Table of Contents

Chapter 1 Overview of New Features 1-1
1.1 Introduction 1-1
1.2 Existing Features of S5600 Series Switches 1-1
1.3 New Features 1-2
1.4 Logging onto A Switch through Web Network Management Terminals 1-6
1.5 Command History 1-9
1.6 The Broadcasting Packet Suppression Function 1-10
1.6.1 Configuring the Broadcasting Packet Suppression Function 1-10
1.6.2 ip forward-broadcast 1-10

Chapter 1 Overview of New Features

1.1 Introduction

Quidway S5600 Series Ethernet Switches are wire speed layer 3 switching products supporting Intelligent Resilient Framework (IRF) feature. Besides saving user cost otherwise invested on module rack-type switches, the S5600 series with IRF technique also offer excellent network availability, upgradeability, performance and power network control capacity. The series include the following main types of switches:

1.2 Existing Features of S5600 Series Switches

Table 1-1 Existing features of S5600 series switches

Feature	Description
VLAN	• IEEE 802.1Q-compliant • Port-based VLAN (virtual local area network) • Voice VLAN
Spanning tree protocol (STP)	• STP/RSTP supported • IEEE 802.1D-/IEEE 802.1w-complicant
Flow control	• IEEE 802.3 flow control (full duplex) • Back-pressure-based flow control (half duplex)
Broadcast storm suppression	Supported
Multicast	• IGMP Snooping (internet group management protocol snooping) supported • IGMP (internet group management protocol) supported • PIM-DM (protocol-independent multicast-dense mode) supported • PIM-SM (protocol-independent multicast-sparse mode) supported (S5600-EI only)
IP-based routing	• Static route supported • RIP (routing information protocol) v1/v2 supported • OSPF (open shortest path first) supported • Routing policy supported
DHCP	• DHCP (dynamic host configuration protocol) relay supported • DHCP client supported
Port aggregation	Supported
Mirroring	• Flow-based mirroring • Port-based mirroring

Feature	Description
Security	• Hierarchical user management and password protection • IEEE 802.1x authentication • Packet filtering • SSH • Centralized MAC address authentication • Port isolation
QoS (Quality of service)	• Flow classification • Packet redirecting • Bandwidth allocation • Priority • Port priority queue • Queue scheduling: SP (strict priority), WRR (weighted round robin) • Time band • QoS profile
Management/ Maintenance	• Configuration through CLI (command line interface) • Configuration through Console port • Configuration through Ethernet ports (by using Telnet or SSH) • Configuration through Console ports (by using Modems) • SNMP (simple network management protocol), Quidview NMS and RMON (1/2/3/9 group MIBs of RMON [Remote Monitoring]) • Web-based network management • System log • Hierarchical alarm • Debug information output • PING, Tracerout, and multicast traceroute • Remote maintenance through Modems, Telnet, and SSH
Remote power supply	PoE (power over Ethernet) supported
Loading and upgrade	• XModem • FTP (file transfer protocol), TFTP (trivial file transfer protocol)

1.3 New Features

Table 1-2 lists the new features of S5600 series Ethernet switches and the related modules.

Table 1-2 New features

Module	Feature
00-Overview of New Features	• Logging onto a switch through Web network management terminals • Command history • The Broadcasting Packet Suppression Function
01-IRF	• RMON on IRF • HGMP on IRF • Testing peer fabric port
02-Port	• Port security • Setting global broadcast storm suppression ratio • Cable testing • The **display brief interface** command (simplifies the **display interface** command) • Updating the information in the Port Loop Testing section
03-DLDP	DLDP (Device Link Detection Protocol)
04-VLAN	• Voice VLAN • Protocol-based VLAN • Configure VLANs in batch
05-GVRP	GVRP (GARP VLAN Registration Protocol)
06-VLAN VPN	VLAN VPN (QinQ)
07-DHCP	• DHCP Server • DHCP Snooping • DHCP accounting • Option 184 support (DHCP server) • Option 82 support (DHCP relay) • Updating the information in the DHCP Relay section
08-ARP	Gratuitous ARP packets sending/receiving
09-MSTP	• MSTP, compatible with STP and RSTP • QinQ BPDU Tunnel • Huawei-3Com-proprietary MSTP overhead standard
10-802.1X	• Version checking (802.1x supplicant system) • Guest VLAN • 802.1x PEAP • Performing 802.1x authentication and MAC address-based authentication simultaneously • 802.1x-trusted MAC address • 802.1x client checking

