V1910-CMW520-R1513P05 Release Notes

Software Feature Changes

Contents

Release 1513P05

This release has the following changes:

Null

Release 1513P01

This release has the following changes:

Null

Release1513

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 1 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

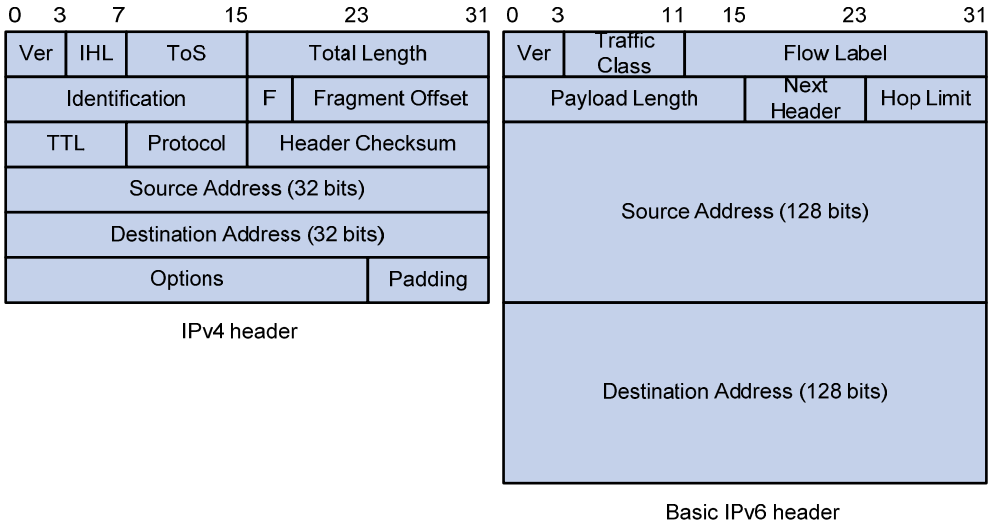
Overview

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 2 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 3 IPv6 Service

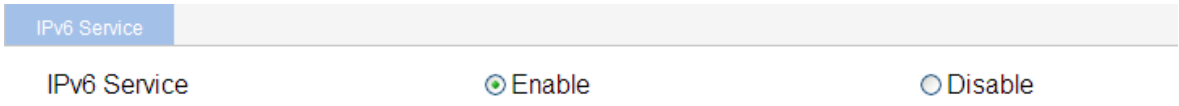


Table 2 Configuration items

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 1 Local user configuration page

