Document	
Release Notes WeOS 5.28.1	
Date May 11, 2026	Document No 224004-gd3028f2

WeOS 5.28.1
Release Notes

Contents

Document	
Release Notes WeOS 5.28.1	
Date May 11, 2026	Document No 224004-gd3028f2

Legal Information

The contents of this document are provided “as is”. Except as required by applicable law, no warranties of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose, are made in relation to the accuracy and reliability or contents of this document. Westermo reserves the right to revise this document or withdraw it at any time without prior notice. Under no circumstances shall Westermo be responsible for any loss of data or income or any special, incidental, and consequential or indirect damages howsoever caused.

More information about Westermo at http://www.westermo.com

Document	
Release Notes WeOS 5.28.1	
Date May 11, 2026	Document No 224004-gd3028f2

Important User Information

This section details important user information, directed in particular to new users of WeOS 5:

For help with getting started using WeOS 5, refer to the Quick Start Guide in section 5.

User Guide

In WeOS 5, the primary user documentation is referred to as the WeOS 5 *User Guide*. Compared to the WeOS 4 *Management Guide*, the User Guide is a web first publication focusing on use-cases, documented in stand-alone "HowTo:s", and configuration guides for all supported sub-systems.

The User Guide is included in the release Zip file in the sub-directory: `doc/weos/user-guide/`. To access the documentation, open the following file in your web browser:

`file://Downloads/WeOS-5.28.1/doc/weos/user-guide/index.html`

The *User Guide* is also available online at `https://docs.westermo.com/weos/weos-5/`.

Document	
Release Notes WeOS 5.28.1	
Date May 11, 2026	Document No 224004-gd3028f2

1 Summary of Changes

This section details new features added in this minor release.

Users new to WeOS 5 are recommended to read section 7 carefully, as it high-lights some of the major differences between WeOS 4 and WeOS 5.

1.1 News in 5.28.1

The subsection below describe news in WeOS 5.28.1. In addition, section 2.1 includes information on fixed issues.

1.1.1 Security Patched Boot Loader

WeOS 5.28.1 is delivered with a security patched boot loader, Barebox v2024.03.0-4, to remediate a vulnerability affecting devices with Secure Boot. Without the patched boot loader the chain of trust required for Secure Boot may be compromised. More details are available in security advisory Westermo-26-01.

Please note that this release and future WeOS 5 releases will **require a boot loader upgrade** if running a Barebox version older than v2024.03.0-4. Details about upgrading the firmware is available in section 6.1.

1.1.2 Boot Loader Downgrade Prevention

Because of the boot loader upgrade as mentioned in section 1.1.1, WeOS 5.28.1 will block downgrades of Barebox to versions older than v2024.03.0-4.

1.1.3 Certificate-based Authorization in IPsec

Support for establishing IPsec tunnels using IKEv2 with certificate-based authentication has been added. Configuration allows for selecting of an end-entity (leaf) certificate for authentication towards the peer and ca-certificate that is a root-CA certificate validating the incoming peer's certificate chain.

1.2 News in 5.28.0

The subsection below describe news in WeOS 5.28. In addition, section 2.2 includes information on fixed issues.

1.2.1 Issue 21076 - Redfox and Lynx-5000

In this release a problematic behaviour with flushing of FDB entries has been corrected. This issue could lead to long failover times on topology changes as the flushing operation could fail to clear

learned FDB entries. In networks where protocols the relies on FDB flushing for network convergence such as FRNT, RiCo, RSTP or MRP is used with the effected products it is **strongly recommended that these devices are upgraded.**

1.2.2 VRRP Accept Mode

Support for VRRP Accept Mode, as per RFC 5798, has been added. When enabled, the VRRP instance will accept packets destined to the VRRP virtual IP address, regardless of VRRP state. This can be useful in certain scenarios, for instance if the virtual IP address is used as a destination for network services, or when setting the virtual IP address to an address that is already used by the base interface.

The default value of Accept Mode is enabled.

1.2.3 SCEP handling of no dedicated RA

Now the WeOS SCEP client handles situation when the SCEP server does not provide dedicated RA-certificate(s).

For more information see the WeOS User Guide section *Configuration Guides → PKI → Enrollment*.

1.2.4 Custom TRDP telegrams

Operational mode-etbn limitations for Custom TRDP telegrams have been removed. Support for aliases in Custom Telegrams has been added. Support for configuring custom telegrams as sent by any device or by only the master consist ECSP has been added for outgoing custom telegrams when opera mode full is used.

1.2.5 Application Hosting

This version of WeOS introduces application hosting feature, which allows container applications to be installed, configured and managed within the host OS.

1.2.6 IPsec Identity Handling Revised

The handling of IKE identities (`local-id` and `remote-id`) for IPsec tunnels has been revised. When a value is supplied without an explicit type keyword, WeOS now uses *autodetect* mode.

