Prepared by	Document	
Joachim Nilsson	Release Notes WeOS 4.5.1	
Approved by	Date	Document No
	March 25, 2011	089604-r20885

Release Notes WeOS 4.5.1

Contents

Prepared by	Document	
Joachim Nilsson	Release Notes WeOS 4.5.1	
Approved by	Date	Document No
	March 25, 2011	089604-r20885

1 About

Westermo WeOS is a network operating system specifically designed for industrial grade rugged Ethernet switches and routers. It is based on the Cricket 3rd generation software platform with support for RedFox, 2nd generation Wolverine and Viper, Lynx+ switches, and the Falcon VDSL2 router.

The Linux based platform 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.

Westermo has several projects underway to boost hardware capability to be able to roll out WeOS on even more products than the current offering. There is also a wide range of software features on the road map for WeOS itself.

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

Version Number Format

WeOS version numbers have three digits. The main reason for the third digit is to emphasize 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, which currently is Cricket. 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., 4.5.1 would be the first patch release in the 4.5.0 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 This custom has now been replaced by the more common –betaN notation, for internal and limited distribution beta releases, and –rcN, for release candidates.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.

2 Summary of Changes

WeOS 4.5.0 is the first release with support for the *Lynx+ 110*, the first *WeOS Level 1* type product. Also featured is support for the new *Viper-12*, a rugged M12 connector unit. Another noteworthy item is the support for the new *RedFox 8-FX* 100 Mbps fiber board.

Other notable changes and additions are listed below. Also, see section 5, for details on bug fixes and other changes not mentioned here.

Modem Replacement

Modem replacement is an extension to Serial Over IP. It is an AT command interpreter that allows Serial Over IP connections to be controlled using AT commands. This makes it easier to replace old PSTN or leased line modems with new DSL modems in existing installations.
The Modem replacement supports :

- Mapping PSTN numbers to IP addresses:ports
- Configurable result codes (OK, Error, Connect and disconnect)
- User defined command strings and responses.
- Auto answer of incoming connections (configurable)
- Disabled/enable verbose result codes and echo.
- A limited AT command set

Supported AT commands:

- `ATA` - Answer
- `ATD` - Dial
- `ATE` - Echo
- `ATH` - Hangup
- `ATI` - Identification
- `ATO` - Online
- `ATV` - Verbose

In addition to the supported AT commands, most other common AT commands are valid, but will only respond with OK.

Ping Trigger in Alarm System

A new alarm trigger type, *ping trigger*, is now supported. It can be used to trigger an alarm event when network reachability to a peer IP is lost (or when reachability is achieved).

An example is shown below. Here a *ping trigger* is created to indicate alarm via *digital out* when the peer becomes reachable.

```
lynx:/config/alarm/#> trigger ping
Trigger 2: Peer is mandatory
lynx:/config/alarm/trigger-2/#> peer bbc.co.uk
lynx:/config/alarm/trigger-2/#> number 3
lynx:/config/alarm/trigger-2/#> interval 3
lynx:/config/alarm/trigger-2/#> action 2
lynx:/config/alarm/trigger-2/#> end
lynx:/config/alarm/#> action 2
lynx:/config/alarm/action-2/#> target led
lynx:/config/alarm/action-2/#> end
lynx:/config/alarm/#> show
Trigger Class       Enabled  Action  Source
================================================================================
      1 frnt        YES           1  Ring 1
      2 ping        YES           2  peer bbc.co.uk

Action  Targets
================================================================================
      1  snmp log led digout
      2  log led
================================================================================
Summary alarm traps: Disabled
```

SNMP Summary Alarm Trap and Status

This release adds support for SNMP *summary alarm traps* and *summary alarm status*. The *summary alarm status* is *OK* when all configured alarm sources are *OK*, toggle to *Warning* as soon as any alarm is triggered. When status changes from *OK* to *Warning* a *summaryStatusWarning* trap is sent, and when the status changes to *OK* again a *summaryStatusOK* trap is sent.

The summary alarm status utilises the flexible alarm/event handling system in WeOS, and the status value matches the colour of the unit's front panel status LED, the "ON" LED. When the ON LED turns:

- *Red*, the *summaryAlarmStatus* has value *Warning (1)*, and a *summaryAlarmWarning* trap is sent.
- *Green*, the *summaryAlarmStatus* has value *OK (2)*, and a *summaryAlarmOK* trap is sent.

