Vyatta—A Brocade Company | Release Notes

Vyatta Release 3.5R5

August 2015

Document Part No. 53-1003886-01

Vyatta
San Jose, CA 95134
www.brocade.com
408 333 8400

Contents

The Vyatta Release 3.5R5 release notes include the following sections:

Security

3.5R5 RELEASE

The following security issues are resolved in this release:

- [CVE-2015-1793] Alternative chains certificate forgery (VRVDR-13197)
- [CVE-2015-3416] sqlite3 security update (VRVDR-12263)
- [CVE-2015-4620] bind9 security update (VRVDR-13170)

3.5R4 RELEASE

There are no security issues resolved for Release 3.5R4.

3.5R3 RELEASE

The following are the security issues resolved in this release:

- [CVE-2015-1782] libssh2 security update (VRVDR-7536)
- [CVE-2013-1813] Busybox vulnerabilities (VRVDR-7754)
- [CVE-2011-4327] OpenSSH vulnerability (VRVDR-7834)

- [CVE-2015-0209, CVE-2015-0286, CVE-2015-0287, CVE-2015-0288, CVE-2015-0289, CVE-2015-0292] OpenSSL regression update (VRVDR-7864)

- [CVE-2013-4449, CVE-2014-9713, CVE-2015-1545] OpenLDAP security update (VRVDR-7974)

- [CVE-2015-2188, CVE-2015-2189, CVE-2015-2191] wireshark security update (VRVDR-7986)

- [CVE-2014-3660] libxml security update (VRVDR-8096)

- [CVE-2015-1798, CVE-2015-1799] ntp security update (VRVDR-8405)

- [CVE-2015-3143, CVE-2015-3144, CVE-2015-3145, CVE-2015-3148] cURL security update (VRVDR-8845)

- [CVE-2014-8159, CVE-2014-9715, CVE-2015-2041, CVE-2015-2042, CVE-2015-2150, CVE-2015-2830, CVE-2015-2922, CVE-2015-3331, CVE-2015-3332, CVE-2015-3339] linux security update (VRVDR-9126)

- [CVE-2015-3153] curl security update (VRVDR-9321)

- [CVE-2015-3451] libxml-libxml-perl security update (VRVDR-9340)

- [CVE-2015-3294] dnsmasq security update (VRVDR-9433)

- [CVE-2015-4047] ipsec-tools security update (VRVDR-11276)

- [CVE-2015-3809, CVE-2015-3810, CVE-2015-3811, CVE-2015-3812, CVE-2015-3813, CVE-2015-3814, CVE-2015-3815] wireshark security update (VRVDR-11513)

- [DSA 3255-1] zeromq3 security update (VRVDR-9977)

- Leap second adjustment vulnerability (VRVDR-8082)

3.5R2 RELEASE

- [CVE-2015-0209, CVE-2015-0286, CVE-2015-0287, CVE-2015-0288, CVE-2015-0289, CVE-2015-0292] OpenSSL security update (VRVDR-7809)

- [CVE-2014-9653] File security update (VRVDR-7785)

- [CVE-2015-0261, CVE-2015-2153, CVE-2015-2154, CVE-2015-2155] tcpdump security update (VRVDR-7742)

- [CVE-2014-9656, CVE-2014-9657, CVE-2014-9658, CVE-2014-9660, CVE-2014-9661, CVE-2014-9663, CVE-2014-9664, CVE-2014-9666, CVE-2014-9667, CVE-2014-9669, CVE-2014-9670, CVE-2014-9671, CVE-2014-9672, CVE-2014-9673, CVE-2014-9675] Freetype security update (VRVDR-7715)

- [CVE-2015-0282, CVE-2015-0294] GNUTLS26 SECURITY UPDATE (VRVDR-7712)

- [CVE-2014-1569] NSS INCORRECTLY HANDLES CERTAIN ASN.1 LENGTHS (VRVDR-7652)

- [CVE-2014-3591, CVE-2015-0837] VULNERABILITIES IN LIBGCRYPT (VRVDR-7631)

- [CVE-2014-3591, CVE-2015-0837, CVE-2015-1606] VULNERABILITIES IN GNU PRIVACY GUARD (VRVDR-7630)

3.5R1 RELEASE

The following are the security issues resolved in this release:

- [CVE-2014-9221] StrongSWAN DoS vulnerability
- [CVE-2014-9680] sudo security update
- [CVE-2012-3406, CVE-2013-7424, CVE-2014-4043, CVE-2014-9402, CVE-2015-1472, CVE-2015-1473] C library vulnerabilities

Supported Products

Vyatta Release 3.5R5 supports the following products:

- Brocade Vyatta vRouter 5650—Bare metal
- Brocade Vyatta vRouter 5655—Virtual Machine (VM)

Unsupported Products

Vyatta Release 3.5R5 does not support the following products:

- Brocade Vyatta 5415 vRouter
- Brocade Vyatta 5420 vRouter

Supported NICs

The following table is a categorized list of network interface cards (NICs) supported by the 5600 vRouter dataplane for bare metal installations and for PC-Passthrough or SR-IOV configurations.

NIC vendor and model	Description	Controller type	3.2.1	3.5R2	3.5R3 and later	QA tested
Intel 85598 / 82598 AF / 82598 AT / 82598 AT2 / 82598 EB / 82599 EB / 82599 EN	Dual 10GE with SFP+	82599EB	Yes	Yes	Yes	
Intel X540 T1 / X540 T2 / X540-AT2	Dual 10GE copper	X540	Yes	Yes	Yes	Yes
Intel X520	Dual 10GE fiber		Yes	Yes	Yes	Yes
Broadcom 57710 / 57711 / 57711 E / 57712 / 57712 MF	Dual 10GE		Yes	Yes	Yes	
Broadcom 57800 / 57800 MF	Dual 10GE	57800S	Yes	Yes	Yes	
Broadcom 57810 / 57810 MF / 75810 VF	Dual 10GE	57810S	Yes	Yes	Yes	
Intel 82540 / 82545 / 82546 / 82571 / 82572 / 82573 / 82574 / 82583	1GE	E1000 style single queue devices			Yes	
Intel 82575 / 82576 / 82580 / I350 / I210 / I211 / I354 / DH89XXC	1GE	Multiqueue devices			Yes	

New Features

3.5R5 RELEASE

There are no new features for Release 3.5R5.