Compatibility note: This change may affect existing configurations. If tunnels that were working before fail to authenticate after upgrading, verify that the identity type used by each peer matches on both sides. Typically auto-detection works, use an explicit type keyword to avoid ambiguity.

For more information see the WeOS User Guide section *Configuration Guides → Tunnels and VPN → IPsec → Identity types*.

1.2.7 Port Access Control

This version of WeOS includes a large amount of additions and adjustments to the Port Access Control support. A summary of these changes includes:

- **VLAN Assignment Support** - Support for dynamic VLAN assignment has been added for both 802.1X and MAC-based authentication (MAB). Ports can now be assigned to VLANs as provided by the RADIUS server.
- **Configurable Port Method** - Support for configuring Port Method has been added. Previously, the implicit behavior was to authenticate each client individually based on their MAC address. This behavior is now configurable via the `port-method` setting, which supports two modes:
  - `mac-based` - Clients are authenticated based on their MAC address. All clients must be individually authenticated to be granted access. This is the default mode and matches the previous implicit behavior.
  - `port-based` - If a single client is authenticated on the port, the entire port is opened, granting access to all other clients on the network. This is the new mode introduced by this feature.
- **Multiple Port Access Instances** - Support for creating multiple port access instances has been added, allowing port-specific configuration settings.
- **Quiet Period for 802.1X** - Support for configuring Quiet Period has been added for 802.1X authentication. The quiet period is a time interval, after a failed authentication attempt, during which any new authentication requests from the same client will not be processed.
- **Improved RADIUS Communication** - RADIUS attribute handling has been improved for both 802.1X and MAB to provide more accurate and compliant communication with RADIUS servers.
- **MAB Service Type Configuration** - Support for configuring the RADIUS Service-Type attribute for MAC Authentication Bypass (MAB) requests has been added. The `service-type` setting determines how authentication credentials are sent to the RADIUS server during MAB authentication:
  - `call-check` - Uses Service-Type 10 (Call Check). The device will use the client's MAC address as both username and password in the authentication request to the RADIUS server. This is the default mode.
  - `authenticate-only` - Uses Service-Type 8 (Authenticate Only). The device will not send any username or password in the authentication request to the RADIUS server. This was the previous implicit behavior for MAB authentication.

- **WEB Configuration** - The WEB GUI's configuration interface for Port Access Control has been completely redesigned to provide improved usability and access to new features.
- **CLI Configuration** - The CLI configuration for Port Access Control has been refactored to improve handling of existing options while also providing access to new features.
- **Improved Status Pages** - Both the WEB page and CLI context for Port Access Control status have been completely redesigned to try and improve what information is displayed and how it is presented. The status information can be displayed per Port Access Control instance or unified across all instances, and can be filtered to focus on four different aspects:
  - `802.1X Authentications` - Shows currently authenticated 802.1X clients with their details.
  - `MAC Auth Authentications` - Shows currently authenticated MAC authentication clients (both MAB and local accept list).
  - `Ports` - Shows status of the ports, as they relate to Port Access Control.
  - `VLAN Assignment` - Shows VLAN assignment status per port.

For more information see the WeOS User Guide section *Configuration Guides → Bridging/Switching → 802.1X & MAC-Auth*.

2 Fixed Issues

2.1 WeOS 5.28.1

Fixed issues in WeOS 5.28.1 (as relative to 5.28.0).

Issue	Category	Description
#21118	TCN	etbnd spams log with timeout entries in some systems running custom TRDP data

2.2 WeOS 5.28.0

Fixed issues in WeOS 5.28.0 (as relative to 5.27).

Issue	Category	Description
#21076	System	Flushing fdb can take a long time (Redfox and Lynx 5000
#21013	AAA	Possible to bypass password policy when updating expired password
#21011	VPN	Automatic detection of identifiers in ipsec configuration may result in interoperability issues
#20976	Ports	SFP-1100-0818 - 10G-ZR are unable to get link up
#20975	TCN	ECSP_STATUS remote or local inauguration inhibition flag not correctly cleared after coupling
#20974	TCN	Backup ECSP fails to generate the TTDB and report 0 consist coupled when the ECSP times out from a coupled consist
#20954	AAA	User with role Engineer cannot change configuration
#20946	System	CLI stuck in connection loop for 15+ seconds if no FQDN connectivity in Wireguard peer
#20895	Port Monitoring	Disabling/deleting Port Monitor on Lynx 5000 and Redfox causes communication stop
#20894	WEB	The DHCP option 12 and do not allow FQDN to be set via WEB but is allowed in CLI and according validation schema
#20886	MRP	EC-62439-2-MIB Do Not Count Up
#20835	Ports	Port priority can't handle change or reboot
#20816	Firewall	Neither input nor forward rules can have "ANY" as interface
#20752	General	PKI : only first certificate in a bundled visible
#20737	VRRP	VRRP do not consider vrrp-startup-delay at bootup if another vrrp device is active and spam logfile with bad entries

