LANCOM Systems

macmon nac intelligent einfach

MACMON NAC WHITEPAPER

LANCOM-Switches

Inhaltsverzeichnis

Version: 1.2_de

macmon und LANCOM

Die Hersteller macmon secure GmbH (macmon, Netzwerkzugangskontrolle) und LANCOM (Switches und AccessPoints) haben im Zuge einer intensiven Zusammenarbeit die Kompatibilität der Produkte miteinander abgestimmt und verifiziert. Die Zusammenarbeit und vor allem der gute direkte Kontakt sorgen dabei dafür, dass auch zukünftig die Kompatibilität gewährleistet ist und bei unerwarteten Zwischenfällen die direkte Kommunikation für schnelle Lösungen sorgt. Im Folgenden werden daher die bestätigten Funktionalitäten dargestellt und genauer beschrieben.

Netzwerkgeräte mit gleichem Funktionsumfang

Von LANCOM angegebene Komponenten mit gleichem Funktionsumfang (bezogen auf die Interaktion mit 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

Getestete Funktionen

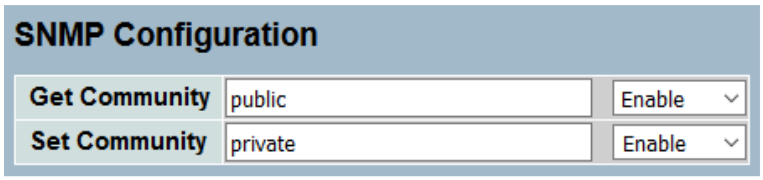
Auslesen der MAC-Adressen:	✓
Auslesen der MAC-Adressen inklusive MAC-Adressen-VLANs :	✓
Auslesen der VLANs an den Interfaces:	✓
Setzen der VLANs an den Interfaces:	✓
Interfaces Auslesen:	✓
Interface-Status Auslesen:	✓
Interface sperren/entsperren:	✓
802.1X-Status auslesen:	✓
802.1X-Status setzen:	✓
LLDP Auslesen:	✓
CDP Auslesen:	
MAC Authentication Bypass mit VLAN:	
MAC Authentication Bypass ohne VLAN:	✓
802.1X mit VLAN für ein Gerät an einem Port:	sessionbasiert / portbasiert
802.1X mit VLAN für mehrere Geräte an einem Port:	
802.1X ohne VLAN für mehrere Geräte an einem Port:	✓
Change of Autorisation:	

SNMP

Für die Verwaltung der LANCOM-Geräte mit macmon auf SNMP-Basis sind folgende Einstellungen notwendig.

Anlegen der Lese- und Schreib-Community für SNMPv1/2c

LANCOM-Switch-GUI → System → SNMP → Configuration



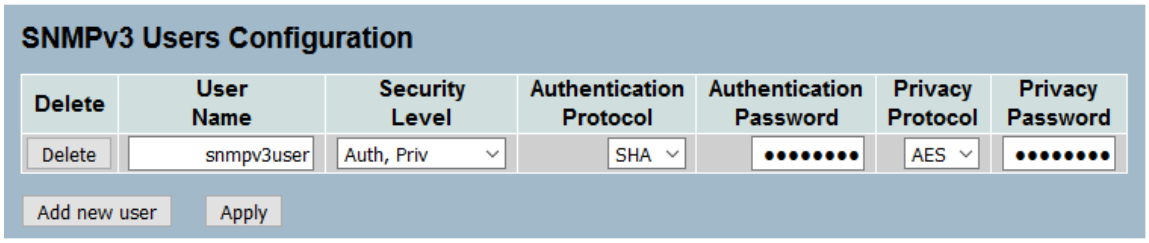
Anlegen der Lese- und Schreibberechtigung für SNMPv3 (empfohlen)

Die folgenden Schritte müssen der Reihe nach durchgeführt werden:

SNMPv3-Benutzer

LANCOM-Switch-GUI → System → SNMP → User

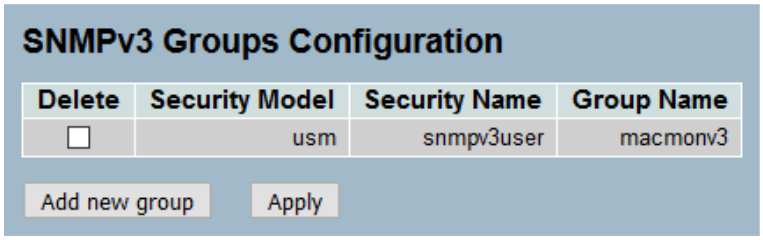
In diesem Menüpunkt werden der SNMPv3-Benutzer sowie die Verschlüsselungsparameter der SNMP-Kommunikation zwischen dem Switch und macmon definiert. Diese Daten werden für die Erstellung der SNMPv3-Zugangsdaten in macmon benötigt.



