Sicherheitsrelevante Einstellungen von LCOS SX-basierten Switches der Serie LANCOM GS-23xx

Inhaltsverzeichnis

LCOS SX-Version und -Syntaxbeschreibung

Die beschriebenen **Einstellungen beziehen sich auf Switches der Serie LANCOM GS-23xx mit der minimalen LCOS SX-Version 3.32.** Um eine umfassende Absicherung insbesondere im Umfeld der zentralen Administratoren-Verwaltung erreichen zu können, werden die Funktionen der LCOS SX-Version 3.32 vorausgesetzt.

Bereits in früheren Softwareständen verfügbare Einstellungen können für diese sinngemäß übernommen werden.

Zu allen aufgeführten Konfigurationsparametern werden der Kommandozeilenpfad und die notwendigen Befehle zum Setzen der beschriebenen Parameter sowie eine Übersicht der möglichen Werte aufgeführt.

System Management

Benutzerkonten und globale Passwort-Richtlinie verwalten

In diesem Bereich können Administratoren Benutzerkonten erstellen, modifizieren und verwalten. Zudem kann die globale Passwortrichtlinie festgelegt werden.

Pfad:

/account

Mögliche Kommandos:

- **add:**
  Hinzufügen oder Bearbeiten eines Benutzerkontos
- **delete:**
  Löschen eines Benutzerkontos
- **show:**
  Anzeigen vorhandener Benutzerkonten

Syntax:

```
add <privilege level> <name> <password>

delete <name>

show
```

Mögliche Werte:

privilege level:
Die Berechtigungsstufe des Benutzers. Angegeben wird ein Zahlenwert von 1 (niedrigste Berechtigungsstufe) bis 15 (höchste Berechtigungsstufe), **siehe auch Kapitel Privilege Level.**

name:
Bis zu 32 Zeichen zur Festlegung des Benutzernamens. Wenn der Benutzername NICHT bereits in der Kontotabelle vorhanden ist, wird mit dem ausgewählten Konto ein Konto erstellt.

Wenn der Benutzername bereits in der Kontotabelle vorhanden ist, wird das ausgewählte Konto mit dem angegebenen Konto aktualisiert.

password:
Bis zu 32 Zeichen zur Festlegung des Passwortes.

Enforce Password Rules:

Dieser Schalter erzwingt die folgende Richtlinie für das Gerät und die Administratorkennwörter:

- Die Länge des Passworts muss mindestens 8 betragen und die maximal zulässige Länge beträgt 32 Zeichen.
- Das Passwort muss mindestens 3 der folgenden 4 Zeichenklassen enthalten: Klein- und Großbuchstaben, numerische Zeichen und Sonderzeichen.

Bitte beachten Sie, dass nach dem Aktivieren dieses Schalters die Richtlinie nicht sofort auf vorhandene Kennwörter überprüft wird. Die Konformität wird nur bei zukünftigen Kennwortänderungen überprüft.

Mögliche Werte;

- Yes
- No (Standardeinstellung)

Empfohlene Einstellung:

- Yes

Syntax:

```
Enforce-Password-Rules yes
Enforce-Password-Rules no
```

Privilege level (Berechtigungsstufen)

In diesem Bereich können Berechtigungsstufen für fest vorgegebene Gruppen vergeben werden. Jede Gruppe stellt die Konfigurationsmöglichkeit für eine Funktion auf dem Switch dar.

So gibt z.B. die Gruppe “Account” vor, ob es möglich ist, Benutzerkonten in der Konfiguration eines Switch zu konfigurieren. Je nach vergebenem privilege level ist es dem jeweiligen Benutzer möglich oder nicht möglich.

Pfad:

/privilege

Möglliche Kommandos:

- **group:**
  Ändern eines privilege-level für eine Gruppe.
- **show:**
  Anzeigen konfigurierter privilege-level aller Gruppen

Syntax:

```
group <group-name> <privilege-level>

show
```

Mögliche Werte:

group-name:

Account	GARP	LLDP	Maintenance	QoS	Single_IP
Aggregation	GVRP	LLDP_MED	Mirroring	SFlow	Spanning_Tree
Diagnostics	IP	Loop_Protect	PoE	SMTP	System
EEE	IPMC_Snooping	MAC_Table	Ports	SNMP	Trap_Event
Easyport	LACP	MVR	Private_VLANs	Security	UPnP
VCL	VLANs	Voice_VLAN			

privilege-level:
Die Berechtigungsstufe der Gruppe. Angegeben wird ein Zahlenwert von 1 (niedrigste Berechtigungsstufe) bis 15 (höchste Berechtigungsstufe).

SNMP(v3)

In diesem Menü wird die Verwendung des SNMP-Protokolls konfiguriert. **Wir empfehlen ausschließlich die Nutzung des SNMPv3-Protokolls.** SNMPv1 und SNMPv2 werden ebenfalls unterstützt.

Im Folgenden werden die Parameter zur SNMPv3-Konfiguration beschrieben.

