

Angora Networks

Verge Enterprise Ethernet Switches

VERGE ethernet switch family, provides next generation solutions you need to support your business requirements on different technologies that request robust products with high capacity and extensive security. Verge includes features, that makes it possible to protect your sensitive data and use the bandwidth that your applications requested, more effectively by maximizing your business critical applications availability.
With 8, 24 or 48 high density Gigabit Ethernet interface and 4 SFP+ uplinks, it provides top class solutions on your continuously expanding work environment with unified access technologies support. VERGE switches are ideal combination of ease of installation and use, support options and features that meets your business requirements and provides a better edge to edge connected workspace.

Enterprise Applications

Whether you need to build an high speed network to connect your users to centralized services, or aggregate your traffic, or a complete solution to deliver voice, video and data, VERGE provides different options for all your needs:

Aggregation: With its 4x10 Gigabit interface, you can connect your edge devices, to your network backbone in a redundant way and provide robust and high speed network access to all your endpoints.

Secure Connectivity: VERGE allows all your users to access easily and securely to your resources. High performance and secure and reliable connectivity help high speed processing and file transfer, and also improve network uptime , that keeps your business flows uninterrupted.

Unified Communications: VERGE, with different management options, provides advanced traffic management intelligence and high performance , and also helps you deliver different communications traffic over a single network. Specific requirements for voice, video and data can be met with different specifications over a single device.

High Security Guest Access: VERGE helps you share your network with your guests or other devices outside your enterprise, on your public places such as waiting rooms, hotels or even inside your office, by applying highly secure authentication methods. Powerful yet easy to configure security and traffic segmentation features, not only helps you isolate your private network from guests, it also protect your guests sessions from each other.

Highest Level of Security

VERGE, prevents unauthorized access while protecting your information with its rich security feature set
• Limits and blocks access to specific segments in your network, with its advanced network security features, such as IEEE 802.1x port security. Web based authentication support, allows easier access, by using a simple and useful interface instead of using 802.1x for all types of client endpoints.
• Detects and blocks directed attacks via Dynamic ARP Inspection, IP Source Guard and DHCP Snooping with its advanced protection methods.
• Comprehensive security features such as, RA Guard, ND Inspection, DHCP6 Protection, Neighbor Binding Integrity Check and IPv6 first hop security provides protection against address spoofing and man-in-the-middle attacks on IPv6 networks.
• Embedded SSL encryption, allows switch management traffic transferred with highest security.
• Extensive Access Control Lists (ACL), limit unauthorized users access and provide basic security against network attacks.
• Time based ACL and port security allows you to limit network access by predefined time intervals such as business hours.
• Guest VLANs, while providing internet and network access to your visitors and guests, it also isolates your corporate traffic.
• Automatic single mac address based security can be applied, while your users roam from one wi-fi access point to other.
• Layer 2 isolation within the same VLAN can be implemented with private VLAN support.
• Broadcast, multicast and unknown unicast storm controls are supported
• Management sessions can be authenticated via RADIUS, TACACS+ and local database.

Ease of Deployment and Operation

VERGE family is designed for easy installation and operation for enterprise customers and service providers.

• Easy to use graphical user interface, minimize the time required to install, manage and troubleshoot your network and allows different features to be configured very quickly without any new IT head count.
• Command Line Interface (CLI), you can use to configure and monitor all features.
• With port intelligence, VERGE switches can automatically detects the connected devices, and applies related security, QoS and availability options.
• Remote configuration and management services are provided by Simple Network Management Protocol (SNMP), and improve your workflows and also allows multiple device configurations.
• VERGE switches can be integrated with management systems and automation and orchestration solutions via REST API* support.

IPv6 Support

As the current IP address scheme is evolving to support growing number of connected devices, VERGE support your migration to next generation IPv6 deployments. While allowing support for current IPv4 networks, VERGE helps you run a dual stack network, and change your infrastructure on your own pace without affecting your day to day business flows.

