Vyatta Network OS Release Notes, 1801

These release notes document changes made for the Vyatta Network OS Release 1801.

Supported Products

The Vyatta Network OS supports the following products:

- vRouter
- VNF Platform
- Distributed Services Platform. Note that this platform is not being formally released in release 1801.

Behavior Changes

Refer to Features and CLI commands in the following pages of this document of these notes for behavior changes in this release.

Features

New features

VXLAN Tunnel Support

This feature adds support for VXLAN and VXLAN-GPE tunnels.

The following configuration mode commands are used:

- set interfaces tunnel tun0 encapsulation < vxlan | vxlan-gpe >
- set interfaces tunnel tun0 vxlan-id <0-16777216>
- set interfaces tunnel tun0 transport multicast-group <ipv4-address | ipv6-address>
- set interfaces tunnel tun0 transport routing-instance <vrf-name>
- set protocols static vxlan-mac interface <if-name> mac <mac-addr> remote-ip <ip-address> [vni <vni>]

Policy Based IPSEC with Firewalls and DNAT/SNAT

This adds the ability to run interface-based firewalls, zone-based firewalls, DNAT, and SNAT with policy-based IPSec site-to-site tunnels

The following configuration mode commands are used:

- set interfaces virtual-feature-point <vfpN>
- security vpn ipsec site-to-site peer <peer> tunnel <num> uses <vfpN>
- set interfaces virtual-feature-point <vfpN> firewall in <rule-set-name>
- set interfaces virtual-feature-point <vfpN> firewall out <rule-set-name>

- set interfaces virtual-feature-point <vfpN> firewall local <rule-set-name>
- set service nat source rule <num> outbound-interface <vfpN>
- set service nat destination rule <num> inbound-interface <vfpN>
- set service nat ipv6-to-ipv4 rule <num> inbound-interface <vfpN>

TCP SYN Packet MSS Clamping

This feature adds the ability to modify the value of the TCP MSS option in SYN and SYN ACK packets

in order to configure MSS clamping, the following configuration mode commands are used under the existing "interface <iftype> <ifname>" command:

- ip tcp-mss mtu
- ip tcp-mss mtu-minus ***value***
- ip tcp-mss limit ***value***
- ipv6 tcp-mss mtu
- ipv6 tcp-mss mtu-minus ***value***
- ipv6 tcp-mss limit ***value***

Values range from 1 to 65535.

Assign Cost to Summary Route in OSPFv2 and OSPFv3

This feature provides a way to configure a fixed cost to be advertised with the summary route.

The following configuration mode commands are used:

- set protocols ospf [process <process-ID>] area <area-ID> range <IPv4-prefix> **metric <0..16777214>**
- set routing routing-instance <name> protocols ospf process <process-ID> area <area-ID> range <IPv4-prefix> **metric <0..16777214>**
- set protocols ospfv3 [<process-name>] area <area-ID> range <IPv6-prefix> **metric <0..16777214>**
- set routing routing-instance <name> protocols ospfv3 <process-name> area <area-ID> range <IPv6-prefix> **metric <0..16777214>**
- set protocols ospfv3 process <process-name> address-family ipv4 unicast area <area-ID> range <IPv4-prefix> **metric <0..16777214>**
- set routing routing-instance <name> protocols ospfv3 process <process-name> address-family ipv4 unicast area <area-ID> range <IPv4-prefix> **metric <0..16777214>**

Assign Tag to Static Route

This feature provides the ability to assign tags to static routes and ability to filter and redistribute into other routing protocols based on that. It should work for both IPv4 and IPv6 static routes

The following configuration mode commands are used:

- set protocols static interface-route <v4prefix> next-hop-interface <interface> **tag <1..4294967295>**
- set protocols static interface-route <v4prefix> next-hop-routing-instance <name> next-hop-interface <interface> **tag <1..4294967295>**
- set protocols static interface-route6 <v6prefix> next-hop-interface <interface> **tag <1..4294967295>**

- set protocols static interface-route6 <v6prefix> next-hop-routing-instance <name> next-hop-interface <interface> **tag <1..4294967295>**
- set protocols static route <v4prefix> blackhole **tag <1..4294967295>**
- set protocols static route <v4prefix> unreachable **tag <1..4294967295>**
- set protocols static route <v4prefix> next-hop <v4address> **tag <1..4294967295>**
- set protocols static route <v4prefix> next-hop-routing-instance <name> next-hop <v4address> **tag <1..4294967295>**
- set protocols static route6 <v6prefix> blackhole **tag <1..4294967295>**
- set protocols static route6 <v6prefix> unreachable **tag <1..4294967295>**
- set protocols static route6 <v6prefix> next-hop <v6address> **tag <1..4294967295>**

Track Interface State to a vhost Interface

This feature will monitor the link status of a configured set of interfaces and set the guest interface link status when all the monitored host interfaces are down.

The following configuration mode commands are used:

- set interfaces vhost <dpFvhostN> transport-link <intf>

IPSLA Support

This feature allows monitors to measure various SLA parameters and to modify PBR routing based upon these measures.

The following configuration mode commands are used:

- set service path-monitor monitor **<name>** history results **<mhsize>**
- set service path-monitor monitor **<name>** history policy-state-change **<phsize>**
- set service path-monitor policy **<name>** type ping **jitter**
- set service path-monitor policy **<name>** type ping **loss**
- set service path-monitor host **<name>** type **twping**
- set service path-monitor host **<name>** type twping dscp **<dscp-value>**
- set service path-monitor host **<name>** type twping padding **<pad-size>**
- set service path-monitor host **<name>** type twping control-port **<port>**
- set service path-monitor host **<name>** type twping port-range start **<low>**
- set service path-monitor host **<name>** type twping port-range end **<high>**
- set service path-monitor host **<name>** type twping source-address **<address-or-interface>**
- set service path-monitor policy **<name>** type **twping reflect jitter** ...
- set service path-monitor policy **<name>** type **twping reflect time** ...
- set service path-monitor policy **<name>** type **twping round-trip jitter** ...
- set service path-monitor policy **<name>** type **twping round-trip loss** ...
- set service path-monitor policy **<name>** type **twping round-trip time** ...
- set service path-monitor policy **<name>** type **twping send jitter** ...
- set service path-monitor policy **<name>** type **twping send time** ...
- set service path-monitor monitor **<name>** type **twping...**
- set service path-monitor monitor **<name>** type {ping | twping} routing-instance **<ri-name>**

Firewall/QoS: Make the Policer Overhead configurable

This feature allows configuration of L2 overheads which are added to a packet during transmission over Ethernet

The following configuration mode commands are used:

- set policy qos name "name" shaper class "id" match "name" police frame-overhead "inherit | 0-1000"
- set policy action name "name" police frame-overhead "inherit | 0-1000"

QoS: Make Qlimit for WRED configurable

This feature adds support for weighted random early detection (WRED) queues up to 8192 packets long

The following configuration mode commands are used:

- set policy qos name <policy-name> shaper traffic-class <0..3> random-detect max-threshold <1.8191>
- set policy qos name <policy-name> shaper traffic-class <0..3> random-detect min-threshold <1..8190>

Firewall/QoS: Add Aggregate Policer capability for a set of class matches

This feature adds resource groups of IP protocol values, resource groups of DSCP values and action group to be configured which can contain one or more features. These groups can then be used in firewall and QoS.