SNMP System Konfiguration:

Pfad:

/snmp

Kommando:

mode

Syntax:

```
mode <Wert>
```

Mögliche Werte:

- **enable:**
  Aktiviert die Verwendung des SNMP-Protokolls
- **disable:**
  Deaktiviert die Verwendung des SNMP-Protokolls.

SNMPv3 Benutzer Konfiguration (Sicherheitsprofil):

Pfad:

/snmp

Kommando:

user

Syntax:

```
user <username> <security level> <auth-pwd> <auth-protocol> <priv-pwd>
```

Mögliche Werte:

- **username:**
  Name des SNMP-Benutzerkontos.
- **security level:**
  Angabe der Sicherheitsstufe.
  - **NoAuth, NoPriv:** Keine Authentifizierung und keine Privatsphäre. Bei Verwendung dieser Sicherheitsstufe müssen **keine weiteren Parameter, wie auth-pwd, auth-protocol und priv-pwd angegeben werden.**
  - **Auth, NoPriv:** Authentifizierung und keine Privatsphäre. Bei Verwendung dieser Sicherheitsstufe müssen **die Parameter, auth-pwd, auth-protocol angegeben werden.**
  - **Auth, Priv:** Authentifizierung und Privatsphäre. Bei Verwendung dieser Sicherheitsstufe müssen **die Parameter, auth-pwd, auth-protocol und priv-pwd angegeben werden.**
- **auth-pwd:**
  Eine Zeichenfolge, die die Authentifizierungskennwortphrase identifiziert. Für das MD5-Authentifizierungsprotokoll beträgt die zulässige Zeichenfolgenlänge 8 bis 32.

  Für das SHA-Authentifizierungsprotokoll beträgt die zulässige Zeichenfolgenlänge 8 bis 40. Der zulässige Inhalt besteht aus ASCII-Zeichen von 33 bis 126.

- **auth-protocol:**
  Gibt das Authentifizierungsprotokoll an, zu dem dieser Eintrag gehören soll. Mögliche Authentifizierungsprotokolle sind:
  - **Keine:** Kein Authentifizierungsprotokoll **(nicht empfohlen)**
  - **MD5:** Ein optionales Flag, das angibt, dass dieser Benutzer das MD5-Authentifizierungsprotokoll verwendet.
  - **SHA:** Ein optionales Flag, das angibt, dass dieser Benutzer das SHA-Authentifizierungsprotokoll verwendet. **Die Verwendung des SHA-Algorithmus wird empfohlen.**
- **priv-pwd:**
  Eine Zeichenfolge, die die Datenschutzkennwortphrase identifiziert. Die zulässige Zeichenfolgenlänge beträgt 8 bis 32, und der zulässige Inhalt ist ASCII Zeichen von 33 bis 126.

SNMPv3-Gruppen

Pfad:

/snmp

Kommando:

group

Syntax:

```
group <security model> <security name> <group name>
```

Mögliche Werte:

- **security model:**
  Gibt das Sicherheitsmodell an, zu dem dieser Eintrag gehören soll. Mögliche Sicherheitsmodelle sind:
  - **v1:** Reserviert für SNMPv1.
  - **v2c:** Reserviert für SNMPv2c.
  - **usm:** Benutzerbasiertes Sicherheitsmodell (USM). **Diese Einstellung wird für SNMPv3 enmpfohlen.**
- **security name:**
  Eine Zeichenfolge, die den Sicherheitsnamen angibt, zu dem dieser Eintrag gehören soll. Die zulässige Zeichenfolgenlänge beträgt 1 bis 32 und zulässiger Inhalt sind ASCII-Zeichen von 33 bis 126.
- **group name:**
  Eine Zeichenfolge, die den Gruppennamen angibt, zu dem dieser Eintrag gehören soll. Die zulässige Zeichenfolgenlänge beträgt 1 bis 32 und zulässiger Inhalt sind ASCII-Zeichen von 33 bis 126.

SNMPv3-Ansichten

Pfad:

/snmp

Kommando:

view

Syntax:

```
view <view name> <view type> <oid subtree>
```

Mögliche Werte:

- **view name:**
  Eine Zeichenfolge, die den Ansichtsnamen angibt, zu dem dieser Eintrag gehören soll. Die zulässige Zeichenfolgenlänge beträgt 1 bis 32 und zulässiger Inhalt sind ASCII-Zeichen von 33 bis 126.
- **view type:**
  Gibt den Ansichtstyp an, zu dem dieser Eintrag gehören soll. Mögliche Ansichtstypen sind:
  - **included:** Ein optionales Flag, das angibt, dass dieser Ansichtsunterbaum enthalten sein soll.
  - **excluded:** Ein optionales Flag, das angibt, dass dieser Ansichtsunterbaum ausgeschlossen werden soll.

  Wenn der Ansichtstyp eines Ansichtseintrags "excluded" ist, sollte im Allgemeinen ein anderer Ansichtseintrag mit dem Ansichtstyp "included" vorhanden sein, und sein OID-Teilbaum sollte den Ansichtseintrag "excluded" überschreiten.
- **oid subtree:**
  Die OID, die den Stamm des Teilbaums definiert, der der benannten Ansicht hinzugefügt werden soll. Die zulässige OID-Länge beträgt 1 bis 128. Der zulässige Zeichenfolgeninhalt ist eine digitale Zahl oder ein Sternchen (*).

