Document	
Release Notes WeOS 5.26.1	
Date October 31, 2025	Document No 224004-ge55b5af

WeOS 5.26.1
Release Notes

Contents

1 Summary of Changes . . . 5
1.1 News in 5.26.1 . . . 5
1.1.1 Out-of-Order Problem on Viper-20 for Routed Traffic . . . 5
1.2 News in 5.26.0 . . . 5
1.2.1 Flooding of unicast to CPU . . . 5
1.2.2 Custom TRDP telegrams . . . 6
1.2.3 Firewall - ALG Helpers . . . 6
1.2.4 Port-Provisioning Extension . . . 6
1.2.5 FRNT alarm command . . . 6
1.2.6 Rico-Uplink alarm . . . 7
1.2.7 IPsec IKEv1 with PSK authentication . . . 7
1.2.8 Authentication Chains . . . 7
1.2.9 RADIUS-server message-authenticator extension . . . 7
1.2.10 Policy Traffic Filtering . . . 7
1.2.11 Deprecation Notice - p2p1step . . . 7
1.2.12 AAA RBAC Adjustments . . . 7
1.2.13 Web . . . 8
1.2.14 Downgrade Prevention . . . 8
1.2.15 Lynx Product Family Extension . . . 8
1.2.16 File Transfer Extension . . . 8
2 Fixed Issues . . . 9
2.1 WeOS 5.26.0 . . . 9
2.2 WeOS 5.26.1 . . . 11
3 Known Limitations . . . 12
3.1 Ring Coupling version 2 not supported . . . 12
3.2 Port Access Control . . . 12
3.3 RMON . . . 12
3.4 Login . . . 12

3.5 Setting Date Manually . . . 13
3.6 Available ports for boot specific functionality . . . 13
3.7 Routing Hardware Offloading . . . 13
3.8 Redundancy protocols on Relay ports . . . 14
3.9 FRNT . . . 14
3.10 RSTP . . . 14
3.11 IEC 61375 . . . 14
3.12 Custom TRDP telegrams . . . 15
3.13 LLDP . . . 15
3.14 Port Monitoring . . . 16
3.14.1 Cross switch core limitation . . . 16
3.14.2 Address learning is always active on switchcore interconnection . . . 16
3.15 Media Redundancy Protocol (MRP) . . . 16
3.16 10G SFP Ports . . . 17
3.17 Search function in User Guide . . . 17
3.18 RedBox PTP Boundary Clock . . . 17
3.19 Ingress rate limiting . . . 17
3.20 Policy Traffic Filtering . . . 17
4 Known Issues . . . 18
4.1 List of known issues . . . 18
4.2 #18163: Work-around for OSPF NSSAs convergence issue . . . 23
5 Quick Start Guide . . . 24
5.1 Default User and Password . . . 24
5.2 General . . . 24
5.3 CLI . . . 25
6 Firmware Upgrade . . . 27
6.1 WeOS Image . . . 27
6.2 Boot Loader . . . 27
7 Significant differences between WeOS 4 and WeOS 5 . . . 28

Document	
Release Notes WeOS 5.26.1	
Date October 31, 2025	Document No 224004-ge55b5af

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 5.26.1	
Date October 31, 2025	Document No 224004-ge55b5af

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-5.26.1/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 5.26.1	
Date October 31, 2025	Document No 224004-ge55b5af

1 Summary of Changes

This section details new features added in this major 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 5.26.1

This section describes news in WeOS 5.26.1 (as relative to WeOS 5.26.0). In addition, section 2.2 includes information on fixed issues.

1.1.1 Out-of-Order Problem on Viper-20 for Routed Traffic

Previously, routed packets could arrive in a different order than received. This issue has been resolved in WeOS 5.26.1, but with a trade-off:

- For a single stream* of routed traffic, the theoretical maximum routing performance is now limited to 450–500 Mbit/s.
- When routing multiple streams*, the impact of this limitation is reduced or may not be noticeable.

* A stream is defined as packets with the same source, destination and ports.

Important Note

The actual maximum routing performance without offloading depends on the number of other services and protocols running on the device. The theoretical maximum is not guaranteed.

