www.westermo.com

WeConfig

Westermo Configuration and Management Tool, version 1.14

Legal information

The contents of this document are provided “as is”. Except as required by applicable law, no warranties of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose, are made in relation to the accuracy and reliability or contents of this document. Westermo reserves the right to revise this document or withdraw it at any time without prior notice.

Under no circumstances shall Westermo be responsible for any loss of data or income or any special, incidental, and consequential or indirect damages howsoever caused.

More information about Westermo can be found at **http://www.westermo.com**

Table of Contents

1. WeConfig Quick Start Guide

The Westermo configuration and management tool, WeConfig, is used for configuration and maintenance of Westermo products.

2. Installation

To be able to locate the connection to the WeConfig computer, use WinPcap 4.1.3, which is also automatically installed.

WeConfig will not be able to find the connection between the computer and the network if the NIC discard LLDP frames. This is known to happen with low end USB NICs.

3. Device Requirements

WeConfig is designed for Westermo devices with WeOS version 4.13 or later. WeConfig will however find and try to display some information about other types of devices too. Earlier WeOS versions might have functional features, but they are however not supported.

The following functionalities must be enabled on the managed switches/routers to get the most out of the tool:

- IPConfig protocol
- HTTPS (Web) must be enabled on port 433. Administrator password must be setup in the *Project settings* dialogue.
- SNMP protocol
  - The read community must be set. The same read community must be be setup in *Procect settings* dialogue.
  - The SNMP trap host must be set to the IP-address of the WeConfig computer if traps should be listed in WeConfig. For full functionality, MS Windows Trap Host server needs to be disabled. WeConfig has its own built in trap host server.
- LLDP protocol
- SSH must be enabled

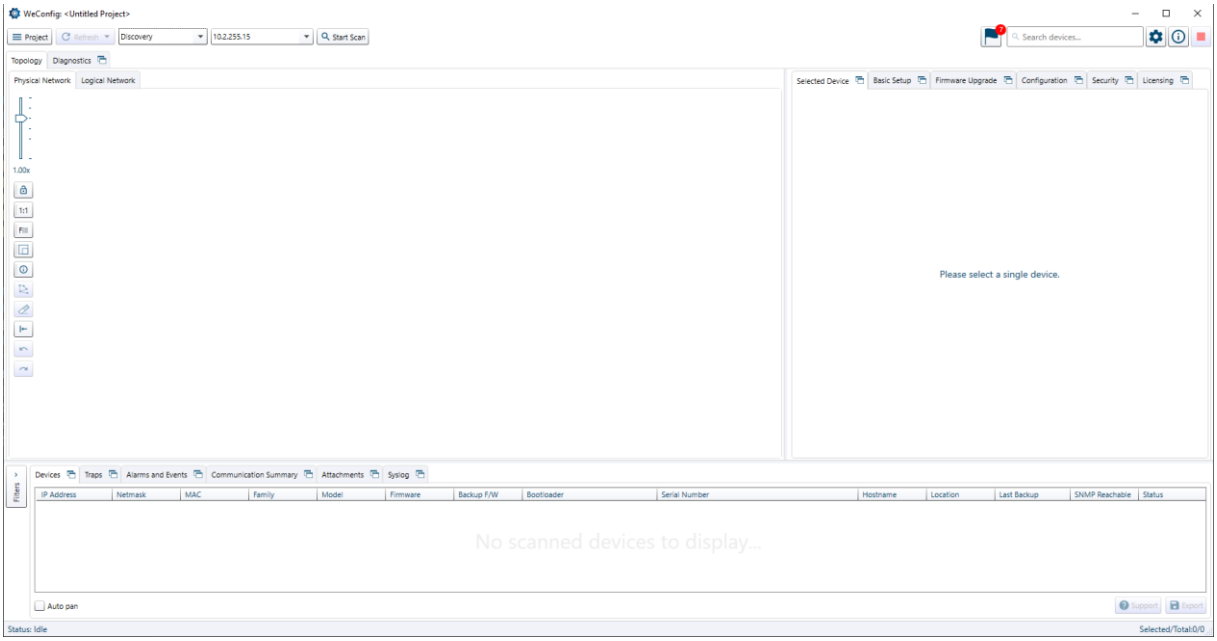
The functionality dependent on the respective item above is described below.

- Use SNMP to gather information from the device. This includes topology information in order to draw a device map. The topology information gathered with the use of SNMP requires the LLDP protocol to be enabled on the devices.
- Link information and automatic unit discovery can be performed if SNMP traps are set up on the devices. The topology map will mark link status based on link traps received, and new devices connected can be automatically discovered through link traps.
- Basic Setup uses the IPConfig protocol to configure devices. IPConfig protocol must be enabled on the devices to use Basic Setup.
- Backup, restore, firmware and bootloader upgrade all use the HTTPS interface.
- Upgrade with HTTPS-upload method uses the HTTPS interface.
- All configuration functions are performed with SSH; hence SSH must be enabled on the target devices.

When launch of interactive SSH sessions to the devices (e.g. via context menu), WeConfig will start Putty (see http://www.putty.org/). To use another SSH client, it must be setup in the tool settings.

4. Basic Usage

4.1 User Interface



In the top section, the global operations are present. There is a drop-down list to select between:

- Device scan, either using:
  - Discovery - combines Westermo IPConfig protocol and mDNS, or
  - ICMP Ping Discovery

  (See chapter "4.3 Scan for Devices" for more information)
- Update of device information with the use of SNMP

There is also a *Project* button for project management up in the left corner.
On the right top side there is a *Flag* button for notifications (see chapter "4.5 Notifications", a search field used to search for devices (it can handle multiple search terms to narrow down the search result), a user guide button, a cog wheel button for tool settings, an *i* button for information and a stop button to stop ongoing work.

The large empty area is split into two main tabs: the *Topology* view, and the *Diagnostics* view. The *Topology* view contains two tabs: a *Physical Network* and a *Logical Network*.

- *Topology*

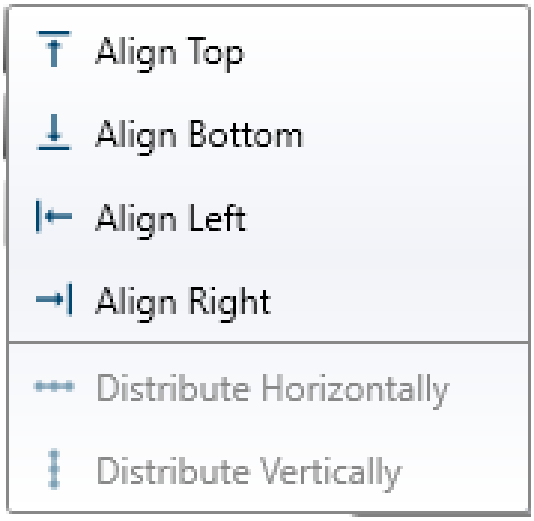
  The *Physical Network* will display network devices and their connections. To the left in this tab are display options for the Topology view, e.g. zoom and auto layout and alignment functionality. The "i" icon gives more information about links in the topology map. The "eraser" icon clears the project from devices but keeps settings and configuration backup files. The area to the right, the operations panel, contains different tabs for information display and configuration and maintenance.

