DRIVENETS®

DNOS Release Notes

Downloaded: September 19, 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	18.1.0.29
CAL	DriveNets Golden Image	18.1.0.29
StrataX	DNOS NCM NOS	1.2.0
Base-OS	Base-OS	2.18101891028
FW and ONIE	DNOS NCM FW and ONIE Bundle	18.0.0.5
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.

BGP Automated-Steering over ISIS-SR Flex-Algo

BGP Automated-Steering over Flex-Algo is now supported for BGP IPv4 NH and IPv6 NH. BGP routes are automatically steered over Flex-Algo by the Color extended communities attached to them. If a received BGP route has a color extended community with a value equal to a color associated with a specific Flex-Algo, it will be resolved through the specific Algo's topology.

DNOS supports an optional configuration of Color value to a local Flex-algo value. Once configured, Flex-Algo routes will be installed in the matching `Color-MPLS-NH` table (Colored label RIB) or `Color-mpls-nh-ipv6` table if the associated prefix is an IPv6 prefix. This allows for BGP Automated steering of colored routes over Flex-Algo.

Note that if color is not locally associated with a Flex-Algo, Flex-Algo routes will only be installed to the ILM table (Label FIB) for label-switching purposes. This is suitable for core routers, for example, which are not participating in BGP, and only participate in the Flex-Algo topology.

Colored BGP routes are resolved over the Color-MPLS-NH and `Color-MPLS-NH` table, matching the received color extended community value, as follows:

Find a resolution to the BGP Next-Hop in the `Color-MPLS-NH` / `Color-MPLS-NH-ipv6` table. This table can be populated by either SR-TE policies or by Flex-Algo (Flex-Algo can only populate the color-mpls-nh-ipv6 table). If both are present, the administrative distance will be the tiebreaker.

If no match is found, resolve in the mpls-nh/mpls-nh-ipv6 (algo 0) table.

If the no-fallback flag is set, steps 2 and 3 will be skipped, and the route will be installed, pointing to null0. Traffic will be dropped.

If no match is found, the route will not be installed (If it is a BGP MPLS route).

If the received BGP route is an IPv4/6 unicast, then the last additional step would be to resolve the BGP NH over the IPv4/6 routing table.

ISIS IPv6-Unicast Traffic-Engineering Extensions

Traffic Engineering extensions are now supported on ISIS IPv6-Unicast topology.

To enable IPv6 traffic engineering extensions on ISIS, enable the IPv6-Unicast topology (MT ID 2) with the `protocols isis instance address-family ipv6-unicast` command, and enable traffic-engineering under address-family IPv6-unicast with the `traffic-engineering enabled` command.

When enabled, the following information will be advertised in their corresponding TLVs and Sub-TLVS:

IPv6-Router-ID (TLV 140)

Admin-group (TLV 222)

Extended admin-group (TLV 222)

SRLG (TLV 139)

Link-delay parameters (TLV 222)

Application-Specific Link attributes (ASLA) sub-TLV 16 (TLV 222) when Flex-Algo is enabled on the ISIS instance.

ISIS IPv6 Dynamic Link Delay Measurement and Advertisement

Dynamic link delay is calculated by Simple-TWAMP (STAMP) link delay sessions, which are now supported over IPv6 links. On a given interface/sub-interface, either an IPv4 Simple-TWAMP session or an IPv6 Simple-TWAMP session can be enabled. Either of the sessions' link delay results will feed the ISIS Single-Topology or the ISIS Multi-Topology, for both IPv4 and IPv6 topologies. Link delay parameters are advertised under TLV 22 for IPv4 topology, TLV 222 for IPv6 topology, and in ASLA sub-TLV, if enabled in ISIS and Flex-Algo is configured. The supported parameters are Min/Max unidirectional link delay, average link delay, and unidirectional delay variation. ISIS delay normalization is also supported now for IPv6 interfaces under the ISIS configuration.

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` command to view the measured link delay values.

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

ISIS-SR IPv6 Multi-topology Flex-Algo

Flex-Algo IPv6-unicast in Multi-topology has been added to ISIS SR-MPLS. So far, only IPv4-unicast topology and prefixes were supported over ISIS SR-MPLS.

Flex-Algo allows for IGP constraint-based computations and creates separate IGP algorithms according to the defined 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 provide ECMP within the Flex-Algo topology natively, and the ability to minimize the Segment-Routing label stack, opposed 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 and IPv6-unicast Multi-topology

Supported over ISIS SR-MPLS infrastructure only

Flex-Algo participation

Flex-Algo definition advertisement

Support for the following constraints:

Include any/all admin-groups

Exclude any/all admin-groups

Exclude SRLG

Support for the following Metric types:

Minimum IGP metric

Minimum TE metric

Minimum Delay metric

Support advertisement of the above TE parameters in legacy TE TLVs and in ASLA sub-TLV

Supports TI-LFA and Micro-loop avoidance on per Algo, per topology

Supports SRLG-disjoint TI-LFA protection

Support BGP automated steering for BGP IPv4 NH and IPv6 NH over Flex-Algo, by supporting 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) for IPv4 prefix-sids, or in the Color-MPLS-NH-Ipv6 table, for IPv6 prefix-sids. This allows for BGP automated steering of the colored BGP routes to Flex-Algo resolution. 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/Color-MPLS-NH-IPv6, which will enforce that if a colored BGP route does not have a Flex-Algo resolution in the matching Color-MPLS-NH/Color-MPLS-NH-IPv6 table, traffic will not fallback to Algo 0 (MPLS-NH/MPLS-NH-IPv6 - 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.

