MICROSENS

Application Note

Basic Configuration of G6 Devices

MICROSENS GmbH & Co. KG
Kueferstr. 16
59067 Hamm/Germany

Tel. +49 2381 9452-0
FAX +49 2381 9452-100
E-Mail info@microsens.de
Web www.microsens.de

Summary

This document outlines the basic configuration steps that are usually needed to set up a MICROSENS G6 switch for operation.

It also explains basic network switching concepts and leads through example configurations step-by-step, using hands-on scenarios.

It builds on information from the Quick Installation Guide that is shipped together with each MICROSENS G6 device.

Glossary

Acronyms and abbreviations used in the document.

Term	Description
EEE	Energy Efficient Ethernet (IEEE 802.3az)
IP	Internet Protocol
LACP	Link Aggregation Control Protocol (IEEE 802.1AX)
LAG	Link Aggregation
LAN	Local Area Network
LED	Light Emitting Diode
MAC	Media Access Control
MDI/MDI-X	Media Dependent Interface/Crossed
MSTI	Multiple Spanning Tree Instance
MSTP	Multiple Spanning Tree Protocol (IEEE 802.1s)
MVRP	Multiple VLAN Registration Protocol (IEEE 802.1ak, GVRP successor)
PACC	Port Access Control
PD	Powered Device (PoE role)
PDU	Protocol Data Unit
PoE	Power-over-Ethernet (IEEE 802.3af)
PoE+	Power-over-Ethernet Plus (IEEE 802.3at)
PSE	Power Sourcing Equipment (PoE role)
RADIUS	Remote Authentication Dial-In User Service
RSTP	Rapid Spanning Tree Protocol (IEEE 802.1w)
RTC	Real Time Clock
SFP	Small Form Factor Pluggable Transceiver
STP	Spanning Tree Protocol (IEEE 802.1D)
TCAM	Ternary Content Addressable Memory
TCP	Transfer Control Protocol

Term	Description
UDP	User Datagram Protocol
VAC	Voltage Alternating Current
VDC	Voltage Direct Current
VID	VLAN ID
VLAN	Virtual Local Area Network

Table of Contents

Introduction

This document helps you to start operating your MICROSENS G6 switch. It explains basic switching concepts and afterwards leads through the required setup steps for deploying the switches in the network environment.

The following sequence has proven to be useful in practice:

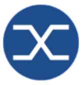
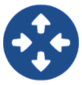
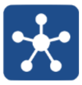
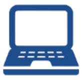
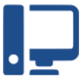
- Set up the device for network management access by entering the IP parameters
- Familiarise yourself with the user interfaces
- Check the firmware version on the device and update it if necessary
- If necessary, load a previously created configuration file into the device
- Configure the device ports
- Protect the device from unauthorised access
- Secure or separate network data with VLANs
- If appropriate, synchronise the device’s system time with the time of a network time server (NTP server)
- Perform an operation diagnosis

Typographical Conventions

The following typographical elements are used in this document:

Typographical Elements	**Explanation**
•	List element, 1st order
◦	List element, 2nd order
www.microsens.de	Hyperlink to a website or an email address
Note:	A note tags an important fact
□	Work step
<…>	Placeholder for a real value. Replace <IP Address> with e.g. 192.168.1.2.
[…]	Optional input
{…|…}	Choose one of the values offered, e.g. from {Disabled|Enabled}, choose Enabled.
»	Work step result
Visualization	A GUI string that appears in the Web Manager
Command	A string to enter in the Command Line Interface
» Output	A string output by the Command Line Interface
░	Work step(s) in the Web Manager (GUI)
█	Work step(s) in the Command Line Interface (CLI)

The following symbols are used in this document:

Symbol	Explanation
	Switch
	Router
	Hub
	Arbitrary computer
	Server

Information on the MICROSENS Website

Registered users can find current firmware versions as well as further information on our web site:

- Registration: www.microsens.de > Partner-Login > Follow the link "Please register here" > Fill in the online registration form and submit it
    - You will receive an email from MICROSENS with a user name and a password.
- Login: www.microsens.de > Partner-Login > Enter user name and password > Click the "Login" button.
    - Firmware images: Navigate to your device and select the tab "Services".
    - For further information select one of the other tabs.

Note:
Make sure your browser allows the execution of scripts.

1 Basic Administration

Note:
The memory card (SD card on MICROSENS Industrial Switch, microSD card on MICROSENS Micro Switch and Desktop Switch) that is supplied for your MICROSENS Switch is formatted in a non-Microsoft Windows® format. Do not reformat the memory card, otherwise the device will not be able to recognise it. If the memory card is defective, please contact your MICROSENS representative or the MICROSENS support (support@microsens.de) for a replacement.

Note:
MICROSENS G6+ Switches are equipped with an internal memory where they store their complete setup. So they do not necessarily need a microSD card as external memory. MICROSENS G6 Micro Switches on the other hand do not have an internal memory and therefore the use for a microSD card to store their setup is mandatory.

1.1 Default User Levels for Management Access

The following user levels (roles with specific access rights) are preset:

User	Password	Access	Comments
public	microsens	Read only	This user cannot make any changes.
user	microsens	Limited write	This user has write access to selected parameters such as aliases, time, test functions, etc.
admin	administrator	Full rights	This user can adjust all settings.

1.2 Configuring the IP Parameters

For managing the device over the network, the device needs valid IP parameters (an IP address, a network mask and a standard gateway entry). The device automatically obtains these parameters via DHCP (factory settings). It is also possible to configure the IP parameters with help of:

- the software “Switch IP Configuration Tool” (also “Switch IP Config Tool”),
- the software “Network Management Platform” (NMP) or
- CLI access via serial interface and appropriate cable (this is common for industrial devices). The default serial port configuration is 115200-8-N-1 (for more information see section "User Interfaces" on page 10).

The leaflet “Quick Installation Guide” included with each MICROSENS G6 device describes how to prepare a device for network management. It is also available on the MICROSENS website (see “Information on the MICROSENS Website” on page 7). The Quick Installation Guide’s IP address assignment section is repeated below.

Note:
The person performing the setup of IP parameters is required to be logged in as user “admin” and to know the appropriate passwort.

1.2.1 Using the Switch IP Config Tool

The Switch IP Config utility is available for download on our web site as a ZIP archive:

- Go to www.microsens.de > Support > Software-Tools

The ZIP archive "IP-Config Tool" contains an English documentation and the software offers an English user interface.

- Download, install and start the software. Installation prerequisites are:
  - all Microsoft Windows ® operating systems
  - 512 MB RAM
  - 2 MB free disk space
  - display resolution of at least 1024*768
  - Java Runtime Environment (JRE) version 1.5 or higher installed

  Note:
  In order to check whether JRE is installed on your PC or not, please open the Microsoft Windows® command line window (Start > Run >CMD) and type

  ```
  java –version
  ```

  The following output means that the JRE is installed and the current JRE version is 1.6.0_15:

  ```
  java version "1.6.0_15"
  Java(TM) SE Runtime Environment (build 1.6.0_15-b03)
  Java HotSpot(TM) Client VM (build 14.1-b02, mixed mode, sharing)
  ```

  If the JRE is not installed you can download it from Sun's web page:
  http://java.sun.com/javase/downloads/index.jsp

- Select the network interface of the administrative workstation that is intended to be used for configuring the device.
- Activate the button **MAC-based Device Discovery** (take the firewall configuration into account).

  Note:
  The software lists the MICROSENS devices by their MAC address.

- From this list, assign the IP parameters to the device and store them into the non-volatile memory by activating the "Send" button.

1.2.2 Using the Software Application "Network Management Platform"

With the Network Management Platform (NMP), MICROSENS offers a universal management software for configuring and monitoring all MICROSENS network components centrally. Due to its clear graphic design and sophisticated automatic functions, it assists the network administrator significantly.

NMP offers a multilingual user interface. The functionality of the Switch IP Config Tool is included.

A current version of the software is available for download on our web site:

- www.microsens.de > Support > Software-Tools

To use the software, a license key is necessary. A test license can be obtained from the local MICROSENS sales contact or directly from MICROSENS (sales@microsens.de).

1.3 User Interfaces

Once the IP parameters have been set up, the device is ready for network management.

MICROSENS G6 devices offer several user interfaces, for both:

- Separate management (seperately for each device)
- Centralised management (centralised for all devices)

These interfaces are accessible via different protocols.

1.3.1 Separate Management

Interface	Protocol	Explanation	Transport	Default
Web Manager	HTTPS	Graphical user interface (GUI), usage: https://<IP Address>. Further user documentation can be downloaded using the Web Manager's link "Documentation" in the navigation bar.	Encrypted	Enabled
	HTTP	Graphical user interface, may be used as a substitute for https.	*Unencrypted*	*Disabled*
Command Line Interface	SSH	Text-based user interface (CLI).	Encrypted	Enabled
	Telnet	Text-based user interface.	*Unencrypted*	Enabled

The **Web Manager** is a Graphical User Interface (GUI) that allows the user to conveniently monitor the device's status as well as to view and modify its settings.

A detailed description of the **Command Line Interface** can be found in the document "Product Manual Firmware, Generation 6" that is included in each firmware and can also be downloaded via the Web Manager's link "Documentation" in the navigation bar.

Note:

- Web Manager: Access the Web Manager either via HTTPS (default) or HTTP.
  - Enabling HTTP access will automatically disable HTTPS access and vice versa
  - MICROSENS recommends using the Web Manager via HTTPS
- Command Line Interface: Access the CLI either via SSH, Telnet or serial interface.
  - Enable or disable SSH and Telnet access independently
  - MICROSENS recommends disabling Telnet access for improved security if it is not in use.
- In case of MICROSENS G6 devices which are deployed in critical environments MICROSENS recommends to manage these devices only via the command line interface and to disable other user interfaces as described below.

Using the Command Line Interface (CLI):

□ Open an SSH or Telnet application and connect to the device through it's IP address.

□ Supply the admin's user name and password.

At the prompt, enter the command

□ **`Management.WEB.protocol = DISABLED`**

Note:
Output format in the following CLI examples depends on the terminal width and will not wrap automatically as shown.

Note:
The access via serial interface (default serial port configuration: 115200-8-N-1) requires an appropriate console cable depending on the type of device:

- For Micro Switch use p/n: MS190410-01,5
- For Industrial Switch use p/n: MS190411-01,8

1.3.2 Centralised Management

User Interface	Protocol	Explanation	Transport	Default
Network Management Platform (NMP)	HTTPS	MICROSENS software for centralised management	Encrypted	Enabled
Any compatible 3rd party software	SNMPv1	Simple Network Management Protocol	*Unencrypted*	Enabled
	SNMPv2c	Simple Network Management Protocol	*Unencrypted*	Enabled
	SNMPv3	Simple Network Management Protocol	Encrypted	Enabled

Note:
MICROSENS recommends disabling SNMPv1 and SNMPv2c access for improved security if they are not in use.

Further documentation:

- For details on the MICROSENS Network Management Platform, see the respective documentation.
- For details on third party software, see the documentation that comes with the software.

Note:
NMP uses the device's webserver for HTTPS connections using a secured HTTPS connection on TCP/IP port 1025 to read or write system parameters. Thus, the Web Manager can be disabled on HTTP (port 80) and HTTPS (port 443) connections. HTML information is not available on TCP/IP port 1025.

1.4 Firmware Version

MICROSENS is constantly working on their products. This may include new firmware to improve performance and add new functions.

1.4.1 Check the Firmware Version on the Device

Using the Web Manager:

- □ Open a web browser. Make sure it can access the device’s IP address and scripts are allowed for the given URL.
- □ Type **`https://<Device IP Address>`** in the address line and press the Enter key (Example: **`https://192.168.1.2`**).
- □ Supply the admin’s user name and password in the browser dialogue and confirm.
- □ If necessary, change the Web Manager’s language by selecting it from the drop-down list located at the bottom of the navigation bar to the left.
- □ In the navigation bar select the menu entry **System**.
- □ In the Web Manager’s screen **System** to the right, select the tab **Firmware**.
  - » The device’s current firmware version is shown in the table labelled **Firmware Status**.
  - » More available firmware versions already stored on the device are shown in the table labelled **List of Available Firmware**.

Using the Command Line Interface (CLI):

- □ Open an SSH or Telnet application and connect to the device through it’s IP address.
- □ Supply the admin’s user name and password.
- □ At the prompt, enter the command

```
Device.System.Firmware.running_version
```

Note:
After a few characters which make the following command unambiguous, the CLI will auto-complete the command.

1.4.2 Check the Firmware Version on the MICROSENS Web Site

Registered users can find current firmware versions as well as further information on our website (see “Information on the MICROSENS Website” on page 7).

- Login: www.microsens.de > Partner-Login > Enter user name and password > Click the “Login” button
  - ◦ Navigate to your device and select the tab “Services”
  - ◦ The list shows the newest firmware versions first
  - ◦ If you want to download a firmware, click on its link
- When asked whether to open or save the file, it is usually safe to choose “Save”.

- Open the downloaded ZIP archive. It contains the firmware file as well its release notes and documentation.
- Extract all files in the archive
- Read the release notes

Notes:

- Make sure your browser allows scripts for the given URL
- The operating system needs to be able to handle ZIP archives (most current operating systems do)

1.4.3 Update the Firmware on the Device

Using the Web Manager:

□ Open the device's Web Manager.

□ Select the **System** screen, then select the tab **Firmware**.

□ Firmware versions already stored in the device are shown in the table labelled **List of Available Firmware** (along with their respective image size and build date).

Note:
If the appropriate firmware is already available on the device, just click the respective **Apply** button to update. This will restart the switch with the desired firmware. The following steps are obsolete.

□ In the table labelled **Firmware Upload**, click the **Search...** button

Note:
Depending on the operating system's language settings, the button text may differ (e.g. **Durchsuchen...**).

□ In the file upload dialogue, select the desired firmware file (usually it has the file name extension .msu), then click the file dialogue's **Open** button.

□ Click the **Start Upload and Apply** button.

Notes:

- If the firmware is already stored in the device, the Web Manager will prompt to overwrite it.
- For only storing the new firmware without applying it immediately, use the **Start Upload** button instead of the **Start Upload and Apply** button.

» The Web Manager will show the upload progress with a progress bar and the subsequent update steps in the log windows below. After these steps are complete and the update requires a reboot, the device will automatically perform a reboot. The reboot takes approximately 45 seconds, depending on the device type and the device configuration.

□ Re-login to check the new firmware version.

Using the Command Line Interface (CLI):

□ **`Management.Files.firmware.display_files`**

```
» NOTE: This will execute an action command with the following
  function:
  Displays a list of all available software files.
  Type y to continue, else to quit: _
```

□ Type **y** to continue.

```
» executing..
  Listing available firmware files
  a1234v100502.msu
  b1234v100503.msu

  -- END OF ACTION RESPONSE --
```

□ If the respective firmware is not available on the device, download it from an FTP server with the following command:

```
Management.Files.firmware.download =
ftp://<user name>:<password>@<IPaddress>
/users/admin/Downloads/mf5916v100504a.msu
```

Note:
It is necessary to have a valid FTP server access with **`<user name>`** and **`<password>`**.

□ **`Management.Files.firmware.install_software_update = mf5916v100504a.msu`**

» If the update requires a reboot, the device will automatically perform a reboot.

1.5 Loading an Existing Configuration File

In many cases there may be an already existing setup for the new device. Possible reasons for that are:

- A configuration file was created in advance with an offline tool.
- An existing device is to be replaced by a new identical one.

MICROSENS devices offer the following possibilities:

- Loading an existing configuration file from a server.
- When replacing an existing device, it is possible to transfer the configuration file by using the microSD card.
- Using the MICROSENS Network Management Platform NMP.

1.5.1 Loading an existing Configuration File from a Server

The configuration transfer is carried out in two steps:

- Save the switch's current setup to an FTP server
- Load the configuration file into the new switch from the FTP server

Note:
It is necessary to have a valid FTP server access with **`<user name>`** and **`<password>`**.

