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	18.0.0.5
CAL	DriveNets Golden Image	18.0.0.5
StrataX	DNOS NCM NOS	1.2.0
Base-OS	Base-OS	2.18001548005
FW and ONIE	Firmware and ONIE bundled packages for all cluster element types (NCC, NCM, NCF and NCP)	18.0.0.1
DNOR	DriveNets Network Orchestrator	15.1.0.1

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

Management-Infra

DNOS Alarms Management

The new alarms management feature provides a persistent and reliable communication channel, and a single source of truth, compared with system events. The alarms are triggered by pre-defined conditions and have pre-defined configurable severities. A user can configure the alarm severity and can acknowledge/close an alarm. The alarms can be fetched by any controller supporting on-change subscription via gRPC.

To enable DNOS alarms, use the `system alarms admin-state enabled` command.

To change an alarm severity, use the `system alarms inventory alarm [module] [alarm-name] severity` command.

For any other miscellaneous configuration, use the `system alarms` configuration hierarchy.

Use the `request system alarms history purge before-time` command to purge alarms history.

Use the `set alarm operator state ack alarm [alarm-operator-id]` command to acknowledge an alarm.

Use the `set alarm operator state closed alarm [alarm-operator-id]` command to close an alarm.

For displaying various system alarms information, use the `show system alarms` show command hierarchy.

Datapath

Additional SNMP Parameters for NCP and NCF

To provide further hardware environment information, via SNMP, to customers that still use SNMP instead of gRPC telemetry, the following parameters can now be polled via SNMP for all NCP and NCF models:

Fan statistics

Power statistics

PSU input voltage

Temperature sensors reading.

	**If a device is absent from the platform, for example, a fan or power supply unit is missing, the parameters of these missing units are either shown as an 'absent' status or '-1'.**

NCP-36CD-S 10Gb Breakout Interfaces

10Gb interface breakouts that were previously only supported on NCP-40C, are now supported on NCP-36CD-S too. 10Gb breakout interfaces are based on QSFP+ (40Gb) transceivers that support a physical breakout of 40Gb to 4x10Gb Network Interfaces (NIFs).

To configure 10Gb breakout NIFs, use the `interfaces ge400-x/y/z breakout 10g-4x` configuration command.

Integrated Routing and Bridging Interfaces

Integrated Routing and Bridging (IRB) interfaces have been introduced in DNOS. IRB interfaces allow for inter-subnet routing, connecting between an L2 bridge domain and a VRF (global VRF or non-global). Routing protocols (BGP, ISIS, OSPF), first-hop gateway redundancy protocols (VRRP) and relay protocols, such as DHCP relay, can run on IRB interfaces.

To configure an IRB interface, use the `interfaces irb` command.

To associate the IRB interface with a bridge-domain, use the `network-services bridge-domain instance <name> router-interface` command.

To associate the IRB interface with a non-default VRF (L3VPN), use the `network-services vrf instance <name> interface irb` command.

To display information of an IRB interface, use the `show interfaces irb` show command.

SNMP

Cisco Compatible SNMP IP-MIB Format

DNOS only supported an ASCII representation of the IP address, while the Cisco controller expected a Decimal representation. This was causing an Interop issue while the Cisco controller tried to discover the DNOS logical inventory. DriveNets now supports an optional IP-MIB format for interoperability with Cisco controllers preventing the issue.

To use the Decimal representation of IP-MIB, use the `system snmp compatibility-mode cisco` command.

Management

Flattened Show Config Command

In DNOS, the CLI show config command was presented in a hierarchical fashion; commands were displayed with a proper indention under the appropriate configuration container. This created a challenge for users that wanted to copy-paste a section or sections of the configuration from a saved file. To overcome this issue, DriveNets has implemented a `display-set` to present a flat configuration without the hierarchy.

The user can now retrieve the current configuration from DNOS in a flattened format, either for all set configurations or for a specific hierarchy requested by the user (e.g., just for the interfaces

hierarchy). In both cases, the configuration output in flattened format is presented to the user in full lines/paths relative to the top hierarchy.

To view a flattened output of the user configuration, use the `show config | flatten` command. Any line entered from the flattened output will keep the CLI prompt at the top hierarchy. In addition, DNOS now supports using multiple pipes, e.g., `show config interfaces | flatten | include interfaces`.

ISIS-SR Flex-Algo

The Flex-Algo mechanism has been added to the ISIS-SR feature. Flex-Algo allows for IGP constraint-based computations and creates separate IGP algorithms according to the defined set of constraints and metric types. It complements the SR-TE solution by adding new prefix segments with specific optimization objectives and constraints and allows calculating constrained-based network paths with no need to construct SR-TE policies.

Some of the advantages of Flex-Algo include the ability to provide TI-LFA per Algo, taking into consideration the Flex-Algo definition, the ability to natively provide ECMP within the Flex-Algo topology, and the ability to minimize the Segment-Routing label stack, in oppose to a native SR-TE policy solution, which may need to leverage multiple labels, to satisfy the required constraints of the policy.

Supported capabilities:

Supported on ISIS IPv4-Unicast only

Flex-Algo participation

Flex-Algo definition advertisement

Support the following constraints:

Include any/all admin-groups

Exclude any/all admin-groups

Exclude SRLG

Support of the following Metric types:

Minimum IGP metric

Minimum TE metric

Minimum Delay metric

Supports TI-LFA and Micro-loop avoidance on per Algtopology basis

Supports an optional configuration of association of the color value to the local Algo value. Once configured, Flex-Algo routes will be installed in the associated `Color-MPLS-NH` table (Colored label RIB). This allows for BGP automated steering of the colored BGP routes to Flex-Algo resolution. BGP automated steering is a Beta feature in this release. If color is not associated with

a Flex-Algo upon configuration, Flex-Algo routes will be installed only to the ILM table (Label FIB) for label-switching purposes only

No-fallback flag - if color and no-fallback are set in the Flex-Algo configuration, a default route to null0 will be installed in the Color-MPLS-NH (Colored label RIB), which will enforce that if a colored BGP route does not have a Flex-Algo resolution in the matching color-mpls-nh table, traffic will not fallback to Algo 0 (MPLS-NH - Label RIB). Instead, traffic will be blackholed

To create a Flex-Algo definition profile with the desired constraints and metric type, use the `protocols segment-routing mpls flex-algo advertise-definition` configuration hierarchy.

To advertise the Flex-Algo definition, use the `advertise` flag under the `protocols isis instance flex-algo` configuration hierarchy.

For solely participating in a Flex-Algo, but not advertising a definition, use the `protocols isis instance flex-algo` configuration hierarchy without the optional `advertise` flag.

For associating a color value to a Flex-Algo, use the `color` configuration command under the abovementioned `protocols isis instance flex-algo` configuration hierarchy. `Color` is an optional configuration if BGP automated steering is desired.

Routing

LDP-tunneling over OSPF SR-TE Policy

The new feature, LDP tunneling over OSPF SR-TE, allows you to connect non-SR-capable routers running LDP with SR-capable routers running LDP. This feature can be used to forward traffic between different LDP domains, for example, by connecting the LDP routers in one domain to an SR-capable router or network that connects to another LDP domain.

To configure LDP-tunneling over SR-TE, use the `mpls policy ldp-tunneling` command under the `protocols segment-routing` hierarchy.

VPWS Steer-path Policy

VPWS steer-path policy enables the stitching of a Pseudo Wire (PW) of an L2VPN-VPWS service over a specific RSVP-TE tunnel or SR-TE policy.

DNOS, previously, only supported stitching an SR-TE policy to a PW, by using the `network-services vpws instance [instance] pw [address] sr-te policy [policy]` command. This command has now changed to `network-services vpws instance [instance] pw [address] steer-path` to support both RSVP-TE and SR-TE.

Use the `network-services vpws instance [instance] pw [address] steer-path rsvp-te [tunnel-name]` command to stitch a PW to a specific RSVP-TE tunnel. Use the `network-services vpws instance [instance] pw [address] steer-path sr-te policy [policy-name]` command to stitch a PW to a specific SR-TE policy.

ISIS Dynamic Link Delay Measurement and Advertisement

It is possible now to advertise link delay parameters in ISIS. Dynamic link delay is calculated by Simple-TWAMP (STAMP) link delay sessions. Link delay parameters are advertised under TLV 22. The supported parameters are Min/Max unidirectional link delay, average link delay, and unidirectional delay variation - Sub-TLVs 34, 33, and 35, respectively. ISIS delay normalization, which is also now supported, allows the normalization of the computed link delay value and relaxes the negligible differences between collected delay values on various links. That way, the normalized values would be advertised in ISIS, and the ISIS routers can leverage ECMP better in the network.

To measure and advertise link delay parameters in ISIS, use the `services performance-monitoring interfaces interface` configuration hierarchy, and associate the measuring interface to ISIS, under the `protocols isis instance interface` configuration hierarchy.

Use the `show services performance-monitoring link-delay interfaces` show command to see the measured link delay values.

To enable ISIS delay normalization, use the `protocols isis instance interface delay-normalization` configuration command.

Community-list match-all

Currently, in DNOS, when evaluating a route in a community list, it needs only to conform to one entry in the community list for it to match that community list. Now, the `match all` option is also available, meaning a route needs to conform to all communities specified in the community list to match that community list.

To use `match all` the user needs to use this configuration:

`routing-policy policy <policy-name> rule <id> <allow/deny> <match/*match-all*> <community/extcommunity/large-community> <community-name>`.

BGP Remote-AS Hierarchy

DNOS supports the configuration of remote-AS per neighbor level, even if this neighbor is associated with a neighbor-group with a different remote-AS configuration. Previously, all neighbors configured under a BGP neighbor-group were bound to the remote-AS configuration of that neighbor-group. This allowed the flexibility of having multiple neighbors with the same inherited neighbor-group configuration but with different remote-AS. The explicit configuration of

remote-AS on the neighbor overrides the remote-AS configured on the neighbor-group for that neighbor.

Cluster Manager

NCP- 64X12C-S and NCP-40C/NCP-10CD Hybrid Clusters

DriveNets has certified two new hybrid cluster types, CL-49, and CL-86. They provide a mix of multiple NCPs with different ASICs (J2 and J2c in this case) and allow for native 1Gb-400Gb interfaces in a hybrid cluster with no breakout cables.

The CL-49 is comprised of up to two NCCs, up to two NCMs, up to three NCFs (NCF-48CD), and up to 14 NCPs (four NCP-64X12C-S and ten NCP-40C /NCP-10CD). A CL-86 is comprised of up to two NCCs, up to two NCMs, up to six NCFs (NCF-48CD), and up to 24 NCPs (six NCP-64X12C-S and 18 NCP-40C /NCP-10CD).

TWAMP

IPv4 Simple-TWAMP (STAMP) Link Delay Measurement

Simple-TWAMP (STAMP) Link delay sessions are now supported; up till now, DriveNets only supported STAMP Endpoint delay sessions.

STAMP link-delay sessions are often used to dynamically measure the link's delay parameters, such as Min/Max unidirectional link delay, average link delay, and unidirectional delay. This information can be advertised in IGP protocols, such as ISIS. DNOS router can fully interoperate with 3rd party routers measuring link delay via TWAMP-Light.

STAMP (enhanced TWAMP-Light) and TWAMP-Light are interoperable and can be used interchangeably when:

Both work in an unauthenticated mode

STAMP works in Stateless mode (TWAMP-Light is also stateless by design)

To configure the Simple-TWAMP link-delay profile characteristics, use the `services performance-monitoring profiles link-delay` command for configuring characteristics such as probe-interval, computation-interval, advertisement thresholds, DSCP-value, etc.

To enable link delay measurement, and associate a link-delay profile, use the `services performance-monitoring interfaces interface` configuration hierarchy.

To configure the device's Simple-TWAMP protocol characteristics, such as session-sender destination port on all Simple-TWAMP sessions, and local reflector port, use the `services simple-twamp session-sender` and `services simple-twamp session-reflector` respectively.

To display information about Simple-TWAMP Link-delay sessions, use `show services performance-monitoring link-delay interfaces` show command.

WhiteBox

IPv4 DHCP Relay

IPv4 DHCP relay connects a DHCP client and a DHCP server that is not on the same physical network by relaying the DHCP messages between the two. The now configurable DHCP option 82, also known as the DHCP Relay Agent Information option, is a set of fields that can be added to DHCP messages. This provides additional information about the DHCP relay agent that forwarded the message. The DHCP option 82 allows the DHCP server to identify the client's location or a set of specific characteristics and assign an appropriate IP address or network configuration. It is also used for security, for example, to prevent DHCP spoofing attacks.

To configure a DHCP relay-agent, use the `interfaces [interface] dhcp relay-agent` configuration hierarchy.

To configure the DHCP relay-agent's option-82, use the `interfaces [interface] dhcp relay-agent option-82` configuration hierarchy.

Use the `show interfaces dhcp relay statistics` command to display DHCP relay-agent-related statistics.

