systems. Based upon my professional experience, it appears to me that Comtech offered a reasonable proposal, closely aligned to NG9-1-1 standard, while

---

1 Brian Rosen, Exh. BR-4C at 15 (WMD Response to Public Counsel Data Request No. 3, Attachment Washington State Military Department Contract E09-196 at 14).
2 See Rosen, Exh. BR-18C (Comtech Response to Public Counsel Data Request No. 4 with Confidential Attachment B.1(b)).
CenturyLink countered with an IP interconnect at odds with those standards.

CenturyLink also told Comtech that it could use SS7 to interconnect.

Faced with the available choices from CenturyLink, Comtech preferred the SS7 interconnect. CenturyLink and Comtech went ahead and implemented the SS7 interconnect.

Q. Refer to Exhibit SET-1TC at 8 and 58 and Exhibit CDK-1TC at 12–13.

CenturyLink’s witnesses insist SS7 was an appropriate technology choice for the interconnect. Why was SS7 inappropriate for this use case?

A. SS7 was inappropriate for this use case because it introduced unnecessary complexity and additional opportunity for failure into the state’s critical 9-1-1 system with less ability for the system to quickly recover from failures. At the time of this migration, the OSPs were still connected to the CenturyLink ESInet by the older Centralized Automatic Message Accounting (CAMA) technology, and the Public Safety Answering Points (PSAPs) were also connected using older CAMA technology. This meant that there was interwork between the SS7 or CAMA connections from the OSP to the CenturyLink ESInet, and another conversion between the ESInet and the CAMA connections to the PSAPs. The choice of using SS7 for the interconnect meant two additional conversions (IP to SS7 and SS7 to IP) were introduced into the system. This resulted in a total of four conversions for every call destined for a transitioned PSAP.

Every transition adds complexity and the opportunity to introduce failure into the system. Furthermore, SS7 has a known weakness, which is that designers have to
anticipate all possible failures and engineer backup paths into the system expressly. In contrast, IP networks have the very desirable characteristic that they automatically discover backup paths and use them, regardless of how circuitous or complex the path is, if that is the only way to get from point A to point B.

In extreme failure conditions, IP networks are more likely to work compared to SS7 networks. Indeed, there were IP connections between the contractors providing location information for calls (Automatic Location Identification query), and they worked throughout the incident. NG9-1-1 is being deployed across the country for this reason, among others, and to my knowledge, no new 9-1-1 systems use SS7 except for connections to originating service providers who have not converted to SIP.

Q. Was there anything else unusual about this SS7 interconnect?
A. Yes. In addition to lack of diversity, which I will discuss later in my testimony, CenturyLink instructed Comtech to use a third party, Transaction Network Services (TNS), to provide the actual SS7 interconnect between its contractor (Intrado) and Comtech. Both Intrado and Comtech had relationships with TNS prior to this interconnect. TNS is a commercial supplier of SS7 interconnect. It is not a carrier, and does not offer or claim to offer 9-1-1 capability. Its network is not subject to diversity requirements, and it does not claim to offer audited diverse paths within its

---

4 Rosen, Exh. BR-29C (Comtech Response to Public Counsel Data Request No. 9).
5 Rosen, Exh. BR-18C at 1.
network as 9-1-1 providers are required to do.

Q. Refer to Carl Klein’s Exhibit CDK-1TC at 12–13 and Exhibit SET-1TC at 44–45. CenturyLink witnesses Klein and Turner object to your characterization of SS7 as obsolete. Do you agree with these objections?

A. No. SS7 is being phased out all over the country in favor of SIP, the signaling protocol used in NG911, as well as wireless networks, Voice over Internet Protocol (VoIP) networks, and enterprise networks. SIP is replacing SS7, as well as the other signaling for telephone calls, as it was originally designed to do. I have been involved with the development of SIP since its inception, and I know well that SS7 is phasing out and SIP is becoming dominant.

Wireless networks have almost completely phased out SS7, the remaining SS7 are almost all confined to interfaces to non-wireless carriers. Larger telephone carriers are phasing out SS7 within their networks, especially at interconnects between service providers. Through discussions with other industry professionals, it is my understanding that carriers have asked the Federal Communications Commission (FCC) to allow them to only allow SIP interconnect and not support SS7 interconnect with other carriers, but the FCC has not issued an order addressing this issue.6

Moreover, many SS7 vendors have left the business, and usage has been declining for a long time. A significant problem in older SS7 networks is that the

