



Release Notes

VeloCloud SD-WAN

Version 5.2.5



Arista.com

Arista Networks

DOC-2025-06-16

Headquarters	Support	Sales
5453 Great America Parkway Santa Clara, CA 95054 USA +1-408-547-5500 www.arista.com/en/	+1-408-547-5502 +1-866-476-0000 support@arista.com	+1-408-547-5501 +1-866-497-0000 sales@arista.com

© Copyright 2025 Arista Networks, Inc. All rights reserved. The information contained herein is subject to change without notice. The trademarks, logos, and service marks ("Marks") displayed in this documentation are the property of Arista Networks in the United States and other countries. Use of the Marks is subject to the Arista Networks Terms of Use Policy, available at www.arista.com/en/terms-of-use. Use of marks belonging to other parties is for informational purposes only.

Contents

Chapter 1: Arista VeloCloud SD-WAN 5.2.5 Release Notes.....1

Arista VeloCloud SD-WAN 5.2.5 Release Notes

This document contains the following sections

- [Introduction](#)
- [What Is in The Release Notes](#)
- [Edge/Gateway Resolved Issues](#)
- [Known Issues](#)

Introduction

Arista SASE 5.2.5 | 16th June 2025

- Arista SD-WAN™ Gateway Version **R5251-20250410-GA**
- Arista SD-WAN™ Edge Version **R5251-20250603-GA-162396**



Note: Release 5.2.5 is an Edge/Gateway software release only and does not have a SASE Orchestrator component.

The SASE Orchestrator remains on 5.2.3+ LTS and additional fixes for Orchestrator issues will continue to be added through rollup builds in accordance with LTS policy.

Check for additions and updates to these release notes.

What Is in The Release Notes

The release notes cover the following topics:

Recommended Use

This release is recommended only for customers who require the **Symantec Web Security Service (WSS) Integration (PoP-to-PoP)** feature and other functionality first made available in Release 5.2.0. If the Symantec Web Security Service (WSS) Integration (Pop-to-Pop) functionality is not required by customers, it is recommended to stay on the 5.2.4 release.



Important: Release 5.2.5 contains all Edge and Gateway fixes that are listed in the 5.2.4 Release Notes up to Edge/Gateway version **R5250-20241126-GA**.

5.2.5 is a Long-Term Support (LTS) Release

Arista VeloCloud SD-WAN/SASE introduced a Long-Term Support (LTS) policy to enhance the operational efficiency of our partners and customers during the implementation of new software. Release 5.2.3+ is the first LTS release, and SD-WAN Release 5.2.5 for the Edge/Gateway continues off of 5.2.3+ as an LTS Release.

For additional information about our Long-Term Support program see: *Arista SD-WAN/SASE Long-Term Support Release (96246)*.

Compatibility

Release 5.2.5 Gateways and Hub Edges support all previous Arista SD-WAN Edge versions greater than or equal to Release 4.2.0.

The following SD-WAN interoperability combinations were explicitly tested:

Orchestrator	Gateway	Edge	
		Hub	Branch/Spoke
5.2.3	4.5.2	4.5.2	4.5.2
5.2.3	5.2.5	4.5.2	4.5.2
5.2.3	5.2.5	5.2.5	4.5.2
5.2.3	5.2.5	4.5.2	5.2.5
5.2.3	5.2.5	5.2.3	5.2.3
5.2.3	5.2.5	5.2.5	5.2.0
5.2.3	5.2.3	5.2.3	5.2.5
6.0.0	5.2.4	5.2.4	5.2.4
6.0.0	5.2.5	5.2.4	5.2.4
6.0.0	5.2.5	5.2.5	5.2.4
6.0.0	5.2.5	5.2.4	5.2.5

Important: Arista SD-WAN Release 4.0.x has reached End of Support; Releases 4.2.x, 4.3.x, and 4.5.x have reached End of Support for Gateways and Orchestrators.

- Release 4.0.x reached End of General Support (EOGS) on September 30, 2022, and End of Technical Guidance (EOTG) December 31, 2022.
- Release 4.2.x Orchestrators and Gateways reached End of General Support (EOGS) on December 30, 2022, and End of Technical Guidance on (EOTG) March 30, 2023.
- Release 4.2.x Edges reached End of General Support (EOGS) on June 30, 2023, and will reach End of Technical Guidance (EOTG) September 30, 2025.
- Release 4.3.x Orchestrators and Gateways reached End of General Support (EOGS) on June 30, 2023, and End of Technical Guidance (EOTG) September 30, 2023.
- Release 4.3.x Edges reached End of General Support (EOGS) on June 30, 2023, and will reach End of Technical Guidance (EOTG) September 30, 2025.
- Release 4.5.x Orchestrators and Gateways reached End of General Support (EOGS) on September 30, 2023, and End of Technical Guidance on (EOTG) December 31, 2023.
- For more information please consult the Knowledge Base article: *Announcement: End of Support Life for Arista SD-WAN Release 4.x (88319)*.



Note: Arista VeloCloud SD-WAN Release 5.x is approaching the of End of Support for 5.0.x, 5.1.x, 5.2.0, 5.2.2, and 5.4.x Orchestrator and Gateway versions.

- Release 5.0.x Orchestrator, Controller, and Gateway will reach End of General Support (EOGS) on February 28, 2025, and End of Technical Guidance (EOTG) February 28, 2026.
- Release 5.0.x Edges will reach End of General Support (EOGS) on February 28, 2026, and End of Technical Guidance (EOTG) February 28, 2027.
- Release 5.1.x Orchestrator, Controller, and Gateway will reach End of General Support (EOGS) on February 28, 2025, and End of Technical Guidance (EOTG) February 28, 2026.
- Release 5.1.x Edges will reach End of General Support (EOGS) on February 28, 2026, and End of Technical Guidance (EOTG) February 28, 2027.
- Release 5.2.0 and 5.2.2 Orchestrator, Controller, and Gateway will reach End of General Support (EOGS) on February 28, 2025, and End of Technical Guidance (EOTG) February 28, 2026.
- Release 5.2.0 and 5.2.2 Edges will reach End of General Support (EOGS) on February 28, 2026, and End of Technical Guidance (EOTG) February 28, 2027.
- Release 5.4.x Orchestrator, Controller, and Gateway will reach End of General Support (EOGS) on February 28, 2025, and End of Technical Guidance (EOTG) February 28, 2026.
- Release 5.4.x Edges will reach End of General Support (EOGS) on February 28, 2026, and End of Technical Guidance (EOTG) February 28, 2027.
- For more information please consult the Knowledge Base article: *Announcement: End of Support Life for Arista VeloCloud SD-WAN Release 5.x* (381499).

Release 5.2.3 and 5.2.4 are Long Term-Support Releases and are not included in this notice as the Orchestrator, Gateway, and Edge for these versions do not reach EOGS until March, 2027.

Upgrade Paths Gateway and Edge

The following lists the paths for customers wishing to upgrade their Gateway or Edge from an older release to Release 5.2.5.

