Bedienungsanleitung

LT-Switch

FW-Version 6.x
Version 1.0 (März 2021)

Dieses Handbuch gilt für die Firmware-Version 6.0 der folgenden Produkte:

LT-PITE-402GBTME

barox Kommunikation AG
Im Grund
CH-5405 Baden-Dättwil

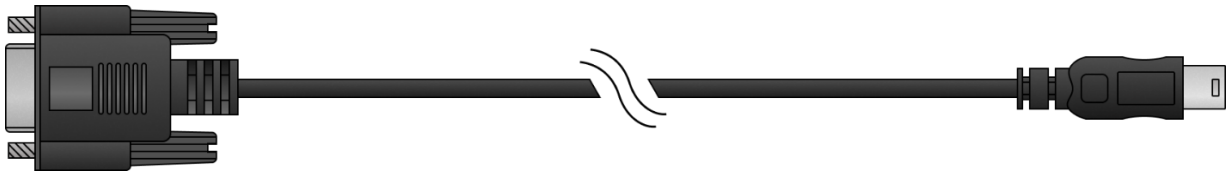
barox Kommunikation GmbH
Weiler Straße 7
D-79540 Lörrach

INHALT

CLI-Verwaltung

Konfiguration über die serielle Konsole

LT-Switches unterstützen die CLI-Verwaltung. Sie können den Switch über die Konsole oder Telnet per CLI verwalten.
Bevor Sie die serielle RS-232-Konsole konfigurieren, verbinden Sie den RS-232-Anschluss des Switches über ein RJ45-zu-DB9-Buchse-Kabel mit dem COM-Anschluss Ihres PCs.



1. Verbinden Sie Ihren PC mit dem Konsolenanschluss des Switches.
2. Starten Sie das serielle Terminalprogramm.
3. Passen Sie die Port-Einstellungen des seriellen Terminalprogramms an den Konsolenport an:
   - ❖ 115200 Baud
   - ❖ 8 Datenbits
   - ❖ Keine Parität
   - ❖ 1 Stoppbit
   - ❖ Keine Flusskontrolle
4. Der Benutzername und das Passwort des Administrators lauten standardmäßig „admin/admin“. Geben Sie den Benutzernamen und das Passwort ein, um sich bei der seriellen Konsole anzumelden.

```
Press ENTER to get started

Username: admin
Password:
# configure terminal
```

Konfiguration über die Telnet-Konsole

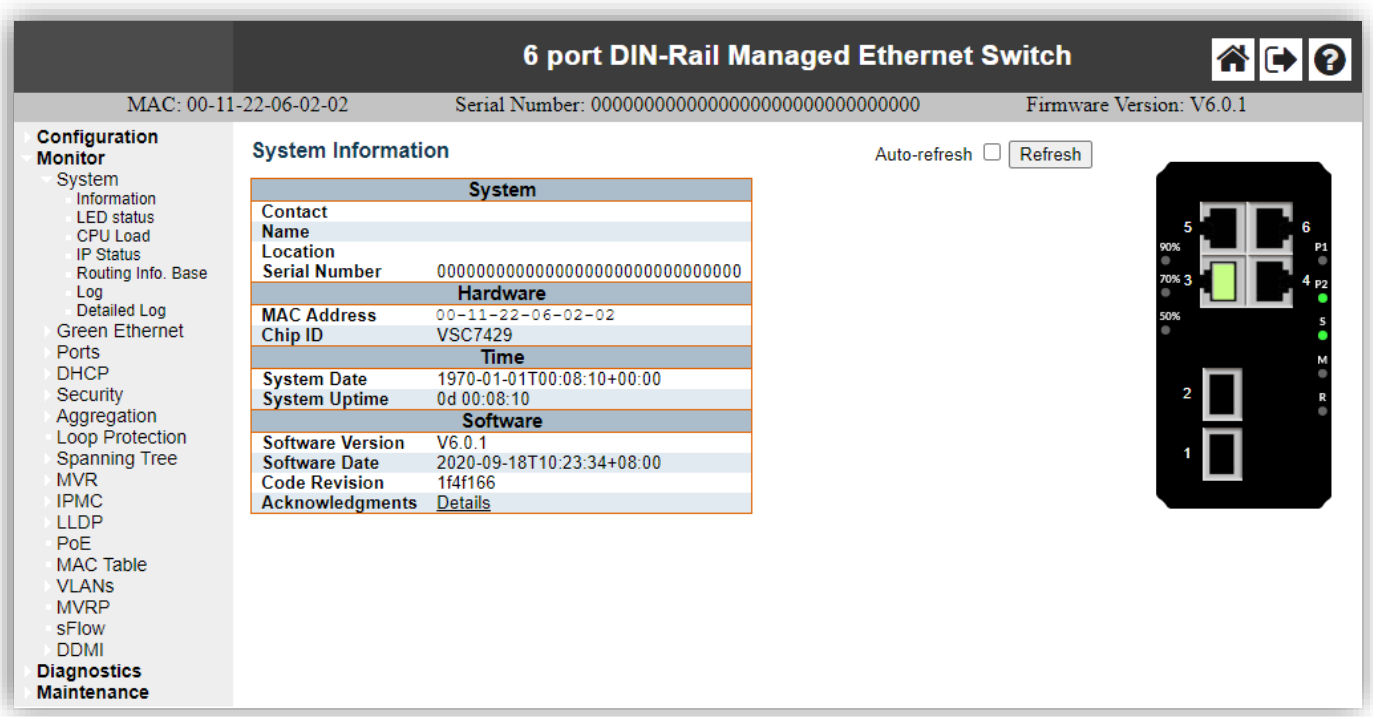
1. Verbinden Sie Ihren PC und die Switches im selben logischen Subnetz.
2. Starten Sie das Telnet-Programm.
3. Konfigurieren Sie die Standardeinstellungen des Telnet-Programms für die Switches:
   - **IP-Adresse:** 192.168.1.254
   - **Subnetzmaske:** 255.255.255.0
   - **Standard-Gateway:** keine
4. Der Benutzername und das Passwort des Administrators lauten standardmäßig „admin/admin“. Geben Sie den Benutzernamen und das Passwort ein, um sich bei der Telnet-Konsole anzumelden.

```
Press ENTER to get started

Username: admin
Password:
# configure terminal
```

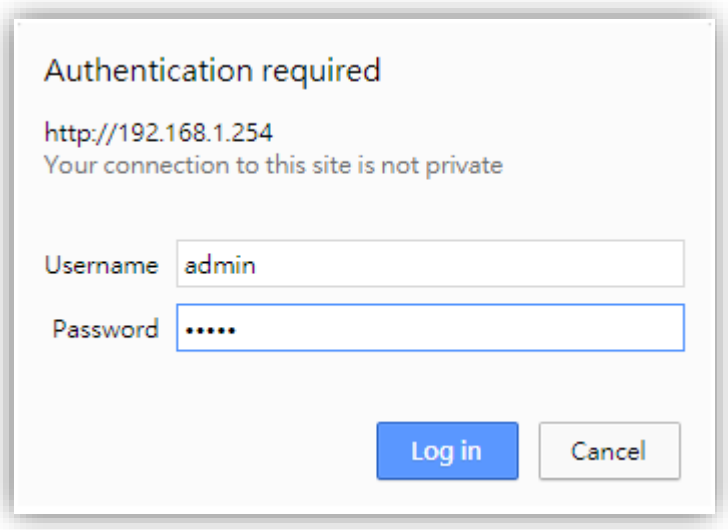
Web-Verwaltung

Neben der CLI-basierten Verwaltung unterstützen die LT-Ethernet-Switches auch die webbasierte Verwaltung.
In diesem Abschnitt wird die Webkonsole für einen industriellen Management-Switch dieser Serie beschrieben. Es handelt sich um eine **benutzerfreundliche** Oberfläche mit erweiterten Verwaltungsfunktionen, die es Ihnen ermöglicht, die Switches über einen Internetbrowser zu verwalten.



Verbindung zur Webkonsole herstellen

1. Stellen Sie über einen Browser eine Verbindung zur Standard-IP-Adresse her: http://192.168.1.254 Die Anmeldeseite wird angezeigt.
2. Der Benutzername und das Passwort des Administrators lauten standardmäßig „admin/admin“. Geben Sie den Benutzernamen und das Passwort ein und klicken Sie anschließend auf die Schaltfläche „Anmelden“.



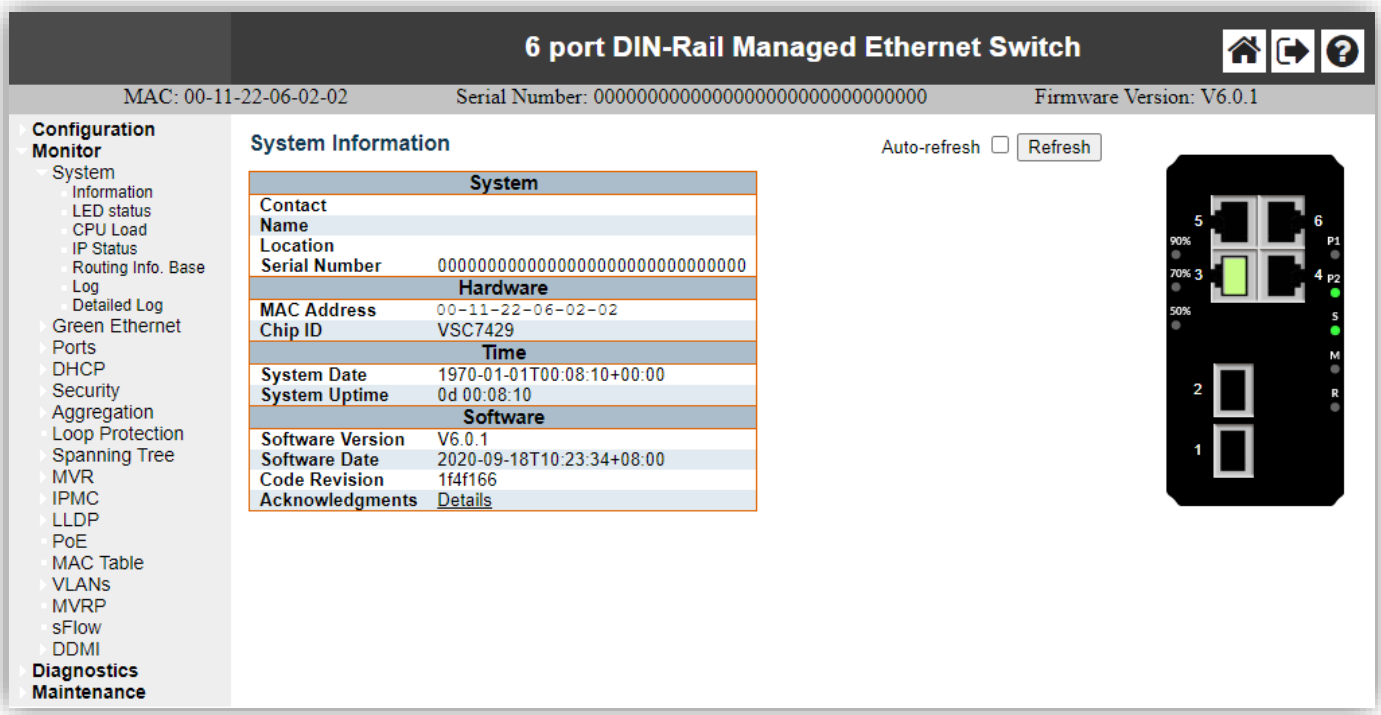
HINWEIS	Stellen Sie sicher, dass sich der PC und die Switches im selben logischen Subnetz befinden.

Überwachung

Konfiguration > System > Informationen

Übersicht über den Switch-Status

Nach der Anmeldung bei der Web-GUI-Oberfläche bietet die Seite „Übersicht über den Switch-Status“ einen Überblick über den aktuellen Status des Switch-Systems und der Ports.



- **Systemstatus**

LED	Farbe		Beschreibung
P1, P2	Grün	Ein	Stromeingang 1/2 ist aktiv
		Aus	Stromeingang 1/2 ist inaktiv
STATUS	Grün	Ein	Normalbetrieb
		Aus	Ausgeschaltet
		Blinkt	Geräteinitialisierung
	Rot	Ein	Fehler Alarm ist gesetzt, der Zustand ist jedoch inaktiv
MASTER	Grün	Ein	ERPS-Eigentümermodus (Ring-Master) ist bereit
		Aus	Der ERPS-Eigentümermodus ist nicht aktiv
RING	Grün	Ein	Ring Das Netzwerk ist aktiv und funktioniert einwandfrei
		Aus	Das Ring-Netzwerk ist inaktiv
		Blinkt	Ring-Netzwerk funktioniert nicht ordnungsgemäß oder ist falsch konfiguriert
PoE-Last	-	Aus	PoE-Last ≤ 50 %
	Blau	Ein	PoE-Last 51–70 %
	Rot	Ein	PoE-Auslastung 71–90 %
	Rot	Blinkt	PoE-Auslastung 91–100 %

Port-Status

Port	Status		
RJ45	 Deaktiviert	 Nach unten	 Link
SFP	 Deaktiviert	 Aus	 Link

Kontrollkästchen

Kontrollkästchen	Beschreibung
Automatische Aktualisierung	Aktivieren Sie dieses Kontrollkästchen, um die Seite automatisch zu aktualisieren. Die automatische Aktualisierung erfolgt alle 3 Sekunden.

Schaltflächen

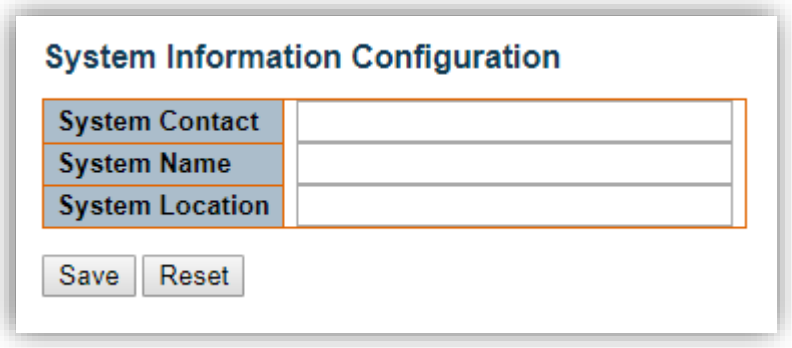
Schaltfläche	Beschreibung
Aktualisieren	Klicken Sie hier, um die Seite zu aktualisieren.

Konfiguration

Konfiguration > System > Informationen

Systeminformationen – Konfiguration

Hier werden die Systeminformationen des Switches angezeigt.