The *Logical Network* will display network devices divided into logical groups. The groups are displayed to the left in a tree-view. To group devices, select the desired devices and select *Make layer*. To ungroup, select the group and select *"Deconstruct layer"*.

- *Diagnostics*
  The *Diagnostics* view shows a graph of monitored devices and applicable data sources.

The bottom panel main view is the list view where all detected devices will be listed after a scan (Devices tab). It also contains a Traps tab, *Communication Summary* tab and an *Attachments* tab. Optionally, it contains an *Alarms & Events* tab, if alarm monitor is enabled. The *Filters* button to the left in the *Devices* tab shows/hides a filter panel where predefined filters can be applied to the device list and the topology map. The *Devices* tab and the *Traps* tab can be undocked (click the icon) and resized. When undocked, just close the window to dock it again.

4.1.1 Align Devices



To align devices in the topology, select the desired devices and select an appropriate edge to align on. For example, elect to align to top, all devices are aligned to the top. The baseline for the alignment is the topmost device of the selected devices. Align on bottom, left and right sides work the same way. To make the space between devices equal, use the *distribute* function. For example, select an array of devices, and choose to distribute horizontally. WeConfig will then measure the distance between the left and right most device. The measured distance will then be equally divided among the devices between the left and right most device. WeConfig will only move the middle devices along the horizon.

Distribute space vertically works similarly, but along the vertical. Note that WeConfig does not guarantee that there will be any space between the devices after a distribution operation. For example, if the distance between the left and right most devices is less than required, then the devices will overlap along the horizon. No align or distribute operation take connections between devices into consideration. These operations are purely geometrical.

4.1.2 Lock Topology

Click the *Padlock* in the left panel to lock or unlock the topology view. When it is locked it is not possible to move devices with the mouse nor with the *Auto Layout* or *Align Selected Devices* buttons. *Zoom* and *Pan* still works when locked.

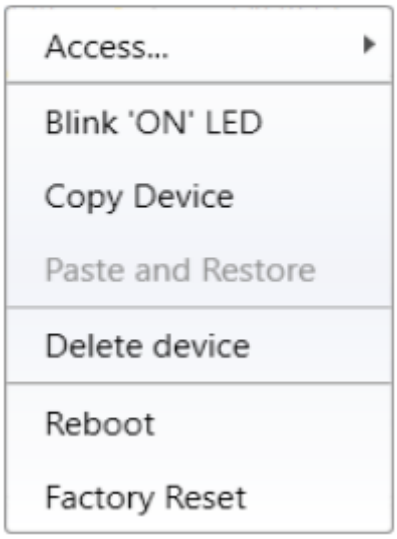
4.1.3 Undo/Redo

The Undo/Redo operations applies to actions made in the topology view, such as move or delete devices or connections. *Undo* and *Redo* buttons are located in the left panel but keyboard shortcuts can also be used, *Ctrl+Z* to undo and *Ctrl+Y* to redo.

4.2 Context Menu

Right-click in the topology and a context menu is shown.

Right click in the white area between the devices, and the context menu should only contain one option:



Right click on a device and the menu contains several options. The context menu options might change depending on type of selected device.

4.2.1 Add Device

Add device allows to add devices ad-hoc to the topology. The application will ask for a model, IP address, host name and location.

4.2.2 Set Image

Right-click a non-Westermo device to bring up the context menu with the *Set Image* option. Use this to set a custom image for the device.

4.2.3 Blink "ON"-LED

Right-click a Westermo device to bring up the context menu with the *Blink* "ON"-LED option. Using this option will start the devices' "ON"-LED to blink which make it easier to identify the device visually. The device will keep blinking as long as it is selected.

4.2.4 Access

Under the access sub menu, three choices are given to access the device, either through HTTP, HTTPS or SSH/CLI. If SSH/CLI is elected, the configured SSH client is used (see application settings for options).

4.2.5 Add Connection

This is used to set the connection between two devices manually.

4.2.6 Copy Device

Select *Copy Device* from the context menu on the source device. WeConfig will copy the settings from the latest saved backup configuration for the device. Right-click the target device and choose

Paste and *Restore*. WeConfig will change the settings for the target device to the settings from the source device. This is a useful operation when a faulty device has been replaced with a new one.

4.2.7 Delete Devices

This removes the selected devices and all their connections from the topology.

4.2.8 Reboot

This reboots the selected device.

4.2.9 Factory Reset

Factory Reset resets the selected device to the factory configuration. Use with caution.

4.2.10 Disable/Enable SNMP

Select this option to enable/disable SNMP. Note: Only valid for MRD/BRD devices.

4.3 Scan for Devices

To get started, a scan operation is necessary. To get as much information as possible with the scan operations, the SNMP read community string should first be set in the project settings dialogue to allow automatic SNMP queries to collect information about the units, e.g. the topology information to draw the topology map.

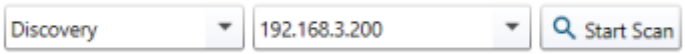
Perform a re-scan and any newly found devices will be located at a fixed position on the topology map, with a slight overlap of each other. An auto-layout performance or to position by hand is necessary. Each newly detected device will also be marked with a "New" icon; this icon will be removed in the next scan or when the project is saved.

Devices will not be automatically removed at any time. They can be deleted with the context menu on devices in topology map or in the device list. Links between devices can also be removed manually; just click the "i" icon on the left to show the information icon on all links, click the information icon for link of interest and operate on displayed info.

The links between devices are displayed in different colours based on the type. Blue colour for fibre, brown for copper, green for DSL and black for manually added links or unknown type.

4.3.1 Discovery Scan

The *Discovery* scan is recommended for new units (factory default settings) or unknown configurations. The *Discovery scan* combines IPConfig, mDNS and Powerline scan. The scan will find devices and show them in the topology where further operations can be performed. Note, the IPConfig protocol can be turned off on the Westermo devices. If so, they will not be identified with the IPConfig protocol. The mDNS and Powerline scan can be enabled/disabled from general *Settings*, see chapter "4.6 Settings". Powerline scan is disabled per default.



Select an IP address in the drop-down list to scan with the associated network interface. The subnet mask for the IP address should be 255.255.255.0. If a different subnet mask is used, an alternative IP address can be added, see chapter "4.3.3 Alternative IP Setting".

4.3.2 ICMP Ping Discovery

The *ICMP Ping Discovery* is recommended for scan of units when they are configured, since it will also find other units in the network, and thus get a more complete map of the network. If devices from other vendors supply topology information in the same manner as WeOS devices, the topology map will also be able to display their connections in the topology view.

