

Document Release Notes WeOS 5.23.0	
Date December 11, 2024	Document No 224004-g7bb880bc49

WeOS 5.23.0 Release Notes

Contents

1	Summary of Changes	5
1.1	News in 5.23.0	5
1.1.1	IPv6 Static Unicast Routing	5
1.1.2	Web GUI - Static Unicast Route Configuration	5
1.1.3	SSL tunnels	5
1.1.4	Policy Traffic Filtering	6
1.1.5	Redfox & Lynx-5000 - Offloading Unicast Routing	6
1.1.6	Encryption of Secrets in Configuration files	6
1.1.7	DNS - Reject AAAA requests	7
1.1.8	IEC-61375 - Web Configuration and Status	7
1.1.9	Flood Unknown Multicast to CPU	7
1.1.10	Ring Chaining Concept	8
1.1.11	Date and Time - Daylight Saving Time control	8
1.1.12	Alarm - External Media Events	8
1.1.13	Metrics	8
2	Fixed Issues	9
2.1	WeOS 5.23.0	9
3	Known Limitations	10
3.1	Ring Coupling version 2 not supported	10
3.2	Port Access Control	10
3.3	Firewall	10
3.4	Login	10
3.5	Setting Date Manually	11
3.6	Available ports for boot specific functionality	11
3.7	Routing Hardware Offloading	11
3.8	FRNT	11
3.9	RSTP	12
3.10	IEC 61375	12

Document Release Notes WeOS 5.23.0	
Date December 11, 2024	Document No 224004-g7bb880bc49

3.11	LLDP	13
3.12	Port Monitoring	13
3.12.1	Cross switch core limitation	13
3.13	Media Redundancy Protocol (MRP)	13
3.14	10G SFP Ports	14
3.15	Search function in User Guide	14
4	Known Issues	15
4.1	List of known issues	15
4.2	#18163: Work-around for OSPF NSSAs convergence issue	18
5	Quick Start Guide	19
5.1	Default User and Password	19
5.2	General	19
5.3	CLI	20
6	Firmware Upgrade	22
6.1	WeOS Image	22
6.2	Boot Loader	22
7	Significant differences between WeOS 4 and WeOS 5	23



Document Release Notes WeOS 5.23.0	
Date December 11, 2024	Document No 224004-g7bb880bc49

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 5.23.0	
Date December 11, 2024	Document No 224004-g7bb880bc49

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-5.23.0/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 5.23.0	
Date December 11, 2024	Document No 224004-g7bb880bc49

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 highlights some of the major differences between WeOS 4 and WeOS 5.

1.1 News in 5.23.0

The subsections below describe news in WeOS 5.23.0. In addition, section 2.1 includes information on fixed issues.

1.1.1 IPv6 Static Unicast Routing

Support has been added for basic IPv6 static unicast routing. This allows for the creation of up to 256 individual static routes.

Note: By default, IPv6 is disabled on the device and must be enabled under the IPv6 configuration context. Furthermore, unicast forwarding (routing) must also be enabled in the same context to allow the device to forward IPv6 traffic.

1.1.2 Web GUI - Static Unicast Route Configuration

The static unicast route configuration page in the web GUI has been entirely reworked. Mainly to improve the general user experience and to add support for IPv6 static unicast routes, in addition to the existing IPv4 static unicast routes.

1.1.3 SSL tunnels

The server option "listen" has been removed and replaced by two new configuration options: "bind-dev" and "local-address". "listen" will be translated to the more conservative "bind-dev" when reading an old configuration.

The "crypto" option is removed for setups using certificate authentication method. Two new options have been added: "data-ciphers" and "data-ciphers-fallback", available for certificate setups. When loading an existing config "crypto" is automatically translated to "data-ciphers-fallback" for certificate setups.

The option "tls-version-min" has been added. Defaulting to 1.2 if not set explicitly.

The default setting for compression for new tunnels has been changed from "adaptive" to "off".

The authentication method "secret" is considered deprecated and will be removed in upcoming releases. The default authentication method for new tunnels has been changed from "secret" to "cert".

Document Release Notes WeOS 5.23.0	
Date December 11, 2024	Document No 224004-g7bb880bc49

For more information see the WeOS User Guide section *Configuration Guides → Tunnels & VPN → OpenVPN Tunnels*.

