



DESIGNED & ENGINEERED IN TÜRKİYE

THE UPPER SEGMENT OF CRITICAL-INFRASTRUCTURE NETWORKING

SMG-SW Series

The ring breaks.
The protection message doesn't.

A modular L2/L3 switch up to 100G for harsh field conditions — for substations, rail systems, industrial plants and telecom/ISP access networks. Zero-loss HSR/PRP · hardware-timestamped PTP · OT security built in · full MPLS/EVPN routing — in one SMG-SW operating system.

100G

PER SLOT

3

RING PROTOCOLS

0

LOSS — HSR/PRP

IEC 62443

OT SECURITY



SMG-SW818 · 2U modular chassis, 8 expansion slots, redundant power



01

COMPANY

The Company That Builds the Industrial Backbone

Simgenet Mühendislik is a Turkish engineering company delivering industrial networking and critical-infrastructure communication systems. The SMG-SW operating system is **entirely original**, developed in house at Simgenet.

2000

FOUNDED

500+

COMPLETED PROJECTS

30+

COUNTRIES SERVED

100+

PRODUCT TYPES

■ Why our own switch

For years we have deployed industrial switches in substations, rail systems and operator access networks. The gaps we saw in the field were always the same: QoS that did not protect protection traffic, rings that were not truly seamless, devices that were hard to manage. SMG-SW was built from that experience and **validated with our own measurement platform, SVP**.

■ Why our own software

- **Technological sovereignty** — no dependency on foreign-vendor licences and roadmaps
- **Features to the specification** — the protocol and screen the project requires are added
- **One operating system, every chassis** — the same SMG-SW OS on all three chassis; management concepts shared with the router family
- **Long service life** — support across a 15–20 year infrastructure lifecycle

Our departments are separate. The software of Simgenet-branded products is developed by our own **manufacturing and R&D department**; transmission systems and field deployment are delivered by separate specialist teams. We measure the network we build with SVP and hand over the result with its standard reference.

Our Mission

To deliver innovative, reliable and sustainable technology for industrial networks and critical-infrastructure communications, safeguarding our customers' business continuity.

Our Vision

To become Türkiye's most trusted and innovative network-infrastructure technology partner, recognized as a global brand.

02

PLATFORM

What is the SMG-SW Series?

SMG-SW is a **managed Layer 2/3 switch family for harsh field conditions**, designed for power-utility automation, rail, industrial plants and operator access networks. It delivers the full feature set of the upper segment — seamless rings, hardware-timestamped PTP, built-in OT security and a complete routing stack — in a single SMG-SW image, with the concepts network engineers already know. Port layout is defined per project by cards; the device grows later.

■ Modular chassis, ports by card

There is no fixed port count: 1G copper/fibre, 10G, 40G and 100G cards are fitted to a 1U four-slot or 2U eight-slot chassis. The same device grows later by adding cards.

■ One operating system, one skill set

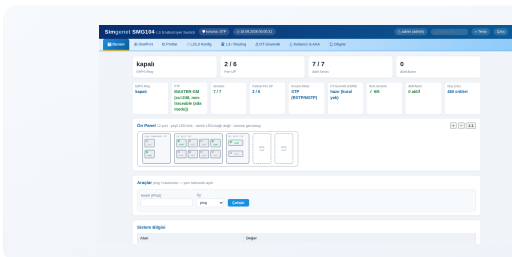
The SMG-SW operating system shares its management concepts with the SMGOS router family. Engineers manage switch and router with the same concepts and the same show output; training and spares are a single line item.

■ Validated with evidence

Spanning tree, LLDP, LACP, IGMP, port security and PTP behaviour are developed by measuring against independent peer devices with the Simgenet SVP test platform; run records instead of an "it works" statement.

