DRIVENETS®

DNOS Release Notes

Downloaded: October 4, 2023

Contents

Software and Firmware Support Highlights

The following table lists the software deliveries available in this release

Software	Description	Software Image
DNOS	DriveNets Network Operating System	18.2.0.17
CAL	DriveNets Golden Image	18.2.0.17
StrataX	DNOS NCM NOS	1.2.0
Base-OS	Base-OS	2.18202243016
FW and ONIE	DNOS NCM FW and ONIE Bundle	18.2.0.1.1
DNOR	DriveNets Network Orchestrator	18.2.0.4

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

NCC Hyper-Threading

We have implemented a new standard for running DNOS with Hyper-Threading (HT) enabled. The default setting for NCCs is now to have HT enabled, which can be achieved by upgrading to the latest BaseOS. By enabling multiple threads to run simultaneously on a single core, HT allows for more efficient use of CPU resources, leading to improved system performance and faster task processing.

You can disable Hyper-Threading via Linux, but it's advised not to disable it while running DNOS as it can cause potential degradation.

New CAL Commands

The automatic ZTP procedure allows you to configure the CAL gRPC server listen port and DNOR address-list automatically. However, this can only be done once and only if there was no previous CLI configuration. To have a backup option, you can now manually configure, display, and clear the CAL gRPC server listen port.

To configure the CAL gRPC server listen port, use the `set gi grpc server listen port <1-65535>` command.

To show the configured CAL gRPC server listen port, use the `show gi grpc server listen port` command.

To clear the CAL gRPC server listen port (set it back to its default - 52443), use the `clear gi grpc server listen port` command.

You can also clear the DNOR address-list, by using the `clear mgmt dnor-server` command.

DNOR Reachability Status via CAL CLI

DNOR's reachability status can now be viewed via the new CAL CLI show command: `show mgmt dnor-server reachability`.

New NCP-36CD-S Transceivers

The II-VI 400G ZR+ QSFP-DD-DCO (output power 0 dBm) and the Ciena 400G ZR+ QSFP-DD-DCO (output power range of -7 to +4 dBm) transceivers are now certified. They are both compatible

with the NCP-36CD-S. Both enable direct router connection to access, metro, and regional DWDM transport networks without requiring intermediary interfaces, by so eliminating an entire optical equipment layer which significantly reduces capital and operational expenditures.

400G Acacia ZR+ Transceiver

The Acacia ZR+ transceiver (DP04QSDD-HE0) is now certified. This transceiver can support distances of up to 1000km with a Tx power of up to 1dBm. It is compatible with the NCP-36CD-S in ZR400-OFEC-16QAM application mode. With +1dBm's Tx power, it can also work well with most WDM systems that use add/drop schemes.

Fixed show interface control transceiver Command

We have fixed the following issues in the `show interfaces control transceiver` command:

Unused optical lanes are no longer presented.

Irrelevant optical data is no longer presented when a DAC cable is used.

Improved Transceiver Operational Data Presentation

The CLI output in the `show interfaces` command has been improved for two transceiver types:

When using DAC, the optical-related lines are now removed.

When using optical transceivers, only the active lanes info appears.

Multicast-only Fast Reroute (MoFRR) Secondary Interface Traffic

When using Multicast-only Fast Reroute (MoFRR) in the network, each node registers to a primary and a secondary upstream multicast hop. As a result, the node receives a primary stream of the multicast group and a secondary stream with the same traffic. Only the packets received on the primary interface are accepted and forwarded. The packets from the secondary interface are counted as dropped packets and are used as a hot standby in case of failure on the primary interface.

This drop indication poses challenges for network operators to maintain and troubleshoot the network. Drop counters usually indicate a misconfig or network issue, whereas MOFRR packets received on standby interface are expected. To avoid these challenges, packets received from the secondary interface are no longer counted as dropped packets.

The incoming traffic rate of MOFRR standby traffic per multicast group can be viewed using the `show multicast route` command.