1.1.4 Policy Traffic Filtering

With this release Policy Traffic Filtering has been introduced. Policy Traffic Filtering enables filtering of traffic to be offloaded to hardware and has the ability to match across multiple layers of the packet.

As of this release, this function is only supported for the Redfox 5000/7000 and Lynx 5000 series.

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

1.1.5 Redfox & Lynx-5000 - Offloading Unicast Routing

With this release WeOS introduces Hardware offloading for Unicast routing on the Redfox 7000/5000 and Lynx-5000 series. This allows Unicast Routes to be handled directly in the devices switch core, providing line-speed level routing performance for the offloaded routes.

The offloading setting is in this release limited in scope and therefore not enabled by Default.

The Known limitations for offloading in this release are:

- 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

For more information see the WeOS User Guide section *Configuration Guides → Routing → Offloading*.

1.1.6 Encryption of Secrets in Configuration files

As of this release it is now possible to encrypt the secrets in the WeOS configuration file to provide some protection from unwanted information disclosure.

Encrypted Secrets is available in three possible iterations.

Document Release Notes WeOS 5.23.0	
Date December 11, 2024	Document No 224004-g7bb880bc49

- Portable - Providing a WeOS firmware shared encryption key allowing for full mobility of the configuration file between WeOS 5 devices.
- HWUID - Device-Specific encryption key, any configuration that is used with this key type will not be portable between devices.
- Password - Password-derived encryption key, allowing for restricted portability where the users needs to provide the correct passwords for configuration secrets to be decrypted correctly.

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

1.1.7 DNS - Reject AAAA requests

With this release it is now possible to configure the DNS Proxy Server to always reject AAAA lookups requested by DNS clients.

For more information see the WeOS User Guide section *Configuration Guides* → *Network Services* → *DNS Proxy Server*.

1.1.8 IEC-61375 - Web Configuration and Status

It is now possible to Configure and View the status and settings of IEC-61375 in WeOS.

1.1.9 Flood Unknown Multicast to CPU

It is now possible to control how flooding of unknown Multicast towards the CPU is handled in select WeOS platforms. This configuration control exists to provide users with some more granular control of how the CPU is affected by large amounts of Unknown Multicast Traffic in a network.

This setting can be set to three different states:

- Don't flood - This will not flood Unknown Multicast traffic to the CPU. This will break some use cases by design and should only be used as a testing setting or in very distinct use cases.
- Always Flood - This is the current default option in WeOS and will have all Unknown Multicast Traffic flood to the CPU.
- Auto - This setting will contextually enable and disable flooding of Unknown Multicast traffic towards the CPU as certain settings are Enabled in the Device. This will in future releases become the preferred Default setting.

For more information see the WeOS User Guide section *Configuration Guides* → *Bridging/Switching* → *Bridge*.

Document Release Notes WeOS 5.23.0	
Date December 11, 2024	Document No 224004-g7bb880bc49

1.1.10 Ring Chaining Concept

In the release it is now possible to configure a device to perform a topology inauguration over a Dynamic Ring Ladder analogous to the topology inauguration within IEC-61375. Ring Chaining (RICH) does not as of this release provide any inherent routing or NAT integrations. The main usage is to provide a structured list of rings that are included in the Ring Ladder topology to the user or a system through SNMP.

For more information see the WeOS User Guide section *Configuration Guides → Bridging/Switching → RICH*.

1.1.11 Date and Time - Daylight Saving Time control

In the release it is now possible to configure a device to within its time zone either regard or disregard daylight savings time. This is a mechanism to help in cases where local governments doesn't provide sufficient headway on changes as it relates to time zone legislation.

For more information see the WeOS User Guide section *Configuration Guides → Network Services → NTP*.

1.1.12 Alarm - External Media Events

In the release it is now possible to configure a device to trigger Alarm's for External Media triggers. The new triggers monitors the Media availability and remaining capacity.

For more information see the WeOS User Guide section *Configuration Guides → Alarm, LEDs and Logging → Alarm*.

1.1.13 Metrics

In the release it is now possible to configure a device to monitor some of the used device resources and report them through SNMP OIDs and through a new monitoring interface Called Metrics.