Bundle Interface Shaper

The egress hierarchical shaper attachment function has now been added to bundle interfaces as well as physical and sub-interfaces. The shaper limits the amount of traffic passing on an interface, preventing the loss of traffic due to congestion. When the traffic rate rises above a predefined value, the shaper buffers the excess packets until the rate/second drops below the predefined value. At that point, the buffered packet is sent to the interface. The shaper allows shaping the main physical interface/bundle or logical interface for the whole subnet and then attaches a second level of policy with Class-based Weighted Fair Queueing (CBWFQ).

To configure a hierarchical shaper attachment, first, configure a parent policy with a shape action and specified child policy under the action and then include the `QoS policy [parent-policy-name] out` statement under the `interfaces [interface]` CLI hierarchy.

Egress QoS and Interface Shapers for Bundles Sub-interfaces

Interface shapers and egress QoS configuration on a sub-interface of a bundle were not supported on DNOS. They were only supported on sub-interfaces of a physical interface. Bundles only supported non-hierarchical egress QoS, and all sub-interfaces of that bundle were bound to the QoS scheme configured on the physical bundle interface. As of DNOS v18.0, sub-interfaces of bundles can hold their own QoS policies and use their own QoS schemes and shapers.

Syslog

Increase in Syslog Servers

There has been an increase in the number of syslog servers DNOS supports, from eight servers to ten:

They are provisioned over OOB or In-band

CPRL wise, the rate of the syslog messages remains 1K/s of messages as before (this is the rate before multiplication to x servers)

CPRL burst of 50K

CAL

Beacon Reporting Recovery Mode

In previous DNOS versions, both NCCs in a system in recovery mode, running in CAL mode, would beacon that the system is in recovery mode. From DNOS v18.0, both NCCs in a system in recovery mode, running in DNOS mode, will also beacon that the system is in recovery mode.

Please pay extra attention, in a system in recovery mode running in DNOS mode, that both NCCs beacon. This is unlike a stable system, in which only the active NCC beacons the information of both NCCs.

gNMI

Disabling TLS 1.0 and 1.1

DNOS supported the connectivity of legacy clients with older TLS versions, such as 1.0 and 1.1. Now all TLS versions below 1.2 are disabled and only TLS versions 1.2 and 1.3 are supported. This is hardcoded and not configurable. This is done to lower vulnerabilities and affects TLS-enabled gRPC clients connecting to DNOS who must now support either TLS 1.2 or TLS 1.3 for TLS-based connections.

Resolved Issues

Issue ID	Description	Component
SW-90119	ISIS instance configuration is not properly removed from the router upon loading the factory default config. It is only removed from the CLI, but it is still active in the backend.	CLI
SW-85851	When configuring a routing-policy with the rule 0, the commit is executed and the rule 0 is ignored by the system.	CLI
SW-85636	Autocomplete is not supported for `routing-policy prefix list rule`. Pressing TAB in the RULEs command displays a helpline.	CLI
SW-98906	When an NCP is activated in a Bridge-Domain service some bundle MAC addresses may be missing from the show table in the NCP. There is no effect on the running MAC table.	Datapath
SW-94694	The packet is sent with a bad UDP checksum, when working with `stamp performance monitoring` or `stamp reflector` on an NCP-40C / NCP-36CD-S acting as a reflector, with a padding size smaller than 70 bytes.	Datapath

Issue ID	Description	Component
SW-99677	Due to an internal software bug, the CMC crashes when trying to upgrade the system from v17.2 to v18.0. This happens when there are more than 64 packages loaded into the system.	DNOS Deployment, Upgrade, Revert
SW-98559	Due to a software limitation, changing the vLAN attributes on a sub-interface with VRRP configured on it causes the VRRP to break.	Interfaces
SW-98202	When tracking a physical interface that is part of a bundle, the physical interface is considered down.	Interfaces
SW-96318	When moving a sub interface into a different VRF, the LL address is deleted from the sub interface. This happens between the commit stages 3 and 4. While existing in stage 3 the relevant state update is not performed on the oper-list by the oper-state. This leads to the loss of the oper-up and as a result the deletion of the LL address from the sub interface.	Interfaces
SW-93336	The FEC Bit Error Counters and the BER features don't work for 100G breakout interfaces.	Interfaces
SW-99532	Performance-monitoring profiles are not always properly removed from the system when removed via the CLI. As a result, the system might warn the user that the maximum number of profiles has been reached even though they do not appear in `show-config`.	Management
SW-92884	In some cases where both BGP-LFA, and ISIS-LFA are available, the MoFRR standby IIF could select an interface that is only link disjoint. This while node disjoint is available or is the same as the primary.	Multicast
SW-99002	When using NETCONF, the VPWS PW pw-id is not correctly obtained from oper-items of config entries.	NETCONF
SW-99000	The VPWS instance description is not correctly obtained from oper-items of config entries when using NETCONF.	NETCONF

Issue ID	Description	Component
SW-98871	Deleting rules from the prefix-list via NETCONF fails, both for ipv4 and ipv6. The RPC returns 'OK', but the rule specified for deletion remains in the configuration.	NETCONF
SW-95086	Configuring interconnected boxes in a way that creates a SyncE source loop between them, may result in an unexpected source being selected and ESMC packets being transmitted with QL_DNU.	None
SW-90723	The `set auto-bandwidth sample` sometimes does not set the sample bandwidth.	RSVP
SW-88308	QPPB doesn't take precedence over FIB with no destination. A BGP route with a drop destination, e.g. null0 (which is the case of an aggregate-route), dropping the match traffic has a higher preference over handling it by QPPB. As a result, traffic that is matched on the BGP aggregate-route will not comply with the behavior required by QPPB, even if the route has QPPB source/dest-class (imposed by the BGP policy by matching route attributes), and traffic will be dropped. In such a case, an alert will be generated that the egress ACL is reduced and must be confirmed prior to upgrade: A large TCAM is required for QPPB to operate. The supported scale of IPv4 Egress ACL needs to be reduced because one large TCAM is redacted from it, resulting in a reduced scale by 2000 ipv4 rules per NCP. Egress IPv4 ACL updated scale: 10240 rules per NCP. Note that for NCP-36CD-S, it is still per NCP and not per J2C+. It is required to update the CLI & Commit validation to enforce the new rule scale limitation.	White Box

Limitations

Issue ID	Description	Component	Solution
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	Currently, there is no solution, fix, or workaround to overcome this issue.
SW-22552	Only the primary path is used when a route is resolved via a BGP route with LFA.	BGP	Currently, there is no solution, fix, or WA to overcome this issue.
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	Currently, there is no solution, fix or workaround to overcome this issue.
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 is used for configuring 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	There is no workaround. The default VRF configuration is not done via the network-services hierarchy but via the top hierarchy. The management VRFs are not configurable, and the user should not attempt to configure them.
SW-43391	Up to 10 simultaneous CLI sessions can be supported on a Standalone NCP.	CLI	Currently, there is no solution, fix, or workaround to overcome this issue.

Issue ID	Description	Component	Solution
SW-20421	When trying to configure 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	Remove the management interface configuration from the routing protocol hierarchy.
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	Apply the `show file tech-support` command when the system reaches its UP state.
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	Currently, there is no solution, fix, or workaround to overcome this issue.
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	Currently, there is no solution, fix, or workaround to overcome this issue.
SW-13193	With ISIS on an interface configured with an MTU above 9222, ISIS adjacency cannot be established.	Interfaces	Decrease the interface MTU below 9222.

Issue ID	Description	Component	Solution
SW-45496	The ISIS process will crash if more than 1536 ISIS circuits are configured.	ISIS	Currently, there is no solution, fix, or workaround to overcome this issue.
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	Currently, there is no solution, fix, or WA to overcome this issue.
SW-85530	Connection to a remote server using the 'run ssh' command will generate an SSH_SESSION_LOGIN_FAILED system event with the user 'bublik' on the remote server. This is a mock user used to fetch the ssh banner and print to the screen before using the actual ssh credentials provided.	Management	Currently, there is no solution, fix, or workaround to overcome this issue.
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	Currently, there is no solution, fix, or workaround to overcome this issue.
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	Upgrade to the new ONIE, DN ONIE 2019.06.
SW-42116	System switchover is logged as System failover.	NCE Management	Currently, there is no solution, fix, or workaround to overcome this issue.
SW-83003	DNI platforms don't have bit error counters available, and symbol error counters are post-FEC. As a result, the	None	Currently, there is no solution, fix, or workaround to overcome this issue.

Issue ID	Description	Component	Solution
	signal degrade and signal failure alarms relying on BER calculation have inherent inaccuracy.		
SW-51282	NTP processes can reset in some scenarios.	NTP	NTP restarts do not affect the system. Timing is unaffected.
SW-77634	Upgrading a DNI-based cluster to v16.2 requires the removal of the NCP configuration. This limitation is applicable 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	Remove the NCP configuration prior to the upgrade by using the no ncp command. Any other configuration referencing NCP interfaces must be removed as well, e.g., protocols interface configuration. You can now complete the upgrade and then reconfigure all the NCPs with the correct AGCXD40S hardware model, by using the command 'system ncp 0 model NCP-40C hw-model AGCXD40S admin-state enabled' and re-adding the removed NCP configuration.
SW-76547	RN1: For low-speed subscribers, there is no differentiation between WRED and Weighted Tail Drop (WTD) thresholds. RN2: There are continuous unexpected tail drops over the WRED max threshold.	QOS	RN1: The minimum queue or threshold size set in the hardware is 125kB. For low-rate subscribers, two different thresholds values configured in temporal units (milliseconds or microseconds) may both be converted to the same minimum value. To keep the differentiation for low-speed subscribers, use the hardware-mapping speed configuration, setting the minimum speed of

Issue ID	Description	Component	Solution
			all traffic below 1gpbs to a speed of 1gpbs. This is the default configuration. RN2: To avoid or minimize continuous tail drops, increase the difference between the max WRED threshold and the queue size. For low-rate queues, use the hardware mapping speed conversion table to avoid setting both to the minimum 125kB queue and threshold sizes. Have at least a 250KB difference between the queue size and the max WRED threshold.
SW-25836	Packet reorder may happen when the same stream contains multiple classes and the QoS policy is not attached.	QOS	Currently, there is no solution, fix, or workaround to overcome this issue.
SW-25352	Multiple egress policies can be created, yet only a single egress policy can be attached.	QOS	Currently, there is no solution, fix, or workaround to overcome this issue.
SW-24214	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	QOS	Currently, there is no solution, fix, or workaround to overcome this issue.

<table>
<tr><th>Issue ID</th><th>Description</th><th>Component</th><th>Solution</th></tr>
<tr><td></td><td>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>
<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><td></td></tr>
</table>

Issue ID	Description	Component	Solution
SW-23773	Egress match counters count the ingress (not the egress) packet bytes, including Ethernet and other terminated layers.	QOS	Currently, there is no solution, fix, or WA to overcome this issue.
SW-23072	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.	User Management	Currently, there is no solution, fix, or WA to overcome this issue.

Known Issues

Issue ID	Description	Component	Solution
SW-103870	When LACP goes into down state on an interface, an alarm will not be triggered and will not populate the `active alarms list`. Only a system event will be generated.	Alarms	Currently, there is no workaround.
SW-106267	When OSPFv2 is configured with `max-metric router-lsa on-startup` and the user removes the entire OSPF configuration and performs a rollback, max-metric will not be sent at startup, although it is enabled in the CLI. When `max-metric router-lsa on-startup` function is enabled, and the user removes the entire OSPF configuration, then re-apply the configuration manually (not via rollback), the `max-metric router-lsa on-startup` function	OSPF	Remove the entire OSPF configuration again and commit. Then do rollback 1 and commit. After this, manually add the 'max-metric knob' and commit.

