GENEXIS

ALWAYS CONNECTED

GeneOS 3.0.0-R Release Notes

GeneOS 3.0.0-R Release Notes

Table of Contents

List of Tables

Document information

GEN-DOC-3.0.0-R-RN. Published 2016-12-02.

Copyright and Legal Notice

Genexis B.V., Genexis Holding B.V. and subsidiaries herein collectively known as Genexis.

GeneOS, DRG, HRG, Hybrid, GAPS, program models and other software content and this documentation ("the Intellectual Property Rights") are protected by the Dutch Copyright Act (*Auteurswet*) and Genexis declares that it is the author and claims copyright (*Auteursrecht*) for the Intellectual Property Rights. Reproduction and distribution without authorization by Genexis B.V. is prohibited. The prohibition includes every form of reproduction and distribution.

Every effort has been made to ensure that the information in this document is complete and accurate at the time of printing. However, information is subject to change without notice. Genexis assumes no liability for damages incurred directly or indirectly from errors, omissions or discrepancies between the software and this document.

Genexis, FiberXport and DRG are trademarks of Genexis.

All other trademarks, service marks and trade names are the property of their respective owners.

Purchasers, licensees and users accept and acknowledge that the products contain components (including components carrying certain firmware) and combinations of components that constitute trade secrets protected by Genexis or its partners. Purchasers, licensees and users warrant that the delivered products will not be opened or dismantled, copied, altered or in any other way modified. Furthermore, purchasers, licensees and users agree not to attempt to reverse engineer, disassemble, modify, translate, create derivate works, rent, lease, loan, or without written permission distribute or sublicense the software, in whole or in part.

The products and its hardware, firmware and software, including technical data, may be subject to EU and U.S export control laws, including the U.S Export Administration Act and its associated regulations and the International Traffic in Arms Regulations administerd by the US Department of State, and may be subject to export or import regulations in other countries. Purchasers and licensees agree to comply strictly with all such regulations and acknowledges that it has the responsibility to obtain licenses to export, re-export, or import hardware, firmare and software.

Purchasers and licensees are not entitled to, and Genexis is not in any event liable to pay, compensation for damages which delivered products or software has caused to other property or to persons or any other consequential damages, including but not limited to loss of profit, loss of production or any other indirect damages.

GeneOS 3.0.0-R Release Notes

Introduction

The software preinstalled on Genexis Residential gateway (RGs) is referred to as GeneOS.

The new features and resolved issues are relative to the GeneOS 2.3.0-R release.

Supported Platforms and Models

GeneOS supports multiple products, which can be logically grouped into software platforms. GeneOS firmware releases include firmware images for each supported platform. The firmware image name includes the platform name, in the form *geneos-<platform>-<version>-<release-level>.img*, e.g. *geneos-lunar-3.0.0-R.img*

The product platform is identified in information provided by the devices, e.g. in the DHCP vendor class identifier and TR-069 information. The correct firmware must be used for each product, and to ensure this, devices will only upgrade to firmware for the correct platform. GeneOS currently supports the following platforms: polar and lunar. The details of which products are supported in each platform are shown in *Table 1*

Table 1. Supported platforms and models

Platform	Model
polar	FiberTwist-P2410, FiberTwist-P2420
lunar	Platinum-7840, DRG7820, DRG7870

New Features in GeneOS 3.0.0-R

This release includes the following new features:

- IPv4 Port Forwarding
- Configurable GUI Access
- DNS Server Override
- Extended CATV Support
- VLANTermination Objects
- IPv4 DMZ Host
- Configurable Wireless Authentication Mode
- Layer 2 QoS Egress Rate Limiting
- Layer 2 QoS Queue Scheduling
- IPv6 Internet Service
- IGMPv2 Snooping

Since the persistently stored database used by earlier versions of GeneOS contains incompatible data model information, the database will be removed following the reboot after the firmware upgrade to 3.0.0-R. As a result the device will need to be reconfigured after the firmware upgrade completes.

IPv4 Port Forwarding

Added support for IPv4 port forwarding, which allows traffic to reach internal hosts even when the connection is initiated from the external network. Typical use case is supporting a server, e.g. a web server, on the internal network, for which external access is needed. IPv4 Port Forwarding is configurable via CLI, TR-069 and GUI.

