

Prepared by Magnus Öberg, Mattias Walström	Document Release Notes WeOS 4.16.0	
Approved by Jonas Nylander	Date February 11, 2015	Document No 089604-g9439795

## Release Notes WeOS 4.16.0

### Contents

<b>1</b>	<b>News</b>	<b>5</b>
<b>2</b>	<b>Summary of Changes</b>	<b>6</b>
2.1	gethostbyname security issue “GHOST” . . . . .	6
2.2	WeConnect . . . . .	6
2.3	TLS Authentication support for SSL VPN tunnels . . . . .	6
<b>3</b>	<b>Technology Previews</b>	<b>8</b>
3.1	Password Encryption . . . . .	8
3.2	Interface Always Up . . . . .	9
3.3	Interface Admin Distance Trigger . . . . .	9
3.4	Interface Gateway . . . . .	10
3.5	SFP DDM Alarm . . . . .	10
3.6	Serial Low Latency . . . . .	10
3.7	SNMP RIPv2-MIB and OSPF-MIB . . . . .	12
3.8	NTP Server (with GPS time-base support) . . . . .	12
3.9	TFTP Server . . . . .	13
3.10	Preferred (remote) NTP server . . . . .	13
3.11	Guest User . . . . .	13
3.12	New VLAN Features . . . . .	14
3.13	Packet Capture – Tcpdump . . . . .	14
3.14	CLI Welcome Message . . . . .	14
3.15	Custom HTTPS certificates . . . . .	15
3.16	Additional DDNS features . . . . .	15
3.17	USB functionality . . . . .	17
3.18	VPN . . . . .	17
3.19	IEEE 802.1AX/802.3ad Link aggregation . . . . .	18
3.20	PPPoE Server . . . . .	19
3.21	Serial HDX mode . . . . .	19

Prepared by Magnus Öberg, Mattias Walström	Document Release Notes WeOS 4.16.0	
Approved by Jonas Nylander	Date February 11, 2015	Document No 089604-g9439795

3.22	DHCP client “ARP ping” option . . . . .	19
3.23	Support for disabling DHCP snooping in DHCP relay agent . . . . .	20
3.24	ICMP redirect control . . . . .	20
3.25	Firewall conntrack flushing . . . . .	21
3.26	RSTP support for VLAN tagging of BPDU’s . . . . .	21
3.27	FRNT support for variable hello-time . . . . .	22
<b>4</b>	<b>Known Limitations</b>	<b>23</b>
4.1	Platform . . . . .	23
4.2	CLI . . . . .	24
4.3	SNMP . . . . .	24
4.4	Web . . . . .	24
4.5	IPConfig Tool . . . . .	24
4.6	SHDSL . . . . .	25
4.7	Firewall . . . . .	25
4.8	IPsec . . . . .	25
4.9	SSL VPN . . . . .	25
4.10	Link aggregation . . . . .	26
4.11	Serial Over IP . . . . .	26
4.12	Software Upgrade . . . . .	26
4.13	802.1X . . . . .	26
4.14	Bootstrapping configuration via BOOTP . . . . .	27
4.15	Bandwidth limiting in frames per second . . . . .	27
<b>5</b>	<b>Known Issues</b>	<b>28</b>
<b>6</b>	<b>Fixed Issues</b>	<b>30</b>
<b>7</b>	<b>Accessing the Command Line Interface</b>	<b>32</b>
<b>8</b>	<b>Firmware Upgrade</b>	<b>35</b>
8.1	What Firmware Image to Use . . . . .	35
8.2	Upgrading early RedFox units to 4.3.0 or later . . . . .	36
8.3	Upgrading From the CLI . . . . .	36

Prepared by Magnus Öberg, Mattias Walström	Document Release Notes WeOS 4.16.0	
Approved by Jonas Nylander	Date February 11, 2015	Document No 089604-g9439795

## About

Westermo WeOS is a network operating system designed for industrial grade rugged Ethernet switches and routers. Fully supporting RedFox, 2<sup>nd</sup> 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://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.