Key Capabilities

- RSTP / MSTP — PortFast, BPDU/root/loop guard, err-disable recovery
- ERPS (G.8032), MRP (IEC 62439-2), HSR/PRP RedBox (IEC 62439-3)
- PTP boundary clock — IEC 61850-9-3 power profile, gPTP; hardware timestamping
- IEC 61850 GOOSE/SV priority protection and OT allowlist
- 802.1X / MAB / CoA, port security, DHCP snooping, IPsec, DAI
- OSPF, IS-IS, BGP, MPLS/L3VPN, Segment Routing, EVPN-VXLAN, VRRP, BFD, IPsec/OpenVPN
- LACP, LLDP, QinQ, IGMP snooping, jumbo frames
- HTTPS web + industry-familiar CLI, AAA, SNMPv3, signed-package updates



Status dashboard and live front panel

Ring, PTP, services, OT security and alarm status at a glance; the front panel shows the real port layout and link state, empty slots drawn dashed.

Port	Status	Role	MTU	Counters	Label	PTP
Port1	Up	10G	9000	0	0	0
Port2	Up	10G	9000	0	0	0
Port3	Up	10G	9000	0	0	0
Port4	Up	10G	9000	0	0	0
Port5	Up	10G	9000	0	0	0
Port6	Up	10G	9000	0	0	0
Port7	Up	10G	9000	0	0	0
Port8	Up	10G	9000	0	0	0

Port management in one table

Physical ports, MTU, counters, label and role on the same screen; critical ports cannot be shut down by mistake.

Router chassis, switch software. SMG-SW411, SMG-SW104 and SMG-SW818 are the switch editions of the SMG411, SMG104 and SMG818V5 router chassis. Same card catalogue, same power and environmental specifications; only the role and software profile differ.



03

HARDWARE

Chassis and Port Architecture

Port count is not a fixed property of the product; it is the result of **slot count × installed card**. Each slot accepts a card of independent speed and interface type; 1G copper, 10G fibre and 100G cards can be mixed in the same chassis.



SMG-SW411

- 1U rackmount, compact
- 1G and 10G cards
- Branch, field cabinet, access edge



SMG-SW104

- 1U rackmount, 4 expansion slots
- 1G / 10G / 40G / 100G cards
- Substation, aggregation layer



SMG-SW818

- 2U rackmount, 8 expansion slots, redundant power
- Cards from 1G to 100G
- Backbone, control centre, high port density

■ Card catalogue (Simgenet)

- **1G:** 8× SFP · 4× SFP · 8× RJ45 · 4× RJ45
- **10G:** 2× SFP+ · 4× SFP+
- **40G:** 2× QSFP+
- **100G:** 2× QSFP28
- A different card in every slot; mixed configurations allowed

■ Example port capacities

- SMG-SW818 · 8 slots × 8×1G = **64 × 1G**
- SMG-SW818 · 8 slots × 2×100G = **16 × 100G**
- SMG-SW818 · 6 × (8×1G) + 2 × (2×100G) = 48 × 1G + 4 × 100G uplinks
- SMG-SW104 · 4 slots × 8×1G = **32 × 1G**; 4 × 2×10G = 8 × 10G
- Port labels in slot/port notation (e.g. Gi4/0/2, Te c/0/0); cards are recognized automatically

■ Common platform features

- 220 VAC power; 2× redundant power supplies on SMG-SW818
- Operating temperature -20 °C to +60 °C
- Dedicated RJ45 Ethernet management port — HTTPS web and SSH CLI
- SFP/QSFP optical diagnostics (DDM): temperature, supply, TX/RX power live

Slot	Port	Speed	Type	Identity
1	1	10G	SFP+	10G-SFP+
1	2	10G	SFP+	10G-SFP+
1	3	10G	SFP+	10G-SFP+
1	4	10G	SFP+	10G-SFP+
2	1	10G	SFP+	10G-SFP+
2	2	10G	SFP+	10G-SFP+
2	3	10G	SFP+	10G-SFP+
2	4	10G	SFP+	10G-SFP+
3	1	10G	SFP+	10G-SFP+
3	2	10G	SFP+	10G-SFP+
3	3	10G	SFP+	10G-SFP+
3	4	10G	SFP+	10G-SFP+
4	1	10G	SFP+	10G-SFP+
4	2	10G	SFP+	10G-SFP+
4	3	10G	SFP+	10G-SFP+
4	4	10G	SFP+	10G-SFP+

Automatic slot / card recognition

Installed cards are listed automatically with slot, port, speed/type and identity; port names follow the slot/port scheme, and cable and link diagnostics run per port.