Issue ID	Description	Component	Solution
	becomes active immediately, even if you did not restart the device.		When this happens, remove the 'max-metric knob' and add it manually or via rollback.
SW-103869	When BFD goes into down state, an alarm will not be triggered and will not populate the `active alarms list`. Only a system event will be generated.	Alarms	Currently, there is no workaround.
SW-103866	When an SR policy goes into down state, an alarm will not be triggered and will not populate the `active alarms list`. Only a system event will be generated.	Alarms	Currently, there is no workaround.
SW-103172	ISIS maximum routes limit and threshold alarms will not be triggered and will not populate the `active alarms list`. Only a system event would be generated.	Alarms	Currently, there is no workaround.
SW-102541	The RADIUS_SERVER_STATE_CHANGE_NOT_AVAILABLE alarm will not be triggered when connectivity to the Radius server is lost. Only a system event will be generated.	Alarms	Will be fixed in 18.2
SW-106468	Some memory may not be freed if a BGP peer session was restarted due to the maximum prefix condition	BGP	N/A
SW-100903	Traffic over IPv6 routes with IPv4 nexthops is not supported.	BGP	Currently, there is no workaround.
SW-101514	After the BaseOS upgrade, the hostname returns to the default name, vRouter. This makes it	CLI	To change the default name,

Issue ID	Description	Component	Solution
	unreachable by name, as the system only recognizes the newly configured hostname.		use the 'system name' configuration command after the BaseOS upgrade.
SW-48206	When an NTP server is unreachable, disabling the management interface (lo0) might cause the `show system NTP` command to return an error. NTP functionality is not affected.	CLI	Currently, there is no workaround.
SW-21067	Running the command `show interface ctrl-ncm-x` displays an 'uptime' value of 0. There is no impact to the system. It is a CLI display issue.	CLI	You can view the interface uptime value via the StrataX operation system, using the `run start shell ncm X` command.
SW-89997	The default value of a double-tagged sub-interface is 0x88a8 for the outer tag and 0x8100 for the inner tag. Therefore, the default TPID value has been removed and is now written by the datapath behind the scenes. Making it seem like the TPID is configured manually.	Datapath	Currently, there is no workaround.
SW-106817	Revert operation pre-check test falsely fails when pre-checking SW revert from version 18 to version 17.2. The revert operation is still successful, although the pre-check test fails.	DNOS Deployment, Upgrade, Revert	Currently, there is no workaround.
SW-22899	Failure of the standby NCC might cause the active ssh session to be inaccessible for about two minutes.	High Availability	Currently, there is no workaround.

Issue ID	Description	Component	Solution
SW-98773	Received ARP message in the bridge-domain with a dst-mac of the IRB is flooded to the bridge-domain's attachment circuits (as well as being punted to the CPU as needed).	Interfaces	Currently, there is no workaround.
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	If the management interface is disabled, the uptime of the interface can be ignored.
SW-36535	The IPMI interface remains in the 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.
SW-100375	The actual limitation is per physical when configuring an interface shaper for a bundle. If the limitation is below 2.6G, it will limit it to 2.6G (min shaper for physical).	Interfaces	Currently, there is no workaround.
SW-104759	Mellanox cards from HP with interfaces configured to work in InfiniBand mode (default mode) are not supported	Interfaces	Manually configure the interface to Ethernet.
SW-106244	A router may not be considered SR / Flex-Algo capable if router capabilities are advertised from a non-0 lsp fragment.	ISIS	Make sure all fragments are scanned for the router capability tlv when providing information to the relevant topology.

Issue ID	Description	Component	Solution
SW-40860	When changing the number of maximum paths under ISIS, abnormal traffic loss is seen for a duration of 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 not valid, 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 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.	LDP	Currently, there is no workaround.
SW-42531	Configuring a Syslog server with a hostname and not an IP may cause syslog messages not to be sent to the server.	LOG	Configure Syslog server with IP address
SW-39013	At scale, when there is a fast log rotation, there may be a mismatch between the log .gz file timestamp and the log timestamps within the file.	LOG	Currently, there is no workaround.

Issue ID	Description	Component	Solution
SW-100397	An FTP_SESSION_LIMIT_CLEARED event is wrongly sent when reaching the maximum number of sessions allowed.	Managementt	Currently, there is no workaround.
SW-90960	`show mpls route p2mp` displays `stale` routes after a zebra restart.	Managementt	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 3. 'rollback 1' (re-creates interface 'x') 4. delete interface 'x' 5. commit <<<<< Failure here	Managementt	For similar scenarios as above, the proposed workaround is to perform the commit immediately after the 'rollback' command.
SW-44069	Configured data-connection-timeout value is not strict. The configured value is the minimum amount of time the connection is allowed before being disconnected. The maximum amount of time will not exceed twice the configured value for the data-connection-timeout.	Managementt	Currently, there is no workaround.
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.	MPLS	Currently, there is no workaround.

Issue ID	Description	Component	Solution
	Therefore, there is a time gap in which there is no replication, and packets may drop.		
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, and 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.
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-96242	The Make Before Break process is aborted if a former primary IIF is chosen as a standby IIF, causing traffic loss of up to 40 seconds.	Multicast	Currently, there is no workaround.
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-105030	Some traffic loss may be experienced during the system restart of a router acting as VRRP backup. The issue is mostly related to the high scale of interfaces.	None	Currently, there is no workaround.

Issue ID	Description	Component	Solution
SW-101775	The login prompt is different based on how you try to connect, console, ssh-tacacs, ssh-local-users, ssh-radius.	None	Currently, there is no workaround.
SW-105104	Configuring a new md5 key and removing an existing key in the same commit results in removing only the existing key	OSPF	1. Remove the md5 key and commit. 2. Add the new key and commit.
SW-79291	During a DNOS upgrade, the cluster fabric-type configuration is reset to its default values. This might lead to traffic forwarding errors if the fabric-type configuration does not match the installed fabric cable type.	Platform	Following an upgrade, apply the correct fabric-type configuration according to the installed fabric cables and perform a system restart.
SW-106390	When adding a policer to an existing rule, while other rules have policers and that policy was attached to an interface, the commit will fail.	QOS	1. Detach that policy from the interface and commit. 2. Change the policy and commit. 3. Attach the policy to the interface.
SW-101092	The shape-only policy for a bundle in core mode is not stable.	QOS	Open issue
SW-97959	The `show qos interfaces` command shows a wrong value for high-priority rates when an egress policy is attached to a 100G breakout interface that originated from a 400G interface.	QOS	Currently, there is no workaround.

Issue ID	Description	Component	Solution
SW-48083	The MSS for BGP sessions that are established via RSVP tunnels, is lower than the egress interface MTU. This happens when communication from the Linux host that's supposed to egress via an RSVP tunnel is not sent directly via the egress interface because these types of routes are not installed in Linux. Instead, a tunnel interface is used that has the MTU set to a higher value than the maximum possible MTU on the real interface, which constantly triggers the PL-PMTU. When BGP sends big packets, they get discarded and retransmitted by a Linux IP stack with a lower segment size.	RSVP	Currently, there is no workaround.
SW-21257	RSVP Node-bypass tunnels may be routed via a tunnel's tail node. There is no impact on traffic. The RSVP tunnel route might be sub-optimal.	RSVP	Currently, there is no workaround.
SW-82474	The `run traceroute mpls nil-fec` command fails when using binding-sid labels because the binding-sid is not known to the OAM process.	Segment Routing	Currently, there is no workaround.
SW-100574	When running an snmp walk for IP-MIB::ipAddressIfIndex or IP-MIB::ipAddressIfIndex.ipv6, there are some missing MIBs for loopback interfaces.	SNMP	Run an snmp walk for IP-MIB. This includes everything.
SW-98421	A static route that is resolved by an imported L3VPN BGP route stays inactive.	Static Route	Currently, there is no workaround.
SW-104888	In case of a misconfiguration with two static routes using each other as a solution, and one of them having an additional ECMP nexthop with a valid solution, the RIB-Manager will keep endlessly updating these routes and installing them.	Static Route	Fix the static route configuration so that they don't point to each other.

Issue ID	Description	Component	Solution
SW-101494	Telnet is not sending TELNET_SESSION_LOGIN_FAILED event on a cluster. The standalone event is sent properly.	TELNET	Currently, there is no workaround.
SW-88651	Taking Tech Support (TS) files simultaneously from multiple CLI shows an 'Unexpected Error' instead of showing the normal error. The exact cause is still under investigation.	TS DNOS	The issue should not appear if a TS is not taken simultaneously. The workaround is taking a TS at a later point.
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-100056	Due to a BCM issue, there is no enforcement of MTU on flooded traffic sent on an IRB interface.	WhiteBox	Currently, there is no workaround.

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.	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.

Issue ID	Description	Component	Solution
	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.		
SW-84538	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.

Release 18.0.1 - 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	18.0.1.1
CAL	DriveNets Golden Image	18.0.0.1
StrataX	DNOS NCM NOS	1.2.0
Base-OS	Base-OS	2.18011596011
FW and ONIE	Firmware and ONIE bundled packages for all cluster element types (NCC, NCM, NCF and NCP)	18.0.0.1
DNOR	DriveNets Network Orchestrator	15.1.0.1

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

Resolved Issues

Issue ID	Description	Component
SW-106468	Some memory may not be freed if a BGP peer session was restarted due to maximum prefix condition	BGP
SW-106390	When adding a policer to an existing rule, while other rules have policers and that policy was attached to an interface, the commit will fail.	QOS

Issue ID	Description	Component
SW-101092	The shape-only policy for a bundle in core mode is not stable.	QOS

Limitations

Issue ID	Description	Component	Solution
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 impossible to match any fragments (initial, non-initial) of the IPv6 packets.	ACL	Currently, there is no solution, fix, or workaround to overcome this issue.
SW-22552	Only the primary path is used when a route is resolved via a BGP route with LFA.	BGP	Currently, there is no solution, fix, or WA to overcome this issue.
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	Currently, there is no solution, fix, or workaround to overcome this issue.
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 also partially configurable via the network-services hierarchy, although their configuration is done under the top hierarchy. The management VRFs appear to the user	CLI	There is no workaround. The default VRF configuration is not done via the network-services hierarchy but via the top hierarchy. The management VRFs are not configurable, and the user should not attempt to configure them.

Issue ID	Description	Component	Solution
	as configurable, although they are not (by design).		
SW-43391	Up to 10 simultaneous CLI sessions can be supported on a Standalone NCP.	CLI	Currently, there is no solution, fix, or workaround to overcome this issue.
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	Remove the management interface configuration from the routing protocol hierarchy.
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	Apply the `show file tech-support` command when the system reaches its UP state.
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	Currently, there is no solution, fix, or workaround to overcome this issue.
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, a breakout cannot be for some transceivers (e.g., INNOLIGHT 400G T-DP4CNT-N00) configured.	Interfaces	Currently, there is no solution, fix, or workaround to overcome this issue.

Issue ID	Description	Component	Solution
SW-13193	With ISIS on an interface configured with an MTU above 9222, ISIS adjacency cannot be established.	Interfaces	Decrease the interface MTU below 9222.
SW-45496	The ISIS process will crash if more than 1536 ISIS circuits are configured.	ISIS	Currently, there is no solution, fix, or workaround to overcome this issue.
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	Currently, there is no solution, fix, or WA to overcome this issue.
SW-85530	Connection to a remote server using the 'run ssh' command will generate an SSH_SESSION_LOGIN_FAILED system event with the user 'bublik' on the remote server. This is a mock user used to fetch the ssh banner and print to the screen before using the actual ssh credentials provided.	Management	Currently, there is no solution, fix, or workaround to overcome this issue.
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	Currently, there is no solution, fix, or workaround to overcome this issue.
SW-76489	An NCM ONIE upgrade from DriveNets ONIE 2020 onwards is not supported. The reason is that the MU (Multi Updater) uses an old FSCK (File system check) while DriveNets ONIE uses a newer one.	NCE Management	Upgrade to the new ONIE, DN ONIE 2019.06.
SW-42116	System switchover is logged as System failover.	NCE Management	Currently, there is no solution, fix, or workaround to overcome this issue.

Issue ID	Description	Component	Solution
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	Currently, there is no solution, fix, or workaround to overcome this issue.
SW-51282	NTP processes can reset in some scenarios.	NTP	NTP restarts do not affect the system. Timing is unaffected.
SW-77634	Upgrading a DNI-based cluster to v16.2 requires the removal of the NCP configuration. This limitation is applicable 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. Adding or editing the hardware model configuration without removing the NCP configuration first is impossible.	Platform	Remove the NCP configuration prior to the upgrade by using the `no ncp` command. Any other configuration referencing NCP interfaces must also be removed, e.g., protocols interface configuration. You can now complete the upgrade and then reconfigure all the NCPs with the correct AGCXD40S hardware model, by using the command 'system ncp 0 model NCP-40C hw-model AGCXD40S admin-state enabled' and re-adding the removed NCP configuration.
SW-76547	RN1: For low-speed subscribers, there is no differentiation between WRED and Weighted Tail Drop (WTD) thresholds. RN2: There are continuous unexpected tail drops over the WRED max threshold.	QOS	RN1: The minimum queue or threshold size set in the hardware is 125kB. For low-rate subscribers, two different thresholds values configured in temporal units (milliseconds or microseconds) may both be converted to the same minimum value. To keep the

Issue ID	Description	Component	Solution
			differentiation for low-speed subscribers, use the hardware-mapping speed configuration, setting the minimum speed of all traffic below 1gpbs to a speed of 1gpbs. This is the default configuration. RN2: To avoid or minimize continuous tail drops, increase the difference between the max WRED threshold and the queue size. For low-rate queues, use the hardware mapping speed conversion table to avoid setting both to the minimum 125kB queue and threshold sizes. Have at least a 250KB difference between the queue size and the max WRED threshold.
SW-258336	Packet reorder may happen when the same stream contains multiple classes and the QoS policy is not attached.	QOS	Currently, there is no solution, fix, or workaround to overcome this issue.
SW-253352	Multiple egress policies can be created, yet only a single egress policy can be attached.	QOS	Currently, there is no solution, fix, or workaround to overcome this issue.
SW-242114	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.	QOS	Currently, there is no solution, fix, or workaround to overcome this issue.

