

HPE 5950-CMW710-R6301P02

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	4
Restrictions and cautions	4
Open problems and workarounds	5
List of solved problems	5
Resolved problems in R6301P02	5
Resolved problems in R6301P01	6
Resolved problems in R6301	6
Resolved problems in F6207	15
Resolved problems in F6206	16
Resolved problems in R6205P03	20
Resolved problems in F6205P02	21
Resolved problems in F6205	22
Resolved problems in F6203	24
Resolved problems in F6202	25
Resolved problems in R6125	25
Resolved problems in R6123	27
Resolved problems in R6106P01	29
Resolved problems in R6106	29
Resolved problems in R6105	29
Software upgrade guidelines	29

Version information

Version number

Version number (outer): HPE Comware Software, Version 7.1.070, Release 6301P02

Version number (inner): V300R009B03D007SP0302

Version history

Table 1 Version history

Version number(inner)	Version Number(outer)	Based Version Number	Release Date	Remark
V300R009B03D007SP0302	5950-CMW710-R6301P02	5950-CMW710-F6301P01	2023-04-28	MIB updates.
V300R009B03D007SP0301	5950-CMW710-R6301P01	5950-CMW710-F6301	2022-12-31	Fixed bugs.
V300R009B03D007SP03	5950-CMW710-R6301	5950-CMW710-F6207	2019-06-12	This version fixed bugs and introduced feature changes. New features include. There are also modified features.
V600R001B02D123	5950-CMW710-F6207	5950-CMW710-F6206	2019-01-28	This version fixed bugs and introduced feature changes. New features include: <ul style="list-style-type: none">Changing the next hop address of VPNv4 routes to a VPN address There are also modified features.

Version number(inner)	Version Number(outer)	Based Version Number	Release Date	Remark
V600R001B02D121	5950-CMW710-F6206	5950-CMW710-R6205P03	2018-08-15	<p>This version fixed bugs and introduced feature changes.</p> <p>New features include:</p> <ul style="list-style-type: none"> • Setting fan tray serial numbers • Simple multichassis link aggregation (S-MLAG) • Configuring PFC deadlock detection <p>There are also modified features.</p>
V600R001B02D115	5950-CMW710-R6205P03	5950-CMW710-F6205P02	2017-11-13	<p>This version fixed bugs and introduced feature changes.</p> <p>New features include:</p> <ul style="list-style-type: none"> • Enabling STP dispute guard • Enabling DNS spoofing • Enabling symmetric load sharing <p>There are also modified features.</p>

Version number(inner)	Version Number(outer)	Based Version Number	Release Date	Remark
V600R001B02D114	5950-CMW710-F6205P02	5950-CMW710-F6205	2017-10-30	<p>This version fixed bugs and introduced feature changes.</p> <p>New features include:</p> <ul style="list-style-type: none"> Setting PFC thresholds Local-MAC address learning Conversational learning for remote MAC address entries <p>Removed features include:</p> <ul style="list-style-type: none"> Ignoring port speed in setting the aggregation states of member ports PBB SPBM <p>There are also modified features.</p>
V600R001B02D108	5950-CMW710-F6205	5950-CMW710-F6203	2017-6-30	<p>Added features:</p> <ul style="list-style-type: none"> One-step ISSU Specifying ignored packet fields for the default link-aggregation load sharing Static SR over MPLS <p>Fixed bugs.</p> <p>Modified features.</p>
V600R001B02D106	5950-CMW710-F6203	5950-CMW710-F6202	2017-4-27	<p>Added features:</p> <ul style="list-style-type: none"> DRNI <p>Fixed bugs.</p>