MicroLoop Avoidance for ISIS address-family IPv6

MicroLoop avoidance was previously only supported on ISIS address-family IPv4. It is now supported on ISIS address-family Ipv6 over an SR-MPLS IPv6 infrastructure. DNOS supports MicroLoop avoidance for Algo 0 and each Flex-Algo topology.

If nodes converge following a change in the network topology change (link down, link up, or metric change events), and they send traffic to neighbor nodes that have not yet converged, packets may briefly loop between the two nodes until the network fully converges. These micro-loops may result in packet loss, jitter, and disordered packets. With segment routing micro-loop avoidance enabled, the node will anticipate if a micro-loop could occur on the new topology and avoid it by creating a temporary loop-free SR-TE policy path to the destination using the list of segment IDs. The policy reverts to the regular forwarding path when the fib-delay timer expires, giving the network enough time to converge fully.

To use segment routing micro-loop avoidance, enable micro-loop avoidance under the `protocols isis <instance-name> address-family` command hierarchy. Use the fib-delay parameter to control how long the system will use micro-loop avoidance before updating the forwarding table. Use maximum-labels to define the maximum number of labels used.

MicroLoop Avoidance for Segment Routing

When there is a change in the network topology (e.g., link down, link up, or metric change events), nodes may converge and send traffic to neighbor nodes that have not yet converged. This may cause packets to loop briefly between the nodes until the network fully converges, resulting in micro-loops. These micro-loops may result in packet loss, jitter, and disordered packets.

When segment routing micro-loop avoidance is enabled, the node can predict the possibility of a micro-loop in the new topology and prevent it by creating a temporary loop-free SR-TE policy path to the destination using the list of segment IDs. When the fib-delay timer expires, the policy reverts to the regular forwarding path, allowing the network enough time to converge fully.

To use segment routing micro-loop avoidance, enable `microloop-avoidance` under the `protocols ospf instance <instance-name>` command hierarchy. Use the `fib-delay` parameter to control how long the system will use micro-loop avoidance before updating the forwarding table. Use `maximum-labels` to define the maximum number of labels used.

OSPFv2 Stub and NSSA Areas

Until now, DNOS supported participating in the OSPFv2 backbone area (Area 0) only. We've added support for participating in OSPFv2 non-backbone areas (other than area 0), backbone-area (area 0, in multiple areas - acting as an area border router), and NSSA and stub areas. NSSA and stub are supported both for ABR roles and for non-ABR roles.

Use the protocols ospf instance <name> area <area> nssa command to set an OSPFv2 area as NSSA.

Use the `protocols ospf instance <name> area <area> nssa no-summary` command to set an OSPFv2 area as totally-NSSA.

Use the `protocols ospf instance <name> area <area> stub` command to set an OSPFv2 area as a stub.

Use the `protocols ospf instance <name> area <area> stub no-summary` command to set an OSPFv2 area as a total stub.

OSPFv2 Multiple Areas ABR Capabilities

Until now, DNOS supported participating in the OSPFv2 backbone area (Area 0) only. We've added support for participating in OSPFv2 non-backbone areas (other than area 0), in backbone-area (area 0), and multiple areas, acting as an Area Border Router (ABR). The DNOS-based router will run in OSPFv2 multi-area automatically when the router is configured with at least two OSPF areas under a single OSPF instance.

The OSPFv2 multi-area support includes support for SR-MPLS by advertising received intra-area SR routes as inter-area SR routes when acting as an ABR.

To configure the OSPF multiple areas, use the `protocols ospf instance <name> area <area>` command.

To advertise aggregated routes to relax the scale of inter-area prefixes, use the `protocols ospf instance <name> area <area> aggregate-route` command. Use the optional `summary-only` CLI flag alongside aggregate-route to not advertise contributing routes (inter-area prefixes) and just advertise the configured aggregated route/s.

To modify certain summarized (LSA type 3) routes metric, or filter specific prefixes from being advertised as inter-area routes, use the `protocols ospf instance <name> area <area> summarization-policy <policy-name>` command.

To disable segment-routing on a specific area, use the `protocols ospf instance <name> area <area> segment-routing disabled` command.

OSPFv2 Multi Instances Support

OSPFv2 now allows configuring multi-instances. You can create multiple OSPFv2 instances, each operating as a separate IGP domain. However, connectivity between instances can only be achieved using MPLS with BGP-LU, as native IP leaking between instances is impossible.