Using the Command Line Interface (CLI):

□ Open the CLI on the switch whose setup is to be transferred to another switch.

□ **`Management.Files.configuration.upload_to_server = <folder name> ftp://<username>:<password>@<IP address>/<path>/`**

```
» NOTE: This will execute an action command with the following
  function:
  The content of the specified configuration folder is compressed
  into a single file (in tar.gz format) and then uploaded to a
  server. Various protocols may be used. Example: upload_to_server
  = folder ftp://user:passwd@ftp.upload.com/dir/ Note the trailing
  / is mandatory. Instead of a hostname an IP address may be
  specified. Instead of ftp other transport formats like tftp or
  http can be specified. The saved file will be prefised by the
  local IP address of the sending device.
  Type y to continue, else to quit: _
```

Note:
A standard **`<folder name>`** is “running”.

□ Type **`y`** to continue.

```
» executing..
  Compressing <folder name>...
  Uploading <folder name>.tar.gz to
  ftp://<username>:<password>@<IP address>/<path>/
  Upload complete.

  -- END OF ACTION RESPONSE --
```

□ Open the CLI on the new switch.

□ **`Management.Files.configuration.download_from_server = <folder name> ftp://<username>:<password>@<IP address>/<path>/`**

```
» NOTE: This will execute an action command with the following
  function:
  A configuration packed as tar or gztar file can be downloaded to
  a custom folder. Example: download_from_server =
  local_config_name
  ftp://name:passwd@machine.domain/full/path/to/config_file/ The
  downloaded config is not automatically activated.
  Type y to continue, else to quit: _
```

□ Type **`y`** to continue.

```
» executing..
  Downloading ftp://<username>:<password>@<IP address>/<path>/ to
  <folder name>
  Download from ftp://<username>:<password>@<IP address>/<path>/
  complete, extracting to <folder name>
```

Using the Command Line Interface (CLI):

```
Overwriting config in folder: <folder name>
Done.

-- END OF ACTION RESPONSE --
```

□ Activate the downloaded setup.

□ **`Management.Files.configuration.restore_from_folder = <folder name>`**

```
» NOTE: This will execute an action command with the following
  function:
  Restores and activates the specific user configuration. Each
  resulting config change will be logged as usual. Specify source
  folder. Synrax: restore_from_folder = folder_name. Important:
  This command does not restore the IP and factory configuration
  files.
  Type y to continue, else to quit: _
```

□ Type **y** to continue.

```
» executing..
  Restoring from folder <folder name> to becoming the running
  configuration.

  <status messages>

  ok - 29 files restored.

  -- END OF ACTION RESPONSE --
```

1.5.2 Transfer an existing Configuration File via a microSD Card or USB Medium

On **G6 devices**, the SD card contains the complete system so that swapping the SD card to another switch will move the complete system to it.

Note:
The SD or microSD card that is supplied for your MICROSENS G6 Switch is formatted in a non-Microsoft Windows® format. Do not reformat the memory card, otherwise the device will not be able to recognise it anymore. If the SD card is defective, please contact your MICROSENS representative or the MICROSENS support (support@microsens.de) for a replacement.

On **G6+ devices**, the setup is stored in the internal memory. This means that the setup transfer is carried out in two steps:

- Save the switch’s current setup to a microSD card or USB medium
- Load configuration file into the new switch

Note:
Depending on the device, type the following commands and use an inserted USB medium (devices with USB port) or a DOS formatted microSD card (Micro Switch) for backup and restore the device’s setup.

Note:
The USB port function is supported starting from firmware version v10.6.0c!

Using the Command Line Interface (CLI):

□ Open the CLI on the switch whose setup you want to transfer to another switch.

□ If you do not want to export the running setup (in the folder “running”) directly to an external medium, you can save it to a backup folder within the device’s internal flash memory first:

```
Management.Files.configuration.backup_to_folder = <folder name>
```

```
» NOTE: This will execute an action command with the following
  function:
  Copies running configuration to a new or existing folder. If the
  folder name already exists the previous configuration is
  overwritten. Syntax: backup_to_folder = my_new_config.
  Type y to continue, else to quit: _
```

□ Type **y** to continue.

```
» executing..
  Backup running configuration files to <folder name>
  ok

  -- END OF ACTION RESPONSE --
```

□ Export the previously saved setup to the respective medium (microSD card or USB medium).

```
Management.Files.configuration.export_to_media = <folder name>
```

Note:
If the folder name already exists on the medium, this command overwrites the previous configuration!

□ Remove the microSD card or USB medium from the former switch and insert it into the new one.

□ Open CLI on the new switch.

□ **Management.Files.configuration.import_from_media = <folder name>**

```
» NOTE: This will execute an action command with the following
  function:
  Restores and activates the specific user configuration. Each
  resulting config change will be logged as usual. Specify source
  folder. Synrax: restore_from_folder = folder_name. Important:
  This command does not restore the IP and factory configuration
  files.
  Type y to continue, else to quit: _
```

□ Type **y** to continue.

Using the Command Line Interface (CLI):

```
» executing..
  Restoring from folder <folder name> to becoming the running
  configuration.

  <status messages>

  ok - 29 files restored.

  -- END OF ACTION RESPONSE --
```

1.5.3 Using the MICROSENS Network Management Platform

The MICROSENS Management Platform NMP is a universal tool, which allows monitoring and configuring of all MICROSENS network devices. The software provides an easy to use GUI and several intelligent functions that support the administrator's daily work.

For more information about configuring MICROSENS switches with NMP please refer to the respective NMP documentation.

1.6 Getting the System Data

Each device has associated system data that

- identifies the device,
- authorises logins and
- provides further basic information.

System data contains

- device information
- login credentials
- module information (if applicable)
- basic settings
- feature status

System data is accessible via Web Manager and CLI, distributed over several views and paths.

Note:
For detailed information about parameters and values, please refer to the document "Product Manual Firmware, Generation 6" that is included in each firmware and can also be downloaded over the Web Manager's link "Documentation" in the navigation bar.

1.6.1 Device Information

Using the Web Manager:

□ Open the Web Manager.

□ Select the **Information** screen to view the following device information:

- Article Number
- Serial Number
- Firmware Version
- Hardware Version
- Uptime
- Local Time
- used MAC address
- used Boot media
- System ObjectID
- Custom Info

Note:
"Local Time" keeps the time since the device's clock was last set. If no time server is available or the time server synchronisation fails, the real time clock should be adjusted manually (see chapter 1.8 Synchronise System Time in the Network).

Using the Command Line Interface (CLI):

□ **`Device.Factory.`**

□ Press the Enter key to show the following and some additional device information:

```
» article_number
  serial_number
  device_mac
  hardware_version
  custom_info
```

□ **`Device.System.`**

□ Press the Enter key to show the following and some additional device information:

```
» last_boot_time
  uptime
  used_mac_address
  used_boot_media
```

□ **`Device.System.firmware.`**

□ Press the Enter key to show information about the active firmware:

```
» running_version     :  10.7.0a
```

Using the Command Line Interface (CLI):

```
build_date          :  2017-06-30 15:44:31
build_number        :  7130
```

- □ **Management.SNMP.device_info.sys_object_id**
- □ Press the Enter key to show the SNMP Enterprise sysOID:

```
» sys_object_id: <object ID>
```

- □ **Management.NTP.show_time_date**
- □ Press the Enter key to show the local time and date:

```
» Note: This will execute an action command with the following
  function:
  Show system time and date.
  Type y to continue, else to quit:
```

- □ Type **y** to continue.

```
» executing..
  Current time and date:
  Wed Oct 21 16:29:00 CEST 2015
  -- END OF ACTION RESPONSE --
```

1.6.2 Module Information

Note:
This function is especially useful for PLM Industrial Switches with expansion modules.

Using the Web Manager:

- □ Open the Web Manager.
- □ Select the **Hardware** screen, then select the tab **Info** to view the module information:
  - Unit Type
  - Article Number
  - Serial Number
  - Hardware Version
  - Project Number
  - occupied Slots
  - Description

Using the Command Line Interface (CLI):

□ **`Device.Hardware.module_info[*].`**

□ Press the Enter key to show the following module information:

```
» unit_type
  article_number
  serial_number
  hardware_version
  project_number
  occupied_slots
  description
```

1.6.3 Basic Setting

Using the Web Manager:

□ Open the Web Manager.

□ Select the **Information** screen to view the following basic settings information:

- Devicename
- Hostname
- Location
- Group
- Contact
- Inventory (may be used for device related inventory number)

Note:
Like serial number, MAC address and production codes, "Inventory" is stored inside the device and not on the removable medium.

Using the Command Line Interface (CLI):

□ **`Management.SNMP.device_info.`**

□ Press the Enter key to show the following basic settings information:

```
» sys_description
  sys_name
  sys_location
  sys_group
  sys_contact
  sys_object_id
```

Using the Command Line Interface (CLI):

□ **`Device.System.inventory`**

» `inventory:`

Note:
Like serial number, MAC address and production codes, "Inventory" is stored inside the device and not on the removable medium.

1.6.4 Feature Status

Using the Web Manager:

□ Open the Web Manager.

□ Select the **Information** screen to view the following feature status information:

- Temperature

Using the Command Line Interface (CLI):

□ **`Device.System.temperature`**

1.7 Determining the Device Status

The device status is a summary of the device's most important pieces of information. The device status consists of the following statuses:

- Info
  - Module Info (i.e. Type, Serial no., Hardware version)
  - Slot Info (i.e. board type, ID)
  - Port Info
- Supplies
  - Powersupply Configuration
  - Powersupply Status
- LEDs
  - LED Configuration
  - LED Status - Port LEDs
  - LED Status - Device LEDs
- Inputs
- Outputs
- Cable test
  - Cable Test Configuration
  - Cable Test Status
- TCAM Status

Note:
For detailed information about parameters and values please refer to the document "Product Manual Firmware, Generation 6", which is included in each software archive and can also be downloaded via the Web Manager's link "Documentation" in the navigation bar.

1.7.1 Info

This section shows general information about the modules that are inserted in the optional extension slots.

Note:
For module information please refer to section 1.6.2 Module Information.

Using the Web Manager:

□ Open the Web Manager.

□ Select the **Hardware** screen, then select the tab **Info** to view the slot and port information:

- Module Info
  - Unit Type
  - Article Number
  - Serial Number
  - Hardware Version
  - Project Number
  - occupied Slots
  - Description
- Slot Info
  - Board Type
  - Board ID
  - Version Bits
- Port Info
  - System Slot
  - Switch Port
  - User Slot
  - User Port
  - SNMP Port
  - SNMP Instance
  - Hardware Port
  - PoE
  - SFP
  - Interface Type
  - Properties

Using the Command Line Interface (CLI):

□ `Device.Hardware.module_info[*].`

□ Press the Enter key to show the following slot information:

Using the Command Line Interface (CLI):

```
» unit_type
  article_number
  serial_number
  hardware_version
  project_number
  occupied_slots
  description
```

□ **`Device.Hardware.slot_info[*].`**

□ Press the Enter key to show the following slot information:

```
» board_type
  board_id
  version_bits
```

□ **`Device.Hardware.port_info[<slot>/<port>].`**

Note:
Depending on the switch's number of ports it is not possible to show an overall view of all port parameters with **`.port_info[*/*]`**. In this case show individual parameters with **`.port_info[*/*].<parameter>`**.

□ Press the Enter key to show the following port information:

```
» system_slot
  switch_port
  user_slot
  user_port
  snmp_port
  snmp_instance
  hardware_port
  interface_type
  properties
```

1.7.2 Supplies

This section shows information about the switch's power supply (all power sources and PoE).

Using the Web Manager:

□ Open the Web Manager.

□ Select the **Hardware** screen, then open the tab **Supplies** to view the power supply status information:

- Power 1
- Power 2
- Running on PoE
- Fan Status

Using the Web Manager:

- □ To enable the power monitoring check the respective option in the table labelled **Powersupply Configuration**.
- □ To update the status table, click the button **refresh table**.

Using the Command Line Interface (CLI):

- □ **`Device.Hardware.`**
- □ Press the Enter key to show the following and some additional power supply information:

```
» power_supply_1_monitored
  power_supply_2_monitored
  power_supply_1_status
  power_supply_2_status
  running_on_poe
  fan_status
```

1.7.3 LEDs

This section shows information about the switch's LEDs status.

Using the Web Manager:

- □ Open the Web Manager.
- □ Select the **Hardware** screen, then open the tab **LEDs** to view the LED status information:
  - LED Status – Port LEDs (each with Ethernet and power ports)
    - Slot/Port
    - Symbol (Ethernet, Power)
    - Color (Ethernet, Power)
    - Blinking (Ethernet, Power)
  - LED Status – Device LEDs
    (every entry with parameters Symbol, Color, Blinking)
    - system_1
    - system_2
    - power_on_1
    - power_on_2
    - ring_1
    - ring_2
    - singnal_in_1 (only on switches with GPIO ports)
    - signal_in_2 (only on switches with GPIO ports)
    - signal_out_1 (only on switches with GPIO ports)
    - signal_out_2 (only on switches with GPIO ports)
- □ To update the status table, click the button **refresh table**.

Using the Command Line Interface (CLI):

□ **`Device.Hardware.port_leds[<slot>/<port>].`**

Note:
Depending on the switch's number of ports it is not possible to show an overall view of all port parameters with **`.port_leds[*/*]`**. In this case you can view individual parameters through **`.port_leds[*/*].<parameter>`**.

□ Press the Enter key to show the following port LED information:

```
» ethernet_color
  ethernet_blinking
  poe_color
  poe_blinking
```

□ **`Device.Hardware.device_leds.`**

□ Press the Enter key to show the following device LED information:

```
» system_1_color
  system_1_blinking
  system_2_color
  system_2_blinking
  power_on_1_color
  power_on_1_blinking
  power_on_2_color
  power_on_2_blinking
  ring_1_color
  ring_1_blinking
  ring_2_color
  ring_2_blinking
  signal_in_1_color
  signal_in_1_blinking
  signal_in_2_color
  signal_in_2_blinking
  signal_out_1_color
  signal_out_1_blinking
  signal_out_2_color
  signal_out_2_blinking
```

1.7.4 Inputs

This section is only used for switches that offer external signal inputs and outputs.

Note:
For more information about the GPIO ports please refer to the application note "Leveraging General Purpose I/O Ports with microScript".

Using the Web Manager:

□ Open the Web Manager.

□ Select the **Hardware** screen, then open the tab **Inputs** to view the signal input status information:

- Input 1
- Input 2

□ To update the status table, click the button **refresh table**.

Using the Command Line Interface (CLI):

□ **`Device.Hardware.io_signal_status.`**

□ Press the Enter key to show the following and some additional power supply information:

```
» input_1_alarm_active
  input_2_alarm_active
```

1.7.5 Outputs

This section is only used for switches that offer external signal inputs and outputs.

Note:
For more information about the GPIO ports please refer to the application note "Leveraging General Purpose I/O Ports with microScript".

Using the Web Manager:

□ Open the Web Manager.

□ Select the **Hardware** screen, then open the tab **Outputs** to view the signal output status information:

- Output 1
- Output 2

□ To update the status table, click the button **refresh table**.

Using the Command Line Interface (CLI):

□ **`Device.Hardware.io_signal_status.`**

Using the Command Line Interface (CLI):

□ Press the Enter key to show the following power supply information:

```
» output_1_relay_active
  output_2_relay_active
```

1.7.6 TCAM Status

This section offers information about the TCAM table entries.

Using the Web Manager:

□ Open the Web Manager.

□ Select the **Hardware** screen, then open the tab **TCAM Status** to view the status information:

- Index (“#”)
- Control File
- Description

□ To update the status table, click the button **refresh table**.

