DRIVENETS®

DNOS Release Notes

Downloaded: September 19, 2023

Contents

Release 17.2 - Software and Firmware Support Highlights

The following table lists the software deliveries available in this release

Software	Description	Software Image
DNOS	DriveNets Network Operating System	17.2.0.16
CAL	DriveNets Cluster Abstraction Layer	17.2.0.16
StrataX	DNOS NCM NOS	1.2.0
Base-OS	Base-OS	2.17201269015
DNOR	DriveNets Network Orchestrator	17.1.3.7

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

Innolight LR4 with Power Class 5

Previously, DriveNets transceivers only featured a power class of 4, meaning their Tx power reached 3.5W. DriveNets has now certified a new transceiver, the TR-FC13R-NCI, with a power class of 5, meaning the Tx power reaches 4W.

Support for power class 4-7 was implemented in DNOS version v15. An issue might have occurred when using the transceiver with previous versions.

New Innolight 400G AOC Gen.2 Fabric Cable

DriveNets has certified the AOC Gen2 fabric cable by Innolight, providing improved firmware and more reliable transceiver-to-fiber connectivity.

Support for Credo 32AWG AEC

We've certified the use of a new Credo AEC cable and transceivers for the NCP-10CD, NCP-36CD-S, and NCP-40C clusters with the following lengths:

CAC405321D1D-D0-HW 0.5m

CAC41X321D1D-D0-HW 1.0m

CAC415321D1D-D0-HW 1.5m

CAC42X321D1D-D0-HW 2.0m

CAC425321D1D-D0-HW 2.5m

CAC43X321D1D-D0-HW 3.0m

CAC45X301D1D-D0-HW 5.0m

These cables belong to Credo's new series, replacing the CAC45X301D1D-A0-HW 5m, which is no longer in the DriveNets BoM.

The AEC works with the same fabric configuration as the AOC, and the optical cable option should be selected when configuring the fabric cable type.

Finisar Copper SFP 1G Transceiver

We've certified a new transceiver, the Finisar Copper SFP 1G (FCLF8522P2BTL). It can be used on the same NCM with the Avago 1G SFP Copper transceiver (that has reached its end-of-life) or different NCMs in the same cluster.

The Finisar Copper SFP 1G converts the SPF to an RJ45 socket and enables the NCM to connect with the other cluster elements using an RJ45 connection.

Local Bridge Domain (BD)

Local Bridge Domain (BD) provides a means to group a set of physical and logical ports into a private domain, allowing flooding, multicast, and broadcast within the domain for Layer 2 bridging.

Data frames are switched within a bridge domain based on the destination MAC address.

Multicast, broadcast, and unknown destination unicast frames are flooded within the bridge domain.

Source MAC address learning is performed on all incoming packets on a bridge domain.

Incoming frames are mapped to a bridge domain by their incoming VLAN/VLANs.

Traffic cannot leak between one bridge domain to another. Each bridge domain is independent.

To configure a BD instance, use the `network-services bridge domain` configuration command. To view information on a BD instance, use the `show bridge-domain instance` command.

Synchronous Ethernet (Sync-E) on NCP-36CD-S

Synchronous Ethernet (Sync-E) technology has been introduced on NCP-36CD-S Standalone. This physical layer technology functions 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 the present-day mobile network, as well as future Long Term Evolution (LTE)–based infrastructures.

Sync-E is defined in the following ITU-T standards - G.8261, G.8261.1, G.8262, G.8264. It is supported only under the following conditions:

- UfiSpace NCP-36CD-S platforms (S9710-76D) hardware revision PVT and above.

- Platform setup in standalone mode. To synchronize different NCPs in an NCP-36CD-S native cluster, users can allocate dedicated network interfaces for an internal NIF to NIF connectivity between NCPs of the same cluster. Besides Sync-E, it's highly recommended not to configure anything on those links.
- In QL-disabled mode, only the network interface is supported. i.e., the 10MHz cannot be used as a reference source when the system is configured as QL-disabled.

DriveNets recommends configuring at least two Ethernet-based reference clock sources where:

- One source is connected to an active port on one of the lower network interface ports (0-17).
- One source is connected to an active port on one of the upper network interface ports (18-35).

This configuration connects different reference sources to each of the J2C+ devices and allows a faster switch between clock sources as part of the SyncE source switch flow.

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

You can configure the SyncE holdoff parameter to values in the 300 to 1800 mSec range, and the timing servo will operate according to the configured value. However, the CLI `show system clock sync` output may not indicate a holdoff state correctly when the configured value is lower than 1000 mSec due to the polling frequency limitations of the timing servo algorithm.

Segment-routing Maximum-SID-Depth (MSD) Increase to Nine SIDs

The Segment-Routing Maximum-SID-Depth (MSD) has been increased from six SIDs to nine.

You can now create SR policies with nine stacked labels. DNOS routers can now impose nine SR transport labels in SR policies and ten labels overall on egress MPLS packets.

This feature is applicable for ISIS-SR and OSPF-SR.

BFD-type Configuration for BGP Neighbors and Neighbor-groups

BFD-type defines the requested BFD session type - single-hop, multi-hop, or automatic. By default, the BFD session type is dictated according to the BGP peering type.