To configure multi-instances of OSPFv2, use the `protocols ospf instance <text>` configuration command.

To view each OSPFv2 instance information, use the `show ospf <instance>` show command

BGP Segment-Routing Prefix-SID

The BGP Prefix-SID Redistribution feature allows advertising IPv4 and IPv6 BGP Prefix-SID for SR-MPLS IPv4/IPv6-based networks. It is now possible for BGP to carry the association of an SR-MPLS Node-SID index with an IPv4/IPv6 prefix. This is achieved by attaching a prefix-SID BGP path attribute containing the label-index value to an IPv4/IPv6 route belonging to either IPv4-LU or IPv6-LU address family.

To enable support for BGP Prefix-SID (RFC 8669) for labeled-unicast sub-address-family, use the prefix-sid enabled command under the `protocols bgp address-family <ipv4-unicast / ipv6-unicast> labeled-unicast` command hierarchy. This will instruct BGP to locally allocate and assign a label from the Segment-Routing Global Block according to the received prefix's Label-Index attribute.

To advertise a label-index value, use the `set sr-label-index` command under the `routing-policy rule allow` a hierarchy of the routing-policy attached to the `redistribute` command under protocols bgp <as-num> address-family ipv4-unicast or protocols bgp <as-num> address-family ipv6-unicast, or to the network command under these AFI/SAFI. Another option is to attach it to the in policy direction of the neighbor-group/neighbor

on the IPv4/IPv6-unicast AFI/SAFI level. Use the optional `global-block-origination` command with the set sr-label-index command to add the Originator SRGB TLV (with a value equal to local SRGB) for the Prefix-SID attribute.

To allow usage of BGP prefix-sid on eBGP adjacencies, use the `allow-external-sid` command, and set the required behavior - <send-only/receive-only/send-receive/disabled>. The `allow-external-sid` command is located under `protocols bgp neighbor address-family <ipv4-unicast / ipv6-unicast> sr-labeled-unicast` or `protocols bgp neighbor-group address-family <ipv4-unicast / ipv6-unicast> sr-labeled-unicast`. This command controls the BGP prefix-SID usage on eBGP sessions between different Autonomous Systems, as required by RFC 8669.

Revised Error Handling for BGP

RFC 7606 introduces new error handling capabilities for BGP routing that minimize the impact on routing by a malformed UPDATE message while still fully maintaining protocol correctness. The RFC enables BGP speakers to detect and remove the routes carried in the malformed UPDATE message from the routing system without resetting the session over which the offending attribute was received; this new capability significantly improves the reliability and security of the BGP protocol.

RSVP WECMP

Equal-cost multi-path routing (ECMP) is a routing strategy in DNOS where Next-Hop packet forwarding to a single destination can occur over multiple best paths, which tie for the top place in routing metric calculations. Weighted Equal Cost Multipath (WECMP) for Resource Reservation Protocol (RSVP), an enhancement of ECMP, allows RSVP traffic to be distributed across multiple tunnels with differing weights based on tunnel bandwidth, providing greater flexibility in load balancing and ensuring that traffic is distributed across available paths.

To display the tunnel weight, use the `show rsvp tunnel` command. To display the tunnel path weight, use the `show route` command.

To enable weighted ECMP for TE tunnel forwarding, use the `protocols mpls traffic-engineering load-balancing` command.

To set the tunnel weight for unequal load-balancing when working with WECMP, use the `protocols rsvp auto-mesh` command.

ISIS WECMP

Equal-cost multi-path routing (ECMP) is a routing strategy in DNOS where Next-Hop packet forwarding to a single destination can occur over multiple best paths, which tie for the top place in routing metric calculations. Weighted ECMP (Equal Cost Multi-Path) routing in ISIS (Intermediate System to Intermediate System) protocol is an enhancement of ECMP. With ISIS WECMP, network operators can now distribute traffic across multiple paths with different weights, providing more efficient use of network resources and improved load balancing.

This feature is handy for large-scale networks that require high availability and redundancy. In ISIS WECMP, traffic is weighted according to the ISIS interface weight, where the default weight is the metric divided by 1G. Network operators can easily configure the desired weights for each available path based on their network requirements.

To display the ISIS-enabled interface bandwidth or weight, use the `show isis interfaces` command. You can also use the `show isis route` command to display the ISIS route path weights.

To enable and set the interface weight for weighted ECMP forwarding, use the `protocols isis instance interface address-family <ipv4/ipv6-unicast>` command.

SRLG Protection in Segment-Routing TI-LFA

Configuring Shared Risk Link Group (SRLG) protection in TI-LFA Fast-reroute for segment routing is now supported.

This allows for a fast reroute backup path that shares no common SRLG with the protected (primary) path.

Links with the same SRLG configuration typically share a common fiber, meaning they may fail if the fiber breaks.

TI-LFA SRLG-disjoint protection attempts to find a backup path that excludes the SRLG of the protected path.

