V1910-CMW520-R1513P95 Release Notes

Software Feature Changes

© Copyright 2015 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.
The information in this document is subject to change without notice.

Contents

Release1513P95 1
Release1513P89 2
Release1513P85 3
Release1513P81 4
Release1513P66 5
New feature: Configuring an NTP polling interval 5
Release1513P62 7
New feature: Configuring GTS on a port 7
Traffic shaping 7
Configuring GTS on a port 8
New feature: Establishing a Telnet connection 9
Overview 9
Command reference 9
telnet 9
Release1513P51 11
Release1513P50 12
Release1513P15 13
Release1513P13 14
Modified feature: Upgrading the PoE software from the CLI 14
Feature change description 14
Command reference 14
upgrade 14
upgrade ipv6 15
Release1513P07 16
Release1513P06 17
Release1513P05 18
Release1513P01 19
Release1513 20
New feature: Automatic configuration file backup for software downgrading 20
Using automatic configuration file backup for software downgrading 20
New feature: Configuring IPv6 21
Overview 21
IPv6 features 21
Enabling IPv6 Service 22
Modified feature: Configuring a local user 23
Feature change description 23

Modified feature: Setting the super password 24
Feature change description 24
Modified feature: Creating users 25
Feature change description 25
Release1512P10 27
Release1512P05 28
Release1511 29
Feature1510 30
New feature: Portal 30
New feature: MLD Snooping 30
New feature: IPv6 routing 30
New feature: Pingv6 30
New feature: Tracertv6 30
New feature: IPv6 acl 30
Release1112 31
Release1111P02 32
Release1111P01 33
Release1111 34
Release1109 35
New feature: Gateway settings 35
Release1108P01 36

Release 1513P95

This release has no feature changes.

Release 1513P89

This release has no feature changes.

Release 1513P85

This release has no feature changes.

Release 1513P81

This release has no feature changes.

Release 1513P66

This release has the following changes:

- New feature: Configuring an NTP polling interval

New feature: Configuring an NTP polling interval

Polling interval was added for NTP.

To configure an NTP polling interval on the **Net Time** tab:

1. Select **Device** > **System Time** from the navigation tree.
2. Click the **Net Time** tab.

Figure 1 NTP configuration page

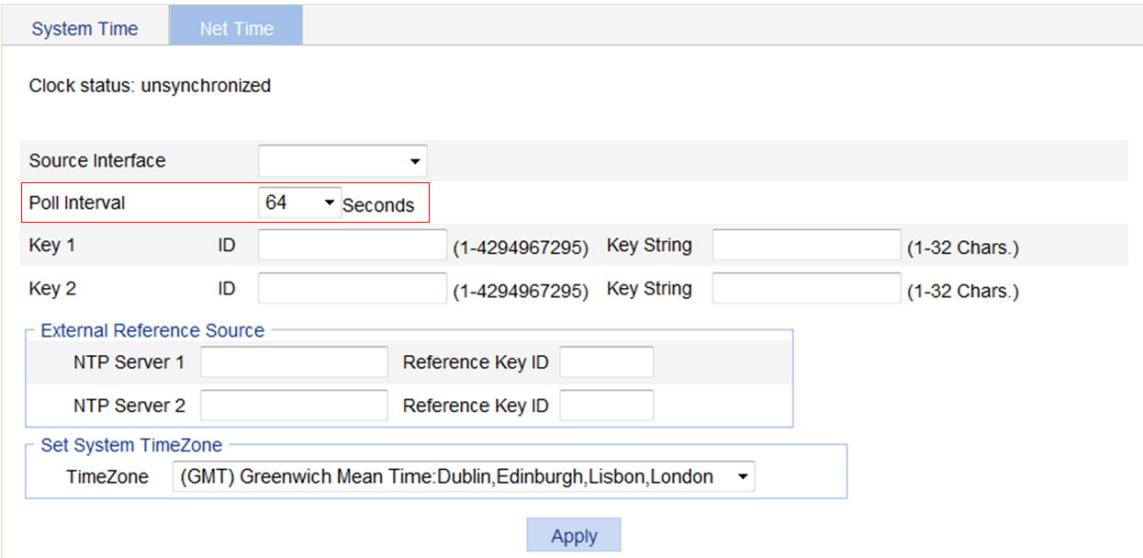


Table 1 Configuration items

Item	Description
Clock status	Display the synchronization status of the system clock.
Source Interface	Set the source interface for an NTP message. This configuration uses the IP address of an interface as the source IP address in the NTP messages. If the specified source interface is down, the source IP address is the IP address of the egress interface. TIP: If you do not want the IP address of a certain interface on the local device to become the destination address of response messages, you can specify the source interface for NTP messages.
Poll Interval	Polling interval. It is the maximum interval between successive NTP messages. The default is 64 seconds.