---

vendor who supplied the equipment is no longer supporting it. While there is some
truth to the statement “it is used to support every 911 network”\textsuperscript{7} and “SS7 must be used to connect certain
carriers, such as CenturyLink and other wireline carriers, who have so far refused to
convert their 9-1-1 calls to SIP. Thus, the older, obsolete technology has to be used
until these carriers are forced to modernize their 9-1-1 support. However, SS7 is not
used in the middle of an NG9-1-1 network. It is only at the edge of the network facing
OSPs that have refused to deliver 9-1-1 calls via SIP. Turner’s testimony confirms
this.\textsuperscript{9}

In addition, SS7 does not support location in 9-1-1, even in older systems.
Location information in E9-1-1 is supplied over dedicated trunks using the Automatic
Location Identification (ALI) database. When OSPs connect via SS7 to NG9-1-1
systems, location comes from a simulated ALI over IP or directly over IP from a
database. SS7 has no facility to support location transmission.

Finally, this failure shows why SS7 is inherently less reliable than IP. There
were only four links, and they all had to be engineered point to point over dedicated
circuits. By contrast, IP networks have many more connections, direct and indirect.
When engineered in the way Comtech proposed, an IP network would have provided
much more tolerance for failures. Specifically, when connecting these two IP
networks via IP, there would not have been any dedicated long-distance links.

\textsuperscript{7} Response Testimony of Carl D. Klein, Exh. CDK-1TC at 12:15–16.
\textsuperscript{8} Response Testimony of Steven Turner, Exh. SET-1TC at 45:3.
\textsuperscript{9} \textit{Id.} at 45:12–20.
Instead, the system would likely have used a mix of Virtual Private Network
connections over public Internet, Multiprotocol Label Switching (or similar)
connections, and direct ties at common colocation facilities. Notably, the IP network
connections between Intrado and Comtech worked during this failure as did the IP-
based ALI connections between CenturyLink and Comtech.10

III. DIVERSITY

Q. Refer to Martin Valence’s Exhibit MDV-1TC at 5–10 and Exhibit SET-1TC at
57–58. CenturyLink’s witnesses cite lack of diversity on Comtech’s part as the
cause of the outage. Please explain diversity and how it applies to the incident.
A. The term “diversity” is used to describe how a network is designed to avoid common
faults. Circuits fail, for a variety of reasons. For example, cables get cut by
construction, weather events occur, electronics fail, or people make mistakes. In an
SS7 network, there are signaling paths and “trunks”. The signaling path is used to
provide instructions on how to set up connections. The trunks carry the actual call
(the “voice path”). The term SS7 generally refers to signaling. By contrast, IP
networks have only one mechanism, and the signaling and voice path run on the same
network.

SS7 networks are constructed of “links” that connect telephone switches and
special purpose Signaling Transfer Points (STPs) to each other. An origination
network switch will signal a request for a connection, which typically would go to its

10 Rosen, Exh. BR-29C.
local STP. The local STP would connect to other STPs, which relay the request to the
destination network STP. The destination network STP then instructs the termination
switch to set up the call.

These signaling requests transit the “links”. Each link is a circuit, ordered
from a service provider. To be reliable, there is more than one link between switches
and STPs and between the STPs. Most commonly, STPs are provisioned in pairs, and
each member of the pair has two links to each of its partner STP. If any link works
(one of the four in the example), then that part of the SS7 signaling network can do its
job. If all four links fail, the SS7 network will be unable to complete calls.

Recommended SS7 network design requires that the links be diverse.

The primary diversity criteria is “geographic” or “geospatial” diversity. This
means that the physical path the link takes does not have anything in common with
other paths. For example, separate fibers in separate conduits should be sufficiently
spaced so a single backhoe incident (e.g., severing a cable) does not disrupt more than
one link in the set. It also means separate switches are in the path of the link, so a
failure of a single switch does not take all four links down. Geographic diversity was
not a factor in this incident.

“Network diversity” is another form of diversity applicable to highly available
systems like 9-1-1. An entire network will sometimes encounter a problem that takes
the whole network down. For example, in this outage the entire optical network went
down, and since there was not network diversity, the interconnect failed.

“Software diversity” is a third form of diversity. By far, the most common
reason for an entire network to fail is a defect or bug in the software from which the network components are built. In most deployed networks today, all the switches or routers are from one company and have common code. This is a “single point of failure” that can affect the entire network.

Software is usually continuously maintained while being used in active networks: problems are found and fixed, new capabilities are added, and obsolete capabilities are removed. Software is released in “versions” and most commonly, one network has one software version running in all of its switches or routers. It is possible, as it was in this case, that a bug only affects some versions of software but not others. Experience shows that serious bugs can occur in one version or many versions, and it is not predictable what happens in any brand of switch or specific network.

Q. Refer to Exhibit MDV-1TC at 5–10 and Exhibit SET-1TC at 27–28, 46, 57–58. Turner and Valence discuss “supplier diversity”. What is supplier diversity?