The intent is that summary alarm traps should be sent **both** when there is a *change* in summary alarm status, **and** when the unit *starts up*. However, currently there exists a bug affecting the ability to send traps at system startup, issue #4017.

The following example uses CLI commands to configure a set of alarm sources to trigger changes in the summary alarm status. The same can of course also be done using the Web interface. Triggers must be set to with the *ON* LED as target in order to affect the summary alarm status. By default new triggers are mapped to *action profile "1"*, which in turn, by default, is setup with all common alarm targets, including the ON LED.

Here alarm triggers for link-alarm (ports 2/1-2/4) and power triggers (DC1 and DC2) are configured to to target the ON LED, thereby also the summary alarm status. It will be *Warning* until DC1 has power, and ports 2/1-2/4 get link-up.

```
redfox:/#> configure
redfox:/config/#> alarm
redfox:/config/alarm/#> trigger link-alarm
redfox:/config/alarm/trigger-2/#> port 2/1-2/4
redfox:/config/alarm/trigger-2/#> end
redfox:/config/alarm/#> trigger power
redfox:/config/alarm/trigger-3/#> end
redfox:/config/alarm/#> show
Trigger Class       Enabled  Action  Source
================================================================================
      1 frnt        YES           1  Ring 1
      2 link-alarm  YES           1  2/1-2/4
      3 power       YES           1  1 2

Action  Targets
================================================================================
      1  snmp log led digout

redfox:/config/alarm/#> end
redfox:/config/#> snmp-server
redfox:/config/snmp/#> trap-host 192.168.2.99
redfox:/config/snmp/#> trapcommunity foobar
redfox:/config/snmp/#> leave
Configuration activated.  Remember "copy run start" to save to flash (NVRAM).
redfox:/#> copy run start
redfox:/#> show alarm
No Trigger      Ena Act Reason
================================================================================
 1 frnt         YES  NO
 2 link-alarm   YES YES Port 2/1 2/2 2/3 2/4  DOWN
 3 power        YES YES DC1 is OFF

redfox:/#>
```

The *summaryStatusWarning* and *summaryStatusOK* traps, as well as the *summaryAlarmStatus* object, are defined WESTERMO-WEOS-MIB:

- Summary Alarm OK OID:
  iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).westermo(16177).common(2).weos(1).notifications(6).genericNotifications(4).genericNotificationPrefix(0).summaryAlarmOK(1)

- Summary Alarm Warning OID:
  iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).westermo(16177).common(2).weos(1).notifications(6).genericNotifications(4).genericNotificationPrefix(0).summaryAlarmWarning(2)

In addition, the summaryAlarmStatus can be read from the unit by regular SNMP-GET operations at the following OID: *iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).westermo(16177).common(2).weos(1).system(5).eventSystem(2).summaryAlarmStatus(1)*

For further details, see the chapters on *"Alarm handling, Front panel LEDs and Digital I/O"* and *"SNMP"* in the WeOS management guide.

Custom Alarm Target Deprecated

In WeOS 4.4.0 a new, very generic, *custom* action for alarms was introduced. It provided a means of performing a system reboot for the new timer trigger.

However, in WeOS 4.5.0 *custom* has been deprecated in favour of dedicated action targets. It is still available in the CLI, but will likely be removed completely in a later release. In 4.5.0 a dedicated reboot target has been added and in 4.6.0 support for restarting IPsec, PPP and DSL services in alarm actions is planned.

NOTE: Be careful! The reboot target action can be combined with any type of trigger, which may not always be what you meant. Only the Web UI displays a warning when activating the reboot action, issue #5992.

GRE Tunnels, IP Aliasing and Loopback Interfaces

Initial, but not yet complete, support for the upcoming VLAN fail-over feature in 4.6.0 is available from the CLI (only) in 4.5.0. This includes, amongst other things, support for IP aliasing, or alias interfaces, loopback interfaces, as alias interfaces on top of the now exposed *lo* interface and GRE tunnels.

