



# HPE 5710-CMW710-R6710P03

## Usage Guidelines

**Keywords:** Version Information, Version changed, Unresolved Problems and Avoidance Measures, List of Solved Problems

**Abstract:** Provide all details about the application version file, include: Version Information, Version changed, Unresolved Problems and Avoidance Measures, List of Solved Problems

**Abbreviations:**

Abbreviations	Full spelling
IRF	Intelligent Resilient Framework
AAA	Authentication, Authorization and Accounting
ARP	Address Resolution Protocol
CMW	Comware
DHCP	Dynamic Host Configuration Protocol
LACP	Link Aggregation Control Protocol
MIB	Management Information Base
MSTP	Multiple Spanning Tree Protocol
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
VLAN	Virtual Local Area Network
RIP	Routing Information Protocol
ECN	Explicit Congestion Notification



# Contents

Version information.....	1
Version number .....	1
Version history .....	1
Release reason .....	1
Restrictions and cautions .....	2
Open problems and workarounds .....	2
List of solved problems .....	2
Resolved problems in R6710P03 .....	2
Resolved problems in R6710.....	7
Resolved problems in E6702.....	12
Resolved problems in F2708 .....	13
Resolved problems in R2702.....	18
Resolved problems in R2612P05 .....	27
Resolved problems in R2612P03 .....	29
Resolved problems in R2612P01 .....	30
Resolved problems in R2612.....	33
Resolved problems in R2611.....	39
Software upgrade guidelines .....	39



# Version information

## Version number

Version number (outer): HPE Comware Software, Version 7.1.070, Release 6710P03

Version number (inner): V300R039B01D064SP180703

## Version history

Table 1 Version history

Version number(inner)	Version Number(outer)	Based Version Number	Release Date	Remark
V300R039B01D064SP180703	5710-CMW710-R6710P03	5710-CMW710-R6710	2023-08-01	None
V300R039B01D039	5710-CMW710-R6710	5710-CMW710-E6702	2022-12-28	None
V300R039B01D018	5710-CMW710-E6702	5710-CMW710-F2708	2022-04-14	None
V300R009B03D007SP19	5710-CMW710-F2708	5710-CMW710-R2702	2020-12-14	None
V300R009B03D007SP03	5710-CMW710-R2702	5710-CMW710-R2612P05	2019-06-12	None
V300R009B01D024SP17	5710-CMW710-R2612P05	5710-CMW710-R2612P03	2019-03-18	None
V300R009B01D024SP16	5710-CMW710-R2612P03	5710-CMW710-R2612P01	2018-10-24	None
V300R009B01D024SP12	5710-CMW710-R2612P01	5710-CMW710-R2612	2018-08-24	None
V300R009B01D024SP09	5710-CMW710-R2612	5710-CMW710-R2611	2018-06-01	None
V300R009B01D024SP07	5710-CMW710-R2611	First Release	2018-04-27	None

## Release reason

Fixed bugs.



# Restrictions and cautions

When the highest-numbered six QSFP+ interfaces on a 5710 switch are used as 40-GE interfaces and configured as IRF physical interfaces, follow these restrictions and guidelines:

- As a best practice, when both ends use one of the first four QSFP+ interface or use one of the last two QSFP+ interfaces, you can use transceiver modules, fiber cables, or copper cables to connect the IRF physical interfaces.
- When one end uses one of the first four QSFP+ interfaces and the other end uses one of the last two QSFP+ interfaces, use transceiver modules or fiber cables to connect IRF physical interfaces.

# Open problems and workarounds

## 202307130980

- Symptom: ARP and ND entries of DRNI extra VLANs cannot be synchronized over the peer link.
- Condition: This symptom might occur if an DRNI member device reboots or its peer-link interface flaps.
- Workaround: None.

# List of solved problems

## Resolved problems in R6710P03

### 202306080897

- Symptom: The device generates message **Failed to save license data to the primary license storage area** at intervals of 24 hours.
- Condition: This symptom occurs when the system fails to read and write the license storage area because of flash memory failure.
- Remarks: None.

### 202305291927

- Symptom: API Device/Base cannot be read on Postman.
- Condition: This symptom might occur when you use Postman to retrieve the Device/Base node.
- Remarks: None.



#### **202305100224**

- Symptom: Protocol packets are dropped in an EVPN VXLAN-DCI network.
- Condition: This symptom occurs if the TTL of the protocol packets is 1.
- Remarks: None.

#### **202211031872**

- Symptom: During the ISSU loading process, one IRF member device experiences packet loss for approximately 18 seconds.
- Condition: This symptom occurs if EVPN VXLAN is configured on IRF member devices, a subordinate member device is restarted, and Layer 3 VXLAN traffic by default matches a blackhole route.
- Remarks: None.

#### **202303131038**

- Symptom: In the output from the display ipv6 interface command, the IPv6 address, interface name, and VPN fields are displayed on different lines, which should be displayed on the same line.
- Condition: This symptom occurs if you execute the display ipv6 interface command.
- Remarks: None.

#### **202305221758**

- Symptom: When the outgoing interface of a VXLAN tunnel is a Layer 3 aggregate interface, the outgoing VXLAN packets carry VLAN tag 4095 unexpectedly. As a result, the peer cannot learn ARP entries.
- Condition: This symptom occurs if the outgoing interface of a VXLAN tunnel is a Layer 3 aggregate interface.
- Remarks: None.

#### **202305300007**

- Symptom: Creation of a VSI interface, Layer 3 subinterface, or Layer 3 aggregate subinterface might fail.
- Condition: This symptom occurs if a VSI interface, Layer 3 subinterface, or Layer 3 aggregate subinterface is created.
- Remarks: None.

#### **202304240579**

- Symptom: Isolation of aggregation member ports no longer takes effect on a DR interface, and the traffic is forwarded between the aggregation member ports.
- Condition: This symptom occurs if the following operations are performed:



- a. Shut down all aggregation member ports of the IPP and DR interfaces, save the configuration, and reboot the device.
  - b. Bring up the aggregation member ports of the IPP.
  - c. After half of the DRNI restoration delay elapses, bring up the aggregation member ports of the DR interfaces.
- Remarks: None.

#### **202209230460**

- Symptom: In gRPC dial-in mode, some sampling paths cannot collect data and the data is collected by other sampling paths.
- Condition: This symptom might occur if you configure multiple sampling paths in gRPC dial-in mode.
- Remarks: None.

#### **202211140499**

- Symptom: OSPF BFD flaps repeatedly.
- Condition: This symptom occurs if you use borrowed loopback interface addresses to establish OSPF neighbor relationship, configure BFD for OSPF, and then reboot the device.
- Remarks: None.

#### **202302150003**

- Symptom: The log file **fabric.log** generated by VCF fabric exhausts the memory.
- Condition: This symptom occurs if the automated deployment scenario of VCF fabric runs for a long period of time or interfaces flap.
- Remarks: None.

#### **202305110216**

- Symptom: On a multicast VXLAN network, multicast traffic cannot be forwarded.
- Condition: This symptom occurs if the device starts with the factory defaults and then you configure multicast VXLAN in the following order: first configure tunnels and VSIs, and then configure multicast.
- Remarks: None.

#### **202304171574**

- Symptom: The switch cannot obtain an IPv6 address after it is rebooted, and IPv6 automatic deployment fails.
- Condition: This symptom occurs if the controller deploys the configuration to change the hardware resource mode during automatic deployment and the controller does not assign a fixed IPv6 address.



- Remarks: None.

#### 202305081426

- Symptom: In an EVPN or VXLAN distributed gateway network, when the device receives a tunneled packet with a source IP address the same as a VSI interface address, the device will reply with a gratuitous ARP response, which can lead to high CPU usage.
- Condition: This symptom might occur if the distributed gateways perform ARP probing in response to traffic.
- Remarks: None.

#### 202306100168

- Symptom: A device attached to an DRNI system with dual-active VLAN gateways configured cannot learn ARP information about a peer.
- Condition: This symptom occurs if a device attached to an DRNI system with dual-active VLAN gateways sends an ARP request to obtain the ARP information about a peer.
- Remarks: None.