SNMPv3-Gruppe

LANCOM-Switch GUI → System → SNMP → Groups

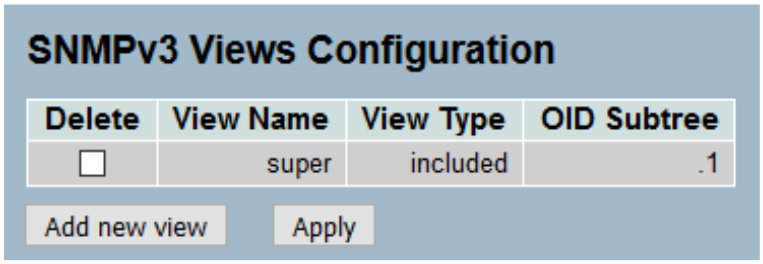
Eine SNMPv3-Gruppe wird erstellt. Der SNMPv3-Benutzer wird der Gruppe zugeordnet.



SNMPv3-Ansicht

LANCOM-Switch GUI → System → SNMP → Views

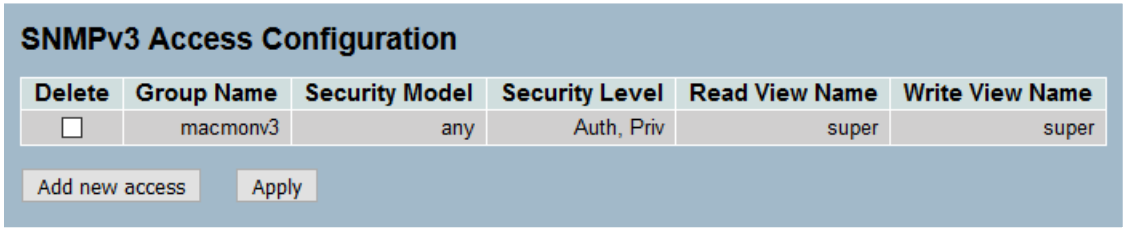
Bei der Erstellung einer SNMPv3-Ansicht wird der MIB-Bereich festgelegt, ab dem ein Auslesen bzw. Schreiben per SNMP erfolgen darf. Mit der Definition ".1" darf auf alle OIDs unterhalb dieser Angabe zugegriffen werden.



SNMPv3-Zugriff

LANCOM-Switch GUI → System → SNMP → Access

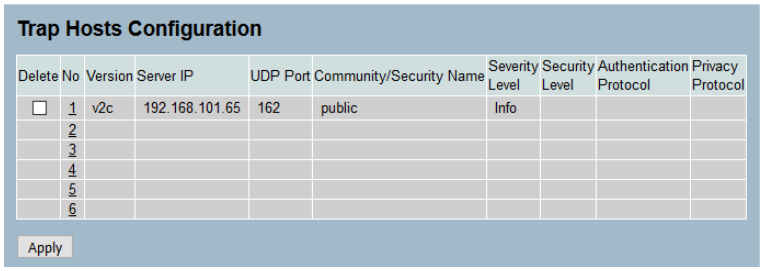
Im Menüpunkt **Access** wird die SNMPv3-Gruppe mit der SNMPv3-Ansicht verbunden. Die Mitglieder dieser Gruppe erhalten hier eine definierte SNMP Lese- und Schreibberechtigung.



Trap-Versand

LANCOM-Switch GUI → System → SNMP → Traps

Bei Bedarf kann der Trap-Versand von Link-Up- bzw. Link-Down-Traps für macmon konfiguriert werden. Der Erhalt der entsprechenden Traps in macmon ist unabhängig vom Scan-Intervall. Es werden somit die Reaktionszeiten von macmon verkürzt, z. B. beim Interface sperren oder VLAN setzen am Switch-Port.