In 4.6.0 support for running GRE tunnels over IPsec is planned. Which will make it easier to bridge remote sites more transparently by using a dynamic routing protocol such as OSPF on top. More on this in WeOS 4.6.0.

Technical Preview: L2TP and PPTP Removed

Since WeOS 4.2.0 experimental L2TP and PPTP tunneling support has been available, in the CLI only, as a technology preview. As of 4.5.0 they are no longer available. Full support, integrated with the existing PPPoE and upcoming support for PPP, is planned for a later release.

2.1 Platform

- When using PPPoE over DSL on Falcon, there is a problem with some ISPs where the PPPoE negotiation will not be completed. The result of this is that the connection does not come up. Fixed in issue #6147, for WeOS 4.5.1.

- A new boot loader image is available for RedFox Industrial, v2.02. No need to upgrade on deployed units, only newly produced units with new flash chip need this.

- Non-Westermo SFPs are now allowed. Be aware that use of non-Westermo SFPs might affect the functional and environmental specifications of the product, thus no warranties are made.

- FRNT is no longer limited to having both its ring ports in the same slot. Issue #3391.

- WeOS now supports two levels of software functionality:

  – *WeOS Level 1 (Layer-2 Switch)*: Products with WeOS software level 1 includes functionality common for layer-2 switches.

  – *WeOS Level 2 (Layer-2/3 Switch)*: Products with WeOS software level 2 includes gateway functionality (routing, NAT and Firewall, etc.) in addition to the layer-2 functionality found in *WeOS level 1*.

  Products launched with WeOS 4.4.0 and earlier will continue to work as layer-2/3 switches (WeOS level 2) after upgrading to 4.5.0. The first product being launched with WeOS level 1 is the *Lynx+ 110* switch.

- DNS proxy support is now a default feature. It is no longer necessary to enable a DHCP server on the LAN interface. Simply setup a name server and your non–primary interface is now able to forward DNS requests. Issue #5230.

- PPPoE support. The new Falcon unit has a dedicated simplified WAN setup where PPPoE is integrated. However, PPPoE support is also available on all other WeOS enabled devices. (Remember to set your external (WAN) interface as primary!)

- In #5207 support for CPU port(s) bandwidth limitation added. This is very useful when using the same device for both routing traffic between VLANs and at the same time running time critical protocols like FRNT. Because when too much traffic is being routed FRNT signaling risk being lost, issue #4951.

```
falcon:/#> configure
falcon:/config/#> system
falcon:/config/system/#> cpu-bandwidth-limit 8M
falcon:/config/system/#> leave
falcon:/#> copy run start
```


The above example sets a bandwidth limit for incoming traffic to 8 Mbps. See the Management Guide for more information.

- Possible to set NTP server address as a FQDN, not just an IP address. Issue #3601.
- As a spin-off to a bug fix (#5288) WeOS 4.4.0 includes support for static MAC filters. This is a necessary feature for setups where, e.g., OSPF/RIP/VRRP routers do not send out IGMP membership reports to subscribe to multicast groups in the 224.0.0.x range.

  Note: This is currently limited to *multicast* MAC filters, even though the syntax and online help says otherwise. This is due to automatic learning enabled on all ports by default today.

  The system `factory-config` for WeOS 4.4.0 has been updated to include default MAC filters for commonly used services. If you do not want to restart your setup from factory settings, simply `show factory` and paste in the relevant lines like this:

```
falcon:/#> configure
falcon:/config/#> fdb
falcon:/config/fdb/#> mac 01:00:5e:00:00:09 port ALL,CPU
falcon:/config/fdb/#> leave
falcon:/#> copy run start
```

  This example adds a filter for the RIPv2 multicast address 224.0.0.9. The fdb mac command only accepts MAC addresses, so you need to translate using RFC1112. Due to the limitations of this IP to MAC mapping the resulting address also maps to 225.0.0.9, 226.0.0.9, etc.
- The DDNS client, inadyn, suffered from a socket leak causing it to fail to update the system IP address at the DDNS service provider. Fixed in issue #5573.
- The firewall NAT rule really does allow all traffic from the internal interface to the external (as well as related replies from the outside coming back in). In 4.4.0 initial support for filtering source networks per each NAT rule and also support for deny rules.
- Issue #5022 details a problem with static routes being set as “kernel routes”. In WeOS 4.5.0 this has been fixed to some extent. However, default routes learned from DHCP or PPPoE (on a primary interface) are still set as kernel routes. This is expected to be remedied in 4.6.0.

