DRIVENETS®

DNOS Release Notes

Downloaded: October 4, 2023

Contents

Software and Firmware Support Highlights

The following table lists the software deliveries available in this release

Software	Description	Software Image
DNOS	DriveNets Network Operating System	18.2.1.1
CAL	DriveNets Golden Image	18.2.1.1
StrataX	DNOS NCM NOS	1.2.0.3
Base-OS	Base-OS	2.18212534001
FW and ONIE	DNOS NCM FW and ONIE Bundle	18.2.0.1.1
DNOR	DriveNets Network Orchestrator	18.2.0.4

For the full list of supported items, see Supported hardware and Supported software and firmware in the documentation portal.

Initial Cluster Configuration

All the initial configuration of a cluster before deployment can now be executed from the CAL CLI. The prerequisite configuration, such as management IP and DNOR address, needs to be executed on the active NCC or NCP (in the case of a standalone).

To access the CAL CLI, use the command `dncli` on the Linux prompt. When DNOS is not implemented, the command directs the CAL CLI; when DNOS is installed, DNOS CLI opens.

Precheck Tracking and History

Precheck history is now saved as a task and can be accessed from the DNOS logs or DNOR 'logs' sub-tab under 'installation'. The history entries preserve the result of the overall precheck and the result for each test.

DNOR Reachability Status Check

You can now check the current DNOR reachability status via a show command that displays a list of DNOR hosts and their reachability status.

To see the reachability status, use the `show mgmt dnor-server reachability` command.

To clear the configured DNOR servers in the system, use the `clear mgmt dnor-server` command.

Enhancements to ZR+ Coherent Optics

Multiple enhancements have been added to DNOS to improve the experience when working with ZR+ coherent optics via the CLI:

After frequency configuration via the CLI, it can take several minutes for the change to take effect after the transceiver is reset. During this period, a link-down indication is provided, but the `show transceiver` command does not indicate the transceiver is being reset. You can now see the reset status under the `show interface transceiver` command.

A new system event has been added, 'PLATFORM_TRANSCEIVER_ZRPLUS_CONFIGURATION_ERROR', that indicates when a

configuration process of the transceiver has failed due to wrong user inputs such as central wavelength.

Several ZR+ specific parameters have been added to the `show transceiver` command:

Transceiver-supported grids.

Transceiver-supported frequency range per grid.

Transceiver (configurable) Tx power.

With grid 75GHz, the spec defines each channel to be 25GHz wide. However, most transceivers require the channel to be an integer multiple of 3, effectively only accepting frequency offsets multiples of 75GHz. To avoid inconsistency, the CLI now rounds up frequencies to the nearest 75GHz multiple instead of 25GHz.

Addition to the show system version Command

If a patch was installed in the system, you can view it in the `show system version` command.

Integrity-report File Retrieval

All files in the integrity report can now be copied from the cluster. When a file is suspected, you can copy the file to a new DNOS directory, 'integrity_report_retrieves'; this directory can be accessed from an external device using SCP or FTP, and it can contain up to 10 files.

To copy a file, use the `request file copy integrity-report-retrieves ncc <<ncc_id>> <<container>> <<source-file-abs-path>> destination-folder [force]` command.

To delete all the files in the directory, use the `request file delete integrity-report-retrieve <<file-path>> | all` command.

New Hardware Utilization System Events Added

DNOS has added new system events that help monitor hardware resource utilization.

File Descriptors utilization event at the process level:

FD_WARNING_LEVEL_REACHED, triggered at 40% FD utilization, cleared after -10% FD utilization.

FD_CRITICAL_LEVEL_REACHED, triggered at 80% FD utilization, cleared after -10% FD utilization.

CPU utilization event at the process level:

CPU_WARNING_LEVEL_REACHED, triggered at 35% CPU utilization, cleared after -20% CPU utilization.

CPU_CRITICAL_LEVEL_REACHED, triggered at 50% CPU utilization, cleared after -20% CPU utilization.

These system events are triggered 30 seconds after the threshold is reached/crossed. They are cleared 30 seconds after the threshold returns to normal.

Display Changes in PIM System Events and Show Commands

The following show commands have changed:

The `protocols pim maximum-states` command is now the `protocols pim maximum-mfib-routes` command.

In the `show pim summary` command:

A 'Total PIM MFIB routes' counter that accommodates all MFIB entries installed due to PIM states (including MoFRR and MBB) has been added.

