H3C S5510 Series Ethernet Switches

Product Overview

H3C S5510 Series Ethernet Switches (the S5510 series) are wire speed L2/L3 Ethernet switches developed by Huawei-3Com Technologies. They are intelligent network management switches intended for a network environment where high performance, dense port distribution, and ease of installation are required.

The S5510 series are designed to accommodate the convergence on intranets and metropolitan area networks (MANs) and to meet the requirements at the access layer. Supporting IPv4/IPv6 double stack, they offer abundant service features and routing functionalities.

The S5510 series Ethernet Switches include the following models: S5510-24P and S5510-24F.

S5510-24P

S5510-24F

Key Features and Benefits

➢ **Comprehensive Support to IPv6-Protect customer's investment effectively**

Based on IPv4/IPv6 double stack, the H3C S5510 series can support various IPv6 features comprehensively, which makes them adapt well to IPv4 -only、IPv6 -only and hybrid networks.

■ Abundant IPv6 routing protocols

Except Neighbor Discovery Protocol (NDP) and Path Maximum Transport Unit (PMTU), the H3C S5510 series also support abundant IPv6 routing protocols, mainly including:

● BGP4+

BGP4+ provides support for IPv6 by mapping IPv6 network layer protocol information to the NLRI (network layer reachable information) and Next Hop attributes.

BGP4+ adds two attributes to support IPv6, they are MP_REACH_NLRI

(multi-protocol reachable NLRI), and MP_UNREACH_NLRI (multi-protocol unreachable NLRI).

- IS-IS v6

  Pv6-capable IS-IS is known as IS-ISv6 dynamic routing protocol, which adds two type-length-values (TLVs) (IPv6 Reachability and IPv6 Interface Address) and a new network layer protocol identifier (NLPID) to support IPv6.

- OSPFv3

OSPFv3 provides support for IPv6, and is different from OSPFv2 in that:

- OSPFv3 is link-based, while OSPFv2 is network-based.
- OSPFv3 allows multiple instances on the same link.
- OPSFv3 identifies neighbors by router ID. OSPFv2, however, identifies neighbors by IP address.

- RIPng

  RIP next generation (RIPng) is enhanced RIP-2.

  Compared with RIP, the following are new in RIPng, which enable it to be implemented in an IPv6 network.

- Port 521 is used to send and receive routing information.
- The prefix (also the mask) is 128 bits in length.
- The next hop address is IPv6 address, which is 128 bits in length.

Based on these routing protocols, S5510 series Ethernet Switches can support IPv4-only、IPv6 -only and hybrid networks, which is more cost-saving and cost-effective for customers.

■ IPv6 over IPv4 tunnel

IPv6 tunneling is to encapsulate IPv6 traffic within IPv4 packets so that IPv6 packets can be transmitted over IPv4 network, which allows isolated IPv6 networks to intercommunication.

The H3C S5510 series support all main IPv6 tunnels,including:

- 6to4 tunnel

  A 6to4 tunnel is a point-to-multipoint automatic tunnel that allows isolated IPv6 domains to be connected over an IPv4 network to remote IPv6 networks. 6to4 tunneling allows the tunnel endpoint to be determined automatically by the IPv4 address concatenated to the destination address of an IPv6 packet. A 6to4 tunnel employs special addresses: 6to4 IPv6 addresses that are in the format of 2002:a.b.c.d: subnet number::interface ID/64, where a.b.c.d represents an IPv4 address. The concatenated IPv4 address determines the tunnel endpoint automatically. This allows for convenient IPv6 channel establishment.

- ISATAP tunnel

  Intra-site automatic tunneling protocol (ISATAP) provides a solution for an increasing number of IPv6 hosts running on existing IPv4 networks as the IPv6 technology becomes more and more popularized. ISATAP is a point-to-point automatic tunneling technology that allows the tunnel endpoint to be determined automatically by the IPv4 address concatenated in the destination address of an IPv6 packet. For ISATAP tunneling, the destination address of the IPv6 packet and the IPv6 address of the tunnel interface must be expressed as special

addresses: ISATAP addresses that are in the format of Prefix (64bit)::5EFE:IPv4-Address. A tunnel can be established automatically by the concatenated IPv4 address for forwarding IPv6 packets. An ISATAP tunnel is primarily used in an IPv4 network for connectivity between IPv6 routers and between a host and an IPv6 router.

- IPv4 compatible tunnel

  Both ends of an IPv4-compatible channel use special IPv6 addresses, namely, IPv4-compatible IPv6 addresses. These addresses are in the format of 0:0:0:0:0:0:a.b.c.d/96, where a.b.c.d represents an IPv4 address. The concatenated IPv4 address determines the tunnel endpoint automatically. This allows for convenient IPv6 channel establishment. However, the function of an IPv4 compatible tunnel is restricted because it must use IPv4-compatible IPv6 addresses, which are IPv4-based.