<table>
<tr><th>Issue ID</th><th>Description</th><th>Component</th><th>Solution</th></tr>
<tr><td></td><td>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>
<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</td><td></td><td></td></tr>
</table>

Issue ID	Description	Component	Solution
	the show commands `show qos interface counters` or `show qos summary` to display the QoS summary table.		
SW-23773	Egress match counters count the ingress (not the egress) packet bytes, including Ethernet and other terminated layers.	QOS	Currently, there is no solution, fix, or WA to overcome this issue.
SW-23072	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.	User Management	Currently, there is no solution, fix, or WA to overcome this issue.

Known Issues

Issue ID	Description	Component	Solution
SW-108546	ISIS maximum routes limit and threshold alarms will not be triggered and will not populate the `active alarms list`. Only a system event would be generated.	Alarms	Currently, there is no workaround.
SW-103870	When LACP goes into down state on an interface, an alarm will not be triggered and will not populate the `active alarms list`. Only a system event will be generated.	Alarms	Currently, there is no workaround.
SW-103866	When an SR policy goes into down state, an alarm will not be triggered and will not populate	Alarms	Currently, there is no workaround.

Issue ID	Description	Component	Solution
	the `active alarms list`. Only a system event will be generated.		
SW-103172	ISIS maximum routes limit and threshold alarms will not be triggered and will not populate the `active alarms list`. Only a system event would be generated.	Alarms	Currently, there is no workaround.
SW-102541	The RADIUS_SERVER_STATE_CHANGE_NOT_AVAILABLE alarm will not be triggered when connectivity to the Radius server is lost. Only a system event will be generated.	Alarms	Will be fixed in 18.2
SW-100903	Traffic over IPv6 routes with IPv4 nexthops is not supported.	BGP	Currently, there is no workaround.
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-48206	When an NTP server is unreachable, disabling the management interface (lo0) might cause the `show system NTP` command to return an error. NTP functionality is not affected.	CLI	Currently, there is no workaround.
SW-21067	Running the command `show interface ctrl-ncm-x` displays an 'uptime' value of 0.	CLI	You can view the interface uptime

Issue ID	Description	Component	Solution
	There is no impact to the system. It is a CLI display issue.		value via the StrataX operation system, using the `run start shell ncm X` command.
SW-89997	The default value of a double-tagged sub-interface is 0x88a8 for the outer tag and 0x8100 for the inner tag. Therefore, the default TPID value has been removed and is now written by the datapath behind the scenes. Making it seem like the TPID is configured manually.	Datapath	Currently, there is no workaround.
SW-22899	Failure of the standby NCC might cause the active ssh session to be inaccessible for about two minutes.	High Availability	Currently, there is no workaround.
SW-98773	Received ARP message in the bridge-domain, with a dst-mac of the IRB, is flooded to the bridge-domain's attachment circuits (as well as being punted to the CPU as needed).	Interfaces	Currently, there is no workaround.
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	If the management interface is disabled, the uptime of the interface can be ignored.
SW-36535	The IPMI interface remains in UP state after the interface is disabled. This happens when access	Interfaces	Currently, there is no workaround.

Issue ID	Description	Component	Solution
	to the IPMI interface is disabled to mimic admin-state disable, and access cannot be regained.		
SW-106244	A router may not be considered as SR / Flex-Algo capable if router capabilities are advertised from a non-0 lsp fragment.	ISIS	Make sure all fragments are scanned for the router capability tlv when providing information to the relevant topology.
SW-40860	When changing the number of maximum paths under ISIS, abnormal traffic loss is seen for a duration of 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 not valid, there is no way to know if the path to root via the

Issue ID	Description	Component	Solution
			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 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.	LDP	Currently, there is no workaround.
SW-42531	Configuring a syslog server with a hostname and not an IP may cause syslog messages not to be sent to the server.	LOG	Configure syslog server with IP address
SW-39013	At scale, when there is a fast log rotation, there may be a mismatch between the log .gz file timestamp and the log timestamps within the file.	LOG	Currently, there is no workaround.
SW-100397	An FTP_SESSION_LIMIT_CLEARED event is wrongly sent when reaching the maximum number of sessions allowed.	Management	Currently, there is no workaround.
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:	Management	For similar scenarios as

Issue ID	Description	Component	Solution
	1. delete interface 'x' 2. commit 3. 'rollback 1' (re-creates interface 'x') 4. delete interface 'x' 5. commit <<<<< Failure here		above, the proposed workaround is to perform the commit immediately after the 'rollback' command.
SW-44069	Configured data-connection-timeout value is not strict. The configured value is the minimum amount of time the connection is allowed before being disconnected. The maximum amount of time will not exceed twice the configured value for the data-connection-timeout.	Management	Currently, there is no workaround.
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.

Issue ID	Description	Component	Solution
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.
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-96242	The Make Before Break process is aborted if a former primary IIF is chosen as a standby IIF, causing traffic loss of up to 40 seconds.	Multicast	Currently, there is no workaround.
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-106817	Revert operation pre-check test falsely fails when pre-checking SW revert from version 18 to version 17.2. The revert operation is still successful, although the pre-check test fails.	None	Currently, there is no workaround.

Issue ID	Description	Component	Solution
SW-104888	In case of a misconfiguration with two static routes using each other as a solution, and one of them having an additional ECMP nexthop with a valid solution, the RIB-Manager will keep endlessly updating these routes and installing them.	None	Fix the static route configuration so that they don't point to each other.
SW-104759	Mellanox cards from HP with interfaces configured to work in InfiniBand mode (default mode) are not supported	None	Manually configure the interface to Ethernet.
SW-100375	The actual limitation is per physical when configuring an interface shaper for a bundle. If the limitation is below 2.6G, it will limit it to 2.6G (min shaper for physical).	None	Currently, there is no workaround
SW-105030	Some traffic loss may be experienced during the system restart of a router acting as VRRP backup. The issue is mostly related to the high scale of interfaces.	None	Currently, there is no workaround.
SW-101775	The login prompt is different based on how you try to connect, console, ssh-tacacs, ssh-local-users, ssh-radius.	None	Currently, there is no workaround.
SW-106267	When OSPFv2 is configured with `max-metric router-lsa on-startup` and the user removes the entire OSPF configuration and performs a rollback, max-metric will not be sent at startup, although it is enabled in the CLI. When `max-metric router-lsa on-startup` function is enabled, and the user removes the entire OSPF configuration, then re-apply the configuration manually (not via	OSPF	Remove the entire OSPF configuration again and commit. Then do rollback 1 and commit. After this, manually add the

Issue ID	Description	Component	Solution
	rollback), the `max-metric router-lsa on-startup` function becomes active immediately, even if you did not restart the device.		'max-metric knob' and commit. When this happens, remove the 'max-metric knob' and add it manually or via rollback.
SW-105104	Configuring a new md5 key and removing an existing key in the same commit, results in removing only the existing key.	OSPF	1. Remove the md5 key and commit 2. Add the new key and commit.
SW-79291	During a DNOS upgrade, the cluster fabric-type configuration is reset to its default values. This might lead to traffic forwarding errors if the fabric-type configuration does not match the installed fabric cable type.	Platform	Following an upgrade, apply the correct fabric-type configuration according to the installed fabric cables and perform a system restart.
SW-107463	When the user changes a sub-interface in one bundle, there might be a minor traffic drop (<2ms) on other bundles. This happens only on a large scale .	QOS	Currently, there is no workaround.

Issue ID	Description	Component	Solution
SW-106980	Configuring more than one qos-tag to queue (QT2Q) mappings on a parent interface (physical or bundle) and its subs is not allowed and is validated on commit. The user can pass the validation when configuring more than one QT2Q mappings on a bundle and its subs in a bundle with no members. The user can then add members to the bundle, leading to unexpected issues, such as commit failure or going into the wrong queues.	QOS	Do not configure QoS policies on a bundle and its subs in a bundle with no members.
SW-97959	The `show qos interfaces` command shows a wrong value for high-priority rates when an egress policy is attached to a 100G breakout interface that originated from a 400G interface.	QOS	Currently, there is no workaround.
SW-48083	The MSS for BGP sessions that are established via RSVP tunnels, is lower than the egress interface MTU. This happens when communication from the Linux host that's supposed to egress via an RSVP tunnel is not sent directly via the egress interface, because these types of routes are not installed in Linux. Instead, a tunnel interface is used that has the MTU set to a higher value than the maximum possible MTU on the real interface, which constantly triggers the PL-PMTU. When BGP sends big packets they get discarded and retransmitted by a Linux IP stack with a lower segment size.	RSVP	Currently, there is no workaround.
SW-21257	RSVP Node-bypass tunnels may be routed via a tunnel's tail node. There is no impact to traffic. The RSVP tunnel route might be sub-optimal.	RSVP	Currently, there is no workaround.
SW-107318	When a Flex-Algo is configured with TE constraints, Cisco routers prefer to reach a specific destination on the higher-cost path	Segment Routing	From v18.1, DNOS starts advertising

Issue ID	Description	Component	Solution
	through Cisco routers instead of a lower-cost path through DNOS routers. According to RFC 8919, DNOS advertises its TE link attributes in ISIS reachability with the legacy sub-TLVs. In addition, DNOS advertises Application-Specific Link Attributes (ASLA) sub-TLV with the Legacy flag (L-flag) set. This informs other routers to take the TE attributes from the legacy TLVs, not the ASLA. Cisco routers ignore this flag. This leads Cisco routers to exclude DNOS routers from the Flex-Algo topology and the Cisco view. This behavior doesn't happen when the metric type for Flex-Algo is set to IGP.		its TE attributes inside the ASLA sub-TLVs with the L-flag not set.
SW-82474	The `run traceroute mpls nil-fec` command fails when using binding-sid labels because the binding-sid is not known to the OAM process.	Segment Routing	Currently, there is no workaround.
SW-100574	When running an snmp walk for IP-MIB::ipAddressIfIndex or IP-MIB::ipAddressIfIndex.ipv6, there are some missing MIBs for loopback interfaces.	SNMP	Run an snmp walk for IP-MIB. This includes everything.
SW-98421	A static route that is resolved by an imported L3VPN BGP route stays inactive.	Static Route	Currently, there is no workaround.
SW-101494	Telnet is not sending TELNET_SESSION_LOGIN_FAILED event on a cluster. The standalone event is sent properly.	TELNET	Currently, there is no workaround.
SW-88651	Taking tech-support simultaneously from multiple CLI shows 'Unexpected Error' instead of showing the normal error. The exact cause is still under investigation.	TS DNOS	The issue should not appear if a TS is not taken

Issue ID	Description	Component	Solution
			simultaneously. The workaround is taking a TS at a later point.
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-100056	Due to a BCM issue, there is no enforcement of MTU on flooded traffic sent on an IRB interface.	White Box	Currently, there is no workaround.

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.

Issue ID	Description	Component	Solution
SW-84538	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.

Release 18.0.2 - 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	18.0.2.6
CAL	DriveNets Golden Image	18.0.2.6
StrataX	DNOS NCM NOS	1.2.0
Base-OS	Base-OS	2.18021922006
FW and ONIE	Firmware and ONIE bundled packages for all cluster element types (NCC, NCM, NCF and NCP)	18.0.0.1
DNOR	DriveNets Network Orchestrator	18.1.0.7

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

Datapath

Finisar 400G LR4

DriveNets now supports using Finisar 400G LR4 NIF (FTCD4323E2PCL) on NCP-36CD-S (NCP3). LR4 enables the transmission up to a 10 km range. According to DriveNets NIF similarity policy, 400G LR4 NIFs tested by UfiSpace will also be supported.

Logs Infrastructure

System Timezone for Debug Traces

System Timezone, a feature that provides a full sync for dates & times between all the containers in all cluster/ SA components, has been enhanced. Currently, the system timezone configuration can also affect internal system traces used for debugging. As a result, all Linux logs, logs, and traces will use the same time zone.

To configure the time zone, use the `system timezone <timezone>` configuration parameter.

Management

mgmt0 Interface Description

The mgmt0 interface can now be configured with a description.

Management Infrastructure

AAA TACACS Command Authorization

TACACS command authorization provides granular control over command execution on network devices by authorizing or denying each specific CLI command using a TACACS server. In such cases, the device doesn't rely on user roles or privileges for authorization; each CLI command is sent to the TACACS server for authorization.

With TACACS Command Authorization, network administrators can now ensure that only authorized users have access to specific commands, reducing the risk of unauthorized configuration changes and security breaches.

SNMP Communities

The number of parallel SNMP communities supported by DNOS was increased to 10.