Continued on next page

Continued from previous page

Issue	Category	Description
#20724	WEB	Rich is an extended functionality in web and non extended functionality in weos
#20712	TCN	ETBN bypass relay control not working in comID 130
#20658	VRRP	Multicast routing intermittent perpetual failure during VRRP failover with preemption
#20533	SNMP	Wrong values in the "ttdpSubnetIPMask" OID anwers, the MIB returns 255.255.252.0 (/22), but shall displays 255.255.192.0 (/18)
#20526	Alarm	The selection of SSL tunnel as alarm target in action diff between CLI and WEB
#20515	TCN	teamd spam logfile at start of device
#20509	WEB	PKI - Enrollment Servers configuration page does not have a Help webpage
#20144	Alarm	Ping Alarm indicates UNREACHABLE when the destination is reachable
#20127	System	Metricsd can cause leak memory
#20091	Link Aggregation	LACP Removal of lag when custom fdb filters referenced to the lag fails assertion of the running-config file
#19924	VRRP	VRRP instance is not restarted when doing a config restore on Vipers
#19255	QoS	Priority-mode IP fails when both ingress and egress ports are fiber ports on Envoy platform
#18362	TCN	Broken/missing ECSPs in train composition handled incorrectly

3 Known Limitations

This section describes known limitations in WeOS.

3.1 Ring Coupling version 2 not supported

Support for FRNT Ring Coupling (RiCo) version 2 was removed in 5.15.0 due to problems with the stability of the function. Most of the use cases for RiCo version 2 can be covered today through the use of FRNTv2 and RiCo v3.

For information around FRNT v2 and RiCo v3 usage please contact local Westermo support.

3.2 Port Access Control (IEEE 802.1X and MAC Authentication)

Wake-on-LAN is currently not possible on controlled ports. The reason is that broadcast traffic is not allowed to egress a controlled port until there is at least one MAC address authenticated on the port.

3.3 RMON

Some Hardware platforms are unable to provide certain RMON counters due to problems with the hardware chipset.

- RCV Error counter does not work on Viper 3512 and 3520
- FC Received (rx_pause) does not work on Lynx 5000 and Redfox

3.4 Login

Known limitations related to the Login service.

Side-effect of disabling console login

When disabling login from console, login via telnet is also prohibited (even when telnet login is enabled).

SSH Public Key Lost When Disabling Built-in User

WeOS 5.13.0 introduces support for importing SSH public key for built-in users, as well as the ability to enable/disable a user. When disabling a user, the intention is that the user shall be prohibited from logging in, while other user configuration is till kept in the configuration file.

However, the disabling of a user currently implies that any SSH public key associated with the user is removed and needs to be imported again upon enabling the user.

3.5 Setting Date Manually

Setting a manual date on the WeOS unit before 1 January 2000 will render an error message.

3.6 Available ports for boot specific functionality

The boot loader rescue mode only supports regular copper ports, not SFP ports. On RedFox-5528, ports 1-4 are also not supported until the system has booted.

3.7 Routing Hardware Offloading

The routing Hardware Offloading support for Viper-TBN introduced in WeOS 5.8 has shown to have instabilities. In particular, when used with dynamic routing, there are issues not yet solved. Therefore hardware offloading has temporarily been Disabled by default.

```
viper:/#> configure
viper:/config/#> ip
viper:/config/ip/#> offload
viper:/config/ip/#> leave
```

When Offloading is Enabled, regular IPv4 forwarding is handled in hardware with some exceptions, see the WeOS 5 User Manual for details (section 'Configuration Guides'/'Routing'/'Offloading').

For Redfox and Lynx-5000 initial Offloading support in 5.23.0. Functionality only cover a very small subset of use cases yet and has a list of restrictions.

The Known limitations for offloading on Redfox and Lynx-5000:

- Routed IPv6 traffic is handled by the CPU
- IP multicast traffic will be routed by the CPU
- Firewall forwarding chain will not impact any routed Unicast traffic
- NAT will not be performed on any routed traffic
- Only VLAN interfaces can be used, usage of Port-interfaces will not perform any traffic forwarding
- Policy-Based Routing will not function
- SSL-tunnel will function to some extent via the CPU but is strongly discouraged from being used in this release

Tracking vrrp instances with mroutes is not supported when offloading is enabled. If this feature is used it is recommended to disable offloading. (opposite steps to the example above).

Use of the WeOS Firewall together Hardware Offloading is not supported and the behaviour of doing so is undefined. The exception is when firewall configuration is limited to *filter input* rules.