Tracking-policy - Multiple Objects

We have added new capabilities for using multiple objects under a tracking policy.:

Number-of-failed-objects - when the number of failed objects reaches above the configured value, group tracking is activated.

TheOR/AND operations used for tracking all objects in a policy

Using OR causes a single-tracked object to trigger the poicy.

Using AND causes all objects to fail at triggering the policy.

L2 Interface Counters

When an interface is configured as an L2 AC using the `l2-service` command, it now includes only L2-related counters.

VLAN Manipulation

DNOS introduces VLAN manipulation, a powerful tool that allows you to manage and manipulate virtual LANs (VLANs) on your network interfaces. Providing greater flexibility and control over network traffic, allowing you to push, pop, preserve, and replace VLANs that aresent or received on a network interface. VLAN manipulation is supported on all types of VLAN interfaces: vlan, QinQ and even port-mode.

The following manipulation actions are supported in DNOS in ingress and egress:

pop - Pop the outermost VLAN tag.

pop-pop - Pop the two outermost VLAN tags.

pop-swap - Pop the outer VLAN tag and swap the inner VLAN tag.

preserve-swap - Preserve the outer VLAN tag and swap the inner VLAN tag.

push - Push an additional VLAN tag to the top of the VLAN stack.

push-push - Push two additional VLAN tags to the top of the VLAN stack.

swap - Swap the outermost VLAN tag.

swap-push - Swap the outermost VLAN tag and push an additional VLAN tag to the top of the VLA stack.

swap-swap - Swap both the outer and inner VLAN tags.

To configure VLAN manipulation ingress mapping, use the `interfaces [if-name] vlan-manipulation ingress-mapping action VLAN-STACK-ACTION [outer-tag VLAN-ID-OUTER] [outer-tpid TPID-OUTER] [inner-tag VLAN-ID-INNER] [inner-tpid TPID-INNER]` under the interface hierarchy.

To configure VLAN manipulation egress mapping, use the `interfaces [if-name] vlan-manipulation egress-mapping action VLAN-STACK-ACTION [outer-tag VLAN-ID-OUTER] [outer-tpid TPID-OUTER] [pcp PRIORITY-OUTER] [inner-tag VLAN-ID-INNER] [inner-tpid TPID-INNER]` under the interface hierarchy.

To display the interfaces with their full configuration, use `the show interfaces detail` command.

Dynamic CPRL Update for Changed Services Ports

Dynamic CPRL update was added due to the following changes in the NETCONF and gRPC (gNMI) service ports:

NETCONF service (default is 830) can now work alongside an SSH service in port 22 (through subsystems).

gNMI service (default is 50051) can now work in port 9339.

New Supported Characters in the system SNMP community Command

The following characters are now supported in the `system SNMP community` command string: ()~!@$%^&*-+={}<>,./_

gNMI Service Port

You can now configure the DNOS gNMI service port to 9339 or 50051 (which is the default value), allowing CLI access for higher-level troubleshooting.

To configure the gNMI service ports, use the `system grpc listen-port <port-number>` command.

Segment Routing Global Block (SRGB) Configurable Range Size Increase

The DNOS Segment Routing Global Block (SRGB) configurable range size has increased from 256k labels to 400k labels because:

The BGP-LU is expected to work with a prefix-sid, meaning the BGP-LU scale will require SIDs from SRGB.

The Flex Algo support of eight Algos will multiply the number of needed SIDs in each node.

The extensive usage of the anycast SID (on top of node SIDs).

SIDs are required to cover both IPv4 & IPv6.

The IS-IS Domain can reach up to 2k nodes.

IPv6 MPLS OAM

Segment-Routing IPv4 MPLS-OAM now includes the MPLS OAM ping and traceroute capabilities of an ISIS IPv6 IGP-prefix segment ID, a generic IPv6 prefix, IPv6 nil-FEC, and the BGP labeled IPv6 prefix. These OAM operations are typically used in Segment-Routing IPv6 MPLS, Flex-Algo IPv6 MPLS, and IPv6 BGP Labeled-Unicast for troubleshooting.