SNMPv3-Zugang

Pfad:

/snmp

Kommando:

access

Syntax:

```
access <groupname> <security model> <security level> <read-view-name> <write-view-name>
```

Mögliche Werte:

- **groupname:**
  Eine Zeichenfolge, die den Ansichtsnamen angibt, zu dem dieser Eintrag gehören soll. Die zulässige Zeichenfolgenlänge beträgt 1 bis 32 und zulässiger Inhalt sind ASCII-Zeichen von 33 bis 126.
- **security model:**
  Gibt das Sicherheitsmodell an, zu dem dieser Eintrag gehören soll. Mögliche Sicherheitsmodelle sind:
  - **any:** Alle folgenden Modelle können verwendet warden.
  - **v1:** Reserviert für SNMPv1.
  - **v2c:** Reserviert für SNMPv2c.
  - **usm:** Benutzerbasiertes Sicherheitsmodell (USM). **Diese Einstellung wird für SNMPv3 empfohlen.**
- **security level:**
  Angabe der Sicherheitsstufe.
  - **NoAuth, NoPriv:** Keine Authentifizierung und keine Privatsphäre
  - **Auth, NoPriv:** Authentifizierung und keine Privatsphäre
  - **Auth, Priv:** Authentifizierung und Privatsphäre

- **read view name:**
  Der Name der MIB-Ansicht, die die MIB-Objekte definiert, für die diese Anforderung die aktuellen Werte anfordern kann. Die zulässige Zeichenfolgenlänge beträgt 1 bis 32, und der zulässige Inhalt besteht aus ASCII-Zeichen von 33 bis 126.
- **write view name:**
  Der Name der MIB-Ansicht, die die MIB-Objekte definiert, für die diese Anforderung möglicherweise neue Werte festlegen kann. Die zulässige Zeichenfolgenlänge beträgt 1 bis 32, und der zulässige Inhalt besteht aus ASCII-Zeichen von 33 bis 126.

SNMP Traps

In diesem Menü können spezifische SNMP-Traps erstellt werden. Wir empfehlen die Verwendung der Trap Version v3 mit Authentifizierung und Privacy.

Pfad:

/snmp

Kommando:

trap

Syntax:

```
trap <trap index> v3 <Trap host IP type> <ip-address> <trap port> <severity level> <secname> AuthPriv <auth-protocol> <auth-pwd> DES <priv-pwd>
```

Mögliche Werte:

- **Trap-index:**
  Wählen Sie, welchen Index Sie für den neuen SNMP-Trap verwenden möchten. Mögliche Werte sind **1 bis 6**.

- **Trap host ip type:**
  Den IP-Type, welchen der Trap Host verwendet. Mögliche Werte sind **ipv4 und ipv6**.

- **IP address:**
  IP-Adresse des Trap Host.

- **Trap port:**
  Geben Sie den vom Trap Host verwendeten Trap Port an. Mögliche Werte sind **1 bis 65535**.

- **Severity level:**
  Geben Sie den Schweregrad an, zu dem ein SNMP Trap erstellt werden soll. **Mögliche Werte sind 0 bis 7:**

  - `<0> Emergency: system is unusable`
  - `<1> Alert: action must be taken immediately`
  - `<2> Critical: critical conditions`
  - `<3> Error: error conditions`
  - `<4> Warning: warning conditions`
  - `<5> Notice: normal but significant condition`
  - `<6> Informational: informational messages`
  - `<7> Debug: debug-level messages`

- **secname:**
  Gibt die Community-Zugriffszeichenfolge beim Senden eines SNMP-Trap-Pakets an. Die zulässige Zeichenfolgenlänge beträgt 1 bis 32, und der zulässige Inhalt besteht aus ASCII-Zeichen von 33 bis 126.

- **auth-protocol:**
  Gibt das Authentifizierungsprotokoll an, zu dem dieser Eintrag gehören soll. Mögliche Authentifizierungsprotokolle sind:

  - **MD5:** Ein optionales Flag, das angibt, dass dieser Benutzer das MD5-Authentifizierungsprotokoll verwendet.
  - **SHA:** Ein optionales Flag, das angibt, dass dieser Benutzer das SHA-Authentifizierungsprotokoll verwendet. **Die Verwendung des SHA-Algorithmus wird empfohlen.**

- **auth-pwd:**
  Eine Zeichenfolge, die die Authentifizierungskennwortphrase identifiziert. Für das MD5-Authentifizierungsprotokoll beträgt die zulässige Zeichenfolgenlänge 8 bis 32.

  Für das SHA-Authentifizierungsprotokoll beträgt die zulässige Zeichenfolgenlänge 8 bis 40. Der zulässige Inhalt besteht aus ASCII-Zeichen von 33 bis 126.

