BEFORE THE WASHINGTON
UTILITIES AND TRANSPORTATION COMMISSION

Docket UT-181051

Washington Utilities & Transportation Commission v. CenturyLink Communications, LLC

RESPONSE OF PUBLIC COUNSEL TO CENTURYLINK DATA REQUEST NO. 38

Request No:	38
Directed to:	Public Counsel
Date Received:	September 23, 202
Date Produced:	October 7, 2022
Prepared by:	Brian Rosen
Witnesses:	Brian Rosen

DATA REQUEST NO. 38.
At page 16 (lines 17-18) of his Cross-Answering Testimony, Mr. Rosen asserts that "bad packets happen." Does Mr. Rosen contend that it was reasonably foreseeable that, in December 2018, four packets would malform into a single larger packet, while retaining header information allowing them to enter the IGCC? If your answer is other than no, fully explain your response and identify all other examples known to Mr. Rosen of any similar packet malformation occurring on a DTN, DTN-X or comparable Dense Wavelength Division Multiplex (DWDM) network.

RESPONSE:
In 50 years of working on packet networks, Mr. Rosen has observed malformed packets occur on virtually all such networks from time to time. Malformed packets are foreseeable. A specific malformation is usually not foreseeable, but there are a few common patterns. When designing packet networks, good practice is to assume malformed packets will occur, and accommodate them as best as possible. Since the header, by definition, is the beginning of a packet, and often malformations affect the beginning or end of packets, totally trusting the length field in the header is not advisable. Further, packet injection is a known attack surface, and by manipulating the length field, an attacker can often trigger a buffer overrun that can be exploited. Thus, good security practice is to be very conservative with length fields. While hardware in a packet receiver usually does assume the length field is correct, software should not, at least as much as feasible.