Ethernet Comparison Reference Guide

Use this guide to help identify the Ethernet technologies that are the best fit for your application.

Network Control Plane Options

These Ethernet technologies control how a network forwards data reliably to the proper destination.

RSTP

Rapid Spanning Tree Protocol

RSTP is designed for ease of use in multivendor environments. It is the most widely used and supported implementation of the spanning tree algorithm (STA) and is used in SEL network switches.

- Better performance and simpler configuration than MSTP (another STA implementation).
- Fixed forwarding behavior on Layer 1 and 2 attributes.
- Allows all traffic by default. Additional cybersecurity measures required.
- 10—20 ms failover times in most scenarios.

Network switches decide how to forward communications based on an algorithm that converges to a physical tree topology by designating or blocking links, favoring the high-speed links. Switches must continually communicate with each other or risk creating loops.

While the plain-text STA control plane is easy to use, it is not cybersecurity-protected in RSTP implementations. Orchestrating change management across the network is difficult, as topology changes can cause network disruptions and all traffic is forced on the same physical links.

Performance is topology-dependent. Network restoration calculations don't start until a failure happens, and failover times depend on the topology and switch count.

OT SDN

Software-Defined Networking

OT SDN is purpose-engineered for OT environments. SDN uses a secure control plane in which all primary and backup network paths are configured by a software flow controller. SEL devices support OT SDN.

- Interoperable open standards-based technology—a popular choice for virtual network and data center applications.
- Fully programmable forwarding behavior on Layer 1–4 attributes.
- Deny-by-default architecture and cryptographically secured control plane improve cybersecurity.
- 100× faster failover time than RSTP.

SDN replaces RSTP with proactive traffic-engineered circuit provisioning, in which switches are instructed how to forward data and how to react to any link failure, eliminating the need for the switches to communicate with each other.

The flow controller programs the switches using secure, authenticated, and encrypted communications using the OpenFlow protocol. Elimination of STA blocked ports allows 100 percent of system bandwidth to be used.

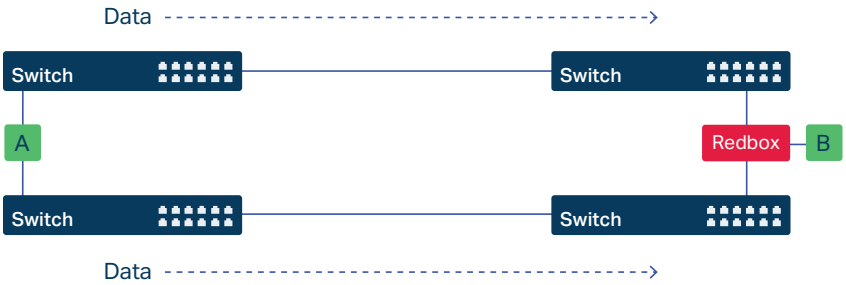
Networks are orchestrated through software applications that automatically configure the network from engineering designs. Topology changes don't cause network disruptions; all SDN switches in a network can be programmed in a single transaction, simplifying network change management.

Traffic Duplication Methods

Traffic duplication ensures reliable data delivery by using specific protocols and network architectures to add communications redundancy. This provides recoverability for single-point-of-failure (N-1) conditions, so that there is no "dark" period for failovers.

PRP

Parallel Redundancy Protocol



PRP provides redundancy via a duplicate network. PRP sends identical communications across two completely separate redundant networks to prevent packet loss. SEL devices support PRP.

- Most commonly used traffic duplication protocol.
- Topology-independent—can be used with any network topology.
- Can be implemented in whichever control plane technology you choose (RSTP or SDN).
- Interoperable with Ethernet devices.

