

Document Release Notes WeOS 5.22.0	
Date October 8, 2024	Document No 224004-g8a1ef74ec6

## WeOS 5.22.0 Release Notes

### Contents

1	Summary of Changes . . . . .	5
1.1	News in 5.22.0 . . . . .	5
1.1.1	Viper-3000 - Secure boot . . . . .	5
1.1.1.1	Signed Branding Packages . . . . .	5
1.1.2	IEC-61375 - Number of supported CNs . . . . .	6
1.1.3	IEC-61375 - Inauguration routing change . . . . .	6
1.1.4	Jumbo-Frame Switching . . . . .	6
1.1.5	SNMP - Improvements . . . . .	6
1.1.5.1	Inform Request . . . . .	6
1.1.5.2	SNMP ifIndex Persistence . . . . .	6
1.1.6	Flow control . . . . .	7
1.1.7	Major Overhaul of the Logging System . . . . .	7
1.1.8	Priority Mode prefer[ipitag] . . . . .	9
1.1.9	OSPF - Tuning Options . . . . .	10
1.1.10	Multicast Snooping Boundary . . . . .	10
1.1.11	IGMP/MLD Webgui Configuration Page . . . . .	11
2	Fixed Issues . . . . .	12
2.1	WeOS 5.22.0 . . . . .	12
2.1.1	Fixed CVEs . . . . .	12
2.2	WeOS 5.20.1 . . . . .	14
3	Known Limitations . . . . .	15
3.1	Ring Coupling version 2 not supported . . . . .	15
3.2	Port Access Control . . . . .	15
3.3	Firewall . . . . .	15
3.4	Login . . . . .	15
3.5	Setting Date Manually . . . . .	16
3.6	Available ports for boot specific functionality . . . . .	16
3.7	Routing Hardware Offloading . . . . .	16

Document Release Notes WeOS 5.22.0	
Date October 8, 2024	Document No 224004-g8a1ef74ec6

3.8	FRNT	16
3.9	RSTP	17
3.10	IEC 61375	17
3.11	LLDP	18
3.12	Port Monitoring	18
3.12.1	Cross switch core limitation	18
3.13	Media Redundancy Protocol (MRP)	18
3.14	10G SFP Ports	19
3.15	Search function in User Guide	19
4	Known Issues	20
4.1	List of known issues	20
4.2	#18163: Work-around for OSPF NSSAs convergence issue	22
5	Quick Start Guide	23
5.1	Default User and Password	23
5.2	General	23
5.3	CLI	24
6	Firmware Upgrade	26
6.1	WeOS Image	26
6.2	Boot Loader	26
7	Significant differences between WeOS 4 and WeOS 5	27



Document Release Notes WeOS 5.22.0	
Date October 8, 2024	Document No 224004-g8a1ef74ec6

## 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 5.22.0	
Date October 8, 2024	Document No 224004-g8a1ef74ec6

## 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-5.22.0/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 5.22.0	
Date October 8, 2024	Document No 224004-g8a1ef74ec6

## 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 5.22.0

The subsections below describe news in WeOS 5.22.0. In addition, section 2.1 includes information on fixed issues.

#### 1.1.1 Viper-3000 - Secure boot

In this release support has been added for Secure boot of the Viper-3000 series products. This means that the hardware will refuse to start any software that is not signed with correct cryptographic keys. With this the device guarantees that the software that is being started has a trusted origin.

With this introduction some changes has been done to the upgrade process.

- As of 5.22.0 it is only officially supported to perform firmware upgrades using files with .pkg format
- The image-format for all WeOS platforms are now Flattened Image Tree
- To upgrade to 5.22.0 it is required to run  $\geq$ WeOS 5.21.1 with upgrade all
- To downgrade to  $<$ 5.22.0 the only supported target version is 5.21.1 using upgrade all

WeOS can now check within a incoming .pkg file if the current running software versions will function well with the incoming firmware. This has been added to protect the user in cases where specific bootloaders or WeOS versions have been discovered to cause problems in the upgrade process after the firmware was released.

Using the 'force' command for upgrade is strongly discouraged as this allows the upgrade process to skip essential validation checks before flashing the image.

**1.1.1.1 Signed Branding Packages** As of this release it is no longer possible to use unsigned branding packages. All installed packages on device will be rejected unless signed with validation keys. This is done to not break the Secure boot chain of trust concept where WeOS will check the signatures of the packages that can change the devices default behaviour.

Document Release Notes WeOS 5.22.0	
Date October 8, 2024	Document No 224004-g8a1ef74ec6

## 1.1.2 IEC-61375 - Number of supported CNs

In this release the number of supported CNs for a Consist has been limited to three. This change has been made to better align with the functional behaviour when using Offloading. In previous releases Offloading of routing has been unstable and unpredictable in cases where more than one CN was used.

