

# <u>GS8F2C</u> Web Smart + Managed GbE Fiber Switch

GS8F2C web smart+ managed GbE fiber switch is the next-generation fiber switch offering powerful L2 features with better functionality and usability. That delivers the cost-effectively business and transports Ethernet services via fiber or copper connections.

GS8F2C delivers 8 (100M/1G) SFP ports and 2 combo Gbe RJ45/SFP ports. GS8F2C provides high HW performance and environment flexibility for SMBs and Enterprises.

The embedded Device Managed System (DMS) features provides users with the benefits of easy-touse/configure/install/troubleshoot in the video surveillance, wireless access, and other SMBs and Enterprises applications. GS8F2C is ideal to deliver management simplicity, better user experience, and lowest total cost of ownership.

## Specifications -

- Web Smart+ features provide easier manageability, basic security and QoS
- Built in Device Management System (DMS)
- DHCP Server
- IEEE 802.3az EEE Energy Efficient Ethernet standard for green Ethernet



## **Benefits**

Cost-effective Ethernet Switch for Enterprise-class

The switch delivers advanced functionality in Web Smart+ managed switch including DHCP client, IGMP, LLDP, etc. It also has basic security features such as IEEE 802.1x to protect your network from unauthorized access.

It helps users to build on the market-leading price/performance with Web Smart+ managed GbE switch, and provide ease of use for enterprise and SMB deployments.

• Easy to Install, Configure and Troubleshoot by Device Management System

The DMS provides embedded functions to facilitate devices management at anytime and anywhere. Its user-friendly interface helps users to manage devices intuitively.

It supports various IP device types (e.g. PC, IP-phone, IP-camera, WiFi-AP) for end users to enhance manageability and save time/cost during installation/maintenance stages.



• Lowing Total Cost of Ownership (TCO) with Energy-efficient Design

The switch is designed to help companies to save power needs and reduce TCO by Energy Efficient Ethernet (IEEE 802.3az). It can be used for customers to build a green Ethernet networking environment.

Port Configuration

Total Ports	SFP (100M/1G)	Uplinks (100M/1G)	Console
10	8	2 Combo	

Hardware Performance

Forwarding Capacity	Switching	Mac Table	Jumbo Frames
(Mpps)	Capacity (Gbps)	(K)	(Bytes)
14.88	20	8	9216

### **Environmental Range**

Operating Temperature		Storage Temperature		Operating Humidity	Altitude	
Fahrenheit	Centigrade	Fahrenheit	Centigrade	10% to 90% non-	Feet	Meters
32 to 149	0 to 65	-4 to 158	-20 to 70	condensing	< 10000	<3000

#### Dimension, Weights, Humidity

Dimension (WxHxD)		We		
Millimeter	Inches	Kilograms	Pounds	Mounting Type
280x 44x 166	11x 1.7x 6.5	<2.5	<5.5	Desktop, Wall

#### Voltage and Frequency

	AC Input Voltage and Frequency
Voltage	100 - 240 VAC
Frequency	47 - 63Hz

Certification

Electromagnetic Emissions (EMC)

## CE, FCC Part 15 Class A

#### Software Features

	Layer 2 Switching
Spanning Tree Protocol (STP)	Standard Spanning Tree 802.1d Rapid Spanning Tree (RSTP) 802.1w Multiple Spanning Tree (MSTP) 802.1s
Trunking	Link Aggregation Control Protocol (LACP) IEEE 802.3ad Static aggregation
VLAN	Supports up to 4K VLANs simultaneously (out of 4096 VLAN IDs)