## 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 3.1

Prepared by Magnus Öberg, Mattias Walström	Document Release Notes WeOS 4.16.0	
Approved by Jonas Nylander	Date February 11, 2015	Document No 089604-g9439795

- *Interface Always Up*: CLI only, expert level setting, section 3.2
- *Trigger to control Interface Admin Distance*: CLI only, section 3.3
- *Setting default gateway per interface*: CLI only, section 3.4)
- *SFP DDM Alarm and SNMP Trap Support*: Alarm settings in CLI only, section 3.5
- *Serial Low Latency*: CLI only, section 3.6
- *SNMP MIBs for RIP and OSPF*: See section 3.7
- *NTP Server with GPS support*: CLI only, section 3.8
- *TFTP Server*: CLI only, section 3.9
- *Preferred (remote) NTP server*: CLI only, section 3.10
- *Guest User*: CLI only, section 3.11
- *New VLAN Features*: CLI only support for disabling 'secure' mode and MAC address learning. See section 3.12
- *Tcpdump*: CLI only. See section 3.13
- *CLI welcome message*: Ability to set custom CLI welcome message. See section 3.14
- *Certificate handling, import/export in WebUI*: See section 3.15
- *Additional DDNS features*: See section 3.16
- *USB boot*: CLI only, section 3.17. Separate feature from "USB Autobackup/restore" and "USB Configuration Deployment"!
- *IPsec Backup Peer*: IPsec initiators may now be configured with two responder addresses, section 3.18
- *L2TP/IPsec and PPTP VPNs for mobile phone access*: Server only, CLI only. See section 3.18
- *Enable/disable IPsec and SSL VPN tunnels via alarm trigger and action*, section 3.18
- *IEEE 802.1AX/802.3ad Link aggregation with FLHP link qualification*: See section 3.19
- *IEEE 802.1AX/802.3ad Link aggregation over SHDSL links*: See section 3.19
- *PPPoE Server*: CLI only, section 3.20
- *Serial HDX mode*: CLI only, ,section 3.21
- *DHCP client arping option*: CLI only, section 3.22
- *Support for disabling DHCP snooping in DHCP relay agent*: CLI only, section 3.23

Prepared by Magnus Öberg, Mattias Walström	Document Release Notes WeOS 4.16.0	
Approved by Jonas Nylander	Date February 11, 2015	Document No 089604-g9439795

- *ICMP redirect control*: CLI only, section 3.24
- *Firewall conntrack flushing*: CLI only, section 3.25
- *RSTP support for VLAN tagging of BPDU's*: CLI only, section 3.26
- *FRNT support for variable hello-time*: CLI only, section 3.27

Prepared by Magnus Öberg, Mattias Walström	Document Release Notes WeOS 4.16.0	
Approved by Jonas Nylander	Date February 11, 2015	Document No 089604-g9439795

## 1 News

The main additions in WeOS 4.16 are the support for the Westermo cloud VPN service, "WeConnect" and TLS authentication. WeOS 4.16 also introduces two tech previews, "Interface Always Up" (see section 3.2) and "FRNT support for variable hello-time" (see section 3.27).

More changes and additions are listed below. Also, see section 6, for details on bug fixes and other changes not mentioned here.

Prepared by Magnus Öberg, Mattias Walström	Document Release Notes WeOS 4.16.0	
Approved by Jonas Nylander	Date February 11, 2015	Document No 089604-g9439795

## 2 Summary of Changes

### 2.1 gethostbyname security issue “GHOST”

WeOS 4.16.0 fixes a security problem in the `gethostbyname()` family of functions in `glibc`. The bug is described in CVE-2015-0235 and has also been nicknamed "GHOST".

WeOS 4.12.0 to 4.15.3 have vulnerable versions of `glibc` installed. Our recommendation is to upgrade to WeOS-4.16.0 where this bug is fixed.

### 2.2 WeConnect

WeOS 4.16 introduces support for the Westermo cloud VPN service, “WeConnect”. WeConnect is a service that is sold separately, and can be used to connect sites and clients with each other in an easy and secure way. Please see our home page at: <http://www.westermo.com> for information about ordering this service and for additional information. There is also some WeOS specific information in the management guide.

WeConnect is managed with an on-line web portal where networks, clients and nodes are defined. A Secure Network Code and a One Time Password will be created in the portal and this information is entered into the WeConnect installation guide in WeOS. WeOS will do a secured download and configure everything needed to connect to the service automatically.