Hence, if the Firewall is use to configure *filter forwarding* rules, *NAPT* rules or *port forwarding* rules on a Viper-TBN, it is necessary to disable the Hardware Offloading (opposite steps to the example above).

```
viper:/#> configure
viper:/config/#> ip
viper:/config/ip/#> no offload
viper:/config/ip/#> leave
viper:/#>
```

3.8 Redundancy protocols on Relay ports

It is only supported to run link-aggregation as the selected option for redundancy on Relay ports. This is due to the fact that any other protocol can end up in very uncertain situations in cases where the bypass-relays are used.

In the future WeOS may refuse enabling these protocols on relay ports.

3.9 FRNT

Fastlink must be enabled manually for FRNT (gigabit Ethernet) ring ports.

Fastlink is a unique feature of Westermo products to optimise gigabit Ethernet link-down fail-over times in layer-2 redundancy protocols such as FRNT.

3.10 RSTP

WeOS 5 supports RSTP, compliant to IEEE 802.1D-2004. Due to limitations in the WeOS 4 implementation of RSTP, a WeOS 4 unit will keep ports in blocking mode longer than needed when connected to a WeOS 5 node.

Hence, mixing WeOS 4 and WeOS 5 units in RSTP topologies may exhibit relatively long periods with limited connectivity during topology changes, this applies to both link failure and when a link comes up again.

Link aggregate path-cost use the configured port speed value(s) and not the negotiated speed value. This can lead to RSTP making the non-optimal path selection. Work-around this issue by setting a fixed path-cost in the spanning-tree port configuration.

3.11 IEC 61375

In this release, not all of the recovery use cases, nor the optional cases, are supported.

TTDP and non-TTDP multicast can be used simultaneously in this release, but is considered unstable and is strongly recommended to be avoided.

"Automatic Gap Insertions", when several vehicles have the same name, can lead to unexpected behaviour.

When recovery-mode is set to deferred/wait, an ECSC must be running on the configured multicast address. If no ECSC is running and sending data on the configured multicast address, no node will come up at all.

It is strongly recommended to enable inauguration inhibition on all nodes to reduce spurious re-inaugurations and guarantee a stable train communication.

The “ECSP inhibit sync” function should only be enabled in consists with simple or straightforward ECN configurations. In complex configurations with non-symmetric ETBN/ECN connections and/or configurations where different ETBNs are master routers for different ECNs simultaneously, the backup ETBNs will not be able to unambiguously determine which ETBN is the master router/ECSP, which can in turn lead to unexpected behaviour with regards to the local inauguration inhibition value. In these cases, manually setting the local inauguration inhibition values on the backup ETBNs, via the ETBN_CTRL telegram, should instead be performed.

VRRP virtual IP address ("VIP") is primarily intended to be used as a gateway/router address, and not as a host address. However, using the VIP as a host address, that at any one time belongs to the currently active ECSP is a common use case. When using the VIP in this way, for ECSC-ECSP communication, it is recommended that the "vmac" option in the VRRP configuration be turned off for all VRRP instance whose VIPs are used in this way.

3.12 Custom TRDP telegrams

The implementation of Custom TRDP telegrams has some limitations:

- Data from up to 32 device ports can be included across all defined datasets.
- Data from up to 8 VLANs can be included across all defined datasets.
- Data from up to 4 FRNTv2 rings can be included across all defined datasets. FRNTv2 is the only supported ring protocol for which data can be included.

3.13 LLDP

When using Link Aggregation, the individual member ports will transmit LLDP frames using the MAC address of the link aggregation interface, i.e. all member links in an aggregate will be using the same MAC address.

3.14 Port Monitoring

It is not possible to utilise port monitoring directly on a link aggregation port interface. However it is still fully possible to monitor the individual member ports that constitute any given link aggregate.

Therefore, in order to fully monitor an aggregate, monitoring must be configured for each of the aggregate member ports.

3.14.1 Cross switch core limitation

It is not possible to use port-monitor where the source and destination ports are splitt between switchcore 2 and 3 on Viper-120 and Viper-220 products.

Having the source and Destination port on the same switch core or one of the source or destination ports on ports ethX7, ethX8, ethX14 or ethX20 while the other resides on one of the other switchcores is possible.

3.15 Media Redundancy Protocol (MRP)

- *MRM not supported for MRP 30 profile:* WeOS 5 units can be configured to operate in MRP 200 or MRP 30 profile. However, for MRP 30 profile, configuring the WeOS 5 unit as MRP Master (MRM) is not supported. A WeOS 5 unit can be used as MRP Client (MRC) with MRP 30 profile with MRMs from other vendors.

  More details: When a link comes up between two MRP clients, the clients send *link-up* messages to the MRP master. The MRP 30 ms profile only gives the MRP master 4 ms to block its secondary port from the time the MRP clients send their first *link-up* message. The WeOS 5 MRP Master is not always capable of doing that, resulting in a short transient loop in the MRP ring when the ring is healed.