Basic Layer 3 Features

VERGE allows your network to be segmented, by initially supporting static Layer 3 routing for inter-vlan packet forwarding without any drop on performance.

Energy Efficiency

VERGE integrates a variety of power saving features on all models, providing most energy-efficient switching portfolio. VERGE switches are designed to save energy by optimizing power usage, which helps protecting our environment and minimize costs, providing eco-friendly operation without any performance loss.
• Supports Energy Efficient Ethernet IEEE 802.3az standard, which helps reducing power consumption by changing the port status to sleep state during quite periods, after analyzing the traffic passing from this port.
• Latest application specific integrated circuits, using 65/40 nanometer technology, and low power/high performance ARM based CPU, minimize energy requirements
• Automatic power cut option provided on down link state.
• Leds can be turned off to save power.
• Embedded intelligence adjusts signal levels based on cable length.

© 2020 Angora Networks. All rights reserved. Angora Networks and the Angora Networks logo are trademarks of Angora Networks in Turkey. All other trademarks are the trademarks of their respective owners. Angora Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Feature	Description		
Performance			
RAM	512MB		
Flash	128MB		
Switching capacity and forwarding rate All switches are wire speed and nonblocking	Model Name	Capacity in Millions of packets per second (mpps)	Switching Capacity in gigabits per second (Gbps)
	ANW-2023-24G	71.3	128
	ANW-2023-48G	104.16	176
	ANW-2023-32G	88.1	144
	ANW-2023-8G	38.1	56
Layer 2 Switching			
Spanning Tree Protocol	Standard 802.1d Spanning Tree support.		
	Fast convergence using 802.1w (Rapid Spanning Tree RSTP), enabled by default 8 instances are supported.		
	Multiple Spanning Tree instances using 802.1s (MSTP).		
Port Grouping	Support for IEEE 802.3ad Link Aggregation Control Protocol (LACP).		
	Up to 8 groups.		
	Up to 8 ports per group with 32 candidate ports for each (dynamic) 802.3ad link aggregation.		
VLAN	Support for up to 4096 VLANs simultaneously port-based and 802.1Q tag-based VLANs MAC-based VLAN Management VLAN. 1000 active VLANs.		
	Private VLAN, also known as protected ports, with multiple uplinks Guest VLAN Unauthenticated VLAN.		
	Dynamic VLAN assignment via RADIUS server along with 802.1x client authentication.		
Voice VLAN	Voice traffic is automatically assigned to a voice-specific VLAN and treated with appropriate levels of QoS.		
	Auto voice* capabilities deliver networkwide zero-touch deployment of voice endpoints and call control devices.		
Multicast TV VLAN	Multicast TV VLAN allows the single multicast VLAN to be shared in the network while subscribers remain in separate VLANs (also known as MVR).		
Q-in-Q VLAN	VLANs transparently cross a service provider network while isolating traffic among customers.		
Generic VLAN Registration Protocol (GVRP)/ Generic Attribute Registration Protocol (GARP)	Protocols for automatically propagating and configuring VLANs in a bridged domain.		