Maximum and Threshold counters were renamed to reflect the total of the MFIB entries.

The following system events have been renamed and updated to accommodate actual MFIB entries installed for the PIM states (including MoFRR and MBB):

'PIM_MAXIMUM_STATES_THRESHOLD_CLEARED' is now 'PIM_MAXIMUM_MFIB_ROUTES_THRESHOLD_CLEARED'.

'PIM_MAXIMUM_STATES_THRESHOLD_EXCEEDED' is now 'PIM_MAXIMUM_MFIB_ROUTES_THRESHOLD_EXCEEDED'.

'PIM_MAXIMUM_STATES_LIMIT_CLEARED' is now 'PIM_MAXIMUM_MFIB_ROUTES_LIMIT_CLEARED'.

'PIM_MAXIMUM_STATES_LIMIT_REACHED' is now 'PIM_MAXIMUM_MFIB_ROUTES_LIMIT_REACHED'.

OSPFv2 Multi-area SR-TE Policy

DNOS now supports multi-area SR-TE policies. Previously, DNOS supported single-area SR-TE policies only, where the head SR-TE policy node and the policy's destination router were in the

same OSPFv2 area. DNOS supports explicitly configured multi-area SR-TE policies or empty-path multi-area policies. Explicitly configured policies are policies constructed with a user-defined segment list, empty-path policies are policies with no segment list definition, and the SR-TE policy automatically derives the destination's SR node-sid as a single SID in the SR-TE policy stack.

A new optional ‘external’ knob is also introduced as part of the newly supported SR-TE multi-area policy. The external optional knob is used in cases where the destination node-sid is not resolvable on the head SR-TE node, for example, in cases of stub or NSSA OSPFv2 areas. When the ‘external’ knob is not set, DNOS's default behavior automatically derives the policy's destination address as the last label/segment of the policy's label stack, unchanged from the previous DNOS behavior. When the ‘external’ knob is set, the policy's destination address is automatically derived and added to the policy's label stack.

OSPF-SR Adjacency SID Protection

Link adjacency-SID protection creates a link-protection TI-LFA path to the adjacent node behind the given Adjacency-SID. The link protection is installed as an alternate path for adjacency-SID ILM entry, allowing SR head nodes to create SR policies with protected adjacency SIDs, in which DNOS can act as a Point of Local Repair (PLR) and protect the relevant adjacency SIDs in cases of link failures.

ISIS Duplicate System-ID Detection

ISIS duplicate system-ID issues are now prevented by implementing the Fingerprint TLV as described in RFC 8196. The Fingerprint TLV can be used to detect an ISIS duplicate system-ID. When a router receives an ISIS LSP with a Fingerprint TLV, it compares the fingerprint value with its calculated fingerprint value. If the values match, the received LSP is a duplicate and can be discarded; this mechanism helps to prevent network instability caused by duplicate system-IDs in an ISIS network.

The LSP fingerprint is disabled by default. To enable it, configure `lsp-fingerprint` under protocols isis.

Configurable Packet Length for Netflow Exporter

Previously, the DNOS router only supported predefined packet length when using Netflow. Now you can configure a specific packet length for exported packets, ranging from 522 to 9286. If you do not configure a value, the default packet length is 1468.

To configure the Netflow exporter packet length, use the `services flow-monitoring exporter-profile EXP_SERVER_1 packet-length<522-9286>` command.

To view the current Netflow exported packet length, use the `show services flow-monitoring exporter-profile EXP_SERVER_1` command.

BUM Policer

L2-Service Enabled Interfaces and Sub-Interfaces may be prone to attacks of broadcast, multicast, and unknown-unicast (BUM) packets. For EVPN, Bridge-Domain, VPLS, and other L2VPN services (except VPWS), these BUM packets flood all other members of the L2 service. To flood a packet to the other interfaces, the packet must be replicated once for each member participating in the service. To reduce the number of replicated packets, the BUM policer can be used per L2 service instance.

Early Alert for DDR4 DIMM

We now support an early alert mechanism for DDR4 DIMM on the NCP-40C, NCP-10CD, and NCF Ufispace platforms. A system event is generated 'PLATFORM_MEMORY_CONSISTENT_CORRECTABLE_ERROR' if the error count on the RAM is above a certain threshold (6,219*2*0.8 = 9,950 [correctable error count]), the error count is monitored via the x86 correctable errors counter registers, every hour. If a measurement is above the threshold, another measurement follows 2 seconds later to validate the result, and if the results match and both attempts pass the threshold, the system event is triggered to indicate the DIMM may require a replacement, as a consistent bit flip is detected.