The following configuration mode commands are used:

- policy actions group [name]
- set resource group dscp-group <name> description <description> dscp <valid-dscp-value> [a list of values]
- set resource group protocol-group <name> description <description> protocol <valid-protocol-value> [a list of values]

CPU Tuning Support in VNF Platform

This feature allows the pinning individual virtual CPUs to their own cpuset.

The following configuration mode commands are used:

- set virtualization guest <N> vcpupin vcpu <M> cpuset <P>

UEFI Secure Boot

This feature enables cryptographically signing the boot loader, the kernel image and any kernel modules with an x509 certificate

There are no related configuration commands.

Modified features

There are no modified features in this release.

Deprecated features

There are no deprecated features in this release.

CLI Commands and API Calls

CLI commands

New commands

New configuration commands

The following is an exhaustive list of configuration commands have been added to this release.

TCP SYN Packet MSS Clamping

```
interfaces bonding <tagnode> ip tcp-mss
interfaces bonding <tagnode> ip tcp-mss limit <value>
interfaces bonding <tagnode> ip tcp-mss mtu
interfaces bonding <tagnode> ip tcp-mss mtu-minus <value>
interfaces bonding <tagnode> ipv6 tcp-mss
interfaces bonding <tagnode> ipv6 tcp-mss limit <value>
interfaces bonding <tagnode> ipv6 tcp-mss mtu
interfaces bonding <tagnode> ipv6 tcp-mss mtu-minus <value>
interfaces bonding <tagnode> vif <tagnode> ip tcp-mss
interfaces bonding <tagnode> vif <tagnode> ip tcp-mss limit <value>
interfaces bonding <tagnode> vif <tagnode> ip tcp-mss mtu
interfaces bonding <tagnode> vif <tagnode> ip tcp-mss mtu-minus <value>
interfaces bonding <tagnode> vif <tagnode> ipv6 tcp-mss
interfaces bonding <tagnode> vif <tagnode> ipv6 tcp-mss limit <value>
interfaces bonding <tagnode> vif <tagnode> ipv6 tcp-mss mtu
interfaces bonding <tagnode> vif <tagnode> ipv6 tcp-mss mtu-minus <value>
interfaces bridge <tagnode> ip tcp-mss
interfaces bridge <tagnode> ip tcp-mss limit <value>
interfaces bridge <tagnode> ip tcp-mss mtu
interfaces bridge <tagnode> ip tcp-mss mtu-minus <value>
interfaces bridge <tagnode> ipv6 tcp-mss
interfaces bridge <tagnode> ipv6 tcp-mss limit <value>
interfaces bridge <tagnode> ipv6 tcp-mss mtu
interfaces bridge <tagnode> ipv6 tcp-mss mtu-minus <value>
interfaces dataplane <tagnode> ip tcp-mss
interfaces dataplane <tagnode> ip tcp-mss limit <value>
interfaces dataplane <tagnode> ip tcp-mss mtu
interfaces dataplane <tagnode> ip tcp-mss mtu-minus <value>
interfaces dataplane <tagnode> ipv6 tcp-mss
interfaces dataplane <tagnode> ipv6 tcp-mss limit <value>
interfaces dataplane <tagnode> ipv6 tcp-mss mtu
```

```
interfaces dataplane <tagnode> ipv6 tcp-mss mtu-minus <value>
interfaces dataplane <tagnode> vif <tagnode> ip tcp-mss
interfaces dataplane <tagnode> vif <tagnode> ip tcp-mss limit <value>
interfaces dataplane <tagnode> vif <tagnode> ip tcp-mss mtu
interfaces dataplane <tagnode> vif <tagnode> ip tcp-mss mtu-minus <value>
interfaces dataplane <tagnode> vif <tagnode> ipv6 tcp-mss
interfaces dataplane <tagnode> vif <tagnode> ipv6 tcp-mss limit <value>
interfaces dataplane <tagnode> vif <tagnode> ipv6 tcp-mss mtu
interfaces dataplane <tagnode> vif <tagnode> ipv6 tcp-mss mtu-minus <value>
interfaces l2tpeth <tagnode> ip tcp-mss
interfaces l2tpeth <tagnode> ip tcp-mss limit <value>
interfaces l2tpeth <tagnode> ip tcp-mss mtu
interfaces l2tpeth <tagnode> ip tcp-mss mtu-minus <value>
interfaces l2tpeth <tagnode> ipv6 tcp-mss
interfaces l2tpeth <tagnode> ipv6 tcp-mss limit <value>
interfaces l2tpeth <tagnode> ipv6 tcp-mss mtu
interfaces l2tpeth <tagnode> ipv6 tcp-mss mtu-minus <value>
interfaces l2tpeth <tagnode> vif <tagnode> ip tcp-mss
interfaces l2tpeth <tagnode> vif <tagnode> ip tcp-mss limit <value>
interfaces l2tpeth <tagnode> vif <tagnode> ip tcp-mss mtu
interfaces l2tpeth <tagnode> vif <tagnode> ip tcp-mss mtu-minus <value>
interfaces l2tpeth <tagnode> vif <tagnode> ipv6 tcp-mss
interfaces l2tpeth <tagnode> vif <tagnode> ipv6 tcp-mss limit <value>
interfaces l2tpeth <tagnode> vif <tagnode> ipv6 tcp-mss mtu
interfaces l2tpeth <tagnode> vif <tagnode> ipv6 tcp-mss mtu-minus <value>
interfaces openvpn <tagnode> ip tcp-mss
interfaces openvpn <tagnode> ip tcp-mss limit <value>
interfaces openvpn <tagnode> ip tcp-mss mtu
interfaces openvpn <tagnode> ip tcp-mss mtu-minus <value>
interfaces openvpn <tagnode> ipv6 tcp-mss
interfaces openvpn <tagnode> ipv6 tcp-mss limit <value>
interfaces openvpn <tagnode> ipv6 tcp-mss mtu
interfaces openvpn <tagnode> ipv6 tcp-mss mtu-minus <value>
interfaces tunnel <tagnode> ip tcp-mss
interfaces tunnel <tagnode> ip tcp-mss limit <value>
interfaces tunnel <tagnode> ip tcp-mss mtu
interfaces tunnel <tagnode> ip tcp-mss mtu-minus <value>
interfaces tunnel <tagnode> ipv6 tcp-mss
interfaces tunnel <tagnode> ipv6 tcp-mss limit <value>
interfaces tunnel <tagnode> ipv6 tcp-mss mtu
interfaces tunnel <tagnode> ipv6 tcp-mss mtu-minus <value>
interfaces vti <tagnode> ip tcp-mss
interfaces vti <tagnode> ip tcp-mss limit <value>
interfaces vti <tagnode> ip tcp-mss mtu
interfaces vti <tagnode> ip tcp-mss mtu-minus <value>
interfaces vti <tagnode> ipv6 tcp-mss
interfaces vti <tagnode> ipv6 tcp-mss limit <value>
interfaces vti <tagnode> ipv6 tcp-mss mtu
interfaces vti <tagnode> ipv6 tcp-mss mtu-minus <value>
```