- Manually configured tunnel

  A manually configured tunnel is a point-to-point link. Each link is an independent tunnel. Manually configured tunnels are primarily used for stable connections that require regular secure communication between two edge routers or between a host and an edge router, or for connection to remote IPv6 networks.

Through these tunnels, S5510 series Ethernet Switches provide the packet transition capability from IPv4-only networks to integrated IPv4- and IPv6-based networks, which protects customer's investment in network very well, and makes customer's network can not only adapt present internet condition, but also meet future internet development requirements.

■ Multicast

- IGMP Snooping

  Internet group management protocol snooping (IGMP Snooping) provides a mechanism to manage and control multicast groups. When IGMP Snooping is not enabled, multicast packets are broadcast on Layer 2. While when IGMP Snooping is enabled, the packets are multicast instead of being broadcast on Layer 2.

- IGMPv1/v2/v3

  Internet group management protocol (IGMP) manages the members of an IP multicast group by establishing and maintaining the multicast membership between IP hosts and the directly connected multicast routers.

- PIM-DM/SM

  Protocol independent multicast, dense mode (PIM-DM) is a multicast routing protocol suitable for small-sized networks where multicast group members are relatively dense.

  Protocol Independent Multicast, Sparse Mode (PIM-SM) is a multicast routing protocol mainly used in large-scaled networks where group members are scattered sparsely.

- Multicast Source Discovery Protocol

  Multicast Source Discovery Protocol (MSDP) is used to discover multicast

source information in other PIM-SM domains. MSDP is significant to the Any-Source Multicast (ASM) model only.

- MLDv1 snooping

  Multicast listener discovery (MLD) is an IPv6 protocol responsible for managing multicast members. It is used to establish and maintain multicast group membership between hosts and the neighboring multicast routers directly connected to them.

■ IPv6 ACL

The H3C S5510 series support traffic classification based on source IPv6 address, destination IPv6 address, Layer 4 port, protocol type, and so on.

- Numeric basic IPv6 ACLs

  Rules are defined based on Lay 3 source IPv6 address. The value range for basic IPv6 ACL numbers is 2000 to 2999.

- Numeric advanced IPv6 ACLs

  Rules are defined based on L3 source IP address, destination IP address, source port, and destination port. The value range for numeric advanced IPv6 ACL numbers is 3000 to 3999.

■ VRRP v3

VRRP is a fault-tolerant protocol that can improve the reliability of the connection between a router and an external network by providing a backup mechanism.

VRRP ensures reliability by assigning the routers on a LAN segment to a standby group. In this group, there always exists a Master router to complete the task of virtual router. All other routers in the group serve as Backup to monitor the Master all the time. When the Master fails to work, the Backups will elect a new Master automatically to provide routing services for the hosts on the network segment.

■ IPv6 applications

The H3C S5510 series support a range of IPv6 applications on IPv6 network, such as Ping IPv6, Tracert IPv6,IPv6 telnet and IPv6 TFTP.

➢ **Excellent Service Deployment and Guarantee Capability—Boost customer's network usability and security greatly**

■ Strong Multicast Capabilities (supporting IPv4/IPv6 multicast)

H3C S5510 Series support abundant IPv4 and IPv6 multicast features, including:

- IGMP Snooping
- IGMPv1/v2/v3
- PIM-DM/SM
- Multicast Source Discovery Protocol

Through these features above, S5510 series can greatly save customer's network bandwidth, and enable customer to deploy a wide range of key network services.

■ VLAN VPN (QinQ, Selective QinQ)/VLAN Translation Functionalities

VLAN VPN enables VLAN Tags of private networks to be inserted in those of the public networks so that the packets can travel across carrier's network (public network) with nested VLAN tags carried. VLAN VPN is also known as QinQ. When a packet of this type travels across the public network, only the outer VLAN Tag (that is,

the public network VLAN Tag) is used and that of the private network remains intact.

Compared with MPLS-based L2 VPN, VLAN VPN has the following features:

- It provides simpler L2 VPN tunnels.
- It can be implemented through full-static configuration, without the need of a signaling protocol.

Selective QinQ is also known as VLAN-based QinQ. It determines whether or not an outer VLAN tag is inserted into a packet on the user side. It also determines the outer VLAN tag to be inserted into a packet by the VLAN tag the packet carries.

VLAN Translation, also known as VLAN mapping or VLAN switch, is mainly used in L2 networks. A switch with VLAN translation enabled can translate the VLAN IDs carried in the data packets it receives from private networks into those used in the carrier's network.