Gateway

Upgrading a Gateway using Release 4.5.0 or later to Release 5.2.5 is fully supported for all Gateway types.



Important: When deploying a new Gateway using 5.2.4 the VMware ESXi instance must be **at least version 6.7, Update 3 up to version 7.0**. Using an earlier ESXi instance will result in the Gateway's Dataplane Service failing when trying to run Release 5.2.3 or later.



Important: Prior to upgrading a Gateway to 5.2.4, the ESXi instance must be upgraded to **at least version 6.7, Update 3 up to version 7.0**. Using an earlier ESXi instance will result in the Gateway's Dataplane Service failing when trying to run Release 5.2.3 or later.

Edge

An Edge can be upgraded directly to Release 5.2.4 from any Release 4.x or later.

New Hardware Platforms

Release 5.2.5 includes support for VeloCloud Edge models 710-5G, 720, and 740.

For more information, please consult the *announcement for these new Edge models*.

New Features and Enhancements

Symantec Web Security Service (WSS) Integration (PoP-to-PoP)

This feature brings low latency, high throughput, and high availability connectivity to Symantec WSS via a multi-tenant Geneve tunnel established between the VeloCloud Gateway and Symantec WSS in GCP PoPs. Customers can configure a Business Policy to send traffic to Symantec WSS for inspection using this new feature as an alternative to the Non SD-WAN Destination via Edge capability.



Note: This feature was released in 6.1 and has now been made available on the Edge for 5.2.5.

Important Notes

Limitation with BGP over IPsec on Edge and Gateway, and Azure Virtual WAN Automation

The BGP over IPsec on Edge and Gateway feature is not compatible with Azure Virtual WAN Automation from Edge or Gateway. Only static routes are supported when automating connectivity from an Edge or Gateway to an Azure vWAN.

Limitation When Deactivating Autonegotiation on an Arista SD-WAN Edge Models 520, 540, 620, 640, 680, 3400, 3800, and 3810

When a user deactivates autonegotiation to hardcode speed and duplex on ports GE1 - GE4 on an Arista SD-WAN Edge model 620, 640 or 680; on ports GE3 or GE4 on an Edge 3400, 3800, or 3810; or on an Edge

520/540 when an SFP with a copper interface is used on ports SFP1 or SFP2, the user may find that even after a reboot the link does not come up.

This is caused by each of the listed Edge models using the Intel Ethernet Controller i350, which has a limitation that when autonegotiation is not used on both sides of the link, it is not able to dynamically detect the appropriate wires to transmit and receive on (auto-MDIX). If both sides of the connection are transmitting and receiving on the same wires, the link will not be detected. If the peer side also does not support auto-MDIX without autonegotiation, and the link does not come up with a straight cable, then a crossover Ethernet cable will be needed to bring the link up.

For more information please see the KB article *Limitation When Deactivating Autonegotiation on Arista SD-WAN Edge Models 520, 540, 620, 640, 680, 3400, 3800, and 3810* (87208).

Document Revision History

June 16th, 2025. Third Edition.

- Added Fixed Issue #162396 in the **R5251-20250603-GA-162396** Resolved Issues section.

April 20th, 2025. Second Edition.

- Added a new Edge/Gateway rollup build **R5251-20250410-GA** to the **Edge/Gateway Resolved** section. This is the third Edge/Gateway rollup build and is the new default Edge GA build for Release 5.2.5.
- Edge/Gateway build **R5251-20250410-GA** includes the fixes for issues #92235, #131462, #141113, #142997, #147825, #148063, #148852, #148985, #149307, #150646, #150755, #151654, #151764, #151806, #151812, #151891, #151892, #152094, #152144, #152258, #152283, #152429, #152463, #152775, #153444, #153640, #153924, #155311, #155461, #155517, #155822, #155881, #155974, #156458, #156473, #157187, #157665, #157667, #157837, #157898, #157962, #158032, #158144, #158195, #158456, #158500, ##158568, # 159329, #159092, #159337, #159532, #159733, #159845 and #160080 each of which is documented in this section.

December 4th, 2024. First Edition.

- Added a new feature to the build **R5250-20241126-GA** to the **New Features and Enhancements** section.

Edge/Gateway Resolved Issues

Resolved in Edge Version R5251-20250603-GA-162396

Edge version R5251-20250603-GA-162396 was released on 06-16-2025 and is the updated GA build for Release 5.2.5. This build replaces the previous GA build R5251-20250410-GA. This Edge build addresses the below critical issue since R5251-20250410-GA.



Important: Customers must only use the R5251-20250603-GA-162396 build and not use R5251-20250410-GA.

Fixed Issue 162396: This security issue was identified as part of our internal Secure Software Development Life Cycle activities.

Our recommendation is to consume the latest version at the earliest.

Resolved in Edge/Gateway Version R5251-20250410-GA

Edge/Gateway version R5251-20250410-GA was released on 04-24-2025 and resolves issues in Edge and Gateway since Edge/Gateway version R5250-20241126-GA.

Fixed Issue 92235: A customer deploying an Edge LTE model (510-LTE, 610-LTE, 710-5G) may observe that the LTE link goes down and does not recover or has LTE link connectivity issues that the LTE Edge does not mitigate.

A customer can encounter this condition in one of two scenarios. Where a SIM is experiencing a persistent error condition, or where it is experiencing a temporary error condition.

A persistent error condition is considered one that requires external intervention to recover the device, and includes for example: A SIM-PIN or SIM-PUK is locked; a SIM error; or a modem firmware failure that is not automatically recovered by a device self-reset (in other words, the modem is stuck). Some of these conditions cannot be recovered without external user intervention (for example, a missing SIM).

A temporary error condition is detected by the modem management as a failure to complete a full connection attempt, including IP addressing setup in the associated data interface.

Temporary error conditions may be for example: Failure to register in the operator network (for example, illegal UE, IMSI unknown in HSS, and so forth); Registered in the network for limited services (for example, PS services not allowed, emergency services only, and so forth); Network errors preventing registration (for example, failure during attach, congestion, insufficient resources, and so forth); Rejected APN configuration (for example, missing or unknown APN, failed user authentication, service option not supported, activation rejected by PDN GW, and so forth); and Network errors preventing data connectivity (for example, service temporarily unavailable, congestion, operator determined barring, severe network failure, restricted service area, and so forth).

For either condition, the LTE Edge takes no actions. An LTE Edge with a fix for this issue will automatically attempt to recover the LTE link from either condition with no additional configuration required.

For the persistent error condition the LTE Edge software will assess the cause of the condition and will then decide whether or not to recover the modem by power cycling it (only the LTE modem, not the Edge itself). For the temporary error condition where the network is experiencing temporary issues that cause the connection attempts to fail, the LTE Edge would stop its LTE modem from attempting to connect for a period of time to avoid making the situation even worse.



Note: This issue and the fix for it apply only to LTE Edges and is not applicable to Edges using USB modems.

Fixed Issue 131462: MAC table is not updated after HA/VRRP failovers.

Whenever a state transition occurs in VRRP or HA, we may end up with an incorrect MAC table that can break traffic flow.

