Prepared by	Document	
Jon-Olov Vatn	Release Notes WeOS 5.12.1	
Approved by	Date	Document No
Jonas Nylander	September 22, 2021	224004-ge77b51c

WeOS 5.12.1
Release Notes

Contents

Prepared by	Document	
Jon-Olov Vatn	Release Notes WeOS 5.12.1	
Approved by	Date	Document No
Jonas Nylander	September 22, 2021	224004-ge77b51c

Legal Information

Prepared by	Document	
Jon-Olov Vatn	Release Notes WeOS 5.12.1	
Approved by	Date	Document No
Jonas Nylander	September 22, 2021	224004-ge77b51c

Important User Information

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

- WeOS 5.12 has been interoperability tested with WeOS 4.30. For mixed WeOS 5 and WeOS 4 networks using the latest of these two feature releases are the recommended WeOS versions (currently WeOS 5.12.1 and WeOS 4.30.1).
- When using WeConfig to manage WeOS 5.12, WeConfig 1.13.1, or later is recommended.

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: `user-guide/`. To access the documentation, open the following file in your web browser:

`file://Downloads/WeOS-5.12.1/user-guide/index.html`

The `user-guide/` directory can also be placed on an intranet web server for easy access from within an organization. The directory is fully relocatable and does not need to be placed in the root folder of the web server.

Prepared by	Document	
Jon-Olov Vatn	Release Notes WeOS 5.12.1	
Approved by	Date	Document No
Jonas Nylander	September 22, 2021	224004-ge77b51c

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 5.12.0

WeOS 5.12.0 contains new features and bug fixes. The new features are described in the sections below, while fixed issues are listed in section 2.

1.1.1 Firewall Hit Counters

WeOS 5.12.0 adds the ability to create *named* firewall hit counters and bind them to one or more individual firewall rules.

Example of traffic counter for the web interface

```
example:/config/ip/firewall/#> counter web
example:/config/ip/firewall/#> input accept dport 80 proto tcp bind-counter web
example:/config/ip/firewall/#> input accept dport 443 proto tcp bind-counter web
example:/config/ip/firewall/#> leave
Applying configuration.
Configuration activated.  Remember "copy run start" to save to flash (NVRAM).
example:/#> show ip firewall counter web

Users
001 input accept dport 80 proto tcp bind-counter web
002 input accept dport 443 proto tcp bind-counter web

Value
packets 75 bytes 4500
example:/#>
```

For more information, see the WeOS User Guide, section on 'Firewall' within 'Configuration Guides'/'IP'.

1.1.2 Extended IF-MIB Support (High-Capacity Counters)

Support for the following high-capacity counters of the IF-MIB ifXTable is now included:

- ifHCInUcastPkts
- ifHCInMulticastPkts

- ifHCInBroadcastPkts
- ifHCOutOctets
- ifHCOutUcastPkts
- ifHCOutMulticastPkts
- ifHCOutBroadcastPkts

Use of high-capacity (64 bit) counters simplifies monitoring of packet counters, as compared to 32 bit counters which can wrap around quite frequently.

Please see the associated IF-MIB conformance file in the release zip for complete information on WeOS IF-MIB support and deviations.

1.1.3 IEC 62439-2 MRP MIB

Support for the SNMP MRP MIB (IEC 62439-2 MRP MIB) is included (read-only). See the associated IEC-62439-2-MIB conformance file in the release zip for details on WeOS MRP MIB support and deviations.

1.1.4 WESTERMO-TCN MIB (Private 'Train MIB')

Support for WESTERMO-TCN-MIB is added, a private MIB complementing the standard MIBs for IEC 61375 Train Communication Networks (TTDP-MIB and TRDP-MIB).

WESTERMO-TCN-MIB provides ability to read and set the local etbnInhibition flag (IEC 613875-2-5), and is equivalent to the 'inhibit' field in ETBN_CTRL message defined in IEC 61375-2-3.

Westermo still recommends using the standard TRDP mechanisms defined in IEC 61375-2-3 to manage the local etbnInhibition flag. The WESTERMO-TCN-MIB is provided for those instead preferring the use of SNMP for this purpose.