Unidirectional Link Detection (UDLD)	UDLD monitors physical connection to detect unidirectional links caused by incorrect wiring or cable/port faults to prevent forwarding loops and blackholing of traffic in switched networks.
Dynamic Host Configuration Protocol (DHCP) Relay at Layer 2	Relay of DHCP traffic to DHCP server in different VLAN; works with DHCP Option 82.
Internet Group Management Protocol (IGMP) versions 1, 2, and 3 snooping	IGMP limits bandwidth-intensive multicast traffic to only the requesters; supports 1K multicast groups (source-specific multicasting is also supported).
IGMP Querier	IGMP querier is used to support a Layer 2 multicast domain of snooping switches in the absence of a multicast router.
Head-of-line (HOL) Blocking	HOL blocking prevention.
Jumbo Frames	Up to 9K (9216) bytes.
Layer 3	
IPv4 Routing	Wirespeed routing of IPv4 packets. Inter-VLAN routing. 16000 IPv4 route* RIP, RIPng, OSPF, OSPFv3*
Classless Interdomain Routing (CIDR)	Support for CIDR.
Layer 3 Interface	Configuration of Layer 3 interface on physical port, LAG, VLAN interface, or loopback interface.
DHCP Relay at Layer 3	Relay of DHCP traffic across IP domains.
User Datagram Protocol (UDP) Relay	Relay of broadcast information across Layer 3 domains for application discovery or relaying of bootP/DHCP packets.
DHCP Server	Switch functions as an IPv4 DHCP server serving IP addresses for multiple DHCP pools/scopes.
	Support for DHCP options.
Security	
Secure Shell (SSH) Protocol	SSH is the secure replacement for Telnet traffic. SCP also uses SSH. SSH v1 and v2 are supported.
Secure Sockets Layer (SSL)	SSL support: Encrypts all HTTPS traffic, allowing highly secure access to the browser based management GUI on the switch.
IEEE 802.1X (Authenticator Role)	802.1X: RADIUS authentication and accounting, MD5 hash; guest VLAN; unauthenticated VLAN, single/multiple host mode and single/multiple sessions Supports time-based 802.1X.
	Dynamic VLAN assignment.
Web-Based Authentication	Web based authentication provides network admission control through web browser to any host devices and operating systems.
STP Bridge Protocol Data Unit (BPDU) Guard	Security mechanism to protect the network from invalid configurations. Port enabled for BPDU Guard is shut down if a BPDU message is received on that port.

STP Root Guard	This prevents edge devices thst are not in the network administrator's control, from becoming Spanning Tree Protocol root nodes.
DHCP Snooping	Filters out DHCP messages with unregistered IP addresses and/or from unexpected or untrusted interfaces. This prevents rogue devices from behaving as DHCP Servers.
IP Source Guard (IPSG)	When IP Source Guard is enabled on a port, the switch filters out IP packets received from the port if the source IP addresses of the packets have not been statically configured or dynamically learned from DHCP snooping. This prevents IP Address Spoofing.
Dynamic ARP Inspection (DAI)	The switch discards ARP packets from a port if there is no static or dynamic IP/MAC bindings or if there is a discrepancy between the source or destination addresses in the ARP packet. This prevents man-in-the-middle attacks.
IP/MAC/Port Binding (IPMB)	The preceding features (DHCP Snooping, IP Source Guard, and Dynamic ARP Inspection) work together to prevent DOS attacks in the network, thereby increasing network availability.
Secure Core Technology (SCT)	Makes sure that the switch will receive and process management and protocol traffic no matter how much traffic is received.
Secure Sensitive Data (SSD)	A mechanism to manage sensitive data (such as passwords, keys, and so on) securely on the switch, populating this data to other devices, and secure autoconfig. Access to view the sensitive data as plaintext or encrypted is provided according to the user configured access level and the access method of the user.
Layer 2 isolation Private VLAN Edge (PVE) with community VLAN	PVE (also known as protected ports) provides Layer 2 isolation between devices in the same VLAN, supports multiple uplinks.
Port Security	The ability to lock source MAC addresses to ports and limits the number of learned MAC addresses.
RADIUS/TACACS+	Supports RADIUS and TACACS authentication.
Storm Control	Broadcast, multicast, and unknown unicast.
RADIUS Accounting	The RADIUS accounting functions allow data to be sent at the start and end of services, indicating the amount of resources (such as time, packets, bytes, and so on) used during the session.
DoS Prevention	Denial-of-service (DOS) attack prevention.
ACLs	Support for up to 512 rules.
	Drop or rate limit based on source and destination MAC, VLAN ID or IP address, protocol, port, differentiated services code point (DSCP)/IP precedence, TCP/UDP source and destination ports, 802.1p priority, Ethernet type, Internet Control Message Protocol (ICMP) packets, IGMP packets, TCP flag, time-based ACLs supported.
Quality of Service	
Priority Levels	8 hardware queues.
Scheduling	Strict priority and weighted round-robin (WRR). Queue assignment based on DSCP and class of service (802.1p/CoS).
Class of Service	Port based; 802.1p VLAN priority based; IPv4/v6 IP precedence/type of service (ToS)/DSCP based; differentiated services (DiffServ); classification and remarking ACLs, trusted QoS.
Rate Limiting	Ingress policer; egress shaping and rate control; per VLAN, per port, and flow based.
Congestion Avoidance	A TCP congestion avoidance algorithm is required to minimize and prevent global TCP loss synchronization. 12 MB Buffer.
Standards	
Standards	IEEE 802.3 10BASE-T Ethernet, IEEE 802.3u 100BASE-TX Fast Ethernet, IEEE 802.3ab 1000BASE-T Gigabit Ethernet, IEEE 802.3ad LACP, IEEE 802.3z Gigabit Ethernet, IEEE 802.3x Flow Control 802.3 Auto-negotiation, MDIX, Auto-MDIX IEEE 802.ID (STP, GARP, and GVRP), IEEE 802.10/p VLAN, IEEE 802.lw RSTP, IEEE 802.1s Multiple STP, IEEE 802.IX Port Access Authentication, IEEE 802.3af, IEEE 802.3at, RFC 768, RFC 783, RFC 791, RFC 792, RFC 793, RFC 813, RFC 879, RFC 896, RFC 826, RFC 854, RFC 855.