Fixed Issue 138303: SD-WAN Edge may experience data plane service failure and restart due to race condition accessing DNS cache entry.

Dataplane Service failure and restart issue is the result of a race condition in the DNS cache where an entry is being accessed and its reference stored by a thread and then due to context switch another thread deletes

the entry .When the former thread is scheduled and it tries to access the entry , it results in memory violation leading to crash since its reference to the DNS cache entry is no longer valid .

Fixed Issue 141113: An SNMP walk may get timed out and fail to complete when the Edge has an interface configured for a PPPoE link which is stuck in a down state.

This issue only occurs if the PPPoE link on the interface is never up. If the interface is up and goes down for some reason the SNMP walk will successfully complete.

On an Edge without a fix for this issue, ensure that any configured PPPoE link is capable of coming up, in other words ensure the peer PPPoE server is enabled.

Fixed Issue 142997: After approximately 4,000 connections have been made to the same destination (i.e. destination IP address, protocol and port), users may experience degraded performance when accessing that destination via direct internet breakout with NAT from an Edge.

Due to an issue with how in-use and available network ports are tracked for the Edge WAN IP address(es) when used for NAT, the Edge may fail to allocate an available port when applying source NAT for new connections. Performance degradation will increase with increasing traffic to the affected destination(s) and time since the Edge was last rebooted.

Fixed Issue 147825: Stale entries may be present in the DNS cache.

While sending DNS traffic to populate the DNS cache, entries are created with a TTL of 5 minutes. When the TTL expires, the entries remain in the cache.

Fixed Issue 148063: Tunnels are not forming on the eHA link while it is in standby mode.

When both CELL and GE eHA links are present in standby mode, they may be assigned the same link identifier. This can cause eHA link packets to be sent to the wrong link, leading to potential communication issues.

Fixed Issue 148852: For a High Availability Edge pair, a network configuration may not be applied to the HA Edge.

In instances where the Orchestrator check fails and a NULL netmask is sent to the Edge, the Edge does not gracefully handle the NULL netmask. As a result it does not update the configuration for any interface. For an HA Edge without a fix for this issue, the workaround is to add an IP address to the interface for which the netmask is NULL. Or you can set the interface to DHCP.

Fixed Issue 148985: The default route in the kernel occasionally disappears after system upgrades, DHCP lease renewals, interface changes (up/down), or static configuration updates.

The kernel's default route sometimes disappears for routed interfaces. This issue has been observed following release upgrades, DHCP lease renewals, interface changes (up/down), and other events. While the exact root cause remains elusive, in one instance, an incorrect default gateway configuration in a static setup was identified as the culprit. A workaround has been implemented to check interface information in ubus and compare it to the kernel's default route. Missing routes, if any, are then added.

Fixed Issue 149307: Setting interface Autoneg to off does not get applied after changing the L2 parameter of Autoneg from on to off.

When L2 setting of a DPDK PMD-bound interface is set to Autoneg off with a specific speed and duplex mode, the network settings get pushed and the edge process gets restarted but the L2 settings on the interface still shows autoneg On and advertising all available link modes.

Fixed Issue 150646: A customer deploying a Virtual Edge with an AWS type may observe that they cannot find the latest 5.2.x image on the AWS Marketplace to download.

This defect is to address the 5.2.x AWS Edge AMI to be uploaded to the AWS marketplace from allowing the upload.

Fixed Issue 150755: For a customer who has configured Network & Flood protection for a Non-Wi-Fi or LTE Edge model, client users may observe that their traffic is throttled by the Edge Firewall even though the configured thresholds have not been met.

The Network & Flood protection CPS (Connections per Second) thresholds are not set for Non-Wi-Fi and also LTE Edge variants, and as a result the feature does not work as expected.

Fixed Issue 151654: A link may not come up on a VeloCloud Edge where both the Edge's Ethernet port and the peer port have auto-negotiation set to off.

For the Edge port, auto-negotiation is set to off and the user has manually configured the speed and duplex of the port through the UI. The issue is the result of differing implementations of auto-negotiation between the Edge and the peer device.



Note: On an Edge without a fix for this issue, the user should turn on autonegotiation on the Edge's Ethernet port.

Fixed Issue 151764: Route auto-correction may not occur for Dynamic Edge-to-Edge via Gateway routes after a route flap.

In the case of Edge-to-Edge (Branch-to-Branch) via the Gateway, the expected behavior is to have the same route in both Routing Information Base (RIB) and the Forwarding Information Base (FIB). Due to a software defect, when the tunnel towards the Gateway flaps, a new route is installed into the FIB. Because this new route is installed on the FIB, on learning the underlay route auto-correction is done only for the route in the RIB and skipped for the FIB. This issue is only encountered where Edge-to-Edge via Gateway is enabled.

Fixed Issue 151806: Standby Edge restart multiple times or multiple HA_SPLIT_BRAIN_DETECTED events sent by HA enabled Edge.

Standby Edge may miss heartbeat from peers due to stall in packet processing and this leads to Standby Edge being moved to Active state. When the packet processing is resumed, the Edge detects split brain (Active/Active state) and to resolve the split brain the newly HA state transition Edge goes for restart to avoid any packet loss.

Fixed Issue 151812: On the Monitor > Edge > Flows page of Orchestrator UI, a user may observe an incorrect hostname for an Edge's local interface IP address.

In certain scenarios, the Edge's Deep Packet Inspection (DPI) engine can extract and give the server's hostname from a traffic flow that can wrongly be mapped to the Edge's IP address instead of the server's IP address. This incorrect mapping gets stored in the DNS cache as well, and then gets propagated to the

Orchestrator too, causing confusion. To handle this, Edge now extracts the hostname and the IP address from the DPI.

Fixed Issue 151891: The remote diagnostics functionality, specifically the HA_INFO command utilizing JSON APIs, is experiencing issues.

The HA_INFO command in Remote Diagnostics fails with an 'invalid key' error when executed via JSON APIs.

Fixed Issue 151892: A user may observe inaccurate Edge WAN link path status on the Orchestrator UI.

During certificate renewal, the established path in the Edge will tear down and a new path is established. Here the sequence is: a new path comes up and the old path is moved to a quiet state, does a fast re-init and waits for 7 seconds for the path to be deleted. When the old path is deleted, the Edge wrongly updates the connection state as DEAD for the new path and so the path state is shown as DEAD on the Orchestrator UI under the **Monitor** pages.

While the status is incorrect, this has no impact on customer traffic.

Fixed Issue 152094: For a customer enterprise site deployed with a High Availability topology, the customer may observe that the Edge has experienced an Active-Active "Split Brain" state and the Standby Edge has been rebooted to recover.

Two types of heartbeats are sent: one via the HA link every 100ms, and another via the WAN link every 300ms. During forced or voluntary failover, the active edge should not send heartbeats via the WAN link, even after restarting. However, this safeguard check is missing in the WAN heartbeat logic, leading to an A/A state.