802.1 Q tog-based VLAN   Protocol based VLAN   IP subnet-based VLAN   Private VLAN Edge (PVE)   MAC-based VLAN   Q-in-Q (double tog) VLAN   Voice VLAN   GARP VLAN Registration Protocol (GVRP) (option)   DHCP Relay   Relay of DHCP traffic to DHCP server in different VLAN.   Works with DHCP Option 82   IGMP querier   supports 512 multicast groups   IGMP Querier   Supports 512 multicast groups   IGMP querier is used to support a Layer 2 multicast domain of snooping   Switches in the absence of a multicast router   IGMP proxy IGMP snooping with proxy reporting or report suppression actively filters   IGMP proxy IGMP packets in order to reduce load on the multicast router   Multicast VLAN forward multicast traffic over Layer 2 network in conjunction with IGMP snooping.   Secure Sockets SSL encrypts the http traffic, allowing advanced secure access to the browser-based management GUI in the switch.   Leper 2 Isolation PVE (also known as protected ports) provides L2 isolation between clients in the same VLAN. Supports multiple host mode and single/multiple sessions Supports IGMP-RADIUS based 802.1X   Dynamic VLAN Edge Prevents illegal IP address from accessing to specific port in the switch.		
Protocol based VLAN   IP subnet-based VLAN   Private VLAN Edge (PVE)   MAC-based VLAN   Q-in-Q (double tag) VLAN   Voice VLAN   GARP VLAN Registration Protocol (GVRP) (option)   DHCP Relay   Works with DHCP Option 82   IGMP v1/v2   IGMP querier   Supports 512 multicast groups   IGMP Querier   IGMP aperiter is used to support a Layer 2 multicast domain of snooping switches in the absence of a multicast router   MLD v1/v2   IGMP proxy   IGMP snooping with proxy reporting or report suppression actively filters IGMP packets in order to reduce load on the multicast router   MLD v1/v2   Delivers IPv6 multicast packets only to the required receivers   Multicast VLAN Registration (MWR)   Relegistration (MWR)   IEEE802.1X: RADIUS authentication, authorization and accounting, MD5 hash, guest VLAN, single/multiple host mode and single/multiple sessions Supports IGMP-RADIUS based 802.1X Dynamic VLAN assignment   Layer 1 solation PVE (also known as protected ports) provides L2 isolation between clients in the same VLAN. Supports multiple uplinks   Port Security Locks MAC addresses to ports, and limits the number of learned MAC address   Prosurce Guard Prevents illegal IP address from accessing to		Port-based VLAN
IP subnet-based VLAN   Private VLAN Edge (PVE)   MAC-based VLAN   Q-in-Q (double tag) VLAN   Voice VLAN   GARP VLAN Registration Protocol (GVRP) (option)   DHCP Relay   Relay of DHCP traffic to DHCP server in different VLAN.   Works with DHCP Option 82   IGMP v1/v2   IGMP Querier   supports 512 multicast groups   IGMP Querier   IGMP Proxy   IGMP snooping with proxy reporting or report suppression actively filters   IGMP packets in order to reduce load on the multicast router   MLD v1/v2   Delivers IPv6 multicast packets only to the required receivers   Snooping   Nulticast VLAN   Registration (MWR)   security   Secure Sockets   Layer (SSL)   Layer (SSL)   Private VLAN, single/multiple host mode and single/multiple sessions   Supports IGMP-RADIUS sade 802.1X   Dynamic VLAN assignment   Layer 2 Isolation   PVE (also known as protected ports) provides L2 isolation between clients in the same VLAN. Supports multiple uplinks   Port Security Locks MAC addresses to ports, and limits the number of learned MAC address		0
Private VLAN Edge (PVE)   MAC-based VLAN   Q-in-Q (double tag) VLAN   Voice VLAN   GARP VLAN Registration Protocol (GVRP) (option)   DHCP Relay   Relay of DHCP traffic to DHCP server in different VLAN.   Works with DHCP Option 82   IGMP v1/V2   IGMP Querier   IGMP querier is used to support a Layer 2 multicast domain of snooping switches in the obsence of a multicast router   MLD v1/V2   IGMP packets in order to reduce load on the multicast router   MLD v1/V2   Pelivers IPv6 multicast packets only to the required receivers   Snooping   Delivers IPv6 multicast packets only to the required receivers   Snooping   VLD v1/V2   Secure Sockets   SSL encrypts the http traffic, allowing advanced secure access to the browser-based management GUI in the switch   IEEE802.1X   Suports IGMP-RADIUS based 802.1X   Dynamic VLAN asignment   Layer 2 Isolation   Private VLAN Edge   Por Versoping   Pic Kalso known as protected ports) provides L2 isolation between clients in the same VLAN. Supports multiple uplinks   Port Security   Locks MAC addresses to ports, and limits the number of learn		
MAC-based VLAN   Q-in-Q (double tog) VLAN   Voice VLAN   GARP VLAN Registration Protocol (GVRP) (option)   DHCP Relay   Works with DHCP Option 82   IGMP v1/v2   IGMP Querier   switches in the absence of a multicast traffic to only the requesters.   Sopoping   IGMP Proxy   IGMP packets in order to reduce load on the multicast router   ILCMP packets in order to reduce load on the multicast volter   MUL v1/v2   Snooping   Delivers IPv6 multicast packets only to the required receivers   Multicast VLAN   Registration (MVR)   Recurs Sockets   Layer (SSL)   IEEE 802.1X   Sopoping   VE (also known as protected ports) provides L2 isolation between clients in Private VLAN. Supports IMMUL based 802.1X   Dynamic VLAN signment   Layer 2 Isolation   Private VLAN Edge   Port Security   Locks MAC addresses to ports, and limits the number of learned MAC address   Supports IGMP-RADIUS based 802.1X   Dynamic VLAN signment   Layer 2 Isolation   Private VLAN   Port Security		IP subnet-based VLAN
Q-in-Q (double tag) VLAN   Voice VLAN   GARP VLAN Registration Protocol (GVRP) (option)   PHCP Relay Relay of DHCP traffic to DHCP server in different VLAN.   Works with DHCP Option 82   IGMP v1/v2 IGMP limits bandwidth-intensive multicast traffic to only the requesters.   Snooping Supports 512 multicast groups   IGMP Querier IGMP querier is used to support a Layer 2 multicast domain of snooping switches in the absence of a multicast router   IGMP Proxy IGMP snooping with proxy reporting or report suppression actively filters IGMP proxy   Multicast VLAN Registration (MVR)   Registration (MVR) to sadedicated manually configured VLAN, called the multicast VLAN, to forward multicast traffic over Layer 2 network in conjunction with IGMP snooping.   Secure Sockets SSL encrypts the http traffic, allowing advanced secure access to the browser-based management GUI in the switch   Layer (SSL) IEEE 802.1X: RADIUS authentication, authorization and accounting, MD5 htsh, guest VLAN, single/multiple host mode and single/multiple sessions Supports IGMP-RADIUS based 802.1X   Dynamic VLAN assignment PVE (also known as protected ports) provides L2 isolation between clients in frivate VLAN Edge   Port Security Locks MAC addresses to ports, and limits the number of learned MAC addresses to ports, and limits the number of learned MAC addresses   IP Source Guard		Private VLAN Edge (PVE)
Voice VLAN   GARP VLAN Registration Protocol (GVRP) (option)     DHCP Relay   GARP VLAN Registration Protocol (GVRP) (option)     DHCP Relay   Relay of DHCP traffic to DHCP server in different VLAN. Works with DHCP Option 82     IGMP V1/v2   IGMP limits bandwidth-intensive multicast traffic to only the requesters. Snooping     Supports 512 multicast groups   IGMP querier is used to support a Layer 2 multicast domain of snooping switches in the absence of a multicast router     IGMP Proxy   IGMP snooping with proxy reporting or report suppression actively filters IGMP proxy     MLD v1/v2   Delivers IPv6 multicast packets only to the required receivers     Snooping   It uses a dedicated manually configured VLAN, called the multicast VLAN, to forward multicast traffic over Layer 2 network in conjunction with IGMP snooping.     Secure Sockets   SSL encrypts the http traffic, allowing advanced secure access to the browser-based management GUI in the switch     IEEE 802.1X   IEEE802.1X: RADIUS authentication, authorization and accounting, MD5 shab, guest VLAN, single/multiple host mode and single/multiple sessions Supports IGMP-RADIUS based 802.1X Dynamic VLAN assignment     Layer 2 Isolation   Prevents allegal IP address from accessing to specific port in the switch     RADIUS/ TACACS+   Supports RADIUS and TACACS+ authentication. Switch as a client     RADIUS/ TACACS+   Prevents traffic on a LAN from being disrupted by a bro		MAC-based VLAN