As part of introducing the BFD-type feature, DNOS now features single-hop BFD sessions for directly connected iBGP neighbors, in addition to the previous support of multi-hop BFD sessions for non-directly connected iBGP neighbors (BGP single-hop BFD was previously on eBGP only).

To configure the BFD session type, use the `bfd bfd-type` command under the `protocols bgp neighbor-group/neighbor` hierarchies.

To display information about the BFD sessions, use the `show bfd sessions` and `show bfd sessions detail` commands.

Static On-Demand-Next Hop BGP over OSPF SR-TE Policies

BGP services (Native/IPv4/IPv6) and L3-VPN (IPv4/IPv6) over predefined colored OSPF SR-TE policies can now be used.

When color requirements are imposed, prefixes will have a color-extended community assigned to them, SR-TE policy forwarding (matching the color) will be preferred regardless of SR-TE, LDP, or SR AD. A colored prefix can automatically steer BGP traffic based on the defined SR policy color.

To set the extcommunity color, use the `set extcommunity color additive <color-value>, <color-value>` configuration command.

To view the extcommunity color, use the `show bgp color` and `show bgp route detail` commands.

OSPF Segment-Routing Traffic-Engineering Policy Coloring

Configuring OSPF SR-TE policy coloring is now possible. Creating multiple OSPF SR-TE policies for the same destination is possible by assigning different color values to the policy.The colored policies can be used with traffic steering in the following ways:

- L2-VPN services with manually attached colored SR-TE policies.
- L3-VPN services with predefined colored policies with known BGP Next-Hop destination.

Received BGP routes with color-extended communities are automatically steered over matching colored SR policies.

To configure SR-TE policy coloring, use the `protocols` segment-routing mpls policy color configuration command.

To view the SR-TE route color information, use the show route color-mpls-nh or show route color-mpls-nh detail commands.

OSPF SR-TE Explicit Paths with Adjacency-SID Based on Labels and IPv4 Hops

OSPF SR-TE policy construction is now possible using an adjacency-SID as follows:

The adjacency SID can be specified as the first label - it only has a local significance.

The adjacency SID can also be specified as a non-first label - relating to the transit node egress interface through which the policy should be built.

The adjacency-SID is defined with labels and IPv4 hops. IPv4 hops prevent adjacency-SID labels from being non-persistent across a router reload.

The adjacency-SID is given to an interface. Two different routers can have the same adjacency-SID on each; the adjacency-SID can represent a different interface.

To configure the adjacency-SID, use the `segment-routing mpls path segment-list hop` command. To view it, use the `show segment-routing policy` command.

Route-Policy Chaining

Policy chaining enhances the ability to attach more than a single policy to a BGPs export/import policy.

Policy chaining allows operators to reduce the number of route policies (RPLs) in the network and simplifies operations by reusing generic policies for several BGP peers while maintaining customized per-peer policy rules using an additional attachment of a policy. The new feature allows the attachment of up to 20 policies.

To attach multiple policies, use the `bgp address-family redistribute` configuration command. To evaluate policies, use the configuration command `policy on-match next-policy.`

NCP-64X12C-S 1G Support

1G on ports 0 to 63 is now available on the NCP-64X12C-S, expanding its fanout diversity for broader use cases. It allows plugging 1G or 10G supporting optical cables and configuring ports 0-63 to operate at either 1G or 10G speed (10G being the default port speed). Ports 64-75 remain at 100G speed without breakout or configuration change support.

To configure the speed of ports 0-63, use the `interfaces [interface-name] speed [port-speed]` configuration command.

Ethernet VPN (EVPN)

Service providers widely deploy existing L2VPN solutions such as VPLS and VPWS. Over time, these services posed challenges and limitations such as redundancy, multicast optimization, provisioning simplicity, flow-based load balancing, and more. The Ethernet VPN (EVPN), now used by DriveNets, is a private L2 VPN based on the BGP control plane. EVPN was designed to be the next-generation VPN that addresses existing L2 challenges and advanced integration with existing L3VPN service support for EVPN over MPLS.

To configure an L2VPN EVPN service, use the `network-services evpn instance` configuration command. To show EVPN instances use the `show network-services evpn` command.

LDP VPWS NSR

LDP VPWS Non-Stop Routing (NSR) is an internal mechanism on a node that allows the LDP control plane for VPWS to switch over with zero topology information loss, both internally and as seen in the service remote nodes. During the NSR process, network traffic is unaffected. When LDP NSR is enabled, VPWS service will be protected by NSR in the event of an NCC failure.

ISIS-SR Adjacency SID Protection

Support for link adjacency-SID protection has been added. Previously only adjacency-SID protection when TI-LFA was running was supported. It creates a link-protection TI-LFA path to the adjacent node behind the given Adjacency-SID.

The link protection is installed as an alternate path for adjacency-SID ILM entry. It allows SR head nodes to create SR policies with protected adjacency SIDs, in which DNOS can act as a Point of Local Repair (PLR) and protect the relevant adjacency SIDs in cases of link failures.

Secondary IPv4 Addresses on L3 Interfaces

Secondary IP addresses on L3 interfaces/sub-interfaces are now available if there is a lack of host addresses in the IPv4 subnet or a need to group different logical subnets under a single VLAN.