Positioning. SMG-SW818 for 100G density and the backbone role; SMG-SW104 for 1G/10G port density and 100G uplinks; SMG-SW411 for the compact access edge. All three use the same card catalogue and the same software.



04

LAYER 2

Switching, Spanning Tree and Aggregation

A loop-free, predictable and manageable Layer 2: the complete set of standard spanning-tree protections, dynamic link aggregation and topology visibility — a switch **whose behaviour does not change as the network grows**.

■ VLAN and switching

- 802.1Q VLAN; access and trunk ports; inter-VLAN routing (SVI)
- **QinQ (802.1ad)** — S-VLAN/C-VLAN double tagging, for operator access and double tagging over HSR
- MAC learning and table, static MAC, jumbo frames 9000 B
- Port mirroring (SPAN): source/destination/direction

■ Spanning Tree — RSTP / MSTP

- IEEE 802.1D/802.1Q; MSTP instance → VLAN mapping, region configuration
- **PortFast, BPDU guard, root guard, loop guard**, BPDU filter
- err-disable and automatic recovery; MAC-table flush on topology change
- Role / root hand-over / failover validated against independent peer switches with SVP

■ Link aggregation — LACP (802.1AX)

- Dynamic LACP (fast/slow) and static LAG
- Takeover on member loss, redistribution on member return
- Safe behaviour when the far end has LACP disabled

■ Neighbour discovery — LLDP (802.1AB)

- Mandatory TLVs + system description, capabilities, management address
- Fixed chassis-id; neighbour table in web and CLI (`show lldp neighbors`)
- For topology visibility and NMS discovery

■ Multicast — IGMP snooping

- IGMP v1/v2/v3; querier, fast-leave, static mrouter port
- GOOSE/SV and video multicast forwarded only to member ports

■ Storm and control-plane protection

- Storm watchdog: pps and load thresholds, broadcast/multicast alarm
- **CoPP** — control-plane protection, 17 traffic classes
- The management path stays open even during a data storm

With the concepts you already know. Industry-established concepts and outputs such as spanning-tree guard loop, switchport port-security and show etherchannel are the same; the command syntax is the Simgenet CLI. The existing network team masters the device without retraining.



05

CONTINUITY AND TIME

Ring Redundancy and PTP

In critical infrastructure a switch has two duties: not losing traffic at the moment of failure, and carrying **the same time** to every device on the network. SMG-SW offers three ring protocols and a hardware-timestamped PTP boundary clock in the same software — **the ring breaks, the protection message is not lost; the antenna is only at the centre, time is at every IED.**

■ ERPS — ITU-T G.8032

Ethernet ring protection; RPL owner and non-owner roles, WTR; protected ring ports. For operator and campus rings.

■ MRP — IEC 62439-2

Media Redundancy Protocol; MRM (manager) and MRC (client) roles. Compatibility with the PLC ecosystem in industrial-automation rings.

■ HSR / PRP RedBox — IEC 62439-3

Zero-loss seamless redundancy; RedBox mode, supervision frames, neighbour table. **VLAN-tagged and QinQ-encapsulated HSR** — a product differentiator.