Module	Feature
11-AAA&Radius&Tacacs	• Separated authentication, authorization, and accounting • Authenticated users need to be authenticated again when the device restarts. • Delivering of trunk ports and hybrid ports in Tag VLAN is supported when performing 802.1x authentications. • The tag authentication method field is added to RADIUS protocol.
12-Centralized MAC address-based authentication	Centralized MAC address-based authentication
13-SSH2.0	• SSH2.0 • Automatic RSA public key configuring
14-Routing	• OSPF neighbor information is added. • Commands used to display RIP interface information are added. • RIP equivalent route
15-Multicast	• IGMP Snooping • The number of IGMP groups can be limited on interface. • Adding multicast MAC addresses manually • Multicast source port suppression
16-VRRP	• VRRP (virtual router redundancy protocol) • Monitoring VRRP-enabled ports
17-Auto detect	The auto detect function
18-QoS/ACL	• Mirroring remote ports • Flow statistics for ACL rules defined using the **deny** keyword • Improvements made for the depth-first order of ACL matching • DSCP (differentiated services code point) refined when defining ACL rules • Delivering ACLs in RADIUS • Configuring synchronization for the schedule of aggregation ports • Protocol packet priority • Controlling Telnet users
19-PoE Profile	PoE Profile (power over Ethernet profile)

Module	Feature
20-File system management and seven-segment display	• Upgrading all the units of a fabric using the App (or BootROM, Web) files of an unit • Setting an App file of a fabric or an unit of a fabric to be the primary/a secondary configuration file • Specifying a fabric or an unit of a fabric to use the primary configuration file, a secondary configuration file, or no configuration file to start. • Performing specific file-related operations for a fabric or an unit of a fabric, such as deleting files stored in the storage devices of a Ethernet switch, displaying the information about specified files or directories in the storage devices of a Ethernet switch, and clearing the recycle bin. • Customizing the password for entering the BOOT menu • Configuration file backup/recovery • Seven-segment display, which indicates the progress of loading software using FTP/TFTP
21-Information center	• Exporting switch synchronization information • Setting the format of time stamps to be sent to log hosts
22-Maintanence and debugging	• Configuring Telnet users with specified source IP addresses/source ports • Terminating specified FTP connections using commands • Saving debugging information into Flash • Displaying the information about all enabled types of debugging • Displaying the statistics of MAC addresses of a switch
23-Hwping	Hwping
24-EAD	EAD (endpoint admission defense)
25-SNMP RMON	• Adding querying/setting operations performed by administrators to switch logs • SNMP Agent logging • Newly added commands used to display the information about the Trap list
26-Specifying the source IP addresses of the packets of specified services	Specifying the source IP addresses of the packets of specified services through commands
27-Loopback detection	The loopback detection function

1.4 Logging onto A Switch through Web Network Management Terminals

An S5600 series switch has a WEB server built-in. You can log onto a switch through a Web network management terminal to manage/maintain the switch in an intuitive way by interacting with the built-in Web server

To log onto a switch through a Web network management terminal, you need to perform configurations for both the switch and the Web network management terminal.