Systemkontakt

Einstellung	Beschreibung	Werkseinstellung
Max. 255 Zeichen	Die textuelle Identifikation der Kontaktperson für diesen verwalteten Knoten sowie Informationen dazu, wie diese Person kontaktiert werden kann. Die zulässige Zeichenfolgenlänge beträgt 0 bis 255, und der zulässige Inhalt besteht aus den ASCII-Zeichen 32 bis 126.	Keine

Systemname

Einstellung	Beschreibung	Werkseinstellung
Max. 255 Zeichen	Ein administrativ zugewiesener Name für diesen verwalteten Knoten. Üblicherweise handelt es sich dabei um den vollqualifizierten Domänennamen des Knotens. Ein Domänenname ist eine Textzeichenfolge, die aus Buchstaben (A–Z, a–z), Ziffern (0–9) und dem Minuszeichen (-) besteht. Leerzeichen sind als Teil eines Namens nicht zulässig. Das erste Zeichen muss ein Buchstabe sein. Außerdem darf weder das erste noch das letzte Zeichen ein Minuszeichen sein. Die zulässige Zeichenfolgenlänge beträgt 0 bis 255.	Keine

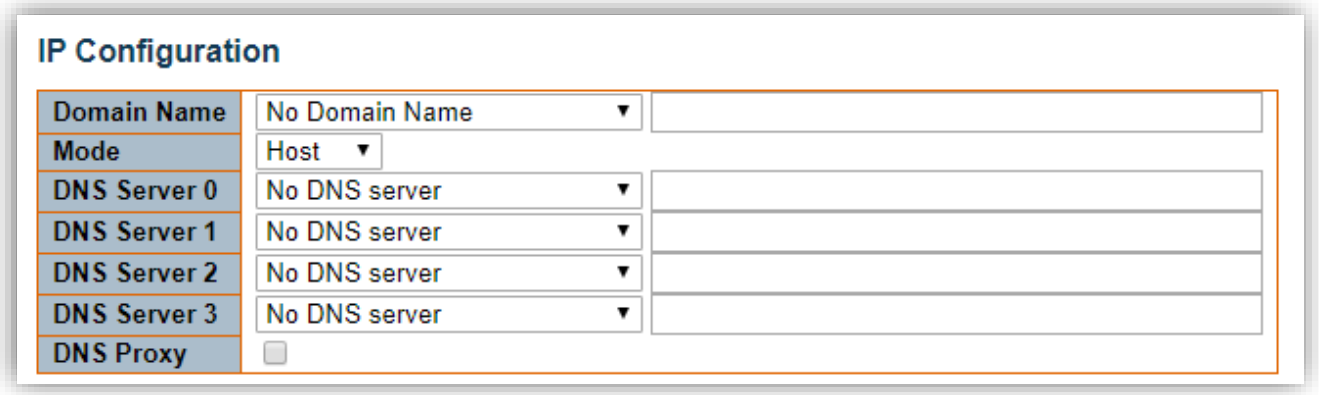
Systemstandort

Einstellung	Beschreibung	Werkseinstellung
Max. 255 Zeichen	Der physische Standort dieses Knotens (z. B. Telefonraum, 3. Stock). Die zulässige Zeichenfolgenlänge beträgt 0 bis 255, und der zulässige Inhalt besteht aus den ASCII-Zeichen 32 bis 126.	Keine

Konfiguration > System > IP

IP-Konfiguration

Konfigurieren Sie die grundlegenden IP-Einstellungen, verwalten Sie IP-Schnittstellen und IP-Routen.
Die maximal unterstützte Anzahl an Schnittstellen beträgt 8 und die maximale Anzahl an Routen 32.



Domänenname
Die Namenszeichenfolge der lokalen Domäne, zu der das Gerät gehört.
Bei den meisten Abfragen nach Namen innerhalb dieser Domäne können relative Kurznamen verwendet werden. Das System hängt dann den Domänennamen als Suffix an unqualifizierte Namen an.
Wenn der Domänenname beispielsweise auf „example.com“ festgelegt ist und Sie das PING-Ziel mit dem unqualifizierten Namen „test“ angeben, qualifiziert das System den Namen zu „test.example.com“.

Einstellung	Beschreibung	Werkseinstellung
Kein Domänenname	Es wird kein Domainname verwendet.	Kein Domänenname
Konfigurierter Domänenname	Geben Sie den Namen der lokalen Domäne explizit an. Stellen Sie sicher, dass der konfigurierte Domänenname mit der von Ihrer Organisation vorgegebenen Domäne übereinstimmt.	
Von beliebigen DHCPv6-Schnittstellen	Es wird der erste Domänenname verwendet, der im Rahmen einer DHCPv6-Zuweisung an eine DHCPv6-fähige Schnittstelle angeboten wird.	
Von dieser DHCPv6-Schnittstelle	Geben Sie an, von welcher DHCPv6-fähigen Schnittstelle ein bereitgestellter Domänenname bevorzugt werden soll.	

Modus
Legen Sie fest, ob der IP-Stack als Host oder als Router fungieren soll.

Einstellung	Beschreibung	Werkseinstellung

Host	Der IP-Verkehr zwischen Schnittstellen wird nicht weitergeleitet.	Host
Router	Der IP-Verkehr wird zwischen allen Schnittstellen weitergeleitet.	

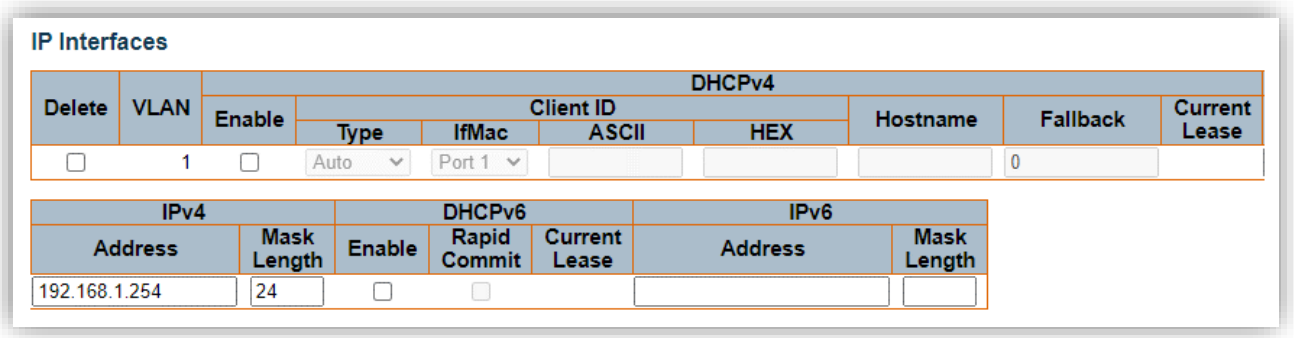
DNS-Server
Diese Einstellung steuert die vom Switch durchgeführte DNS-Namensauflösung. Es stehen vier Server zur Konfiguration zur Verfügung, wobei der Index des Servers die Präferenz (ein niedrigerer Index hat höhere Priorität) bei der DNS-Namensauflösung angibt. Das System wählt nacheinander den aktiven DNS-Server aus der Konfiguration aus, wenn der bevorzugte Server nach fünf Versuchen nicht antwortet.

Einstellung	Beschreibung	Werkseinstellung
Von beliebigen DHCPv4-Schnittstellen	Es wird der erste DNS-Server verwendet, der im Rahmen eines DHCPv4-Leases für eine DHCPv4-fähige Schnittstelle bereitgestellt wird.	Kein DNS-Server
Kein DNS-Server	Es wird kein DNS-Server verwendet.	
Konfiguriertes IPv4	Geben Sie die gültige IPv4-Unicast-Adresse des DNS-Servers explizit in Dezimalschreibweise mit Punkten an. Stellen Sie sicher, dass der konfigurierte DNS-Server erreichbar ist (z. B. per PING), um den DNS-Dienst zu aktivieren.	
Von dieser DHCPv4-Schnittstelle	Geben Sie an, von welcher DHCPv4-fähigen Schnittstelle ein bereitgestellter DNS-Server bevorzugt werden soll.	
Konfiguriertes IPv6	Geben Sie die gültige IPv6-Unicast-Adresse (außer Link-Local) des DNS-Servers explizit an. Stellen Sie sicher, dass der konfigurierte DNS-Server erreichbar ist (z. B. über PING6), um den DNS-Dienst zu aktivieren.	
Von dieser DHCPv6-Schnittstelle	Geben Sie an, von welcher DHCPv6-fähigen Schnittstelle ein bereitgestellter DNS-Server bevorzugt werden soll.	
Von allen DHCPv6-Schnittstellen	Es wird der erste DNS-Server verwendet, der im Rahmen einer DHCPv6-Zuweisung an eine DHCPv6-fähige Schnittstelle angeboten wird.	

DNS-Proxy
Wenn der DNS-Proxy aktiviert ist, leitet das System DNS-Anfragen an den aktuell konfigurierten DNS-Server weiter und antwortet den Client-Geräten im Netzwerk als DNS-Resolver. Derzeit wird nur der IPv4-DNS-Proxy unterstützt.

IP-Schnittstellen

Klicken Sie auf die Schaltfläche **„Schnittstelle hinzufügen“**, um eine neue IP-Schnittstelle hinzuzufügen. Es werden maximal 8 Schnittstellen unterstützt.

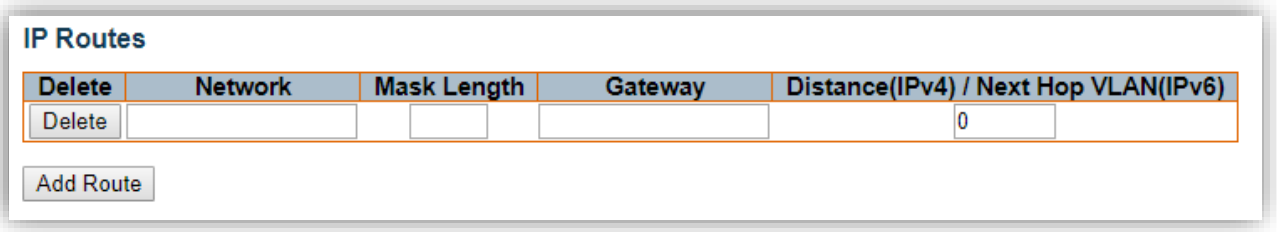


Einstellungen	Beschreibung
Löschen	Wählen Sie diese Option, um eine vorhandene IP-Schnittstelle zu löschen.
VLAN	Das mit der IP-Schnittstelle verknüpfte VLAN. Nur Ports in diesem VLAN können auf die IP-Schnittstelle zugreifen. Dieses Feld ist nur beim Anlegen einer neuen Schnittstelle zur Eingabe verfügbar.
IPv4-DHCP aktiviert	Aktivieren Sie den DHCPv4-Client, indem Sie dieses Kontrollkästchen aktivieren. Wenn diese Option aktiviert ist, konfiguriert das System die IPv4-Adresse und die Subnetzmaske der Schnittstelle mithilfe des DHCPv4-Protokolls. Der DHCPv4-Client gibt den konfigurierten Systemnamen als Hostnamen bekannt, um die DNS-Auflösung zu ermöglichen.
Typ der IPv4-DHCP-Client-Kennung	Der Typ der DHCP-Client-Kennung. Der Benutzer kann zwischen „Auto“, „ifmac“, „ASCII“ und „HEX“ wählen.
IPv4-DHCP-Client-Kennung „ifmac“	Der Schnittstellenname der DHCP-Client-Kennung. Wenn der DHCPv4-Client aktiviert ist und der Typ der Client-Kennung „ifmac“ lautet, wird die Hardware-MAC-Adresse der konfigurierten Schnittstelle im Feld der DHCP-Option 61 verwendet.
IPv4-DHCP-Client-Identifikator ASCII	Die ASCII-Zeichenkette der DHCP-Client-Kennung. Wenn der DHCPv4-Client aktiviert ist und der Typ der Client-Kennung „ascii“ lautet, wird die ASCII-Zeichenkette im Feld der DHCP-Option 61 verwendet.
IPv4-DHCP-Client-Kennung (HEX)	Die hexadezimale Zeichenfolge der DHCP-Client-Kennung. Wenn der DHCPv4-Client aktiviert ist und der Typ der Client-Kennung „hex“ lautet, wird der hexadezimale Wert im Feld der DHCP-Option 61 verwendet.
IPv4-DHCP-Hostname	Der Hostname des DHCP-Clients. Wenn der DHCPv4-Client aktiviert ist, wird der konfigurierte Hostname im Feld der DHCP-Option 12 verwendet. Ist dieser Wert eine leere Zeichenfolge, verwendet das Feld den konfigurierten Systemnamen sowie die letzten drei Bytes der System-MAC-Adresse als Hostname.
IPv4-DHCP-Fallback-Timeout	Die Anzahl der Sekunden, in denen versucht wird, eine DHCP-Lease zu erhalten. Nach Ablauf dieser Zeitspanne wird eine konfigurierte IPv4-Adresse als IPv4-Schnittstellenadresse verwendet. Der Wert Null deaktiviert den Fallback-Mechanismus, sodass DHCP so lange weitere Versuche unternimmt,

	bis eine gültige Lease erhalten wird. Zulässige Werte liegen zwischen 0 und 4294967295 Sekunden.
Aktuelle IPv4-DHCP-Lease	Bei DHCP-Schnittstellen mit einer aktiven Zuweisung zeigt diese Spalte die aktuelle Schnittstellenadresse an, wie sie vom DHCP-Server bereitgestellt wird.
IPv4-Adresse	Die IPv4-Adresse der Schnittstelle in Dezimalschreibweise mit Punkten. Wenn DHCP aktiviert ist, wird in diesem Feld die Fallback-Adresse konfiguriert. Das Feld kann leer gelassen werden, wenn kein IPv4-Betrieb auf der Schnittstelle gewünscht ist – oder keine DHCP-Fallback-Adresse gewünscht ist.
IPv4-Subnetzmaske	Die IPv4-Netzmaske in Bit (Präfixlänge). Gültige Werte liegen für eine IPv4-Adresse zwischen 0 und 30 Bit. Wenn DHCP aktiviert ist, wird in diesem Feld die Netzmaske der Fallback-Adresse konfiguriert. Das Feld kann leer gelassen werden, wenn kein IPv4-Betrieb auf der Schnittstelle gewünscht ist – oder keine DHCP-Fallback-Adresse gewünscht ist.
DHCPv6 aktivieren	Aktivieren Sie den DHCPv6-Client, indem Sie dieses Kontrollkästchen aktivieren. Wenn diese Option aktiviert ist, konfiguriert das System die IPv6-Adresse der Schnittstelle mithilfe des DHCPv6-Protokolls.
DHCPv6 Rapid Commit	Aktivieren Sie die DHCPv6-Rapid-Commit-Option, indem Sie dieses Kontrollkästchen aktivieren. Wenn diese Option aktiviert ist, beendet der DHCPv6-Client den Warteprozess, sobald eine Antwortnachricht mit einer Rapid-Commit-Option empfangen wird. Diese Option kann nur verwaltet werden, wenn der DHCPv6-Client aktiviert ist.
Aktuelle DHCPv6-Lease	Bei einer DHCPv6-Schnittstelle mit einer aktiven Lease zeigt diese Spalte die vom DHCPv6-Server zugewiesene Schnittstellenadresse an.
IPv6-Adresse	Die IPv6-Adresse der Schnittstelle. Eine IPv6-Adresse besteht aus 128-Bit-Datensätzen, die als acht Felder mit jeweils bis zu vier Hexadezimalziffern dargestellt werden, wobei die einzelnen Felder durch einen Doppelpunkt (:) getrennt sind. Beispiel: fe80::215:c5ff:fe03:4dc7. Das Symbol :: ist eine spezielle Syntax, die als Kurzform zur Darstellung mehrerer 16-Bit-Gruppen aufeinanderfolgender Nullen verwendet werden kann; es darf jedoch nur einmal vorkommen. Das System akzeptiert ausschließlich gültige IPv6-Unicast-Adressen, mit Ausnahme von IPv4-kompatiblen Adressen und IPv4-zugeordneten Adressen. Das Feld kann leer gelassen werden, wenn kein IPv6-Betrieb auf der Schnittstelle gewünscht ist.
IPv6-Maske	Die IPv6-Netzmaske, angegeben in Bit (Präfixlänge). Gültige Werte liegen für eine IPv6-Adresse zwischen 1 und 128 Bit. Das Feld kann leer gelassen werden, wenn kein IPv6-Betrieb auf der Schnittstelle gewünscht ist.

IP-Routen

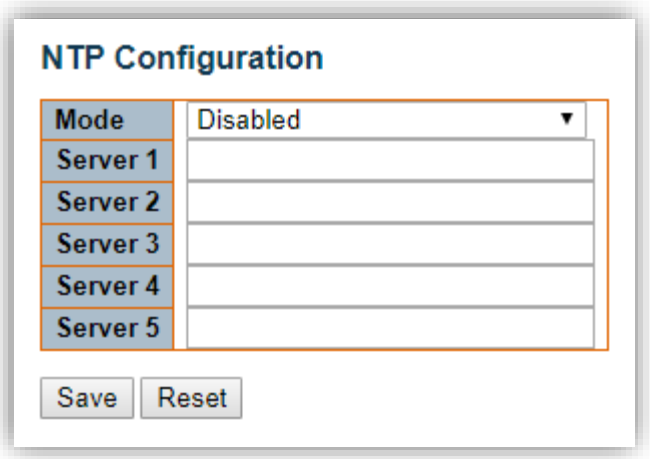
Klicken Sie auf die Schaltfläche **„Route hinzufügen“**, um eine neue IP-Route hinzuzufügen. Es werden maximal 32 Routen unterstützt.



