Prepared by	Document	
Fredrik Pettersson	Release Notes WeOS 4.28.3	
Approved by	Date	Document No
Niklas Mörth	March 30, 2020	089604-gf3a241f

Release Notes WeOS 4.28.3

Contents

Prepared by	Document	
Fredrik Pettersson	Release Notes WeOS 4.28.3	
Approved by	Date	Document No
Niklas Mörth	March 30, 2020	089604-gf3a241f

Prepared by	Document	
Fredrik Pettersson	Release Notes WeOS 4.28.3	
Approved by	Date	Document No
Niklas Mörth	March 30, 2020	089604-gf3a241f

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 can be found at the following Internet address: http://www.westermo.com.

Prepared by	Document	
Fredrik Pettersson	Release Notes WeOS 4.28.3	
Approved by	Date	Document No
Niklas Mörth	March 30, 2020	089604-gf3a241f

About

Westermo WeOS is a network operating system designed for industrial grade rugged Ethernet switches and routers. Fully supporting RedFox, 2^{nd} generation Wolverine and Viper, Lynx switches, and the Falcon ADSL/VDSL2 router.

WeOS is a Linux based software platform that has been in operation since 2006 on custom made RedFox Mil, RedFox Aero and RedFox Rail products. With the advent of the RedFox Industrial line of products the platform was given a major overhaul to improve standards compliance as well as compatibility requirements with existing Westermo product offerings. The result is WeOS, the Westermo Operating System.

For more information about Westermo and other product offerings see http://www.westermo.com/.

Version Number Format

WeOS version numbers have three fields. The main reason for the third field is to emphasise the difference between feature and bug fix releases.

The generally available (GA) releases are named 4.X.Y. The number four (4) denotes the platform generation. The X is the feature release number, where new functionality is introduced, and Y is the patch revision number, reserved for security and bug fix releases. E.g., 4.15.1 would be the first patch release in the 4.15.0 series.

For customers in our beta release program it is worth pointing out that previously version numbers 9.00 – 9.99 were used for beta releases and developer builds. This custom has now been replaced by the more common –betaN notation, for internal and limited distribution beta releases, and –rcN, for release candidates. We believe this to be easier to keep track of since the base release version is visible in all stages of the release cycle.

Prepared by	Document	
Fredrik Pettersson	Release Notes WeOS 4.28.3	
Approved by	Date	Document No
Niklas Mörth	March 30, 2020	089604-gf3a241f

1 Summary of Changes

1.1 WeOS 4.28.0

1.1.1 FRNTv2

WeOS 4.28.0 introduces support for a new version of FRNT (FRNTv2). FRNTv2 supports multiple ring and sub-ring instances, thus can be used to build more complex LAN infrastructures.

FRNTv2 is not backwards compatible with version 0, thus an FRNTv2 instance can not act as focal point or member in an FRNTv0 ring. However, it is possible to run both FRNTv0 and FRNTv2 on the same switch. That is, the switch can be part of an FRNTv0 ring and one or more FRNTv2 rings at the same time.

1.1.2 Port Monitoring is now persistent

Port monitoring has become a regular configuration setting. The change means that port monitoring settings are now part of the configuration file and are saved across reboot. This enables port monitoring to be used in applications with permanent mirroring of traffic to a recording device.

In earlier releases port monitoring was only provided as a troubleshooting tool, where the settings were not stored in the configuration.

1.1.3 Support for new Private MIBs

Two new private MIB files are introduced, complementing the regular WeOS 4 private MIB (WESTERMO-WEOS-MIB). The new MIBs are:

- WESTERMO-FRNT-MIB: This MIB defines a generic FRNT MIB module with objects for both FRNTv0 and FRNTv2. FRNTv0 objects can also be accessed in the WESTERMO-WEOS-MIB.
- WESTERMO-INTERFACE-MIB: This MIB defines an Interface MIB module listing all ports and interfaces and their reference index. The purpose of this reference index is to have a predictable index for ports and interfaces.

Both of these MIBs are shared between WeOS 4 and WeOS 5.

1.1.4 Changes to the factory default configuration

With WeOS 4.28.0, there is no FRNT alarm trigger included in the factory default setting. This change only affects users who configures FRNT on a WeOS unit reset to factory default settings.

In this case you must manually add an FRNT alarm trigger if you wish to get notified upon changes in FRNT ring status. Please see the chapter on “Alarm handling, Front panel LEDs and Digital I/O” in the *WeOS Management Guide* for more information on how to configure an alarm trigger for FRNT.

1.2 WeOS 4.28.1

No new functionality in this release only fixed issues, see chapter 3.

1.3 WeOS 4.28.2

No new functionality in this release only fixed issues, see chapter 3.

1.4 WeOS 4.28.3

This release includes an important security fix (security vulnerability CVE-2020-8597, see below), and a set of bug fixes, see chapter 3 for details. There is no new functionality in this release.

Fix for security vulnerability CVE-2020-8597 All WeOS systems explicitly configured to use PPP should be upgraded to WeOS version 4.28.3 or greater to fix this vulnerability.

A security vulnerability in the PPP package was published 2020-03-02. It is a critical vulnerability scoring 9.8 on NIST. It might allow a remote attacker to crash parts of WeOS or even run remote code execution. This vulnerability is most likely (unconfirmed) affecting WeOS systems configured to use PPP or more specifically “PPPoE” or "PPP over Serial Port". For more information om PPP, see the “PPP Connections” chapter in the WeOS Management Guide.

2 Known Limitations

This section includes known reported bugs and missing features, which may not necessarily be *limitations*, in many cases they may constitute severe operational drawbacks.

2.1 Platform

- A system with many VLANs setup requires more time at boot. This was first reported in #3291, but even after having fully optimised all data paths there still remains a significant delay. E.g., creating 128 VLANs on a RedFox Industrial takes apx. 6 seconds longer than creating a single VLAN.
- The new alarm configuration lacks support for RMON triggers.
- Running an FRNT ring over copper SFPs is not recommended, due to slow response time from copper SFPs.
- Limited support for low–level interaction with PHYs and link partners.
- Moving ports from one VLAN to another can change the MAC address of the corresponding VLAN interface leading to loss of connectivity. The symptoms are that Web and SSH connections to the device suddenly "freeze" due to stale ARP caches. The effects of which can take several minutes to resolve.

  WeOS 4.3.0, and later, include support for gratuitous ARP on MAC address changes. However, not all client systems allow gratuitous ARP, although configurable, for security reasons. For cases where this effect is undesirable, e.g. a management interface, it is recommended to set a static MAC address using the CLI.
- Port monitoring fails to preserve the VLAN priority, issue # 4152. Fix planned for a later release.
- When toggling bridge priority on the elected root bridge storm is easily provoked, issue #4203. Fix planned for a later release.
- In some setups when RSTP gets link up it has been reported to take very long to reconfigure, issue #4707.
- The traffic types configurable for port ingress rate limit has side effects. Selecting multicast will also rate limit broadcast. Selecting unknown unicast will also limit broadcast and multicast. This behaviour will likely change in a later release. Issue #6939.
- Ports in VLAN are not moved to the default VLAN (1) when the VLAN is disabled. Issue #12921.