On the basis of mighty VLAN features, on one hand, H3C S5510 series are more cost-saving and cost effective for customer, since based on H3C S5510 series powerful VLAN features, customer can design and divide their network at random according to their current and future needs without purchasing more network devices. On the other hand, H3C S5510 series provide customer with great flexibility to deploy various key network applications based on VLAN, such as internet access and Video on Demand, and excellent network expandability for future growth.

■ Diverse QoS/ACL Functionalities

H3C S5510 series support powerful ACL features, including:

- Numeric basic ACLs

  Rules are defined based on L3 source IP address only. The value range for numeric basic ACL numbers is 2000 to 2999.

- Numeric advanced ACLs

  Rules are defined based on L3 source IP address, destination IP address, source port, and destination port. The value range for numeric advanced ACL numbers is 3000 to 3999.

- Numeric L2 ACLs

  Rules are defined based on protocol type, 802.1p priority, source MAC address, and destination MAC address. The value range for numeric L2 ACL numbers is 4000 to 4999.

- Numeric user-defined ACLs

  A user-defined ACL performs a match on any byte of the first 80 bytes in a L2 data packet and then the packet is processed accordingly. The value range for numeric user-defined ACL numbers is 5000 to 5999.

H3C S5510 series supports the following two types of ACL flow templates:

- User-defined flow templates, which are used to in combination to implement user-defined ACLs.
- Default flow templates, which contain basic fields except user-defined ACLs.

Through these ACLS, H3C S5510 series can screen a wide range of invalid and cantankerous accesses to protected customer’s network and greatly enhancing customer’s networks security,

H3C S5510 series Ethernet Switches also support diverse QoS features, including:

- Flow-based traffic rate limit

By issuing the corresponding command, Customer can configure a flow-based traffic rate limit that limits the mean rate, peak rate, burst size, maximum burst size, priority of traffic not exceeding the threshold, and the priority of excessive traffic of a specific flow. This prevents a data flow from occupying all system bandwidth, thus avoiding data flow congestion.

- Flow-based priority tag

This feature enables the switch to automatically set IP priority, differentiated services codepoint priority (DSCP) priority, 802.1P priority, and discard priority for the data based on the type of flow entering the port, so that a specific type of data is processed in preference to others.

- Flow-based packet VLAN ID change

Customer can configure the switch to change the VLAN ID of the specified type of incoming data packets, so as to implement VLAN-based packet redirection.

- Flow-based redirection of packets to another port or IP next hop

This feature enables the switch to redirect incoming packets to another port or IP next hop based on the flow type of these packets. The S5510 series support packet redirection to IPv4 next hop and IPv6 next hop.

- Flow-based traffic statistics

The switch can implement the traffic statistics feature on a port to take statistics of the specified type of incoming/outgoing flows that exceed or do not exceed the traffic limit.

- Flow-based traffic mirroring

Customer can configure the switch to mirror the specified type of traffic to another port so that Customer can monitor and manage the data on the network by using a traffic monitoring tool.

- Port-based queue scheduling

Queue scheduling addresses the resource contention when the switch forwards multiple packets. There are three queue scheduling algorithms: Strict Priority (SP) and Weighted Round Robin (WRR). Algorithms forward the packets in the egress queues in their own principles.

- Port mirroring and RSPAN

Port mirroring is used to copy the data on the monitored port to the specified monitoring port for data analysis and monitoring.

Remote switched port analyzer (RSPAN) implements remote port mirroring. It allows the mirrored port and the mirroring port to be configured on different switches.

- Port-based and queue-based traffic shaping

Traffic shaping is used to control traffic output rate so that packets are output at an even rate.

- Port-based congestion avoidance

When congestion occurs, the switch releases queue resources by dropping packets, while avoiding putting packets in high-delay queues, thereby eliminating the congestion.

- **High Security and Reliability -Guarantee customer's network secruity and stability highly**

H3C S5510 series provide overall measures to meet customer's requirements for security, mainly including:

- Hierarchical management and password protection of users: S5510 series divide command lines into four levels: visitor, monitor, operator, and administrator, in ascending order, which ensure different users get only their designated privileges.
- IEEE 802.1X compliant access user authentication can control the connected customer premises equipment (CPE) at the port level. In implementing 802.1X, the S5510 series not only support the port-based access authentication, but also extends and optimizes it by:
  - Allowing a physical port to be connected to several terminals
  - Supporting access control (namely, user authentication) based on MAC address in addition to port
  - Binding the MAC address and IP address of an authenticated user host to a VLAN.
  - This greatly enhances the security, operability and manageability of the system.
- AAA and RADIUS authentication
- HWtacacs+: primarily implements AAA for multiple types of users in the server/client mode. It can be used to authenticate, authorize, and account PPP and VPDN access users and login users.

