VYATTA, INC. | Release Notes

Vyatta Community Edition 3 (VC3)

October 2007

Document Part No. A0-0097-10-0002

Vyatta
1301 Shoreway Drive
Suite 200
Belmont, CA 94002
vyatta.com

Contents

New in This Release

- **Multilink Point-to-Point Protocol support.** This release introduces support for multilink Point-to-Point Protocol (MLPPP) bundling as described in RFC 1990. MLPPP allows you to group PPP interfaces, typically on T1 or E1 lines into a single virtual link, resulting in greater performance than a single low-speed link but lower cost than a high-speed link.
- **IPsec VPN clustering.** IPsec VPN can now be configured in a cluster. Clustering can be used as a failover mechanism to provide high availability for mission-critical services. The cluster monitors the nodes providing the IPsec VPN tunnel at a designated address. If the system detects that the node has failed, or that the link to the node has failed, the system migrates both the VPN tunnel and the IP addresses to a backup node. Failover is currently supported between two nodes: a primary node and a secondary node.
- **Enhanced serial interface support.** Serial interface support has been improved in a number of ways. Additions include:
  - Ability to add a description to a serial link.
  - Authentication for PPP-encapsulated interfaces. Connections can be authenticated by password, user ID, or system name, and the PAP, CHAP, MS-CHAP, MS-CHAP v.2 and EAP authentication protocols are supported.
  - LCP echo support for PPP-encapsulated interfaces.
  - Configurable Maximum Transmission Unit (MTU) and Maximum Receive Unit (MRU) for T1- and E1-encapsulated interfaces.
  - Ability to specify external or internal clock for T1- and E1-encapsulated interfaces
  - Support for the Frame Relay t392 (polling verification timer) LMI signaling option.
  - Inverse ARP support on Frame Relay permanent virtual circuits (PVCs).

  - Additional options for the “show interfaces serial” command, including an option to provide trace-level logging or raw frames for a serial interface.
  - Redesigned the output of the “show interface serial” command to increase clarity and consistency.
- **Improvements to Firewall.** Many improvements and enhancements have been added to firewall support in Release VC3:
  - Negated values can now be specified for the following fields: "protocol," source/destination "address," and source/destination "network." This allows exclusion of addresses and networks. For example, the rule “set firewall name TEST rule 1 source network !192.168.0.0/24” will match packets whose source address is NOT in the 192.168.0.0/24 network.
  - The “show firewall” command now displays information for all user-defined firewall rule sets. Previous releases allowed viewing only one firewall rule set at a time.
  - A description can now be configured for each firewall rule, such as "Allow inbound SSH traffic."
  - The “show firewall,” “show firewall <name>,” and “show firewall <name> rule <num>” commands now display the source ports and destination ports, if they have been set.
  - Each firewall rule can now support multiple source and destination “port-number” and “port-name” values within a single firewall rule. In addition, the “port-name” option now allows any port names defined in the file /etc/services. This ability was previously only available for NAT rules.
  - The "protocol" field for firewall rules now allows any protocol number or name listed in the file /etc/protocols. This ability was previously only available for NAT rules.
  - A firewall rule can now filter traffic by source MAC address using the “mac-address” option. The “mac-address” option also allows the negation operator, so that specific MAC addresses can be filtered. For example “set firewall name FW1 rule 10 source mac-address !01:02:03:AA:BB:CC” will match any packets whose source MAC address is NOT 01:02:03:AA:BB:CC
- **NAT address and network exclusion.** Negated values can now be specified for the following fields: "protocol," source/destination "address," and source/destination "network." This allows, for example, VPN traffic to be excluded from NATting. For example, the rule “set service nat name TEST rule 1 source network !192.168.0.0/24” will match packets whose source address is NOT in the 192.168.0.0/24 network.
- **New filtering options for “show bgp” commands.** A number of filtering options have been added to the “show bgp neighbor-routes” and “show bgp peers” commands. In addition, the output of these commands has been slightly redesigned for more clarity.

- **Ability to save support information to file.** A "save" option has been added to the "show tech-support" command to allow system information to be saved in a user-specified file.
- **Auto-synchronization to package repository.** The "auto-sync" option has been added to the "system package" configuration node. This option allows you to direct the system to update the repository cache at a defined interval, specified in days.
- **Ability to prevent the reboot on kernel panic.** A "reboot-on panic" option has been added to the "system" statement to direct the system not to reboot if a kernel panic occurs. This allows you to inspect system information to determine what caused the panic.
- **Bug fixes.** Over 100 issues have been resolved with Release VC3. A summary list of these is provided in the "Resolved Issues" section, which begins on page 4.