#### 202305120926

- Symptom: The device gets stuck after a controller deploys the default action to interfaces on the device.
- Condition: This symptom occurs if the device has port security settings and the controller uses multiple sessions to deploy the default action.
- Remarks: None.

#### 202304250098

- Symptom: After the **peer advertise vpn-reoriginate ibgp** command is executed, the local device removes private AS numbers (in the range of 65512 to 65534) from routes before advertising those routes to the specified peers. This operation affects the results of optimal route selection on the peers. When you execute the **display bgp update-group l2vpn evpn** command to view the update group information for the specified peers, the command output displays **Public-AS-Only: Yes**.
- Condition: This symptom occurs if you execute the **peer advertise vpn-reoriginate ibgp** command. This command enables the device to remove private AS numbers (in the range of 65512 to 65534) from routes before the device advertises those routes to the specified peers.
- Remarks: None.

#### 202305100217

- Symptom: When an endpoint sends an RARP message, the route used for forwarding traffic to the endpoint flaps, and traffic loss occurs.



- Condition: This symptom occurs if an endpoint dualhomed or singlhomed to an EVPN DRNI system sends an RARP packet.
- Remarks: None.

#### 202303160020

- Symptom: When a DHCP user comes online, the DHCP process is closed abnormally.
- Condition: This symptom might occur if the following conditions exist:
  - a. The DHCP user comes online through interface 1 and two IP addresses (for example, IP address A and IP address B) are obtained.
  - b. The DHCP user later comes online through interface 2 and IP address A is obtained.
  - c. The clientinfo entries on the DHCP relay device are reset.

#### 202306060566

- Symptom: After OSPF establishes a neighbor relationship with a neighboring device, the neighbor cannot learn the default route advertised by the local device.
- Condition: This symptom might occur if you create OSPF view without associating any interfaces and then execute the **nssa default-route-advertise** command.
- Remarks: None.

#### 202305200093

- Symptom: The device is disconnected from the controller when a patch is installed from the controller.
- Condition: This symptom occurs if you install a patch from the controller and restart the xmlcfgd process when the patch is installed.
- Remarks: None.

#### 202301120578

- Symptom: After an incremental patch is uninstalled, the **display boot-loader** command does not display information about a non-incremental patch.
- Condition: This symptom occurs if both an incremental patch and a non-incremental patch are installed.
- Remarks: None.

#### 202206071105

- Symptom: When you configure an **s-vid** (outer VLAN IDs) match criterion for a VPLS Ethernet service instance, you can only specify a single VLAN ID and cannot specify a VLAN ID range.
- condition: This symptom occurs when you configure a packet match criterion for an Ethernet service instance of a VPLS network.





#### 202305220011

- Symptom: IP address conflicts occur between four leaf devices because of inconsistent ARP and MAC information, and the CPU usage of the leaf devices reaches 70%.
- Condition: This symptom occurs if the following conditions exist:
  - With ARP proxy enabled, a probe packet is sent when a remote ARP rule for EVPN is withdrawn.
  - A probe packet is sent if a remote ARP rule overwrites a local ARP entry.
- Remarks: None.

## Resolved problems in R6710

#### 202208241285

- Symptom: A QoS policy applied to a control plane cannot filter the protocol packets to the control plane
- Condition: This symptom occurs when you apply a QoS policy to a control plane to filter protocol packets.
- Remarks: None.

#### 202211010383

- Symptom: When a client-oriented MACsec connection is established between an Aruba device and HPE switch, the MACsec protocol cannot come up, and the connection cannot be established correctly.
- Condition: This symptom occurs if a client-oriented MACsec connection is established between an Aruba device and HPE switch.
- Remarks: None.

#### 202204071026

- Symptom: A QoS policy applied to a VSI takes effect only on traffic forwarded at Layer 2 and does not take effect on traffic forwarded at Layer 3.
- Condition: This symptom occurs if a QoS policy is applied to a VSI.
- Remarks: None.

#### 202211050218

- Symptom: After the BFD MAD configuration is deleted from a VLAN interface, the configuration remains.
- Condition: This symptom occurs if the following operations are performed:
  - a. Configure BFD MAD on the VLAN interface, and bind the VLAN interface to a VPN instance.



- b. Configure BFD MAD on an aggregate interface. Bind the aggregate interface to the same VPN instance as the VLAN interface.
  - c. Delete the BFD MAD configuration from the VLAN interface.
  - d. Delete the VLAN interface configured with BFD MAD.
- Remarks: None.

#### 202211050189

- Symptom: After an IRF member device is rebooted, the **display bfd session** command output displays two BFD MAD sessions.
- Condition: This symptom occurs if the following operations are performed:
  - a. Configure BFD MAD on an aggregate interface, and bind the aggregate interface to a VPN instance.
  - b. Delete the BFD MAD configuration from the aggregate interface.
  - c. Configure BFD MAD on a VLAN interface. Bind the VLAN interface to the same VPN instance as the aggregate interface.
  - d. Configure BFD MAD on the aggregate interface again.
  - e. Reboot an IRF member device. After the device is rebooted and the IRF fabric is formed again, execute the **display bfd session** command to display the BFD MAD sessions.
- Remarks: None.

#### 202204090439

- Symptom: The console gets stuck after repeated execution of the **port-security enable** or **port-security port-mode** command.
- Condition: This symptom occurs if the **port-security enable** or **port-security port-mode** command is repeatedly executed.
- Remarks: None.

#### 202207121416

- Symptom: IS-IS neighbors are disconnected during an ISSU.
- Condition: This symptom might occur if the device has established IS-IS neighbor relationships and an ISSU is performed to upgrade the software from 27xx to 67xx.
- Remarks: None.

#### 202209120087

- Symptom: A QoS policy that contains multiple class-behavior associations is applied to the outbound direction of the device. When the actions in a class-behavior association are modified, traffic might match another class-behavior association by mistake.
- Condition: This symptom occurs if the following operations are performed:



- a. Apply a QoS policy to multiple interfaces. A behavior contains the counting or CAR action.
- b. Modify the actions in a traffic behavior or match criteria in a traffic class in the QoS policy or another QoS policy. Or, apply the QoS policy again.

- Remarks: None.

#### **202109131526**

- Symptom: Untagged packets cannot be forwarded for a local VLAN to a remote VXLAN.
- Condition: This symptom might occur if the device is operating in border mode and forwards untagged packets of a local VLAN over a VXLAN tunnel.
- Remarks: None.

#### **202208311310**

- Symptom: IPv6 automated device deployment is interrupted.
- Condition: This symptom might occur if the device performs IPv6 automated device deployment.
- Remarks: None.

#### **202207080423**

- Symptom: MAC authentication users flap on an aggregate interface 8 minutes after they come online.
- Condition: This symptom might occur if MAC authentication user offline detection is enabled by default.
- Remarks: None.

#### **202206291177**

- Symptom: The device receives NA packets that do not carry the target link-layer address field and does not learn ND entries from the NA packets.
- Condition: This symptom might occur if the device receives unrequested NA packets that do not carry the target link-layer address field.
- Remarks: None.

#### **202206230765**

- Symptom: The device reports a permission deny error.
- Condition: This symptom might occur if command authorization is enabled and the **repeat** command is executed for more than 1000 times.
- Remarks: None.

#### **202206060838**

- Symptom: In Layer 3 multicast on a cascaded M-LAG network, IGMP packets are looped between M-LAG interfaces.



- Condition: This symptom occurs if an M-LAG interface receives IGMP query packets.
- Remarks: None.

#### 202210250334

- Symptom: The number of free resources in the **display resource-monitor resource nexthoppool1** command output increases all the time, and a resource alarm is triggered
- Condition: This symptom occurs if the switch learns a large number of ARP entries and you execute the **reset arp** command.
- Remarks: None.

#### 202209200820

- Symptom: Memory is leaked.
- Condition: This symptom occurs if you add and delete Layer 3 aggregate subinterfaces.
- Remarks: None.