3.5R4 RELEASE

There are no new features for Release 3.5R4.

3.5R3 RELEASE

- **ALG**—This release includes a change in ALG (Application Layer Gateway) secondary packet flow behavior and the application of a firewall rule set. This release includes the ability of an ALG protocol to create a pinhole to enable an ALG-related packet flow to pass through the firewall. If the ALG primary flow is allowed to pass through the firewall, the secondary related flows are automatically enabled through the firewall. You no longer have to specify firewall rules to enable ALG-related flows.

  For more information about ALGs, refer to *Brocade Vyatta ALG Reference Guide*.

- **BFD**—Bidirectional Forwarding Detection (BFD) is a simple control protocol that is used to detect faults between two forwarding systems that are connected by a link. BFD is comparable to the detection components of well-known routing protocols.

  The current release of the Vyatta router has the following BFD features:
  - Protocols such as BGP, OSPFv2, OSPFv3, and static routes
  - Both IPv4 and IPv6 addresses
  - Both single hop and multiple hops
  - BFD parameters:
    - minimum-rx interval
    - minimum-tx interval
    - detect-multiplier
    - simple password authentication

  The current release of the Vyatta router has the following BFD limitations.
  - Demand mode is not supported.
  - BFD over LDP and over LAG are not supported.
  - Echo mode is not supported.

The following configuration commands are now supported on your Vyatta router.

- **interfaces dataplane** *if_name* **ip ospf fall-over bfd**
  Initiates a BFD session for all OSPFv2 neighbors on a physical interface.

- **interfaces dataplane** *if_name* **ip ospfv3 fall-over bfd**
  Initiates a BFD session for all OSPFv3 neighbors on a physical interface.

- **interfaces dataplane** *if_name* **vif** *vif-id* **ip ospf fall-over bfd**
  Initiates a BFD session for all OSPFv2 neighbors on a VIF.

- **interfaces dataplane** *if_name* **vif** *vif-id* **ip ospfv3 fall-over bfd**
  Initiates a BFD session for all OSPFv3 neighbors on a VIF.

- **protocols bfd destination** *destination_ip_address* **source** *source_ip_address* **helper-session**
  Initiates a BFD session with a neighboring system with which the source system

shares a routing protocol such as static route; however, the neighboring system does not share a static route with the source system.

- **protocols bfd destination** *destination_ip_address* **source** [*source_ ip_address* | **any**] **template** *template_name*
  Associates a BFD template with a BFD session that is specified by the source and destination IP addresses.

- **protocols bfd template** *template_name*
  Creates a BFD template that specifies the minimum-rx value, minimum-tx value, multiplier value, and authentication type for the BFD session.

- **protocols bgp** *asn* **neighbor** *ip_address* **fall-over bfd**
  Initiates a BFD session with a neighboring peer with which the system already shares a BGP session.

- **protocols ospf area** *area-id* **virtual-link** *router_id* **fall-over bfd**
  Initiates a BFD session between two OSPFv2 neighbors on a virtual link.

- **protocols ospfv3 area** *area-id* **virtual-link** *router_id* **fall-over bfd**
  Initiates a BFD session between two OSPFv3 neighbors on a virtual link.

- **protocols static route** *destination_ipv4_address* **next-hop** *nexthop_ipv4_address* **fall-over bfd**
  Initiates a BFD session between two systems on a static route by using IPv4 addressing.

- **protocols static route6** *destination _ipv6_address* **next-hop** *nexthop_ipv6_address* **fall-over bfd**
  Initiates a BFD session between two systems on a static route by using IPv6 addressing.

The following operational commands are now supported on your Vyatta router.

- **show bfd** [**session** {**detail** [*destination_ipv4_address* | *destination _ipv6_address*] | **interface** *if_name* }]
  Displays information about a BFD session on the system.

For more information about BFD, refer to *Brocade Vyatta BFD Reference Guide*.

- **BGP multiple cluster IDs**—The BGP multiple cluster IDs feature lets you configure a route reflector such that the route reflector associates a cluster ID with each peer to unite groups of clients into different clusters. This association also allows you to disable the reflection of routes between route reflection clients in the same cluster, that is, it disables intracluster route reflection

The following configuration commands are now supported on your Vyatta router.

- o **protocols bgp** *asn* **neighbor id cluster-id** *cluster-id*
  Defines a cluster ID for a neighbor.

- o **protocols bgp** *asn* **peer-group** *name* **cluster-id** *cluster-id*
  Defines a cluster ID for a peer group.

- o **protocols bgp** *asn* **parameters no-client-to-client-reflection cluster-id** *cluster-id*
  Enables or disables route reflection for a cluster.

- o **protocols bgp** *asn* **parameters no-client-to-client-reflection cluster-id any**
  Enables or disables route reflection for the all intracluster client-to-client route reflection.

- o **protocols bgp** *asn* **parameters no-client-to-client-reflection all**
  Enables or disables route reflection from a BGP route reflector to clients.

For more information about BGP multiple cluster IDs, refer to *BGP Reference Guide*

- **BGP ASN support in NetFlow**—The BGP autonomous system (AS) numbers, such as the IP Source AS, IP Destination AS, IP Source Mask, and IP Destination Mask fields, were previously set to zero. The BGP AS numbers are now set appropriately and are extracted by the flow monitoring service from the sampled packets and exported to the NetFlow collector.

  For more information about BGP ASN support in NetFlow, refer to *Vyatta Services Reference Guide*.

- **Classless static routes using DHCP**—This release introduces support for classless static routes using DHCP. By default, this feature is enabled on the Vyatta system. In exceptional circumstances, when the default behavior is not required, it can be disabled by using one of the following commands:

  - o **interfaces dataplane** *interface-name* **dhcp-options no-rfc3442**
    Disables support for the classless static route option for DHCP on a dataplane interface.