Configurable GUI Access

HTTP access to GUI from LAN clients added to existing HTTPS access. End user can change the default behaviour to any combination of HTTP and HTTPS access, or disable access.

DNS Server Override

Allows the use of whole home DNS-based parental control over sites the LAN clients can visit, the end user can define alternative upstream DNS servers, instead of using the ones provided by the ISP.

Extended CATV Support

CATV service support on DRG7870 and FiberTwist-P2420.

VLANTermination Objects

Support for VLAN Termination objects is added in the stack between each IP.Interface object and the relevant Ethernet.Link object.

Since the persistently stored database used by earlier versions of GeneOS contains incompatible data model information, the database will be removed following the reboot after the firmware upgrade. As a result the device will need to be reconfigured after the firmware upgrade completes.

Further information about VLANTermination object, including ACS integration changes necessary to configure interfaces using TR-069 are described in GeneOS 3.0.0 VLANTermination Tech Note.

IPv4 DMZ Host

The Demilitarized Zone (DMZ) host is a computer in the private network. It can be accessed from the Internet regardless of firewall protection and all IP traffic is forwarded to the corresponding port of the DMZ host. DMZ host configuration only affects routed traffic and has no effect on traffic that is targeted to the RG itself, e.g. management and VoIP. Any port forwarding rules are observed before traffic is forwarded to DMZ host.

Configurable Wireless Authentication Mode

WPA and WPA2 mixed mode and *WPA2 only* are configurable by the user and the operator. *WPA and WPA2 mixed mode* is the default setting, which permits the coexistence of WPA and WPA2 clients on a common SSID. During WPA and WPA2 mixed mode, the Access Point advertises the supported encryption ciphers (TKIP, AES) that are available for use. The client selects the encryption cipher it would like to use. For maximum security, the recommended setting for the user is *WPA2 only*. In *WPA2 only* mode, AES is the supported encryption cipher.

Layer 2 QoS Egress Rate Limiting

Egress rate shaping is used to limit data bursts that can congest a network. A maximum limit rate can be set to limit the egress data rate on a port. Before being transmitted, the frames queued on the port may be stored in a buffer and then sent into the network with delays inserted between the frames. Egress rate shaping increases delay and possibly jitter. Some frames may be dropped because of insufficient buffers. The CLI command **rate-limit egress <rate>** is used to configure the limit rate for egress traffic. For details about the rate-limit command, see GeneOS Command Reference.

Layer 2 QoS Queue Scheduling

Each physical interface has four transmit queues for egress traffic. Each layer 2 frame that needs to be transmitted is enqueued in one of the transmit queues. The transmit queues are then serviced based on the transmit queue scheduling algorithm.

- Strict Priority (SP): All the frames in the highest priority queue are transmitted before the frames in the next highest priority queue, and so on until the lowest priority queue.
- Weighted Round Robin (WRR): Traffic in higher priority queues are transmitted before traffic in lower priority queues based upon a weighting. A number of frames from the top priority queue are transmitted, followed by some from the next priority queue and so on to the lowest priority queue. This ensures that even the lower priority queues are able to transit some frames. For details about the queue-scheduling command, see GeneOS Command Reference.

IPv6 Internet Service

The IPv6 Internet service provides LAN and WLAN clients access to Internet via a configurable VLAN interface. The Internet service includes basic firewall, basic stateful DHCPv6

on WAN and SLAAC for LAN clients. When IPv6 internet is enabled on an upstream interface using the **ipv6 address dhcpv6** command a DHCPv6 client will be started to obtain an IPv6 address for the interface. The Internet service is disabled by default to allow the operator to configure the service interface to be used to access the Internet. See the GeneOS Command Reference for details about how to enable the IPv6 Internet service.

IGMPv2 Snooping

IGMP snooping provides a way to constrain multicast traffic on Layer 2 VLAN interfaces. By snooping the IGMPv2 membership reports sent by hosts, GeneOS builds multicast forwarding tables to deliver traffic only to those interfaces with active receivers of the multicast group. IGMPv2 snooping significantly reduces the volume of multicast traffic received on other ports.