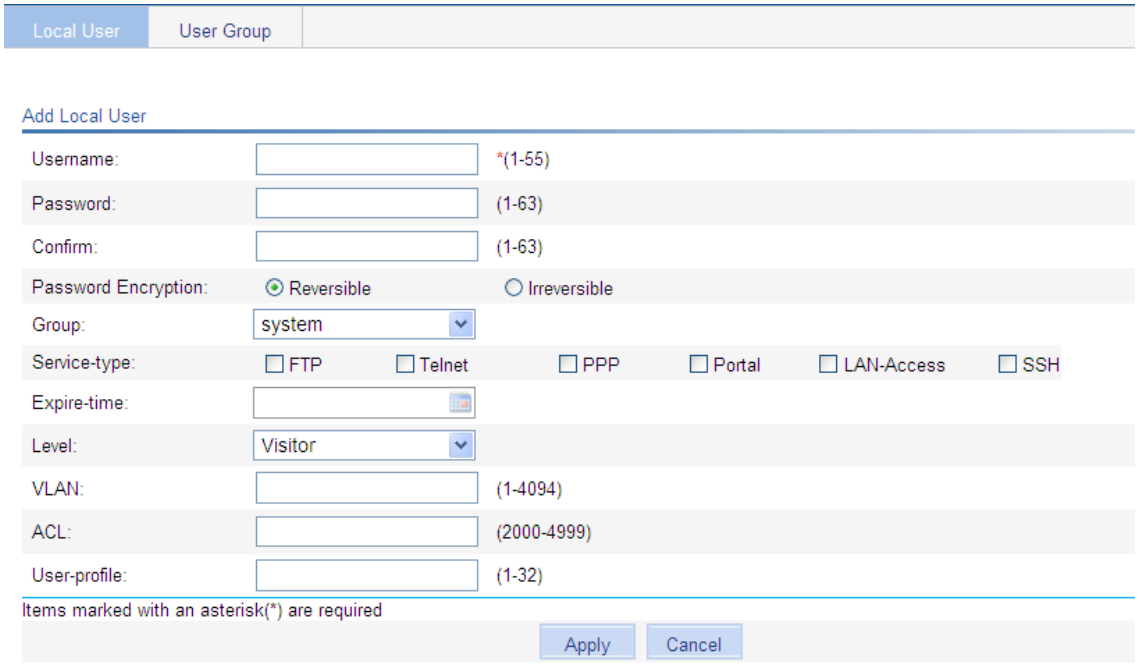


Table 3 Configuration items

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 4 Super password

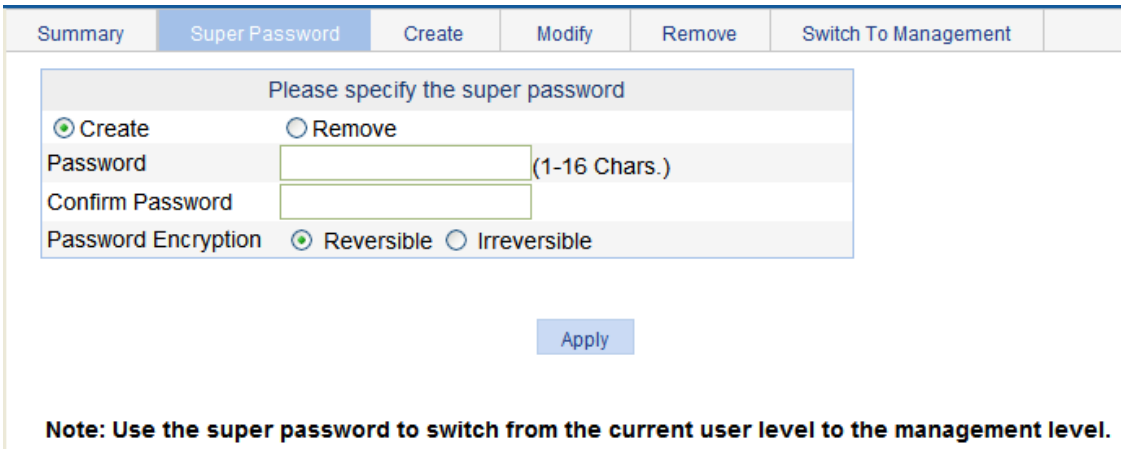


Table 4 Configuration items

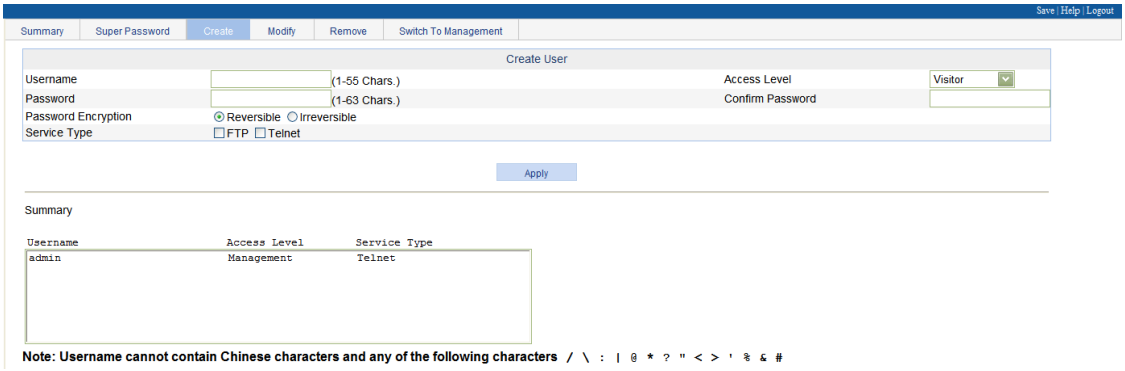
Item	Description
Create/Remove	Select the operation type: • **Create**—Configure or modify the super password. • **Remove**—Remove the current super password.
Password/Confirm Password	Enter the same password twice.
Password Encryption	Set an encryption method for securing the password in the database: • **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.

Table 5 Creating a user



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 the following changes:

Null

Release 1512P05

This release has the following changes:

Null

Release 1511

This release has the following changes:

Null

Feature1510

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 the following changes:

Null

Release 1111 P01

This release has the following changes:

Null

Release 1111

This release has the following changes:

Null

Release1109

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 the following changes:

Null