In the release a few configuration options has been removed as they are now by default enabled when using TTDP and Offloading.

The following settings have thus been removed from TTDP configuration, and are implicitly enabled.

- optimize-vrrp-failover
- blackhole-mroute-iface

In previous versions the 'optimize-vrrp-failover' setting was limited to 1 CN.

## 1.1.3 IEC-61375 - Inauguration routing change

To comply with IEC61375 conformance requirements, an ETBN will no longer route to or from the ETB when it is not in the TTDP inaugurated state (as described in IEC61375-2-5:2014 section 8.5.1)

See section 2.1 where issues #19489 and #19450 has been resolved.

## 1.1.4 Jumbo-Frame Switching

On Lynx-3000 series it is now possible to enable switching of jumbo frames up to MTU 9000. Routed MTU size is still limited to 1500 Bytes.

For more information, see the WeOS User Guide section *Configuration Guides* → *Jumbo-Frame Switching*.

## 1.1.5 SNMP - Improvements

Now it's possible to use SNMP version 3 authentication and encryption handling with traps. The number of trap hosts are also increased from three to eight.

Thee supported Auth and Crypto types that can be configured for SNMPv3 has been extended.

**1.1.5.1 Inform Request** In this release it is now also possible to make use of Inform-request as the notification type for SNMP events.

**1.1.5.2 SNMP ifIndex Persistence** Selecting this configuration option allows ifIndex to be persistent and predictable. Doing so can be useful when logic to resolve the ifIndex can not be performed in a NMS.

Document Release Notes WeOS 5.22.0	
Date October 8, 2024	Document No 224004-g8a1ef74ec6

- Vlan interfaces will have the same ifindex as VID e.g. vlan1 = 1
- Port interfaces will be the same id according to port name + 4095, e.g eth1 = 4096
- SSL interfaces will have offset 4300, e.g. ssl4 = 4304
- Other interfaces will have dynamically allocated "ifIndex" + 5000

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

## 1.1.6 Flow control

For Lynx-3000 series devices it is possible to enable Flow Control according to 802.3x. In cases where Ethernet uplinks can become saturated it can be better to instruct downstream devices to back-off from sending traffic towards the switch instead of dropping traffic as the switch buffer runs out of space.

For more information see the WeOS User Guide section *Configuration Guides* → *Ethernet/LAN Ports* → *Flow Control*.

## 1.1.7 Major Overhaul of the Logging System

The underlying logging application has been exchanged for a new one. This has been done to improve how logging is handled in the system. Furthermore, it has been done in order to facilitate improvements that have been done to the customizable logging sinks in the system. However, the general changes to the logging system should not significantly impact the user experience. The intention is that all the default logging should still work as before.

The logging sinks allow the user to configure special logging destinations for specific log messages. This can be used to send log messages to a remote syslog server, or to a file located on the internal RAM Disk or an external media device such as a USB stick or SD card.

With this release the old sink configuration has been completely overhauled. This was done partly to make it easier to understand and use, but also to make it more flexible and powerful by providing a wider range of configuration options.

Now, instead of just configuring the sink itself, the user can specify the source(s) of the log messages, the intended destination(s) and optional filter(s). These three components can then be freely combined and linked together to form the sink(s). All of these components can be used multiple times in the configuration, allowing for a very flexible and powerful logging system.

These new individual sink components also come with a host of new features and options that were not available in the old system. The following is a short summary of what is now possible to configure for each of the components:

Document Release Notes WeOS 5.22.0	
Date October 8, 2024	Document No 224004-g8a1ef74ec6

- Sources - Create up to 32 different sources. The source type can be either locally originated log messages, or messages received from a remote syslog server.
  - For remote sources:
    - \* Specify a specific interface on the device to listen on.
    - \* Specify the transport protocol of the incoming messages (UDP, TCP or TLS).
    - \* Specify the IP protocol version to use (IPv4 or IPv6).
    - \* Specify the port number to listen on.
  - Destinations - Create up to 32 different destinations. The destination type can be either a file on the internal RAM Disk, or an external media device (USB stick or SD card), or a remote syslog server.
    - For file destinations:
      - \* Specify the file media.
      - \* Specify the file name and path.
      - \* Specify a file rotation policy, including how many files to keep, how large each file is allowed to be, and how many compressed files to keep.
    - For remote destinations:
      - \* Specify the transport protocol to use (UDP, TCP or TLS).
      - \* Specify the IP protocol version to use (IPv4 or IPv6).
      - \* Specify the port number to send to.
      - \* Specify the location of the remote syslog server:
        - Using an IP address.
        - Using a hostname or a FQDN (Fully Qualified Domain Name).
        - Use a DHCP enabled interface. The destination will then be automatically updated if the provided interface receives a DHCP lease that includes DHCP option 7 (Log Server). The option 7 value will specify the IP address of the remote syslog server.
      - \* Optionally specify throttling of messages sent to the remote syslog server. This can be used to limit the number of messages sent to the server per second, to avoid overloading the server.
  - Filters - Create up to 32 different filters. A number of different filter types are available. These can be used to filter out log messages based on different criteria:



Document Release Notes WeOS 5.22.0	
Date October 8, 2024	Document No 224004-g8a1ef74ec6

- Filter on the facility of the log messages.
  - Filter on the severity of the log messages.
  - Filter on the hostname of the device that generated the log messages.
  - Filter on the content of the log messages.
  - Filter on the program/application name that generated the log messages.
  - Filter on the subnet of the source IP address of the log messages.
  - Set a rate limit on the number of log messages that are allowed to pass through the filter per second. Any messages that exceed the configured rate will be instantly dropped.
- Sinks - Create up to 32 different sinks. A sink is a combination of one or more sources, one or more destinations, and optionally, one or more filters.

For more detailed information on the new logging system, see the WeOS User Guide section *Configuration Guides* → *Alarm, LEDs and Logging* → *Logging*. This documentation also includes a number of examples providing guidance on how to configure the new logging system.

**Note:** We have attempted to make the new logging sink configuration as backwards compatible as possible with the old system. However, due to the extensive changes made to the system, it is not possible to guarantee that all old configurations will work as before.

Therefore, we recommend reviewing and updating any existing logging sink configurations after upgrading to this release.

The new logging configuration will *NOT* be compatible if you downgrade to any version of WeOS older than WeOS 5.22.0.

### 1.1.8 Priority Mode prefer[ip|tag]

The new priority mode 'prefer[ip|tag] allows the following:

For 'prefer tag', use VLAN tag (PCP) priority for an incoming VLAN tagged IP packet. For untagged IP packet, use DSCP priority. For VLAN tagged non-IP packet, use VLAN tag priority.

For 'prefer ip', use IP (DSCP) priority for an incoming VLAN tagged IP packet or an untagged IP packet. For VLAN tagged non-IP packets, use VLAN tag priority.

For this release, priority mode prefer option is limited to the Viper-3000 and, Lynx-3000 series.

For more detailed information on this setting, see the WeOS User Guide section *Configuration Guides* → *Ethernet/LAN Ports* → *Ethernet Ports*.

Document Release Notes WeOS 5.22.0	
Date October 8, 2024	Document No 224004-g8a1ef74ec6

## 1.1.9 OSPF - Tuning Options

In this release support is added to granularly control OSPF protocol timers and thresholds. These are advanced protocol configuration options that can be used to tune the performance of the OSPF protocol to suit the system requirements.

If these settings are not used with careful consideration and testing for the specific system, changing these parameters could have adverse effects of the performance and stability of the routing protocol.

These configuration options has been added

- lsa-min-arrival
- lsa-min-interval
- spf-delay
- spf-min-hold-time
- spf-max-hold-time
- interface retransmit-interval
- interface transmit-delay

For more detailed information on this setting, see the WeOS User Guide section *Configuration Guides* → *IP* → *OSPF*.

## 1.1.10 Multicast Snooping Boundary

Support is being introduced for a configuration option referred to as Multicast Snooping Boundary. This boundary is configured on a per-port basis and limits where IGMP/MLD control traffic is allowed to traverse, both for ingress and egress. The types of control traffic encompassed by this feature include IGMP and MLD queries, reports, and leaves.

This feature allows for the creation of multiple IGMP/MLD domains within a single Layer 2 network. This can be useful in scenarios where multiple multicast domains are required or beneficial, but the network is not segmented into separate VLANs. An example of this could be when constructing multiple FRNT rings and connecting them with RiCo, where each ring should also be a separate multicast domain. In this case, the RiCo ports connecting the rings could be configured with a Multicast Snooping Boundary to prevent IGMP/MLD control traffic from one ring from traversing to the other.

This feature could also just be used on individual ports connecting to parts of the network where we do not want any IGMP/MLD control traffic to traverse.

As of this release the function does not work for MLD on Redfox 5000/7000 or Lynx 5000 series.

Document Release Notes WeOS 5.22.0	
Date October 8, 2024	Document No 224004-g8a1ef74ec6

For more detailed information on this setting, see the WeOS User Guide section *Configuration Guides* → *Bridging/Switching* → *IGMP/MLD Snooping*.

### **1.1.11 IGMP/MLD Webgui Configuration Page**

The IGMP/MLD configuration page in the webgui has received a major overhaul.