Using the Command Line Interface (CLI):

□ **`Device.Hardware.tcam_status[*].`**

□ Press the Enter key to show the TCAM status information:

```
» control_file
  description
```

1.8 Synchronise System Time in the Network

1.8.1 External NTP server

The switch starts with the date and the time at the point of connection (i.e. 2015-08-23 13:19:00). Per factory default (see section "Reset the Device to Factory Default Settings" on page 37), the NTP (Network Time Protocol) synchronisation is disabled. The device may be configured for automatic NTP synchronisation.

Using the Web Manager:

□ Open the Web Manager.

□ Select the **RTC/NTP** screen, then open the tab **Status** to view the current RTC/NTP settings.

□ Open the tab **Configuration** to enter the time server configuration.

□ Activate the option **NTP synchronisation enabled**.

□ Activate the option **NTP server per DHCP (option 42)**.

□ Activate the option **always trust server** to trust unreliable NTP servers.

Using the Web Manager:

□ Define the **Main Time Server** (i.e. 192.53.103.108)

Note:
If necessary, define another NTP server as **Backup Time Server**.

□ Define the **Synchronisation Interval (min.)** (i.e. 10080)

□ Select the **Time Zone** (i.e. Germany)

□ Click the button **apply to running configuration** to save the changes to the running configuration.

□ Click the button **Start** to begin synchronisation immediately.

Note:
To check whether the selected NTP server is available, enter its IP address an click the respective button **ping**.

Note:
Leave all other values default unless their functions and implications are familiar.

Using the Command Line Interface (CLI):

□ **`Device.Hardware.module_info[*].`**

□ Press the Enter key to show the RTC/NTP settings. Use the following commands to configure the RTC/NTP settings.

□ **`Management.NTP.main_ntp_server = 192.53.103.108`**

□ **`Management.NTP.backup_ntp_server = <IP address>`** `(optional)`

□ **`Management.NTP.sync_interval = 10080`**

□ **`Management.NTP.time_zone = Germany`**

Note:
To obtain a list of available time zones use **`Management.NTP.list_time_zones`**.

□ Start the time synchronisation with

`Management.NTP.sync_now`

1.8.3 Setting time and date manually

It is also possible to define the time settings manually.

Using the Web Manager:

- □ Open the Web Manager.
- □ Select the **RTC/NTP** screen, then open the tab **Configuration** to enter the time server configuration.
- □ In the section **Manual Time Settings** set the time and date and click the respective **apply to** button.

Using the Command Line Interface (CLI):

```
□ Device.System.set_time = 19:28:10
□ Device.System.set_date = 2015-10-21
```

1.9 Virtual Cable Test

1.9.1 Introduction

The MICROSENS Virtual Cable Test (VCT) is a measurement tool to obtain information about some physical parameters of copper based cable and connectors applied to MICRSOSENS G6 switches. Matching parameter values between all connected components is a mandatory prerequisite to ensure valid exchange of data between network devices.

The main parameters which influence the results of these measurements are:

- Impedance of the cable which should be a defined value of 100 Ohms and the
- Termination value of the remote port which ideally should have the same value.

Each deviation from these values leads to a degradation of signal quality which again – in the worst case – may lead to a loss of data.

Most scenarios described in the context of this document are based on the assumption that all impacted cables and connectors are free of faults. The case of defective connections will be treated in a separate section.

1.9.2 How does it work

The implemented measurement procedure is based on the Time Domain Reflectometry (TDR) method which again leverages a functional block of the switching circuit for copper ports of MICROSENS G6 switches. For measurement purposes, the switch sends a defined short signal (pulse) over the cable. This signal travels down the cable. Reaching the opposite end of the cable, one of – in general – three different behavioural patterns will occur. Each pattern depends on the kind of line termination at the end of the cable:

- **No termination of the remote end**
  If the remote end of the cable is not terminated (this can be interpreted as open ended or infinite termination), the signal will travel back along the cable bearing the same polarity and same amplitude as sent.

- **Short-circuit on remote end**
  If there is a short-circuit at the end (termination = 0), the signal will travel back along the cable bearing an inverted polarity but the same amplitude

- **Matched termination of the remote end**
  If the termination does exactly match the impedance of the cable, the signal will not be reflected along the line back to the switch

With relation to real conditions, the following aspects should be kept in mind:

- The polarity of the returned signal provides information about the kind of termination mismatch:
  - The terminating impedance is smaller than the line impedance.
  - The terminating impedance is identical with the line impedance.
  - The terminating impedance is the greater than the line impedance.
- The amplitude of the returned signal is an indicator for the amount of mismatch.
- Furthermore, signal loss and signal deformation along the cable are additional effects causing amplitude-reductions of the returned signal.
- The time the pulse needs to travel along the cable and to return to the sending switch can directly be used to calculate the (remaining) length of the cable. The algorithm is based on the assumption of constant pulse velocity along the line.

1.9.3 How will the properties of a 'Cable' be measured?

In comparison to a simple line of wire, a copper based networking cable is a rather complex item. Since networking cables are designed for high frequency data transfers, they have some specific properties. A standard networking cable consists of 4 twisted wire pairs. Each of these pairs has a defined line impedance of 100 Ohms. During a VCT-cycle all 4 pairs are measured. The *pair-individual* outcome of a measurement cycle requires interpretation.

Application of a VCT measurement cycle to an operative port will disturb the running data connection. Therefore, VCT measurement cycles may only be performed on networking ports which are in link down state. If a measurement cycle is forced to a port running an existing link, it will automatically lead to a link loss. After completion of the measuring cycle the previously existing link state will be re-established.

If a networking port of a MICROSESNS G6 switch is enabled and set to 'auto cable test enabled', a VCT measurement cycle will be performed periodically each 10 seconds as soon as the link at the particular port is down.

1.9.4 What are the results of a VCT cycle?

The results of a measuring cycle mainly depend on the line termination at the other end of the switch's outgoing line:

- On a well terminated pair there is no reflection, so that the time for travelling along the cable cannot be measured. The meaning of the term 'well terminated' will be explained below.
- In any other case, the cable length (as expected) can be calculated from time difference between sending the pulse and receiving of the pulses reflection.
- A weighted value representing the amplitude of the reflected pulse on each pair (range from -127 to 127) can be used to interpret the status of its particular pair. In

a second step, information on the status values of all 4 pairs can be calculated to obtain a cable status value.

The status of each pair, the total cable status and the summed reflection amplitudes are shown as status values alongside with a time stamp of last VCT measurement.

1.9.5 How will these values be interpreted?

As mentioned above, the amplitude value depends on the cable length. The way to interpret these values depends on the cable length, too. Therefore it is not possible to use static reference values. A well terminated cable may have a small-sized reflection which may be caused by the contacts of the RJ45 connector or by tolerances of the electrical elements inside the switch. If an amplitude value is below a certain threshold it can still be interpreted as 'well terminated'. However, the threshold itself depends on the cable length.

So the length is separated into several ranges to compare the reflections with separate values:

Length	Thresholds, when cable is				
	shorted	low terminated	pair ok	high terminated	open
0 m … 10 m	-127…-91	-90…-19	-18…+18	+19…+90	+91…+127
10 m … 50 m	-127…-81	-80…-17	-16…+16	+17…+80	+81…+127
50 m … 110 m	-127…-51	-50…-13	-12…+12	-13…+50	+51…+127
110 m … 140 m	-127…-31	-30…-11	-10…+10	+10…+30	+31…+127
140 m … ∞ m	-127…-21	-20…-7	-6…+6	+7…+20	+21…+127

According to this method it is possible to calculate an individual **pair status** as one of the following values:

Icon	Value	Meaning
●	Not available	Pair has not been measured yet.
✓	Pair OK	Pair is well terminated with conditions from the table above
●	Pair open	Reflection exceeds positive threshold from the table above
!	Low termination	Reflection is positive but less than threshold
!	High termination	Reflection is negative but less than threshold
●	Same pair shorted	Reflection underruns negative threshold
!	Cross pair shorted	Reflection underruns negative threshold

The generation of a status value for the complete cable requires some assumptions to achieve meaningful results. If the link is up, no measurement cycle takes place and each pair status is set to **'Pair OK'** as an assumption. In this case the **cable status** is assumed as **'Terminated'**. In all other cases the cable status will be calculated from pair status results:

Icon	Value	Meaning
!	Defective	At least one pair status is **‘Same pair shorted’**.
●	No cable	Cable length is detected as being 0 m.
●	Plugged in locally	All pairs are open and length is > 0 m.
!	Plugged in remotely	All four pairs are well terminated or terminated high.
!	Termination too low	All four pairs are terminated low.
✓	Terminated	At least two pairs are **‘Pair OK’** and length > 0 m Alternatively link is up.
?	Not available	No pair status is available and port is in link down state.

1.9.6 Connection Detection

A particular use case covers the physical detection of a connection without regard to an active link. VCT can be used for this purpose as described below:

If the cable status is detected as

- terminated (link up leads to termination too) or
- plugged in remotely (amplitude < threshold) or
- termination too low,

it is assumed that a device is connected. In any other case it is assumed that no device is connected.

To decide on the termination of powered-off devices some issues need to be considered. In the easiest case there is a device using one of the following termination techniques:

- Networking ports of older devices using a passive termination made out of real *passive* resistors. These resistors are always present, whether the device is powered-on *or* powered-off. The VCT always outputs the status ‘terminated’.
- Modern networking devices consist of an active termination – the terminating resistors are active components that change their electrical characteristics after being powered off. In this case they will set to high impedance. In consequence, the VCT cannot get a result out of a ‘terminated’ pair.

Nevertheless, in many cases the reflected amplitude of a connected device with active termination differs from the corresponding values achieved with measuring cycles applied to an actually existing open end cable. In most cases VCT is able to distinguish between these types of difference.

As each hardware is a little different, it is not predictable which reflection values are estimated and how to separate the results from an open end cable. This is the reason why the separation can be configured by defining the value of a reflection threshold:

If set to 0, the length sensitive default thresholds are used as described above, and in many cases this may be sufficient.

If there is need for an individual adaption, the threshold can be adopted to the connected device in control. The cable status provides a value for the reflection. This is the sum of all four reflected amplitudes, so theoretically there could be a value ranging from a minimum of -508 to a maximum of 508 (i.e. 4 cable pairs, each a value of either -127 or 127), which will not be reached in daily situations.

In case the default settings are not sufficient, the following procedures should be followed:

- Connect the powered-off device to the switch with the cable to use (a minimum length of 3 meters is required).
- Wait for 2-3 measurement cycles until the value of reflection remains quite stable and then note this value.
- Disconnect the device from the cable but keep this cable still connected to it's switchport.
- Wait for 2-3 measurement cycles again and note this second value. It should be a little higher than the first noted value. If it is not higher, you may have to repeat both measurements until there are reliable results.
- Now, for the selected port, calculate the median of those two values and apply the resulting value to the configuration value reflection threshold of this particular port.

From now on, the VCT uses this value to distinguish between pair statuses **'Pair open'** and **'High termination'**. This will lead to a separation of the two cable statuses **'Plugged in locally'** (i.e. open end) and **'Plugged in remotely'** (i.e. connected).

1.9.7 Events

There are two types of events supported by the VCT feature:

- One event type reports any change of a pair status. It is a set of parameters comprising the respective port number, the index of the pair with changed termination status and the index of the pair with changed length.
- The second event type is a pair of events that reports a cable connection status change, either **'Connection established'** or **'Connection lost'**.

The parameter of these events is the port number. The port's specific parameter of reflection hysteresis has influence on sending this type of event. With the help of this value, a permanent toggling of connection status due to variance in measured amplitudes can be avoided.

A **'Connection established'** event is triggered if the measured amplitude exceeds the result of the calculation of 'amplitude threshold' plus 'hysteresis'.

A **'Connection lost'** event is triggered if measured amplitude falls below the result of the calculation of 'amplitude threshold' minus 'hysteresis'.

Each event can be configured to trigger a microScript which is able to react to those changes in a way a customer may need.

Events can be enabled or disabled via the parameter **'Event generation'**.

- If this parameter is set to **'disabled'**, no events of VCT regarding types will occur.
- If it is set to **'any change'**, all three types will be triggered in case of matching conditions.
- If set to **'connections only'** only, the last both types will be triggered.

1.9.9 Hints

Some additional hints may help to understand the switches behaviour:

- If a port is disabled by management, no cable test is done.
- If auto cable test isn't enabled for a port, no VCT-events will be triggered.
- With the help of event settings and logging settings, events can be used to trigger syslog messages or SNMP traps which can be resolved by an external receiver.
- If the used interpretation of pair status to get a common cable status possibly does not match special needs, the status change event can be used to trigger a microScript. Here, an individual interpretation of all available pair status information can be implemented.

1.9.10 Perform the Virtual Cable Test

Using the Web Manager:

□ Open the Web Manager.

□ Select the **Hardware** screen, then open the tab **Cable Test** to view the cable test configuration and status information:

□ In the upper section of the dialogue, configure the cable test as follows:

- **Slot/Port**: Shows the respective slot/port affected by this configuration.
- **Auto Cable Test enabled**: When enabled, a cable test is performed each time the link goes down. The test is only performed for copper ports or dual media ports in copper mode.
- **Events enabled**: Set this option to **'any change'** or **'connections only'** to trigger a respective event type or **'disabled'** to disable the event trigger.
- **Reflection Threshold**: Sets the reflection threshold as it is described in section 1.9.6 "Connection Detection" on page 33.
- **Reflection Hysteresis**: Sets the reflection hysteresis as it is described in section 1.9.7 "Events" on page 34.
- **Test Now**: Starts a cable test. If the port is in link up status it will be forced to link down first. This will disrupt the current data traffic!

□ Click the button **apply to running configuration** to save the changes to the running configuration.

□ In the lower section, the dialogue shows the cable test statuses as follows:

- **Slot/Port**: Shows the respective slot/port for this status values.
- **Link**: Indicates the port role as uplink or normal port.
- **Cable**: Indicates the cable status.
- **Timestamp**: Shows the timestamp of the last executed cable test.
- **Pair 0 (1/2)**: Shows the pair status of the respective twisted pair wires.
- **Pair 1 (3/6)**: Shows the pair status of the respective twisted pair wires.

Using the Web Manager:

- **Pair 2 (4/5)**: Shows the pair status of the respective twisted pair wires.
- **Pair 3 (7/8)**: Shows the pair status of the respective twisted pair wires.
- **Reflection**: Indicates the weighted value of the reflection on all twisted pair cables on the respective slot/port.

□ To update the status table, click the button **refresh table**. For an automatic table refresh every five seconds, enable the respective option.

Using the Command Line Interface (CLI):

□ **`Device.Hardware.cable_test_config[<slot>/<port>].enable_auto_cable_test = {Enabled|Disabled}`**

□ **`Device.Hardware.cable_test_config[<slot>/<port>].event_generation = {DISABLED|ANY_CHANGE|CABLE_UNPLUGGED}`**

□ **`Device.Hardware.cable_test_config[<slot>/<port>].reflection_threshold = {0…508}`**

□ **`Device.Hardware.cable_test_config[<slot>/<port>].reflection_hysteresis = {0…65535}`**

To manually start a cable test enter

□ **`Device.Hardware.cable_test_config[<slot>/<port>].start_test_now`**

Note:
If the port is in link up status it will be forced to link down first. This will disrupt the current data traffic!

□ **`Device.Hardware.cable_test_status[<slot>/<port>].`**

Note:
Depending on the switch's number of ports it is not possible to show an overall view of all port parameters with **`.cable_test_status[*/*]`**. In this case show individual parameters with **`.cable_test_status[*/*].<parameter>`**.

□ Press the Enter key to show the following cable test information:

```
» update_time_stamp        :
  pair_0_state             :
  pair_0_distance_to_fault:
  pair_1_state             :
  pair_1_distance_to_fault:
  pair_2_state             :
  pair_2_distance_to_fault:
  pair_3_state             :
  pair_3_distance_to_fault:
  reflection_value         :
  cable_status             :
```

Note:
If output is truncated, a "~" character is displayed as the output line's last character.