To operate MPLS OAM use the `run ping mpls` and `run traceroute mpls` commands.

Flex-Algo Algorithm Scale Increase

Previously, DNOS supported three user-defined flexible algorithms per ISIS instance; it now supports eight. In total, DNOS supports ten algorithms per IS-IS instance - eight user-defined flexible algorithms (Algorithms 128-255), SPF (Algorithm 0), and strict-SPF (Algorithm 1).

To configure the flexible algorithm, enter the Flex-Algo configuration mode using the `protocols isis instance flex-algo` command.

BGP Segment-routing Prefix-SID Collision Handling Enhancements

DNOS now supports BGP Segment-routing Prefix-SID collision handling. Some of the changes are:

Handling receiving multiple prefixes with the same BGP label index

A new system event, 'BGP_SR_CONFCLITING_PREFIX_SAME_LABEL_INDEX' that indicates when receiving different prefixes with the same label index and when allocating a new dynamic label to avoid conflicting IN labels.

A new CLI show command, `show bgp segment-routing prefix-sid db`, which displays conflicting prefixes, including their origin (advertising neighbor) and last update time, address-family, and conflicts between different address families.

RSVP-TE End-to-End Path Protection System Events Enhancements

DNOS introduces new path-protected RSVP-TE tunnels system events:

'RSVP_TUNNEL_LSP_SWITCH' - indicates that a given tunnel's working (active) path has either switched from the primary LSP to the secondary LSP or vice versa.

'RSVP_TUNNEL_E2E_PROTECTION_UP' indicates the installation of an alternate (backup) LSP.

'RSVP_TUNNEL_E2E_PROTECTION_DOWN' - indicates that a tunnel is no longer path-protected, meaning only one installed LSP is currently installed

OSPF Dynamic Link Delay Measurement and Advertisement

It is now possible to advertise link delay parameters in OSPFv2. Dynamic link delay is calculated by Simple-TWAMP (STAMP) link delay sessions. The link delay parameters that are advertised in the opaque LSA type 10 under link TLV are: Min/Max unidirectional link delay, average link delay, and unidirectional delay variation - Sub-TLV 28, sub-TLV 27, and sub-TLV 29, respectively. Link delay helps make path-selection decisions based on performance data (such as latency) in a cost-effective and scalable way. It is also a superior alternative to using hop count or cost as routing metrics.

OSPFv2 delay normalization is now also supported. It normalizes the computed link delay value and reduces the negligible differences between collected delay values on various links. By doing

so, the normalized values are advertised in OSPFv2, and the OSPFv2 routers can better leverage ECMP in the network.

To measure and advertise link delay parameters in OSPFv2, use the `services performance-monitoring interfaces interface` configuration hierarchy, and associate the measuring interface to OSPFv2 under the `protocols ospf instance [name] area [id] interface` configuration hierarchy.

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

To enable OSPFv2 delay normalization, use the `protocols ospf instance [name] area [id] interface [name] delay-normalization` configuration command.

BGP Minimum Hold-time

You can now configure a minimum BGP hold-time per session that prevents the session from establishing if the BGP hold time is lower than the minimum set.

To adjust the threshold for minimum-hold-time, use the `protocols bgp neighbor minimum-hold-time` command.

IS-IS SR-TE Dynamic CSPF Policies

Dynamic SR-TE policies define constraints, such as include admin-group, exclude admin-group, exclude SRLG, algorithms (0-1, 128-255), different metric types (IGP|TE|delay), metric margin, etc. Dynamic policies also support creating up to 8 dynamic segment-lists for maximum topology resource utilization.

Use the `protocols segment-routing mpls path [name] dynamic constraints` and `protocols segment-routing mpls policy [name] path [name]` commands to provision a dynamic SR-TE policy.