2.2 CLI

- When issuing, e.g., `show running` not all settings are shown. This is due to WeOS 4.3.0 and later only showing differences to the system default. Support for `show running [all]`, where the optional 'all' keyword would list everything, is planned for a later release.
- The on–line help is not only insufficient, it is sometimes even misleading. E.g., some commands do not support the `no` prefix, some commands do not support `show` and no commands in configure context support `repeat`. Cleanup and improvement is a work in progress.

2.3 MRP

MRP ring ports have to be on the same slot when used on products with multiple slots. MRP does not support aggregate ports.

2.4 SNMP

The SNMP chapter of the WeOS Management Guide lists supported standard MIBs, including limitations to specific tables for some MIBs. Additional deviations from the standard MIBs may exist. For some MIBs, you find more detailed MIB conformance information in the WeOS release zip-archive.

2.5 Web

- Inspecting RMON counters in the Port Statistics page may need a manual reload before the actual values are displayed.
- Due to security reasons the username and password must always be provided when logging in, i.e auto-completion is not supported in the login form.

2.6 IPConfig Tool

Limitations in current v10.4.0 of IPConfig Tool for Windows™.

- The WeOS version is encoded in the old version numbering format to be fully compliant in all Windows™ releases. E.g., version 4.3.0 is encoded as 4.03 and version 4.3.1 is also encoded as 4.03. Hence, version 4.10.0 would be encoded as 4.10.
- Due to limitations in the version field of IPConfig the patch level of the WeOS version is not visible in the tool. No fix planned.
  Workaround: Verify patch revision from Web, CLI or SNMP.

- Limitations in field length causes problem with upgrade from IPConfig Tool, i.e. too long file names are not supported. No fix planned.
  Workaround: Rename image file name to a shorter name before attempting upgrade. Note, the file name is *not* used in any way to encode any information for the upgrade process.

2.7 SHDSL

- SHDSL link can sometimes on older DDW-225/226 hardware be lost due to slowly dropping SNR margin, issue #5317. This seems to be caused by high traffic load on the link. Fixed on boards with hardware revisions 3 or newer, DDW-225 (5013-0750) and DDW-226 (5013-0740). This board update was introduced in production from serial number 4645 on the DDW-225 (3642-0250) respectively 4931 for the DDW-226 (3642-0240).

2.8 Firewall

- Port forwarding does not work well with interfaces using DHCP assigned IP addresses. A fix is planned for a later release.

2.9 IPsec

- MTU override may not work as expected, sending a message over the IPsec tunnel will not respect mtu override on the other end. **Workaround:** Always have the same MTU on the interfaces on both ends of the tunnel.
- The remote IP address of the IPsec gateway may in some circumstances not be reachable from an IP address associated with the IPsec tunnel. Issue #5987
  Workaround: Always connect to an IP on the IPsec gateway that is reachable from within the tunnel.
- DPD restart/clear is sometimes unreliable. If the responder is configured with dpd-action clear and then rebooted, the tunnel will sometimes not be renegotiated.
  Workaround 1: If only using static IP addresses and only one initiator, change both nodes to be initiators and set dpd-action hold on both sites.
  Workaround 2: Use a ping trigger towards an IP inside the tunnel and connect the ping trigger to a tunnel action (See section 5.18). Remember to set 'retrain interval 30' in the action configured, this will create another level of DPD outside the IKE traffic, but it will be encrypted.
  Workaround 3: If it is not possible to use DPD hold (multiple initiators or not static IP) you can on the initiator(s), create a tunnel action (see section 5.18) and set it to be retrained after a few seconds. Use a ping trigger and set peer as an IP inside the tunnel, and connect it to the tunnel action.

2.10 SSL VPN

WeOS implements SSL VPN using OpenVPN with the following known limitations

- To be able to use dynamic or static routing over a ssl interface you will have to use a layer 2 tunnel. Layer 3 tunnels will not work as expected in this scenario.
- No support for revocation lists
- No check for certificate type, a client certificate can be used as a server certificate and reversed.
- When using layer3, OpenVPN supports multiple topologies, p2p, net30 and subnet, WeOS only support subnet.
- Not possible to add a layer2 interface to a VLAN.

2.11 Link Aggregation

WeOS supports link aggregation in line with IEEE 802.3ad. However, the current support for link aggregation contains several limitations such as:

- VLAN support: There is no support to add a link aggregate to a VLAN. Instead, each of the individual member links need to be added to the appropriate VLANs.
- Port settings: There is no support to configure port settings for the link aggregate. Instead, each of the individual member ports need to be configured uniformly, e.g., with respect to port speed/duplex mode.
- Only link aggregation of Ethernet ports is supported. Aggregation of SHDSL ports is provided as technology preview. Configuration of xDSL ports (ADSL/VDSL) ports in an aggregate, or mixing Ethernet and SHDSL/xDSL ports, an aggregate may be possible, but this is not supported and the behaviour is undefined, issue # 8117.

2.12 Serial over IP

- Issue #8251 details how a sender of broadcast data also receives a copy of the data.
  Workaround: When using broadcast destination, please select a listen interface.

2.13 Software Upgrade

- No support (yet) for scheduled upgrades, i.e. ability to upgrade @02:30 to limit downtime during regular office hours. Feature request registered in issue #3363. Support planned for a later release.

2.14 802.1X

- 802.1X authentication in combination with LACP, RSTP or FRNT is unpredictable. Connectivity to the unit may be lost if the primary link goes down.

2.15 Bootstrapping Configuration via BOOTP

- Bootstrapping the configuration file using BOOTP is only possible over the WeOS unit's Ethernet ports. DSL ports (SHDSL, ADSL, VDSL) can not be used.
- It is only possible to use BOOTP/TFTP to download the WeOS configuration file (certificates for IPsec, etc., can not be downloaded).

2.16 Bandwidth Limiting in Frames per Second

The frames per second (fps) mode for the "traffic shaping" setting (layer-2 feature) is

- only supported on Ethernet ports (not on DSL ports)
- not supported on certain RedFox models. See management guide for further details.

Similarly, the frames per second mode (fps) for the "CPU bandwidth limit" setting is not available on some RedFox models (it is not available on RedFox models with architecture "xscale", use the CLI command "show system-information" to find out the architecture of your product).

Note: There are currently *no warnings* when the "fps" does not apply for traffic shaping or CPU bandwidth limit. In such cases, the rate setting will ignore the fps attribute and interpret the rate in bps.

2.17 Flow Control

The WeOS flow control support has the following two limitations:

- When enabling *802.3x flow-control* on a port, that port will permanently operate in flow-control mode without involving Ethernet auto-negotiation mechanisms.
- When configuring flow-control in "slot based" WeOS products (for example RFI), a port with 802.3x flow-control enabled will only send Pause frames when causing congestion on another port in the same slot; not when causing congestion on a port in another slot. For example, if port 1/1 has flow control enabled, it will send Pause frames when causing congestion on on port 1/2, but not when causing congestion on port 2/1. Similar restrictions apply to WeOS Viper, RedFox Rail (RFR) and RedFox Industrial Rack (RFIR) products.

