Firmware-Features

Micro Switch/Desktop Switch Generation 6

1	**IP Stack**	
1	Dual Stack	Parallel handling of IPv4 and IPv6 protocol.
2	IPv4 Stack	Internet Protocol v4 handling with support of IPv4, ARP, DHCP, ICMP.
3	IPv4 Standard	RFC 791 (IPv4), RFC 826 (ARP), RFC 792 (ICMP), RFC 2131 (DHCP)
4	IPv6 Stack	Internet Protocol v6 handling with support of IPv6, DHCPv6, ICMPv6, NDP.
5	IPv6 Standard	RFC 2460/2464/3484/3513 (IPv6), RFC 2462 (Address Configuration), RFC 2463 (ICMPv6), RFC 2461 (Neighbor Discovery Protocol), RFC 3315 (DHCPv6)
2	**Port Control**	
1	Administration	Port disable, Individual port alias
2	Ethernet TP	Auto-Negotiation, speed, duplex mode, flow-control, Auto MDI/MDI-X
3	Ethernet Fiber / SFP	Speed, duplex mode, flow-control
4	Green IT	Latest chip technology supports Energy Efficient Ethernet (EEE) according to IEEE Std. 802.3az.
3	**Power-over-Ethernet (PoE)**	
1	Function	Sourcing of power to connected devices via standard network Twisted-Pair cable
2	802.3at mode	PoE+ voltage is turned on only after powered device (PD) is detected and classified on port. Output voltage and power is monitored. Port power is shut down if limits are exceeded.
3	802.3af mode	PoE voltage is turned on only after powered device (PD) is detected and classified on port. Output voltage and power is monitored. Port power is shut down if limits are exceeded.
4	Power Management	Power limit can be defined per port and per total device. Additionally the class of the powered device (PD) can be limited per port.
5	Standards	IEEE Std. 802.3af (Data Terminal Equipment Power via Media Dependent Interface), IEEE Std. 802.3at (Data Terminal Equipment Power via Media Dependent Interface).
4	**Switch Functions**	
1	Port Monitor	Monitor port for the connection of a network protocol analyser. Traffic of the port to be analysed is copied to the monitor port.
2	RMON counters	17 integrated counters for detailed traffic analysis and network trouble shooting.
3	MAC Table	Access to table of MAC addresses learned by the switch. Can be filtered per port, VLAN address type and entry type (dynamic/static).
5	**Virtual LANs (VLANs)**	
1	Function	Logical structuring of physical networks by adding a Virtual LAN ID (VID) to each Ethernet packet. Incoming packets are filtered and forwarded according to their VID. Each port can be configured for Access, Hybrid or Trunk VLAN processing mode. 256 independent VLANs out of the full range of 1 to 4095 can be filtered per device.
2	Access Mode	For the connection of non-VLAN capable end devices (e.g. PCs). Outgoing packets are send untagged. Incoming packets are tagged with the port default VLAN ID (PVID).
3	Trunk Mode	For the interconnection of VLAN capable switches. Outgoing packets are always send tagged. Incoming packets are received tagged. Incoming packets without VLAN tag are tagged with the port default VLAN ID (PVID).
4	Hybrid Mode	For the connection of VLAN capable and non-VLAN capable devices on the same port (e.g. VoIP-phone (tagged) and PC (untagged)). Outgoing packets are send tagged, except packets for the port default VLAN ID (PVID), which are untagged. Incoming packets are received untagged for the port default VLAN (PVID), all other packets are tagged.
5	Priority Override	VLAN priority code point of incoming packets can be overwritten with the VLAN specific priority defined in the VLAN filter.
6	Voice VLAN	VLAN ID used by LLDP/CDP to assign VLAN to connected VoIP-phone.
7	RSTP VLAN	VLAN ID used by Spanning Tree instance for BPDU tagging.
8	Unauthorized VLAN	VLAN ID assigned by Port Based Access Control to unauthorized ports (guest VLAN).
9	Management VLAN	VLAN ID used by the management agent (device internal port).
10	Standard	IEEE Std. 802.1D, IEEE Std. 802.1Q, IEEE Std. 802.1p

6	**Quality of Service (QoS)**	
1	Priority Queues	4 priority queues per port.
2	Prioritization Scheme	Strict priority (higher priority always first) or weighted fair queuing (8:4:2:1 highest to lowest).