OSPFv2 LFA FRR

The OSPF Loop-Free Alternate (LFA) Fast Reroute (FRR) has been extended to support OSPFv2 and inter-area and external OSPF routes. This feature provides LFA protection for OSPFv2 instances by preinstalling backup routes per prefix. Without LFA FRR, OSPFv2 has to re-run SPF to find a new

path when the primary path fails. With LFA FRR, OSPFv2 pre-computes a backup path for inter-area and external OSPF routes and installs the backup next hop in the forwarding table.

To configure OSPFv2 LFA FRR, use the `protocols ospf instance <name> fast-reroute` command.

EVPN-VPWS

EVPN-VPWS is a point-to-point L2 service powered by the BGP control plane. Using it, you can create seamless L2 connectivity between remote sites, utilizing BGP signaling and routing suite such as routing policies. EVPN-VPWS service supports port mode and VLAN mode interfaces along with multihoming scenarios to ensure network resiliency and traffic load balancing. With EVPN-VPWS, traffic is encapsulated and sent to remote sites without relying on MAC-learning, allowing service providers to span and scale services with fewer resources across the network.

To display brief information for all EVPN-VPWS instances, use the `show evpn-vpws { instance [name] }` command.

To configure an L2VPN EVPN VPWS service, use the `network-services evpn-vpws instance` command.

IS-IS Auto SR-TE Policies

The new Auto-policy (On demand) SR-TE templates allow you to create dynamic SR-TE policies based on the received BGP updates with a matching color extended community and attach the colored SR-TE policy to the BGP NH peer that advertised those updates. Auto-policies can delete themselves once there are no BGP paths with a matching <next-hop, color>. The Auto-policies can also leverage dynamic CSPF SR-TE paths, including constructing policies over flexible algorithms.

Create the policy template, use the `protocols segment-routing mpls auto-policy template color <0-4294967295>` command.

Use the `protocols segment-routing mpls path [name] dynamic constraints` to provide a dynamic path with path computation constraints.

Use the `protocols segment-routing mpls auto-policy template [color-value] path [name]` command to associate the dynamic SR-TE path name configured with the desired SR-TE constraints for the above-mentioned auto-policy template.

Use the `protocols segment-routing mpls auto-policy` command to define the general attributed and behavior of all auto-policy templates in the system, such as - template name prefix and delete-delay time.

EVPN Multihoming

EVPN multihoming provides network resiliency and traffic load-balancing for EVPN services. In a multihoming scenario, a Customer Edge (CE) device can be multihomed over two or more Peering Edge (PE) devices for redundancy. If one PE device fails, traffic on the service is still protected. With BGP signaling, EVPN multihoming also supports traffic load-balancing across different PE endpoints connected to the same CE device.

There are 2 two main EVPN multihoming operation modes as defined by RFC 7432:

All Active (default) - provides traffic load-balancing along with PE protection. In this scenario, all PE devices connected to the same CE device forward traffic from and to the CE device. So, when a remote PE device sends traffic to an all-active multihomed CE device, the traffic is load balanced across the PE devices.

Single active - only a single PE device is selected to forward traffic from and to the CE device; the rest of the PE devices are used as a backup. This scenario allows you to accurately limit the bandwidth towards the CE device.

Pre-checks for the ONIE-boot Partition

To avoid failed ONIE or firmware upgrades resulting from a full /mnt/onie-boot partition, we've implemented a new logic that fails the upgrade pre-check and stops any upgrade or deployment if the /mnt/onie-boot partition is full.

Optimized Ufi NCF-48CD

To reduce costs, the Ufi NCF-48CD has been optimized:

The CPU now has four cores instead of eight.

The RAM is now 32G instead of 64G.

These changes do not impact the device's performance. To view the changes to the device, use the `show system hardware` command under the CPU model.

ATP SSD Lifetime Utilization Calculation

ATP platforms that include SSD memory now display a more accurate SSD lifetime calculation following an update to the SSD lifetime formula.

Multiple System Profiles

This feature will be available in the future. It will allow you to configure multiple system profiles, which can help you distribute and develop your features more effectively.

Note: switching between system profiles will force the reboot of the WB agent and the NCP.

You can use these CLI commands when the feature is available:

To configure a system profile, use `the system profile <profile_name>` command.