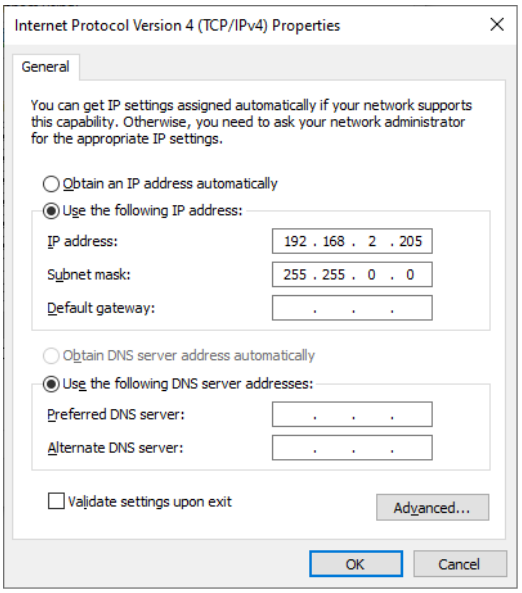
Enter a start address and end address for the IP-range to ping. Click the red *Cancel* button to cancel a ping scan operation in progress.

4.3.3 Alternative IP Setting

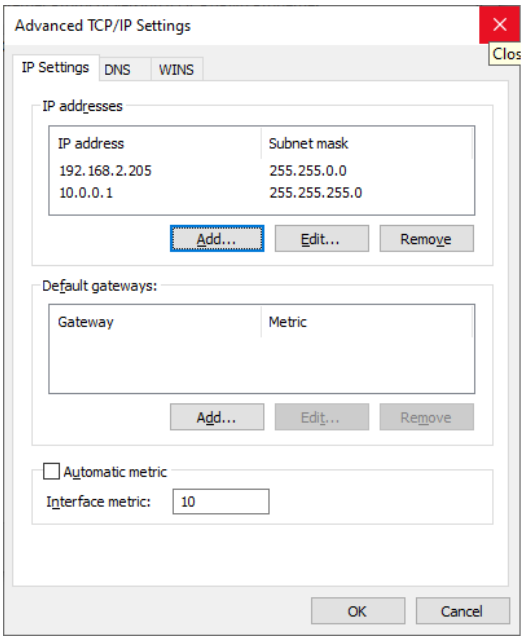
An address with subnet mask 255.255.255.0 must be used to scan, due to a shortcoming in the IPConfig protocol. To work around this problem, there are two solutions: Let WeConfig installer install WinPcap (which is default), to let WeConfig work around the limitations of IPConfig, or follow the text below.

Make sure that the PC's interface connected to the device network is a member of a subnet that is 8 bits wide. If no such subnet is available, add an additional address for smoother operation. Make sure the address selection does not interfere with other devices in the network.

Open *Network Settings* with the Windows control panel in the TCP/IP properties dialogue and click *Advanced button*.



Now click the *Add* button and enter an alternative address with subnet mask 255.255.255.0. There should now be two addresses available.



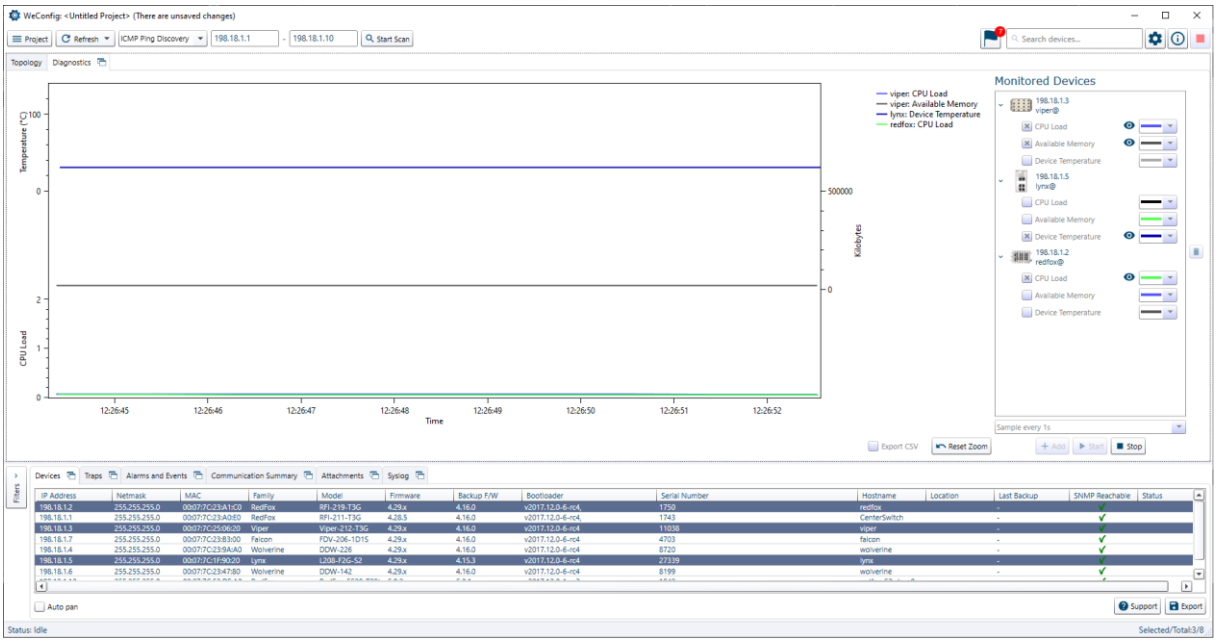
4.4 Diagnostics

In *Trend diagnostics,* the following data sources can be plotted:

- Available memory
- CPU load
- Device temperature
- FRNT change count
- PoE Power
- RSSI
- SFP Rx/Tx Power
- SFP Port temperature
- SHDSL SNR margin

To monitor the data source, select the desired devices in the list below, and click the *Add* button located on the right side. Only the applicable data sources for the selected devices will be possible to probe. Select the desired data source on the devices in the list on the right side and click the *Start* button.

If needed to log the sample data for later analysis, make sure to check just below the graph, and select a path to the file. It is imperative not to open the CSV file in Excel or any other application at sample, as the file might become locked then.



It is possible to show and hide individual graphs at the sampling. Click the "eye" icon in the list of monitored devices on the right side. Although WeConfig will auto-assign colours to each graph, it is possible to change the colour for each graph. Select the colour of choice in the combo box in the device list.

Click on any individual graph line to trace the line and then move the mouse near the graph line. WeConfig will show a cross hair on the graph line, and a panel with the exact value at that point on the graph.