2.18 LLDP

The WeOS LLDP support has the following known limitation:

When connected to Windows 10 PC with LLDP driver enabled, the WeOS unit will not respond to SNMP requests for the “remsysname” LLDP SNMP OID. The proposed work-around is to disable the LLDP driver on the Windows 10 PC.

2.19 IGMP

WeOS sends IGMP frames (query and membership report) with the optional IP option “Router Alert”, according to RFC 2113. It is not possible to disable the inclusion of the “Router Alert” option.

Not all routers or end devices, parse the IP header properly to figure out the location of the IGMP payload. Instead they assume the IP header is 20 bytes long and always read offset that location. Hence, for those end devices this means loss of IGMP related functionality.

2.20 TTDP (IEC 61375-2-5)

This limitation only applies RFR-212-FB (the only WeOS 4 product capable of running IEC 61375-2-5 TTDP).

The WeOS 4 TTDP implementation sends TTDP TOPOLOGY frames with the *ETBN-CN-CNX* field(s) encoded in ’big endian’ byte order. There has been (and still is) some confusion on how to interpret the standard, and there are vendors encoding this field either as ’big endian’ or as ’little endian’.

The WeOS 4 TTDP implementation only interoperates with TTDP implementations capable of encoding the ETBN-CN-CNX field as ’big endian’.

3 Fixed Issues

Fixed issues in WeOS 4.28.0:

Issue	Category	Description
#17702	Web	Remove LACP ports before removing them from FRNT breaks Web
#17393	DHCP	DHCP Option 82 assigning wrong default gateway per port

Fixed issues in WeOS 4.28.1:

Issue	Category	Description
#17725	Ports	Lynx-DSS-L108-F2G-S2-12VDC - Problem with serial port 1
#17603	LLDP	LLDP does not report Management IP Address associated with default VLAN
#17530	System	Watchdog service cannot read reset reason on Corazon platform
#17499	Alarm	Link-Alarm on show port is inverted when condition is set to high from CLI or WEB
#17756	WEB	Port monitor does not work correctly in web
#17748	WEB	Autogenerated web certificate key is shorter than 2048 bits
#17445	LLDP	Log filled up with not useful information from LLDP
#17736	LED	Port LED not indicating Alarm (YELLOW) for ports with "condition high" link-alarm
#17712	CLI	"show monitor" may give assert
#15972	TTDP	Double firewall rules sometimes break TTDP 1-1 NAT (RNAT)

Fixed issues in WeOS 4.28.2:

Issue	Category	Description
#17824	DHCP	Non-unique DHCP host entries on different subnets not allowed
#17803	DHCP	DHCP/DNS server constantly restarting when using static DNS server assignment
#17672	Microlok	Logical connections are breaking down and reestablishing regularly when traffic load is increased

Fixed issues in WeOS 4.28.3:

Issue	Category	Description
#17874	CLI	Alarm trigger FRNT causing warning when leaving config (Invalid FRNT ring id)
#17868	WEB	'Tools->Tech Support' page links to startup and running configs broken
#17851	TTDP	TTDP re-inauguration not triggered in decoupled consist despite 'etbnInhibition false' in all ETBNs
#17787	DHCP	DHCP Replies stuck and looped at intermediate (snooping) DHCP relay agent

In addition, WeOS 4.28.3 includes an important security fix for CVE-2020-8597, see section 1.4 for details.

4 Known Issues

Issue	Category	Description
#17838	802.1X	Radius server FQDN causes 802.1X to crash
#17815	CLI	Reset reason not shown by 'show watchdog' status command
#17804	CLI	Port monitor available in admin context
#17802	IGMP	IGMP Querier election is not working in case of multinetting
#17681	System	Port Monitor accepts incoming traffic
#17625	Logging	Ping trigger error filling up log with useless information
#17610	Web	Max CN binding error when applying SSL configuration in Web
#17602	Web	Selecting PAF changes SHDL port 2 to CO from CPE automatically
#17597	Alarm	Automatic selection of source IP for SNMP Traps causes problems for WeConfig to display the alarm
#17580	Web	Rate-limit resets to match all traffic types via any port configuration in Web
#17554	OSPF	OSPF network type misleading for OSPF over GRE (type is Point-to-Point)
#17526	Ports	Port temporary enable function will never timeout on fiber ports
#17383	IP Multicast	VRRP with mroute-ctrl fails to forward 'mcast routes with wildcard source IP' upon VRRP failover
#17295	802.1X	802.1X will wipe authenticated users if changes are made to a VLAN
#17284	Alarm	Creating an alarm using ddm-rx-power will not trigger an alarm based on the specified values
#17220	RSTP	STP sending BPDUs on non STP-port's after reconfiguration.
#17061	RIP	Falcon: Problem binding RIP socket
#16970	WEB	Configuring DHCP Server static lease matching clientid (option 61) via Web lacks '01' prefix
#16835	CLI	ipcalc command - 'network id' has a sticky /24 output
#16801	Serial	Termination for RS485 not working
#16052	LLDP	Sometimes a reboot is needed on the device with the different VLAN name to prompt the LLDP MGMT IP address to disappear
#14936	IGMP	Loss of multicast in FRNT ring when switch in ring restarts
#14838	DHCP	DHCP host option tftp-server causes offer to be sent untagged
#14661	VPN	OpenVPN: CLI reports tunnel up when interface is down
#14378	Firewall	NAT fails to translate source IP at high packet load
#14363	DSL	Communication over DSL port sometimes uni-directional after recovery
#14325	DHCP	DHCP-server refuses to (re-)deliver option 82 static and client ID based leases after configuration change

Issue	Category	Description
#14307	System	A SSH session will not time out if idle timeout is longer than keepalive
#14041	Firewall	DHCP relay configured with multiple VLANs may not be able to handle server response (dropped in firewall)
#13846	DHCP	Match rule precedence order in DHCP server differs between different clients
#13693	VPN	Rebooting responder may result in loss of tunnel connectivity
#13515	System	NULL character sometimes added to the output produces more data than received
#13415	NTP	NTP client does not adjust time if the difference exceeds 1s after being offline
#12663	Ports	CLI freezes when connecting a gigabit fiber link with autoneg disabled to a WeOS device with autoneg on
#10797	General	IPsec backup peer sometimes fails to establish the tunnel when switching from backup to primary
#10703	General	SSL VPN reports tunnel up, even though parameters are not matching on server and client sides
#10516	VPN	VPN LED for SSL VPN server should indicate up only when at least one client is connected
#10336	Serial	Serial driver sometimes introduce gaps between characters in a data stream
#8286	LAGG	Combining dynamic VLANs (AVT) and link aggregates does not work
#7500	VPN	IPsec with certificates and identity using 'auto' will not work
#7276	Firewall	IPsec no remote network causes NAPT rules to be bypassed
#6180	System	RedFox 8FX: System instability issues with 1000Mbps fiber in 100Mbps SFP slot
#4929	RSTP	Looping admin edge ports causing a storm
#4707	RSTP	Long reconfiguration time for RSTP at link up, up to 32 sec
#4203	RSTP	Storm occurs quite frequently when toggling RSTP bridge priority

5 Technology Previews

WeOS contains hidden and undocumented features called technology previews. Westermo provides no support for undocumented features. Features specifically marked as tech previews can be completely redesigned, removed or changed in such a way that after an upgrade they are *not guaranteed* to work!

