LANCOM Systems

macmon nac smartly simple

MACMON NAC WHITE PAPER

LANCOM Switches

Table of Contents

Version: 1.2_en

macmon and LANCOM

Through close cooperation, the manufacturers macmon secure GmbH (macmon, network access control) and LANCOM (switches and access points) have adapted and verified their products to ensure compatibility. This cooperation and, above all, the high level of direct contact ensure that the products will continue to be compatible in the future. Direct communication also provides quick solutions in the event of unexpected incidents. In the following document, the tested functionalities are presented and described in more detail.

Network Devices with the Same Range of Functionalities

Components specified by LANCOM with the same range of functions (based on interaction with macmon):

LANCOM GS-2310P+, LANCOM GS-2326, LANCOM GS-2326P+, LANCOM GS-2328, LANCOM GS-2328P, LANCOM GS-2328F, LANCOM GS-2352P, LANCOM GS-2352

Tested Functions

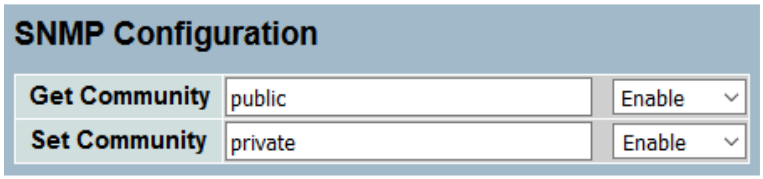
Reading the MAC addresses:	✓
Reading the MAC addresses including MAC address VLANs:	✓
Reading the VLANs on the interfaces:	✓
Configuring the VLANs on the interfaces:	✓
Reading interfaces:	✓
Reading interface statuses:	✓
Disabling/enabling interfaces:	✓
Reading 802.1X statuses:	✓
Configuring 802.1X statuses:	✓
Reading LLDPs:	✓
Reading CDPs:	
Bypassing MAC addresses with VLAN:	
Bypassing MAC addresses without VLAN:	✓
802.1X with VLAN for one device on one port:	session-based / port-based
802.1X with VLAN for multiple devices on one port:	
802.1X without VLAN for multiple devices on one port:	✓
Change of authorization:	

SNMP

The following settings are required to manage the LANCOM devices with macmon based on SNMP.

Creating the Read and Write Community for SNMPv1/2c

LANCOM Switch GUI → System → SNMP → Configuration



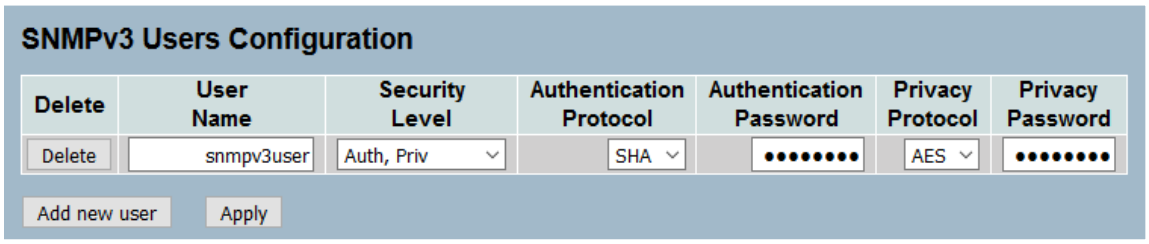
Creating Read and Write Authorization for SNMPv3 (Recommended)

The following steps must be carried out in this order:

SNMPv3 User

LANCOM Switch GUI → System → SNMP → User

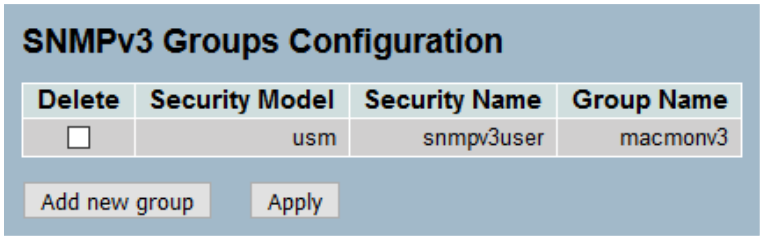
This menu item defines the SNMPv3 user and the encryption parameters of the SNMP communication between the switch and macmon. This data is required for the creation of the SNMPv3 credentials in macmon.



SNMPv3 Group

LANCOM Switch GUI → System → SNMP → Groups

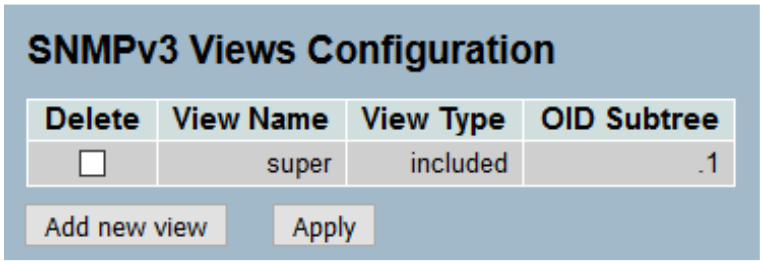
An SNMPv3 group is created. The SNMPv3 user is assigned to the group.



