NTS Networker
User Documentation

12.11.2014

NTS Netzwerk Telekom Service AG

Parkring 4, 8074 Grambach

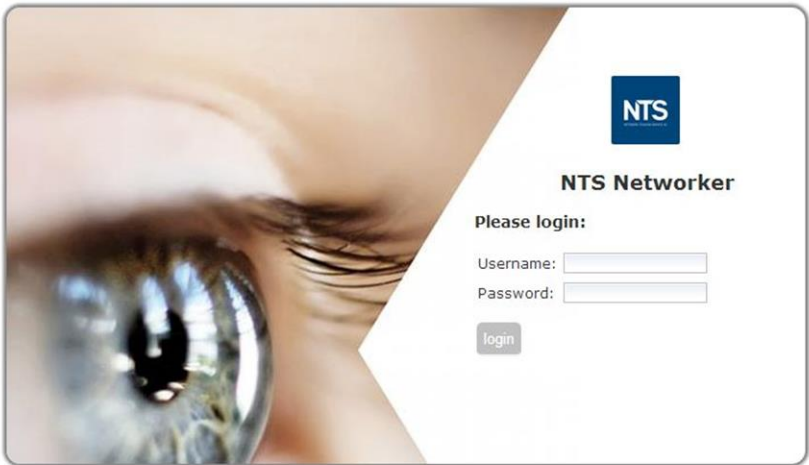office-graz@nts.eu www.nts.eu

Inhaltsverzeichnis

1   Overview

NTS Networker enables IT-Helpdesk personnel to configure network components (switches) in realtime on a device group or device level. It also enables configuration and maintenance of network interfaces or ports through a web interface. All events are logged automatically and the logs can be displayed and filtered within the same tool. Furthermore, it is possible to view a graphical network topology around a freely selectable network device with configurable granularity (network hop-depth)

1.1   Login

To log in use the Active Directory user account that has been assigned to you by the Networker adminstrator.
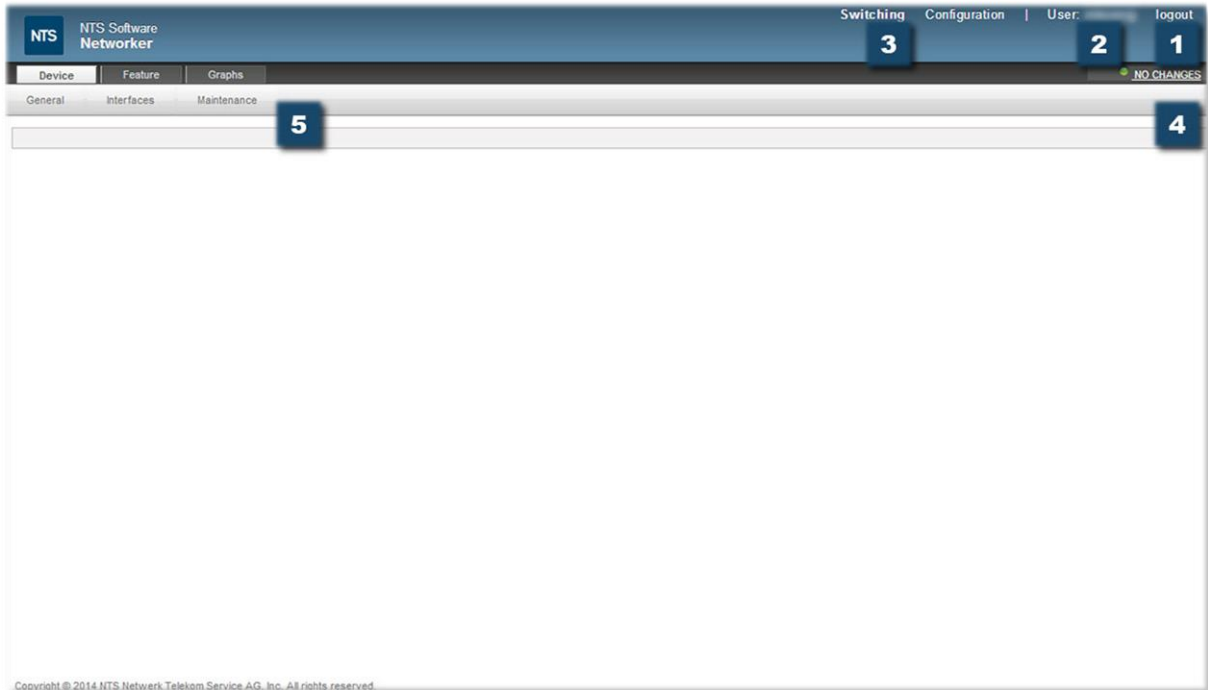
1.2   Start

Login with your Active Directory user and password.