Version number(inner)	Version Number(outer)	Based Version Number	Release Date	Remark
V600R001B02D104	5950-CMW710-F6202	5950-CMW710-R6125	2017-3-28	Added features: <ul style="list-style-type: none"> • FC and FCoE • MACsec • EEE • PBB • MPLS L2VPN • VPLS • SPBM • ERPS • FNA(HPE FlexFabric Network Analytics) • DCBX Modified features. Fixed bugs.
V600R001B02D019	5950-CMW710-R6125	5950-CMW710-R6123	2017-1-13	<ul style="list-style-type: none"> • Fixed bugs • Modified features
V600R001B02D011	5950-CMW710-R6123	5950-CMW710-R6106P01	2016-9-30	New feature and new devices.
V600R001B01D017SP01	5950-CMW710-R6106P01	5950-CMW710-R6106	2016-9-11	New feature: Load balancing among BGP routes with different AS_PATH attributes of the same length
V600R001B01D017	5950-CMW710-R6106	5950-CMW710-R6105	2016-5-31	Fixed bugs
V600R001B01D016	5950-CMW710-R6105	First release	2016-4-11	None

Release reason

Added features.

Restrictions and cautions

To connect an interface on the LSWM124XG2QL(JH180A) interface module or a 25-GE interface with a GE transceiver module to another device, you must perform the following tasks on the interface:

- Set the interface speed to 1000 Mbps by using the **speed 1000** command.
- Configure the interface to operate in full duplex mode by using the **duplex full** command.

When multiple queues on one interface or multiple interfaces exceed the buffer usage threshold in FNA at the same time, alarms are not reported for some queues, and the corresponding queue monitor graphs are incorrect.

Multicast packets cannot trigger FNA alarms on the following interfaces:

- 10-GE interfaces on the HPE FlexFabric 5950 32QSFP28 Switch (JH321A) and HPE FlexFabric 5950 32QSFP28 TAA-compliant Switch (JH322A).
- GE interfaces on the HPE FlexFabric 5950 48SFP28 8QSFP28 Switch (JH402A) and HPE FlexFabric 5950 4-slot Switch (JH404A).

Open problems and workarounds

201612230336

- Symptom: After a tunnel interface comes up, the interface cannot decapsulate and forward packets received from VTEPs.
- Condition: This symptom occurs if multiple tunnels exist and the source IP address of one tunnel is the global source IP address. Then, the tunnel that is not configured with a source IP address can come up, but the tunnel interface cannot decapsulate and forward packets received from VTEPs.
- Workaround: Make sure the source IP address configured for a tunnel is different from the global source IP address.

201808170465

- Symptom: NetStream is unavailable on a shutdown GigabitEthernet interface on the rear panel.
- Condition: This symptom might occur if NetStream is enabled on a shutdown GigabitEthernet interface on the rear panel.
- Workaround: Bring up the GigabitEthernet interface.

201901150116

- Symptom: In a VPLS network, if RSVP is used to distribute labels for MPLS TE tunnels, an MPLS TE tunnel cannot switch traffic from the failed primary path to the backup path.
- Condition: This symptom might occur if RSVP is used to distribute labels for MPLS TE tunnels in a VPLS network.
- Workaround: None.

List of solved problems

Resolved problems in R6301P02

None.

Resolved problems in R6301P01

202212280349/202212021236

- Symptom: A VLAN interface fails to forward traffic at Layer 3 during an ISSU.
- Condition: This symptom occurs when an ISSU is performed.

Resolved problems in R6301

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.

201904020262

- Symptom: In an EVPN distributed relay environment, the interface where a single-armed AC is configured cannot forward packets.
- Condition: This symptom occurs if the IPP interface setting is cancelled and then restored for a tunnel interface .

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.

201903210720

- Symptom: In an EVPN distributed relay environment, the DR system sends out multiple copies of unknown unicast packets.
- Condition: This symptom might occur if the following operations have been performed:
 - a. Use a VXLAN tunnel as the IPL and reboot the DR system.
 - b. Receive unknown unicast packets from the remote AC.

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.

201903080004/201903070270

- Symptom: In an MPLS network, a P device drops packets continuously.
- Condition: This symptom might occur if the link between the P device and another P device or a PE device flaps for a long time more than once.

201805040745

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

201902140542

- Symptom: In an EVPN distributed relay environment, the IPL cannot work correctly.
- Condition: This symptom might occur if you configure VLAN-based VXLAN assignment and then configure EVPN distributed relay.

