NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Lesson Learned

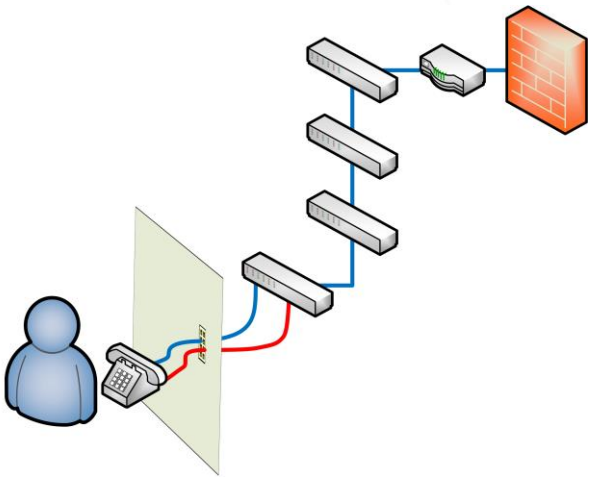
Networking Packet Broadcast Storms

Primary Interest Groups
Balancing Authorities (BAs)
Generator Operators (GOPs)
Reliability Coordinators (RCs)
Transmission Operators (TOPs)
Transmission Owners (TOs) that own and operate an Energy Management System (EMS)

Problem Statement
When a second network cable was connected from a voice over internet protocol (VOIP) phone to a network switch lacking proper settings, a packet broadcast storm prevented network communications from functioning, and supervisory control and data acquisition (SCADA) was lost for several hours. Broadcast storm events have also arisen from substation local area network (LAN) issues.

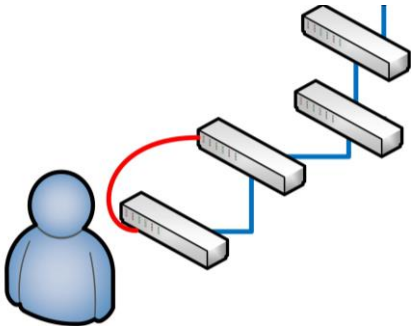
Details
A conference room was set up for a training class that needed to accommodate multiple PCs. The bridge protocol data unit (BPDU) packet propagation prevention setting was disabled on a port in the conference room in order to place a network switch off of that port. Upon completion of the training, the network switch was removed; however, the BPDU packet propagation setting was inadvertently not restored. As part of a telephone upgrade project, the traditional phone in this conference room was recently replaced by a VOIP phone. Later, an additional network cable was connected to the output port of this VOIP phone into a secondary network jack within the conference room.

When the second network cable was connected from a VOIP phone to a network switch lacking proper settings, a switching loop resulted. Spanning tree protocol is normally used to prevent switching loops from propagating broadcast packets continuously until the network capacity is overwhelmed. A broadcast packet storm from the switching loop prevented network communications from functioning and SCADA was lost for several hours. The effects of this condition are like a self-inflicted denial of service (DoS) attack.