Behavior Changes

Release VC3 includes the following behavior changes:

- The "service http" configuration option has been changed to "service webgui" to better reflect its function, which is to provide access to the Vyatta web GUI.
- The default random number device for generating RSA signatures has been changed. In previous releases, the default random number device was /dev/urandom. Starting with Release VC3, the default random number device is /dev/random. The /dev/random device generates random numbers using system entropy, which is more secure, but slower, than /dev/urandom, which is a software-based random number generator. Be aware that the system generates random numbers during install and upgrade. When the system is installing or upgrading, the system is generating little entropy; therefore, using /dev/random as the random number generator may causes the system to become unavailable during install or upgrade for as long as 30 to 60 minutes. For more information, please see the "IPsec VPN" chapter of the Vyatta OFR Configuration Guide, in the section about generating RSA keys for IPsec VPN.

Upgrade Notes

The system may be upgraded from Release VC2.x to Release VC3 using an ordinary package upgrade. The URL for updating to Release VC3 code is http://archive.vyatta.com/vyatta/. The repository is “community”. The component is “main”, as in the following configuration example:

```
package {
   repository community {
      component: "main"
      url: "http://archive.vyatta.com/vyatta"
   }
}
```

To update the community edition, issue the following commands:

```
apt-get update
apt-get -y install vc-base
full-upgrade
```

Resolved Issues

Bug ID	Component	Severity	Description
316	RIP	major	XORP 261: RIP configuration - commits without required parameters (TC 3.2.2.1.3)
361	BGP	critical	XORP 289: update "show bgp routes " command with prefix and BGP attributes
458	BGP	critical	XORP 360: show bgp routes provides variable output sequence
637	firewall	major	FW - IP range help update
646	static	major	static route next-hop does not get updated
671	firewall	major	FW - Change Request: add "show firewall" command listing all firewalls
674	firewall	major	FW - iptables error message passing
680	firewall	major	FW - tab completion and help issues
704	CLI	major	"show interfaces" reporting incorrect link status
733	CLI	major	"show route" command completion
803	VRRP	major	VRRP - add "show vrrp interface <interface>" command (TC 3.2.5.7.3)

1201	interfaces	major	Sangoma 486: Setting interface to ignore Cisco HDLC keepalives does not work
1207	interfaces	major	Sangoma 487: Configuring PPP authentication does not force authentication
1386	policy	minor	Policy redistribution problem for static routes to ospf
1394	interfaces	critical	Interrupt conflict when Sangoma T3 driver is enabled
1399	interfaces	unavailable	cli allows configuration of non-existent serial interfaces
1408	BGP	major	Output from "show bgp routes" is not sorted by address
1450	interfaces	minor	serial e1 with ppp sometimes doesn't come up
1502	firewall	minor	minor inconsistency in firewall show command
1530	system	major	slow boot with compact flash: hdc: dma_timer_expiry: dma status == 0x21
1553	interfaces	minor	sangoma 1087: some wanpipe daemon commands no longer work.
1576	interfaces	minor	serial: config allows from configuration of non-existing interfaces
1577	interfaces	major	serial: fractional T1 does not work
1581	interfaces	unavailable	serial: can't change mtu
1582	interfaces	minor	"show interfaces serial" incomplete
1592	system	enhancement	Password Recovery Process
1597	CLI	unavailable	serial: deleting timeslots node does not propagate down to wanpipe conf file
1599	interfaces	minor	Sangoma 1151: C-HDLC keepalives being sent 1 second later than configured value
1600	CLI	major	Commit failure with large configuration
1603	CLI	minor	serial - clear counters all and clear counters ppp flush incorrect statistics
1604	CLI	minor	Serial - add line protocol status to show interfaces serial output
1631	firewall	critical	When a firewall is removed from an interface iptables still shows the chain attached to that interface
1632	firewall	major	Firewall delete sequence causes problems with loading config
1635	SNMP	minor	SNMP statistics are not reported