The following is by no means a complete list, but details features that may become supported in the next upcoming feature release.

- *Password Encryption*: CLI only, section 5.1
- *Trigger to control Interface Admin Distance*: CLI only, section 5.2
- *Setting default gateway per interface*: CLI only, section 5.3)
- *SFP DDM Alarm and SNMP Trap Support*: Alarm settings in CLI only, section 5.4
- *Serial Low Latency*: CLI only, section 5.5
- *SNMP MIBs for RIP and OSPF:* See section 5.6
- *NTP Server with GPS support*: CLI only, section 5.7
- *TFTP Server*: CLI only, section 5.8
- *Guest User*: CLI only, section 5.10
- *New VLAN Features:* CLI only support for disabling 'secure' mode and MAC address learning. See section 5.11
- *Additional SSH settings:* CLI only support for setting SSL port, idle-timeout and keepalive interval for the WeOS SSH server. See section 5.12
- *Additional Telnet settings:* CLI only support for setting Telnet port for the WeOS Telnet server. See section 5.13
- *Tcpdump:* CLI only. See section 5.14
- *CLI welcome message:* Ability to set custom CLI welcome message. See section 5.15
- *Additional DDNS features*: See section 5.16
- *USB functionality*: *USB boot* and *USB logging*. CLI only, section 5.17.

  Separate feature from "USB Autobackup/restore" and "USB Configuration Deployment"!
- *IPsec and SSL VPN extensions:* Ability for IPsec initiators to be configured with two responder addresses (*IPsec Backup Peer*), IPsec and SSL VPN tunnels can be enabled/disabled via alarm trigger and action, and SSL VPN tunnels can be configured using a standard OpenVPN configurationfile (.ovpn). See section 5.18.
- *PPPoE Server*: CLI only, section 5.19

- *Serial HDX mode*: CLI only, section 5.20
- *DHCP client arping option*: CLI only, section 5.21
- *Support for disabling DHCP snooping in DHCP relay agent*: CLI only, section 5.22
- *Firewall conntrack flushing*: CLI only, section 5.23
- *RSTP support for VLAN tagging of BPDU's*: CLI only, section 5.24
- *Remote IO support*: CLI only, section 5.25
- *Storm control*: CLI only, section 5.26

5.1 Password Encryption

Passwords for PPP, DDNS, RADIUS, IPsec secrets, SNMP v2 community strings, etc., are by default stored in clear text in the WeOS configuration. As of WeOS 4.15.0 these strings can be encrypted using a built-in secret key to provide a very basic level of security. This is by no means a cryptographically secure encryption, and can possibly more be likened to obfuscation rather than true encryption. Nevertheless, it is likely good enough for most users.

To enable password encryption in the running configuration and save it to the startup configuration, simply type:

```
example:/#> config
example:/config/#> encrypt passwords
example:/config/#> leave
example:/#> copy run start
```

To further secure an installation the user can provide a custom encryption key. This key will be device specific and must be entered again if exporting the configuration to another device. The key can be at most 64 characters long and will be securely[1] stored in built-in flash of the device to be able to boot.

```
example:/#> config
example:/config/#> encrypt passwords key XYZZY
example:/config/#> leave
example:/#> copy run start
```

To change custom key from 'XYZZY' to 'QWERTY' the user will be prompted to input the current custom encryption key. This prompt will not appear when changing from the default built-in key. To change from a custom key back to the default built-in key type:

```
example:/#> config
example:/config/#> encrypt passwords default
Configuration encrypted with a custom key, please input current key.
Password: *****                              (Silent prompt, no feedback)
```

[1] The custom key is in itself encrypted before stored in a file on built-in flash.

```
example:/config/#>  leave
example:/#>  copy run start
```

Password encryption is a per-file feature of WeOS. If you change to another configuration file, using the `copy` command, that file determines if password encryption is enabled or disabled. When changing to a file *with* encryption you can be prompted for its secret key, if a custom secret key was used to encrypt its passwords.

When disabling password encryption, using the `no encrypt` command, all password strings will be scrambled using a random secret key. This maybe seems a bit unintuitive, but is a security measure to protect your secrets from being decrypted by someone with access to a copy of your encrypted configuration and rogue WeOS device.

A factory reset, using crossed cables or the factory reset login on the console, will wipe all configurations, including any custom secret keys.

5.2 Interface Admin Distance Trigger

In a setup with multiple upstreams, e.g. at least two different Internet Service Providers (ISPs) on two separate VLAN interfaces, the device selects the primary ISP based on the configured interface distance.

To enable fail-over between multiple ISPs a *ping trigger* can be configured and connected to the interface's distance. (CLI only atm.)

As long as the ping reaches its target beyond the ISP, e.g. BBC.com, the interface distance remains at its configured setting, but when the trigger fires, due to BBC.com becoming unreachable via that ISP, the distance is automatically adjusted to 255 (infinity) for the associated default route.

While connectivity to BBC.com via the primary ISP is down, the secondary ISPs default route will be used instead, but as soon as connectivity is restored the system will fall-back to the primary ISP again.

```
example:/config/iface-vlan1/#>  distance 10 trigger 2
```

NOTE: Make sure to configure the trigger (ID 2 in this example) to use the *correct outbound interface*, otherwise the ping will use the default route, and you will get interesting flapping.

5.3 Interface Gateway

As a sign of things to come it is also possible to set the gateway address on interfaces with a static address. This as a complement to the possibility to setup a default route in IP configuration context.

Future additions will include DNS and NTP servers, as well as domain search prefix configurable on a per-interface basis, all activated according to the interface distance.

```
example:/config/iface-vlan1/#>  gateway 192.168.2.1
```


Please note, this setting is only available for interfaces of type **inet static**.

5.4 SFP DDM Alarm

Support to read status of Westermo DDM SFPs has been available since WeOS 4.13.1.

As a tech preview, there is now support for SFP DDM Alarm handling (of Westermo DDM SFPs), including SNMP DDM Alarm Trap support in the Westermo Private MIB. SFP DDM alarm triggers are configurable from the CLI only. Alarm can be configured set from voltage, bias-current, temperature, rx-power and tx-power.