The WeConnect installer is available in the web interface under the menu “WeConnect”. It is also available in a CLI version invoked like this:

```
router:/#> weconnect
```

Note that this is not done inside the normal configuration, but as its own command at the exec prompt.

### 2.3 TLS Authentication support for SSL VPN tunnels

WeOS 4.16.0 adds the possibility to add extra security and resilience for DDOS attacks by enabling TLS Authentication for a SSL VPN tunnel.

An extra crypto key is used to sign all control traffic involved in the SSL VPN protocol on both sides of the tunnel. Incoming VPN traffic will be checked with this extra key, and the traffic is immediately discarded if the signature does not match.

This increases the security and has the positive side effect of adding some protection against DDOS attacks. The attacker’s traffic will be discarded immediately as it is not signed by the key. Used

Prepared by Magnus Öberg, Mattias Walström	Document Release Notes WeOS 4.16.0	
Approved by Jonas Nylander	Date February 11, 2015	Document No 089604-g9439795

in combination with the UDP protocol mode in SSL VPN, your unit also becomes undetectable by probing attempts i.e. port scanning.



Prepared by Magnus Öberg, Mattias Walström	Document Release Notes WeOS 4.16.0	
Approved by Jonas Nylander	Date February 11, 2015	Document No 089604-g9439795

## 3 Technology Previews

### 3.1 Password Encryption

A much requested feature of other manufacturers is the ability to encrypt passwords in the configuration. In WeOS 4.15.0 tech-preview (CLI only) support for this has been added. Web support for enabling this feature, and thus making it official, is expected in the next major WeOS release.

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<sup>1</sup> 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)
example:/config/#> leave
example:/#> copy run start
```

---

<sup>1</sup>The custom key is in itself encrypted before stored in a file on built-in flash.

Prepared by Magnus Öberg, Mattias Walström	Document Release Notes WeOS 4.16.0	
Approved by Jonas Nylander	Date February 11, 2015	Document No 089604-g9439795

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.

## 3.2 Interface Always Up

This is an expert level setting to disable the link propagation from physical access ports to VLAN interfaces. This setting is exclusively reserved for a few selected use-cases and can only be controlled from the CLI.

When the interface is set as 'always' enabled the setting cannot be disabled from the WebUI and the SNMP `ifAdminStatus` will show `Testing(3)`.

```
example:/config/iface-vlan1/#> enable always
```

This setting may significantly impact layer-3 protocols such as RIP, OSPF, VRRP, and more – the protocols will have to fall-back to other methods to detect link-down, e.g. hello message timeout and similar. Do not use this setting unless you really know what you are doing.

## 3.3 Interface Admin Distance Trigger

The new multiple upstream feature works great as long as the device can get link down. In most cases, however, you unfortunately do not get link down. To this end it is possible to adjust the interface distance dynamically using a ping trigger. As long as the ping reaches a target via the interface in question the distance remains at its configured setting, but when the trigger fires the distance is automatically adjusted to 255 (infinity) for the associated default route.

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

Make sure to setup 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.

Prepared by Magnus Öberg, Mattias Walström	Document Release Notes WeOS 4.16.0	
Approved by Jonas Nylander	Date February 11, 2015	Document No 089604-g9439795

### 3.4 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**.

### 3.5 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)
```

### 3.6 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:

Prepared by Magnus Öberg, Mattias Walström	Document Release Notes WeOS 4.16.0	
Approved by Jonas Nylander	Date February 11, 2015	Document No 089604-g9439795

```
example:/config/#> seroip 1
example:/config/seroip-1/#> mode serialllowlatency
example:/config/seroip-1/#> port <SERIAL-PORT>
example:/config/seroip-1/#> remote-frame-delay
example:/config/seroip-1/#> remote-frame-delay <0-2147483647> (0..231)
example:/config/seroip-1/#> remote-frame-size <0-512>
example:/config/seroip-1/#> local-frame-delay <0-2147483647> (0..231)
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.

Prepared by Magnus Öberg, Mattias Walström	Document Release Notes WeOS 4.16.0	
Approved by Jonas Nylander	Date February 11, 2015	Document No 089604-g9439795

### 3.7 SNMP RIPv2-MIB and OSPF-MIB

Tech preview support of SNMP MIBs:

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

### 3.8 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 part 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 use 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.

Prepared by Magnus Öberg, Mattias Walström	Document Release Notes WeOS 4.16.0	
Approved by Jonas Nylander	Date February 11, 2015	Document No 089604-g9439795

### 3.9 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://
```