Einstellung	Beschreibung
Löschen	Wählen Sie diese Option, um eine vorhandene IP-Route zu löschen.
Netzwerk	Das Ziel-IP-Netzwerk oder die Host-Adresse dieser Route. Gültige Formate sind die Dezimalschreibweise mit Punkten oder eine gültige IPv6-Notation. Eine Standardroute kann den Wert **0.0.0.0** oder die IPv6-Notation **::** verwenden.
Maskenlänge	Die Ziel-IP-Netzwerk- oder Host-Maske, angegeben in der Anzahl der Bits (Präfixlänge). Sie legt fest, wie viel von einer Netzwerkadresse übereinstimmen muss, damit diese Route zutrifft. Gültige Werte liegen zwischen 0 und 32 Bits bzw. 128 für IPv6-Routen. Nur eine Standardroute hat eine Maskenlänge von **0** (da sie mit allem übereinstimmt).
Gateway	Die IP-Adresse des IP-Gateways. Gültige Formate sind die Dezimalschreibweise mit Punkten oder eine gültige IPv6-Notation. Gateway und Netzwerk müssen vom gleichen Typ sein.
Entfernung (nur für IPv4)	Der Distanzwert eines Routeneintrags wird verwendet, um den Routern Prioritätsinformationen der Routing-Protokolle bereitzustellen. Wenn zwei oder mehr verschiedene Routing-Protokolle beteiligt sind und dasselbe Ziel haben, kann der Distanzwert zur Auswahl des besten Pfades herangezogen werden.
VLAN des nächsten Hops (nur für IPv6)	Die VLAN-ID (VID) der spezifischen IPv6-Schnittstelle, die dem Gateway zugeordnet ist. Die angegebene VID liegt im Bereich von 1 bis 4095 und ist nur wirksam, wenn die entsprechende IPv6-Schnittstelle gültig ist. Wenn es sich bei der IPv6-Gateway-Adresse um eine Link-Local-Adresse handelt, muss das Next-Hop-VLAN für das Gateway angegeben werden. Wenn die IPv6-Gateway-Adresse keine Link-Local-Adresse ist, ignoriert das System das Next-Hop-VLAN für das Gateway.

Konfiguration > System > NTP

NTP-Konfiguration



Modus

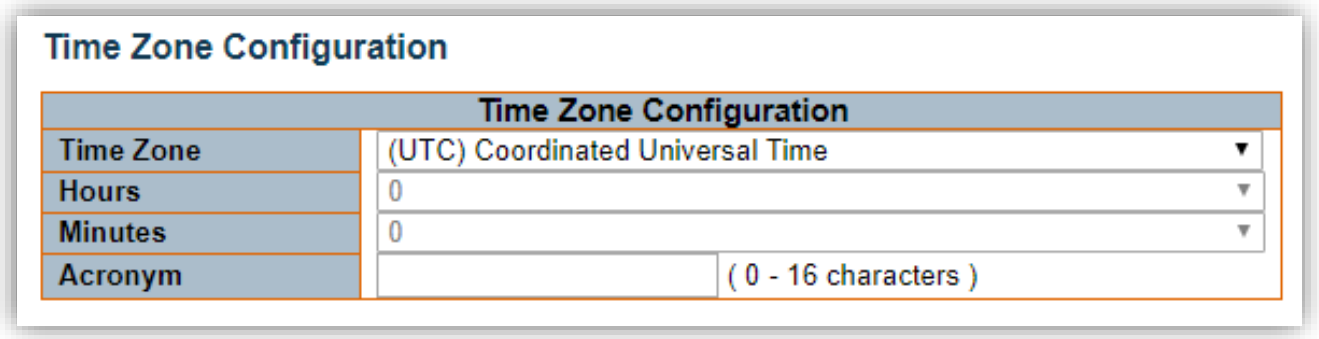
Einstellung	Beschreibung	Werkseinstellung
Aktiviert	Aktiviert den Betrieb im NTP-Client-Modus.	Deaktiviert
Deaktiviert	Deaktivieren Sie den NTP-Client-Modus.	

Server

Einstellung	Beschreibung	Werkseinstellung
IPv4- oder IPv6-Adresse eines NTP-Servers	Eine IPv6-Adresse besteht aus 128-Bit-Datensätzen, die als acht Felder mit jeweils bis zu vier Hexadezimalziffern dargestellt werden, wobei die einzelnen Felder durch einen Doppelpunkt (:) voneinander getrennt sind. Beispiel: fe80::215:c5ff:fe03:4dc7. Das Symbol :: ist eine spezielle Syntax, die als Kurzform zur Darstellung mehrerer 16-Bit-Gruppen aufeinanderfolgender Nullen verwendet werden kann; es darf jedoch nur einmal vorkommen. Es kann auch eine gültige IPv4-Adresse darstellen. Beispiel: ::192.1.2.34. Darüber hinaus kann es auch eine Domain-Adresse akzeptieren.	Keine

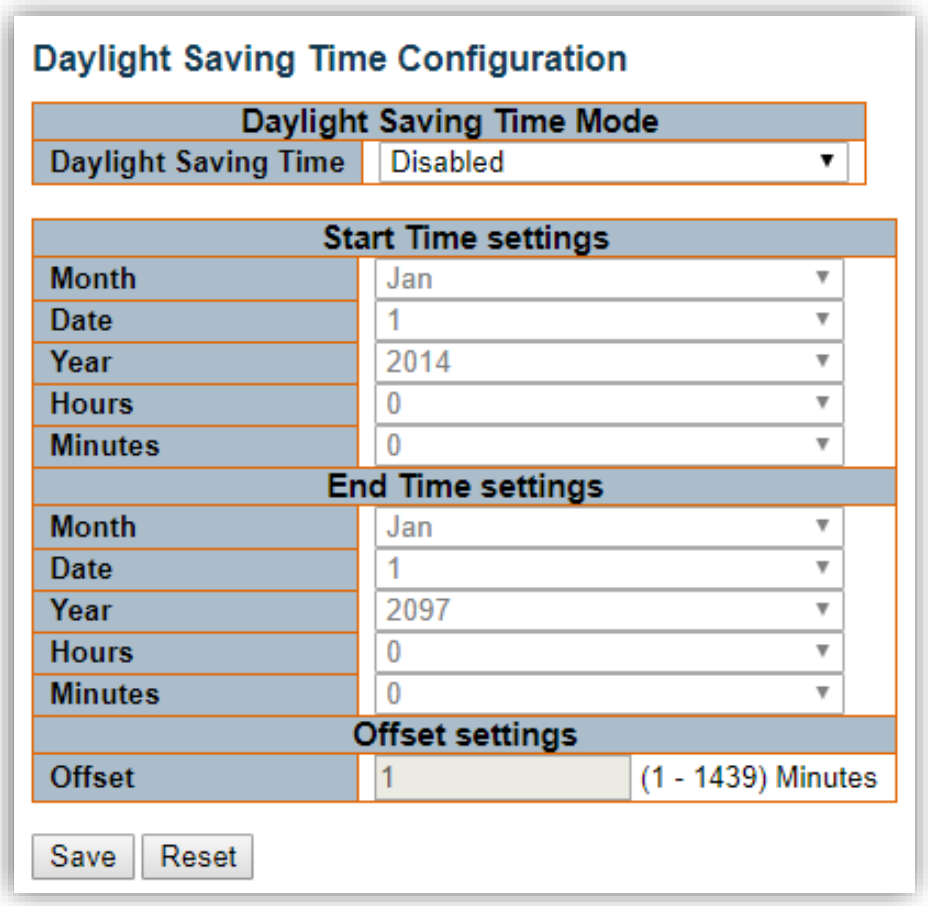
Konfiguration > System > Zeit

Zeitzonenkonfiguration



Schauplatz	Beschreibung	Werkseinstellung
Zeitzone	Listet verschiedene Zeitzonen weltweit auf. Wählen Sie die entsprechende Zeitzone aus der Dropdown-Liste aus und klicken Sie auf „Speichern“, um die Einstellung zu übernehmen. Die Option „Manuelle Einstellung“ wird für Zeitzonen verwendet, die nicht in der Auswahlliste enthalten sind.	UTC
Stunden	Anzahl der Stunden Abweichung von UTC. Das Feld ist nur bei manueller Zeitzoneneinstellung verfügbar.	0
Minuten	Anzahl der Minuten, um die die Zeit gegenüber UTC verschoben ist. Das Feld ist nur bei manueller Zeitzoneneinstellung verfügbar.	0
Kürzel	Der Benutzer kann das Akronym der Zeitzone festlegen. Dabei handelt es sich um ein vom Benutzer konfigurierbares Akronym zur Identifizierung der Zeitzone. (Bereich: bis zu 16 Zeichen) Beachten Sie, dass die Zeichenfolge „“ eine spezielle Syntax ist, die für eine leere Eingabe reserviert ist.	Keine

Konfiguration der Sommerzeit



Sommerzeitmodus

Einstellung	Beschreibung	Werkseinstellung
Sommerzeit	Hiermit wird die Uhr entsprechend den unten festgelegten Einstellungen für eine definierte Dauer der Sommerzeit vor- oder zurückgestellt. Wählen Sie „Deaktivieren“, um die Sommerzeitkonfiguration zu deaktivieren. Wählen Sie „Wiederkehrend“ und legen Sie die Dauer der Sommerzeit fest, um die Konfiguration jedes Jahr zu wiederholen. Wählen Sie „Einmalig“ und legen Sie die Dauer der Sommerzeit für eine einmalige Konfiguration fest.	Deaktiviert

Einstellungen für die Startzeit
Wählen Sie den Startmonat, das Startdatum, das Startjahr sowie die Startstunden und -minuten aus.

Einstellungen für die Endzeit
Wählen Sie den Endmonat, das Enddatum, das Endjahr, die Endstunden und die Endminuten aus.

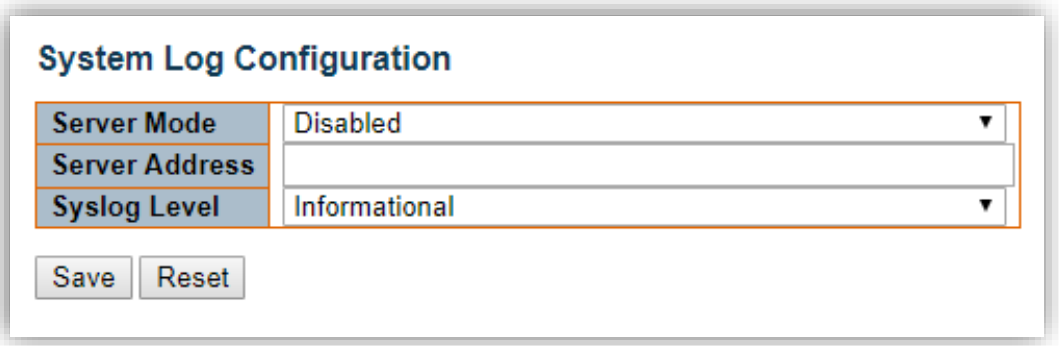
Einstellungen für den Versatz

Einstellung	Beschreibung	Werkseinstellung

Offset	Geben Sie die Anzahl der Minuten ein, die während der Sommerzeit hinzugefügt werden sollen. (Bereich: 1 bis 1439)	1

Konfiguration > System > Protokoll

Konfiguration des Systemprotokolls



Servermodus
Gibt den Servermodus an. Wenn dieser Modus aktiviert ist, werden die Syslog-Meldungen an den Syslog-Server gesendet. Das Syslog-Protokoll basiert auf UDP-Kommunikation und wird über den UDP-Port 514 empfangen. Da UDP ein verbindungsloses Protokoll ist, das keine Bestätigungen bereitstellt, sendet der Syslog-Server keine Bestätigungen an den Absender zurück. Das Syslog-Paket wird immer gesendet, auch wenn der Syslog-Server nicht existiert.

Einstellung	Beschreibung	Werkseinstellung
Aktiv	Servermodus aktivieren.	Deaktiviert
Deaktiviert	Deaktivieren Sie den Servermodus.	

Serveradresse
Gibt die IPv4-Hostadresse des Syslog-Servers an. Wenn der Switch über eine DNS-Funktion verfügt, kann dies auch ein Domänenname sein.

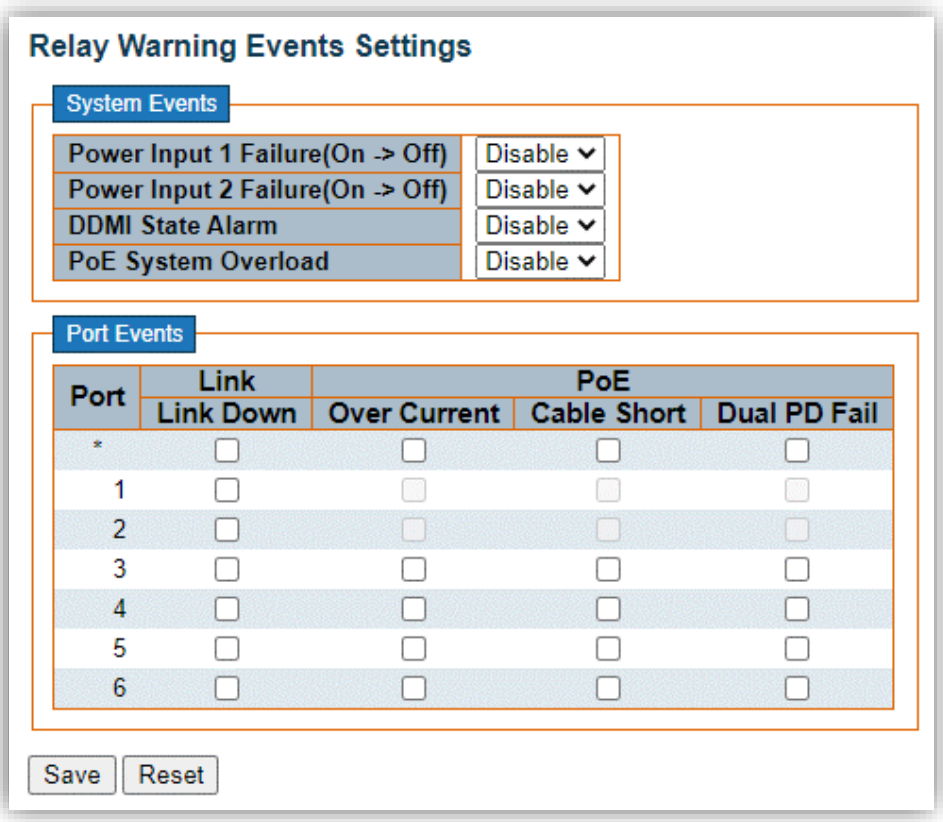
Syslog-Stufe
Gibt an, welche Art von Meldungen an den Syslog-Server gesendet werden.

Einstellung	Beschreibung	Werkseinstellung
Fehler	Sendet die spezifischen Meldungen, deren Schweregrad kleiner oder gleich „Fehler (3)“ ist.	Information
Warnung	Sendet die spezifischen Meldungen, deren Schweregrad kleiner oder gleich „Warnung“ (4) ist.	
Hinweis	Sendet die spezifischen Meldungen, deren Schweregrad kleiner oder gleich „Hinweis“ (5) ist.	
Informativ	Sendet die spezifischen Meldungen, deren Schweregrad kleiner oder gleich „Informativ“ (6) ist.	

Konfiguration > System > Ereigniswarnung > Relais

Einstellungen für Relais-Warnereignisse

Die Relaiswarnfunktion nutzt den Relaisausgang, um den Benutzer zu benachrichtigen, wenn bestimmte, vom Benutzer konfigurierte Ereignisse eintreten.



Systemereignisse

Ereignisse bei Stromausfall
Zeigt den Betrieb im Abschaltmodus an. Der Warnrelaisausgang wird ausgelöst, wenn der Switch abgeschaltet wird.

Einstellung	Beschreibung	Werkseinstellung
Aktiviert	Betrieb im Stromausfall-Ereignismodus aktivieren.	Deaktiviert
Deaktiviert	Deaktivieren Sie den Betrieb im Stromausfall-Ereignismodus.	

DDMI-Zustandsalarm
Zeigt den Alarmbetrieb der SFP-DDMI-Informationen an. Warnung Der Relaisausgang wird ausgelöst, wenn der aktuelle SFP-DDMI-Wert des Switches den Alarmschwellenwert überschreitet.
* Die DDMI-Funktion wird nur vom SFP-Modell unterstützt.

