

RUGGEDCOM RS8000A hardened, fully managed, Ethernet switches; 2 x 10/100BaseTX + 2 x 10BaseFL + 4 x 100BaseFX; 128-bit encryption;



Figure similar

<b>product type designation</b>	<b>RUGGEDCOM RS8000A</b>
<b>transfer rate</b>	
transfer rate	10 Mbit/s, 100 Mbit/s
number of ports / maximum	8
<b>interfaces / other</b>	
number of electrical connections	
• for operator console	1
• for management purposes	0
type of electrical connection	
• for operator console	RS232
• for signaling contact	3-pole terminal block, screwable
• for power supply	5-pole screw contact
<b>signal inputs/outputs</b>	
relay design	Form-C contact relay (SPDT)
type of relay output	Changeover contact (CO)
operational current / of the signaling contacts	
• at DC / at 30 V / maximum	1 A
<b>supply voltage, current consumption, power loss</b>	
product options / wide range power supply	Yes
<b>type of voltage / 1 / of the supply voltage</b>	DC
• supply voltage / 1 / rated value	24 V
• power loss [W] / 1 / rated value	15 W
• supply voltage / 1 / rated value	10 ... 36 V
<b>type of voltage / 2 / of the supply voltage</b>	DC
• supply voltage / 2 / rated value	48 V
• supply voltage / 2 / rated value	36 ... 59 V
<b>type of voltage / 3 / of the supply voltage</b>	DC
• supply voltage / 3 / rated value	88 ... 300 V
<b>type of voltage / 4 / of the supply voltage</b>	AC
• supply voltage / 4 / rated value	85 ... 265 V
<b>ambient conditions</b>	
ambient temperature	
• during operation	-40 ... +85 °C
• note	A maximum operating temperature of +85 °C is permissible for a duration of 16 hours
operating condition / fanless operation	Yes
protection class IP	IP3X
<b>design, dimensions and weights</b>	
design	compact

width	200.3 mm
height	61.8 mm
depth	248.92 mm
net weight	2.25 kg
product feature / conformal coating	optional
material / of the enclosure	18 AWG galvanized steel enclosure
fastening method	
• 19-inch installation	No
• 35 mm top hat DIN rail mounting	Yes
• wall mounting	Yes
<b>product features, product functions, product components / general</b>	
number of automatically learnable MAC addresses	8192
storage capacity	
• of message buffer / maximum	256 kbyte
switch latency period	4 µs
transfer rate / of the switch	1.6 Gbit/s
number of priority channels	2
product feature	
• Store & Forward switching method	Yes
• Zero-Packet-Loss technology	Yes; Zero-Packet-Loss applies to fiber optic interfaces
<b>product functions / management, configuration, engineering</b>	
product function	
• CLI	Yes
• web-based management	Yes
• MIB support	Yes
• RMON	Yes
product function / switch-managed	Yes
protocol / is supported	
• Telnet	Yes
• HTTP	Yes
• HTTPS	Yes
• TFTP	Yes
• SFTP	Yes
• SNMP v1	Yes
• SNMP v2	No
• SNMP v2c	Yes
• SNMP v3	Yes
• IGMP (snooping/querier)	Yes
number of groups / at IGMP	256
product function	
• for MIB support / by BRIDGE-MIB	RFC4188
• for MIB support / by IF-MIB	RFC2863
• for MIB support / by RMON-MIB	RFC2819
• for MIB support / by RSTP-MIB	RFC4318
• for MIB support / by SNMPv2-MIB	RFC1907
• for MIB support / by SNMPv2-SMI	RFC2578
• for MIB support / by SNMPv2-TC	RFC2579
• for MIB support / by TCP-MIB	RFC2012
• for MIB support / by UDP-MIB	RFC2013
<b>product functions / VLAN</b>	
product function	
• VLAN - port based	Yes
number of VLANs / maximum	64
VLAN identification number	1 ... 1000
protocol / is supported / GVRP	Yes
<b>product functions / DHCP</b>	
product function	
• DHCP client	Yes
• DHCP Option 82	Yes
• DHCP Option 66	No