A. Supplier diversity is having more than one supplier of a network component. To a customer like Comtech, supplier diversity means getting circuits from more than one carrier. Valence claims that because CenturyLink has more than one network, it can offer supplier diversity.¹¹ In my opinion, that is not supplier diversity. Rather, in this context, supplier diversity would be using multiple vendors for circuits. For example,

¹¹ Response Testimony of Martin Valence, Exh. MDV-1TC at 4:6–16.
Q. How is software diversity different from supplier diversity?

A. Software diversity is diversity of software within a network. Since the root of most modern total network failures is software failure, professionally, I recommend using components that do not all rely on the same software. CenturyLink does not appear to provide software diversity.

While the failure only occurred on one of its networks, another network using the same vendor, experienced a separate, but similar failure. CenturyLink claims the versions of the software were different, and the failures that occurred on one network could not have occurred on the other. I find that at least debatable, but without testing and the ability to reproduce the failure, we do not really know. Sometimes, a carrier like CenturyLink will use supplier diversity (meaning, it uses more than one vendor) as equivalent to software diversity, because usually vendors write their own software. I prefer expressing it as software diversity because it is the software that takes down networks.

Q. Several kinds of diversity have been mentioned in testimony. Will you more completely explain “Software Diversity” and how that affected this incident?

A. As I have explained in prior testimony, software underlies all modern telecommunications devices. Error (“bug”) free software, especially in large complex devices, does not exist. Errors are a fact of life. While software developers have many tools available to them to detect the presence of errors in their code, they are not

---

12 Rosen, Exh. BR-16C (Comtech Confidential Response to Public Counsel Data Request No. 3).
foolproof. Software failures are almost universally the underlying problem that causes
an entire 9-1-1 system to fail. The triggering event might be a human, hardware, or
environmental failure, but the underlying reason the entire system fails is software.

The fundamental reason this is true is that our most common defense against
total system failure is redundancy. A redundant system does not depend on a single
instance of anything: there are multiple instances, geographically dispersed, so that a
failure in one instance can be compensated for by another instance. We say that we
have no single point of failure in such a system because redundancy ensures a single
failure, or in many cases, multiple failures, will not bring the system down.

Unfortunately, the complex devices from which we build 9-1-1 systems, all run the
same software. The vendors of the systems select one vendor who writes the software
once, and all instances run the same software. This means the software is a single
point of failure and redundancy in such an example would not prevent total system
failure. A bug in the code is a bug in every instance of that device in a system.

The only defense against this problem is to use interoperable devices based on
standards. If devices conform to carefully constructed standards, devices from
multiple vendors can perform nearly identically to each other and interoperate with
each other. Not every function is likely to be standardized. For example, the
management and provisioning of the device may not conform to standards (indeed,
standard may not exist for those functions), but the function of the device can be
standardized in a way that multiple vendor’s devices can be fielded in a single
system.
Major telecom service providers used to qualify two or more vendors, insist the vendors conform to standards, and field more than one vendor’s devices in a network. If a software bug affected all of a vendor’s devices, it was highly unlikely to affect another vendor’s devices, and the entire network would not fail. However, cost considerations have led those service providers to abandon multiple vendor networks. Thus, it is now uncommon to see multiple vendors supplying the same function in one network. That makes all such networks subject to the single point of failure: the software. Customers do not have an option to choose a service provider who would not be subject to that problem because they all use single vendors.

The Green network failed because a software failure was a single point of failure in the network, and that caused the widespread outage to the 9-1-1 network.

Q. Could software diversity have prevented this incident?

A. Possibly. Despite CenturyLink’s claim that version differences between its networks offered some protection, a single vendor and a single version of that vendor’s software was installed on the network that failed. Moreover, the other network failed earlier in the year. So, deploying different versions of software from a single vendor did not prevent network failure.

In this specific case, if there were two vendors and the network were designed reasonably, it is likely that there would have been at least one link that worked at any time. CenturyLink had recent experience, the Red network failure, where a software fault in Infinera networks could take down the entire network. In this incident, there was a different fault than what caused the first incident, but it had the same result: the
entire network failed.