### 3.10 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
```

### 3.11 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.

Prepared by Magnus Öberg, Mattias Walström	Document Release Notes WeOS 4.16.0	
Approved by Jonas Nylander	Date February 11, 2015	Document No 089604-g9439795

### 3.12 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<sup>2</sup> VLAN tag is silently dropped.

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
```

### 3.13 Packet Capture – Tcpcap

Previously only available to developers and support personnel, this release now adds support for the tcpcap 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 tcpcap 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:/#> tcpcap vlan1
```

### 3.14 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>
```

---

<sup>2</sup>I.e., a VLAN ID not configured for the given port, in either tagged or untagged mode.

Prepared by Magnus Öberg, Mattias Walström	Document Release Notes WeOS 4.16.0	
Approved by Jonas Nylander	Date February 11, 2015	Document No 089604-g9439795

- **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."
```

### 3.15 Custom HTTPS certificates

Tech preview of custom certificates for HTTPS. This allows you to upload your own certificates and they will be used in the HTTPS traffic. Useful if you want to remove all certificate warnings in a unified network environment. If not specified, the default Westermo self-signed certificates will be used. Only supported from the CLI.

```
example:/config/web/#> certificate <LABEL>
```

### 3.16 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)



Prepared by Magnus Öberg, Mattias Walström	Document Release Notes WeOS 4.16.0	
Approved by Jonas Nylander	Date February 11, 2015	Document No 089604-g9439795

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.

Prepared by Magnus Öberg, Mattias Walström	Document Release Notes WeOS 4.16.0	
Approved by Jonas Nylander	Date February 11, 2015	Document No 089604-g9439795

### 3.17 USB functionality

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
```

### 3.18 VPN

- Import an SSL tunnel using a OpenVPN configuration file This can configure up a SSL VPN tunnel in WeOS using a standard OpenVPN configuration file (.ovpn) either with the certificates 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
```

- Tech preview of upcoming *PPTP* support, server only. See the online help for more details.

```
example:/config/tunnel/#> pptp
```

Some clients (for example iPhone) has the option to send all traffic through the tunnel. To get this to work you need to add a name server in the PPTP configuration.

```
example:/config/tunnel/pptp/#> ppp name-server 8.8.8.8
```

It is possible to configure firewall rules that will apply on all connected clients, not on each client, for example:

```
example:/config/ip/firewall/#> filter allow in pptp0 proto icmp
```

Prepared by Magnus Öberg, Mattias Walström	Document Release Notes WeOS 4.16.0	
Approved by Jonas Nylander	Date February 11, 2015	Document No 089604-g9439795

- Tech preview of upcoming *L2TP/IPsec* support, server only. See the online help for more details.

```
example:/config/tunnel/#> pptp
```

or

```
example:/config/tunnel/#> l2tp  
example:/config/tunnel/l2tp/#> ipsec
```

Some clients, e.g., iPhone, has the option to send all traffic through the tunnel. To get this to work you need to add a name-server in the L2TP configuration.

```
example:/config/tunnel/l2tp/#> ppp name-server 8.8.8.8
```

It is possible to configure firewall rules that will apply on all connected clients, not on each client, for example:

```
example:/config/ip/firewall/#> filter allow in l2tp0 proto icmp
```

- 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
```

### 3.19 IEEE 802.1AX/802.3ad Link aggregation

FLHP is a Westermo proprietary protocol used to qualify if a link has full connectivity and can be used to qualify if a link should be a member of an aggregate. It is only at technology preview function and is not a supported function.

As a technology preview it is possible to use 802.1AX link aggregation on SHDSL links. Note: On SHDSL products with PAF support, it is recommended to use PAF instead. LACP link aggregation does not work for DSL ports on DDW-142.

Prepared by Magnus Öberg, Mattias Walström	Document Release Notes WeOS 4.16.0	
Approved by Jonas Nylander	Date February 11, 2015	Document No 089604-g9439795

### 3.20 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
```

### 3.21 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.

### 3.22 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.

Prepared by Magnus Öberg, Mattias Walström	Document Release Notes WeOS 4.16.0	
Approved by Jonas Nylander	Date February 11, 2015	Document No 089604-g9439795

### 3.23 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.

### 3.24 ICMP redirect control

This CLI only setting allows ICMP redirects to be disabled per interface. It only controls the sending of ICMP redirects. WeOS currently never accept incoming ICMP redirects, but this may change in future versions.