To configure the IPv4 secondary addresses, use the `interfaces ipv4-address <A.B.C.D/x> secondary` configuration command under the interfaces hierarchy. To display

information about the interfaces, use `show interfaces`, `show interfaces detail`, and `show interfaces ip` commands.

Virtual Router Redundancy Protocol (VRRP)

Virtual Router Redundancy Protocol (VRRP) is introduced. It's a first-hop redundancy protocol that allows two or more routing interfaces to share a Virtual IP (VIP). A master routing interface is elected to be the master IP based on VRRP priority. This interface takes ownership of the VIP IP address, and other VRRP interfaces in the domain listen to the master advertisements and hop on. This allows end hosts to recover connectivity rapidly if the primary router fails.

VRRP can be enabled on interfaces associated with default VRF.

To enable VRRP on an interface and enter interface configuration mode, use the `protocols vrrp interface` configuration command. To view information on all the VRRP-enabled interfaces, use the `show vrrp` command.

Interface State Transitions Counter

DriveNets certified an Interface State Transitions Counter has been introduced. This feature counts the number of times the port has transitioned from operational UP to operational DOWN and can be crucial for troubleshooting. This feature supports the following interfaces: NIFS, Bundles, Fabric, and NCMs.

To display the state transitions counter, use the `show interfaces detail` command. To clear the counter of the interface, use the `clear interfaces counters` clear command.

IPv4 Simple-TWAMP (STAMP) Endpoint Delay Measurement

DriveNets introduces Simple-TWAMP (STAMP) sessions; previously, DriveNets only featured Full TWAMP.

STAMP sessions are often used to check service-level agreement (SLA) compliance, and the STAMP feature is often used in that context. With STAMP, users can activate, test, monitor, and troubleshoot their network endpoints without using dedicated testing devices. STAMP simplifies the communication model of TWAMP and greatly relaxes its requirements by skipping the process of establishing a control session.

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

- Both work in unauthenticated mode.
- STAMP works in Stateless mode (TWAMP-Light is also stateless by design).

To configure the Simple-TWAMP session characteristics, use the `services performance-monitoring profiles endpoint-delay` command for configuring characteristics such as test duration, frame size, and threshold parameters to be examined in the STAMP test, dscp-value, etc.

To configure the Simple-TWAMP session, use the `services performance-monitoring simple-twamp session` configuration hierarchy to initiate the STAMP sender-session, set its source and destination address, and associate the endpoint-delay profile to define the session's characteristics.

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

To display information about Simple-TWAMP sessions, use `show service simple-twamp sessions` command.

NCP-40C Standalone EdgeCore

We've expanded the range of supported hardware and certified EdgeCore NCP-40C SA, AS7926-40XKFB white box. The device is smaller and has a different layout of the physical ports than the current Ufisapce NCP-40C. In all other respects, they are identical.

BER Counters

Introducing Bit Error Rate (BER) Counters. BER is calculated by comparing the transmitted sequence of bits to the received bits and counting the number of errors. BER includes two counters:

•Signal Degrade error level.

•Signal Failure error level threshold.

Upon exceeding or reaching the Signal Degrade error level or Signal Failure error level thresholds, the system will generate a system event. In case of a signal failure, the interface will be shut down operationally by the system. To configure the administrative state of the Signal Failure alarm, use

the `interfaces [interface-name] ber-sf admin-state [admin-state]` command.

To configure the administrative state of the Signal Degrade alarm, use the `interfaces [interface-name] ber-sd threshold [threshold]` command.

To configure the threshold for the Signal Degrade alarm, use the `interfaces [interface-name] ber-sf threshold [threshold]` command.

Disabling CBC Ciphers for SSH and NETCONF

All CBC ciphers are now disabled to prevent a decryption vulnerability. This is hard-coded and not configurable. It affects direct SSH sessions and NETCONF sessions over SSH.

CTR and GCM ciphers are available on the device.

Supported Ciphers are aes128-ctr, aes192-ctr, aes256-ctr, aes128-gcm@openssh.com, aes256-gcm@openssh.com

LDAP Server Hold-time and Retry-time

LDAP delay parameters are now available; they provide additional time for a failed server to recover from failure.

Retry-time - prevents a failed LDAP server from being retried too soon. If an LDAP server is marked as unavailable, it must not be used for LDAP requests until the retry time has expired. Once the retry time has expired, the LDAP server may be marked as available to accept LDAP requests.

Hold-down - LDAP hold-down timer is triggered when all the LDAP servers are unavailable.

The purpose of these timers is to prevent unnecessary delays due to LDAP requests being sent to unavailable servers.

To prevent a failed LDAP server from being retried too soon, use the `system ldap server timers retry-time` configuration command. To prevent all LDAP requests from being sent to any LDAP servers, use the `system ldap server timers hold-down` configuration command.

Enrichment of the Information in CAL Reports

This feature provides more detailed information when GI reports to DNOR's users during and after versioning processes (deployment, updates, and rollback).

The following information is detailed:

- When a node starts and finishes the preparation phase before the actual installation and when it starts and finishes the installation itself.
- When a node is rebooting and pending a reboot.
- Which hardware modules (SPS, BIOS, etc.) GI updates during the firmware update. Each module's current and target version, whether the update succeeds or fails, and the time it starts and finishes.
- Internal phases are occurring during the BaseOS update.
- Information in real-time when the process is still running and after the cycle ends (history).