Einstellung	Beschreibung	Werkseinstellung
Aktiviert	DDMI-Informationsmeldungen aktivieren.	Deaktiviert
Deaktiviert	DDMI-Informationswarnungen deaktivieren.	

PoE-Systemüberlastung
Zeigt das gesamte PoE-Leistungsbudget an. Der Warnrelaisausgang wird ausgelöst, wenn das gesamte PoE-Leistungsbudget überlastet ist.

Einstellung	Beschreibung	Werkseinstellung
Aktiviert	Aktivieren Sie das PoE-Systemüberlastungsereignis.	Deaktiviert
Deaktiviert	Deaktivieren Sie das PoE-Systemüberlastungsereignis.	

Port-Ereignisse

Ereignisse zum Port-Verbindungsstatus
Zeigt den Betriebsstatus der Portverbindung an. Warnung Der Relaisausgang wird ausgelöst, wenn die Portverbindung unterbrochen ist.

Einstellung	Beschreibung
Verbindung unterbrochen	Legt fest, ob die Warnung bei einem Port-Verbindungsausfall an diesem Switch-Port aktiviert ist.

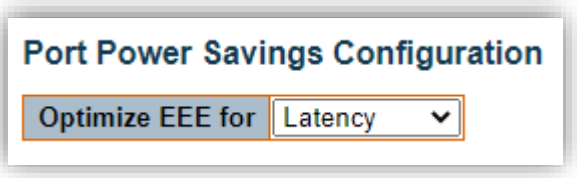
Port-PoE-Statusereignisse
Zeigt den Port-Verbindungsstatus und den PoE-Betriebsstatus an. Der Warnrelaisausgang wird ausgelöst, wenn die Portverbindung unterbrochen ist oder die konfigurierten PoE-Ereignisse eintreten.

Einstellung	Beschreibung
Überstrom	Legt fest, ob die Warnung bei einem PoE-Überstromereignis an diesem Switch-Port aktiviert ist.
Kabelkurzschluss	Legt fest, ob die Warnung bei einem PoE-Kabelkurzschluss an diesem Switch-Port aktiviert ist.

Ausfall von zwei PDs	Legt fest, ob die Warnung bei einem Ausfall von zwei PDs am BT-Port aktiviert ist (nur wenn die Überprüfung auf zwei PDs deaktiviert ist).

Konfiguration > Green Ethernet > Energieeinsparung am Port

Konfigurations en zur Energieeinsparung am Port

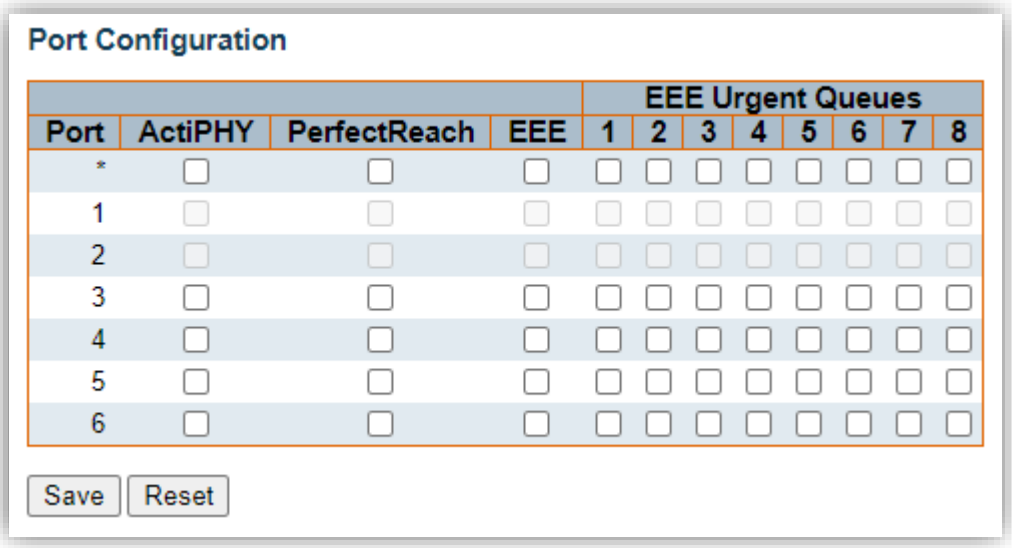


Was ist EEE?
EEE ist eine Energiesparoption, die den Stromverbrauch bei geringer oder keiner Datenauslastung reduziert.
EEE funktioniert, indem die Schaltkreise bei fehlendem Datenverkehr abgeschaltet werden. Sobald ein Port Daten zur Übertragung empfängt, werden alle Schaltkreise wieder eingeschaltet. Die Zeit, die zum Einschalten der Schaltkreise benötigt wird, wird als Wakeup-Zeit bezeichnet. Die Standard-Wakeup-Zeit beträgt 17 µs für 1-Gbit-Verbindungen und 30 µs für andere Verbindungsgeschwindigkeiten. EEE-Geräte müssen sich auf den Wert der Wakeup-Zeit einigen, um sicherzustellen, dass sowohl beim empfangenden als auch beim sendenden Gerät alle Schaltkreise eingeschaltet sind, wenn Datenverkehr übertragen wird. Die Geräte können Informationen zur Wakeup-Zeit über das LLDP-Protokoll austauschen.
EEE funktioniert für Ports im Auto-Negotiation-Modus, bei dem der Port entweder auf den 1-Gbit- oder den 100-Mbit-Vollduplex-Modus ausgehandelt wird.
Bei Ports, die nicht EEE-fähig sind, sind die entsprechenden EEE-Kontrollkästchen ausgegraut, sodass EEE dort nicht aktiviert werden kann.
Wenn ein Port zur Energieeinsparung abgeschaltet wird, wird der ausgehende Datenverkehr in einem Puffer gespeichert, bis der Port wieder eingeschaltet wird. Da das Abschalten und Einschalten des Ports mit einem gewissen Overhead verbunden ist, lässt sich mehr Energie einsparen, wenn der Datenverkehr gepuffert werden kann, bis ein großer Datenburst übertragen werden kann. Das Puffern des Datenverkehrs führt zu einer gewissen Latenz im Datenverkehr.

EEE optimieren für
Der Switch kann so eingestellt werden, dass EEE entweder auf maximale Energieeinsparung oder auf minimale Datenübertragungslatenz optimiert wird.

Einstellung	Beschreibung	Werkseinstellung
Leistung	Beste Energieeinsparung	Latenz
Latenz	Geringste Datenverkehrs-Latenz	

Port-Konfiguration

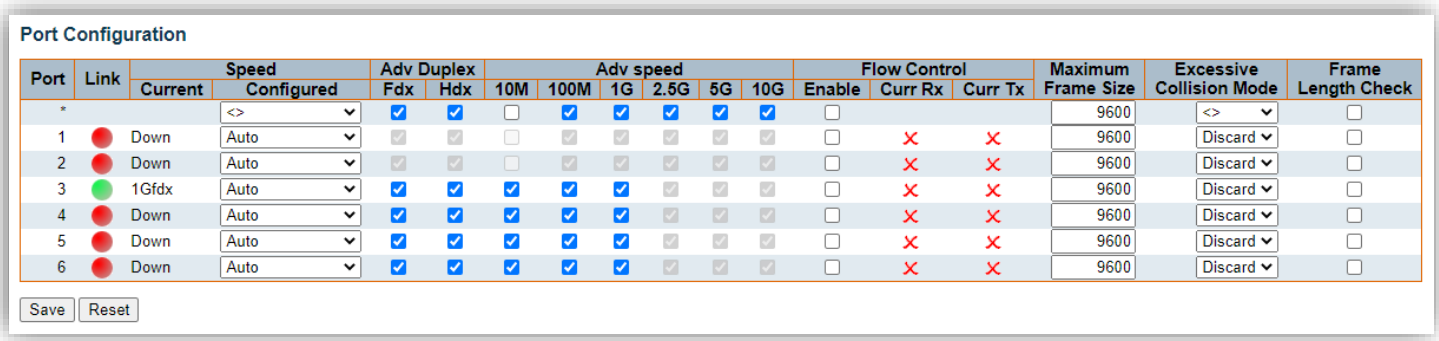


Einstellung	Beschreibung
Port	Die Switch-Port-Nummer des logischen Ports.
ActiPHY	Energiesparmodus bei unterbrochener Verbindung aktiviert. ActiPHY senkt die Leistungsaufnahme eines Ports, wenn keine Verbindung besteht. Der Port wird für einen kurzen Moment mit Strom versorgt, um festzustellen, ob ein Kabel eingesteckt ist.
PerfectReach	Energiesparfunktion für die Kabellänge aktiviert. PerfectReach ermittelt die Kabellänge und senkt die Leistungsaufnahme bei Ports mit kurzen Kabeln.
EEE	Legt fest, ob EEE für diesen Switch-Port aktiviert ist. Um die Energieeinsparung zu maximieren, wird die Verbindung nicht sofort hergestellt, sobald Daten für einen Port zur Übertragung bereitstehen, sondern in eine Warteschlange gestellt, bis ein Datenburst zur Übertragung bereit ist. Dies führt zu einer gewissen Latenz im Datenverkehr. Auf Wunsch ist es möglich, die Latenz für bestimmte Frames zu minimieren, indem die Frames einer bestimmten Warteschlange zugeordnet (mithilfe von QoS) und diese Warteschlange dann als dringende Warteschlange markiert wird. Wenn eine dringende Warteschlange Daten zur Übertragung erhält, werden die Schaltkreise sofort hochgefahren und die Latenz auf die Aufwachzeit reduziert.
EEE-Dringlichkeitswarteschlangen	Eingestellte Warteschlangen aktivieren die Übertragung von Frames, sobald Daten verfügbar sind. Andernfalls verschiebt die Warteschlange die Übertragung, bis ein Burst von Frames übertragen werden kann.

Konfiguration > Ports

Port-Konfiguration

Auf dieser Seite werden die aktuellen Portkonfigurationen angezeigt. Hier können die Ports auch konfiguriert werden.



Port

Dies ist die logische Portnummer für diese Zeile.

Verbindung

Der aktuelle Verbindungsstatus wird grafisch dargestellt.

Farbe	Beschreibung
Grün	Die Verbindung ist aktiv.
Rot	Die Verbindung ist unterbrochen.

Aktuelle Verbindungsgeschwindigkeit

Zeigt die aktuelle Verbindungsgeschwindigkeit des Ports an.

Konfigurierte Verbindungsgeschwindigkeit

Wählt eine beliebige verfügbare Verbindungsgeschwindigkeit für den angegebenen Switch-Port aus. Es werden nur die Geschwindigkeiten angezeigt, die von dem jeweiligen Port unterstützt werden.

Einstellung	Beschreibung	Werkseinstellung
Deaktiviert	Deaktiviert den Betrieb des Switch-Ports.	Auto
Auto	Der Port führt eine automatische Geschwindigkeitsaushandlung mit dem Verbindungspartner durch und wählt die höchste Geschwindigkeit aus, die mit dem Verbindungspartner kompatibel ist.	
10 Mbit/s HDX	Erzwingt den 10-Mbps-Halbduplex-Modus für den CU-Port.	
10 Mbit/s FDX	Erzwingt den 10-Mbps-Vollduplex-Modus für den CU-Port.	
100 Mbit/s HDX	Erzwingt den Halbduplex-Modus mit 100 Mbit/s am CU-Port.	
100 Mbit/s FDX	Erzwingt den 100-Mbps-Vollduplex-Modus für den CU-Port.	
1 Gbit/s FDX	Erzwingt den 1-Gbit/s-Vollduplex-Modus für den Port.	
2,5 Gbit/s FDX	Erzwingt den Serdes-Port im 2,5-Gbit/s-Vollduplex-Modus.	
5 Gbit/s FDX	Erzwingt den 5-Gbit/s-Vollduplex-Modus für den SerDes-Port.	
10 Gbit/s FDX	Erzwingt den 10-Gbit/s-Vollduplex-Modus für den SerDes-Port.	
SFP_Auto	Ermittelt automatisch die Geschwindigkeit des SFP.	

	Hinweis: Da es keine standardisierte Methode zur automatischen Erkennung von SFPs gibt, erfolgt diese hier durch Auslesen des SFP-ROMs. Aufgrund des Fehlens einer standardisierten Methode zur automatischen SFP-Erkennung können einige SFPs möglicherweise nicht erkannt werden.	
100-FX	SFP-Port mit 100-FX-Geschwindigkeit.	
1000-X	SFP-Port mit 1000-X-Geschwindigkeit.	

Duplex-Einstellung
Wenn „Duplex“ auf „Auto“ (d. h. automatische Aushandlung) eingestellt ist, gibt der Port dem Verbindungspartner nur den angegebenen Duplex-Modus als **Fdx** oder **Hdx** bekannt. Standardmäßig gibt der Port alle unterstützten Duplex-Modi bekannt, wenn „Duplex“ auf „Auto“ eingestellt ist.

Geschwindigkeit anzeigen
Wenn die Geschwindigkeit auf „Auto“ (d. h. automatische Aushandlung) eingestellt ist, gibt der Port nur die angegebenen Geschwindigkeiten (**10 M, 100 M, 1 G, 2,5 G, 5 G, 10 G**) an den Verbindungspartner weiter. Standardmäßig gibt der Port alle unterstützten Geschwindigkeiten an, wenn die Geschwindigkeit auf „Auto“ eingestellt ist.

Flusskontrolle
Wenn für einen Port **„Auto Speed“** ausgewählt ist, gibt dieser Abschnitt die Flusssteuerungsfähigkeit an, die dem Verbindungspartner mitgeteilt wird.
Wenn eine feste Geschwindigkeitseinstellung ausgewählt ist, wird diese verwendet. Die Spalte „Aktuelle Rx“ gibt an, ob Pausenframes am Port beachtet werden, und die Spalte „Aktuelle Tx“ gibt an, ob Pausenframes am Port gesendet werden. Die Rx- und Tx-Einstellungen werden durch das Ergebnis der letzten automatischen Aushandlung bestimmt.
Aktivieren Sie die Spalte „Konfiguriert“, um die Flusskontrolle zu verwenden. Diese Einstellung hängt mit der Einstellung für die „Konfigurierte Verbindungsgeschwindigkeit“ zusammen.

HINWEIS	Der 100FX-Standard unterstützt keine automatische Aushandlung (Auto Negotiation), daher werden die Flusssteuerungsfunktionen im 100FX-Modus immer als deaktiviert angezeigt.

Maximale Frame-Größe

Einstellung	Beschreibung	Werkseinstellung
1518–9600	Geben Sie die maximal zulässige Frame-Größe für den Switch-Port ein, einschließlich FCS. Der Bereich liegt zwischen 1518 und 9600 Byte.	9600

Modus bei übermäßigen Kollisionen
Konfigurieren Sie das Verhalten des Ports bei Übertragungskollisionen.

Einstellung	Beschreibung	Werkseinstellung
Verwerfen	Frame nach 16 Kollisionen verwerfen.	Verwerfen
Neustart	Backoff-Algorithmus nach 16 Kollisionen neu starten.	

Rahmenlängenprüfung

Legt fest, ob Frames mit falscher Frame-Länge im Feld „EtherType/Length“ verworfen werden sollen. Ein Ethernet-Frame enthält ein Feld „EtherType“, das zur Angabe der Nutzdatengröße (in Byte) des Frames für Werte von 1535 und darunter verwendet werden kann. Liegt der Wert im Feld „EtherType/Length“ über 1535, bedeutet dies, dass das Feld als EtherType verwendet wird (zur Angabe, welches Protokoll in den Nutzdaten des Frames gekapselt ist).

Einstellung	Beschreibung	Werkseinstellung
Aktiviert	Frames mit einer Nutzdatengröße von weniger als 1536 Byte werden verworfen, wenn das Feld „EtherType/Length“ nicht mit der tatsächlichen Nutzdatenlänge übereinstimmt.	Nicht markiert
Nicht markiert	Frames werden nicht aufgrund einer Nichtübereinstimmung der Frame-Länge verworfen.	