Resolved Issues

Issue ID	Description	Component
SW-123577	Traffic loss may happen for labeled routes when race occurs. When this happens, the acknowledged sequence is set to a maximum 64-bit value, which then causes all sequences to be acknowledged, and, as a result, they are advertised immediately, even before reaching HW.	BGP
SW-122911	When a df election hasn't taken place yet - the displayed time of the last df election is wrong, as seen in the `show evpn show evpn instance <> ethernet-segments` command.	EVPN
SW-80224	The management interface's uptime is shown when the interface is disabled. This issue has no impact on the functionality of the management interfaces. When the management interface is enabled, the displayed uptime of the interface is correct.	INTERFACES
SW-122598	MPLS OAM trace command may wrongly fail when using it for a BGP-LU route resolved via RSVP tunnel.	MPLS OAM
SW-123250	Removing an interface from OSPF during GR may still leave OSPF enabled on that interface.	OSPF
SW-122986	coldStart and warmStart SNMP traps are not sent in the case of a system restart.	SNMP
SW-121956	After an NCC switchover or a system restart, the system event logs are written in UTC time even though the time zone is configured.	System Events & Logging

Known Issues

Issue ID	Description	Component	Solution
SW-77147	On rare occasions, when executing the `show bfd sessions` CLI command, some BFD sessions may appear with an uptime value of -1 days. There is no adverse effect on the network operations.	BFD	Clear the BFD sessions to trigger a reset in the uptime.
SW-108914	In an EVPN afi/safi, if a type-3 IM route is received with a different P-Multicast Service Interface (PMSI) tunnel type than the supported type of ingress replication, it is rejected instead of being ignored/retransmitted.	BGP	Currently, there is no workaround.
SW-100903	Traffic over IPv6 routes with IPv4 nexthops is not supported.	BGP	Currently, there is no workaround.
SW-124229	The CLI configuration rebase session fails during commit confirm.	CLI	Reopen a new CLI session after a commit confirm rollback.
SW-113263	The user might be unable to delete commands that share the optional parameter 'n' as other commands in the same hierarchy.	CLI	Delete the entire command and not only the optional 'n' parameter.
SW-125945	You cannot view the active NCC's CLI logs and traces stored on the standby NCC.	CLI	Enter the node_manager container on the standby NCC to view the logs from there or create a techsupport file to inspect the

Issue ID	Description	Component	Solution
			files from the techsupport archive.
SW-101514	After the BaseOS upgrade, the hostname returns to the default name, vRouter. This makes it unreachable by name, as the system only recognizes the newly configured hostname.	CLI	To change the default name, use the `system name` configuration command after the BaseOS upgrade.
SW-124846	On standalone setups, the HW clock does not have a battery. In addition, in CAL, there is no support for NTP time synchronization. As a result, in some cases, the clock might move backward, and tasks' timestamps might be inaccurate.	DNOS Deployment, Upgrade, Revert	This is a view issue only.
SW-125345	In a high-scale scenario, when an interface has more than hundreds of active subs, in redundancy mode, and a CE device sends high-rate traffic there are a few seconds of traffic loss.	EVPN	Currently, there is no workaround.
SW-124547	Because LACP is not supported on EVPN, there may be traffic loss of a few seconds when enabling AC in all-active MH EVPN service.	EVPN	Currently, there is no workaround.
SW-123353	For EVPN services, when a DN and Cisco router are multi-homed together and running MOD DF election algorithm - Cisco's service carving elects DFs per ESI/EVI combination and not	EVPN	Configure the Preference Algorithm to be used on all the routers.

Issue ID	Description	Component	Solution
	per ESI/ETH-TAG. This leads to traffic loss.		
SW-122829	When an AC interface goes up, only one system even should be generated, 'INTERFACE_UP'. Instead, the system events are generated in this order: • 'INTERFACE_UP' • 'INTERFACE_DOWN' • 'INTERFACE_UP' This happens because there is a momentary flap of the interface on its way UP due to the L2-service being enabled on the interface.	EVPN	Currently, there is no workaround.
SW-122282	In EVPN, the two routes, type-1/EVI, and type1/ESI, depend on each other. If one of them doesn't exist, the other one should not be used for installation. of the PE device as the NH device. DNOS only checks if type 1/ESI exists, which can lead to installation issues.	EVPN	Currently, there is no workaround.
SW-120751	DF election happens only if there is a change in the type four EVPN messages. Due to this, when an AC goes down, or the EVPN-VPWS service is admin-disabled, it is not the last AC that uses this ESI. The type four remains, and no change happens in the DF election since DNOS does not check the existence of type 1/EVI routes.	EVPN	Currently, there is no workaround.