Item		Description
Key 1		Set NTP authentication key. The NTP authentication feature should be enabled for a system running NTP in a network that requires high security. This feature enhances the network security by means of client-server key authentication, and prohibits a client from synchronizing with a device that has failed authentication.
Key 2		You can set two authentication keys, each of which has a key ID and key string. • **ID**—ID of a key. • **Key string**—A character string for MD5 authentication key.
External Reference Source	NTP Server 1/Reference Key ID	Specify the IP address of an NTP server, and configure the authentication key ID used for the association with the NTP server. Only if the key provided by the server is the same with the specified key will the device synchronize its time to the NTP server. You can configure two NTP servers. The clients will choose the optimal reference source. IMPORTANT: The IP address of an NTP server is a unicast address, and cannot be a broadcast or a multicast address, or the IP address of the local clock source.
	NTP Server 2/Reference Key ID	
TimeZone		Set the time zone for the system.

Release 1513P62

This release has the following changes:

- New feature: Configuring GTS on a port
- New feature: Establishing a Telnet connection

New feature: Configuring GTS on a port

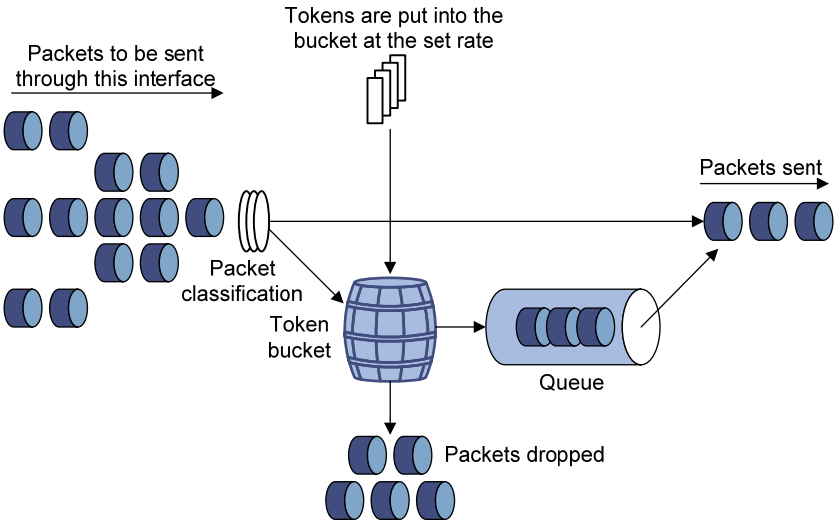
Traffic shaping

Traffic shaping shapes the outbound traffic.

Generic traffic shaping (GTS) limits the outbound traffic rate by buffering exceeding traffic. You can use traffic shaping to adapt the traffic output rate on a device to the input traffic rate of its connected device to avoid packet loss.

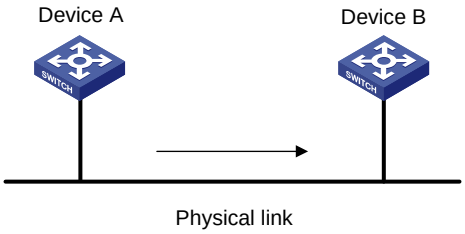
The difference between traffic policing and GTS is that packets to be dropped with traffic policing are retained in a buffer or queue with GTS, as shown in Figure 1. When enough tokens are in the token bucket, the buffered packets are sent at an even rate. Traffic shaping can result in additional delay and traffic policing does not.

Figure 1 GTS



For example, in Figure 2, Device B performs traffic policing on packets from Device A and drops packets exceeding the limit. To avoid packet loss, you can perform traffic shaping on the outgoing interface of Device A so packets exceeding the limit are cached in Device A. Once resources are released, traffic shaping takes out the cached packets and sends them out.