Indeed, CenturyLink’s expert witness Turner clearly states that software diversity is an essential safeguard:

Best network engineering practices require network redundancy for critical network infrastructure such as signaling. Network redundancy is implemented by means of ensuring route diversity. Route diversity does not simply mean geographic diversity of the transport facilities for the network. Its meaning is much broader. It requires that redundant network components must travel on different routes not only using diverse transport facilities, but also with no single points of failure either from a physical equipment or software standpoint.\(^\text{13}\)

Turner repeatedly cites the need for “no single points of failure”, but the software was a known single point of failure. CenturyLink had observed a software single point of failure in the Red network failure. Software as a single point of failure is a very well-known problem, and it has occurred several times, as I stated in the Response of Public Counsel to CenturyLink’s Data Request No. 17.\(^\text{14}\)

Q. **How did all types of diversity affect this incident?**

A. All four links in the part of the network from TNS to Comtech were provisioned on the same CenturyLink network. There was no network diversity. The incident caused failures on all the switches in the network used by the interconnect, and it failed.

There was also no software diversity, but it did not affect other networks that were running the same brand of switches in CenturyLink and there were version differences in the networks.

We do not know if there was geographic diversity, but we do know Comtech

\(^{13}\) Turner, Exh. SET-1TC at 25:5–11 (emphasis added).

\(^{14}\) Rosen, Exh. BR-31 (Public Counsel’s Response to CenturyLink’s Data Request No. 17).
Q. Refer to Exhibit MDV-1TC at 5–6. Valence claims you do not understand how supplier diversity affects CenturyLink networks. Please respond.

A. My statement was, “CenturyLink built its optical network using multiple optical network switches supplied by one vendor, Infinera Corporation. Had CenturyLink deployed two vendors, the nationwide failure that impacted Washington’s 9-1-1 system either would not have happened, or the scope and duration of the failure would have been reduced dramatically.”15 That is a completely accurate statement, as demonstrated by the discussion above regarding diversity. The failed “Green” network was constructed with switches supplied by a single vendor, Infinera. Had there been two vendors, the 9-1-1 failure would likely not have happened. While Valence explains that CenturyLink has more than one network and therefore, it could offer a form of supplier diversity, in my opinion that is not actual or functional supplier diversity. Importantly, at least one of the networks that CenturyLink offered as part of its definition of supplier diversity used the same manufacturer.

Q. Refer to MDV-1TC at 11-20. Valence describes the differences between the “Red” and “Green” network and states that these differences were significant enough that CenturyLink had no reason to believe the Green network could fail in the same way the Red network failed. What is your reaction to that?

A. The Red network failure showed that it was possible for the entire optical network to fail when the management channel, which was not being used, became clogged with

15 Direct Testimony of Brian Rosen, Exh. BR-1CTr at 20:5–9 (footnote omitted).
packets and exhausted resources in the switch to the point where revenue traffic was impeded. When doing root cause analysis on highly available systems, the root cause is not what failed. The root cause is why that failure caused the entire system to fail.

Highly available systems are supposed to be immune to failures that impact the entire system. The failure to focus on the second half of the analysis is a very common oversight in root cause analysis. The cause of the immediate failure is not the root cause (or at least, not the root cause we care the most about). The more relevant root cause is why the entire system failed even when the immediate failure occurred.

Consider an analogy of a bridge that collapsed. Suppose that salt corroded a strut, and the strut failed, triggering the collapse. The root cause is not that the strut collapsed. The root cause is that corrosion caused by salt on a single strut took the entire bridge down.

The root of the failure here was that the network management system could create a packet storm that shut down the network. Infinera only focused on what caused the packet storm. CenturyLink accepted this explanation and compounded it by not insisting Infinera disable the management channel on the Green network. Bad packets happen. Bugs in code handling packets happen. But, if the entire network can be disabled because it is possible for the management channel to create a packet storm, the management channel should be turned off until it is no longer possible for a packet storm on the management channel to take down the network. As an example, Infinera could have disabled the ability of the management channel to send any
packets. It could have also refused to process any received packets. That the cause of
the packet storm in the Red network was different from the cause of the packet storm
in the Green network is immaterial. The real problem was that the network could
generate a packet storm and be taken down by such a packet storm, regardless of
cause.

Further, packet storms may arise under various scenarios. CenturyLink’s
networks should have been resilient enough to withstand packet storms, regardless of
cause.

Q. Refer to Exhibit MDV-1TC at 10–11. Valence opines that the outage on the
green network was not foreseeable. Was it?

A. As I have explained, the evidence shows that CenturyLink knew that packet storms
on the management channel were possible, resulting in the network going down.

CenturyLink knew that any Infinera-based network would be vulnerable to packet
storms. In my professional opinion, CenturyLink should have insisted that Infinera
disable the management channel and fix the root cause so that it was not possible to
take down the network if a packet storm occurred on the management channel. The
management channel should have been disabled in such a way that it could not send
packets, and reception of packets could not tie up the switches’ resources.