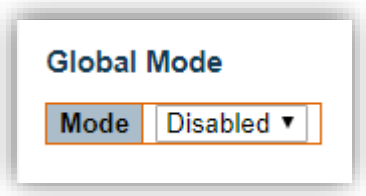
HINWEIS	Es gibt keine Verwerfungszähler, die Frames zählen, die aufgrund einer nicht übereinstimmenden Frame-Länge verworfen werden.

Konfiguration > DHCP > Server > Modus

Konfiguration des DHCP-Server-Modus

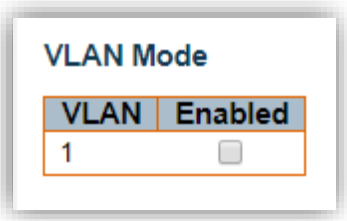
Auf dieser Seite werden der globale Modus und der VLAN-Modus konfiguriert, um den DHCP-Server pro System und pro VLAN zu aktivieren bzw. zu deaktivieren.

Globaler Modus



Einstellung	Beschreibung	Werkseinstellung
Aktiviert	DHCP-Server pro System aktivieren.	Deaktiviert
Deaktiviert	DHCP-Server pro System deaktivieren.	

VLAN-Modus



Modus

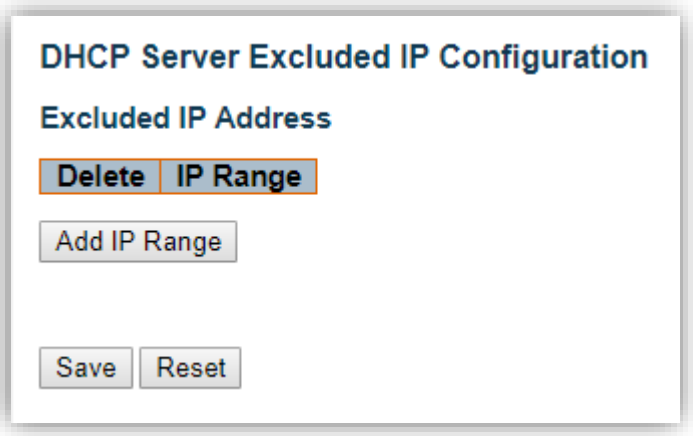
Einstellung	Beschreibung	Werkseinstellung
Aktiviert	DHCP-Server pro VLAN n aktivieren.	Nicht markiert
Nicht markiert	DHCP-Server pro VLAN n deaktivieren.	

Konfiguration > DHCP > Server > Ausgeschlossene IP-Adressen

Konfiguration der ausgeschlossenen IP-Adressen für den DHCP-Server

Auf dieser Seite werden ausgeschlossene IP-Adressen konfiguriert. Der DHCP-Server weist diese ausgeschlossenen IP-Adressen keinen DHCP-Clients zu.

Ausgeschlossene IP-Adresse



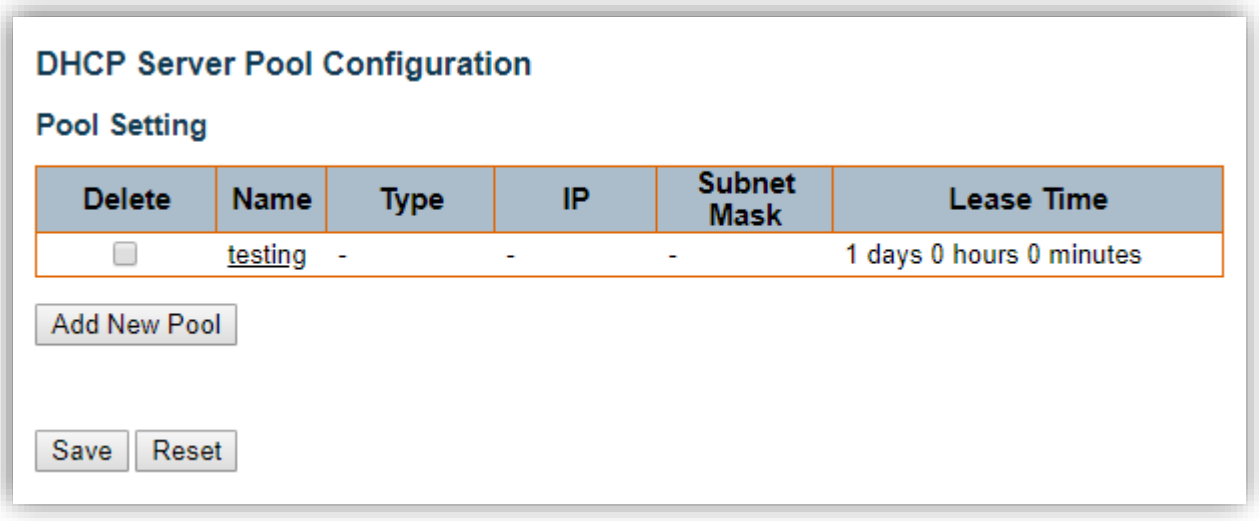
IP-Bereich

Legen Sie den IP-Bereich fest, der als ausgeschlossene IP-Adressen gelten soll. Die erste ausgeschlossene IP-Adresse muss kleiner oder gleich der zweiten ausgeschlossenen IP-Adresse sein. Wenn der IP-Bereich jedoch nur eine einzige ausgeschlossene IP-Adresse enthält, können Sie diese entweder als erste oder als zweite ausgeschlossene IP-Adresse oder als beides eingeben.

Konfiguration > DHCP > Server > Pool

Konfiguration des DHCP-Server-Pools

Auf dieser Seite werden DHCP-Pools verwaltet. Entsprechend dem DHCP-Pool weist der DHCP-Server dem DHCP-Client eine IP-Adresse zu und übermittelt ihm Konfigurationsparameter.



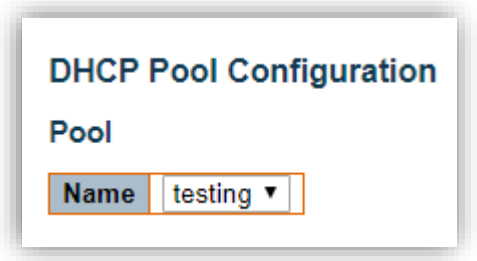
Pool-Einstellungen

Durch das Hinzufügen eines Pools und die Vergabe eines Namens wird ein neuer Pool mit „Standard“-Konfiguration erstellt. Wenn Sie alle Einstellungen einschließlich Typ, IP-Subnetzmaske und Lease-Dauer konfigurieren möchten, können Sie auf den Poolnamen klicken, um zur Konfigurationsseite zu gelangen.

Einstellungen	Beschreibung
Name	Legen Sie den Poolnamen fest, der alle druckbaren Zeichen außer Leerzeichen zulässt. Wenn Sie die detaillierten Einstellungen konfigurieren möchten, klicken Sie auf den Poolnamen, um zur Konfigurationsseite zu gelangen.
Typ	Gibt an, um welchen Pooltyp es sich handelt. **Netzwerk:** Der Pool definiert einen Pool von IP-Adressen, um mehr als einen DHCP-Client zu bedienen. **Host:** Der Pool dient einem bestimmten DHCP-Client, der durch eine Client-ID oder eine Hardware-Adresse identifiziert wird. Wenn „-“ angezeigt wird, bedeutet dies, dass der Pool nicht definiert ist.
IP	Zeigt die Netzwerknummer des DHCP-Adresspools an. Wenn „-“ angezeigt wird, bedeutet dies, dass sie nicht definiert ist.
Subnetzmaske	Zeigt die Subnetzmaske des DHCP-Adresspools an. Wird „-“ angezeigt, ist sie nicht definiert.
Lease-Zeit	Zeigt die Lease-Zeit des Pools an.

Konfigurationsseite „Pool-Einstellungen“

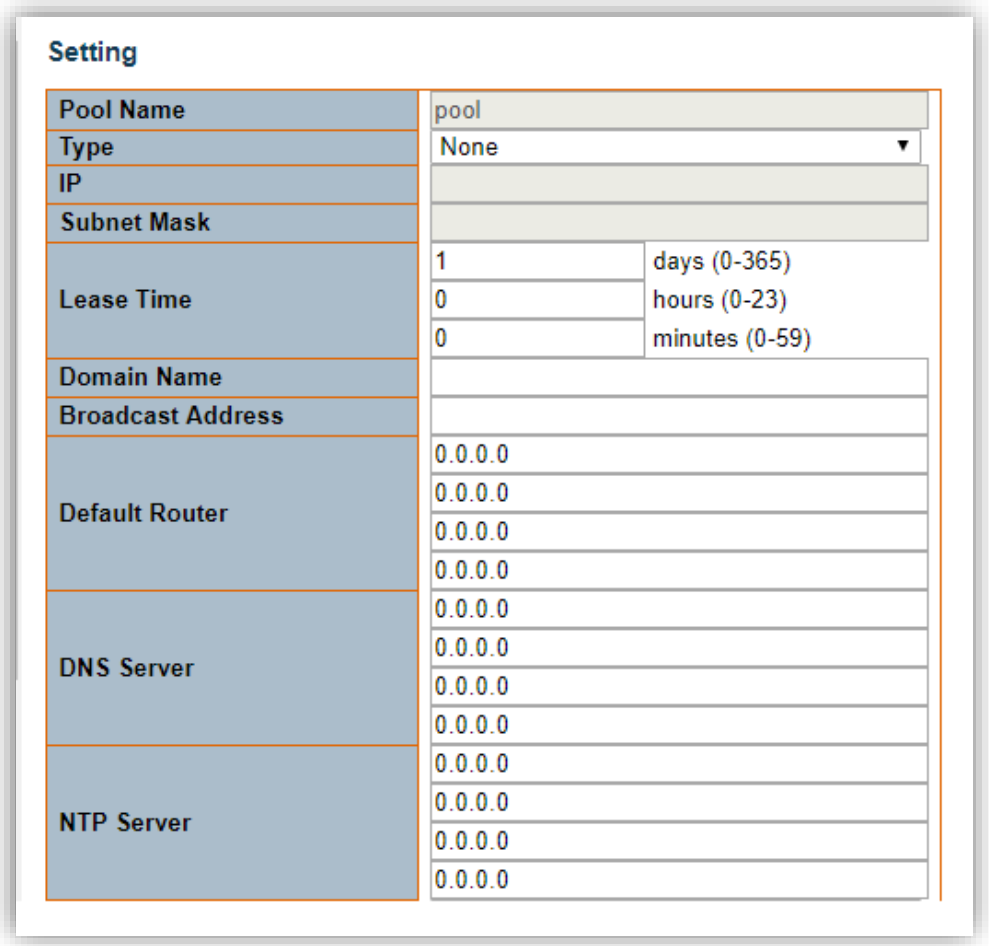
Pool

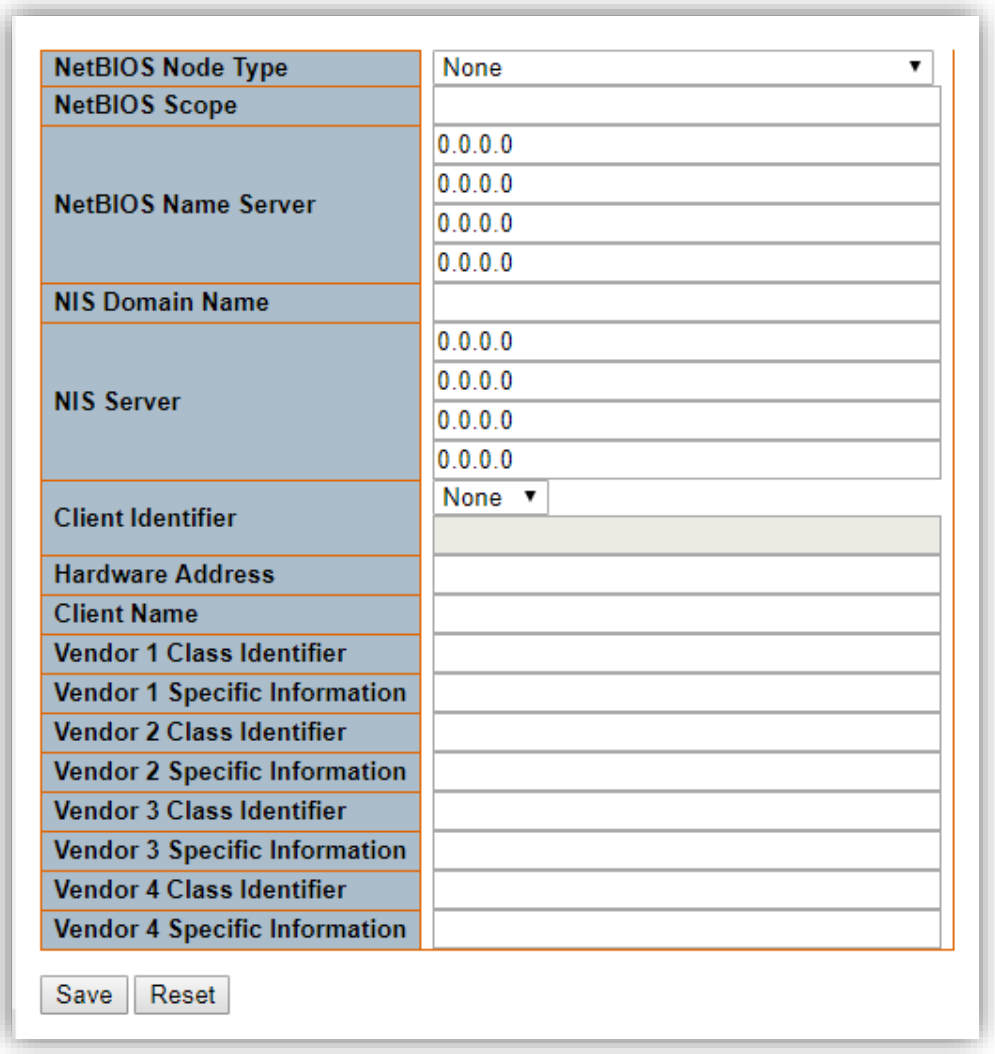


Pool

Einstellungen	Beschreibung
Name	Wählen Sie einen Pool anhand des Poolnamens aus.

Einstellung



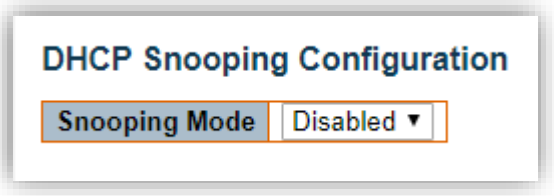


Einstellung	Beschreibung
Name	Zeigt den Namen des ausgewählten Pools an.
Typ	Geben Sie an, um welchen Pooltyp es sich handelt. **Netzwerk:** Der Pool definiert einen Pool von IP-Adressen, um mehr als einen DHCP-Client zu bedienen. **Host:** Der Pool dient einem bestimmten DHCP-Client, der durch eine Client-ID oder eine Hardware-Adresse identifiziert wird.
IP	Geben Sie die Netzwerknummer des DHCP-Adresspools an.
Subnetzmaske	Geben Sie die Subnetzmaske des DHCP-Adresspools an.
Lease-Zeit	Geben Sie die Lease-Zeit an, die es dem Client ermöglicht, eine Lease-Zeit für die IP-Adresse anzufordern. Sind alle Werte 0, bedeutet dies, dass die Lease-Zeit unbegrenzt ist.
Domänenname	Geben Sie den Domänennamen an, den der Client bei der Auflösung des Hostnamens über DNS verwenden soll.
Broadcast-Adresse	Geben Sie die im Subnetz des Clients verwendete Broadcast-Adresse an.
Standard-Router	Geben Sie eine Liste von IP-Adressen für Router im Subnetz des Clients an.
DNS-Server	Geben Sie eine Liste der für den Client verfügbaren DNS-Nameserver an.
NTP-Server	Geben Sie eine Liste von IP-Adressen an, die die für den Client verfügbaren NTP-Server bezeichnen.

