DANOS-Vyatta edition

Disaggregated Network Operating System Version 2009a

Release Notes

October 26, 2020

IP Infusion Inc.
3965 Freedom Circle, Suite 200
Santa Clara, CA 95054
+1 408-400-1900
http://www.ipinfusion.com/

For support, questions, or comments via E-mail, contact:
support@ipinfusion.com

Contents

About this Release

These release notes document changes made for DANOS-Vyatta edition (DVE) 2009a.

Supported Solutions

DANOS-Vyatta edition supports the following two solutions with the 2009a release.

- **Cell-Site Router:** Current and future mobile backhaul services including 5G with high bandwidth and low latencies. The cell site router solution can be deployed on qualified hardware platforms shown in table below.
- **Virtual SD Edge:** Virtual Router to build and manage enterprise-class networking services and VPN technologies for the public and private cloud or data center. The supported hypervisors and cloud platforms are listed below.
- **Branch SD Edge:** Secure WAN connectivity to enterprise resources in the public or private cloud. Includes enterprise class networking features and optimized for performance on supported uCPE platforms listed below.
- **Universal SD Edge:** Next generation uCPE solution for open and secure WAN connectivity, the universal SD-Edge may be deployed on Whitebox uCPE devices with virtualization support for dynamically adding new services increasing agility and lower the operational costs for Enterprises and MSPs. The list of supported uCPE platforms and validated third-party VNFs are listed below**.**

Supported Platforms

DANOS-Vyatta edition supports the following platforms in 2009a:

- UfiSpace S9500-30XS
- Silicom-uCPE-xSmall
- Silicom-uCPE-Small
- Silicom-uCPE-Medium
- Silicom-uCPE-Large
- Silicom Barcelona uCPE

Supported Chipsets

DANOS-Vyatta edition supports the following switch chipsets in 2009a:

- Broadcom's BCM88470 Series, also known as the StrataDNX® *Qumran-AX* switch series
- Broadcom’s BCM56160/BCM56172 Series, also known as the StrataXGS® Hurricane-3 series
- Marvell’s 88E6190X series

Hardware / Platform Compatibility List

DANOS-Vyatta edition 2009a supports the platforms as shown in the following table.

Note: See the feature matrix for a complete list of features supported on each platform.

UFI Space

Model	Switching ASIC	Port configuration	Hardware Revision	DVE Solution
UfiSpace S9500-30XS	Broadcom BCM88470_B0	20 port 10G, 8 port 25G and 2 ports 100G	Label Revision: 2 CPU CPLD version: 20	Layer-3 Cell-Site Router

Silicom

Model	Switching ASIC	Port Configuration	Hardware Model	DVE Solution
Silicom-uCPE-xSmall	Marvell's 88E6190X	4x1GbE 2x1GbE (POE+) 2xSFP	80500-0150-G12	Branch SD Edge Universal SD Edge
Silicom-uCPE-Small	Broadcom's BCM56160	10x 1GbE RJ45 4x SFP+ 4 of 1GbE supports POE+*	80500-0179-G11	Branch SD Edge Universal SD Edge
Silicom-uCPE-Medium	Broadcom's BCM56160	10x 1GbE RJ45 4x SFP+ 4 of 1GbE supports POE+*	80500-0180-G11	Branch SD Edge Universal SD Edge
Silicom-uCPE-Large	Broadcom's BCM56172	32x 1GE RJ45 8x SFP+ 32 of 32 supports (POE+)	80500-0181-G11	Branch SD Edge Universal SD Edge
Silicom Barcelona uCPE	NA	• NM slot 0: 4x 1G RJ-45, 2x 10G SFP+ • NM slot 1: 4x 1G RJ-45, 2x 10G SFP+	SKYD_CC	Branch SD Edge Universal SD Edge