1665	firewall	enhancement	Enhancement request: Add Firewall Description field for specific rules
1690	system	minor	Ethernet (tulip driver) interface fails after 3 days. System booted from Live CD.
1703	CLI	unavailable	"show interfaces system" hangs
1711	firewall	unavailable	Firewall: Incorrect log message when configuring firewall
1721	system	unavailable	Router manager configuration directory is not preserved
1754	interfaces	unavailable	template failure on removing vif interface
1758	VRRP	unavailable	vrrp: "show vrrp" has no output
1760	system	unavailable	no error message when "delete system login user" fails
1790	BGP	major	"show bgp peer" output incorrect for route reflector clients
1791	BGP	unavailable	XORP 697: BGP crash - invalid peer AS
1799	policy	unavailable	policy statements only allow a single AS prepend
1803	BGP	unavailable	BGP crash (merged XORP build)
1820	BGP	unavailable	"clear bgp <IP>" does not clear BGP session
1834	system	unavailable	segfault on restart syslog daemon
1891	policy	unavailable	Policy/BGP: Exporting with "aggregate-prefix-len" did NOT "Originate an aggregate route with this prefix length"
1893	NAT	major	nf_conntrack module reduces performance when NAT not in use
1898	BGP	unavailable	The function RibOutTable::add_route() in xorp_bgp is consuming too much CPU
1908	documentation	unavailable	Policy statement parameters duplicated in command reference guide
1910	BGP	unavailable	Peer flap can cause xorp_bgp crash
1912	documentation	unavailable	Incorrect logging severity example in configuration guide
1913	CLI	unavailable	XORP Deleting an existing interface without removing DHCP config cause routermanager to fail on restart.
1932	firewall	enhancement	Display Port Information on 'show firewall' commands

1937	BGP	unavailable	BGP: No community information was displayed in the output of "show bgp routes ipv4 detail"
1941	BGP	unavailable	BGP: "show bgp routes" shall not display peer bgp-id but peer address.
1945	NAT	enhancement	Reduce the number of configuration statements for NAT by using defaults
1949	VPN	unavailable	vpn: missing help string for "show vpn ipsec sa detail connection"
1950	policy	critical	Policy/BGP: "action reject" works as "action accept" for BGP Export/Redistribution
1965	CLI	unavailable	[NEW CLI] need mechanism for specifying mandatory nodes
1967	CLI	unavailable	[new cli] forward slash not handled "/" for values (multinodes)
1974	CLI	unavailable	[new cli] new cli needs to support closest update action needs to be executed
1979	interfaces	unavailable	Comments in wanpipe config files can cause xorp crashes
1980	SNMP	unavailable	snmp contact/location/description not working
1981	BGP	unavailable	BGP: "show bgp routes/neighbor-routes ipv4 detail" couldn't display localpref of ebgp routes being changed by import policy.
1986	BGP	major	No BGP routes in table with repeated peer restart
1987	interfaces	critical	Routes are not removed from FIB on link failure
2004	policy	unavailable	prevent user from assigning redistribution policy on a per peer basis
2007	policy	unavailable	Export policy will not filter redistribution policy on same protocol
2014	NAT	unavailable	NAT and Firewall: Add the ability to use negated match criteria for firewall and NAT rules
2015	firewall	major	'Show Firewall <name> statistics' command displays incorrect statistics when firewall logging is enabled
2037	interfaces	unavailable	Wanpipe: Cisco-HDLC encapsulation did not work
2051	BGP	unavailable	BGP Route Reflector server not tx learned routes from client

2053	CLI	minor	NETLINK Error When Attempting to Delete a Disabled Interface Address
2076	DHCP	minor	DHCP: Configuration may not be fully validated
2095	policy	unavailable	Policy/BGP: BGP crashed after its export policy was changed and committed
2104	VPN	enhancement	VPN Enhancement: Key generation command should default to /dev/random
2109	BGP	minor	BGP: Deleting/committing "multihop" may not enforce desired multihop behavior
2110	GUI	unavailable	set service http port xx fails to commit
2114	firewall	minor	"show firewall" should require firewall name
2126	system	trivial	install-system cosmetics
2127	system	major	Missing information in "show version"
2133	firewall	unavailable	creating empty firewall config in interface crashes rtrmgr
2145	policy	unavailable	Policy: "network4" supports operators ">=", "<=", "!=" and "==" in configuration, but only does "==" correctly
2147	documentation	major	Source NAT many: many command has incorrect syntax "network" instead of "range"
2152	firewall	enhancement	allow specifying multiple source/destination port numbers/names in a firewall rule
2153	firewall	enhancement	allow more flexibility in firewall "protocol" specification
2159	VPN	unavailable	IPSEC: Creating 10 IPSec Tunnels in VPN runs out of Crypto helper for v500
2168	CLI	unavailable	exists parameter not working in new CLI
2169	BGP	unavailable	do_c_format() calls malloc() too much
2171	CLI	unavailable	exists parameter syntax needs to be changed
2174	CLI	unavailable	referencing node path (instead of value) always returns last segment of path
2177	CLI	unavailable	var referencing returns substituted chars
2178	system	unavailable	System doesn't reboot after a kernel panic
2179	CLI	unavailable	Document arithmetic precedence in new CLI