NetBIOS-Knotentyp	Geben Sie die Option „NetBIOS-Knotentyp“ an, um NetBIOS-über-TCP/IP-Clients zuzulassen, die gemäß den Angaben in RFC 1001/1002 konfiguriert werden können.
NetBIOS-Gültigkeitsbereich	Geben Sie den Parameter „NetBIOS-Gültigkeitsbereich über TCP/IP“ für den Client gemäß RFC 1001/1002 an.
NetBIOS-Namensserver	Geben Sie eine Liste von NBNS-Namensservern in der Reihenfolge ihrer Präferenz an.
NIS-Domänenname	Geben Sie den Namen der NIS-Domäne des Clients an.
NIS-Server	Geben Sie eine Liste von IP-Adressen an, die die für den Client verfügbaren NIS-Server bezeichnen.
Client-Kennung	Geben Sie die eindeutige Kennung des Clients an, die verwendet werden soll, wenn es sich bei dem Pool um einen Host handelt.
Hardware-Adresse	Geben Sie die Hardware-Adresse (MAC-Adresse) des Clients an, die verwendet werden soll, wenn der Pool vom Typ „Host“ ist.
Client-Name	Geben Sie den Namen des Clients an, der verwendet werden soll, wenn der Pool vom Typ „Host“ ist.
Hersteller-Klassenkennung	Geben Sie an, ob der DHCP-Client optional den Herstellertyp und die Konfiguration eines DHCP-Clients identifizieren soll. Der DHCP-Server übermittelt dem Client, der die Option 60 „Herstellerklassenkennung“ sendet, die entsprechenden spezifischen Informationen der Option 43.
Hersteller-spezifische Informationen	Geben Sie herstellerspezifische Informationen entsprechend der Option 60 „Herstellerklassenkennung“ an.

Konfiguration > DHCP > Snooping

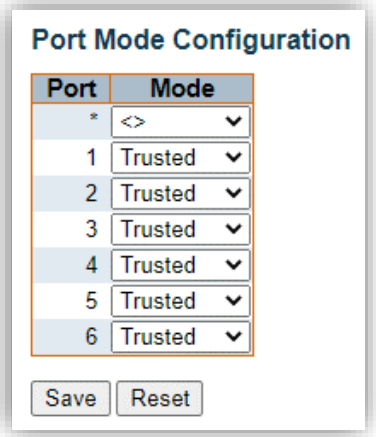
DHCP-Snooping-Konfiguration



Snooping-Modus

Einstellung	Beschreibung	Werkseinstellung
Aktiviert	Aktiviert den DHCP-Snooping-Modus. Wenn der DHCP-Snooping-Modus aktiviert ist, werden DHCP-Anfragen an vertrauenswürdige Ports weitergeleitet, und es werden nur Antwortpakete von vertrauenswürdigen Ports zugelassen.	Deaktiviert
Deaktiviert	Deaktivieren Sie den DHCP-Snooping-Modus.	

Konfiguration des Port-Modus

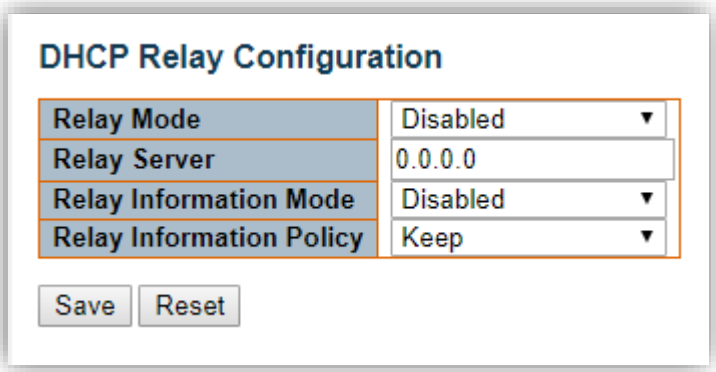


Einstellung	Beschreibung	Werkseinstellung
Vertrauenswürdig	Konfiguriert den Port als vertrauenswürdige Quelle für DHCP-Nachrichten.	Vertrauenswürdig
Nicht vertrauenswürdig	Konfiguriert den Port als nicht vertrauenswürdige Quelle für die DHCP-Nachrichten.	

Konfiguration > DHCP > Relay

DHCP-Relay-Konfiguration

Ein DHCP-Relay-Agent wird verwendet, um DHCP-Nachrichten zwischen den Clients und dem Server weiterzuleiten und zu übertragen, wenn diese sich nicht in derselben Subnetzdomäne befinden. Er speichert die IP-Adresse der eingehenden Schnittstelle im GIADDR-Feld des DHCP-Pakets. Der DHCP-Server kann anhand des Werts im GIADDR-Feld das zugewiesene Subnetz ermitteln. Stellen Sie in einem solchen Fall bitte sicher, dass die Switch-Konfiguration der VLAN-Schnittstellen-IP-Adresse und der PVID (Port-VLAN-ID) korrekt ist.



Relay-Modus

Einstellung	Beschreibung	Werkseinstellung
Aktiv	Aktivieren Sie den DHCP-Relay-Modus. Wenn der DHCP-Relay-Modus aktiviert ist, leitet der Agent DHCP-Nachrichten zwischen den Clients und dem Server weiter, wenn diese sich nicht in derselben Subnetzdomäne befinden. Aus Sicherheitsgründen wird die DHCP-Broadcast-Nachricht nicht weitergeleitet.	Deaktiviert
Deaktiviert	Deaktivieren Sie den DHCP-Relay-Modus.	

Relay-Server

Einstellung	Beschreibung
IP-Adresse.	Gibt die IP-Adresse des DHCP-Relay-Servers an.

Relay-Informationsmodus

Gibt den Betriebsmodus der DHCP-Relay-Informationsoption an. Das Format der Option 82 „Circuit ID“ lautet „[vlan_id][module_id][port_no]“. Die ersten vier Zeichen stehen für die VLAN-ID, das fünfte und sechste Zeichen sind die Modul-ID (bei eigenständigen Geräten ist diese immer gleich 0, bei stapelbaren Geräten entspricht sie der Switch-ID) und die letzten beiden Zeichen sind die Portnummer. Beispielsweise bedeutet „00030108“, dass die DHCP-Nachricht von VLAN-ID 3, Switch-ID 1 und Port-Nr. 8 empfangen wurde. Der Wert der Remote-ID der Option 82 entspricht der MAC-Adresse des Switches.

Einstellung	Beschreibung	Werkseinstellung
Aktiviert	Aktiviert den Betrieb im DHCP-Relay-Informationsmodus. Wenn der Betrieb im DHCP-Relay-Informationsmodus aktiviert ist, fügt der Agent bei der Weiterleitung an den DHCP-Server bestimmte Informationen (Option 82) in eine DHCP-Nachricht ein und entfernt diese bei der Weiterleitung an den DHCP-Client wieder aus der DHCP-Nachricht. Dies funktioniert nur, wenn der DHCP-Relay-Betriebsmodus aktiviert ist.	Deaktiviert
Deaktiviert	Deaktivieren Sie den DHCP-Relay-Informationsmodus.	

Richtlinie für Relay-Informationen

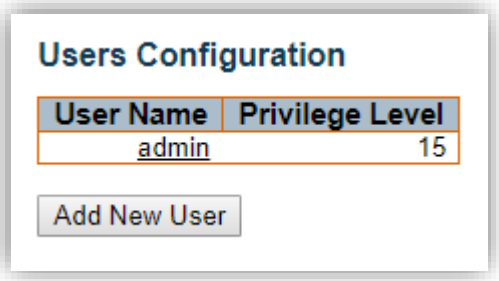
Gibt die Richtlinie für die DHCP-Relay-Informationen an. Wenn der DHCP-Relay-Informationsmodus aktiviert ist und der Agent eine DHCP-Nachricht empfängt, die bereits Relay-Agent-Informationen enthält, wendet er die Richtlinie an. Die Richtlinie „Ersetzen“ ist ungültig, wenn der Relay-Informationsmodus deaktiviert ist.

Einstellung	Beschreibung	Werkseinstellung
Ersetzen	Die ursprünglichen Relay-Informationen werden ersetzt, wenn eine DHCP-Nachricht empfangen wird, die diese bereits enthält.	Beibehalten
Beibehalten	Behalten Sie die ursprünglichen Weiterleitungsinformationen bei, wenn eine DHCP-Nachricht empfangen wird, die diese bereits enthält.	
Verwerfen	Verwerfen Sie das Paket, wenn eine DHCP-Nachricht empfangen wird, die bereits Weiterleitungsinformationen enthält.	

Konfiguration > Sicherheit > Switch > Benutzer

Diese Seite bietet einen Überblick über die aktuellen Benutzer. Derzeit besteht die einzige Möglichkeit, sich auf dem Webserver als anderer Benutzer anzumelden, darin, den Browser zu schließen und erneut zu öffnen.

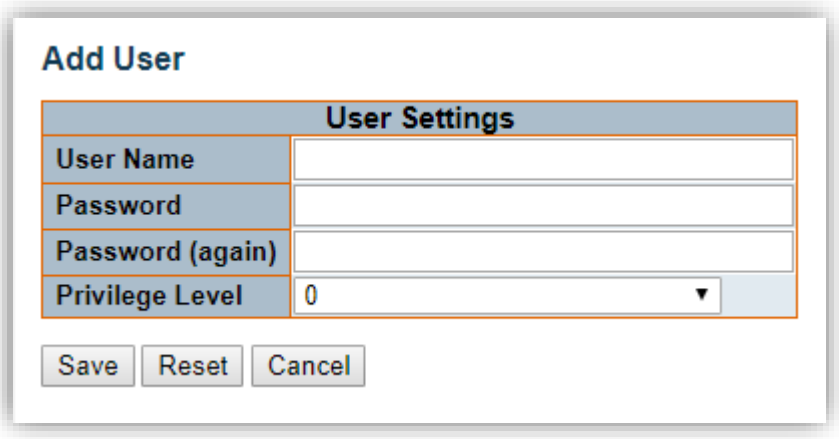
Benutzerkonfiguration



Einstellung	Beschreibung	Werkseinstellung
Benutzername	Der Name, der den Benutzer identifiziert.	Keine
Berechtigungsstufe 0–15	Die Berechtigungsstufe des Benutzers. Der zulässige Bereich liegt zwischen 0 und 15. Bei einer Berechtigungsstufe von 15 hat der Benutzer Zugriff auf alle Gruppen, d. h., ihm wird die vollständige Kontrolle über das Gerät gewährt. Andere Werte müssen sich hingegen auf die jeweilige Gruppenberechtigungsstufe beziehen. Die Berechtigungsstufe des Benutzers muss mindestens der Gruppenberechtigungsstufe entsprechen, um Zugriff auf diese Gruppe zu erhalten. Standardmäßig verfügt die Berechtigungsstufe 5 der meisten Gruppen über Lesezugriff und die Berechtigungsstufe 10 über Lese- und Schreibzugriff. Für die Systemwartung (Software-Upload, Zurücksetzen auf Werkseinstellungen usw.) ist die Benutzerberechtigungsstufe 15 erforderlich. Im Allgemeinen kann die Berechtigungsstufe 15 für ein Administratorkonto, die Berechtigungsstufe 10 für ein Standardbenutzerkonto und die Berechtigungsstufe 5 für ein Gastkonto verwendet werden.	0

Benutzer hinzufügen/bearbeiten

Klicken Sie auf die Schaltfläche **„Neuen Benutzer hinzufügen“**, um einen neuen Benutzer hinzuzufügen. Sie können auch auf „Benutzername“ klicken, um einen Benutzer zu bearbeiten.



Benutzername

Einstellung	Beschreibung	Werkseinstellung
Max. 31 Zeichen	Eine Zeichenfolge, die den Benutzernamen angibt, zu dem dieser Eintrag gehören soll. Die zulässige Zeichenfolge hat eine Länge **von 1 bis 31**. Der gültige Benutzername darf Buchstaben, Zahlen und Unterstriche enthalten.	Keine

Passwort

Einstellung	Beschreibung	Werkseinstellung
Max. 31 Zeichen	Das Passwort des Benutzers. Die zulässige Zeichenlänge liegt **zwischen 0 und 31**. Alle druckbaren Zeichen einschließlich Leerzeichen sind zulässig.	Keine

Berechtigungsstufe

Einstellung	Beschreibung	Werkseinstellung
0–15	Die Berechtigungsstufe des Benutzers. Der zulässige Bereich liegt **zwischen 0 und 15**. Bei einer Berechtigungsstufe von 15 hat der Benutzer Zugriff auf alle Gruppen, d. h., ihm wird die vollständige Kontrolle über das Gerät gewährt. Andere Werte müssen sich hingegen auf die jeweilige Gruppenberechtigungsstufe beziehen. Die Berechtigungsstufe des Benutzers muss mindestens der Gruppenberechtigungsstufe entsprechen, damit er Zugriff auf diese Gruppe erhält. Standardmäßig verfügt die Berechtigungsstufe 5 der meisten Gruppen über Lesezugriff, während die Berechtigungsstufe 10 Lese- und Schreibzugriff gewährt. Für die Systemwartung (Software-Upload, Zurücksetzen auf Werkseinstellungen usw.) ist die Benutzerberechtigungsstufe 15 erforderlich. Im Allgemeinen kann die Berechtigungsstufe 15 für ein Administratorkonto, die	0

	Berechtigungsstufe 10 für ein Standardbenutzerkonto und die Berechtigungsstufe 5 für ein Gastkonto verwendet werden.	

Konfiguration > Sicherheit > Switch > Berechtigungsstufen

Konfiguration der Berechtigungsstufen

Privilege Level Configuration

Group Name	Privilege Levels			
	Configuration Read-only	Configuration/Execute Read/write	Status/Statistics Read-only	Status/Statistics Read/write
Aggregation	5	10	5	10
Alarm	5	10	5	10
DDMI	5	10	5	10
DHCP	5	10	5	10
DHCPv6_Client	5	10	5	10
Diagnostics	5	10	5	10
Discovery	5	10	5	10
ERPS	5	10	5	10
EventWarning	5	10	5	10
Firmware	5	10	5	10
FRR	5	10	5	10
Green_Ethernet	5	10	5	10
IP	5	10	5	10
IPMC_LIB	5	10	5	10
IPMC_Snooping	5	10	5	10
LACP	5	10	5	10
LLDP	5	10	5	10
Loop_Protect	5	10	5	10
MAC_Table	5	10	5	10
MEP	5	10	5	10
Miscellaneous	15	15	15	15
Modbus	5	10	5	10
MRP	5	10	5	10
MVR	5	10	5	10
NTP	5	10	5	10
POE	5	10	5	10
Ports	5	10	1	10
Private_VLANs	5	10	5	10
QoS	5	10	5	10
RMirror	5	10	5	10
RMON	5	10	5	10
Security(access)	10	10	5	10
Security(network)	5	10	5	10
sFlow	5	10	5	10
SNMP	5	10	5	10
Spanning_Tree	5	10	5	10
System	5	10	1	10
Traceroute	5	10	5	10
uFDMA_AIL	5	10	5	10
uFDMA_CIL	5	10	5	10
VCL	5	10	5	10
VLANs	5	10	5	10
XXRP	5	10	5	10

Save Reset

Gruppenname
Der Name, der die Berechtigungsgruppe identifiziert. In den meisten Fällen besteht eine Berechtigungsgruppenebene aus einem einzelnen Modul (z. B. LACP, RSTP oder QoS), einige wenige enthalten jedoch mehr als eines. Die folgende Beschreibung definiert diese Berechtigungsgruppen im Detail:

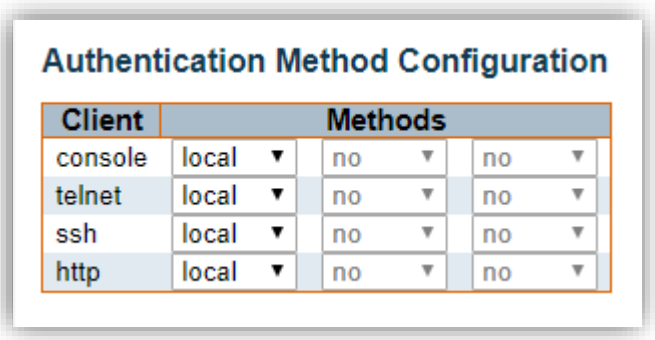
- **System:** Kontakt, Name, Standort, Zeitzone, Sommerzeit, Protokollierung.
- **Sicherheit:** Authentifizierung, Systemzugriffsverwaltung, Port (umfasst Dot1x-Port, MAC-basiert und MAC-Adressbegrenzung), ACL, HTTPS, SSH, ARP-Prüfung, IP-Quellschutz.
- **IP:** Alles außer Ping.
- **Port:** Alles außer VeriPHY.
- **Diagnose:** Ping und VeriPHY.
- **Wartung:** CLI – System-Neustart, System auf Standard zurücksetzen, Systemkennwort, Konfiguration speichern, Konfiguration laden und Firmware laden. Web – Benutzer, Berechtigungsstufen und alle Funktionen unter „ -Wartung“.
- **Debug:** Nur in der CLI verfügbar.