Virtual Machine

Vendor	Platform	Version	DVE Solution
LINUX	KVM	1.5.3	Virtual SD Edge
VMWare	ESXI	6.7	Virtual SD Edge
Azure	VHD	Cloud Marketplace	Virtual SD Edge
AWS	AMI	Cloud Marketplace	Virtual SD Edge

Azure Market Place

https://azuremarketplace.microsoft.com/en-/marketplace/apps/ipinfusion1590066770520.virtual-sd-edge-1-0?tab=Overview

AWS Market Place

https://aws.amazon.com/marketplace/pp/B08F9CC1D4?ref_=srh_res_product_title

Third-party Party VNFs Validated

- DANOS-Vyatta Edition VM 2009a
- Cisco CSR1000v VM
- Fortinet-Fortigate VM 6.2

Optics and Accessories

The DANOS-Vyatta editon NOS supports the following SFP and SFP+ transceivers:

Tranceivers Supported for UfiSpace S9500-30XS

- Brocade/E1MG-SX-OM-1000BASE-SX
- Brocade/E1MG-LX-OM-1000BASE-LX
- Brocade/E1MG-LHA-OM-1000BASE-EX
- Brocade/10G-SFPP-SR-10GBASE-SR
- Brocade/10G-SFPP-LR-10GBASE-LR
- Brocade/10G-SFPP-ER-10GBASE-ER

- 1GE-Copper: FCLF8522P2BTL
- 1GE (SFP): FTLF8519P3BNL
- 1GE LX (SFP): FTLF1318P3BTL
- 1GE (SFP): FTLF1518P1BTL
- 10GE SR (SFP+): FTLX8574D3BCL
- 10GE LR (SFP+): FTLX1475D3BCL

- 10GE ER (SFP+): FTLX1672D3BCL
- 1GE-Copper: FCLF8522P2BTL

- 1GE LX (SFP): FTLF1318P3BTL
- 1GE EX (SFP): FTLF1421P1BTL-RN
- 1GE ZX (SFP): FTLF1518P1BTL
- 10GE LR (SFP+): FTLX1475D3BTL
- 10GE ER (SFP+): FTLX1672D3BTL
- 25GE LR (SFP28): FTLF8536W4BTL
- 100GE LR4 (QSFP28): FTLC1154RDPL4

Edgecore Tranceivers Supported for UfiSpace S9500-30XS

SFP Type	Serial Number
EN-SFPP-ER	S06300018
EN-SFP10G-SR	S06290330
EN-SFP1G-LX	S06290340
EN-SFP1G-EX	S06290343
EN-SFP1G-SX	S06290351
EN-SFP28-SR	S06290322
EN-SFP1G-ZX	S06290348
EN-SFP10G-ER	S06290392
EN-SFP10G-LR	S06290328
EN-SFP10-LRi	S06300015
EN-SFP1G-LXi	S06300006
EN-SFP10G-SRi	S06300011
EN-SFP1G-SXi	S06300002
EN-QSFP28-SR4	S06290333-36
EN-QSP28-LR4	S06290337-38

Edgecore Tranceivers Supported for Silicom-uCPE- Devices

SFP Type	Serial Number
EN-SFPP-ER	S06300018
EN-SFP10G-SR	S06290330
EN-SFP1G-LX	S06290340
EN-SFP1G-EX	S06290343
EN-SFP1G-SX	S06290351
EN-SFP28-SR	S06290322
EN-SFP1G-ZX	S06290348
EN-SFP28-LR	S06290397

EN-SFP10G-ER	S06290392
EN-SFP10G-LR	S06290328
EN-SFP1G-RJ45	S06290401
EN-SFP10-LRi	S06300015
EN-SFP1G-LXi	S06300006
EN-SFP10G-SRi	S06300011
EN-SFP1G-SXi	S06300002

New Features

For a complete feature list, please refer to the Feature Matrix.

New features – Broadcom Qumran AX Platform

Hardware Layer 3 Forwarding

Physical ports may now be configured as isolated L2 domains rather than as switchports in a single L2 domain. This allows L3 configuration on physical ports directly.