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.

201812110026

- Symptom: In an EVPN network, an access port sends packets with VLAN tags.
- Condition: This symptom might occur if two route reflectors are used and link switchover between them has occurred.

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.

201903280399

- Symptom: When EVPN and DRNI are used together on the switch, frequent tunnel interface flapping might cause traffic interruption.
- Condition: This symptom might occur if frequent tunnel interface flapping occurs.

Resolved problems in F6207

201808290235

- Symptom: Symmetric load sharing might not take effect.
- Condition: This symptom occurs if symmetric load sharing is configured on the device.

201811010044

- Symptom: The panel of the LSWM116Q interface module is displayed incorrectly on IMC.
- Condition: This symptom occurs if the LSWM116Q interface module is installed in subslot 4 of the device and managed by IMC.

201811090022

- Symptom: When an aggregation group has more than eight member ports, the excessive member ports do not have traffic.
- Condition: This symptom occurs if more than eight ports on a single device are added to an aggregation group and the corresponding aggregate interface receives unknown unicast traffic.

201811130637

- Symptom: When a specific port acts as the monitor port of Layer 2 remote port mirroring, no traffic is mirrored to the monitor port.
- Condition: This symptom occurs if the following conditions exist:
 - a. On an IRF fabric, Layer 2 remote port mirroring is configured.
 - b. In the remote probe VLAN, the monitor port and the reflector port reside on different IRF member devices and have the same port number.

201812050136

- 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.

201812190652

- Symptom: A PBR policy fails to be applied because the ACL resources are insufficient.
- Condition: This symptom occurs if the following conditions exist:

- a. The PBR policy is applied to interfaces belonging to different interface groups.
- b. When you apply the PBR policy, the next hop of the PBR policy does not exist in the routing table.
- c. The next hop of the PBR policy becomes reachable in the routing table.

201812270200

- Symptom: A 40-GE interface is split into 10-GE breakout interfaces, and these 10-GE interfaces are configured as Layer 3 interfaces. Some breakout interfaces might be in an incorrect STP state and fail to learn ARP entries.
- Condition: This symptom occurs if the following operations are performed:
 - a. Split a 40-GE interface into 10-GE breakout interfaces.
 - b. Configure these 10-GE breakout interfaces as Layer 3 interfaces.

201812290518

- Symptom: Layer 3 packets sent out of a specific interface are dropped.
- Condition: This symptom occurs if a specific interface forwards Layer 3 packets.

201901110111

- Symptom: The CPU usage of the COPPD process becomes high.
- Condition: This symptom occurs if the following conditions exist:
 - a. Configure the RSVP protocol, and enable BFD for RSVP.
 - b. The device resides in the middle of the tunnel, and the downstream device is unreachable.

201901110113

- Symptom: The Comsh task remains, and the CPU usage becomes high.
- Condition: This symptom occurs if the following operations are performed:
 - a. Log in to the device through Telnet.
 - b. Use the **lock-key** command to set the user line locking key.
 - c. Press this shortcut key to lock the remote connection.
 - d. Disconnect the remote connection when the remote connection is still locked.

201901170294

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

Resolved problems in F6206

201708310741

- Symptom: In a DRNI network, the keepalive link goes down.

- Condition: This symptom occurs if the device is configured with both DRNI and OpenFlow.

201712180820

- Symptom: In an EVPN DRNI network, the downlink interface receives redundant traffic.
- Condition: This symptom occurs if a DR interface on a DR device is shut down when the downlink host is silent.

201807120129

- Symptom: MPLS traffic cannot be forwarded.
- Condition: This symptom occurs if the following conditions exist in a CTOC network:
 - a. Primary and backup tunnels are configured.
 - b. The traffic is switched to the backup tunnel when a node fails.
 - c. The traffic is switched back to the primary tunnel when the link restores.

201807190749

- Symptom: CRC error packets appear when FC traffic is being forwarded.
- Condition: This symptom occurs if a 16G FC module is used to transmit the FC traffic.