<ul style="list-style-type: none"> <li>• DHCP Option 67</li> </ul>	No
<b>product functions / routing</b>	
protocol / is supported <ul style="list-style-type: none"> <li>• PPP</li> </ul>	Yes
<b>product functions / redundancy</b>	
product function <ul style="list-style-type: none"> <li>• redundancy procedure STP</li> <li>• redundancy procedure RSTP</li> <li>• redundancy procedure MSTP</li> <li>• eRSTP</li> </ul>	Yes Yes Yes Yes
protocol / is supported <ul style="list-style-type: none"> <li>• STP</li> <li>• RSTP</li> <li>• MSTP</li> </ul>	Yes Yes Yes
<b>product functions / security</b>	
product function <ul style="list-style-type: none"> <li>• IEEE 802.1x (radius)</li> <li>• RADIUS client</li> </ul>	No Yes
protocol / is supported <ul style="list-style-type: none"> <li>• RADIUS</li> <li>• TACACS+</li> <li>• SSL</li> </ul>	Yes Yes Yes
key length <ul style="list-style-type: none"> <li>• with SSL</li> <li>• with RSA</li> </ul>	128 bit 1024 bit
product function / port-rate-limiting	Yes
<b>product functions / time</b>	
product function <ul style="list-style-type: none"> <li>• SNTP client</li> <li>• SNTP server</li> </ul>	Yes Yes
protocol / is supported <ul style="list-style-type: none"> <li>• SNTP</li> </ul>	Yes
<b>standards, specifications, approvals</b>	
standard <ul style="list-style-type: none"> <li>• for safety / from CSA and UL</li> </ul>	cCSAus (Compliant with CSA C22.2 No. 60950, UL60950, EN60950)
reference code <ul style="list-style-type: none"> <li>• according to IEC 81346-2</li> <li>• according to IEC 81346-2:2019</li> </ul>	KF KFE
<b>standards, specifications, approvals / CE</b>	
certificate of suitability / CE marking	Yes
standard <ul style="list-style-type: none"> <li>• for EMC</li> </ul>	FCC Part 15 (Class A), EN55022 (CISPR22 Class A)
<b>standards, specifications, approvals / other</b>	
laser protection class	Complies with 21 CFR chapter 1, subchapter J
certificate of suitability <ul style="list-style-type: none"> <li>• IEC 61850-3</li> </ul>	Yes
<b>standards, specifications, approvals / product conformity</b>	
product conformity <ul style="list-style-type: none"> <li>• according to IEEE 802.3-10BaseT</li> <li>• according to IEEE 802.3u-100BaseTX</li> <li>• according to IEEE 802.3u-100BaseFX</li> <li>• according to IEEE 802.3x-Flow Control</li> <li>• according to IEEE 802.1d-MAC Bridges</li> <li>• according to IEEE 802.1d-STP</li> <li>• according to IEEE 802.1p-class of service</li> <li>• according to IEEE 802.1Q-VLAN tagging</li> <li>• according to IEEE 802.1w-RRST</li> <li>• according to IEEE 802.1x-port based Network Access Control</li> <li>• RFC768-UDP</li> </ul>	Yes Yes Yes Yes Yes Yes Yes Yes Yes Yes Yes Yes

- RFC783-TFTP
- RFC791-IP
- RFC792-ICMP
- RFC793-TCP
- RFC826-ARP
- RFC854-Telnet
- RFC894-IP over Ethernet
- RFC1112-IGMPv1
- RFC1519-CIDR
- RFC1541-DHCP (client)
- RFC2030-SNTP
- RFC2068-HTTP
- RFC2236-IGMPv2

Yes  
Yes  
Yes  
Yes  
Yes  
Yes  
Yes  
Yes  
Yes  
Yes  
Yes  
Yes  
Yes

#### further information / internet links

##### internet link

- to website: Selection guide for cables and connectors
- to website: Industry Mall/RUGGEDCOM selector
- to website: Industrial communication
- to website: Siemens RUGGEDCOM
- to website: Image database
- to website: CAX-Download-Manager
- to website: Industry Online Support

<https://support.industry.siemens.com/cs/ww/de/view/109766373>  
<https://www.siemens.com/ruggedcom-selector>  
<https://www.siemens.com/simatic-net>  
<https://www.siemens.com/ruggedcom>  
<https://www.automation.siemens.com/bilddb>  
<https://www.siemens.com/cax>  
<https://support.industry.siemens.com>

#### security information

##### security information

Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks. In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place. For additional information on industrial cybersecurity measures that may be implemented, please visit [www.siemens.com/cybersecurity-industry](http://www.siemens.com/cybersecurity-industry). Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats. To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under <https://www.siemens.com/cert>. (V4.7)

#### Approvals / Certificates

##### General Product Approval



[Manufacturer Declaration](#)



EG-Konf.



CB

[inspection certificate](#)

##### Dangerous Good

##### Environment

[Dangerous Goods Information](#)



last modified:

3/26/2024