```
example:/config/#> iface vlan1
example:/config/iface-vlan1/#> no redirect (Disable ICMP redirect)
example:/config/iface-vlan1/#> redirect (Default, enabled)
```

The default WeOS behaviour is to send ICMP redirect messages if a more direct route is detected on the network. This is an optimisation to avoid excess routing hops within a local area network.

ICMP redirection may cause some confusion if you are debugging a network as it overrides the configured next-hops.

Disabling ICMP redirect may also be useful if you have equipment in your network that handles ICMP redirect in a bad or incomplete way.

Prepared by Magnus Öberg, Mattias Walström	Document Release Notes WeOS 4.16.0	
Approved by Jonas Nylander	Date February 11, 2015	Document No 089604-g9439795

### 3.25 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 v4.14.2, 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)
```

### 3.26 RSTP support for VLAN tagging of BPDU's

WeOS 4.15.1 has 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 BPDU's, 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 BPDU's 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.

Prepared by Magnus Öberg, Mattias Walström	Document Release Notes WeOS 4.16.0	
Approved by Jonas Nylander	Date February 11, 2015	Document No 089604-g9439795

### 3.27 FRNT support for variable hello-time

WeOS 4.16.0 has support for changing the time of how often the hello packet will be transmitted. The hello time can be changed between 20 ms up to 1 second individually for each FRNT ring port. This feature will improve reconfiguration time at link down when link change detection is slow, i.e DSL, Giga bit copper links. The maximum expected reconfiguration time at link down is around 5 x hello time when relying only on hello packets.

When lowering the FRNT Hello time below the default time of 100 ms, we recommend limiting the CPU bandwidth to approximately 256 kbit/s. This may be done automatically in future releases but this limit will also limit the routing performance so now it has to be configured manually.

Syntax:

```
[no] hello-time <20-1000,20-1000>
```

Example: /config/frnt-1/#> hello-time 50,500

Prepared by Magnus Öberg, Mattias Walström	Document Release Notes WeOS 4.16.0	
Approved by Jonas Nylander	Date February 11, 2015	Document No 089604-g9439795

## 4 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.

### 4.1 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.



Prepared by Magnus Öberg, Mattias Walström	Document Release Notes WeOS 4.16.0	
Approved by Jonas Nylander	Date February 11, 2015	Document No 089604-g9439795

## 4.2 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.

## 4.3 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.

## 4.4 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.

## 4.5 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.

Prepared by Magnus Öberg, Mattias Walström	Document Release Notes WeOS 4.16.0	
Approved by Jonas Nylander	Date February 11, 2015	Document No 089604-g9439795

## 4.6 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).

## 4.7 Firewall

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

## 4.8 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 (configured with clear) is rebooted, the tunnel will sometimes not be renegotiated. This is planned to be fixed in future WeOS releases.  
**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:** 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 3.18) 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.

## 4.9 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.

Prepared by Magnus Öberg, Mattias Walström	Document Release Notes WeOS 4.16.0	
Approved by Jonas Nylander	Date February 11, 2015	Document No 089604-g9439795

- 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.

#### 4.10 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.

#### 4.11 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.

#### 4.12 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.

#### 4.13 802.1X

- 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.

Prepared by Magnus Öberg, Mattias Walström	Document Release Notes WeOS 4.16.0	
Approved by Jonas Nylander	Date February 11, 2015	Document No 089604-g9439795

#### 4.14 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).

#### 4.15 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.

Prepared by Magnus Öberg, Mattias Walström	Document Release Notes WeOS 4.16.0	
Approved by Jonas Nylander	Date February 11, 2015	Document No 089604-g9439795