Voice VLAN   GARP VLAN Registration Protocol (GVRP) (option)     DHCP Relay   GARP VLAN Registration Protocol (GVRP) (option)     DHCP Relay   Relay of DHCP traffic to DHCP server in different VLAN. Works with DHCP Option 82     IGMP V1/v2   IGMP limits bandwidth-intensive multicast traffic to only the requesters. Snooping     Supports 512 multicast groups   IGMP querier is used to support a Layer 2 multicast domain of snooping switches in the absence of a multicast router     IGMP Proxy   IGMP snooping with proxy reporting or report suppression actively filters IGMP proxy     MLD v1/v2   Delivers IPv6 multicast packets only to the required receivers     Snooping   It uses a dedicated manually configured VLAN, called the multicast VLAN, to forward multicast traffic over Layer 2 network in conjunction with IGMP snooping.     Secure Sockets   SSL encrypts the http traffic, allowing advanced secure access to the browser-based management GUI in the switch     IEEE 802.1X   IEEE802.1X: RADIUS authentication, authorization and accounting, MD5 shab, guest VLAN, single/multiple host mode and single/multiple sessions Supports IGMP-RADIUS based 802.1X Dynamic VLAN assignment     Layer 2 Isolation   Prevents allegal IP address from accessing to specific port in the switch     RADIUS/ TACACS+   Supports RADIUS and TACACS+ authentication. Switch as a client     RADIUS/ TACACS+   Prevents traffic on a LAN from being disrupted by a bro		Q-in-Q (double tag) VLAN
GARP VLAN Registration Protocol (GVRP) (option)     DHCP Relay   Relay of DHCP traffic to DHCP server in different VLAN. Works with DHCP Option 82     IGMP v1/v2   IGMP limits bandwidth-intensive multicast traffic to only the requesters. Snooping     Supports 512 multicast groups   IGMP querier is used to support a Layer 2 multicast domain of snooping witches in the absence of a multicast router     IGMP Proxy   IGMP snooping with proxy reporting or report suppression actively filters IGMP packets in order to reduce load on the multicast router     MLD v1/v2   Delivers IPv6 multicast packets only to the required receivers     Snooping   It uses a dedicated manually configured VLAN, called the multicast VLAN, to forward multicast traffic over Layer 2 network in conjunction with IGMP snooping.     Secure Sockets   SSL encrypts the http traffic, allowing advanced secure access to the browser-based management GUI in the switch     IEEE 802.1X   IEEE802.1X: RADIUS authentication, authorization and accounting, MD5 hash, guest VLAN, single/multiple host mode and single/multiple sessions Supports IGMP-RADIUS based 802.1X Dynamic VLAN assignment     Layer 2 Isolation Private VLAN Edge   PVE (also known as protected ports) provides L2 isolation between clients in the same VLAN. Supports multiple uplinks     Port Security   Locks MAC addresses to ports, and limits the number of learned MAC address     IP Source Guard   Prevents illegal IP address from accessing to specific port in the switch<		
DHCP Relay   Relay of DHCP traffic to DHCP server in different VLAN. Works with DHCP Option 82     IGMP v1/v2   IGMP limits bandwidth-intensive multicast traffic to only the requesters. Snooping   Supports 512 multicast groups     IGMP Querier   IGMP querier is used to support a Layer 2 multicast domain of snooping switches in the absence of a multicast router     IGMP Proxy   IGMP proxy reporting or report suppression actively filters IGMP proxy     MLD v1/v2 Snooping   Delivers IPv6 multicast packets only to the required receivers     Multicast VLAN Registration (MVR)   It uses a dedicated manually configured VLAN, called the multicast VLAN, to forward multicast traffic over Layer 2 network in conjunction with IGMP snooping.     Secure Sockets   SSL encrypts the http traffic, allowing advanced secure access to the browser-based management GUI in the switch     IEEE 802.1X   IEEE802.1X: RADIUS authentication, authorization and accounting, MD5 hash, guest VLAN, single-multiple host mode and single/multiple sessions Supports IGMP-RADIUS based 802.1X Dynamic VLAN assignment     Layer 2 Isolation Private VLAN Edge   PVE (also known as protected ports) provides L2 isolation between clients in the same VLAN. Supports multiple uplinks     Port Security   Locks MAC addresses to ports, and limits the number of learned MAC address     IP Source Guard   Prevents traffic on a LAN from being disrupted by a broadcast, multicast, or unicast storm on a port     DHCP Snooping		GARP VLAN Registration Protocol (GVRP) (option)
DIFCE Relay   Works with DHCP Option 82     IGMP V1/v2   IGMP limits bandwidth-intensive multicast traffic to only the requesters. Supports 512 multicast groups     IGMP Querier   IGMP querier is used to support a Layer 2 multicast domain of snooping switches in the absence of a multicast router     IGMP Proxy   IGMP approximation of snooping with proxy reporting or report suppression actively filters IGMP packets in order to reduce load on the multicast router     MLD v1/v2 Snooping   Delivers IPv6 multicast packets only to the required receivers     Multicast VLAN Registration (MVR)   It uses a dedicated manually configured VLAN, called the multicast VLAN, to forward multicast traffic over Layer 2 network in conjunction with IGMP snooping.     Secure Sockets   SSL encrypts the http traffic, allowing advanced secure access to the browser-based management GUI in the switch     IEEE 802.1X   IEEE802.1X: RADIUS authentication, authorization and accounting, MD5 hash, guest VLAN, single/multiple host mode and single/multiple sessions Supports IGMP-RADIUS based 802.1X Dynamic VLAN assignment     Layer 2 Isolation Private VLAN Edge   PVE (also known as protected ports) provides L2 isolation between clients in the same VLAN. Supports multiple uplinks     Port Security   Locks MAC addresses to ports, and limits the number of learned MAC address     IP Source Guard   Prevents illegal IP address from accessing to specific port in the switch     RADIUS/ TACACS+   Supports RADIU		
IGMP v1/v2 IGMP limits bandwidth-intensive multicast traffic to only the requesters.   Snooping Supports 512 multicast groups   IGMP Querier IGMP querier is used to support a Layer 2 multicast domain of snooping switches in the absence of a multicast router   IGMP Proxy IGMP snooping with proxy reporting or report suppression actively filters IGMP packets in order to reduce load on the multicast router   MLD v1/v2 Delivers IPv6 multicast packets only to the required receivers   Snooping It uses a dedicated manually configured VLAN, called the multicast VLAN, to forward multicast traffic over Layer 2 network in conjunction with IGMP snooping.   Secure Sockets SSL encrypts the http traffic, allowing advanced secure access to the browser-based management GUI in the switch   IEEE 802.1X IEEE802.1X: RADIUS authentication, authorization and accounting, MD5 hash, guest VLAN, single/multiple host mode and single/multiple sessions supports IGMP-RADIUS based 802.1X   Private VLAN Edge PvE (also known as protected ports) provides L2 isolation between clients in the same VLAN. Supports multiple uplinks   Port Security Locks MAC addresses to ports, and limits the number of learned MAC address   IP Source Guard Prevents illegal IP address from accessing to specific port in the switch   RADIUS/ TACACS+ Supports RADIUS and TACACS+ authentication. Switch as a client   Pheres traffic on a LAN from being disrupted by a broadcast, multicast, or un	DHCP Relay	