QoS Feature Support

Support for QoS on physical ports with L3 configuration is also provided.

Layer 3 Egress ACLs

This feature extends the simple, stateless IP Packet filter support in hardware to add egress ACLs. It adds the ability to block outbound locally sourced traffic and transit traffic. The filter support is only provided for non-reassembled packets and only affects L3 packets which are L3 processed i.e. an L3 packet which is L2 forwarded between links in a VLAN would not be affected.

Layer 3 ACL Support

This feature extends the support for IP Packet filtering to include the following fields: ICMP_TYPE/ICMPV6_TYPE, ICMP_CODE/ICMPV6_CODE, L4_SRC_PORT, L4_DST_PORT, IP_TTL and IP_DSCP.

Traffic Forwarding Classification based on protocol

This feature provides the ability to assign a forwarding class to any locally originated control and management traffic, based on protocol (e.g. OSPF, BFD, Telnet).

IEEE 1588v2 Slave (sink) Clock for time/phase sync [G.8275.2]

Extends support for G.8275.2 telecom profiles with or without assisted partial timing (APTS) support.

Zero Touch Provisioning

ONIE Installer Zero Touch Provisioning Support.

STP, RSTP, MSTP Support

This feature provides support for the STP/RSTP/MSTP bridging protocols in hardware.

BFD strict mode support with BGP client

BGP fall-over BFD allows action to be taken by BGP when a BFD session fails for a neighbor. Currently a BFD session is instigated after a BGP session is established. This feature adds BGP “strict-mode” operation, which prevents BGP session establishment until both the local and remote speakers have a stable BFD session.

Per-interface MAC Limiting

Per-interface MAC limiting is a security feature which protects against the flooding of the Ethernet Switching Table. This feature allows the user to set a maximum limit for the number of MAC addresses that can be learned on the layer 2 interface. When the limit is reached no new MAC addresses will be learned and traffic from these MAC addresses will be dropped.

New features – Marvell 88E6190X, Broadcom Hurricane 3 Platform

MIB support for Path Monitor

This feature provides read only MIB for Path Monitor which allows the collection of measurement history from Path Monitor tests of all types (currently ping and twping (TWAMP)). This includes: round trip latency, round trip jitter, number of test packets sent, number of test packets declared lost. In conjunction with the existing functionality provided by Path Monitor this allows a management system to collect and report site-to-site metrics for a set of traffic classes.

New features – CGNAT VNF Use Case

NETCONF - Rollback support

Rollback is a feature that is currently available on the configuration CLI. The "rollback" command allows reverting the configuration to a previously committed configuration, perhaps to return to a known good configuration, or undo experimental configuration changes. This feature adds new NETCONF RPCs that make the rollback operation available to NETCONF clients.

NETCONF support for BGP soft reset

The existing operational command to reset BGP is used to trigger a "replay" of the received and/or issued prefixes associated with a particular neighbor (software reconfiguration). This feature allows the same operational command to be issued via a NETCONF RPC to trigger the reset.

New features – General Purpose

Linux Update

The Base Linux OS is Debian 10 and the Linux Kernel is updated in this release to Version 5.4 (LTS).

Protocol Dependent Mappings for SNAT

SNAT maps from an internal source address and ID (where ID can be a port number) to an external

address and ID, by allocating these from a given pool. This feature adds support for three separate pools (rather than a single shared pool). One pool will be used for assigning TCP ports, another for assigning UDP ports, and the third one for ICMP and other protocols.

Conditional BGP Advertisement (IPV4 & IPV6)

This feature allows a BGP speaker to advertise a set of BGP routes or withdraw the set of routes using route-maps.

BGP Best External Route

This feature allows a BGP backup path to be advertised for an eBGP learned path to an iBGP peer, when the internal best path was learned from the internal peer. The advertising of the best external route can be done via a full mesh of iBGP peers, or using diverse paths via Route Reflectors.