  - o **interfaces dataplane** *interface-name* **vif** *vif-id* **dhcp-options no-rfc3442**
    Disables support for the classless static route option for DHCP on a virtual interface.

  - o **interfaces dataplane** *brx* **dhcp-options no-rfc3442**
    Disables support for the DHCP classless static route option for a bridge group.

For more information about Classless static routes using DHCP, refer to *LAN Interfaces Reference Guide* and *Bridging Reference Guide*.

- **Configurable EtherTypes for QoS scheduling**—For scheduling of QoS packets, EtherTypes for the outer VLAN tag are configurable. EtherTypes 0x8100, 0x9100, 0x9200, 0x9300 and 0x88A8 are supported.

  The following configuration command is now supported on your Vyatta router.

  interfaces dataplane *interface-name* **vlan-protocol** ethertype
  Configures the Ethertype for VLAN packets.

  For more information about EtherTypes for QoS scheduling, refer to *LAN Interfaces Guide.*

- **Hot-plugging**—The Vyatta router supports *hot-plugging*, which allows a running Vyatta router to automatically discover a PCI network interface that is virtually plugged into the guest virtual machine, without having to restart the router. Hot-plugging is supported on the VMware ESX and Linux Kernel-Based Virtual Machine (KVM) virtualization platforms.

  For more information about hot-plugging, refer to *Basic System Reference Guide*.

- **Q-in-Q**—The Vyatta Q-in-Q implementation supports multiple VLAN tags in an IP packet frame, allowing extension of the VLAN ID space from 4K to 16M while also reducing the number of VLANs to manage.

  The following configuration commands are now supported on your Vyatta router.

  - **interfaces dataplane** *interface-name* **vif** *vif-id* **vlan** *outer-vid*
    Configures the ID of the outer VLAN for Q-in-Q.

  - **interfaces dataplane** *interface-name* **vif** *vif-id* **inner-vlan** *inner-vid*
    Configures the ID of the inner VLAN for Q-in-Q.

  - **policy qos** *policy-name* **shaper vlan** *outer-vid*
    Specifies the outer and inner VLAN IDs for a QoS policy.

  For more information about Q-in-Q, refer to *LAN Interfaces Guide.*

- **RIP version 1 support**—The Vyatta router now supports RIP version 1.

  The following configuration command is now supported on your Vyatta router.

  - **protocols rip version 1**
    Defines RIP version 1.

- **Rate-limit policing in firewall**—The Vyatta router now supports definition of a rate limit for a firewall rule.

  The following configuration command is now supported on your Vyatta router.

  security firewall name *name* **rule** *rule-number* **police ratelimit** *limit*
  Defines the rate limit in packets per second for a firewall rule.

  For more information about rate limits for firewall rules, refer to *Firewall Reference Guide.*

- **SPAN and RSPAN port mirroring**—This release supports Switch Port Analyzer (SPAN) and Remote SPAN (RSPAN) that enable you to monitor and troubleshoot network traffic. SPAN mirrors traffic on one or more source interfaces on a Vyatta router to a destination interface on the same router. RSPAN mirrors traffic to a destination interface on a remote Vyatta router. RSPAN mirroring has source and destination Vyatta routers.

  The following configuration commands are now supported on your Vyatta router.

  - **service portmonitor session** *id* **description** *string*
    Specifies a description for a port-monitoring session.

  - **service portmonitor session** *id* **destination** *interface-name* [**vif** *vid*]
    Specifies the destination interface for a port-monitoring session.

  - **service portmonitor session** *id* **disable**
    Disables a port-monitoring session.

  - **service portmonitor session** *id* **source** *interface-name* [**vif** *vid*]
    Specifies the source interface for a port-monitoring session.

  - **service portmonitor session** *id* **source** *interface-name* **direction** {**both** | **rx** | **tx**}
    Specifies the direction of the port monitoring for a physical source interface of a SPAN or RSPAN-source session.

  - **service portmonitor session** *id* **source** *interface-name* **vif** *vid* **direction** {**both** | **rx** | **tx**}
    Specifies the direction of the port monitoring for a VLAN source interface of a port-monitoring session.

  - **service portmonitor session** *id* **type span** | **rspan-source** | **rspan-destination**
    Defines the identifier and type for a port-monitoring session.

The following operational commands are now supported on your Vyatta router.

- **show portmonitor session** [*id*]
  Displays the port-monitoring configuration information for the session.

For more information about port mirroring, refer to *Services Reference Guide*.

- **Symmetric routing for VRRP and BGP**—This release introduces CLI commands to apply symmetric routing for edge routers using VRRP (Virtual Router Redundancy Protocol) and Border Gateway Protocol (BGP).

  The following configuration commands are now supported to enable VRRP state change notifications to BGP.

  - **interfaces dataplane** *dp* vrrp **vrrp-group** *group-instance* **notify** *client*
    Configures BGP as a client to notify VRRP state changes
  - **protocols bgp** *asn* **neighbor** *uplink-bgp-nbr* **vrrp-failove**r *vrrp-group vrrp-group-instance* **MED** *MED-value-backup-path*
    Sets MED configuration in the Vyatta router for the neighbor.
  - **protocols bgp** *asn* **neighbor** *uplink-bgp-nbr* **vrrp-failover** *vrrp-group vrrp-group-instance* **prepend-as** *prepend-as-path-to-be-used-on-backup-path*
    Sets prepend-as configuration in the Vyatta router for the neighbor.
  - **protocols bgp** *asn* **neighbor** *uplink-bgp-nbr* **vrrp-failove**r *vrrp-group vrrp-group-instance* **route-map** *globalmap*
    Sets route-map configuration in the Vyatta router for the neighbor.

  For more information about symmetric routing for VRRP and BGP, refer to *High Availability Reference Guide*.

- **VPN Link Status MIB**—The Vyatta system supports Simple Network Multicast Protocol (SNMP) traps to monitor the transitioning state of IPsec security associations (SA) that are used to notify a manager of asynchronous events in real time. The collection, post-processing, and reporting of these events can be configured or customized with no changes to the Vyatta router.