Standards	RFC 858, RFC 894, RFC 919, RFC 922, RFC 920, RFC 950, RFC 1042, RFC 1071, RFC 1123, RFC 1141, RFC 1155, RFC 1157, RFC 1350, RFC 1533, RFC 1541, RFC 1624, RFC 1700, RFC 1867, RFC 2030, RFC 2616, RFC 2131, RFC 2132, RFC 3164, RFC 3411, RFC 3412, RFC 3413, RFC 3414, RFC 3415, RFC 2576, RFC 4330, RFC 1213, RFC 1215, RFC 1286, RFC 1442, RFC 1451, RFC 1493, RFC 1573, RFC 1643, RFC 1757, RFC 1907, RFC 2011, RFC 2012, RFC 2013, RFC 2233, RFC 2618, RFC 2665, RFC 2666, RFC 2674, RFC 2737, RFC 2819, RFC 2863, RFC 1157, RFC 1493, RFC 1215, RFC 3416	
IPv6		
IPv6	IPv6 host mode, IPv6 over Ethernet, Dual IPv6/IPv4 stack IPv6 neighbor and router discovery (ND), IPv6 stateless address autoconfiguration, Path maximum transmission unit (MTU) discovery, Duplicate address detection (DAD), ICMP version 6, IPv6 over IPv4 network with Intrasite Automatic Tunnel Addressing Protocol (ISATAP) support, USGv6 and IPv6 Gold Logo certified	
IPv6 QoS	Prioritize IPv6 packets in hardware.	
Pv6 ACL	Drop or rate limit IPv6 packets in hardware.	
IPv6 First Hop Security	RA guard. ND inspection. DHCPv6 guard. Neighbor binding table (snooping and static entries). Neighbor binding integrity check.	
Multicast Listener Discovery (MLD vl/2) Snooping	Deliver IPv6 multicast packets only to required receivers.	
IPv6 Applications	Web/SSL, Telnet server/SSH, ping, traceroute. Simple Network Time Protocol (SNTP), Trivial File Transfer Protocol (TFTP), SNMP, RADIUS, syslog, DNS client, Telnet Client, DHCP Client, DHCP Autoconfig, IPv6 DHCP Relay, TACACS.	
IPv6 RFCs Supported	RFC 4443 (which obsoletes RFC2463): ICMP version 6 RFC 4291 (which obsoletes RFC 3513): IPv6 address architecture RFC 4291: IPv6 addressing architecture, RFC 2460: IPv6 specification.	
	RFC 4861 (which obsoletes RFC 2461): neighbor discovery for IPv6.	
	RFC 4862 (which obsoletes RFC 2462): IPv6 stateless address autoconfiguration.	
	RFC 1981: path MTU discovery.	
	RFC 4007: IPv6 scoped address architecture.	
	RFC 3484: default address selection mechanism. RFC 5214 (which obsoletes RFC 4214): ISATAP tunneling. RFC 4293: MIB IPv6: textual conventions and general group. RFC 3595: textual conventions for IPv6 flow label.	
Management		
Web User Interface	Built-in switch configuration utility for easy browser-based device configuration (HTTP/HTTPS). Supports configuration, system dashboard, system maintenance, and monitoring.	
SNMP	SNMP versions 1, 2c, and 3 with support for traps, and SNMP version 3 user-based security model (USM).	
Standard MIBs	draft-ietf-bridge-8021x-MIB	rfc2011-MIB
	draft-ietf-bridge-rstpmib-04-MIB	draft-ietf-entmib-sensor-MIB
	draft-ietf-hubmib-etherif-MIB-v3-00-MIB	lldp-MIB
	draft-ietf-syslog-device-MIB	lldpextdotl-MIB
	ianaaddrfamnumbers-MIB	lldpextdot3-MIB
	ianaifty-MIB	lldpextmed-MIB
	ianaprot-MIB	p-bridge-MIB
	inet-address-MIB	q-bridge-MIB
	ip-forward-MIB	rfcl389-MIB