SNMPv3 View

LANCOM Switch GUI → System → SNMP → Views

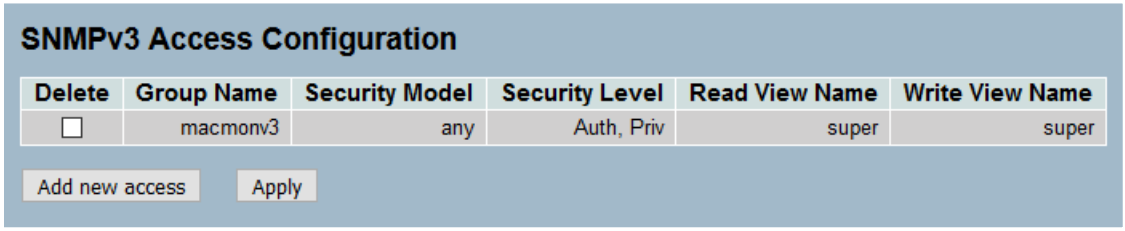
When creating an SNMPv3 view, the MIB area is defined, from which reading or writing using the SNMP is permitted. By entering ".1", all OIDs below this level can be accessed.



SNMPv3 Access

LANCOM Switch GUI → System → SNMP → Access

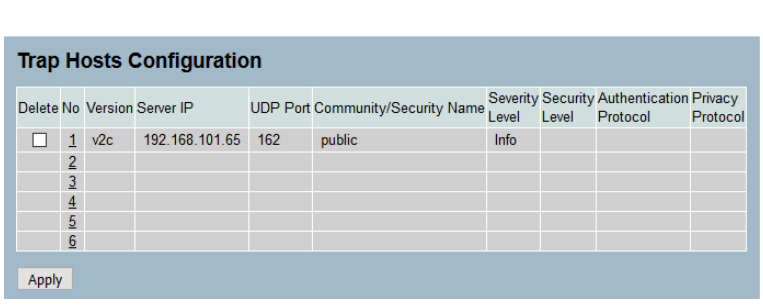
In the menu item **Access**, the SNMPv3 group is connected to the SNMPv3 view. The members of this group receive specific SNMP read and write authorization.



Sending Traps

LANCOM Switch GUI → System → SNMP → Traps

If necessary, the trap sending of link-up or link-down traps can be configured for macmon. The receipt of the corresponding traps in macmon is independent of the scan interval. This will reduce macmon response times, e.g. when disabling the interface or configuring the VLAN on the switch port.



Neighborhood Detection

LANCOM Switch GUI → System → Configuration → LLDP → LLDP Configuration

The LANCOM switches support neighborhood detection via LLDP. To ensure that the LLDP data can be read out correctly by macmon via SNMP, these parameters must be configured for the individual ports.

			Optional TLVs				
Port	Mode	CDP aware	Port Descr	Sys Name	Sys Descr	Sys Capa	Mgmt Addr
*	<>	☐	☐	☐	☐	☐	☐
1	Enabled	☐	☑	☑	☑	☑	☑

VLAN Management

Two tables are available on the LANCOM switches for tagged or untagged port VLAN assignment.

The VLAN Membership Table

LANCOM Switch GUI → System → Configuration → VLAN → VLAN Membership

The general VLAN membership of ports is defined in this table. If the port VLAN membership for certain ports is only defined in the VLAN membership table, this means that these ports have a "tagged" membership in this VLAN.

VLAN Membership Configuration

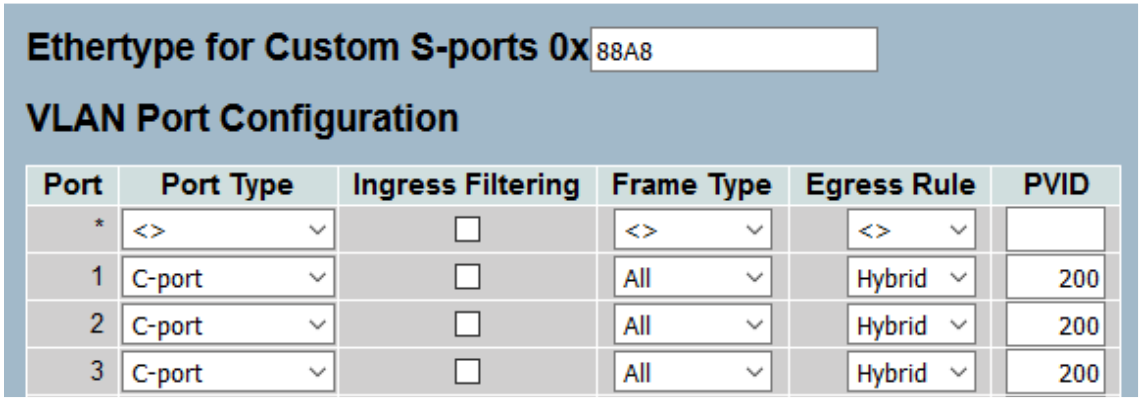
Start from VLAN 1 with 60 entries per page.