  For more information, see *IPsec Site-to-Site VPN Reference Guide*.

- **XenServer**—XenServer is supported for Brocade Vyatta 5600 vRouter version 3.5R3.

  For more information about XenServer, refer to *XenServer Installing and Upgrading Guide*.

3.5R2 RELEASE

There are no new features for Release 3.5R2.

3.5R1 RELEASE

- **Hyper-V Support**—The Vyatta system can be installed on the Hyper-V hypervisor. No upgrade is available for this release. For more information, refer to *Hyper-V Installing and Upgrading Guide.*

- **Flow Monitoring**—You can configure your Vyatta system to provide flow monitoring, a service that allows network administrators to collect IP flow information from the Vyatta system.

  Configuration commands:

  - **interfaces dataplane** *interface* **flow-monitoring selector** *selector-name*
    Associates a packet selector with a dataplane interface through which the traffic to be monitored flows.

  - **service flow-monitoring exporter udp-collector address** *ip-address*
    Specifies the IPv4 or IPv6 address of the NetFlow collector.

  - **service flow-monitoring exporter udp-collector port** *udp-port*
    Specifies the UDP port of the NetFlow collector.

  - **service flow-monitoring selector** *selector-name* **randomly out-of** *num-of-packets*
    Creates a random-packet selector and specifies the size of the packet sample window from which to select a packet.

  Operational commands:

  - **clear flow-monitoring**
    Clears the flow-monitoring statistics.

  - **show flow-monitoring**
    Displays the flow-monitoring statistics.

  For more information about Flow Monitoring, refer to *Services Reference Guide*.

- **RIP and RIPng Enhancements**—The following new commands are now supported on your Vyatta system:

    - **reset ip rip route**
      Resets data in the RIP routing table.

    - **reset ipv6 ripng route**
      Resets data in the RIPng routing table.

  For more information about these commands, refer to *RIP Reference Guide* and *RIPng Reference Guide*.

- **SIP ALG**—VoIP ALG consists of SIP ALG, which allows VoIP traffic to pass between the private and public sides of a firewall by using NAT.

    - **set system alg sip disable**
      Disables SIP ALG functionality.

    - **delete system alg sip disable**
      Enables SIP ALG functionality.

    - **set system alg sip port** *port-number*
      Adds a SIP control port to use for tracking initial connections.

    - **delete system alg sip port** *port-number*
      Adds a SIP control port to use for tracking initial connections.

  For more information on SIP ALG, refer to *Basic System Reference Guide*.

- **VRRP**—This release introduces the support of Virtual Router Redundancy Protocol, Version 3 (VRRPv3) with IPv6 addresses.

  The following commands are introduced:

    - **set interfaces dataplane** *interface* **vrrp vrrp-group** *group-id* **fast-advertise-interval** *interval*
    - **set interfaces dataplane** *interface* **vrrp vrrp-group** *group-id* **accept** *accept*
    - **set interfaces dataplane** *interface* **vrrp vrrp-group** *group-id* **rfc-compatibility**
    - **set interfaces dataplane** *interface* **vrrp vrrp-group** *group-id* **version** *version*
    - **set interfaces dataplane** *interface* **vrrp vrrp-group** *group-id* **track-interface** *interface*
    - **set interface dataplane** *interface* **vrrp vrrp-group** *group-id* **track-interface** *interface* **weight**
    - **set interface dataplane** *interface* **vrrp vrrp-group** *group-id* **track-interface** *interface* **weight value** *number*

- **set interfaces dataplane** *interface* **vrrp vrrp-group** *group-id* **track-interface** *interface* **weight type** *type*

For more information, refer to *High Availability Reference Guide.*

- **BGP Enhancements**

You can send a multi-exit discriminator (MED) value that is based on the IGP metric. When you configure a MED value based on the IGP metric for a neighbor, the MED value is copied from the IGP metric and sent to the neighbor. Copying the MED value from the IGP metric allows eBGP peers from neighboring AS to send traffic to a local AS by using the shortest path. The shortest path is based on the IGP administrative domain.

The following commands have been added:

- **set protocols bgp** *asn* **parameters bestpath igp-metric-ignore**
- **set protocols bgp** *asn* **neighbor** *id* **med-out igp**
- **set protocols bgp** *asn* **neighbor** *id* **med-out igp delay-updates**
- **set protocols bgp** *asn* **neighbor** *id* **med-out minimum-igp**
- **set protocols bgp** *asn* **peer-group** *name* **med-out igp**
- **set protocols bgp** *asn* **peer-group** *name* **med-out igp delay-updates**
- **set protocols bgp** *asn* **peer-group** *name* **med-out minimum-igp**

Named community list is supported.

The following command has been added:

set policy route route-map *map-name* **rule** *rule-num* **set add-community** *community*

You can append a community list on a received prefix with new communities.

The following commands have been updated:

- **set policy route community-list** [**standard** | **expanded**] {*list-num* | *list-name*}

- **set policy route community-list** [**standard** | **expanded**] {*list-num* | *list-name*} **description** *desc*

- **set policy route community-list** [**standard** | **expanded**] {*list-num* | *list-name*} **rule** *rule-num*

- **set policy route community-list** [**standard** | **expanded**] {*list-num* | *list-name*} **rule** *rule-num* **action**

- **set policy route extcommunity-list** [**standard** | **expanded**] {*list-num* | *list-name*} **rule** *rule-num* **description** *desc*

- **set policy route extcommunity-list** [**standard** | **expanded**] {*list-num* | *list-name*} **rule** *rule-num* **regex** *regex*
- **set policy route extcommunity-list** [**standard** | **expanded**] {*list-num* | *list-name*} **rule** *rule-num* **rt** *route-target*
- **set policy route extcommunity-list** [**standard** | **expanded**] {*list-num* | *list-name*} **rule** *rule-num* **soo** *site-of-origin*

For more information, refer to *BGP Reference Guide* and *Routing Policies Reference Guide.*

- **SNMP MIB access restrictions**—This release introduces the support for limiting access to specific MIBs by access list and/or community.