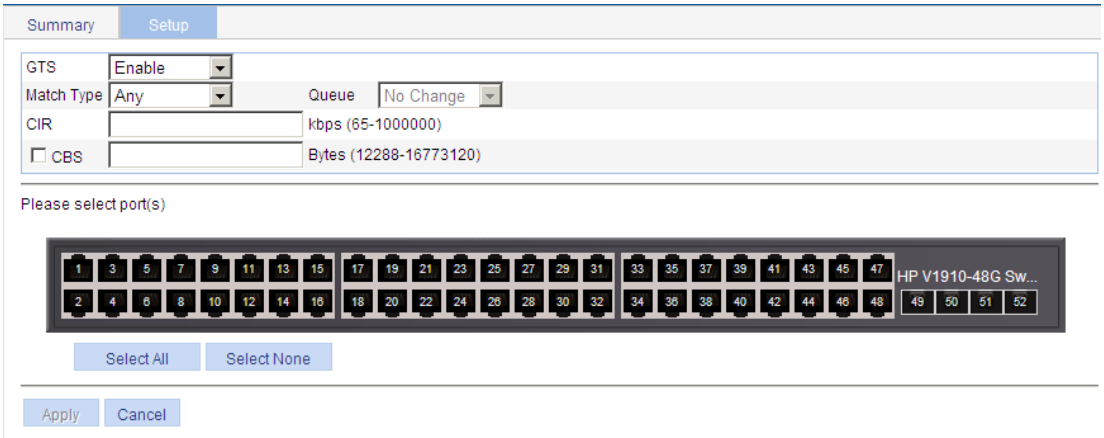
Figure 2 GTS application



Configuring GTS on a port

3. Select **QoS** > **GTS** from the navigation tree.
4. Click the **Setup** tab to enter the GTS configuration page.

Figure 3 Configuring GTS on a port



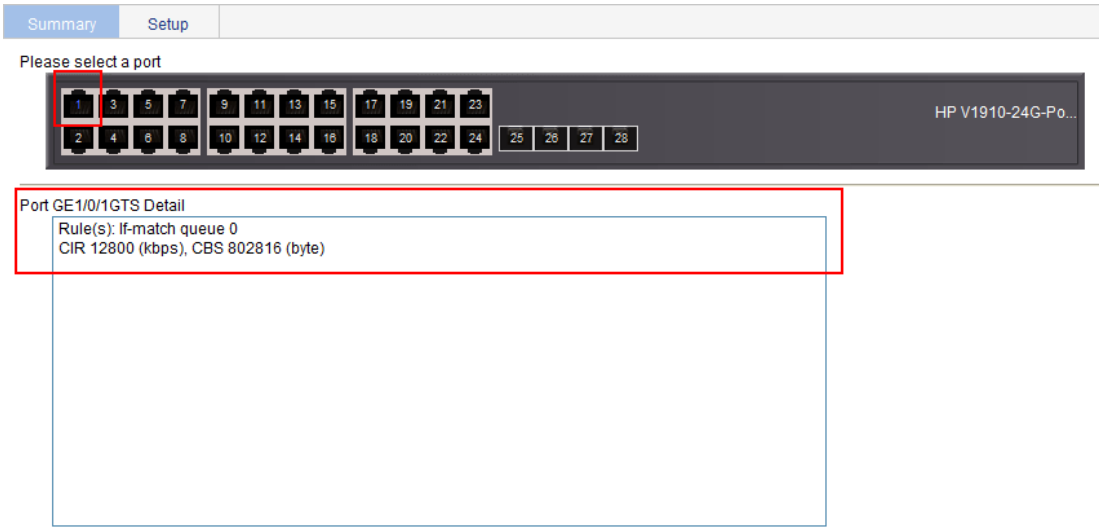
5. Configure GTS on a port as described in Table 2.
6. Click **Apply**.

Table 1 Configuration items

Item	Description
GTS	Enable or disable GTS on the port.
Match Type	Options include: • **Any**—Shapes all packets on the port. • **Queue**—Shapes the packets of a specific queue.
Queue	Select a queue if you select **Queue** for **Match Type**.
CIR	Set the committed information rate (CIR), the average traffic rate.
CBS	Set the committed burst size (CBS). If the field is not set, the switch automatically calculates an appropriate CBS value based on the CIR value.

7. Click the **Summary** tab, and select the configured port to view the GTS configuration result, as shown in Figure 4.

Figure 4 GTS configuration result



New feature: Establishing a Telnet connection

Overview

You can use the device as a Telnet client to log in to and manage a Telnet server. For successful Telnet connection establishment, make sure the Telnet client and server can reach each other.

Command reference

telnet

Syntax

telnet *remote-host* [*service-port*] [**source** { **interface** *interface-type interface-number* | **ip** *ip-address* }]

Parameters

remote-host: IPv4 address or host name of a remote host, a case insensitive string of 1 to 20 characters.

service-port: TCP port number of the Telnet service on the remote host. It is in the range of 0 to 65535. The default is 23.

source: Specifies the source interface or source IPv4 address of Telnet packets.

interface *interface-type interface-number*: Specifies the source interface by its type and number. The source IPv4 address of the Telnet packets that are sent is the IPv4 address of the specified source interface. *interface-type interface-number* represents the interface type and number.

ip *ip-address*: Specifies the source IPv4 address of Telnet packets.