BGP Nexthop Tracking

BGP mantains a nexthop cache which is refreshed every minute with the current RIB state, where a change in state is applied to the BGP RIB. This feature allows BGP to register the BGP nexthops with the RIB, where any change in the reachability or meta data related to the nexthop is notified to BGP. BGP is then able to apply the event change without having to poll the RIB, thus improving BGP convergence.

Provide CLI to clear OSPF per-interface counters

Provision of an operational command to clear the OSPF interface counters. Corresponding show interface output is extended to include a timestamp of when the counters were last cleared.

Logging Enhancements

This feature provides the ability to filter 'show log' output based on time, clear stored system logs, and to configure the amount of storage used for the system logs.

Modified features

No features have been modified in this release.

Deprecated features

The VRRP run-transition-scripts subtree is now deprecated. Equivalent, more secure, functionality can be found under the notify subtree. This can be used to trigger state changes in BGP and IPSec.

Defects

Issues Resolved

Issue number	Priority	Summary
VRVDR-53342	Critical	uSDE-->Node showing error while checking “show interfaces dataplane dp0s9 affinity” Attach
VRVDR-53314	Major	dhcp-client overlap-subnet script fails on DANOS due to missing vrfmanager Python module
VRVDR-53278	Critical	Desired speed in VOQ setup can overflow int param
VRVDR-53275	Major	Flexware : Update platform detection for new large based on latest production boxes
VRVDR-53244	Major	Barcelona board should be made generic
VRVDR-53199	Major	Configuring unreachable static route causes a zebra & dataplane restart
VRVDR-53191	Major	IPsec commands do not work unless acm rules for 'rpc-default' and 'notification-default' are configured
VRVDR-53138	Blocker	IPsec RA-VPN Client and Server regression broken on latest Halifax regression builds
VRVDR-53102	Critical	OSPFv2: prefer loopback address for use as forwarding address in NSSA LSAs
VRVDR-53065	Critical	YANG tweaks to allow NCS to compile DVE YANG files
VRVDR-53062	Major	Missing logs for enforcement action taken for licensing
VRVDR-53061	Major	Allow ACL rulesets to set an address-family flag in the group structure
VRVDR-53022	Major	[ext]community-list and access-list translation issues in DANOS
VRVDR-53014	Critical	commit-confirm not working via vcli scripts
VRVDR-52997	Major	tacplusd get_tty_login_addr() may overflow buffer
VRVDR-52995	Critical	Grub update during image upgrade is broken
VRVDR-52994	Critical	BFD: Show bfd session details shows incorrect stats

Issue number	Priority	Summary
VRVDR-52993	Critical	License enforcement for hardware other than UFI-SPACE is bringing down the dataports
VRVDR-52918	Blocker	1912f - Hardware CPP not conforming to limiter rates
VRVDR-52912	Critical	service-user creation fails due to moved SSSD databases
VRVDR-52910	Major	service-users LDAP password and local encrypted-password values not redacted in audit logs or TACACS+ authorization requests
VRVDR-52909	Major	RIP MD5 passwords not redacted in audit logs or TACACS+ authorization requests
VRVDR-52906	Blocker	QoS - Bandwidth Must match <<number><suffix>>
VRVDR-52885	Critical	The dataplane interfaces are down when configuring the cpu-affinity
VRVDR-52855	Critical	Creating service users fails
VRVDR-52851	Major	FAL Broadcom plugin needs to be tuned to optimize to 100G QoS performance
VRVDR-52850	Critical	Egress ACL in s/w path will not match router originated traffic
VRVDR-52843	Major	Output of static entries in ARP table has changed
VRVDR-52841	Critical	S9500-30XS: Receiving only 10Gig traffic going over 25Gig links
VRVDR-52825	Minor	Configuring three sub-levels of time-zone is not possible, causing upgrade from earlier version to fail
VRVDR-52740	Critical	show interfaces affinity and show interfaces identify returns error "Error: Unknown RPC"
VRVDR-52739	Major	Port value in tunnel policy without specifying protocol causes error "protocol must be formatted as well-known string." for IPsec 'show' commands
VRVDR-52677	Major	When multiple peers use the same local-address, no authentication ids, and unique pre-shared-keys IKEv2 based IPsec stuck in 'init' for all but one peer
VRVDR-52611	Major	i40e driver silently drops multicast packets causing VRRP dual master
VRVDR-52546	Minor	GUI hangs/loading and finally timeout with an error message on browser