- **priv-pwd:**
  Eine Zeichenfolge, die die Datenschutzkennwortphrase identifiziert. Die zulässige Zeichenfolgenlänge beträgt 8 bis 32, und der zulässige Inhalt ist ASCII Zeichen von 33 bis 126.

Sicherheit

SSH Konfiguration

In diesem Dialog kann die SSH Funktionalität global ein- oder ausgeschaltet werden.

Es können zudem neue SSH-Host-Schlüssel für das System erzeugt werden.

Hinweis:

Beachten Sie die Hinweise zur Erzeugung von SSH-Host-Schlüsseln in folgendem Knowledge Base Dokument: https://support.lancom-systems.com/knowledge/pages/viewpage.action?pageId=42106882

Pfad:

/ssh

Mögliche Kommandos:

- mode
- show
- regen-hostkey

Syntax:

```
mode <status>
show
regen-hostkey
```

Mögliche Werte:

- **status:**
  - **enable:** Aktiviert die SSH-Funktion
  - **disable:** Deaktiviert die SSH-Funktion

Authentifizierungsmethoden

Pfad:

/ssh

Mögliche Kommandos:

- fallback
- method
- show
- lock login-failures
- lock minutes

Syntax:

```
fallback <fb-service> (disable|enable)
method <service> <auth-method>
show
lock login-failures <Anzahl Loginversuche>
lock minutes <Minuten>
```

Mögliche Werte:

- **fb-service:**
  - **console:**
    Fallback über die Konsole.
  - **ssh:**
    Falback über das SSH-Protokoll.
- **disable:**
  Deaktiviert die gewählte Fallback-Methode.
- **enable:**
  Aktiviert die gewählte Fallback-Methode.

- **service:**
  - **console:**
    Authentifizierung über die Konsole.
  - **ssh:**
    Authentifizierung über das SSH-Protokoll.
- **auth-method:**
  - **local:**
    Lokale Authentifizierung
  - **tacacs+:**
    Authentifizierung über den Tacacs+ Dienst.
  - **RADIUS:**
    Authentifizierung über den RADIUS-Dienst.
- **Anzahl Loginversuche:**
  Gibt an, nach wie vielen Anmeldeversuchen eine Anmeldung gesperrt wird. **Wertebereich 0 bis 99, Standardwert 5.**
- **Minuten:**
  Gibt an, wie lange (in Minuten) die Konfiguration gegen ein erneutes Anmelden gesperrt bleibt. **Wertebereich 1 bis 99, Standardwert 5 Minuten.**

IP Source Guard

IP Source Guard ist eine Sicherheitsfunktion, mit der der IP-Verkehr auf nicht vertrauenswürdigen DHCP-Snooping-Ports eingeschränkt wird, indem der Verkehr basierend auf der DHCP-Snooping-Tabelle oder manuell konfigurierten IP-Quellverbindungen gefiltert wird.

Es hilft, IP-Spoofing-Angriffe zu verhindern, wenn ein Host versucht, die IP-Adresse eines anderen Hosts zu fälschen und zu verwenden.

Pfad:

/ip-source-guard

Mögliche Kommandos:

- mode
- add
- delete
- limit
- port mode
- show
- translate

Syntax:

```
mode <status>
add <port-list> <vlan-id> <ip-address> <mac-address>
delete <port-list> <vlan-id> <ip-address> <mac-address>
limit <port-list> <maximal dyn. clients>
port-mode <port-list> <port-status>
show <information>
translate
```

Mögliche Werte:

- **status:**
  - **enable:** Aktiviert die IP Source Guard-Funktion.
  - **disable:** Deaktiviert die IP Soure Guard-Funktion.
- **port-list:**
  Portliste, mögliche Werte sind abhängig vom jeweiligen Switch-Modell. Einzelne Ports werden durch Komma getrennt. Portbereiche werden durch einen Bindestrich (1,3-5) verbunden.
- **vlan-id:**
  Mögliche Werte zur Angabe einer VLAN-ID sind 1 bis 4094.
- **IP-Address:**
  Die IP-Adresse, für welche die IP Source Guard-Funktion erlaubt/nicht erlaubt ist.
- **mac-address:**
  Die MAC-Adresse, für welche die IP Source Guard-Funktion erlaubt/nicht erlaubt ist im Format 0a-1b-2c-3d-4e-5f.
- **maximal dyn. Clients:**
  Geben Sie die maximale Anzahl dynamischer Clients an, die an einem bestimmten Port gelernt werden können.

  Wenn der Portmodus aktiviert und der Wert “maximal dyn. Clients” gleich 0 ist, bedeutet dies, dass nur die Weiterleitung von IP-Paketen zugelassen wird, die mit statischen Einträgen auf dem bestimmten Port übereinstimmen.
- **port-status:**
  - **enable:** Aktiviert den Port.
  - **disable:** Deaktiviert den Port.
- **information:**
  - **binding-table:**
    zeigt die IP-Binding Tabelle
  - **config:**
    zeigt die aktuelle IP Source Guard Konfiguration an.
- **translate:**
  Mit diesem Befehl können Sie dynamische IP Source Guard-Einträge in statische Einträge übersetzen.