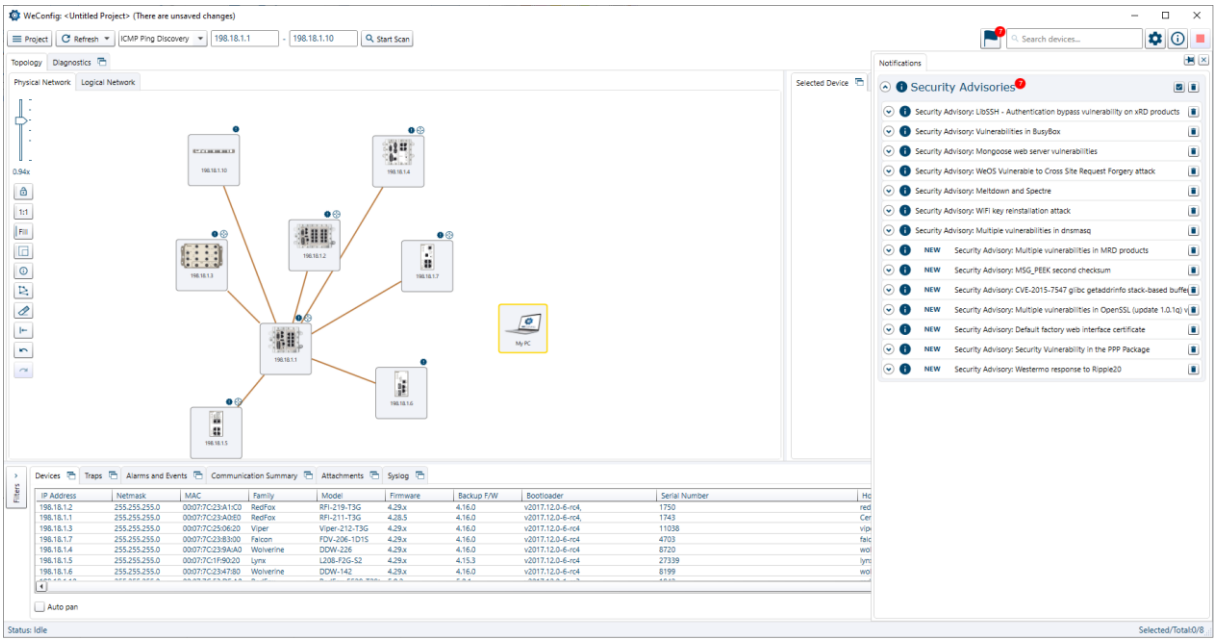
Use the scroll wheel on the mouse to zoom in and out on the graph. Right-click on the graph. Drag the mouse while the right button is pressed down to pan the graph up/down/left/right. Click the middle mouse-button, and keep it pressed down. Form a rectangular area over the graph. When the middle button is released, the selected area will be zoomed in. It is possible to reset the zoom. Double-click the middle button or click the *Reset Zoom* button.

When a monitor session is restarted, the graph is cleared. Data saved to CSV will not be lost. A new monitor session will add data to the CSV file, not replace it.

4.5 Notifications

WeConfig has an information section where notifications are shown. Three types of notification severities are shown:

- Information
- Warnings
- Errors



Click the "flag" icon in the upper right to view/hide the notification list. Use the Pin button to pin the information. Each notification can then be expanded to show more details. The flag changes colour depending on the severity of the notifications in the list:

- Blue = Information
- Yellow = Warnings
- Red = Errors
- Unfilled = No notifications

The number (if any) presented in a badge over the "flag" icon indicates how many unread notifications that exist in the list. The badge will flash during a short time to indicate that new notifications exist.

The notifications are grouped in categories:

- *Application* - Shows information about the application. Can be hints about installation packages, error information, configuration guideline etc.
- *Security Advisories* - Known security advisories for products published by Westermo.
- *Software Updates* - Information that new versions are available. Can be new firmware for Westermo devices, new language packages, new WeConfig etc.
- *Security Hardening* - If Security Scanning is enabled, WeConfig can identify security hardening possibilities and suggest actions.

4.6 Settings

Settings made via the cogwheel are valid for the applications and will automatically be applied for all new projects (can be changed per project, see chapter "5.2 Settings").
The following settings can be made:

- *Application* - Configure search path to firmware, editors, SSH client etc. from here configured.
- *Default* Project - Same settings as for the project settings (see chapter "5.2.1 General").
- *Advanced* - Settings regarding graphical layout and possibility to enable/disable automatic hardening scanning. Settings regarding discovery can be set here. Powerline and mDNS scan can be enabled/disabled. For mDNS, there is also the possibility to enable/disable ARP-ing of link local addresses for the PC.

- *Notifications* - Notifications that is not of interest for a user can be set as ignored from the *Notifications* area. This means that any following notifications of this type will not be viewed. Here in the settings dialog, these settings can be turned on/off.

5. Projects

5.1 Management

Projects are saved, renamed or deleted with the options found under the *Project* button in the top panel. The projects can be password protected with a password, look at the Project menu.

5.2 Settings

Project settings are also found under the Project button in the top panel.

5.2.1 General

In this dialog the following can be configured: severity of the notifications in the list:

- Default settings for SNMP read community
- If hostname and location should be visible in the topology
- If WeConfig should automatically scan for new devices
- If scheduled backup should be enabled
- Settings for retrial regarding firmware upgrade
- SNMP auto refresh options
- Enabling the WeConfig as Syslog server
- Enabling Alarm monitoring function
- Enabling Alarm/Event logging function

5.2.2 Device Access

Access authority and ports (ssh, web) can be set per device on project level, via the Device Access menu option. These settings are used for device access and are not actually applied on device level. To change the settings on the device, use the functionality under tabs *Configuration/ Password* and *Configuration/SNMP*.

In Device Access, the Management IP address can be selected. All known addresses on a device interface (vlan) are fetched during a *refresh* action. In Device Access the address that WeConfig should use to contact the device can be selected. The selected addresses are stored in the project.