  Besides, HWTACACS implements more reliable transmission and encryption than RADIUS and therefore is more suitable for security control.
- MAC-based centralized authentication maintains a table of user MAC addresses. Upon detecting a new user (by examining the source MAC address of the packets), the switch enabled with this function carries the MAC address as the username and password for authenticating the new user. If a match is found, the MAC address is added to the corresponding port. This means the user is authenticated. If no match is found, the packet is discarded and user authentication fails.
- Port isolation means isolation of the ports of a switch so that packets cannot be forwarded between a port and another port (or another group of ports). This prevents visiting between the ports, secures user network, and allows a low-cost intelligent community network to be built while effectively controlling unnecessary broadcasting and increasing the network throughput.
- IP + MAC + port binding

  You can configure IPv4 addresses, MAC addresses, and port binding on the S5510 series. If the IP address or MAC address bound to a port is changed, no packet with that MAC address or IP address can be forwarded through the port.

- VRPP: VRRP is a fault-tolerant protocol that can improve the reliability of the connection between a router and an external network. VRRP ensures reliability by assigning the routers on a LAN segment to a standby group. In this group, there always exists a Master router to complete the task of virtual router. All other routers in the group serve as Backup to monitor the Master all the time. When the Master fails to work, the Backups will elect a new Master automatically to provide routing services for the hosts on the network segment.
- S5510 series support both VRPP v2 and V3, which are based on IPv4 and IPv6 respectively.
- Two power supply modules: allows for power load balancing and redundant backup.

➢ **Full-Gigabit Access and Hardware Forwarding –Improve customer's network performance greatly**

At speeds of 1000 Mbps, Gigabit access port provides the bandwidth to meet new and evolving network demands, alleviate bottlenecks, and boost performance while increasing the return on existing infrastructure investments. Today's workers are placing higher demands on networks, running multiple, concurrent applications. For example, a worker joins a team conference call through an IP videoconference, sends a 10-MB spreadsheet to meeting participants, broadcasts the latest marketing video for the team to evaluate, and queries the customer-relationship-management database for the latest real-time feedback.

The H3C S5510 series provide full-Gigabit electrical and SFP ports, which guarantee sufficient access bandwidth and service quality of bandwidth-intensive and time-sensitive network applications.

In addition, H3C S5510 series also support hardware forwarding, which breaks through the bottle-neck of performance and thus greatly improving customer's network performance.

➢ **Superior Manageability and Maintainability –Reduce customer deployment and maintenance cost sharply**

The H3C S5510 series provide various simple and effective methods to faciltate customer to manage and maintain network.

- Supporting SNMP: Simple Network Management Protocol (SNMP) is currently the most widely used network management protocol. It adopts a polling mechanism and offers an underlying function set, which is suitable for a networking environment requiring a small size, high speed, and low cost.
- Supporting RMON: RMON is implemented on the basis of the SNMP architecture and compatible with the current SNMP framework, requiring no modification to the protocol. RMON enables SNMP to monitor remote network devices more effective and actively. This provides a means of high-efficient monitoring of subnet operation. Additionally, RMON can also reduce the traffic between the network management station and agents, thereby allowing for simple and yet powerful management of large-scale internets.
- Supporting HGMPv2:

HGMPv2 has the following advantages:

- It simplifies configuration and management.
- It enables topology discovery and display, which facilitates network monitoring and debugging.
- It allows customer to upgrade software and configure parameters on multiple switches at the same time.
- It does not depend on network topology or distance.
- It saves IP address.

- Supporting Virtual Cable Test (VCT): With this way, Customer can conveniently test whether a cable is short circuited or open and test the length of faulty portion of the cable, so as to locate the network fault.
- Supporting Secure Shell (SSH): SSH offers security protection and powerful authentication function to safeguard the router from attacks such as IP address spoofing and plain text cipher interception when a user logs in to a router from an insecure network.

In addition, S5510 series also support Network Time Protocol (NTP), Debug Information Output, Ping and Tracert Command, HWPing. These ways provide powerful support to customer to administrate and monitor network, as well to facilitate customer to diagnose network fault quickly and conveniently.