Description

Use **telnet** to telnet to a remote host.

To stop the current Telnet connection, use the **quit** command.

The source IPv4 address or source interface specified by this command is applicable to the current Telnet connection only.

Examples

Telnet to the remote host 1.1.1.2, specifying the source IP address of Telnet packets as 1.1.1.1.

```
<Sysname> telnet 1.1.1.2 source ip 1.1.1.1
```

Release 1513P51

This release has no feature changes.

Release 1513P50

This release has no feature changes.

Release 1513P15

This release has no feature changes.

Release 1513P13

This release has the following changes: Modified feature: Upgrading the PoE software from the CLI

Modified feature: Upgrading the PoE software from the CLI

Feature change description

The **poe** keyword was added to the **upgrade** and **upgrade ipv6** commands for PoE software upgrading.

Command reference

upgrade

Syntax

upgrade *server-address source-filename* { **bootrom** | **poe** |**runtime** }

Parameters

server-address: IPv4 address or host name (a string of 1 to 20 characters) of the TFTP server.

source-filename: Specifies the software package file name on the TFTP server.

bootrom: Upgrades the Boot ROM image.

poe: Upgrades the PoE software.

runtime: Upgrades the system software image.

Description

Use **upgrade** *server-address source-filename* **bootrom** to upgrade the Boot ROM image. If the Boot ROM image in the downloaded software package file is not applicable, the original Boot ROM image is used.

Use **upgrade** *server-address source-filename* **runtime** to upgrade the system software image. If the system software image in the downloaded software package file is not applicable, the original system software image is used.

Use **upgrade** *server-address source-filename* **poe** to upgrade the PoE software.

To complete a Boot ROM image or system software image upgrade, you must reboot the device.

Upgrading the PoE software does not require a reboot.

NOTE:

The Boot ROM image and system software image for the switch are released as one **.bin** package file.

Examples

Download software package file **main.bin** from the TFTP server to upgrade the Boot ROM image.

```
<Sysname> upgrade 192.168.20.41 main.bin bootrom
```

Download software package file **main.bin** from the TFTP server to upgrade the system software image.

```
<Sysname> upgrade 192.168.20.41 main.bin runtime
```

Download software package file **poe.bin** from the TFTP server to upgrade the PoE software.

```
<Sysname> upgrade 192.168.20.41 poe.bin poe
```

upgrade ipv6

Syntax

upgrade ipv6 *server-address source-filename* { **bootrom** | **poe** | **runtime** }

Parameters

server-address: IPv6 address of the TFTP server.

source-filename: Specifies the software package file name on the TFTP server.

bootrom: Upgrades the Boot ROM image.

poe: Upgrades the PoE software.

runtime: Upgrades the system software image.

Description

Use **upgrade ipv6** *server-address source-filename* **bootrom** to upgrade the Boot ROM image. If the Boot ROM image in the downloaded software package file is not applicable, the original Boot ROM image is used.

Use **upgrade ipv6** *server-address source-filename* **runtime** to upgrade the system software image. If the system software image in the downloaded software package file is not applicable, the original system software image is used.

Use **upgrade ipv6** *server-address source-filename* **poe** to upgrade the PoE software.

To complete a Boot ROM image or system software image upgrade, you must reboot the device.

Upgrading the PoE software does not require a reboot.

NOTE:

The Boot ROM image and system software image for the switch are released as one **.bin** package file.

Examples

Download software package file **main.bin** from the TFTP server to upgrade the Boot ROM image.

```
<Sysname> upgrade ipv6 2001::2 main.bin bootrom
```

Download software package file **main.bin** from the TFTP server to upgrade the system software image.

<Sysname> upgrade ipv6 2001::2 main.bin runtime

Download software package file **poe.bin** from the TFTP server to upgrade the PoE software.

```
<Sysname> upgrade ipv6 2001::2 poe.bin poe
```

Release 1513P07

This release has no feature changes.

Release 1513P06

This release has no feature changes.

Release 1513P05

This release has no feature changes.

Release 1513P01

This release has no feature changes.