5.2.3 Configuration Manager

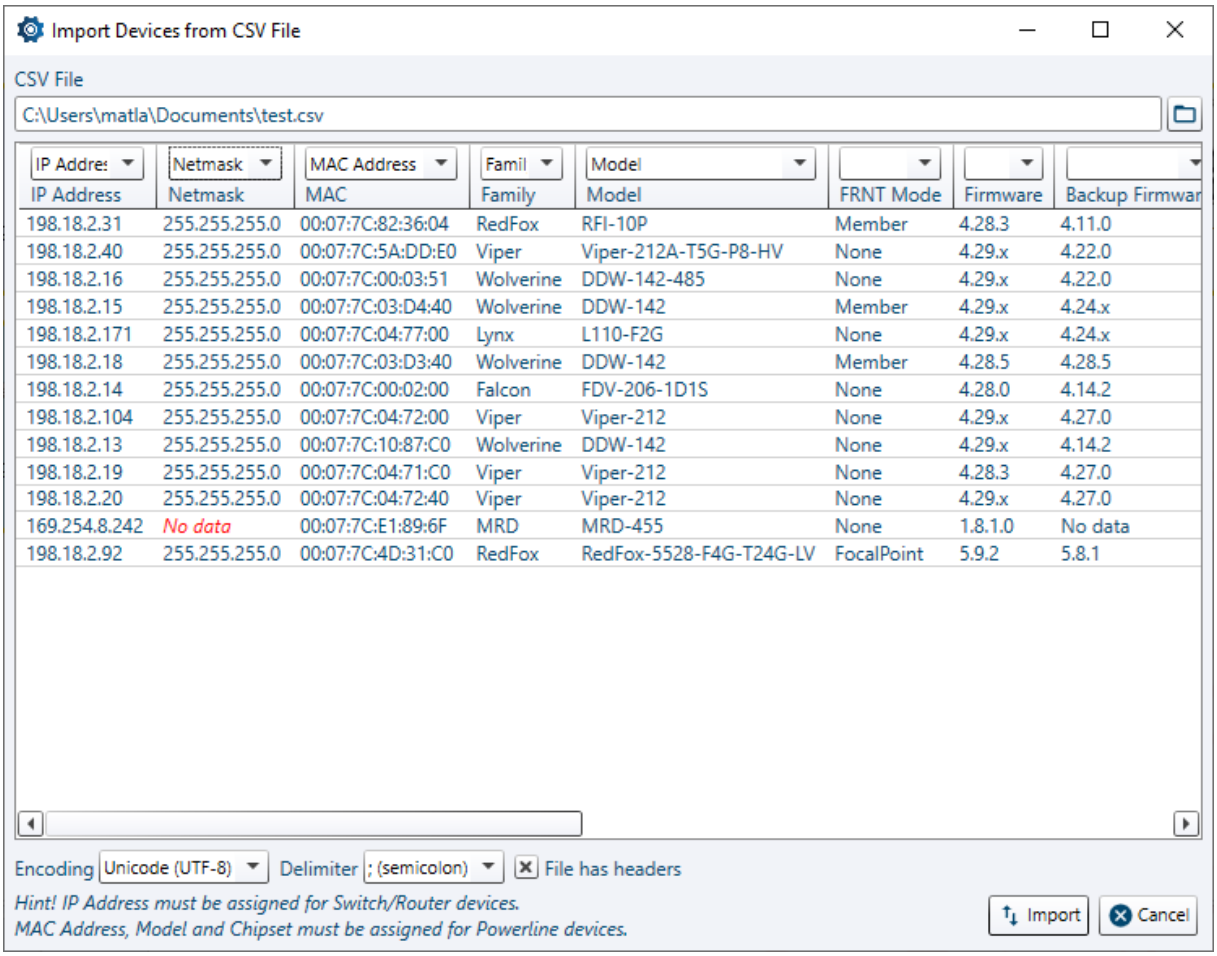
The *Configuration Manager* can be used to manage all configuration files contained in the project. For example:

- Delete a configuration
- Edit a configuration
- Export a configuration to a separate file
- Associate a configuration with another device

5.2.4 Import of Devices

To import devices into the project from a CSV file, choose *Import/Devices* from the *Project* menu. Browse for the CSV file, and specify encoding, delimiter and whether the file has headers or not. The

defaults are often good enough. Use the combo boxes to specify which column in the CSV file should map to which device attribute. Click *Import* to start.



5.3 Project Gold File

Project gold file is a template file which represents an entire network with the devices and all their connections and settings. This gold file can be used to setup new networks on network topologies that are exactly the same regarding the number of devices, model and physical connections.

5.3.1 Export from Current Project

In order to make a template of the current project, the following criteria must be met:

- WeConfig's connection in the topology is known
- All devices must support the gold file functionality

Currently, only WeOS devices are supported. Export functionality can be found under the *Project* button in the top panel and under the menu option *Templates* and *Export* from current project.

5.3.2 Build Network from Template

Browse and select the gold file template which will then be applied on the network. The build-network-process is wizard-based. It will guide and inform what to do to complete the operation. *Build network from template* functionality can be found under *Project* button in the top panel and under menu option *Templates* and *Build network from template*.

5.4 Reports

Under the *Reports* menu, found under the *Project* button in the top panel, the different reports are found. The reports contain information about:

- *Deployment*, the devices and their connections
- *Security Baseline*, potential vulnerabilities and security issues
- *Network Baseline*, characteristics and settings tied to the function and performance of a system

The reports are displayed in a report viewer after creation. From the viewer, the report can be printed or exported to numerous formats. All reports are saved as attachments in the project.

6. Operations Panel

The tabs *Selected Device, Basic Setup, Firmware Upgrade, Configuration, Security, Licensing* and *CLI* can be undocked (click the  icon) and resized. When undocked, just close the window to dock it again.

6.1 Selected Device

6.1.1 Properties

Select a device and the device information will be displayed in the *Selected Device* tab in the operations panel. The information is collected with SNMP. Information is updated when a device is selected, or when the global operation *Refresh* is used.

During *selection/refresh* of a device, information is also fetched via SSH connection. For instance, all known addresses on a device interface (vlan). In *Device Access* the address that WeConfig should use to contact the device can be selected.

6.1.2 Configuration Files

Select a device and currently available configuration file backups are listed (in local time order) in the *Configuration Files* tab in the operations panel. Configuration can be backed up, restored, edited, imported, exported or deleted.

When selecting *Automatically update baseline after backup* the following backup will be used as new baseline, see also chapter "6.6.6 Configuration Baselines" for more information.
Configuration files can also be copied between units with the copy/paste functionality found in the device context menus in topology map or device list.

When a listed configuration backup file differs from previous entry in the list, an "i" icon is shown to the left of the entry. Click the icon to show actual file differences in a separate window. WeConfig uses an internal viewer that shows differences. This viewer can be changed to any other viewer via the tools settings (upper right corner of WeConfig).

6.1.3 Communication Details

Select a device and a port on the device in the *Communication Summary* tab (found in the bottom panel) and a detailed view of communication information is displayed in this tab. The information can be automatically updated by selecting an interval option in the Auto refresh drop-down found on the *Communication Summary* tab in the bottom panel.

6.1.4 Attachments

Attached information (e.g. notes, images etc.) specific for the device can be managed. The attachments are saved in the project file.

6.2 Basic Setup

Select devices in the topology map (Ctrl + click a device to select devices in desired order) or device list view (Ctrl+A in the list selects all devices) and click the *Add* button in the *Basic Setup* tab to add them to the work selection for the basic setup of devices. IP address, subnet mask, default gateway, hostname and location can be set. IP address field also accepts CIDR notation. accepts CIDR notation, for example 198.18.2.1/24.

Use the *Fill* functionality to generate IP-series. Use the sort feature to order the units or select them in the desired order.

Leave one or more fields empty and *Fill* will leave the field as is.

6.3 Firmware Upgrade

To be able to use this feature, download the firmware packages to the WeConfig computer. The folder where the files will be placed must be configured in the tool-settings dialogue. The default upgrade protocol is HTTPS. If TFTP/FTP is selected, a TFTP or FTP server must be installed on the WeConfig computer.

Note: Use the same folder for all firmware packages whether HTTPS or TFTP/FTP is used. Select devices in the topology map (Ctrl + click a device to select devices in desired order) or list view (Ctrl+A in the list selects all devices) and click the *Add* button in the *Firmware Upgrade* tab to add them to the work selection for the basic setup of devices.

Use the sort feature to order the units in desired order before upgrade or select them in the desired order.

