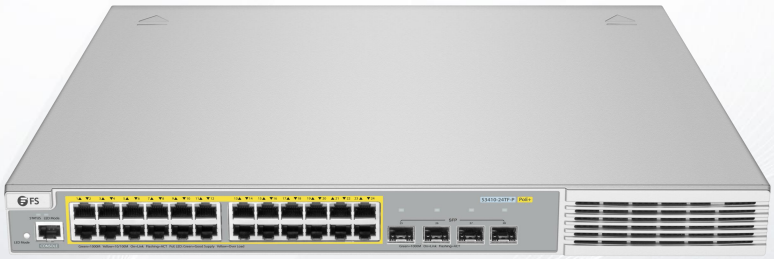
S3410-24TF-P Switch

HIGH PERFORMANCE WITH WIDE RANGE OF ROUTING PROTOCOLS FOR BUSINESS

S3410-24TF-P Switch is next-generation L2+ gigabit managed switch with 56Gbps switching capacity.



Overview

S3410-24TF-P is next-generation gigabit Ethernet switch. They support full gigabit downlink data exchange and 1G uplink data exchange. With the brand-new hardware architecture and FSOS, the S3410-24TF-P switch is capable of providing more resource entries, faster hardware processing, and better operation effects, thereby giving you a new experience. The switch also support a wide range of routing protocols, including static routing, Routing Information Protocol (RIP), and Open Shortest Path First (OSPF), which can fully meet requirements for convergence devices on networks of different scales.

Benefits

- Layer 2+ Switches
- BCM56152 Switch Chip
- Support up to 4 Units Stacking
- Industry-standard CLI & Web Management
- IPv4/IPv6 Dual-stack Multi-layer Switching
- Support VRRP, RLDP, REUP
- Green Ethernet, Energy Efficiency

Product Characteristics

Sound Security Protection Policies

Address Resolution Protocol (ARP) viruses or attacks are a type of common and influential network attack. The S3410-24TF-P switch supports ARP spoofing prevention in multiple modes. Regardless of whether clients automatically obtain addresses from the DHCP server or use static IP addresses, the S3410-24TF-P switch records clients' authentic IP+MAC addresses and compare addresses in ARP packets with recorded IP+MAC addresses when switch ports receive the ARP packets from hosts. The switches forward only ARP packets whose addresses match the recorded IP+MAC addresses and discard fake ARP packets. In this way, ARP spoofing is shielded outside the network and network users are protected from ARP virus attacks.

The S3410-24TF-P switch is capable of actively defending against various Distributed Denial of Service (DDoS) attacks on networks. Computers may be infected with viruses due to network openness or attackers may launch attacks on network devices and servers for various purposes, resulting in network unavailability. The common ARP flooding attacks can lead to the failure of the gateway to respond to requests. ICMP flooding attacks can paralyze network devices due to high CPU load. DHCP request flooding attacks deplete addresses of the DHCP server, and users cannot obtain IP addresses for network access.

The S3410-24TF-P switch provides an industry-leading hardware CPU protection mechanism: CPU Protect Policy (CPP). It classifies data traffic sent to the CPU, processes the traffic by queue priority, and limits the bandwidth rate as required. This protection mechanism fully protects the CPU against illegitimate traffic occupancy, malicious attacks, and resource consumption, thereby ensuring the CPU security and protecting the switches.

The S3410-24TF-P switch adopt the innovative Network Foundation Protection Policy (NFPP) technology to limit the rate of ARP packets, ICMP requests, DHCP requests, and other packets sent to networks. The switches discard packets whose rate exceeds the threshold, identify attack behaviors, and isolate users launching attacks. In this way, the basic networks are protected from network attacks, and therefore the network stability is guaranteed.

DHCP snooping enables the S3410-24TF-P switch to receive DHCP responses only from trusted ports and prevent spoofing from unauthorized DHCP servers. With DHCP snooping, the switches dynamically monitor ARP packets, check users' IP addresses, and discard illegitimate packets that do not match bound entries, thereby effectively preventing ARP spoofing and source IP address spoofing.