Policy Based IPSEC with Firewalls and DNAT/SNAT

```
interfaces virtual-feature-point <ifname>
interfaces virtual-feature-point <ifname> address <value>
interfaces virtual-feature-point <ifname> description <value>
interfaces virtual-feature-point <ifname> disable
interfaces virtual-feature-point <ifname> ip tcp-mss
interfaces virtual-feature-point <ifname> ip tcp-mss limit <value>
interfaces virtual-feature-point <ifname> ipv6 tcp-mss
interfaces virtual-feature-point <ifname> ipv6 tcp-mss limit <value>
interfaces virtual-feature-point <ifname> mtu <value>

interfaces virtual-feature-point <ifname> ip unnumbered donor-interface <tagnode>
interfaces virtual-feature-point <ifname> ip unnumbered donor-interface <tagnode>
      preferred-address <value>
interfaces virtual-feature-point <ifname> ipv6 unnumbered donor-interface <tagnode>
interfaces virtual-feature-point <ifname> ipv6 unnumbered donor-interface <tagnode>
      preferred-address <value>
```

```
interfaces virtual-feature-point <ifname> firewall in <value>
interfaces virtual-feature-point <ifname> firewall local <value>
interfaces virtual-feature-point <ifname> firewall out <value>

interfaces virtual-feature-point <ifname> policy route pbr <value>

security firewall name <ruleset-name> rule <tagnode> dscp-group <value>
security firewall name <ruleset-name> rule <tagnode> protocol-group <value>

security vpn ipsec site-to-site peer <tagnode> tunnel <tagnode> uses <value>
```

VXLAN Tunnel Support

```
interfaces tunnel <tagnode> encapsulation vxlan
interfaces tunnel <tagnode> encapsulation vxlan-gpe
interfaces tunnel <tagnode> transport multicast-group <value>
interfaces tunnel <tagnode> vxlan-id <value>
interfaces tunnel <tagnode> transport routing-instance <value>
```

Firewall/QoS: Make the Policer Overhead configurable

```
policy action
policy action name <id>
policy action name <id> mark dscp af11
policy action name <id> mark dscp af12
policy action name <id> mark dscp af13
policy action name <id> mark dscp af21
policy action name <id> mark dscp af22
policy action name <id> mark dscp af23
policy action name <id> mark dscp af31
policy action name <id> mark dscp af32
policy action name <id> mark dscp af33
policy action name <id> mark dscp af41
policy action name <id> mark dscp af42
policy action name <id> mark dscp af43
policy action name <id> mark dscp cs1
policy action name <id> mark dscp cs2
policy action name <id> mark dscp cs3
policy action name <id> mark dscp cs4
policy action name <id> mark dscp cs5
policy action name <id> mark dscp cs6
policy action name <id> mark dscp cs7
policy action name <id> mark dscp default
policy action name <id> mark dscp ef
policy action name <id> mark dscp va
policy action name <id> mark pcp <value>
policy action name <id> police
policy action name <id> police bandwidth <value>
policy action name <id> police burst <value>
policy action name <id> police frame-overhead <value>
policy action name <id> police ratelimit <value>
policy action name <id> police then action drop
policy action name <id> police then mark dscp af11
policy action name <id> police then mark dscp af12
policy action name <id> police then mark dscp af13
policy action name <id> police then mark dscp af21
policy action name <id> police then mark dscp af22
policy action name <id> police then mark dscp af23
policy action name <id> police then mark dscp af31
policy action name <id> police then mark dscp af32
policy action name <id> police then mark dscp af33
policy action name <id> police then mark dscp af41
policy action name <id> police then mark dscp af42
policy action name <id> police then mark dscp af43
policy action name <id> police then mark dscp cs1
policy action name <id> police then mark dscp cs2
policy action name <id> police then mark dscp cs3
policy action name <id> police then mark dscp cs4
```

```
policy action name <id> police then mark dscp cs5
policy action name <id> police then mark dscp cs6
policy action name <id> police then mark dscp cs7
policy action name <id> police then mark dscp default
policy action name <id> police then mark dscp ef
policy action name <id> police then mark dscp va
policy action name <id> police then mark pcp <value>

policy qos name <id> shaper class <id> match <id> action-group <value>
policy qos name <id> shaper class <id> match <id> dscp-group <value>
policy qos name <id> shaper class <id> match <id> police frame-overhead <value>
policy qos name <id> shaper class <id> match <id> protocol-group <value>
policy qos profile <id>
policy qos profile <id> bandwidth <value>
policy qos profile <id> burst <value>
policy qos profile <id> description <value>
policy qos profile <id> map dscp <id>
policy qos profile <id> map dscp <id> to <value>
policy qos profile <id> map pcp <id>
policy qos profile <id> map pcp <id> to <value>
policy qos profile <id> period <value>
policy qos profile <id> queue <id>
policy qos profile <id> queue <id> description <value>
policy qos profile <id> queue <id> traffic-class <value>
policy qos profile <id> queue <id> weight <value>
policy qos profile <id> traffic-class <id>
policy qos profile <id> traffic-class <id> bandwidth <value>
policy qos profile <id> traffic-class <id> description <value>

resources group address-group <tagnode> address-range <start>
resources group address-group <tagnode> address-range <start> to <value>
resources group dscp-group <group-name>
resources group dscp-group <group-name> description <value>
resources group dscp-group <group-name> dscp af11
resources group dscp-group <group-name> dscp af12
resources group dscp-group <group-name> dscp af13
resources group dscp-group <group-name> dscp af21
resources group dscp-group <group-name> dscp af22
resources group dscp-group <group-name> dscp af23
resources group dscp-group <group-name> dscp af31
resources group dscp-group <group-name> dscp af32
resources group dscp-group <group-name> dscp af33
resources group dscp-group <group-name> dscp af41
resources group dscp-group <group-name> dscp af42
resources group dscp-group <group-name> dscp af43
resources group dscp-group <group-name> dscp cs1
resources group dscp-group <group-name> dscp cs2
resources group dscp-group <group-name> dscp cs3
resources group dscp-group <group-name> dscp cs4
resources group dscp-group <group-name> dscp cs5
resources group dscp-group <group-name> dscp cs6
resources group dscp-group <group-name> dscp cs7
resources group dscp-group <group-name> dscp default
resources group dscp-group <group-name> dscp ef
resources group dscp-group <group-name> dscp va
resources group protocol-group <group-name>
resources group protocol-group <group-name> description <value>
resources group protocol-group <group-name> protocol <value>
```