  To avoid this, it is recommended to use the MRP 200 ms profile instead. For link-down scenarios, MRP 200 ms profile conducts failover as fast as the 30 ms profile, given that MRCs in the ring are capable of sending MRP *link-down* messages (WeOS units have this capability).

- *Use of MRP with virtual L2 ports (SSL VPN ports):* MRP is specified for use with Ethernet ports (full duplex, 100 Mbit/s or higher). WeOS enables the use of running MRP over SSL L2 VPNs, but requires the VPN to run over a high-performance network to work well. Furthermore, only the MRP ’200 profile’ can be used with SSL VPNs.

3.16 10G SFP Ports

The 10G SFP ports on RedFox-7528 have the following limitations:

- IEEE 1588/PTP is currently not supported on 10G SFP ports.

- 10G SFP ports are only to be used for 10G Fiber SFPs or 1G Fiber SFPs, not copper SFPs or 100 Mbit/s Fiber SFPs.
- Status of MDI/MDIX and polarity shows value 'Invalid' ('N/A' or 'Not Applicable' would be more appropriate).

3.17 Search function in User Guide

The User Guide included within the release-zip is Web based. The Search function in the User Guide navigation pane only works if you make the pages available via a Web Server. That is, the Search function does not work when opening the User Guide via your local file system.

At https://docs.westermo.com/weos/weos-5/ you can browse the WeOS 5 User Guide online, with Search function included.

3.18 RedBox PTP Boundary Clock

RedBoxes running Boundary Clock in an HSR ring must be connected with all A ports in the same direction. As the BC prioritizes synchronizing from the A port, if two BC are synchronizing towards each other neither of them may end up in a stable state.

Connect devices as shown below:

```
ethA-RB-ethB <-> ethA-RB-ethB <-> ethA-RB-ethB ....
```

3.19 Ingress rate limiting

On Viper-3000 series and Lynx-3000 series, ingress rate limiting of multicast traffic includes broadcast.

3.20 Policy Traffic Filtering

For Redfox 7000/5000 and Lynx 5000-series, policy traffic filtering counters are not functional for drop filters and are therefore not displayed.

3.21 Static unicast MAC filters for link aggregates

Static unicast FDB filters are known to not work as expected when the port associated with the filter is a link aggregate that spans multiple switch cores.

4 Known Issues

4.1 List of known issues

Issue	Category	Description
#21086	System	Show fdb includes unexisted enteries
#21078	System	Setting static speed/duplex works only the first time (Viper 3000)
#21077	TCN	TTDP remote-inhibit flag does not consider both ends simultaneously
#21068	Alarm	Alarm instance is not restarted when doing a config restore
#21067	IGMP	IGMP membership reports forwarded on all ports
#21063	SNMP	SNMP commands depend on order they are defined
#21040	VLAN	Creating lots of VLANs can lose LAN settings
#21038	System	Metrics not showing correct values on Viper 3000 and Lynx 3000
#21037	Link Aggregation	"no lag <X>" does not removing lag <X> from "show running configuration"
#21016	Ports	Redfox and Lynx 5000 autoneg to 1Gbps/s may fail and fall back to 100Mbps
#21015	TCN	If ECSP-ADDR is undefined (auto) then ETBND fails to start
#20991	NTP	NTP client may take one full poll interval to start requesting remote server when starting in larger systems
#20973	NTP	Missing some documented NTP log messages
#20964	WEB	Session timeout does not work when using multiple browser tabs
#20957	System	Lynx 5000 and Redfox inconsistent hotswap of External media disk without partitions
#20953	System	Sending DSCP priority packets from cpu will use Lowest Priority queue (0)
#20935	System	Ingress rate limiting unknown unicast also limits known unicast when routing
#20919	General	certificate store isn't findable by client utilities
#20909	Policy	Trap counter in Policy Filtering does not work
#20896	Any	mDNS discovery not working on Redbox
#20891	Kernel	Port priority does not work across switchcores (DSA)
#20888	Ports	Redfox and Lynx 5000 SFP handler can fail to setup the correct low level duplex settings for Gbps SFPs
#20868	System	Ports Eth1-Eth4 on Redfox can become unable to transmit packets after sustained CPU routing overload
#20833	System	Buffer overflow via crafted input leading to denial of service