To view the configured profiles and which features are not supported on the current profile, use the `show system npu-resources` command.

Automated Configuration of DNOR

You can now use DHCP options 60/61 and 66/67 in the NCC CAL or the NCP CAL in a standalone to automatically configure:

DNOR servers

DNS address-list

CAL gRPC server listen port.

Configurable NETCONF Explicit Listen-port (830)

You can now configure the DNOS NETCONF service port to 22 or 830 (default).

NOTE: NETCONF becomes a sub-system of the SSH session when it is configured with the same SSH port (22).

Display-XML

The new command, `show config | display-XML`, allows you to display the `show config` output in XML format. The `edit_config` option allows you to display the `show config` output in an output equivalent to the `NETCONF edit_config` RPC structure so that the output can be used as a NETCONF RPC command.

Resolved Issues

Issue ID	Description	Component
SW-103866	When an SR policy goes into the down state, an alarm will not be triggered and will not populate the `active alarms list`. Only a system event will be generated.	Alarms
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
SW-109674	Sporadic packet loss of less than 0.001% occurs when running traffic near the maximum supported throughput.	BaseOS
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. This would take a valid path from the ECMP group since the maximum-path number is small.	BGP
SW-111119	The BGP-LU-SR route remains stuck in ILM (infinitely) after being withdrawn from BGP.	BGP
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
SW-113375	Rule routing-policy set Accumulated IGP Metric Attribute (AIGP) settings are displayed twice in the show-config output.	CLI
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
SW-115960	On NCP-36CD-S and NCP-64X12C-S, the MU version 2.1.1 FW packages do not override previous FW packages when loaded on DNOS versions other than v18.2.	Infra

Issue ID	Description	Component
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
SW-111846	After changing the time zone to a non-default one, the time zone change is not applied to the host and in: - containerlog_<container_name>_<container_id> logs - system-events logs - ssh/telnet/netconf/cli logs - supervised logs in all NCEs container kernel logs.	LOG
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
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 with ASLA advertised and parallel links.	None
SW-115825	An OSPF config that is applied on a disabled interface incorrectly might not run on that interface.	OSPF
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, leading to the OSPF neighbors having IP information without SR information for a short time.	OSPF
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
SW-112584	OSPF does not update the interface address in the SR Extended Link LSA in the SR topology.	OSPF
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

Issue ID	Description	Component
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
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
SW-105964	In the micro-loop solution, ISIS Uloop 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
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
SW-113363	When remote Syslog servers are configured in DNOS, the global priority level, such as `system logging syslog event-group all severity info` will not have the desired effect on the local `system-events.log` contents. The maximum priority level logged in `system-events.log` will be the highest level configured for remote servers or 'warning' which is the default level.	System Events & Logging
SW-114571	Removing an interface from the EVPN service and then deleting it in the same transaction can cause a system crash if the interface is then recreated and inserted into a Layer 2 service.	White Box
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 installed. In the same commit, which configured VPWS instance is installed may differ. This results in traffic loss.	White Box
SW-112563	In L2- service-enabled interfaces, the displayed TX rate may be inaccurate by a margin of 5%.	White Box

Issue ID	Description	Component
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

Limitations

Issue ID	Description	Component
SW-40319	In an IPv6 Egress ACL, if a rule includes a 'protocol' match (for example, TCP, UDP, ICMP) and the traffic pattern hits it, it is not possible to match any fragments (initial, non-initial) of the IPv6 packets.	ACL
SW-22552	Only the primary path is used when a route is resolved via a BGP route with LFA.	BGP
SW-87458	The CLI fails to point to the wrong word for routing-policy prefix list rules commands. When an invalid command is entered, the CLI always points to the first word (`rule`).	CLI
SW-72999	There is no validation for management default VRFs - mgmt0, mgmt-ncc-0/0, and mgmt-ncc-1/0. They appear under the network-services hierarchy, which configures non-default In-band VRFs. Default VRFs are partially configurable via the network-services hierarchy, too, although their configuration is done under the top hierarchy. The management VRFs appear to the user as configurable, although they are not (by design).	CLI
SW-43391	Up to 10 simultaneous CLI sessions can be supported on a Standalone NCP.	CLI
SW-20421	When configuring OOB management interfaces with a routing protocol during the commit, the following error is presented ‘ERROR: Command failed due to unexpected reason.’ There is no impact on the system.	CLI
SW-20233	During the system boot, the `show file tech-support` command might not function until the system reaches its UP state. There is no impact on the system.	CLI
SW-122171	In an EVPN/EVPN-VPWS service working in an AA mode, when connecting a physical link to a CP device, traffic loss	Datapath

