SEL Application Guide Volume II AG2019-15

Maintaining Switched-Mode Relay Responsiveness in an RSTP Network

Tyler Songstad, Jason Dearien, Amandeep Kalra

Introduction

The switched mode or pass-through mode in SEL relays provides a way for users to connect many relays to a network without connecting each relay directly to a managed switch. One popular use of this feature is to connect several relays to each other, creating a network of relays, then connecting at least two relays to a managed switch for redundancy. This effectively increases the port density of the devices on the managed switches. This configuration is popular because it reduces cost and the number of devices in a network without sacrificing redundancy—each relay has a redundant path to the network.

This configuration is not without tradeoffs, however. Under certain failure conditions, a subset of the relays connected in this manner can seem unresponsive for extended periods of time, sometimes as long as five minutes.

In this application guide, you will learn the underlying mechanisms that cause this behavior, the effect on various applications, and how to maximize the responsiveness of relays in this configuration.

NOTE: Rapid Spanning Tree Protocol (RSTP) was added to the SEL-700 series as an option (firmware version R302 and later) when using switched mode. Having RSTP enabled mitigates the issues mentioned because the RSTP feature properly reconfigures the network in case of a network event. This application guide is still applicable to older SEL-700 series devices or other SEL relays that use switched mode without RSTP.

Background

To understand the root cause of the observed behavior, you must understand Ethernet switching, media access control (MAC) address tables, managed and unmanaged Ethernet switches, RSTP, TCP/UDP, and switched mode in SEL relays.

Ethernet Switching

Ethernet switching is described in the IEEE 802.1D bridging standard. Traffic forwarding is based on MAC addresses and MAC address learning. In address learning, a switch listens on ports for all traffic (called promiscuous mode). The switch looks at the source address for each packet received on each port and learns the MAC address for that source on this port. In this way, a switch knows where to send traffic without sending data out a port on which the destination device does not reside. In a standard network, there should only be one active path by which a device can be reached.

If a switch must forward a packet with a destination for which the switch does not have an associated port, the switch will flood the packet. Flooding involves sending data out all ports except the port on which the information was received.

MAC Address Tables

The association in a switch between a MAC address and a port is stored in a MAC address table. If a switch has an entry for a MAC address in its table, it will send packets that have that destination MAC address only out the associated port.

If a MAC address table entry is not refreshed, it expires. A MAC address table entry is refreshed when the switch receives a packet with a source address that matches the entry. The time-out for an entry in a MAC address table varies, but it is commonly five minutes by default. If an entry in the MAC address table expires, packets destined for that address will be flooded until a response from the device is received and the MAC address is learned again.

If a switch receives a packet from a device on a port other than the port associated with that MAC address in the MAC tables, the MAC table entry for that device will be updated to the new port.

Managed and Unmanaged Ethernet Switches

Managed Ethernet switches have configurable features such as VLAN filtering and RSTP (described in the next section). Unmanaged Ethernet switches have no configuration options. Both managed and unmanaged Ethernet switches dynamically learn MAC addresses as described previously.

RSTP

RSTP is a method by which Ethernet switches can communicate and logically open connections to prevent physical loops in a network.

RSTP information is communicated with packets known as Bridge Protocol Data Units (BPDUs). Switches that do not implement RSTP (such as unmanaged switches) will not consume BPDUs and will instead treat them as regular broadcast traffic.

It is important to note that RSTP can affect the logical layout of a network. Therefore, after an RSTP event, a device that was reachable by one port may now be reachable only through another port on the switch/device. An unmanaged switch, therefore, could send data to the wrong port after an RSTP network event.

During an RSTP event, managed switches (those participating in RSTP) flush their MAC tables, so switches must relearn where devices are logically located within the network.

Managed switches continually send BPDUs to other managed switches. The rate at which a managed switch sends these BPDUs is determined by a setting called the “Hello Time”. After a managed switch does not receive any BPDUs on a port for three times the Hello Time, the switch will reenable the port, because doing so should no longer cause a loop in the network. This allows RSTP switches to heal networks (restore communications after a network event) even when the network contains unmanaged switches.

For more information on RSTP, see the SEL application guide on the subject [1].

TCP and UDP Protocols

TCP guarantees the recipient will receive the packets in order by numbering them. The recipient sends packets back to the sender saying it received the packets. If the sender does not receive verification, it will resend the packets to ensure the recipient received them.