Using the Command Line Interface (CLI):

□ **`Device.Port.status[*/*].link_up`**

```
» [slot/port].link_up
```

1.10 Reset the Device to Factory Default Settings

In some cases it can be required to set back the switch configuration to factory default settings. This may be necessary if a misconfiguration blocks any access to the switch (e.g. by incomplete VLAN settings) or a clean system is required.

The factory default settings are stored in the internal configuration folder "factory". This folder is always available and write-protected.

Using the Command Line Interface (CLI):

□ **`Management.Files.configuration.restore_from_folder = factory`**

```
» NOTE: This will execute an action command with the following
  function:
  Restores and activates the specified user configuration. Each
  resulting config change will be logged as usual. Specify source
  folder. Syntax: restore_from_folder = folder_name. Important:
  This command does not restore the IP and factory configuration
  files.
  Type y to continue, else to quit:
```

If no network access to the device is possible, the configuration can also be restored by pressing the system button on the device front panel. The button must be pressed continuously for approx. 10 sec. to initiate the restore process. The system LED is blinking blue during the operation.

Note:
The factory default settings do not affect the IP address settings. After a reset to factory default, the device is still accessible via the IP address configured before the restore. The IP address can always be reassigned using the NMP Auto-Discovery function.

2 Advanced Configuration

2.1 Configuration of the Device Ports

The ports are among a switch's most important components, so it is natural to configure them early. The port configuration can be subdivided into the following categories:

- Assigning an alias (a name) to a port.
- Assigning a role to a port (Local, Uplink, Downlink).
- Switching a port on or off.
- Selecting a port's medium on SFP combo ports (if available).
- Setting a port's physical layer parameters (bit rate, duplex mode, …).
- Enabling or disabling the port's power consumption control (EEE).
- Enabling or disabling loop protection on a port (default is disabled).

2.1.1 Port Alias

An alias is a human readable name for a port to facilitate operation, identification and documentation.

Using the Web Manager:

□ Open the Web Manager.

□ Select the **Ports** screen, then select the tab **Configuration**.

□ In the column **Alias**, enter or change the ports' aliases.

□ Click the button **apply to running configuration** to save the changes to the running configuration.

Note:
This also saves the changes to the device's non-volatile memory.

Using the Command Line Interface (CLI):

```
□ Device.Port.config[<slot/port>].alias = <new port alias>
  » [slot/port].alias: <new port alias>
```

2.1.2 Port Role

A port role is a typical example for how a port is used within the network topology. A port's role has implications on functions like DHCP snooping that rely on the port role. There are three main scenarios besides the default role:

- Local: Port is connected to a single device (also called "edge" role).
- Uplink: Port is connected to a core network (directly or indirectly).
  A core network is the network where important central nodes (like DHCP or file servers) are usually located.

- Downlink: Port is connected to a distribution/fringe network (directly or indirectly). A distribution network typically consists of a number of terminal devices that are clients with reference to the core network and that are connected to the core network via one or more workgroup switches.
- Default: In case of doubt, select the "default" role. This value (local, uplink, downlink) is preset and depends on port number and device type.

Using the Web Manager:

□ Open the Web Manager.

□ Select the **Ports** screen, then select the tab **Configuration**.

□ In the column **Role**, select the new port role from the drop-down list.

□ Click the button **apply to running configuration** to save the changes to the running configuration.

Using the Command Line Interface (CLI):

□ **`Device.Port.config[<slot/port>].role = {DEFAULT|LOCAL|UPLINK|DOWNLINK}`**

```
» [slot/port].role: <new port role>
```

2.1.3 Port Enabling

A port can administratively be enabled or disabled for operation. When disabled, the respective port is shut down.

Using the Web Manager:

□ Open the Web Manager.

□ Select the **Ports** screen, then select the tab **Configuration**.

□ In the column **enabled**, mark the checkbox to enable the port, or unmark it to disable the port.

□ Click the button **apply to running configuration** to save the changes to the running configuration.

Using the Command Line Interface (CLI):

□ **`Device.Port.config[<slot/port>].port_operation = {Enabled|Disabled}`**

```
» [slot/port].port_operation: <new port operation mode>
```

2.1.4 Port Medium (SFP Combo Ports Only)

Some device types are equipped with SFP combo ports. A SFP combo port offers to use either its so-called TX or copper port (a RJ-45 socket) or its SFP socket (usually for a fiber SFP).

With the configuration setting "Medium", specify which socket of a given port will be used. This usage may be preferred or forced.

- "Prefer <Medium>": Both media fiber and copper are accepted but the medium configured as preferred is chosen if available.
- "Force <Medium>": Only the medium configured as forced is accepted, the other one is rejected.

Using the Web Manager:

□ Open the Web Manager.

□ Select the **Ports** screen, then select the tab **Configuration**.

□ In the column **Medium**, select the port's dual media mode settings from the drop-down list.

□ Click the button **apply to running configuration** to save the changes to the running configuration.

Using the Command Line Interface (CLI):

□
```
Device.Port.config[<slot/port>].dual_media_mode =
{FIBER_PRIORITY|COPPER_PRIORITY|FORCE_FIBER|FORCE_COPPER}
```

```
» [slot/port].dual_media_mode: <new port media mode>
```

2.1.5 Port Connection Settings

A port's basic connection settings encompass the desired speed (bitrate), its duplex mode and whether or not these values are to be negotiated by the switch and its connection partner automatically.

The features "Flow Control" and "Medium Crossing" are also related to the connection settings.

Using the Web Manager:

□ Open the Web Manager.

□ Select the **Ports** screen, then select the tab **Configuration**.

□ In the column **A-Neg.**, enable or disable Auto Negotiation.

If enabled, the two connection partners will auto-negotiate the connection's speed, the duplex mode and the flow control setting. No further configuration of these parameters is necessary.

Using the Web Manager:

□ In the column **Speed**, use the radio buttons to select the desired speed.

Note:
When Auto Negotiation is enabled, the port will advertise the configured speed as its highest possible speed. Therefore, MICROSENS recommends to leave the speed at the highest setting.

For switches supporting SFP ports, the setting "SFP auto" selects the fastest data rate which is supported by the inserted SFP supports.

□ In the column **full Duplex**, enable or disable the Full Duplex mode.

Note:
When Auto Negotiation is enabled, the port will only advertise its duplex mode capability if the Full Duplex setting is locally configured. Therefore, MICROSENS recommends to leave the Full Duplex setting enabled.

□ In the column **Flow Control**, enable or disable flow control (according to IEEE 802.3x).

Note:

- Flow control is only supported on full duplex connections.
- When Auto Negotiation is enabled, the port will only advertise its flow control capability if the Flow Control setting is locally configured.

□ In the column **MDI(X)**, use the drop-down list to select the ports' MDI(X) settings.

Note:
If set to "Auto", the port will automatically adapt its transmit/receive circuit pins to the cable type in use and the connection partner's transmit/receive circuit pin settings.

Conversely, the values "MDI" and "MDIX" set the port's mode to the respective pinout.

□ Click the button **apply to running configuration** to save the changes to the running configuration.

Using the Command Line Interface (CLI):

□
```
Device.Port.config[<slot/port>].auto_negotiation =
{Disabled|Enabled}
```

□
```
Device.Port.config[<slot/port>].speed =
{10_MBIT|100_MBIT|1000_MBIT|SFP_AUTO}
```

□
```
Device.Port.config[<slot/port>].full_duplex = {Disabled|Enabled}
```

□
```
Device.Port.config[<slot/port>].flowcontrol = {Disabled|Enabled}
```

□
```
Device.Port.config[<slot/port>].mdi_mode =
{AUTO|FORCE_MDI_STD|FORCE_MDIX}
```

2.1.6 Port EEE (Energy Efficient Ethernet)

Ethernet connections in 1000Base-T permanently require a significant amount of power, even if no data is transmitted. To reduce power consumption, 1000Base-T segments with Energy Efficient Ethernet support (IEEE 802.3az) can enter a low power idle mode if no data is transmitted. This mode can reduce power comsumption significantly.

Note:
EEE must be supported by both ports of a segment. If only one port supports EEE, standard power mode is used.

Using the Web Manager:

- □ Open the Web Manager.
- □ Select the **Ports** screen, then select the tab **Configuration**.
- □ In the column **EEE**, enable or disable the Energy Efficient Ethernet option.
- □ Click the button **apply to running configuration** to save the changes to the running configuration.

Using the Command Line Interface (CLI):

□
```
Device.Port.config[<slot/port>].energy_efficiency =
{Disabled|Enabled}
```

2.1.7 Port Loop Protection

Local loop protection detects parallel links to the same switch or loops between local ports to avoid endless packet streams. If enabled, the switch will temporarily disable or shut down data forwarding (port is set into blocking mode) should an Ethernet loop condition occur.

Note:
This only happens if no redundancy protocol is used on the respective port. For more information about redundancy protocols please refer to the Application Note "Using Redundancy Protocols with G6 Devices".

Using the Web Manager:

- □ Open the Web Manager.
- □ Select the **Ports** screen, then select the tab **Configuration**.
- □ In the column **Loop Prot.**, enable or disable the loop protection option.
- □ Click the button **apply to running configuration** to save the changes to the running configuration.

Using the Command Line Interface (CLI):

□
```
Device.Port.config[<slot/port>].loop_protection =
{Disabled|Enabled}
```

2.2 Port Security

The switch offers a wide range of port-based access control related features. There are different ways to configure the port-based access control:

- IEEE 802.1X Authentication, including:
  - Learned MAC time out
  - Dynamic VLAN
- RADIUS MAC Authentication, including:
  - Learned MAC time out
  - Dynamic VLAN
- MAC locking (including MAC learning)
- Limited number of MACs
- IP address logging

Generally administrate the port security with Web Manager and CLI.

Using the Web Manager:

□ Open the Web Manager.

□ Select the **Port Access** screen, then select the tabs **Basic Configuration**, **Port Configuration** and **MAC Lock Table**.

Using the Command Line Interface (CLI):

□ To display the actual port security settings, enter

```
Protocol.PACC.
```

and press the Enter key.

□

```
enable_port_access_cont~: Disabled
reauthentication_period : 0
nas_identifier          :
mac_separator_char      : :
mac_spelling            : LOWER_CASE
mac_password_source     : USE_MAC
mac_password_string     : NOPASSWORD
primary_auth_server_name:
primary_acct_server_name:
fallback_auth_server_na~:
fallback_acct_server_na~:
server_down_timeout     : 120
```

Note:
In this Application Note we show two configuration examples for MAC locking and IEEE 802.1X authentication to demonstrate the basic configuration of port-based access control. For further information about authentication facilities, standards, parameters and options, please refer to the chapter “Port-based Access Control” in the document “Product Manual

Firmware, Generation 6" that is included in each software archive and can also be downloaded via the Web Manager's link "Documentation" in the navigation bar.

Note:
Ensure that the switch's uplink port and the port that is currently used to administrate the switch will not be blocked once Port Access is generally enabled. Otherwise the administrator may be locked out!

2.2.1 MAC-based Port Access Control

The method of "MAC locking" allows multiple users to be authenticated based on their respective MAC address. Therefore, MAC addresses can be configured and assigned to specific ports manually or automatically.

In small businesses, using MAC-based PACC might be reasonable as far as the effort is concerned.

To grant port access for a MAC address manually, follow these steps.

Using the Web Manager:

- □ Open the Web Manager.
- □ Select the **Port Access** screen, then select the tab **MAC Lock Table**.
- □ In the field **new unique name** specify a **Value** as a name for the new MAC table entry (e.g. "Office_1").
- □ Click the button **generate entry**. The new entry with default values appears in the MAC table.
- □ Enter a valid **MAC Address** for this entry (e.g. "0a:1b:2c:3d:4e:5f").
- □ Enter the permitted ports for this entry in form of a hexadecimal port mask.

  Note:
  Every port represents a corresponding bit position. The binary "0001" means "Port 1/1", the binary "0010" means "Port 1/2" and so on.
  So "1111" represents ports 1/1 to 1/4 in binary, which is "0xf" in hexadecimal notation.
- □ Click the button **apply to running configuration** to save the changes to the running configuration.
- □ Change to the tab **Basic Configuration** and check the option **enable port access control**.
- □ Click the button **apply to running configuration** to save the changes to the running configuration.
- □ Change to the tab **Port Configuration** and change the **authorize mode** of the respective port to "VIA_MAC_TABLE".
- □ Click the button **apply to running configuration** to save the changes to the running configuration.
- □ To view the actual port status, change to the tab **Port Status** and click the button **refresh**.

Using the Command Line Interface (CLI):

□ **`Protocol.PACC.authorised_macs[*].name = Office_1`**

□ **`Protocol.PACC.authorised_macs[Office_1].name = Office_1`**

□ **`Protocol.PACC.authorised_macs[Office_1].mac_address = 0a:1b:2c:3d:4e:5f`**

□ **`Protocol.PACC.authorised_macs[Office_1].permitted_ports = 1/1, 1/2, 1/3, 1/4`**

Note:
Alternatively, the specification of permitted ports is possible in the form of a hexadecimal port mask: Every port represents a corresponding bit position. The binary “0001” means “Port 1/1”, the binary “0010” means “Port 1/2” and so on.

So “1111” represents ports 1/1 to 1/4 in binary, which is “0xf” in hexadecimal notation. Therefore, the configuration command above could be written as follows:

□ **`Protocol.PACC.authorised_macs[Office_1].permitted_ports = 0xf`**

□ Activate the port-based access control with

```
Protocol.PACC.enable_port_access_control = Enabled
```

□ Set the authorise mode at desired ports with

```
Protocol.PACC.port_config[1/1].authorize_mode = VIA_MAC_TABLE
```

□ To view the actual port status, enter

```
Protocol.PACC.port_status[*].
```

and press the Enter key.

```
» Parameter         : [1/1]     [1/2]      [1/3]      [1/4]
  authorization_st~: UNDEFINED UNDEFINED UNDEFINED UNDEFINED
  authorization_mo~: NONE      NONE      NONE      NONE
  user_mac         :
  user_name        :
  vlan_alias       :
  vlan_id          : 0         0         0         0
  last_state_change: 2015-10-~ 2015-10-~ 2015-10-~ 2015-10-~
  number_of_macs_t~: 0         0         0         0
  number_of_learne~: 0         0         0         0
```

2.2.2 IEEE 802.1X Authentication

With IEEE 802.1X authentication, multiple users can be authenticated using a central RADIUS server based on an username/password combination or a certificate.

By using RADIUS, a network wide authentication database can be used. This eliminates the need to configure every unit separately.

Note:
The following example shows the configuration of IEEE 802.1X authentication using a username/password combination. It is assumed that the respective user's login data already exists in the RADIUS authentication database.

Using the Web Manager:

□ Open the Web Manager.

□ Select the **Authentication Server** screen.

□ If the respective RADIUS server is not configured yet, click on the button **add table entry**.

□ Enter the server's data as required:
- **Name** (e.g. "RADIUS_Sales"),
- **Type** ("RADIUS"; leave this default value of the new table entry),
- **Address** (e.g. "192.168.0.210"),
- **UDP Port** (e.g. "1812"; leave the default value of the new table entry unless there are different RADIUS server setting)
- **shared secret** (as configured in the RADIUS server for this RADIUS client)

Note:
Optionally configure a second RADIUS server as fallback server.

□ Click the button **apply to running configuration** to save the changes to the running configuration.

□ Select the **Port Access** screen, then select the tab **Basic Configuration**.

□ Check the option **enable port access control**.

□ Define the **primary auth server name** (e.g. "RADIUS_Sales").

□ Optionally define a **fallback auth server name** as it is configured in the **Authentication Server** screen.

□ Click the button **apply to running configuration** to save the changes to the running configuration.

□ Change to the tab **Port Configuration**.

□ For **Authorized Mode** of the respective port, select "IEEE 802.1X via RADIUS" from the drop-down list.

□ Click the button **apply to running configuration** to save the changes to the running configuration.

□ To view the actual port status, change to the tab **Port Status** and click the button **refresh** at the respective list.