#### 202201171691

- Symptom: A QoS policy is still in effect after it is removed from a VSI interface.
- Condition: This symptom occurs if you perform the following operations:
  - a. Create a QoS policy without class-behavior associations, and apply it to a VSI interface.
  - b. Configure a class-behavior association in the QoS policy, and remove the QoS policy from the VSI interface.
- Remarks: None.

#### 202112270288

- Symptom: In an IRF fabric with multichassis aggregation, the memory is exhausted, and the switch reboots when a large number of MAC authentication users come online on an aggregate interface.
- Condition: This symptom occurs if offline detection and reauthentication are enabled.
- Remarks: How many users can cause this problem depends on the size of the memory. In this example, 16000 users come online in four groups at 300 users per second (4000 in each group).

#### 202206010870

- Symptom: In a network with two IRF fabrics, BFD MAD flaps.
- Condition: This symptom occurs if the following operations are performed:
  - a. Enable BFD MAD on interfaces in the same VLAN.
  - b. Perform a master/subordinate switchover on one IRF fabric.
- Remarks: None.



#### 202204290654

- Symptom: In an IRF fabric with multichassis link aggregation, some of the aggregation member ports cannot forward traffic, causing uneven hashing after member ports are shut down and then brought up.
- Condition: This symptom occurs if the aggregate interface acts as an outgoing interface for a VXLAN tunnel.
- Remarks: None.

#### 202204191568

- Symptom: The convergence time of the Monitor Link down function is long.
- Condition: This symptom occurs when the downlink interfaces in a monitor link group are shut down because an uplink interface goes down.
- Remarks: None.

#### 202204230202

- Symptom: A MAC address move does not trigger an ND move.
- Condition: This symptom might occur in an underlay M-LAG network if the **mac-address mac-move fast-update** command is executed.
- Remarks: None.

#### 202109131526

- Symptom: The device cannot forward untagged packets from a VLAN to a remote VXLAN.
- Condition: This symptom occurs if the device in border mode forwards untagged packets from a VLAN out of a VXLAN tunnel.
- Remarks: None.

#### 202205091696

- Symptom: The reply to an HTTP request on a device carries the server:HTTPD field, which is used to identify the server information. The vulnerability scanners consider that the server field might disclose the server information and result in attacks.
- Condition: This symptom occurs if the device receives HTTP requests.
- Remarks: None.

#### 202205091688

- Symptom: The memory leaks for the routed module.
- Condition: This symptom occurs if you configure a gRPC sensor path to collect route information, and then make routes on the device flap.
- Remarks: None.



#### 202203141354

- Symptom: After the device is rebooted, the detection interval configured for the BFD echo session does not take effect, and is displayed as the default value.
- Condition: This symptom occurs if the following operations are performed on a DRNI network:
  - a. Configure a static BFD echo session with a detection interval different from that configured for the BFD echo session on an interface. The session can be negotiated as up.
  - b. Save the configuration, and then reboot the device.
- Remarks: None.

#### 202205171718

- Symptom: When identical static ARP entries are configured on the DR member devices in a DR system, configuration fails on one DR member device.
- Condition: This symptom might occur if identical static ARP entries are configured on the DR member devices in a DR system.
- Remarks: None.

#### 202105150186

- Symptom: After an aggregate interface authenticates a MAC authentication user, an IRF master/subordinate switchover occurs, and the user goes offline 10 minutes later.
- Condition: This symptom occurs if an aggregate interface authenticates a MAC authentication user and an IRF master/subordinate switchover occurs.
- Remarks: None.

#### 202204290651

- Symptom: Layer 3 aggregate subinterfaces do not forward traffic.
- Condition: This symptom might occur if cross-device aggregation is configured in stack deployment and both Layer 3 aggregate subinterfaces and Layer 3 subinterfaces act as equal-cost outgoing interfaces for a VXLAN tunnel.
- Remarks: Shut down and bring up any outgoing interface for the VXLAN tunnel after patch installation.
- Remarks: None.

## Resolved problems in E6702

None.



## Resolved problems in F2708

### 202006240947

- Symptom: When you apply a QoS policy, the system prompts that the QoS and ACL resources are insufficient.
- Condition: This symptom occurs if the traffic classifiers of the QoS policy reference both IPv4 and IPv6 ACLs.
- Remarks: None.

### 202004081619

- Symptom: The device cannot be logged in.
- Condition: This symptom occurs if password control is enabled on the device and the system time change causes the login password to expire.
- Remarks: None.

### 202006150135

- Symptom: When a 10-GE interface on an 5710 24XGT 6QS+/2QS28 Switch JL689A connects to a peer GE interface, packet loss occurs.
- Condition: This symptom occurs if a 10-GE interface on an 5710 24XGT 6QS+/2QS28 Switch JL689A connects to a peer GE interface.
- Remarks: None.

### 202008140876

- Symptom: The time in the **display clock** command output is not accurate.
- Condition: This symptom occurs if the following conditions exist:  
The **clock protocol ntp** command is executed to specify NTP for obtaining the time.  
The time difference between the system and the NTP server exceeds 68 years.
- Remarks: None.

### 202006280209

- Symptom: The number of received packets and the number of sent packets on an interface abnormally increase in the interface statistics.
- Condition: This symptom occurs if a 40-Gbps transceiver module is removed from a 100-GE interface.
- Remarks: None.

### 202010150963

- Symptom: The **reset packet-drop** command cannot clear the dropped packet statistics for an interface.



- Condition: This symptom occurs if the **reset packet-drop** command is executed to clear the dropped packet statistics when congestion occurs on an interface.
- Remarks: None.

#### 202002251001

- Symptom: No error message is prompted for patch installation failure.
- Condition: This symptom occurs if you log in to the device through Telnet or SSH and the patch installation fails.

#### 202005191016

- Symptom: A 10-GE transceiver module inserted into a 40-GE interface by using a 40-GE to 10-GE adapter fails to transmit optical signals correctly.
- Condition: This symptom occurs if a 10-GE transceiver module is inserted into a 40-GE interface by using a 40-GE to 10-GE adapter.
- Remarks: None.

#### 202005090333

- Symptom: After you configure a PBR policy and enable packet statistics for a Layer 3 Ethernet subinterface, the PBR policy cannot take effect.
- Condition: This symptom might occur if you configure a PBR policy and enable packet statistics for a Layer 3 Ethernet subinterface.
- Remarks: None.

#### 202004300168

- Symptom: For a 40-GE interface manually shut down, a 10-GE transceiver module inserted into this interface by using a 40-GE to 10-GE adapter can transmit optical signal correctly. After the transceiver module is removed and reinstalled in the 40-GE interface, the interface comes up.
- Condition: This symptom occurs when the following operations have been performed:
  - a. Execute the **shutdown** command on the 40-GE interface.
  - b. Insert a 40-GE to 10-GE adapter into the 40-GE interface.
  - c. Insert a 10-GE transceiver module into the adapter and connect the interface to a peer device.
  - d. Remove and reinstall the 10-GE transceiver module in the interface.
- Remarks: None.

#### 202004231154/202004240282

- Symptom: In a VRRP group, the device with higher priority is elected as the backup and cannot become the master.





- Condition: This symptom might occur if you continuously modify the device priorities to perform master/backup switchover in the VRRP group (with version VRRPv2 or VRRPv3).
- Remarks: None.

#### 202004290297

- Symptom: The match order of issued PBR policy nodes is incorrect.
- Condition: This symptom might occur if PBR policies are issued to multiple interfaces and the interface (pointing to a next hop in a PBR policy) in an ARP entry has change to another interface.
- Remarks: None.

#### 202004290738

- Symptom: IPv4 or IPv6 Layer 3 VPN traffic is interrupted when the public network routes repeatedly flap on an IRF fabric.
- Condition: This symptom might occur if the following conditions exist:
  - On the IRF fabric, a multichassis aggregate interface acts as the output interface of BGP public network routes.
  - The member ports of the aggregate interface are repeatedly shut down and then brought up.
- Remarks: None.

#### 202001130806

- Symptom: When executing the **irf member renumber** command, the system should output a message indicating that a reboot is required for this command to take effect. However, the system does not output this message.
- Condition: This symptom occurs when the **irf member renumber** command is executed.