DNOS Resource Monitoring

DNOS resource monitoring was enhanced to track compute resources such as memory, CPU, file descriptors, and disk IO per process and system.

When a certain resource crosses a predefined system threshold, a system event is sent specifying the severity of the exception.

A new process (Moninode) was also introduced to track and alert upon possible memory leaks. Moninode uses a rating score to trigger Abnormal Process Memory Usage alerts by periodically monitoring the memory state per process and updating process ratings due to memory usage.

Resolved Issues

Issue ID	Description	Component
SW-94261	BGP may have stopped sending updates to peers in some scale scenarios due to an NSR-related bug. BGP might have crashed as well.	BGP
SW-93352	A memory leak was observed when a BGP prefix was resolved over another BGP default route.	BGP
SW-89879	In a large-scale setup, simultaneously removing the redistribution for multiple route types could clear BGP redistributed routes of only one type.	BGP
SW-82944	A change in a community or extended community does not trigger an update to the advertised routes for an alternate path.	BGP
SW-89050	Changing the IP address in the RSVP explicit path causes inconsistency between the system configuration and the 'show config' output. The system is configured correctly (ORM), but the index is removed from the 'show config'. This only affects indexes with optional attributes: 'exclude,' 'include-loose,' and 'include-strict'.	CLI
SW-86292	The command `no vlan <vlan-id> tpid` fails if no 'tpid' value is specified	CLI
SW-84238	In the system config high-scale, there are a couple of actions that may take up to 30 seconds: • Entering the configure mode • Rolling back the system • Viewing the user config (show-config) from outside the configure mode • Executing show policy/community/as-path commands.	CLI

SW-89509	When an Alias key is saved with two words using the `show system cli-alias` command, only one word is saved, and the command fails to work.	CLI
SW-86060	Some of the options in the system debug file are not working: • Pim • FW_upgrade • Node_manager • Bfd • CLI • Trius These options became obsolete with various system re-factoring, and the system debug file option was not updated.	INFRA
SW-89934	Disabling one of the control interfaces from the CLI (ctrl-ncc-0/1 for this example) on one of the NCCs and then restarting the ctrl_interface agent will cause the enabling command of that interface to fail.	INTERFACES
SW-81887	During a rib-manager reset or switchover event, traffic loss may be experienced over routes redistributed into ISIS. This incident may occur when redistributing a big scale of connected/ static (2-3 thousand).	ISIS
SW-79818	On rare occasions, between the time that the router advertises the adj-sid label to the time it is installed, other routers might use the uninstalled label.	ISIS
SW-76459	VPWS HA is supported only when using LDP GR and not with LDP NSR.	LDP
SW-70443	Removing the prefix length doesn't work correctly in the following flow: CLI commands: dnRouter(cfg)# routing-policy extcommunity-list newest rule 1 allow rt val 1.2.3.0/8:65535 dnRouter(cfg)# commit dnRouter(cfg)# routing-policy extcommunity-list newest rule 1 allow rt	MANAGEMENT

	val 1.2.3.0:65535 dnRouter(cfg)# commit The second configuration command is not updated in routing, and the change is not reflected in vtysh.	
SW-91523	Pasting a large NETCONF configuration might take longer than expected.	NETCONF
SW-94092	When FTP is disabled, the wrappers that control the IB and OOB FTP daemons reach a CPU load of ~100%.	NETCONF
SW-93499	The OSPF adjacency may flap if configured with a low dead interval in scale CSPF scenarios.	OSPF
SW-64974	Accessing UEFI BIOS causes KBP to stop working.	PLATFORM
SW-50316	LSCPU core files might be generated at system runtime. This does not impact the system's stability.	PLATFORM
SW-91129	If we configure the following in the same commit: • Egress QoS policy. • Create sub over phy X. • Attach the egress QoS policy to the sub. • Add phy X to some bundle. • A commit failure is received.	QOS
SW-88263	When the following occurs: • The lag has an egress QoS policy attached. • Interface is part of a lag. • The QoS egress policy has strict priority and WRR queues. • Traffic towards WRR queue should cause over-subscription of the interface. In this case, the WRR traffic causes a drop in strict priority traffic.	QOS

SW-90155	When configuring the admin-group with any type and performing a no command for a non-configured admin-group type with the name previously used, the admin-group is wrongly deleted from the CLI.	RSVP
SW-90576	Wrong rate calculation for TX segment routing	Segment Routing
SW-74307	The system was unable to support binary arguments.	System Events & Logging
SW-94409	TELNET, even when disabled, accepts incoming connections over IPv6 to print the message to the terminal that the service is disabled. This will trigger an increased CPU issue.	TELNET
SW-92905	Executing a login attempt with TELNET that closes before a user inputs a username causes a thread to open that does not terminate and might increase the system CPU.	TELNET
SW-90727	BFD sessions may enter INTERNAL_ERROR in sporadic cases due to a Broadcom issue.	WhiteBox
SW-89558	Any trigger that can cause the NCP to disconnect/connect to the FIB-Manager (like Fab. min. links, for example) can lead to FIB installation errors that will cause an NCP restart, possibly more than once, which will end in NCP in safe mode.	WhiteBox
SW-90755	DNI - configuring breakout on port >= 20 leads to safe mode.	White Box