The available resources that can be tracked are

- Memory usage
- CPU Usage
- Port Usage

These Metrics can be configured to provide the information in a structured way through HTTP(s).

For more information see the WeOS User Guide section *Configuration Guides → Management Interfaces → Metrics*.

Document Release Notes WeOS 5.23.0	
Date December 11, 2024	Document No 224004-g7bb880bc49

2 Fixed Issues

2.1 WeOS 5.23.0

Fixed issues in WeOS 5.23.0 (as relative to 5.22).

Issue	Category	Description
#20064	SNMP	SNMP inform resends blocks all other SNMP requests until finished with the resends
#20020	General	On interface IP change, TTDP will source NAT replies from the interface to the 10.128.x.x IP range
#19982	Logging	Facility filter that uses cron_sol silently fails to apply
#19966	Ring Coupling	Coupling ports remains in blocking on isolated nodes
#19945	WEB	Forced mode is missing for flow control
#19944	WEB	Jumboframes for Lynx 3000 not exposed on web
#19943	CLI	Interacting with certificates in CLI/WEB is very slow
#19938	VPN	SSL tunnels "listen" doesn't have any effect
#19937	WEB	UI unresponsive if browser window is closed during upgrade
#19907	Logging	Syslog-ng leaks memory on configuration reload (SIGHUP)
#19901	WEB	Bold text not displayed correctly on some pages
#19875	System	OpenVPN clients configuration partly lost at reboot of device
#19607	General	Configuring ports for dir1, dir2 in TTDP doesn't work as described in help

Document Release Notes WeOS 5.23.0	
Date December 11, 2024	Document No 224004-g7bb880bc49

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 Firewall

When using VRRP and firewall it is required to disable vmac on the VRRP instance to allow for the firewall rules to match according to in IFACE vlan.

It is still possible to use IP-Address matching on traffic. This current limitation is restricted to rules matching on incoming interfaces.

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.

Document Release Notes WeOS 5.23.0	
Date December 11, 2024	Document No 224004-g7bb880bc49

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').

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 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.

Document Release Notes WeOS 5.23.0	
Date December 11, 2024	Document No 224004-g7bb880bc49

3.9 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.

3.10 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.

Document Release Notes WeOS 5.23.0	
Date December 11, 2024	Document No 224004-g7bb880bc49

3.11 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.

3.12 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.

3.12.1 Cross switch core limitation

It is not possible to use port-monitor where the source and destination ports are split 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.

3.13 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.

Document Release Notes WeOS 5.23.0	
Date December 11, 2024	Document No 224004-g7bb880bc49

3.14 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).

3.15 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.

Document Release Notes WeOS 5.23.0	
Date December 11, 2024	Document No 224004-g7bb880bc49

4 Known Issues

4.1 List of known issues

Issue	Category	Description
#20058	System	RMON counters not working correctly
#20052	WEB	redirect_url users (e.g. Config/System/Date&Time -> Set time and Tools/Ping) are broken
#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, the ON LED will remain RED after boot
#20042	Kernel	TC get an exception when deleting the TC rules in IGMP context
#19998	General	Metrics for Ports not working on Lynx 5000
#19995	SNMP	Mismatch Between CLI and SNMP Output for RMON Data
#19993	WEB	Upgrade does not reload Web when finished
#19991	DHCP	Disabling Gateway setting in 'Server-setting' breaks Inherit Gateway in 'Subnet-setting'
#19987	System	The unit fails to run a valid MAC-auth configuration and instead run fallback configuration
#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
#19964	LED	The LED indicators for FRNT and RSTP on both Lynx and Redfox do not turn off when the protocol is disabled
#19949	AAA	User uids are not persistent
#19948	AAA	All Administrator users are created with uid 0
#19947	System	IPv6 SCP not working (copy, upgrade)
#19946	System	Upgrade not working using SCP, device also gets soft-locked
#19940	WEB	Broken JavaScript on "Edit IPsec Tunnel X" page
#19932	WEB	IPsec DPD Delay in web input validation error
#19928	TCN	Offloading with TCN does not allow for fragmented packets to be forwarded
#19926	System	Configuration Hash does not update from cfg://URI copy to startup-config
#19924	VRRP	VRRP instance is not restarted when doing a config restore
#19909	VPN	Disabling compression does not actually disable compression
#19903	System	Configuration restore do not clear previous added route from system