Delete	VLAN ID	VLAN Name	1	2	3	4	5	6	7	8	9	10	11	12	13
☐	1	default	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
☐	110	voice	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
☐	200	clients	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
☐	103	guest	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

The VLAN Port Configuration Table

LANCOM Switch GUI → System → Configuration → VLAN → Ports

The PVID (Port VLAN ID) is defined in this table. If the port VLAN membership for certain ports is defined in the membership table and in the VLAN port configuration table (by the PVID), the relevant ports have an “untagged” VLAN membership.



When configuring VLANs, macmon only deals with untagged VLANs. The old port VLAN membership in the membership table and in the VLAN port configuration table is removed and replaced by a new combination in both tables. An example is shown in the figure:

VLAN membership table: Port 1 = VLAN 200
VLAN port configuration table: Port 1 = PVID 200
Untagged Access VLAN: 200

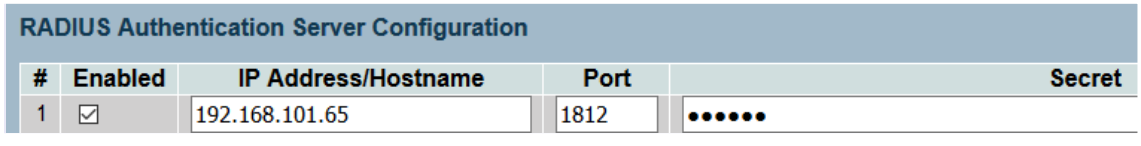
802.1X/RADIUS

The following settings are required to use the LANCOM devices with macmon via 802.1X:

Configuration of the RADIUS Server

LANCOM Switch GUI → System → Security → AAA → Configuration

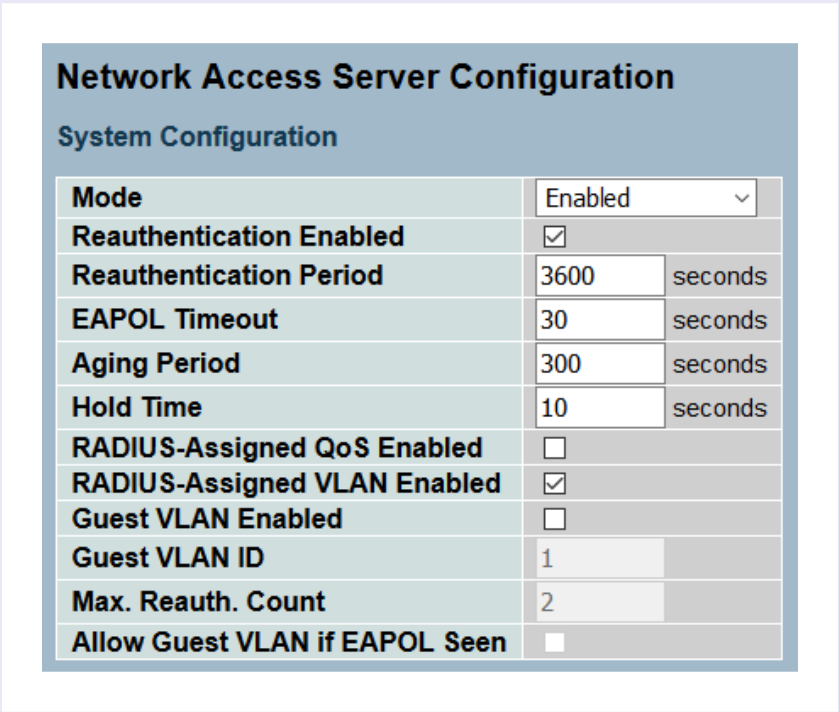
In this menu, macmon is defined as a RADIUS server and a secret is stored. In macmon, this configuration is linked to the LANCOM network device as RADIUS credentials.



Network Access Server Configuration

LANCOM Switch GUI → System → Security → NAS → Configuration

This configuration sets the global parameters for RADIUS communication between the switch, macmon and the supplicant (endpoint).



