

RY-LGSOTR38-14

- **19" L2 und L3 Switch**
- **LWL-Ports: 12 x 100M/1G/2.5G/5G/10G**
- **LWL-UpLink-Ports: 2 x 1G/2.5G/5G/10G/25G**
- **Managebar, ringfähig, statisches und dynamisches Routing**
- **OSPFv2/v3 und RIPv1/v2**
- **Geregelter Lüfter**
- **Redundante Speisung 230VAC**

Dieser Layer-2 und Layer-3 Switch wurde eigens für Anwendungen mit hoher Datenlast, wie z.B. Video over IP, Video streaming auch in Verbindung mit Multicast entwickelt. Durch die schnellen Ports mit 10G und zwei uplink-ports mit 25G eignet sich der RY-LGSOTR38-14 als Distributionswitch in grösseren Netzen. Dieser Anwendung wird auch die redundanten Netzteile gerecht. Der Switch besitzt weitreichende Sicherheitsfunktionen, die sowohl den Switch selbst als auch den Netzwerkverkehr schützen. Mit den weitreichenden Managementmöglichkeiten lassen sich auch komplexe Netzwerkanforderungen erfüllen.

Produktinformationen

Kurzbeschreibung
19"-Switch für Distribution-Anwendung mit starken Sicherheitsfunktionen

Spezielle Eigenschaften
Durch die hohen Portgeschwindigkeiten von 12 x 10G und 2 x 25G eignet sich dieser Switch als Distributionswitch

Montageart
19"-Bauweise

Lüftung
Lüfter

Lieferumfang
Switch
19"-Montagewinkel
Selbstklebende Gerätefüße
Netzkabel
1 Netzteil, das zweite Netzteil für eine redundante Speisung muss separat bestellt werden
Konsolenkabel RJ45 auf D-Sub 9
Hinweiskarte QIG

Technische Daten

PoE Ports	Kein PoE
LWL Ports	12 x SFP oder SFP+ 100M/1G/2.5G/5G/10G
Uplink Ports	2 x SFP, SFP+ oder SFP28 1G/2.5G/5G10G/25G
Konsolenport	RS232, RJ45 Inkl. Konsolenkabel
Speisespannung	2 x 100-240VAC, 50-60Hz Redundante Einspeisung durch zwei Netzteile möglich Hot swappable
Leistungaufnahme	Max. 30W
Betriebstemperatur	0°C bis 50°C
Verlustleistung	136 BTU/h
Abmessungen	442 x 300 x 44mm (BxTxH)
Backplane	340GBit/s
MAC Tabelle	32k
Forwarding Rate	253 Mpps
Konfiguration	Web GUI, DMS, SNMPv1, v2c und v3, Konsole, Telnet, RMON Die Managementzugangsmethoden können einzeln deaktiviert werden.
Porteinstellungen	Port disable/enable, Autonegotiation 10/100/1000Mbps, Flow Control disable/enable, Datenratenkontrolle auf jedem Port, max. Framesize, Power Control
Port Statusanzeige	Anzeige pro Port: Geschwindigkeit, Link Status, Flow Control Status, Autonegotiation Status, Trunk Status
Layer3 Funktionen	IPv4 und IPv6 Unicast: statisches Routing RIP v1/v2: Das Routing Information Protocol (RIP) ist ein internes Routing-Protokoll, das auf dem Distanzvektor-Routing basiert und innerhalb eines autonomen Systems verwendet wird. OSPF v2/v3 : OSPF ist ein Link-State-Routing-Protokoll. Es ist für den internen Betrieb in einem einzelnen autonomen System konzipiert. Jeder OSPF-Router unterhält eine identische Datenbank, die die Topologie des autonomen Systems beschreibt. Aus dieser Datenbank wird eine Routing-Tabelle berechnet, indem ein Shortest-Path-Baum erstellt wird.
VLAN	**Tag-basiertes VLAN nach 802.1Q** Unterstützt bis zu 4K-VLANs gleichzeitig (von 4096 VLAN-IDs)

Port-basiertes VLAN
Ein Portmitglied eines VLANs kann zu anderen isolierten Ports desselben VLANs und privaten VLANs isoliert werden.

