RY-LGSP38-28

- **19" L2 and L3 switch with PoE+**
- **Copper ports: 24 x10/100/1000TX**
- **Fibre ports: 4 x SFP/SFP+ 1G/10G**
- **Manageable, ring-capable, static and dynamic routing**
- **OSPFv2/v3 und RIPv1/v2**
- **Non Stop PoE**
- **Controlled fans**
- **Power supply 230VAC**

This layer-2 and layer-3 switch was specially developed for applications with high data loads, such as video over IP, video streaming also in connection with multicast. The switch has extensive security features that protect both the switch itself and the network traffic. The PoE allows IP cameras to be powered via the data cable. With the extensive management options, even complex network requirements can be met.

Product information

Brief description
19" switch with management, strong security features and PoE +

Special Feature for Video Networks
Active monitoring of the camera
The switch continuously monitors PoE-powered cameras. In the event of a camera failure, the switch automatically restarts the camera. At the same time, the switch sends an SNMP message.

Active monitoring of the PoE supply
If, for example, too much power is demanded from the switch due to a defective camera, the switch alerts via SNMP.

Active management of PoE power
When the switch is started up, the individual PoE ports can start up with a time delay to prevent overloading the PoE power supply units.

Active integration of the switch in video management systems
For the popular video management systems Milestone and Siveillance Video, SW modules are available which allow direct integration of the switch management and the DMS into this VMS.

Uninterruptible PoE power supply
The PoE supply to the PDs is not interrupted when the switch is rebooted.

Jumbo frames even at 100 Mbps
Jumbo Frames up to 10'240Bytes are also supported at 100MBit/s

DMS

DMS (Device Management System)

The switch has an integrated network monitoring and control system that gives the user a good overview of the entire network in a very simple way. This DMS system has the following features:

Graphical network overview
The network topology view provides a quick overview of all switches and end devices present in the network, such as IP cameras or servers, including the IP address, device type and designation. Plans and maps can be stored as background images, allowing the user to quickly access specific network devices even without knowledge of the IP structure.

Device search
This function also allows targeted access to a specific device in larger networks. Newly added devices, such as an exchanged IP camera, are displayed immediately and allow the user to access the device immediately without knowing the IP address.

Data traffic display
The data traffic can be graphically displayed per port over a time axis.

Error handling and security
Network diagnostics between master switch and connected terminals.
Protection mechanisms such as data rate limitation allow effective protection against unwanted access.
With IEEE802.3ah and IEEE802.1ag, tools for the structuring of networks are available.

Special Features
The switch has extensive safety functions. For example, the ACL allows not only to protect the switch itself, but also the traffic in the network.
Non-Stop PoE: When the switch is rebooted, the PoE supply to the connected cameras is not interrupted. As soon as the switch is operational again, so are the camera images.

Technical data

Copper Ports	24 x 10/100/1000TX, PoE+, RJ45 Maximum PoE power over all ports: 370W
Fiber Ports	4 x SFP/SFP+, 1G/10G We recommend the use of our barox SFPs. We do not test or guarantee the compatibility of our devices with SFPs from other manufacturers..
Console Port	1 x RS232, RJ45
Supply Voltage	100-240VAC, 50-60Hz

Power Consumption	Max. 40W (without PoE) / 410W (with PoE)
MTBF	25°C: 188'146h 50°C: 59'932h
Operating temperature	0°C to 50°C
Dimensions	442 x 211 x 44mm (WxDxH)
Weight	Gross weight: 4.1 kg Net weight: 3.3 kg
Backplane	128GBit/s
MAC Table	32k
Configuration	Web GUI, DMS, SNMPv1, v2c and v3, Console, Telnet, RMON Individual management accesses can be disabled
PoE Management	**Port configuration** Supports PoE configuration function per port. **PoE scheduling** Supports per-port PoE scheduling to turn PoE devices (PDs) on/off. **Automatic check** Check the connection status of the PDs. Restart the PDs if there are no responses. **Power delay** The PoE ports can be turned on with a time delay to protect the switch from overload. **Non-Stop PoE, Soft Reboot** The switch also supplies power to the PDs during soft reboot.
Port Settings	Port disable/enable, Autonegotiation 10/100/1000Mbps, Flow Control disable/enable, Data rate control on each port, max. framesize, Power Control
Port Status Display	Display per port: speed, link status, flow control status, autonegotiation status, trunk status
Layer3 Functions	IPv4 and IPv6 Unicast: Static Routing RIP v1/v2: Routing Information Protocol (RIP) is an internal routing protocol based on distance vector routing used within an autonomous system. OSPF v2/v3 : OSPF is a link-state routing protocol. It is designed for internal operation in a single autonomous system. Each OSPF router maintains an identical database that describes the topology of the autonomous system. A routing table is calculated from this database by creating a shortest-path tree.
Communication Redundancy	Standard Spanning Tree (STP), IEEE802.1d Rapid Spanning Tree (RSTP), IEEE802.w Multiple Spanning Tree (MSTP), IEEE802.1s