ARP Inspection

ARP Inspection ist eine Sicherheitsfunktion, welche verwendet wird, um z.B. Angriffe zu verhindern, welche durch sog. “vergiften” von ARP Caches gegen mit Layer 2 Netzwerken verbundene Hosts oder Netzwerkgeräte gestartet werden können.

Diese Funktion wird verwendet, um solche Angriffe zu blockieren. Nur gültige ARP-Anforderungen und -Antworten können das Switch-Gerät durchlaufen.

ARP spoofing prevention

Pfad:

/arp-spoofing

Mögliche Kommandos:

- spoofing mode
- spoofing-portmode
- spoofing-action
- spoofing limit
- reopen spoofing

Syntax:

```
spoofing mode <status>
spoofing portmode <port-list> <status>
spoofing action <port-list> <action>
spoofing limit <port-list> <range>
reopen spoofing <port-list> | static-gateway <1-4>
```

Mögliche Werte:

- **status:**
  - **enable:** Aktiviert die ARP spoofing prevention.
  - **disable:** Deaktiviert die ARP spoofing prevention.
- **port-list:**
  Portliste, mögliche Werte sind abhängig vom jeweiligen Switch-Modell. Einzelne Ports werden durch Komma getrennt. Portbereiche werden durch einen Bindestrich (1,3-5) verbunden.
- **action:**
  Wenn das Limit erreicht ist, kann der **Switch eine der folgenden Aktionen ausführen:**
  - **None:** Lassen Sie nicht mehr als MAC-Adressen auf dem Port zu, aber ergreifen Sie ansonsten keine weiteren Maßnahmen.
  - **Trap:** Wenn am Port Limit + 1 MAC-Adressen angezeigt werden, senden Sie einen SNMP-Trap. Wenn das **Aging deaktiviert ist**, wird nur ein SNMP-Trap gesendet. Wenn das **Aging aktiviert** ist, werden jedes Mal neue SNMP-Traps gesendet, wenn das Limit überschritten wird.
  - **Drop & Trap:** Die neuen SNMP-Traps werden gesendet und das Paket wird verworfen.
  - **Shutdown:** Wenn am Port Limit + 1 MAC-Adressen angezeigt werden, fahren Sie den Port herunter. Dies bedeutet, dass alle gesicherten MAC-Adressen vom Port entfernt werden und keine neue Adresse gelernt wird. Selbst wenn die Verbindung am Port physisch getrennt und wieder verbunden wird (durch Trennen des Kabels), bleibt der Port heruntergefahren. Es gibt drei Möglichkeiten, den Port erneut zu öffnen:
    - 1) Starten Sie den Switch neu.
    - 2) Deaktivieren und aktivieren Sie die Grenzwertsteuerung am Port oder am Switch erneut.
    - 3) Klicken Sie auf die Schaltfläche **Reopen** oder **führen Sie den reopen Befehl in der Konsole** aus..
  - **Trap & Shutdown:** Wenn am Port Limit + 1 MAC-Adressen angezeigt werden, werden sowohl die oben beschriebenen Aktionen "Trap" als auch "Shutdown" ausgeführt.
- **range:**
  Hier kann ein **Wert von 1 bis 100** angegeben werden.

IP-DoS prevention by ACL

Pfad:

/arp-spoofing

Mögliche Kommandos:

- dos icmp
- dos tcp
- dos udp
- dos-port1
- dos-port2
- dos-port3
- dos-port4

Syntax:

```
dos icmp <status>
dos tcp <status>
dos udp <status>
dos-port1 <port-status>
dos-port2 <port-status>
dos-port3 <port-status>
dos-port4 <port-status>
```

Mögliche Werte:

- **status:**
  - **enable:** Aktiviert die IP-DoS prevention für das jeweilige Protokoll.
  - **disable:** Deaktiviert die IP-DoS prevention für das jeweilige Protokoll.
- **port-status:**
  - **enable:** Aktiviert den Port als Server Port.
  - **disable:** Deaktiviert den Port als Server Port.

DHCP snooping

Das DHCP snooping kann z.B. verhindern, das ein potentieller Angreifer dem Netzwerk eigene DHCP-Server hinzufügen kann.

Pfad:

/dhcp-snooping

Mögliche Kommandos:

- clear
- mode
- port-mode
- show

Syntax:

```
clear statistics <port-list>

mode <status>

port-mode <port-list> <port-status>

show config

show statistics <port-id>
```

Mögliche Werte:

- **port-list:**
  Portliste, mögliche Werte sind abhängig vom jeweiligen Switch-Modell. Einzelne Ports werden durch Komma getrennt. Portbereiche werden durch einen Bindestrich (1,3-5) verbunden.
- **status:**
  - **enable:** Aktiviert das DHCP snooping.
  - **disable:** Deaktiviert das DHCP snooping.
- **port-status:**
  - **trusted:** Konfiguriert den Port als vertrauenswürdige Quelle für die DHCP-Nachrichten
  - **untrusted:** Konfiguriert den Port als nicht vertrauenswürdige Quelle für die DHCP-Nachrichten.
- **port-id:**
  ID des Ports, für den die Statistik angezeigt werden soll.