Fixed Issue 152144: Edges having interfaces configured with DHCP which have IP addresses in the same subnet may stop establishing tunnels from several interfaces after a DHCP lease renewal.

For example, if an Edge has 3 interfaces: GE3, GE4, and GE6 with IP addresses in the same network, a DHCP lease renewal on an interface or an IP address update on GE3 interface can result in the GE4 and GE6 interfaces to stop establishing VCMP (management) or IPsec tunnels.

Fixed Issue 152258: A secure flag for a BGP route may not be removed if a user disables Secure BGP Routes on a Partner Gateway hand-off configuration.

In this scenario, if the secure flag remains on the BGP route where the customer wanted it removed can result in unexpected routing and traffic disruption.

Fixed Issue 152283: The interface GE5 and GE6 on Edge model 6x0 types with a 9.13 or newer BIOS may not detect carriers if the user disables auto-negotiation.

This behavior is inconsistent, but if encountered on a 6x0 Edge without a fix for this issue, the user should re-enable auto-negotiation on the Orchestrator and save changes, and then disable auto-negotiation.

Fixed Issue 152429: After an HA failover, a few remote routes may not be installed in the FIB.

After an HA failover of the hub, when the tunnel to the spoke comes up but is unstable for some time, the routes from that spoke may be removed as they are considered stale. However, later when the tunnel

becomes stable, the routes are not installed again into the FIB because of mishandling of tunnel up/down events.

Fixed Issue 152463: Spokes not attempting to form dynamic B2B tunnels with clusters as HUBs.

When a cluster is configured just as a HUB and not VPN_HUB, we end up not parsing the 'edgeHubCluster' which ends up in this issue. This occurs only if the cluster is configured as a VPN HUB.

Fixed Issue 152775: An Edge may not update a Partner Gateway's IPv6 static routes with a secure flag if Encrypt is enabled for PG static routes.

This impacts customer traffic that would match those IPv6 static routes and that use a Partner Gateway.

Fixed Issue 153444: When VNF is enabled, ports 4321, 4322, and 5901 become exposed during port scanning.

We run monitoring services for QEMU on ports 4321, 4322, and 5901. The fix is to run them on the localhost IP instead of 0.0.0.0.

Fixed Issue 153640: Overlay routes are not present in Zebra (BGP/OSPF) redistribute tables and hence advertised to (BGP/OSPF) peers.

During spoke movement between hubs/cluster, upgrade/reboot or during a service restart, the system may end up in a timing issue. The remote-spoke UP event is processed first with hub reachability when not set to true. This is followed by remote route addition triggered by the gateway and hub UP event. After the above sequence of events, the route will be present in FIB with reachability True, but would not be synced to BGP/OSPF.

Fixed Issue 153924: Upon receiving an ingress packet on a Marvell switch port, the switch floods it to all other ports if the switch does not have the packet's destination MAC address in its MAC table.

Marvell switches use their Address Translation Unit (ATU) table to forward received packets. If the ATU table does not contain the destination MAC address, the switch floods the packet to all other ports.

Fixed Issue 155311: The MibTree IfXTable functionality is not working as expected.

The MibTree IfXTable issue is caused by the Python framework's MRO strategy and the lack of 'self' references for ifstats.

Fixed Issue 155461: Edges go into 'mgmt-only' mode if no routed interfaces are configured.

Edge interfaces support two modes, namely switched and routed. The issue may show up if one configures all the interfaces in switched mode.

Fixed Issue 155517: The switch experiences multiple cyclic restarts and HA instability when the WAN port connection is repeatedly disrupted.

We restart the DHCP client on every failover, which implicitly flaps the interface and causes HA instability.

Fixed Issue 155822: Network traffic may be interrupted for approximately one minute when rebooting the standby edge device using a Marvell switch.

When using Marvell switches on 610 and 5x0 edge devices in an HA setup, an L2 loop may form briefly during the standby edge's reboot, resulting in a network outage.

Fixed Issue 155881: Customers may experience random edge freezes when a DNS server is hosted behind the edge and receives a high volume of DNS requests.

When a customer's DNS server is hosted behind an edge and DNS queries are sent via the WAN interface, the packets are subject to the DPI engine, even if they have been classified.

Fixed Issue 155974: The Edge device occasionally gets stuck in the initialization stage after being powered off and on.

During power off, the Edge's log buffer can sometimes become corrupted, leading to failed log allocations and the Edge getting stuck in the init stage when attempting to log.

Fixed Issue 156376: Traffic destined for a 0.0.0.0 IP address from a remote spoke site to the hub site may be incorrectly routed, preventing it from reaching its intended destination.

The hub misinterprets traffic with a destination IP of 0.0.0.0 as management traffic. This misinterpretation causes the hub to route the traffic to an incorrect interface, preventing it from reaching its intended destination. This issue only occurs when the destination IP is 0.0.0.0 and a static route for 0.0.0.0/32 is configured on the hub.

Fixed Issue 156458: Users may encounter gateway crashes.

The issue stems from handling external CA certificates. When a CA certificate contains multiple CRL distribution points and/or Authority Access Information, it can lead to crashes in rare cases.

Fixed Issue 156473: The customer may see a warning that the integrity check failed, indicating a potential issue with the system.

This may happen when a customer attempts to upgrade a Gateway using an image generated with a different signing key internally.

Fixed Issue 156637: Protection system does not trigger because the threshold value is wrong in the Edge.

Customers testing network and flood protection settings on 720/740 models, when configuring a 25 percent threshold, find that the protection is triggered at a certain threshold, but the actual trigger occurs at a different value.

Fixed Issue 157187: When VRRP is enabled on a sub-interface in an edge device, traffic using the VRRP MAC address is being dropped.

When VRRP is enabled on a sub-interface and the edge device acts as the VRRP master, a bug in the code causes the parent interface to be fetched instead of the sub-interface. This results in traffic being dropped due to a MAC address mismatch.

Fixed Issue 157665: When the IDPS is enabled, the `/var/log/suricata.log` file grows in size over time without being rotated. This can lead to increased system memory usage on low-end platforms, potentially causing the system to run out of memory.

With IDPS enabled, the engine generates logs during initialization, rule parsing, and rule reloads (which occur daily with updated IDPS bundles). These logs are written directly to `/var/log/suricata.log`, leading to file growth that can consume significant space in tmpfs, especially on low-end platforms. To address this, we've disabled direct file logging and implemented a logger callback. This allows the edge to leverage its own logging infrastructure, which includes file rotation based on configured size limits.

Fixed Issue 157667: Spokes routes are missing on cluster members after tunnel flaps.

Customers may experience an ISP outage on their hub for a few minutes. This outage caused all tunnels to the spokes and gateways to flap, resulting in numerous CONNECT/DISCONNECT events. These events led to delays in processing stale route timers and deleting routes from the FIB.

Fixed Issue 157837: OSPFd may restart in an Edge router.

Enabling OSPFd on a limited number of interfaces in an edge router, followed by its complete disabling, can potentially lead to memory corruption and a crash of the OSPFd process. This is due to the memory cleanup process, which may not be designed to handle partial enablement scenarios.

