SEL SDN

Software-Defined Networking

A better OT network awaits

- Eliminate common LAN security threats with deny-by-default architecture.
- Improve network failover times to under 100 µs.
- Simplify network configuration for demanding IEC 61850 systems.
- Streamline data collection for cybersecurity audits and NERC CIP compliance.

Key Features

SEL Uses SDN to Optimize Operational Technology (OT) Networks

Traditional Ethernet switches generally behave similarly regardless of the environment (one size fits all). With SDN, LAN switching can be tuned or optimized for the specific requirements of the environment. Only SEL has implemented SDN with the goal of optimizing an OT network. SEL SDN allows you to purpose-engineer networks like you purpose-engineer the power system.

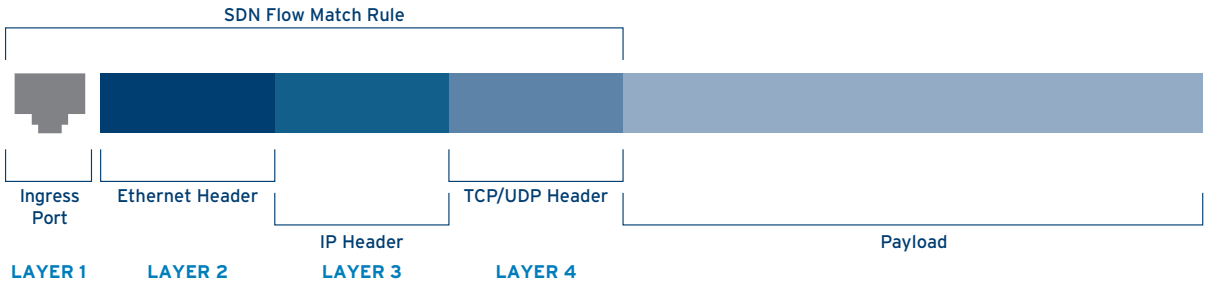
Eliminate Cyber Vulnerabilities

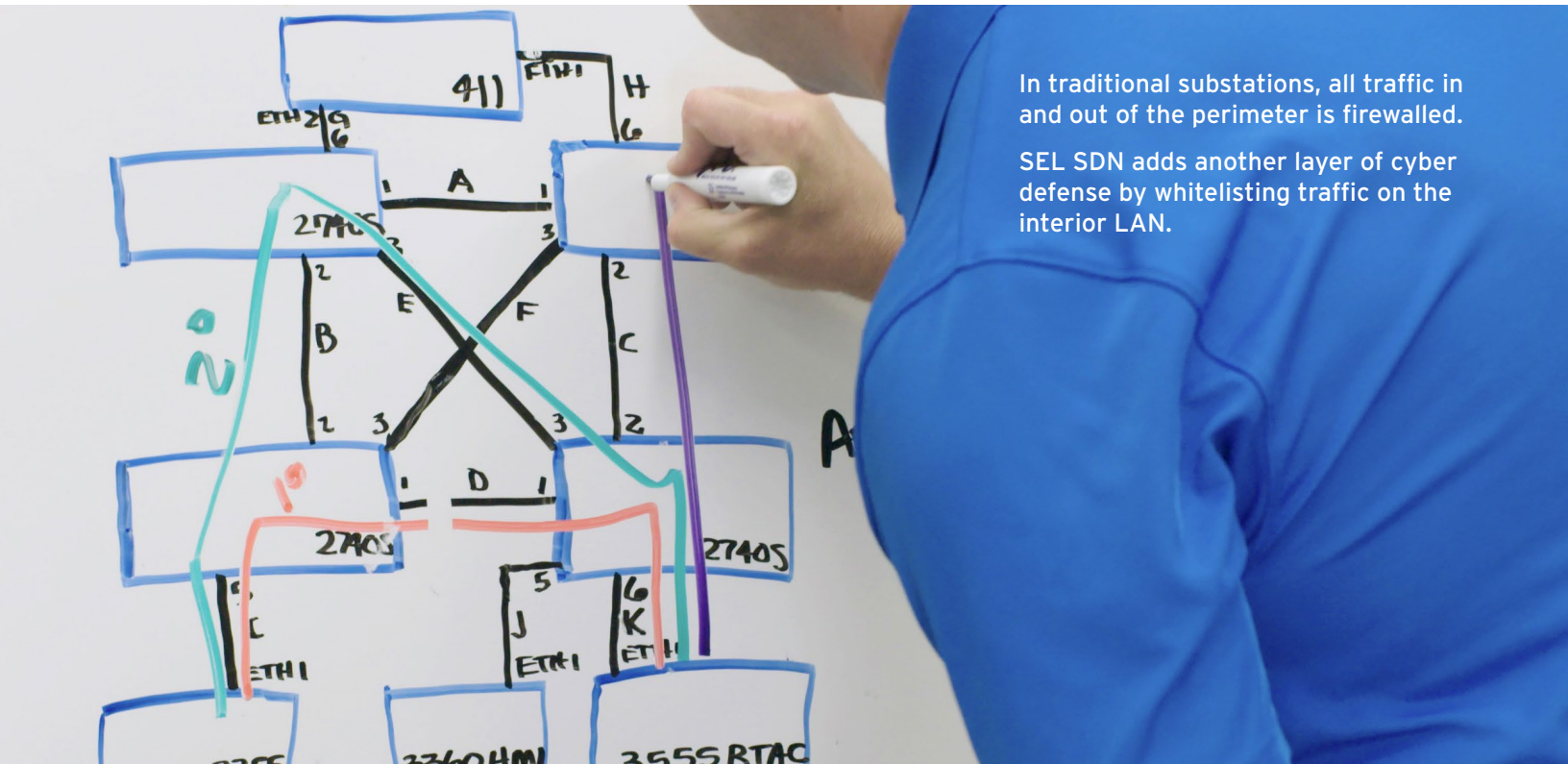
Traditional networks use features like MAC tables, the Rapid Spanning Tree Protocol (RSTP), and cast types for many conveniences, including plug-and-play functionality. However, these features also make traditional networking vulnerable to cybersecurity threats, including MAC flooding and table poisoning, Address Resolution Protocol (ARP) spoofing, Bridge Protocol Data Unit (BPDU) attacks, and more. With SEL SDN, all network flows and backup paths are specifically defined in the controller, so there is no need for MAC tables or RSTP. In addition, SDN uses traffic engineering to process forwarding behavior, rather than relying on cast types.