Snooping   Supports 512 multicast groups     IGMP Querier   IGMP querier is used to support a Layer 2 multicast domain of snooping switches in the absence of a multicast router     IGMP Proxy   IGMP snooping with proxy reporting or report suppression actively filters IGMP packets in order to reduce load on the multicast router     MLD v1/v2 Snooping   Delivers IPv6 multicast packets only to the required receivers     Multicast VLAN Registration (MVR)   It uses a dedicated manually configured VLAN, called the multicast VLAN, to forward multicast traffic over Layer 2 network in conjunction with IGMP snooping.     Secure Sockets   SSL encrypts the http traffic, allowing advanced secure access to the browser-based management GUI in the switch     IEEE 802.1X:   RADIUS authentication, authorization and accounting, MD5 hash, guest VLAN, single/multiple host mode and single/multiple sessions Supports IGMP-RADIUS based 802.1X Dynamic VLAN assignment     Layer 2 Isolation Private VLAN Edge   PVE (also known as protected ports) provides L2 isolation between clients in the same VLAN. Supports multiple uplinks     Port Security   Locks MAC addresses to ports, and limits the number of learned MAC address     IP Source Guard   Prevents isllegal IP address from accessing to specific port in the switch     RADIUS/ TACACS+   Supports RADIUS and TACACS+ authentication. Switch as a client     PHCP Snooping   A feature acts as a firewall between untrusted hosts and trusted DHCP servers<		
IGMP Querier   IGMP querier is used to support a Layer 2 multicast domain of snooping switches in the absence of a multicast router     IGMP Proxy   IGMP snooping with proxy reporting or report suppression actively filters IGMP packets in order to reduce load on the multicast router     MLD v1/v2 Snooping   Delivers IPv6 multicast packets only to the required receivers     Multicast VLAN Registration (MVR)   It uses a dedicated manually configured VLAN, called the multicast VLAN, to forward multicast traffic over Layer 2 network in conjunction with IGMP snooping.     Security   SsL encrypts the http traffic, allowing advanced secure access to the browser-based management GUI in the switch     IEEE 802.1X   SSL encrypts the http traffic, allowing advanced and single/multiple sessions Supports IGMP-RADIUS authentication, authorization and accounting, MD5 hash, guest VLAN, single/multiple host mode and single/multiple sessions Supports IGMP-RADIUS based 802.1X Dynamic VLAN assignment     Layer 2 Isolation Private VLAN Edge   PVE (also known as protected ports) provides L2 isolation between clients in the same VLAN. Supports multiple uplinks     Port Security   Locks MAC addresses to ports, and limits the number of learned MAC address     IP Source Guard   Prevents illegal IP address from accessing to specific port in the switch     RADIUS/ TACACS+   Supports RADIUS and TACACS+ authentication. Switch as a client     PhCP Snooping   A feature acts as a firewall between untrusted hosts and trusted DHCP servers		
IGMP Querier   switches in the absence of a multicast router     IGMP Proxy   IGMP snooping with proxy reporting or report suppression actively filters IGMP packets in order to reduce load on the multicast router     MLD v1/v2 Snooping   Delivers IPv6 multicast packets only to the required receivers     Multicast VLAN Registration (MVR)   It uses a dedicated manually configured VLAN, called the multicast VLAN, to forward multicast traffic over Layer 2 network in conjunction with IGMP snooping.     Secure Sockets   SSL encrypts the http traffic, allowing advanced secure access to the browser-based management GUI in the switch     IEEE 802.1X   IEEE802.1X: RADIUS authentication, authorization and accounting, MD5 hash, guest VLAN, single/multiple host mode and single/multiple sessions Supports IGMP-RADIUS based 802.1X     Port Security   Locks MAC addresses to ports, and limits the number of learned MAC address     Port Security   Locks MAC addresses from accessing to specific port in the switch     RADIUS/ TACACS+   Supports RADIUS and TACACS+ authentication. Switch as a client     Prevents traffic on a LAN from being disrupted by a broadcast, multicast, or unicast storm on a port     DHCP Snooping   A feature acts as a firewall between untrusted hosts and trusted DHCP servers     Loop Protection   To prevent unknown unicast, broadcast and multicast loops in Layer 2 switching configurations.     Supports up to 384 entries. Drop or rate limitation based	Shooping	
IGMP Proxy IGMP snooping with proxy reporting or report suppression actively filters IGMP packets in order to reduce load on the multicast router   MLD v1/v2 Snooping Delivers IPv6 multicast packets only to the required receivers   Multicast VLAN Registration (MVR) It uses a dedicated manually configured VLAN, called the multicast VLAN, to forward multicast traffic over Layer 2 network in conjunction with IGMP snooping.   Secure Sockets SSL encrypts the http traffic, allowing advanced secure access to the browser-based management GUI in the switch   IEEE 802.1X IEEE802.1X: RADIUS authentication, authorization and accounting, MD5 hash, guest VLAN, single/multiple host mode and single/multiple sessions Supports IGMP-RADIUS based 802.1X Dynamic VLAN assignment   Layer 2 Isolation Private VLAN Edge PVE (also known as protected ports) provides L2 isolation between clients in Private VLAN Edge   Port Security Locks MAC addresses to ports, and limits the number of learned MAC address   IP Source Guard Prevents Itagla IP address from accessing to specific port in the switch   RADIUS/ TACACS+ Supports RADIUS and TACACS+ authentication. Switch as a client   Storm Control Prevents traffic on a LAN from being disrupted by a broadcast, multicast, or unicast storm on a port   DHCP Snooping A feature acts as a firewall between untrusted hosts and trusted DHCP servers   Loop Protection To prevent unknown unicast, broadcast and multicast loops in Layer 2 switching configurati	IGMP Querier	
IGMP packets in order to reduce load on the multicast router   MLD v1/v2 Snooping Delivers IPv6 multicast packets only to the required receivers   Multicast VLAN Registration (MVR) It uses a dedicated manually configured VLAN, called the multicast VLAN, to forward multicast traffic over Layer 2 network in conjunction with IGMP snooping.   Security Security   Secure Sockets SSL encrypts the http traffic, allowing advanced secure access to the browser-based management GUI in the switch   IEEE 802.1X IEEE802.1X: RADIUS authentication, authorization and accounting, MD5 hash, guest VLAN, single/multiple host mode and single/multiple sessions Supports IGMP-RADIUS based 802.1X Dynamic VLAN assignment   Layer 2 Isolation Private VLAN Edge PVE (also known as protected ports) provides L2 isolation between clients in the same VLAN. Supports multiple uplinks   Port Security Locks MAC addresses to ports, and limits the number of learned MAC address   IP Source Guard Prevents illegal IP address from accessing to specific port in the switch   RADIUS/ TACACS+ Supports RADIUS and TACACS+ authentication. Switch as a client   PHCP Snooping A feature acts as a firewall between untrusted hosts and trusted DHCP servers   Loop Protection To prevent unknown unicast, broadcast and multicast loops in Layer 2 switching configurations.   Supports up to 384 entries. Drop or rate limitation based on: Source and destination MAC, VLAN ID or IP address, protocol, port, Diffe		
MLD v1/v2 Snooping Delivers IPv6 multicast packets only to the required receivers   Multicast VLAN Registration (MVR) It uses a dedicated manually configured VLAN, called the multicast VLAN, to forward multicast traffic over Layer 2 network in conjunction with IGMP snooping.   Secure Sockets SSL encrypts the http traffic, allowing advanced secure access to the browser-based management GUI in the switch   IEEE 802.1X IEEE802.1X: RADIUS authentication, authorization and accounting, MD5 hash, guest VLAN, single/multiple host mode and single/multiple sessions Supports IGMP-RADIUS based 802.1X Dynamic VLAN assignment   Layer 2 Isolation Private VLAN Edge PVE (also known as protected ports) provides L2 isolation between clients in the same VLAN. Supports multiple uplinks   Port Security Locks MAC addresses to ports, and limits the number of learned MAC address   IP Source Guard Prevents illegal IP address from accessing to specific port in the switch   RADIUS/ TACACS+ Supports RADIUS and TACACS+ authentication. Switch as a client   Storm Control Prevents traffic on a LAN from being disrupted by a broadcast, multicast, or unicast storm on a port   DHCP Snooping A feature acts as a firewall between untrusted hosts and trusted DHCP servers   Loop Protection To prevent unknown unicast, broadcast and multicast loops in Layer 2 switching configurations.   Supports up to 384 entries. Drop or rate limitation based on: Source and destination MAC, VLAN ID or IP address, protocol, port, Dif	IGMP Proxy	