  For more information, refer to *Remote Management Reference Guide.*

- **vRouter Orchestration on vCenter with OpenStack**—The vRouter can now automatically set the IP address for the OAM interface and add the default route when it is deployed by OpenStack on VMware ESXi.

Behavior Changes

3.5R5 RELEASE

There are no behavior changes for Release 3.5R5.

3.5R4 RELEASE

There are no behavior changes for Release 3.5R4.

3.5R3 RELEASE

- The **vlan** option is now mandatory for a virtual interface (vif) configuration. Older vif configurations without a specified VLAN ID will now be migrated upon an image upgrade to have a VLAN ID inserted. For example:

  set interface dataplane dp0s7 vif 100
  will become
  set interface dataplane dp0s7 vif 100 vlan 100

  Older configurations with an optional VLAN ID will continue to work as before.

- As per VRVDR-8061, when an incoming interface does not have an IPv4 address, the 5600 vRouter forwards IPv4 frames that are received on the IPv4 pipeline for an interface to the slow-path. If you configure NAT64 translation on the 5600 vRouter, also configure an IPv4 address on the incoming interface, that is, incoming for the forward direction of the NAT64 candidate traffic. Otherwise, the NAT64 post-translated frame, which is an IPv4 frame, is forwarded to the slow-path and breaks the reverse NAT translation in the reverse direction when the end-receiver replies.

3.5R2 RELEASE

There are no behavior changes for Release 3.5R2.

3.5R1 RELEASE

There are no behavior changes for Release 3.5R1.

System Limitations

3.5R5 RELEASE

To move an IP address from one interface to another interface, you must perform a commit after removing the old address. After configuring the new address, perform a commit again.

3.5R4 RELEASE

There are no system limitations for Release 3.5R4.

3.5R3 RELEASE

- VMware does not support Q-in-Q ethertypes 0x88A8, 0x9100, 0x9200, and 0x9300. Only 0x8100 is supported.

- As per VRVDR-10931, due to a bug in Hyper-V, packet forwarding stops on a 5600 vRouter interface when the outbound transit traffic rate exceeds 1Gb per second on a Hyper-V 2012R2. To recover from this issue, reboot the Vyatta instance.

- PCI passthrough is not supported on Xen physical volumes.

- As per RFC 6192, fragments destined to the local CPU are dropped by the dataplane. To avoid having allowed CPU-bound fragments from being dropped, a firewall rule must be configured to allow them through the interface so that the fragments can be reassembled. If neither firewall nor NAT is configured, packet fragments are not inspected and are forwarded unchanged. However, in accordance with RFC 6192, any fragments that are destined to a router local address are dropped.

An input firewall allows fragments to be reassembled. For IPv4, if the packets arrive on an interface for which firewall is configured, the fragments are reassembled at input before passing to the firewall. If all the fragments of a packet are not received, then the packet is dropped. The reassembled packet passes through the remainder of the forwarding path and firewall does not recognize fragments at either input or output. At output, the packet is refragmented, if necessary. This behavior also applies to a packet arriving on an interface that is assigned to a firewall zone.

RSVP packets are sent hop-by-hop and since they can be large, they would benefit from being fragmented. The following commands can ensure that an RSVP is responded to.

```
vyatta@R1# set security firewall name RSVP rule 10 action accept
vyatta@R1# set security firewall name RSVP rule 10 protocol rsvp
```

- The VPN Link Status MIB service does not restart each time SNMP is reconfigured, but is designed to restart upon SNMP reconfiguration at a future release.

- As per VRVDR-12210, when you disable a physical interface on which an IPsec tunnel is defined and then re-enable it, the IPsec daemon does not detect the interface state toggle and does not reinject the routes for the remote prefixes into the kernel. Use the **restart vpn** operational mode command to resynchronize the IPsec-related routes.

- As per VRVDR-12122, for the BFD clients to run multihop BFD sessions over ECMP paths, each client requires a separate BFD session on each of the ECMP path, apart from running the BFD session between the source and the destination.

- Per VRVDR-12607, when 60 or more static routes (or otherwise, a DHCP Message size 807 bytes and above) are configured on the server, no static routes are leased on the 5600 vRouter. This issue normally requires the setting of option 57 - Maximum DHCP Message Size - on the 5600 vRouter (see RFC 3442 section on Avoiding Sizing Constraints), but this option is currently not supported. The workaround to this issue is to set option 57 on the DHCP server, and the static routes will be leased.

3.5R2 RELEASE

There are no system limitations for Release 3.5R2.

3.5R1 RELEASE

- Hyper-V has the following limitations:
  - Jumbo packets are not getting forwarded with Hyper-V.
  - Hyper-V supports only IPv4 at this time.
  - Hyper-V only boots with a maximum of six network adapters.
  - The functionality of VLAN interfaces does not work in Hyper-V. The routes are not learned on vif interfaces.

- The graceful restart feature has the following limitation:

  The Vyatta system keeps the forwarding-state-preserved; however, the BGPd process is not restartable, so graceful restart is supported only in helper mode.

- On systems with multiple memory channels, memory may be allocated to the wrong NUMA node. This may occur on bare metal installations with more than 16 GB of RAM installed. The BIOS may allow for disabling a particular channel, which can be done as a workaround to this problem.

Upgrade Notes

3.5R5 RELEASE

Ubuntu 14.04 comes with Linux kernel version 3.13.0, which does not support hot plugging. To get hot plugging to work on Ubuntu 14.04, you must upgrade your Ubuntu software to use Linux kernel version 3.13.1 or higher.

3.5R4 RELEASE

There are no upgrade notes for Release 3.5R4.

3.5R3 RELEASE

There are no upgrade notes for Release 3.5R3.

3.5R2 RELEASE

There are no upgrade notes for Release 3.5R2.

3.5R1 RELEASE

There are no upgrade notes for Release 3.5R1.

Resolved Issues

3.5R5 RELEASE

The following are the resolved issues in this release.