In UDP, packets are only sent to the recipient once. The sender does not ensure the recipient received the data. It will continue sending the next packets. If the recipient does not receive the UDP packets, there is no way for the sender or the recipient to know that an error has occurred. There is no guarantee of receipt and there is no standard mechanism for retransmitting missed data, but UDP can be used in certain applications that require low overhead and are resistant to missing packets.

Switched Mode in SEL Relays

SEL relays have a switched mode of operation. This feature enables ports on the relay to become unmanaged switches. On a two-port relay, the relay is logically connected to a three-port unmanaged switch.

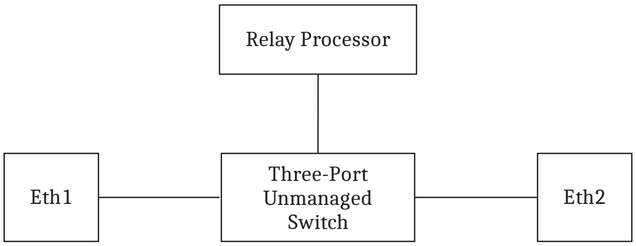

Figure 1 Logical Diagram of Relay in Switched Mode

Logically, the relay is connected to one port of a three-port switch, and the two physical ports of the relay are the two other ports on the switch.

FAILURE SCENARIO

Consider the following scenario.

Physical Configuration

To maximize value in a customer’s network, a network engineer configures a network such that individual relays are not directly connected to a port on a managed switch. Instead, the switched mode setting is used on the relays, and relays are chained together. Because of the behavior of the switched mode setting, the logical state of the network is as follows:

- Each relay is connected to an unmanaged switch.
- These unmanaged switches are connected in a chain, and the two end switches are connected to two managed switches.