Release 1513

This release has the following changes:

- New feature: Automatic configuration file backup for software downgrading
- New feature: Configuring IPv6
- Modified feature: Configuring a local user
- Modified feature: Setting the super password
- Modified feature: Creating users

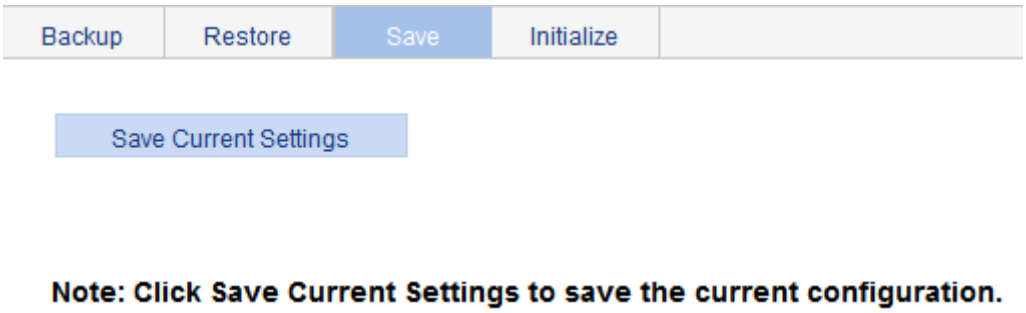
New feature: Automatic configuration file backup for software downgrading

Using automatic configuration file backup for software downgrading

After a software upgrade, the next-startup configuration files created on the old software version might have settings that are incompatible with the new software version.

To ensure compatibility, the system verifies the compatibility of a configuration file with the software version the first time you save configuration to the file after a software upgrade.

Figure 5 Saving the configuration



To save the running configuration:

1. Select **Device** > **Configuration** from the navigation tree.
2. Click the **Save** tab.
3. Click **Save Current Settings**.

The system verifies the compatibility of the configuration file with the software version.

If any incompatibility is found, the system uses the running configuration to overwrite the configuration file after backing up the file for future rollback. The backup file is named in the **_*old-filename*_bak.cfg** format. For example, if the old configuration file is named config.cfg, the backup file is named _config_bak.cfg.

If the backup attempt fails, the system uses the running configuration to overwrite the configuration file without backing up the old configuration. As a result, incompatible settings (such as some password settings) will be lost.

To ensure a successful backup, make sure:

- The switch has enough Flash space for the backup configuration file and the new next-startup configuration file.
- The file name is up to 91 characters.

To load the backup configuration file after a software downgrade, specify the backup file as the next-startup configuration file.

New feature: Configuring IPv6

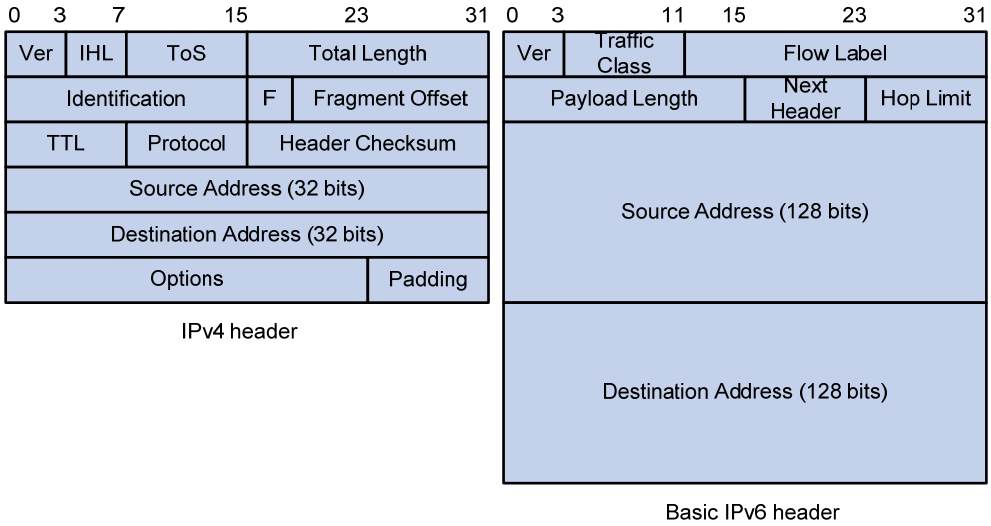
Overview

IPv6, also called IP next generation (IPng), was designed by the IETF as the successor to IPv4. The significant difference between IPv6 and IPv4 is that IPv6 increases the IP address size from 32 bits to 128 bits.