Example:

```
example:/config/#> alarm
example:/config/alarm/#> trigger ddm-temperature          (Create DDM temp. trigger)
example:/config/alarm/trigger-3/#> port 1                    (Trigger on SFP port 1)
example:/config/alarm/trigger-3/#> threshold rising 60    (Rising threshold at 60°C)
example:/config/alarm/trigger-3/#> threshold falling 58   (Falling threshold at 58°C)
```

5.5 Serial Low Latency

Tech preview of *Serial Low Latency* is configurable, from the CLI only. The Serial Over IP application is extended with an additional mode: <seriallowlatency>. This mode is only for use in a point-to-point application where one serial port is connected to the remote unit's serial port over SHDSL (Wolverine units) or Ethernet. No addressing possibility exist.

The Serial Low Latency function is optimised for transferring serial characters at the lowest possible latency to the remote unit with as low jitter as possible. This function is only valid for one instance of serial over IP.

Syntax:

```
example:/config/#> seroip 1
example:/config/seroip-1/#> mode seriallowlatency
example:/config/seroip-1/#> port <SERIAL-PORT>
example:/config/seroip-1/#> remote-frame-delay
example:/config/seroip-1/#> remote-frame-delay <0-2147483647>          (0..2^31)
example:/config/seroip-1/#> remote-frame-size <0-512>
example:/config/seroip-1/#> local-frame-delay <0-2147483647>           (0..2^31)
example:/config/seroip-1/#> local-frame-size <0-512>
example:/config/seroip-1/#> iface <IFNAME>
```

In order to keep characters back-to-back, a data-packing algorithm has been implemented.

-delay parameters are in micro seconds,

-size parameters are in number of characters

local- parameters are used to configure the data-packet algorithm for characters received from the serial port before sending them to the remote unit

remote- parameters are used to configure the data-packet algorithm for characters received from the network side (SHDSL or Ethernet) before transmitting them to the physical serial port.

5.6 SNMP RIPv2-MIB and OSPF-MIB

Tech preview support of SNMP MIBs:

- RFC1724 RIP Version 2 MIB
- RFC1850 OSPF Version 2 MIB

5.7 NTP Server (with GPS Time-Base Support)

Support has been added for WeOS to act as a NTP server in a network. You can enter up to 4 reference clocks or/and a GPS receiver as clock source. In the current version of WeOS it is only possible to configure the server listen on all interfaces.

Add remote NTP server as reference clock (i.e., the unit will act as NTP client; this is a supported feature, see the *WeOS Management Guide* for more information):

```
example:/config/ntp/#> server pool.ntp.org
```

Enable NTP server (technology preview):

```
example:/config/ntp/#> listen              (Start NTP Server on all interfaces)
```

Hint: To limit access to the NTP server to a specific interface you currently have to use the WeOS firewall functionality (firewall functionality is available on the 200-series of WeOS products).

WeOS also have support for using a GPS receiver connected using RS232/422/485 and us it as a reference clock for NTP. This requires a preconfigured GPS receiver, it has to be configured to send NMEA reports. The correct serial port configuration also has to be entered into the serial port context in the CLI. Pulse per second (PPS) is currently not supported, but may be supported in future releases.

Enable GPS support (technology preview):

```
example:/config/#> gps 1                                (Create GPS instance '1')
example:/config/gps-1/#> port 1        (Use GPS attached to serial port '1')
example:/config/gps-1/#> end
example:/config/#> ntp
example:/config/ntp/#> gps 1           (Define GPS instance '1' as clock source.)
```

In the example above, the GPS was attached to serial port ”1”. Additional configuration of serial port 1 (e.g., bit-rate) may be required to match your GPS.

5.8 TFTP Server

WeOS has support to work as a TFTP server in the network, this can be a very useful feature when combining it with the BOOTP configuration deployment, introduced in 4.13. Make sure you have an USB stick inserted in the USB port and then enable the TFTP server.

```
example:/config/tftp-server/#> path usb://
```

5.9 Preferred (Remote) NTP Server

If more than one clock source is configured (multiple remote NTP servers, or a remote NTP server and a local GPS), the unit will synchronise to the source with the best *stratum*. To override this behaviour, an NTP server could be configured to be *preferred*.

```
example:/#> configure
example:/config/#> ntp
example:/config/ntp/#> server ntp.example.com
example:/config/ntp/server-ntp.example.com/#> preferred
```

5.10 Guest User

Basic guest user support is now possible to enable in WeOS. The reserved local username 'guest' must be setup in AAA configuration context to enable this feature:

```
example:/config/aaa/#> username guest guest
Adding new user guest.
example:/config/aaa/#> leave
example:/#> exit
example login: guest
Password:
example:/$>
```

The guest account is very restricted, e.g., it cannot configure the system, read passwords by from configuration files, or otherwise manipulate the state of the system. Only inspect status of ports, VLANs, interfaces and RMON, and do basic network debugging using, e.g., ping or traceroute.

5.11 New VLAN Features

By default WeOS VLANs are setup in 'secure' mode, IEEE 802.1q, so any traffic that, e.g., tries to ingress with an unknown[2] VLAN tag is silently dropped.

[2] I.e., a VLAN ID not configured for the given port, in either tagged or untagged mode.

With some equipment, or in some setups, this 'secure' mode is not desired behaviour. A user may simply want traffic to pass-through the switch unaffected. For this purpose it is now possible to disable the secure mode on a per VLAN basis.

```
example:/config/vlan-1/#> no dot1q
```

It is also possible to disable MAC address learning on a per VLAN basis.

```
example:/config/vlan-1/#> no learning
```

5.12 Additional SSH Server Settings

For the WeOS SSH server it is possible to tweak the default settings for

- Listening (TCP) port (default: 22)
- Keepalive interval (default: 60 seconds)
- Idle timeout (default: Disabled)

These settings are available in the SSH server configuration context (CLI only), for example:

```
example:/#> configure
example:/config/#> ssh
example:/config/ssh/#> port 12345
```

5.13 Additional Telnet Server Settings

For the WeOS Telnet server it is possible to change the default listening port (CLI only).

```
example:/#> configure
example:/config/#> telnet
Activating Telnet with default settings, type 'abort' to cancel.
example:/config/telnet/#> port 34567
```

Note: For security reasons, the Telnet server is disabled by default.

5.14 Packet Capture – TCP Dump

Previously only available to developers and support personnel, this release now adds support for the tcpdump packet capture tool in the CLI. Due to the design of the device's hardware, it is not possible to capture packets on a per-port basis (Layer-2), only per interface (Layer-3), but if a single port is setup in a VLAN the effect will in most cases be the same. With the exception of certain control traffic like IGMP, RSTP, FRNT, 802.1X, etc. Such frames will not be possible to capture, unless the functions in WeOS are completely disabled.

The exposed tcpdump features are limited, but should be sufficient for most use-cases. One such feature is the ability to save the PCAP files to a USB stick, if the device is equipped with a USB port.

See the online help in the CLI for more information and some useful examples to get started.

```
example:/#> tcpdump vlan1
```

5.15 CLI Welcome Message

Support for personalising the WeOS CLI welcome banner is another new feature. It is now possible to add a message that shows up before login, different depending on trying to login from from the console or SSH, and another after successful login, called Message of the Day, or MOTD.