Whitelist All LAN Traffic

SEL SDN uses flow match rules to whitelist network flows. The ingressing packets can be matched against the ingress port, Ethernet source/destination MAC address, Ethertype, VLAN identifier, IP source/destination address, and so on. Packets that do not match the rules do not get forwarded.

In a sense, SEL SDN is acting like a firewall on all traffic traversing the LAN. This provides protection against attacks which physically take place inside the firewalls and also adds protection against unauthorized traffic that slips past firewalls.





Manage the Network Centrally and Securely

The SEL-5056 Software-Defined Network Flow Controller is the central interface for the commissioning, configuration, and monitoring of all SEL-2740S Software-Defined Network Switches. The only changes allowed on the network are made through the flow controller. With SEL SDN, you'll have advanced situational awareness. You'll know exactly what devices are on your network and all the conversations each device is having.

No engineering access interface is necessary on SEL-2740S switches. HTTPS provides encryption and authentication for secure management of SEL-5056 web browser communication. SEL-5056 communication to all SEL-2740S switches occurs through encrypted and authenticated Transport Layer Security (TLS). Keys are securely managed through X.509 certificates.

You can configure user accounts on the SEL-5056 or use the Lightweight Directory Access Protocol (LDAP) to authenticate users. The SEL-5056 and SEL-2740S support Syslog for secure log management. In addition, the flow controller provides backup and restore features for maintaining high reliability.