6.4 Bootloader Upgrade

To be able to use the Bootloader Upgrade, download the firmware package(s) (bootloader is included in the firmware) to the WeConfig computer. The folder where the file(s) are placed must be configured in the tool settings dialogue. The default upgrade protocol is HTTPS.

Select devices in the topology map (Ctrl + click a device to select devices in desired order) or list view (Ctrl+A in the list selects all devices) and click the *Add* button in the *Firmware Upgrade* tab to add them to the work selection. Then select *Device Image = Bootloader*.

The bootloader is selected by pointing out a firmware (pkg file) under the *Firmware* option. Use the sort feature to order the units in desired order before upgrade. The order can also be chosen depending on how you select the units into the configuration tab. Note: Upgrading the bootloader is supported for WeOS 4.27.0 and newer 4.X releases and for WeOS 5.11.0 and newer 5.X releases.

6.5 Configuration

6.5.1 Backup

Select devices in the topology map or list view and click the *Add* button in the *Backup* tab to add them to the work selection to perform backup of devices. Files are saved with UTC time stamp. When selecting *Automatically update baseline after backup* then the following backup will be used as new baseline for the devices, see also chapter "6.6.6 Configuration Baselines" for more information.

6.5.2 SNMP

Select devices in the topology map or list view and click the *Add* button in the *SNMP* tab to add them to the work selection to perform SNMP configuration of the devices.
Edit the fields directly in the list or use the *Fill* functionality (above the list); to use a field when filling, just check the checkbox to the left of the field. To clear all fields in the list click the Clear button.
Click *Apply* and the configuration will be applied on the devices in the list.

6.5.2.1 SNMPv2

Under the tab SNMPv2 for the devices, device access parameters can be specified. If the read community is changed then the Device Access for the project is automatically updated.
Note: To disable the SNMPv2 read community, leave the field blank for the devices.

6.5.2.2 SNMPv3

Under the tab SNMP v3 for the devices, you can create new users and setup authority for the account.

Note: If no read community is specified on the device for SNMPv2 and no SNMPv3 user is specified in *Device Access* for the project, then WeConfig will automatically select one of the new users and update the *Device Access* for the project.

6.5.3 FRNT

Select devices in the topology map (Ctrl + click a device to select devices in desired order) or list view (Ctrl+A in the list selects all devices) and click the *Add* button in the *FRNT* tab to add them to the work selection to perform FRNT configuration of the devices.

Click *Propose Ports* to get a suggestion for the M/N port settings. Edit the fields directly in the list.
Click *Apply* and the configuration will be applied on the devices in the list. Ring coupling (RiCo) can be configured to achieve redundant connectivity between FRNT-rings.

6.5.4 MRP

Select devices in the topology map (Ctrl + click a device to select devices in desired order) or list view (Ctrl+A in the list selects all devices) and click the *Add* button in the *MRP* tab to add them to the work selection to perform MRP configuration of the devices.

For devices running WeOS 5.11 and newer, multiple ring configurations is supported, up to two rings can be added. Only one ring of type Client or two of type Manager is allowed.

Click *Propose Ports* to get a suggestion for the Ring port settings. Edit the fields directly in the list.
Click *Apply* and the configuration will be applied on the devices in the list.

6.5.5 RSTP

Select devices in the topology map (Ctrl + click a device to select devices in desired order), or list view (Ctrl+A in the list selects all devices) and click the *Add* button in the *RSTP* tab to add them to the work selection, to perform RSTP configuration of the devices. Edit the fields directly in the list. To enable RSTP or to set Admin Edge on port level click the "down-arrow" icon to the left of each device in the list. Click *Apply* and the configuration will be applied on the devices in the list.

Note that the network might be instable when the configuration is applied, and the connection might be lost.

6.5.6 VLAN

Select devices in the topology map (Ctrl + click a device to select devices in desired order) or list view (Ctrl+A in the list selects all devices) and click the *Add* button in the *VLAN* tab to add them to the work selection to perform VLAN configuration of the devices.

The *VLAN* tab is divided in two sub tabs, *Ports and Interfaces*. In the *Ports* tab, the VLAN is applied on the actual ports as tagged, untagged or not a member. Edit the fields directly in the list. When a new VLAN is added, it is tagged for all devices in the list, on all ports with a connection to another WeOS device, and for all ports that has either FRNT or RSTP (non Admin Edge) configured. It is important to remember that this is only a suggestion. It is the responsibility of the user to decide which ports shall be tagged.

In the *Interface* tab the actual VLAN interfaces can be configured. Edit the fields directly in the list or use the *Fill* functionality (use the "down-arrow" icon above the list).
Click *Apply* and the configuration will be applied on the devices in the list.

6.5.7 Ethernet Ports

Select devices in the topology map (Ctrl + click a device, to select devices) or list view (Ctrl+A in the list selects all devices) and click the *Add* button in the *Ports* tab to add them to the work selection to perform Ports configuration of the devices.

To set specific speed/duplex on ports, just select wanted speed/duplex in the speed combo box for wanted port.

Note: For WeOS 5 devices several speed/duplex can be selected. To select Auto negotiation, just select this option in the same combo box.

To set specific ingress/egress on ports, just select wanted ingress/egress in the ingress/egress combo box for wanted port.

Click *Apply* and the configuration will be applied on the devices in the list.

6.5.8 SHDSL Ports

Select devices in the topology map, or the device list, and click the *Add* button. WeConfig will only allow to add devices that have SHDSL ports. For each port, select Role (CO/CPE). When applicable, select *G.HS threshold, link rate, EMF* (emergency freeze), *noise margin* and *low jitter*. It will also be possible to select *Pass*. When applicable, it will be possible to select *PAF* (SHDSL bonding).

To ensure that a device is not configured so it is unreachable, WeConfig will detect if port pairs have incompatible configurations. This will only work if all connected SHDSL devices are added to the configuration panel. WeConfig will also remind to click *Propose Order* before the use of new configurations. *Propose Order* will order the devices in such a way that device configurations are applied in such an order that WeConfig is not locked out by unstable intermediate links. This function will only work if WeConfig has established its connection to the topology.

6.5.9 CPU

With this panel it is possible to configure CPU bandwidth throttling. Select devices in the topology map, or the device list, and click the *Add* button. Then for each added device, choose the follow parameters in the combo box:

- *Disable* – no CPU bandwidth will be throttled
- *Auto* – WeOS will automatically throttle the CPU bandwidth as it sees fit
- *Manual* – enter a fixed value (expressed with a unit selected in the combo box to the right)

6.5.10 General

Select devices in the topology map (Ctrl + click a device to select devices in desired order) or list view (Ctrl+A in the list selects all devices) and click the *Add* button in the *General* tab to add them to the work selection to perform general configuration of the devices.

The *General* tab is divided in four sub tabs; *Logging, Network, Time/date* and *Alarm*.
Click *Apply* and the configuration from all *General* sub tabs, will be applied on the devices in the list.