■ PTP boundary clock — IEEE 1588-2019

- Multi-port boundary clock; **hardware timestamping** on 1G/10G switch ports; receives from above, regenerates to downstream ports
- Profiles: **IEC/IEEE 61850-9-3** power profile · 1588 default · **802.1AS gPTP**
- Port role auto/master/slave; domain, priority and clock source configurable
- Familiar command pattern: ptp mode boundary, ptp profile power
- End-to-end time chain with the Simgenet GNSS Server; measured with SVP

■ QoS

- 802.1p / DSCP mapping, priority classes
- Rate limiting (policer): limit low-priority traffic, never touch protection traffic
- NTP client; system-clock discipline

Ring + time together. PTP power profile and GOOSE priority pass through the same port over HSR/PRP; when the ring breaks the protection message is not lost and the time chain does not break. In substation acceptance all three are documented in a single SVP run.

Time Chain and Ring Selection

Centre

Simgenet GNSS Server grandmaster — G.8275.1 / 61850-9-3

Aggregation

SMG-SW818 boundary clock — receives from above, distributes into the ring

Station

SMG-SW104 boundary clock — power profile to IEDs, PMUs and recorders

When ERPS

Operator and campus rings; mixed rings with standard Ethernet devices; manageable revertive behaviour (WTR).

When MRP

PLC and industrial-automation ecosystem; shared ring with IEC 62439-2 compliant devices.

When HSR/PRP

Protection and process bus; zero-loss dual path where the loss of a single frame is not acceptable.



06

OT SECURITY

Operational Technology Security

Every network with PLCs, IEDs, RTUs and sensors — substation, rail signalling, water and energy plants, production lines, ports and defence — asks the same two questions: **who may connect, and what may pass?** SMG-SW answers both at switch level within the IEC 62443 framework; in power-utility automation it also recognizes and protects the protection message itself.

■ QoS-61850 — protection-traffic priority

- GOOSE (0x88B8) and SV (0x88BA) frames protected by PCP; latency and loss budget held under background saturation
- PCP-selective policer: low priority is limited, $PCP \geq 4$ protection traffic is never touched
- Priority-class scheduling at egress
- IEC 60870-5-104, DNP3 and Modbus-TCP SCADA traffic in the same QoS scheme

■ OT security — port allowlist and IDS

- **GOOSE/SV port allowlist:** only defined APPIDs and IEDs pass through that port; tagged and untagged frames
- Flood limit: GOOSE/SV floods limited per port
- **GOOSE-IDS:** stNum/sqNum inconsistency, replay and spoofed-source detection
- **IEC 62351-6** HMAC verification; OT asset inventory

■ IEC 62443-aligned management

- Session and lockout policy, password policy, role separation (IEC 62443-4-2)
- Event log: RFC 5424 severity, message-ID catalogue, actor and source IP
- Secret masking: hidden fields in running-config and backups
- Software updates with signed packages; backup / restore / rollback

■ Ethernet OAM — CFM 802.1ag / Y.1731

- CCM continuity, LBM loopback, LTM linktrace
- DMM delay measurement (1588-timestamped)
- End-to-end service monitoring at operator circuit hand-over

The same hardening for every OT sector. Rejection of non-inventoried devices (802.1X/MAB, port security), blocking of rogue DHCP/ARP/IP sources (snooping, DAI, IPSG), control-plane protection (CoPP) and an IEC 62443-4-2 management policy; in power utilities, GOOSE/SV allowlist and IDS on top. Acceptance is measured under load with Simgenet SVP and delivered as a single standard-referenced report.

Example Layout — Substation

Process bus

SV/GOOSE, HSR/PRP, power-profile
PTP — SMG-SW104 RedBox

Station bus

MMS, GOOSE, IEC 104 — allowlist,
QoS-61850, IGMP snooping

WAN / centre

OSPF/BGP, IPsec, R-GOOSE transport
— SMG-SW818 / SMG router



07

SECURITY

Access Control and Layer-2 Security

Even when an unauthorized device is plugged into a port it never joins the network; rogue DHCP servers, ARP poisoning and MAC flooding stop at the switch. **Nothing undefined passes** — and every event is recorded with who and from where.