1.2 News in 5.26.0

The subsections below describe news in WeOS 5.26.0. In addition, section 2.1 includes information on fixed issues.

1.2.1 Flooding of unicast to CPU

This release introduces the ability to enable or disable flooding of unknown unicast traffic to the CPU. By default (as in previous releases), unknown unicast traffic is always forwarded to the CPU. To reduce the CPU load, it is now possible to disable this behaviour to prevent unknown unicast traffic from reaching the CPU.

Important considerations: Disabling this feature may lead to unexpected behaviour, depending on your network configuration. In particular, flooding unknown unicast traffic to the CPU may be required in the following scenarios:

- Use of virtual interfaces, such as when configuring tunnel interfaces.
- Operation of specific network applications.
- Hardware limitations on the switch.

Some network protocols rely on this traffic to function correctly. Disabling it may impact dynamic learning or protocol behaviour in environments where unknown unicast traffic is expected.

Recommendation: Use this feature with caution. When disabling flooding of unknown unicast, ensure your network is thoroughly tested to verify proper operation in your specific deployment.

1.2.2 Custom TRDP telegrams

This release includes support for user defined TRDP telegrams that can be used for device monitoring and some device operation controls.

For more information, see the WeOS User Guide section *Configuration Guides → Train → Custom TRDP telegrams*.

1.2.3 Firewall - ALG Helpers

Application Level Gateway (ALG) Helpers now support custom ports for FTP and TFTP via cli and web interface.

For more information, please see the WeOPS User Guide section *Configuration Guides → Firewall and NAT → Firewall*

1.2.4 Port-Provisioning Extension

Port provisioning has been extended with a *mode* attribute, which allows two different modes of operation to be configured: *one-shot* - which reflects original functionality, meaning it allows provisioning to be executed only once, upon boot. *always* - unlike *one-shot*, it makes provisioning run on every device bootup.

Port-Provisioning has also been extented to support Viper-3000 products in this release.

For more information, see the WeOS User Guide section *Configuration Guides → Generic Maintenance → Provisioning*.

1.2.5 FRNT alarm command

FRNT as a trigger when configuring an alarm has been removed since it has been flagged as derecated for some time. The configuration will be converted to the new Ring trigger on boot.

1.2.6 Rico-Uplink alarm

The option to configure a Rico-Uplink alarm has been removed since the RICO version intended for the alarm is no longer supported.

1.2.7 IPsec IKEv1 with PSK authentication

IPsec IKEv1 with PSK authentication is now available for back compatibility with WeOS4 devices. Note that IKEv1 is considered less secure than IKEv2 and should only be used when necessary.

For more information, please see the WeOS User Guide section *HowTos → Tunnels and VPN → IPsec IKEv1*

1.2.8 Authentication Chains

The old login method selecting is replaced with authentication chains. Authentication chains allow for more flexible configuration of multiple authentication methods.

1.2.9 RADIUS-server message-authenticator extension

When configuring aaa/remote-servers for unencrypted RADIUS, the clients can be made to ignore missing message-authenticator attributes from the server. Only use this to accept non-secure RADIUS servers. WeOS itself will always send the message-authenticator attribute however.

1.2.10 Policy Traffic Filtering

Additional traffic filtering capabilities have been added to the to the traffic policy subsystem. Additionally, policy traffic counters for configured filters have been added to the WeOS Web GUI and CLI.

For more information, please see the WeOS User Guide section *Configuration Guides → Policy Filtering → Policy*.

1.2.11 Deprecation Notice - p2p1step

In future releases, the timestamping mode "onestep" will always use the best timestamping mode when possible, and the "p2p1step" option will disappear. Deprecation warnings have been added to both the CLI and the WebUI.

1.2.12 AAA RBAC Adjustments

A new user role, the Viewer, has been introduced to replace the Guest role, which is now deprecated.

A new user role, the Engineer, has been introduced, who has permissions to view and read objects and values with-in the device and also to configure most functionality except some security features like AAA, PKI or audit logs.

The permissions of the existing user roles, like the Operator, have been slightly modified according to the new RBAC framework, which splits the CLI commands into different RBAC modules and assigns permissions to the user roles on those RBAC modules.