3	Layer1 Priority	Static priority queue can be assigned for each port.
4	Layer2 Priority	Incoming packets are forwarded according to the priority code point in their VLAN tag. The 8 VLAN priority code points can be individually mapped on the 4 priority queues.
5	Layer3 Priority	Incoming packets are forwarded according to the value of the DiffServ Codepoint (IPv4) / TrafficClass (IPv6) in the their IP header. Maximum 64 codepoints are supported. For each code point the corresponding priority queue can be mapped.
6	Traffic shaping	5 ingress rate shaping buckets per port. Supports rate and priority based rate shaping
7	Standard	IEEE Std. 802.1p (VLAN priority code point), RFC 2474/3260 (IPv4 DiffServ/IPv6 Traffic Class)
7	**Spanning Tree Protocol**	
1	Rapid Spanning Tree (RSTP)	Automatic detection of loops and redundant network paths. Single STP instance running in configurable VLAN. Rapid Spanning Tree Protocol (RSTP) backwards compatible to Spanning Tree standard (STP).
2	MSTP	Seperate STP instances running in configurable VLAN groups.
3	Standard	IEEE Std. 802.1D-2004
4	PVST	RSTP per VLAN for one VLAN
8	**Multicast Forwarding**	
1	IGMP Snooping	Snooping of Internet Group Management Protocol (IGMPv1/v2/v3) for IPv4. Automatic detection and forwarding of IPv4 multicast-streams. Unregistered packets can be flooded or blocked. Multicast routers can be detected by discovery or by query message.
2	MLD Snooping	Snooping of Multicast Listener Discovery (MLDv1/v2) for IPv6. Automatic detection and forwarding of IPv6 multicast-streams. Multicast routers can be detected by discovery or by query message.
3	Standard	RFC 4541 (IGMP), RFC 3810/4604 (MLD)
9	**Real Time Clock (RTC)**	
1	Function	Internal device clock can be syncronized with external NTP server.
2	Protocol	Network Time Protocol (NTP)
3	Standard	RFC 4330 (NTP)
10	**Link Layer Discovery Protocol (LLDP)**	
1	Function	Advertising identity, capabilities, and neighbors on a connected network segment.
2	LLDP-MED	Media Endpoint Discovery for the auto-discovery of LAN policies.
3	Standard	IEEE Std. 802.1AB (LLDP), ANSI/TIA-1057 (LLDP-MED)
11	**Cisco Discovery Protocol (CDP)**	
1	Function	CDP v1, v2 for automatic detection of capabilites of neighbor CDP enabled devices.
2	Voice VLAN	Support of Voice VLAN for configuration of connected Cisco VoIP-phone.
12	**Port Access Control**	
1	Function	Port-Based Network Access Control with dynamic port VLAN support and fallback to MAC based authentication methods. Network access is controlled at the port level. Supports IEEE Std. 802.1X Authentication, RADIUS MAC Authentication, MAC Locking and forced authorized/unauthorized mode.
2	Communication	EAPOL, RADIUS
3	Authentication Protocols	EAP-MD5, EAP-PEAP (inner protocol: MSCHAPv2), EAP-TLS, EAP-TTLS (inner protocols: EAP-MD5, EAP-TLS, PAP)
4	IEEE 802.1X Authentication	Multiple users can be authenticated using central RADIUS server based on username/password or certificate.
5	RADIUS MAC Authentication	Multiple users can be authenticated using central RADIUS server based on their MAC addresses.
6	MAC locking	Multiple users can be authenticated based on their MAC addresses. Authorized MAC addresses are stored permanently in the device. They can be configured manually or automatically by locking the first MAC addresses learned on the port.
7	Dynamic VLAN	RADIUS server can provide user specific VLAN ID using tunnel-attribute in accept message. Port VLAN is dynamically set accordingly. Unauthorized users may be placed in an unauthorized VLAN ('guest VLAN') or blocked completely.