Using the Command Line Interface (CLI):

□ Configure the respective RADIUS server:

```
Management.RADIUS.server[*].name = RADIUS_Sales
```

Using the Command Line Interface (CLI):

□ **Management.RADIUS.server[RADIUS_Sales].server_type = RADIUS**

□ **Management.RADIUS.server[RADIUS_Sales].host_address = 192.168.0.210**

□ **Management.RADIUS.server[RADIUS_Sales].udp_port = 1812**

Note:
Leave the default value for UDP port unless there is a different RADIUS server setting.

□ Enter the shared secret as it is configured in the RADIUS server for this RADIUS client:

```
Management.RADIUS.server[RADIUS_Sales].shared_secret =
<RADIUS server's shared secret>
```

Note:
Optionally configure a second RADIUS server as fallback server.

□ Activate the port-based access control with

```
Protocol.PACC.enable_port_access_control = Enabled
```

□ Define the primary authentication server:

```
Protocol.PACC.primary_auth_server_name = RADIUS_Sales
```

□ Optionally define a fallback authentication server:

```
Protocol.PACC.primary_auth_server_name = <fallback server name>
```

□ Select the authorised mode for the respective port:

```
Protocol.PACC.port_config[<slot>/<port>].authorized_mode =
802_1X_VIA_RADIUS
```

□ To view the actual port status, enter

```
Protocol.PACC.port_status[*/*].
```

and press the Enter key.

```
» Parameter          : [1/1]     [1/2]       [1/3]      [1/4]
  authorization_st~: UNDEFINED UNDEFINED UNDEFINED UNDEFINED
  authorization_mo~: NONE      NONE      NONE      NONE
  last_state_change: 2017-11-~ 2017-11-~ 2017-11-~ 2017-11-~
  number_of_macs_t~: 0         0         0         0
  number_of_learne~: 0         0         0         0
```

2.3 Frame Forwarding

MICROSENS switches forward frames according to their internal forwarding database to help reduce the network's load to a minimum. This database consists of several parts. The dynamic part of the forwarding database takes care of learning (and aging) unicast source addresses and helps forwarding frames based on their destination address, purging them due to their expired lifespan or flooding frames from so far unknown source addresses.

The forwarding database can also be populated manually (the static part).

Ethernet frames are usually forwarded based on their destination MAC address. A received frame's destination MAC address can fall into four categories:

- **Known unicast address (has already been learned as source address)**
  Frames with a known unicast destination address are only forwarded to the port on which the MAC address has already been learned as the source address. This way, the switch saves the network components connected to the other switch ports from unnecessary traffic.
- **Unknown unicast address**
  By default, only frames with unknown unicast destination addresses (e.g. not yet learned as source addresses or already aged out) are forwarded to all ports that are member of the same VLAN (except the receiving one). This behavior is called 'flooding'. In most cases, the traffic is bidirectional and the destination address will be learned as the source address of a frame received as traffic in the reverse direction.
- **Multicast address**
  Multicast addresses are also forwarded to all switch ports of the same VLAN because they are intended to reach multiple destinations at once. Due to the switches' flooding behavior, multicast frames can place a considerable load on a network. MICROSENS switches offer several features to control the forwarding of multicast frames. I.e., it is possible to limit the forwarding to only those ports where known receivers that want to receive traffic with a specific multicast destination address are connected. These features can be static (configured manually) or dynamic (protocols that take care of solicited multicast traffic).
- **Broadcast address**
  A broadcast address is a special case of multicast addresses, meaning that broadcast frames share most properties with multicast frames.

The switches maintain a table of MAC addresses (with VLAN filtering enabled: one table per VLAN). These MAC address tables are the base for deciding on how to forward a received frame.

2.3.1 Displaying the MAC table

Using the Web Manager:

□ Open the Web Manager.

□ Select the **MAC Tables** screen, then select the tab **MAC table**.

Using the Command Line Interface (CLI):

□ **`Device.MAC.mac_table[*].`**

```
» Parameter :  [00:03:c~ [00:03:c~ [00:03:c~ [00:03:c~ [00:03:c~
  mac       :  00:03:c1~ 00:03:c1~ 00:03:c1~ 00:03:c1~ 00:03:c1~
  port      :  1/1       1/4       1/2       1/3       1/1
  state     :  LEARNED   MULTICAST MULTICAST MULTICAST LEARNED
  vlan      :  0         0         0         0         0
  Hit q to quit or any other key to continue with next indices ..
```

2.3.2 Display Filters for MAC Address

The easiest way to get an overview about the MAC table's content is by applying a display filter. Apply any of the following filter parameters simultaneously to drill down on the entries that are to be examined:

- Entry type
- Address type
- Address value
- Port selection
- VLAN selection

The filters are disabled by default, showing all MAC table entries.

Note:
Deleting all learned MAC addresses from the MAC address table without rebooting the device is only possible with the CLI.

Using the Web Manager:

□ Open the Web Manager.

□ Select the **MAC Tables** screen, then select the tab **MAC table**. The following settings are configured in the section **Filter Settings**.

□ In the row **Entry Type**, mark or unmark the checkbox "enabled". If enabled, select one of the radiobuttons "dynamic" or "static".

□ In the row **Address Type**, mark or unmark the checkbox "enabled". If enabled, select one of the radiobuttons "Unicast" or "Multicast".

□ In the row **Address (hex)**, mark or unmark the checkbox "enabled". If enabled, fill in the MAC address mask.

Note:
It is possible to use single bytes to filter MAC addresses with this particular address element. E.g. using only the first three bytes from the left will filter all vendor specific MAC addresses.

□ In the row **Port Selection**, mark or unmark the checkbox "enabled". If enabled, select any of the port checkboxes.

□ In the row **VLAN selection**, mark or unmark the checkbox "enabled". If enabled, enter a list of VLAN IDs or ranges.

Using the Web Manager:

□ Click the button **refresh table** to apply the display filter to the current MAC table. The results are shown in the table below the button.

Additionally, it is possible to hide MAC addresses on uplink and downlink ports to reduce the number of shown table entries and to increase MAC table reading via SNMP.

□ Select the **MAC Tables** screen, then select the tab **Configuration**.

□ In the section **SNMP-BRIDGE-MIB Filter**, activate the option **Hide MACs on uplink/downlink Ports (port role)**.

□ Click the button **apply to running configuration** to save the changes to the running configuration.

Using the Command Line Interface (CLI):

□ **Device.MAC.filter_mac = {00…ff[:00…ff[:00…ff[:00…ff[:00…ff[:00…ff]]]]]}**

Note:
Entering first bytes of a MAC address will list the MAC addresses that start with these address parts.

Entering **Device.MAC.filter_mac =** (without MAC address) will list all MAC addresses stored in the MAC address table.

```
» BEGIN ALL MAC addresses:
  MAC                  Port     State          VLAN
  00:03:cd:03:00:d9    1/1      LEARNED        0
  00:0c:29:04:5d:6d    1/1      LEARNED        0
  01:00:0c:cc:cc:cc    2/1      MULTICAST      0
  END
```

□ **Device.MAC.filter_port = <port number>**

Note:
The shorthand port format like “1” for port 1/1 may be used, even a range like “1-3” is possible.

```
» BEGIN Ports matching 1-3:
  MAC                 Port     State        VLAN
  00:60:a7:11:22:33   1/2      MULTICAST    0
  00:60:a7:11:22:33   1/3      MULTICAST    0
  00:60:a7:11:22:33   1/1      MULTICAST    0
  END
```

Using the Command Line Interface (CLI):

□ **`Device.MAC.filter_vlan = <VLAN ID list>`**

Note:
Supply VLAN ID as single parameter ("1") or parameter list ("1,2,3") or parameter range ("100-300").

□ **`Device.MAC.filter_user_ports`**

Note:
This action needs no parameters and lists only MAC addresses associated with user ports.

```
» NOTE: This will execute an action command with the following
  function:
  Filter MAC table to show only MACs associated with user ports.
  This excluded the links. This view eliminates MACs which are not
  of local interest. No parameter is required.
  Type y to continue, else to quit:
  BEGIN Ports matching 1-4:
  MAC                Port      State      VLAN
  00:a0:57:1a:aa:cd  1/1       LEARNED    0
  00:a0:57:1a:12:58  1/4       MULTICAST  0
  00:a0:57:3a:a2:23  1/2       MULTICAST  0
  00:a0:57:44:3a:28  1/3       MULTICAST  0
  68:f7:28:fc:a8:94  1/1       MULTICAST  0
  00:a0:57:11:f2:85  1/1       LEARNED    0
  00:a0:57:25:d4:ff  1/1       LEARNED    0
  00:a0:57:28:a6:86  1/2       MULTICAST  0
  00:a0:57:ab:2e:e8  1/3       MULTICAST  0
  68:f7:28:fc:8a:4c  1/1       LEARNED    0
  END

  -- END OF ACTION RESPONSE --
```

□ **`Device.MAC.filter_custom = <parameter>`**

This action requires some guidelines to work:

- -m <MAC>: a MAC address
- -s <SEPARATOR>: determines the MAC adresses' separator
- -p <PORT>: a port number
- -v <VLAN>: a VLAN ID

□ To filter multicast MAC addresses only, use the following parameters:

```
Device.MAC.filter_multicast_vlan = <VLAN ID>
Device.MAC.filter_multicast_port = <Slot/Port,Port,Port-Port>
```

□ This action deletes all learned MAC addresses from the MAC address table:

```
Device.MAC.clear_learned_mac_table
```

Using the Command Line Interface (CLI):

- This action deletes all MAC addresses with a given VLAN ID from the MAC address table:

  ```
  Device.MAC.clear_mac_table_for_vlan = <VLAN ID>
  ```

- To hide the MAC addresses on uplink and downlink ports, use the following parameter:

  ```
  Device.MAC.hide_macs_on_link_ports = Enabled
  ```

Note:
This function only works on the SNMP BRIDGE-MIB's "dot1dTpFdbTable" and "dot1qTpFdbTable".

2.3.3 Displaying Authorised MAC addresses

Besides the normal learned or static configured MAC addresses in the MAC address table, MICROSENS G6 devices hold a special table with MAC addresses that are currently authorised via port access control.

Note:
For more information about port access control please refer to section "2.2 Port Security".

Using the Web Manager:

- Open the Web Manager.
- Select the **MAC Tables** screen, then select the tab **authorized MACs**.

Using the Command Line Interface (CLI):

- **Device.MAC.currently_authorized_macs[*].**

```
» database:  [1]                  [2]
  mac     :  00:03:cd:11:22:33    00:03:cd:22:33:44
  port    :  1/6                  1/2
  state   :  LEARNED              LEARNED
  vlan    :  0                    0
```

2.3.4 MAC Address Aging

As given MAC addresses may disappear from the network segment (i.e. a device has been unplugged from the network), the MAC address table removes entries once they have reached a maximum age. This avoids cluttering the table with useless entries and makes room for the addition of new entries (called "learning") or still existing entries ("relearning").

Notes:

- Even MAC addresses that are in use are subject to aging. The switch relearns the MAC address immediately when it appears as a frame's source address. In the meantime, the switch floods frames with the respective destination MAC address.
- A reboot empties the MAC address table.

Note:
The MAC Table can also be cleared using the following CLI commands:

```
Device.MAC.clear_learned_mac_table
Device.MAC.clear_mac_table_for_vlan = <VLAN ID>
```

Using the Web Manager:

□ Open the Web Manager.

□ Select the **MAC Tables** screen, then select the tab **Configuration**.

□ In the table **Aging Time**, enter a value between 15 and 3825 for "global Aging Time" (unit: seconds).

Note:
The parameter "Global Aging Time" sets an upper limit for the so-called "Used Aging Time". The "Used Aging Time" can be shorter than the "Global Aging Time", e.g. when requested by RSTP.

□ Click the button **apply to running configuration** to save the changes to the running configuration.

Using the Command Line Interface (CLI):

```
□ Device.MAC.global_aging_time = {15…3825}
```

Note:
To show the actual used aging time, use

```
Device.MAC.used_aging_time
   » used_aging_time: 3825
```

2.4 LACP (Link Aggregation Control Protocol)

The **LACP** (Link Aggregation Control Protocol in accordance with IEEE 802.3ad) is a network protocol for dynamic link aggregation between two network nodes. The resulting logical link of two or more aggregated connections (formerly also called "group", "trunk" or "port channel") offers higher bandwidth as well as redundancy in case of one of the physical connections breaking down. In either case, the load is distributed automatically among the remaining physical connections. A link aggregation is configured by combining at least two existing parallel redundant connections between two devices to form one logical connection based on priority settings. Any combination of copper and fiber connections can be used for a link aggregation, assuming all related ports' data rates match and are in full-duplex mode.

The LACP system priority is used to form the so-called "**LACP System ID**" by appending the switch's base MAC address to the configured LACP system priority. For any given connection with parallel lines, the switch with the lowest LACP System ID decides which ports are included in the aggregation. This mechanism is similar to the priority characteristics used with Spanning Tree Protocols.

Note:
Although LACP offers redundancy in case of physical connection malfunction, the original intention of LACP is to gain higher bandwidth due to parallel connections. For more information about genuine redundancy protocols, please refer to the Application Note "Using Redundancy Protocols with G6 Devices".

The LACP implementation of MICROSENS G6 devices supports a maximum of 16 aggregation links with the channel ID ranging from 1 to 16. Before using LACP, at least one group has to be defined.

In addition, MICROSENS switches also offer static link aggregation.

2.4.1 Setup Steps for Static Link Aggregation

Static link aggregation is useful for partner devices that do not support LACP. When setting up a static link aggregation, avoid loops during the configuration by

- making sure only one of the parallel physical connections is in operation,
- manually including each port in the planned link aggregation,
- doing this on the devices on both ends of the link aggregation,
- setting at least one of the participating devices into active LACP operational mode and
- not enabling (e.g. plugging in) the parallel connections until completing these steps.

Note:
In active mode the device will send LACP PDUs out on the configured links with the purpose of initiating a negotiation. In passive mode, it will only reply to LACP PDUs. Therefore, it is important that at least one switch works in active mode.

2.4.2 Pitfalls when using LACP

Using LACP can cause network problems when disregarding some basic requirements:

- Configure LACP on all devices first and plug in cables last. Otherwise a network loop occurs unintentionally.

- Before removing a switch’s port from the aggregation trunk, remove the respective network cable. Otherwise a network loop will occur.
- At least one LACP device has to be configured in active mode. If not, the devices do not exchange LACP packets and the link aggregation never starts.

2.4.3 Example: Setting up Dynamic Link Aggregation

Unlike static link aggregation, LACP uses dynamic link aggregation to negotiate which ports are to be included in an aggregation. This also helps with avoiding loops. MICROSENS recommends using the “dynamic” setting.

Assuming the physical link between the workgroup switch (Figure 1, ②) and the core switch (Figure 1, ③) consists of old network cables that only support a bit rate of 100 Mb/s; Nevertheless, the network administrator is asked to provide higher throughput and redundancy at minimal cost. As quick fix until a long-term solution is installed, the administrator decides to use a second network cable (already existing) to form a link aggregation with a maximum bit rate of 200 Mb/s and a connection redundancy. Since the second cable is already in place and the switches both have an unused port, the upgrade can be made quickly and at minimal cost.

Element	Description
①	Arbitrary Client Computer, Representing a Workgroup
②	Workgroup Switch Core Uplink: Port 1/5 Unused/reserve: Port 1/6
③	Core Switch Workgroup Downlink: Port 2/1 Unused/reserve: Port 2/2
④	Administration Workstation
⑤	Server

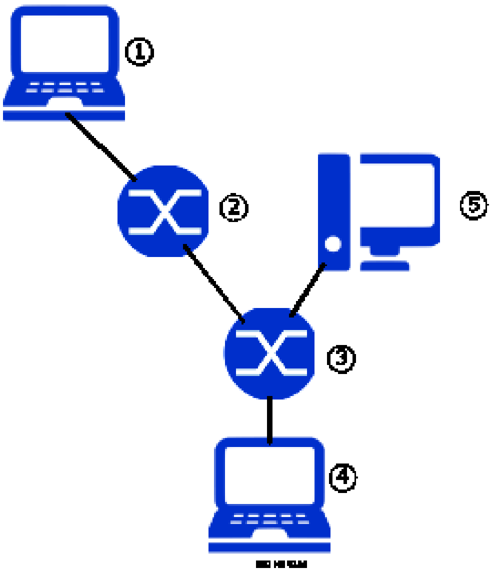


Figure 1: Simplified Company Network

General network requirements:

- Switch ③ shall be in control of the link aggregation.
- The switch-over time needs to be as short as possible.
- No loops shall form during the reconfiguration.