1.1.5 New Default Bootloader - Special Note for Lynx/RedFox

WeOS 5.12.0 is shipped with a new version of the Barebox bootloader (2017.12.0-7). In short, customers with existing Lynx and RedFox units are recommended to upgrade the bootloader on their units to Barebox 2017.12.0-7. This can be done via the CLI (as described in section 6.2), or via the Web Interface (available in WeOS 5.11.0 or later). Although not urgent for users of WeOS 5.12.0 or earlier, it is *strongly recommended to upgrade the bootloader on Lynx and RedFox units* before applying next feature release (5.13.0 or later).

More details
Earlier versions of the bootloader has a potential problem where the boot configuration can be reset to

default on RedFox and Lynx. For now, the issue is extremely rare, and would only occur for users (a) changing the boot configuration (e.g., to specify 'net-boot' to retrieve startup configuration via DHCP rather than flash), and (b) doing this in a way requiring substantial boot configuration storage (e.g., specify a very long DHCP 'clientid'). The result would be that the specific boot settings are replaced with the factory default boot settings.

Although experiencing this issue is currently rare, it is recommended that customers with non-default boot settings upgrade the bootloader on Lynx and RedFox units. The reason is that in the next feature release (WeOS 5.13.0) there will be improvements to boot configuration functionality, with the unfortunate side-effect that the mentioned issue will affect all Lynx and RedFox units with non-default boot configuration, unless the bootloader has been upgraded. An alternative to upgrade the bootloader pro-actively on Lynx and RedFox is to await the release of WeOS 4.13.0 and instead use the bootloader included in that release, in case it holds a new default bootloader version.

1.1.6 Improved Support for Ethernet Port Statistics

Support to view Ethernet packet counters and statistics are now available via the Web interface. Earlier this was only available via the CLI. For the CLI the output format is changed to improve readability.

```
example:/#> rmon
example:/rmon/#> statistics eth1
In Good Octets   : 774807          Out Octets      : 1147160
In Unicasts      : 1023            Out Unicasts    : 1072
In Broadcasts    : 1476            Out Broadcasts  : 2054
In Multicasts    : 1511            Out Multicasts  : 1564
In Bad Octets    : 0
In Filtered      : N/A             Out Filtered    : N/A
Undersize        : 0               Oversize        : 0
Fragments        : 0               Jabber          : 0
Multiple         : 0
Excessive        : 0               Late            : 0
Other Collisions: 0                Deferred        : 0
example:/rmon/#>
```

Output 'N/A' is listen when a certain counter is not available.

1.1.7 New ETBN Syslog Events (IEC 61375)

Two new syslog events are generated by units configured as IEC 61375 train routers (ETBNs) at system startup.

- "TTDP stack ready"
- "ECSC communication established"

For more information, see list of Security Related Events in the 'Logging Support' section in the User Guide ('Configuration Guides'/'General'/'Logging').

1.1.8 Changes and Recommendations Regarding 'listen' Setting

Some management services (SSH, HTTP, HTTPS, …) provide a 'listen <INTERFACE>' setting to associate them with a specific set of network interfaces rather than all. An example for SSH is shown below.

```
example:/config/management/ssh/#> listen vlan1
example:/config/management/ssh/#>
```

For the purpose of limiting access to SSH and other services, the general recommendation is instead to use the WeOS firewall facilities, see an example below.

```
example:/config/#> ip
example:/config/ip/#> firewall
example:/config/ip/firewall/#> input accept in vlan1 proto tcp dport ssh
example:/config/ip/firewall/#>
```

What is new in WeOS 5.12.0 is that the 'listen' setting for NTP Server has been removed. Thus, customers who earlier has used the listen setting for NTP should add a corresponding firewall rule instead when upgrading to WeOS 5.12.0.

Note: When the WeOS firewall is enabled, the default policies for input and forwarding filters are 'drop'. Thus you should ensure to add white-list/allow input rules for all services you wish to access on the unit and (for products running WeOS extended) allow forwarding rules for all traffic patterns you wish the unit to route.

For information on the WeOS firewall functionality, see WeOS User Guide, sections on 'Firewall' in 'Configuration Guides'/'IP' and in 'HowTos'/'IP'.

1.1.9 Application Hosting (Containers)

Note: *This feature is only available in certain products and to selected customers.*

WeOS 5.12.0 introduces support for application hosting. See WeOS User Guide, sections on 'Container' under 'Configuration Guides' and 'HowTos' respectively.