8	IP Address Detection	The IP address of the connected user is detected via ARP snooping. User IP address information can be logged using RADIUS accounting function.
9	Standard	IEEE 802.1X-2004 (Port-Based Network Access Control).

13	**Login**	
1	Function	Implements user based and view based authentication and scope limiting. Supports unlimited number of user/groups and views (limited by system memory constrains only). Offers ultimate flexibility with precise access control.
14	**Command Line Interface (CLI)**	
1	Function	Intuitive command-set with auto-complete and redo-buffer. Individual console prompt string, Console inactivity timeout. Supports full scripting and editing of script files. Supports color displays. Permits offline configuration as well as management of an unlimited number of user configuration sets (limited by system memory constrains only). IPv6 access supported
2	Telnet	Telnet via TCP/IP port 23.
3	Secure Shell (SSH)	SSH via TCP/IP port 22. Authentication methods RSA, Diffie-Hellman Key Exchange. Encryption protocols 3DES-CBC, HMAC-SHA1.
15	**Web Manager**	
1	Function	Integrated Web Manager with graphical user interface (GUI) for complete device configuration and administration using standard web browser. IPv6 access supported
2	Protocol	HTML v4.01,HTTP, HTTPS, Java Script
3	Browser compatibility	Firefox 4.x, IE 8.x, Javascript support required.
16	**Simple Network Management Protocol (SNMP)**	
1	SNMPv1/v2c	Simple Network Management Protocol v1, v2c (SNMPv1, v2c) to access device information stored in Management Information Base (MIB). Security provided by community strings for Set/Get commands and optionally by G6 login scheme.
2	Traps (SNMPv1/v2c)	Traps, Notifications sent to unlimited number of independently configurable receiver destinations (limited by system memory constrains only). Sending of message is triggered by internal device status change events. Event triggers can be configured individually per destination. Test function to trigger Trap/Notification for simplified configuration check (Web Manager and CLI only).
3	SNMPv3	Simple Network Management Protocol v3 (SNMPv3) for secure access to device information stored in Management Information Base (MIB). SNMPv3 supports data encryption, User-based Security Model (USM) and View-based Access Control Model (VACM).
4	Traps (SNMPv3)	Trap/Notification, InformRequest, Response sent to independently configurable receivers. Sending of message is triggered by internal device status change events. Informs provide secured messaging by requiring response message Event triggers can be configured individually per receiver.
5	MIBs	MIB-2, Enterprise-MIB (MICROSENS G6 MIB). File can be downloaded from the integrated Web Manager.
6	Standard	RFC 1155/1156/1157 (SNMPv1), RFC 1901/1905/1906 (SNMPv2), RFC 3411/3412/3584 (SNMPv3), RFC 2574/3414 (USM), RFC 2575/3415 (VACM)
17	**RADIUS Client**	
1	Function	RADIUS client via UDP/IP ports 1812 (access), 1813 (accounting) for Remote Authentication Dial In User Service (RADIUS) server for authorizing user access and logging of user accounting information.
2	Redundancy	In case of a response timeout, the next RADIUS server is requested.
3	Standard	RFC 2865 (RADIUS), RFC 2866 (Accounting), RFC 2868 (Tunnel Attributes)
18	**Files**	
1	Configuration	File transfers may be used to upgrade the software or to load configuration files. The unit supports TFTP, FTP, SFTP, HTTP, HTTPS transfer protocols. Additionally files may be loaded via DHCP directives (options 60/66/67).
2	Firmware Update	Software download can be complete or incremental. Individual modules may be upgraded, normally without influencing service. Flexible system permits customized upgrade files if required.
19	**Syslog Client**	
1	Function	Syslog messages are triggered by system events and can be send to unlimited number of Syslog servers (limited by system memory constrains only).
2	Standard	RFC 5424
20	**Event Manager**	
1	Function	Mapping of device status changes (Triggers) to actions e.g. sending out SNMP trap, Syslog message etc.
2	Customizable events	Event severeness and alert level freely configurable. Event text strings may be customized via user interface with developer rights.
3	Traps and Syslog	Unlimited number of trap and/or Syslog receivers. Event may be filtered individually on a group level.