2.2 CLI

WeOS now includes additional CLI settings for fine tuning of certain Ethernet PHY parameters. These settings are only expected to be used by customers with very special requirements – *the default settings is sufficient for most use cases*.

- Tab completion now works for commands in current context, global, parent and even local show commands. Issue #4906.

- The '?' key now works as expected. It lists alternatives and online help. Issue #4906.
- *Adapting receiver for shielded or unshielded cable:* The cable characteristics differs for shielded and unshielded TP cables. It is now possible to specify whether shielded or unshielded TP cables are used for 10/100 Base-TX ports, and thereby fine tune the receiver performance for optimal performance.
  Default: shielded
- *Signal power mode:* It possible to select between two signal power modes on the Ethernet data signaling pins for 10/100 Base-TX ports. The *low-power* mode is sufficient in most use cases, but for very long cables or cables with specific characteristics it may be necessary to *disable low-power mode*.
  Default: low-power

These settings apply to 10/100 Base-TX ports, excluding SFP/SFF ports as well as ports also capable of 1000 Mbit/s speeds.

Other features:

- From WeOS 4.3.0 and later it is possible to use the `abort` command even in the top-level configuration context. Disabling services, e.g. spanning-tree, or removing all VLANs can now safely be aborted. Remember to try the Ctrl-d key combo.
- When attempting to leave configuration context in interactive mode, the CLI now performs a simplistic sanity check and warns the user if:

  1. All ports have been disabled, or
  2. All VLANs have been disabled, or
  3. All interfaces have been disabled (`no up`), or when
  4. Any other subsystem returns an error during the "pre commit phase".

  Unfortunately this does not cover all faulty scenarios, but the hope is that it covers at least the most common ones.
- When leaving configuration context using the `leave` or `end` commands a friendly "heads up" reminder about `copy run start` is displayed. This is currently shown regardless if the user has made any changes or not. Improvements to this are planned for a later release.
- When configuring interfaces the `inet static` stanza is now mandatory to be able to access commands to set static IPv4 address. This is in preparation for the upcoming `inet6 static`, for IPv6 configuration.
  Note: The WeOS .cfg configuration files have used this syntax since 4.0.0, hence this change only affects interactive use.

- A long standing issue with the awkward use of `no vlans`, et consortes, in .cfg configuration files has been resolved. When loading a configuration file the database is now first cleared and system defaults are used. This could affect users that are used to load "diff configurations", however that is still supported by pasting in into a *non–interactive* CLI session's configuration context.
- The recommended way of pasting in configurations into the terminal is to use the `copy console running-config` command.
- In an effort to become even more compliant with existing CLIs on the market, only differences to the WeOS defaults are saved in the .cfg files. This is still an ongoing effort, so not all subsystems have been updated yet.
  This is a backwards compatible change.
- When entering the configure context the ON LED will flash on the unit, similar to what the IPConfig tool does. Useful for locating a device or verifying the correct unit is being configured.
- The CLI format version has been stepped up to v1.5 in all .cfg files saved using WeOS 4.5.0.
- Upgrade from devices with a USB port is now supported (CLI only).
  Syntax: `upgrade <pri|sec|boot> usb://image.ext`
- The repeat prefix to some show commands did not work in WeOS 4.4.0, issue #5684. Symptoms include either it does not work at all, no repeat, only a single run, or the output is garbled. Fixed in WeOS 4.5.0-beta2.

2.3 SNMP

- Wrong DSL port type used in ifTable. Issue #5224.
- Occasionally the SNMP sub-agent caused "Out of memory" conditions on Wolverine units. Fixed in issue #5256.
- FRNT traps always showed port state as forward. Fixed in issue #5293.
- The implementation of StaticEgressPorts in the Q-BRIDGE, VLAN, MIB was incorrect, issue #3572. This is fixed in 4.5.0-beta1, issue #5467.

2.4 Web

- A Basic Setup page has been added for Falcon. It wraps most common settings needed for WAN access in one page.
- DHCP Server now possible to configure in Web.