Bug ID	Severity	Component	Summary
VRVDR-9314	Minor	L3 dataplane	The **show dataplane route** command responds slowly when the routing tables are large (500K).
VRVDR-13451	Major	Firewall	The firewall drops packets after the running of the **show firewall dp0p***X* command.
VRVDR-13541	Major	Firewall	The outbound firewall with the default action of accept allows the stateful return traffic that the inbound firewall should drop.
VRVDR-8410	Major	Firewall, NAT	The dataplane becomes unresponsive due to NAT traffic.
VRVDR-13218	Major	NAT	The system runs out of memory due to dataplane memory usage when attempting to add approximately 10K destination NAT rules.
VRVDR-12866	Major	QoS	Changing the QoS **shaper frame-overhead** value no longer affects throughput numbers.
VRVDR-13539	Major	QoS	Remove the unnecessary conversion from bits to bytes in the QoS migration script.
VRVDR-12665	Major	System	When the 5600 vRouter is configured with the archive configuration option to a remote SCP location, it fails.
VRVDR-12526	Major	TACACS	The IP address of the TACACS user is not sent as a part of the accounting record for any executed command.
Resolved issues that were known issues in the previous releases			
VRVDR-12199	Minor	Control Plane, L2 dataplane	When padding is in an incoming packet, the packet is dropped between the dataplane and the control plane.
VRVDR-8342	Minor	L3 dataplane	BGP routes are preferred over standard and connected routes.

3.5R4 RELEASE

The following are the resolved issues in this release.

Bug ID	Severity	Component	Summary
VRVDR-12574	Major	Control Plane	Memory growth occurs in vplaned.
VRVDR-12608	Major	Interfaces	Backward compatibility issue occurs with previous QinQ versions when creating vifs.
VRVDR-12234	Minor	System	The vyatta-op group is used in rule 9998 of default operational rulesets instead of the vyattaop group for the other rules.
VRVDR-12613	Major	TACACS	Unexpected type changes in YANG files occurred.
Resolved issues that were known issues in the previous releases			
VRVDR-10258	Minor	NTP	NTP is not synchronizing in the general availability (GA) Release 3.5R2.

3.5R3 RELEASE

The following are the resolved issues in this release.

Bug ID	Severity	Component	Summary
VRVDR-11663	Major	ALG	This release supports a change in the ALG secondary packet flow behavior and the application of a firewall rule set. It includes the ability of an ALG to create a pinhole to enable an ALG-related packet flow to pass through the firewall. If the ALG primary flow is allowed to pass through the firewall, the related secondary flow or flows are automatically enabled through the firewall. You no longer have to specify specific firewall rules to enable ALG-related flows.
VRVDR-325	Major	BGP	BGP does not recognize Optional and Transitive attribute flags when the Extended Length flag is set in a Community path attribute.
VRVDR-9045	Minor	BGP	A peer-group change is not applied when a neighbor is moved from one peer-group to another group.
VRVDR-10257	Minor	BGP	Trap collectors are not recognizing BGP traps sent by the Vyatta router.

VRVDR-9108	Major	Config Infrastructure	The config.boot file permission is changed after upgrading the 5600 vRouter from release 3.2.1R3 to 3.5R2.
VRVDR-7301	Minor	Config Infrastructure	A warning message is displayed even though a committed configuration is saved.
VRVDR-2143	Major	Connsync	Connsync becomes unresponsive with a large queue of sessions.
VRVDR-7080	Minor	DHCP	After upgrading the Vyatta router from release 3.2.1R4 to 3.2.1R5, the commit fails during boot due to an invalid listento interface that is configured for a DHCP server.
VRVDR-7779	Major	DMVPN	The spoke does not reregister NHRP when the HUB is rebooted, maintaining IPsec in the up state.
VRVDR-7879	Major	DMVPN	DMVPN IPsec spoke-to-spoke connections fail to establish.
VRVDR-4658	Minor	DMVPN	When DMVPN spokes with separate NHRP preshared secrets attempt to connect, only the first spoke is authenticated successfully.
VRVDR-5478	Minor	DMVPN	DMVPN spoke traffic cannot transit two separate tunnels through the hub.
VRVDR-7730	Major	DMVPN, VPN	The VPN tunnel goes down if the MTU is configured on the physical interface.
VRVDR-10973	Major	DPDK	All dataplane interfaces transition from the u/u to u/D state as traffic is increased during performance testing.
VRVDR-7095	Major	Firewall	During boot, a brief window occurs in which traffic is not being blocked by the firewall.
VRVDR-9067	Major	Firewall	Firewall zones on a 5600 vRouter accept traffic by default instead of dropping traffic as does a 5400 vRouter.
VRVDR-11063	Major	Firewall	A gradual memory leak occurs after each commit on a 5600 vRouter that is running release 3.5R2.
VRVDR-7210	Minor	Firewall	Return traffic is not being sent back to the originator with a zone-based stateful firewall configuration.
VRVDR-7355	Minor	Firewall	IPv6, self-originated, or ping packets that are 1453 bytes or greater fail when the firewall is enabled.
VRVDR-8334	Major	Firewall, QoS	PCP marking does not work.
VRVDR-7756	Minor	GRE	The **ip bridge-group** parameters on a tunnel interface cause the commit to fail.
VRVDR-7731	Major	GUI	The Config.boot file cannot be saved through the SCP path on a GUI portal.