Nachbarschaftserkennung

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

Die LANCOM-Switches unterstützten die Nachbarschaftserkennung per LLDP. Damit die LLDP-Daten korrekt per SNMP von macmon ausgelesen werden können, müssen diese Parameter für die einzelnen Ports gesetzt werden.

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

VLAN-Management

Für die Port-VLAN-Zuordnung, tagged bzw. untagged, stehen auf den LANCOM-Switches zwei Tabellen zur Verfügung.

Die VLAN-Mitgliedschaftstabelle

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

In dieser Tabelle wird die generelle VLAN-Mitgliedschaft von Ports definiert. Ist die Port-VLAN-Zugehörigkeit für bestimmte Ports ausschließlich in der VLAN-Mitgliedschaftstabelle definiert, so bedeutet das, dass diese Ports eine "tagged" Mitgliedschaft in diesem VLAN besitzen.

VLAN Membership Configuration

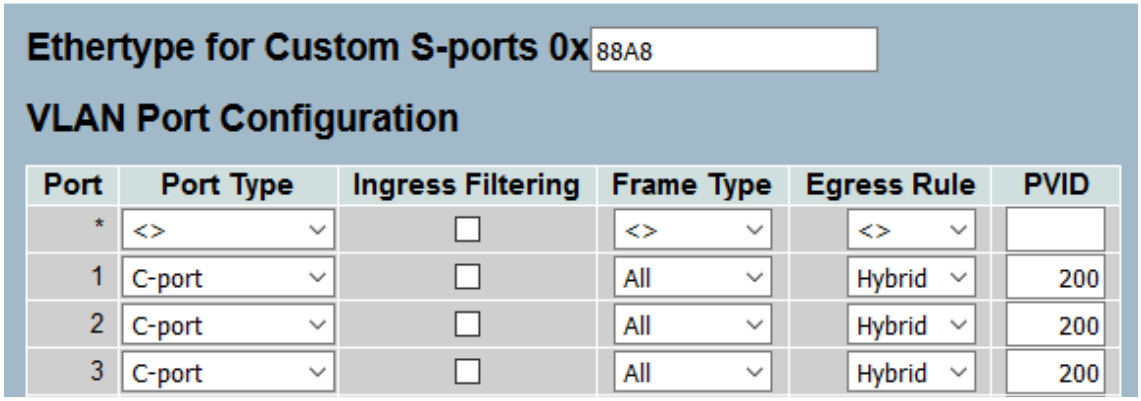
Start from VLAN 1 with 60 entries per page.

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	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Die VLAN-Port-Konfigurationstabelle

LANCOM-Switch GUI → System → Configuration → VLAN → Ports

In dieser Tabelle wird die PVID (Port VLAN ID) definiert. Ist die Port-VLAN-Zugehörigkeit für bestimmte Ports in der Mitgliedschaftstabelle und in der VLAN-Port-Konfigurationtabelle (durch die PVID) gesetzt, so haben die betreffenden Ports eine „untagged" VLAN-Zugehörigkeit.



Beim VLAN setzen behandelt macmon ausschließlich die untagged VLANs. Hierbei wird in der Mitgliedschaftstabelle und in der VLAN-Port-Konfigurationtabelle die alte Port-VLAN-Zugehörigkeit entfernt und durch eine neue Kombination in beiden Tabellen ersetzt. Beispiel in den Abbildungen:

VLAN-Mitgliedschaftstabelle: Port 1 = VLAN 200 (siehe Tabelle „VLAN Membership Configuration")
VLAN-Port-Konfigurationstabelle: Port 1 = PVID 200 (siehe Tabelle „VLAN Port Configuration")
Daraus resultiert Untagged Access VLAN: 200

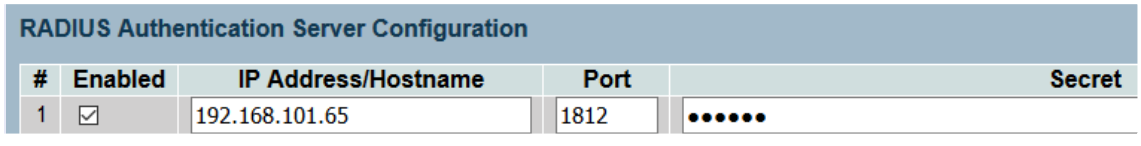
802.1X/RADIUS

Für die Verwendung der LANCOM-Geräte mit macmon über 802.1X sind die folgenden Einstellungen notwendig:

Konfiguration des RADIUS-Servers

LANCOM-Switch GUI → System → Security → AAA → Configuration

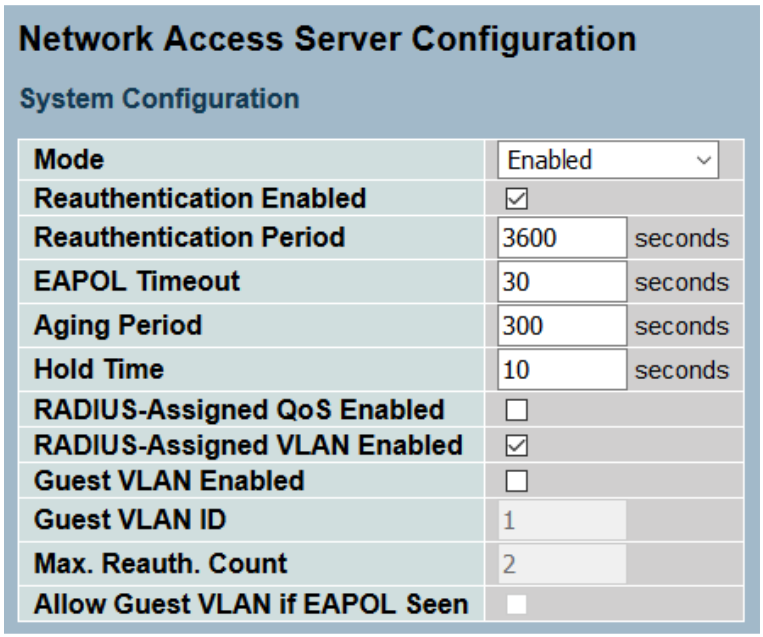
In diesem Menü wird macmon als RADIUS-Server definiert und ein Secret hinterlegt. Diese Konfiguration wird in macmon als RADIUS-Zugangsdaten an das LACNCOM-Netzwerkgerät gebunden.



Network Access Server-Konfiguration

LANCOM-Switch GUI → System → Security → NAS → Configuration

Diese Konfiguration setzt die globalen Parameter für die RADIUS-Kommunikation zwischen dem Switch, macmon und dem Supplikanten (Endgerät).



Network Access Server Configuration

System Configuration

Mode	Enabled
Reauthentication Enabled	☑
Reauthentication Period	3600 seconds
EAPOL Timeout	30 seconds
Aging Period	300 seconds
Hold Time	10 seconds
RADIUS-Assigned QoS Enabled	☐
RADIUS-Assigned VLAN Enabled	☑
Guest VLAN Enabled	☐
Guest VLAN ID	1
Max. Reauth. Count	2
Allow Guest VLAN if EAPOL Seen	☐

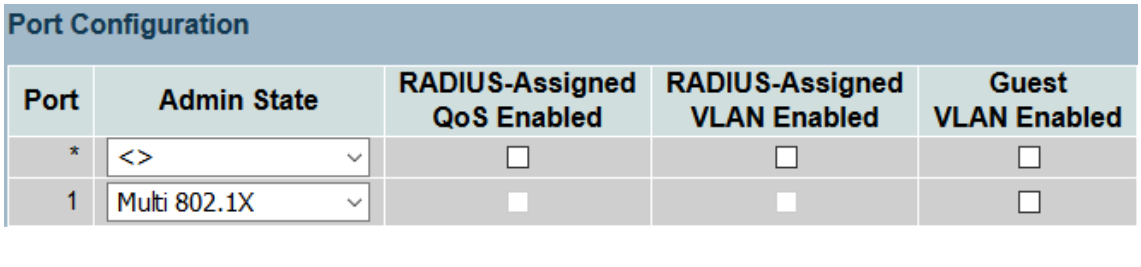
Die Port-Konfigurationstabelle

LANCOM-Switch GUI → System → Security → NAS → Configuration

In der Port-Konfigurationstabelle, wird die Authentifizierungsmethode an den Switch-Ports definiert. Die folgenden Methoden werden von macmon unterstützt:

MAC-Adressen-basierte Authentifizierung

Authentifizierung eines einzelnen Endgerätes am Port mit der MAC-Adresse. Die RADIUS-Session wird mit dem am Switch-Port konfigurierten Access-VLAN durchgeführt.