Berechtigungsstufen
Die Berechtigungsstufen können zwischen **0** und **15** konfiguriert werden (wobei 0 die niedrigste und 15 die höchste Stufe ist). Jede Gruppe verfügt über eine Berechtigungsstufe für die folgenden Untergruppen: Konfiguration (nur Lesen), Konfiguration/Ausführung (Lesen/Schreiben), Status/Statistiken (nur Lesen), Status/Statistiken (Lesen/Schreiben) (z. B. zum Löschen von Statistiken). Die Benutzerberechtigung muss mindestens der Berechtigungsstufe der Gruppe entsprechen, um Zugriff auf diese Gruppe zu erhalten.

Konfiguration > Sicherheit > Switch > Authentifizierungsmethode

Konfiguration der Authentifizierungsmethode

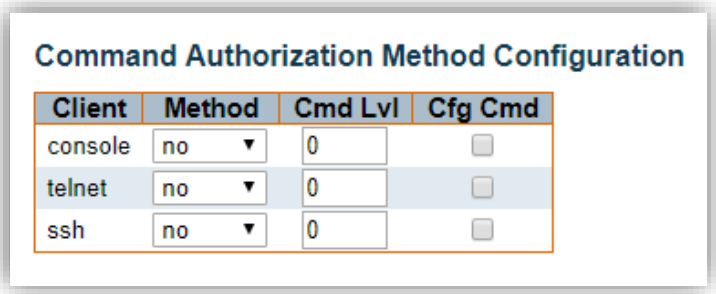
Im Abschnitt „Authentifizierung“ können Sie konfigurieren, wie ein Benutzer authentifiziert wird, wenn er sich über eine der Management-Client-Schnittstellen beim Switch anmeldet.



Einstellung	Beschreibung
Client	Der Management-Client, für den die folgende Konfiguration gilt.
Methoden	Die Methode kann auf einen der folgenden Werte gesetzt werden: • **no:** Die Authentifizierung ist deaktiviert und eine Anmeldung ist nicht möglich. • **local:** Zur Authentifizierung wird die lokale Benutzerdatenbank auf dem Switch verwendet. • **radius:** Verwenden Sie einen oder mehrere Remote-RADIUS-Server zur Authentifizierung. • **tacacs:** Es werden Remote-TACACS+-Server zur Authentifizierung verwendet. Methoden, die Remote-Server beinhalten, werden abgebrochen, wenn die Remote-Server offline sind. In diesem Fall wird die nächste Methode ausprobiert. Jede Methode wird von links nach rechts ausprobiert, bis eine Methode einen Benutzer entweder akzeptiert oder ablehnt. Wenn ein Remote-Server für die primäre Authentifizierung verwendet wird, wird empfohlen, die sekundäre Authentifizierung auf „local“ zu konfigurieren. Dadurch kann sich der Management-Client über die lokale Benutzerdatenbank anmelden, falls keiner der konfigurierten Authentifizierungsserver erreichbar ist.

Konfiguration der Befehlsautorisierung

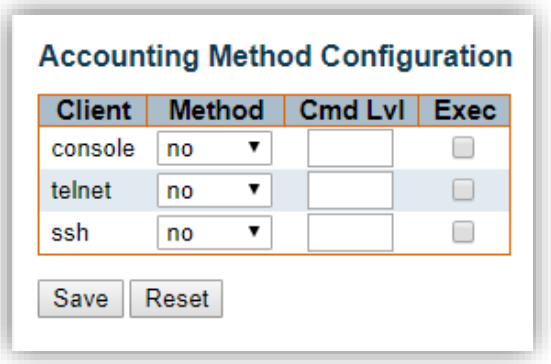
Im Abschnitt „Befehlsautorisierung“ können Sie die für einen Benutzer verfügbaren CLI-Befehle einschränken.



Einstellung	Beschreibung
Client	Der Management-Client, für den die folgende Konfiguration gilt.
Methoden	Die Methode kann auf einen der folgenden Werte gesetzt werden: • **no:** Die Befehlsautorisierung ist deaktiviert. Dem Benutzer wird entsprechend seiner Berechtigungsstufe Zugriff auf CLI-Befehle gewährt. • **tacacs:** Es werden Remote-TACACS+-Server für die Befehlsautorisierung verwendet. Sind alle Remote-Server offline, erhält der Benutzer Zugriff auf CLI-Befehle entsprechend seiner Berechtigungsstufe.
Cmd Lvl (0–15)	Autorisiert alle Befehle mit einer Berechtigungsstufe, die höher oder gleich dieser Stufe ist. Gültige Werte liegen im Bereich von 0 bis 15.
Cfg Cmd	Autorisiert zusätzlich Konfigurationsbefehle.

Konfiguration der Protokollierungsmethode

Im Abschnitt „Abrechnung“ können Sie die Abrechnung von Befehlen und Exec-Befehlen (Anmeldungen) konfigurieren.

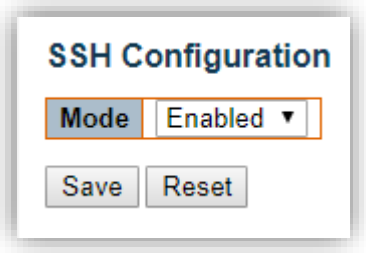


Einstellung	Beschreibung
Client	Der Management-Client, für den die folgende Konfiguration gilt.
Methoden	Die Methode kann auf einen der folgenden Werte gesetzt werden: • **no:** Die Abrechnung ist deaktiviert. • **tacacs:** Für die Abrechnung werden externe TACACS+-Server verwendet.

Befehlsebene (0–15)	Aktiviert die Protokollierung aller Befehle mit einer Berechtigungsstufe, die größer oder gleich dieser Stufe ist. Gültige Werte liegen im Bereich von 0 bis 15. Lassen Sie das Feld leer, um die Befehlsprotokollierung zu deaktivieren.
Exec	Aktivieren Sie die Protokollierung von „exec“-Befehlen (Anmeldung).

Konfiguration > Sicherheit > Switch > SSH

SSH-Konfiguration

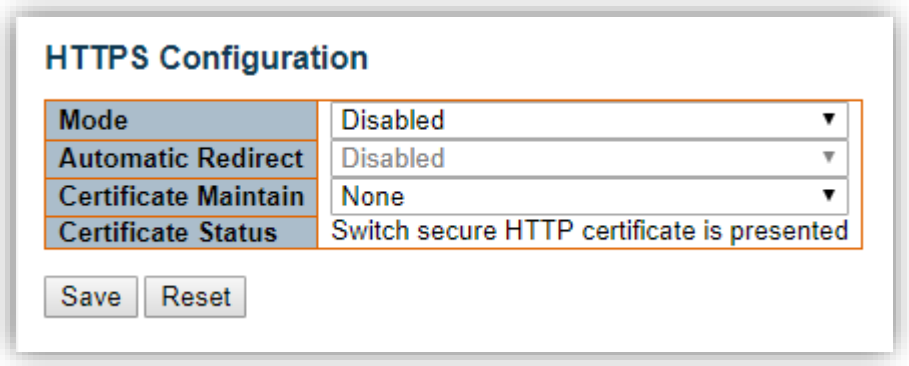


Einstellung	Beschreibung	Werkseinstellung
Aktiviert	SSH-Modus aktivieren.	Aktiviert
Deaktiviert	Deaktivieren Sie den SSH-Modus.	

Konfiguration > Sicherheit > Switch > HTTPS

HTTPS-Konfiguration

Auf dieser Seite können Sie die HTTPS-Einstellungen konfigurieren und das aktuelle Zertifikat auf dem Switch verwalten.



Modus

Einstellung	Beschreibung	Werkseinstellung
Aktiviert	HTTPS-Modus aktivieren.	Deaktiviert
Deaktiviert	Deaktivieren Sie den HTTPS-Modus.	

Automatische Weiterleitung

Gibt den HTTPS-Umleitungsmodus an. Diese Einstellung ist nur relevant, wenn „HTTPS-Modus aktiviert“ ausgewählt ist. Wenn der Umleitungsmodus aktiviert ist, wird die HTTP-Verbindung automatisch auf eine HTTPS-Verbindung umgeleitet.
Beachten Sie, dass der Browser die Umleitung aus Sicherheitsgründen möglicherweise nicht zulässt, es sei denn, das Zertifikat des Switches wird vom Browser als vertrauenswürdig eingestuft. In diesem Fall müssen Sie die HTTPS-Verbindung manuell herstellen.

Einstellung	Beschreibung	Werkseinstellung
Aktiviert	Aktiviert den HTTPS-Weiterleitungsmodus.	Deaktiviert
Deaktiviert	Deaktivieren Sie den Betrieb im HTTPS-Weiterleitungsmodus.	

Zertifikat verwalten

Einstellung	Beschreibung	Werkseinstellung
Keine	Keine Aktion.	Keine
Löschen	Das aktuelle Zertifikat löschen.	
Hochladen	Eine PEM-Datei eines Zertifikats hochladen. Mögliche Methoden sind: **Webbrowser** oder **URL**.	
Erstellen	Ein neues selbstsigniertes RSA-Zertifikat generieren.	

Passphrase für das Zertifikat

Einstellung	Beschreibung	Werkseinstellung
Passphrase	Geben Sie in diesem Feld die Passphrase ein, falls Ihr hochgeladenes Zertifikat durch eine bestimmte Passphrase geschützt ist.	Keine

Zertifikat hochladen

Laden Sie eine PEM-Datei mit dem Zertifikat auf den Switch hoch. Die Datei sollte das Zertifikat und den privaten Schlüssel zusammen enthalten. Falls Sie zwei separate Dateien für das Zertifikat und den privaten Schlüssel haben, verwenden Sie den Linux-Befehl „cat“, um diese zu einer einzigen PEM-Datei zusammenzufügen. Beispiel: *cat my.cert my.key > my.pem*
Beachten Sie, dass ein RSA-Zertifikat empfohlen wird, da die meisten neueren Browser-Versionen die Unterstützung für DSA in Zertifikaten eingestellt haben, z. B. Firefox v37 und Chrome v39.

Einstellungen	Beschreibung	Werkseinstellung
Webbrowser	Laden Sie ein Zertifikat über den Webbrowser hoch.	Webbrowser
URL	Laden Sie ein Zertifikat über eine URL hoch. Die unterstützten Protokolle sind HTTP, HTTPS, TFTP und FTP. Das URL-Format lautet <Protokoll>://[<Benutzername>[:<Passwort>]@]<Host>[:<Port>][/<Pfad>]/<Dateiname>. Beispiel: Tftp://10.10.10.10/new_image_path/new_image.dat, http:// username:password@10.10.10.10:80/new_image_path/new_image.dat. Ein gültiger Dateiname ist eine Zeichenfolge, die aus Buchstaben (A–Za-z), Ziffern (0–9), einem Punkt (.), einem Bindestrich (-) und einem Unterstrich (_) besteht. Die maximale Länge beträgt 63 Zeichen, und der Bindestrich darf nicht das erste Zeichen sein. Dateinamen, die ausschließlich aus „.“ bestehen, sind nicht zulässig.	

Zertifikatsstatus

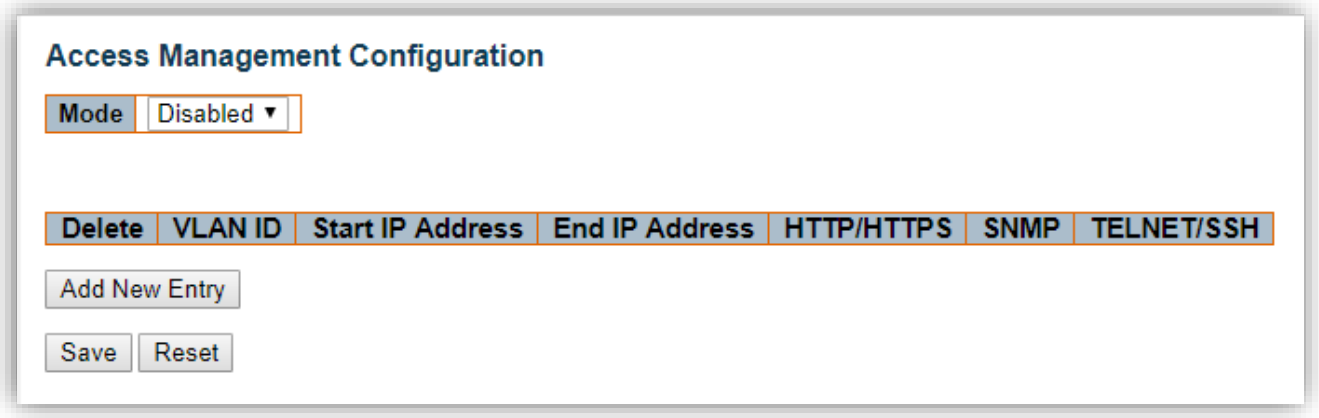
Zeigt den aktuellen Status des Zertifikats auf dem Switch an.

- Das Secure-HTTP-Zertifikat des Switches wird vorgelegt.
- Das Secure-HTTP-Zertifikat des Switches wird nicht vorgelegt.
- Das Secure-HTTP-Zertifikat des Switches wird gerade generiert.

Konfiguration > Sicherheit > Switch > Zugriffsverwaltung

Konfiguration der Zugriffsverwaltung

Konfigurieren Sie auf dieser Seite die Zugriffsverwaltungstabelle. Die maximale Anzahl an Einträgen beträgt **16**. Wenn der Anwendungstyp mit einem der Einträge in der Zugriffsverwaltung übereinstimmt, wird der Zugriff auf den Switch gewährt.



Modus

Gibt den Betriebsmodus der Zugriffsverwaltung an.

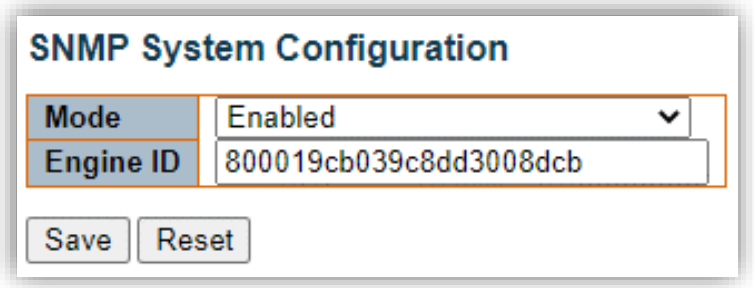
Einstellung	Beschreibung	Werkseinstellung
Aktiviert	Aktivieren Sie den Betrieb im Zugriffsverwaltungsmodus.	Deaktiviert
Deaktiviert	Deaktivieren Sie den Betrieb im Zugriffsverwaltungsmodus.	

Neuen Eintrag hinzufügen

Einstellung	Beschreibung
Löschen	Aktivieren Sie dieses Kontrollkästchen, um den Eintrag zu löschen. Er wird beim nächsten Speichern gelöscht.
VLAN-ID	Gibt die VLAN-ID für den Eintrag in der Zugriffsverwaltung an.
Start-IP-Adresse	Gibt die Start-IP-Adresse für den Zugriffsverwaltungseintrag an.
End-IP-Adresse	Gibt die End-IP-Adresse für den Zugriffsverwaltungseintrag an.
HTTP/HTTPS	Gibt an, dass der Host über die HTTP/HTTPS-Schnittstelle auf den Switch zugreifen kann, sofern die IP-Adresse des Hosts mit dem im Eintrag angegebenen IP-Adressbereich übereinstimmt.
SNMP	Gibt an, dass der Host über die SNMP-Schnittstelle auf den Switch zugreifen kann, sofern die IP-Adresse des Hosts mit dem im Eintrag angegebenen IP-Adressbereich übereinstimmt.
TELNET/SSH	Gibt an, dass der Host über die TELNET/SSH-Schnittstelle auf den Switch zugreifen kann, sofern die IP-Adresse des Hosts mit dem im Eintrag angegebenen IP-Adressbereich übereinstimmt.