VLAN	**Tag-based VLAN according to 802.1Q** Supports up to 4K VLANs simultaneously (out of 4096 VLAN IDs) **Port-based VLAN** A port member of a VLAN can be isolated to other isolated ports of the same VLAN and private VLANs. **Private VLAN edge (PVE).** Private VLANs are based on the source port mask and there are no connections to VLANs. This means that VLAN IDs and private VLAN IDs can be identical. **Voice VLAN** The Voice VLAN feature allows voice traffic to be forwarded on the Voice VLAN. **Guest VLAN** The IEEE 802.1X Guest VLAN feature allows a guest VLAN to be configured for each 802.1X port on the device to provide restricted services to non-802.1X compliant clients. **Q-in-Q (double tag) VLAN** This can be used to set specific requirements for VLAN IDs and the number of VLANs to support. **802.1v protocol VLAN** Classifying multiple protocols into a single VLAN often forces VLAN boundaries that are inappropriate for some of the protocols. This requires the presence of a non-standard entity that forwards frames containing the protocols for which the VLAN boundaries are unsuitable between VLANs. **MAC-based VLAN** The MAC-based VLAN feature allows incoming untagged packets to be assigned to a VLAN, classifying traffic based on the source MAC address of the packet. **IP subnet-based VLAN** In an IP subnet-based VLAN, all end workstations in an IP subnet are assigned to the same VLAN. In this VLAN, users can move their workstations without having to reconfigure their network addresses. **Management VLAN** Management VLAN is used to manage the switch from a remote location using protocols such as Telnet, SSH, SNMP, Syslog, and so on.
Link Aggregation	IEEE 802.3ad LACP / Static Trunk, supports five groups of 16-port trunks or static trunk.
QoS	**Hardware queue** Supports eight hardware queues. **Classification** Port-based: Traffic QoS by port. 802.1p: VLAN priority-based Layer 2 CoS QoS class of service is a parameter used in data and voice protocols to distinguish the types of payloads included in the transmitted packet. DSCP-based Differentiated Services (DiffServ) Layer 3 DSCP QoS: IP packets

can carry either an IP priority value (IPP) or a Differentiated Services Code Point (DSCP) value. QoS supports the use of both values because DSCP values are backward compatible with IP priority values.
Classification and re-marking of TCP/IP ACLs: QoS through ACL

Rate-limiting
Ingress policing
Egress shaping and per-port speed control

Scheduling
Strict Priority and Weighted Round Robin (WRR): Weighted Round Robin is a scheduling algorithm that uses the weights assigned to queues to determine how much data is emptied from a queue before it is moved to the next queue.

Security

Certified authentication
A private HTTPS key can be stored for management access.

User management
User rights can be freely set in up to 15 levels.

ACL
The switch allows up to 512 entries. Drop or rate restriction based on source/destination MAC/IP address or VLAN ID. Rules and conditions for incoming packets can be set per port. Rules include protocols, IP ports, and address ranges. Rules can be set using either the authorization or exclusion method. Criteria are: TCP/ UDP source and destination ports, 802.1p priority, Ethernet type, Internet Control Message Protocol (ICMP) packet.

Port Security
MAC address management per port and IP source guard: MAC address can be checked in combination with IP address.

Storm Control
Prevents traffic on a LAN from being disrupted by a broadcast, multicast, or unicast flood on a port.

RADIUS Authentication, 802.1X
Authorization and accounting, MD5 hash, guest VLAN, single/multiple host mode, and single/multiple sessions.
Supports IGMP RADIUS-based 802.1X
Dynamic VLAN assignment

TACACS+ authentication
The switch supports TACACS+ authentication. Switch as a client.

Secure Shell (SSH)
SSH secures Telnet traffic into or out of the switch, SSH v1 and v2 are supported.

Secure Socket Layer (SSL)
SSL encrypts HTTP traffic, providing advanced secure access to the browser-based management GUI in the switch.

HTTPS & SSL (Secured Web)
Hyper Text Transfer Protocol Secure (HTTPS) is the secure version of HTTP.

	BPDU Guard BPDU Guard, an extension of STP, removes a node that reflects BPDUs back into the network. It enforces the boundaries of the STP domain and keeps the active topology predictable by not allowing network devices behind a BPDU Guard-enabled port to participate in STP. **DHCP Snooping** With DHCP Snooping, the switch has a feature that acts as a firewall between untrusted hosts and trusted DHCP servers. **Loop Protection** Loop Protection prevents unknown unicast, broadcast, and multicast loops in Layer 2 switching configurations.
Multicast	**IGMP v1/v2/v3 Snooping** IGMP restricts bandwidth-intensive multicast traffic to requesters. Supports 1024 multicast groups. **IGMP Querier** IGMP Querier is used to support a Layer 2 multicast domain of snooping switches when no multicast router is available. **IGMP Proxy** IGMP Snooping with proxy reporting or report suppression actively filters IGMP packets to reduce load on the multicast router. **MLD v1/v2 Snooping** Delivers IPv6 multicast packets only to the required receivers. **Multicast VLAN Registration (MVR)** A dedicated, manually configured VLAN, called the Multicast VLAN, to forward multicast traffic over a Layer 2 network in conjunction with IGMP snooping.
Standards	IEEE 802.3 10Base-T IEEE 802.3u 100Base-TX/100BASE-FX IEEE 802.3z Gigabit SX/LX IEEE 802.3ab Gigabit 1000T IEEE 802.3x Flow Control and Back pressure IEEE 802.3ad Port trunk with LACP IEEE 802.1d Spanning tree protocol IEEE 802.1w Rapid spanning tree protocol IEEE 802.1s Multiple spanning tree protocol IEEE 802.1p Class ofservice IEEE 802.1Q VLAN Tagging IEEE 802.1x Port Authentication Network Control IEEE 802.1ab LLDP IEEE 802.3af/at Power over Ethernet IEEE 802.az Energy Efficient Ethernet