■ 802.1X port access control

- **802.1X authenticator** — port-based, RADIUS/EAP; dynamic VLAN assignment
- **MAB** (MAC authentication bypass) — for IEDs and sensors without certificates
- **CoA / Disconnect (RFC 5176)** — session teardown and re-authorization from the NAC server
- Filter-Id → dynamic access list
- Works with the Simgenet NAC Server and third-party NAC/RADIUS

■ Port security

- Allowed MAC count per port (maximum)
- Violation action: **shutdown / restrict / protect**
- **Sticky MAC** (persistent learning) and aging (absolute)
- err-disable and recovery; recorded in the event log

■ DHCP snooping, IPSG, DAI

- **DHCP snooping** — trusted/untrusted ports, binding table
- **IP Source Guard** — source-IP filtering against the binding table
- **Dynamic ARP Inspection** — validation against ARP poisoning
- All three together: rogue DHCP servers, IP/ARP spoofing and MAC flooding are blocked

■ Access lists and control plane

- IPv4 / IPv6 / MAC ACL; ingress and egress; per port
- CoPP — 17-class control-plane protection
- Storm watchdog: pps and load thresholds
- Critical-port protection: management/timing ports cannot be shut down from the web

■ Management security

- HTTPS mandatory; SSH CLI; brute-force lockout
- RBAC: admin / operator / viewer
- AAA: local + RADIUS + TACACS+ + LDAP; local fallback when the server is unreachable
- SNMPv3 authPriv; remote syslog

■ Hardening evidence

- DAI, IPSG, port-security and 802.1X behaviour verified with SVP NAC/AAA test vectors
- Regression on every release with known-PASS / known-FAIL controls
- Result: numbered run record and lockable report

Layered Defence

Port

802.1X / MAB, port security, err-disable
— who may connect

Layer 2

DHCP snooping, IPSG, DAI, ACL, storm
watchdog — what may pass

Management

AAA, RBAC, CoPP, SNMPv3, event log
— who may manage



08

LAYER 3

Routing, MPLS and Encrypted Transport

SMG-SW is a Layer-3 switch and carries **a complete routing stack in the same scope as the SMGOS router family**: IGP/BGP, MPLS and Segment Routing, EVPN-VXLAN, integrated VPN and sub-second convergence. It connects to the backbone at the aggregation layer without a separate router.

■ Interior gateway protocols and BGP

- **OSPFv2** — stub/NSSA areas, virtual-link, MD5 and key-chain authentication · multi-level **IS-IS** · **EIGRP** and **RIP**
- **BGP** — peer-group, standard/extended/large communities, ECMP, confederation, route dampening, Graceful Restart
- **BGP FlowSpec** — in-line DDoS-mitigation rules distributed dynamically network-wide
- Policy: named access-lists and prefix-lists, route-map, PBR, redistribution, per-protocol administrative distance
- Multicast: **PIM**, **IGMP**, **MSDP**; RPF and static mroute

■ MPLS, Segment Routing and EVPN

- **LDP** (discovery, dual-stack, IGP-sync) · **MPLS L3VPN / VPNv4** (route-target per VRF) · static **pseudowire** L2 circuit emulation
- **SR-MPLS** (OSPF / IS-IS integrated) · **SR-TE** policies (segment-list, candidate-path) · external controller via **PCEP**
- **EVPN-VXLAN** — Type 1–5 routes, symmetric IRB, multihoming (ESI), anycast gateway
- **VRF-lite** routing separation; inter-VLAN routing (SVI)

■ Integrated VPN and encryption

- **IPsec / IKEv2 site-to-site** — ESP AES-128/192/256 and AES-GCM; DH groups including ECP-521 and Curve25519; SHA-256/384/512
- **OpenVPN** server — certificate profiles, remote access with local or RADIUS authentication
- **DMVPN / NHRP** dynamic hub-and-spoke
- Control plane: HMAC-SHA-512 key-chain, SSH, encrypted passwords

■ High availability and fast convergence

- **VRRP v2/v3** — priority, preempt, timers
- ECMP load sharing and nexthop-group; BGP / IGP Graceful Restart
- Profiled **BFD** and **Seamless-BFD**; BFD-triggered failover
- **TI-LFA / LFA** fast reroute (OSPF and IS-IS)