#### 201912260195

- Symptom: 10-GE ports on the local device are connected to the breakout interfaces of a 40-GE port on the neighbor device through AOC cables. Packet loss occurs on all the 10-GE ports connected to the breakout interfaces.
- Condition: This symptom occurs if you remove and then insert the AOC cable for one of the 10-GE breakout interfaces on the neighbor device.

#### 202002060416

- Symptom: BFD MAD still remains in Faulty sate on an IRF fabric after the IRF fabric recovers from an IRF split event.
- Condition: This symptom occurs if the following conditions exists:
  - a. The IRF fabric contains two member devices and BFD MAD is configured on the IRF fabric.



- b. The IRF fabric splits and then recovers.

#### 202001190271

- Symptom: The telnet operation hangs with a low probability.
- Condition: This symptom might occur if you telnet to the device, and enable command accounting but the accounting server is not available.

#### 201905210848

- Symptom: The link aggregation module cannot process services when the BFD session flaps.
- Condition: This symptom might occur if you configure collaboration between Ethernet link aggregation and BFD.

#### 202002180298

- Symptom: The packet statistics for VLAN interfaces and VSI interfaces are incorrect.
- Condition: This symptom occurs if packet statistics are collected for VLAN interfaces and VSI interfaces.

#### 201912300910

- Symptom: When the automatic configuration feature is used to replace an IRF member device, the IRF member devices not replaced also reboot during the replacement process.
- Condition: This symptom occurs when the automatic configuration feature is used to replace an IRF member device.

#### 201908060060

- Symptom: The help information for the **display interface** command cannot be displayed.
- Condition: This symptom occurs if the **ifmgr** process is restarted.

#### 201912170482

- Symptom: After a reboot, the switch cannot forward VXLAN traffic based on a static route, and a static ARP entry becomes a blackhole entry.
- Condition: This symptom might occur if the following operations are performed on the switch:
  - a. Configure a static ARP entry.
  - b. Save the running configuration.
  - c. Reboot the switch.

#### 201911040571

- Symptom: Failed to create a VSI interface by using the **interface vsi** command.
- Condition: This symptom might occur if the following operations are performed:
  - a. Create a service loopback group and assign member ports to the service loopback group.
  - b. Create GRE tunnel interfaces.



- c. Create a VSI interface.

#### 201910080448

- Symptom: Transient packet loss occurs on an interface when the **undo packet-filter** command is executed to remove an ACL from the interface.
- Condition: This symptom might occur if the ACL has multiple rules and the action is set to deny in the last rule.

#### 201907290489

- Symptom: The host cannot ping the gateway that has a PBR policy configured.
- Condition: This symptom might occur when you ping the switch (acting as the gateway) configured with a PBR policy from the host.

#### 201906060558

- Symptom: An interface configured with a PBR policy flaps and the PBR policy no longer takes effect when ECMP is configured on the interface.
- Condition: This symptom might occur if ECMP is configured on an interface where a PBR policy is applied.

#### 201905141113/201901070710

- Symptom: Some tunneled packets are lost on the output interface.
- Condition: This symptom occurs when the output interface for tunneled packets changes from a physical interface to an aggregate interface.

#### 201907231134

- Symptom: The session timeout information still exists in the **display dot1x connection** command output after the server deletes the Session-Timeout attribute during an 802.1X reauthentication.
- Condition: This symptom occurs if the server assigns the Session-Timeout attribute to an 802.1X user during the first authentication and then deletes the Session-Timeout attribute during an 802.1X reauthentication.

#### 201907020289

- Symptom: A user fails MAC authentication on an interface if its MAC address has been learned by another interface of the switch.
- Condition: This symptom might occur if a MAC authentication user accesses an interface and its MAC address has been learned by another interface of the switch.

#### 201905210842

- Symptom: Multiple Telnet users exist and cannot be deleted after certain operations are performed.



- Condition: This symptom might occur if the following operations are performed:
  - a. Telnet to the switch from multiple terminals.
  - b. On each terminal, execute the **telnet 127.0.0.1** command multiple times and press Ctrl + K.
  - c. Execute the **display users** command on the switch.

#### 201908010003

- Symptom: The virtual IP addresses of new VRRP groups cannot be pinged after the number of VRRP groups exceeds 512.
- Condition: This symptom might occur if more than 512 VRRP groups are configured.

#### 201908280757

- Symptom: Layer 3 traffic forwarding is interrupted.
- Condition: This symptom might occur after you disable packet statistics for the Layer 3 aggregate subinterface by using the **undo traffic-statistic enable** command.

#### 201905160399

- Symptom: The CPU usage keeps at 100% for a long time after a recursion loop occurs.
- Condition: This symptom might occur if the following conditions exist:
  - The device has two BGP routes, route **1** and route **2**. Route **1** has a primary next hop **a** and a backup next hop **b** (specified by using FRR); route **2** has a primary next hop **b** and a backup next hop **a** (specified by using FRR).
  - Both **a** and **b** are on the same network segment as the destination networks of route **1** and route **2**.
  - The interfaces pointing to both **a** and **b** go down within a short period of time. As a result, the device selects the backup next hop for both routes. A recursion loop occurs.

## Resolved problems in R2702

#### 201905200485/201901090410

- Symptom: On the IRF fabric, the management address fails to be displayed in the LLDP information received from the neighboring devices.
- Condition: This symptom might occur if the following conditions exist:
  - a. VLAN interfaces are created on the IRF fabric and IP addresses are assigned to the interfaces.
  - b. An IRF subordinate device reboots.

#### 201812060001

- Symptom: The XMLCFGD process creates a core file unexpectedly.



- Condition: This symptom might occur if a NETCONF connection is established to the device to manage the device and NETCONF is used to reboot the device.

#### 201809290321

- Symptom: On a DRNI network, a device reboots because of memory exhaustion.
- Condition: This symptom might occur if the following conditions exist:
  - a. The keepalive timeout timer on the secondary DR member device is set to the maximum value.
  - b. A configuration rollback is performed on the primary DR member device to cancel the DRNI configuration and then another configuration rollback is performed to recover the DRNI configuration.

#### 201902010798

- Symptom: A device management user fails to obtain another user role by using the **super** command.
- Condition: This symptom might occur if the device management user logs in to the device after passing HWTACACS authentication and executes the **super** command to obtain another user role.

#### 201904010489

- Symptom: The device fails to forward traffic correctly.
- Condition: This symptom might occur if a loop exists on the device, which causes the ARP table to update repeatedly and then causes FIB table update failure.

#### 201903211294

- Symptom: The device reboots unexpectedly.
- Condition: This symptom might occur if the control plane deploys entries that contain unassigned IP addresses to the data plane on a control-/data-plane separated network.

#### 201807190673

- Symptom: The ofcd process fails because of exception.
- Condition: This symptom might occur if the established OpenFlow tunnel is attacked by exception OpenFlow packets in which the length of the protocol header field is 0.

#### 201809110564

- Symptom: The cp process still remains on the device after the connection to the controller is terminated.
- Condition: This symptom might occur if the controller deploys the **save** command through NETCONF to save the running configuration and then terminates the connection to the device.



#### 201811060548

- Symptom: The CPU usage rises rapidly during inter-VPN traffic forwarding.
- Condition: This symptom might occur if BGP redirects direct routes between multiple VPN instances.

#### 201809200079

- Symptom: The RADIUS server fails to assign an authorization VLAN name to a user after the user passes authentication.
- Condition: This symptom might occur if the authorization VLAN name is in the format of \000XXXXX\000.

#### 201904010490

- Symptom: The device reboots unexpectedly.
- Condition: This symptom might occur if ARP entries are deleted when SNMP is walking the ARP table.

#### 201904020841

- Symptom: The device reboots unexpectedly.
- Condition: This symptom might occur if TCP MSS is set on a subinterface and the subinterface is repeatedly deleted and created when SLB traffic is forwarded.