Issue number	Priority	Summary
VRVDR-52468	Major	Neg Rx value not updated if requested value cannot be used
VRVDR-52451	Critical	bgpd process crashed when performing snmpwalk with BGP configuration
VRVDR-52404	Major	ICMP error returned with corrupted inner header causes seg-fault when passed through a FW/NAT44/PBR rule with logging enabled
VRVDR-52401	Critical	Degradation of throughput by 10%-40% on v150 with 100M physical interface & QOS
VRVDR-52383	Critical	PTP: Internal errors causing PTP stack not to be created
VRVDR-52188	Major	"start virt guest XYZ" doesn't report errors
VRVDR-51749	Critical	DHCPv6 address not getting renewed automatically on client node after DHCP server rebooted and only works when delete/reconfig DHCPv6 add config on client node,works fine for DHCPv4
VRVDR-51678	Critical	PTP: Slave clock sees significant time-error when GPS signal fails on SIAD, when it switches to PTP
VRVDR-51332	Major	PTP: Unable to cope with config change where master and slave swap ds-ports (slave does not come up)
VRVDR-51256	Critical	ACM VCI component does not seem to work correctly with only default values
VRVDR-47760	Blocker	J2: QoS - Increase configuration limits for 100G for hardware platforms
VRVDR-43307	Critical	vyatta-ike-sa-daemon: TypeError: 'IKEConfig' object does not support indexing

Resolved Security Vulnerabilities

The following security issues are resolved in this release:

- CVE-2020-25595, CVE-2020-25596, CVE-2020-25597, CVE-2020-25599, CVE-2020-25600, CVE-2020-25601, CVE-2020-25602, CVE-2020-25603, CVE-2020-25604: Debian DSA-4769-1: xen security update
- CVE-2019-3874, CVE-2019-19448, CVE-2019-19813, CVE-2019-19816, CVE-2020-10781, CVE-2020-12888, CVE-2020-14314, CVE-2020-14331, CVE-2020-14356, CVE-2020-14385, CVE-2020-14386, CVE-2020-14390, CVE-2020-16166, CVE-2020-25212, CVE-2020-25284, CVE-2020-25285, CVE-2020-25641, CVE-2020-26088: Debian DLA-2385-1: linux-4.19 LTS security update
- CVE-2020-12829, CVE-2020-14364, CVE-2020-15863, CVE-2020-16092: Debian DSA-4760-1: qemu security update
- CVE-2020-8619, CVE-2020-8622, CVE-2020-8623, CVE-2020-8624: Debian DSA-4752-1 : bind9 - security update