Snooping   Delivers IPvo multicast packets only to the required receivers     Multicast VLAN Registration (MVR)   It uses a dedicated manually configured VLAN, called the multicast VLAN, to forward multicast traffic over Layer 2 network in conjunction with IGMP snooping.     Secure Sockets   SSL encrypts the http traffic, allowing advanced secure access to the browser-based management GUI in the switch     IEEE 802.1X   IEEE802.1X: RADIUS authentication, authorization and accounting, MD5 hash, guest VLAN, single/multiple host mode and single/multiple sessions Supports IGMP-RADIUS based 802.1X Dynamic VLAN assignment     Layer 2 Isolation Private VLAN Edge   PVE (also known as protected ports) provides L2 isolation between clients in the same VLAN. Supports multiple uplinks     Port Security   Locks MAC addresses to ports, and limits the number of learned MAC address     IP Source Guard   Prevents illegal IP address from accessing to specific port in the switch     RADIUS/ TACACS+   Supports RADIUS and TACACS+ authentication. Switch as a client     PhCP Snooping   A feature acts as a firewall between untrusted hosts and trusted DHCP servers     Loop Protection   To prevent unknown unicast, broadcast and multicast loops in Layer 2 switching configurations.     Supports up to 384 entries. Drop or rate limitation based on: Source and destination MAC, VLAN ID or IP address, protocol, port, Differentiated services code point (DSCP) / IP precedence		IGMP packets in order to reduce load on the multicast router
Snooping It uses a dedicated manually configured VLAN, called the multicast VLAN, to forward multicast traffic over Layer 2 network in conjunction with IGMP snooping.   Secure Sockets SSL encrypts the http traffic, allowing advanced secure access to the browser-based management GUI in the switch   IEEE 802.1X IEEE802.1X: RADIUS authentication, authorization and accounting, MD5 hash, guest VLAN, single/multiple host mode and single/multiple sessions Supports IGMP-RADIUS based 802.1X   Dynamic VLAN Edge PVE (also known as protected ports) provides L2 isolation between clients in the same VLAN. Supports multiple uplinks   Port Security Locks MAC addresses to ports, and limits the number of learned MAC address   IP Source Guard Prevents illegal IP address from accessing to specific port in the switch   RADIUS/ Supports RADIUS and TACACS+ authentication. Switch as a client   PhCP Snooping A feature acts as a firewall between untrusted hosts and trusted DHCP servers   Loop Protection To prevent unknown unicast, broadcast and multicast loops in Layer 2 switching configurations.   Supports up to 384 entries. Drop or rate limitation based on: Source and destination MAC, VLAN ID or IP address, protocol, port, Differentiated services code point (DSCP) / IP precedence	MLD v1/v2	Delivers IPv6 multicast packets only to the required receivers
Multicast VLAIN Registration (MVR) forward multicast traffic over Layer 2 network in conjunction with IGMP snooping.   Secure Sockets SSL encrypts the http traffic, allowing advanced secure access to the browser-based management GUI in the switch   IEEE 802.1X IEEE802.1X: RADIUS authentication, authorization and accounting, MD5 hash, guest VLAN, single/multiple host mode and single/multiple sessions Supports IGMP-RADIUS based 802.1X Dynamic VLAN assignment   Layer 2 Isolation Private VLAN Edge PVE (also known as protected ports) provides L2 isolation between clients in the same VLAN. Supports multiple uplinks   Port Security Locks MAC addresses to ports, and limits the number of learned MAC address   IP Source Guard Prevents illegal IP address from accessing to specific port in the switch   RADIUS/ TACACS+ Supports RADIUS and TACACS+ authentication. Switch as a client   Storm Control A feature acts as a firewall between untrusted hosts and trusted DHCP servers   Loop Protection To prevent unknown unicast, broadcast and multicast loops in Layer 2 switching configurations.   Loop Protection To prevent unknown unicast, broadcast and multicast loops in Layer 2 switching configurations.   A Clis Supports up to 384 entries. Drop or rate limitation based on: Source and destination MAC, VLAN ID or IP address, protocol, port, Differentiated services code point (DSCP) / IP precedence	Snooping	Delivers if vo monicusi puckers only to the required receivers
Multicast VLAIN Registration (MVR) forward multicast traffic over Layer 2 network in conjunction with IGMP snooping.   Secure Sockets SSL encrypts the http traffic, allowing advanced secure access to the browser-based management GUI in the switch   IEEE 802.1X IEEE802.1X: RADIUS authentication, authorization and accounting, MD5 hash, guest VLAN, single/multiple host mode and single/multiple sessions Supports IGMP-RADIUS based 802.1X Dynamic VLAN assignment   Layer 2 Isolation Private VLAN Edge PVE (also known as protected ports) provides L2 isolation between clients in the same VLAN. Supports multiple uplinks   Port Security Locks MAC addresses to ports, and limits the number of learned MAC address   IP Source Guard Prevents illegal IP address from accessing to specific port in the switch   RADIUS/ TACACS+ Supports RADIUS and TACACS+ authentication. Switch as a client   Storm Control A feature acts as a firewall between untrusted hosts and trusted DHCP servers   Loop Protection To prevent unknown unicast, broadcast and multicast loops in Layer 2 switching configurations.   Supports up to 384 entries. Drop or rate limitation based on: Source and destination MAC, VLAN ID or IP address, protocol, port, Differentiated services code point (DSCP) / IP precedence		It uses a dedicated manually configured VLAN, called the multicast VLAN, to
Registration (MVR) snooping.   Secure Sockets SSL encrypts the http traffic, allowing advanced secure access to the browser-based management GUI in the switch   IEEE 802.1X IEEE802.1X: RADIUS authentication, authorization and accounting, MD5 hash, guest VLAN, single/multiple host mode and single/multiple sessions Supports IGMP-RADIUS based 802.1X   Dynamic VLAN assignment PVE (also known as protected ports) provides L2 isolation between clients in the same VLAN. Supports multiple uplinks   Port Security Locks MAC addresses to ports, and limits the number of learned MAC address   IP Source Guard Prevents illegal IP address from accessing to specific port in the switch   RADIUS/ TACACS+ Supports RADIUS and TACACS+ authentication. Switch as a client   Storm Control Prevents traffic on a LAN from being disrupted by a broadcast, multicast, or unicast storm on a port   DHCP Snooping A feature acts as a firewall between untrusted hosts and trusted DHCP servers   Loop Protection To prevent unknown unicast, broadcast and multicast loops in Layer 2 switching configurations.   Supports up to 384 entries. Drop or rate limitation based on: Source and destination MAC, VLAN ID or IP address, protocol, port, Differentiated services code point (DSCP) / IP precedence		