Planning Steps

- Combine switch ②’s ports 1/5 and 1/6 to a link aggregation.
- Combine switch ③’s ports 2/1 and 2/1 to a link aggregation.
- Assign a system priority that is lower than the deafult to switch ③.
- Set the transmit interval to 1 second for both switches.
- Configure the link aggregation first and plug in the cables last.

Overview

Switch	Trunk ID	Trunk Name	Port	Trunk ID	LACP enabled	Link Agg.	System Priority	Oper. Mode	Transmit Interval
③	1	Workgroup 1	2/1	1	Enabled	Dynamic	32768	Active	1 sec
			2/2	1					
②	1	Workgroup 1	1/5	1	Enabled	Dynamic	65535	Active	1 sec
			1/6	1					

Note:
The "Trunk ID" and "Trunk Name" do not necessarily need to be the same on both switches but it simplifies the administration because the link aggregation between these switches is obvious upon first sight.

Sequence

This leads to the following sequence:

- Make sure the second network cable is unplugged at switch ③ (Port 2/2) or switch ② (Port 1/6).
- Configure Switch ③.
- Configure Switch ②.
- Plug in the second network cable between switch ③ and switch ②.

Configuration Steps

Note:
Make sure the second network cable is unplugged at switch ③ (Port 2/2) or switch ② (Port 1/6).

Using the Web Manager:

□ Open the Web Manager on the respective switch.

□ Select the **LACP** screen, then select the tab **Trunk Configuration**.

□ For **Trunk ID** "1", assign the name "Workgroup 1" and mark the checkbox **enable**.

□ Click the button **apply to running configuration** to save the changes to the running configuration.

□ Select the tab **Port Configuration**.

On switch ③:

□ Assign both **Port** "2/1" and "2/2" the **Trunk-ID** "1".

On switch ②:

□ Assign both **Port** "1/5" and "1/6" the **Trunk-ID** "1".

On the respective switch:

□ Click the button **apply to running configuration** to save the changes to the running configuration.

Using the Web Manager:

□ Select the tab **Basic Configuration**.

□ Mark the checkbox **LACP enabled**.

□ Set the value for **Link Aggregation** at "dynamic".

Note:
This is the default value.

On switch ③:

□ Set the value for **System Priority** to "32768".

On switch ②:

□ Set the value for **System Priority** to "65535".

Note:
This is the default value.

On the respective switch:

□ Set the value for **Operational Mode** at "active".

Note:
This is the default value.

□ Set the value for **Transmit Interval** at "fast (1 sec)".

□ Click the button **apply to running configuration** to save the changes to the running configuration.

Now plug in the second network cable between switch ③ and switch ②.

Using the Command Line Interface (CLI):

□ Open the CLI on the respective switch.

□ **`Protocol.LACP.trunk_config[1].name = Workgroup 1`**

□ **`Protocol.LACP.trunk_config[1].trunk_enable = Enabled`**

On switch ③:

□ **`Protocol.LACP.port_config[2/1].trunk_id = 1`**
□ **`Protocol.LACP.port_config[2/2].trunk_id = 1`**

On switch ②:

□ **`Protocol.LACP.port_config[1/5].trunk_id = 1`**
□ **`Protocol.LACP.port_config[1/6].trunk_id = 1`**

On the respective switch:

□ **`Protocol.LACP.config.link_aggregation = DYNAMIC`**

Using the Command Line Interface (CLI):

□ **`Protocol.LACP.config.mode = ACTIVE`**

□ **`Protocol.LACP.config.transmit_interval = FAST`**

On switch ③:

□ **`Protocol.LACP.config.system_priority = 32768`**

On switch ②:

□ **`Protocol.LACP.config.system_priority = 65535`**

□ Now plug in the second network cable between switch ③ and switch ②.

2.5 Auto Configuration via DHCP

Storing configuration script files on a TFTP server allows for a central distribution of device configurations on start-up via DHCP auto configuration.
This is carried out via DHCP options 66 and 67:

- DHCP option 66: TFTP Server IP Address
- DHCP option 67: Configuration File Path and Name

With DHCP auto configuration, it is possible to automatically roll out new configuration files on every booting MICROSENS G6 device in the corporate network.

Note:
The DHCP auto configuration only works with a TFTP server because the MICROSENS G6 switch does not send any credentials to the server.

2.5.1 General Process of DHCP Auto configuration

As shown in Figure 2, the communication between MICROSENS G6 switch, DHCP server and TFTP server works as follows:

Element	Description
1	MICROSENS G6 Switch
2	DHCP Server
3	TFTP Server

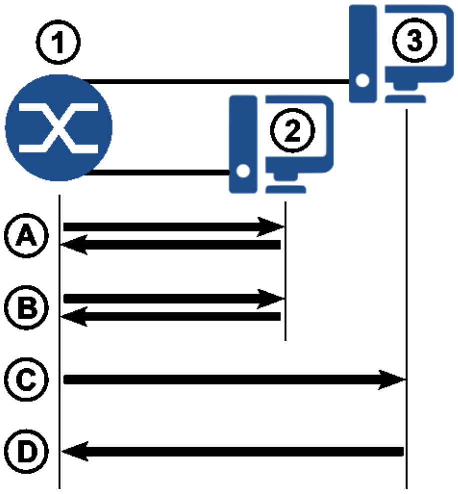


Figure 2: DHCP Auto Configuration (Simplified Drawing)

Step Ⓐ:

On start-up, switch ① does not own valid network settings like IP address or network mask yet and therefore broadcasts a “DHCP Discover” message into the network. The respective DHCP server ② answers with a “DHCP Offer” message, containing a set of necessary network settings.

Step Ⓑ:

Switch ① chooses its configuration settings and sends a “DHCP Request” to DHCP server ②. The server answers with a “DHCP Ack” message to confirm these settings.

Additionally, the DHCP server sends the IP address of TFTP server ③ (DHCP option 66) and the path and file name of the configuration file for the MICROSENS G6 switch (DHCP option 67).

Step Ⓒ:
After receiving the TFTP server's address, switch ① connects to TFTP server ③.

Step Ⓓ:
Switch ① downloads the respective configuration file and executes the containing configuration script.

2.5.2 Prerequisites

The following preparations have to be made in order to use the DHCP auto configuration feature:

- The DHCP server must be configured to use the DHCP options 66 and 67. Please refer to the respective DHCP server's user documentation.
- The configuration script has to be created and stored on the TFTP server.
- The switch has to be configured in mode "DHCP with script".

2.5.3 Pitfalls when using DHCP auto configuration

Please note the following conditions for using the DHCP auto configuration feature:

- Do not use fixed device IP addresses inside the configuration script to avoid every auto configured device getting the same IP address.
- Several switches will possibly obtain the same configuration file if you are not using MICROSENS microScript for the configuration script (see chapter "Using MICROSENS microScript for flexible DHCP auto configuration scripts" on page 73).

2.5.4 Creating the Configuration Script

Note:
Use the MICROSENS Network Management Platform (NMP) to create configuration files conveniently. Please refer to the respective section in the NMP documentation.

Note:
Do not use device-specific values inside the configuration script (e.g. device name or IP address).

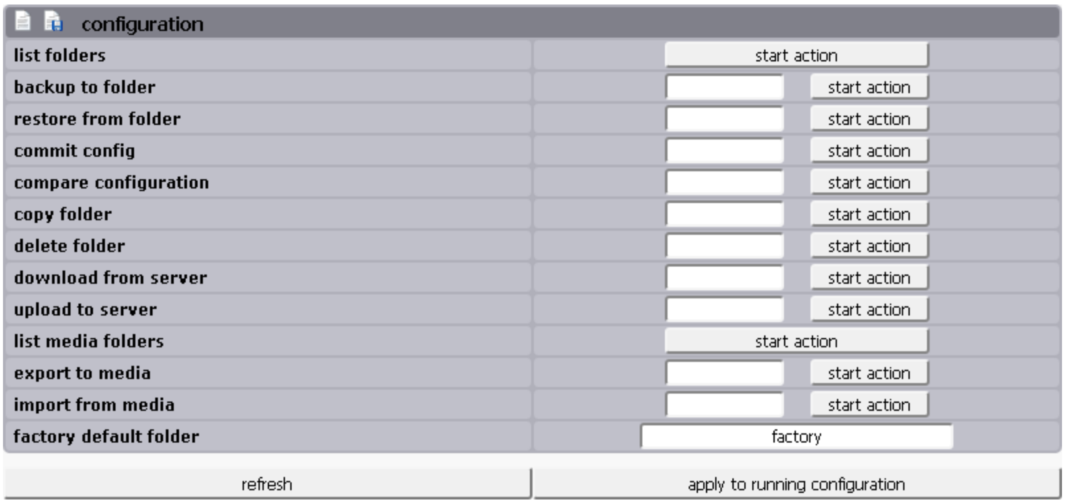
There are three different options to create a configuration script file:

- Option 1: Use the current configuration of a device.
- Option 2: The running configuration of a device must not be changed.
- Option 3: Manual changes of a device's factory configuration.

Using the Web Manager:

Option 1: Use the current configuration of a device

- Open the Web Manager on the device that should outline the master configuration.
- Configure this device completely as required.
- Select the **Files** screen, then select the tab **Configuration**.

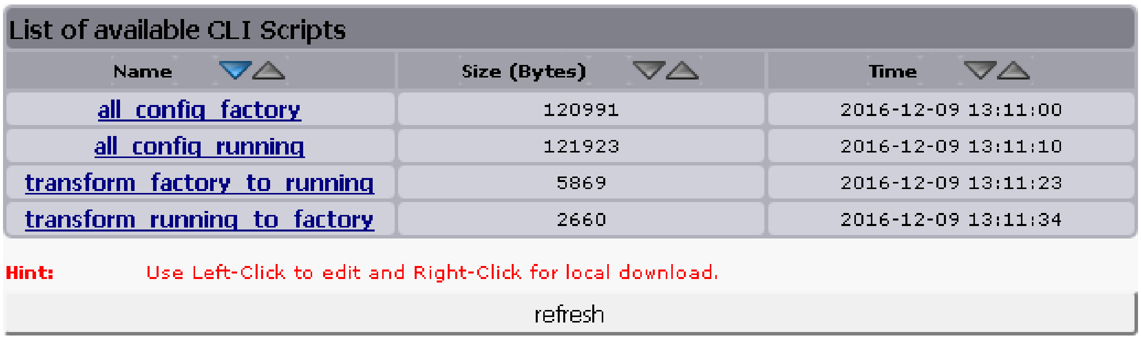


configuration

list folders		start action
backup to folder		start action
restore from folder		start action
commit config		start action
compare configuration		start action
copy folder		start action
delete folder		start action
download from server		start action
upload to server		start action
list media folders		start action
export to media		start action
import from media		start action
factory default folder	factory	

Figure 3: DHCP Auto Configuration - Compare Configuration

- Leave the parameter field of **compare configuration** empty and click on the respective button **start action**. This will create a CLI script for the running configuration.
- Select the **Scripting** screen. By default the tab **CLI Scripts** opens. In the **List of available CLI Scripts**, left-click on the entry "all config running".



List of available CLI Scripts

Name	Size (Bytes)	Time
all_config_factory	120991	2016-12-09 13:11:00
all_config_running	121923	2016-12-09 13:11:10
transform_factory_to_running	5869	2016-12-09 13:11:23
transform_running_to_factory	2660	2016-12-09 13:11:34

Hint: Use Left-Click to edit and Right-Click for local download.

Figure 4: DHCP Auto Configuration - List of available CLI Scripts

Note:
You can use the CLI script "`transform_factory_to_running`" if the DHCP auto configuration is meant to be rolled out for new devices with factory settings.

Using the Web Manager:

To upload the script file to a TFTP server, choose one of the following two options:

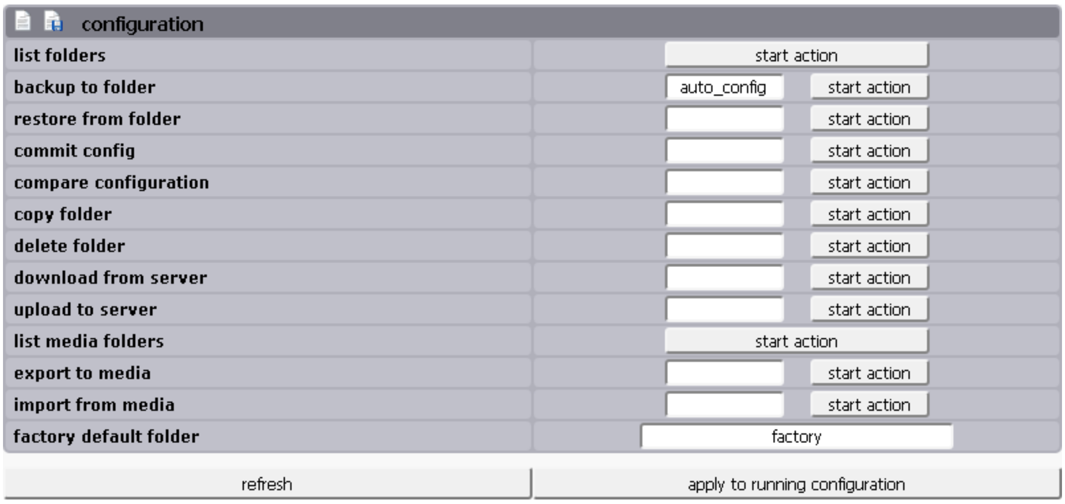
1. Download the respective file to your local drive and use an TFTP client (or any other file transfer client) to upload it to the TFTP server.
2. In the Web Manager’s section **Upload to Server / Download from Server**, enter the respective TFTP server's address, transfer protocol and login credentials. Click the button **Upload** to upload the script file to the server.

Note:
To use the upload feature within the Web Manager you have to enable the respective file transfer protocol under **System > File Transfer Configuration**.

Option 2: The running configuration of a device must not be changed

□ Open the Web Manager on the device that should outline the master configuration.

□ Select the **Files** screen, then select the tab **Configuration**.



configuration

list folders		start action
backup to folder	auto_config	start action
restore from folder		start action
commit config		start action
compare configuration		start action
copy folder		start action
delete folder		start action
download from server		start action
upload to server		start action
list media folders		start action
export to media		start action
import from media		start action
factory default folder	factory	

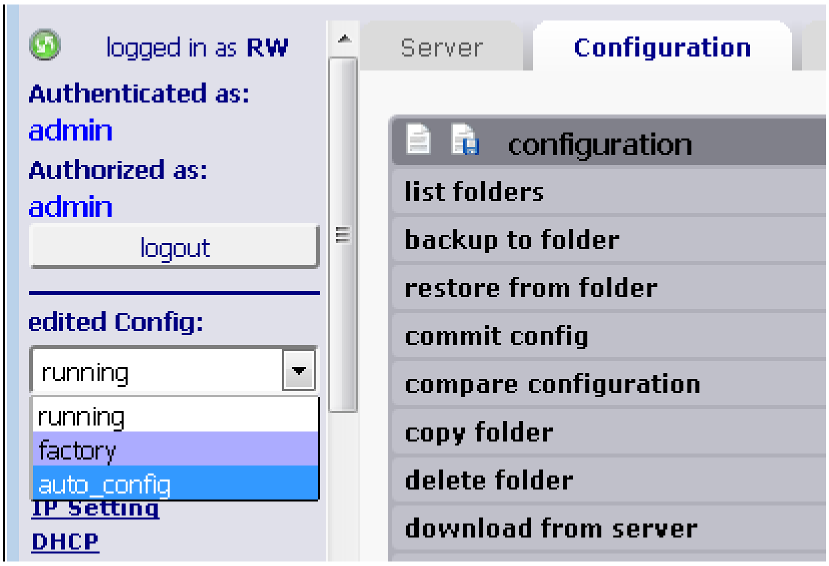
Figure 5: DHCP Auto Configuration - Backup Running Configuration

□ In the parameter field **backup to folder**, enter a new backup folder “`auto_config`” for the running configuration and click on the respective button **start action**.