Resolved issues

Table 2. Resolved issues

Issue number	First discovered in release	Description
31695		Firewall rule for IP 0.0.0.0/0 added via CLI cannot be deleted
	If a firewall rule is created with the IP address 0.0.0.0/0 as either source or destination, then subsequent attempts to delete this rule via the CLI will fail. Workaround: Delete the rule via ACS or create a new access list with the desired changes and apply it on the interface, and delete the complete original access list.	
31686		Unable to ping6 delegated IPv6 address from WAN
	It may not be possible to correctly ping6 a LAN client from WAN side when the LAN client address is a delegated prefix address.	
31636		Ping to LAN host IP successful from upstream server when internet is enabled
	ICMP traffic may be forwarded from WAN to LAN even when port forwarding is disabled	
31629		Renew and rebind timer values not used
	The DHCP renew and rebind timer option values optionally provided by upstream DHCP servers are not observed by the DHCP client. The DHCP client simply renews at 50% of the DHCP lease duration. As a result setting DHCP renew and rebind timers which differ from the default values (of 50% and 87.5% of the lease as defined by RFC2131) has no effect on the DHCP client behaviour.	
31627		Device.WiFi.AccessPoint.i.Security. data model incorrect
31620		"show running-config context" support not operational
	"show running-config" cannot be used with specific contexts	
31607		Successful phone call generates error messages
	There are error log messages even for a successful call - these messages are misleading and can be ignored/	
31606		Excessive VoIP logging messages
	Excessive SIP log messages overwrite other log messages which may mean that important information is lost from the logs	
31605		VoIP class5 call-waiting is presented as enabled although not supported
	Call-waiting is presented as enabled in show-running even if the feature is not supported yet.	
31600		Disable suspend-resume time by default
	Call suspend-resume timer is non-zero by default. As a result call is not terminated immediately called party hangs up call.	
31590		Illegal value returned when requesting timezone

Issue number	First discovered in release	Description
	Reading timezone value via CWMP where the timezone is set as timezone, i.e. not a location, e.g. Etc/GMT+04, results in unexpected response value. -04 in this example.	
31584		Incorrect "dhcp client send-option" command option
	The "dhcp client send-option" command is poorly constructed and allows incorrect commands to be entered. The command also allows any option to be set, but only option 60 is supported currently.	
31581		ACS cannot read NTP server values
	Configured NTP server values cannot be correctly read back using CWMP - the values returned are always "" for all NTP servers.	
31580		UTC timezone used after reboot
	Configuration of timezone works when configured, but does not work after a reboot - the timezone in effect after a reboot is UTC	
31560		*show ip route* has limitations in displaying routes for virtual interfaces
	The CLI command *show ip route* is not able to display routes for VLAN per customer virtual interfaces. This limitation is also present for native VLAN interfaces where the VLAN ID is greater than 255.	
31558		Incorrect type of DHCPv4 option values
31552		Ping command does not support virtual interfaces
	The CLI ping command does not support VLAN per customer virtual interfaces, e.g. geneos# ping www.example.com source-interface vlan1/1 ping: bad address vlan1/1	
31547		Incorrect IP address validation
	IPv4 address validation in GUI forms is incorrect - any address of the form xxx.xxx.xxx.xxx where x is 0 - 9 is allowed, e.g. 192.168.1.999	
31530		Default DHCP server pool size not shown as default
	The default DHCP server default pool size is not denoted as default by being preceded by "!".	
31520		Renew and rebind timers not updated in "show dhcp client lease"
	When the DHCP server does not explicitly provide renew and rebind timer values through DHCP options 58 and 59 respectively, the renew and rebind timer values in "show dhcp client lease" output may always be "0h0m0s". Note that this is a cosmetic issue only, renew and rebind do occur at the time expected by the lease.	
31517		Occasional network connectivity issues
	Occasional network connectivity issues on all network interfaces. When it happens, clients loose WiFi connectivity and cannot authenticate again. At the same time, access to management interface is unavailable, DHCP lease expires and LAN ports has no service. The issue is usually triggered by traffic on wireless.	
31514		Virtual interfaces have incorrect interface name