Issue ID	Description	Component	Solution
SW-125798	When a local AC is attached to an ESI that operates in a single-active mode and acts as the DF, there is a short period in which traffic is broadcast when switching the AC link from down to up.	EVPN	Currently, there is no workaround.
SW-122241	When a local AC that is a physical interface attached to an ESI (and it has multiple sub-interfaces configured, that inherit its ESI configuration) goes down, there may be a short period of downtime.	EVPN	Disable the sub-interfaces before disabling the physical interface.
SW-124251	After a revert of the RE patch, show commands failed to execute in the CLI.	High Availability	Execute a `request system ncc switchover`.
SW-117705	Pre-check on an ONIE partition might fail though there is enough space in the partition, and the upgrade will be successful.	High Availability	You may proceed with the upgrade procedure though the pre-check failed on the ONIE partition, after checking there is free space in the partition.
SW-123308	The `show system utilization limits` command displays threshold default values in the node level (not per user config).	Infra	The process-level thresholds can be seen, but they can be changed, as per design
SW-36535	The IPMI interface remains in UP state after the interface is disabled. This happens when access to the IPMI interface is disabled to mimic admin-state disable, and access cannot be regained.	Interfaces	Currently, there is no workaround.

Issue ID	Description	Component	Solution
SW-125235	ISIS crashes if it has more than four NLPIDs/supported protocols. It supports and is expected to have a maximum of two NLPIDs/supported protocols - ipv4 and ipv6).	ISIS	Currently, there is no workaround.
SW-122339	Performance issues are experienced when shortcuts are enabled on all the policies.	ISIS	Disable the shortcuts if they are not in use.
SW-110756	Uloop protection, which protects against loop risk, might not work when working with links that have partially configured address families. For example, both sides of the same link are configured with ipv4, but only one side is configured with ipv6.	ISIS	To prevent this issue, a link must be configured with both address families or only one address family on both sides.
SW-40860	When changing the number of maximum paths under ISIS, abnormal traffic loss is seen for about 1 second.	ISIS	Currently, there is no workaround.
SW-40847	There is no option to remove summary-only from the ISIS aggregate-route command.	ISIS	Remove the entire aggregate route and reconfigure it without the summary-only keyword.
SW-86711	MBB is not triggered when an old upstream is no longer one of the valid upstreams.	LDP	When an old upstream is invalid, there is no way to know if the path to root via the old upstream is still physically valid. Therefore, to avoid long traffic loss, a new path is installed immediately.
SW-45541	With a segment-routing-only router, if LDP is preferred, LDP doesn't have a Primary NH to the	LDP	Currently, there is no workaround.

Issue ID	Description	Component	Solution
	LER (SR-only router). Therefore, LDP incorrectly installs an alternate-only route towards LSR (SR/LDP router), resulting in a permanent loop between two LSRs.		
SW-125830	When disconnecting an NCC from the NCM, a few processes crash at various points. TS crashes when checking NCM IDs from ORM, mgmt_interface_manager crashes at the HA lib, and syslog_relay crashes at the transaction manager lib.	Management	HA handles the scenario by restarting the processes. No follow-up action is required.
SW-114118	In the following situation where there are two TACACS servers - server A only with authorization, and server B with authorization and authentication. If server A has a higher priority than server B, we will see in `show system aaa-servers tacacs` that authorization is active on server B even though it was done by server A.	Management	There is no workaround for this, it is only a show issue. The authorization/authentication will be done in the order of priority and the function each server has.
SW-90960	`show mpls route p2mp` displays ‘stale’ routes after a zebra restart.	Management	Start a new CLI session.
SW-78728	Invoking the following sequence of commands will lead to a commit failure: 1. delete interface 'x' 2. commit	Management	For similar scenarios as above, the proposed workaround is to perform the commit immediately after the 'rollback' command.