IPv6 features

IPv6 removes several IPv4 header fields or moves them to the IPv6 extension headers to reduce the length of the basic IPv6 packet header. The basic IPv6 packet header has a fixed length of 40 bytes to simplify IPv6 packet handling and to improve forwarding efficiency. Although IPv6 address size is four times the IPv4 address size, the basic IPv6 packet header size is only twice the size of the option-less IPv4 packet header.

Figure 6 IPv4 packet header format and basic IPv6 packet header format



Larger address space

The source and destination IPv6 addresses are 128 bits (16 bytes) long. IPv6 can provide 3.4 x 10^{38} addresses to meet the requirements of hierarchical address division and the allocation of public and private addresses.

Hierarchical address structure

IPv6 uses the hierarchical address structure to speed up route lookups and reduce the IPv6 routing table size through route aggregation.

Address autoconfiguration

To simplify host configuration, IPv6 supports stateful and stateless address autoconfiguration:

- Stateful address autoconfiguration enables a host to acquire an IPv6 address and other configuration information from a server (for example, a DHCP server).
- Stateless address autoconfiguration enables a host to automatically generate an IPv6 address and other configuration information by using its link-layer address and the prefix information advertised by a router.

To communicate with other hosts on the same link, a host automatically generates a link-local address based on its link-layer address and the link-local address prefix (FE80::/10).

Built-in security

IPv6 defines extension headers to support IPsec. IPsec provides end-to-end security for network security solutions and enhances interoperability among different IPv6 applications.

QoS support

The Flow Label field in the IPv6 header allows the device to label the packets and facilitates the special handling of a flow.

Enhanced neighbor discovery mechanism

The IPv6 neighbor discovery protocol is implemented through a group of Internet Control Message Protocol version 6 (ICMPv6) messages to manage the information exchange among neighboring nodes on the same link. The group of ICMPv6 messages replaces Address Resolution Protocol (ARP) messages, Internet Control Message Protocol version 4 (ICMPv4) Router Discovery messages, and ICMPv4 Redirect messages and provides a series of other functions.

Flexible extension headers

IPv6 eliminates the Options field in the header and introduces optional extension headers to provide scalability and improve efficiency. The Options field in the IPv4 packet header contains up to 40 bytes, whereas the IPv6 extension headers are restricted to the maximum size of IPv6 packets.

Enabling IPv6 Service

1. Select **Network** > IPv6 Management from the navigation tree to enter the **IPv6 Service** page.
2. Click **Enable** for IPv6 Service.

Figure 7 IPv6 Service

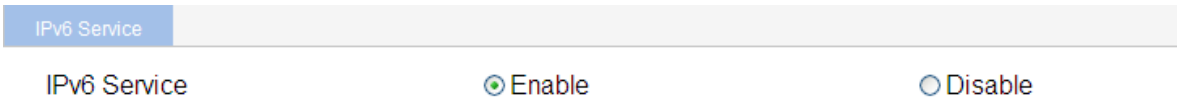


Table 2 Configuration items

Item	Description
IPv6 Service	Enable or disable IPv6. By default, IPv6 Service is enabled.

Modified feature: Configuring a local user

Feature change description

The **Password Encryption** option was added for local user accounts.