#### 201807300378/201905090714

- Symptom: A memory leak occurs on the SNMP process.
- Condition: This symptom occurs if the following conditions exist:
  - a. SNMP notifications for system logs are disabled.
  - b. The NMS walks the SYSLOG-MSG-MIB to obtain data.

#### 201811070579

- Symptom: The lauthd process creates a core file unexpectedly.
- Condition: This symptom might occur if the **local-user-export class network guest url b** command is executed consecutively several times.

#### 201811060248

- Symptom: The IMC server forcibly logs out a portal user after the user passes portal authentication.
- Condition: This symptom might occur if the portal authentication server runs IMC PLAT 7.3 and security policy confirmation (such as ACL and VLAN) is deployed on the IMC server.

#### 201810230548/201809120806

- Symptom: A memory leakage occurs on a subordinate device in an IRF fabric.



- Condition: This symptom might occur if portal users that obtain IP addresses through DHCP carries Option 82 or Option 18 when they come online.

#### **201809200058**

- Symptom: The Aaad process on an IRF fabric creates a core file unexpectedly.
- Condition: This symptom might occur if the following conditions exist:
  - A large number of IPoE users come online through the IRF fabric.
  - Master/subordinate switchover repeatedly takes place.
  - The AAA process reboots repeatedly.

#### **201812070009/201812061078**

- Symptom: Specific UDP packets get lost during forwarding.
- Condition: This symptom might occur if a UDP packet has the following characteristics:
  - The packet is a fragment packet.
  - The packet carries MPLS labels.
  - The third and fourth bytes in the IP header of non-first fragment packets is 0D AF.

#### **201811060034**

- Symptom: An IPsec SA is established between the device and the peer device through IKEv2 negotiation and the security protocol is ESP. IPsec protocol packets from the peer device are discarded because the packet length exceeds the port MTU.
- Condition: This symptom might occur if TFC padding is enabled and IPsec packet fragmentation is disabled on the peer device.

#### **201903211236**

- Symptom: The CLI of a device in an IRF fabric gets stuck and no commands can be input.
- Condition: This symptom might occur if a large number of tunnels flap and IRF master/subordinate switchover repeatedly takes place.

#### **201902020055**

- Symptom: IS-IS neighbor relationship cannot be established.
- Condition: This symptom occurs if the following operations are performed:
  - a. Configure the network type as P2P and enable IS-IS on an interface.
  - b. Reboot the device.

#### **201904020277**

- Symptom: ARP entries become blackhole entries, and packets are lost.
- Condition: This symptom occurs if the following operations are performed:



- a. Multiple Layer 2 aggregation groups exist in the network, and loops exist in some aggregation groups.
- b. Enable ARP active acknowledgement.
- c. Configure static routes on a Layer 3 interface. Shut down and then bring up the Layer 3 interface, or MAC address moves occur on the Layer 3 interface.

#### **201902020232**

- Symptom: The master IRF member device might reboot unexpectedly at a low probability.
- Condition: This symptom occurs if the following operations are performed:
  - a. Set a small idle timeout value for TCP connections.
  - b. Initiate a large number of TCP connections for services using TCP (for example, BGP and HTTP) on the local end.

#### **201811060022**

- Symptom: The memory leaks for the IPFS module.
- Condition: This symptom occurs if the following conditions exist:
  - A large amount of traffic with varying quintuples is forwarded by software.
  - The fast forwarding entries age out.

#### **201902020140**

- Symptom: After the TCP client connection is closed, the memory leaks.
- Condition: This symptom occurs if the following operations are performed:
  - a. The client sends a large amount of data to the server. The server cannot process so much data, so the server responds with Zero Window.
  - b. The client starts the persist timer after receiving Zero Window.
  - c. The client actively closes the connection.

#### **201902020187**

- Symptom: The CPU usage might be high at a low probability.
- Condition: This symptom occurs if a large number of packets are transmitted when a user logs in through nested Telnet.

#### **201812070478**

- Symptom: An interface on a subordinate IRF member device cannot join a voice VLAN again after leaving the voice VLAN.
- Condition: This symptom occurs if the following operations are performed:
  - a. Enable LLDP on an interface on a subordinate IRF member device, and configure a voice VLAN on the interface. Connect the interface to a voice device supporting LLDP/CDP.





- b. Establish or disconnect the LLDP neighbor relationship on the subordinate IRF member device.

#### 201811060177

- Symptom: After an IP phone successfully comes online, the gateway cannot ping the IP phone for a period of time.
- Condition: This symptom occurs if the following operations are performed:
  - a. Connect an interface to a Cisco IP phone, enable CDP-compatible LLDP on the interface, and assign the IP phone to a voice VLAN.
  - b. The interface repeatedly comes up and goes down.

#### 201811060399

- Symptom: A DHCP client cannot obtain an IP address.
- Condition: This symptom occurs if the device acts as a DHCP sever, multiple address pools are configured, and some address pools are configured with address ranges for dynamic allocation by using the **address range** command.

#### 201812060884

- Symptom: The XMLCFGD process exits exceptionally.
- Condition: This symptom occurs if the following operations are performed:
  - a. The device acts as a DHCP Sever. In a DHCP address pool, configure more than 13 static IP address bindings.
  - b. Use SoapUI to get the data of the DHCP/DHCPStatic table.

#### 201810290644

- Symptom: During auto upgrade, the **using tengige** command is mistakenly executed. As a result, the comsh process becomes abnormal, and related interfaces disappear.
- Condition: This symptom occurs because the **using tengige** command is mistakenly executed during the configuration recovery process. On the device, the **using tengige** command takes effect in real time, but the configuration file incorrectly contains the command.

#### 201903290556

- Symptom: Interface flapping causes the CPU usage to reach 100%.
- Condition: This symptom occurs if the following operations are performed:
  - a. Multiple routes of BGP neighbors are configured with FRR. The active and backup next hops of FRR are reverse for two routes (for example, the active and backup next hops of route A are 1 and 2, and the active and backup next hops of route B are 2 and 1), and the next hops 1 and 2 are in the network segments of routes A and B.
  - b. Shut down the interfaces corresponding to the two next hops in sequence.



#### 201903290558

- Symptom: When the spanning tree mode is switched to PVST, the device will be stuck for a period of time.
- Condition: This symptom occurs if a large number of VLANs and interfaces exist on the device and the spanning tree mode is switched to PVST.

#### 201811060535

- Symptom: When an interface card is unplugged and plugged, the aggregate interface creation event on the interface card is not reported. As a result, the aggregate interface on the interface card is not set to the drive, and the aggregate interface member ports cannot forward traffic.
- Condition: This symptom occurs because the interface management module does not report the aggregate interface creation event during the startup process when an interface card is plugged.
- Occurrence probability: This symptom occurs only when interface events are not reported. In an environment, there are a large number of interface events. In a complicated environment, the occurrence probability is high. In a test environment, the occurrence probability is low.

#### 201807060250

- Symptom: Some traffic is broadcast on a DR interface.
- Condition: This symptom occurs if an aggregate interface leaves and then joins a DR group and continuously receives traffic.

#### 201903110087

- Symptom: The BFD session on a Layer 3 aggregate interface flaps.
- Condition: This symptom occurs if the following operations have been performed:
  - a. Configure a Layer 3 aggregate interface with member ports on different cards, enable BFD for OSPF, and use MD5 authentication for BFD control packets.
  - b. Remove a member port from the Layer 3 aggregation group and then add it back to the aggregation group.

#### 201806040598

- Symptom: The secure MAC address entry is not removed from the **display mac-address** command after a user goes offline.
- Condition: This symptom occurs if port security is configured and the user goes offline after passing authentication.

#### 201701100257

- Symptom: Traffic detection fails in a Fabric Director scenario.
- Condition: This symptom occurs if a QoS policy is issued multiple times.



#### 201806070741

- Symptom: The **remark dscp** command issued by OpenFlow does not take effect.
- Condition: This symptom occurs if the Output action is issued by OpenFlow at the same time.

#### 201904020301

- Symptom: The relevant MAC address entry is not removed from the **display mac-address** command after an 802.1X user moves to a different VLAN on the same port.
- Condition: This symptom occurs if an 802.1X user moves to a different VLAN on the same port.