## 5 Known Issues

Issue	Category	Description
#4203	RSTP	Storm occurs quite frequently when toggling RSTP bridge priority
#4462	Ports	Cross switchcore 802.3x flow control
#4707	RSTP	Long reconfiguration time for RSTP at link up, up to 32 sec
#4895	RSTP	RSTP show blocked port on LED when port is in forwarding state
#4929	RSTP	Looping admin edge ports causing a storm
#5649	RSTP	Non root switch sends out BPDUs with the same bridge ID as the root
#5987	VPN	IPsec: Wayward ARP caused by IPsec added route
#6180	System	RedFox 8FX: System instability issues with 1000Mbps fiber in 100Mbps SFP slot
#6223	Ports	Unit crashes when traffic is looped back to the interface it came from
#6268	FRNT	Long FRNT reconfiguration time for Wolverine units on power-up
#6920	PPP	PPPoE termination message (PADT) from server not handled properly
#7275	System	Fiber patch cable connected to 100 Mbps in one end and 1000 Mbps in the other cause complete systems lockup
#7276	VPN	IPsec "no remote network" causes NAPT rules to be bypassed
#7322	USB	USB autobackup/restore can restore configuration of a Lynx to a RedFox => FAIL
#7367	System	Bad response from DynDNS server may prevent the DNS name from being updated
#7453	PoE	Viper sometimes fails to toggle ports during over-allocation of power
#7500	VPN	IPsec with certificates and identity using 'auto' will not work
#8093	System	Broken USB-stick causes failure in WeOS
#8251	Serial over IP	Sender of UDP broadcast also receives transmitted data
#8260	VLAN	Removing forbid on dynamic vlans not working
#8286	Link Aggregation	Combining dynamic VLANs (AVT) and link aggregates does not work
#8373	System	Moving the 1100-0148 SFP causes an interrupt storm
#8451	Ports	Interrupted availability due to large packets - DDW-226
#8784	System	Compatibility issues with MRD and DR units for VRRP
#9214	SNMP	SNMP ifOutDiscards is a 16 bit value but should be counter type
#9295	VPN	VPN performance on 1500 byte packets suffers from minor packet loss on the MPC85xx platform
#9431	DHCP	DHCP server does not assign option 82 address to unit replacement until lease times out

Prepared by Magnus Öberg, Mattias Walström	Document Release Notes WeOS 4.16.0	
Approved by Jonas Nylander	Date February 11, 2015	Document No 089604-g9439795

Issue	Category	Description
#9514	FRNT	FRNT not stable when on 32 kbit/s SHDSL link with traffic load
#9564	RSTP	RSTP not always blocking ports
#9875	System	MAC authentication in combination with RSTP is unpredictable
#9909	Link Aggregation	LACP: Changing aggregate type may cause ports to remain in forward state
#10336	Serial	Serial driver does not always keep data stay together in data packets
#10516	VPN	Let VPN LED for SSL VPN server indicate up only when there is at least one client connected
#10564	DHCP	BOOTP does not work using Option 82
#10569	QoS	Wrong priority for WeOS services.
#10670	Firewall	Configuration of the firewall through an external/routed interface causes loss of connection
#10703	VPN	SSL VPN reports tunnel up, even though parameters are not matching on server and client sides
#10744	Link Aggregation	Link aggregation blocking if disabled ports are re-enabled
#10797	VPN	IPsec backup peer does sometimes not work
#10901	System	The FDB shows different entries when issuing the command <code>sh fdb</code> several times
#11003	Ring coupling	Sometimes long reconfiguration time, 3-4 sec, on quick link changes
#11198	NTP	Multiple remote NTP servers can only be specified via the CLI
#11480	Ring coupling	Inefficient multicast distribution can lead to link saturation
#11577	Firewall	Route associated with NAT rule remains after NAT rule deletion

Prepared by Magnus Öberg, Mattias Walström	Document Release Notes WeOS 4.16.0	
Approved by Jonas Nylander	Date February 11, 2015	Document No 089604-g9439795