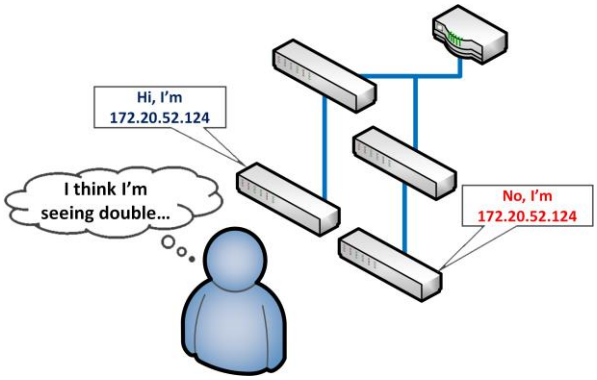


Similar broadcast storm events have occurred

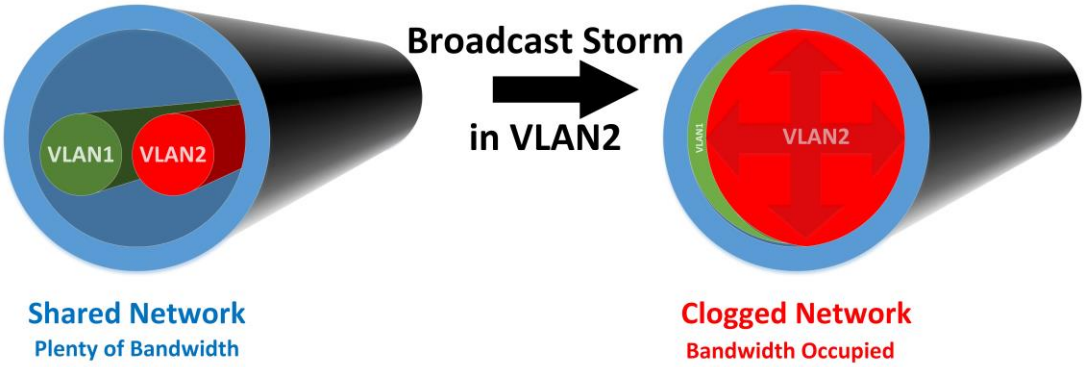
In one case, a substation technician performing routine system maintenance at a substation inadvertently connected an unused ethernet cable between two ethernet switches where an ethernet connection was already established. This created a communications loop with multiple ports seeing a duplicate MAC address. This loop created a broadcast storm that ultimately caused a loss of SCADA capability from the remote terminal units (RTUs) to the utility's EMS. Eventually, the cable was identified as the problem and removed, and EMS capability was fully restored.



At another location, a technician copied the configuration from another switch while preparing a new network switch to ensure their configuration was similar. However, the technician neglected to change the IP address of the new switch, so the new switch duplicated the IP address of the existing network switch. The duplicate IP address caused a packet storm that blocked network traffic and the entity's primary control center experienced a complete loss of SCADA data.



Another case involved substation data and commercial data on separate virtual local area networks (VLANs) passing through the same physical network switches. When station data was defeated by a broadcast storm due to an issue at a station under construction, the switches became overwhelmed, and the separate business traffic ceased as well.



Corrective Actions

In the IP phone case, the entity worked to narrow down the switching loop network location by isolating network segments, pinpointing the trouble spot, and finally shutting down the device and the port it was utilizing. They worked with the network hardware vendor to help review hardware global settings and receive remediation recommendations based on this specific incident.

The vendor recommended that network port settings be set to block BPDU packet propagation from non-spanning tree protocol enabled devices unless purposely allowed.[1]

In the station cases, locating and eliminating the unintended loop was the corrective action. In some cases, incompatibilities between network device manufacturers complicates use of spanning tree protocol.

In the cloned IP case, the solution was removing one of the two switches and assigning it a different IP address.

Lessons Learned

- Entities should use BPDU packet propagation prevention where a non-spanning tree protocol enabled device could be connected. These devices are usually end-user devices. Spanning tree protocol is normally used to prevent switching loops from propagating broadcast packets continuously until the network capacity is overwhelmed.
- Complete physical separation between SCADA Operations networks and business networks, VoIP, and external facing networks is preferred over VLAN for avoiding network traffic congestion and security issues. Where a vendor provides network services, a contract specifying maintenance of physical separation is necessary to enforce it.
- Where physical separation is not feasible, and Layer 2 Quality of Service (QoS) settings are supported, Layer 2 QoS can be used to avoid issues of heavy network traffic cutting off vital traffic. With proper QoS enabled for Layer 2 control packets, control packet rates exceeding a certain level to a switch will be dropped and not forwarded.[2]

- In addition to physical separation of networks and Layer 2 Quality of Service settings, there are additional, proprietary settings provided for additional control of central processing unit (CPU) loading and broadcast storm control. Entities should investigate these proprietary settings as appropriate with their networking vendor(s).
- Use a checklist and peer reviews when configuring and installing new equipment to avoid unintended loops or duplicate IP addresses.
- Establish standardized settings for network devices that include settings necessary to avoid packet storms.

[1] See https://learningnetwork.cisco.com/blogs/vip-perspectives/2016/03/10/advanced-stp-features-portfast-bpdu-guard-and-bpdu-filter and https://www.juniper.net/documentation/en_US/junos/topics/example/rate-limiting-storm-control-configuring.html for more technical discussions.

[2] A technical QoS setting discussion may be found here: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/44sg/configuration/guide/Wrapper-44SG/qos.pdf

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)	MRO – Event Analysis
Source of Lesson Learned:	Midwest Reliability Organization
Lesson Learned #:	20181001
Date Published:	October 2, 2018
Category:	Communications

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.