Q. Refer to Exhibit MDV-1TC at 20–22. Valence insists that CenturyLink offers
diversity options that are available by essentially checking a box and paying a
small fee. He cites the following text:

You can order diverse routing for 911/E911 circuits if facilities are
available. These trunks must be provisioned to conform to the
standard CAMA signaling format. When CenturyLink facilities are available, CenturyLink will comply with diversity of facilities and systems as ordered by you. Where there is alternate routing of 911/E911 calls to a PSAP in the event of failures, CenturyLink shall make that alternate routing available to you.\footnote{Valence, Exh. MDV-1TC at 21:2–7 (citing webpage: https://www.centurylink.com/wholesale/pcat/911.html).}

What is your response?

A. Beyond the statement cited by Valence, I do not know what CenturyLink advises customers about diversity. Regardless, that specific statement by Valence is a red herring because it is not applicable to what Comtech ordered. It ordered facilities that used SS7 signaling, not CAMA, which is the only option the quoted statement describes.

Q. Refer to Exhibit MDV-1TC at 9–10; Exhibit SET-1TC at 9:26–29; and Exhibit CDK-1TC at 13:4–7. CenturyLink’s witnesses claim that the reason for the failure was that Comtech did not use supplier diversity in connections between TNS and its system. Is that true?

A. Yes. If Comtech had provisioned the SS7 signaling links with supplier diversity (in this context, network diversity), the failure would not have happened. But, if CenturyLink had agreed to the IP interconnect Comtech proposed, the failure would also not have happened. If CenturyLink had used software diversity in its Green network, the failure would not have happened. If CenturyLink/Infinera had disabled the management channel, the failure would not have happened. If CenturyLink had used its own STPs (especially in-state STPS) rather than using TNS, the failure would not have happened.
Many errors were made here, **any one of which**, if undone or corrected, would have avoided the failure.

**IV. TRANSITION RESPONSIBILITIES**

**Q.** Refer to Exhibit CDK-1TC at 6–9; Exhibit SET-1TC at 40:8–10; and Stacy Hartman’s Exhibit SJH-12C. CenturyLink’s witnesses claim the point of demarcation was in the middle of the TNS network. Please explain what a point of demarcation is.

**A.** When a service provider provides a telecom service to a customer, or where two service providers interconnect, it is routine to describe a “point of demarcation” that defines when responsibility shifts from the customer to the service provider (and vice versa) or where responsibility shifts from one service provider to another. In my experience, the point of demarcation is typically described in the contract between the parties, but may also be described in agreements between the parties beyond contracts. One party cannot unilaterally assert the point of demarcation: it is an agreement. The point of demarcation is important because if a failure occurs, the contract usually specifies **who** is liable for failure (and what penalties may be incurred) using the point of demarcation as the point at which liability shifts.

**Q.** Based on your review, where was the point of demarcation at the time of the outage?

**A.** In Exhibit SET-7C, Comtech supplied a drawing of an IP-based interconnect, which proposes a point of demarcation. Turner cites this as evidence of where the point of
demarcation should be.\textsuperscript{17} However, the interconnect shown in Exhibit SET-7C is not
the interconnect that was actually implemented because Comtech clarified that
CenturyLink rejected that proposal.\textsuperscript{18} As a result, the point of demarcation identified
by Turner was not the point of demarcation between CenturyLink and Comtech at the
time of the December 2018 outage.

Further, Turner places the point of demarcation in the middle of the TNS
network,\textsuperscript{19} on which neither Comtech nor CenturyLink had any control, visibility, or
influence. In my professional experience, that is not a tenable point of demarcation.
Comtech provided a drawing showing where it believed the point of demarcation was
at the time of the outage: at Comtech’s first piece of equipment.\textsuperscript{20} That point is at
least a reasonable and viable point of demarcation.

Even though Comtech identified a viable point of demarcation, there was no
agreement between CenturyLink and Comtech regarding where the point of
demarcation actually existed. As the underlying contracts and amendments make
clear, the point of demarcation was simply not specified between CenturyLink and
Comtech. This is highly unusual, as the point of demarcation is usually carefully
defined in contract. Without an agreed point of demarcation, it is nearly impossible to
assign responsibility at any specific point in the network. That there is no point of
demarcation means CenturyLink \textbf{cannot} establish that it was not responsible for a

\textsuperscript{17} Turner, Exh. SET-1TC at 43.
\textsuperscript{18} Rosen, Exh. BR-32C (Comtech’s Response to Public Counsel Data Request No. 31).
\textsuperscript{19} Rosen, Exh. BR-5 (CenturyLink Supplemental Response to Public Counsel Data Request No. 7, Attachment
PC-7a).
\textsuperscript{20} Rosen, Exh. BR-32C (Comtech’s Response to Public Counsel Data Request No. 31, Attachment).
failure in the middle of the 9-1-1 network, especially since the actual part that failed was a **CenturyLink optical network** that carried part of the 9-1-1 network.