Specifications

Port Configuration	S5510-24P	S5510-24F
Fixed ports	(1) 24 × 10/100/1000 Mbps electrical ports (2) 1 console port	(1) 24 Gigabit SFP ports (2) 1 console port
Extended Ports	4 Gigabit SFP ports (Combo)	4 × 10/100/1,000 Mbps electrical ports (Combo)
Extended Module	None	None

Software Features

Feature	S5510-24P/24F
Wire speed L2/L3 forwarding	Switching capacity: 48 Gbps Packet forwarding rate: 35.71 Mpps
Link Aggregation	Supports aggregation of Fast Ethernet (FE) ports Supports aggregation of Gigabit Ethernet (GE) ports Supports link aggregation control protocol (LACP) Supports manual link aggregation

MAC address	Supports 12 K MAC addresses Supports MAC address black hole Supports MAC address learning limit
Port	Supports IEEE 802.3x flow control (full-duplex) Supports Back-pressure based flow control (half duplex) Supports port-based broadcast suppression Supports port priority settings
VLAN	Supports port-based VLANs (4,094 VLANs) Supports protocol-based VLANs Supports VLANs based on IPv4 subnets Supports voice VLANs Supports GVRP/GARP Supports VLAN VPN (QinQ, Selective QinQ) and BPDU tunnel Supports VLAN Translation
DHCP	Supports DHCP Server Supports DHCP-Relay Supports DHCP Client Supports DHCP Snooping
UDP Helper	Supports UDP Helper
DNS	Supports static domain name resolution Supports dynamic DNS client Supports IPv4 addresses and IPv6 addresses
ARP	Supports ARP Supports gratuitous ARP Supports ARP Proxy
IP routing	Supports static route and default route Supports Routing Information Protocol (RIP) v1/v2 Supports RIPng Supports Open Shortest Path First (OSPF) v1/v2 Supports OSPFv3 Supports IS-IS Supports IS-ISv6 Supports Border Gateway Protocol (BGP) Supports for BGP4+ for IPV6 Supports equivalent route Supports routing policy

Multicast	Supports Internet Group Management Protocol (IGMP) Snooping Supports IGMPv1/v2/v3 Supports Protocol Independent Multicast-Dense Mode (PIM-DM) Supports Protocol Independent Multicast-Sparse Mode (PIM-SM) Supports Multicast Source Discovery Protocol (MSDP) Supports MLD Snooping	
STP/RSTP/MSTP	Supports STP/RSTP Supports MSTP Supports STP protection	
RRPP	Supports Rapid Ring Protection Protocol (RRPP)	
IPV6	Supports Neighbor Discovery (ND) Supports PMTU Supports IPv6 Ping and IPv6 Tracert Supports IPv6 Telnet Supports IPv6 TFTP	
IPv6 over IPv4 Tunnel	Supports manual Tunnel configuration Supports 6to4 tunnel Supports ISATAP tunnel Supports Auto-tunnel (namely, IPv4 compatible tunnel)	
QoS/ACL	Supporting ACLs	• Supports traffic classification based on source MAC address, destination MAC address, source IP address, destination IP address, Layer 4 port, protocol type, VLAN, and so on • Supports basic ACL • Supports advanced ACL • Supports L2 ACL • Supports user-defined ACL
	Supports ACL flow template	• Supports user-defined flow template • Supports default flow template

	Supporting QoS	• Flow-based traffic rate limit • Supports flow-based priority tag • Flow-based packet VLAN ID change • Flow-based redirection of packets to another port or IP next hop • Flow-based traffic statistics • Flow-based traffic mirroring • Supports SP/WRR/SP+WRR queue scheduling • Supports port mirroring and RSPAN (remote port mirroring) • Supports port traffic shaping • Supports congestion avoidance and drop policies
	Supporting IPv6 ACLs	• Supports traffic classification based on source IPv6 address, destination IPv6 address, Layer 4 port, protocol type, and so on • Supports basic IPv6 ACL • Supports advanced IPv6 ACL
	Supports Time Range	
	Supports Routing Policy	
Security Features	• Supports hierarchical management and password protection of users • Supports IEEE 802.1X authentication • Supports AAA • Supports RADIUS authentication • Supports HWTACACS+ • Supports centralized MAC address based authentication • Supports port isolation • Supports IP + MAC + port binding	
Reliability	Supports Virtual Redundancy Routing Protocol (VRRP)	
Loading and upgrade	• Supports loading and upgrade through XModem protocol • Supports loading and upgrade through file transfer protocol (FTP) • Supports loading and upgrade through trivial file transfer protocol (TFTP)	

Management	• Supports configuration through the Command line interface (CLI) • Supports configuration through Telnet • Supports configuration through Console port • Supports Simple Network Management Protocol (SNMP) v1/v2c/v3 • Supports Remote Monitoring (RMON) 1/2/3/9 groups of MIBs • Supports Huawei QuidView NMS • Supports Web-based network management • Supports system log • Supports hierarchical alarms • Supports Huawei Group Management Protocol (HGMP) v2 • Supports remote dialing through modem • Supporting NTP • Supporting SSH • Supports power supply status detection and alarms
Maintenance	• Supporting Debugging Information Output • Supports PING and Tracert • Supporting HWPing • Supports remote maintenance through Telnet • Supports Virtual Cable Test