Standard MIBs	ip-MIB	rfcl493-MIB
	RFC1155-SMI	rfcl611-MIB
	RFC1213-MIB	rfcl612-MIB
	SNMPv2-MIB	rfcl850-MIB
	SNMPv2-SMI	rfcl907-MIB
	SNMPv2-TM	rfc2571-MIB
	RMON-MIB.my	rfc2572-MIB
	dcb-raj-DCBX-MIB-1108-MIB	rfc2574-MIB
	rfcl724-MIB	rfc2576-MIB
	RFC-1212.my_for_MG-Soft	rfc2613-MIB
	rfcl213-MIB	rfc2665-MIB
	rfcl757-MIB RFC-	rfc2668-MIB
	1215.my SNMPv2-	rfc2737-MIB
	CONF.my	rfc2925-MIB
	SNMPv2-TC.my	rfc3621-MIB
	rfc2674-MIB	rfc4668-MIB
	rfc2575-MIB	rfc4670-MIB
	rfc2573-MIB	trunk-MIB
	rfc2233-MIB	tunnel-MIB
	rfc2013-MIB	udp-MIB
	rfc2012-MIB	
Remote Monitoring (RMON)	Embedded RMON software agent supports 4 RMON groups (history, statistics, alarms, and events) for enhanced traffic management, monitoring, and analysis.	
IPv4 and IPv6 Dual Stack	Coexistence of both protocol stacks to ease migration.	
Firmware Upgrade	Web browser upgrade (HTTP/HTTPS), TFTP upgrade and upgrade over SCP running over SSH.	
	Upgrade can be initiated through console port as well.	
	Dual images for resilient firmware upgrades.	
Port Mirroring	Traffic on a port can be mirrored to another port for analysis with a network analyzer. Up to 8 source ports can be mirrored to one destination port. Single session is supported. Remote port mirroring.	
VLAN Mirroring	Traffic from a VLAN can be mirrored to a port for analysis with a network analyzer or RMON probe. Up to 8 source VLANs can be mirrored to one destination port. Single session is supported.	
DHCP options (12, 66, 67, 82, 129, and 150)	DHCP options facilitate tighter control from a central point (DHCP server) to obtain IP address, autoconfiguration (with configuration file download), DHCP relay, and hostname.	
Secure Copy (SCP)	Securely transfer files to and from the switch.	
Autoconfiguration with Secure Copy (SCP) File Download	Enables secure mass deployment with protection of sensitive data.	
Text-Editable Config Files	Config files can be edited with a text editor and downloaded to another switch, facilitating easier mass deployment.	
CLI	Scriptable command-line interface. A full CLI as well as a menu-based CLI is supported. User privilege levels 1 and 15 are supported for the CLI.	
Other Management	Traceroute; single IP management; HTTP/HTTPS; SSH v2; RADIUS; port mirroring; TFTP upgrade; DHCP client; BOOTP; SNTP; Xmodem upgrade; cable diagnostics; ping; syslog; Telnet. Sflow support, RESTAPI, telemetry applications.	
Time-Based Port Operation	Link up or down based on user-defined schedule (when the port is administratively up).	
Login Banner	Configurable multiple banners for web as well as CLI.	