Issue ID	Description	Component	Solution
	3. 'rollback 1' (re-creates interface 'x') 4. delete interface 'x' 5. commit <<<<< Failure here		
SW-90599	Very small traffic loss of up to 10ms can be experienced when updating/replacing mpls multicast (p2mp) route replication. This will happen only in the case of a link addition to ECMP between 2 adjacent routers. The issue is that one replication is deleted and one is added, and while we remove the deleted replication immediately, we can't add the new one until it is verified that the tunnel encapsulation (egress label) is installed in the cluster. Therefore, there is a time gap in which there is no replication and packets may drop.	MPLS	Currently, there is no workaround.
SW-89139	Multipath information STLV is encoded before the label stack STLV in the DDM TLV. This leads to an interop issue with Juniper, e.g., this order causes Juniper to drop reply messages.	MPLS	Currently, there is no workaround.
SW-82225	There is an interop issue with CISCO, it fails to traceroute MPLS BGP-LU over SR, RCA.	MPLS	Currently, there is no workaround.
SW-82174	An interop issue with Juniper causes ping MPLS generic to fail.	MPLS	Currently, there is no workaround.

Issue ID	Description	Component	Solution
SW-81808	There is an interop issue with Juniper. DN sends multipath STLV before the label-stack STLV in the DDM TLV and Juniper expects the label-stack to come before multipath, thus dropping the packet.	MPLS	Currently, there is no workaround.
SW-120216	MPLS Ping/trace to BGP-LU prefixes resolved by SR-TE policies do not work.	MPLS OAM	Currently, there is no workaround.
SW-116373	The MPLS OAM IPv6 traceroute generic/isis multipath fails when transit has parallel links with sub interfaces.	MPLS OAM	Currently, there is no workaround.
SW-115886	MPLS ping does not work for the 6PE route (IPv6 BGP-LU route over IPv4 LSPs).	MPLS OAM	Currently, there is no workaround.
SW-114137	The `MPLS OAM IPv6 traceroute` command may return with a timeout failure on one or more hops.	MPLS OAM	Run the `MPLS OAM IPv6 traceroute` command a second time.
SW-46394	Multicast groups may not clear immediately after admin-disable loopback interface on RP.	Multicast	Clear the PIM tree with the command clear pim tree to remove the Multicast groups immediately or wait for the next join timeout.
SW-112305	The NCS enters safe mode when NAT instances are configured to use Mellanox cards plugged to PCI slots assigned to NUMA 1.	NC-Plus	Connect Mellanox cards to PCI slots assigned to NUMA 0.
SW-122298	The configuration path in NETCONF for VRRP globals	NETCONF	Apply the NETCONF configuration for class-of-service and startup-

Issue ID	Description	Component	Solution
	(namely class-of-service and startup-delay) is under /drivenets-top/network-services/vrfs/vrf[vrf-name='default']/protocols/vrrp, and not under the /drivenets-top/protocols/vrrp path. Changing the configuration in the /drivenets-top/protocols/vrrp path has no effect and does not appear in the CLI.		delay using the /drivenets-top/network-services/vrfs/vrf[vrf-name='default']/protocols/vrrp path.
SW-113167	Applying configuration while using the NETCONF Get operation might cause the operation to fail.	NETCONF	If the NETCONF Get operation fails, retry it.
SW-123273	System events sent in the startup, before the syslog daemon connects to a remote syslog server, are not sent to the remote syslog server. This includes Cold restart events.	None	All the events can be seen locally, in the system events log.
SW-112410	Changing the router ID while running OSPF on a high scale may generate the Type 10 Router Information LSA with max-age.	None	Clear the OSPF process.
SW-107260	Uloop protection, which protects against loop risk, might calculate a strict-spf solution in a node that does not support strict-spf.	None	It is recommended to set all nodes in the topology to support the strict-spf algorithm.
SW-104888	In case of a misconfiguration with two static routes using each other as a solution, one of them having an additional ECMP Next-Hop with a valid solution, the RIB-Manager will keep endlessly	None	Fix the static route configuration so they don't point to each other.