- **Console login:**
  `example:/config/system/#>` **[no] issue <MESSAGE>**
- **SSH login:**
  `example:/config/system/#>` **[no] issue-net <MESSAGE>**
- **Message of the Day:**
  `example:/config/system/#>` **[no] motd <MESSAGE>**

Example:

```
example:/config/system/#> issue "Company Inc. Gateway | Welcome operator!"
example:/config/system/#> issue-net "Only authorized personnel, contact
   +46(0)123-456\nThis session is logged for any intrusion attempts!"
example:/config/system/#> motd "Site policy:\n o Do not change live
   system!\n o Contact sysadmin for help or system problems."
```

5.16 Additional DDNS Features

More DDNS Providers

The WeOS DDNS client, Inadyn, now has support for a few more DDNS providers: 3322, ZoneEdit, easyDNS, DNS-O-Matic, ChangeIP, nsupdate.info, DuckDNS, and Loopia. This in addition to the already supported: DynDNS, FreeDNS, and No-IP.

HTTPS/SSL Support

Some DDNS providers support HTTPS update, this WeOS 4.15.1 and later support an SSL check box in the WebUI and a 'ssl' setting in the CLI to enable this feature. Please note, you need to make sure your DDNS provider supports this before enabling SSL.

Forced Update

The DDNS client only sends an update to your DDNS provider when the IP address changes, and a forced update every week. In some cases, however, you may need to manually force an update. Currently this is only possible from the CLI (web support is planned for a later release)

```
example:/#> ip ddns update
```

See the system log file for both the action and results of the update. The actual DNS update may take a while to propagate to your Internet Service Provider (ISP), so please don't issue this command multiple times thinking this will speed up the process. It all depends on how your DNS record is setup at the DDNS provider.

Also, if you do this too often some DDNS providers will disable your account, or your DNS entry, for excessive updates. This is a policy of the DDNS provider.

5.17 USB Functionality

5.17.1 USB Boot

An exciting USB function referred to as "USB boot" is available as technology preview. Instead of using the USB stick as (continuous) backup, it can also be used to boot from. This has been available from WeOS 4.6.0, but is still only a technology preview. The directory structure used in 4.6.0 has changed in 4.8.0. To activate this, on the unit, simply log in to the CLI.

```
example:/#> boot
example:/boot/#> boot-order usb
```

5.17.2 USB Logging

Log files can be directed to a USB stick by using the "usb' setting in the *logging* configuration context (CLI).

First, insert a USB stick *prepared* to have a top directory named *log*.

```
example:/#> configure
example:/config/#> logging
example:/config/logging/#> usb
example:/config/logging/#> leave
example:/#> dir usb://log
================================================================================
/usb/log - Contents of USB File System
================================================================================
               0 2015-05-19 11:43 alarm
             539 2015-05-19 11:43 auth.log
```



```
   0 2015-05-19 11:43 cli
   0 2015-05-19 11:43 debug.log
 106 2015-05-19 11:43 kern.log
1625 2015-05-19 11:43 messages
 286 2015-05-19 11:43 ntp.log
   0 2015-05-19 11:43 ppp.log
   0 2015-05-19 11:43 ssl.log

================================================================================
Free: 167.0 MiB Total: 965.0 MiB
example:/#>
```

As many USB sticks are terribly slow, you might need to add a boot delay (USB bootstrap timeout).

```
example:/#> boot
example:/boot/#> usb
example:/boot/usb/#> timeout 5
example:/boot/usb/#> show
Status        : Enabled
Timeout       : 5 second(s)
example:/boot/usb/#> leave
example:/#>
```

See the WeOS Management Guide (in particular the chapter ”General Switch Maintenance”) for more information on USB support (bootstrap settings, supported USB sticks and file systems, etc.)

5.18 IPsec and SSL VPN Extensions

- Import an SSL tunnel using a OpenVPN configuration file This can configure up a SSL VPN tunnel in WeOS using a standard OpenVPN configurationfile (.ovpn) either with the certficates embedded or you can upload the certificates on your own.

  ```
  server:/#> tunnel import ssl 100 tftp://192.168.1.2/test.ovpn
  ```

- IPsec Backup Peer This is a technology preview of upcoming IPsec redundancy support.

  IPsec initiators may be configured with two responder addresses. If IPsec fails to connect to the primary responder, it will try to connect to the backup responder. The primary responder will periodically be checked, and a switch back is initiated if possible.

  ```
  example:/config/alarm/#> trigger ping
  example:/config/alarm/trigger-1/#> peer 192.168.22.2
  example:/config/alarm/trigger-1/#> end
  example:/config/alarm/#> end
  example:/config/#> tunnel
  example:/config/tunnel/ipsec-0/#> backup 192.168.23.2 trigger 1
  example:/config/alarm/#> leave
  ```


- Enable/disable IPsec and SSL VPN tunnels via alarm trigger and action

```
example:/config/alarm/action-4/#> target tunnel
example:/config/alarm/action-4/#> tunnel ipsec 0
```

  This can be used to for example have a service tunnel that you want to enable from digital in. In that case you just create a digital in trigger and connect it to the action created above. When the trigger is “true”, the VPN tunnel will be enabled.

  It is also possible to retrain the tunnel, to not keep it in error state, this is useful if you want to restart the tunnel on an event:

```
example:/config/alarm/action-4/#> retrain interval 30
```

5.19 PPPoE Server

PPPoE *server* support is available from the CLI only. This allows a WeOS unit to serve up to 16 PPPoE clients, using a local user database for client authentication and authorisation.

By default, the PPPoE server will have address `10.2.0.1`, and hand out addresses in the range `10.2.0.2 - 10.2.0.9`, but this can easily be changed, as is illustrated in the following example:

```
example:/config/pppoe-0/#> server                    (Enables PPPoE server)
example:/config/pppoe-0/#> address 1.2.3.4           (Set local IP address)
example:/config/pppoe-0/#> pool 1.2.3.10 10                    (Using size)
example:/config/pppoe-0/#> pool 1.2.3.10 1.2.3.19             (Using range)
```

Use local user database ”0” to authenticate/authorise PPPoE clients:

```
example:/config/pppoe-0/#> aaa-auth local-db 0
```

5.20 Serial HDX Mode

Serial HDX mode, to handle legacy Serial – V.23 HDX application/equipment with RTS/CTS and DCD control on serial port devices like the Lynx, Wolverine and the Falcon. Currently available from the CLI only.

```
example:/config/serial-1/#> hdx                      (Enable HDX mode)
example:/config/serial-1/#> no hdx
```

This function is limited to handle RTS-CTS delay of 23 ms and a guard time for the DCD signal of 10 ms. By default, serial HDX mode is disabled.

5.21 DHCP Client ”ARP Ping” Option

This allows a WeOS unit to disable the “ARP ping” setting in the DHCP client.


```
example:/config/iface/vlan-1/#> no arping                    (Disable ARP ping)
example:/config/iface/vlan-1/#> arping                       (Default, enabled)
```

If the arping setting is disabled, the DHCP client in WeOS sets the IP address assigned by the DHCP server without first performing an ARP ping of the new IP Address.