- The location indicator ("Here I am!") blink with the ON LED is now also possible to access from the Web UI. See Tools –> IPConfig for “Flash On LED”.
- Support for firewall deny rules.
- Support for adding new firewall rules at a specific position.
- Possible to reorder firewall rules.
- New generic WeOS header image. With product name, firmware version and hostname@location displayed for easy identification purposes.

2.5 SHDSL

- Turbo Speed now available, up to 15.3 Mbps data rate.
- Possible to disable SHDSL ports. Useful to check link traps on the other side of a link. Issue #5238.
- The SHDSL SNR monitoring trigger does not use HI/LO levels, issue #4961.

2.6 Firewall

- Issue #5369: Changing the input policy to allow no longer gives access to management services *disabled* in the interface management setting. I.e., if HTTP is disabled on an interface it is no longer possible to gain access simply by changing the input policy to allow. In cases where this is actually desired, an explicit allow rule must be created.
- Issue #6156: The stateful inspection function in the WeOS firewall blocks asymmetric traffic flows. This occurs both when the firewall is enabled and disabled. Asymmetric traffic flows can occur when you, e.g., have two equal cost paths to reach a remote IP subnet, and the router(s) on that subnet chose a different return path.
  Fixed in WeOS 4.5.1 by introducing the firewall `[no] spi` setting, default is to have Stateful Packet Inspection enabled. Hence, to handle assymetric setups you need to disable SPI.
- Support for deny rules and rule reordering, both CLI and Web.
- Sometimes the forward chain policy did not stay set after a reboot. Fixed in issue #5193.

2.7 VPN

- IPsec/IKEv1 support in WeOS 4.5.0 has been upgraded to Openswan v2.6.32.
- The VPN LED (previously ST2), visible on all new products, is now fully supported.

- In some (invalid) setups the IPsec daemon “pluto” crashed and did not recover, issue #5056. Improved documentation and online validation of the configuration has been added to WeOS 4.4.0.

  Symptoms: First the user notices that all tunnels go down, then the CLI command `show tunnel ipsec` gives no output at all, even if there are multiple tunnels configured.

  To be sure this bug is the problem, in the CLI issue the command `show log` and look for the line `ipsec__plutorun: Segmentation fault`:

```
Feb  4 01:12:00 lynx pluto[2824]: packet from 10.0.0.1:500: received and ignored
       informational message
Feb  4 01:12:00 lynx ipsec__plutorun: Segmentation fault
Feb  4 01:12:00 lynx ipsec__plutorun: !pluto failure!:  exited with error status
       139 (signal 11)
Feb  4 01:12:00 lynx ipsec__plutorun: restarting IPsec after pause...
```

- Sometimes when updating an existing IPsec tunnel the changes did not take effect, issue #5036.

3 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.

3.1 Platform

- A system with many VLANs setup requires more time at boot. This was first reported in #3291, but even after having fully optimized 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.
- On some computers, with some operating systems, the Westermo console port USB cable can block the boot sequence. Disconnect the USB-to-console cable when no terminal program, e.g., PuTTY is running. Issue #5984.
- The new alarm configuration lacks support for RMON triggers. Furthermore the community string that can be configured for each SNMP alarm action is missing in the actual trap.
- Issues #4494, #4502 and #4508 concern continued caveats with the feature preview link aggregation support.
- Running an FRNT ring over copper SFPs is currently not supported, or recommended, due to slow response time from copper SFPs.
- No CLI configuration support for managing multiple users and their capabilities.
- No CLI configuration support for static multicast routes.
- No LACP support in link aggregation.
- RSTP, IGMP Snooping, FRNT, etc. not supported over link aggregates.
- No support for any port authentication, either MAC nor IEEE 802.1x based.
- 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. Fix planned for a later release.
- SHDSL link can sometimes be lost due to slowly dropping SNR margin, issue #5317. This seems to be caused by high traffic load on the link. Fix currently unknown.
- 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. This may however be fixed in #5625.
- LLDP does not work correctly in all configurations. It has been disabled in the Westermo factory defaults, issue #4067. Fix planned for a later release.
- When downgrading to a release < 4.1.0 the user must perform a password reset due to password cryptography enhancements from 4.1.0 and later. A password reset is only allowed on the console port, simply login with user “password” and password “reset”, see the Management Guide for details.