Note:
If the folder name already exists, this command overwrites the previous configuration script.

□ In the row **list folders**, click the button **start action** to show a list of user folders. The new folder name appears in the list.

Using the Web Manager:



logged in as **RW**

Authenticated as:
admin

Authorized as:
admin

logout

edited Config:

running ▾

- running
- factory
- auto_config

IP Setting

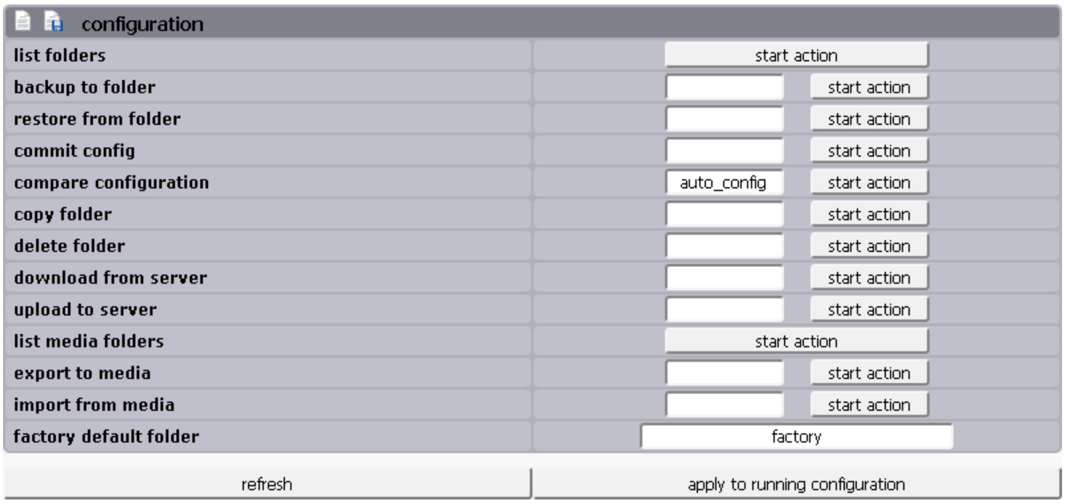
DHCP

Figure 6: DHCP Auto Configuration - Change Edited Configuration

□ In the Web Manager's main menu on the left, change the **edited Config** to "`auto_config`". Now every configuration change is saved to this backup configuration.

□ Configure the device completely as required.

□ Select the **Files** screen, then select the tab **Configuration**.



configuration		
list folders		start action
backup to folder		start action
restore from folder		start action
commit config		start action
compare configuration	auto_config	start action
copy folder		start action
delete folder		start action
download from server		start action
upload to server		start action
list media folders		start action
export to media		start action
import from media		start action
factory default folder	factory	

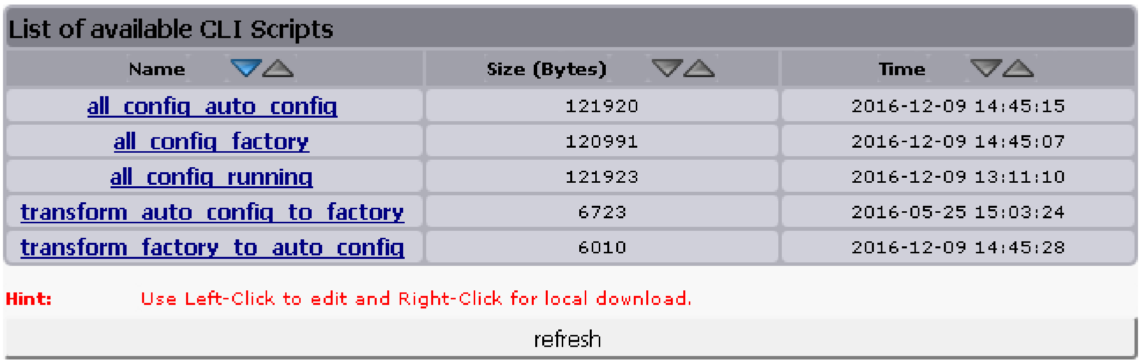
refresh | apply to running configuration

Figure 7: DHCP Auto Configuration - Compare with Running Configuration

□ In the parameter field of **compare configuration**, enter "`auto_config`" and click on the respective button **start action**. This will create a CLI script for the backup configuration.

Using the Web Manager:

□ Select the **Scripting** screen. By default the tab **CLI Scripts** opens. In the **List of available CLI Scripts**, left-click on the entry "`all_config_auto_config`".



List of available CLI Scripts

Name	Size (Bytes)	Time
all_config_auto_config	121920	2016-12-09 14:45:15
all_config_factory	120991	2016-12-09 14:45:07
all_config_running	121923	2016-12-09 13:11:10
transform_auto_config_to_factory	6723	2016-05-25 15:03:24
transform_factory_to_auto_config	6010	2016-12-09 14:45:28

Hint: Use Left-Click to edit and Right-Click for local download.

Figure 8: DHCP Auto Configuration - List of available CLI Scripts

Note:
You can use the CLI script "`transform_factory_to_auto_config`" if the DHCP auto configuration is meant to be rolled out for new devices with factory settings.

To upload the script file to a TFTP server, choose one of the following two options:

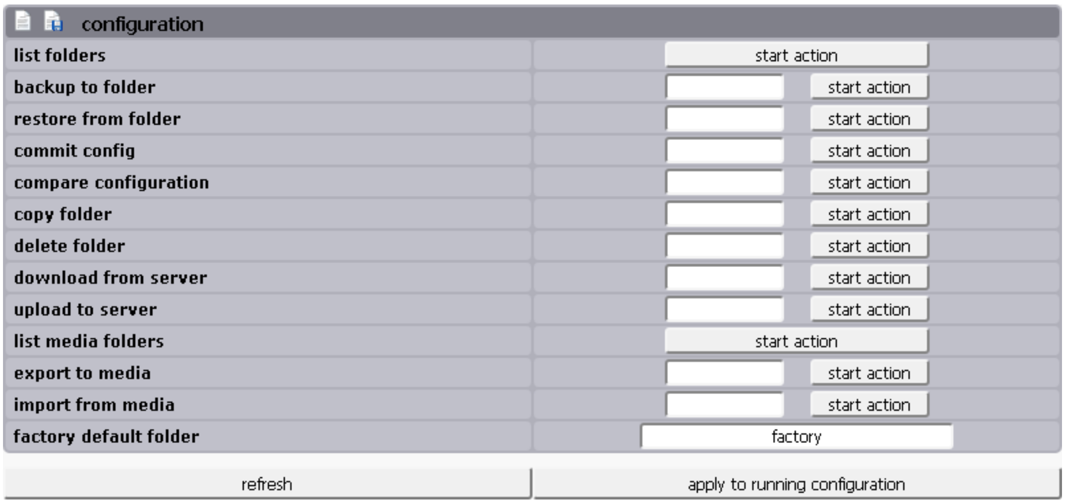
1. Download the respective file to your local drive and use an FTP client to upload it to the TFTP server.
2. In the Web Manager's section **Upload to Server / Download from Server**, enter the respective TFTP server's address, transfer protocol and login credentials. Click the button **Upload** to upload the script file to the server.

Note:
To use the upload feature within the Web Manager you have to enable the respective file transfer protocol under **Files > Server**.

Using the Web Manager:

Option 3: Manual changes of the device's factory configuration

- □ Open the Web Manager on the device that should outline the master configuration.
- □ Select the **Files** screen, then select the tab **Configuration**.

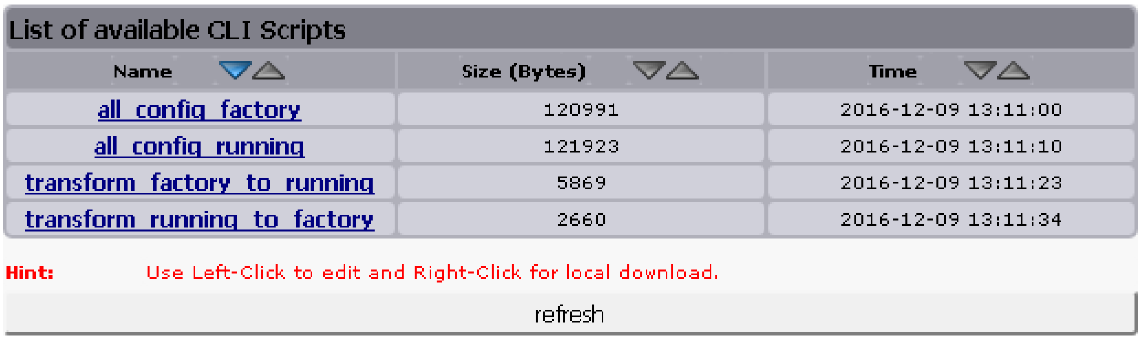


configuration

list folders		start action
backup to folder		start action
restore from folder		start action
commit config		start action
compare configuration		start action
copy folder		start action
delete folder		start action
download from server		start action
upload to server		start action
list media folders		start action
export to media		start action
import from media		start action
factory default folder	factory	

Figure 9: DHCP Auto Configuration - Generating Factory CLI Script

- □ Leave the parameter field of **compare configuration** empty and click on the respective button **start action**. This will create the CLI scripts for the running and factory configuration.
- □ Select the **Scripting** screen. By default the tab **CLI Scripts** opens. In the **List of available CLI Scripts**, left-click on the entry "`all_config_factory`".



List of available CLI Scripts

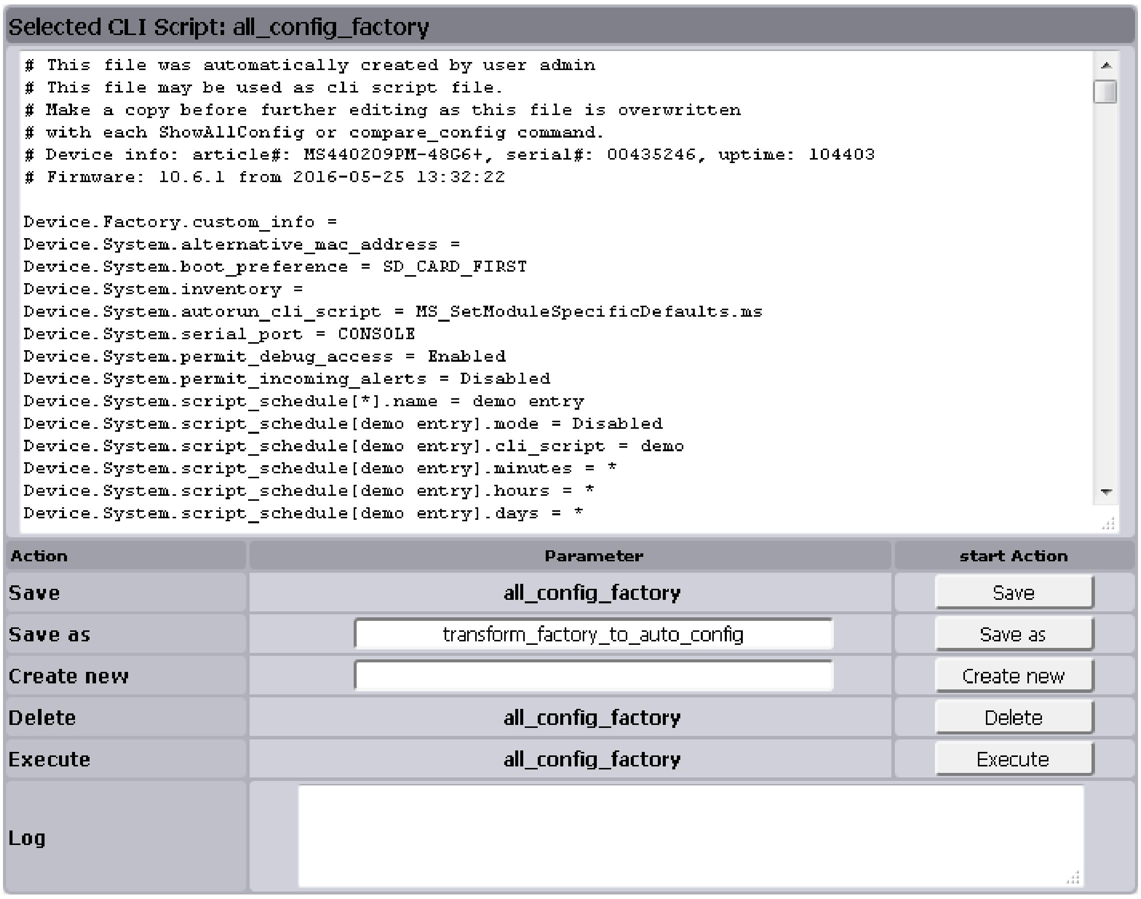
Name	Size (Bytes)	Time
all_config_factory	120991	2016-12-09 13:11:00
all_config_running	121923	2016-12-09 13:11:10
transform_factory_to_running	5869	2016-12-09 13:11:23
transform_running_to_factory	2660	2016-12-09 13:11:34

Hint: Use Left-Click to edit and Right-Click for local download.

Figure 10: DHCP Auto Configuration - List of available CLI Scripts

Using the Web Manager:

- □ The script opens in the text field of the section **Selected CLI Script: all_config_factory**.



Selected CLI Script: all_config_factory

```
# This file was automatically created by user admin
# This file may be used as cli script file.
# Make a copy before further editing as this file is overwritten
# with each ShowAllConfig or compare_config command.
# Device info: article#: MS440209PM-48G6+, serial#: 00435246, uptime: 104403
# Firmware: 10.6.1 from 2016-05-25 13:32:22

Device.Factory.custom_info =
Device.System.alternative_mac_address =
Device.System.boot_preference = SD_CARD_FIRST
Device.System.inventory =
Device.System.autorun_cli_script = MS_SetModuleSpecificDefaults.ms
Device.System.serial_port = CONSOLE
Device.System.permit_debug_access = Enabled
Device.System.permit_incoming_alerts = Disabled
Device.System.script_schedule[*].name = demo entry
Device.System.script_schedule[demo entry].mode = Disabled
Device.System.script_schedule[demo entry].cli_script = demo
Device.System.script_schedule[demo entry].minutes = *
Device.System.script_schedule[demo entry].hours = *
Device.System.script_schedule[demo entry].days = *
```

Action	Parameter	start Action
Save	all_config_factory	Save
Save as	transform_factory_to_auto_config	Save as
Create new		Create new
Delete	all_config_factory	Delete
Execute	all_config_factory	Execute
Log		

Figure 11: DHCP Auto Configuration - Selected CLI Script

- □ Manually change the options and parameters of the script.
- □ Enter the script name "`transform_factory_to_auto_config`" in the field **Save as** and click on the button **Save as.** The new script appears in the **List of available CLI Scripts**.

To upload the script file to a TFTP server, choose one of the following two options:

1. Download the respective file to your local drive and use an FTP client to upload it to the TFTP server.
2. In the Web Manager's section **Upload to Server / Download from Server**, enter the respective TFTP server's address, transfer protocol and login credentials. Click the button **Upload** to upload the script file to the server.

Note:
To use the upload feature within the Web Manager you have to enable the respective file transfer protocol under **Files > Server**.