By default, the arping option is enabled.

5.22 Support for Disabling DHCP Snooping in DHCP Relay Agent

The MV88E6097 chipset has a bug in its DHCP snooping functionality where it can mistake UDP fragments for DHCP frames. Customers have reported this as an issue when using the Network File System (NFS). As of WeOS 4.15.0 there exist a CLI only setting in the DHCP relay agent to disable the DHCP snooping feature of the MV88E6097 chipset on a per-port basis.

```
example:/config/dhcp-relay/#> option82
example:/config/dhcp-relay/#> port eth 1
example:/config/dhcp-relay/port-eth1/#> no snooping          (Default, enabled)
```

The problem with disabling DHCP snooping is that in "flat" networks where the DHCP client, relay and server are in the same broadcast domain (same LAN). The DHCP server will receive two DHCP requests from the client. The recommended workaround is to run the DHCP server on a different port, e.g. 6767, and have the relay agent forward all requests to the server on that port. That way the server will ignore broadcasted DHCP requests. However, this requires that all client requests pass through a relay agent, which in many setups may not be possible.

5.23 Firewall Conntrack Flushing

This CLI only feature controls automatic flushing of the firewall connection tracking mechanism on route changes.

The connection tracking mechanism is an optimisation in the firewall. Firewall rules are only evaluated once per connection, and are placed in a cache. This cache speeds things up for the rest of the packets belonging to the same session.

This may have some side effects if dynamic routing is enabled. A deny rule on a specific interface may not be respected if a connection is enabled through some other interface and then moves to the interface through dynamic routing events.

Enabling automatic flushing on route events makes traffic to be re-evaluated in the firewall at route changes, thus solving this problem.

Note: NAT also uses the same connection tracking cache for its internal state. Flushing the cache may result in that existing *NAT:ed connections can break and reset*. Please use with care!

Since WeOS 4.14.2, this setting *flushes everything* in the connection tracking cache at routing events. This feature will be changed in a future version to enable a more selective flushing that will avoid flushing connections that are not affected by a specific routing change.

```
example:/config/ip/firewall/#> conntrack-flush routes     (Flush at route events)
example:/config/ip/firewall/#> conntrack-flush auto       (Default, no flushing)
```

5.24 RSTP Support for VLAN Tagging of BPDUs

WeOS 4.15.1 introduced very experimental support for transmitting VLAN tagged RSTP frames (BPDU's). This can be used to interface with equipment from other manufacturers on a limited set of ports.

```
example:/config/spanning-tree/#> stp-port 1                    (Select port/ports)
example:/config/spanning-tree/stp-port-eth1/#> vid 1234  (Set VLAN tag 1234 on all BPDU's)
```

This feature does not affect reception of RSTP BPDUs, nor does it introduce support for RSTP per VLAN, or any similar variant offered by other manufacturers. All it does is on a per-port basis enable a WeOS device to add an IEEE 802.1Q VLAN tag to all BPDUs egressing an RSTP port.

At this point it is unclear if this feature will ever become anything more than a technology preview. Instead, later versions of WeOS are more likely to add actual RSTP per VLAN support, or even true MSTP.

5.25 Remote IO Support for Digital Output

WeOS 4.18.0 introduced support for remote control of the digital output. The remote control is done via CGI web requests. WeOS 4.19.0 added SNMP trap for remote IO control.

The remote IO control is by default inactive and need to be configured and enabled before use. You also need to configure the alarm and trigger with Remote IO to activate the digital output.

Example of how to enable Remote IO via CLI configuration:

```
example:/config/#> alarm
example:/config/alarm#> trigger rio-cgi
example:/config/alarm/trigger-2#> leave
```

Alarm action 1 is used unless an other action is set. The standard configuration action 1 sets the digital out as one of its targets.

The digital output is active for a certain time. For making the output active for 25000 milliseconds (25 s) request this URL:

```
http://192.168.2.200/cgi-bin/adm/io?timer1=25000
```


5.26 Storm Control

In WeOS 4.18.0 the tech preview storm control alarm was introduced. Storm control consists of a trigger (storm-detect) and an action (shutdown-port). The storm-detect trigger monitors the traffic (frames per second) for a selected port. If the traffic count exceeded the threshold the trigger will activate the selected alarm action. The storm-detect trigger can be made persistent. The action shutdown-port disables a selected port.

In WeOS 4.20.0 the storm control feature remains a tech preview but has been changed slightly:

- The feature has been temporarily limited to Lynx-family devices.
- The action has been renamed to 'port' (from 'shutdown-port')

When applying storm control to the network, the network has to be set up to minimize disturbances from the storm. E.g. the following settings on other devices in the network has to be considered:

- CPU-bandwidth limiting should be set on the devices where storm control is set up.
- FDB aging-timeout, since a storm may replace correct FDB entries and thus traffic may be directed the wrong way.

Also note that use of the *1100-0148 SFP* will disturb the storm-control functionality in the device and the pertinent SFP is not recommended for use together with storm control.

Example of a storm-control configuration via CLI.:

```
example:/config/#> alarm
example:/config/alarm/#> action 2
example:/config/alarm/action-2/#> target port led
example:/config/alarm/action-2/#> end
example:/config/alarm/#> trigger storm-detect
example:/config/alarm/trigger-2/#> action 2
example:/config/alarm/trigger-2/#> port 1-2
example:/config/alarm/trigger-2/#> persistent 300
example:/config/alarm/trigger-2/#> threshold 500
example:/config/alarm/trigger-2/#> end
example:/config/alarm/#> show
Trigger  Type          Enabled    Action  Source
================================================================================
      1  frnt          YES             1  Instance 1
      2  storm-detect  YES             2  1-2

Action  Targets
================================================================================
      1  snmp log led digout
      2  log led port
```

6 Accessing the Command Line Interface

The RedFox switch supports a classic Command Line Interface (CLI) that can be accessed via the console port at 115200@8N1 or Secure Shell (SSH), for details see the Secure Shell RFC4251. WeOS supports protocol version 2 only.

Issue `help` or `show tutorial` at the prompt to access the built–in help and tutorials. See the WeOS Management Guide for more information.

Recommended Clients

UNIX OpenSSH, `http://www.openssh.com`

Win32 PuTTY, `http://www.chiark.greenend.org.uk/~sgtatham/putty/`, note that PuTTY is also useful for connecting to serial port consoles.

Please follow the directions for installation and usage applicable to your system and client.

Logging In

To gain access to the CLI you need:

- An SSH client
- The switch IP#
- The user name and password

Units shipping with WeOS have by default all ports assigned untagged to VLAN 1[3], and is configured to acquire an IP address via DHCP, but also with a static IP address: 192.168.2.200 with netmask 255.255.255.0. The unit's will also be reachable via a link-local address, i.e, an address in range 169.254.x.x (where 'x' is a number 0-255).