Multiple Service Features

Supports line-rate IPv4/IPv6 dual-stack multi-layer switching. Networks can be planned and designed based on IPv6 network requirements and the switches can be used to flexibly create IPv6 network communication solutions.

Support a wide range of IPv4 routing protocols, including static routing, RIP, and OSPF. Users can select appropriate routing protocols based on network environments, to flexibly build networks.

Support abundant IPv6 routing protocols, including static routing, Routing Information Protocol next generation (RIPng), and OSPFv3. A routing protocol can be selected flexibly to either upgrade the existing network to an IPv6 network or build a new IPv6 network.

Stacking

The S3410-24TF-P switch support the stacking, in which multiple physical devices are connected and virtualized into one logical device. The devices use the same IP address, Telnet process, and command line interface (CLI) for management and support automatic version check and automatic configuration. Users need to manage only this logical device to enjoy the work efficiency and use experience brought by multiple devices.

Simplified management: Administrators can manage multiple switches in a unified manner, with no need to connect to each switch for configuration and management

Simplified network topology: A stacking switch can connect to peripheral devices on a network through aggregate links. Therefore, no layer-2 loop exists and the Multiple Spanning Tree Protocol (MSTP) does not need to be configured.

Fault recovery within milliseconds: A stacking switch connects to peripheral devices through aggregate links. If one device or member link in the stacking malfunctions, data and services can be switched to another member link within only 50–200 milliseconds.

High scalability: User devices can be added to or removed from a virtualized network in a "hot swap" manner, without affecting normal operation of other devices.

Increase in return on investment: Aggregate links used for connecting the stacking switche to peripheral devices not only provide redundancy links but also implement load balancing. All network devices and bandwidth resources are fully leveraged. Any 10G port can be used to build a stacking network through data transmission cables. No additional cables and expansion cards are required, and the types of ports and cables are not limited. Therefore, the return on investment is maximized.

High Reliability

Support Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), and MSTP. They help the S3910-48TF switch achieveS fast convergence, improve the fault tolerance capability, and ensure stable network operation and load balance of links. The switches utilize network channels appropriately to raise the utilization of redundant links.

Support the Virtual Router Redundancy Protocol (VRRP), it helps the switches effectively ensure the network stability.

Support the Rapid Link Detection Protocol (RLDP), the switches can quickly detect the link connectivity and unidirectional optical fiber links. The port loop detection function helps the switches prevent network failures caused by loops resulting from unauthorized port connection to hubs.

Support REUP. When STP is disabled, the Rapid Ethernet Uplink Protection Protocol (REUP) can still provide basic link redundancy and millisecond-level fault recovery faster than STP.

Easy Network Maintenance

The S3410-24TF-P switch supports the Simple Network Management Protocol (SNMP), Remote Network Monitoring (RMON), log and configuration backup using USB flash drives, and Syslog for routine network diagnosis and maintenance. Administrators can also use CLI, Web-based management, telnet, and other methods to manage and maintain devices conveniently.

Technical Specification

S3910-48TF switch comes with full gigabit downlink data exchange and 1G uplink data exchange. Here's a look at the details.

CHARACTERISTICS

	S3410-24TF-P
Ports	
10/100/1000BASE-T RJ45	24
1G/10G SFP+	4
Console Port	1
Operating System	
OS	FSOS
Key Components	
Switch Chip	BCM56152
CPU	ARM A9 Single-Core CPU, 800 MHz
Performance	
Layer Type	Layer 2+
Switching Capacity	56 Gbps
Forwarding Rate	42 Mpps
Flash Memory	256MB
SDRAM	512MB
Packet Buffer	1.5MB
Jumbo Frame	9216
Stackability	Up to 4 Units
MAC Address	16K
Number of VLANs	4K
Switch Method	Storage and forward
MTBF (Hours)	>200K
Authentication Methods	802.1X, AAA