Hardware Features

Dimensions (HxWxD)	43.6 × 440 × 360 mm (1.7 × 17.3 × 11.8 in.)
Weight	<5 kg (11 lb.) per switch without power modules <1 kg (2.2 lb) per power module
Input Voltage	The S5510 series can be AC-powered or DC-powered. AC: Rated voltage range: 100 VAC to 240 VAC; 50 Hz or 60 Hz Max voltage range: 90 VAC to 264 VAC; 50 Hz or 60 Hz DC: Rated voltage range: -48 V to -60 V Max voltage range: -36 V to -72 V
Maximum System Power Consumption	S5524P-AC/S5524P-DC: 80W S5524F-AC/S5524F-DC: 75W
Operating temperature	0°C to 45°C (32°F to 113°F)
Relative humidity (noncondensing)	10% to 90%

Industry standards support

- **Ethernet Protocols**

IEEE 802.1D (STP)

IEEE 802.1p (CoS)

IEEE 802.1Q (VLANs)

IEEE 802.1s (MSTP)

IEEE 802.1W (RSTP)

IEEE 802.1Q (GVRP)

IEEE 802.1X (Security)

IEEE 802.3i (10BASE-T)

IEEE 802.3u (Fast Ethernet)

IEEE 802.3x (Flow Control)

IEEE 802.3z (Gigabit Ethernet)

IEEE 802.3ad (Link Aggregation)

IEEE802.3p (four levels of priority)

IEEE 802.3ac (VLAN Tag Frame Extension **)**

- **Administration Protocols**

RFC 1812 (IPv4)

RFC 2460 (IPv6)

RFC 826 (ARP)

RFC 959 (FTP)

RFC 783 (TFTP)

RFC 768 (UDP)

RFC 791 (IP)

RFC 792 (ICMP)

RFC 793 (TCP)

RFC 2461 (Neighbor Discovery for IPv6)

RFC 2463 (ICMPv6)

RFC 1981 (Path MTU)

RFC 2622 (Routing policy)

RFC 2474 (Diffserv)

RFC 2131 (DHCP)

RFC 1058 (RIPv1)

RFC1723 (RIPv2)

RFC2080 (RIPng)

RFC 2328 (OSPF v2)

RFC 2740 (OSPF v3)

RFC 2370 (OSPF Opaque LSA Option)

RFC 1587 (OSPF NSSA option)

RFC 1765 (OSPF Database Overflow)

RFC 1771(BGP-4)

RFC 1142 (IS-IS)

RFC 2338 (VRRP)

RFC 2362 (PIM-SM)

RFC 1112 (IGMPv1)

RFC 2236 (IGMPv2)

RFC 3376 (IGMPv3)

RFC 3618 (MSDP)

RFC 2865 (Radius Authentication)

RFC 2866 (Radius Accounting)

RFC 2869 (RADIUS Extensions)

RFC 2267 (Network Ingress Filtering)

RFC 1157 (SNMP)

RFC 1902 (SNMPv2)

RFC 854 (Telnet)

RFC 896 (Congestion control in IP/TCP network)

RFC 925 (Multi-LAN ARP/Proxy ARP)

RFC 1122 (Requirements for Internet Hosts)

RFC 1156 (TCP/IP MIB)

RFC 1212 (Concise MIB definitions)

RFC 1213 (MIB for Network Management of TCP/IP based internets (MIB II))

RFC 1757 (RMON (groups 1 2 3 and 9))

RFC 1901 (Community based SNMPv2)

RFC 2573 (SNMPv3 Applications)

RFC 2576 (Coexistence between SNMP V1, V2, V3)

RFC 2597 (Assured Forwarding PHB group (partial support))

RFC 2618 (Radius Authentication Client MIB)

RFC 2620 (Radius Accounting MIB)

RFC 2819 (Remote Network Monitoring MIB (group 1,2,3,9))

RFC 2865 (Remote Authentication Dial In User Service)

RFC 2869bis (Radius Support for Extensible Authentication Protocol (EAP))

RFC 2932IP (Multicast Routing MIB)

RFC 3046 (DHCP/BootP Relay)

Safety and Compliance

- **Emissions / Agency Approvals**

CISPR 22 Class A

FCC Part 15 Class A

EN 55022 Class A

ICES -003 Class A

VCCI Class A

AS/NZS CISPR22 Class A

EN 61000-3-2

EN 61000-3-3

- **Immunity**

Product conforms to:

EN 55024: 1998

EN 61000-4-2

EN 61000-4-3

EN 61000-4-4

EN 61000-4-5

EN 61000-4-6

EN 61000-4-11

- **Safety Agency Certifications**

UL 60950-1:2003
IEC 60950-1: 2001
EN 60950-1: 2001
EN60825-1:1993+A1:1997 and EN60825-2:2000
AS/NZS 3260
CSA C22.2 No 60950-1:2003

Typical Applications

Application 1 : Broadband Ethernet Access for Residential Community

S5510 series Ethernet switches can operate on the distribution layer of a broadband MAN. You can connect it to a backbone router or Layer 3 switch in the uplink direction through its GigabitEthernet optical ports, and connect it to Layer 2/Layer 3 devices operating as the portal devices of community networks through its GigabitEthernet optical ports. Additionally, you can use multiple GigabitEthernet ports to form GigabitEthernet trunk ports so as to broaden the uplink and downlink bandwidth.

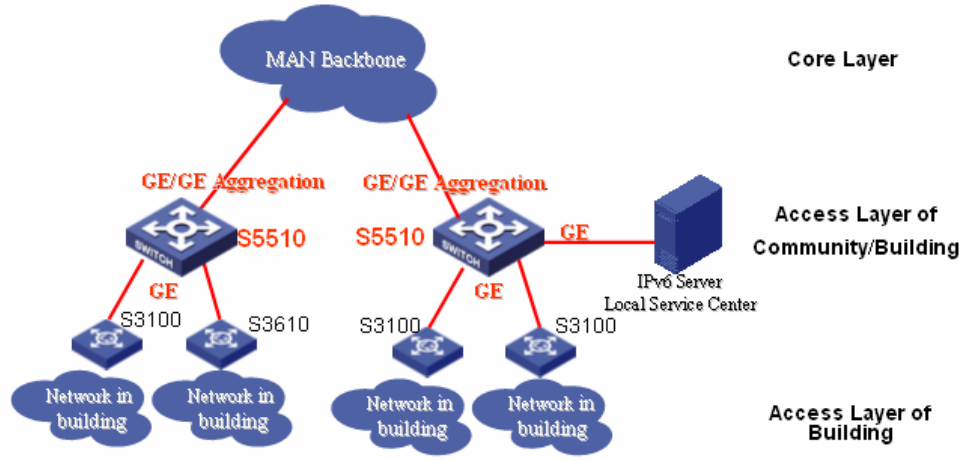

Figure 1-1 Network diagram for using S5510 series Ethernet switches in broadband MAN

Application 2: Application in Networks of Branches or Small/Medium-Sized and Large Enterprises

In the branches of a small-/medium-sized or large enterprises, you can use S5510 series Ethernet switches as the backbone layer devices. In this case, network devices can connect to an S5510 Ethernet switch in the following ways.

- Connecting the Layer 2/Layer 3 Ethernet switches (such as S3026/3526 Ethernet switches) of workgroups to GigabitEthernet optical ports or electrical interfaces
- Connecting to the other floors/buildings through long-/short-haul GigabitEthernet optical ports
- Connecting to the server directly through GigabitEthernet/100 Mbps electrical ports or connecting to the server group through the Layer 2/Layer 3 Ethernet switches in the workgroup through GigabitEthernet/100 Mbps electrical ports
- Connecting to routers through 10/100 Mbps electrical ports

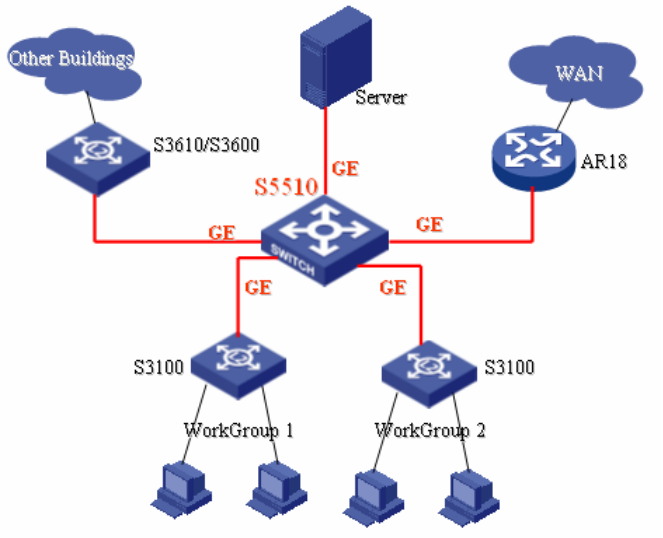

Figure 1-2 Using S5510 series Ethernet switches in networks of small-/medium-sized and large enterprises

Application 3: S5510 series application in large enterprise and campus network

S5510 series Ethernet switches can operate as the distribution layer devices in the networks of large enterprises and campus networks. In this case, you can connect an S5510 Ethernet switch to a backbone router or Layer 3 switches through its GigabitEthernet optical ports or electrical ports, and connect Layer 2 or Layer 3 devices in workgroups to the GigabitEthernet optical ports or electrical ports of the S5510 Ethernet switch.