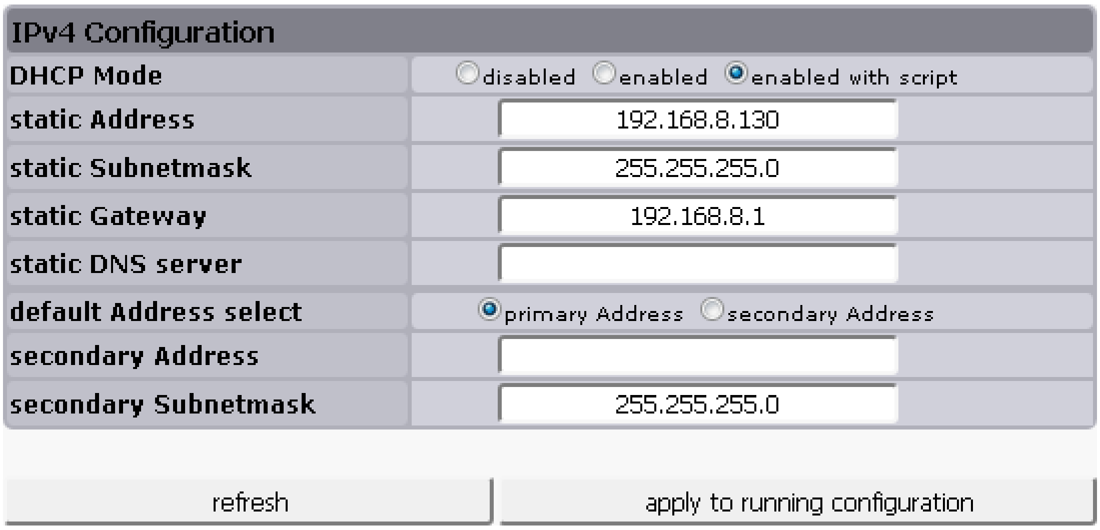
Using the Web Manager:

Note:
If you do not want to use the minimalistic Web Manager's text editor, you can use the text editor of your operating system. Just copy and paste the configuration into a new text file, make the respective changes with the stand-alone text editor and upload the text file to the TFTP server with an FTP client.

Note:
Please note that the path and directory of the uploaded file have to match the DHCP option 67 determined in the DHCP server settings.

□ On all devices that should obtain their auto configuration by DHCP option 66 and 67, select the **IP Setting** screen, then select the tab **IPv4 Configuration**.

□ Change the **DHCP Mode** to "**enabled with script**".



IPv4 Configuration

DHCP Mode	○ disabled ○ enabled ● enabled with script
static Address	192.168.8.130
static Subnetmask	255.255.255.0
static Gateway	192.168.8.1
static DNS server	
default Address select	● primary Address ○ secondary Address
secondary Address	
secondary Subnetmask	255.255.255.0

Figure 12: DHCP Auto Configuration - Enable DHCP with Script

□ Next time the respective device logs into the network, it will obtain the configuration file from the TFTP server in the network and will execute it.

Using the Command Line Interface (CLI):

Option 1: Use the current configuration of a device

□ Open the CLI on the device that should outline the master configuration.

□ □ Configure this device completely as required.

□ **`Management.Files.configuration.compare_configuration =`**

```
» NOTE: This will execute an action command with the following
  function:
  […]

  Comparing running configuration against factory configuration.
  Comparing running with factory
  -> comparing /running with /factory

  Create parameter list of factory ...
  Create parameter list of running ...

  Creating transformation script file:
  transform_factory_to_running
  69 values are different.
  1 dynamic table entries to delete.

  Creating transformation script file:
  transform_running_to_factory
  56 values are different.
  3 dynamic table entries to delete.

  Hit q to quit or any other key to continue..
  Use Management.Files.Scripts.show_file to view the
  transformation files.

  -- END OF ACTION RESPONSE –
»
```

Using the Command Line Interface (CLI):

□ **`Management.Files.Scripts.list_file`**

```
» NOTE: This will execute an action command with the following
  function:
  Displays a list of all available script files, their size and
  date of last change.
  Type y to continue, else to quit:
  Listing available script files
      120992 Dec 14 12:24 all_config_factory
      121924 Dec 14 12:24 all_config_running
        5870 Dec 14 12:24 transform_factory_to_running
        5043 Dec 14 12:25 transform_running_to_factory

  -- END OF ACTION RESPONSE -
»
```

Note:
You can use the CLI script "`transform_factory_to_running`" if the DHCP auto configuration is meant to be rolled out for new devices with factory settings.

□ **`Management.Files.server.enable_tftp = Enabled`**

```
» enable_tftp: Enabled
```

□ **`Management.Files.configuration.upload_to_server = <all_config_running|transform_factory_to_running> tftp://<user:password>@<server_address>/<path>/`**

Option 2: The running configuration must not be changed

□ **`Management.Files.configuration.backup_to_folder = auto_config`**

□ **`OfflineConfiguration = auto_config`**

```
» You are now working on folder: auto_config
» Folder: auto_config»
```

Configure this device completely as required. Every configuration change is made in the folder "auto_config". After the configuration is finished, switch back to the normal live mode of operation:

□ **`Folder: auto_config>>OnlineConfiguration.`**

```
» You are now working on the live configuration again
»
```

Using the Command Line Interface (CLI):

□ **Management.Files.configuration.compare_configuration = factory auto_config**

```
» NOTE: This will execute an action command with the following
  function:
  […]
  Type y to continue, else to quit:
  Comparing factory with auto_config
  -> comparing /factory with /custom/auto_config

  Create parameter list of auto_config ...
  Create parameter list of factory ...

  Creating transformation script file:
  transform_auto_config_to_factory
  57 values are different.
  3 dynamic table entries to delete.

  Creating transformation script file:
  transform_factory_to_auto_config
  70 values are different.
  1 dynamic table entries to delete.

  Use Management.Files.Scripts.show_file to view the
  transformation files.

  -- END OF ACTION RESPONSE --
»
```

□ □ **Management.Files.Scripts.list_file**

```
» NOTE: This will execute an action command with the following
  function:
  Displays a list of all available script files, their size and
  date of last change.
  Type y to continue, else to quit:
  Listing available script files
      121923 Dec 14 13:24 all_config_auto_config
      120992 Dec 14 13:24 all_config_factory
      121924 Dec 14 12:24 all_config_running
        5094 Dec 14 13:24 transform_auto_config_to_factory
        5920 Dec 14 13:24 transform_factory_to_auto_config
        5870 Dec 14 12:24 transform_factory_to_running
        5043 Dec 14 12:25 transform_running_to_factory

  -- END OF ACTION RESPONSE --
»
```

Using the Command Line Interface (CLI):

Note:
You can use the CLI script "`transform_factory_to_auto_config`" if the DHCP auto configuration is meant to be rolled out for new devices with factory settings.

□ **`Management.Files.server.enable_tftp = Enabled`**

```
» enable_tftp: Enabled
```

□ **`Management.Files.configuration.upload_to_server = <all_config_running|transform_factory_to_running> tftp://<user:password>@<server_address>/<path>/`**

Option 3: Manual changes of the device's factory configuration

□ **`Management.Files.configuration.compare_configuration =`**

```
» NOTE: This will execute an action command with the following
  function:
  […]

  Comparing running configuration against factory configuration.
  Comparing running with factory
  -> comparing /running with /factory

  Create parameter list of factory ...
  Create parameter list of running ...

  Creating transformation script file:
  transform_factory_to_running
  69 values are different.
  1 dynamic table entries to delete.

  Creating transformation script file:
  transform_running_to_factory
  56 values are different.
  3 dynamic table entries to delete.

  Hit q to quit or any other key to continue..
  Use Management.Files.Scripts.show_file to view the
  transformation files.

  -- END OF ACTION RESPONSE –
»
```

Using the Command Line Interface (CLI):

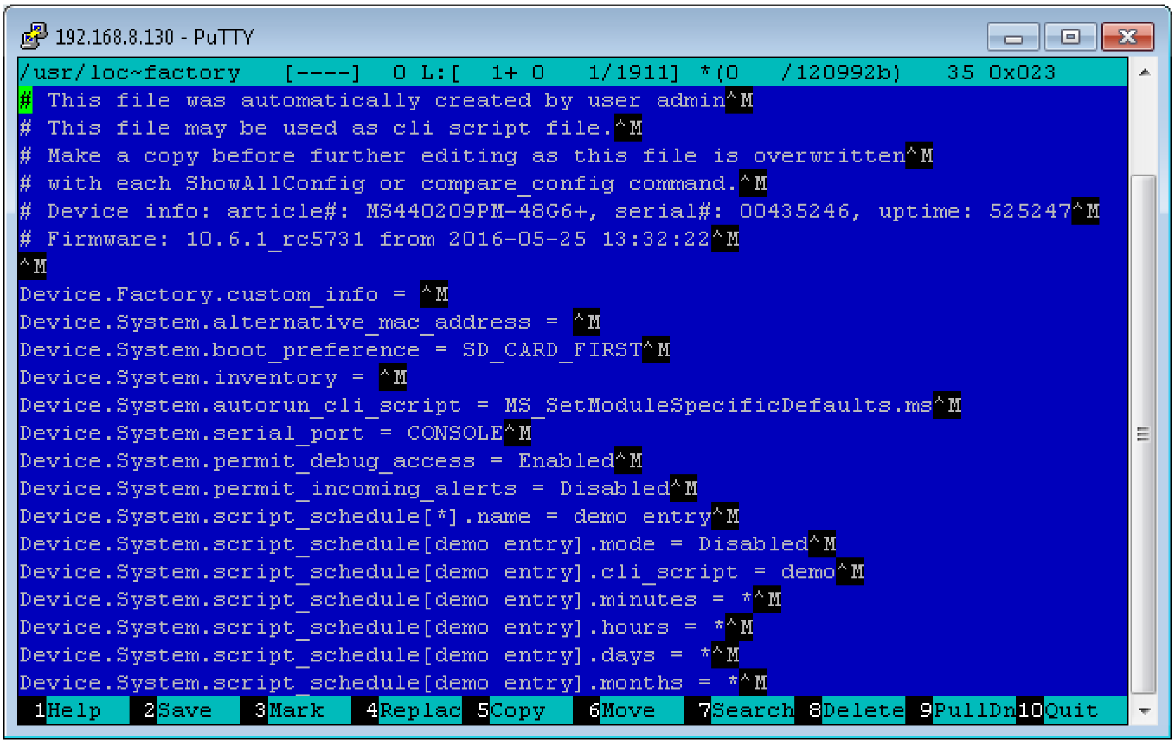
□ **`Management.Files.Scripts.list_file`**

```
» NOTE: This will execute an action command with the following
  function:
  Displays a list of all available script files, their size and
  date of last change.
  Type y to continue, else to quit:
  Listing available script files
      120992 Dec 14 12:24 all_config_factory
      121924 Dec 14 12:24 all_config_running
        5870 Dec 14 12:24 transform_factory_to_running
        5043 Dec 14 12:25 transform_running_to_factory

  -- END OF ACTION RESPONSE –
»
```

□ **`EditScriptFile all_config_factory`**

□ The built-in script editor opens with the folder content of "`all_config_factory`".



```
/usr/loc~factory   [----]  0 L:[  1+ 0   1/1911] *(0   /120992b)   35 0x023
# This file was automatically created by user admin^M
# This file may be used as cli script file.^M
# Make a copy before further editing as this file is overwritten^M
# with each ShowAllConfig or compare_config command.^M
# Device info: article#: MS440209PM-48G6+, serial#: 00435246, uptime: 525247^M
# Firmware: 10.6.1_rc5731 from 2016-05-25 13:32:22^M
^M
Device.Factory.custom_info = ^M
Device.System.alternative_mac_address = ^M
Device.System.boot_preference = SD_CARD_FIRST^M
Device.System.inventory = ^M
Device.System.autorun_cli_script = MS_SetModuleSpecificDefaults.ms^M
Device.System.serial_port = CONSOLE^M
Device.System.permit_debug_access = Enabled^M
Device.System.permit_incoming_alerts = Disabled^M
Device.System.script_schedule[*].name = demo entry^M
Device.System.script_schedule[demo entry].mode = Disabled^M
Device.System.script_schedule[demo entry].cli_script = demo^M
Device.System.script_schedule[demo entry].minutes = *^M
Device.System.script_schedule[demo entry].hours = *^M
Device.System.script_schedule[demo entry].days = *^M
Device.System.script_schedule[demo entry].months = *^M
 1Help   2Save   3Mark   4Replac 5Copy   6Move   7Search 8Delete 9PullDn10Quit
```

Figure 13: DHCP Auto Configuration - CLI - Built-in Script Editor

Hitting function key 'F2' saves all changes to the configuration file.

Hitting function key 'F10' closes the editor and returns to normal CLI mode.

Note:
MICROSENS microScript accepts both UNIX and Microsoft Windows ® style line termination (i.e. for Microsoft Windows ® the "**^M**" chars in Figure 13).

Using the Command Line Interface (CLI):

□ Manually change the options and parameters of the script. Hit function key ‘F2’ to save the changes to the configuration script file.

□ □ **`Management.Files.server.enable_tftp = Enabled`**

```
» enable_tftp: Enabled
```

□ **`Management.Files.configuration.upload_to_server = all_config_factory tftp://<user:password>@<server_address>/<path>/`**

2.5.5 Using MICROSENS microScript for flexible DHCP auto configuration scripts

The script language MICROSENS microScript enables the user to expand the switch functionality according to their demands without changing the system's firmware.

Basically, a simple script can store a value for every parameter of the switch directly. Thus it is possible to configure several identical switches with the same parameter settings easily.

Some parameters of the configuration are device specific (e.g. IP address or login credentials). It would be disastrous for the corporate network if e.g. all devices obtained the same IP address on roll-out. Therefore it is possible to use MICROSENS microScript with variables and conditional expressions to customise the configuration.

Note:
MICROSENS microScript accepts both UNIX and Microsoft Windows ® style line termination (LF).

Save these script files locally either as a microScript file with the extension `.ms` or as a simple text file with the extension `.txt`. MICROSENS switches are able to work with both file types.

The following script snippet shows how to set the device's name based on its MAC address:

```
1    Device.IP.v4_config.dhcp_mode = DHCP_WITH_SCRIPT
2    :var $name = " "
3    Device.System.used_mac_address %
4    :if V0 == "00:60:A7:04:E2:17"
5    :   set $name = "Device 101"
6    :elseif V0 == "00:60:A7:04:E2:16"
7    :   set $name = "Device 102"
8    :elseif V0 == "00:60:A7:04:E1:EC"
9    :   set $name = "Device 103"
10   :endif
11   Management.SNMP.device_info.sys_name = {$name}
```

-
  ```
  1   Device.IP.v4_config.dhcp_mode = DHCP_WITH_SCRIPT
  ```
  The script sets the device's DHCP mode to "DHCP auto config".

-
  ```
  2   :var $name = " "
  ```
  It defines the variable $name and empties it by default.

-
  ```
  3   Device.System.used_mac_address %
  ```
  The script reads the MAC address of the device.

-
  ```
  4   :if V0 == "00:60:A7:04:E2:17"
  5   :   set $name = "Device 101"
  6   :elseif V0 == "00:60:A7:04:E2:16"
  7   :   set $name = "Device 102"
  8   :elseif V0 == "00:60:A7:04:E1:EC "
  9   :   set $name = "Device 103"
  10  :endif
  ```
  Due to the device's MAC address the script assigns the variable $name with the respective value.

-
  ```
  11  Management.SNMP.device_info.sys_name = {$name}
  ```
  The script sets the device name to the value of the variable $name.

Disclaimer

All information in this document is provided ‘as is’ and subject to change without notice.
MICROSENS GmbH & Co. KG disclaims any liability for the correctness, completeness or quality of the information provided, fitness for a particular purpose or consecutive damage.
Any product names mentioned herein may be trademarks and/or registered trademarks of their respective companies.

Document ID: AN-16010_2017-12-15