Issue ID	Description	Component
	is experienced. This happens because the CE device sends traffic immediately while the PE core side has not converged.	
SW-120856	When disconnecting a physical link from a CE device in an EVPN PE router, there might be traffic loss for a few seconds.	EVPN
SW-34870	The interface configuration parameter, mtu-ipv6, affects the IPv4 ping when running the `run ping IPv4_ADDR` command. This does not affect transit traffic.	ICMP
SW-89325	Only the default application can be used for 400G transceivers supporting multiple applications. For example, a 400G Base-DR4+ transceiver with a default native 400G application may also support breakout to 100G, according to its CMIS data. However, while the transceiver supports breakout and may appear so in DNOS, for some transceivers (e.g., INNOLIGHT 400G T-DP4CNT-N00), a breakout cannot be configured.	Interfaces
SW-13193	With ISIS on an interface configured with an MTU above 9222, ISIS adjacency cannot be established.	Interfaces
SW-121390	In certain ISIS scales and topologies where the ISIS LSP is divided into many fragments, there can be cases where the SPF calculation may be triggered before all fragments of the LSP are received. In such cases, ISIS might result in a temporary wrong path selection.	ISIS
SW-45496	The ISIS process will crash if more than 1536 ISIS circuits are configured.	ISIS
SW-23899	The Syslog server list in the show system logging command output is not updated with the configured facility type. There is no impact on the system; it is a CLI display issue.	LOG
SW-107823	Committing complex QoS and ACL 100K config lines causes memory issues.	Management

Issue ID	Description	Component
SW-35900	A static route for an OOB management network can't be configured if a specified Next-Hop interface is in DHCP mode.	Management
SW-76489	An NCM ONIE upgrade from DriveNets ONIE 2020 onwards is not supported. The reason for that is that the MU (Multi Updater) uses an old FSCK (File system check) while DriveNets ONIE uses a newer one.	NCE Management
SW-83003	DNI platforms don't have bit error counters available, and symbol error counters are post-FEC. As a result, the signal degrade and signal failure alarms relying on BER calculation have inherent inaccuracy.	None
SW-109311	The maximum throughput decreases on NCS NAT interfaces if any of the two transceivers used for the management connections to the NCMs are missing or malfunctioning.	None
SW-51282	NTP processes can reset in some scenarios.	NTP
SW-77634	Upgrading a DNI-based cluster to v16.2 requires the removal of the NCP configuration. This limitation applies to DNI clusters only and does not include Standalones. The NCP configuration in v16.2 or higher requires an explicit setting of the NCP hardware model to AGCXD40S (the default is S9700-53DX). If it is not set when the NCP reconnects, the NCP enters safe mode due to misconfiguration. It is not possible to add or edit the hardware model configuration without removing the NCP configuration first.	Platform
SW-76547	For low-speed subscribers, there is no differentiation between WRED and Weighted Tail Drop (WTD) thresholds. There are continuous unexpected tail drops over the WRED max threshold.	QOS

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

<table><tr><th>exp-null</th><th>qos-tag</th><th>drop-tag</th></tr><tr><td>0</td><td>0</td><td>green</td></tr><tr><td>1</td><td>1</td><td>yellow</td></tr><tr><td>2</td><td>2</td><td>green</td></tr><tr><td>3</td><td>3</td><td>yellow</td></tr><tr><td>4</td><td>4</td><td>green</td></tr><tr><td>5</td><td>5</td><td>green</td></tr><tr><td>6</td><td>6</td><td>green</td></tr><tr><td>7</td><td>7</td><td>green</td></tr></table></td><td>QOS</td></tr>
</table>