All links of the protected path that share any SRLG with the candidate backup paths are excluded.

To configure SRLG-disjoint, use the `protection-mode level <level-1, level-2, level-1-2> <node,link> srlg-disjoint` command under the isis instance address-family ti-fast-reroute hierarchy.

Assuming srlg-mode strict is not configured when set with protection-mode = link, the preference of protection path will be:

Find a protection path that provides both srlg-disjoint and link protection.

If no path is found, find a protection path that provides link protection.

Assuming srlg-mode strict is not configured when set with protection-mode = node, protection path preference will be:

Find a protection path that provides both srlg-disjoint and node protection.

If no path is found, find a protection path that provides node protection.

If no path is found, find a protection path that provides both srlg-disjoint and link protection.

If no path is found, find a protection path that provides link protection.

To prefer SRLG protection over node protection, use the srlg-over-node enabled command under the isis instance address-family ti-fast-reroute hierarchy.

Assuming srlg-mode strict is not configured, the protection path preference will be:

Find a protection path that provides both srlg-disjoint and node protection.

If no path is found, find a protection path that provides both srlg-disjoint and link protection.

If no path is found, find a protection path that provides node protection.

If no path is found, find a protection path that provides link protection.

To set SRLG protection as mandatory, with no fallback to non-SRLG-disjoint protection, use the srlg-mode strict command, under the isis instance address-family ti-fast-reroute hierarchy.

When set, the above protection path order will also exclude all steps that don't include an SRLG protection.

BGP Support for Redistributing a Specific OSPFv2 Instance

It is now possible to specify the OSPFv2 instance you want to configure. Instead of BGP redistributing the entire OSPFv2 database.

To redistribute a specific OSPFv2 instance, use the `protocols bgp <as> address-family ipv4-unicast redistribute ospf instance <instance name>` command.

OSPF metric and a routing policy can be applied upon redistribution using the following commands:

```
protocols bgp <as> address-family ipv4-unicast redistribute ospf instance <instance name> metric <metric value>
```

```
protocols bgp <as> address-family ipv4-unicast redistribute ospf instance <instance name> policy <policy 1>, <policy 2>
```

OSPFv2 Route Scale - 32k

OSPFv2 can now contain 32000 routes in an LS database to cater to larger-scale networks. Previously it could only contain 9000 routes.

BGP RR - Multiple Clusters IDs

Previously in hierarchical Route Reflector (RR) implementations, a device could only have a single, global cluster-ID. Now RR clients can have multiple cluster IDs: a global cluster-ID and additional cluster IDs that are assigned to clients (neighbors).

To configure the cluster ID, use the CLI configuration commands under the BGP hierarchy. To display information on BGP neighbor connections, use `show bgp neighbors` CLI show command.

OSPFv2 Node Scale - 2k

OSPFv2 can now contain 2000 nodes in an LS database to cater to larger-scale networks. Previously it could only contain 1200 nodes.

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.

Ping and Traceroute NETCONF RPC

Operators can now use ping and traceroute NETCONF RPC to automate network operations and troubleshooting. With Ping RPC, you can now test the reachability of network devices and diagnose connectivity issues. At the same time, the Trace RPC enables you to trace the path packets taken through the network and identify potential points of failure. Both features are implemented as standard NETCONF operations and can be accessed using any NETCONF client.

Interface Traffic Utilization Threshold Alerts

DNOS can now generate SNMP trap notifications, and system events, for utilization threshold crossing of physical network interfaces and physical fabric interfaces on the NCP (NIF, FIF). Interface utilization is calculated separately for input and output directions (Rx/Tx), and the threshold applies to both rates independently. By default, the NIF and FIF utilization traps should be triggered if the utilization rate reaches 100%. To avoid thrashing, event clearing occurs when the utilization value gets below the threshold value minus 2% (i.e., 97% for default values).

Note: Both system events and SNMP trap notifications will be supported on breakout interfaces. However, SNMP polling of interface utilization Tx and Rx parameters are supported only on physical network interfaces. The interface utilization threshold is not supported on sub-interfaces, only on physical interfaces.

Use the `interfaces <if-name> util-rate-threshold <0-100>` command to configure the utilization threshold.

SNMP Trap for Storage Disk Failures

To improve the SNMP traps for hardware failure so they are equivalent to the Syslog, a new SNMP trap for the PLATFORM_DISK_FAILED system event was added. The new SNMP trap's name is dnHwMonDiskFailed. The MIB file name is DRIVENETS-HWMON-MIB.mib This trap applies to NCP/NCF and NCC platforms.

SNMP Traps for CPU and Memory Utilization

Previously, DNOS could only generate CPU and memory threshold crossing events with a fixed threshold value of 90% utilization. Now DNOS allows configuring thresholds in CPU and memory utilization and can generate SNMP traps when these thresholds are crossed. This feature is now available in NCP, NCF, and NCC.