Issue number	First discovered in release	Description
	Virtual interfaces used in VLAN per customer scenarios have the incorrect interface name in "show interface" output, e.g. geneos# show interface vlan1/2 vlan1_2 Link encap:Ethernet HWaddr 00:0F:94:BA:9D:ED inet addr:192.168.3.128 Bcast:192.168.3.255 Mask:255.255.255.0 inet6 addr: fe80::20f:94ff:feba:9ded/64 Scope:Link UP BROADCAST RUNNING MULTICAST MTU:1586 Metric:1 RX packets:374 errors:0 dropped:6 overruns:0 frame:0 TX packets:13 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:0 RX bytes:23505 (22.9 KiB) TX bytes:1502 (1.4 KiB)	
31504		Get RPC fails on partial path name
	GAPS client handles Get RPC incorrectly when fails on partial name.	
31499		Get RPC return error on non-existent path name (node)
	GAPS client returns an error to Get RPC for non-existent path name.	
31486		End user cannot configure LAN domain name
	It is not possible for the end user to configure the LAN domain name via the GUI	
31485		Missing rules in ACL
	Sometimes the show running-config does not showing the complete ACL, specifically ICMP rules may be missing. Workaround: Following a reboot all rules will be visible	
31466		GAPS Inform interval configuration does not take effect
	Changes to the GAPS client inform interval may not be recognised, and therefore the inform interval may not be altered after the interface had been changed. Workaround: The new interval will be used after a reboot.	
31440		DHCP client lease not renewed when indicated
	Under some circumstances the renew and rebind times shown in the "show dhcp client lease" output can be negative, e.g. "0h-1m-59s". This is a cosmetic issue reflecting a difference between the estimated time until the renew and rebind timers are triggered and the actual timer values.	
31438		Missing Internet service information
	The Internet GUI page always reports the Internet service gateway and DNS servers as 0.0.0.0	
31429		Incorrect display of management interface IP address configuration
	Non-default interfaces show "!ip address dhcp" which indicates that DHCP client is operational by default. This is not the case for non-default interfaces. It is necessary for "ip address dhcp" command to be issued for non-default interfaces.	
31228		DHCPv4 client randomisation and backoff
	The DHCPv4 client request frequency is not randomised and does not increase.	

Issue number	First discovered in release	Description
31200		3 seconds DHCP discover interval
	The DHCP client uses a constant 3s retry timer when DHCP server does not respond. This can result in a DHCP storm when large numbers of devices reboot synchronously, e.g. follow a power outage. Requests should follow an exponentially increasing backoff algorithm as specified by RFC2131.	
30578		Clock and logging always uses UTC timezone
	Clock and logging are performed using UTC timezone and not using local timezone or daylight saving.	

Known issues

Table 3. Known issues

Issue number	First discovered in release	Description
31704		show running displays "ip igmp snooping" on all upstream interfaces
	ip igmp snooping is displayed in show running on other upstream interfaces where ip igmp snooping is disabled.	
31692		Device.Time.CurrentLocalTime is incorrectly coded
	The Device.Time.CurrentLocalTime fetched from the device is incorrectly coded, e.g. a value of *2016-11-23T23:25:21+0000* - the timezone information at end of the string (*+0000*) should be "Z", "+00:00" or "-00:00" according to the dateTime definition in TR-069.	
31691		DNS server is not updated with DHCPv4/DHCPv6 DNS option
	The DNS proxy does not correctly fail over to secondary upstream DNS servers if the primary server is not available.	
31681		DHCPv6 client does not use Max Solicit Timeout option value
	The DHCPv6 client does not use the Max Solicit Timeout option value returned by the DHCPv6 server to limit the maximum delay for retransmissions of its Solicit messages.	
31658		Unable to connect to CLI after configuring IPv6 address
	Management connectivity is lost after ipv6 address dhcpv6 is configured on management interface on Polar	
31656		Default wlan security mode displayed
	Under some circumstances the wlan security mode displayed is wpa-wpa2, which is the default value. Rebooting may cause the value to not be shown, but may reappear after subsequent reboot. geneos# show running-config group wlan ! version geneos-lunar-3.0.0-N161027 wlan country gb wlan 2g channel 5 interface wlan1 wlan security passphrase "" wlan security authentication wpa-wpa2 interface wlan2 wlan security passphrase "" wlan security authentication wpa-wpa2 !end	
31641		"no ip address" command is not implemented
	The "no ip address" command is not currently implemented. Instead the "ip address none" command is available for relevant contexts to remove ip address configuration. Note that the "ip address none" command is deprecated and will be replaced by "no ip address" in a future release of GeneOS.	
31597		Device.DNS.Client.Enable cannot be written