Limitations

Issue ID	Description	Component	Solution
SW-40319	In IPv6 Egress ACL, if a rule includes a 'protocol' match (for example, TCP, UDP, ICMP) with the traffic pattern, it is impossible to match any fragment (initial, non-initial) of IPv6 packets.	ACL	Currently, there is no solution, fix, or workaround to overcome this issue.
SW-22552	Only the primary path is used when a route is resolved via a BGP route with LFA.	BGP	Currently, there is no solution, fix, or workaround to overcome this issue.
SW-87458	The CLI fails to point to the wrong word for routing-policy prefix list rules commands. When an invalid command is entered, the CLI always points to the first word (`rule`).	CLI	Currently, there is no solution, fix or workaround to overcome this issue.
SW-72999	There is no validation for management VRFs (mgmt0, mgmt-ncc-0/0 and mgmt-ncc-1the /0). The four-system default VRFs appear under the network-services hierarchy used for configuring non-default inband VRFs. Moreover, the default VRF is also partially configurable through the network-services hierarchy, although its configuration is done under the top hierarchy. The management VRFs appear to	CLI	There is no workaround. The default VRF configuration is not done from the network-services hierarchy but rather from the top hierarchy. The management VRFs are not configurable, and the user should not attempt to configure them.

	the user to be configurable, although they are not actually (by design).		
SW-43391	Up to 10 simultaneous CLI sessions can be supported on a Standalone NCP	CLI	Currently, there is no solution, fix, or workaround to overcome this issue.
SW-20421	When trying to configure management interfaces (out-of-band) with a routing protocol, when committing the system, an error is presented. ERROR: Command failed due to unexpected reasons. There is no impact to the system.	CLI	Remove the management interface configuration from the routing protocol hierarchy.
SW-20233	During system boot, the show file tech support command might not function until the system reaches the 'up' state. There is no impact on the system.	CLI	The command should be applied once the system reaches the 'up' state.
SW-34870	The interface configuration parameter mtu-ipv6 affects IPv4 ping when running the run ping IPv4_ADDR CLI command. This does not affect transit traffic.	ICMP	Currently, there is no solution, fix, or workaround to overcome this issue.
SW-13193	With ISIS on an interface configured with an MTU above 9222, ISIS adjacency cannot be established.	INTERFACES	Decrease interface MTU below 9222.
SW-45496	The ISIS process will crash if more than 1536 ISIS circuits are configured.	ISIS	Currently, there is no solution, fix, or workaround to overcome this issue.

SW-23899	The syslog server list in the show system logging command output is not updated with the configured facility type. The system has no impact; it is a CLI display issue.	LOG	Currently, there is no solution, fix, or workaround to overcome this issue.
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	Currently, there is no solution, fix, or workaround to overcome this issue.
SW-35900	A static route for an OOB management network can't be configured if a specified next-hop interface is in DHCP mode.	MANAGEMENT	Currently, there is no solution, fix, or workaround to overcome this issue.
SW-76489	An NCM ONIE upgrade from DriveNets ONIE 2020 onwards is not supported. The reason is that the MU (Multi Updater) uses an old FSCK (File system check) while DriveNets ONIE uses a newer one.	NCE MANAGEMENT	Upgrade to the new ONIE, DN ONIE 2019.06.
SW-42116	System switchover is logged as System failover.	NCE MANAGEMENT	Currently, there is no solution, fix, or workaround to overcome this issue.
SW-51282	NTP processes can reset in some scenarios.	NTP	NTP restarts do not affect the system. Timing is unaffected.
SW-77634	Upgrading the DNI-based cluster to version v16.2 requires the removal of the	PLATFORM	Remove the NCP configuration before upgrading by using the no ncp command. Any other configuration

	NCP configuration This limitation applies to DNI clusters only, not to Standalone. NCP configuration in v16.2 or higher requires an explicit setting of the NCP hardware model to AGCXD40S (default is S9700-53DX). If it is not set when the NCP reconnects, it will enter safe mode due to misconfiguration. It isn't possible to add or edit the hardware model configuration without first removing the NCP configuration.		that references NCP interfaces must also be removed, e.g., protocols interface configuration.
SW-76547	RN1: There is no differentiation between WRED and Weighted Tail Drop (WTD) thresholds for low-speed subscribers. RN2: There are continuous unexpected tail drops over the WRED max threshold.	QOS	RN1: The minimum queue or threshold size set in hardware is 125kB. Two different threshold values configured in temporal units (milliseconds or microseconds) may be converted to the same minimum value for low-rate subscribers. To keep the differentiation for low-speed subscribers, use the hardware-mapping speed configuration, setting the minimum speed of all traffic below 1gpbs to a speed of 1gpbs. This is the default configuration. RN2: To avoid or minimize continuous tail drops, increase the difference between max wred threshold and the queue size. For low rate queues, use the hardware mapping speed conversion table to avoid setting both to the minimum 125kB queue and threshold sizes. Have at least a