Use the configure `system ncp 0 max-mem-util-threshold <percentage>` CLI command to define the memory utilization threshold parameter.

Use the configure `system ncp 0 max-cpu-util-threshold <percentage>` CLI command to define the CPU utilization threshold parameter.

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 meet their specific needs better. 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.

Tracking-policy

In a dual-homed Customer Edge – Provider Edge (CE-PE) connection, A CE device is connected to more than one PE for redundancy; in such cases, core failures must be transmitted to the CE, which results in service protection on the CE level. A tracking policy tracks objects and performs predefined actions upon failure/threshold crossing. A network operator can define a single/group of objects to track using a tracking policy and bind this policy to an action. Now, the user can track a core interface and, upon failure, take the CE-facing interface; this will allow a multihomed CE to move the secondary PE once all links on the primary PE fail.

Synchronous Ethernet (Sync-E) on NCP- 64X12C-S

The Standalone NCP-64X12C-S (aka NCP-Light) now incorporates Synchronous Ethernet (Sync-E) technology. This is a physical layer technology that operates regardless of the network load and supports hop-by-hop frequency transfer, where all interfaces in the path must support Sync-E. It enables delivering synchronization services that meet the requirements of present-day mobile networks. Sync-E is defined in the following ITU-T standards - G.8261, G.8261.1, G.8262, G.8264, supported by DNOS.

To set the interface mode to synchronous or non-synchronous, use the `interface mode` configuration command. To view if an interface is in synchronous or non-synchronous mode, use the `show interfaces detail` command.

QinQ Default TPID Value

The default outer TPID value for OinO interfaces has changed from 0x88a8 to 0x8100. The inner value remains 0x8100. This change improves the user experience for initial configuration and configuration changes.

To configure a sub-interface with QinQ encapsulation (802.1ad double-tagged VLAN), use the `interfaces vlan-tags outer-tag inner-tag` 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.

DNOS Patching Mechanism

DriveNets has added granular DNOS container upgrades that provide a patching mechanism relevant to bug fixes and lower the time needed to fix any sev-1 issues. The patches can either be hot or cold. Hot patches include Management and Control traffic affecting containers (i.e., ME, RE, etc.) that will not have downtime during the patch. Cold patches include Traffic affecting containers (i.e., Datapath and Fabric). In an NCE, there will be up to one patch at a time; if a new patch is required, it will aggregate the previous patch.

Hybrid Fabric Cables and Auto Detect Fabric Cable Type per Port

DriveNets now supports two new capabilities:

Up till now, fabric cables in a cluster had to be the same type. Now you can use mixed-fabric cable types in a cluster. This allows deploying DAC / AEC and AOC fabric cable types in the same cluster, dramatically reducing the HW cost and the cluster's power consumption. For example, CL-32 –

Power comparison: before hybrid (using only the AEC fabric cable) = 7.3kW. After hybrid (using AEC+DAC fabric cables) = 6.6kW (10% reduction).

Cost: before hybrid: 198k$. After hybrid - 191. (3.5% reduction).

The default fabric cable type was defined according to the cluster type during the deployment. The user could also manually select the fabric cable type, and this change would apply to all FIFs. Now the fabric cable type will be detected per port, and if needed, link training will be activated to optimize the SI parameters. The following modifications will be made in the CLI due to this new capability:

config system fabric type - removed.

show system fabric type - removed.

show interface fabric transceiver – auto-detect is added.

To display the list of values and configuration of the fabric interface transceiver, use the `show interface fabric transceiver` command.

ACL-Based QOS Classification

Access Control List (ACL) based Quality of Service (QoS) classification has been added to DNOS. This feature provides network operators the ability to match traffic based on specific criteria such as source and destination IP addresses, ports, and protocols and assign it to a particular Class of Service (COS). This ensures that critical applications receive the necessary bandwidth and network resources. To use the feature, assign an ACL under traffic-class-map as a match statement. Create multiple ACLs and QoS classes to support complex network environments and business requirements. Monitor and analyze network traffic using DNOS comprehensive reporting and analytics tools.

To display the detailed QoS policy attached to a specific interface, use the `show qos interfaces` command.

To configure the seq-qos with which packets matching the rule will be influenced, use the `access-lists rule set-qos` command.

Change nVidia Mellanox Mode from Infiniband to Ethernet by BaseOS

Until now, nVidia Mellanox dual mode (Infiniband / Ethernet) ConnectX-5 NIC and their HPE OEM NIC (HPE PN 872726-B21) arrived with Infiniband as default and required a command to switch them to Ethernet mode. This could have caused a problem with ZTP for NCC1 in a cluster to

receive its configuration through the 100G control port. Now, when installing/upgrading the HPE NCC nodes BaseOS, any HPE nVidia Mellanox NIC that arrives with Infiniband as default will automatically change its mode of operation into Ethernet.

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 knob.