  If a console port access is not available a crossed cable factory reset may be the only way to regain access.

  Note: In most cases the downgrade results in the password being reset to system default.

3.2 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`. In WeOS 4.5.0 a first cleanup has been made, but more work remains and will be performed incrementally in coming releases.
- No support for displaying SNTP status, NTP server stats. Best way currently is to manually check system time against another SNTP synchronized computer. The syslog is also a possible location to see what is going on. See “show log”.
- 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.

3.3 Web

- Inspecting RMON counters in the Port Statistics page may need a manual reload before the actual values are displayed.

3.4 Serial over IP

- When configured as TCP server. If a client reboots due to power failure or otherwise loose the connection without properly closing the TCP session. The server may take up to 16 minutes to detect that the session is lost. During this time the client want be able to reconnect to server. Issue #6033.

3.5 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.

3.6 Firewall

- Port forwarding does not work well with interfaces using DHCP assigned IP addresses. A fix is planned for a later release.
- Issue #6118 details how the service rules for Serial over IP cannot be overridden with custom packet filter rules. Fix planned for WeOS 4.6.0.

3.7 VPN

- In some cases when one of the IPsec endpoints closes the tunnel the connection cannot be reestablished automatically. This may occur when the connection is configured with static peer IP addresses on both end points and the tunnel uses NAT traversal.
  Workaround: The IPsec connection on one or both peers have to be restarted manually. In the CLI this is done in admin-exec context using: `tunnel ipsec restart`

- 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.
- It should be impossible to select “clear” as dpd-action on an initiator, it is however currently available as a configurable option. (Also, “hold” as dpd-action should work, but currently does not.)
- Supernetting using IPsec may stop access to local WeOS interface. This will be the case if for example configure local-subnet: 192.168.2.0/24, remote-subnet: 192.168.0.0/16 and a local interface with IP address 192.168.2.200/24, in this case nodes located on the 192.168.2.0/24 subnet will not be able to contact or receive services from 192.168.2.200. Issue #6153.

3.8 Link aggregation

Link aggregation is only provided as an unsupported technology preview feature. All use of the link aggregation feature except for testing is discouraged.

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

- Aggregation control: Link aggregates can be configured statically or be managed dynamically via the Westermo FLHP protocol. LACP is currently **not** supported.
- 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.
- Layer-2 protocols: Layer-2 redundancy protocols such as FRNT or RSTP cannot be used on a link aggregate or any of its member ports. Neither can IGMP snooping, thus VLANs where any link aggregate has a member port must have IGMP disabled.

When configuring link aggregation on switches in an operational network, there is a potential risk for a broadcast storm to occur. WeOS currently does not support the use of RSTP or FRNT on aggregated ports. The operator must therefore ensure that no layer-2 forwarding loop is established when connecting switches via aggregated links.

4 Known Issues

Issue	Category	Description
#3881	DSL	Initial SHDSL firmware load fails sometimes, fallback mechanism always works
#4856	DSL	SHDSL link up indicated on LEDs and CLI/Web before link is fully qualified
#5317	DSL	SHDSL SNR Margin falls with high load over the link
#5818	DSL	Auto-negotiated SHDSL link does not respect the desired SNR criteria
#6118	Firewall	Serial Over IP allow rules inserted before configurable packet filter rules
#4494	FLHP	Aggregated SHDSL Link does not work after FLHP reboot
#4502	FLHP	Traffic across link aggregation breaks when a physical link is removed
#4506	FLHP	FLHP and aggregation configuration
#4508	FLHP	Link aggregation with FLHP does not start when activated, needs reboot
#4951	FRNT	FRNT goes down during sustained high network load
#5571	FRNT	Focal Point does not indicate FRNT Alarms as it should
#6161	Ports	Port names are mixed in CLI between copper and DSL in fallback mode.
#3139	QoS	QoS interboard contention
#4203	RSTP	Storm occurs quite frequently when toggling RSTP bridge priority
#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
#6033	Serial over IP	Long timeout for lost TCP-server connections
#6022	SNMP	Not all OIDs in hdsl2ShdslEndpointCurrTable implemented
#3248	System	No warning in CLI/Web when other users are managing the system
#4067	System	LLDP sends incorrect data.
#5984	System	Unit does not boot if console is attached to system w/o running terminal client
#5987	System	Wayward ARP caused by IPsec route
#6180	System	RedFox 8FX: System instability issues with 1000Mbps fiber in 100Mbps SFP slot
#6213	System	Loading new config, or restoring backup, does not terminate old PPP/PPPoE sessions
#6254	System	Ping command from CLI hanged (once in testing)
#4215	VPN	No IP connection with local interface
#5092	VPN	IPsec: ID type inet fails in aggressive mode between WeOS peers
#5733	VPN	IPsec: MTU override does not apply when WeOS is sender
#5980	VPN	IPsec not reestablished to a server with DynDNS
#6112	VPN	IPsec initiator dpd-action hold and clear does not work
#6150	VPN	IPsec firewall rules does not always exist
#6153	VPN	IPsec: Supernetting hijacks services
#6226	VPN	IPsec is not restarted when outbound interface settings are modified
#5655	VRRP	VRRP sometimes never leaves INIT state when configuration is changed