201801190600

- Symptom: 10-GE interfaces on the LSWM124XG2Q and LSWM124XG2QFC interface modules do not come up.
- Condition: This symptom occurs if the HPE FlexFabric 5950 4-slot Switch has LSWM124XG2Q and LSWM124XG2QFC interface modules installed.

201806120020

- Symptom: The RSVP process exits exceptionally after certain operations.
- Condition: This symptom occurs if the public network tunnels are configured with TE FRR and IP address conflicts exist in a CTOC network.

201806120097

- Symptom: The device might reboot unexpectedly at a low probability.
- Condition: This symptom occurs if the HPE FlexFabric 5950 4-slot Switch uses an LSWM116Q interface module.

201805220109

- Symptom: When an IRF physical interface goes down, the other interfaces in the same group as the IRF physical interface flap.
- Condition: This symptom occurs if a 40-GE interface on an LSWM116Q interface module of the HPE FlexFabric 5950 4-slot Switch is used as an IRF physical interface.

201803190071

- Symptom: When ACLs are issued to multiple Layer 3 aggregate interfaces, the ACLs take effect on only one Layer 3 aggregate interface.

- Condition: This symptom occurs if ACLs are issued to multiple Layer 3 aggregate interfaces and rules are added to or deleted from these ACLs.

201803170047

- Symptom: Issued ACLs might not take effect.
- Condition: This symptom occurs if ACLs are repeatedly issued or repeatedly dynamically modified.

201802050250

- Symptom: The device reboots unexpectedly.
- Condition: This symptom occurs if the **shutdown** and **undo shutdown** commands are executed on the FC interface connecting to a server or storage device.

201711290143

- Symptom: A user cannot come online.
- Condition: This symptom occurs if the switch is configured to operate in FCF mode.

201803290351

- Symptom: PFC deadlock detection takes effect only on the first interface where it is configured, and does not take effect on the subsequent interfaces where it is configured.
- Condition: This symptom occurs if PFC deadlock detection is configured on two or more interfaces of the device.

201711030407

- Symptom: CVE-2017-1000253
- Condition: Local attackers may exploit this issue to gain root privileges.

201712220137

- Symptom: CVE-2017-3736
- Condition: An attacker can exploit this issue to gain access to sensitive information that may aid in further attacks.

201712190381

- 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.

201802060169

- Symptom: CVE-2017-15896
- Condition: An attacker can exploit this issue to bypass TLS validate and encrypt, send application data to Node.js.
- Symptom: CVE-2017-3737
- Condition: Successfully exploiting this issue will allow attackers to bypass security restrictions and perform unauthorized actions; this may aid in launching further attacks.
- Symptom: CVE-2017-3738
- Condition: An attacker can exploit this issue to gain access to sensitive information that may aid in further attacks.

201805250759

- Symptom: CVE-2016-9586
- Condition: Attackers can exploit this issue to execute arbitrary code in the context of the affected application. Failed exploit attempts will result in denial-of-service conditions.

201710180649

- Symptom: MACsec connections cannot be set up if a transceiver module or subcard is removed and re-installed when MACsec traffic exists.
- Condition: This symptom might occur if a transceiver module or subcard is removed and re-installed when MACsec traffic exists.

201710240487

- Symptom: EVPN traffic forwarding fails if the remote VTEP switches between tunnels.
- Condition: This symptom might occur if the remote VTEP switches between tunnels.

201710270200

- Symptom: An interface cannot forward traffic after its MACsec configuration is removed.
- Condition: This symptom might occur if MACsec configuration is removed from an interface.

201706270683

- Symptom: NetStream fails to collect traffic statistics on an interface when NetStream is disabled on other interfaces.
- Condition: This symptom occurs if NetStream is configured on multiple interfaces and then NetStream is disabled on one of these interfaces.

201609230034

- Symptom: BFD session flapping occurs when SSL VPN AC interfaces are shut down.
- Condition: This symptom might occur if SSL VPN AC interfaces are shut down.