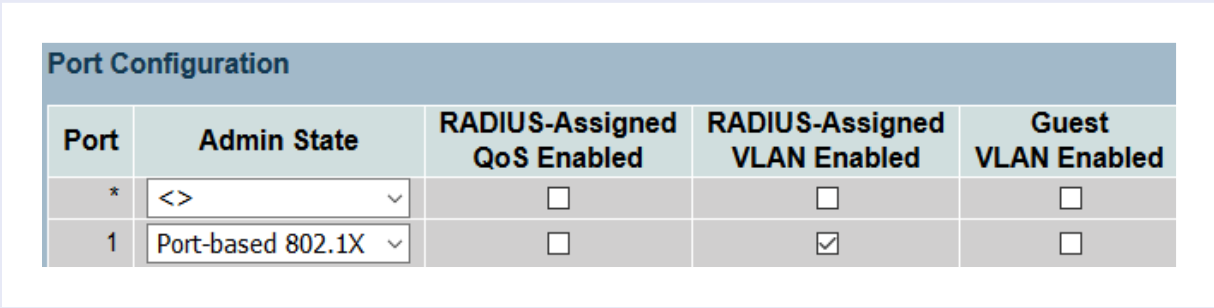


Port Configuration

Port	Admin State	RADIUS-Assigned QoS Enabled	RADIUS-Assigned VLAN Enabled	Guest VLAN Enabled
*	<>	☐	☐	☐
1	Multi 802.1X	☐	☐	☐

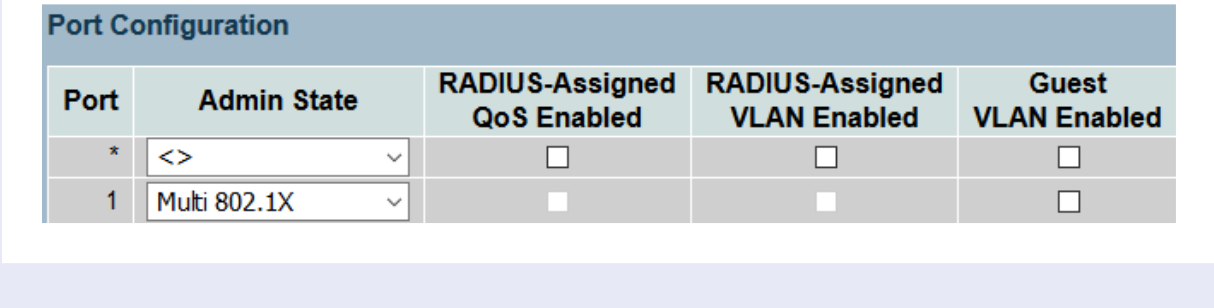
Port-basierte 802.1X-Authentifizierung

Authentifizierung eines einzelnen Endgerätes am Port per 802.1X (mit Benutzername/Passwort oder mit Zertifikat). Ein Session-VLAN kann als RADIUS-Attribut von macmon an den Switch übergeben werden.



Multi 802.1X

Authentifizierung mehrerer Endgeräte am Port per 802.1X (mit Benutzername/Passwort oder mit Zertifikat). Die RADIUS-Session wird für jedes Endgerät mit dem am Switch-Port konfigurierten Access-VLAN durchgeführt.



Konfiguration der Netzwerkgeräteklasse in macmon

Die aufgeführten LANCOM-Switches arbeiten mit folgender Kombination aus Aktionen und Methoden optimal mit macmon zusammen:

Aktion	Methoden
MAC-Adressen auslesen:	Q-Bridge
Interfaces auslesen:	IF-MIB::ifEntry
Interface-Status auslesen:	IF-MIB::ifOperStatus
VLANs auslesen:	Q-Bridge (untagged)
Topologie auslesen:	Topologie (LLDP
Dot1X-Status auslesen:	IEEE 802.1X
Interfaces (ent)sperren:	IF-MIB::ifAdminStatus
VLAN setzen:	Q-Bridge
Dot1X-Status setzen:	IEEE 8021-PAE-MIB::dot1xAuthAuthControlledPortControl

Kontakt

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