Resolved Issues

Issue ID	Description	Component
SW-103870	When LACP goes into a 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
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
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
SW-106244	A router may not be considered SR / Flex-Algo capable if router capabilities are advertised from a non-0 lsp fragment.	ISIS
SW-100397	An FTP_SESSION_LIMIT_CLEARED event is wrongly sent when reaching the maximum number of sessions allowed.	Management
SW-85530	Connection to a remote server using the run ssh command will generate a SSH_SESSION_LOGIN_FAILED system event with the user 'bublik' on the remote server. This mock user is used to fetch the ssh banner and print to the screen before using the actual ssh credentials provided.	Management
SW-104759	Mellanox cards from HP with interfaces configured to work in InfiniBand mode (default mode) are not supported	None
SW-100375	When configuring an interface shaper for a bundle, the actual limitation is per physical. If the limitation is below 2.6G, it will limit it to 2.6G (min shaper for physical).	None
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.	OSPF

Issue ID	Description	Component
	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.	
SW-105104	Configuring a new md5 key and removing an existing key in the same commit results in removing only the existing key	OSPF
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
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
SW-105009	PW remains stuck in a `remote not ready` state after swapping PW-IDs of 2 VPWS services in one CLI commit	RIB
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
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

Issue ID	Description	Component
SW-109506	Due to a hardware issue, the reference clock to the data path ASICS of the DNI NCP-40C is inaccurate. There was a missing script to update the reference clock.	White Box
SW-100056	Due to a BCM issue, there is no enforcement of MTU on flooded traffic sent on an IRB interface.	White Box

Limitations

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

Issue ID	Description	Component
SW-34870	The interface configuration parameter, mtu-ipv6, affects the IPv4 ping when running the run ping IPv4_ADDR command. This does not affect transit traffic.	ICMP
SW-89325	Only the default application can be used for 400G transceivers supporting multiple applications. For example, a 400G Base-DR4+ transceiver with a default native 400G application may also support breakout to 100G, according to its CMIS data. However, while the transceiver supports breakout and may appear so in DNOS, for some transceivers (e.g., INNOLIGHT 400G T-DP4CNT-N00), a breakout cannot be configured.	Interfaces
SW-13193	With ISIS on an interface configured with an MTU above 9222, ISIS adjacency cannot be established.	Interfaces
SW-45496	The ISIS process will crash if more than 1536 ISIS circuits are configured.	ISIS
SW-23899	The Syslog server list in the show system logging command output is not updated with the configured facility type. There is no impact on the system; it is a CLI display issue.	LOG
SW-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 mock user is used to fetch the ssh banner and print to the screen before using the actual ssh credentials provided.	Management
SW-35900	A static route for an OOB management network can't be configured if a specified Next-Hop interface is in DHCP mode.	Management
SW-107823	Committing complex QoS and ACL 100K config lines causes memory issues.	Management
SW-76489	An NCM ONIE upgrade from DriveNets ONIE 2020 onwards is not supported. The reason for that is that the MU (Multi	NCE Management

Issue ID	Description	Component
	Updater) uses an old FSCK (File system check) while DriveNets ONIE uses a newer one.	
SW-42116	System switchover is logged as System failover.	NCE Management
SW-83003	DNI platforms don't have bit error counters available, and symbol error counters are post-FEC. As a result, the signal degrade and signal failure alarms relying on BER calculation have inherent inaccuracy.	None
SW-109311	The maximum throughput decreases on NCS NAT interfaces if any of the two transceivers used for the management connections to the NCMs are missing or malfunctioning.	None
SW-51282	NTP processes can reset in some scenarios.	NTP
SW-77634	Upgrading a DNI-based cluster to v16.2 requires the removal of the NCP configuration. This limitation applies to DNI clusters only and does not include Standalones. The NCP configuration in v16.2 or higher requires an explicit setting of the NCP hardware model to AGCXD40S (the default is S9700-53DX). If it is not set when the NCP reconnects, the NCP enters safe mode due to misconfiguration. It is not possible to add or edit the hardware model configuration without removing the NCP configuration first.	Platform
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
SW-25836	Packet reorder may happen when the same stream contains multiple classes and the QoS policy is not attached.	QOS

<table>
<tr><th>Issue ID</th><th>Description</th><th>Component</th></tr>
<tr><td>SW-25352</td><td>Multiple egress policies can be created, yet only a single egress policy can be attached.</td><td>QOS</td></tr>
<tr><td>SW-24214</td><td>When enabling EXPLICIT NULL behavior for the LSP, the classification of incoming packets at the tunnel tail-end does not consider the policy set on the ingress port. Rather, it uses a default mapping between the MPLS EXP bits carried in the EXPLICIT NULL label and the qos-tag and drop-tag set.
MPLS packets with EXPLICIT NULL topmost label will be classified according to the fixed table below and therefore will potentially receive different per-hop-behaviors.
exp-null qos-tag drop-tag

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

Issue ID	Description	Component
	To prevent this from happening, disable EXPLICIT NULL using the configuration command rsvp explicit-null under the rsvp hierarchy. To view the QoS interface counters use 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
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

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 will be generated.	Alarms	Currently, there is no workaround.
SW-103866	When an SR policy goes into a 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 will be generated.	Alarms	Currently, there is no workaround.
SW-77147	On rare occasions, when executing the show bfd sessions CLI command, some BFD sessions may appear with an uptime value of -1 day. 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 an IPv4 Next-Hop is not supported.	BGP	Currently, there is no workaround.
SW-113225	In the BGP multi-path installation of a route, if one of the paths has the same Next-Hop as the BEST path, it will be added to the set of Next-Hops installed in the RIB.	BGP	Increase the size of the ECMP group, i.e., the maximum ibgp/ ebgp.