Issue ID	Description	Component	Solution
	updating these routes and installing them.		
SW-101775	The login prompt differs based on how you try to connect, console, ssh-tacacs, ssh-local-users, ssh-radius.	None	Currently, there is no workaround.
SW-126051	OSPF timers refresh configures the refresh interval on values rounded by 10, the impact on the OSPF functionality is negligible.	OSPF	You may see that in the output of `show ospf` the value of the refresh timer is rounded down to the closest multiple of 10. Other than that, it may experience an LSA refresh a few seconds earlier.
SW-125787	Alternate routes can still be installed after disabling TI-LFA if it is disabled immediately after an SPF run.	OSPF	Currently, there is no workaround.
SW-125491	RFC incompliant DNOS is installing default route even if P bit is not set, this can cause a loop in the network.	OSPF	Currently, there is no workaround.
SW-118336	Strict-spf policies might use spf labels if there are routers in the topology that don't support strict-spf.	OSPF	Currently, there is no workaround.
SW-108828	In an interface with an ingress QoS policy attached to it if the user changes the L2 service mode of the interface. The ingress QoS policy will no longer work on the interface.	QOS	Detach the ingress QoS policy and reattach it (2 commits).
SW-113576	If there are two default routes in the RIB, one static/BGP, another	RIB	If one of the default routes is static, then a static route with the

Issue ID	Description	Component	Solution
	IGP/BGP, and PIM routes are also used, the solution of the default static/BGP route becomes unavailable. This causes the RIB-Manager's memory usage to increase continuously until the solution of the static route is available again, or one of the default routes is removed.		IP Next-Hop and interface should be used.
SW-122384	If an Anycast prefix is advertised by two routers that share a common Next-Hop, the Flex Algo routes of the Anycast prefix may have a duplicate Next-Hop. This causes the balance of the ECMP group to change (which is an unharmful side effect).	Segment Routing	Currently, there is no workaround.
SW-121212	When there aren't enough labels in the SRLB for a dynamic binding-sid. The policies get stuck in the initializing state, and ISIS may not trigger out-of-labels system events.	Segment Routing	Be aware of the label ranges and scale when working with auto-policies.
SW-117280	In two connected ASBRs between the SR and LDP domain, the best path to prefix C is from ASBR A -> ASBR B -> C. But, if the best path is changed to ASBR A -> C because of a metric change or link-up event. A five-second data loss may occur on traffic that bypasses ASBR A to reach prefix C.	Segment Routing	Currently, there is no workaround.
SW-110446	When moving between an IS-IS Multi-Topology to an IS-IS Single-Topology, the IPv6 Flex-Algo	Segment Routing	Currently, there is no workaround.

Issue ID	Description	Component	Solution
	routes installed in the TWAMP-based table <color-mpls-nh-ipv6> go into inactive mode and are not cleared. IPv6 Flex-Algo routes should not be installed inside the table <color-mpls-nh-ipv6> because they are not supported.		
SW-125769	If no SNMP community is configured, the iptables rules block all SNMP traffic, including the one from the local host. This leads to the `run snmp walk/get/getnext` commands running over the local host. A timeout error is received in the CLI.	SNMP	Configure an SNMP community over the default VRF.
SW-98421	A static route that is resolved by an imported L3VPN BGP route stays inactive.	Static Route	Currently, there is no workaround.
SW-35926	When the user tries to log in during the first few minutes after a DNOS restart, in an AAA function, with In-band servers. DNOS AAA enters hold-down for the configured hold-down period (default 10 min).	User Management	Currently, there is no workaround.
SW-124570	When configuring a bundle with sub-bundles with an egress policy attached to the bundle and sub-bundle. After the first commit where you add a new member to the bundle and attach a new egress policy to a sub-bundle that does not have a policy attached. After the second	White box	Split the first commit to two separate commits: - add a new member. - attach the new egress policy to the sub-bundle.

Issue ID	Description	Component	Solution
	commit where you remove a member from the bundle, the commit fails.		
SW-124240	During a breakout when attaching to a non-default VRF on the same commit, the result is a breakout child interface with a wrong VRF. This does not happen on sub-interfaces.	White box	Change the VRF back.