<table>
<tr><td></td><td></td><td></td><td>250KB difference between the queue size and the max wred threshold.</td></tr>
<tr><td>SW-25836</td><td>Packet reorder may be caused when the same stream contains multiple classes and if the QoS policy is not attached.</td><td>QOS</td><td>Currently, there is no solution, fix, or workaround to overcome this issue.</td></tr>
<tr><td>SW-25352</td><td>Multiple egress policies can be created, yet only a single egress policy can be attached.</td><td>QOS</td><td>Currently, there is no solution, fix, or workaround to overcome this issue.</td></tr>
<tr><td>SW-24214</td><td>When enabling EXPLICIT NULL behavior for the LSP, the classification of incoming packets at the tunnel tail-end does not consider the policy set on the ingress port. Rather, it uses a default mapping between the MPLS EXP bits carried in the EXPLICIT NULL label and the qos-tag and drop-tag set.
MPLS packets with an EXPLICIT NULL topmost label will be classified according to the fixed table below and, therefore will potentially receive different per-hop-behaviors.
exp-null qos-tag drop-tag
<table><tr><th>exp-null</th><th>qos-tag</th><th>drop-tag</th></tr><tr><td>0</td><td>0</td><td>green</td></tr><tr><td>1</td><td>1</td><td>yellow</td></tr></table></td><td>QOS</td><td>Currently, there is no solution, fix, or workaround to overcome this issue.</td></tr>
</table>

	<table><tr><td>2</td><td>2</td><td>green</td></tr><tr><td>3</td><td>3</td><td>yellow</td></tr><tr><td>4</td><td>4</td><td>green</td></tr><tr><td>5</td><td>5</td><td>green</td></tr><tr><td>6</td><td>6</td><td>green</td></tr><tr><td>7</td><td>7</td><td>green</td></tr></table> This might result in traffic drops due to traffic being queued differently than configured or egress traffic receiving a different QoS marking. Enabling EXPLICIT NULL will always result in this behavior. To prevent this from happening, disable EXPLICIT NULL using the configuration command `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	Currently, there is no solution, fix, or workaround to overcome this issue.

SW-23072	CPRL classifies management protocols by preconfigured protocol ports and doesn't support dynamic port ranges. For example, the TACACS port is 49, if it changes, CPRL will not classify TACACS traffic.	User Management	Currently, there is no solution, fix, or workaround to overcome this issue.

Known Issues

Issue ID	Description	Component	Solution
SW-90119	ISIS instance configuration is not removed correctly from the router upon loading the factory default config. It is only removed from the CLI, but still active in the backend.	CLI	Manually remove the ISIS configuration with the `no isis instance X` or `no isis` commands before performing a load factory default. If load factory default was already applied, perform rollback and manually remove the ISIS configuration.
SW-106267	RN 1: 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. RN 2: When `max-metric router-lsa on-startup` function is enabled, and the user removes the entire OSPF configuration, then re-apply the configuration manually (not via rollback), the `max-metric router-lsa on-startup` function becomes active immediately, even if you did not restart the device.	OSPF	RN 1: Remove the entire OSPF configuration again and commit. Then do rollback 1 and commit. After this, manually add the 'max-metric knob' and commit. RN 2: When this happens, remove the 'max-metric knob' and add it manually or via rollback.
SW-858551	When configuring a routing policy with the rule 0, the commit is	CLI	A solution is not needed; the system ignores the rule 0.

	executed, and the system ignores rule 0.		
SW-48206	When an NTP server is unreachable, disabling the management interface (lo0) might cause the `show system NTP` command to return an error. NTP functionality is not affected.	CLI	Currently, there is no workaround.
SW-21067	Running the command `show interface ctrl-ncm-x` displays an 'uptime' value of 0. There is no impact on the system. It is a CLI display issue.	CLI	Currently, there is no workaround.
SW-98906	When an NCP transitions to UP state in a Bridge-Domain service, some bundle MAC addresses may be missing from the show table in the NCP. There is no effect on the running MAC table.	DATAPATH	The `clear bridge-domain mac-table` command will also solve the show issue.
SW-89997	In v17.1, the default value of a double-tagged sub-interface is 0x88a8 for the outer tag and 0x8100 for the inner tag. Therefore, the default TPID value was removed and written by the datapath behind the scenes, and it may seem like the TPID was configured manually.	DATAPATH	Currently, there is no workaround.
SW-90056	x/0/30/1 200G breakout interface is not coming up due to an incorrect signal integrity configuration for port 30 lane 8.	INTERFACES	Fixed the signal integrity parameters for port 30.
SW-22899	Failure of the standby NCC might cause the active ssh session to be inaccessible for about two minutes.	High Availability	Currently, there is no workaround.