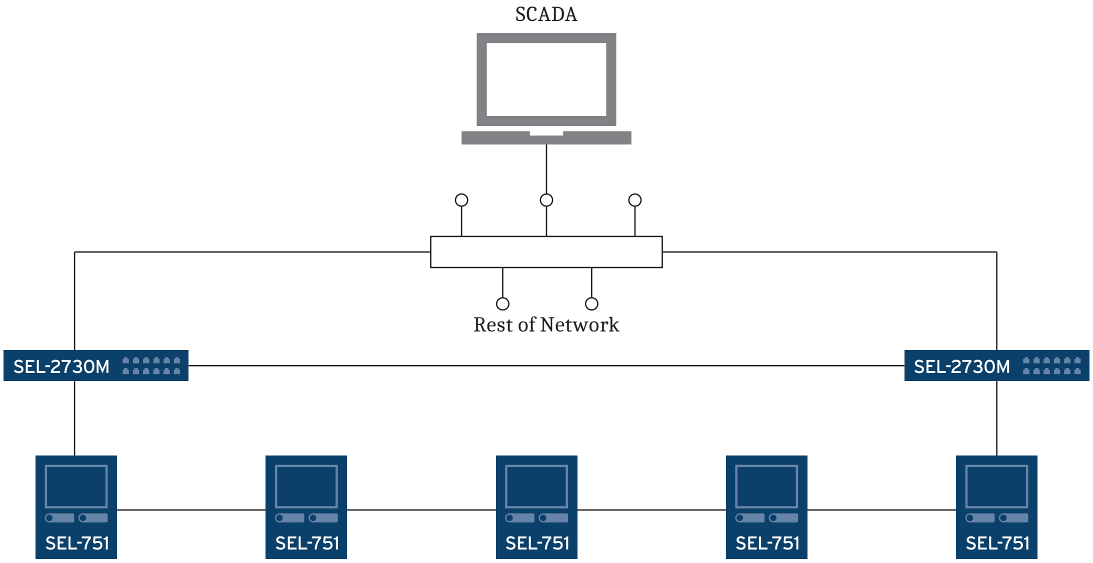

Figure 2 Example Physical Configuration

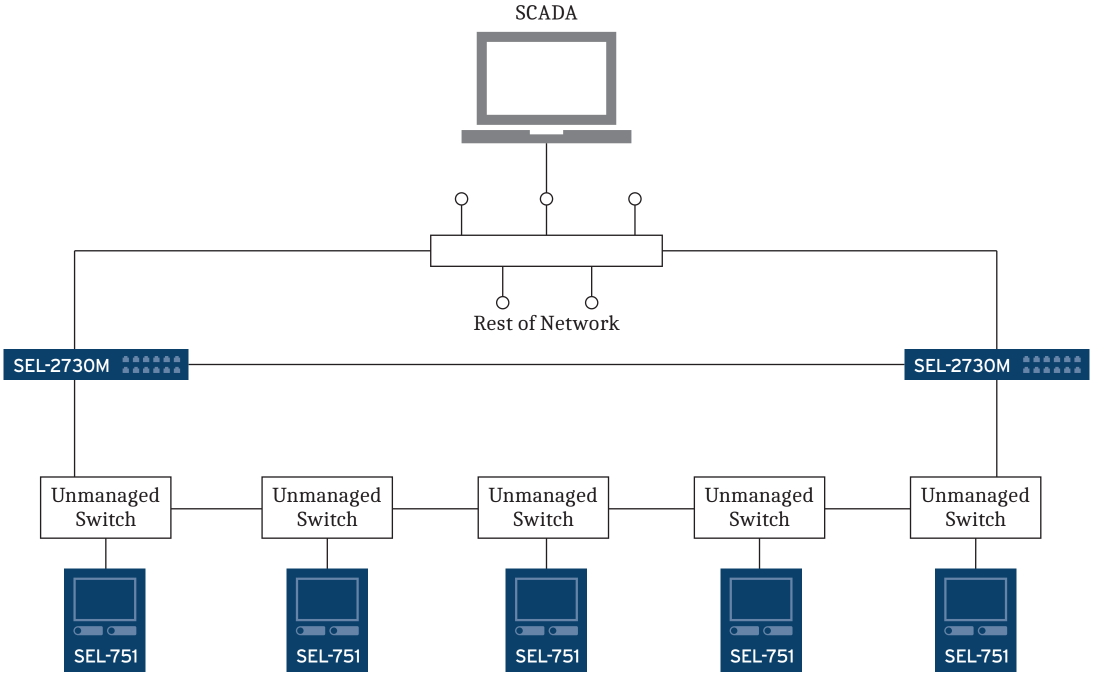

Figure 3 Logically Equivalent Configuration

DNP Configuration

To minimize unwanted DNP traffic on the network, the network engineer configures all relays to send unsolicited DNP data to SCADA. In this case, the network engineer has not configured SCADA to poll any of the relays, and instead configures SCADA to allow unsolicited DNP packets from the relays.

In another attempt to reduce traffic on the network, the network engineer also configures all relays to send DNP data via UDP rather than TCP.

Observed Behavior

After a network event (known or unknown to the SCADA operator), SCADA receives no data from one or more relays in the chain of switched-mode relays for five minutes or longer. SCADA reports that the relays are offline. After the relays have been unresponsive for five or more minutes, they come back online and are reachable by SCADA. Relay logs show no unusual activity or events.

Root Cause of Observed Behavior

For this example, consider the following network:

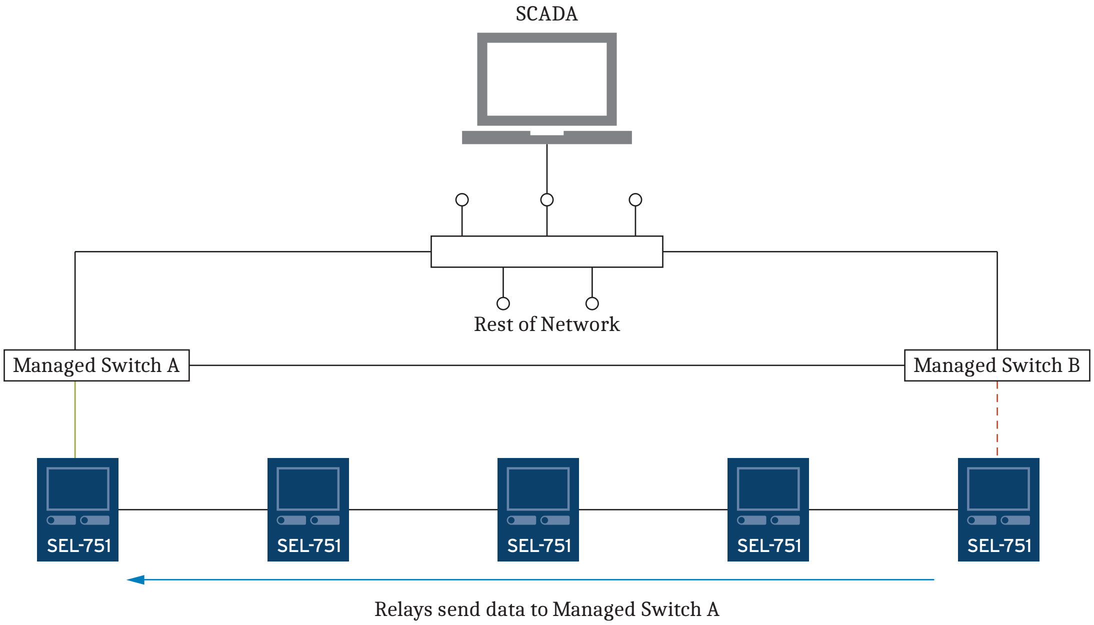

Figure 4 Network Steady State

In this example, RSTP disables the link between Managed Switch B and the SEL-751 directly connected to it. Because of this, the relays must communicate with SCADA by sending all traffic through Managed Switch A. After a network event, however, the logical configuration of the switches may change. Because of RSTP, switches open and close various ports to prevent loops, and SCADA may become reachable only through Switch B. Consider the following example of a link failure in the string of switched-mode relays:

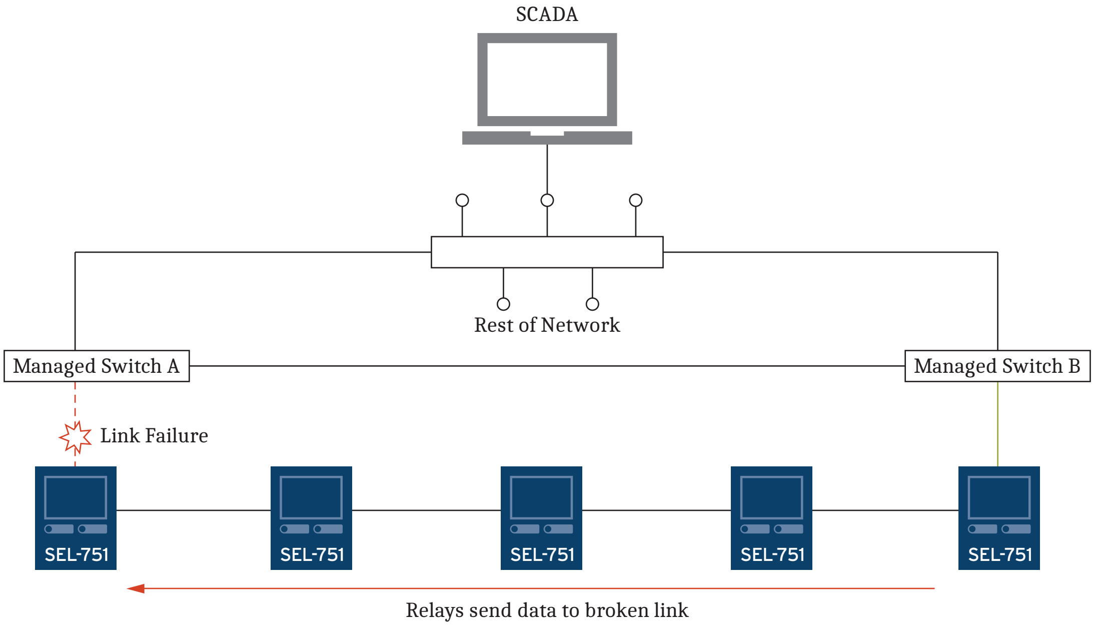

Figure 5 Network After Link Failure

The unmanaged switches in the relays do not participate in RSTP. When a network event occurs, the unmanaged switches inside the relays have no mechanism to determine that a network change has occurred. The switches, therefore, do not flush MAC tables, and instead use outdated information.

Because there is no mechanism for reporting link failures to other switches in the network, relays upstream of the link send their traffic to the broken link. This also means that the managed switches have no visibility of the fault in the network.

After 6–8 seconds, the managed switches will restore the link to the relays. However, because the relays have not updated the MAC tables (there is no mechanism for flushing MAC tables on link failure in unmanaged switches), all upstream relays continue to send their SCADA data to the broken link. The switches in the relays will flush their MAC address tables after five minutes. After the tables are flushed, the relays relearn the port to send SCADA data to and can successfully communicate with SCADA because traffic will be flooded on the network and the switches will learn the new topology.