Security     Secure Sockets Layer (SSL)   SSL encrypts the http traffic, allowing advanced secure access to the browser-based management GUI in the switch     IEEE 802.1X   IEEE802.1X: RADIUS authentication, authorization and accounting, MD5 hash, guest VLAN, single/multiple host mode and single/multiple sessions Supports IGMP-RADIUS based 802.1X Dynamic VLAN assignment     Layer 2 Isolation Private VLAN Edge   PVE (also known as protected ports) provides L2 isolation between clients in the same VLAN. Supports multiple uplinks     Port Security   Locks MAC addresses to ports, and limits the number of learned MAC address     IP Source Guard   Prevents illegal IP address from accessing to specific port in the switch     RADIUS/ TACACS+   Supports RADIUS and TACACS+ authentication. Switch as a client     Storm Control   Prevents traffic on a LAN from being disrupted by a broadcast, multicast, or unicast storm on a port     DHCP Snooping   A feature acts as a firewall between untrusted hosts and trusted DHCP servers     Loop Protection   To prevent unknown unicast, broadcast and multicast loops in Layer 2 switching configurations.     Supports up to 384 entries. Drop or rate limitation based on: Source and destination MAC, VLAN ID or IP address, protocol, port, Differentiated services code point (DSCP) / IP precedence	Registration (MVR)	,
Secure Sockets Layer (SSL)SSL encrypts the http traffic, allowing advanced secure access to the browser-based management GUI in the switchIEEE 802.1XIEEE802.1X: RADIUS authentication, authorization and accounting, MD5 hash, guest VLAN, single/multiple host mode and single/multiple sessions Supports IGMP-RADIUS based 802.1X Dynamic VLAN assignmentLayer 2 Isolation Private VLAN EdgePVE (also known as protected ports) provides L2 isolation between clients in the same VLAN. Supports multiple uplinksPort SecurityLocks MAC addresses to ports, and limits the number of learned MAC addressIP Source Guard RADIUS/ TACACS+Prevents illegal IP address from accessing to specific port in the switchStorm ControlPrevents traffic on a LAN from being disrupted by a broadcast, multicast, or unicast storm on a portDHCP SnoopingA feature acts as a firewall between untrusted hosts and trusted DHCP serversLoop ProtectionTo prevent unknown unicast, broadcast and multicast loops in Layer 2 switching configurations.ACLsSupports up to 384 entries. Drop or rate limitation based on: Source and destination MAC, VLAN ID or IP address, protocol, port, Differentiated services code point (DSCP) / IP precedence		
Layer (SSL)browser-based management GUI in the switchIEEE 802.1XIEEE802.1X: RADIUS authentication, authorization and accounting, MD5 hash, guest VLAN, single/multiple host mode and single/multiple sessions Supports IGMP-RADIUS based 802.1X Dynamic VLAN assignmentLayer 2 Isolation Private VLAN EdgePVE (also known as protected ports) provides L2 isolation between clients in the same VLAN. Supports multiple uplinksPort SecurityLocks MAC addresses to ports, and limits the number of learned MAC addressIP Source GuardPrevents illegal IP address from accessing to specific port in the switchRADIUS/ TACACS+Supports RADIUS and TACACS+ authentication. Switch as a clientStorm ControlPrevents traffic on a LAN from being disrupted by a broadcast, multicast, or unicast storm on a portDHCP SnoopingA feature acts as a firewall between untrusted hosts and trusted DHCP serversLoop ProtectionTo prevent unknown unicast, broadcast and multicast loops in Layer 2 switching configurations.ACLsSupports up to 384 entries. Drop or rate limitation based on: Source and destination MAC, VLAN ID or IP address, protocol, port, Differentiated services code point (DSCP) / IP precedence	Secure Sockets	
IEEE 802.1XIEEE802.1X: RADIUS authentication, authorization and accounting, MD5 hash, guest VLAN, single/multiple host mode and single/multiple sessions Supports IGMP-RADIUS based 802.1X Dynamic VLAN assignmentLayer 2 Isolation Private VLAN EdgePVE (also known as protected ports) provides L2 isolation between clients in the same VLAN. Supports multiple uplinksPort SecurityLocks MAC addresses to ports, and limits the number of learned MAC addressIP Source GuardPrevents illegal IP address from accessing to specific port in the switchRADIUS/ TACACS+Supports RADIUS and TACACS+ authentication. Switch as a clientStorm ControlPrevents traffic on a LAN from being disrupted by a broadcast, multicast, or unicast storm on a portDHCP SnoopingA feature acts as a firewall between untrusted hosts and trusted DHCP serversLoop ProtectionTo prevent unknown unicast, broadcast and multicast loops in Layer 2 switching configurations.ACLsSupports up to 384 entries. Drop or rate limitation based on: Source and destination MAC, VLAN ID or IP address, protocol, port, Differentiated services code point (DSCP) / IP precedence		
IEEE 802.1Xhash, guest VLAN, single/multiple host mode and single/multiple sessions Supports IGMP-RADIUS based 802.1X Dynamic VLAN assignmentLayer 2 Isolation Private VLAN EdgePVE (also known as protected ports) provides L2 isolation between clients in the same VLAN. Supports multiple uplinksPort SecurityLocks MAC addresses to ports, and limits the number of learned MAC addressIP Source GuardPrevents illegal IP address from accessing to specific port in the switchRADIUS/ TACACS+Supports RADIUS and TACACS+ authentication. Switch as a clientStorm ControlPrevents traffic on a LAN from being disrupted by a broadcast, multicast, or unicast storm on a portDHCP SnoopingA feature acts as a firewall between untrusted hosts and trusted DHCP serversLoop ProtectionTo prevent unknown unicast, broadcast and multicast loops in Layer 2 switching configurations.ACLsSupports up to 384 entries. Drop or rate limitation based on: Source and destination MAC, VLAN ID or IP address, protocol, port, Differentiated services code point (DSCP) / IP precedence		
IEEE 802.1XSupports IGMP-RADIUS based 802.1X Dynamic VLAN assignmentLayer 2 Isolation Private VLAN EdgePVE (also known as protected ports) provides L2 isolation between clients in the same VLAN. Supports multiple uplinksPort SecurityLocks MAC addresses to ports, and limits the number of learned MAC addressIP Source GuardPrevents illegal IP address from accessing to specific port in the switchRADIUS/ TACACS+Supports RADIUS and TACACS+ authentication. Switch as a clientStorm ControlPrevents traffic on a LAN from being disrupted by a broadcast, multicast, or unicast storm on a portDHCP SnoopingA feature acts as a firewall between untrusted hosts and trusted DHCP serversLoop ProtectionTo prevent unknown unicast, broadcast and multicast loops in Layer 2 switching configurations.ACLsSupports up to 384 entries. Drop or rate limitation based on: Source and destination MAC, VLAN ID or IP address, protocol, port, Differentiated services code point (DSCP) / IP precedence		
Dynamic VLAN assignmentLayer 2 Isolation Private VLAN EdgePVE (also known as protected ports) provides L2 isolation between clients in the same VLAN. Supports multiple uplinksPort SecurityLocks MAC addresses to ports, and limits the number of learned MAC addressIP Source GuardPrevents illegal IP address from accessing to specific port in the switchRADIUS/ TACACS+Supports RADIUS and TACACS+ authentication. Switch as a clientStorm ControlPrevents traffic on a LAN from being disrupted by a broadcast, multicast, or unicast storm on a portDHCP SnoopingA feature acts as a firewall between untrusted hosts and trusted DHCP serversLoop ProtectionTo prevent unknown unicast, broadcast and multicast loops in Layer 2 switching configurations.ACLsSupports up to 384 entries. Drop or rate limitation based on: Source and destination MAC, VLAN ID or IP address, protocol, port, Differentiated services code point (DSCP) / IP precedence	IEEE 802.1X	
Layer 2 Isolation Private VLAN EdgePVE (also known as protected ports) provides L2 isolation between clients in the same VLAN. Supports multiple uplinksPort SecurityLocks MAC addresses to ports, and limits the number of learned MAC addressIP Source GuardPrevents illegal IP address from accessing to specific port in the switchRADIUS/ TACACS+Supports RADIUS and TACACS+ authentication. Switch as a clientStorm ControlPrevents traffic on a LAN from being disrupted by a broadcast, multicast, or unicast storm on a portDHCP SnoopingA feature acts as a firewall between untrusted hosts and trusted DHCP serversLoop ProtectionTo prevent unknown unicast, broadcast and multicast loops in Layer 2 switching configurations.ACLsSupports up to 384 entries. Drop or rate limitation based on: Source and destination MAC, VLAN ID or IP address, protocol, port, Differentiated services code point (DSCP) / IP precedence		