## 6 Fixed Issues

### 4.16.0

Fixed issues in WeOS v4.16.0 since v4.15.3

Issue	Category	Description
#11823	Alarm	Digital I/O does not work on RedFox RFIR with AC-power
#11922	System	GHOST Vulnerability CVE-2015-0235
#9235	Serial over IP	Add warning when configuring invalid seroip multicast mode without default gateway
#10785	WEB	Usability: Remove enable/disable from DHCP Relay Option 82 policy dropdown
#10800	Serial over IP	Allow + character as a dial modifier in modem replacement
#10918	WEB	Disabling SSL client causes a 443 port in use warning
#11081	VPN	SSL VPN occasionally retrains at start up
#11214	System	SSH server may crash with segmentation fault
#11215	LLDP	Hostname change is slow to propagate to neighbours.
#11272	Firewall	NAT from GRE not working
#11295	WEB	SNMP v3 user type not displayed and saved correctly
#11319	WEB	OSPF WEB Status Page: Auto Refresh setting unworking
#11358	System	Add support for disabling link propagation for layer-3 VLAN interfaces
#11433	System	DDNS: No update if user manually edits their DNS record at provider
#11449	System	DHCP/OpenVPN/PPPoE sometimes restarts right efter (re)config
#11473	Serial over IP	Serial over IP Multicast breaks at boot
#11488	WEB	Configuring a very large session timeout leads to instant session timeout
#11492	Boot Loader	Factory reset appears to forget cleanup of boot loader settings
#11536	IGMP	IGMP asserts during reconfiguration due to loss of aggregate
#11542	VLAN	Setting "no dot1q" on VLAN1 does not warn that you will lose management access
#11557	CLI	Thrown out from CLI when entering the wrong syntax for FRNT ring ports
#11594	WEB	Rate-limit not activated if set by web
#11595	Link Aggregation	Enabling mirroring on an aggregate port can cause storm
#11610	System	Configured value for SSH idle-timeout and keepalive doesn't match
#11614	System	File descriptor leak in finit v1.8 – used from WeOS 4.13.0 to 4.15.3

Prepared by Magnus Öberg, Mattias Walström	Document Release Notes WeOS 4.16.0	
Approved by Jonas Nylander	Date February 11, 2015	Document No 089604-g9439795

Issue	Category	Description
#11617	CLI	Thrown out from CLI when using upgrade 'force' without a target partition
#11651	WEB	VLAN WebGUI page could do with a better/cleaner layout on RFIR 27 port
#11659	VPN	Test ipsec/supernet_at_responder fails on Audrey
#11690	NTP	NTP web restart button not working
#11696	DHCP	DHCP server without address pool hands out leases from subnet
#11734	System	Double hardware definitions for the RFIR, both 1xx and 2xx has own product_model_numbers.
#11754	WEB	PPPoE web setting accepts a Service-Name with blankspace



Prepared by Magnus Öberg, Mattias Walström	Document Release Notes WeOS 4.16.0	
Approved by Jonas Nylander	Date February 11, 2015	Document No 089604-g9439795

## 7 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<sup>3</sup>, 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

---

<sup>3</sup>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.

Prepared by Magnus Öberg, Mattias Walström	Document Release Notes WeOS 4.16.0	
Approved by Jonas Nylander	Date February 11, 2015	Document No 089604-g9439795

the safe side while scanning for your device, expect it to take anything from 30 seconds to one minute after power-on.

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 v4.9.2 4.9.2 -- Oct  2 16:01 CEST 2012  
Type: 'help' for help with commands, 'exit' to logout or leave a context.
```

Prepared by Magnus Öberg, Mattias Walström	Document Release Notes WeOS 4.16.0	
Approved by Jonas Nylander	Date February 11, 2015	Document No 089604-g9439795

```
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.

Prepared by Magnus Öberg, Mattias Walström	Document Release Notes WeOS 4.16.0	
Approved by Jonas Nylander	Date February 11, 2015	Document No 089604-g9439795

## 8 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.

### 8.1 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-4.16.0.pkg:** All products, WeOS 4.16.0

#### 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:

**imx27-redboot-4.11.bin:** Falcon, Lynx, Viper, Wolverine DDW-142/225/226

Prepared by Magnus Öberg, Mattias Walström	Document Release Notes WeOS 4.16.0	
Approved by Jonas Nylander	Date February 11, 2015	Document No 089604-g9439795

**xscale-redboot-2.03.bin:** RedFox

**ppc-uboot-5.01.bin:** RFR-212-FB

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

## 8.2 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 3: Affected RedFox models.

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

## 8.3 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)...
```

Prepared by <b>Magnus Öberg, Mattias Walström</b>	Document <b>Release Notes WeOS 4.16.0</b>	
Approved by <b>Jonas Nylander</b>	Date <b>February 11, 2015</b>	Document No <b>089604-g9439795</b>

```
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.

Good Luck! //The WeOS Team