2   UI Overview

Edit Button

1: **Logout** Button

2: displays currently logged in **User**. A mouse-over displays the assigned role(s)

3: Switch between the **Switching (user)** and **Configuration (admin)** interface mode (only available, if you have an admin role assigned to your user account).

4: Display of pending changes. A click on this field opens the „Write Memory"-interface where the changes can be finally deployed on all affected devices (see chapter 3.1.4).

5: Four main tabs (functionality depends on the selected interface mode [Switching or Configuration])
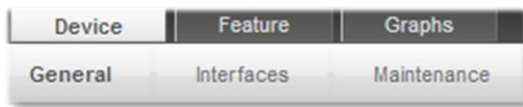
RELAX,
WE CARE

3   Switching

The switching mode divides the interface into three tabs Device, Feature, and Graphs.These tabs offer a further (second) level of navigation, displayed right below the tabs:
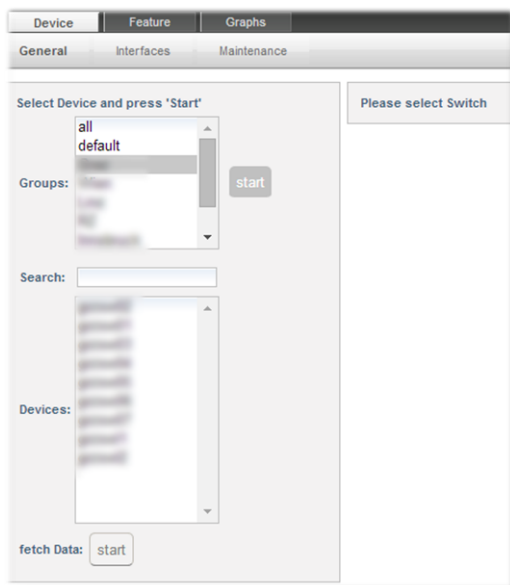
3.1   Device

The first tab "Device" is split into three subgroups General, Interfaces, and Maintainance. In this section, you can make changes on single ports and devices.

3.1.1   General

In the "General"-section you find an overview of all devices of a group or all single devices.

There you can fetch live data to display different kinds of information on the devices.

Press the start button next to the selection boxes to gather data, either for whole groups or for single devices.

This generates a table that displays (depending on your selection) all relevant data for every device of a group (or the single device), namely, Name, sysname, IP Adresse, Uptime, sysLocation, Model, SW Version, Feature, and Serial Number.

3.1.2   Interfaces

In the Interfaces sub-section, you can configure devices at port level. Again, select the corresponding group (1) and the device you wish to configure (2). Click on start (3) to gather and display the current port data. You may search (RegEx) or sort the columns ifDescr and ifAlias (4).

A click on the edit button (right most column) (5) opens the interface configuration dialogue.

Again, you find three subsections in this window.

3.1.3   Edit Interface – General

In the "General" part, you see the currently deployed port configuration. In addition, you can set an interface alias name. Use the other tabs VLAN and Port Security to configure the corresponding properties.

3.1.3.1   Edit Interface – VLAN

This section enables VLAN configuration of ports. Here, you can assign a VLAN and a Voice VLAN (if applicable) to the selected port.

Press the commit button to apply the changes. Apparently, close exits the window without saving the changes.

Attention: The changes will be rolled out and be active at once. Nonetheless, in case of a switch reboot, they will be deleted. To save changes permanently, they must be written to the memory (see chapter 3.1.4 Maintainance).

3.1.3.2   Edit Interface – Port Security

The tab Port Security offers configuration of security options. As soon as port security is activated, connection attempts that are lacking 802.1x authentication are rejected.

Use the option „Sticky" to bind client MAC addresses to the port instead of 802.1x authentification. This means, that only a predefined number of clients will be allowed to connect to the selected port. Each unique connection will be stored as valid MAC address, until the maximum count is reached. Set this number with the „max secure adresses" field. Any other MAC address will not get a connection on this port.

In addition, if the MAC adress changes, the client would no longer be able to connect to this port. In this case, you can clear all "sticky" MAC addresses with the "clear" button. This means, all stored MAC addresses are deleted and the process starts again.

Click commit to apply your changes. Close closes the window.

Attention: The changes will be rolled out and be active at once. Nonetheless, in case of a switch reboot, they will be deleted. To save changes permanently, they must be written to the memory (see chapter 3.1.4 Maintainance).