Reduce Network Failover Times by Two Orders of Magnitude

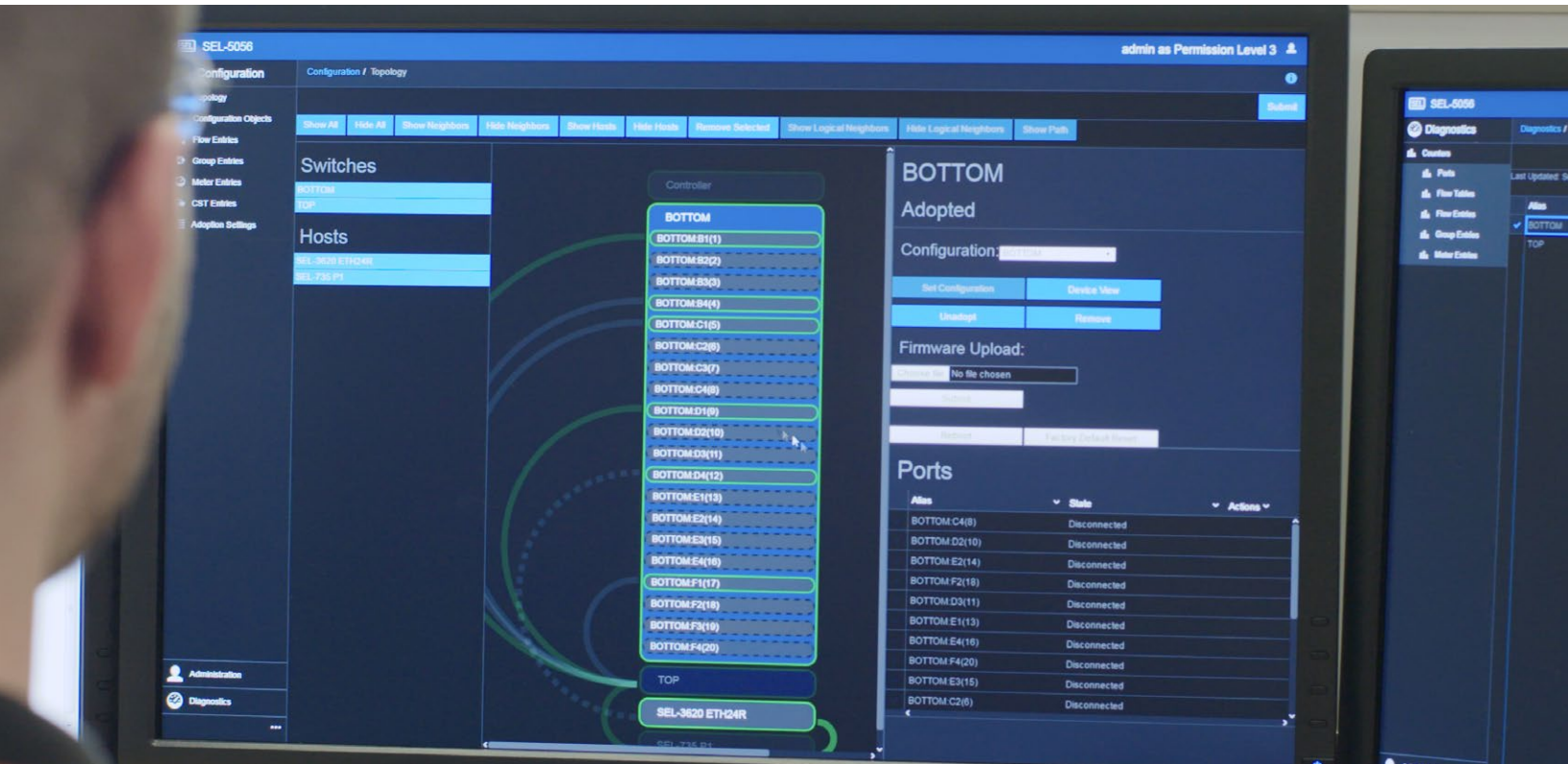
The SEL-5056 configures redundant paths not only to the primary path but also to the secondary path. This enables SEL-2740S switches to heal the network significantly faster than RSTP Ethernet switches because there is no waiting for discovery or convergence times. This fast failover is critical for applications using IEC 61850 GOOSE messages and IEC 61850-9-2 Sampled Values.

Control Network Traffic With Greater Precision

With SDN, it's easier to manage large amounts of network traffic than it is with traditional networking. The difference is that SDN eliminates unnecessary traffic on your network. Instead of having a node broadcast to all other nodes on the LAN, you can engineer specific paths and remove the extraneous ones. This ensures bandwidth availability and high performance in critical applications, such as IEC 61850 GOOSE messaging. And unlike RSTP switches, there are no blocked ports limiting bandwidth. For Ethernet-based control, SDN eliminates several problems inherent in traditional Ethernet switches.

Network Failover Times

Traditional RSTP Switches	SEL SDN Switches
>10 ms	**<0.1 ms**



Control Network Flows Precisely

The SEL-5056 is a Microsoft Windows Server-based software tool for SDN configuration and management. This flow controller configures primary and backup paths for each communications flow on SEL-2740S switches by using attributes of a specific protocol session and forwarding paths instead of requiring MAC addresses and VLANs. This eliminates the additional network-required tags or labels and simplifies operations. With the removal of RSTP, the network bandwidth is free for operational data and free from RSTP topology design restrictions.

SEL-5056 network configuration can be performed in the field with all IEDs connected or performed offline in a lab. Offline configuration provides flexibility and can reduce the downtime required for field installations.

The SEL-5056 provides comprehensive monitoring of all path- and packet-level network statistics of each communications flow, increasing awareness of the network health and status. In addition, you can programmatically test the network implementation before deployment.

Automate Configuration

Learn & Lock is an optional extension for the SEL-5056 that provides supervised automation for commissioning SDN switches, learning what conversations are trying to happen, and provisioning circuits to allow those conversations. Learn & Lock streamlines configuration by discovering devices on the LAN and creating a set of flows for the current traffic.