Fixed Issue 157898: Link shows as deactivated in Orchestrator for a HA Edge.

After a specific sequence of HA state transitions, we keep pushing old events repeatedly to the Orchestrator. If LINK_DEAD is one of these events that we continuously push, the link state will be stuck deactivated on the Orchestrator.

Fixed Issue 157962: Customer may observe tunnel establishment failure.

If, for any reason, IP addresses associated with a tunnel interface are removed, the Linux kernel will also remove the default route for that tunnel interface. When the IP addresses are re-added, the default route for the tunnel interface will be missing from the routing table.

Fixed Issue 158032: An Edge router may occasionally get stuck in the init stage after a restart.

Before the logging ring buffer's first wraparound, blocks allocated but not written to since the Edge's last restart remain unreset. This may lead to problems with subsequent log buffer allocations after restarting, potentially causing the Edge to become stuck in the init phase when attempting to log.

Fixed Issue 158144: The event 'Edge USB Ports Enable Failure' is incorrectly triggered on edge devices that do not support the USB disable feature. This event should only occur on devices where USB disable functionality is present but fails to execute.

Edge devices, despite lacking support for USB port disabling, perform checks for USB port disable status in various scenarios. This results in the erroneous reporting of 'Edge USB Ports Enable Failure' events, even though USB disable functionality is not available.

Fixed Issue 158195: LAN clients can not access some tagged VLANs on 5x0 and 610 edges if the configured untagged VLANs differ.

On 5x0 and 610 Edge devices, when users configure switched interfaces as trunk ports, the Edge creates VLAN interfaces. However, this process can fail if the untagged VLAN configurations on the Edge device differ. This failure prevents clients from accessing the intended VLANs.

Fixed Issue 158456: HA Edge drops all the traffic received on LAN interfaces.

When LoS (Loss of Signal) is configured on the HA Edge, the LAN port is incorrectly blocked on the Active Edge. This results in all traffic received on the LAN interfaces being dropped.

Fixed Issue 158500: Edges stop forwarding LAN-side tagged traffic between LAN and WAN after upgrading to 5.2 or newer when the network configuration is managed by a 4.x Orchestrator.

When using a 4.x Orchestrator, administrators configure Edge network settings. Orchestrator uses untagged interfaces for LAN, meaning it does not specify VLANs in the configuration. After upgrading both Edge and Orchestrator to version 5.2 or newer, the Edge software fails to generate the correct LAN network configuration due to the missing VLAN information. This incompatibility prevents the Edges from processing LAN-side tagged packets.

Fixed Issue 158568: The sentence "WebSocket JSON format response for 'SYSTEM INFORMATION' cpu 30savg_pct is empty. Usually customer can request for this info via postman.

When requesting system information, the call actually triggers a health check, which retrieves the **cpu_30s_avg_pct**. However, starting with release 5.1, we no longer send **cpu_30s_avg_pct**. Instead, we send **cpu_60s_avg_pct**. Because **cpu_30s_avg_pct** is not found, Postman will display it as 0.

Fixed Issue 159329: Return packets are dropped and NAT table entries are leaked for Internet-bound flows originating from the Partner Gateway (PG) handoff interface VLANs.

Internet-bound flows that originate from the PG handoff interface are not properly handled in the Gateway leading to dropped packets and leaked resources.

Fixed Issue 159092: When the active edge in an HA pair occasionally reports its peer as "unknown," this can disrupt enhanced HA traffic.

An error in calculating the last seen time for the standby Edge causes the active edge to incorrectly assume a lack of communication. This leads to the active Edge declaring the standby edge as 'unknown', resulting in the reset of enhanced HA connections.

Fixed Issue 159337: TCP connections between e2e peers may be disrupted when one side is upgraded or loses context, especially if the connections use fixed port numbers.

When a customer upgrades their Edge on one side of an e2e TCP connection (e.g., the client side) and the TCP server behind another edge has also lost context of the connection, new TCP connections initiated from behind the upgraded customer can become stuck in an established state without transmitting any meaningful traffic.

Fixed Issue 159532: When the Orchestrator's manual DNS source interface configuration is not reflected on the Edge, DNS packets originating from the Edge device carry an incorrect source address. Without proper routing to this incorrect source, DNS reply packets will not reach the Edge.

Users need to select a specific DNS source interface in the orchestrator, rather than using the automatic selection.

Fixed Issue 159733: NAT sessions are leaked when L7 Health Check is enabled.

NAT sessions are leaked when L7 Health Check is enabled on ZScaler IPsec and GRE CSS tunnels.

Fixed Issue 159845: Severity of some of the INFORMATIONAL alerts are wrongly reported to Orchestrator.

Recent changes to Suricata rule metadata by NSX have caused incorrect impact score calculations for some INFO-level alerts. This only affects monitoring and has no impact on traffic.

Fixed Issue 160080: Overlay and datacenter routes are being refreshed frequently, with their age being reset to 1.

Spokes initiating DE2E tunnels to multiple edges with the same public IP will trigger frequent hub configuration messages towards the gateways. This occurs whenever DE2E tunnel establishment fails after N attempts. The failures stem from the lack of defined behavior when DE2E is attempted towards multiple edges with the same public IP. As a result, the gateways refresh the routes they previously advertised in response to the hub configuration messages.

Fixed Issue 162024: The {{debug.py --enterprise_top}} may fail and will not display any valid output.

The user may face this issue when attempting to run the {{debug.py --enterprise_top}} command in a scenario in which the displayed counter's value would have 12 digits or more.

Resolved in Edge/Gateway Version R5250-20241126-GA

Edge/Gateway version R5250-20241126-GA was released on 12-04-2024. This release includes all the fixes up to Edge/Gateway build R5241-20241112-GA.

Known Issues

Open Issues in Release 5.2.5.



Note: Release 5.2.5 is an Edge/Gateway Release only and does not include an Orchestrator component. As a result, no Orchestrator known issues are listed in 5.2.5 Release Notes and such issues continue to be tracked in the 5.2.4 Release Notes.

Edge/Gateway Known Issues

Issue 151806: High Availability PANIC is noticed on Edges.

Standby Edge restarts multiple times or multiple HA_SPLIT BRAIN_DETECTED events are sent by High Availability enabled Edge. Standby Edge misses heartbeat from peer due to stall in packet processing and this leads to Standby Edge moved to Active State. When the packet processing is resumed, Edge detects split brain (Active/Active state) and to resolve the split brain the newly High Availability state transition edge goes for restart to avoid any packet loss.

Workaround: Increase High Availability default failover time to a higher value may reduce or solve the HA split brain.

Issue 14655:

Plugging or unplugging an SFP adapter may cause the device to stop responding on the Edge 540, Edge 840, and Edge 1000 and require a physical reboot.

Workaround: The Edge must be physically rebooted. This may be done either on the Orchestrator using **Remote Actions > Reboot Edge**, or by power-cycling the Edge.

Issue 25504:

Static route costs greater than 255 may result in unpredictable route ordering.

Workaround: Use a route cost between 0 and 255.