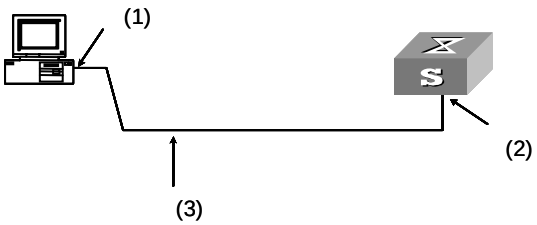
Table 1-3 Requirements for logging onto switches through Web network management terminals

Item	Requirement
Switch	The management VLAN is configured. The routes between the switch and the Web network management terminal are reachable.
	The user name and password used to log onto the switch are configured.
Web network management terminal	A Web browser is installed.
	The IP address used to log onto the management VLAN of the switch is obtained.

I. Setting up the connection for Web-based configuration

Before performing Web-based configuration for an Ethernet switch, you need to configure an IP address for the interface of the management VLAN of the switch.

- Setup the connection for local configuration through the Console port. Figure 1-1 illustrates the way to connect a Web network management terminal, which usually is a PC, to a switch.



(1) RS-232 port (2) Console port (3) Configuration cable

Figure 1-1 Setup the connection for local configuration through Console port

- Launch terminal emulation program (such as Terminal in Windows 3.X or HyperTerminal in Windows 9X) on the PC, with the baud rate set to 9600 bps, data bit set to 8, parity checking set to none, and data flow control set to none.

- Turn on the Ethernet switch and strike Enter after the switch POST (power-on self test), the prompt appears in the terminal display, as shown in Figure 1-2.

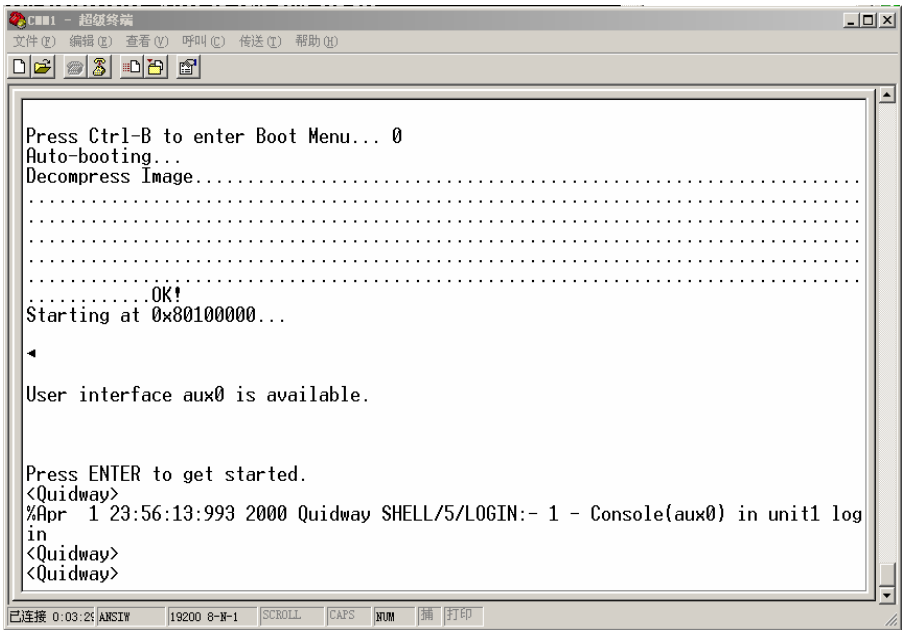


Figure 1-2 The interface of a terminal emulation program

- Assign an IP address to the interface of the management VLAN of the Ethernet switch by executing the following commands in the interface of the terminal emulation program.

```
<Quidway> system
# Enter management VLAN view.
[Quidway] interface vlan-interface 1# Remove the existing management VLAN interface IP address.
[Quidway-VLAN-interface1] undo ip address# Configure the IP address of the interface of the management VLAN to be 10.153.17.82.
[Quidway-VLAN-interface1] ip address 10.153.17.82 255.255.255.0
```

II. Setting the user name and password

After establishing the connection between the Web network management terminal and the switch through the Console port, you can configure the user name and password for Web network management users on the switch.