Issue ID	Description	Component	Solution
	This would take a valid path from the ECMP group since the maximum-path number is small.		
SW-108914	In an EVPN afi/safi, if a type-3 IM route is received with a different P-Multicast Service Interface (PMSI) tunnel type than the supported type of ingress replication, it is rejected instead of being ignored/retransmitted.	BGP	Currently, there is no workaround.
SW-110347	BGP ILM routes are not installed with SR-TE policy as the Next-Hop, causing the colors attribute not to impact the BGP-LU routes ILM resolution.	BGP	Currently, there is no workaround.
SW-112452	DNOS CLI allows invalid NAT interface configurations that do not have a VLAN-ID to be committed; they then are not applied.	CLI	Ensure that NAT interfaces have a VLAN-ID defined.
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-113375	Rule routing-policy set Accumulated IGP Metric Attribute (AIGP) settings are displayed twice in the show-config output.	CLI	Currently, there is no workaround.
SW-113263	The user might be unable to delete commands that share the optional parameter 'n' as other commands in the same hierarchy.	CLI	Delete the entire command and not only the optional 'n' parameter.
SW-22899	Failure of the standby NCC might cause the active ssh session inaccessible for about two minutes.	High Availability	Currently, there is no workaround.
SW-111846	After changing the time zone to a non-default one, the time zone change is not applied to the host and some container kernel logs.	INFRA	A patch will be delivered next release.
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	Interfaces	Currently, there is no workaround.

Issue ID	Description	Component	Solution
	disabled. This happens when access to the IPMI interface is disabled to mimic admin-state disable, and access cannot be regained.		
SW-110756	Uloop protection, which protects against loop risk, might not work when working with links that have partially configured address families. For example, both sides of the same link are configured with ipv4 but only one side is configured with ipv6.	ISIS	To prevent this issue, a link must be configured with both address families on both sides or only one address family on both sides.
SW-40860	When changing the number of maximum paths under ISIS, abnormal traffic loss is seen for about 1 second.	ISIS	Currently, there is no workaround.
SW-40847	There is no option to remove summary-only from the ISIS aggregate-route command.	ISIS	Remove the entire aggregate-route and reconfigure it without the summary-only keyword.
SW-86711	MBB is not triggered when an old upstream is no longer one of the valid upstreams.	LDP	When an old upstream is invalid, there is no way to know if the path to root via the old upstream is still physically valid. Therefore, to avoid long traffic loss, a new path is installed immediately.
SW-45541	With a segment-routing-only router, if LDP is preferred, LDP doesn't have a Primary NH to the LER (SR-only router). Therefore, LDP incorrectly installs an alternate-only route towards LSR (SR/LDP router), resulting in a	LDP	Currently, there is no workaround.

Issue ID	Description	Component	Solution
	permanent loop between two LSRs.		
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-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-113605	It is not possible to change the NCE's name via DNOR when AAA is enabled on DNOS. When AAA is enabled, the wrong connection PID is identified while establishing the session, leading to a failure in NETCONF while trying to access non-existent information.	Management	Disable AAA when changing the NCE's name or configure via NETCONF manually.
SW-90599	Very small traffic loss of up to 10ms can be experienced when updating/replacing mpls	MPLS	Currently, there is no workaround.

Issue ID	Description	Component	Solution
	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.		
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 and 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.

Issue ID	Description	Component	Solution
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-112305	The NCS enters safe mode when NAT instances are configured to use Mellanox cards plugged into PCI slots assigned to NUMA 1.	NC-Plus	Connect Mellanox cards to PCI slots assigned to NUMA 0.
SW-113167	Applying configuration while using the NETCONF Get operation might cause the operation to fail.	NETCONF	If the NETCONF Get operation fails, retry it.
SW-107260	Uloop protection, which protects against loop risk, might calculate a strict-spf solution in a node that does not support strict-spf.	None	It is recommended to set all nodes in the topology to support the strict-spf algorithm.
SW-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-105947	Topology-Independent Loop-Free Alternate (TI-LFA) protection using SRLG should be provided per Flex-Algo topology. This does not always occur when working with a Flex Algo environment	None	Currently, there is no workaround.