#### 201904110239

- Symptom: A DR system fails to be established.
- Condition: This symptom occurs if a manually created tunnel interface is used as the IPL.

#### 201903150058

- Symptom: In a DRNI network, the DR interface of the secondary DR device is still up after the IPP interface is brought down.
- Condition: This symptom occurs if the secondary DR device is in DRNI MAD DOWN state.

#### 201812060999

- Symptom: In a DRNI network, the DR interface is set to DRNI DOWN state.
- Condition: This symptom might occur if the IPP interface flaps.

#### 201805040745

- Symptom: In a multiple VSC environment, the device cannot connect to the primary VSC.
- Condition: This symptom might occur if the OVSDB process is restarted.

#### 201810300310

- Symptom: The management Ethernet port goes down in an IRF fabric.
- Condition: This symptom might occur after a master/subordinate switchover is performed.

#### 201711070993

- Symptom: In a VXLAN network, VMs in different network segments cannot communicate.
- Condition: This symptom occurs if a VXLAN gateway group is used as the gateway.

#### 201805020138/201805020139

- Symptom: An additional coldStart log is printed every time the switch sends a trap.
- Condition: This symptom occurs after the switch reboots.

#### 201904020313

- Symptom: A user can join and leave the multicast group without passing authentication.



- Condition: This symptom occurs if both MLD and IPv6 portal authentication are configured on the VLAN interface.

#### 201903180860

- Symptom: A serial port hangs in a DRNI network.
- Condition: This symptom might occur if the following operations have been performed:
  - a. Enable and disable configuration consistency check repeatedly.
  - b. Execute the **display drni consistency type2 global** command.

#### 201810100474

- Symptom: ICMPv6 packets are counted into the **IP-other** protocol type.
- Condition: This symptom occurs when the switch receives ICMPv6 packets.

#### 201811090192

- Symptom: The MAC address entry is not removed from the **display mac-address** command after a MAC authentication user goes offline.
- Condition: This symptom occurs if the MAC authentication user comes online and then goes offline.

#### 201904030323

- Symptom: The remote host has the TCP timestamps vulnerability.
- Condition: This symptom occurs if the host implements RFC 1323.

#### 201812061014

- Symptom: HPE Comware 7 stored and reflected XSS Vulnerability
- Condition: An xss reflected in the web portal of the appliance HP Comware switch 7.1.045. Attackers can exploit this issue to open a web browser and log in to the application using valid or not credentials.

#### 201902010459

- Symptom: CVE-2018-5407
- Condition: OpenSSL is prone to a local information-disclosure vulnerability. Local attackers can exploit this issue to obtain sensitive information. This may aid in further attacks.

#### 201812050851

- Symptom: Files in the flash might fail to be deleted at a low probability.
- Condition: This symptom occurs if multiple consoles operate the device simultaneously.

#### 201811230657

- Symptom: CVE-2018-15473



- Condition: OpenSSH is prone to a user-enumeration vulnerability. An attacker may leverage this issue to harvest valid user accounts, which may aid in brute-force attacks. OpenSSH through 7.7 are vulnerable; other versions may also be affected.

#### **201903140269/201904020861**

- Symptom: After the operating mode of a device is switched from L3GW to L2GW, the L3VNI configuration remains.
- Condition: This symptom occurs if the following operations are performed:
  - a. Configure the device to operate in L3GW mode, and configure L3VNIs.
  - b. Configure the device to operate in L2GW mode, save the configuration, and reboot the device.

## **Resolved problems in R2612P05**

#### **201902220726/201810240573**

- Symptom: After the switch restarts up with the factory defaults, the DHCP server assigns the switch a new IP address instead of the one before the restart.
- Condition: This symptom occurs if the switch restarts up with the factory defaults and acts as a DHCP client.

#### **201902220813**

- Symptom: If VRRP groups with the same ID are configured on different VLAN interfaces, only one of the VRRP groups takes effect.
- Condition: This symptom might occur if VRRP groups with the same ID are configured on different VLAN interfaces.

#### **201902220757**

- Symptom: SNMP fails to get the MAC address of an aggregate interface from the dot1dTpFdbAddress node.
- Condition: This symptom might occur if SNMP reads the dot1dTpFdbAddress node.

#### **201902220753/201810110532**

- Symptom: After the aggregate interface of an aggregation group is assigned to an isolation group and then is removed from it, traffic received on a member port of the aggregation group is forwarded out of other member ports erroneously.
- Condition: This symptom might occur if an aggregate interface is assigned to an isolation group and then is removed from it.



#### **201902220749**

- Symptom: After queue scheduling is configured on an interface, transient traffic loss occurs on a non-related interface.
- Condition: This symptom might occur if queue scheduling is configured on an interface.

#### **201902220748**

- Symptom: The switch might generate dead loop logs when deleting multicast entries.
- Condition: This symptom might occur if the following conditions exist:
  - a. A large number of aggregate interfaces are configured, and they receive dense multicast traffic.
  - b. Aggregate interfaces are shut down.

#### **201902220732**

- Symptom: BGP sessions are interrupted.
- Condition: This symptom occurs if the following operations are performed:
  - a. A Layer 3 virtual interface is bound to a VPN, and a BGP neighbor relationship is established.
  - b. PBR is applied to the Layer 3 virtual interface.

#### **201902220722**

- Symptom: In a VCF fabric, IP addresses are re-assigned to Loopback 0 interfaces after leaf nodes automatically form an IRF fabric.
- Condition: This symptom might occur if the switch as a leaf node joins the IRF fabric automatically formed by other leaf nodes.

#### **201902220710/201812030086**

- Symptom: Packet loss might occur.
- Condition: This symptom occurs if link-aggregation traffic redirection is configured and some slots are rebooted.

#### **201902220704/201812050851**

- Symptom: Files in the flash might fail to be deleted at a low probability.
- Condition: This symptom occurs if multiple consoles operate the device simultaneously.

#### **201902220665/201803280447**

- Symptom: On an IRF fabric, the state of a VXLAN tunnel is inconsistent on the IRF master and subordinate, which causes VXLAN forwarding failure.
- Condition: This symptom might occur if VXLAN tunnels are configured on an IRF fabric.



#### **201903131055/201903131049/201903131051**

- Symptom: The PBR function might not take effect on interfaces.
- Condition: This symptom occurs if the following operations are performed:
  - a. PBR is configured on multiple interfaces.
  - b. Route flapping frequently occurs.

#### **201903140301/201903140302/201709130770**

- Symptom: Traffic might fail to be forwarded between VXLANs.
- Condition: This symptom occurs if the following operations are performed:
  - a. The VCFC controller deploys configurations to spine and leaf devices.
  - b. On a leaf device, multiple VXLANs are configured, and a large number of VMs come online.
  - c. A large number of VMs migrate to other VXLANs.

## **Resolved problems in R2612P03**

#### **201809120302**

- Symptom: Multiple copies of packets mirrored by Layer 2 remote port mirroring are received.
- Condition: This symptom occurs if the following operations are performed:
  - a. Create multiple mirroring groups, and assign ports to mirroring groups.
  - b. Configure reflector ports for remote mirroring groups.

#### **201809050319/201808230872**

- Symptom: After NETCONF is used to deploy the BFD-related configuration, the BFD process fails to start.
- Condition: This symptom occurs if NETCONF is used to deploy the BFD configuration.

#### **201809050305**

- Symptom: When an IPL fails, the corresponding Layer 3 interfaces cannot properly learn ARP entries. As a result, traffic is interrupted.
- Condition: This symptom occurs if the following operations are performed:
  - a. In a DRNI network, configure the same MAC address for the VLAN interfaces of the VLANs to which the DR interfaces of the IPL belong.
  - b. Shut down the IPL.

#### **201809040359/201809030027/201809030023**

- Symptom: After an IRF master/subordinate switchover, the AC configuration on the device might be deleted and the VM traffic cannot be forwarded at a low probability.



- Condition: This symptom occurs if the following operations are performed:
  - a. On an IRF fabric, the controller automatically deploys the VXLAN function.
  - b. Reboot the master IRF member device.