201708310704

- Symptom: A 10-GE copper interface cannot come up.
- Condition: This symptom occurs if an external loopback test is performed on the 10-GE copper interface.

201709260138

- Symptom: CVE-2017-3735
- Condition: Successfully exploiting this issue will allow attackers to bypass security restrictions and perform unauthorized actions; this may aid in launching further attacks.

201711270371

- Symptom: The management Ethernet interface might fail to be pinged.
- Condition: This symptom occurs if a master/subordinate switchover occurs to an IRF fabric.

Resolved problems in R6205P03

201709260138

- Symptom: CVE-2017-3735
- Condition: Successfully exploiting this issue will allow attackers to bypass security restrictions and perform unauthorized actions; this may aid in launching further attacks.

201710180649

- Symptom: MACsec connections cannot be set up if a transceiver module or subcard is removed and re-installed when MACsec traffic exists.
- Condition: This symptom might occur if a transceiver module or subcard is removed and re-installed when MACsec traffic exists.

201710240487

- Symptom: EVPN traffic forwarding fails if the remote VTEP switches between tunnels.
- Condition: This symptom might occur if the remote VTEP switches between tunnels.

201710270200

- Symptom: An interface cannot forward traffic after its MACsec configuration is removed.
- Condition: This symptom might occur if MACsec configuration is removed from an interface.

201706270683

- Symptom: NetStream fails to collect traffic statistics on an interface when NetStream is disabled on other interfaces.
- Condition: This symptom occurs if NetStream is configured on multiple interfaces and then NetStream is disabled on one of these interfaces.

201609230034

- Symptom: BFD session flapping occurs when SSL VPN AC interfaces are shut down.
- Condition: This symptom might occur if SSL VPN AC interfaces are shut down.

201708310704

- Symptom: A 10-GE copper interface cannot come up.
- Condition: This symptom occurs if an external loopback test is performed on the 10-GE copper interface.

Resolved problems in F6205P02

201706050458

- Symptom: In an EVPN network, traffic is duplicated.
- Condition: This symptom occurs if the following conditions exist:
 - In an EVPN network, the outgoing interface of a VXLAN tunnel is a Layer 3 aggregate interface.
 - The **shutdown** or **undo shutdown** command is executed on an interface transmitting traffic.

201706090010

- Symptom: Residual rawip sockets exist and occupy the memory.
- Condition: This symptom occurs if the switch performs NQA operations for a long time.

201705250358

- Symptom: An FC aggregate interface cannot come up.
- Condition: This symptom occurs if the member ports of the FC aggregate interface are all on subordinate IRF member devices.

201705060255

- Symptom: NetStream fails to collect traffic statistics on an interface.
- Condition: This symptom occurs if IPv6 NetStream filtering is enabled on the interface.

201609060180

- Symptom: The following symptoms occur on an interface that hosts an AC:
 - If the priority trust mode is not set, the interface cannot perform EXP value mapping correctly for MPLS packets with an EXP value of 0, and the 802.1p priority of the packets is set to 0 after priority mapping.
 - If the priority trust mode is set to 802.1p or DSCP, the 802.1p priority of packets is set to 0 after priority mapping.

- Condition: This symptom might occur if the priority trust mode is not set or the **qos trust dot1p** or **qos trust dscp** command is executed on an interface that hosts an AC.

201708250543

- Symptom: On a DR interface, traffic among different service instances associated with the same VSI cannot be forwarded.
- Condition: This symptom occurs if the DR interface is configured with ACs and the **shutdown** and **undo shutdown** commands are executed on the member ports of the DR interface.

201708310748

- Symptom: NetStream fails to collect traffic statistics on an interface.
- Condition: This symptom occurs if IPv6 NetStream filtering is enabled on the interface.

201709080177

- Symptom: A fiber management interface cannot come up.
- Condition: This symptom occurs if the transceiver module is removed from and then installed into a fiber management interface on a subordinate IRF member device.