Document Release Notes WeOS 5.22.0	
Date October 8, 2024	Document No 224004-g8a1ef74ec6

## 2 Fixed Issues

### 2.1 WeOS 5.22.0

Fixed issues in WeOS 5.22.0 (as relative to 5.21.1).

Issue	Category	Description
#19838	Ports	Some SFP-links do not always come up on RedFox 5000/7000 series and Lynx-5000 series
#19837	VLAN	VLAN Assignment in Web Interface changes for all ports
#19817	VPN	OpenVPN Servers will not start when using tap and tun on same device
#19816	WEB	Port Access control Authentication server drop down is empty
#19811	IEEE1588/PTP	Lynx-RB sometimes gets stuck failing to timestamp/synchronize
#19801	WEB	Unable to remove igmp router ports in the web interface
#19792	IP Multicast	Multicast routing not possible over GRE as interface
#19787	IP Multicast	IGMP not correctly enabled by PIM if interface name has been changed in configuration
#19762	PoE	Kernel log spammed with PoE messages
#19755	VRRP	MDNSD crash causes VRRP to fail
#19723	WEB	Not possible to create or edit SNMPv3 RWuser from web
#19712	Link Aggregation	Long aggregate names are truncated and can create duplicates
#19678	System	Iface MTU (Auto) does not change the MTU from previous configured values in runtime
#19655	SNMP	TimeStamp in ifLastChange is inconsistent with TimeStamp for SNMPTrap triggered by Link-Alarm for LinkDown event
#19641	General	Removed users can remain logged in in WEB
#19529	WEB	Cannot apply Boot Configuration with firefox and saved password.
#19490	TCN	ETBN should only forward train-wide MULTICAST packets when ETBN is inaugurated
#19489	TCN	ETBN should only forward train-wide UNICAST packets when ETBN is inaugurated
#19387	System	Using CLI config + abort causes "config change"
#19385	System	Static Unicast MAC entries can not be added to the FDB
#18768	SNMP	ipRouteTable is updated very slowly

#### 2.1.1 Fixed CVEs

- CVE-2022-40320
- CVE-2021-36369

Document Release Notes WeOS 5.22.0	
Date October 8, 2024	Document No 224004-g8a1ef74ec6

- CVE-2023-31124
- CVE-2023-31147
- CVE-2023-28450
- CVE-2021-3672
- CVE-2023-32067

Document Release Notes WeOS 5.22.0	
Date October 8, 2024	Document No 224004-g8a1ef74ec6

## 2.2 WeOS 5.20.1

Fixed issues in WeOS 5.20.1 (as relative to 5.20.0).

Issue	Category	Description
#19097	TCN	ETBN redundancy switchover blocks local ECN to backbone multi-cast communication 1.5s in failed consist
#19096	TCN	ETBN redundancy switchover blocks local ECN to backbone unicast communication 1.5s in failed consist

Document Release Notes WeOS 5.22.0	
Date October 8, 2024	Document No 224004-g8a1ef74ec6

## 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 5.22.0	
Date October 8, 2024	Document No 224004-g8a1ef74ec6

### 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 5.22.0	
Date October 8, 2024	Document No 224004-g8a1ef74ec6

## 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 5.22.0	
Date October 8, 2024	Document No 224004-g8a1ef74ec6

## 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 5.22.0	
Date October 8, 2024	Document No 224004-g8a1ef74ec6

### 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 5.22.0	
Date October 8, 2024	Document No 224004-g8a1ef74ec6

## 4 Known Issues

### 4.1 List of known issues

Issue	Category	Description
#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
#19654	TCN	ETBND vrrp interface with vmac does not work for ecsp communication if configuration is done in specific order
#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
#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)
Continued on next page		

Document Release Notes WeOS 5.22.0	
Date October 8, 2024	Document No 224004-g8a1ef74ec6

Continued from previous page		
Issue	Category	Description
#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
#18076	MRP	Probing MRP status (30 ms profile) during heavy load may cause reboot (Viper-TBN)
Continued on next page		

Document Release Notes WeOS 5.22.0	
Date October 8, 2024	Document No 224004-g8a1ef74ec6

Continued from previous page		
Issue	Category	Description
#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 5.22.0	
Date October 8, 2024	Document No 224004-g8a1ef74ec6

## 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 5.22.0	
Date October 8, 2024	Document No 224004-g8a1ef74ec6

## 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 5.22.0	
Date October 8, 2024	Document No 224004-g8a1ef74ec6

```
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 5.22.0	
Date October 8, 2024	Document No 224004-g8a1ef74ec6

## 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-5.22.0.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-5.22.0.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-5.22.0.pkg
```

Document Release Notes WeOS 5.22.0	
Date October 8, 2024	Document No 224004-g8a1ef74ec6

## 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<sup>1</sup>. For more information, see the CLI online help text for `help running-config`

---

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

This page intentionally left blank.