Known Hardware Issues

Issue ID	Description	Component	Solution
SW-79143	The KBP (Knowledge-Based Processor) supports up to 8 different ranges for ACL rules. KBP uses range resources to allow the user to configure an ACL rule with a range and avoid the expansion of this rule into the hardware, which saves KBP resources. Once these ranges are used, they cannot be reused, even if the rules that used them have been deleted. When a 9th rule is configured, the rule is expanded in the KBP and may exhaust the KBP resources.	ACL	Commit failure triggered by the ACL configuration causes the relevant NCPs to restart. The restart frees all the range resources in KBP, making all 8 ranges available to use.
SW-845338	With Priority-based Flow Control (PFC) enabled, The BCM HW can't map between several Traffic Classes (TC) to different egress queue pairs. Only one of the TCs will stop the queue.	QOS	Configure one TC per egress queue (using the `egress qos policy`) Egress queue pair 0 - SEF queue Egress queue pair 1 - EF queue. Egress queue pair 2 - HP queue Egress queue pair 3 - default rule only.
SW-122776	Move events for dynamic MAC entries are not triggered when a MAC limit is reached, both for a VSI limit and a global limit.	White box	Currently, there is no solution, fix, or workaround to overcome this issue.

Limitations

Issue ID	Description	Component
SW-40319	In an IPv6 Egress ACL, if a rule includes a 'protocol' match (for example, TCP, UDP, ICMP) and the traffic pattern hits it, it is not possible to match any fragments (initial, non-initial) of the IPv6 packets.	ACL
SW-22552	Only the primary path is used when a route is resolved via a BGP route with LFA.	BGP
SW-87458	The CLI fails to point to the wrong word for routing-policy prefix list rules commands. When an invalid command is entered, the CLI always points to the first word (`rule`).	CLI
SW-72999	There is no validation for management default VRFs - mgmt0, mgmt-ncc-0/0, and mgmt-ncc-1/0. They appear under the network-services hierarchy, which configures non-default In-band VRFs. Default VRFs are partially configurable via the network-services hierarchy, too, although their configuration is done under the top hierarchy. The management VRFs appear to the user as configurable, although they are not (by design).	CLI
SW-43391	Up to 10 simultaneous CLI sessions can be supported on a Standalone NCP.	CLI
SW-20421	When configuring OOB management interfaces with a routing protocol during the commit, the following error is presented ‘ERROR: Command failed due to unexpected reason.’ There is no impact on the system.	CLI
SW-20233	During the system boot, the `show file tech-support` command might not function until the system reaches its UP state. There is no impact on the system.	CLI
SW-124006	In the L2-cross-connect feature, which allows cross-connecting traffic between two sub-interfaces, the traffic on	Datapath

Issue ID	Description	Component
	the cross-connect service uses the traffic queues of the physical port and not the sub-interface queues, if those are defined.	
SW-122171	In an EVPN/EVPN-VPWS service working in an AA mode, when connecting a physical link to a CP device, traffic loss is experienced. This happens because the CE device sends traffic immediately while the PE core side has not converged.	Datapath
SW-120856	When disconnecting a physical link from a CE device in an EVPN PE router, there might be traffic loss for a few seconds.	EVPN
SW-34870	The interface configuration parameter, mtu-ipv6, affects the IPv4 ping when running the `run ping IPv4_ADDR` command. This does not affect transit traffic.	ICMP
SW-89325	Only the default application can be used for 400G transceivers supporting multiple applications. For example, a 400G Base-DR4+ transceiver with a default native 400G application may also support breakout to 100G, according to its CMIS data. However, while the transceiver supports breakout and may appear so in DNOS, for some transceivers (e.g., INNOLIGHT 400G T-DP4CNT-N00), a breakout cannot be configured.	Interfaces
SW-13193	With ISIS on an interface configured with an MTU above 9222, ISIS adjacency cannot be established.	Interfaces
SW-121390	In certain ISIS scales and topologies where the ISIS LSP is divided into many fragments, there can be cases where the SPF calculation may be triggered before all fragments of the LSP are received. In such cases, ISIS might result in a temporary wrong path selection.	ISIS
SW-45496	The ISIS process will crash if more than 1536 ISIS circuits are configured.	ISIS