Figure 8 Local user configuration page

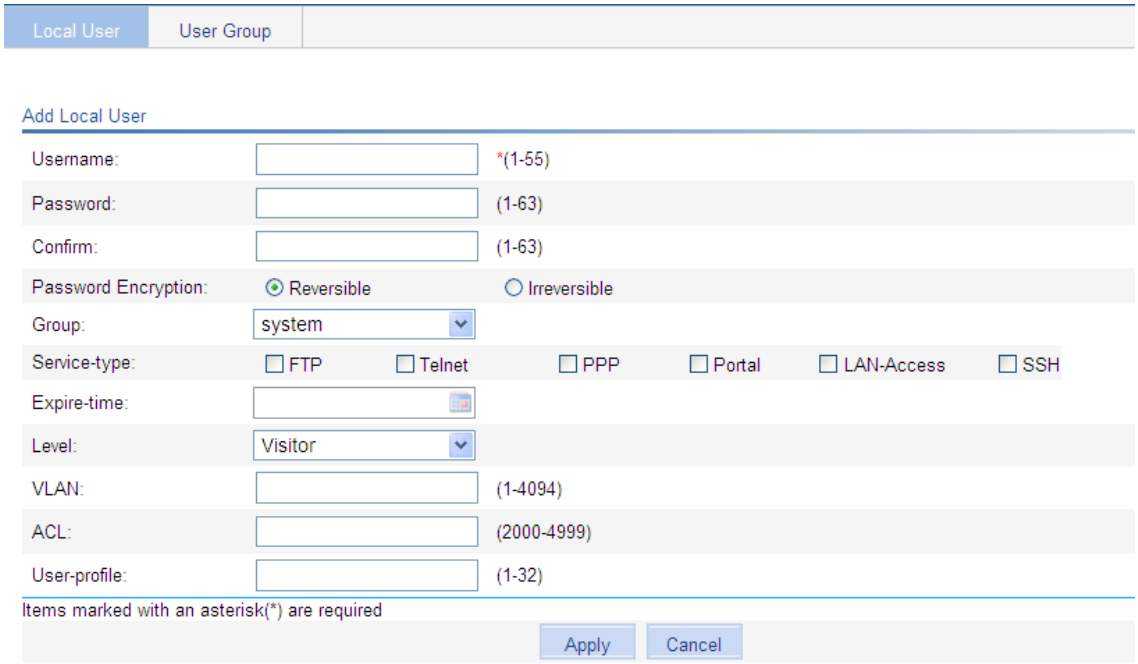


Table 3 Configuration items

Item	Description
Username	Specify a name for the local user.
Password Confirm	Specify and confirm the password of the local user. The settings of these two fields must be the same. IMPORTANT: HP recommends that you do not specify a password starting with spaces because spaces at the beginning of the password string will be ignored, but they count at the user login page.
Password Encryption	Set an encryption method for securing the password in the database: • **Reversible**—The password is saved after being encrypted with a reversible encryption algorithm. • **Irreversible**—The password is saved after being encrypted with a irreversible encryption algorithm.
Group	Select a user group for the local user.

Item	Description
Service-type	Select the service types for the local user to use, including FTP, Telnet, portal, LAN-access, and SSH. LAN-access primarily represents Ethernet users, such as 802.1X users. The switch series does not support PPP. IMPORTANT: If you do not specify any service type for a local user who uses local authentication, the user cannot pass authentication and therefore cannot log in.
Expire-time	Specify an expiration time for the local user, in the HH:MM:SS-YYYY/MM/DD format. When the NAS authenticates a local user with the expiration time argument configured, it checks whether the expiration time has elapsed. If not, the NAS permits the user to log in.
Level	Select an authorization level for the local user, which can be Visitor, Monitor, Configure, or Management, in ascending order of priority. This option is effective only for FTP, Telnet, and SSH users.
VLAN	Specify the VLAN to be authorized to the local user after the user passes authentication. This option is effective only for LAN-access and portal users.
ACL	Specify the ACL to be used by the NAS to restrict the access of the local user after the user passes authentication. This option is effective only for LAN-access and portal users.
User-profile	User profile for the local user. The switch series does not support this option.

Modified feature: Setting the super password

Feature change description

The **Password Encryption** option was added for securing the super password.

Figure 9 Super password

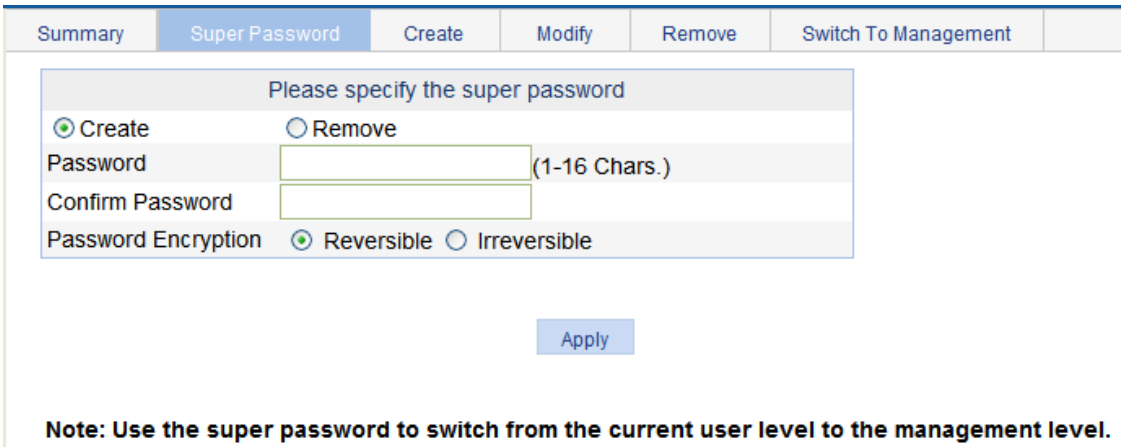


Table 4 Configuration items

Item	Description
Create/Remove	Select the operation type: • **Create**—Configure or modify the super password. • **Remove**—Remove the current super password.
Password/Confirm Password	Enter the same password twice.
Password Encryption	Set an encryption method for securing the password in the database: • **Reversible**—The password is saved after being encrypted with a reversible encryption algorithm. • **Irreversible**—The password is saved after being encrypted with a irreversible encryption algorithm.