- *Logging* - Configure Syslog Server 1 and 2
- *Network* - Configure default gateway, enable/disable routing and DNS server 1 and 2
- *Time/date* - Either configure time/date with current host time or SNTP. Configure time zone, NTP server address and NTP poll interval
- *Alarm* - Disable link alarm on all ports, enable on all tagged ports, enable on all untagged ports, enable on all FRNT ports, enable on all RSTP ports (non Admin Edge) or enable on all ports that currently have link status up (link to PC excluded)

6.5.11 Password

Select devices in the topology map (Ctrl + click a device to select devices in desired order) or list view (Ctrl+A in the list selects all devices) and click the *Add* button in the Password tab to add them to the work selection to perform password(s) configuration of the devices.

The password(s) stored in *Device Access* is automatically updated when password(s) is changed.
Note: The devices that are affected by multiple passwords are the MRD/BRD family.

6.5.12 Powerline

If powerline devices exist in the topology, the *Powerline* configuration tab is visible.
Select powerline devices in the topology map and click *Add* in the *Powerline* tab to add them to the work selection to perform configuration of the devices.

6.6 Security

6.6.1 Port Protection

This panel will show if the ports on a device are protected by MAC filter/802.1X and if the ports is used. It will offer options to enable/disable the port and/or set *Link Up Alarm* triggers.

6.6.2 MAC filter

Use this panel to scan the network for access port traffic and to make MAC filters for each access port, such that it will only allow traffic that has been observed at the scan. WeConfig will assist to build a ”white list” for all access ports.

Access ports are ports that connect to non-Westermo devices, such as PLCs, printers, cameras, etc. To start the scan, first add the devices and then click *Scan*. It is imperative that all devices has LLDP turned on for all ports, or this scan will fail.

WeConfig will continuously query the selected devices for access port activity, until the *Finish* button is clicked. To be certain that all relevant access ports have been detected as such, keep the scan running as long as possible to capture all normal traffic that flows 4100-22000 25 through the

network. If possible, manually exercise the network with the end-point applications for which the network was designed.

The list in the panel will be populated with devices and their ports, together with found non-Westermo addresses, as well as any previous MAC filter settings. The list is basically the blue print for the MAC filters WeConfig will configure when *Apply* is clicked.

Before the configuration is applied, it is possible to do the following operations:

- Disable access ports – useful for ports that have not been detected as ”used”. For rapid configuration use either *Enable used* or *Disable unused*.
- Optimize MAC addresses to MAC wildcards – useful for ports that have detected several distinct devices from a single vendor
- Add hard-coded MAC addresses (or wildcards) that should be exempt from the MAC filter

As the list can become very large, it is possible to opt to only show certain ports:

- Unused ports only
- Trunk ports only (ports that connect to other Westermo devices)
- Access ports only

Note: Before applying the configuration, make sure that it is correct. It is possible to be locked out from the network!

6.6.3 802.1X

To configure 802.1X port authentication, select appropriate devices in either the topology view or the device list, and click *Add*.

If this configure is from scratch, consider using the *RADIUS Settings Template* feature, which allows for the configure of RADIUS settings in one place, and then propagate those settings to all devices added to the list with the *Fill* button.

To propagate the RADIUS settings from one device onto all devices, select the ”master device's” RADIUS settings and click the *Make template* button. Now the template area has the same settings as the ”master device”. Then click *Fill* to propagate to all devices. To add a RADIUS server, select *Server* in the *Type* combo box. Add a description, address (IP or DNS name), and service password. Click the button with a plus sign on it, and the entry will be added to the table above the input fields.

To add a RADIUS server group, first create one or more server entries. Then select *Server group* in the *Type* combo box and add a description. To link server entries to this group, type in the descriptions of the entries in the *Server members* textbox, separated by a comma. Click the *+* button and the entry will be added to the table above the input fields. To select an entry in the RADIUS server/groups table as the entry to use for 802.1X authentication, click the checkbox on the correct row.

For each device and VLAN that should be protected by 802.1X, click the desired *Enabled* checkbox. If any port on any device and VLAN should be excluded from 802.1X authentication, then click the desired port's checkbox in the *Excluded ports* area. To apply the configuration, click *Apply*.

6.6.4 Management Hardening

Use this panel to scan all or the selected devices in the project for known management hardening issues. These include the use of:

- HTTP for the web service
- SNMPv2 write community
- The default admin password (westermo)

- IPConfig
- Telnet

When *Scan* is clicked, each device in the project will be interrogated for any of these issues. When the scan is finished, WeConfig will list all devices and their found issues.

WeConfig will by default suggest removing all issues. If the default admin password has been used on any device, it will not be possible to apply the fixes until the password has been changed.

If any of the known issues are ignored, it is necessary to be explicit and uncheck the issue. This can be done easily from the *Autofill* section.

6.6.5 Routing Hardening

With this panel it is possible to scan all or the selected devices in the project that are configured to be routers. It detects OSPF or RIP router settings that do not use MD5- HMAC to sign routing traffic. When *Scan* is clicked, each device in the project will be interrogated to see whether there are router configurations that do not use MD5-HMAC signatures. A presentation of each device with an issue, all VLANs and all routing protocols that do not use MD5- HMAC. Then it is possible to enter the key ID and key for each device/VLAN/protocol combination. The *Autofill* section can be used to great effect for this, if there are many devices. To apply the settings, click *Apply*.

6.6.6 Configuration Baselines

With this panel it is possible to setup a configuration baseline for any device. A configuration baseline is a configuration file, to which all future backups are compared to. If a change is detected, the device's *Status* column in the device list will indicate that there is a baseline difference. Optionally, if *Alarms & Events* have been enabled, an alarm will be posted in that list to persistently mark the anomaly.

To add a configuration baseline for any device, first make sure the device is in a known secure state. Then take a backup of the device with WeConfig. Once the backup has been made, select the device in the topology map or the device list, and then click the *Add* button. The device will be added to the list with a configuration baseline set to *No baseline selected*. Select the backup that is to be the security baseline and click *Apply*.

6.7 Licensing

Select devices in the topology map (Ctrl + click a device to select devices in desired order) or list view (Ctrl+A in the list selects all devices) and click the *Add* button in the *Licensing* tab to add them to the work selection to perform configuration of the devices.

Licenses can be managed for the selected devices, either separately or as a bundle. A bundle contains licenses for multiple devices. (Note: Only 4.23 and newer are supported).

6.8 CLI

To enable the CLI tab you need to open the general Settings for WeConfig and select the *Advanced User Interface*.

When enabled, select devices in the topology map (Ctrl + click a device to select devices in desired order) or list view (Ctrl+A in the list selects all devices) and click the *Add* button in the CLI tab to add them to the work selection to perform CLI scripting of the devices.

The resulting output of a CLI scripting can be exported to a text file.

7. Bottom Panel

7.1 Filters

In this section quick filters for the devices in the network is set, e.g. highlight, dim, hide devices, depending on the filter parameters set.

7.2 Devices

Devices lists all devices found when scanning. To automatically pan the topology map to the device selected in this list, check the *Auto pan* checkbox found below the list. Click on the headings to sort the list.