Assign Cost to Summary Route in OSPFv2 and OSPFv3

```
protocols ospf area <tagnode> range <tagnode> metric <value>
protocols ospf process <instance> area <tagnode> range <tagnode> metric <value>

routing routing-instance <instance-name> protocols ospf process <instance> area <tagnode>
       range <tagnode> metric <value>

protocols ospfv3 address-family ipv4 unicast area <tagnode> range <tagnode> metric <value>
```

```
protocols ospfv3 area <tagnode> range <tagnode> metric <value>
protocols ospfv3 process <tagnode> address-family ipv4 unicast area <tagnode> range
      <tagnode> metric <value>
protocols ospfv3 process <tagnode> area <tagnode> range <tagnode> metric <value>

routing routing-instance <instance-name> protocols ospfv3 process <process-name> address-family
      ipv4 unicast area <tagnode> range <tagnode> metric <value>
routing routing-instance <instance-name> protocols ospfv3 process <process-name> area <tagnode>
      range <tagnode> metric <value>

protocols rip log bfd
```

Assign Tag to Static Route

```
protocols static interface-route <tagnode> next-hop-interface <tagnode> tag <value>
protocols static interface-route6 <tagnode> next-hop-interface <tagnode> tag <value>
protocols static route <tagnode> blackhole tag <value>
protocols static route <tagnode> next-hop <tagnode> tag <value>
protocols static route <tagnode> unreachable tag <value>
protocols static route6 <tagnode> blackhole tag <value>
protocols static route6 <tagnode> next-hop <tagnode> tag <value>
protocols static route6 <tagnode> unreachable tag <value>

routing routing-instance <instance-name> protocols static interface-route <tagnode>
      next-hop-interface <tagnode> tag <value>
routing routing-instance <instance-name> protocols static interface-route6 <tagnode>
      next-hop-interface <tagnode> tag <value>
routing routing-instance <instance-name> protocols static route <tagnode> blackhole tag <value>
routing routing-instance <instance-name> protocols static route <tagnode> next-hop <tagnode>
      tag <value>
routing routing-instance <instance-name> protocols static route <tagnode> unreachable
      tag <value>
routing routing-instance <instance-name> protocols static route6 <tagnode> blackhole tag <value>
routing routing-instance <instance-name> protocols static route6 <tagnode> next-hop <tagnode>
      tag <value>
routing routing-instance <instance-name> protocols static route6 <tagnode> unreachable
      tag <value>

protocols static interface-route <tagnode> next-hop-routing-instance <routing-instance>
      next-hop-interface <interface-name> tag <value>
protocols static interface-route6 <tagnode> next-hop-routing-instance <routing-instance>
      next-hop-interface <interface-name> tag <value>
protocols static route <tagnode> next-hop-routing-instance <routing-instance> next-hop <tagnode>
      tag <value>
protocols static route6 <tagnode> next-hop-routing-instance <routing-instance>
      next-hop <tagnode> tag <value>
routing routing-instance <instance-name> protocols static interface-route <tagnode>
      next-hop-routing-instance <routing-instance> next-hop-interface <interface-name>
      tag <value>
routing routing-instance <instance-name> protocols static interface-route6 <tagnode>
      next-hop-routing-instance <routing-instance> next-hop-interface <interface-name>
      tag <value>
routing routing-instance <instance-name> protocols static route <tagnode>
      next-hop-routing-instance <routing-instance> next-hop <tagnode> tag <value>
routing routing-instance <instance-name> protocols static route6 <tagnode>
      next-hop-routing-instance-v6 <routing-instance> next-hop <tagnode> tag <value>
```