201708310760

- Symptom: MACsec cannot operate correctly on an MKA-enabled interface.
- Condition: This symptom occurs if the **speed** command is used to set the speed for an interface supporting MACsec.

Resolved problems in F6205

201705230173

- Symptom: On an EVPN network with distributed EVPN gateways, outgoing packets on an Ethernet service instance carry an 802.1Q VLAN tag unexpectedly.
- Condition: This symptom might occur if the device acts as an EVPN gateway to perform Layer 3 forwarding and the Ethernet service instance is configured to match frames that do not have an 802.1Q VLAN tag.

201612050269

- Symptom: CVE-2016-7427
- Condition: An attacker with access to the NTP broadcast domain can periodically inject specially crafted broadcast mode NTP packets into the broadcast domain which, while being logged by ntpd, can cause ntpd to reject broadcast mode packets from legitimate NTP broadcast servers
- Symptom: CVE-2016-7428

- Condition: An attacker with access to the NTP broadcast domain can send specially crafted broadcast mode NTP packets to the broadcast domain which, while being logged by ntpd, will cause ntpd to reject broadcast mode packets from legitimate NTP broadcast servers
- Symptom: CVE-2016-7431
- Condition: Zero Origin timestamp problems were fixed by Bug 2945 in ntp-4.2.8p6. However, subsequent timestamp validation checks introduced a regression in the handling of some Zero origin timestamp checks.

201702220570

- Symptom: CVE-2017-3730
- Condition: OpenSSL is prone to denial-of-service vulnerability. Attackers can exploit this issue to cause a denial-of-service condition.
- Symptom: CVE-2017-3731
- Condition: OpenSSL is prone to denial-of-service vulnerability. An attacker may exploit this issue to crash the application, resulting in denial-of-service condition.
- Symptom: CVE-2017-3732
- Condition: OpenSSL is prone to an information-disclosure vulnerability. An attacker can exploit this issue to gain access to sensitive information that may aid in further attacks.

201704280171

- Symptom: CVE-2015-3405
- Condition: An attacker can exploit the ntp-keygen utility to spoof an NTP client or server.
- Symptom: CVE-2014-9297
- Condition: An attacker can exploit this issue. When an NTP client decrypted a secret received from an NTP server.
- Symptom: CVE-2015-9298
- Condition: An attacker could bypass source IP restrictions and send malicious control and configuration packets.

201704280531

- Syptom: CVE-2017-64558
- Condition: NTP are prone to a buffer-overflow vulnerability because it fails to properly bounds-check user-supplied data before copying it into an insufficiently sized buffer.

- Symptom: CVE-2016-9042

Condition: NTP is prone to a denial-of-service vulnerability. An attacker can exploit this issue to cause a denial-of-service condition, denying service to legitimate users.

Resolved problems in F6203

201704010616

- Symptom: An IRF fabric splits when the IRF fabric has 8K VPLS PWs and the public network interface on the IRF fabric flaps.
- Condition: This symptom might occur if the IRF fabric has 8K VPLS PWs and the public network interface on the IRF fabric flaps.

201703310499

- Symptom: FNA is not available for GE interfaces on the FlexFabric 5950 48SFP28 8QSFP28 or FlexFabric 5950 4-slot switch.
- Condition: This symptom might occur if FNA is configured on GE interfaces of the FlexFabric 5950 48SFP28 8QSFP28 or FlexFabric 5950 4-slot switch.

201704240426

- Symptom: A memory exhaustion occurs on the switch when the switch is enabled with FNA and keeps generating notification messages for a long time.
- Condition: This symptom might occur if the switch is enabled with FNA and keeps generating notification messages for a long time.

201703160569

- Symptom: A 10-GE interface that is installed with a GE transceiver module and connected to another device cannot come up if the 10-GE interface is on one of the following hardware:
 - LSWM124XG2QL(JH180A) interface module.
 - FlexFabric 5950 32QSFP28 switch.
 - FlexFabric 5950 32QSFP28 TAA-compliant switch.
- Condition: This symptom might occur if the 10-GE interface is installed with a GE transceiver module and connected to another device and the 10-GE interface is on one of the following hardware:
 - LSWM124XG2QL(JH180A) interface module.
 - FlexFabric 5950 32QSFP28 switch.
 - FlexFabric 5950 32QSFP28 TAA-compliant switch.