Continued on next page

Continued from previous page

Issue	Category	Description
#20831	AAA	IPSec ESP cipher authentication value does not match the CLI/config settings
#20828	System	Deactivating Watchdog in Lynx + RedFox 5000 & 7000 series reboots the unit continuously
#20826	VPN	Dpd timeout treated as constant in schema and not written to strongswan configuration file (only applicable for IKEv1)
#20822	Alarm	Configuring RING alarms from WEB results in wrong acvtive mode (condition)
#20820	WEB	Web becomes unusable when an upgrade was aborted or done without a reboot
#20771	WEB	WEB page is sporadically not updated after configuration
#20749	TCN	TCN can fail to build TTDB properly in the extremity 2 backup TBN when cstinfo have same cstID and/or vehID
#20748	System	RMON does not show Filtered/Discarded values
#20733	Firewall	Port forwarding can not handle other protocols than TCP and UDP
#20703	VLAN	Incorrect ARP requests sent when bridging LAGs on Redfox and Lynx 5000
#20662	Any	no boot does not reset allow-untrusted/unlock-license
#20627	Port Access Control	Inconsistent and delay in MAC Address Authentication
#20617	VLAN	Packets seen on different VLAN in specific circumstances
#20603	System	Upgrade command can hang device forever in runlevel 9
#20578	NTP	RTC may lock at wrong time at power down if backwards time jump has happened
#20574	Logging	Excessive logging during configuration change
#20571	System	Active SSH sessions not closed when a config restore is done via WEB allowing password manipulation in file afterwards
#20410	DHCP	Unable to bind IP address when short DHCP leasetime is provided
#20312	AAA	Possible to get locked out if lockout policy is set and no valid connection to Radius server
#20309	System	Firmware upgrade could reset the user password
#20281	System	The error message "Failed to add audit entry to audit daemon" is spammed when applying large configs
#20249	System	Repeated connections via telnet may cause the telnet service to become unresponsive
#20233	HW	RTC: System time might not be stored correctly
#20231	WEB	Fail with restoring config in WEB but no fault messages

Continued on next page

Continued from previous page

Issue	Category	Description
#20201	System	Rebooting after disabling offloading will remove all traffic policies
#20150	System	DHCP Reply seems to be offloaded, cannot accept address
#20102	SNMP	SNMP value for frntStatusVid1/2 show no data in tables
#20047	WEB	The user is redirected to the login page when editing firewall rules is tried
#20045	LED	After initiating a 'factory reset' from the web GUI, a device will boot up, but the ON LED will remain RED even when boot is com
#20040	Any	When IP address is changed from CLI, a gratuitous ARP is send with the old IP instead of new one
#19965	WEB	FRNTv2 is not shown in Status summary page when it is enabled
#19958	Boot Loader	Envoy Barebox uses precompiled ATF
#19957	General	Port statistics not available on Redfox and Lynx 5000
#19928	TCN	Offloading with TCN does not allow for fragmented packets to be forwarded
#19903	System	configuration restore do not clear previous added route from system
#19882	System	Upgrade from ftp sever with DNS name does not work
#19880	WEB	Refreshing page when upgrade of bootloader or secondary restarts the upgrade if it's done
#19878	CLI	Config abort do not work correctly with an in valid configuration
#19870	IGMP	Multicast Snooping Boundary for MLD does not work on Dagger based systems
#19826	System	Large amount of authenticated SSH sessions causes denial-of-service condition
#19818	SNMP	Syntax errors in Westermo MIB files for FRNT and EVENT
#19777	WEB	Upgrading primary image from web ui does not report flashing done in http response
#19756	VRRP	The vmac of VRRP causes strange log messages and VRRP not to work properly
#19711	WEB	Cannot access help in some menus in webGUI when browser tree menu has gone past the bottom of the screen
#19517	Logging	When PoE-chip goes repetitively down many Kernel logs is generated and stored
#19498	IGMP	Duplicate multicast packets over link-aggregates when changing router timeout (Dagger)

Continued on next page

Continued from previous page

Issue	Category	Description
#19410	IGMP	Missmatch between MDB and ATU for mc group 239.193.0.1 when etbn is acting as router, sender and consumer of data
#19323	FRNT	FRNT Focal point Topology Counter rush with LACP links (Dagger)
#19262	Ports	Traffic not handled on Envoy ports using Copper SFPs
#19251	PoE	Lynx 3510 PoE leds continuously blinking in case of LV supply
#19181	Ports	Port-Priority-mode IP and Offloading broken with DSCP set field
#18967	System	Joins on SSL ports does not lead to the CPU port being added to the ATU
#18675	Link Aggregation	Long failover time (aggregate member link up/down) in link-aggregate interoperability case (WeOS5 'Dagger' vs WeOS4)
#18163	OSPF	Routes to 'redistributed connected E1 routes' lost within NSSA areas upon topology change
#18151	Logging	Long-running programs log events to syslog with the wrong time stamp on timezone changes
#18076	MRP	Probing MRP status (30 ms profile) during heavy load may cause reboot (Viper-TBN)
#18069	QoS	ARP packets treated with lowest priority and may be missed/dropped under load
#17995	System	Service discovery not available in safe-config

4.2 #20888 & #20868 Redfox and Lynx 5000 1Gbps SFP issues

The port will operate in half-duplex mode when using a 1 Gigabit SFP module that is hot plugged into a gigabit SFP slot on Redfox 5000 or Lynx 5000 or when a 1 Gigabit SFP module is used in any SFP+ slot on Redfox 7000. Also note that the port may become unable to transmit frames over that port after sustained device overload until the port is reset.