## Resolved problems in R2612P01

### **201807270157/201806210622**

- Symptom: When you use Director to replace the master spine device, the leaf device configuration changes.
- Condition: This symptom occurs if the automated VCF fabric deployment function is used to enable the device to cooperate with Director and implement automated configurations.

### **201807270712/201807270721/201807270711**

- Symptom: After a master/subordinate switchover, an IRF fabric sends redundant RSCN packets to servers.
- Condition: This symptom occurs if the following operations are performed:
  - a. In an FCoE network, enable hardware zoning and configure RSCN on an IRF fabric.
  - b. Reboot the master IRF member device.

### **201808060501/201808060502/201808060503**

- Symptom: The controller might fail to deploy flow entries to the subordinate IRF member devices.
- Condition: This symptom occurs if the following operations are performed:
  - a. An IRF fabric acts as an OpenFlow switch and establishes a secure channel with the controller.
  - b. The controller deploys flow entries to the subordinate IRF member devices.

### **201807270142/201806200386/201805300594**

- Symptom: After the DR interface comes up, it will go down and then come up once.
- Condition: This symptom occurs if you view the DR interface status after the IPL comes up.

### **201807270145/201806250510/201803190222**

- Symptom: A client cannot join a multicast group.
- Condition: This symptom occurs if the client comes online through portal and requests to join the multicast group in a multicast network.

### **201807270161/201806120577/201806270423/201806120577**

- Symptom: After the reload delay timer set for a DR device expires, the DR device role is still None.





- Condition: This symptom occurs if the following operations are performed:
  - a. Execute the **drni auto-recovery reload-delay *delay-value*** command to enable DR system auto-recovery and set the reload delay timer.
  - b. Configure both the IPP and keepalive link to be down.
  - c. Save the configuration and reboot the DR device.

#### **201807270168/201806270402/201806070375/201806070389**

- Symptom: When the **display drni role** command is used to display DR role information on the secondary DR device, the **Effective role** field displays **Primary**.
- Condition: This symptom occurs if the IPP is repeatedly shut down and brought up in a DRNI network.

#### **201807270130/201807030034/201806290366/201806290360**

- Symptom: After the whole IRF fabric is rebooted, SNMP obtains an incorrect value for the snmpEngineBoots node.
- Condition: This symptom might occur if the master member device of the IRF fabric changes after the IRF fabric is rebooted.

#### **201807270124/201806270357/201806040701**

- Symptom: The chip time is different on the master IRF member device and subordinate IRF member device.
- Condition: This symptom occurs if an IRF fabric is configured with PTP and the chip time on the master IRF member device and subordinate IRF member device is viewed.

#### **201806260327/201807270176/201807060219**

- Symptom: A DR system fails after certain operations are performed.
- Condition: This symptom might occur if the following operations are performed:
  - a. Configure a tunnel interface as the IPP.
  - b. Configure dynamic tunnels on the DR member devices, and the dynamic tunnels share the destination IP address with the tunnel that acts as the IPL.
  - c. Delete the IPP tunnel interface and reconfigure it.

#### **201807270182/201807030632/201807310533**

- Symptom: On the secondary DR member device, a DR interface in DRNI DOWN state is removed from its DR group. After the DR interface is reassigned to the DR group, its state becomes DOWN.
- Condition: This symptom might occur if the following operations are performed:
  - a. Configure a Layer 2 aggregate interface as a DR interface and assign it to a DR group on the secondary DR member device.



- b. Remove the DR interface from its DR group and then reassign it to the DR group when the IPL is down.

#### **201807270188/201806010178/201807030865**

- Symptom: On a DR member device, member ports of a DR interface cannot become Selected after the device is rebooted.
- Condition: This symptom might occur if the following operations are performed:
  - a. Execute the **lACP edge-port** command on the DR interface.
  - b. Save the configuration and reboot the DR member device.

#### **201807270193/201807070082/201807070098**

- Symptom: RSVP has memory leaks if RSVP authentication fails.
- Condition: This symptom might occur if RSVP authentication fails.

#### **201807270196/201807100205/201807100209**

- Symptom: Memory leaks occur if the switch repeatedly generates and deletes a large number of multicast entries.
- Condition: This symptom might occur if the switch repeatedly generates and deletes a large number of multicast entries.

#### **201807060212/201807270199/201807060355**

- Symptom: DR member devices might fail to forward Layer 3 traffic after certain operations are performed.
- Condition: This symptom might occur if the following operations are performed:
  - a. Configure a VXLAN tunnel interface as the IPP of the DR system.
  - b. Configure the DR member devices to establish dynamic tunnels to external networks.
  - c. Delete the VXLAN tunnel interface.
  - d. Shut down and then bring up the interfaces connected to the external networks.
  - e. Create a VXLAN tunnel interface and configure it as the IPP.

#### **201807270206/201806290774/201807100295**

- Symptom: Third-party services, service chain, and PBR are configured on an 5940 switch that acts as a leaf node in a VCF fabric. After the **reset arp all** command is executed, PBR configuration does not take effect.
- Condition: This symptom might occur if the **reset arp all** command is executed on the 5940 switch.

#### **201807270207/201806280646/201806270600**

- Symptom: Memory leaks for the OVSD module. About 50 bytes leak every 10 seconds. If the controller re-deploys the configuration, about 80 bytes leak.



- Condition: This symptom occurs if the device has the OVSDb service enabled, and the data in the OVSDb database are modified after the controller deploys a global table containing the master controller IP to the OVSDb database.

#### 201807170279/201807270285/201804100876

- Symptom: The device name configured for a device by using the **sysname** command does not take effect.
- Condition: This symptom occurs if the following operations are performed:
  - a. Configure automated underlay network deployment on the device.
  - b. Use the **sysname** command to modify the device name, save the configuration, and reboot the device.

#### 201807270468/201805220131

- Symptom: After the device runs for a period of time, the MACsec data packets cannot be forwarded.
- Condition: This symptom occurs if the device acts as a MACsec client and establishes a device-oriented MACsec network with a Huawei or Cisco device.

#### 201807270215/201806260106/201806250611

- Symptom: The device might reboot unexpectedly.
- Condition: This symptom occurs if an aggregation group has more than 32 member ports and any member port leaves the aggregation group.

#### 201808210067

- Symptom: If the **undo irf mac-address persistent** command is executed on an IRF fabric configured with VXLAN, overlay traffic forwarding fails after an IRF master/subordinate switchover.
- Condition: This symptom might occur if the **undo irf mac-address persistent** command is executed on an IRF fabric configured with VXLAN, and an IRF master/subordinate switchover occurs.

## Resolved problems in R2612

#### 201805120143/201805120129

- Symptom: Auto-RP listening does not take effect.
- Condition: This symptom might occur if the following operations are performed:
  - a. Enable Auto-RP listening on the device.
  - b. Configure a Layer 2 aggregate interface as a trunk port and assign it to a VLAN.
  - c. Enable PIM-SM on the VLAN interface.



#### 201805110585

- Symptom: On a DRNI+STP network, traffic interruption occurs after the IPL goes down and then comes up.
- Condition: This symptom might occur if the following operations are performed:
  - a. Configure an aggregate interface on each DR member device as the IPP.
  - b. Reboot a DR member device so that the DR member devices are assigned new roles.

#### 201805110581/201803270029

- Symptom: On a DRNI+STP network where the DR system operates correctly, it takes DR interfaces ten minutes to come up after they are set to DRNI MAD DOWN state.
- Condition: This symptom might occur if a DR member device reboots and then the IPP goes down.

#### 201805110456

- Symptom: The ovsdb-server process exits unexpectedly.
- Condition: This symptom might occur after a VTEP is enabled with the OVSDb server feature and establishes an OVSDb connection with the controller.

#### 201805090685

- Symptom: An IRF subordinate device reboots unexpectedly after the **display interface** command is executed on the IRF fabric.
- Condition: This symptom might occur if Layer 3 Ethernet subinterfaces are created on the IRF fabric.