Typical Positioning

Access

SMG-SW411 — L2 access, VLAN, port security, 10G uplink

Aggregation

SMG-SW104 — SVI routing, OSPF/BGP, ring, 100G uplink

Backbone

SMG-SW818 — MPLS/SR, EVPN, VRF, IPsec, up to 100G

Common management, every role. Because the SMG-SW switch and the SMGOS router share the same management concepts, access, aggregation and core are managed with the same concepts; L3VPN, pseudowire and EVPN-VXLAN services are offered side by side on the switch as well.



09

MANAGEMENT

Web, CLI, Backup and Monitoring

Web and CLI share the same configuration source; every change is validated, applied and read back from the device. A management surface that **needs no extra training**, and an auditable change history.

■ HTTPS web interface (EN/TR)

- Tabs: Status · Ports · Config (VLAN, ERPS, Spanning-Tree, LACP, PTP, DHCP-Snoop, IGMP-Snoop, Port-Security, ACL, QoS, CoPP, SPAN, OSPF/BGP/IS-IS/BFD/LDP/IPsec/VRF, LLDP, syslog/NTP) · OT Security · Slot/Card · Users & AAA · Events/Alarms
- SVG front panel, real port counters, MAC table, live policer counters
- Every change **validate** → **apply** → **read back**; an invalid setting is rejected with a clear error
- Dark/light theme, inline editing, copy to table

■ CLI (SSH) — industry-familiar

- `show running-config · show interfaces status · show spanning-tree · show port-security · show etherchannel · show lldp neighbors · show ptp · show mac-address-table · show log`
- Same concepts and show output; the command syntax is the Simgenet CLI
- Web and CLI share a single configuration source; every web function is available from the CLI
- Running-config on one page; secrets masked

■ Configuration safety

- Persistent configuration: save, reboot, same state
- Consistent backup and restore; integrity and device-identity check on restore
- **Rollback** from a faulty change; factory reset (double confirmation)
- Software updates with **signed packages**; version stamp; boot audit
- One-click diagnostic bundle

■ NMS and monitoring

- SNMP v2c / **v3 authPriv**; SIMGENET MIB (identity, status, RedBox, DDM)
- Event → automatic trap (ring change, service down); SNMP verified with common NMS and SIEM systems
- Structured remote syslog; event/alarm log (X.733 severity classes)
- SFP DDM optical-power threshold alarm

CLI Output from a Live Device

```

SMG-SW104# show spanning-tree
Spanning tree enabled protocol rstp
  Root ID    8.000.96:09:D3:21:51:6B (this bridge)
  Hello 2 s   Max Age 20 s   Fwd Delay 15 s
Interface   Role  Sts  Cost  Prio.Nbr  Type
Gi4/0/0     Desg  FWD  2000  8.001    P2p
Gi4/0/1     Desg  FWD  2000  8.002    P2p
Gi4/0/3     Desg  FWD  2000  8.003    Edge P2p

```

```

SMG-SW104# show ptp
PTP Boundary Clock, domain 0
  Profile      : power (IEC/IEEE 61850-9-3)
  Clock ID    : 9409d3.ffff.21516b  class 248
  GM          : 9409d3.ffff.215167  (1 step)
  Offset      : 4.0 ns  path delay 504.0 ns
Port         State  Delay-mech
Gi4/0/2      SLAVE  E2E
Te c/0/0     MASTER P2P

```



10

APPLICATIONS

Use Cases and Positioning

■ Power / substation

Station and process bus: HSR/PRP RedBox, IEC 61850-9-3 PTP boundary clock, GOOSE/SV priority and allowlist, IEC 104/DNP3 routing; IEC 62443-aligned management.

■ Rail / transport

Station rings (ERPS/MRP), QoS priority and PTP for signalling traffic; OSPF/BGP connection to the centre, field access control with port security.