Issue number	First discovered in release	Description
	Its is not possible for an ACS to write values to the Device.DNS.Client.Enable parameter using CWMP	
31585		"ip rule" command handles priority inconsistently
	The "ip rule" command does not handle optional priority value correctly. The command syntax behaviour is incorrect, and any priority value defined is not displayed in "show running-configuration".	
31577		Certain CLI commands not correctly functioning after CWMP provisioning [Ticket#1011602]
	Under some circumstances it is not possible to read system configuration via CLI, i.e. "show running-configuration" when device has been configured though CWMP following ACS discovery using DHCP options.	
31496		No uplink with some non-compliant SFPs
	It is not possible to get link using some incorrectly coded SFPs. MSA-compliant coded SFPs work correctly, however others may not.	
31477		Incorrect Internet interface statistics
	The Internet interface statistics reported on the GUI and in CLI are incorrect.	
31399		5GHz wireless Internet access broken if using 20MHz bandwidth
	If one configures a manual 5GHz channel, and configures 20MHz channel bandwidth, then the client can associate with the AP, but no traffic is forwarded to or received from the Internet service interface. Workaround: Use default channel bandwidth as there is little to be gained from manually setting this to a reduced value.	
31396		"show running-config" does not display similar rules
	The output from "show running-config" may not show some ACL rules in some cases - this is true when similar rules are applied with specific source addresses to ACLs before they are applied to an interface. The rules are correctly applied to the interface. Workaround: The ACL rules are visible in the output of "show ip access-list <name>"	
31394		Zero WLAN clients always shown
	The number of wireless clients shown for interfaces wlan1 and wlan2 is always zero irrespective of the number of clients actually connected.	
31392		Incorrect channel list when 2.4GHz interface disabled
	If the 2.4GHz interface is disabled, the channel selection list available for manual selection will be incorrect. This is problematic if the end user wants to enable the interface and select a manual channel. Workaround: Enable the interface and save the configuration change, then select the desired channel and save the configuration change again.	

Issue number	First discovered in release	Description
31386		The default dial plan cannot be restored to default by "no dial plan"
	It is not possible to return to the default dial plan value using the "no dial plan" command. Workaround: Explicitly change the dial plan value to the default value, i.e. geneos(config-voice)# dial plan "(xx.T)"	
31378		wlan configuration commands are visible in polar CLI
	Wireless configuration commands are visible in command line on Polar platform products which do not support wireless functionality. Affects: FiberTwist-P2410	
31373		DTMF relay method "inband" fails, and sip-info produces low quality tones.
	DTMF relay methods display different levels of functionality. The in-band method produces poor quality results at the receiver, and with the SIP-INFO method one can hear a "pop" with each tone, which my present correct tone detection at the receiver. RFC2833 works well. Workaround: Use RFC2833 DTMF relay	
31366		Missing priority keyword
	The "ip rule" CLI command includes the ability to define the rule priority using the "priority" keyword. The keyword is missing from the command implementation, and therefore correctly formatted commands which define priority values cannot be entered.	
31348		Some 5GHz wireless channels ignore channel bandwidth dependency
	When operating in the FCC regulatory domain, e.g. in "us", some channels in the U-NII-2c band, e.g. channel 165, can only be used when operating with 20MHz channel bandwidth. Selecting these channels when using larger channel bandwidth may be accepted, but may result in a different channel being used. Workaround: Do not manually select channels from U-NII-2c band, i.e. channels 149 - 165, unless you have manually selected appropriate channel bandwidth beforehand.	
31338		No voice in an established call or no ringback tone is played
	Sometimes there is one-way or no voice traffic between the endpoints when a call is made.	
31227		DHCP client does not renew lease after link down
	When uplink is dropped, upstream interfaces do not perform DHCP renewal when link is re-established.	
31199		No DHCP Release upon system reload
	DHCP client does not release the DHCP lease when performing a planned reboot.	