2186	CLI	unavailable	"create:" action should be optional in new CLI templates
2187	VRRP	enhancement	Show VRRP shows incorrect interface state
2190	interfaces	unavailable	WAN interface is not seen after being configured for hdlc
2191	BGP	unavailable	BGP expand statement adds 0's into AS-PATH
2196	CLI	unavailable	new cli: syntax causes core dump
2197	CLI	unavailable	new cli: syntax using exists always fails
2199	interfaces	critical	Moving T1 cable to one of the WAN interfaces causes the console to hang
2202	firewall	enhancement	Layer 2 filtering needs to be supported on Vyatta Firewall
2219	CLI	unavailable	comparison operator failing with different type warning
2230	CLI	unavailable	NEW CLI: Doesn't return help message back to xorpsh
2272	system	unavailable	PERC4 drivers missing from distort
2275	VRRP	critical	xorp rtrmgr memory leak
2280	interfaces	minor	Invalid parse error reported for hw-id value when loading 2.0 config on a 2.2 system
2286	interfaces	unavailable	wanpipe-T-A301-SH.tpl needed
2291	GUI	major	GUI does not start and Lighttp settings are set to default.
2292	system	unavailable	full-upgrade does not take into account networking problems
2320	CLI	unavailable	Enhancement: Add LCP Echo Option to multilink interface
2323	interfaces	unavailable	Frame relay "t392dte" parameter should be "t392dce"
2325	VRRP	unavailable	vrrp backup exits on interface enable/disable
2326	system	minor	"show version all" hangs
2327	system	enhancement	Need commands added to tech-support script.
2328	CLI	enhancement	Need a way to save tech-support output to file in CLI
2355	VPN	unavailable	VPN: “vpn rsa-key generate” command does not complete in VMWare
2359	VRRP	minor	Missing VRRP help

2360	VRRP	minor	Show VRRP output order needs to be consistent.
2405	CLI	enhancement	Configuration downgrade command required

Known Issues

Bug ID	Description
354	XORP 341: default BGP TTL is > 1 (TC 3.2.4.1.17) By default, the Vyatta router is able to establish eBGP neighbor adjacencies with routers that are not directly connected—that is, that require an IP TTL larger than 1. The default behavior for Cisco and Juniper routers is to not allow this, unless an eBGP neighbor is explicitly configured as "multi-hop". Recommended action: If interoperating with other devices, be aware of this behavior, which may not be as expected.
1445	The “service nat protocol” option should have a selection for both TCP and UDP. Currently, the system does not allow specifying both the TCP and UDP protocols within a single rule. Recommended action: If both protocols are required, create two separate NAT rules.
1900	BGP crashes peer after manual flap from Juniper or Vyatta neighbor If a BGP connection is cleared with either a "clear bgp neighbor" (from a Juniper eBGP peer) or a "disable true" (from a Vyatta eBGP peer), the remote peer crashes, and frequently an iBGP neighbor to the remote peer also crashes. Recommended action: None.
2006	Enhancement request: If the protocol is not specified in the “from” term of a policy statement, then the “from” protocol should be set to whatever protocol is using the policy. For example, if the policy has been applied as a BGP export/redistribution policy, the “from” protocol should be set to BGP. This is expected behavior. Recommended action: Be aware that the “from” protocol is not implicitly set, and ensure that you always explicitly specify the “from” protocol for every term of an export/redistribution policy.
2108	Config partition can't be seen from the Linux shell after when utilizing Dell Diagnostics. After the Dell Diagnostics utility partition has been created and the appropriate configuration and root partitions have been created from the Linux shell and are visible, the configuration partition does not appear when the Vyatta operation system is installed to the hard drive. Recommended action: None. This issue is not service-affecting.
2112	BGP: setting/committing BGP confederation identifier without enabling the peer confederation member causes the BGP process to crash. Recommended action: Enable the peer confederation member before committing the BGP confederation identifier.