Issue 25742:

Underlay accounted traffic is capped at a maximum of the capacity towards the Arista SD-WAN Gateway, even if that is less than the capacity of a private WAN link which is not connected to the Gateway.

Issue 32960:

Interface “Autonegotiation” and “Speed” status might be displayed incorrectly on the Local Web UI for activated Arista SD-WAN Edges.

Workaround: Refer to the Orchestrator UI under **Remote Diagnostics > Interface Status**.

Issue 32981:

Hard-coding speed and duplex on a DPDK-configured port may require an Arista SD-WAN Edge reboot for the configurations to take effect as it requires turning DPDK off.

Workaround: There is no workaround for this issue.

Issue 52955: DHCP decline is not sent from Edge and DHCP rebinding is not restarted after DAD failure in Stateful DHCP.

If DHCPv6 server allocates an address which is detected as duplicate by the kernel during a DAD check then the DHCPv6 client does not send a decline. This will lead to traffic dropping as the interface address will be marked as DAD check failed and will not be used. This will not lead to any traffic looping in the network but traffic blackholing will be seen.

Workaround: There is no workaround for this Issue.

Issue 53219: After an Arista SD-WAN Hub Cluster rebalances, a few Spoke Edges may not have their RPF interface/IIF set properly.

On the affected Spoke Edges, multicast traffic will be impacted. What happens is that after a cluster rebalance, some of the Spoke Edge fail to send a PIM join.

Workaround: This issue will persist until the affected Spoke Edge has an Edge Service restart.

Issue 53934: In an enterprise where an Arista SD-WAN Hub Cluster is configured, if the primary Hub has Multihop BGP neighborships on the LAN side, the customer may experience traffic drops on a Spoke Edge when there is a LAN side failure or when BGP is not configured on all segments.

In a Hub cluster, the primary Hub has Multihop BGP neighborship with a peer device to learn routes. If the physical interface on the Hub by which BGP neighborship is established, goes down, then BGP LAN routes may not become zero despite BGP view being empty. This may cause Hub Cluster rebalancing to not happen. The issue may also be observed when BGP is not configured for all segments and when there are one or more Multihop BGP neighborships.

Workaround: Restart the Hub which had the LAN-side failure (or BGP not activated).

Issue 57210: Even when an Arista SD-WAN Edge is working normally and is able to reach the internet, the LED in the Local UI's Overview page shows as "Red".

The Edge's Local UI determines the Edge's connectivity by whether it can resolve a well known name via Google's DNS resolver (8.8.8.8). If it cannot do so for any reason, then it thinks it is offline and shows the LED as red.

Workaround: There is no workaround for this issue, except to ensure that DNS traffic to 8.8.8.8 can reach the destination and be resolved successfully.

Issue 61543: If more than one 1:1 NAT rule is configured on different interfaces with the same Inside IP, the inbound traffic can be received on one interface and the outbound packets of the same flow can be routed via different interface.

For the NAT flows from Outside to Inside, the 1:1 NAT rules will be matched against the Outside IP and the interface where the packets are received. For the outbound packets of the same flow, the Arista SD-WAN Edge will try to match the NAT rules again comparing the Inside IP and the outbound traffic can be routed via the interface configured in the first matching rule with "Outbound Traffic" configured.

Workaround: There is no workaround for this issue outside of ensuring no more than one 1:1 NAT rule is configured with a particular Inside IP address.

Issue 65560: Traffic from a customer to PE (Provider Edge) device fails.

BGP neighborship between a Partner Gateway and Provider Edge does not get established when tag-type is selected as "none" on the handoff configuration. This is because ctag, stag values get picked from /etc/config/gatewayd instead of the handoff configuration on the Orchestrator when tag-type is "none".

Workaround: Update the ctag, stag values to 0 each under vrf_vlan->tag_info in /etc/config/gatewayd. Do a vc_procmmon restart.

Issue 67879: A Cloud Security Service (CSS) tunnel is deleted after a user changes a WAN Overlay setting from auto-detect to user-defined on a WAN interface setting.

After saving the changes, the CSS tunnels do not come back up until the customer takes down and then puts back up the tunnel. Changing the WAN configuration will bring down the CSS tunnel and parse the CSS setup again. However, in some corner cases, the *nvs_config>num_gre_links* is 0 and the CSS tunnel fails to come up.

Workaround: Deactivate the CSS setup, and then reactivate it and this will bring the CSS tunnel up.

Issue 68057: DHCPv6 release packet is not sent from the Arista SD-WAN Edge on the changing of a WAN interface address mode from DHCP stateful to static IPv6 address and the lease remains active till reaching its valid time.

The DHCPv6 client possesses a lease which it does not release when the configuration change is done. The lease remains valid till its lifetime expires in the DHCPv6 server and is deleted.

Workaround: There is no way of remediating this issue as the lease would remain active till valid lifetime.

Issue 68851: If an Arista SD-WAN Edge and Arista SD-WAN Gateway each have the same TCP syslog server configured, the TCP connection is not established from the Edge to the syslog server.

If the Edge and Gateway each have the same TCP server and if the syslog packets from the Edge are routed via the Gateway, the syslog server sends a TCP reset to the Edge.

Workaround: Send the syslog packets direct from the Edge instead of routing via a Gateway or configure a different syslog server for the Edge and Gateway.

Issue 81852: For an Arista SD-WAN Edge that is using a Zscaler type Cloud Security Service (CSS) which uses GRE tunnels that has turned on L7 Health Check, when that Edge is upgraded to Release 5.0.0, in some instances the customer may observe L7 Health Check errors.

This is typically seen during software upgrade or during startup time. When L7 Health check for a CSS using GRE tunnels is turned on, error messages related to socket getaddress error may be seen. The observed error is intermittently seen, and not consistent. Because of this, L7 Health Check probe messages are not sent out.

Workaround: Without the fix, to remediate the issue, a user needs to turn off and then turn back on the L7 Health Check configuration, and this feature would then work as expected.

Issue 82184: On an Arista SD-WAN Edge which is running Edge Release 5.0.0, when a traceroute or traceroute6 is run to the Edge's br-network IPv4/IPv6 address, the traceroute will not properly terminate when a UDP probe used.

Traceroute or traceroute6 to the Edge's br-network IPv4/IPv6 address will not properly when Default Mode (in other words, UDP probe) is used.

Workaround: Use -I option in traceroute and traceroute6 to use ICMP probe and then traceroute to br-network IPv4/IPv6 address will work as expected.

Issue 85402: For a customer enterprise using BGP with Partner Gateways configured, a user may observe that some BGP neighborships are down and this causes customer traffic issues.

If a customer has maximum-prefix configured on a router which has BGP peering with the Edge and Gateway, the BGP session may be dropped by the router.

For example, if the router has BGP configured to only receive max 'n' number of prefixes, but the Edge and Gateway have more than 'n' number of prefixes to be advertised in the absence of any filters. Now if the BGP filter configuration is changed on the Orchestrator, even if the total number of prefixes allowed in the outbound direction is less than 'n', the issue will be encountered where more than 'n' prefixes are sent to the peer before any filters are applied. This causes the router to tear down the session.