■ Telecom / ISP access and aggregation

QinQ, LACP, ERPS rings, LDP/MPLS transport, CFM/Y.1731 service OAM; modular ports from 1G to 100G; NMS integration via SNMPv3.

■ Industrial plant / water / government / defence

IEC 62443 hardening on PLC and SCADA networks: NAC integration with 802.1X/MAB/CoA, DHCP snooping/IPSG/DAI, ACL and CoPP; MRP/ERPS rings; AAA (RADIUS/TACACS+/LDAP) and central event logging.

Model Positioning

SMG-SW411

Access edge, field cabinet — compact
1U, 1G/10G

SMG-SW104

Substation and aggregation — 1U, 4
slots, 100G uplink

SMG-SW818

Backbone and control centre — 2U, 8
slots, redundant power, up to 100G

Upper-segment feature set. SMG-SW411 and SMG-SW104 are the compact L3 switch class, SMG-SW818 the modular backbone class; the feature set is built to the upper segment of critical-infrastructure switching, and management uses the concepts network teams already know.

Evidence-based hand-over. We measure the switched network we build with our own test platform, SVP, and document the result with its standard reference — instead of an "it works" statement, a measured and lockable report is delivered.



11

TECHNICAL SPECIFICATIONS

Simgenet SMG-SW Series

FEATURE	SMG-SW SERIES
Product class	Managed L2/L3 switch for harsh field conditions; SMG-SW operating system, developed entirely in house at Simgenet
Models / chassis	SMG-SW411 (1U, compact) · SMG-SW104 (1U, 4 slots) · SMG-SW818 (2U, 8 slots, redundant power, up to 100 G)
Port structure	Slot × Simgenet card: 8×1G SFP · 4×1G SFP · 8×/4× RJ45 · 2×10G SFP+ · 4×10G SFP+ · 2×40G QSFP+ · 2×100G QSFP28; port count is defined by the installed cards (e.g. 8 slots × 8×1G = 64 ports)
L2	VLAN (802.1Q) access/trunk · QinQ (802.1ad) · MAC learning/table · jumbo 9000 B · LACP (802.1AX, fast/slow) · LLDP (802.1AB-2016)
Spanning Tree	RSTP + MSTP (instance/VLAN, region) · PortFast · BPDU guard · root guard · loop guard · BPDU filter · err-disable recovery
Ring / redundancy	ERPS (ITU-T G.8032) · MRP (IEC 62439-2) · HSR/PRP RedBox (IEC 62439-3), VLAN-tagged and QinQ-encapsulated HSR
Multicast	IGMP snooping v1/v2/v3 (querier, fast-leave, static mrouter)
Timing	PTP boundary clock (IEEE 1588-2019), multi-port; hardware timestamping on 1G/10G switch ports; profiles IEC/IEEE 61850-9-3 (power), 1588 default, 802.1AS (gPTP) · NTP
QoS	802.1p / DSCP mapping · priority classes · IEC 61850 GOOSE/SV priority protection · rate limiting (policer)

Continued on the next page: Layer 3, access and Layer-2 security, OT security, OAM, management, AAA, NMS, hardware and reference standards.