For more information, please see the WeOS User Guide section *Configuration Guides → AAA and User Management → AAA*.

1.2.13 Web

Added support for a configurable setting to allow suppression of login authentication error messages on the Web login page. The release also includes some minor adjustments and improvements to the configuration pages for management services (WEB, SSH, Telnet, CLI, Console).

1.2.14 Downgrade Prevention

To prevent users from downgrading to a WeOS version that does not support their product model, an additional check has been added. If a downgrade to an unsupported version is attempted, the upgrade will be blocked and an error message will be displayed.

1.2.15 Lynx Product Family Extension

WeOS 5.26.0 introduces support for the latest additions to the Lynx-3000 family: the Lynx-3510-F4G-T6G-LV and Lynx-3510-F2G2.5-F2G-T6G-LV. Both models are available in Standard and Extended versions, and feature an integrated TPM (Trusted Platform Module) chip for enhanced cryptographic security.

1.2.16 File Transfer Extension

Any CLI command that performs a file transfer action (*upgrade, package install, PKI import, unlock license, file import, file export*) now has support for all of the following protocols: TFTP, FTP, SCP, SFTP, HTTP, and HTTPS. In addition to that, these commands also have support for the option to use an external storage device as the designated source or destination.

For more information, please see the WeOS User Guide for each individual section.

2 Fixed Issues

2.1 WeOS 5.26.0

Fixed issues in WeOS 5.26.0 (as relative to 5.25).

Issue	Category	Description
#20586	System	SCEP enrollment leave out the Subject Alt-Name field when generating the enrollment request
#20495	QoS	Ingress-rate-limit combine multiple options (mc and bc) doesn't work
#20494	VPN	Trying to set an invalid PSK on an IPSec tunnel does not give clear explanation
#20493	SNMP	'show json ports' does not respect ifIndexPersistance setting
#20480	CLI	Significant delays may be encountered on 5.25 following reconfiguration, possibly due to lock
#20477	WEB	Get time from client not timezone aware
#20474	WEB	Warning text in WEB looks messy
#20468	System	Port provisioning doesn't work/exist on Viper-A
#20463	General	SCEP: audit event logs missing when enrollement or renewal failes
#20433	System	Backup configuration file includes wrong PTP step_threshold
#20413	General	FRR 8.5.1 CVE-2024-31951
#20409	General	FRR 8.5.1 CVE-2024-31950
#20306	VPN	Typing "sh ipsec X" with incomplete tunnel settings shows unwanted output
#20292	LED	HW-Alarm does not control LED consitently
#20280	LED	LED-flash tool does not work
#20241	Any	Disabling stateless NAT rule does not function
#20111	CLI	Port priority-mode 'prefer', autocompletes to 'preferred'
#20107	WEB	Firewall counters not shown in the status section
#20101	SNMP	SNMP value for frntStatusBlockingPort show wrong data with an offest of "-1"
#20006	General	Unclear IPsec error message when trying to set PSK with both success/error messages
#19894	VPN	Diffuse error message when IPsec PSK length < 8 characters
#19815	VPN	No information with "sh tunnel ipsec X" if tunnel is not up
#19786	Routing	Autocompletion (tabbing) in configure>tunnel>ipsec context can crash CLI
#19638	General	Only admin user can change their password in Web