Issue ID	Description	Component
	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 `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-113105	On a large cluster, due to the amount of data the SNMP responder process is managing, it is possible that running snmpwalk and snmpbulkwalk will cause a timeout with default values.	SNMP
SW-122979	When a route that produces a routing loop is added to the RIB, it can become inactive, and the Next-Hop using becomes unreachable by BGP or the static route. The Next-Hop remains inactive even after the looped route is removed.	Static Route
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-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-108914	In an EVPN afi/safi, if a type-3 IM route is received with a different P-Multicast Service Interface (PMSI) tunnel type than the supported type of ingress replication, it is rejected instead of being ignored/ retransmitted.	BGP	Currently, there is no workaround.
SW-100903	Traffic over IPv6 routes with IPv4 Next-Hops is not supported.	BGP	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-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-123353	For EVPN services, when a DN and Cisco router are multi-homed together and running MOD DF election algorithm - Cisco's service carving elects DFs per ESI/EVI	EVPN	Configure the Preference Algorithm to be used on all the routers.

Issue ID	Description	Component	Solution
	combination and not per ESI/ETH-TAG. This leads to traffic loss.		
SW-122829	When an AC interface goes up, only one system even should be generated, 'INTERFACE_UP'. Instead, the system events are generated in this order: • 'INTERFACE_UP' • 'INTERFACE_DOWN' • 'INTERFACE_UP' This happens because there is a momentary flap of the interface on its way UP because of the L2-service being enabled on the interface.	EVPN	Currently, there is no workaround.
SW-122911	When a DF election hasn't taken place yet - the displayed time of the last DF election is wrong (seen in the `show evpn show evpn instance <> ethernet-segments` command).	EVPN	Currently, there is no workaround.
SW-122282	In EVPN, the two routes, type-1/EVI, and type1/ESI, depend on each other. Meaning if one of them doesn't exist, the other one should not be used for the installation of the PE device as the NH device. DNOS only checks if type 1/ESI exists, which can lead to installation issues.	EVPN	Currently, there is no workaround.
SW-120751	DF election happens only if there is a change in the type four EVPN messages. Due to this, when an AC goes down or the EVPN-VPWS service is admin-disabled, it is not the last AC that uses this ESI. The	EVPN	Currently, there is no workaround.

Issue ID	Description	Component	Solution
	type four remains and no change happens in the DF election since DNOS does not check the existence of type 1/EVI routes.		
SW-123308	The `show system utilization limits` command displays threshold default values in the node level (not per user config).	Infra	The system threshold values cannot be seen, but they can be changed.
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-122339	Performance issues are experienced when shortcuts are enabled on all the policies.	ISIS	Disable the shortcuts if they are not in use.
SW-110756	Uloop protection, which protects against loop risk, might not work when working with links that have partially configured address families. For example, both sides of the same link are configured	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.

Issue ID	Description	Component	Solution
	with ipv4, but only one is configured with ipv6.		
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-867111	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-455541	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-114118	In the following situation, there are two TACACS servers - server A only with authorization and server B with authorization and authentication. If server A has a higher priority than server B, we will see in `show system aaa-servers tacacs` that authorization is active on server B	Management	There is no workaround for this, and it is only a show issue. The authorization/authentication will be done in the order of priority and the function each server has.

Issue ID	Description	Component	Solution
	even though it was done by server A.		
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-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	MPLS	Currently, there is no workaround.