5 Fixed Issues

This includes all -beta releases leading up to 4.5.1 from 4.5.0-rc1.

4.5.1-rc2

Issue	Category	Description
#6249	FRNT	At reconfiguration sometimes the FRNT daemon does not restart as it should
#6260	Serial over IP	Command ATD does not return correct response

4.5.1-rc1

Issue	Category	Description
#6080	CLI	Entering "move" without parameters in ip firewall context crashes CLI
#6147	PPP	PPPoE MRU parameter negotiation may cause problems with a Cisco DSLAM
#6148	FRNT	Member switch with FRNT ports in different slots hinders a broken ring to come up
#6149	LED	RFR-12 does not show any green led when link up.
#6156	Firewall	Asymmetric routing fails
#6167	VRRP	Unable to transit to master state when date is prior to 1970
#6175	CLI	Command "seriop" is available on devices without serial port
#6178	Serial over IP	Mode atcmd does not clean up correctly
#6179	Serial over IP	Mode atcmd, reopening of port is not done when hanging up
#6181	System	Port priority is not saved in configuration file
#6182	System	Disable a VLAN shows "no senable" in config file
#6200	CLI	FDB: Removing non-existing MAC address with port argument may cause context switch

4.5.0-rc7

Issue	Category	Description
#6136	VPN	IPsec supernetting with overlapping subnet, regression from 4.4.0

4.5.0-rc6

Issue	Category	Description
#6144	CLI	Alarm triggers: Support for parsing 4.6.0 format trigger IDs

4.5.0-rc5

Issue	Category	Description
#5980	VPN	IPsec not reestablished to a server with DynDNS
#6049	VPN	Streaming data and DPD event sometimes cause SA mismatch between WeOS peers
#6086	SNMP	entPhySensorValue for DC2 always 2 (DC2 low)
#6122	Ports	Port without mounted SFPs is not powered down properly

4.5.0-rc4

Issue	Category	Description
#6049	VPN	Streaming data and DPD event sometimes cause SA mismatch between WeOS peers.
#6063	System	All routes dissappear in a specific scenario.
#6065	DHCP	Zebra broadcast address warning on DHCP client.

4.5.0-rc3

Issue	Category	Description
#5961	CLI	Syntax check for RIP/OSPF authentication does not work.
#5979	WEB	Edit management services on Wan interface redirects browser to an invalid IP
#5981	PPP	Falcon will not get an IP address from ISP (BT) using PPPOE
#5988	Firewall	Port forwarding impacts traffic on IPsec tunnel
#5992	WEB	Action with reboot on not intended trigger type can give reboot loop
#5993	Boot Loader	Fix flash timing in RedFox bootloader
#6012	IGMP	Querier election fails if unit gets better IP at runtime
#6021	System	zebra[422]: netlink_interface_addr can’t find interface by index
#6034	WEB	Serial over IP interface always defaults to port 9000 on edit
#6039	System	FDB overrides user added rule/unable to forward packets to CPU
#6060	Firewall	Race condition with conntrack when restarting firewall