- Add a Telnet user account on the switch, setting user level to 3 (the administration level).

```
# Set the username to admin.
[Quidway] local-user admin# Set the user level to 3.
[Quidway-luser-admin] service-type telnet level 3
# Set the password to admin.
[Quidway-luser-admin] password simple admin
```

- Configure a static route between the switch and the gateway.

```
[Quidway] ip route-static ip-address 0.0.0.0 255.255.255.255
```

III. Logging onto a switch through a Web network management terminal

- Figure 1-3 illustrates the way to set up remote connections for Web-based configuration.

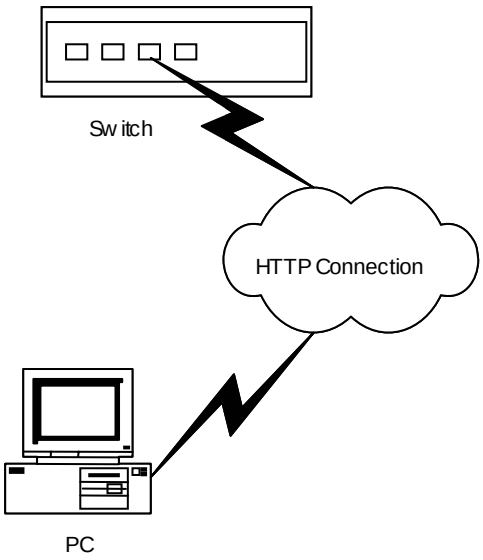


Figure 1-3 Setup the connection for remote Web-based configuration

- Connect the Web network management terminal, which usually is a PC, to the switch and log onto the switch through a Web browser by entering http://10.153.17.82 in the address bar. (Make sure the route between the Web network management terminal and the switch is reachable.)
- After the logon interface of the Web network management system appears (as shown in Figure 1-4), enter the user name and password just configured and click the Login button. The main page of the Web network management system appears.

Figure 1-4 The logon interface of the Web network management system

1.5 Command History

CLI can store the latest specified number of executed commands for users to recall and execute again. By default, CLI stores 10 latest executed commands. Table 1-4 lists history command-related operations.

Table 1-4 Access history commands

Operation	Command or keys	Description
Display history commands	**display history-command**	Displays valid history commands.
Recall the previous history command	Pressing the Up arrow key or <Ctrl + P>	This operation recalls the previous stored command (if it exists).
Recall the next history command	Pressing the Down arrow key or <Ctrl + N>	This operation recalls the next stored command (if it exists).

Note:

- As the Up and Down keys have different meanings in HyperTerminal running on Windows 9x than in Terminal (running on Windows 3.X) and Telnet, these two keys can be used to recall history commands only in terminals running Windows 3.x or Telnet running in Windows 3.x. You can press <Ctrl + P> or <Ctrl + N> in Windows 9x to achieve the same purpose.
- For multiple successively executed commands, only the first one is stored as a history command if the commands are the same.

1.6 The Broadcasting Packet Suppression Function

1.6.1 Configuring the Broadcasting Packet Suppression Function

You can specify whether or not to receive broadcasting packets sourced from directly connected networks by performing the configurations listed in Table 1-5.

Table 1-5 Configure the broadcasting packet suppression function

Operation	Command	Description
Enter system view	**system-view**	—
Specify to receive broadcasting packets sourced from directly connected networks	**ip forward-broadcast**	Optional By default, broadcasting packets sourced from directly connected networks are denied.

The following is the newly added command concerning broadcasting packets sourced from directly connected networks.

1.6.2 ip forward-broadcast

Syntax

ip forward-broadcast

undo ip forward-broadcast

View

System view

Parameter

None

Description

Use the **ip forward-broadcast** command to specify to receive broadcasting packets sourced from directly connected networks.

Use the **undo ip forward-broadcast** command to specify to deny broadcasting packets sourced from directly connected networks.

By default, broadcasting packets sourced from directly connected networks are denied.

Example

Deny broadcasting packets sourced from directly connected networks.

```
<Quidway> system-view
```

```
System View: return to User View with Ctrl+Z.
[Quidway] undo ip forward-broadcast
```