1.1.10 GRE Outbound Interface Setting

Support is added to specify outbound interface for GRE tunnels.


```
example:/config/tunnel/gre-1/#> local 192.168.2.66
example:/config/tunnel/gre-1/#> remote 192.168.11.5
example:/config/tunnel/gre-1/#> outbound vlan2
```

In the example above, the unit would only send GRE packets to its 'remote' peer (192.168.11.5) if reachable via interface vlan2. This can be useful if the route to the remote is learned dynamically (VPN tunnel established, via RIP or OSPF, etc), and to avoid sending GRE packets via the default route if the route is not available via the intended interface. Another possibility for this case is to use 'blackhole' routes (see User Guide, section 'Unicast Routing' under 'Configuration Guides'/'Routing'.

1.2 News in 5.12.1

WeOS 5.12.1 reverses a minor formatting change (introduced in WeOS 5.12.0) in the the output of the 'show version' command, which caused issues for WeConfig 1.13.1 and earlier.

2 Fixed Issues

2.1 WeOS 5.12.0

Fixes in WeOS 5.12.0 (as relative to 5.11.0):

Issue	Category	Description
#18453	TCN	Inter-consist ECN routes setup with incorrect mask in multiple ETB scenarios
#18432	TCN	URIs for devices in a multimedia CN of a remote consist are not resolved at all by a ETBN in local cst
#18431	TCN	If URIs for devices in the multimedia CN are provided with 'lcst', the DNS resolver returns the wrong IP address (same as TCMS)
#18425	Firewall	Tech support file lacks firewall status information
#18411	WEB	Text is overlapping on certificate web management pages
#18405	VPN	Stateless NAT issue when using an SSL tunnel
#18403	LED	Link-alarm does not set port LED 'yellow' (Lynx/RedFox)
#18399	Ports	100 Mbit/s Fiber SFPs unable to get link up
#18388	Logging	Syslog packets sent to remote server shows year 1969 when 'RFC5424 format' is selected
#18378	TCN	'show ttdp' shows wrong Inhibition Train: Value
#18368	TCN	'show ttdp' shows faulty consist info sometimes with inhibit
#18367	TCN	Valid topology frames sometimes dropped due to incorrect timeout and filling log
#18366	MRP	Temporary storm occurs on when rebooting MRP manager in intact ring
#18358	WEB	Web interface in WeOS 5 has FPS selectable for egress rate limit
#18343	Boot Loader	Barebox resets boot-config at startup for large boot-configs (>4096 bytes)
#18335	System	Routing Hardware Offloading is unstable for multicast routing (Viper-TBN/Viper-208)
#18307	SNMP	Incorrect response type for OID frntStatusTimeSinceLastChange
#18305	SNMP	Incorrect ifRefifIndex assignment when using link-aggregates or SSL interfaces (WESTERMO-INTERFACE-MIB)
#18299	MRP	Duplication of MRP packets by MRC at link-up may cause MRM to block port too early (Viper)
#18298	WEB	SFP DDM values not shown in Web
#18273	TCN	TTDP will occasionally not reinaugurate upon topology change"
#18071	CLI	CLI configuration autocompletion for "config/port/mdix-mode" incorrect

Issue	Category	Description
#18018	System	Port monitor can cause mac-addresses to be learned to be located at the local CPU-bridge
#18014	WEB	Routing Hardware Offloading setting missing in Web (Viper-TBN/Viper-208)
#18006	WEB	Web does not report when it failed to apply uploaded configuration
#17998	LED	FRNT LED always solid green after reconfiguration
#17991	VPN	L2VPN bridging unable to switch traffic when enabling Routing Hardware Offloading (Viper-TBN/Viper-208)
#17964	TCN	Use of VRRP and HW Offloading can break unicast upon VRRP failover (Viper-TBN)
#17753	WEB	Web Server Reflected XSS for invalid URL
#17746	DHCP	Manually configured DHCP relay remoteid hex values over 0x7f not stored correctly in config file
#17662	WEB	The same outbound iface in DNS or Static Multicast context can be added multiple times
#17659	WEB	No indication that a local user has to be created in order for the Configuration/AAA/Login page to be usable
#17650	WEB	LAGs and SSL tunnels are not all visible when configuring VLANs or IGMP snooping
#17627	DHCP	PID is always "0" with "show dhcp-server" command

Issue #18343 requires the bootloader to be upgraded to Barebox 2017.12.0-7, see section 1.1.5.

Issue #17964 was fixed already in WeOS 5.9.2 and issue #17650 was fixed in WeOS 5.10.0, but were incorrectly listed as a 'known issue' in subsequent Release Notes.