Private VLAN Edgethe same VLAN. Supports multiple uplinksPort SecurityLocks MAC addresses to ports, and limits the number of learned MAC addressIP Source GuardPrevents illegal IP address from accessing to specific port in the switchRADIUS/ TACACS+Supports RADIUS and TACACS+ authentication. Switch as a clientStorm ControlPrevents traffic on a LAN from being disrupted by a broadcast, multicast, or unicast storm on a portDHCP SnoopingA feature acts as a firewall between untrusted hosts and trusted DHCP serversLoop ProtectionTo prevent unknown unicast, broadcast and multicast loops in Layer 2 switching configurations.ACLsSupports up to 384 entries. Drop or rate limitation based on: Source and destination MAC, VLAN ID or IP address, protocol, port, Differentiated services code point (DSCP) / IP precedence		,
Port SecurityLocks MAC addresses to ports, and limits the number of learned MAC addressIP Source GuardPrevents illegal IP address from accessing to specific port in the switchRADIUS/ TACACS+Supports RADIUS and TACACS+ authentication. Switch as a clientStorm ControlPrevents traffic on a LAN from being disrupted by a broadcast, multicast, or unicast storm on a portDHCP SnoopingA feature acts as a firewall between untrusted hosts and trusted DHCP serversLoop ProtectionTo prevent unknown unicast, broadcast and multicast loops in Layer 2 switching configurations.ACLsSupports up to 384 entries. Drop or rate limitation based on: Source and destination MAC, VLAN ID or IP address, protocol, port, Differentiated services code point (DSCP) / IP precedence	/	
Port Security address   IP Source Guard Prevents illegal IP address from accessing to specific port in the switch   RADIUS/ TACACS+ Supports RADIUS and TACACS+ authentication. Switch as a client   Storm Control Prevents traffic on a LAN from being disrupted by a broadcast, multicast, or unicast storm on a port   DHCP Snooping A feature acts as a firewall between untrusted hosts and trusted DHCP servers   Loop Protection To prevent unknown unicast, broadcast and multicast loops in Layer 2 switching configurations.   ACLs Supports up to 384 entries. Drop or rate limitation based on: Source and destination MAC, VLAN ID or IP address, protocol, port, Differentiated services code point (DSCP) / IP precedence	Private VLAN Edge	
IP Source GuardPrevents illegal IP address from accessing to specific port in the switchRADIUS/ TACACS+Supports RADIUS and TACACS+ authentication. Switch as a clientStorm ControlPrevents traffic on a LAN from being disrupted by a broadcast, multicast, or unicast storm on a portDHCP SnoopingA feature acts as a firewall between untrusted hosts and trusted DHCP serversLoop ProtectionTo prevent unknown unicast, broadcast and multicast loops in Layer 2 switching configurations.ACLsSupports up to 384 entries. Drop or rate limitation based on: Source and destination MAC, VLAN ID or IP address, protocol, port, Differentiated services code point (DSCP) / IP precedence	Port Security	
RADIUS/ TACACS+Supports RADIUS and TACACS+ authentication. Switch as a clientStorm ControlPrevents traffic on a LAN from being disrupted by a broadcast, multicast, or unicast storm on a portDHCP SnoopingA feature acts as a firewall between untrusted hosts and trusted DHCP serversLoop ProtectionTo prevent unknown unicast, broadcast and multicast loops in Layer 2 switching configurations.Supports up to 384 entries. Drop or rate limitation based on: Source and destination MAC, VLAN ID or IP address, protocol, port, Differentiated services code point (DSCP) / IP precedence		address
RADIUS/ TACACS+Supports RADIUS and TACACS+ authentication. Switch as a clientStorm ControlPrevents traffic on a LAN from being disrupted by a broadcast, multicast, or unicast storm on a portDHCP SnoopingA feature acts as a firewall between untrusted hosts and trusted DHCP serversLoop ProtectionTo prevent unknown unicast, broadcast and multicast loops in Layer 2 switching configurations.Supports up to 384 entries. Drop or rate limitation based on: Source and destination MAC, VLAN ID or IP address, protocol, port, Differentiated services code point (DSCP) / IP precedence	IP Source Guard	Prevents illegal IP address from accessing to specific port in the switch
TACACS+Supports RADIUS and TACACS+ authentication. Switch as a clientStorm ControlPrevents traffic on a LAN from being disrupted by a broadcast, multicast, or unicast storm on a portDHCP SnoopingA feature acts as a firewall between untrusted hosts and trusted DHCP serversLoop ProtectionTo prevent unknown unicast, broadcast and multicast loops in Layer 2 switching configurations.Supports up to 384 entries. Drop or rate limitation based on: Source and destination MAC, VLAN ID or IP address, protocol, port, Differentiated services code point (DSCP) / IP precedence		5 5 1 1
Storm ControlPrevents traffic on a LAN from being disrupted by a broadcast, multicast, or unicast storm on a portDHCP SnoopingA feature acts as a firewall between untrusted hosts and trusted DHCP serversLoop ProtectionTo prevent unknown unicast, broadcast and multicast loops in Layer 2 switching configurations.Supports up to 384 entries. Drop or rate limitation based on: Source and destination MAC, VLAN ID or IP address, protocol, port, Differentiated services code point (DSCP) / IP precedence		Supports RADIUS and TACACS+ authentication. Switch as a client
Storm Control unicast storm on a port   DHCP Snooping A feature acts as a firewall between untrusted hosts and trusted DHCP servers   Loop Protection To prevent unknown unicast, broadcast and multicast loops in Layer 2 switching configurations.   Supports up to 384 entries. Drop or rate limitation based on: Source and destination MAC, VLAN ID or IP address, protocol, port, Differentiated services code point (DSCP) / IP precedence	TACACJT	Description of the second state of the second
DHCP Snooping A feature acts as a firewall between untrusted hosts and trusted DHCP servers   Loop Protection To prevent unknown unicast, broadcast and multicast loops in Layer 2 switching configurations.   Supports up to 384 entries. Drop or rate limitation based on: Source and destination MAC, VLAN ID or IP address, protocol, port, Differentiated services code point (DSCP) / IP precedence	Storm Control	
DHCP Snooping   servers     Loop Protection   To prevent unknown unicast, broadcast and multicast loops in Layer 2 switching configurations.     Supports up to 384 entries. Drop or rate limitation based on:   Source and destination MAC, VLAN ID or IP address, protocol, port, Differentiated services code point (DSCP) / IP precedence		
Loop Protection To prevent unknown unicast, broadcast and multicast loops in Layer 2 switching configurations.   Supports up to 384 entries. Drop or rate limitation based on:   Source and destination MAC, VLAN ID or IP address, protocol, port,   Differentiated services code point (DSCP) / IP precedence	DHCP Spooping	A teature acts as a tirewall between untrusted hosts and trusted DHCP
Loop Protection   switching configurations.     Supports up to 384 entries. Drop or rate limitation based on:   Source and destination MAC, VLAN ID or IP address, protocol, port,     Differentiated services code point (DSCP) / IP precedence   Differentiated services code point (DSCP) / IP precedence		
Supports up to 384 entries. Drop or rate limitation based on: Source and destination MAC, VLAN ID or IP address, protocol, port, Differentiated services code point (DSCP) / IP precedence	Loop Protoction	To prevent unknown unicast, broadcast and multicast loops in Layer 2
Source and destination MAC, VLAN ID or IP address, protocol, port, Differentiated services code point (DSCP) / IP precedence	Loop Holechon	switching configurations.
Source and destination MAC, VLAN ID or IP address, protocol, port, Differentiated services code point (DSCP) / IP precedence		
Differentiated services code point (DSCP) / IP precedence		
	ACLs	TCP/ UDP source and destination ports
		802.1p priority Ethernet type