- CVE-2018-20346, CVE-2018-20506, CVE-2018-8740, CVE-2019-16168, CVE-2019-20218, CVE-2019-5827, CVE-2019-9936, CVE-2019-9937, CVE-2020-11655, CVE-2020-13434, CVE-2020-13630, CVE-2020-13632, CVE-2020-13871: Debian DLA-2340-1: sqlite3 security update
- CVE-2019-18814, CVE-2019-18885, CVE-2019-20810, CVE-2020-10766, CVE-2020-10767, CVE-2020-10768, CVE-2020-12655, CVE-2020-12771, CVE-2020-13974, CVE-2020-15393: Debian DLA-2323-1: linux-5.4 new package
- [DSA 4746-1] net-snmp security update
- CVE-2020-16135: Debian DLA-2303-1: libssh security update
- CVE-2020-12762: Debian DLA-2301-1: json-c security update
- CVE-2019-5188: Debian DLA-2290-1: e2fsprogs security update
- CVE-2020-8177: Debian DLA-2295-1: curl security update
- CVE-2020-10713, CVE-2020-14308, CVE-2020-14309, CVE-2020-14310, CVE-2020-14311, CVE-2020-15706, CVE-2020-15707: Debian DSA-4735-1: grub2 - security update
- [DSA 4733-1] qemu security update
- CVE-2019-18348 CVE-2020-8492 CVE-2020-14422: Debian DLA-2280-1: python3.7 security update
- [DSA 4728-1] qemu security update
- [DSA 4723-1] xen security update
- CVE-2018-19044 / CVE-2018-19045 / CVE-2018-19046: Insecure temporary file usage in keepalived
- CVE-2020-3810: Debian DSA-4685-1: apt - security update

Known issues

The following table lists the known issues in this release.

Component	Key	Summary
Bonding	VRVDR-53410	Bonding interface keep flapping when cpp-limiter applied with OSPF configuration along with running ipv6 traffic.
Security	VRVDR-53099	tacacs+ starts only when service is restarted manually. Workaround: Manually restart tacplusd.service
STP	VRVDR-52924	MAC addresses are not flushed after topology change occurred.
Licensing – CSR	DANV-188	Once enforcement action is triggered after 20 mins of inactive license on a device and ports are moved to admin-down, then installing a valid license, ports which are not configured are not coming up once the device is up after reboot. Workaround: Ports can be brought UP by manually shut and noshut.
OSPFv3	VRVDR-52395	Ospf6d crashed with 70k/128k routes when ospfv3 process reset
Bonding	VRVDR-52439	vyatta-snmp-vrf process crashed when run snmpwalk for the first time over bonding interface
OSPFv3	VRVDR-51587	Ospf6d is crashing with 70k routes in switchover scenario
OSPFv2, OSPFv3	VRVDR-51189	Interop: DR/BDR election doesn't happen as per protocol standard between DVE & Cisco
BGP	VRVDR-51188	BGP-3 provisioning/session Failed when existing bgp neighbour config modified with peer-group
OSPFv3	VRVDR-51032	OSPFv3 session DOWN after configuring area type stub between UFI and NOKIA/CISCO
DHCPv4	VRVDR-51452	DHCPv4 IP Address is not received after soft reboot and works fine once system is hard rebooted

Limitations, Restrictions or Behavior Changes

While the OS does support IKEv1, it is stringly recommended that IKEv2 is used to avoid security vulnerabilities associated with IKEv1, such as reflector and Amplifier DoS attacks.
Removal of TACACS+ local-user-name authorization argument support. Support for the local-user-name authorization argument, which allowed TACACS+ users to login as an already configured local user, has been removed from the 2009 release. DVE supports on-the-fly creation of a local user during the login process for TACACS+ users. Presence of the local-user-name argument in authorization replies will now cause an authorization failure. All currently supported DVE releases include the capability for on-the-fly local user creation. In releases prior to 2009, this happens when local-user-name is not present in the session authorization reply.
In AWS, legacy Xen instance types will not work. The feature adds support for the modern nitro (KVM) instance types only – please use those.

MIBs

New MIBs

The following new MIBs have been introduced in this release:
ATT-VROUTER-PATH-MON-MIB
ATT-VROUTER-PATH-MON-TWPING-MIB

Modified MIBs

No MIBs have been modified in this release.

Deprecated MIBs

There are no deprecated MIBs in this release.

RFCs and Standards

The following standards have been added or additional parts have been implemented in this release:

- RFC2474, Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers
- RFC2475, An Architecture for Differentiated Services
- RFC6774, Distribution of Diverse BGP Paths

Licenses

MSTP / RSA

/* Copyright (C) 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved.

License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.

These notices must be retained in any copies of any part of this documentation and/or software.
*/