2.2 WeOS 5.12.1

WeOS 5.12.1 holds no fixed issues except for the one mentioned in section 1.2.

3 Known Limitations

This section describes known limitations in WeOS.

3.1 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.

3.2 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. For use cases with static routing setups, hardware offloading can be enabled as shown in the example below.

```
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 behavior 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:/#>
```

3.3 SNMP

SNMP in WeOS 5 is read-only.

When configuring SNMPv3 authentication it will not inform the user if the password length is valid (minimum of 8 characters).

The MIBs folder in the release ZIP-file contains a conformance folder listing all supported MIBs and OIDs.

3.4 FRNT

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

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

3.5 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.

3.6 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 behavior. This is also true when Ethernet speed on backbone ports is set to Gigabit speed.

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.

Gigabit speed on backbone ports limits the handling of lost and recovering middle nodes.

Since hardware offloading was introduced in WeOS 5.8.0, Viper TBN can now route data at a faster rate than the CPU could previously, leading to a potential of overloading the CPU during the time when the offloading tables are being set up. Since this happens during TTDP train inauguration, 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.

3.7 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. The MAC Local bit (02) is also set.

3.8 Port Monitoring

It is not possible to utilize 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.

3.9 Link Aggregation

The current release WeOS 5.12 is not fully compatible with link aggregation in release WeOS 5.6 or earlier; this is due to a bug in WeOS 5.6, which included ports of different speeds in the aggregate.

3.10 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 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.

For an online version of the latest WeOS 5 User Guide we refer to the Westermo Web site (`https://www.westermo.com`, see *Solutions* and *WeOS*).

3.11 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.

3.12 Firewall configuration on layer-2 units only in CLI

For layer-2 WeOS 5 units (software level *WeOS Standard*), the firewall configuration can be used to set *input filters*, i.e., to control access to local services (SSH, Web, DHCP, …). However, firewall configuration on layer-2 units is currently limited to CLI.

4 Known Issues

4.1 List of known issues

Issue	Category	Description
#18469	System	An additional card is incorrectly listed under 'System Information' (Type UNKNOWN)
#18440	DHCP	NetBoot does not immediately continue when receiving DHCP offer missing option 67/68
#18413	VPN	SSL/OpenVPN with PSK is not working unless immediately replacing 'inet ssl' with 'inet static' on SSL iface
#18382	VRRP	Deleting a VLAN interface with VRRP instance breaks the web interface configuration->VRRP.
#18377	Logging	Syslog events may be missed during syslogd restart
#18365	QoS	ARP packets treated with lowest priority
#18362	TCN	Broken/missing ECSPs in train composition handled incorrectly
#18356	General	mDNS is not functional when configured to listening on specific interfaces
#18289	MRP	On MRC link-up with profile 30 ms MRM responds too slow resulting in short transient storm
#18286	TCN	Multiple tractor vehicles in single consist not supported
#18275	VRRP	Not possible to match on VRRP interface in firewall
#18166	IGMP	Delayed loss of IGMP multicast in FRNT ring when switch in ring restarts
#18164	Documentation	VLAN priority listed as setting although not supported
#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
#18139	IGMP	IGMP join sent untagged on tagged VLAN port
#18127	TCN	Topology frames may not be sent out on the backbone if a lag in direction 2 is physically up but logically down.
#18090	Link Aggregation	Flooded traffic is forwarded through detached ports (Lynx/RedFox)
#18087	System	Port monitoring 'mirror port' is not isolated
#18076	MRP	Probing MRP status (30 ms profile) during heavy load may cause reboot (Viper-TBN)
#18069	TCN	ARP frames may be missed/dropped under load
#18068	VRRP	VRRP frames may be missed/dropped under high load

Issue	Category	Description
#18045	MRP	The MRM switch is unreachable if ring port is 'lowest port' on VLAN (RedFox/Lynx)
#18024	System	DDNS service crashes if there are special characters in password
#17995	System	Service discovery not available in safe-config
#17982	IGMP	IGMP snooping may occasionally fail to store learnt group MAC addresses in FDB (Viper-TBN)
#17941	IP Multicast	Manual FDB MAC entry skips CPU port and automatically adds all ports with a VLAN with IGMP snooping disabled (Viper-TBN)
#17353	Alarm	Link Alarm can fail when included in aggregate

4.2 #18289: Work-around for handling MRM issues with MRP 30 ms profile

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. Currently 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).