Privater VLAN-Edge (PVE)
Private VLANs basieren auf der Quellportmaske und es gibt keine Verbindungen zu VLANs. Das bedeutet, dass VLAN-IDs und private VLAN-IDs identisch sein können.

Voice VLAN
Die Voice VLAN-Funktion ermöglicht die Weiterleitung des Sprachverkehrs auf dem Voice VLAN.

Gast-VLAN
Mit der IEEE 802.1X-Gast-VLAN-Funktion kann ein Gast-VLAN für jeden 802.1X-Port auf dem Gerät konfiguriert werden, um nicht-802.1X-konforme Clients mit eingeschränkten Diensten zu versorgen.

Q-in-Q (double tag) VLAN
Damit lassen sich spezifische Anforderungen an VLAN-IDs und die Anzahl der zu unterstützenden VLANs einstellen.

802.1v-Protokoll-VLAN
Die Klassifizierung mehrerer Protokolle in ein einzelnes VLAN erzwingt oft VLAN-Grenzen, die für einige der Protokolle ungeeignet sind. Dies erfordert das Vorhandensein einer Nicht-Standard-Einheit, die die Rahmen mit den Protokollen, für die die VLAN-Grenzen ungeeignet sind, zwischen VLANs weiterleitet.

MAC-basiertes VLAN
Die MAC-basierte VLAN-Funktion ermöglicht es, eingehende unmarkierte Pakete einem VLAN zuzuordnen und so den Verkehr auf der Grundlage der Quell-MAC-Adresse des Pakets zu klassifizieren.

IP-Subnetz-basiertes VLAN
In einem IP-Subnetz-basierten VLAN werden alle Endarbeitsplätze in einem IP-Subnetz dem selben VLAN zugewiesen. In diesem VLAN können Benutzer ihre Arbeitsstationen verschieben, ohne ihre Netzwerkadressen neu konfigurieren zu müssen.

Management-VLAN
Management-VLAN wird für die Verwaltung des Switches von einem entfernten Standort aus unter Verwendung von Protokollen wie Telnet, SSH, SNMP, Syslog usw. verwendet.

Link Aggregation	IEEE 802.3ad LACP / Static Trunk, unterstützt fünf Gruppen von 16-Port Trunks oder Static Trunk.
QoS	**Hardware-Warteschlange** Unterstützt acht Hardware-Warteschlangen. **Klassifikation** Portbasiert: Verkehrs-QoS nach Port 802.1p: Die auf VLAN-Priorität basierende Schicht 2 CoS QoS Dienstklasse ist

ein Parameter, der in Daten- und Sprachprotokollen verwendet wird, um die Arten von Nutzlasten zu unterscheiden, die in dem übertragenen Paket enthalten sind. DSCP-basierte differenzierte Dienste (DiffServ) Schicht 3 DSCP-QoS: IP-Pakete können entweder einen IP-Prioritätswert (IPP) oder einen DSCP-Wert (Differentiated Services Code Point) tragen. QoS unterstützt die Verwendung beider Werte, da DSCP-Werte abwärtskompatibel mit IP-Prioritätswerten sind. Klassifizierung und Neumarkierung von TCP/IP-ACLs: QoS durch ACL

Rate-Limiting
Ingress-Policer
Egress-Shaping und Geschwindigkeitskontrolle pro Port

Scheduling
Strikte Priorität und gewichteter Round-Robin (WRR): Weighted Round Robin ist ein Planungsalgorithmus, der die den Warteschlangen zugewiesenen Gewichte verwendet, um zu bestimmen, wie viele Daten aus einer Warteschlange geleert werden, bevor sie in die nächste Warteschlange verschoben werden.

Security

Zertifizierte Authentifizierung
Es kann ein privater HTTPS-Schlüssel für den Managementzugang hinterlegt werden.

Benutzerverwaltung
Die Rechte der Benutzer können in bis zu 15 Ebenen frei eingestellt werden.