It is important to note that you can observe this behavior in scenarios other than a broken link in the chain of relays. A change anywhere in the network that causes the port/SCADA MAC address information in the relays to become outdated can result in a similar failure scenario.

Effect on Applications

IEC 61850 GOOSE

Because GOOSE is multicast, the packets are sent out both ports of the relay. This was verified by observing Wireshark captures of an example network in steady state. All relays sent GOOSE packets out both ports. Because of this, the relays will not send GOOSE traffic out the wrong port after a broken link/network reconfiguration. The relays do not need to wait for MAC tables to be flushed to send GOOSE packets successfully.

However, the managed switches still do not recognize the broken link until managed switches heal the network. In the worst-case scenario (*Figure 5*), the relays do not have a connection to the managed switches until the managed switch opens the discarding port.

In testing, we observed an outage of GOOSE traffic for approximately 7 to 8 seconds.

Broadcast/Multicast

All Layer 2 broadcast/multicast traffic should be sent out both ports of a relay just as GOOSE is. We expect that all L2 broadcast and multicast traffic will have a maximum outage time of approximately 7 to 8 seconds. This outage will be longer in networks where the Hello Time is longer. A longer Hello Time will cause the managed switches to wait longer before healing the network.

Protection

Because some relays are unable to communicate with the rest of the network for six or more seconds, communications-assisted protection will be unavailable until the relays can communicate. However, this behavior does not affect local protection.

If the messaging requirements for a given network can tolerate a six-second or longer communications outage from the relays, this configuration can work well.

Maximizing Relay Responsiveness

DNP Via TCP: No Polling

Because TCP requires multiple back and forth packets between the client and the server, any interruption of packets will cause TCP keep-alive packets to be sent.

If a network event occurs, the relays will still send all traffic toward the broken link. Once SCADA sends TCP keep-alive packets, the relays relearn the position of SCADA and communications are restored. During testing, communication with the relays was interrupted for approximately one minute.

DNP Via UDP: Polling

As with TCP keep-alive packets, DNP polling creates a scenario where SCADA attempts to communicate with the affected relays after the network event occurs. Once SCADA sends some traffic to the relays, the unmanaged switches in the relays relearn the position of SCADA and communication is restored. During testing, communication with the relays was restored after approximately one minute. However, this number was unpredictable and varied widely depending on DNP polling interval times. In general, the fastest communication restoration happened in about 10 seconds with polling set to the minimum configurable time of 100 ms. SEL does not recommend configuring a DNP polling time of 100 ms, but this shows how more frequent polling can reduce communication outage times. In our testing, the default polling time (integrity poll every 60 seconds, Class 1, 2, and 3 polling every 5 seconds with a poll time-out of seven seconds) resulted in communications outages of less than one minute. It is important to note that various network factors can affect these times.

Other Protocols

The failover characteristics of other Ethernet protocols were not directly tested. However, the behavior can be extrapolated from the data gathered and details of a given protocol. In general, multicast and broadcast traffic from the relay will be interrupted until the managed switches heal the network (at least six seconds). For any TCP protocol, an interruption should last approximately one minute as observed with DNP over TCP. For UDP protocols, an interruption should last no longer than five minutes. In any case, communication with the relays can be restored faster by sending traffic addressed to affected relays, forcing them to relearn the position of devices in the network.

Conclusion

This application guide discussed the behavior of the switched mode of SEL relays and how to optimize performance when using this mode and RSTP is not an available option. Switched mode in SEL relays is an appropriate solution when the discussed network performance meets all application requirements. If using SEL-700 series devices, SEL recommends using R302 or later and enable the RSTP option to increase performance.

Reference

[1] J. Dearien, “Understanding RSTP and Choosing the Best Network Topology,” SEL Application Guide (AG2017-21), 2017. Available: selinc.com.

Technical Support

We appreciate your interest in SEL products and services. If you have questions or comments, please contact us at:

Schweitzer Engineering Laboratories, Inc.
2350 NE Hopkins Court
Pullman, WA 99163-5603 U.S.A.
Tel: +1.509.338.3838
Fax: +1.509.332.7990
Internet: selinc.com/support
Email: info@selinc.com

SCHWEITZER ENGINEERING LABORATORIES, INC.
2350 NE Hopkins Court • Pullman, WA 99163-5603 U.S.A.
Tel: +1.509.332.1890 • Fax: +1.509.332.7990
selinc.com • info@selinc.com