12

TECHNICAL SPECIFICATIONS

Security, Management and Hardware

FEATURE	SMG-SW SERIES
L3 / routing	Static · OSPFv2 · IS-IS · EIGRP · RIP · BGP (communities, ECMP, confederation, GR, FlowSpec) · PBR / route-map / prefix-list · PIM / IGMP / MSDP · VRF-lite · VRRP v2/v3 · BFD / S-BFD · TI-LFA
MPLS / overlay	LDP · MPLS L3VPN (VPNv4) · pseudowire · SR-MPLS · SR-TE · PCEP · EVPN-VXLAN (Type 1–5, symmetric IRB, ESI multihoming)
VPN	IPsec/IKEv2 site-to-site (AES-GCM, ECP-521, Curve25519) · OpenVPN server · DMVPN / NHRP
Access security	802.1X authenticator (RADIUS/EAP, dynamic VLAN) · MAB · CoA/Disconnect (RFC 5176) · Filter-Id → dynamic ACL · port security (maximum / violation shutdown-restrict-protect / sticky / aging)
Layer-2 security	DHCP snooping + binding table · IP Source Guard · Dynamic ARP Inspection · IPv4/IPv6/MAC ACL (ingress/egress) · CoPP (control-plane protection) · storm watchdog (pps/load thresholds)
OT security	IEC 61850 GOOSE/SV port allowlist + flood limit · GOOSE-IDS · IEC 62351-6 HMAC · OT asset inventory · IEC 62443-4-2 session/lockout policy
OAM / monitoring	CFM 802.1ag / Y.1731 (CCM continuity check, LBM/LTM loopback and linktrace, DMM delay measurement) · SPAN port mirroring · SFP DDM optical diagnostics · cable/link diagnostics
Management	HTTPS web (EN/TR, role-based admin/operator/viewer) · SSH CLI with industry-familiar show family · running-config on one page · validate → apply → read-back · backup / restore / rollback / factory reset · software updates with signed packages
AAA	Local + RADIUS + TACACS+ + LDAP; RBAC; brute-force lockout
NMS	SNMP v2c/v3 (authPriv) + SIMGENET MIB + traps · SNMP verified with common NMS and SIEM systems and structured remote syslog · event/alarm log (X.733 severity)
Hardware recognition	Automatic slot/card recognition (SMBIOS/PCI), port labelling, SVG front panel
Management port	Dedicated RJ45 Ethernet management port — HTTPS web and SSH CLI
Power / environment	220 VAC; SMG-SW818 2× redundant power · -20 °C to +60 °C

Reference Standards

IEEE 802.1Q · 802.1D · 802.1ad (QinQ) · 802.1AX (LACP) · 802.1AB-2016 (LLDP) · 802.1X · 802.1ag (CFM) · 802.1AS · IEEE 1588-2019 · IEC/IEEE 61850-9-3 · IEC 61850-8-1 / 9-2 · IEC 62351-6 · IEC 62439-2 (MRP) · IEC 62439-3 (HSR/PRP) · IEC 62443-4-2 · ITU-T G.8032 (ERPS) · G.8013 / Y.1731 · RFC 2865 / 2866 (RADIUS) · RFC 8907 (TACACS+) · RFC 5176 (CoA) · RFC 3580 · RFC 2328 (OSPF) · RFC 4271 (BGP) · RFC 5575 (FlowSpec) · RFC 5880 / 7880 (BFD / S-BFD) · RFC 5036 (LDP) · RFC 4364 (L3VPN) · RFC 8402 (SR) · RFC 7432 / 8365 (EVPN-VXLAN) · RFC 5798 (VRRP) · RFC 7296 (IKEv2) · RFC 3411–3418 (SNMPv3) · RFC 5424 (syslog) · IEC 60870-5-104 · IEEE 1815 (DNP3) · X.733



Why Simgenet SMG-SW

Seamless rings, unbroken time

HSR/PRP, ERPS and MRP; with the hardware-timestamped PTP boundary clock the power-profile time chain reaches every IED.

OT security built in

Who may connect, what may pass: 802.1X/MAB, port security, snooping/DAI/IPSG, CoPP and IEC 62443 management; GOOSE/SV allowlist and IDS in power utilities.

Managed with the concepts you know

Industry-established concepts and show output; web and CLI share one configuration source; no extra training needed.

Modular, original and proven

A chassis that grows by card from 1G to 100G; software entirely developed in house at Simgenet; every feature validated against independent peer devices with the SVP test platform.

GET IN TOUCH

Address

Kartal / İstanbul, Türkiye

Phone

+90 555 600 4506

E-mail · Web

info@simgenet.net · simgenet.net

Simgenet Mühendislik Enerji San. ve Tic. Ltd. Şti.

Product Brochure · SMG-UB-SW-EN · Rev. 5 · © 2026

Engineered in Türkiye