Continued on next page

Continued from previous page

Issue	Category	Description
#19449	WEB	Packets and Bytes always 0 for firewall counters under WEB
#20708	TCN	TCN input validation of cstinfo file report "semantic error" for correct files and block TTDB
#20689	System	Validation error for assigning iface that contain logical ports in DHCP-relay
#20668	Ring Coupling	Ring Coupling supervision not detecting lost node and only lost link
#20664	VPN	SSL tunnel fail to establish if the client cert was signed by MD5 or SHA1 after a firmware upgrade to WeOS5.23.0 or newer
#20660	System	WeOS permanent hang during upgrade
#20657	Boot Loader	Incorrect SIGN LED behavior
#20647	System	USB upgrade with .pkg does not work
#20645	FRNT	FRNTv2 ring recovery when a member comes back can take over 1700ms
#20643	System	New VRRP interface not defines as pure interfaces and get deleted by confd on config read in at startup
#20631	WEB	New VRRP interface not part of WEB configuration as selectable interfaces for services like DNS and NTP
#20630	Alarm	RiCo-Link alarm locks as active and report not active to user
#20597	Ring Coupling	RiCo spam Audit log with state changes every second
#20539	WEB	system common html error
#20538	WEB	vlan_stats page html error
#20537	WEB	Watchdog web page html error
#20527	WEB	Spelling and grammar issues under Metrics configuration page in WEB
#20521	System	Validation error for dhcp-server -> subnet -> domain configuration
#20516	Logging	Audit log file can be removed from file/log context
#20459	CLI	File/export: entire filesystem available for export
#20453	Alarm	FRNT alarm stuck as FRNT not active regardless of state
#20417	VPN	MPTCP in SSL tunnel not starting subflow link in some circumstances
#20328	TCN	TCN may miss to activate ECSP master state even if the VRRP state is set as Master
#20279	WEB	Error occurs when the user deletes an IPsec tunnel
#20266	Build/Image/Zip	Upgrade from USB does not work

Continued on next page

Continued from previous page

Issue	Category	Description
#20212	Port Access Control	Valid MAC addresses blocked if too much traffic is sent during link up
#20100	SNMP	SNMP value for frntStatusTimeSinceLastChange has wrong format
#19964	LED	The LED indicators for FRNT and RSTP on both Envoy and Dagger do not turn off when the protocol is disabled
#19950	CLI	Command injection in clish 'show' command
#19946	System	Upgrade not working using SCP, device also gets soft-locked

2.2 WeOS 5.26.1

Fixed issues in WeOS 5.26.1 (as relative to 5.26.0).

Issue	Category	Description
#20770	AAA	RADIUS hostname is functional but does not accept "-" character in strings
#20763	WEB	SSL-tunnel status web page is broken
#20762	WEB	PIM status web page is broken
#20760	WEB	Link-aggregate status web page is broken
#20756	WEB	VRRP status web page is broken
#20744	TCN	Custom-TRDP telegrams blocked from working on L2 platform after moved into TTDP context
#20740	System	WeOS reports wrong model name for RedBox devices
#20455	WEB	FRNT status page doesn't display FRNTv0 status on WEB
#19783	System	Out-of-order problem on Viper-20 for routed traffic
#19721	TCN	Setting port Admin state as "No Enable" not respected on TTDP LAG ports

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:

- The Custom TRDP telegrams feature is only available if the TTDP (IP-TCN) operational mode is either **full** or **off**. It is currently not supported in **etbn-only** mode.
- 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.

3.14.2 Address learning is always active on switchcore interconnection

For products that include multiple switchcores it is not possible to disable dynamic forwarding database learning entierly. Traffic will always be learned on the interconnection ports. Therefore, dsabling learning on all ports may not result in all traffic being flooded.

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.

4 Known Issues

4.1 List of known issues

Issue	Category	Description
#20726	TCN	Custom-trdp input file validation does not accept comment in items and refuse to accept file
#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
#20703	VLAN	Incorrect ARP requests sent when bridging LAGs on Redfox and Lynx 5000
#20694	VPN	IPsec Unable to change Role from Initiator to Responder.
#20693	WEB	DHCP-relay webpage does not return errors if validation error occurs
#20690	System	System crash with reboot after X hours when running "repeat show logging"
#20662	Any	no boot does not reset allow-untrusted/unlock-license
#20658	VRRP	Multicast routing intermittent perpetual failure during VRRP failover with preemption
#20653	System	Excuting show FDB over SSH towards dagger devices breaks FRNT ring in special circumstances
#20649	Alarm	Interval is not saved to config file for Trigger types Media and Media-Threshold
#20633	RSTP	SNMP service not responding causes RSTP to storm
#20627	Port Access Control	Inconsistent and delay in MAC Address Authentication
#20623	VPN	IPsec: The status box for the IPsec tunnel is always empty
#20622	VPN	IPsec: Web shows different status than CLI
#20617	VLAN	Packets seen on different VLAN in specific circumstances
#20613	PTP	Viewing PTP Status in WEB may crash PTP daemon
#20605	VRRP	Disable VRRP VMAC interface for services where it should not be used
#20603	System	Upgrade command can hang device forever in runlevel 9
#20601	System	Metric page not working on Alstom ETBN HW
#20600	System	Restore configuration fails to restore a valid configuration file
#20582	System	SSH key display issues
#20578	NTP	RTC may lock at wrong time at power down if backwards time jump has happened