NAS (Network Access Server)

NAS ist eine Abkürzung für Network Access Server. Der NAS soll als Gateway dienen, um den Zugriff auf eine geschützte Quelle zu schützen. Ein Client stellt eine Verbindung zum NAS her, und der NAS stellt eine Verbindung zu einer anderen Ressource her und fragt, ob die vom Client angegebenen Anmeldeinformationen gültig sind. Basierend auf der Antwort erlaubt oder verbietet der NAS dann den Zugriff auf die geschützte Ressource. Ein Beispiel für eine NAS-Implementierung ist IEEE 802.1X.

Pfad:

/nas

Mögliche Kommandos:

- mode
- reauthentication
- reauth-period
- port-state

Syntax:

```
mode <status>
reauthentication <mode>
reauth-period <Time>
port-state <port-list> <auth-method>
```

Mögliche Werte:

- **status:**
  - **enable:** Aktiviert die NAS-Funktion.
  - **disable:** Deaktiviert die NAS-Funktion.
- **Time:**
  Hier kann ein Zahlenwert von 1 bis 3600 eingetragen werden. **Der Standardwert ist 3600.**
- **port-list:**
  Portliste, mögliche Werte sind abhängig vom jeweiligen Switch-Modell. Einzelne Ports werden durch Komma getrennt. Portbereiche werden durch einen Bindestrich (1,3-5) verbunden.

- **auth-method:**
  - **Force authorited:**
    In diesem Modus sendet der Switch einen EAPOL Success-Frame, wenn die Portverbindung hergestellt wird, und jedem Client am Port wird der Netzwerkzugriff ohne Authentifizierung gewährt.
  - **Force unauthorized:**
    In diesem Modus sendet der Switch einen EAPOL-Error-Frame, wenn die Portverbindung hergestellt wird, und jedem Client am Port wird der Netzwerkzugriff verweigert.
  - **Port-based 802.1X:**
    In der 802.1X-Welt wird der Benutzer als Supplicant bezeichnet, der Switch als Authentifizierer und der RADIUS-Server als Authentifizierungsserver. Der Authentifizierer fungiert als Man-in-the-Middle und leitet Anforderungen und Antworten zwischen dem Supplicant und dem Authentifizierungsserver weiter.

    Zwischen dem Supplicant und dem Switch gesendete Frames sind spezielle 802.1X-Frames, sogenannte EAPOL-Frames (EAP Over LANs). EAPOL-Frames kapseln EAP-PDUs (RFC3748). Zwischen dem Switch und dem RADIUS-Server gesendete Frames sind RADIUS-Pakete.

    RADIUS-Pakete kapseln auch EAP-PDUs zusammen mit anderen Attributen wie der IP-Adresse, dem Namen und der Portnummer des Supplicants auf dem Switch. EAP ist sehr flexibel, da es verschiedene Authentifizierungsmethoden wie MD5-Challenge, PEAP und TLS ermöglicht.

    Wichtig ist, dass der Authentifizierer (der Switch) nicht wissen muss, welche Authentifizierungsmethode der Supplicant und der Authentifizierungsserver verwenden oder wie viele Informationsaustausch-Frames für eine bestimmte Methode benötigt werden. Der Switch kapselt einfach den EAP-Teil des Frames in den entsprechenden Typ (EAPOL oder RADIUS) und leitet ihn weiter.

    Nach Abschluss der Authentifizierung sendet der RADIUS-Server ein spezielles Paket mit einer Erfolgs- oder Fehleranzeige. Neben der Weiterleitung dieser Entscheidung an den Supplicant verwendet der Switch sie, um den Verkehr auf dem mit dem Supplicant verbundenen Switch-Port zu öffnen oder zu blockieren.

- **Single 802.1X:**
  Bei der portbasierten 802.1X-Authentifizierung wird der gesamte Port für den Netzwerkverkehr geöffnet, sobald ein Supplicant erfolgreich an einem Port authentifiziert wurde. Auf diese Weise können andere mit dem Port verbundene Clients (z. B. über einen Hub) auf den erfolgreich authentifizierten Client zurückgreifen und Netzwerkzugriff erhalten, obwohl sie wirklich nicht authentifiziert sind. Verwenden Sie die Single 802.1X-Variante, um diese Sicherheitsverletzung zu überwinden.

  Single 802.1X ist eigentlich kein IEEE-Standard, bietet jedoch viele der gleichen Eigenschaften wie portbasiertes 802.1X. In Single 802.1X kann höchstens ein Supplicant gleichzeitig am Port authentifiziert werden. Bei der Kommunikation zwischen dem Supplicant und dem Switch werden normale EAPOL-Frames verwendet. Wenn mehr als ein Supplicant mit einem Port verbunden ist, wird derjenige berücksichtigt, der zuerst kommt, wenn die Verbindung des Ports hergestellt wird.