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

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

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

4.4 #18045: Work-around and heads-up on upcoming change in MAC assignment

In previous release note (5.10.0) the change described here was listed to be included in WeOS 5.11.0. Instead of stating a specific release, the release including the change will list this in its 'News' section.

In WeOS 5, a VLAN network interface (vlan1, vlan2, …) by default inherits its MAC address from one of its associated ports (eth1, eth2, …). From a coming feature release and onward, all VLAN network interfaces will instead use the unit's base MAC address as their MAC address. Information on this will

be included in the release notes of the release including the change, thus information here is primarily a heads-up.

In most setups, a future upgrade to that release will go smoothly. The exception is when the VLAN interface MAC is used for specific purposes, e.g., when a DHCP server assigns IP address to the WeOS 5 unit based on its MAC address. If that is the case, it is recommended that you already now start to prepare.

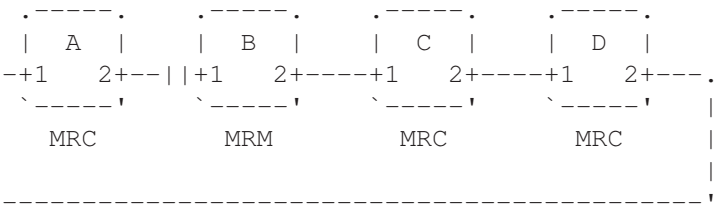
- In case you need to keep your existing VLAN MAC, you can configure it statically, overriding the WeOS default MAC assignment algorithm.

```
example:/#> show iface
INTERFACE          OPER  ADDRESS/LENGTH      SOURCE      MAC/PTP ADDRESS
lo                 UP    127.0.0.1/8         static      00:00:00:00:00:00
vlan1              UP    192.168.2.23/24     static      00:07:7c:1c:cf:a1
                         169.254.69.180/16   link-local
vlan2              UP    192.168.5.11/24     static      00:07:7c:1c:cf:a8
example:/#> configure
example:/config/#> iface vlan1
example:/config/iface-vlan1/#> mac 00:07:7c:1c:cf:a0
example:/config/iface-vlan1/#> end
example:/config/#> iface vlan2
example:/config/iface-vlan2/#> mac 00:07:7c:1c:cf:a8
example:/config/iface-vlan2/#> leave
```

- In the specific example where a DHCP server assigns IP addresses based on the unit's MAC, you could consider changing the assignment algorithm to use *clientid* or *option82* (Port ID). Alternatively, the DHCP server could be prepared to use the unit's new MAC address, the base MAC, when assigning the IP address. The base MAC of the unit can be found in several ways, e.g., using the "show system-information" CLI command.

The rationale for shifting the default VLAN assignment mechanism relates to issue #18045: The MRM switch is unreachable if ring port is 'lowest port' on VLAN (RedFox/Lynx)", see list of known issues above.

The problem can occur between an MRM(B) and its neighbor(A) on the link with the blocked port. In short, when A wish to communicate with B, it should send packets through port 1 towards D, which in turn forwards them to C, and so on. But in some setups, A may be "tricked" to send packets to B in the other direction, reaching B on its blocked port, where they will be dropped.



(The example here is for MRP, but the same situation can occur for FRNT between the 'focal point'

and its neighbor 'member' switch.) When this happens, the simplest workaround in WeOS 5.10 is to assign VLAN MAC addresses on the MRM(B) to its base MAC. As mentioned above, this will be the default behaviour from the release including this change. More details are given below.

- VLAN interfaces (e.g., vlan1) inherit the MAC address from one of its associated ports; giving precedence to the MAC of the 'lowest untagged port', e.g., MAC address of eth1.
- eth1 port MAC is also used for some low level (MGMT) signalling protocols, e.g., as source MAC in LLDP and MRP packets going out through eth1.
- "WeOS 5 RedFox and Lynx" (Dagger platform) learn MAC address not only from regular packets, but also from MGMT packets.
- In the example above, node A risk to learn the MAC of B's interface vlan1 from the wrong direction (from MGMT packets coming from B's port eth1), thus A will be unable to reach B on vlan1. Changing the MAC of B's vlan1 to B's base-MAC will remedy the problem.

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-5.12.1.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-5.12.1.pkg.
Current boot loader: *Barebox 2017.12.0-7*

`redfox-4d-3b-20:/#>` **upgrade boot <SERVER-ADDRESS> WeOS-5.12.1.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/