Continued on next page

Continued from previous page

Issue	Category	Description
#20574	Logging	Excessive logging during configuration change
#20572	System	SFP information is missed in techsupport file and webGUI
#20571	System	Active SSH sessions not closed when a config restore is done via WEB allowing password manipulation in file afterwards
#20569	TCN	comID-131 field etbnRole loses state for not redundant setups after first request
#20548	WEB	Setting password in Encrypted Secrets in WEB doesn't work
#20533	SNMP	Wrong values in the "ttdpSubnetIPMask" OID anwers, the MIB returns 255.255.252.0 (/22), but shall display 255.255.192.0 (/18)
#20528	AAA	Downgrade of factory reset device could force the device to enter failsafe mode
#20526	Alarm	Unexpected errors and behaviors during selecting of iface as target in action via both webGUI and CLI
#20517	CLI	Erase command tab-completion is handled different depending on context
#20515	TCN	Teamd spam logfile at start of device
#20513	QoS	Rate limit limits to about half of the value set on egress for Coronet
#20509	WEB	PKI: Enrollment Servers configuration page does not have a Help webpage
#20507	QoS	Rate limit on egress does not limit on switchcore 0
#20505	AAA	Error message 'Could not delete file <cert-name>' appears when importing new pki certificate
#20483	VPN	SSL interface has "(null)" option as cipher in Web
#20481	Logging	'show logfile' does not generate an audit event
#20478	WEB	Configuring Local User DB doesn't work
#20475	VLAN	FDB entries are not correctly cleared when VLANs are removed
#20435	Flash	The Coronet platform seems to have 14MB config area (/mnt) in Barebox but 15 MB in the WeOS dts
#20416	SNMP	SNMP Read and Write community can not be same as that blocks Write function
#20414	General	FRR 8.5.1 CVE-2024-34088
#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
#20302	WEB	WEB status for TCN missing most data

Continued on next page

Continued from previous page

Issue	Category	Description
#20281	System	The error message "Failed to add audit entry to audit daemon" is spammed when applying large configs
#20274	Alarm	Entering the severity command with unknown option will crash clish
#20249	System	Defensics: Repeated connections to telnet may cause a DoS condition on telnet service
#20246	General	Route Monitor doesn't reset the admin distance to the configured value if an alarm triggered
#20245	VPN	IPsec tunnel can be established with wrong PSK in special circumstances
#20233	HW	RTC: System time might not be stored correctly
#20231	WEB	Fail with restoring config in WEB but no fault messages
#20229	Kernel	JFFS2 fails to enforce directory write permissions for unlink() and remove()
#20221	DHCP	DHCP snooping not limiting to defined VLAN and snoop up all port 67 request
#20220	WEB	Impossible to set peer as a DNS name in SSL client tunnel
#20216	WEB	Cipher cannot be set via WebGUI in the Open VPN settings
#20209	Port Access Control	MAC auth only accept the first wild-card entry in a range
#20201	System	Rebooting after disabling offloading will remove all traffic policies
#20150	System	DHCP Reply seems to be offloaded, cannot accept address
#20144	Alarm	Ping Alarm indicates UNREACHABLE when the destination is reachable
#20127	System	Metricsd can cause leak memory
#20102	SNMP	SNMP value for frntStatusVid1/2 show no data in tables
#20091	Link Aggregation	LACP Removal of lag when custom fdb filters referenced to the lag fails assertion of the running-config file
#20067	DHCP	DHCP server send out empty option 121/249 fields to clients not requesting the options if set on any static lease
#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