Management-Infra

Syslog Server Severity

Syslog severity can now be configured per server rather than across the entire system. This will offer greater flexibility and control for network operators, enabling them to fine-tune their logging settings to better meet their specific needs. With this new functionality, users can easily adjust Syslog severity levels for individual servers, ensuring that critical logs are correctly identified and addressed.

The default severity per the Syslog server is a warning. You can change the severity to emergency, critical, error, warning, notification, info, and debug. To configure the severity per Syslog server, use the `system logging syslog server severity` command.

Routing

LDP-sync hold-time

DNOS now supports LDP Sync Hold-time on OSPFv2. When `max-hold-time` is set, the advertisement of 'max-metric' in the IGP interface due to the LDP-sync logic (when there is no LDP neighbor over the interface) will be no more than the set ‘max-hold-time’ timer. If the LDP session recovers earlier and LDP-sync logic no longer requires max-metric to be advertised, the interface will return to the configured metric value.

To configure LDP Sync Hold-time on OSPFv2 use the `protocols ospf instance <instance> area <area> interface <interface> ldp-sync <enabled/disabled> max-hold-time <1..65535>` command.

Setting a Community List in a Routing Policy

You can now set a community list in routing policies, not just a single community value. This allows setting multiple communities instead of specifying all communities one by one in each rule, as was done till now.

To modify the communities lists of the BGP route per provided community-list and list-option, use the `policy set community-list` command.

To modify the extcommunities lists of the BGP route per provided extcommunity-list and the list-option, use the `policy set extcommunity-list` command.

To modify the large-communities lists of the BGP route per provided large-community-list and list-option, use the `policy set large-community-list` command.

Increase ARP and NDP Entry Scale

Previous versions of DNOS supported 10K ARP and NDP entry scale, combined. Now, DNOS supports 50K ARP and NDP entry scale, combined.

As part of this increment, the number of ARP and NDP entries on a single Integrated Routing and Bridging (IRB) interface was increased to support the maximum scale of the system, which is 50k.

Resolved Issues

Issue ID	Description	Component
SW-105030	Some traffic loss may be experienced during the system restart of a router acting as VRRP backup. The issue is mostly related to the high scale of interfaces.	None
SW-107463	When the user changes a sub-interface in one bundle, there might be a minor traffic drop (<2ms) on other bundles. This happens only on a large scale.	QOS
SW-106980	Configuring more than one qos-tag to queue (QT2Q) mappings on a parent interface (physical or bundle) and its subs is not allowed and is validated on commit. The user can pass the validation when configuring more than one QT2Q mappings on a bundle and its subs in a bundle with no members. The user can then add members to the bundle, leading to unexpected issues, such as commit failure or going into the wrong queues.	QOS

Limitations

Issue ID	Description	Component	Solution
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 impossible to match any	ACL	Currently, there is no solution, fix, or workaround to overcome this issue.

Issue ID	Description	Component	Solution
	fragments (initial, non-initial) of the IPv6 packets.		
SW-22552	Only the primary path is used when a route is resolved via a BGP route with LFA.	BGP	Currently, there is no solution, fix, or WA to overcome this issue.
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	Currently, there is no solution, fix, or workaround to overcome this issue.
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 also partially configurable via the network-services hierarchy, 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	There is no workaround. The default VRF configuration is not done via the network-services hierarchy but via the top hierarchy. The management VRFs are not configurable, and the user should not attempt to configure them.
SW-433391	Up to 10 simultaneous CLI sessions can be supported on a Standalone NCP.	CLI	Currently, there is no solution, fix, or workaround to overcome this issue.
SW-204221	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	Remove the management interface configuration from the routing protocol hierarchy.

Issue ID	Description	Component	Solution
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	Apply the `show file tech-support` command when the system reaches its UP state.
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	Currently, there is no solution, fix, or workaround to overcome this issue.
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, a breakout cannot be for some transceivers (e.g., INNOLIGHT 400G T-DP4CNT-N00) configured.	INTERFACES	Currently, there is no solution, fix, or workaround to overcome this issue.
SW-13193	With ISIS on an interface configured with an MTU above 9222, ISIS adjacency cannot be established.	INTERFACES	Decrease the interface MTU below 9222.
SW-45496	The ISIS process will crash if more than 1536 ISIS circuits are configured.	ISIS	Currently, there is no solution, fix, or workaround to overcome this issue.
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	Currently, there is no solution, fix, or WA to overcome this issue.

Issue ID	Description	Component	Solution
SW-85530	Connection to a remote server using the 'run ssh' command will generate an SSH_SESSION_LOGIN_FAILED system event with the user 'bublik' on the remote server. This is a mock user used to fetch the ssh banner and print to the screen before using the actual ssh credentials provided.	MANAGEMENT	Currently, there is no solution, fix, or workaround to overcome this issue.
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	Currently, there is no solution, fix, or workaround to overcome this issue.
SW-76489	An NCM ONIE upgrade from DriveNets ONIE 2020 onwards is not supported. The reason is that the MU (Multi Updater) uses an old FSCK (File system check) while DriveNets ONIE uses a newer one.	NCE MANAGEMENT	Upgrade to the new ONIE, DN ONIE 2019.06.
SW-42116	System switchover is logged as System failover.	NCE MANAGEMENT	Currently, there is no solution, fix, or workaround to overcome this issue.
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	Currently, there is no solution, fix, or workaround to overcome this issue.
SW-51282	NTP processes can reset in some scenarios.	NTP	NTP restarts do not affect the system. Timing is unaffected.
SW-77634	Upgrading a DNI-based cluster to v16.2 requires the removal of the NCP configuration. This limitation is	PLATFORM	Remove the NCP configuration prior to the upgrade by using the no ncp command. Any

Issue ID	Description	Component	Solution
	applicable 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. Adding or editing the hardware model configuration without removing the NCP configuration first is impossible.		other configuration referencing NCP interfaces must also be removed, e.g., protocols interface configuration. You can now complete the upgrade and then reconfigure all the NCPs with the correct AGCXD40S hardware model, by using the command 'system ncp 0 model NCP-40C hw-model AGCXD40S admin-state enabled' and re-adding the removed NCP configuration.
SW-76547	RN1: For low-speed subscribers, there is no differentiation between WRED and Weighted Tail Drop (WTD) thresholds. RN2: There are continuous unexpected tail drops over the WRED max threshold.	QOS	RN1: The minimum queue or threshold size set in the hardware is 125kB. For low-rate subscribers, two different thresholds values configured in temporal units (milliseconds or microseconds) may both be converted to the same minimum value. To keep the differentiation for low-speed subscribers, use the hardware-mapping speed configuration, setting the minimum speed of all traffic below 1gpbs to a speed of 1gpbs. This is the default configuration. RN2: To avoid or minimize continuous tail drops, increase the difference between the max WRED threshold and the queue size. For low-rate

<table>
<tr><th>Issue ID</th><th>Description</th><th>Component</th><th>Solution</th></tr>
<tr><td></td><td></td><td></td><td>queues, use the hardware mapping speed conversion table to avoid setting both to the minimum 125kB queue and threshold sizes. Have at least a 250KB difference between the queue size and the max WRED threshold.</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><td>Currently, there is no solution, fix, or workaround to overcome this issue.</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><td>Currently, there is no solution, fix, or workaround to overcome this issue.</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></table></td><td>QOS</td><td>Currently, there is no solution, fix, or workaround to overcome this issue.</td></tr>
</table>

<table>
<tr><th>Issue ID</th><th>Description</th><th>Component</th><th>Solution</th></tr>
<tr><td></td><td>
<table>
<tr><th>exp-null</th><th>qos-tag</th><th>drop-tag</th></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>
<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><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><td>Currently, there is no solution, fix, or WA to overcome this issue.</td></tr>
</table>

Issue ID	Description	Component	Solution
SW-23072	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.	User Management	Currently, there is no solution, fix, or WA to overcome this issue.

Known Issues

Issue ID	Description	Component	Solution
SW-108546	ISIS maximum routes limit and threshold alarms will not be triggered and will not populate the `active alarms list`. Only a system event would be generated.	Alarms	Currently, there is no workaround.
SW-103870	When LACP goes into down state on an interface, an alarm will not be triggered and will not populate the `active alarms list`. Only a system event will be generated.	Alarms	Currently, there is no workaround.
SW-103866	When an SR policy goes into down state, an alarm will not be triggered and will not populate the `active alarms list`. Only a system event will be generated.	Alarms	Currently, there is no workaround.
SW-103172	ISIS maximum routes limit and threshold alarms will not be triggered and will not populate the `active alarms list`. Only a system event would be generated.	Alarms	Currently, there is no workaround.

Issue ID	Description	Component	Solution
SW-102541	The RADIUS_SERVER_STATE_CHANGE_NOT_AVAILABLE alarm will not be triggered when connectivity to the Radius server is lost. Only a system event will be generated.	Alarms	Will be fixed in 18.2
SW-77147	On rare occasions, when executing the `show bfd sessions` 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-100903	Traffic over IPv6 routes with IPv4 Next-Hop is not supported.	BGP	Currently, there is no workaround.
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-48206	When an unreachable NTP server is present, disabling the management interface (lo0) might cause the show system NTP command to return an error. NTP functionality is not affected.	CLI	Currently, there is no workaround.
SW-21067	Running the command `show interface ctrl-ncm-x` displays an 'uptime' value of 0. There is no impact on the system. It is a CLI display issue.	CLI	You can view the interface uptime value via the StrataX operation system, using the `run start shell ncm X` command.
SW-89997	The default value of a double-tagged sub-interface is 0x88a8 for the outer tag and	DATAPATH	Currently, there is no workaround.

Issue ID	Description	Component	Solution
	0x8100 for the inner tag. Therefore, the default TPID value has been removed and is now written by the datapath behind the scenes. Making it seem like the TPID is configured manually.		
SW-22899	Failure of the standby NCC might cause the active ssh session to be inaccessible for about two minutes.	High Availability	Currently, there is no workaround.
SW-98773	Received ARP message in the bridge-domain, with a dst-mac of the IRB, is flooded to the bridge-domain's attachment circuits (as well as being punted to the CPU as needed).	INTERFACES	Currently, there is no workaround.
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	If the management interface is disabled, the uptime of the interface can be ignored.
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.
SW-106244	A router may not be considered as SR / Flex-Algo capable if router capabilities are advertised from a non-0 lsp fragment.	ISIS	Make sure all fragments are scanned for the router capability tlv when providing information to the relevant topology.

Issue ID	Description	Component	Solution
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 not valid, 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 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.	LDP	Currently, there is no workaround.
SW-115050	Prefix-list rules are not written to the local and remote accounting log (TACACS), but the prefix-list is modified in the logs.	LOG	Currently, there is no workaround.
SW-42531	Configuring a Syslog server with a hostname and not an IP may cause Syslog messages not to be sent to the server.	LOG	Configure Syslog server with IP address
SW-39013	At scale, when there is a fast log rotation, there may be a mismatch between the	LOG	Currently, there is no workaround.

Issue ID	Description	Component	Solution
	log .gz file timestamp and the log timestamps within the file.		
SW-100397	An FTP_SESSION_LIMIT_CLEARED event is wrongly sent when reaching the maximum number of sessions allowed.	MANAGEMENT	Currently, there is no workaround.
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 3. 'rollback 1' (re-creates interface 'x') 4. delete interface 'x' 5. commit <<<<< Failure here	MANAGEMENT	For similar scenarios as above, the proposed workaround is to perform the commit immediately after the 'rollback' command.
SW-44069	Configured data-connection-timeout value is not strict. The configured value is the minimum amount of time the connection is allowed before being disconnected. The maximum amount of time will not exceed twice the configured value for the data-connection-timeout.	MANAGEMENT	Currently, there is no workaround.
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	MPLS	Currently, there is no workaround.

Issue ID	Description	Component	Solution
	label) is installed in the cluster. Therefore, there is a time gap in which there is no replication and packets may drop.		
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, and 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.
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-96242	The Make Before Break process is aborted if a former primary IIF is chosen as a standby IIF, causing traffic loss of up to 40 seconds.	Multicast	Currently, there is no workaround.
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-108200	In DNOR - Components - Summary - Network, the Out-of-Band and In-band IPv6 statuses are not properly displayed.	NCE MANAGEMENT	Currently, there is no workaround.