201704250571

- Symptom: In an IRF fabric, forwarded Layer 2 packets arrive at the incoming interface of the packets again.
- Condition: This symptom occurs with a low probability if an interface in the IRF fabric is split into breakout interfaces and then the breakout interfaces are combined.

Resolved problems in F6202

201612050269

- Symptom: CVE-2016-7427
- Condition: An attacker with access to the NTP broadcast domain can periodically inject specially crafted broadcast mode NTP packets into the broadcast domain which, while being logged by ntpd, can cause ntpd to reject broadcast mode packets from legitimate NTP broadcast servers
- Symptom: CVE-2016-7428
- Condition: An attacker with access to the NTP broadcast domain can send specially crafted broadcast mode NTP packets to the broadcast domain which, while being logged by ntpd, will cause ntpd to reject broadcast mode packets from legitimate NTP broadcast servers
- Symptom: CVE-2016-7431
- Condition: Zero Origin timestamp problems were fixed by Bug 2945 in ntp-4.2.8p6. However, subsequent timestamp validation checks introduced a regression in the handling of some Zero origin timestamp checks.

201611030036

- Symptom: Flow mirroring does not take effect.
- Condition: This symptom occurs if flow mirroring is configured in the outbound direction of a Layer 3 interface or Layer 3 aggregate interface.

Resolved problems in R6125

201610100291

- Symptom: On a VXLAN or EVPN network, unknown unicast, broadcast, or multicast packets are duplicated or lost after they are forwarded.
- Condition: This symptom occurs if the Ethernet service instance of a VSI is created on a cross-chassis Layer 2 aggregate interface, of which member ports are on different IRF member devices.

201612270330

- Symptom: The system prompts that the memory is insufficient when the BGP neighborhood information is displayed.
- Condition: This symptom occurs if SNMP is used to read BGP information multiple times and causes memory leak.

201610240176

- Symptom: Inter-data center Layer 2 forwarding fails in an EVPN-DCI network.
- Condition: This symptom might occur if Layer 2 traffic is forwarded between two data centers of an EVPN-DCI network.

201609060256

- Symptom: Frequent LDP protocol flapping causes hardware nexthop entry leakage and forwarding failure.
- Condition: This symptom might occur if the LDP protocol flaps frequently.

201610140317

- Symptom: CVE-2016-6304;
- Condition: OpenSSL is prone to denial-of-service vulnerability. An attacker may exploit this issue to cause a denial-of-service condition.
- Symptom: CVE-2016-6306
- Condition: OpenSSL is prone to a local denial-of-service vulnerability. A local attacker can exploit this issue to cause a denial-of-service condition.

201611070341

- Symptom: CVE-2016-8858
- Condition: A remote user can send specially crafted data during the key exchange process to trigger a flaw in `kex_input_kexinit()` and consume excessive memory on the target system. This can be exploited to consume up to 384 MB per connection.

201611080162

- Symptom: CVE-2016-5195
- Condition: An unprivileged local user could use this flaw to gain write access to otherwise read-only memory mappings and thus increase their privileges on the system.

201609140425

- Symptom: After L2VPN is disabled, the EVPN-enabled device cannot forward traffic correctly because some EVPN ARP entries are not deleted .
- Condition: This symptom might occur if L2VPN is disabled on the EVPN-enabled device.