3.1.4 Maintainance

If the port configuration was changed (see chapter 3.1.2 Interfaces or chapter 3.2 Feature (user privileges only), it is necessary to store the information permanently on the switch to keep the changes after a reboot. This can be done in the Maintainance section.
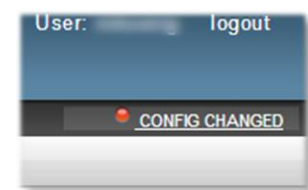
If there are any unwritten (i.e. not permanently stored) configuration changes, the change state display says "CONFIG CHANGED". When hovering the mouse over this UI part, all devices that have pending changes and are ready for permanent deployment are listed in a popup.
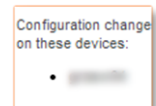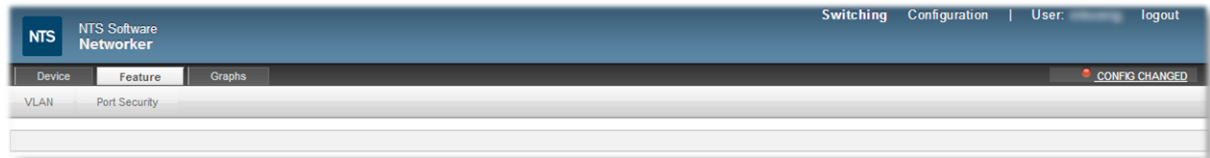

A click on „CONFIG CHANGED" or on the "Maintainance" sub-tab within the "Device" tab opens the maintainance interface:
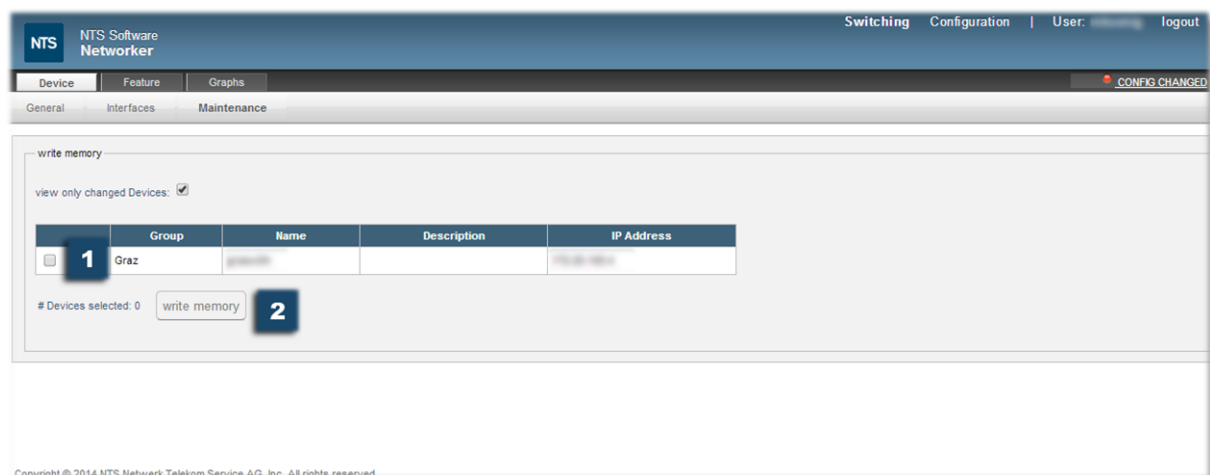
In the first column (1) you can select the devices. When you press the "write memory" button (2), the changes are permanently written to the memory of the selected devices.
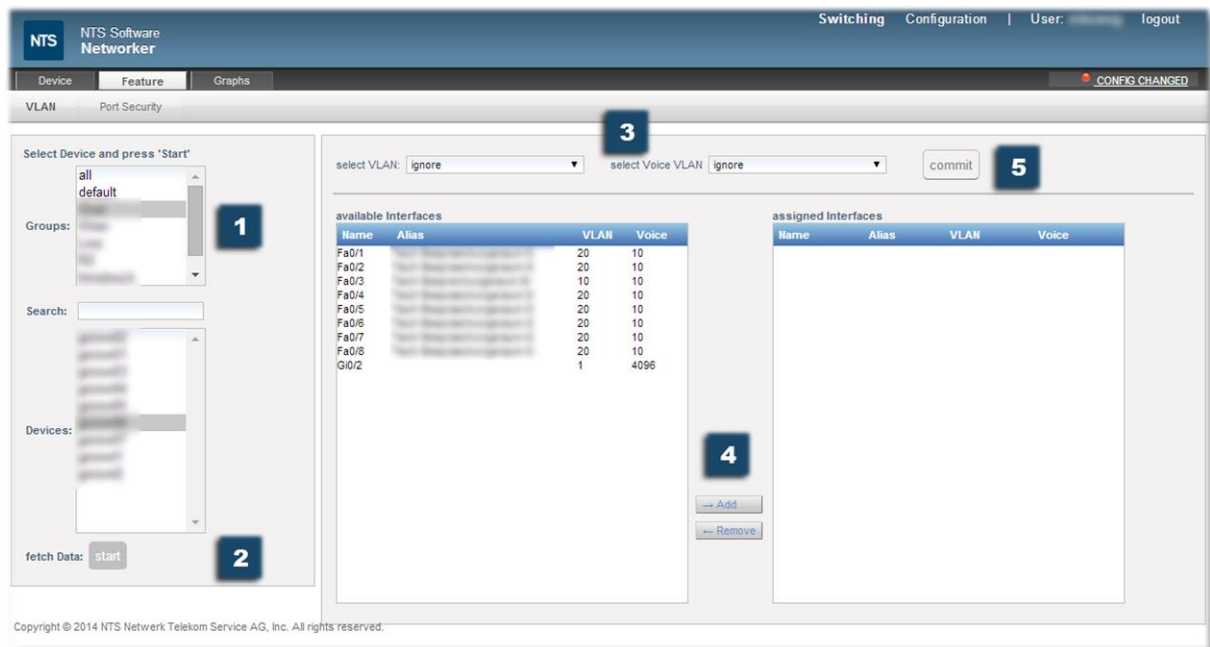
3.2 Feature (user privileges only)

