NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Lesson Learned

Telecom Provider Failure Induced Loss of ICCP from Regional Neighbors

Primary Interest Groups
Reliability Coordinators (RCs)
Balancing Authorities (BAs)
Transmission Operators (TOPs)
Transmission Owners (TOs)

Problem Statement
A registered RC experienced a temporary loss of inter-control center communications protocol (ICCP) data feeds from their regional neighbors. This loss of connectivity was due to third-party telecommunications vendor equipment that experienced a malfunction. For the next nine hours, these data links were intermittently unavailable. There was no adverse effect on the Bulk Electric System.

Details
Data communications services were provided by two major telecommunications service providers (referred to in this document as "Telco A and Telco B") at two disparate RC data center locations for the purpose of independent redundancy. With this incident, it was discovered that even though the two data centers the RC used for that purpose are geographically disparate, there was a point of convergence for the Telco A connections several hops into their respective networking infrastructure at a northeast regional hub. That common hub location had a hardware failure that affected the RC connections and many other Telco A customers. At both of the RC data centers, Telco A's connections were considered to be the primary pathway from a network routing perspective.

The RC attempted to site switch between its two RC data center locations, but the ICCP communications remained unstable due to the failure at this single point of convergence and because the data exchange was attempting to use Telco A's pathway at both RC data center locations.

The second problem that was encountered was that the Border Gateway Protocol (BGP) WAN configuration, that was resident at both of the RC data centers, favored using Telco A's connections, if the links were active at all. Because of the hardware failure, Telco A's connections were intermittently affected and therefore the traffic continued to attempt to use the damaged (Telco A) pathways even though Telco B's links were available and functioning properly at both RC data center locations. This had the effect of a "flapping" of the network traffic between the two telco-provided network pathways.

Once the network services provider was fully engaged and became aware of this situation, the BGP configuration was adjusted to ignore Telco A's communication pathways until the hardware problem was corrected. This restored stability for the ICCP connectivity to regional partners through Telco B's connections.

Corrective Actions

There are two corrections that are being put into place as a result of this incident.

- The BGP configuration at both RC data center locations was adjusted to not "fail back" to Telco A's pathways in the event Telco A's pathways become inoperable. This will allow for corrections to be made and the reliance on Telco A's pathways would only become the favored path once whatever problem causing the failure was completely addressed.
- The second corrective action taken was for Telco A to rebuild one of the RC's data center location's pathways to take away that regional point of convergence. This would effectively safeguard against a future failure affecting that regional hub.

Lesson Learned

The RC understood that they had contracted for vendor diversity at both of their geographically disparate locations. There had been testing performed to assure themselves that the connections would restart using the redundant links that were provided if there was a router or circuit failure locally to the RC's data center. What wasn't tested was if there was a more pervasive problem within one of the telco providers' networks that didn't directly affect the circuits that were installed locally within the RC locations; nor whether the Telcos utilized each other's facilities at any point in the system they were providing ICCP data.

Recommendations to avoid similar issues:

- When contracting with multiple vendors for data communications services for the purpose of redundancy, one should never assume that geographic diversity alone provides that redundancy. Ensure redundant circuit physical separation and independence of supporting equipment and power for the duration of the service is specified in the contract along with means for verification. Include language to maintain that separation will be preserved if the provider merges with or is sold to another telco.
- Validate the independence by testing with the vendor to attempt to simulate this type of failure to assure that the redundancy in place covers this type of failure scenario.
- Ensure that the data center does not continually automatically "fail back" to a preferred provider under intermittent conditions. Using a sustained signal timer or requiring manual intervention to switch back could suffice.

NERC's goal with publishing lessons learned is to provide industry with technical and understandable information that assists them with maintaining the reliability of the bulk power system. NERC requests that you provide input on this lesson learned by taking the short survey provided in the link below.

Click here for: Lesson Learned Comment Form

For more Information please contact:

NERC – Lessons Learned (via email) NPCC – Event Analysis

Source of Lesson Learned:	Northeast Power Coordinating Council
Lesson Learned #:	20190503
Date Published:	May 15, 2019
Category:	Communication

This document is designed to convey lessons learned from NERC's various activities. It is not intended to establish new requirements under NERC's Reliability Standards or to modify the requirements in any existing Reliability Standards. Compliance will continue to be determined based on language in the NERC Reliability Standards as they may be amended from time to time. Implementation of this lesson learned is not a substitute for compliance with requirements in NERC's Reliability Standards.