IP-SLA Support

```
service path-monitor monitor <name> history policy-state-change <value>
service path-monitor monitor <name> history results <value>

service path-monitor monitor <name> compliance-status-override disabled
service path-monitor monitor <name> compliance-status-override enabled

service path-monitor host <name> type ping data-size <value>
service path-monitor policy <name> requires type ping jitter
service path-monitor policy <name> requires type ping jitter robustness <value>
service path-monitor policy <name> requires type ping jitter threshold <value>
```

```
service path-monitor policy <name> requires type ping jitter tolerance <value>
service path-monitor policy <name> requires type ping loss robustness <value>
service path-monitor policy <name> requires type ping loss threshold <value>
service path-monitor policy <name> requires type ping loss tolerance <value>

service path-monitor monitor <name> type ping routing-instance <value>
service path-monitor monitor <name> type ping routing-instance default

service path-monitor host <name> type twping
service path-monitor host <name> type twping control-port <value>
service path-monitor host <name> type twping dscp af11
service path-monitor host <name> type twping dscp af12
service path-monitor host <name> type twping dscp af13
service path-monitor host <name> type twping dscp af21
service path-monitor host <name> type twping dscp af22
service path-monitor host <name> type twping dscp af23
service path-monitor host <name> type twping dscp af31
service path-monitor host <name> type twping dscp af32
service path-monitor host <name> type twping dscp af33
service path-monitor host <name> type twping dscp af41
service path-monitor host <name> type twping dscp af42
service path-monitor host <name> type twping dscp af43
service path-monitor host <name> type twping dscp cs1
service path-monitor host <name> type twping dscp cs2
service path-monitor host <name> type twping dscp cs3
service path-monitor host <name> type twping dscp cs4
service path-monitor host <name> type twping dscp cs5
service path-monitor host <name> type twping dscp cs6
service path-monitor host <name> type twping dscp cs7
service path-monitor host <name> type twping dscp default
service path-monitor host <name> type twping dscp ef
service path-monitor host <name> type twping dscp va
service path-monitor host <name> type twping padding <value>
service path-monitor host <name> type twping port-range end <value>
service path-monitor host <name> type twping port-range start <value>
service path-monitor host <name> type twping source-address <value>
service path-monitor monitor <name> type twping
service path-monitor monitor <name> type twping host <value>
service path-monitor monitor <name> type twping interface <value>
service path-monitor monitor <name> type twping interval <value>
service path-monitor policy <name> requires type twping
service path-monitor policy <name> requires type twping reflect jitter
service path-monitor policy <name> requires type twping reflect jitter robustness <value>
service path-monitor policy <name> requires type twping reflect jitter threshold <value>
service path-monitor policy <name> requires type twping reflect jitter tolerance <value>
service path-monitor policy <name> requires type twping reflect time
service path-monitor policy <name> requires type twping reflect time robustness <value>
service path-monitor policy <name> requires type twping reflect time threshold <value>
service path-monitor policy <name> requires type twping reflect time tolerance <value>
service path-monitor policy <name> requires type twping round-trip jitter
service path-monitor policy <name> requires type twping round-trip jitter robustness <value>
service path-monitor policy <name> requires type twping round-trip jitter threshold <value>
service path-monitor policy <name> requires type twping round-trip jitter tolerance <value>
service path-monitor policy <name> requires type twping round-trip loss robustness <value>
service path-monitor policy <name> requires type twping round-trip loss threshold <value>
service path-monitor policy <name> requires type twping round-trip loss tolerance <value>
service path-monitor policy <name> requires type twping round-trip time
service path-monitor policy <name> requires type twping round-trip time robustness <value>
service path-monitor policy <name> requires type twping round-trip time threshold <value>
service path-monitor policy <name> requires type twping round-trip time tolerance <value>
service path-monitor policy <name> requires type twping send jitter
service path-monitor policy <name> requires type twping send jitter robustness <value>
service path-monitor policy <name> requires type twping send jitter threshold <value>
service path-monitor policy <name> requires type twping send jitter tolerance <value>
service path-monitor policy <name> requires type twping send time
service path-monitor policy <name> requires type twping send time robustness <value>
service path-monitor policy <name> requires type twping send time threshold <value>
```

```
service path-monitor policy <name> requires type twping send time tolerance <value>

service path-monitor monitor <name> type twping routing-instance <value>
service path-monitor monitor <name> type twping routing-instance default

policy route pbr <tagnode> rule <tagnode> dscp-group <value>
policy route pbr <tagnode> rule <tagnode> protocol-group <value>

service twamp server use-legacy-authentication

routing routing-instance <instance-name> service twamp server use-legacy-authentication
```

Other

```
service diamond session-name <name> collector netconf get path-map <path>
service diamond session-name <name> collector netconf get path-map <path> to <value>

interfaces bonding <tagnode> cpu-affinity <value>
interfaces bonding <tagnode> receive-cpu-affinity <value>
interfaces bonding <tagnode> transmit-cpu-affinity <value>

interfaces dataplane <tagnode> receive-cpu-affinity <value>
interfaces dataplane <tagnode> transmit-cpu-affinity <value>

system modems
system modems connection-settings <connection-name>
system modems connection-settings <connection-name> apn <value>
system modems connection-settings <connection-name> interface <name>
system modems connection-settings <connection-name> number <value>
system modems connection-settings <connection-name> password <value>
system modems connection-settings <connection-name> pin <value>
system modems connection-settings <connection-name> user <value>
```

New operational commands

The following operational commands have been added to this release.

```
show vxlan mac [ interface <if-name> ] [ mac <macaddr> ]
clear vxlan mac [ interface <if-name> ] [ mac <mac-address> ]

show ip ospf database summary self-originate
show ipv6 ospfv3 database inter-prefix self-originate

show service path-monitor average [monitor <monitor>]
show service path-monitor history [monitor <monitor>]
show service path-monitor state-change [monitor <monitor>] [detail]
clear path-monitor history [monitor <monitor>]
clear path-monitor state-change [monitor <monitor>]
clear path-monitor average [monitor <monitor>

show virtualization guest <guest> vcpuinfo
show virtualization guest <guest> vcpuinfo
```

Modified commands

There are no modified commands in this release.

Deprecated commands

The following commands have been deprecated in this release

```
service diamond session-name <name> collector netconf get path <value>
```

```
system ip arp
```

Modified API calls

New API calls

The following NetConf RPC calls have been added

```
set-compliance-status input monitor <value>
set-compliance-status input policy <value>
set-compliance-status input status automatic
set-compliance-status input status compliant
set-compliance-status input status non-compliant
set-compliance-status input timeout <value>

twping input interface <value>
twping input source-address <value>

lookup-rpc-destination-by-module-name input module-name <value>
lookup-rpc-destination-by-module-name output destination <value>
validate-notification input input <value>
validate-notification input module-name <value>
validate-notification input name <value>
validate-notification input namespace <value>
validate-notification output output <value>
```