4.5.0-rc2

Issue	Category	Description
#4906	CLI	Add support for tab-completion in CLI sub commands
#5052	CLI	Support for showing only limited parts of "show running"
#5365	DSL	Ping fails for SHDSL turbo rates 8248k, 8760k and 9272k
#5589	SNMP	Support for CPU and memory utilization
#5837	CLI	Add support for configuration of RIP timers
#5898	System	Removing the default gateway does not have any effect
#5913	LED	Alarm LED (yellow) does not work for SFP-ports without SFP plugged in

Issue	Category	Description
#5917	DSL	xDSL link uptime does not account for time warps
#5920	System	RSTP always enabled after reboot
#5924	CLI	Add list of available alarm triggers to CLI online help
#5925	PPP	Routing web traffic through PPPoE does not work for some sites
#5942	LED	LED does not turn yellow when a port is blocked on RedFox Lite
#5951	System	Alias interfaces is not removed when base VLAN is removed.

4.5.0-rc1

Issue	Category	Description
#3360	CLI	Warn if DHCP acquired system settings exist
#3882	Ports	Add CLI support for Ethernet port low-power and shielded cable settings
#4184	VPN	IPsec daemon gives multiple errors about ike_alg_register_enc() when (re)starting
#5499	PPP	PPP connection on a VLAN not connected to anything...
#5530	CLI	Make it easier to enable management for all services
#5593	LED	RSTP/FRNT/VPN LEDs flicker spuriously at boot
#5631	WEB	Create custom 404 (page not found) error pages
#5747	System	Interface status is down for interfaces with no address
#5755	WEB	Default GW updated also with PPP on non-primary VLAN
#5756	System	Difference between factory-config and running-config after HW factory reset
#5760	PPP	Configured MTU for PPP interface (PPPoE) does not bite
#5797	System	Add support for non-Westermo branded SFPs
#5894	WEB	Configuration of 'reboot' alarm action not possible from web
#5903	CLI	New syntax upgrade pri uri://ip/file.img does not work anymore
#5914	FRNT	FRNT VLANs 4020 and 4021 not removed when disabling FRNT

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, RSTP enabled on all ports and a static IP address: 192.168.2.200 with netmask 255.255.255.0.

Use the IPConfig 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.

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
MAC                IP                  Ver.           Type     Status
==========================================================================
00:07:7c:86:04:b5  192.168.2.200/24    4.0.           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/RedFox Version 4.0.0 cricket/4.0.x@13930 -- May 18 14:20 CEST 2009
redfox:/#> ^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.

Note, the secondary CPU image and the boot loader firmewares can only be upgraded from the CLI. 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.

Primary and Secondary

List of primary and secondary CPU firmware images.

fw4XY.img: Falcon, WeOS 4.X.Y

lw4XY.img: Lynx+, WeOS 4.X.Y

lm4XY.img: Lynx 1400G, WeOS 4.X.Y (customer specific)

rw4XY.img: RedFox, WeOS 4.X.Y

ww4XY.img: Wolverine DDW-225/226, WeOS 4.X.Y

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 is also very CPU platform specific. Also, unless the release notes explicitly recommends it you should not upgrade the boot loader. List of bootloader firmware images:

imx27-redboot-4.XX.bin: Falcon, Lynx+, Lynx 1400G, Wolverine DDW-225/226

xscale-redboot-2.XX.bin: All RedFox products

Use the command `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

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

7.3 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.

```
redfox:/#> upgrade pri 192.168.2.42 rw400.img
Reading MTD partition information from FLASH
netflash: login to remote host 192.168.2.42
ftp: connect: Connection refused
netflash: ftping file "rw400.img" from 192.168.2.42
No control connection for command: Connection refused
netflash: failed to load new image
Trying TFTP instead...
Reading MTD partition information from FLASH
netflash: fetching file "rw400.img" from 192.168.2.42
.....................................................................................
netflash: got "rw400.img", length=5918720
netflash: Signature OK - Sig = RFox
netflash: CramFS OK - CRC = 0x194F663B
netflash: Flashing primary image, reboot is forced.
netflash: Killing processes to protect FLASH during upgrade...
netflash: programming FLASH device /dev/mtd1
.................................
netflash: Updating RedBoot FIS directory
```

```
Writing updated MTD partition information to FLASH
netflash: Rebooting.
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