Issue ID	Description	Component	Solution
	an interop issue with Juniper, e.g., this order causes Juniper to drop reply messages.		
SW-82225	There is an interop issue with CISCO. 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.
SW-115886	MPLS ping does not work for the 6PE route (IPv6 BGP-LU route over IPv4 LSPs).	MPLS OAM	Currently, there is no workaround.
SW-120216	MPLS Ping/trace to BGP-LU prefixes resolved by SR-TE policies do not work.	MPLS OAM	Currently, there is no workaround.
SW-122598	MPLS OAM trace command may wrongly fail when using it for a BGP-LU route resolved via RSVP tunnel.	MPLS OAM	Use the ddmap option in the MPLS trace command to work around the issue.
SW-116373	The MPLS OAM IPv6 traceroute generic/isis multipath fails when transit has parallel links with sub-interfaces.	MPLS OAM	Currently, there is no workaround.

Issue ID	Description	Component	Solution
SW-114137	The `MPLS OAM IPv6 traceroute` command may return with a timeout failure on one or more hops.	MPLS OAM	Run the `MPLS OAM IPv6 traceroute` command a second time.
SW-46394	Multicast groups may not clear immediately after admin-disable loopback interface on RP.	Multicast	Clear the PIM tree with the command clear pim tree to remove the Multicast groups immediately or wait for the next join timeout.
SW-112305	The NCS enters safe mode when NAT instances are configured to use Mellanox cards plugged 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-112410	Changing the router ID while running OSPF on a high scale may generate the Type 10 Router Information LSA with max-age.	None	Clear the OSPF process.
SW-107260	Uloop protection, which protects against loop risk, might calculate a strict-spf solution in a node that does not support strict-spf.	None	It is recommended to set all nodes in the topology to support the strict-spf algorithm.
SW-104888	In case of a misconfiguration with two static routes using each other as a solution, and 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 that they don't point to each other.

Issue ID	Description	Component	Solution
SW-123273	System events sent in the startup, before the syslog daemon connects to a remote syslog server, are not sent to the remote syslog server. This includes Cold restart events.	None	All the events can be seen locally, in the system events log.
SW-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-123250	Removing an interface from OSPF during GR may still leave OSPF enabled on that interface.	OSPF	Currently, there is no workaround.
SW-108828	In an interface with an ingress QoS policy attached to it, if the user changes the L2 service mode of the interface. The ingress QoS policy will no longer work on the interface.	QOS	Detach the ingress QoS policy and reattach it (2 commits).
SW-113576	If there are two default routes in the RIB, one static/BGP, another 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 default routes is static, then a static route with the IP Next-Hop and interface should be used.
SW-122384	If an Anycast prefix is advertised by two routers that share a common Next-Hop, the Flex Algo routes of the Anycast prefix may	Segment Routing	Currently, there is no workaround.

Issue ID	Description	Component	Solution
	have a duplicate Next-Hop. This causes the balance of the ECMP group to change (which is an unharmful side effect).		
SW-121212	When there aren't enough labels in the SRLB for a dynamic binding-sid. The policies get stuck in the initializing state, and ISIS may not trigger out-of-label system events.	Segment Routing	Be aware of the label ranges and scale when working with auto-policies.
SW-117280	In two connected ASBRs between the SR and LDP domain, the best path to prefix C is from ASBR A -> ASBR B -> C. But if the best path is changed to ASBR A -> C because of a metric change or link-up event. A five-second data loss may occur on traffic that bypasses ASBR A to reach prefix C.	Segment Routing	Currently, there is no workaround.
SW-110446	When moving between an IS-IS Multi-Topology to an IS-IS Single-Topology, the IPv6 Flex-Algo 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-122986	coldStart and warmStart snmp traps are not sent in the case of a system restart.	SNMP	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.

Issue ID	Description	Component	Solution
SW-121956	After an NCC switchover or a system restart, the system event logs are written in UTC time even though the time zone is configured.	System Events & Logging	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.

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.
SW-122776	Move events for dynamic MAC entries are not triggered when a MAC limit is reached, both for a VSI limit and a global limit.	White box	Currently, there is no solution, fix, or workaround to overcome this issue.

Documentation Highlights

To view the v18.2 related documents:

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

2.Select Library from the top menu

3.Select the 18.2 version filter on the left pane

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