Modified feature: Creating users

Feature change description

The **Password Encryption** option was added for local user accounts.

Figure 10 Creating a user

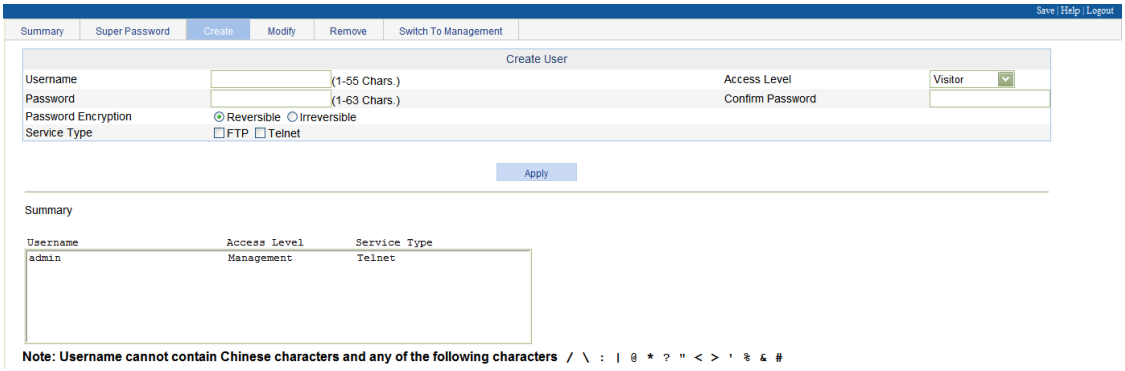


Table 5 Configuration items

Item	Description
Username	Set a username for the user.
Access Level	Select an access level for the user. Users of different levels can perform different operations. User levels, in order from low to high, are as follows: • **Visitor**—Users of this level can only perform ping and traceroute operations. They can neither access the data on the device nor configure the device. • **Monitor**—Users of this level can perform ping and traceroute operations and access the data on the device but cannot configure the device. • **Configure**—Users of this level can perform ping and traceroute operations, access data on the device, and configure the device, but they cannot upgrade the host software, add/delete/modify users, or back up/restore the configuration file. • **Management**—Users of this level can perform any operations on the device.
Password/Confirm Password	Enter the same password twice.
Password Encryption	Set an encryption method for securing the password in the database: • **Reversible**—The password is saved after being encrypted with a reversible encryption algorithm. • **Irreversible**—The password is saved after being encrypted with a irreversible encryption algorithm.
Service Type	Select the service types for the user to use, including FTP and Telnet. The terminal service allows users to log in from the console port. You must select at least one service type.

Release 1512P10

This release has no feature changes.

Release 1512P05

This release has no feature changes.

Release 1511

This release has no feature changes.

Feature 1510

This release has the following changes:

- New feature: Portal
- New feature: MLD Snooping
- New feature: IPv6 routing
- New feature: Pingv6
- New feature: Tracertv6
- New feature: IPv6 acl

New feature: Portal

For more information about Portal, see Configuring Portal authentication in *HP 1910 Switch Series User Guide*.

New feature: MLD Snooping

For more information about MLD snooping, see Configuring MLD snooping in *HP 1910 Switch Series User Guide*.

New feature: IPv6 routing

For more information about IPv6 routing, see Configuring IPv4 and IPv6 routing in *HP 1910 Switch Series User Guide*.

New feature: Pingv6

For more information about Pingv6, see Using diagnostic tools in *HP 1910 Switch Series User Guide*.

New feature: Tracertv6

For more information about Tracertv6, see Using diagnostic tools in *HP 1910 Switch Series User Guide*.

New feature: IPv6 acl

For more information about IPv6 acl, see Configuring ACLs in *HP 1910 Switch Series User Guide*.

Release 1112

This release has no feature changes.

Release 1111 P02

This release has no feature changes.

Release 1111 P01

This release has no feature changes.

Release 1111

This release has no feature changes.

Release 1109

This release has the following changes: New feature: Gateway settings

New feature: Gateway settings

For more information about Gateway settings, see Configuration wizard in *HP 1910 Switch Series User Guide.*

Release 1108P01

This release has no feature changes.