Issue number	First discovered in release	Description
31145		CLI crashes when configuring long hostname
	Using a hostname which is greater than 32 characters in length may result in the CLI crashing. Workaround: Either do not use hostname command, or limit hostname length to less than or equal to 32 characters.	
31143		Vendor Config file download fails
	CWMP triggered download of configuration files may fail to complete successfully.	
31135		Cannot remove ACL rule by sequence identifier
	Removing ACL rules by sequence number is not supported. Workaround: Remove rules by entering complete rule preceded by "no", or remove the entire ACL.	
31100		tcp/2008 port open
	Port 2008/tcp is used internally, but is visible externally. This presents a service security risk. Workaround: Block port 2008/tcp in defined ACLs	
31074		COS mapping is not applied until after reboot
	Class of Service configuration, e.g. by "cos mapping" command is not applied to the switch until after a reboot has occurred. Workaround: Perform a reboot after applying cos mapping configuration	
31069		TFTP firmware upgrade failure
	On rare occasions, TFTP upgrade copy commands may timeout. Workaround: Repeat command execution	
31062		cos mapping dot1p 0,1 on queue 0 not visible with show running command
	"cos mapping" configuration for queue 0 is not displayed in "show running-config" output.	
31016		VLAN interface cannot be shutdown
	It is not possible to disable upstream VLAN interfaces using the "shutdown" command. Interfaces which are "shutdown" will still be operating, but no warning or error is given.	
31013		Device.DNS.Client.Server. objects cannot be created by an ACS
	It is not possible for an ACS to create DNS.Client.Server.i. objects.	
30998		Scheduled firmware download failure
	If a firmware upgrade, or file download, is scheduled for a time in the future by TR-069 management system, the download may not execute at the correct time if a system reboot occurs between the time when the download command is given and the scheduled download time.	

Issue number	First discovered in release	Description
30953		Ping command option handling
	When using the ping command, if one enters a size option, it is then not possible to enter a count option - the reverse order works correctly. Workaround: Specify the any count option before the size option.	
30947		Cryptic upgrade failure messages
	Error and warning messages generated in the event of an upgrade failure do not clearly explain the cause of the upgrade failure.	
30939		WAN and LAN RJ45 ports shows different LED behaviour for 100Mbps
	The behaviour of the WAN connector LEDs do not comply with defined behaviour when the link speed is 100Mbps - only the yellow LED should be lit. Affects: Platinum-7840	
30890		Layer 2 traffic leaks to LAN interface
	Layer 2 traffic bridged between the WAN and LAN ports may leak to the layer 3 LAN interface.	
30882		SYN flood attack prevents connection
	Rate limiting may not prevent SYN flood making it impossible to access an interface.	
30881		CPU port counters can not be retrieved
	It is not currently possible to access internal interface statistics counters.	
30880		L3 interfaces are visible in CLI and ACS
	It is possible to see layer 3 interface definitions via management interface even though the device is layer 2 only. Affects: FibreTwist-2410	
30870		Incorrect TR-181 interface object used
	The Device.Ethernet.Interface object is used as the WAN physical layer interface, therefore the Device.Optical.Interface should be used instead. Affects: FibreTwist-2410	
30854		LEDs flicker in dimmed states
	When LED dimming is enabled, there is some high frequency flickering in the HIGH and LOW dimming states. In the ON and OFF there is no flickering.	
30843		ACS may not receive parameter change notification
	The ACS may not receive an Inform with *4 VALUE CHANGE* from device within 120 seconds of change to a parameter	
30762		Occasional DNS lookup for new hostname fails

Issue number	First discovered in release	Description
	Sometimes a DNS lookup for a non-cached hostname may result in a failure response even though the hostname does exist in the DNS entries.	
30580		"show interface" generates error for some interfaces
	The output from the "show interface <interface>" command can generate errors where the interface name is currently not supported, e.g. "lan", "wlanX"	