The following Operational State commands have been added to the NetConf API;

```
 interfaces virtual-feature-point <ifname> policy route pbr-state name <group-name>
interfaces virtual-feature-point <ifname> policy route pbr-state name <group-name>
       rule <rule-number>
interfaces virtual-feature-point <ifname> policy route pbr-state name <group-name>
       rule <rule-number> bytes <value>
interfaces virtual-feature-point <ifname> policy route pbr-state name <group-name>
       rule <rule-number> packets <value>

policy qos state if-list <ifname> shaper subport-list <subport> rules groups <name>
       rule <rule-number> action-group <value>
policy qos state if-list <ifname> shaper subport-list <subport> rules groups <name>
       rule <rule-number> exceeded-bytes <value>
policy qos state if-list <ifname> shaper subport-list <subport> rules groups <name>
       rule <rule-number> exceeded-packets <value>

interfaces virtual-feature-point <ifname> firewall state in name <group-name>
interfaces virtual-feature-point <ifname> firewall state in name <group-name> rule <rule-number>
interfaces virtual-feature-point <ifname> firewall state in name <group-name> rule <rule-number>
       bytes <value>
interfaces virtual-feature-point <ifname> firewall state in name <group-name> rule <rule-number>
       packets <value>
interfaces virtual-feature-point <ifname> firewall state local name <group-name>
interfaces virtual-feature-point <ifname> firewall state local name <group-name>
       rule <rule-number>
interfaces virtual-feature-point <ifname> firewall state local name <group-name>
       rule <rule-number> bytes <value>
interfaces virtual-feature-point <ifname> firewall state local name <group-name>
       rule <rule-number> packets <value>
interfaces virtual-feature-point <ifname> firewall state out name <group-name>
interfaces virtual-feature-point <ifname> firewall state out name <group-name>
       rule <rule-number>
interfaces virtual-feature-point <ifname> firewall state out name <group-name>
       rule <rule-number> bytes <value>
```

```
interfaces virtual-feature-point <ifname> firewall state out name <group-name>
       rule <rule-number> packets <value>

service path-monitor status monitor <name> averages jitter <value>
service path-monitor status monitor <name> averages loss <value>
service path-monitor status monitor <name> averages rtt <value>
service path-monitor status monitor <name> averages timestamp <value>
service path-monitor status monitor <name> policy <name> history <timestamp> jitter <value>
service path-monitor status monitor <name> policy <name> history <timestamp> loss <value>
service path-monitor status monitor <name> policy <name> history <timestamp> rtt <value>
service path-monitor status monitor <name> results <timestamp>
service path-monitor status monitor <name> results <timestamp> failure-reason <value>
service path-monitor status monitor <name> results <timestamp> jitter <value>
service path-monitor status monitor <name> results <timestamp> loss <value>
service path-monitor status monitor <name> results <timestamp> rtt <value>
service path-monitor status monitor <name> type <value>

service path-monitor status monitor <name> policy <name> overridden-state Compliant
service path-monitor status monitor <name> policy <name> overridden-state Marginally Compliant
service path-monitor status monitor <name> policy <name> overridden-state Non-Compliant
service path-monitor status monitor <name> policy <name> overridden-state Unknown
service path-monitor status monitor <name> policy <name> overridden-state-expiry <value>

system modem-state modems <equipment-identifier>
system modem-state modems <equipment-identifier> manufacturer <value>
system modem-state modems <equipment-identifier> model <value>
system modem-state modems <equipment-identifier> ports <name>
system modem-state modems <equipment-identifier> ports <name> type AT
system modem-state modems <equipment-identifier> ports <name> type GPS
system modem-state modems <equipment-identifier> ports <name> type MBIM
system modem-state modems <equipment-identifier> ports <name> type QCDM
system modem-state modems <equipment-identifier> ports <name> type QMI
system modem-state modems <equipment-identifier> ports <name> type Unknown
system modem-state modems <equipment-identifier> ports <name> type net
system modem-state modems <equipment-identifier> revision <value>
system modem-state modems <equipment-identifier> signal-quality <value>
system modem-state modems <equipment-identifier> state Connected
system modem-state modems <equipment-identifier> state Connecting
system modem-state modems <equipment-identifier> state Disabled
system modem-state modems <equipment-identifier> state Disabling
system modem-state modems <equipment-identifier> state Disconnecting
system modem-state modems <equipment-identifier> state Enabled
system modem-state modems <equipment-identifier> state Enabling
system modem-state modems <equipment-identifier> state Failed
system modem-state modems <equipment-identifier> state Initializing
system modem-state modems <equipment-identifier> state Locked
system modem-state modems <equipment-identifier> state Registered
system modem-state modems <equipment-identifier> state Searching
system modem-state modems <equipment-identifier> state Unknown.
```

Modified API calls

There following NetConf RPC calls has been modified

```
- validate-rpc-input input rpc-model-name <value>
+ validate-rpc-input input rpc-module-name <value>
```

Deprecated API calls

There are no deprecated API calls in this release.

MIBs

New MIBs

There are no new MIBs in this release.

Modified MIBs

There are no modified MIBs in this release.

Deprecated MIBs

There are no deprecated MIBs in this release.

RFCs and Standards

No RFCs or standards are changed in this release.

Hardware Support

Supported NICs

The following table lists, by vendor and model, network interface cards (NICs) that are supported by the Vyatta Network OS data plane for bare-metal installations, PCI-passthrough, or SR-IOV configurations.

NIC vendor and model	Description	Controller type
Intel 82598, 82598AF, 82598AT, 82598AT2, 8259EB, 82599EB, 82599EN, 82599ES (X520-2)	Dual 10 GbE with SFP+	82599EB
Intel 82599ES	10 GbE with SFI/SFP+	
Intel X540T1, X540T2, X540AT2	Dual 10 GbE copper	X540
Intel X520	Dual 10 GbE fiber	

NIC vendor and model	Description	Controller type
Intel 82504, 82545, 82546, 82571, 82572, 82573, 82574, 82583	1 GbE	E1000-style single-queue device
Intel 82575, 82576, 82580, I350, I210, I211, I354, DH89XXC	1 GbE	Multiqueue device
Intel Ethernet Controller XL710	Converged Network Adapter XL710 10/40 GbE	I40E

Supported NICs

NOTE
The Vyatta Network OS supports the Wind River Accelerated Virtual Port (AVP) poll-mode virtual NIC driver.

Supported SFP and SFP+ Transceivers

A VNF Platform image that runs on a SuperMicro E300-8D system supports the following SFP and SFP+ transceivers:

- 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

Software Upgrade

There are no specific upgrade considerations for release 1801.

Limitations and Restrictions

IPv6 is not supported on the 40G Fortville NIC.

Xlan tunnels do not currently work with a multicast transport. That is the command *set interfaces vxlan xxx transport multicast-group* does not work

vxlan-gpe tunnel cannot be added to a bridge-group due to an underlying kernel issue

While the OS does support IKEv1, AT&T Vyatta strongly recommends that IKEv2 is used to avoid security vulnerabilities associated with IKEv1, such as reflector and Amplifier DoS attacks.

VRRP in RFC Compatibility mode does not work fully on VRFs. Without RFC compatibility mode, VRRP will work fine with VRFs and this should be used as the solution.

The application of the fixes for DSA-4078-1 [Meltdown] affect the performance of the linux kernel. This affect is well publicised and should diminish in effect as the linux community works on better fixes and subsequent releases are made.