2113	The "domain-search" option does not provide additional domains for name lookup. Setting values for domain search does not result in the system successfully resolving unqualified host names to those domains to form Fully Qualified Domain Names (FQDNs). Recommended action: Avoid relying on the “domain-search” option for resolving unqualified host names.
2164	Policy: Setting “aggregate-brief-mode” == false does not set AS Path correctly. Setting "aggregate-brief-mode” to “false" is NOT supported in this release: the result is always as if “aggregate-brief-mode” is set to “true.” In particular, when "aggregate-brief-mode" is not explicitly set, the default is NOT " aggregate-brief-mode: false" (as designed), but "aggregate-brief-mode: true". Recommended action: None.
2256	Vyatta CLI-defined domain search order not is retained in /etc/resolv.conf. If the domain names are configured one after another, but not committed between entries, the system does not preserve the configuration order. Instead, the system re-orders the entries alphabetically. If the domain names are configured one after another but are individually committed, the order of entry is preserved as the search order. Recommended action: When entering domain search order, commit each entry individually after setting the value.
2282	Hardware clock time very wrong results in system hang. If the hardware clock is very wrong—for example, because the motherboard battery is drained—the system crashes in about five minutes. Recommended action: To avoid this situation, make sure the motherboard battery is well-charged. To recover from this situation: 1) Ensure motherboard battery is functioning. 2) Enter BIOS set-up mode. 3) Set clock to current date and time, to within a few seconds. 4) Select "Save settings and exit." 5) Reboot the system.
2299	Policy: Setting or changing an export policy containing a term "then action reject" and then committing did NOT reject routes as expected, when the export policy was already applied to the BGP protocol. The changes to the policy were not applied. Recommended action: Remove the policy from the BGP protocol before changing it (by deleting the BGP protocol “export” option). Change the policy and commit the changes. Then re-apply the export policy to BGP.
2308	Numerous SNMP WARNING messages on boot. When the SNMP agent is enabled, numerous error messages display when the system starts up. Recommended action: None. This display-only issue does not affect operation.
2311	Cannot connect to GUI using HTTP when default HTTPS port is changed. If the HTTPS port is modified from the default, then when the browser attempts to connect the login prompt displays but the connection is not established. A Microsoft Internet Explorer browser reports that it is “waiting for” the Vyatta system, and a Netscape browser reports that it is “connected.” Both messages could be misleading, since in fact the

	connection has failed. Recommended action: Avoid modifying the HTTPS port; instead, use the default port (443).
2337	A configuration error "t1/e1/t3/e3-option is not specified" occurs if mandatory configuration parameters (for example, encapsulation type) are deleted and the configuration committed. On "commit", the state of the interface must be consistent. Recommended action: If you need to need to completely change configuration for a serial interface, delete the configuration node altogether and recreated it.
2338	Actions for a multi-node are not executed in the order in which its values are entered. This may not be desirable where ordering has significance. Configuring each entry and committing them individually preserves the ordering. Recommended action: When configuring multiple instances of a configuration multi-node, commit each instance after setting it.
2342	Interface VRRP configuration must be removed prior to removing vif. If you try to delete a vif configured as a member of a VRRP group, the system will generate an error unless the VRRP configuration is removed prior to deleting the vif. Recommended action: Delete VRRP configuration for a vif and commit the deletion prior to deleting a vif.
2387	VPN will not start if an unconfigured interface is specified. Recommended action: If you refer to an interface in VPN configuration, ensure you have previously assigned the interface an IP address and prefix-length.
2388	VPN process is restarted when an interface is added or deleted. Adding or deleting an interface to the VPN configuration results in a VPN process restart, even if the interface is not involved in the VPN configuration. As a result, existing VPN tunnels will be re-established. Recommended action: None. The VPN tunnels automatically re-establish.
2392	BGP: The BGP session was established even though AS numbers were mis-configured. The expected behavior is that the system fail to establish the session. Recommended action: To avoid undesired behavior, take care to correctly configure BGP AS information.
2397	System: Vyatta system did NOT reboot when a kernel panic occurred during boot (and before initialization). Recommended action: None.
2398	"Operators" and "prefix-length range" in policy config are no longer valid. The "prefix-length range" option in policy configuration node is designed to support match expressions including logical operators. Currently, expressions including operators cause an error. Recommended action: Use only integer values in policy "prefix-length range" configuration statements.

2412	Interfaces rediscovered and reassigned following downgrade. If you downgrade the system to Release VC2.2, the config.boot file created after running the “config-downgrade” command must be manually modified. Recommended action: Open the config.boot file for editing and modify all MAC addresses specified in the “hw-id” entries to be upper case. If this step is not performed prior to re-installation of the VC2.2 release, any Ethernet interfaces will be incorrectly named and the router manager may fail to start.