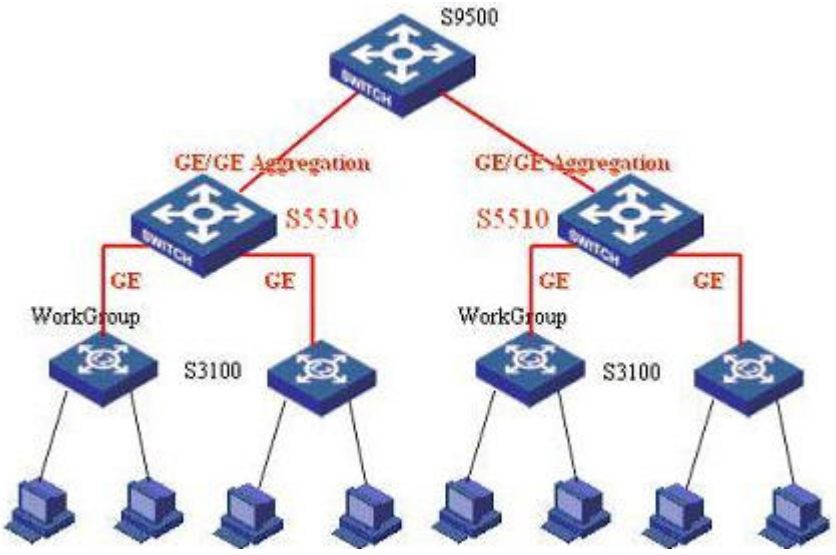

Figure 1-3 Figure 3: H3C S5510 series application in large enterprise and campus network

Application 4:IPv4/IPv6 Hybrid Networking

Full IPv4 networking and full IPv6 networking are similar. At the early stage of IPv6 implementation, however, IPv4/IPv6 hybrid networks are common. This gives full play to the IPv4/IPv6 dual-stack and IPv6 over IPv4 tunneling features provided by the S5510 series and enables flexible networking.

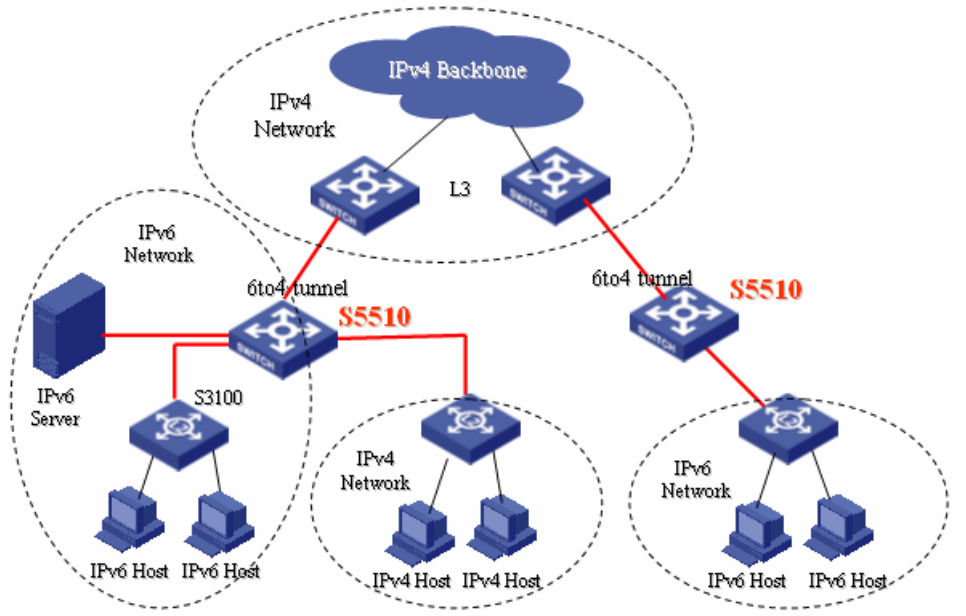

Figure 1-4 Using S5510 series in the IPv4/IPv6 hybrid network of large enterprises and campuses

Huawei-3Com., Ltd.

Add: Liuhe Road
Zhijiang Science Park,
Hangzhou 310053, P.R. China

Tel: +86 86760000

Email: customer_service@huawei-3com.com

Version No. : GE-082230-20061116-BR-V2.0

Website : www.huawei-3com.com