Defects

Security Vulnerabilities

The following security issues are resolved in this release:

- [CVE-2017-5754] Debian DSA-4078-1 : linux - security update, Kernel page-table isolation (KPTI), rogue data cache load aka. variant #3 - Meltdown (VRVDR-40027 and VRVDR-40028)
- [CVE-2017-11408, CVE-2017-13766, CVE-2017-17083, CVE-2017-17084, CVE-2017-17085] Debian DSA-4060-1 : wireshark - security update (VRVDR-39734)
- [CVE-2017-8816, CVE-2017-8817] DSA-4051-1 curl -- security update (VRVDR-39552)
- [CVE-2017-14316, CVE-2017-14317, CVE-2017-14318, CVE-2017-14319, CVE-2017-15588, CVE-2017-15589, CVE-2017-15590, CVE-2017-15592, CVE-2017-15593, CVE-2017-15594, CVE-2017-15595, CVE-2017-15597, CVE-2017-17044, CVE-2017-17045, CVE-2017-17046] DSA-4050-1 xen -- security update (VRVDR-39551)
- [CVE-2017-10672] DSA-4042-1 libxml-libxml-perl -- security update (VRVDR-39363)
- [CVE-2017-0898, CVE-2017-0903, CVE-2017-10784, CVE-2017-14033] DSA-4031-1 ruby2.3 -- security update (VRVDR-39313)
- [CVE-2017-3735, CVE-2017-3736] DSA-4018-1 openssl - security update (VRVDR-39248)
- [CVE-2017-16227] DSA-4011-1 quagga -- security update (VRVDR-39206)
- [CVE-2017-1000257] Debian DSA-4007-1 : curl - security update (VRVDR-39182)
- [CVE-2017-1000256] DSA-4003-1 libvirt -- security update (VRVDR-39125)
- [CVE-2017-7805] Debian DSA-3998-1 : nss - security update (VRVDR-38972)
- [CVE-2017-1000100, CVE-2017-1000101,CVE-2017-1000254] Debian DSA-3992-1 : curl - security update (VRVDR-38890)

- [CVE-2017-9375, CVE-2017-12809, CVE-2017-13672, CVE-2017-13711, CVE-2017-14167] DSA-3991-1 qemu -- security update (VRVDR-38841)
- [CVE-2017-14491, CVE-2017-14492, CVE-2017-14493, CVE-2017-14494, CVE-2017-14495, CVE-2017-14496: DSA-3989-1] dnsmasq -- security update (VRVDR-38819)
- [CVE-2017-14062] DSA-3988-1 libidn2-0 -- security update (VRVDR-38806)
- [CVE-2017-7518, CVE-2017-7558, CVE-2017-10661, CVE-2017-11600, CVE-2017-12134, CVE-2017-12146, CVE-2017-12153, CVE-2017-12154, CVE-2017-14106, CVE-2017-14140, CVE-2017-14156, CVE-2017-14340, CVE-2017-14489, CVE-2017-14497, CVE-2017-1000111, CVE-2017-1000112, CVE-2017-1000251, CVE-2017-1000252, CVE-2017-1000370, CVE-2017-1000371, CVE-2017-1000380] DSA-3981-1 linux -- security update (VRVDR-38517)
- [CVE-2017-11108, CVE-2017-11541, CVE-2017-11542, CVE-2017-11543, CVE-2017-12893, CVE-2017-12894, CVE-2017-12895, CVE-2017-12896, CVE-2017-12897, CVE-2017-12898, CVE-2017-12899, CVE-2017-12900, CVE-2017-12901, CVE-2017-12902, CVE-2017-12985, CVE-2017-12986, CVE-2017-12987, CVE-2017-12988, CVE-2017-12989, CVE-2017-12990, CVE-2017-12991, CVE-2017-12992, CVE-2017-12993, CVE-2017-12994, CVE-2017-12995, CVE-2017-12996, CVE-2017-12997, CVE-2017-12998, CVE-2017-12999, CVE-2017-13000, CVE-2017-13001, CVE-2017-13002, CVE-2017-13003, CVE-2017-13004, CVE-2017-13005, CVE-2017-13006, CVE-2017-13007, CVE-2017-13008, CVE-2017-13009, CVE-2017-13010, CVE-2017-13011, CVE-2017-13012, CVE-2017-13013, CVE-2017-13014, CVE-2017-13015, CVE-2017-13016, CVE-2017-13017, CVE-2017-13018, CVE-2017-13019, CVE-2017-13020, CVE-2017-13021, CVE-2017-13022, CVE-2017-13023, CVE-2017-13024, CVE-2017-13025, CVE-2017-13026, CVE-2017-13027, CVE-2017-13028, CVE-2017-13029, CVE-2017-13030, CVE-2017-13031, CVE-2017-13032, CVE-2017-13033, CVE-2017-13034, CVE-2017-13035, CVE-2017-13036, CVE-2017-13037, CVE-2017-13038, CVE-2017-13039, CVE-2017-13040, CVE-2017-13041, CVE-2017-13042, CVE-2017-13043, CVE-2017-13044, CVE-2017-13045, CVE-2017-13046, CVE-2017-13047, CVE-2017-13048, CVE-2017-13049, CVE-2017-13050, CVE-2017-13051, CVE-2017-13052, CVE-2017-13053, CVE-2017-13054, CVE-2017-13055, CVE-2017-13687, CVE-2017-13688, CVE-2017-13689, CVE-2017-13690, CVE-2017-13725] DSA-3971-1 tcpdump security update (VRVDR-38266)
- [CVE-2017-14482: Debian DSA-3970-1] emacs24 - security update (VRVDR-38265)
- [CVE-2015-9096, CVE-2016-7798, CVE-2017-0899, CVE-2017-0900, CVE-2017-0901, CVE-2017-14064] Debian DSA-3966-1 : ruby2.3 - security update (VRVDR-38172)
- [CVE-2017-1000249] Debian DSA-3965-1 : file - security update (VRVDR-38171)
- [CVE-2017-11185] DSA-3962-1 strongswan security update (VRVDR-38153)
- [CVE-2017-0379] Debian DSA-3959-1 : libgcrypt20 - security update (VRVDR-38114)
- [CVE-2017-0663, CVE-2017-7375, CVE-2017-7376, CVE-2017-9047, CVE-2017-9048, CVE-2017-9049, CVE-2017-9050] Debian DSA-3952-1 : libxml2 - security update (VRVDR-38061)