Continued on next page

Document Release Notes WeOS 5.23.0	
Date December 11, 2024	Document No 224004-g7bb880bc49

Continued from previous page		
Issue	Category	Description
#19902	VPN	IPSec issues with LAN traffic when NAT rule is applied
#19895	Firewall	FTP Alg helpers isn't working when performing FTP file transfers
#19891	Firewall	When leaving the firewall context strange output is generated
#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
#19873	WEB	Using HTTPS uses way more CPU than HTTP
#19870	IGMP/MLD	Multicast Snooping Boundary for MLD does not work on Lynx-5000 and Redfox-5000/7000
#19861	VPN	SSL "tun" interface does not work with certificates towards another WeOS device
#19856	AAA	MAC Auth reauthentication towards remote-server is delayed after boot
#19850	IEEE1588/PTP	Different link speeds causes higher TC error rate
#19847	System	The unit does not apply configuration after it has been "forcefully" uploaded
#19843	System	Profinet do not respect selected interface and uses the lowed iface ID
#19818	SNMP	Syntax errors in Westermo MIB files for FRNT and EVENT
#19783	System	Coronet: Out-of-order problem on Viper-20 remains
#19777	WEB	Upgrading primary image from web gui does not report flashing done in http response
#19721	TCN	Setting port Admin state as "No Enable" not respected on TTDP LAG ports
#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
#19524	WEB	Unable to delete VLAN by WEB when FRNT is enabled (Envoy & Dagger)
#19498	IGMP	Duplicate multicast packets over link-aggregates when changing router timeout (Dagger)
#19410	IGMP	Mismatch between MDB and ATU for mc group 239.193.0.1 when etbn is acting as router, sender and consumer of data
Continued on next page		

Document Release Notes WeOS 5.23.0	
Date December 11, 2024	Document No 224004-g7bb880bc49

Continued from previous page		
Issue	Category	Description
#19367	Ports	SFP:s 1100-0554 and 1100-0555 does not work on 5512 and 5528
#19326	Ports	Adminstatus does not affect operstatus of port if the port is it's own interface (i.e. outside a vlan)
#19323	FRNT	FRNT Focal point Topology Counter rush with LACP links (Dagger)
#19288	FRNT	After configuring FRNT2 on 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
#19231	TCN	2-3 inauguration may never reach operational traindir shared
#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
#18910	TCN	TTDP Topology timeout not adapted for Gigabit ETB, causing ETB inaugurations upon ETBN down event
#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
#18675	Link Aggregation	Long failover time (aggregate member link up/down) in link-aggregate interoperability case (WeOS5 'Dagger' vs WeOS4)
#18643	IEEE1588/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
#18593	QoS	Tagged ports with 'priority-mode ip' is broken
#18377	Logging	Syslog events may be missed during syslogd restart
#18362	TCN	Broken/missing ECSPs in train composition handled incorrectly
#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
Continued on next page		

Document Release Notes WeOS 5.23.0	
Date December 11, 2024	Document No 224004-g7bb880bc49

Continued from previous page		
Issue	Category	Description
#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 #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.

Document Release Notes WeOS 5.23.0	
Date December 11, 2024	Document No 224004-g7bb880bc49

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.

Document Release Notes WeOS 5.23.0	
Date December 11, 2024	Document No 224004-g7bb880bc49

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.

Document Release Notes WeOS 5.23.0	
Date December 11, 2024	Document No 224004-g7bb880bc49

```
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.

Document Release Notes WeOS 5.23.0	
Date December 11, 2024	Document No 224004-g7bb880bc49

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-5.23.0.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-5.23.0.pkg.

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

```
redfox-4d-3b-20: /#> upgrade boot <SERVER-ADDRESS> WeOS-5.23.0.pkg
```

Document Release Notes WeOS 5.23.0	
Date December 11, 2024	Document No 224004-g7bb880bc49

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` syntax¹. For more information, see the CLI online help text for `help running-config`

¹For more information on `jq`, a JSON query tool, see <https://stedolan.github.io/jq/>

This page intentionally left blank.