  Wenn dieser Supplicant innerhalb einer bestimmten Zeit keine gültigen Anmeldeinformationen bereitstellt, erhält ein anderer Supplicant eine Chance. Sobald ein Supplicant erfolgreich authentifiziert wurde, wird nur diesem Supplicant der Zugriff gewährt. Dies ist der sicherste aller unterstützten Modi. In diesem Modus wird das Port Security-Modul verwendet, um die MAC-Adresse eines Supplicants nach erfolgreicher Authentifizierung zu sichern.

- **Multi 802.1X:**
  Multi 802.1X ist - wie Single 802.1X - kein IEEE-Standard, sondern eine Variante, die viele der gleichen Eigenschaften aufweist. In Multi 802.1X können ein oder mehrere Supplicants gleichzeitig am selben Port authentifiziert werden. Jeder Supplicant wird einzeln authentifiziert und mithilfe des Port Security-Moduls in der MAC-Tabelle gesichert.

  In Multi 802.1X ist es nicht möglich, die Multicast-BPDU-MAC-Adresse als Ziel-MAC-Adresse für EAPOL-Frames zu verwenden, die vom Switch an den Supplicant gesendet werden, da dies dazu führen würde, dass alle an den Port angeschlossenen Supplicants auf vom Switch gesendete Anforderungen antworten.

  Stattdessen verwendet der Switch die MAC-Adresse des Supplicant, die vom ersten vom Supplicant gesendeten EAPOL Start- oder EAPOL Response Identity-Frame abgerufen wird. Eine Ausnahme bildet, wenn keine Bittsteller beigefügt sind. In diesem Fall sendet der Switch EAPOL Request Identity-Frames unter Verwendung der BPDU-Multicast-MAC-Adresse als Ziel, um alle möglicherweise am Port befindlichen Supplicants zu aktivieren.

  Die maximale Anzahl von Supplicants, die an einen Port angeschlossen werden können, kann mithilfe der Port Security Limit Control-Funktion begrenzt werden.

- **MAC-based Auth.:**
  Im Gegensatz zu portbasiertem 802.1X ist die MAC-basierte Authentifizierung kein Standard, sondern lediglich eine von der Branche angewandte Best-Practice-Methode. Bei der MAC-basierten Authentifizierung werden Benutzer als Clients bezeichnet, und der Switch fungiert im Namen der Clients als Supplicant.

  Der von einem Client gesendete anfängliche Frame (jede Art von Frame) wird vom Switch abgefragt, der wiederum die MAC-Adresse des Clients als Benutzername und Kennwort für den nachfolgenden EAP-Austausch mit dem RADIUS-Server verwendet. Die 6-Byte-MAC-Adresse wird in eine Zeichenfolge in der folgenden Form "xx-xx-xx-xx-xx-xx" oder "xx.xx.xx.xx.xx.xx" oder "xxxxxxxxxxxx" konvertiert (x ist a hexadezimale Ziffer). Der Switch unterstützt die MD5-Challenge-Authentifizierungsmethode, daher muss der RADIUS-Server entsprechend konfiguriert werden.

  Wenn die Authentifizierung abgeschlossen ist, sendet der RADIUS-Server eine Erfolgs- oder Fehleranzeige, die wiederum dazu führt, dass der Switch mithilfe des Port Security-Moduls den Datenverkehr für diesen bestimmten Client öffnet oder blockiert. Erst dann werden Frames vom Client auf dem Switch weitergeleitet. An dieser Authentifizierung sind keine EAPOL-Frames beteiligt. Daher hat die MAC-basierte Authentifizierung nichts mit dem 802.1X-Standard zu tun.

  Der Vorteil der MAC-basierten Authentifizierung gegenüber der 802.1X-basierten Authentifizierung besteht darin, dass die Clients keine spezielle Supplicant-Software zur Authentifizierung benötigen. Der Nachteil ist, dass MAC-Adressen von böswilligen Benutzern gefälscht werden können - Geräte, deren MAC-Adresse ein gültiger RADIUS-Benutzer ist, können von jedem verwendet werden.

  Außerdem wird nur die MD5-Challenge-Methode unterstützt. Die maximale Anzahl von Clients, die an einen Port angeschlossen werden können, kann mithilfe der Port Security Limit Control-Funktion begrenzt werden.

- **MAC-based single Auth.:**
  MAC-based single Auth. verhält sich wie MAC-based Auth., erlaubt jedoch nur einem Client, eine Verbindung über einen Port herzustellen. Frames von einem zusätzlichen Client werden ignoriert, obwohl bereits ein Client authentifiziert ist.

  Auf diese Weise können Sie die portweiten Konfigurationsoptionen für das von RADIUS zugewiesene VLAN und die von RADIUS zugewiesene QoS an diesem Port festlegen.

AAA (Authentication, Authorization, Accounting)

Der AAA-Server kann ein TACACS + - oder RADIUS-Server sein, welcher zur Erstellung und Verwaltung von Einstellungs-Objekten für die Nutzung von AAA-Server verwendet wird.