4.3 #18163: Work-around for OSPF NSSAs convergence issue

When using OSPF Not-So-Stubby Areas (NSSAs), failover when a router goes down may take a lot longer time than expected. There are two possible work-arounds until this bug is fixed:

- Alternative 1: Let each router get an address on its loopback interface, and include them in the OSPF area, e.g., use OSPF setting "network 192.168.1.5/32 area 1" for a router in (NSSA) area 1 with address 192.168.1.5/32 assigned to its loopback interface (lo).
- Alternative 2: Use 'regular' OSPF areas instead of NSSA areas.

5 Quick Start Guide

WeOS 5 devices are intended to be usable out-of-the-box as a switch. All access ports are assigned to the same VLAN (untagged) and the device tries to acquire a management IP address via DHCP. It also acquires a link-local address (in the 169.254.x.x range). These addresses are advertised with mDNS (Linux/Apple), SSDP (Windows), and LLDP.

5.1 Default User and Password

user: admin

password: admin

5.2 General

Apple, Linux, and Windows users with mDNS installed, can either use an mDNS client to find the device's IP address, or connect using a web browser:

- `http://weos.local`
- `http://redfox-4d-3b-20.local`

The first example is not available if there are many WeOS devices on the same LAN. The latter, and more reliable address, is a combination of the hostname and the last three octets of the device's MAC address in that LAN. In this example the hostname is `redfox` and the MAC address is `00:07:7c:4d:3b:20`.

Windows users without mDNS have SSDP to discover WeOS devices. In Windows 7 there is the *Network and Sharing Center* where a clickable icon for each discovered WeOS device should appear under *Network Infrastructure*. The PC must, however, be in the same subnet (DHCP or link-local) for this to work. Windows users also have the Westermo WeConfig tool to manage their WeOS devices.

Expert users can also use nmap, a port scanner, to scan the network for the device. Be aware though that this might be frowned upon should your device be located on a shared network.

5.3 CLI

WeOS comes with a Command Line Interface (CLI) that can be accessed via a console port at 115200@8N1, or Secure Shell (SSH). Only SSH protocol version 2 is supported. To gain access to the CLI using SSH you need:

- An SSH client, see below
- The device's IP address or DNS/mDNS name, see above
- The user name and password, default user: admin, password: admin

SSH Clients

There are many of SSH clients available, some of them can even be used to connect to the devices using a (USB) serial console port. A few free clients are listed below. Please follow the directions for installation and usage applicable to your operating system and client.

UNIX, Linux, Apple macOS OpenSSH, `https://www.openssh.com`

Apple macOS Termius, `https://www.termius.com`

Windows PuTTY, `https://www.chiark.greenend.org.uk/~sgtatham/putty/`

CLI Overview

The CLI has two main scopes: admin-exec and configure context. The former is what the user lands in after initial login.

```
redfox-4d-3b-20 login: admin
Password: *****
.--.--.--.-----.-----.------.-----.-.--.--------.-----.
|  |  |  |  -__|__ --|_    _|  -__|   _|  .  .  |  _  | http://www.westermo.com
 \__/\__/|_____._____| |__| |_____|__| |__|__|__|_____|        info@westermo.se
   Robust Industrial Data Communications -- Made Easy

\\/ Westermo WeOS v5.3 5.3.x-g7890bde -- Oct 24 19:30 CEST 2018
Type: 'help' for help with commands, 'exit' to logout or leave a context.

redfox-4d-3b-20:/#> help
```

Central concepts in WeOS are: ports, VLANs, and interfaces. To see status of each in admin-exec context, use `show ports`, `show vlans`, and `show ifaces`.

To change settings, enter the configuration context with the command `config`. The same commands as above also apply here, but now display the configured settings. Notice how the CLI prompt changes to show the current scope.


```
redfox-4d-3b-20:/config/#>  iface vlan2
```

To show or change the interface and VLAN properties the user enters the command: `iface vlan2` and `vlan 2`, respectively, with an optional "show" as prefix. E.g. `show iface vlan2`.

```
redfox-4d-3b-20:/config/iface-vlan2#>  help inet
```

The help command is always available. Use it stand-alone or with a context-specific setting to get more detailed help.

To leave a level use the command `end` to save or `abort` (or Control-D) to cancel. To save and exit all levels, and go back to admin-exec, use `leave` (or Control-Z).

```
redfox-4d-3b-20:/config/iface-vlan2#>  leave
Applying configuration.
Configuration activated.  Remember "copy run start" to save to flash (NVRAM).
```

The CLI, unlike the WebUI and WeConfig, has a concept of a running configuration. This is an activated but volatile (RAM only) file that must be saved to built-in flash (non-volatile storage) before rebooting. Many separate config files can be saved, but only one can be the selected startup-config. For details, see the built-in help text for the admin-exec copy and show commands.