**Q. Why is CenturyLink’s assertion that the point of demarcation was in the middle of TNS network untenable?**

**A.** Based upon my professional experience and review of the evidence, it appears to me that CenturyLink defined how the interconnect would work and instructed Comtech to use TNS as the SS7 signaling network. Comtech obliged. With TNS in the middle, there is no obvious point of demarcation between CenturyLink and Comtech. CenturyLink now claims the point of demarcation is literally in the middle of the TNS network. Yet, that point is beyond where Intrado connects to TNS and before CenturyLink connects to TNS. This is untenable, because TNS did not identify the location of the point of demarcation within its network. Furthermore, a point in the middle of TNS’s network would not have been observable or manageable by either CenturyLink or Comtech.

**Q. Do you believe Comtech’s asserted location for the point of demarcation is reasonable?**

**A.** Comtech claims the point of demarcation is in the handoff between TNS and Comtech. Further, it claims that the point of demarcation is on its side of the handoff. This is a reasonable point of demarcation because two of the links that failed were ordered by TNS; two were ordered by Comtech. That makes it harder to assert

---

21 Rosen, Exh. BR-32C (Comtech’s Response to Public Counsel Data Request No. 31, Attachment).

22 Rosen, Exh. BR-15C (Comtech Confidential Response to Public Counsel Data Request No. 1, with Confidential Attachment A).
that the TNS side of the handoff was the point of demarcation. Since CenturyLink
provided the links and it was a CenturyLink network that failed, it lends credence to
the argument that the point of demarcation was on the Comtech side of the TNS-to-
Comtech links.

I am not a lawyer, but I have extensive experience in this industry including
reviewing and advising relating to contracts denoting a point of demarcation. In my
opinion, the fact that there is not an agreed upon point of demarcation means that
CenturyLink cannot claim the outage is all Comtech’s responsibility.

Q. Refer to Exhibit SET-1TC at 40–43. Turner asserts that CenturyLink’s
responsibility for the network under the contract transitioned to Comtech when
Comtech became the Covered 9-1-1 Service Provider. Do you agree?

A. No. In the contract between Washington Military Department (WMD) and
CenturyLink, there is a list of services CenturyLink is required to provide. One of the
services listed is “network”. In this industry, “network” is generally understood to
be the signaling and voice path, plus the interconnects for auxiliary services such as
location. We distinguish the network from the services that ride on the network.

If the entire system had been provided by CenturyLink, the links that failed
would clearly be part of “network”. There was another service, “Covered 9-1-1
Service Provider,” which is a term used by the FCC to define the service provider

---

23 Rosen, Exh. BR-4C at 15 (WMD Response to Public Counsel Data Request No. 3, Attachment Washington State Military Department Contract E09-196 at 14).
who delivers calls to a PSAP. The term is defined by the FCC rules. The contract made CenturyLink responsible for, among other things “network” and “Covered 9-1-1 Service Provider”. Contract modifications were made to accommodate the transition from CenturyLink to Comtech. Amendment M specifically discussed the transition and clearly stated that when a PSAP transitioned from the CenturyLink ESInet to the Comtech ESInet, then Comtech became the Covered 9-1-1 Service Provider.

While the responsibilities of a Covered 9-1-1 Service Provider could have been expanded by contract, and some aspects of network are most often assumed by the Covered 9-1-1 Service Provider, the contract expressly mentions “network” (and “transport”) independently of “Covered 9-1-1 Service Provider”. Based upon the plain language of the contract, clearly, WMD believed it was important that CenturyLink be responsible for network and transport in addition to being the Covered 9-1-1 Service Provider. Amendment M did not relieve CenturyLink of the responsibility for “network” or “transport”. Nor did any other amendment.

That means that CenturyLink was still responsible for the network and transport at the time of the outage. Indeed, WMD has stated it “believes CenturyLink retained a role, and thus an obligation under the Washington Military (WMD) CenturyLink, Contract No. E09-106, until there were no parts of the originating

24 At the time Amendment M to the WMD and CenturyLink contract was executed, the FCC definition of “Covered 9-1-1 Service Provider” was found at 47 C.F.R. §12.4(a)(4). Today the definition is found at 47 C.F.R. §9.19(a)(4). The definitions are the same.

25 Rosen, Exh. BR-4C (WMD Response to Public Counsel Data Request No. 3, Attachment Washington State Military Department Contract E09-196).
network nor the terminating network connected to the CenturyLink/Intrado ESInet.”