The Feature section contains the interfaces for mass or bulk changes. It is divided into the subsections VLAN and Port Security.

3.2.1 VLAN Assignment

Use this interface to bulk-assign VLANs to many interfaces in one operation.

First, choose the group and the device you wish to configure (1). Please note that a multiselection is not possible. Click on fetch data: start (2) to load and display the port configuration of the selected device on the main area.

You can select the VLANs you wish to assign to the ports via the corresponding drop-down fields (3). "Ignore" means that this category will not be changed.

Then you can select the interfaces in the left selection box („available Interfaces") (multi selection is possible using Ctrl/Cmd). Use the „→Add" button (4) to add the interfaces to the right box ("assigned interfaces"). Alternatively, you can undo a selection and delete interfaces from the assigned interfaces box using the „←Remove" button. Click on „commit" (5) to apply all changes.

Attention: The changes will be rolled out and be active at once. Nonetheless, in case of a switch reboot, they will be deleted. To save changes permanently, they must be written to the memory (see chapter 3.1.4 Maintainance).

3.2.2   Port Security

Use this interface to bulk-configure Port Security features.

First, choose the group and the device you wish to configure (1). Click on fetch data: start (2) to load and display the port configuration of the selected device on the main area as a table (3). This table can be sorted by its colums. Alternatively it is search- and filterable via the input fields.

This section enables you to make the same changes as in the Device section (3.1.3.2 Edit Interface – Port Security). However, it enables you to deploy changes bulk-wise for all interfaces on one device. Like in the single configuration dialogue, you can activate port security or sticky mode and you are able to define the maximum MAC addresses number or reset all stored addresses.

Click the commit button (4) to apply all changes.

Attention: The changes will be rolled out and be active at once. Nonetheless, in case of a switch reboot, they will be deleted. To save changes permanently, they must be written to the memory (see chapter 3.1.4 Maintainance).

4   Graph

Click CDP Neighbor to open the network topology generator. There you can create a network topology starting from a certain device. The topology will be generated from the selected start device and display all neighbors through a predefined depth.

4.1   CDP Neighbor

4.1.1   Choose starting point

Again, select group ⑴ and your device to start ⑵. You can choose, if you want to see phone endpoints or disable them to unclutter your topology. It is possible to include or exclude some system names via RegEx.

Set the „discover Depth" ⑶ to define the granularity of the topology (i.e. how many hops over devices should be made). Click on fetch Data: start ⑷ to generate the network graphic. Please note that it may take some time to generate the network graphic, especially depending on the discover depth or the size of your network. The information is collected live and in real time.
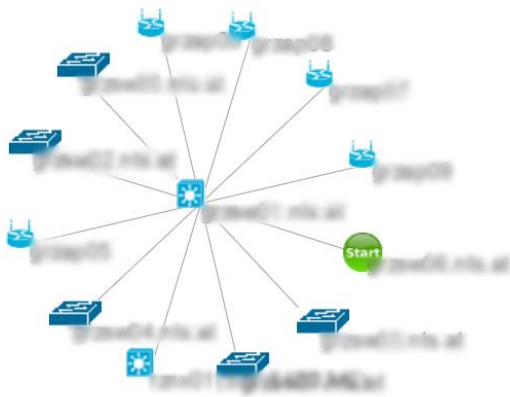
4.1.2 Graphical topology

You may zoom in or out of the view using you mouse scroll-wheel. The canvas can be moved freely to navigate around the network graphic.