Power Efficiency	
IEEE Compliant (802.3az)	Supports 802.3az on all copper ports.
Energy Detect	Automatically turns power off on Gigabit Ethernet and 10/100 RJ-45 port when detecting link down.
	Active mode is resumed without loss of any packets when the switch detects the link up.
Cable length detection	Adjusts the signal strength based on the cable length for Gigabit Ethernet models. Reduces the power consumption for cables shorter than 10m.
Disable port LEDs	LEDs can be manually turned off to save on energy.
General	
ARP Registry	8000
MAC Tables	Up to 16K (16384) MAC addresses.
Discovery	
Link Layer Discovery Protocol (LLDP) (802.lab) with LLDP-MED extensions	LLDP allows the switch to advertise its identification, configuration, and capabilities to neighboring devices that store the data in a MIB. LLDP-MED is an enhancement to LLDP that adds the extensions needed for IP phones.
Cabling Type	Unshielded twisted pair (UTP) Category 5 or better, SM and MM Fiber
Supported SFP Types	1000BaseSX, 1000BaseLX, 1000BaseZX, 1000BaseT, 10GBaseSR,10GBaseLR,10GBaseZR, 10GBaseER.
LEDs	System, Link/Act, Speed, LED power saving option
Stacking	
Device Connection	Connection with 8x 10G ports and standard fiber, without the need for special hardware.
Distance	100m distance between devices. Stack with 2 SFP + and/or 2 SFP + external connections.
Management	One-key management, one-key operating system upgrade. Single Spanning Tree group.
Environmental	
MTBF	328,650
Power	110V: 46.08W 220V: 45.67W. Optional 2x PSU.
Certification	UL 62368, UL 60950, CSA 22.2, CE mark, FCC Part 15 (CFR 47) Class A, ROHS, WEEE
Operating temperature	0° to 50°C (32° to 122°F)
Storage temperature	-20° to 70°C (4° to 158°F)
Operating humidity	10% to 90%, relative, noncondensing
Storage humidity	10% to 90%, relative, noncondensing

Model	Ports				PoE Port
	Copper	SFP	SFP+	Common	
ANW-2023-24GT-4SFP1G	24	4			
ANW-2023-24GT-4SFP1G-P	24	4			24
ANW-2023-24GT-2SFP1G-2SFP10G	24	2	2		
ANW-2023-24GT-2SFP1G-2SFP10G-P	24	2	2		24
ANW-2023-24GT-4SFP10G	24		4		
ANW-2023-24GT-4SFP10G-P	24		4		24
ANW-2023-48GT-4SFP1G	48	4			
ANW-2023-48GT-4SFP1G-P	48	4			48
ANW-2023-48GT-2SFP1G-2SFP10G	48	2	2		
ANW-2023-48GT-2SFP1G-2SFP10G-P	48	2	2		48
ANW-2023-48GT-4SFP10G	48		4		
ANW-2023-48GT- 4SFP10G-P	48		4		48
ANW-2023-32G-4X	8	24	4	8COPPER=8SFP	
ANW-2023-8GT-2SFP1G	8	2			
ANW-2023-8GT-2SFP1G-P	8	2			8
ANW-2023-8GT-1SFP1G-1SFP10G	8	1	1		
ANW-2023-8GT-1SFP1G-1SFP10G-P	8	1	1		8
ANW-2023-8GT-2SFP10G	8		2		
ANW-2023-8GT-2SFP10G-P	8		2		8

VR20200613ENA

* With IP Routing Licence

© 2020 Angora Networks