SW-98202	When tracking a physical interface that is part of a bundle, the physical interface is considered down.	INTERFACES	Currently, there is no workaround.
SW-98559	Changing the VLAN attributes on a sub-interface with VRRP configured on it causes the VRRP to break.	INTERFACES	To change the VLAN attributes on a sub-interface with configured VRRP, remove the VRRP configuration, change the VLAN attributes and reconfigure the VRRP. All in separate commits.
SW-96318	When moving a sub-interface to a new VRF, the Ipv6 link-layer address is removed	INTERFACES	When moving a sub-interface to a new VRF, the Ipv6 layer is removed.
SW-93336	The FEC Bit Error Counters and the BER features don't work for 100G breakout interfaces.	INTERFACES	Currently, there is no workaround.
SW-80224	The management interface's uptime is shown when the interface is disabled. This issue has no impact on the functionality of the management interfaces. When the management interface is enabled, the displayed uptime of the interface is correct.	INTERFACES	If the management interface is disabled, the uptime of the interface can be ignored.
SW-73887	Configured output power is displayed three times in the `show interface transceiver` command. • The `Target output power configuration` – a value configured in the transceiver. • The actual configured power - a value configured by the user, as is. • The transmit avg optical power (per channel) - an actual value measured by the transceiver on	INTERFACES	Currently, there is no workaround.

	that channel, should be close to configured output power but may be slightly different from it.		
SW-36535	The IPMI interface remains in UP state after the interface is disabled. This happens when access to IPMI is disabled to mimic admin-state disable, and access cannot be regained later on.	INTERFACES	Currently, there is no workaround.
SW-40860	When changing the number of maximum paths under ISIS, abnormal traffic loss is seen for about 1 second.	ISIS	Currently, there is no workaround.
SW-40847	There is no option to remove summary-only from the ISIS aggregate-route command.	ISIS	Remove the entire aggregate-route and reconfigure it without the summary-only keyword.
SW-86711	MBB is not triggered when an old upstream is no longer one of the valid upstreams.	LDP	When an old upstream is not valid, there is no way to know if the path to root via the old upstream is still physically valid. Therefore, a new path is installed immediately to avoid long traffic loss.
SW-81356	`Address list to send` lists all the addresses, loopbacks, or LDP-enabled interface addresses. It is sent to an LDP neighbor. After removing/adding an interface to LDP, the interface doesn't always become operational. This is due to an error in the `address list to send` that prevents some interfaces from receiving addresses, thus causing them not to join the UDP socket.	LDP	The interface address is inserted into the `address list to send` only if the interface is 'active' in LDP. Therefore, you need to disable/enable the interface administratively. This means the validation of the transport address (an address in the router address list) is also changed. Validation is now done by LDPD in the lookup of all router's addresses, instead of in LDPE in

			lookup `address list to send`.
SW-45541	With a segment-routing-only router, if LDP is preferred, LDP doesn't have a Primary NH to the LER (SR-only router). Therefore, LDP incorrectly installs an alternate-only route towards LSR (SR/LDP router), resulting in a permanent loop between two LSRs.	LDP	Currently, there is no workaround.
SW-42531	Configuring a syslog server with a hostname and not an IP may cause syslog messages not to be sent to the server.	LOG	Configure syslog server with IP address
SW-39013	At scale, when there is a fast log rotation, there may be a mismatch between the log .gz file timestamp and the log timestamps within the file.	LOG	Currently, there is no workaround.
SW-96724	performance-monitoring profiles are not always properly removed from the system when removed via CLI. As a result, the system might warn the user that the maximum number of profiles has reached even though they do not appear in `show-config`.	MANAGEMENT	Deleting performance-monitoring profiles should be done in separate commits and repeated twice.
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 commit failure: • delete interface 'x'	MANAGEMENT	For similar scenarios as above, the proposed workaround is to perform the commit immediately after the 'rollback' command.

	• commit. • 'rollback 1' (re-creates interface 'x') • delete interface 'x' • commit <<<<< Failure here		
SW-44069	Configured data-connection-timeout value is not strict. The configured value is the minimum amount of time the connection is allowed before being disconnected. The maximum time will not exceed twice the configured value for the data-connection timeout.	MANAGEMENT	Currently, there is no workaround.
SW-90599	Minimal 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. While we remove the deleted replication immediately, we can't add the new one until it is verified that the tunnel encapsulation (egress label) is installed in the cluster. Therefore, there is a time gap in which there is no replication, and packets may drop.	MPLS	Currently, there is no workaround.
SW-89139	Multipath information STLV is encoded before the label stack STLV in the DDM TLV. This leads to an interop issue with Juniper, e.g., Juniper drops reply messages with this order.	MPLS	Currently, there is no workaround.