Issue ID	Description	Component	Solution
	with ASLA advertised and parallel links.		
SW-104888	In case of a misconfiguration with two static routes using each other as a solution, one of them having an additional ECMP Next-Hop with a valid solution, the RIB-Manager will keep endlessly updating these routes and installing them.	None	Fix the static route configuration so they don't point to each other.
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-113499	In OSPFv2 when an Inter-Area Opaque LSA is advertised after a Summary LSA is advertised during an SPF, a small delay between the Summary LSA and the Opaque LSA origination may occur. This may lead to the OSPF neighbors having IP information without SR information for a short time.	OSPF	Currently, there is no workaround.
SW-113331	During a graceful restart, received Opaque LSAs are flushed, and new LSAs for SR-Prefixes and SR-Links are re-originated. This causes the route's neighbors to reinstall SR prefixes and traffic to drop for a few seconds.	OSPF	Currently, there is no workaround.
SW-112410	Changing the router ID while running OSPF on a high scale	OSPF	Clear the OSPF process.

Issue ID	Description	Component	Solution
	may generate the Type 10 Router Information LSA with max-age.		
SW-102335	In the show interfaces command, no output is displayed for the control transceiver for the NCP/NCF because there is a hardware locking issue between the node manager and the datapath.	Platform	Currently, there is no workaround.
SW-111872	In a Flex Algo environment, with TI-LFA as the route's preferred protocol. Following a link failure, the RIB wrongly installs the failed path again before installing the new correct path, resulting in packet loss.	RIB	If SR-TE is the route's preferred protocol, the issue does not occur.
SW-113576	If there are two default routes in the RIB, one static/BGP, another IGP/BGP, and PIM routes are also used, the solution of the default static/BGP route becomes unavailable. This causes the RIB-Manager's memory usage to increase continuously until the solution of the static route is available again or one of the default routes is removed.	RIB	If one of the static routes is static, then a static route with the IP Next-Hop and interface should be used.
SW-48083	The MSS for BGP sessions established via RSVP tunnels is lower than the egress interface MTU. This happens when communication from the Linux host supposed to egress via an RSVP tunnel is not sent directly via the egress interface because these routes are not installed in	RSVP	Currently, there is no workaround.

Issue ID	Description	Component	Solution
	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 on traffic. The RSVP tunnel route might be sub-optimal.	RSVP	Currently, there is no workaround.
SW-112131	Topology-Independent Loop-Free Alternate (TI-LFA) reduces packet loss when routers converge following a topology change due to a link failure. TI-LFA does not work in a Flex Algo environment in some rare conditions, resulting in packet loss.	Segment Routing	Configure an SPF delay of >= 400 msec to overcome the issue.
SW-111100	If there is a topology change when using a PCE path for an SRTE policy, the PCEP path changes forwarding and is removed from the SRTE policy (despite being valid). This causes the SRTE policy to fall back to the configured path.	Segment Routing	To keep the SRTE policy on the PCE path, make the necessary calculations to adjust to the new topology change.
SW-82474	The run traceroute mpls nil-fec command fails when using binding-sid labels because the	Segment Routing	Currently, there is no workaround.

Issue ID	Description	Component	Solution
	binding-sid is unknown to the OAM process.		
SW-105964	In the microloop solution, ISIS microloop calculates a 4-label path when a 3-label path is sufficient. This may happen when a Point of Local Repair (PLR) is the source.	Segment Routing	Currently, there is no workaround.
SW-110446	When moving between an IS-IS Multi-Topology to an IS-IS Single-Topology, the IPv6 Flex-Algo routes installed in the TWAMP-based table <color-mpls-nh-ipv6> go into inactive mode and are not cleared. IPv6 Flex-Algo routes should not be installed inside the table <color-mpls-nh-ipv6> because they are not supported.	Segment Routing	Currently, there is no workaround.
SW-98421	A static route resolved by an imported L3VPN BGP route stays inactive.	STATIC ROUTE	Currently, there is no workaround.
SW-35926	When the user tries to log in during the first few minutes after a DNOS restart, in an AAA function, with In-band servers, DNOS AAA enters a hold-down for the configured hold-down period (default 10 min).	User Management	Currently, there is no workaround.
SW-113073	When the same PW-ID is reused for different VPWS instances, only one of the VPWS instances is installed. In the case of successive commits, the last configured VPWS instance is	White Box	Avoid the reuse of PW-ID across all VPWS instances.

Issue ID	Description	Component	Solution
	installed. In the same commit, which configured VPWS instance is installed may differ. This results in traffic loss.		
SW-112563	For any interface with L2-service enabled, the TX rate displayed may be inaccurate	White Box	Currently, there is no workaround.
SW-108428	In a hybrid cluster, changing the fabric cables between the NCP-64X12C-S and the NCF from DAC cables to AOC cables results in a partially up-state port.	White Box	Restart the NCF.
SW-112563	In L2- service-enabled interfaces, the displayed TX rate may be inaccurate.	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.

Documentation Highlights

To view the v18.1 related documents:

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

2.Select Library from the top menu

3.Select the 18.1 version filter on the left pane

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