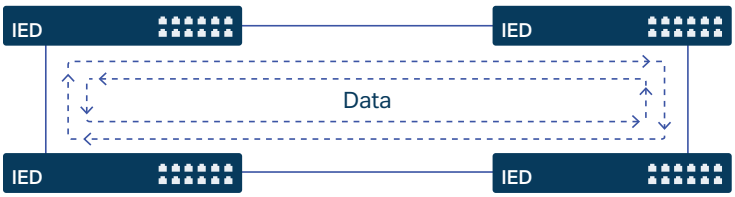
Hosts are dual-network-interfaced, publishing and receiving the same traffic on both interfaces and adding a redundancy control trailer (RCT) to the data payload for PRP management. Hosts expect each network interface to be islanded from each other, which means each host sends and receives traffic from each of the two parallel networks.

PRP hosts produce double the traffic and consume double the traffic. A redbox is required for a non-PRP host to talk with a PRP host.

SDN improves PRP by ensuring only the expected data is delivered to each host and interface and by blocking any unexpected traffic.

HSR

High-Availability Seamless Redundancy



HSR provides redundancy via a switchless ring network topology. It uses a ring topology and specialized hardware to create a fully redundant data delivery architecture.

- Designed to send all traffic through every host on the network twice, which significantly increases the traffic burden on the IED.
- Network topology must be a ring.
- Does not use RSTP or SDN switches.
- Not interoperable with traditional Ethernet devices. (Like EtherCAT, it requires specialized hardware.)

HSR does not require network switches. It is designed to remove switches from the network by connecting all the hosts together in a ring and sending the same communications in both directions around its topology.

To accomplish this, HSR adds a redundancy control field in the packet's Ethernet header, which means that standard Ethernet devices are unable to read HSR packets.

SEL network switches do not support HSR.

Things You Should Know

SDN Proactive Vs. Reactive

- The SEL implementation of OT SDN supports proactive flows.
- Reactive flows require continual controller connectivity, while proactive flows are preconfigured and do not require continual connectivity.
- Proactive flow is preferred for critical networks because the flow controller is not required for reliable network operations.

IPv4 Vs. IPv6

- IPv4 supports 4.2 billion unique addresses; IPv6 supports trillions.
- The industry will eventually migrate to IPv6, but at this point in time, it requires DNS and other name/address services that aren't appropriate for OT applications.
- SEL is actively researching the value IPv6 could bring to OT.

Unicast Vs. Multicast Vs. Broadcast Communications

- Unicast is meant for point-to-point communication. Multicast (like IEC 61850 GOOSE) is meant for point-to-multipoint communication. Broadcast is meant for all devices on a LAN.
- The preferred approach is to limit broadcast and use a direct publish/subscribe model so all the hosts only get the packets each host wants to process.
- SEL offers devices that support all three transmission techniques:
  - Filtering unicast is supported via the SEL-3620 Ethernet Security Gateway and the SEL-3622 Security Gateway.
  - The SEL-2741 Ethernet Switch and SEL-2742S Software-Defined Network Switch can filter all types of traffic. SDN also provisions circuits with a publisher/subscriber perspective, as seen in the IEC 61850 standards.

IRIG-B Vs. NTP Vs. PTP

- IRIG-B is the most accurate (tens of nanoseconds) time synchronization protocol, followed by PTP (hundreds of nanoseconds), followed by NTP (milliseconds).
- NTP and PTP offer time synchronization over Ethernet, while IRIG-B requires a dedicated cable.
- SEL offers devices that support all three time synchronization protocols:
  - All SEL IEDs support IRIG-B inputs.
  - SEL offers full PTP solutions, including clocks, switches, and clients.
  - Other SEL communications devices support NTP.

Useful Terms

NTP

Network Time Protocol

PTP

Precision Time Protocol

Recoverability

The ability to return a system to a working state after a failure, with the ability to continue to recover from more failures.

Redundancy

Additional always-active elements that allow a system to continue normal operation even during failure scenarios.

SEL SCHWEITZER ENGINEERING LABORATORIES

Making Electric Power Safer, More Reliable, and More Economical
+1.509.332.1890 | info@selinc.com | selinc.com

PF00707 • 20230911