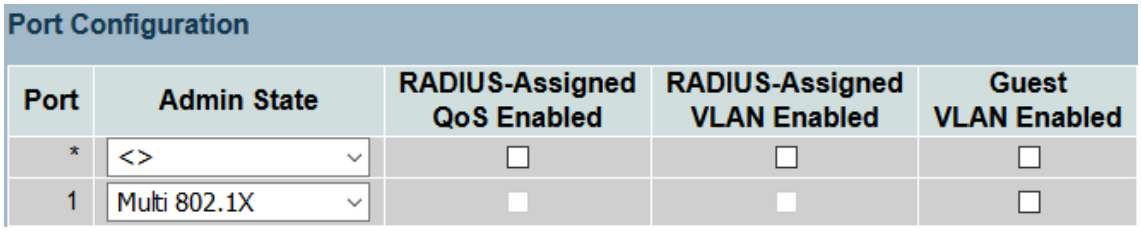
The Port Configuration Table

LANCOM Switch GUI → System → Security → NAS → Configuration

The authentication method at the switch ports is defined in the port configuration table. macmon supports the following methods:

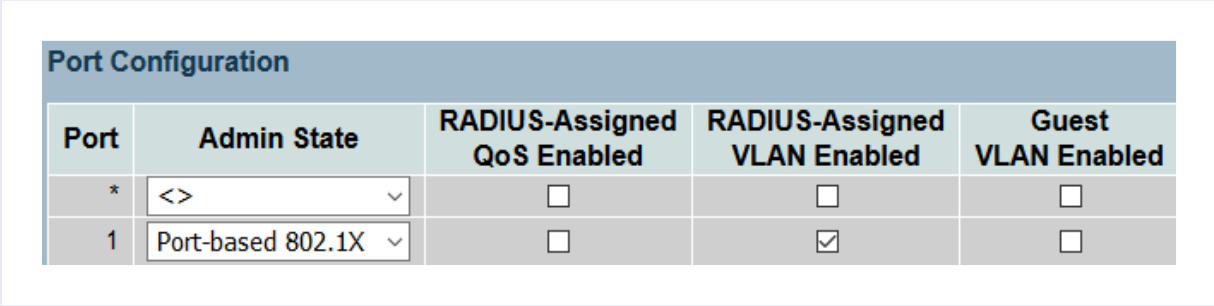
MAC Address-Based Authentication

Authentication of a single endpoint on the port with the MAC address. The RADIUS session is carried out with the Access VLAN configured on the switch port.



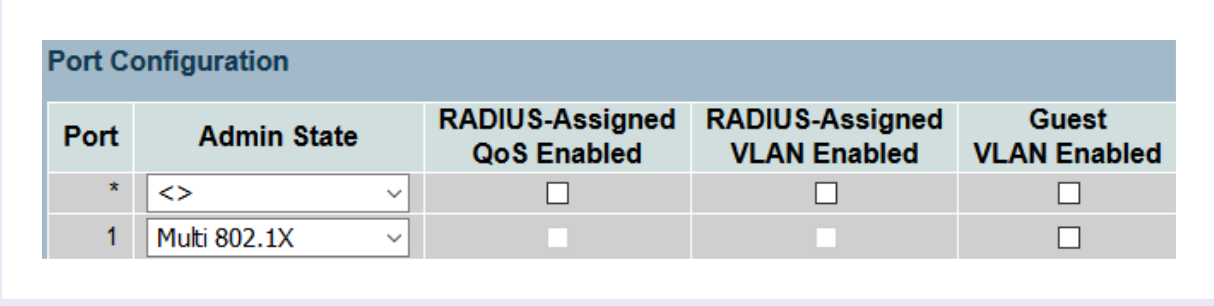
Port-Based 802.1X Authentication

Authentication of a single endpoint on the port via 802.1X (with user name/password or with certificate). A session VLAN can be transferred from macmon to the switch as a RADIUS attribute.



Multi 802.1X

Authentication of multiple endpoints on the port via 802.1X (with user name/password or with certificate). The RADIUS session is carried out for each endpoint with the Access VLAN configured on the switch port.



Configuration of the Network Device Class in macmon

The listed LANCOM switches work optimally with macmon using the following combination of actions and methods:

Action	Methods
Reading MAC addresses:	Q-Bridge
Reading interfaces:	IF-MIB::ifEntry
Reading interface statuses:	IF-MIB::ifOperStatus
Reading VLANs:	Q-Bridge (untagged)
Reading topologies:	Topology (LLDP)
Reading dot1X statuses:	IEEE 802.1X
Disabling/enabling interfaces:	IF-MIB::ifAdminStatus
Configuring VLANs:	Q-Bridge
Configuring dot1X statuses:	IEEE 8021-PAE-MIB::dot1xAuthAuthControlledPortControl

Contact

macmon secure GmbH
Alte Jakobstrasse 79-80 | 10179 Berlin
Tel.: +49 30 2325777-0 | nac@macmon.eu | www.macmon.eu