6 Firmware Upgrade

Firmware upgrade is supported from the CLI, WebUI, and WeConfig tool. The CLI only supports FTP/TFTP upgrade but the WebUI and WeConfig tool can also upgrade via CGI upload – making them the ultimate choice if you have no FTP/TFTP server available or do not care to set one up.

6.1 WeOS Image

WeOS devices run from a built-in flash disk and usually comes with three partitions: primary, secondary, and boot. The latter is for the boot loader (see below) and the primary is the main WeOS image partition. Should this ever get corrupted, e.g. due to power-loss during upgrade, the device will boot using an image from the secondary (or backup) partition. This is a very appreciated, but mostly unknown, robustness feature.

Starting with WeOS 5.28.1, a **boot loader upgrade is required** if you are running Barebox v2024.03.0-3 or earlier to remediate a vulnerability affecting devices with Secure Boot. This means you need to run `upgrade boot` before running `upgrade primary` or `upgrade secondary`. See section 6.2 for details about `upgrade boot`.

Please note that a bug in WeOS versions 5.27.0, 5.27.1 and 5.28.0 will set the device in a state that requires a power cycle if you try to upgrade WeOS without first having upgraded the boot loader.

An alternative is to run `upgrade all` which upgrades all partitions in the correct sequence, not triggering the bug described above, regardless of which WeOS version you are currently running.

To upgrade the primary partition, run:

`redfox-4d-3b-20:/#>` **upgrade primary <SERVER-ADDRESS> WeOS-5.28.1.pkg**

The system must reboot when upgrading the partition image the system started on. This protects against flash corruption issues seen in earlier releases, caused by simultaneous access to the flash during programming or when starting new processes after an upgrade. Also, WeOS warns when one of the partitions has an image with invalid CRC. Attempting to upgrade the partition with the OK CRC is discouraged, upgrade the partition with the invalid CRC first.

As usual, when upgrading from an earlier release, we always recommend backing up your configuration beforehand.

Note: The version string listed in the output from the `show system-information` command in the CLI, or the System Details page in the WebUI, is only updated after reboot.

Note: Starting with WeOS 5.28.1, if you try to downgrade both WeOS and the boot loader from a WeOS package including a Barebox version older than v2024.03.0-4 by running `upgrade all`, you will in effect only downgrade the secondary partition as the `upgrade all` command installs partitions in the following sequence:

- Secondary
- Boot loader
- Primary

Since it is not possible to downgrade the boot loader to a vulnerable version starting in WeOS 5.28.1, the upgrade process will stop after having downgraded the secondary partition.

6.2 Boot Loader

The boot loader firmware has its own version numbering scheme and is CPU platform specific. Unless the release notes explicitly recommend it, there is usually no need to upgrade the boot loader. This and future WeOS releases, however, require a boot loader upgrade if the device is running Barebox v2024.03.0-3 or earlier.

The boot loader firmware is included in the WeOS-5.28.1.pkg.

- Viper-3000 Series (Coronet): Barebox 2024.03.0-3
- RedFox-5000/7000 and Lynx-5000 Series (Dagger): Barebox 2024.03.0-3
- Lynx-3000 Series (Envoy): Barebox 2024.03.0-3
- Lynx-RB (Byron): Uboot 2024.04.0-1

```
redfox-4d-3b-20:/#> upgrade boot <SERVER-ADDRESS> WeOS-5.28.1.pkg
```


7 Significant differences between WeOS 4 and WeOS 5

Some aspects of the CLI are different between WeOS 4 and WeOS 5. Here are some examples:

- Access port names have changed, e.g. `Eth 1` is now `eth1`. Similarly, on products with M12 ports, `Eth X1` is now `ethX1`.
- Port ranges (lists) have changed, e.g. `Eth 1-8` is now `eth1..eth8`
- Server and Internet port settings are now usually input as ADDR:PORT
- IGMP settings have been renamed from `igmp-foo` to `multicast-foo` due to the included MLD snooping support. Hidden compatibility aliases exist to ease the transition
- Stateless NAT (NAT 1-to-1) has moved out from the firewall context
- Enabling management services per interface has moved to each specific service
- Configuration of management services have moved to a separate management sub-context
- New discovery services, in addition to LLDP, are mDNS and SSDP. The latter is for discovery on Windows systems, see also section 5
- The DHCP relay agent CLI syntax has changed considerably
- The `show running-config` command now lists an actual file, in JSON format as mentioned previously. An optional keyword now lists the first level JSON object, and more advanced keywords can also be given in `jq` syntax[1]. For more information, see the CLI online help text for `help running-config`

[1] For more information on jq, a JSON query tool, see https://stedolan.github.io/jq/