SW-82225	CISCO has an interop issue; it fails to traceroute MPLS BGP-LU over SR, RCA.	MPLS	Currently, there is no workaround.
SW-82174	An interop issue with Juniper causes ping MPLS generic to fail.	MPLS	Currently, there is no workaround.
SW-81808	There is an interop issue with Juniper. DN sends multipath STLV before the label-stack STLV in the DDM TLV, and Juniper expects the label-stack to come before multipath, thus dropping the packet.	MPLS	Currently, there is no workaround.
SW-96242	The Make Before Break process is aborted if a former primary IIF is chosen as a standby IIF, causing traffic loss of up to 40 seconds.	Multicast	Currently, there is no workaround.
SW-92884	In some cases where both BGP-LFA, and ISIS-LFA are available. MoFRR standby IF could select an interface that is only link disjoint while node disjoint is available or the same as the primary.	Multicast	Currently, there is no workaround.
SW-62192	In case of an RPF failure, while (S,G) is in SPT state, mroute is removed, and the PIM does not switch to an (S,G) RPT state. Traffic is still forwarded on the (*,G).	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-99002	When using NETCONF, the VPWS PW pw-id is not correctly obtained from oper-items of config entries.	NETCONF	Currently, there is no workaround.
SW-99000	When using NETCONF, the VPWS instance description is not correctly obtained from oper-items of config entries.	NETCONF	Currently, there is no workaround.
SW-91085	When the PCC receives an update message with a missing LSP object, it treats it as a delegetion release request.	PCEP	Currently, there is no workaround.
SW-79291	During a DNOS upgrade, the cluster fabric-type configuration is reset to its default values. This might lead to traffic forwarding errors if the fabric-type configuration does not match the installed fabric cable type.	PLATFORM	Following an upgrade, apply the correct fabric-type configuration according to the installed fabric cables and perform a system restart.
SW-97959	The `show qos interfaces` command shows a wrong value for high-priority rates when an egress policy is attached to a 100G breakout interface that originated from a 400G interface.	QOS	Currently, there is no workaround.
SW-90723	The `set auto-bandwidth sample` sometimes does not set the sample bandwidth.	RSVP	This option is for testing only, and not part of the feature, and is currently under investigation.
SW-48083	MSS for the BGP sessions established via RSVP tunnels is lower than the egress interface MTU. This happens because the communication from the Linux host that is supposed to egress via an RSVP tunnel is not sent directly via the egress interface because these	RSVP	Currently, there is no workaround.

	types of routes are not installed in Linux. Instead, a tunnel interface is used that has the MTU set to a higher value than the maximum possible MTU on the real interface, triggering the PL-PMTU all the time. BGP sends big packets which are discarded and retransmitted later 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-82474	The `run traceroute mpls nil-fec` command fails when using binding-sid labels because the binding-sid is unknown to the OAM process.	Segment Routing	Currently, there is no workaround.
SW-87460	If one of the SNMP child processes is killed or gets stuck, we restart the SNMP process after 120 seconds due to current infrastructure limitations.	SNMP	Currently, there is no workaround.
SW-100187	When reverting the NOS version from 1.2.0 to 1.1.1 a failure message might appear. The message is related to a package signature that is not supported in version 1.1.1.	Stack & Package Management	Ignore the error message and continue to the next step of the revert procedure.
SW-98421	A static route resolved by an imported L3VPN BGP route stays inactive.	STATIC ROUTE	Currently, there is no workaround.
SW-88651	Taking tech support simultaneously from multiple CLI shows	TS DNOS	The issue should not appear if a TS is not taken simultaneously.

	'Unexpected Error' instead of the normal error. The exact cause is still under investigation.		The workaround is to take a TS at a later point.
SW-35926	In an AAA function, where all of the servers are in-band, and the user tries to log in during the first minutes after a DNOS restart (when in-band connectivity is not yet available), DNOS AAA will enter hold-down for the configured hold-down period (default 10 min).	User Management	Currently, there is no workaround.
SW-88308	QPPB doesn't take precedence over FIB with no destination. A BGP route with a drop destination, e.g. null0 (which is the case of an aggregate-route), dropping the match traffic has a higher preference over handling it by QPPB. As a result, traffic matched on the BGP aggregate-route will not comply with the behavior required by QPPB, even if the route has QPPB source/dest-class (imposed by the BGP policy by matching route attributes), and traffic will be dropped. In such a case, an alert will be generated that the egress ACL is reduced and needs to be confirmed before the upgrade: Large TCAM is required for QPPB to operate. The supported scale of IPv4 Egress ACL needs to be reduced because one large TCAM is redacted from it, resulting in a reduced scale by 2000	WhiteBox	Currently, there is no workaround.

	ipv4 rules per NCP. - Egress IPv4 ACL updated scale: 10240 rules Per NCP. Note that for NCP3, it is still per NCP and not per J2C+. Require to update CLI & Commit validation to enforce new rule scale limitation.		

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 expanding 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 of the range resources in KBP, making all eight ranges available.
SW-89325	Breakout can not be configured for some transceivers (e.g., INNOLIGHT 400G T-DP4CNT-N00), even though they appear to support breakout. This is because whenever a breakout interface goes down, it also causes all the interfaces to go down.	INTERFACES	Currently, there is no solution, fix, or WA to overcome this issue.
SW-84538	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.

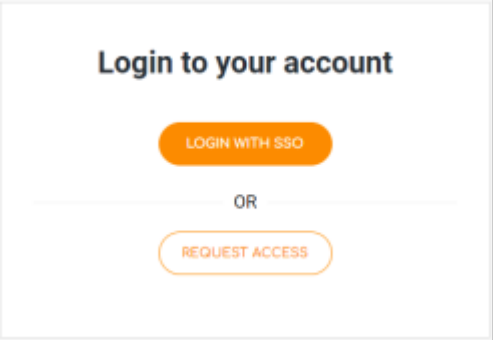
Documentation Highlights

To view the v17.2 related documents:

- Go to https://docs.drivenets.com.
- Select Library from the top menu
- Select the 17.2 version filter on the left pane

If you haven't received an email to activate your account, please contact your account manager, or email documentation@drivenets.com.

If you've activated your new account, login with SSO.



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