- [CVE-2014-9940, CVE-2017-7346, CVE-2017-7482, CVE-2017-7533, CVE-2017-7541, CVE-2017-7542, CVE-2017-7889, CVE-2017-9605, CVE-2017-10911, CVE-2017-11176, CVE-2017-1000363, CVE-2017-1000365] Debian DSA-3945-1 linux security update (VRVDR-38027)
- [CVE-2013-5211] Network Time Protocol (NTP) Mode 6 Scanner (VRVDR-37993)
- [CVE-2017-7346, CVE-2017-7482, CVE-2017-7533, CVE-2017-7541, CVE-2017-7542, CVE-2017-9605, CVE-2017-10810, CVE-2017-10911, CVE-2017-11176, CVE-2017-1000365] DSA-3927-1 linux security update (VRVDR-37959)
- [CVE-2017-9310, CVE-2017-9330, CVE-2017-9373, CVE-2017-9374, CVE-2017-9375, CVE-2017-9524, CVE-2017-10664, CVE-2017-10911] DSA-3920-1 qemu security update (VRVDR-37889)
- [CVE-2017-3142, CVE-2017-3143] Debian DSA-3904-1 : bind9 - security update (VRVDR-37772)
- [CVE-2017-7526: Debian DSA-3901-1 : libgcrypt20 - security update (VRVDR-37751)
- [CVE-2017-7479, CVE-2017-7508, CVE-2017-7520, CVE-2017-7521] Debian DSA-3900-1 : openvpn - security update (VRVDR-37707)
- [CVE-2016-9063, CVE-2017-9233: Debian DSA-3898-1] expat - security update (VRVDR-37694)
- [CVE-2017-1000376] libffi security update (VRVDR-37647)
- [CVE-2017-1000366] DSA-3887-1glibc security update (VRVDR-37644)
- [CVE-2016-10324, CVE-2016-10325, CVE-2016-10326, CVE-2017-7853] Debian DSA-3879-1 : libosip2 - security update (VRVDR-37625)
- [CVE-2017-9526] libgcrypt20 security update (VRVDR-37615)
- [CVE-2008-5161] A vulnerability exists in SSH messages that employ CBC mode (VRVDR-33124)
- [CVE-2016-3739] The (1) mbed_connect_step1 function in lib/vtls/mbedtls.c (VRVDR-28781)
- [CVE-2014-9761] Multiple stack-based buffer overflows in the GNU C Library (aka glibc or libc6) (VRVDR-28636)
- [CVE-2017-16548, CVE-2017-17433, CVE-2017-17434] DSA-4068-1 rsync -- security update (VRVDR-39820)
- [CVE-2017-16536, CVE-2017-1000405] linux security update (VRVDR-39830)
- [CVE-2017-15412] Debian DSA-4086-1 : libxml2 - security update (VRVDR-40019)

Resolved issues

The following table lists the resolved issues in this release:

Component	Key	Summary
Interfaces	VRVDR-39507	some vlan configuration operations fail leaving interface non-operational
OpenVPN	VRVDR-39177	Openvpn server domain-name option not being applied with --push dhcp-option
System	VRVDR-39165	Why does cloud-init take so long to boot and is throwing errors?
Firewall	VRVDR-38960	"Cannot assign loopback interface to a transit zone. It is part of local-zone." error when lo interface is added to a firewall zone
BGP	VRVDR-38913	iBGP Updates sent sooner than MRAI for same route w/ ebgp-multihop '1' configured on ebgp peer
Interfaces	VRVDR-38506	VLAN subinterface counters are incorrect if QOS shaper is applied
OpenVPN	VRVDR-38196	OpenVPN server doesn't push routes to the client
BGP	VRVDR-38162	Please explain relationship of 'un-reachability-half-life' parameter to BGP Dampening Penalty and Suppression Algorithm
System	VRVDR-38150	"set system ip arp" does not give any options / what is the purpose of this command?
BGP	VRVDR-38148	Displayed Reuse time can become greater than max-suppress-time if dampened route is in history but not in RIB.
RIP	VRVDR-38137	RIP Network Admin Distance command doesn't work
DHCP	VRVDR-38083	syntax warning when deleting a dhcp lease from database
IPsec/VPN	VRVDR-38075	When 'restart vpn' is issued from responder, initiator does not re-establish connection
Operational Infrastructure	VRVDR-37958	The "show login" and "show login level" commands reports Admin as Superuser

Component	Key	Summary
BGP	VRVDR-37906	BGP updates are observed sooner than the MinRouteAdvertisementIntervalTimer configured through advertisement-interval
SNMP	VRVDR-37829	snmp port number is not changing from default 161
GUI	VRVDR-37819	ping process keeps running in background if started from Web GUI
IPsec/VPN	VRVDR-37741	IKE cannot complete initialization when interesting traffic is UDP
VRRP	VRVDR-37730	vRouter 5.2R4 is not responding to KEEPALIVED-MIB query after reboot
Entitlement	VRVDR-37717	Rename hard-enf (build B) "Description" and "License" fields in version output
OSPF	VRVDR-37706	show ip ospf neighbor summary command is unreadable
IPv6	VRVDR-37696	IPv6 basic connectivity with VLAN tagging not working
DPDK	VRVDR-37689	High rate of NIC PF interrupts
System	VRVDR-37617	After NTP configuration commit a message "VMware-toolbox-cmd" is returned When config NTP after commit - message "vmware-toolbox-cmd" message is returned
Firewall	VRVDR-37315	'Used' field becomes negative in 'show session-table statistics'
DPDK	VRVDR-37052	Intel i210 NIC reports "no-carrier"
RA_VPN	VRVDR-36378	Client behind NAT is unable to connect to L2TP server
GRE	VRVDR-13641	adding a gre tunnel to a bridge-group causes commit to fail without error message
NAT	VRVDR-39729	dataplane crashes when NAT resource group address has /31 mask
Routing infrastructure	VRVDR-39526	Inter-VRF routing does not work when next hop is interface or next-hop-routing-instance is used

Resolved issues

Known issues

The following table lists the known issues in this release.

Component	Key	Summary
TACACS	VRVDR-15866	TACACS Authentication/Authorization and Accounting out of sync after TACACS servers went offline/online and TACACS user exits session.
Bonding	VRVDR-39750	The 'show interface dataplane <bond-vif>' CLI shows interface statistics but is not a tab completion option under 'show interface dataplane'
Firewall	VRVDR-39772	The 'show log' and 'show log firewall name <FW-RULE>' command no longer displays firewall logs
Firewall	VRVDR-38978	ZBF doesn't allow stateful tracking for locally sourced traffic
QinQ	VRVDR-39860	Commit doesn’t complete and Rollback doesn’t complete properly
GRE	VRVDR-39863	VRRP fails over when customer removes routing-instance with GRE associated and tunnel local-address is part of VRRP
GRE	VRVDR-39985	TCP DF Packets larger than GRE tunnel MTU are dropped with no ICMP fragmentation needed returned
Firewall	VRVDR-39991	Stateful firewall drops packets between 2 subnets on the same interface
NAT	VRVDR-40210	Traceroute does not work when SNAT is enabled on vNAT
NAT	VRVDR-40211	delete session-table source <IP-address:port> and delete session-table destination <IP-address:port> do not work

Known issues