#### 201805070301

- Symptom: The OVSDb connection to the controller is disconnected after a length of time since a VTEP has been enabled with the OVSDb server feature and established an OVSDb connection to the controller.
- Condition: This symptom might occur after a length of time since a VTEP has been enabled with the OVSDb server feature and established an OVSDb connection to the controller.

#### 201805050184

- Symptom: The device fails to set the VXLAN hardware resource mode.
- Condition: This symptom might occur if the following operations:
  - a. Set the VXLAN hardware resource mode.
  - b. Save the running configuration and reboot the device.
  - c. Use the **display hardware-resource** command to display the VXLAN hardware resource mode. The displayed hardware resource mode is not the specified one.



#### 201805100244

- Symptom: The remote fault signal detection feature, which is supported only on fiber ports, can be enabled on copper ports.
- Condition: This symptom might occur if the **link-fault-signal enable** command is executed on copper ports.

#### 201805090323

- Symptom: The system prompts unsupported operation if the speed of a 100-GE interface is repeatedly changed between 100000 Mbps and 10000 Mbps.
- Condition: This symptom might occur if the speed of a 100-GE interface is repeatedly changed between 100000 Mbps and 10000 Mbps by using the **speed 100000** and **speed 10000** commands.

#### 201805040458

- Symptom: The memory of the QACL module slowly leaks.
- Condition: This symptom occurs if actions in traffic behaviors are dynamically modified repeatedly.

#### 201805020139

- Symptom: The device prints coldStart traps unexpectedly when printing port security traps.
- Condition: This symptom occurs when the device is rebooted and prints port security traps.

#### 201805020133

- Symptom: When the device learns secure MAC address entries, it prints the same traps for twice.
- Condition: This symptom occurs if the device has port security enabled and is configured with secure MAC address entries.

#### 201804250026

- Symptom: The Connect Retry timer times out. As a result, BGP might flap.
- Condition: This symptom occurs if the following operations are performed:
  - a. On an IRF fabric, configure BGP NSR.
  - b. Reboot the device after the device has run for a long period of time.

#### 201803270632

- Symptom: The 802.1p-to-local priority map might be modified.
- Condition: This symptom occurs if the following operations are performed:
  - a. Split a 100-GE interface into four breakout interfaces.
  - b. Configure the 802.1p-to-local priority map.



- c. Combine the breakout interfaces into a 100-GE interface.

#### 201804170805

- Symptom: An interface fails to join an aggregation group.
- Condition: This symptom occurs if the following operations are performed:
  - a. Execute the **vtep access port** command to specify a site-facing interface as a VTEP access port.
  - b. Create an aggregation group, and assign the interface to the aggregation group.

#### 201804160611

- Symptom: When the TTL in IPv6 BGP protocol packets is 1, the packets mistakenly match an ACL used for matching IPv6 packets with TTL as 1. As a result, the link flaps.
- Condition: This symptom occurs if IPv6 BGP protocol packets with TTL as 1 are received.

#### 201804120615

- Symptom: A user cannot log in to the device by using NETCONF after certain operations when password control is enabled.
- Condition: This symptom occurs if the following operations are performed:
  - a. Enable password control on the device.
  - b. Repeatedly establish and delete sessions, and perform active/standby process switchover.
  - c. Log in to the device by using NETCONF.

#### 201804120137

- Symptom: In a DRNI network, MAC address entries fail to be synchronized between the primary and secondary devices.
- Condition: This symptom occurs if the following operations are performed:
  - a. In a DRNI, execute the **shutdown** and **undo shutdown** commands on the IPP.
  - b. The device receives a large number of Layer 2 packets with changing source MAC addresses.

#### 201803150880

- Symptom: VLAN-based VXLAN assignment configuration cannot be restored by using an .mdb binary file.
- Condition: This symptom might occur if the following operations are performed:
  - a. Configure a large number of VSIs and enable VLAN-based VXLAN assignment.
  - b. Save the configuration, reboot the switch, and use an .mdb binary file to restore the configuration.



#### 201802280277

- Symptom: The controller cannot discover the site-facing interfaces configured by using **vtep access port** if the switch uses Chinese GB2312 characters as the sysname.
- Condition: This symptom might occur if the sysname of the switch contains Chinese GB2312 characters.

#### 201805150032/201712060462/201712060449

- Symptom: The switch reboots unexpectedly.
- Condition: This symptom occurs if the debugging command is used to disable the linkscan for interfaces.

#### 201805100905/201805100908

- Symptom: The switch acts as a VXLAN VTEP, and an Ethernet service instance that uses the **encapsulation default** criterion is configured on an aggregate interface. After the aggregate interface is shut down and then brought up, traffic received on the Ethernet service instance cannot be forwarded correctly.
- Condition: This symptom might occur if an Ethernet service instance that uses the **encapsulation default** criterion is configured on an aggregate interface, and the aggregate interface is shut down and then brought up.

#### 201804240046/201802240168/201709010504

- Symptom: ACLs might remain at a low probability after certain operations.
- Condition: This symptom occurs if the following operations are performed:
  - a. Configure a routing policy, and specify the next hop of the routing policy as a GRE tunnel interface.
  - b. Modify the source IP address of the GRE tunnel.

#### 201805290161/201805280462

- Symptom: Disabling MAC address learning does not take effect on a Layer 2 aggregate interface.
- Condition: This symptom occurs if the following operations are performed:
  - a. Disable MAC address learning globally.
  - b. In the view of a Layer 2 aggregate interface, execute the **undo mac-address mac-learning enable** command to disable MAC address learning.

#### 201805290049/201805280775

- Symptom: The CLI does not respond after password control is disabled.
- Condition: This symptom occurs if the following operations are performed:
  - a. Enable Password Control on the device. A large number of invalid NETCONF users log in to the device.



- b. Disable password control.**

**201805250503/201805250377**

- Symptom: Some ACL resources remain.
- Condition: This symptom occurs if the following operations are performed:
  - a. The switch operates in FCF mode and connects to multiple nodes.
  - b. Modify the bridge MAC address of the switch.

**201805240699/201805220499**

- Symptom: The device prints deadlock logs when the **step** command is used to modify the rule numbering step for an ACL.
- Condition: This symptom occurs if the following operations are performed:
  - a. Configure a PBR policy on the device, and configure rules for the ACL that the PBR policy uses.
  - b. Apply the PBR policy to packets that an interface forwards.
  - c. Enter the view of the ACL, and use the **step** command to set the rule numbering step.

**201805240599/201805150488**

- Symptom: OpenFlow is disconnected from the controller.
- Condition: This symptom occurs if the following operations are performed:
  - a. Configure OpenFlow on the device and establish a connection to the controller.
  - b. The interface corresponding to the AC is frequently shut down and brought up.

**201805310080/201805310084/201805310093**

- Symptom: The broadcast packets received on a member port of an aggregation group might be broadcast out of other member ports of the aggregation group.
- Condition: This symptom occurs if the following operations are performed:
  - a. Assign local ports to an aggregation group. Delete the aggregation group. Restore the default settings for member ports, and then assign these ports to the aggregation group.
  - b. Execute the **shutdown** and **undo shutdown** command sequence on the aggregation group member ports.
  - c. Switch the mode of the aggregation group to dynamic or static.
  - d. The local device is an STP root bridge. An interface on the peer device repeatedly flaps, and the peer device sends TCN BPDUs.

**201712200877**

- Symptom: CVE-2017-12190
- Condition: Local attacker can exploit these issues to obtain sensitive information that may lead to further attacks.





- Symptom: CVE-2017-12192
- Condition: Attackers can exploit this issue to cause denial-of-service conditions. Due to the nature of this issue, arbitrary code execution may be possible but this has not been confirmed.
- Symptom: CVE-2017-15274
- Condition: An attacker can exploit this issue to cause a local denial-of-service condition.
- Symptom: CVE-2017-15299
- Condition: An attacker can exploit this issue to trigger a kernel panic, denying service to legitimate users.

## Resolved problems in R2611

First release.

## Software upgrade guidelines

Please refer to HPE 5710-CMW710-R6710P03 release notes.