Issue ID	Description	Component	Solution
SW-106817	Revert operation pre-check test falsely fails when pre-checking SW revert from version 18 to version 17.2. The revert operation is still successful, although the pre-check test fails.	None	Currently, there is no workaround.
SW-104888	In case of a misconfiguration with two static routes using each other as a solution, and one of them having an additional ECMP nexthop with a valid solution, the RIB-Manager will keep endlessly updating these routes and installing them.	None	Fix the static route configuration so that they don't point to each other.
SW-104759	Mellanox cards from HP with interfaces configured to work in InfiniBand mode (default mode) are not supported	None	Manually configure the interface to Ethernet.
SW-100375	The actual limitation is per physical when configuring an interface shaper for a bundle. If the limitation is below 2.6G, it will limit it to 2.6G (min shaper for physical).	None	Currently, there is no workaround.
SW-101775	The login prompt is different based on how you try to connect, console, ssh-tacacs, ssh-local-users, ssh-radius	None	Currently, there is no workaround.
SW-106267	When OSPFv2 is configured with `max-metric router-lsa on-startup` and the user removes the entire OSPF configuration and performs a rollback, max-metric will not be sent at startup, although it is enabled in the CLI. When `max-metric router-lsa on-startup` function is enabled, and the user removes the entire OSPF	OSPF	Remove the entire OSPF configuration again and commit. Then do rollback 1 and commit. After this, manually add the ‘max-metric knob’ and commit. When this happens, remove the ‘max-metric

Issue ID	Description	Component	Solution
	configuration, then re-apply the configuration manually (not via rollback), the `max-metric router-lsa on-startup` function becomes active immediately, even if you did not restart the device.		knob' and add it manually or via rollback.
SW-105104	Configuring a new md5 key and removing an existing key in the same commit, results in removing only the existing key	OSPF	1. Remove the md5 key and commit 2. Add the new key and commit.
SW-79291	During a DNOS upgrade, the cluster fabric-type configuration is reset to its default values. This might lead to traffic forwarding errors if the fabric-type configuration does not match the installed fabric cable type.	PLATFORM	Following an upgrade, apply the correct fabric-type configuration according to the installed fabric cables and perform a system restart.
SW-97959	The `show QoS interfaces` command shows a wrong value for high-priority rates when an egress policy is attached to a 100G breakout interface that originated from a 400G interface.	QOS	Currently, there is no workaround.
SW-48083	The MSS for BGP sessions that are established via RSVP tunnels, is lower than the egress interface MTU. This happens when communication from the Linux host that's supposed to egress via an RSVP tunnel is not sent directly via the egress interface, because these types of routes are not installed in Linux. Instead, a tunnel interface is used that has the MTU set to a higher value than the maximum possible MTU on the real interface, which constantly triggers the PL-PMTU. When BGP sends big packets they get discarded	RSVP	Currently, there is no workaround.

Issue ID	Description	Component	Solution
	and retransmitted by a Linux IP stack with a lower segment size.		
SW-21257	RSVP Node-bypass tunnels may be routed via a tunnel's tail node. There is no impact to traffic. The RSVP tunnel route might be sub-optimal.	RSVP	Currently, there is no workaround.
SW-107318	When a Flex-Algo is configured with TE constraints, Cisco routers prefer to reach a specific destination on the higher-cost path through Cisco routers instead of a lower-cost path through DNOS routers. According to RFC 8919, DNOS advertises its TE link attributes in ISIS reachability with the legacy sub-TLVs. In addition, DNOS advertises Application-Specific Link Attributes (ASLA) sub-TLV with the Legacy flag (L-flag) set. This informs other routers to take the TE attributes from the legacy TLVs, not the ASLA. Cisco routers ignore this flag. This leads Cisco routers to exclude DNOS routers from the Flex-Algo topology and the Cisco view. This behavior doesn't happen when the metric type for Flex-Algo is set to IGP.	Segment Routing	From v18.1, DNOS starts advertising its TE attributes inside the ASLA sub-TLVs with the L-flag not set.
SW-82474	The `run traceroute mpls nil-fec` command fails when using binding-sid labels because the binding-sid is not known to the OAM process.	Segment Routing	Currently, there is no workaround.
SW-98421	A static route that is resolved by an imported L3VPN BGP route stays inactive.	STATIC ROUTE	Currently, there is no workaround.
SW-101494	Telnet is not sending TELNET_SESSION_LOGIN_FAILED event on a cluster. The standalone event is sent properly.	TELNET	Currently, there is no workaround.

Issue ID	Description	Component	Solution
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-112563	In L2- service-enabled interfaces, the displayed TX rate may be inaccurate by a margin of 5%.	White Box	Currently, there is no workaround.
SW-110188	The signal integrity parameters were not set correctly on the INPHI gearbox. This meant that the link quality between GB -->J2 and GB-->TRNCVR was insufficient, which might have caused port-link stability issues and/or packet corruption (CRC).	White Box	Fix was provided in the delivered version. When configuring the FEC, reset to the SI parameters was not performed.
SW-109506	Due to a hardware issue, the reference clock to the data path ASICS of the DNI NCP-40C is not accurate. There was a missing script to update the reference clock.	White Box	DN added a script upon init phase to initialize the reference clock.
SW-108935	Disabling or enabling l2-service on an existing interface may cause wrong counters.	White Box	For logical interfaces, a possible workaround would be to explicitly delete the interface and re-create it with the l2-service set as enabled/ disabled. for physical interfaces - no known workaround
SW-100056	Due to a BCM issue, there is no enforcement of MTU on flooded traffic sent on an IRB interface.	White Box	Currently, there is no workaround.

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-84538	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.

Release 18.0.3 - 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	18.0.3.6
CAL	DriveNets Golden Image	18.0.3.6
StrataX	DNOS NCM NOS	1.2.0
Base-OS	Base-OS	2.18032241005
FW and ONIE	Firmware and ONIE bundled packages for all cluster element types (NCC, NCM, NCF and NCP)	18.0.0.1
DNOR	DriveNets Network Orchestrator	18.1.0.7

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

Routing

Routing Policy - set a community and community-list

When using a routing policy, "set community" and “set community-list" can be configured under the same rule.

Now, the set instructions will be executed in a fixed order; first, the "set community-list" instruction will manipulate the route, and then the "set community".
For versions before v18.0.2, a known issue existed; when both actions were configured under the same rule, the order between the actions was non-deterministic.
in 18.0.2, a validation was added in the CLI to block this combination. This validation was removed in 18.0.3.

Limitations

Issue ID	Description	Component	Solution
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 impossible to match any fragments (initial, non-initial) of the IPv6 packets.	ACL	Currently, there is no solution, fix, or workaround to overcome this issue.
SW-22552	Only the primary path is used when a route is resolved via a BGP route with LFA.	BGP	Currently, there is no solution, fix, or WA to overcome this issue.
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	Currently, there is no solution, fix, or workaround to overcome this issue.
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 also partially configurable via the network-services hierarchy, 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	There is no workaround. The default VRF configuration is not done via the network-services hierarchy but via the top hierarchy. The management VRFs are not configurable, and the user should not attempt to configure them.
SW-43391	Up to 10 simultaneous CLI sessions can be supported on a Standalone NCP.	CLI	Currently, there is no solution, fix, or workaround to overcome this issue.

Issue ID	Description	Component	Solution
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	Remove the management interface configuration from the routing protocol hierarchy.
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	Apply the `show file tech-support` command when the system reaches its UP state.
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	Currently, there is no solution, fix, or workaround to overcome this issue.
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, a breakout cannot be for some transceivers (e.g., INNOLIGHT 400G T-DP4CNT-N00) configured.	Interfaces	Currently, there is no solution, fix, or workaround to overcome this issue.
SW-13193	With ISIS on an interface configured with an MTU above 9222, ISIS adjacency cannot be established.	Interfaces	Decrease the interface MTU below 9222.

Issue ID	Description	Component	Solution
SW-45496	The ISIS process will crash if more than 1536 ISIS circuits are configured.	ISIS	Currently, there is no solution, fix, or workaround to overcome this issue.
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	Currently, there is no solution, fix, or WA to overcome this issue.
SW-85530	Connection to a remote server using the 'run ssh' command will generate an SSH_SESSION_LOGIN_FAILED system event with the user 'bublik' on the remote server. This is a mock user used to fetch the ssh banner and print to the screen before using the actual ssh credentials provided.	Management	Currently, there is no solution, fix, or workaround to overcome this issue.
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	Currently, there is no solution, fix, or workaround to overcome this issue.
SW-76489	An NCM ONIE upgrade from DriveNets ONIE 2020 onwards is not supported. The reason is that the MU (Multi Updater) uses an old FSCK (File system check) while DriveNets ONIE uses a newer one.	Management	Upgrade to the new ONIE, DN ONIE 2019.06.
SW-42116	System switchover is logged as System failover.	Management	Currently, there is no solution, fix, or workaround to overcome this issue.
SW-83003	DNI platforms don't have bit error counters available, and symbol error counters are post-FEC. As a result, the	None	Currently, there is no solution, fix, or workaround to overcome this issue.

Issue ID	Description	Component	Solution
	signal degrade and signal failure alarms relying on BER calculation have inherent inaccuracy.		
SW-51282	NTP processes can reset in some scenarios.	NTP	NTP restarts do not affect the system. Timing is unaffected.
SW-77634	Upgrading a DNI-based cluster to v16.2 requires the removal of the NCP configuration. This limitation is applicable 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. Adding or editing the hardware model configuration without removing the NCP configuration first is impossible.	Platform	Remove the NCP configuration prior to the upgrade by using the no ncp command. Any other configuration referencing NCP interfaces must also be removed, e.g., protocols interface configuration. You can now complete the upgrade and then reconfigure all the NCPs with the correct AGCXD40S hardware model, by using the command 'system ncp 0 model NCP-40C hw-model AGCXD40S admin-state enabled' and re-adding the removed NCP configuration.
SW-76547	RN1: For low-speed subscribers, there is no differentiation between WRED and Weighted Tail Drop (WTD) thresholds. RN2: There are continuous unexpected tail drops over the WRED max threshold.	QOS	RN1: The minimum queue or threshold size set in the hardware is 125kB. For low-rate subscribers, two different thresholds values configured in temporal units (milliseconds or microseconds) may both be converted to the same minimum value. To keep the differentiation for low-speed subscribers, use the hardware-mapping speed configuration, setting the minimum speed of

Issue ID	Description	Component	Solution
			all traffic below 1gpbs to a speed of 1gpbs. This is the default configuration. RN2: To avoid or minimize continuous tail drops, increase the difference between the max WRED threshold and the queue size. For low-rate queues, use the hardware mapping speed conversion table to avoid setting both to the minimum 125kB queue and threshold sizes. Have at least a 250KB difference between the queue size and the max WRED threshold.
SW-25836	Packet reorder may happen when the same stream contains multiple classes and the QoS policy is not attached.	QOS	Currently, there is no solution, fix, or workaround to overcome this issue.
SW-25352	Multiple egress policies can be created, yet only a single egress policy can be attached.	QOS	Currently, there is no solution, fix, or workaround to overcome this issue.
SW-24214	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	QOS	Currently, there is no solution, fix, or workaround to overcome this issue.

<table>
<tr><th>Issue ID</th><th>Description</th><th>Component</th><th>Solution</th></tr>
<tr><td></td><td>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>
<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><td></td></tr>
</table>

Issue ID	Description	Component	Solution
SW-23773	Egress match counters count the ingress (not the egress) packet bytes, including Ethernet and other terminated layers.	QOS	Currently, there is no solution, fix, or WA to overcome this issue.
SW-23072	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.	User Management	Currently, there is no solution, fix, or WA to overcome this issue.

Known Issues

Issue ID	Description	Component	Solution
SW-108546	ISIS maximum routes limit and threshold alarms will not be triggered and will not populate the `active alarms list`. Only a system event would be generated.	Alarms	Currently, there is no workaround.
SW-103870	When LACP goes into down state on an interface, an alarm will not be triggered and will not populate the `active alarms list`. Only a system event will be generated.	Alarms	Currently, there is no workaround.
SW-103866	When an SR policy goes into down state, an alarm will not be triggered and will not populate the `active alarms list`. Only a system event will be generated.	Alarms	Currently, there is no workaround.

Issue ID	Description	Component	Solution
SW-103172	ISIS maximum routes limit and threshold alarms will not be triggered and will not populate the `active alarms list`. Only a system event would be generated.	Alarms	Currently, there is no workaround.
SW-102541	The RADIUS_SERVER_STATE_CHANGE_NOT_AVAILABLE alarm will not be triggered when connectivity to the Radius server is lost. Only a system event will be generated.	Alarms	Will be fixed in 18.2
SW-77147	On rare occasions, when executing the `show bfd sessions` 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-100903	Traffic over IPv6 routes with IPv4 Next-Hop is not supported.	BGP	Currently, there is no workaround.
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-48206	When an unreachable NTP server is present, disabling the management interface (lo0) might cause the show system NTP command to return an error. NTP functionality is not affected.	CLI	Currently, there is no workaround.