Workaround: If BGP goes down due to this issue (Maximum Number of Prefixes Reached), flap BGP on the peer using CLI (For FRR/Cisco, "neighbor x shut" followed by "no neighbor x shut"), and the BGP will produce only the desired number of prefixes advertised to the peer.

Issue 92421: When a public and private overlay are configured on the same Edge interface with different custom VLAN tags, there is a chance that the underlay routed traffic may get dropped.

When a public and private overlay are configured on the same interface with different custom VLAN tags, the Edge may learn the ARP entries with the wrong VLAN tags, resulting in the traffic being dropped.

Workaround: Avoid using this configuration. This issue is fixed on Release 5.4.0 and later.

Issue 98136: For customer enterprises using a Hub/Spoke topology where Dynamic Branch To Branch VPN is configured, client users behind a SD-WAN Spoke Edge may observe that some traffic has unexpected latency resulting from the traffic using a sub-optimal path.

Spoke Edge traffic that experiences this issue uses a route that was initially a non-uplink route for a Hub Edge not included in the Profile the Spoke Edge was using. A Dynamic Branch-to-Branch VPN tunnel can be formed from the Spoke Edge to the Hub Edge because of traffic being sent towards some other unrelated prefix and in this instance the non-uplink route is installed in the Spoke Edge.

As a result of this non-uplink route, all traffic towards this prefix starts going through the

Hub Edge and the non-uplink route becomes uplink (community change to uplink community) but the non-uplink route installed previously is not revoked and the traffic takes the Hub Edge path as long as the Dynamic Branch-to-Branch VPN tunnel remains up.

Workaround: Wait for the Dynamic Branch-to-Branch VPN tunnel to tear down, after which the uplink route will not be installed in the Spoke Edge when a new Dynamic Branch-to-Branch VPN tunnel is formed towards the Hub Edge.

Issue 110561: Dynamic tunnels may not come up between the same set of Arista SD-WAN Edges with bidirectional traffic when traffic stops and then restarts.

Issue is observed in a test environment where there are 6000 dynamic tunnels with high bidirectional traffic being sent between the Edges. Even in lower scale testing at 1000 dynamic tunnels, not all the tunnels come up.

Workaround: There is no workaround for this issue.

Issue 111085: When an Arista SD-WAN Edge's WAN link is configured with an IP address in the same network as the Edge's loopback IP, the Edge uses the MAC address of the WAN interface while responding to an ARP request for the Edge's loopback IP address.

This can cause ARP spoof and results in the Management IP being deprecated and network disruptions as a result.

Workaround: There is no workaround for this issue.

Issue 113877: For customers who configure BGP/GRE LAN, those using a TGW GRE will experience BGP flaps and traffic interruption on the TGW secondary tunnel in all segments when the BGP configuration for TGW GRE is modified on the Global segment.

When customer changes a BGP configuration of TGW GRE on the global segment then the secondary tunnel in the global and other segments flap, leading to a BGP connection reset and reconvergence and traffic interruption. The BGP connection will form again, and traffic will restore.

Workaround: There is no workaround for this issue.

Issue 117876: In a customer site using a High Availability topology, if a user activates or deactivates the Enhanced Firewall Services, an Arista SD-WAN HA Edge may experience multiple restarts.

When **Enhanced Firewall Services** is activated or deactivated, only the Active Edge's Device Settings configuration is synchronized immediately with the Standby Edge, with the remainder of the configuration synchronization is only in response to a Standby Edge heartbeat. When the Active Edge is restarted to apply the latest configuration prior to receiving a heartbeat from the Standby Edge it will result in a configuration mismatch between the two HA Edges and they will undergo multiple restarts to complete the configuration synchronization.

Workaround: The only workaround is to turn on or off Enhanced Firewall Services during a maintenance window for HA Edges.

Issue 125274: When a customer runs an SNMP walk, the loopback interface of the Arista SD-WAN Edge is not discovered.

The Edge loopback interface is a unique interface category that the Edge does not classify as either WAN or LAN. As a result, the loopback interface is not in the allow list of interfaces to process for the *snmp-request*.

Workaround: There is no workaround for this issue. The loopback interface status would have to be individually monitored through the Orchestrator UI.

Issue 130674: IPv6 remote routes may be missing if the only physical interface configured with IPv6 is disconnected during Edge boot up and only later reconnected.

An Edge will not install any IPv6 remote routes when the only physical interface configured with IPv6 is not connected to the Edge while it is rebooting and then only later connected.

Workaround: Enable IPv6 loopback, or use a switched interface assigned to a IPv6 VLAN.

Issue 130885: An OSPFv3 route tag may not be updated for an IPv6 external route.

In some corner cases, OSPFv3 does not consider the tag updated by the neighbor for an external route if the update is received within very short interval.

Workaround: Withdraw and re-advertise the external route from the OSPFv3 neighbor.

Issue 131674: ICMP traffic from a Spoke Edge using internet backhaul via a Hub Edge fails if the ICMP flow has to be steered from one link to a different one.

ICMP traffic passing on one of two or more links is expected to be steered to a different link if the existing link goes down or is unusable per QoE.

Workaround: There is no workaround for this issue.

Issue 132492: For a customer who has one or more Non SD-WAN Destinations via Edge configured and uses BGP, when no traffic is passing through the IPsec tunnels, the customer may observe that the tunnels are torn down and BGP routes flap.

This issue is only seen when there is no traffic on the path from the NSD via Edge to the peer. The issue stems from a premature IKE Phase 1 rekey on the Edge and the peer sends multiple Dead Peer Detection (DPD) packets with an old cookie that the Edge does not acknowledge. This results in the peer side deleting both Phase 1 and Phase 2 IKE and tearing down the tunnels which also causes BGP flaps.

Workaround: A user could set up a LAN side client to send a continuous ping to the NSD via Edge peer to prevent the scenario from arising.

Issue 133678: If an Arista SD-WAN Edge is configured for IPv4/IPv6 dual stack, the Edge may lose connectivity to the Orchestrator if the IPv4 link is down.

This issue can occur if the Edge was activated with only an IPv4 link, and an IPv6 link is added only later to the device. At the time the Edge is activated, only the IPv4 Orchestrator address is written to the Edge that manages Orchestrator connectivity. Adding an IPv6 link later does not add the IPv6 address to the file and so if the IPv4 link is removed, the Edge loses connectivity to the Orchestrator.

Workaround: An Edge activated with only an IPv4 link would need to keep at least one IPv4 WAN link connected even though the Edge is dual stack.

Issue 135827: For a customer site deployed with a High Availability topology, the customer may observe multiple HA failovers due to the site experiencing an active-active (split brain) condition.

Under extreme load/scale environments where the flow, tunnel, and routes scale to the limits of a hardware Edge model in conjunction with aggressive route timers (OSPF = 3/12, BGP = 1/3), the HA Standby Edge can sometimes miss an HA heartbeat and be moved to an Active state. When the HA heartbeat is resumed it will report the HA_SPLIT_BRAIN_DETECTED event to the Orchestrator and the Standby Edge will restart to tie-break the HA split brain.