If I were advising WMD, I would not relieve either CenturyLink or Comtech from responsibility for both the network and transport because of the complexity of having an SS7 network in the middle of two IP networks. Indeed, the lack of a clear point of demarcation is indicative of the issues that can arise in transitions. Both CenturyLink and Comtech should have been checking each other, verifying that the entire network was designed and built to meet both companies’ 99.999 percent availability requirement. Both should have been intimately involved in the design and provisioning of the entire interconnect. CenturyLink was responsible for “network” and “transport,” and they were responsible for the entire network, and all of the circuits, including the part that failed in December 2018.

Q. Refer to Valerie Lobdell’s Exhibit VL-1TC at 4:8–9. Lobdell describes the three phased transition approach required by WMD to be “unnecessarily complicated and introduced unknown risks.” Do you agree?

A. No. The phased transition approach was necessary. There are three parts in 9-1-1 networks: the ingress, the core, and the egress. The ingress is the connections from the Originating Service Providers (OSPs) to the 9-1-1 network. The egress is the connections from the 9-1-1 network to the PSAPs. It is not feasible to have a “flash” cutover from one network to the other due to the high risk involved with changing too many things at the same time. Instead, OSPs and PSAPs must be migrated one at a time. While that migration is in process, calls from any OSP to any PSAP must work.

---

26 Rosen, Exh. BR-27 at 3 (WMD Supplemental Response to Public Counsel Data Request No. 7).
Q. Please describe how such transitions ordinarily take place.

A. When performing a migration like this, both the existing and new vendors must have interconnections between their systems. For example, a call from an OSP that had transitioned to the new network must be able to be placed from an OSP that had not yet transitioned. It is very common that all the transitions on one side are completed before any on the other side are completed so that all PSAPs may be transitioned to the new vendor while all OSPs remain untransitioned, or vice versa. Further, it is essential that calls originally sent to a transitioned PSAP be able to be transferred to an untransitioned PSAP, regardless of whether the OSP was transitioned or untransitioned.

Even if OSP and PSAP transitions can be interleaved, because any OSP must be able to send a call to any PSAP, an interconnection between the two networks is required. Further, both networks must make routing decisions. Regardless of order, one network may start routing only to discover that the destination is on the other side of the interconnect, and when the other side gets the call, they must route it to the right PSAP. That is exactly how this migration was specified. Because a flash cutover is not feasible, both networks must be interconnected, and both must route.

In this case, the choice to use an SS7 interconnect between the two IP networks increased the complexity and risk, not the choice to use a phased transition. It would have been much simpler to connect the two IP networks and route calls from one to the other via the IP based signaling that both used. Furthermore, calls must be able to be transferred from one PSAP to another. When a call transfers from an
untransitioned PSAP to a transitioned PSAP, or a transitioned PSAP to an
untransitioned PSAP, it must occur on some interconnect between the systems.

I will note that interconnection of ESInets, rerouting of calls between them,
and transfer of calls between them were not standardized at the time of this event.
However, standards, developed by NENA now exist, and they describe a design
very similar to what Comtech originally proposed. This underscores the fact that
many experts agree with the basic approach Comtech proposed and CenturyLink
rejected.

Q. Refer to Exhibit CDK-1TC at 6:17–18. Klein states that CenturyLink’s
suggested way to accomplish the transition was a recommendation “that calls
destined for a Comtech PSAP be flash-cut to Comtech with CenturyLink out of
the call flow altogether.” What is your opinion of that proposal?

A. I am very surprised that such a suggestion was made. Unless one OSP only serves one
PSAP, then calls from one OSP must be able to go to both untransitioned
(CenturyLink PSAPs) and transitioned PSAPs (Comtech PSAPs). If the OSP is
untransitioned, then it would have to go through the CenturyLink network, some of
its calls would have to interconnect to the Comtech network and be routed to the
transitioned PSAP. Calls to the untransitioned PSAP from that OSP would remain on
the CenturyLink network. If the OSP transitioned, then some of its calls would have
to be sent to the CenturyLink network for delivery to the untransitioned PSAP. If all

27 Nat’l Emergency Number Ass’n (NENA), NENA i3 Standard for Next Generation 9-1-1 (2021),
OSPs were transitioned before any PSAP was transitioned, then when a PSAP transitioned, CenturyLink would not be in the path, but before then, unless they flash cut all the OSPs to Comtech at once, there would be exactly the arrangement that was used, but Comtech would have to route calls to CenturyLink and CenturyLink would route calls to untransitioned PSAPs.