Continued on next page

Continued from previous page

Issue	Category	Description
#20010	General	Metrics - Cannot access the web port using IPv6 address
#19998	General	Metrics on ports not working on Dagger Lynx 5512
#19991	DHCP	Disabling Gateway setting in 'Server-setting' breaks Inherit Gateway in 'Subnet-setting'
#19977	CLI	Custom SNMP engine-id length is not enforced in CLI configuration
#19965	WEB	FRNTv2 is not shown in Status summary page when it is enabled
#19961	WEB	The user is not warned when invalid configuration file was uploaded before restoring
#19958	Boot Loader	Envoy Barebox uses precompiled ATF
#19957	General	Port statistics not available on Redfox and Lynx 5000
#19947	System	IPv6 SCP not working (copy, upgrade)
#19928	TCN	Offloading with TCN does not allow for fragmented packets to be forwarded
#19925	System	Configuration Hash does not get generated after factory reset
#19924	VRRP	VRRP instance is not restarted when doing a config restore on Vipers
#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.
#19850	PTP	Different link speeds causes higher TC error rate
#19826	System	CVE-2024-35246 - 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
#19767	General	Lacking upgrade-condition checking when doing upgrade all
#19764	WEB	The user is able to configure Stateless NAT Rules via WEB on Standard switches
#19760	WEB	CVE-2023-38579 - WebGUI Vulnerability - CROSS-SITE REQUEST FORGERY

Continued on next page

Continued from previous page

Issue	Category	Description
#19756	VRRP	The vmac of VRRP causes strange log messages and VRRP not to work properly
#19720	System	Downgrade to weos4 from weos5 using pkg results in infinite loop trying to open the files
#19711	WEB	Cannot access help in some menus in webGUI when browser tree menu has gone past the bottom of the screen
#19692	Firewall	TCP port 53 listening when DNS server functionality disabled.
#19590	System	Possible to flash sqsq bootloader to WeOS partition on Envoy systems
#19575	IP Multicast	no multicast-snooping does not disable IGMP snooping
#19524	WEB	Unable to delete VLAN by WEB when FRNT is enabled (Lynx 3000, 5000 and Redfox)
#19517	Logging	When PoE-chip goes repetitively down many Kernel logs is generated and stored
#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)
#19288	FRNT	After configuring FRNTv2 on Coronet/Viper 20A the FRNT leds are flashing red
#19262	Ports	Traffic not handled on Envoy ports using Copper SFPs
#19255	QoS	Priority-mode IP fails when both ingress and egress ports are fiber ports on Envoy platform
#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
#19024	Link Aggregation	Using link-aggregates as FRNT ring ports gives long failover times in ring topology changes
#18967	System	Joins on SSL ports does not lead to the CPU port being added to the ATU
#18936	SNMP	SNMP 'GETBULK' Reflection DDoS
#18886	IP Multicast	Static multicast route with wildcard source fails to forward when group first heard on other interface
#18808	Alarm	Link-alarm with multiple ports makes status-relay indicate OK when some port is up and others down
#18683	MRP	Timer interval for sending MRP control packets is too slow

Continued on next page

Continued from previous page

Issue	Category	Description
#18675	Link Aggregation	Long failover time (aggregate member link up/down) in link-aggregate interoperability case (WeOS5 'Dagger' vs WeOS4)
#18643	PTP	RedFox 5528/5728 fiber ports (Eth1-4) have more jitter in the correction field accuracy than the other fiber ports
#18638	CLI	CLI does not allow "?" when configuring local user accounts password using clear-text
#18614	TCN	TTDP NAT rules incorrectly modifies packets between local CNs
#18362	TCN	Broken/missing ECSPs in train composition handled incorrectly
#18289	MRP	On MRC link-up with profile 30 ms MRM responds too slow resulting in short transient storm
#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
#17640	Ports	Combo port with preferred port TP (copper) cannot be used as FRNT port

4.2 #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.

`redfox-4d-3b-20:/#>` **upgrade primary <SERVER-ADDRESS> WeOS-5.26.1.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.

6.2 Boot Loader

The boot loader firmware has its own version numbering scheme and is CPU platform specific. Please note, unless the release notes explicitly recommends it, there is usually no need to upgrade the boot loader.

The boot loader firmware is included in the WeOS-5.26.1.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-5.26.1.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/