	Internet Control Message Protocol (ICMP) packets TCP flag
	Quality of Service
Hardware Queue	Supports 8 hardware queues
Scheduling	Strict priority and weighted round-robin (WRR)
Jenedoning	Queue assignment based on DSCP and class of service
Classification	Port based
	802.1p VLAN priority based
D 1 1	Ingress policer
Rate Limiting	Egress shaping and rate control
	Per port
	Management Traffic on a port can be mirrored to another port for analysis with a network
Port Mirroring	analyzer or RMON probe. Up to N-1 (N is Switch's Ports) ports can be
1 OFF MILLOTING	mirrored to single destination port. A single session is supported.
	Used by network devices for advertising their identities, capabilities, and
IEEE 802.1ab	neighbors on an IEEE 802ab local area network
(LLDP)	Support LLDP-MED extensions
Web GUI Interface	Built-in switch configuration utility for browser-based device configuration
Dual Image	Independent primary and secondary images for backup while upgrading
0	The Universal Plug and Play Forum, an industry group of companies
UPnP	working to enable device-to-device interoperability by promoting Universal
	Plug and Play
DHCP Server	Support DHCP server to assign IP to DHCP clients
Remote Monitoring	Embedded RMON agent supports RMON groups 1,2,3,9 (history, statistics,
(RMON)	alarms, and events) for enhanced traffic management, monitoring and
	analysis
SNMP	SNMP version1, 2c and 3 with support for traps, and SNMP version 3 user-
519/9/1	based security model (USM)
	The industry standard for monitoring high speed switched networks. It gives
s-Flow(option)	complete visibility into the use of networks enabling performance
3-11000(0011011)	optimization, accounting/billing for usage, and defense against security
	threats
Firmware Upgrade	Web browser upgrade (HTTP/ HTTPs) and TFTP
NTP	Network Time Protocol (NTP) is a networking protocol for clock
	synchronization between computer systems over packet-switched
	HTTP/HTTPs
Other	DHCP Client
Management	Cable Diagnostics
	Syslog
	IPv6 Management Device Management System (DMS)
	Topology view: Support intuitive way to configure and manage switches and
	devices with visual relations
Graphical	Floor view: It's easy to drag and drop PoE devices and help you to build
Monitoring	smart workforces
	Map view: Enhance efficiency to drag and drop devices and monitor
	surroundings on google map



Find my Switch	Search your real switches quickly and manage directly.		
Traffic Monitoring	Display visual chart of network traffic of all devices and monitor every port at		
Induic Monitoring	any time from switches		
	Network diagnostic between master switch and devices		
Trouble Shooting	Support protection mechanism, such as rate-limiting to protect your devices		
	from brute-force downloading		