VRVDR-9684	Major	Installer	When negotiating Virtio features, the Vyatta boot log reports the following message: `Cannot configure device:  err=-95, port=1`
VRVDR-7821	Major	Interfaces	The 5600 vRouter PCI pass through with I350 could not ping the virtual interface (vif).
VRVDR-7938	Major	Interfaces	When modifying a bridge configuration, the commit fails with an “unintialized value” message.
VRVDR-10940	Major	Interfaces	When the MTU is configured on a 5600 vRouter interface, the VMware vSwitch does not forward packets to the VM after the Vyatta router is rebooted.
VRVDR-11525	Major	Interfaces	The dataplane creates a duplicate name for a second Intel X520-QDA1 NIC PCIE card when it is installed.
VRVDR-8732	Minor	Interfaces	The **show interfaces dataplane** command does not display the performance counters correctly.
VRVDR-7743	Minor	IPv6, System	The 5600 vRouter could not accept Telnet over IPv6.
VRVDR-7793	Major	L3 dataplane	The dataplane is unresponsive with an out-of-memory (OOM) message.
VRVDR-9314	Minor	L3 dataplane	The **show dataplane route** command responds slowly when the routing tables are large (500K).
VRVDR-8036	Minor	Logging	The **show log** [**firewall**|**nat**] command does not display output that is correctly logged in the /var/log/messages file.
VRVDR-9316	Minor	NAT	After every commit , the following message is displayed: `Port parameters not valid except for TCP and UDP`
VRVDR-10747	Major	Netconf	When compiling a YANG file, a VCE-YANG file compiling issue occurred.
VRVDR-6638	Major	NTP	The **show ntp** command can truncate IPv6 addresses.
VRVDR-8092	Minor	RIP	RIP-connected route is advertised as metric 16.
VRVDR-3195	Major	System	When committing config-sync on a primary router, the following message is displayed: `Failed to sync configuration to remote-router`
VRVDR-7356	Major	System	When config-sync is configured and the standby vRouter is rebooted, it comes up with an empty configuration.
VRVDR-9285	Major	System	An interface description cannot include a shell pipe (|) character.
VRVDR-6425	Minor	VPN	A Vyatta router cannot ping a host, that is directly connected with an IPsec VPN peer.

VRVDR-6394	Minor	VRRP	The transition script has premature exit 0.
Resolved issues that were known issues in the previous releases			
VRVDR-325	Major	BGP	BGP does not recognize the Optional and Transitive attribute flags when the Extended Length flag is set in a Community path attribute.
VRVDR-4694	Minor	DMVPN	When changing the DMVPN tunnel address, opennhrp.ipsec is not updated with the new address, causing IPsec to fail.
VRVDR-6744	Minor	DMVPN, VPN	The DMVPN **show vpn ike sa** command does not display IKE Phase 1 status even when IPSec Phase 2 is established.
VRVDR-3197	Major	Firewall	Stateful firewall permits sessions to be initiated in both directions.
VRVDR-7761	Minor	Interfaces	The TOS default value is now “00” rather than “inherit.”

3.5R2 RELEASE

The following are the resolved issues in this release.

Bug ID	**Severity**	**Component**	**Summary**
VRVDR-7710	Minor	Firewall	“NPF variable ‘.table’ is of type ‘table’ not ‘fam’ at ‘#012’ at line 42#012#0116” appearing in logs after every reboot.
VRVDR-7629	Critical	Interfaces	Bare metal system does not have dataplane interfaces after an image upgrade.
VRVDR-7541	Critical	DHCP	DHCPv6: Multiple DHCP IPv6 pools cause the DHCPv6 server to crash.
VRVDR-6210	Minor	DHCP	Conflicting DHCP lease ranges.

3.5R1 RELEASE

The following are the resolved issues in this release.

Bug ID	**Severity**	**Component**	**Summary**
VRVDR-3168	Major	DHCP	When DHCPv6 and DHCPv4 are configured on different vifs on a DHCP client, only DHCPv6 gets the address and an IPv4 address after the reboot.
VRVDR-4486	Major	DHCP	DHCPv6 leases expiration time is shown as a time before the current system time.

VRVDR-4047	Major	DHCP	DHCP lease time as shown in “show dhcp server leases” is longer than what the server offers.
VRVDR-1383	Major	DHCP	The DHCPv6 server does not return the expected commit error when configuring the wrong address range.
VRVDR-3163	Major	DHCP	Error message: “RTNETLINK answers and could not create vif device message seen when DHCPv6 address is configured to a vif interface.”
VRVDR-3096	Major	DMVPN	DHCP fails to send DHCP offers through a vif interface.
VRVDR-3909	Major	DMVPN	DMVPN does not re-establish connection after rebooting a HUB V-router. DMVPN SPOKE does not reregister after HUB reboots.
VRVDR-3128	Major	Firewall	Firewall is not active if firewall “name” matches firewall CLI option names such as "icmpv6", “protocol”, and so on.
VRVDR-3094	Major	Firewall	Firewall does not drop packets when a single rule is disabled.
VRVDR-2315	Major	Firewall	Some packets are leaked by firewall when disabling second rule even though the first rule should have dropped the packets.
VRVDR-3447	Major	L3 dataplane	Commit fails when enabling the MTU on a vif interface. The CLI has an option to enable the MTU on a VLAN interface.
VRVDR-4587	Major	Netconf	netplug stops calling linkup and linkdown scripts after a race condition with an address change event.
VRVDR-2844	Major	RIB, Routing infrastructure	ZebOS XP: The handling of interface qualified next-hop does not work as expected for non-P2P links. Static interface qualified gateway route support in vyatta-routing need to be fixed.
VRVDR-2209	Major	sFlow	When configuring more than four sflow servers, a commit failure is expected, but does not appear.
VRVDR-4681	Minor	VRRP	VRRP information is not captured in “show tech-support” output.

Known Issues

3.5R5 RELEASE

The following are the known issues in this release.

Bug ID	Severity	Component	Summary
VRVDR-1384	Major	BGP	When BGP peers with a VTI interface, BGP received routes are not installed in the routing table.
VRVDR-12194	Major	BGP	After the deletion and reconfiguration of the BGP protocol, VRRP fails to notify BGP.
VRVDR-12083	Major	DHCP	A DHCP client is not generating a release packet when it is connected to relay.
VRVDR-11622	Minor	DMVPN	When ESP or IKE encryption is changed, the VPN does not respond until the Vyatta router is rebooted.
VRVDR-10931	Major	Hyper-V, L2 Dataplane	Due to a bug in Hyper-V, packet forwarding stops on a 5600 vRouter interface when the outbound transit traffic rate exceeds 1Gb per second on a Hyper-V 2012R2. To recover from this issue, reboot the Vyatta instance.
VRVDR-6415	Minor	Shell	Automatic completion of a command with the question mark (?) fails when it is entered after a pipe (|) character.
VRVDR-12235	Minor	System	The output for the **show login** command always shows a user or group as root.
VRVDR-12581	Major	System	The SNMP query does not reflect the correct hostname when it is changed from the CLI.
VRVDR-12523	Major	TACACS	The 5600 vRouter sends two login requests to the TACACS server for a single successful login.