Use the WeConfig tool, an LLDP client or nmap to find your device. If you have a DHCP server available you can set it up to hand out a known IP addresses for the registered devices MAC addresses. Each unit comes with 16 or 32 MAC addresses assigned, depending on the port count, the base address should be printed on the box and on the unit itself.

The unit is fairly quick to boot, in under 10 seconds is the unit up requesting an IP address — depending on the existence of a DHCP server the fall back to link–local address can take a while. To be on the safe side while scanning for your device, expect it to take anything from 30 seconds to one minute after power–on.

[3]Falcon units come with a slightly different factory configuration. The Ethernet ports on Falcon belong to VLAN1 and are reachable via IP address 192.168.2.200. The xDSL port belongs to VLAN1006 and use DHCP for address assignment.

The following example illustrates how to login to the switch using OpenSSH from a GNU/Linux based host system. The process is similar with PuTTY or other SSH clients.

The operator lists the running configuration with the command `show running`, an overview of ports, vlans and interfaces is available by typing `show ports`, `show vlans` and `show ifaces`. See the `help` or the `show tutorial` for more on line help.

To change some settings, enter the configuration context with the command `conf`, short for "configure". The same commands as shown above also apply here, but now display configured settings.

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

To leave a level the operator must use the command `end` to save and `abort` to cancel.

Any new settings are activated only when the operator leaves the configuration context, using "end".

To save settings to non–volatile RAM (flash disk), the operation uses `copy run start` from admin–exec context.

```
$ ping -b 192.168.2.255
PING 192.168.2.255 (192.168.2.255) 56(84) bytes of data.
64 bytes from 192.168.2.200: icmp_seq=1 ttl=64 time=10.4 ms
64 bytes from 192.168.2.200: icmp_seq=2 ttl=64 time=0.895 ms
^C

$ swping -i eth1
Nr  MAC                IP                   Ver. Type               Status
================================================================================
  1  00:07:7c:86:04:b5  192.168.2.200/24    4.09 RedFox         ------------SI

$ ssh admin@192.168.2.200
The authenticity of host '192.168.2.200 (192.168.2.200)' can't be established.
RSA key fingerprint is 1d:ce:fe:4b:8e:c2:73:42:11:68:73:02:e5:a6:e4:8b.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.2.200' (RSA) to the list of known hosts.
admin@192.168.2.200's password: westermo

.--.--.--.-----.-----.------.-----.-.--.--------.-----.
|  |  |  |  -__|__ --|_    _|  -__|   _|  .  .  |  _  | http://www.westermo.com
 \__/\__/|_____|_____| |__| |_____|__| |__|__|__|_____|        info@westermo.se
   Robust Industrial Data Communications -- Made Easy

\\/ Westermo WeOS 4.9.2 4.9.2 -- Oct  2 16:01 CEST 2012
Type: 'help' for help with commands, 'exit' to logout or leave a context.
example:/#> ^D
$
```

This is a typical session where broadcast ping is first used to locate the device, followed by an IPConfig scan and then SSH login using the default user and password.

7 Firmware Upgrade

Firmware upgrade is supported from the CLI, Web and IPConfig tool. All of them support FTP/TFTP upgrade, but the Web also supports CGI upload from the browser – making it the ultimate choice if you have no FTP/TFTP server available or do not care to set one up.

The version string listed in the output from the `show system-information` command is only updated after reboot.

7.1 What Firmware Image to Use

The image file names are currently limited in length to what the IPConfig tool is capable of handling. This is an intermediate limitation before introducing support for longer human–readable file names in a future IPConfig replacement. The file names are built around the product name and the model, or operating system, it is based upon.

Since version 4.13.1 of WeOS, unified firmware package files are supported. However, it is important to note that a device must first be upgraded to version 4.13.1, using a traditional image file, before package files can be used to upgrade to later versions. WeOS will detect the input image format, so the upgrade procedure is the same when using package files as when using the old format. This applies to both the CLI and the Web interface.

Package Files

List of primary and secondary CPU firmware packages. Bootloader included.

WeOS-4.28.3.pkg: All products, WeOS 4.28.3

Boot Loader

The boot loader firmware can only be upgraded from the CLI. The current version (updated at boot) is visible in the output from the `show system-information` command.

Please note, the boot loader firmware does not follow the WeOS version numbers, it has its own version numbering scheme and it is CPU platform specific. Also, unless the release notes explicitly recommends it, there is no need to upgrade the boot loader.

Current bootloader firmware images:

xscale-redboot-2.03.bin: RedFox

barebox-2017.12.0-3.bin: All other devices

`example:/#> upgrade boot <ip-addr> <firmware>` to upgrade the bootloader.

7.2 Upgrading Early Redfox Units to 4.3.0 or Later

Early RedFox units (Industrial and Rail) delivered with WeOS 4.0.0, comes with a flash memory partition unsuitable for the larger firmware image size of WeOS 4.3.0 and later.

You find information on your product's type of *model*, *article number*, and *serial number* via the Web interface (Menu path: Home ⇒ Details), or via the CLI `show system-information` command.

Model	Article number	Serial number
RFI-18-F4G-T4G	3641-3300	< 1190
RFI-14P-F4G	3641-3200	< 1180
RFI-10P	3641-3110	< 1220
RFI-18P	3641-3100	< 1111

Table 6: Affected RedFox models.

See the management guide for details on how to safely upgrade the system flash table.

7.3 Upgrading Viper 12A and 20A

All Viper 12A and 20A need to be upgraded to WeOS 4.21.3 before upgrading to 4.22.0 if upgrading from Web or CLI.

7.4 Upgrading from the CLI

To be able to upgrade the switch firmware the user must install and run an FTP server or a TFTP server on a network connected to the device. The (T)FTP upgrade uses anonymous login with the password 'support@westermo.se'.

The example below shows that the upgrade command, in CLI, Web and IPConfig first tries FTP and then TFTP, should the FTP connection fail.

```
example:/#> upgrade primary 192.168.2.3 WeOS-4.13.1.pkg

==> Upgrade in progress, console disabled.  Please stand by ... <==

Connecting to 192.168.2.3:21 (192.168.2.3:21)
WeOS-4.13.1.pkg      100% |*******************************| 58549k  0:00:00 ETA

Checking download ...
Unpacking weos (from /upgrade/download)...
Setting up weos (4.13.1-1)...
```



```
Checking rw4131.img ...
   Type: CramFS
     ID: OK (RFox)
   Size: OK
    CRC: OK 0xD5A84E26

Flashing currently active MTD partition, reboot is forced.

Flashing /dev/mtd1 ...
100% \ [=======================================================================]

Updating RedBoot directory with new CRC ...
100% | [=======================================================================]

Done.

Rebooting system ...
Restarting system.
```

The system will force a reboot when upgrading the primary image. This to protect against flash corruption issues seen in earlier releases, caused by simultaneous access to the flash during programming or when starting new processes after upgrade.

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

This is how far the release notes goes, please see the management guide for details. Or get in touch with your local distributor, or Westermo for any questions, support or course material.