WMD chose to transition PSAPs before OSPs, but transitioning OSPs before PSAPs still requires the kind of arrangements that were used. When all the PSAPs were transitioned, the final phase transitioned the OSPs, one at a time. That would effectively be “flash cut” of an OSP from CenturyLink to Comtech, but it is only possible because all the PSAPs were transitioned first. I am not aware of any compelling reason to transition OSPs before PSAPs, but I am certain that doing them one at a time is much preferred over doing them all at the same time. If the PSAPs are transitioned one at a time, then calls will transition both networks for some calls until all OSPs and all PSAPs are cut over.

Q. Refer to Exhibit CDK-1TC at 6 and 10. Klein provides diagrams more closely illustrating the call path at the time of transition. Do you have any comment on those diagrams?

A. Yes. Figure 2 “Non Simplified Phase 1 call flow” illustrates the clear danger of interconnecting two IP networks with an SS7 network. If the IP networks were interconnected in the simplest way, where CenturyLink and Comtech trusted each other (which, for this transition, I think they should have) then the diagram would look like this:
If they did not trust each other, then the diagram would look like this:

Instead what they implemented is this:

Q. Refer to Exhibit SET-1TC at 41–43. Turner claims that “Covered 9-1-1 Service Provider” is much broader than the definition used by the Code of Federal Regulations and uses another FCC document to attempt to show that it is more comprehensive. Turner then disputes that the lack of relief from the responsibility for “network” makes CenturyLink liable for the failure. Would you like to comment?

A. In this situation, the contract specifically called out “network” independently of “Covered 9-1-1 Service Provider”. In a fully transitioned network, we would expect
the Covered 9-1-1 Service Provider to “aggregate 911 traffic from an originating
service provider and deliver it to a 911 call center”, but that would not be the case
here. CenturyLink was aggregating 9-1-1 traffic from an originating service provider
and was part of the delivery path to the 9-1-1 call center. “Network” and “Transport”
means the underlying communications system rather than the services that rides on it,
so making CenturyLink (and, jointly Comtech) responsible for them does not
interfere with Comtech being the Covered 9-1-1 Service Provider.

Q. Refer to Exhibit SET-1TC at 44:6–13. Turner objects to your testimony that the
ALI connections between CenturyLink and Comtech were provisioned over IP
and did not fail. Turner claims they were provided by NoaNet. Is that true?
A. No. NoaNet was used by Comtech to get IP connections to PSAPs. I believe the IP
connections for ALI between Comtech and CenturyLink

V. FAILURES IN THE GREEN NETWORK

Q. Refer to UTC Staff witness James Webber’s Exhibit JDW-1CT at 24:6–16 and
Exhibit SET-1TC at 52–55. Webber suggested that the management channel

---

28 F.C.C., 911 Reliability (last updated Dec. 20, 2021), https://www.fcc.gov/911-reliability. At the time
Amendment M to the WMD and CenturyLink contract was executed, the FCC definition of “Covered 9-1-1
Service Provider” was found at 47 C.F.R. §12.4(a)(4). Today the definition is found at 47 C.F.R. §9.19(a)(4).
The definitions are the same.
29 Rosen, Exh. BR-29C (Comtech Response to Public Counsel Data Request No. 9).
30 Rosen, Exh. BR-4C at 31 (WMD Response to Public Counsel Data Request No. 3, Attachment Washington
State Military Department Contract E09-196 Amendment M Scope of Work).
should have been disabled. Turner provides several statements that claim

**CenturyLink did the right thing. Do you agree?**

A. No. First, Turner suggests that the management channel (Infinera General Communications Channel or IGCC) was disabled.\(^{31}\) It was not. It was indirectly prohibited from operating due to the software limiting packets to a certain size, which only filtered packets that were exactly the size expected to be found on the management channel, or smaller. That is not disabling the channel. If the channel were disabled, there should be no resources consumed by sending or receiving packets. CenturyLink claims the Red management channel was essentially “disabled” and yet a packet storm took it down. Clearly, this was not an effective disablement.

Specifically, this supposedly disabled management channel was capable of sending packets.

Then Turner deflects blame from CenturyLink and places it on Infinera. While customers like CenturyLink do follow the advice of the supplier, they do not do it blindly. Having been employed in my past by large provider of equipment carriers like CenturyLink, I know, as Turner surely knows, that large service providers do not take such advice at face value, but rather ask lots of questions, and very often instruct their vendor to be more conservative than the vendor suggests. This is the nature of large service providers: they are inherently risk averse. Having experienced the Red network failure, CenturyLink should have instructed Infinera to make sure that under no circumstances could a packet storm be created on the Green network. That would

---

\(^{31}\) Turner, Exh. SET-1TC at 55.
mean something more aggressive than just using a packet length filter.

VI. CONCLUSIONS

2 Q. Does this conclude your cross-answering testimony?

3 A. Yes.