Issue ID	Description	Component	Solution
SW-21067	Running the command `show interface ctrl-ncm-x` displays an 'uptime' value of 0. There is no impact on the system. It is a CLI display issue.	CLI	You can view the interface uptime value via the StrataX operation system, using the `run start shell ncm X` command.
SW-89997	The default value of a double-tagged sub-interface is 0x88a8 for the outer tag and 0x8100 for the inner tag. Therefore, the default TPID value has been removed and is now written by the datapath behind the scenes. Making it seem like the TPID is configured manually.	Datapath	Currently, there is no workaround.
SW-22899	Failure of the standby NCC might cause the active ssh session to be inaccessible for about two minutes.	High Availability	Currently, there is no workaround.
SW-98773	Received ARP message in the bridge-domain, with a dst-mac of the IRB, is flooded to the bridge-domain's attachment circuits (as well as being punted to the CPU as needed).	Interfaces	Currently, there is no workaround.
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	If the management interface is disabled, the uptime of the interface can be ignored.
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	Interfaces	Currently, there is no workaround.

Issue ID	Description	Component	Solution
	mimic admin-state disable, and access cannot be regained.		
SW-106244	A router may not be considered as SR / Flex-Algo capable if router capabilities are advertised from a non-0 lsp fragment.	ISIS	Make sure all fragments are scanned for the router capability tlv when providing information to the relevant topology.
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 not valid, there is no way to know if the path to root via the old upstream is still physically valid. Therefore, to avoid long

Issue ID	Description	Component	Solution
			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 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.	LDP	Currently, there is no workaround.
SW-115050	Prefix-list rules are not written to the local and remote accounting log (TACACS), but the prefix-list is modified in the logs.	LOG	Currently, there is no workaround.
SW-42531	Configuring a Syslog server with a hostname and not an IP may cause Syslog messages not to be sent to the server.	LOG	Configure Syslog server with IP address
SW-39013	At scale, when there is a fast log rotation, there may be a mismatch between the log .gz file timestamp and the log timestamps within the file.	LOG	Currently, there is no workaround.
SW-100397	An FTP_SESSION_LIMIT_CLEARED event is wrongly sent when reaching the maximum number of sessions allowed.	Management	Currently, there is no workaround.
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 3. 'rollback 1’ (re-creates interface 'x')	Management	For similar scenarios as above, the proposed workaround is to perform the

Issue ID	Description	Component	Solution
	4. delete interface 'x' 5. commit <<<<< Failure here		commit immediately after the 'rollback' command.
SW-44069	Configured data-connection-timeout value is not strict. The configured value is the minimum amount of time the connection is allowed before being disconnected. The maximum amount of time will not exceed twice the configured value for the data-connection-timeout.	Management	Currently, there is no workaround.
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, and it fails to traceroute MPLS BGP-LU over SR, RCA.	MPLS	Currently, there is no workaround.

Issue ID	Description	Component	Solution
SW-82174	An interop issue with Juniper causes ping MPLS generic to fail.	MPLS	Currently, there is no workaround.
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-96242	The Make Before Break process is aborted if a former primary IIF is chosen as a standby IIF, causing traffic loss of up to 40 seconds.	Multicast	Currently, there is no workaround.
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-108200	In DNOR - Components - Summary - Network, the Out-of-Band and In-band IPv6 statuses are not properly displayed.	NCE Management	Currently, there is no workaround.
SW-106817	Revert operation pre-check test falsely fails when pre-checking SW revert from version 18 to version 17.2. The revert operation is still successful, although the pre-check test fails.	None	Currently, there is no workaround.
SW-104888	In case of a misconfiguration with two static routes using each other as a solution, and one of them having an additional ECMP nexthop	None	Fix the static route configuration

Issue ID	Description	Component	Solution
	with a valid solution, the RIB-Manager will keep endlessly updating these routes and installing them.		so that they don't point to each other.
SW-104759	Mellanox cards from HP with interfaces configured to work in InfiniBand mode (default mode) are not supported	None	Manually configure the interface to Ethernet.
SW-100375	The actual limitation is per physical when configuring an interface shaper for a bundle. If the limitation is below 2.6G, it will limit it to 2.6G (min shaper for physical).	None	Currently, there is no workaround.
SW-101775	The login prompt is different based on how you try to connect, console, ssh-tacacs, ssh-local-users, ssh-radius	None	Currently, there is no workaround.
SW-106267	When OSPFv2 is configured with `max-metric router-lsa on-startup` and the user removes the entire OSPF configuration and performs a rollback, max-metric will not be sent at startup, although it is enabled in the CLI. When `max-metric router-lsa on-startup` function is enabled, and the user removes the entire OSPF configuration, then re-apply the configuration manually (not via rollback), the `max-metric router-lsa on-startup` function becomes active immediately, even if you did not restart the device.	OSPF	Remove the entire OSPF configuration again and commit. Then do rollback 1 and commit. After this, manually add the 'max-metric knob' and commit. When this happens, remove the 'max-metric knob' and add it manually or via rollback.

Issue ID	Description	Component	Solution
SW-105104	Configuring a new md5 key and removing an existing key in the same commit, results in removing only the existing key	OSPF	1. Remove the md5 key and commit 2. Add the new key and commit.
SW-79291	During a DNOS upgrade, the cluster fabric-type configuration is reset to its default values. This might lead to traffic forwarding errors if the fabric-type configuration does not match the installed fabric cable type.	Platform	Following an upgrade, apply the correct fabric-type configuration according to the installed fabric cables and perform a system restart.
SW-97959	The `show QoS interfaces` command shows a wrong value for high-priority rates when an egress policy is attached to a 100G breakout interface that originated from a 400G interface.	QOS	Currently, there is no workaround.
SW-48083	The MSS for BGP sessions that are established via RSVP tunnels, is lower than the egress interface MTU. This happens when communication from the Linux host that's supposed to egress via an RSVP tunnel is not sent directly via the egress interface, because these types of routes are not installed in Linux. Instead, a tunnel interface is used that has the MTU set to a higher value than the maximum possible MTU on the real interface, which constantly triggers the PL-PMTU. When BGP sends big packets they get discarded and retransmitted by a Linux IP stack with a lower segment size.	RSVP	Currently, there is no workaround.

Issue ID	Description	Component	Solution
SW-21257	RSVP Node-bypass tunnels may be routed via a tunnel's tail node. There is no impact to traffic. The RSVP tunnel route might be sub-optimal.	RSVP	Currently, there is no workaround.
SW-107318	When a Flex-Algo is configured with TE constraints, Cisco routers prefer to reach a specific destination on the higher-cost path through Cisco routers instead of a lower-cost path through DNOS routers. According to RFC 8919, DNOS advertises its TE link attributes in ISIS reachability with the legacy sub-TLVs. In addition, DNOS advertises Application-Specific Link Attributes (ASLA) sub-TLV with the Legacy flag (L-flag) set. This informs other routers to take the TE attributes from the legacy TLVs, not the ASLA. Cisco routers ignore this flag. This leads Cisco routers to exclude DNOS routers from the Flex-Algo topology and the Cisco view. This behavior doesn't happen when the metric type for Flex-Algo is set to IGP.	Segment Routing	From v18.1, DNOS starts advertising its TE attributes inside the ASLA sub-TLVs with the L-flag not set.
SW-82474	The `run traceroute mpls nil-fec` command fails when using binding-sid labels because the binding-sid is not known to the OAM process.	Segment Routing	Currently, there is no workaround.
SW-98421	A static route that is resolved by an imported L3VPN BGP route stays inactive.	Static Route	Currently, there is no workaround.
SW-101494	Telnet is not sending TELNET_SESSION_LOGIN_FAILED event on a cluster. The standalone event is sent properly.	TELNET	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	User Management	Currently, there is no workaround.

Issue ID	Description	Component	Solution
	enters hold-down for the configured hold-down period (default 10 min).		
SW-112563	In L2- service-enabled interfaces, the displayed TX rate may be inaccurate by a margin of 5%.	White Box	Currently, there is no workaround.
SW-110188	The signal integrity parameters were not set correctly on the INPHI gearbox. This meant that the link quality between GB -->J2 and GB-->TRNCVR was insufficient, which might have caused port-link stability issues and/or packet corruption (CRC).	White Box	Fix was provided in the delivered version. When configuring the FEC, reset to the SI parameters was not performed.
SW-109506	Due to a hardware issue, the reference clock to the data path ASICS of the DNI NCP-40C is not accurate. There was a missing script to update the reference clock.	White Box	DN added a script upon init phase to initialize the reference clock.
SW-108935	Disabling or enabling l2-service on an existing interface may cause wrong counters.	White Box	For logical interfaces, a possible workaround would be to explicitly delete the interface and re-create it with the l2-service set as enabled/ disabled.

Issue ID	Description	Component	Solution
			for physical interfaces - no known workaround
SW-100056	Due to a BCM issue, there is no enforcement of MTU on flooded traffic sent on an IRB interface.	White Box	Currently, there is no workaround.

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

Issue ID	Description	Component	Solution
			Egress queue pair 3 - default rule only.

Release 18.0.4 - 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	18.0.4.4
CAL	DriveNets Golden Image	18.0.4.4
StrataX	DNOS NCM NOS	1.2.0
Base-OS	Base-OS	2.18042469004
FW and ONIE	Firmware and ONIE bundled packages for all cluster element types (NCC, NCM, NCF and NCP)	18.0.0.1
DNOR	DriveNets Network Orchestrator	18.1.0.7

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

Resolved Issues

Issue ID	Description	Component
SW-124150	The Moni-node process is responsible for collecting periodic resource information of a node. In rare cases, the node's internal network info collection led to a container failure due to a docker resource race-condition.	Monitoring
SW-123284	Changes to the OSPF topology could sometimes trigger RIB updates for all routes that have TI-LFA next-hops, even if there was no actual	OSPF

Issue ID	Description	Component
	change to the routes. This does not cause any traffic loss, but it can cause an insignificant increase in CPU consumption. This could also mislead any user/tool that monitors the RIB route.	

Limitations

Issue ID	Description	Component	Solution
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 impossible to match any fragments (initial, non-initial) of the IPv6 packets.	ACL	Currently, there is no solution, fix, or workaround to overcome this issue.
SW-22552	Only the primary path is used when a route is resolved via a BGP route with LFA.	BGP	Currently, there is no solution, fix, or WA to overcome this issue.
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	Currently, there is no solution, fix, or workaround to overcome this issue.
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 also partially configurable via the network-services hierarchy, although their configuration is done under the top hierarchy. The management VRFs appear to the user	CLI	There is no workaround. The default VRF configuration is not done via the network-services hierarchy but via the top hierarchy. The management VRFs are not configurable, and the user should not attempt to configure them.

Issue ID	Description	Component	Solution
	as configurable, although they are not (by design).		
SW-43391	Up to 10 simultaneous CLI sessions can be supported on a Standalone NCP.	CLI	Currently, there is no solution, fix, or workaround to overcome this issue.
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	Remove the management interface configuration from the routing protocol hierarchy.
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	Apply the `show file tech-support` command when the system reaches its UP state.
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	Currently, there is no solution, fix, or workaround to overcome this issue.
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, a breakout cannot be for some transceivers (e.g., INNOLIGHT 400G T-DP4CNT-N00) configured.	Interfaces	Currently, there is no solution, fix, or workaround to overcome this issue.

Issue ID	Description	Component	Solution
SW-13193	With ISIS on an interface configured with an MTU above 9222, ISIS adjacency cannot be established.	Interfaces	Decrease the interface MTU below 9222.
SW-45496	The ISIS process will crash if more than 1536 ISIS circuits are configured.	ISIS	Currently, there is no solution, fix, or workaround to overcome this issue.
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	Currently, there is no solution, fix, or WA to overcome this issue.
SW-85530	Connection to a remote server using the 'run ssh' command will generate an SSH_SESSION_LOGIN_FAILED system event with the user 'bublik' on the remote server. This is a mock user used to fetch the ssh banner and print to the screen before using the actual ssh credentials provided.	Management	Currently, there is no solution, fix, or workaround to overcome this issue.
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	Currently, there is no solution, fix, or workaround to overcome this issue.
SW-76489	An NCM ONIE upgrade from DriveNets ONIE 2020 onwards is not supported. The reason is that the MU (Multi Updater) uses an old FSCK (File system check) while DriveNets ONIE uses a newer one.	Management	Upgrade to the new ONIE, DN ONIE 2019.06.
SW-42116	System switchover is logged as System failover.	Management	Currently, there is no solution, fix, or workaround to overcome this issue.