Click the *Export* button to export the list to a CSV file. Click the *Support* button to upload tech support files from selected device.

7.3 Powerline Devices

Powerline devices lists all powerline devices found when scanning. If no powerline devices exist in the topology, this tab is not visible. Click on the headings to sort the list. Click the *Export* button to export the list to a CSV file.

7.4 Traps

Traps lists traps received from SNMP agents. Requires configuration of trap host address on the devices.

WeConfig uses Windows trap host when enabled. For full functionality, the Windows trap host must be disabled; in that case WeConfig will use its own trap host server.

Click the *Export* button to export the list to a CSV file. Click the *Clear* button to clear the list.

7.5 Alarm and Events

This tab can be enabled/disabled from the *General Project Setting* dialog under the *Alarm monitoring* section. Enable the *Combine FRNT ring down* and link down will merge the alarms that corresponds into one entry in the alarm and event list.

The supported alarms are Link down, Link up, FRNT, Temp and SNR. Acknowledge the alarms one by one or click the *Ack. all* button to acknowledge the whole visible list. It depends on the applied filter. Each entry can be manually deactivated. Select the alarm and click *Deactivate*. The alarm and event list can be exported into a CSV file.

7.6 Communication Summary

Communication Summary lists a summary of communication information for ports on selected device.

Select a port in the list and detailed information will be available in the *Communication Details* tab found under the *Selected Device* tab in the operations panel to the right.

The communication information can be automatically updated every 5, 10, 30 or 60 seconds. Select an option in the drop-down found below the communication summary list. Click the *Export* button and the list is exported to a CSV file.

7.7 Attachments

Attachments lists all files that have been attached to a project. Attachments are saved in the project file. When a project file is shared, all attachments are shared as well. As a consequence, large files make the project file bigger.

To attach a file to the project, drag a file onto the list from Windows Explorer, or click the *Import* button. To export an attachment from the project, drag the attachment from the list and onto a folder in Windows Explorer, or select the attachment and click *Export*. All files generated by The WeConfig are automatically saved as attachments in the project file.

To open or edit an attachment, click on the file name in the attachment list, and the associated application will be opened for the file. At the closure of the current project (or WeConfig), make sure to save any changes in applications that have attachments open. It is recommended to save and close such applications before the closure of projects or WeConfig.

7.8 Syslog

To enable the *Syslog* tab, go into the *General* project settings and select the *Syslog server* option. All devices that are configured to use WeConfig as Syslog server will display its Syslog messages in this tab. The log messages are filter per device. The *Syslog* can also be exported to file.

8. Tools

The tools are opened from the main *Project* menu.

8.1 SHDSL Reach Calculator

The *SHDSL Reach Calculator* allows to explore indicative signal attenuation and data rates for the two parameters *environment* and *cable*.

Select a combination of environment and cable parameters and click *Add*. The combination will then be plotted on the graph. The Y axis represents a theoretical maximum data rate in Mb/s, and the X axis represents distance in kilometres. To remove a graph line, select the legend on the right side, and click *Remove*.

8.2 SHA256 Hash Calculator

The *SHA256 Hash Calculator* is a tool to calculate SHA256 hash for a selected file (firmware) and it allows the user to compare the calculated SHA Hash with a manually entered one.

8.3 Subnet Calculator

The *Subnet Calculator* is a tool to help the user calculate a subnet based on:

- IP address and Number of wanted hosts/net
- IP range
- IP address and a given netmask.

The tool calculates the following data:

- Subnet address
- Broadband address
- Netmask
- Minimum/maximum IP address
- Number of hosts/nets

9. Language

The WeConfig user interface may be localized for different languages. The language packages are installed separately. The default language for WeConfig is English. Click the "Settings" icon  . In the Application tab, select the desired display language.

Revision notes

Version	Date	Description of changes
WeConfig 1.14	September 2021	Chapter 5.2.2 updated. Chapter 6.1 updated. Chapter 6.4 updated. Chapter 6.5.4 updated Minor changes to wording
WeConfig 1.13	January 2021	New document transferred to new format. Changes of front page. Changed Ch 6.5.7 text updated. Heading 4/4.1 changed. Changed illustration Ch 5.2.4. Changed illustration Ch 4.2. Minor changes to wording
WeConfig 1.12	August 2020	New Westermo logo, Ch 4.3.1 text updated, Ch 4.6 text updated, Ch 6.5.12 new chapter, Ch 7.3 new chapter
WeConfig 1.11	November 2019	Ch 1 text updated, Ch 3 text updated, Ch 4.1 text and illustration updated, illustration added, Ch 4.2 text updated, Ch 4.2.10 new chapter, Ch 4.3.2 text updated, Ch 4.5 text added, illustration added, Ch 4.6 new chapter, Ch 5.2,1 text updated, Ch 6.4 new chapter, Ch 6.4.11 text updated, Ch 9 illustration added
WeConfig 1.10	May 2019	Updated frontpage, Ch 4.4 new screenshot, Ch 4.5 updated, Ch 5.2.2 updated, Ch 6.5.1 new chapter, Ch 6.5.2 updated, Ch 7.6 updated, updated back page
WeConfig 1.9	October 2018	4.1 image updated, 4.5 new chapter, 5.2.1 text updated, 5.4 text updated, 8 entire chapter updated, 9 new chapter
WeConfig 1.8	May 2018	New frontpage, Ch 2, Ch 4.1 updated & new screenshot, Ch 4.2 updated, Ch 4.2.1 new screenshot, Ch 4.2.6, Ch 4.2.9, Ch 4.3.1, Ch 4.3.2, Ch 4.3.3 updated, Ch 4.4 new screenshot & updated, Ch 5.2.2, Ch 5.2.3, Ch 5.2.4, Ch 5.4, Ch 6, Ch 6.1.2 updated, Ch 6.1.4 new chapter, Ch 6.2, Ch 6.4.1 updated, Ch 6.4.2.1, Ch 6.4.2.2, Ch 6.4.4 new chapter, Ch 6.4.5, Ch 6.4.10 updated, Ch 6.4.11 new chapter, Ch 6.5.1, Ch 6.5.3, Ch 6.5.4 updated, Ch 6.6, Ch 6.7, Ch 7.1, Ch 7.7 new chapter, new back page
WeConfig 1.7	June 2017	New chapter 4.2.3, back page updated
WeConfig 1.6	December 2016	Minor updates in WeConfig application., but non that effects the manual

WeConfig 1.5	October 2016	Frontpage illustration updated, 4.1 illustration updated, 4.1.2 and 4.1.3 new chapters, 4.2.1 updated illustration, 4.2.2 new chapter, 4.2.4 updated, 4.2.6 updated, 4.4 updated, 5.3 and 5.4 new chapters, inside of back page Revision notes inserted

Westermo • Metallverksgatan 6, SE-721 30 Västerås, Sweden
Tel +46 16 42 80 00 Fax +46 16 42 80 01
E-mail: info@westermo.com
www.westermo.com