Pfad:

/aaa

Mögliche Kommandos:

- authorization
- fallback-author
- show

Syntax:

```
Authorization <status>

fallback-author <fb-status>

show config

show statistics <aaa-id>
```

Mögliche Werte:

- **status:**
  - **enable:** Aktiviert die Authentifizierung für die AAA-Funktion.
  - **disable:** Deaktiviert die Authentifizierung für die AAA-Funktion.
- **fb-status:**
  - **enable:** Aktiviert die Fallback Authorisierungs-Funktion.
  - **disable:** Deaktiviert die Fallback Authorisierungs-Funktion.
- **aaa-id:**
  ID der AAA-Konfiguration, für den die Statistik angezeigt werden soll. Hier kann ein **Zahlenwert von 1 bis 5 eingegeben** werden.

Port Security

Sie können die Port Security verwenden, um eine Schnittstelle im Input zu limitieren, indem Sie MAC-Adressen begrenzen und identifizieren.

Pfad:

/port-security

Mögliche Kommandos:

- action
- aging
- limit
- mode
- port-mode
- reopen
- show

Syntax:

```
action <port-list> <action-parameter>
aging disable
aging enable <period>
mode <status>
limit <port-list> <max. number of mac addresses>
port-mode <port-list> <port-status>
reopen <port-list>
show config|switch-status
show port-status <port>
```

Mögliche Werte:

- **status:**
  - **enable:** Aktiviert die Port-Security.
  - **disable:** Deaktiviert die Port-Security.
- **port-list:**
  Portliste, mögliche Werte sind abhängig vom jeweiligen Switch-Modell. Einzelne Ports werden durch Komma getrennt. Portbereiche werden durch einen Bindestrich (1,3-5) verbunden.
- **action-parameter:**
  - **both:**
    Es wird ein SNMP-Trap gesendet und der Port wird geschlossen.
  - **none:**
    Es erfolgt keine Aktion.
  - **shutdown:**
    Der Port wird geschlossen.
  - **trap:**
    Es wird ein SNMP-Trap gesendet.
- **period:**
  Angabe der Aging-Zeitspanne. Es ist ein **Wert von 10 bis 10000000 möglich.**
- **max. number of mac addresses:**
  Angabe zur maximalen Anzahl der MAC-Adressen. Es ist ein **Wert von 1 bis 1024 möglich.**
- **port-status:**
  - **enable:** Port aktiviert.
  - **disable:** Port deaktiviert.

Access Management

In diesem Abschnitt wird erläutert, wie Sie die Zugriffsverwaltung des Switches einschließlich HTTP / HTTPS, SNMP und TELNET / SSH konfigurieren. Sie können den Switch über ein Ethernet-LAN oder über das Internet verwalten.

Pfad:

/access-management

Mögliche Kommandos:

- add
- clear
- delete
- mode
- show

Syntax:

```
add <1-16> <ip-protocol> <start-ip> <end-ip> <protocol>
clear statistics
delete <1-16>
mode <status>
show config
show statistics
```

Mögliche Werte:

- **status:**
  - **enable:** Aktiviert das Access Management.
  - **disable:** Deaktiviert das Access Management.
- **ip-protocol:**
  - **ipv4:** Adress-Format in IPv4-Notation
  - **ipv6:** Adress-Format in IPv6-Notation
- **start-ip:**
  Erste IP-Adresse
- **end-ip:**
  Letzte IP-Adresse
- **protocol:**
  - **all:**
    Gibt an, dass der Host von jeder Schnittstelle aus auf den Switch zugreifen kann, wenn die Host-IP-Adresse mit der IP-Adresse im Eintrag übereinstimmt.
  - **snmp:**
    Gibt an, dass der Host über die SNMP-Schnittstelle auf den Switch zugreifen kann, wenn die Host-IP-Adresse mit der IP im Eintrag übereinstimmt.
  - **telnet:**
    Gibt an, dass der Host über die TELNET / SSH-Schnittstelle auf den Switch zugreifen kann, wenn die IP-Adresse des Hosts mit der im Eintrag übereinstimmt.
  - **web:**
    Gibt an, dass der Host über die HTTP / HTTPS-Schnittstelle auf den Switch zugreifen kann, wenn die IP-Adresse des Hosts mit der im Eintrag übereinstimmt

HTTP/HTTPS

In diesem Abschnitt erfahren Sie, wie Sie mit HTTPS sicher auf den Switch zugreifen. HTTPS ist ein sicheres Kommunikationsprotokoll, welches Authentifizierung und Datenverschlüsselung kombiniert, um eine sichere verschlüsselte Kommunikation über den Browser bereitzustellen. **Eine Verwendung des unverschlüsselten HTTP-Protokolls wird nicht empfohlen.**

Pfad:

/https

Mögliche Kommandos:

- mode
- redirect
- min-protocol-version
- show

Syntax:

```
mode <status>
redirect <status>
min-protocol-version <version>
show
```

Mögliche Werte:

- **status:**
  - **enable:** Aktiviert die Funktion **(empfohlen).**
  - **disable:** Deaktiviert die Funktion.
- **version:**
  Gibt die minimal verwendete TLS Protokoll-Version an. **Wir empfehlen die minimale Verwendung des TLS v1.2 Protokolls.**