	S3410-24TF-P
ARP Table	500
Remote Management	SNMP V1/V2/V3, RMON, Syslog
Status Indicators	Status
Power	
Max. Power Consumption	432W
Input Voltage	100VAC~240VAC, 50~60Hz
Physical and Environmental	
Dimensions (HxWxD)	1.73"x17.32"x10.24" (44××440×260mm)
Rack Space	1U
Power Devices	1 Built-in Power Supply
Fan Number	1 Built-in Fan
Operating Humidity	10% to 90% (Non-condensing)
Storage Humidity	5% to 95% (Non-condensing)
Operating Temperature	32°F to 122°F (0ºC to 50ºC)
Storage Temperature	40°F to 158°F (-40ºC to 70º)
Temperature Alarm	Support

FEATURES

Functionality	Description
MAC Address Table	• Static MAC addresses • MAC address filtering
802.1Q VLAN	• 4K 802.1Q VLAN • Port-based VLAN • MAC-based VLAN • Protocol-based VLAN • Private VLAN • Voice VLAN • Private VLAN • IP subnet-based VLAN • GVRP
QinQ	• Basic QinQ • Flexible QinQ
Port Mirroring	• One-to-one mirroring, many-to-one mirroring, one-to-many mirroring • RSPAN, ERSPAN • Flow-based mirroring
ACL	• Standard IP ACLs (IP-based hardware ACLs) • Extended IP ACLs (hardware ACLs based on IP addresses or TCP/UDP port IDs) • MAC-based extended ACLs (hardware ACLs based on source MAC addresses, destination MAC addresses, and optional Ethernet type) • Time-based ACLs • Expert-level ACLs (hardware ACLs based on flexible combinations of the VLAN ID, Ethernet type, MAC address, IP address, TCP/UDP port ID, protocol type, and time) • ACL 80 • IPv6 ACLs • Global ACLs • ACL redirection

FEATURES

Functionality	Description
QoS	• Port traffic identification • Port traffic rate limiting • 802.1p/DSCP/ToS traffic classification • Eight priority queues per port • SP, WRR, DRR, SP+WRR, SP+DRR, RED/WRED queue scheduling mechanisms
DHCP	• DHCP server • DHCP client • DHCP snooping • DHCP relay • IPv6 DHCP snooping • IPv6 DHCP client • IPv6 DHCP relay
Security Features	• 3-tuple binding (IP address, MAC address, and port) • 3-tuple binding (IPv6 address, MAC address, and port) • Filtering of invalid MAC addresses • Port- and MAC-based 802.1x authentication • MAB authentication • Portal authentication and Portal 2.0 authentication • Gateway ARP spoofing prevention • Broadcast storm suppression • Hierarchical management of administrators and password protection • RADIUS and TACAS+ • AAA (IPv4/IPv6) for device login management • SSH and SSH V2.0 • BPDU guard • CPP, NFPP • Port protection
Port Sleeping	• Support
IP Routing	• IPv4/IPv6 Static routing • RIP, RIPng, OSPFv2, OSPFv3 • Routing Policy

FEATURES

Functionality	Description
IPv6 Basic Protocols	• IPv6 addressing, Neighbor Discovery (ND), ICMPv6, IPv6 ping, IPv6 Tracert
Management Features	• SNMP, CLI (telnet/console), RMON, SSH, Syslog, NTP/SNTP, FTP, TFTP, Web
Power Supply	• AC input: • Rated voltage range: 100-240V, 50-60Hz • Maximum voltage range: 90-264V, 50-60Hz • Rated current: 1.5A • HVDC input: • Rated voltage range: 240V • Maximum voltage range: 192-288V • Rated current: 1.5A • DC input: • Rated voltage range: -36~-72V • Rated current: 3.15A

https://www.fs.com

The information in this document is subject to change without notice. FS has made all efforts to ensure the accuracy of the information, but all information in this document does not constitute any kind of warranty.