Issue ID	Description	Component	Solution
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	Currently, there is no solution, fix, or workaround to overcome this issue.
SW-51282	NTP processes can reset in some scenarios.	NTP	NTP restarts do not affect the system. Timing is unaffected.
SW-77634	Upgrading a DNI-based cluster to v16.2 requires the removal of the NCP configuration. This limitation is applicable 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. Adding or editing the hardware model configuration without removing the NCP configuration first is impossible.	Platform	Remove the NCP configuration prior to the upgrade by using the `no ncp` command. Any other configuration referencing NCP interfaces must also be removed, e.g., protocols interface configuration. You can now complete the upgrade and then reconfigure all the NCPs with the correct AGCXD40S hardware model, by using the command 'system ncp 0 model NCP-40C hw-model AGCXD40S admin-state enabled' and re-adding the removed NCP configuration.
SW-76547	RN1: For low-speed subscribers, there is no differentiation between WRED and Weighted Tail Drop (WTD) thresholds. RN2: There are continuous unexpected tail drops over the WRED max threshold.	QOS	RN1: The minimum queue or threshold size set in the hardware is 125kB. For low-rate subscribers, two different thresholds values configured in temporal units (milliseconds or microseconds) may both be converted to the same minimum value. To keep the

Issue ID	Description	Component	Solution
			differentiation for low-speed subscribers, use the hardware-mapping speed configuration, setting the minimum speed of all traffic below 1gpbs to a speed of 1gpbs. This is the default configuration. RN2: To avoid or minimize continuous tail drops, increase the difference between the max WRED threshold and the queue size. For low-rate queues, use the hardware mapping speed conversion table to avoid setting both to the minimum 125kB queue and threshold sizes. Have at least a 250KB difference between the queue size and the max WRED threshold.
SW-25836	Packet reorder may happen when the same stream contains multiple classes and the QoS policy is not attached.	QOS	Currently, there is no solution, fix, or workaround to overcome this issue.
SW-25352	Multiple egress policies can be created, yet only a single egress policy can be attached.	QOS	Currently, there is no solution, fix, or workaround to overcome this issue.
SW-24214	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.	QOS	Currently, there is no solution, fix, or workaround to overcome this issue.

<table>
<tr><th>Issue ID</th><th>Description</th><th>Component</th><th>Solution</th></tr>
<tr><td></td><td>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>
<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</td><td></td><td></td></tr>
</table>

Issue ID	Description	Component	Solution
	the show commands `show qos interface counters` or `show qos summary` to display the QoS summary table.		
SW-23773	Egress match counters count the ingress (not the egress) packet bytes, including Ethernet and other terminated layers.	QOS	Currently, there is no solution, fix, or WA to overcome this issue.
SW-23072	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.	User Management	Currently, there is no solution, fix, or WA to overcome this issue.

Known Issues

Issue ID	Description	Component	Solution
SW-108546	ISIS maximum routes limit and threshold alarms will not be triggered and will not populate the `active alarms list`. Only a system event would be generated.	Alarms	Currently, there is no workaround.
SW-103870	When LACP goes into down state on an interface, an alarm will not be triggered and will not populate the `active alarms list`. Only a system event will be generated.	Alarms	Currently, there is no workaround.
SW-103866	When an SR policy goes into down state, an alarm will not be triggered and will not	Alarms	Currently, there is no workaround.

Issue ID	Description	Component	Solution
	populate the `active alarms list`. Only a system event will be generated.		
SW-103172	ISIS maximum routes limit and threshold alarms will not be triggered and will not populate the `active alarms list`. Only a system event would be generated.	Alarms	Currently, there is no workaround.
SW-102541	The RADIUS_SERVER_STATE_CHANGE_NOT_AVAILABLE alarm will not be triggered when connectivity to the Radius server is lost. Only a system event will be generated.	Alarms	Will be fixed in 18.2
SW-77147	On rare occasions, when executing the `show bfd sessions` 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-100903	Traffic over IPv6 routes with IPv4 Next-Hop is not supported.	BGP	Currently, there is no workaround.
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-48206	When an unreachable NTP server is present, disabling the management interface (lo0) might cause the show system NTP command to return an error. NTP functionality is not affected.	CLI	Currently, there is no workaround.

Issue ID	Description	Component	Solution
SW-21067	Running the command `show interface ctrl-ncm-x` displays an 'uptime' value of 0. There is no impact on the system. It is a CLI display issue.	CLI	You can view the interface uptime value via the StrataX operation system, using the `run start shell ncm X` command.
SW-89997	The default value of a double-tagged sub-interface is 0x88a8 for the outer tag and 0x8100 for the inner tag. Therefore, the default TPID value has been removed and is now written by the datapath behind the scenes. Making it seem like the TPID is configured manually.	Datapath	Currently, there is no workaround.
SW-22899	Failure of the standby NCC might cause the active ssh session to be inaccessible for about two minutes.	High Availability	Currently, there is no workaround.
SW-98773	Received ARP message in the bridge-domain, with a dst-mac of the IRB, is flooded to the bridge-domain's attachment circuits (as well as being punted to the CPU as needed).	Interfaces	Currently, there is no workaround.
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	If the management interface is disabled, the uptime of the interface can be ignored.
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	Interfaces	Currently, there is no workaround.

Issue ID	Description	Component	Solution
	mimic admin-state disable, and access cannot be regained.		
SW-106244	A router may not be considered as SR / Flex-Algo capable if router capabilities are advertised from a non-0 lsp fragment.	ISIS	Make sure all fragments are scanned for the router capability tlv when providing information to the relevant topology.
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 not valid, there is no way to know if the path to root via the old upstream is still physically valid. Therefore, to avoid long

Issue ID	Description	Component	Solution
			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 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.	LDP	Currently, there is no workaround.
SW-115050	Prefix-list rules are not written to the local and remote accounting log (TACACS), but the prefix-list is modified in the logs.	LOG	Currently, there is no workaround.
SW-42531	Configuring a Syslog server with a hostname and not an IP may cause Syslog messages not to be sent to the server.	LOG	Configure Syslog server with IP address
SW-39013	At scale, when there is a fast log rotation, there may be a mismatch between the log .gz file timestamp and the log timestamps within the file.	LOG	Currently, there is no workaround.
SW-100397	An FTP_SESSION_LIMIT_CLEARED event is wrongly sent when reaching the maximum number of sessions allowed.	Management	Currently, there is no workaround.
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 3. 'rollback 1’ (re-creates interface 'x')	Management	For similar scenarios as above, the proposed workaround is to perform the

Issue ID	Description	Component	Solution
	4. delete interface 'x' 5. commit <<<<< Failure here		commit immediately after the 'rollback' command.
SW-44069	Configured data-connection-timeout value is not strict. The configured value is the minimum amount of time the connection is allowed before being disconnected. The maximum amount of time will not exceed twice the configured value for the data-connection-timeout.	Management	Currently, there is no workaround.
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, and it fails to traceroute MPLS BGP-LU over SR, RCA.	MPLS	Currently, there is no workaround.

Issue ID	Description	Component	Solution
SW-82174	An interop issue with Juniper causes ping MPLS generic to fail.	MPLS	Currently, there is no workaround.
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-96242	The Make Before Break process is aborted if a former primary IIF is chosen as a standby IIF, causing traffic loss of up to 40 seconds.	Multicast	Currently, there is no workaround.
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-108200	In DNOR - Components - Summary - Network, the Out-of-Band and In-band IPv6 statuses are not properly displayed.	NCE Management	Currently, there is no workaround.
SW-106817	Revert operation pre-check test falsely fails when pre-checking SW revert from version 18 to version 17.2. The revert operation is still successful, although the pre-check test fails.	None	Currently, there is no workaround.
SW-104888	In case of a misconfiguration with two static routes using each other as a solution, and one of them having an additional ECMP nexthop	None	Fix the static route configuration

Issue ID	Description	Component	Solution
	with a valid solution, the RIB-Manager will keep endlessly updating these routes and installing them.		so that they don't point to each other.
SW-104759	Mellanox cards from HP with interfaces configured to work in InfiniBand mode (default mode) are not supported	None	Manually configure the interface to Ethernet.
SW-100375	The actual limitation is per physical when configuring an interface shaper for a bundle. If the limitation is below 2.6G, it will limit it to 2.6G (min shaper for physical).	None	Currently, there is no workaround.
SW-101775	The login prompt is different based on how you try to connect, console, ssh-tacacs, ssh-local-users, ssh-radius	None	Currently, there is no workaround.
SW-109997	Configuring strict-SPF SIDs on some SR nodes while other SR nodes don't have strict-SPF enabled may result in invalid TI-LFA solutions. More specifically, the backup path for some routes might contain strict-SPF labels which are dropped by an SR node along the path, resulting in traffic loss (if and when the backup path is activated).	OSPF	If TI-LFA is enabled for OSPFv2, do not configure strict-SPF SIDs in the network unless strict-SPF is enabled on all SR nodes.
SW-106267	When OSPFv2 is configured with `max-metric router-lsa on-startup` and the user removes the entire OSPF configuration and performs a rollback, max-metric will not be sent at startup, although it is enabled in the CLI. When `max-metric router-lsa on-startup` function is enabled, and the user removes the entire OSPF configuration, then	OSPF	Remove the entire OSPF configuration again and commit. Then do rollback 1 and commit. After this, manually add the ‘max-

Issue ID	Description	Component	Solution
	re-apply the configuration manually (not via rollback), the `max-metric router-lsa on-startup` function becomes active immediately, even if you did not restart the device.		metric knob' and commit. When this happens, remove the 'max-metric knob' and add it manually or via rollback.
SW-105104	Configuring a new md5 key and removing an existing key in the same commit, results in removing only the existing key	OSPF	1. Remove the md5 key and commit 2. Add the new key and commit.
SW-79291	During a DNOS upgrade, the cluster fabric-type configuration is reset to its default values. This might lead to traffic forwarding errors if the fabric-type configuration does not match the installed fabric cable type.	Platform	Following an upgrade, apply the correct fabric-type configuration according to the installed fabric cables and perform a system restart.
SW-97959	The `show QoS interfaces` command shows a wrong value for high-priority rates when an egress policy is attached to a 100G breakout interface that originated from a 400G interface.	QOS	Currently, there is no workaround.
SW-48083	The MSS for BGP sessions that are established via RSVP tunnels, is lower than the egress interface MTU. This happens when communication from the Linux host that's	RSVP	Currently, there is no workaround.

Issue ID	Description	Component	Solution
	supposed to egress via an RSVP tunnel is not sent directly via the egress interface, because these types of routes are not installed in Linux. Instead, a tunnel interface is used that has the MTU set to a higher value than the maximum possible MTU on the real interface, which constantly triggers the PL-PMTU. When BGP sends big packets they get discarded and retransmitted by a Linux IP stack with a lower segment size.		
SW-21257	RSVP Node-bypass tunnels may be routed via a tunnel's tail node. There is no impact to traffic. The RSVP tunnel route might be sub-optimal.	RSVP	Currently, there is no workaround.
SW-107318	When a Flex-Algo is configured with TE constraints, Cisco routers prefer to reach a specific destination on the higher-cost path through Cisco routers instead of a lower-cost path through DNOS routers. According to RFC 8919, DNOS advertises its TE link attributes in ISIS reachability with the legacy sub-TLVs. In addition, DNOS advertises Application-Specific Link Attributes (ASLA) sub-TLV with the Legacy flag (L-flag) set. This informs other routers to take the TE attributes from the legacy TLVs, not the ASLA. Cisco routers ignore this flag. This leads Cisco routers to exclude DNOS routers from the Flex-Algo topology and the Cisco view. This behavior doesn't happen when the metric type for Flex-Algo is set to IGP.	Segment Routing	From v18.1, DNOS starts advertising its TE attributes inside the ASLA sub-TLVs with the L-flag not set.
SW-82474	The `run traceroute mpls nil-fec` command fails when using binding-sid labels because the binding-sid is not known to the OAM process.	Segment Routing	Currently, there is no workaround.

Issue ID	Description	Component	Solution
SW-98421	A static route that is resolved by an imported L3VPN BGP route stays inactive.	Static Route	Currently, there is no workaround.
SW-101494	Telnet is not sending TELNET_SESSION_LOGIN_FAILED event on a cluster. The standalone event is sent properly.	TELNET	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-112563	In L2- service-enabled interfaces, the displayed TX rate may be inaccurate by a margin of 5%.	White Box	Currently, there is no workaround.
SW-110188	The signal integrity parameters were not set correctly on the INPHI gearbox. This meant that the link quality between GB -->J2 and GB-->TRNCVR was insufficient, which might have caused port-link stability issues and/or packet corruption (CRC).	White Box	Fix was provided in the delivered version. When configuring the FEC, reset to the SI parameters was not performed.
SW-109506	Due to a hardware issue, the reference clock to the data path ASICS of the DNI NCP-40C is not accurate. There was a missing script to update the reference clock.	White Box	DN added a script upon init phase to initialize the reference clock.

Issue ID	Description	Component	Solution
SW-108935	Disabling or enabling l2-service on an existing interface may cause wrong counters.	White Box	For logical interfaces, a possible workaround would be to explicitly delete the interface and re-create it with the l2-service set as enabled/ disabled. for physical interfaces - no known workaround
SW-100056	Due to a BCM issue, there is no enforcement of MTU on flooded traffic sent on an IRB interface.	White Box	Currently, there is no workaround.

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	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.

Issue ID	Description	Component	Solution
	used them have been deleted. When a 9th rule is configured, the rule is expanded in the KBP and may exhaust the KBP resources.		
SW-84538	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.

Documentation Highlights

- Go to https://docs.drivenets.com.
- Select Library from the top menu
- Select the 18.0 version filter on the left pane

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