

## Reason for Outage



**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. The outage was caused by a faulty Infinera network management card that caused invalid traffic replication which increased processing utilization on devices across the network. Where CenturyLink is an emergency 911 provider, 911 calls completed during the incident; however, ALI (Address Locator Information) did not accompany some of those calls. Affected services began to restore as of December 28, and the network traffic had normalized as of December 29. Steps have been taken to remove the circumstances that led to this issue. The technical details and corrective actions are provided below.

### **Cause**

A CenturyLink network management card in Denver, CO was propagating invalid frame packets that were encapsulated and then sent over the network via secondary communication channels. Once on the secondary communication channel, the invalid frame packets multiplied, forming loops and replicating high volumes of traffic across the network, which congested controller card CPUs network wide causing functionality issues and rendering many nodes unreachable. This was not caused by a source external to the CenturyLink network, such as a security incident. The source was an electronic network element within the transport layer of the CenturyLink network driven by a card supplied by Infinera.

Locating the management card in Denver, CO that was sending invalid frame packets across the network took significant analysis and packet captures to be identified as a source as it was not in an alarm status. The CenturyLink network continued to rebroadcast the invalid packets through the redundant (secondary) communication routes. CenturyLink will continue to review troubleshooting steps to ensure that any areas of opportunity regarding potential for restoral acceleration are addressed.

These invalid frame packets did not have a source, destination, or expiration and were cleared out of the network via the application of the polling filters and removal of the secondary communication paths between specific nodes. The management card has been sent to the equipment vendor, Infinera, where extensive forensic analysis is underway regarding the underlying cause, how the packets were introduced in this particular manner. The card has not been replaced and will not be until the vendor review is supplied. There is no increased network risk with leaving it removed. We have taken steps to prevent reoccurrence with the placement of the polling filters and the strategic removal of the secondary communication routes between all impacted nodes. There is no indication that this outage was triggered by any maintenance activity on the card, software, or any neighboring equipment. This was not caused by a source external to the CenturyLink network, such as a security incident.

### **Corrective Actions**

CenturyLink Network Operations Engineering and Executive Leadership met with Infinera to discuss corrective action plans, which are detailed below:

- Secondary communication channels (i.e. internal management channels) that caused invalid traffic replication have been disabled network wide. This is intended to prevent this type of outage from reoccurring.
- Infinera has advised that a network monitoring plan for key parameters that can cause this type of outage has been established.
- Improvements to the existing monitoring and audits of memory and CPU utilization for this type of issue have been put into place. Enhanced visibility processes will quickly identify and terminate invalid packets from propagating the network. This will be jointly and regularly evaluated by Infinera in conjunction with CenturyLink Network Engineering to ensure the health of the affected nodes.
- Infinera continues to analyze the network management card that has been removed from the device in Denver, CO to identify how the invalid packets were introduced and why the encapsulated trait was present. These results will be supplied to CenturyLink Operations Leadership, and any additional areas of opportunity will be appropriately addressed.

### **Resolution**

To restore services, the card in Denver was removed from the equipment, the secondary communication channel tunnels between specific devices were removed across the network, and a polling filter was applied to adjust the way the packets were received in the equipment. As repair actions were underway, it became apparent that additional restoration steps were required for certain nodes, which included either line card resets or Field Operations dispatches for local equipment login. Once completed, most services restored. Lingering outages for a small subset of clients were experienced following that time. The remaining impacts were investigated at the individual circuit level and resolved on a case by case basis to restore all services to a stable state.

### **Summary**

On December 27, 2018, CenturyLink identified an initial service impact in New Orleans, LA beginning at 08:40 GMT. The IP Network Operations Center (NOC) was engaged to investigate the reported trouble. Initial investigation suggested that an equipment fault was causing the trouble, and at 11:57 GMT, Field Operations were engaged to assist with onsite investigation. Additional research identified that the fault was causing service impact across multiple states and not a single site like initially suspected. At 12:49 GMT, the Tier IV Equipment Vendor Support Team (Infinera) was engaged to assist with troubleshooting.

During cooperative troubleshooting with the Tier IV Equipment Vendor Support Team and the CenturyLink IP NOC, a device in San Antonio, TX was suspected to be broadcasting traffic and consuming capacity. The device was isolated, which did alleviate some impact. When services did not restore, investigation remained ongoing and at 14:44 GMT, the trouble was escalated to CenturyLink Service Assurance Leadership. The IP NOC advised that focus shifted to the many additional sites where impact was identified, and remote troubleshooting was not possible. Field Operations personnel were dispatched to sites in Kansas City, MO, New Orleans, LA, Atlanta, GA and Chicago, IL to assist with onsite investigation. Simultaneously, additional NOC teams were engaged which include the National Transport NOC, Local Ethernet, and the Tier III Technical Support Team (Tier III).

Once personnel were on site and as visibility to some affected equipment was regained the Tier IV Equipment Vendor Support Team reviewed logs of the impacted devices. Additionally, a filter was applied to equipment in Kansas City, MO, as well as New Orleans, LA to prevent additional effects. As of 19:17 GMT, troubleshooting to restore visibility to Atlanta, GA and Chicago, IL was still in progress. At 21:35 GMT, visibility was successfully restored to both Chicago, IL and Atlanta, GA, allowing remote troubleshooting to resume. The case had the awareness of CenturyLink Executive Leadership.

At 22:57 GMT, A plan was formed to remove secondary communication channels between select network devices until visibility could be restored, which was undertaken by the Tier IV Equipment Vendor Technical Support team in conjunction with CenturyLink Field Operations and NOC engineers. While that effort continued, investigations into the logs, including packet captures, was occurring in tandem, which ultimately identified a suspected card issue in Denver, CO. Field Operations were dispatched to remove the card. Once removed, it did not appear there had been significant improvement;



however, the logs were further scrutinized by the Vendor's Advanced Support team and CenturyLink Network Operations to identify that the source packet did originate from this card.

CenturyLink Tier III Technical Support shifted focus to the application of strategic polling filters along with the continued efforts to remove the secondary communication channels between select nodes. Services began incrementally restoring. An estimated restoral time of December 28, 2018 at 09:00 GMT was provided; however, as repair efforts steadily progressed, additional steps were identified for certain nodes that impeded the restoration process. This included either line card resets or Field Operations dispatches for local equipment login. Various repair teams worked in tandem on these actions to ensure that services were restored in the most expeditious method available. By December 29, 2018 at 02:30 GMT, it was confirmed that the impacted IP, Voice, and Ethernet Access services were once again operational. Some Point-to-point Transport Waves as well as Ethernet Private Lines were still experiencing issues as multiple Optical Carrier Groups (OCG) were still out of service. The Transport NOC continued to work with the Tier IV Equipment Vendor Support Team and CenturyLink Field Operations to replace additional line cards to resolve the OCG issues. Several cards had to be ordered from the nearest sparing depot. Once the remaining cards were replaced it was confirmed that all services except a very small set of circuits had restored.

The remaining impacted circuits were investigated at the individual circuit level. Various fix actions were performed including additional higher-level card resets, individual span resets, and individual circuit restoration. All remaining affected circuits were successfully returned to a stable state.

*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.***