ACL
Der Switch erlaubt bis zu 512 Einträge. Drop- oder Ratenbeschränkung basierend auf Quell-/Ziel-MAC-/IP-Adresse oder VLAN-ID. Pro Port können Regeln und Bedingungen für eingehende Pakete festgelegt werden. Die Regeln umfassen Protokolle, IP-Ports und Adressbereiche. Die Regeln können wahlweise nach dem Berechtigungs- oder dem Ausschlussverfahren festgelegt werden. Kriterien sind: TCP/ UDP Quell- und Ziel-Ports, 802.1p-Priorität, Ethernet-Typ, ICMP-Paket (Internet Control Message Protocol).

Port Sicherheit
MAC-Adressenverwaltung pro Port und IP-Source-Guard**:** Die MAC-Adresse kann in Kombination mit der IP-Adresse geprüft werden.

Storm Control
Verhindert, dass der Verkehr in einem LAN durch eine Broadcast-, Multicast- oder Unicast-Flut auf einem Port gestört wird.

RADIUS Authentication, 802.1X
Autorisierung und Abrechnung, MD5-Hash, Gast-VLAN, Einzel-/Mehrfach-Host-Modus und Einzel-/Mehrfachsitzungen
Unterstützt IGMP-RADIUS-basiertes 802.1X
Dynamische VLAN-Zuweisung

TACACS+ Authentifizierung
Der Switch unterstützt die TACACS+-Authentifizierung. Switch als Client.

Secure Shell (SSH)
SSH sichert den Telnet-Verkehr in oder aus dem Switch, SSH v1 und v2 werden unterstützt

	Secure Socket Layer (SSL) SSL verschlüsselt den HTTP-Verkehr und ermöglicht so einen erweiterten sicheren Zugriff auf die browserbasierte Management-GUI im Switch. **HTTPS & SSL (Secured Web)** Hyper Text Transfer Protocol Secure (HTTPS) ist die sichere Version von HTTP. **BPDU Guard** Der BPDU Wächter, eine Erweiterung von STP, entfernt einen Knoten, der BPDUs zurück ins Netzwerk reflektiert. Er setzt die Grenzen der STP Domäne durch und hält die aktive Topologie vorhersehbar, indem er keine Netzwerkgeräte hinter einem BPDU Guard-fähigen Port an STP teilnehmen lässt. **DHCP Snooping** Mit DHCP Snooping besitzt der Switch eine Funktion, die als Firewall zwischen nicht vertrauenswürdigen Hosts und vertrauenswürdigen DHCP Servern fungiert. **Loop Protection** Mit der Loop Protection werden unbekannte Unicast-, Broadcast- und Multicastschleifen in Layer-2-Switching-Konfigurationen verhindert.
Multicast	**IGMP v1/v2/v3 Snooping** IGMP beschränkt den bandbreitenintensiven Multicast Verkehr auf die Antragsteller. Unterstützt 1024 Multicast Gruppen. **IGMP Querier** IGMP Querier wird zur Unterstützung einer Layer-2-Multicast-Domäne von Snooping Switches verwendet, wenn kein Multicast Router vorhanden ist. **IGMP Proxy** IGMP Snooping mit Proxy-Berichterstellung oder Berichtsunterdrückung filtert IGMP-Pakete aktiv, um die Last auf dem Multicast Router zu reduzieren. **MLD v1/v2 Snooping** Liefert IPv6-Multicast-Pakete nur an die erforderlichen Empfänger. **Multicast VLAN Registrierung (MVR)** Ein dediziertes, manuell konfiguriertes VLAN, das so genannte Multicast VLAN, um Multicast Verkehr über ein Layer-2-Netzwerk in Verbindung mit IGMP Snooping weiterzuleiten.
Topologie	Standard Spanning Tree (STP), IEEE802.1d Rapid Spanning Tree (RSTP), IEEE802.w Multiple Spanning Tree (MSTP), IEEE802.1s Ethernet Linear Protection Switching (ELPS), ITU-T G.8031 Ethernet Ring Protection Switching, (ERPS), ITU-T G.8032