3.5R4 RELEASE

The following is the known issue in this release.

Bug ID	Severity	Component	Summary
VRVDR-12609	Minor	QinQ	When the VLAN protocol is deleted, the 5600 vRouter successfully deletes it but returns the "ip link set failed" message.

3.5R3 RELEASE

The following are the known issues in this release.

Bug ID	Severity	Component	Summary
VRVDR-12194	Major	BGP	After the deletion and reconfiguration of the BGP protocol, VRRP fails to notify BGP.
VRVDR-12565	Major	BGP	The commit fails when committing the BGP neighbor level maximum prefix CLI.
VRVDR-12583	Major	BGP	The BGP peer-group maximum-prefix warning or threshold configuration fails.
VRVDR-12586	Major	BGP	The BGP route reflector filtering based on cluster-ID configuration fails.
VRVDR-12199	Minor	Control Plane, L2 Dataplane	When padding is in an incoming packet, the packet is dropped between the dataplane and the control plane.
VRVDR-11622	Minor	DMVPN	When ESP or IKE encryption is changed, the VPN does not respond until the Vyatta router is rebooted.
VRVDR-8369	Major	Documentation	The route-map **continue** parameter does not work.
VRVDR-3576	Major	Firewall	Firewall functionality is not working for tunnel interfaces.
VRVDR-11684	Major	Firewall	Forwarding performance drops considerably when two firewalls are daisy-chained to get more than 9,999 rules.
VRVDR-4187	Minor	Firewall, GRE	The firewall input or output on a GRE tunnel interface tunX fails to drop traffic.
VRVDR-2322	Major	Firewall, VPN	Firewall functionality is not working on a VTI interface.
VRVDR-9420	Critical	L3 dataplane	The dataplane does not install the full amount of routes.
VRVDR-8342	Minor	L3 dataplane	BGP routes are preferred over standard and connected routes.
VRVDR-9448	Minor	L3 dataplane	Dataplane interfaces become disabled when the next hop for BGP routes changes.
VRVDR-4601	Major	NAT	NAT does not work when an outbound interface is used as a GRE tunnel.
VRVDR-10258	Minor	NTP	NTP is not synchronizing in the 3.5R2 GA release.

VRVDR-12164	Critical	QinQ	A (Bare-metal rte_igb_pmd) ping does not fail when a DUT1 VLAN protocol is configured with TPID 0x88A8 and a DUT2 VLAN protocol is configured with any of the following TPIDs: 0x8100, 0x9100, 0x9200, 0x9300.
VRVDR-12168	Major	QinQ	The **monitor** command displays the packet as (Q-in-Q) when the packet has only one VLAN tag with TPID 88A8.
VRVDR-12462	Major	QinQ	Traffic receives and forwards between two different ethertypes (88a8 and 8100).
VRVDR-6415	Minor	Shell	Automatic completion of a command with the question mark (?) fails when it is entered after a pipe (|) character.
VRVDR-12235	Minor	System	The output for the **show login** command always shows a user or group as root.
VRVDR-12274	Major	TACACS	The CLI becomes less responsive and the boot time increases from about 2 to 30 minutes when the **protocols static route6** command is in the configuration.

3.5R2 RELEASE

The following are the known issues in this release.

Bug ID	Severity	Component	Summary
VRVDR-325	Major	BGP	BGP does not recognize “Optional and Transitive” attribute flags when the “Extended Length” flag is set in a community path attribute.
VRVDR-7542	Minor	Connsync	NAT session failover does not work with connsync.
VRVDR-6744	Minor	DMVPN, VPN	The “show vpn ike sa” command does not display the IKE Phase 1 status when IPSec Phase 2 is established.
VRVDR-3197	Major	Firewall	Stateful firewall permits sessions to be initiated in both directions.
VRVDR-4628	Minor	Firewall	The firewall rule that follows a rule which has a loopback address is not set correctly.
VRVDR-7740	Critical	Interfaces	WAN bridging does not work.
VRVDR-7761	Minor	Interfaces	TOS default value is now “00” rather than “inherit.”

VRVDR-6514	Major	OSPF, OSPFv3	When created, an interface should be passive by default or else a hello packet can be sent as soon as the interface is created. This can cause a security risk.
VRVDR-7750	Critical	VRRP	The vRouter master in the VRRP SyncGroup stops responding intermittently.

3.5R1 RELEASE

The following are the known issues in this release.

Bug ID	**Severity**	**Component**	**Summary**
VRVDR-1384	Major	BGP	When BGP peers with a VTI interface, the BGP received routes are not installed in the routing table.
VRVDR-7128	Major	BGP	Setting a route map to match an extended community does not work in some cases with regular expressions.
VRVDR-5478	Minor	DMVPN	DMVPN spoke traffic cannot transit two separate tunnels through a hub.
VRVDR-4694	Minor	DMVPN	When changing a DMVPN tunnel address, opennhrp.ipsec fails to get updated with new address and causes IPsec to fail.
VRVDR-7351	Major	Hyper-V	The functionality of VLAN interfaces does not work in Hyper-V. The routes are not learned on vif interfaces.
VRVDR-1780	Major	PBR	Route-map: The “continue” parameter does not work.
VRVDR-4645	Minor	Virtualization	When using the ESX suspend option for a guest virtual machine, the dataplane interfaces might go down.
VRVDR-7614	Major	VRRP	VRRPv2 IPv6: Interoperation between release 3.2.1Rx and 3.5R1 of Vyatta is broken. If you upgrade from Vyatta release 3.2.1Rx to 3.5R1 with VRRPv2 IPv6 configured, and do so by upgrading the routers individually, then these IPv6 VRRP groups end up in a MASTER to MASTER state. The VRRPv2 IPv4 groups are unaffected. The workaround is to upgrade the Vyatta images simultaneously to 3.5R1. Additionally, Brocade recommends that you migrate to using VRRPv3 for IPv6 starting with release 3.5R1 onwards.