Issue ID	Description	Component
SW-23899	The Syslog server list in the show system logging command output is not updated with the configured facility type. There is no impact on the system; it is a CLI display issue.	LOG
SW-107823	Committing complex QoS and ACL 100K config lines causes memory issues.	Management
SW-35900	A static route for an OOB management network can't be configured if a specified Next-Hop interface is in DHCP mode.	Management
SW-76489	An NCM ONIE upgrade from DriveNets ONIE 2020 onwards is not supported. The reason for that is that the MU (Multi Updater) uses an old FSCK (File system check) while DriveNets ONIE uses a newer one.	NCE Management
SW-83003	DNI platforms don't have bit error counters available, and symbol error counters are post-FEC. As a result, the signal degrade and signal failure alarms relying on BER calculation have inherent inaccuracy.	None
SW-109311	The maximum throughput decreases on NCS NAT interfaces if any of the two transceivers used for the management connections to the NCMs are missing or malfunctioning.	None
SW-51282	NTP processes can reset in some scenarios.	NTP
SW-77634	Upgrading a DNI-based cluster to v16.2 requires the removal of the NCP configuration. This limitation applies to DNI clusters only and does not include Standalones. The NCP configuration in v16.2 or higher requires an explicit setting of the NCP hardware model to AGCXD40S (the default is S9700-53DX). If it is not set when the NCP reconnects, the NCP enters safe mode due to misconfiguration. It is not possible to add or edit the hardware model configuration without removing the NCP configuration first.	Platform

<table>
<tr><th>Issue ID</th><th>Description</th><th>Component</th></tr>
<tr><td>SW-76547</td><td>For low-speed subscribers, there is no differentiation between WRED and Weighted Tail Drop (WTD) thresholds.

There are continuous unexpected tail drops over the WRED max threshold.</td><td>QOS</td></tr>
<tr><td>SW-25836</td><td>Packet reorder may happen when the same stream contains multiple classes and the QoS policy is not attached.</td><td>QOS</td></tr>
<tr><td>SW-25352</td><td>Multiple egress policies can be created, yet only a single egress policy can be attached.</td><td>QOS</td></tr>
<tr><td>SW-24214</td><td>When enabling EXPLICIT NULL behavior for the LSP, the classification of incoming packets at the tunnel tail-end does not consider the policy set on the ingress port. Rather, it uses a default mapping between the MPLS EXP bits carried in the EXPLICIT NULL label and the qos-tag and drop-tag set.
MPLS packets with EXPLICIT NULL topmost label will be classified according to the fixed table below and therefore will potentially receive different per-hop-behaviors.
exp-null qos-tag drop-tag

<table><tr><th>exp-null</th><th>qos-tag</th><th>drop-tag</th></tr><tr><td>0</td><td>0</td><td>green</td></tr><tr><td>1</td><td>1</td><td>yellow</td></tr><tr><td>2</td><td>2</td><td>green</td></tr><tr><td>3</td><td>3</td><td>yellow</td></tr><tr><td>4</td><td>4</td><td>green</td></tr><tr><td>5</td><td>5</td><td>green</td></tr></table></td><td>QOS</td></tr>
</table>

<table>
<tr><th>Issue ID</th><th>Description</th><th>Component</th></tr>
<tr><td></td><td>
<table>
<tr><th>exp-null</th><th>qos-tag</th><th>drop-tag</th></tr>
<tr><td>6</td><td>6</td><td>green</td></tr>
<tr><td>7</td><td>7</td><td>green</td></tr>
</table>

This might result in traffic drops, due to traffic being queued differently than configured or egress traffic receiving a different QoS marking.
Enabling EXPLICIT NULL will always result in this behavior.
To prevent this from happening, disable EXPLICIT NULL using the configuration command <code>rsvp explicit-null</code> under the rsvp hierarchy.
To view the QoS interface counters use the show commands <code>show qos interface counters</code> or <code>show qos summary</code> to display the QoS summary table.</td><td></td></tr>
<tr><td>SW-23773</td><td>Egress match counters count the ingress (not the egress) packet bytes, including Ethernet and other terminated layers.</td><td>QOS</td></tr>
<tr><td>SW-123841</td><td>In EVPN Coloring setting a color via BGP import policy does not work properly.</td><td>Segment Routing</td></tr>
<tr><td>SW-113105</td><td>On a large cluster, due to the amount of data the SNMP responder process is managing, it is possible that running snmpwalk and snmpbulkwalk will cause a timeout with default values.</td><td>SNMP</td></tr>
<tr><td>SW-23072</td><td>CPRL classifies management protocols by preconfigured protocol ports and does not support dynamic port ranges. For example, if the TACACS port is 49 and it changes, CPRL will not classify the TACACS traffic.</td><td>User Management</td></tr>
</table>

Documentation Highlights

To view the v18.2.1 related documents:

1.Go to https://docs.drivenets.com.

2.Select Library from the top menu

3.Select the 18.2.1 version filter on the left pane

To receive third party software under a GNU GPL license, see Written Offer for Source Code.