Workaround: To mitigate the risk of an active-active panic, configure the HA failover time to a higher value.

Issue 135938: For an Edge configured with a routed LAN interface and a secondary IP address configured on the routed interface, traffic sent to the secondary IP address connected interface is NATed with the parent interface's IP address.

Whether the user checks the NAT Direct Traffic option or not has no impact, as the traffic is sent out based on the NAT direct configuration of the parent interface.

Workaround: There is no workaround beyond ensuring that the secondary IP address is configured with the expectation that the NAT Direct Traffic option is only applied at the parent level.

Issue 136336: For a customer who configures a Cloud Security Service (CSS) with a Zscaler type, return traffic from Zscaler may get dropped if the Edge has the Common Criteria Firewall enabled.

The Edge would have a Business Policy rule to backhaul internet traffic via that Zscalar tunnel and in this case the return traffic is dropped due to a Reverse Path Forwarding (RPF) failure that occurs during the route lookup for the return traffic.

Workaround: Do not use the Common Criteria Firewall feature while also using Zscaler as a CSS.

Issue 138023: For a customer using a Partner Gateway (PG), a PG-BGP session does not come up when the BGP local IP address and PG Handoff local IP address are from the same subnet.

SD-WAN treats this scenario as two interfaces on a router from the same subnet, which is not supported and can lead to ARP related issues.

Workaround: Change the configuration to avoid the above scenario.

Issue 139855: For a customer enterprise where a High Availability topology is used and the Edges are virtual (not hardware Edges), if a user changes any Edge device setting, the Edge may delete the default route.

This issue is limited to sites where the virtual HA Edges use a unique MAC Address on the LAN interface and have routing configured on the LAN interface. In that scenario the default route via a route interface (WAN overlay) and LAN interface may be removed after any changes on the **Configure > Edge > Device** page, resulting in customer traffic disruption.

Workaround: Perform a network service restart to repopulate the default routes.

Issue 140194: For a customer enterprise site deployed with an Enhanced High Availability topology where a PPPoE link is used on the Standby Edge interface, an SNMPWalk does not work properly for this site.

SNMPWalk output is incomplete for interface related MIBs when there is a PPPoE interface on the Standby Edge in Enhanced HA.

Workaround: None.

Issue 140785: An SD-WAN Edge configured with IPv4 and IPv6 loop back interfaces and their advertise flags enabled may experience a Dataplane Service Failure and restart to recover.

Packet fragmentation from packets 1350 bytes and greater is triggering an exception with the Edge service if configured as above and causing a service failure.

Workaround: There is no workaround for this issue.

Issue 141008: On the Diagnostics > Remote Diagnostics page of the Orchestrator UI, Traceroute using an IP/Hostname destination does not work for IPv6 addresses.

The result from an IPv6 **Traceroute** shows the destination alone, and intermediate hops do not display. IPv4 addresses work as expected.

Workaround: There is no workaround for this issue.

Issue 141041: For a customer enterprise site deployed with a High Availability topology with VNFs installed, where the HA Edge pair or either Edge models 520/540 or 610, reachability to the Standby Edge's VNF from a LAN-connected client may fail.

The Ethernet switch board on these Edge models drops ARP reply packets sent to a LAN client from a Standby Edge's VNF resulting in a loss of reachability.

This issue was first observed for the 5.4.x Edge build and documented in 102583 of the 5.4.0 Release Notes. This ticket tracks the issue for 5.2.3.

Workaround: There is no workaround for this issue.

Issue 141113: An SNMP walk may get timed out and fail to complete when the Edge has an interface configured for a PPPoE link which is stuck in a down state.

This issue only occurs if the PPPoE link on the interface is never up, if the interface is up and goes down for some reason the SNMP walk will successfully complete.

Workaround: Ensure that any configured PPPoE link is capable of coming up, in other words ensure the peer PPPoE server is enabled.

Issue 141273: For a customer enterprise site deployed with a High Availability topology, when HA is later deactivated, the virtual MAC addresses persist on the now standalone Edge ports.

The virtual MAC addresses (VMAC) are programmed on the Active and Standby Edge when HA is activated to facilitate faster convergence during HA failover. However, when HA is deactivated on the Edge, the VMAC is still programmed on it. Also, if the Standby Edge is removed and also used as a separate standalone Edge, the result is duplicate MAC addresses and this leads to switch loop if both Edges (old Active and old Standby) are on the same broadcast Network.

A user can confirm this issue is present because the virtual MAC address prefix always begins with **F0:8E:db**.

Workaround: On an Edge without a fix for this issue the user can either force a factory reset on each standalone Edge to clear the port configuration, or the Support team can remove the /velocloud/ha/virtualmacs file from the Edge and reboot it.

Issue 143450: On a customer enterprise site configured with an Enhanced High Availability topology where Dynamic Branch to Branch VPN is also enabled, client users may observe extended traffic loss after an HA failover.

The issue can be encountered if the Enhanced HA site also has a Business Policy rule configured which includes mandatory link steering. Combined with Dynamic Branch to Branch, this combination can result in a prolonged period of traffic disruption after an HA failover.

Workaround: A customer can either remove the Business Policy rule with mandatory link steering entirely, or modify that rule to remove the mandatory link steering option.

Issue 143828: A customer may observe that an Edge has an unexpectedly high level of memory usage that may get sufficiently high to reach a critical level and trigger a defensive Edge service restart to recover the memory.

One of the factors that contributes to this memory leak is extensive use of CLI commands on the Edge by either a Partner or Operator as part of troubleshooting or monitoring the Edge. These commands are accumulated and never cleared from the relevant Edge process. The use of **Remote Diagnostics** on the Orchestrator UI does not contribute to this issue.

As with any Edge memory usage issue, entry level Edge models with lower RAM specifications (in other words, the Edge models 510, 610, 710, or 520) would be more likely to experience the issue, but it can happen on any Edge model with sufficiently high memory usage.

Workaround: Extensive use of CLI commands on the Edge by either an Operator or Partner should be avoided, and if troubleshooting work is done, the customer should check the Edge's memory usage on the **Edge > Monitor > System** page.

Issue 145393: A customer enterprise site deployed with an Edge model 620, 640, or 680 where firewall logging is configured may observe that the Edge no longer stores new firewall or standard debugging logs.

When this issue is encountered, a 6x0 Edge's eMMC storage experiences an excessive level of wear due to the high volume of writes and rewrites that can be triggered by enabling logging for firewall rules which are matched by a large number of new connections per second in a high traffic customer environment. This issue results in the Edge defensively moving the file partition which hosts logging to a read-only state, and no additional logs are stored.

Workaround: If a customer has an Edge 620, 640, or 640 Edge model and is also using firewall logging, they should avoid enabling logging for firewall rules which can potentially match a large number of new connections in a high traffic environment. The excessive logging frequency that would result can cause undue wear on the Edge's storage and trigger this issue.