The Learn & Lock extension automates the following functions:

- **Topology Management**—Adopting switches, hosts, and links.
- **Communications Circuit Provisioning**—Discovering the Transmission Control Protocol (TCP), User Datagram Protocol (UDP), ARP, and Internet Control Message Protocol (ICMP) conversations on the network and provisioning the circuits to allow them to happen.
- **Reporting**—The ability for the system operator to review or remove devices or learned communications circuits and to save the final state as the baseline for future reference.
- **Network Reset**—The removal of all previous configurations of past Learn & Lock sessions.

Streamline Data Collection for NERC CIP Reporting

Flow Auditor is the first application in the SEL-5057 SDN Application Suite. It works with the SEL-5056 to generate audit reports for NERC CIP-007-6 R1 for each SDN network that the controller manages.

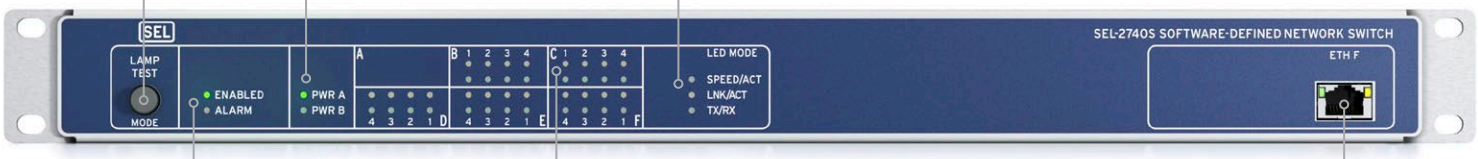
Unlike network scanning, Flow Auditor does not disrupt the operational network or inject any packets on the network. The application audits the controller database for the configuration without needing to pull data from switches. Flow Auditor can create new audit reports at any time for each registered controller without impacting the performance of the operational network. Reports are stored in the Flow Auditor database and can be retrieved and exported through the user interface. Flow Auditor streamlines data collection from days or weeks to minutes!

Flow Auditor supports Microsoft Windows 7, Windows 10, and Windows Server 2016 and is installed on the same computer as the SEL-5056 or on a computer that can reach the flow controller through the network.

Validate Your Design Before It's Deployed

Don't wait until deployment to validate your design. Instead, use the SEL-5056 to programmatically test the network implementation and validate all configurations and contingencies during factory acceptance testing. That way, you eliminate errors before going live and reduce commissioning timelines.

SEL-2740S Overview



Lamp Test button verifies all LEDs are functional and is used to select the LED mode.

Three LED modes supported for Ethernet port status.

Power supply status LEDs.

Ethernet port status LEDs.

Out-of-band flow controller port.

General status indicators. "Enabled" indicates the unit is operational. "Alarm" indicates major or minor alarm conditions.

Slot D provides 10/100/1,000 Mbps data rate support.

Four RJ45 10/100BASE-T ports.

Flow processor and alarm contact.

Lightweight aluminum case ensures maximum reliability and ease of installation.

Five modular slots for copper or fiber Ethernet interface options (in sets of four).

Dual power supply options for hot-swappable redundancy.

SEL-2740S Specifications

General	
Module	**10/100/1000BASE-T Copper** Number of ports: 4 Maximum cable distance: 100 m **1000BASE-SX Fiber-Optic Multimode** Number of ports: 4 Maximum cable distance: 500 m **100BASE-FX Fiber-Optic Multimode** Number of ports: 4 Maximum cable distance: 2 km **10BASE-FL Fiber-Optic Multimode** Number of ports: 4 Maximum cable distance: 2 km **1000BASE-LX10 or -LX Fiber-Optic Single-Mode** Number of ports: 4 Maximum cable distance: 10 km **1000BASE-LX Fiber-Optic Single-Mode** Number of ports: 4 Maximum cable distance: 10 km **1000BASE-EX Fiber-Optic Single-Mode** Number of ports: 4 Maximum cable distance: 40 km **Alarm Contact and Coprocessor**[1]
Power Supply Ratings	Base unit includes one power supply; second supply is optional. **Voltage Options** 100/120/220/230 Vac at 45—65 Hz 100/125/220/250 Vdc 24/48 Vdc[1]
Operating Temperature Range	—40° to +85°C (—40° to +185°F)
Relative Humidity	5—95%, noncondensing
OpenFlow 1.3.4 Support	Number of tables: 4 Flow rules per table: 1,024 Number of groups: 256 Number of action buckets per group: 30 Number of unique action buckets: 128 Number of meters: 64 Number of meter bands per meter: 1
IEEE 1588 PTP Support	Transparent clock, peer-to-peer, IEEE C37.238 power system profile

[1]One alarm contact flow coprocessor module is required in each SEL-2740S, installed in Slot A.

SEL SCHWEITZER ENGINEERING LABORATORIES

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

PF00333 • 20200316