Resolved problems in R6123

201609180002:

- Symptom: CVE-2016-2105
- Condition: Fixed vulnerability in “EVP Encode” in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to cause a denial of service (heap memory corruption) via a large amount of binary data.
- Symptom: CVE-2016-2106
- Condition: Fixed vulnerability in “EVP Encrypt” in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to cause a denial of service (heap memory corruption) via a large amount of binary data.
- Symptom: CVE-2016-2107
- Condition: Fixed vulnerability in OpenSSL before 1.0.1t and 1.0.2h allows remote attackers to obtain sensitive cleartext information via a padding-oracle attack against an AES CBC session.
- Symptom: CVE-2016-2108
- Condition: Fixed vulnerability in OpenSSL before 1.0.1o and 1.0.2 before 1.0.2c allows remote attackers to execute arbitrary code or cause a denial of service (buffer underflow and memory corruption).
- Symptom: CVE-2016-2109
- Condition: Fixed vulnerability in “asn” before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to cause a denial of service (memory consumption) via a short invalid encoding.
- Symptom: CVE-2016-2176
- Condition: Fixed vulnerability in “X509” in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to obtain sensitive information from memory or cause a denial of service.

201607290021 :

- Symptom: CVE-2016-2177
- Condition: Fixed vulnerability in s3_srvr.c, ssl_sess.c, and t1_lib.c functions in OpenSSL through 1.0.2h that allows remote attackers to cause a denial of service (integer overflow and application crash), or possibly have an unspecified other impact by leveraging unexpected malloc behavior.

201606240193:

- Symptom: CVE-2016-4953
- Condition: Fixed vulnerability in NTP 4.x before 4.2.8p8 allows remote attackers to cause a denial of service by sending a spoofed packet with incorrect authentication data at a certain time.
- Symptom: CVE-2016-4954
- Condition: Fixed vulnerability in ntpd in NTP 4.x before 4.2.8p8 allows remote attackers to cause a denial of service by sending spoofed packets from source IP addresses in a certain scenario.
- Symptom: CVE-2016-4956
- Condition: Fixed vulnerability in NTP 4.x before 4.2.8p8 allows remote attackers to cause a denial of service via a spoofed broadcast packet.

201609010406

- Symptom: CVE-2009-3238
- Condition: The get_random_int function in the Linux kernel before 2.6.30 produces insufficiently random numbers, which allows attackers to predict the return value, and possibly defeat protection mechanisms

201603310333

- Symptom: The port mirroring configuration fails to be issued.
- Condition: This symptom occurs if an aggregate interface is configured as the monitor port of a mirroring group.

201604080607

- Symptom: VXLAN traffic cannot be forwarded when the switch acts as a VXLAN IP gateway and has sFlow configured.
- Condition: This symptom occurs if sFlow is enabled on the physical interface corresponding to the VXLAN tunnel.

201604140250

- Symptom: In a VXLAN network, the routing protocols flap.
- Condition: This symptom occurs if the following conditions exist:
 - The switch acts as a VXLAN IP gateway.
 - A large number of VXLAN tunnels are created on the switch.
 - The switch is sending and receiving a large number of ARP packets.

201604200574

- Symptom: OSPF neighborhood flaps.

- Condition: This symptom occurs if an IRF splits.

201512230507

- Symptom: The configuration might fail to be saved.
- Condition: This symptom might occur if you save the configuration.

Resolved problems in R6106P01

None.

Resolved problems in R6106

201604060275

- Symptom: The PBR configuration on a VSI interface does not take effect.
- Condition: This symptom occurs if PBR is configured on a VSI interface of a VXLAN IP gateway.

201604010510

- Symptom: The DHCP snooping entries are not complete.
- Condition: This symptom occurs if both DHCP relay agent and DHCP snooping are configured on the switch in a Layer 3 network.

201604050208

- Symptom: The sub-VLANs of a super VLAN do not send IGMP/MLD queries.
- Condition: This symptom occurs if a super VLAN is configured and IGMP/MLD is configured on the VLAN interface of the super VLAN.

201603310127

- Symptom: Unknown unicast traffic and broadcast traffic are dropped in the outbound direction of an interface.
- Condition: This symptom occurs if the interface is configured as an IRF physical interface and then configured as a common interface.

Resolved problems in R6105

First release.

Software upgrade guidelines

Please refer to HPE 5950-CMW710-R6301P02 release notes.