Konfiguration > Sicherheit > Switch > SNMP > System

SNMP-Systemkonfiguration



Modus

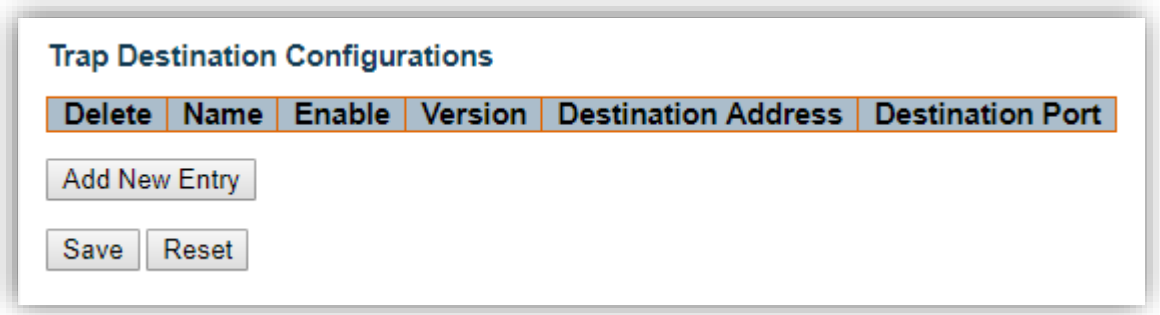
Einstellung	Beschreibung	Werkseinstellung
Aktiviert	Aktiviert den Betrieb im SNMP-Modus.	Aktiviert
Deaktiviert	Deaktivieren Sie den SNMP-Modus.	

Engine-ID
Gibt die SNMPv3-Engine-ID an. Die Zeichenfolge muss eine gerade Zahl (im Hexadezimalformat) mit einer Ziffernanzahl zwischen 10 und 64 enthalten, wobei jedoch weder eine Folge aus ausschließlich Nullen noch aus ausschließlich „F“ zulässig ist. Nur Benutzer mit dieser Engine-ID können auf das Gerät zugreifen (lokale Benutzer); daher wird durch das Ändern der Engine-ID der Zugriff für alle aktuellen lokalen Benutzer widerrufen.

Konfiguration > Sicherheit > Switch > SNMP > Trap

Trap-Konfiguration

Konfigurationen für Trap-Empfänger



Name
Gibt den Namen der Trap-Konfiguration an. Gibt den Namen des Trap-Empfängers an.

Aktivieren
Gibt den Betriebsmodus des Trap-Ziels an.

Einstellung	Beschreibung	Werkseinstellung
Aktiviert	Aktiviert den SNMP-Trap-Modus.	Deaktiviert
Deaktiviert	Deaktivieren Sie den SNMP-Trap-Modus.	

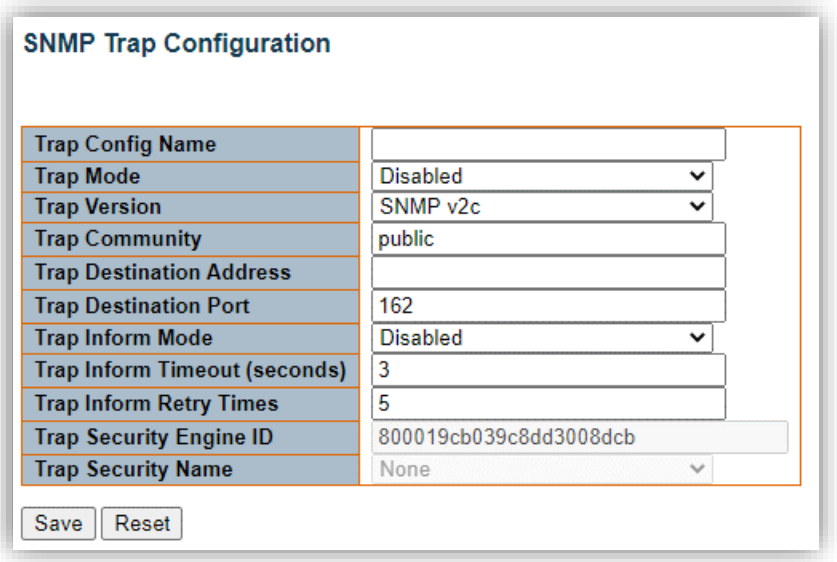
Version

Einstellung	Beschreibung	Werkseinstellung
SNMP v1	Stellt die unterstützte SNMP-Version 1 ein.	SNMP v2c
SNMP v2c	Stellen Sie die unterstützte SNMP-Version 2c ein.	
SNMP v3	Stellen Sie die unterstützte SNMP-Version auf 3 ein.	

Zieladresse
Gibt die Zieladresse für SNMP-Traps an. Es ist eine gültige IP-Adresse in Dezimalschreibweise mit Punkten („x.y.z.w“) zulässig. Außerdem ist ein gültiger Hostname zulässig. Ein gültiger Hostname ist eine Zeichenfolge, die aus Buchstaben (A–Za–z), Ziffern (0–9), einem Punkt (.) und einem Bindestrich (-) besteht. Leerzeichen sind nicht zulässig, das erste Zeichen muss ein Buchstabe sein, und das erste sowie das letzte Zeichen dürfen kein Punkt oder Bindestrich sein.
Gibt die IPv6-Zieladresse für SNMP-Traps an. Eine IPv6-Adresse besteht aus 128-Bit-Einträgen, die als acht Felder mit jeweils bis zu vier Hexadezimalziffern dargestellt werden, wobei die Felder durch einen Doppelpunkt (:) voneinander getrennt sind. Beispiel: **fe80::215:c5ff:fe03:4dc7**. Das Symbol :: ist eine spezielle Syntax, die als Kurzform für
mehrere 16-Bit-Gruppen aufeinanderfolgender Nullen darzustellen; es darf jedoch nur einmal vorkommen. Es kann auch eine gültige IPv4-Adresse darstellen. Zum Beispiel: **::192.1.2.34**.

Zielport
Gibt den Zielport für SNMP-Traps an. Der SNMP-Agent sendet SNMP-Nachrichten über diesen Port; der Portbereich liegt zwischen 1 und 65535.

SNMP-Trap-Konfiguration



Name der Trap-Konfiguration

Einstellung	Beschreibung	Werkseinstellung
1–32 Zeichen	Gibt den Namen der Trap-Konfiguration an, die konfiguriert werden soll. Die zulässige Zeichenfolgenlänge beträgt 1 bis 32, und der zulässige Inhalt besteht aus ASCII-Zeichen von 33 bis 126.	Keine

Trap-Modus

Einstellung	Beschreibung	Werkseinstellung
Aktiviert	Aktiviert den SNMP-Trap-Modus.	Deaktiviert
Deaktiviert	Deaktivieren Sie den SNMP-Trap-Modus.	

Trap-Version

Einstellung	Beschreibung	Werkseinstellung
SNMP v1	Stellt die unterstützte SNMP-Version 1 ein.	SNMP v2c
SNMP v2c	Stellen Sie die unterstützte SNMP-Version 2c ein.	
SNMP v3	Stellen Sie die unterstützte SNMP-Version auf 3 ein.	

Trap-Community

Einstellung	Beschreibung	Werkseinstellung
0 bis 63 Zeichen	Gibt die Community-Zugriffszeichenfolge beim Senden von SNMP-Trap-Paketen an. Die zulässige Zeichenfolgenlänge beträgt 0 bis 63, und der zulässige Inhalt besteht aus ASCII-Zeichen von 33 bis 126.	Öffentlich

Trap-Zieladresse

Einstellung	Beschreibung	Werkseinstellung
IP-Adresse	Gibt die SNMP-Trap-Zieladresse an. Es wird eine gültige IP-Adresse in Dezimalschreibweise mit Punkten („x.y.z.w“) akzeptiert. Außerdem ist ein gültiger Hostname zulässig. Ein gültiger Hostname ist eine Zeichenfolge, die aus Buchstaben (A–Za-z), Ziffern (0–9), einem Punkt (.) und einem Bindestrich (-) besteht. Leerzeichen sind nicht zulässig, das erste Zeichen muss ein Buchstabe sein, und das erste sowie das letzte Zeichen dürfen kein Punkt oder Bindestrich sein. Gibt die IPv6-Adresse des SNMP-Trap-Empfängers an. Eine IPv6-Adresse besteht aus 128-Bit-Datensätzen, die als acht Felder mit jeweils bis zu vier Hexadezimalziffern dargestellt werden, wobei die Felder durch einen Doppelpunkt (:) voneinander getrennt sind. Beispiel: **fe80::215:c5ff:fe03:4dc7**. Das Symbol :: ist eine spezielle Syntax, die als Kurzform zur Darstellung mehrerer 16-Bit-Gruppen aufeinanderfolgender Nullen verwendet werden kann; es darf jedoch nur einmal vorkommen. Es kann auch eine gültige IPv4-Adresse darstellen. Zum Beispiel: ::**192.1.2.34**.	Keine

Trap-Zielport

Einstellung	Beschreibung	Werkseinstellung
1–65535	Gibt den SNMP-Trap-Zielport an. Der SNMP-Agent sendet SNMP-Nachrichten über diesen Port; der Portbereich liegt zwischen 1 und 65535.	162

Trap-Informationsmodus

Einstellung	Beschreibung	Werkseinstellung
Aktiviert	Aktiviert den Betrieb im SNMP-Trap-Inform-Modus.	Deaktiviert
Deaktiviert	Deaktivieren Sie den SNMP-Trap-Informationsmodus.	

Zeitlimit für Trap-Benachrichtigungen (Sekunden)

Einstellung	Beschreibung	Werkseinstellung
0–2147	Gibt das Timeout für SNMP-Trap-Informationsmeldungen an. Der zulässige Bereich liegt zwischen 0 und 2147.	3

Anzahl der Wiederholungsversuche für Trap-Benachrichtigungen

Einstellung	Beschreibung	Werkseinstellung
0–255	Gibt die Wiederholungsversuche für SNMP-Trap-Informationsmeldungen an. Der zulässige Bereich liegt zwischen 0 und 255.	5

Trap-Sicherheits-Engine-ID

Gibt die SNMP-Trap-Sicherheits-Engine-ID an. SNMPv3 sendet Traps und Benachrichtigungen unter Verwendung von USM zur Authentifizierung und zum Datenschutz. Für diese Traps und

Benachrichtigungen ist eine eindeutige Engine-ID erforderlich. Wenn die Option „Trap-Probe-Sicherheits-Engine-ID“ aktiviert ist, wird die ID automatisch ermittelt. Andernfalls wird die in diesem Feld angegebene ID verwendet. Die Zeichenfolge muss eine gerade Zahl (im Hexadezimalformat) mit einer Ziffernanzahl zwischen 10 und 64 enthalten, wobei jedoch keine reinen Nullen und keine reinen „F“s zulässig sind.

Trap-Sicherheitsname
Gibt den SNMP-Trap-Sicherheitsnamen an. SNMPv3-Traps und -Informs verwenden USM für die Authentifizierung und den Datenschutz. Wenn Traps und Informs aktiviert sind, ist ein eindeutiger Sicherheitsname erforderlich.

Konfigurationen für SNMP-Trap-Quellen

Löschen
Aktivieren Sie dieses Kontrollkästchen, um den Eintrag zu löschen. Er wird beim nächsten Speichern gelöscht.

Name
Gibt den Namen des Eintrags an.

Typ
Der Filtertyp für den Eintrag.

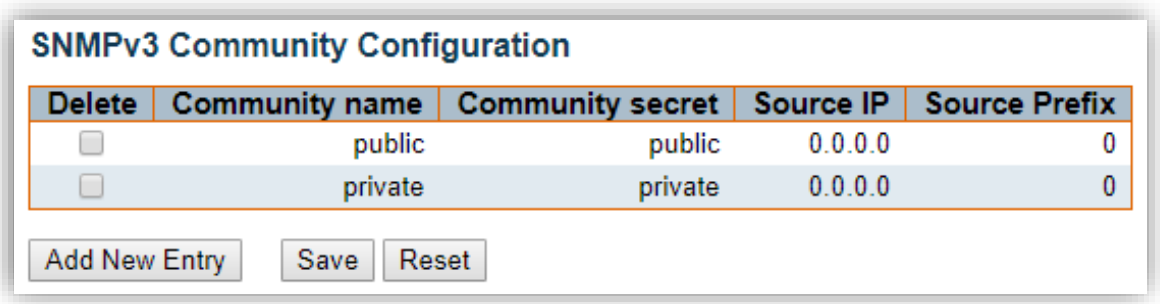
Einstellung	Beschreibung	Werkseinstellung
enthalten	Ein optionales Flag, das angibt, dass ein Trap für die angegebene Trap-Quelle gesendet wird, wenn eine Übereinstimmung vorliegt.	enthalten
ausgeschlossen	Ein optionales Flag, das angibt, dass kein Trap für die angegebene Trap-Quelle gesendet wird, wenn ein Treffer vorliegt.	

Teilmenge-OID
Die Teilmenge-OID für den Eintrag. Der Wert sollte von der Art des Trap-Namens abhängen. Beispielsweise ist „ifIdex“ die Teilmenge-OID von „linkUp“ und „linkDown“. Eine gültige Teilmenge-OID besteht aus einer oder mehreren Ziffern (0–4294967295) oder Sternchen (*), die durch Punkte (.) getrennt sind. Das erste Zeichen darf nicht mit einem Sternchen (*) beginnen, und die maximale Anzahl der OID-Zeichen darf 128 nicht überschreiten.

Konfiguration > Sicherheit > Switch > SNMP > Communities

Konfiguration der SNMPv3-Community

Konfigurieren Sie auf dieser Seite die SNMPv3-Community-Tabelle. Der Indexschlüssel für den Eintrag lautet **„Community**“.



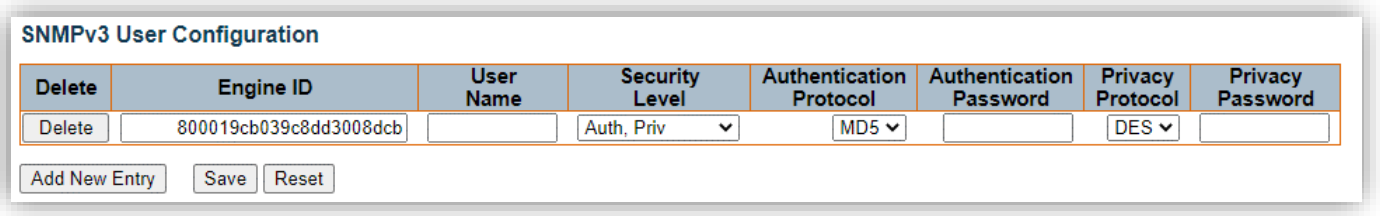
Neuen Eintrag hinzufügen

Einstellung	Beschreibung
Löschen	Aktivieren Sie dieses Kontrollkästchen, um den Eintrag zu löschen. Er wird beim nächsten Speichern gelöscht.
Community-Name	Gibt den Sicherheitsnamen an, mit dem die Community der SNMP-Gruppenkonfiguration zugeordnet wird. Die zulässige Zeichenfolgenlänge beträgt 1 bis 32, und der zulässige Inhalt besteht aus ASCII-Zeichen von 33 bis 126.
Community-Geheimnis	Gibt das Community-Geheimnis (Zugriffszeichenfolge) an, um den Zugriff auf den SNMP-Agenten über SNMPv1 und SNMPv2c zu ermöglichen. Die zulässige Zeichenfolgenlänge beträgt 1 bis 32, und der zulässige Inhalt besteht aus ASCII-Zeichen von 33 bis 126.
Quell-IP	Gibt die SNMP-Zugriffsquelle an. In Kombination mit dem Quellpräfix kann ein bestimmter Bereich von Quelladressen verwendet werden, um das Quell-Subnetz einzuschränken.
Quellpräfix	Gibt das Präfix der SNMP-Quelladresse an.

Konfiguration > Sicherheit > Switch > SNMP > Benutzer

SNMPv3-Benutzerkonfiguration

Konfigurieren Sie auf dieser Seite die SNMPv3-Benutzertabelle. Die Indexschlüssel für die Einträge sind **„Engine-ID“** und **„Benutzername**“.



Neuen Eintrag hinzufügen

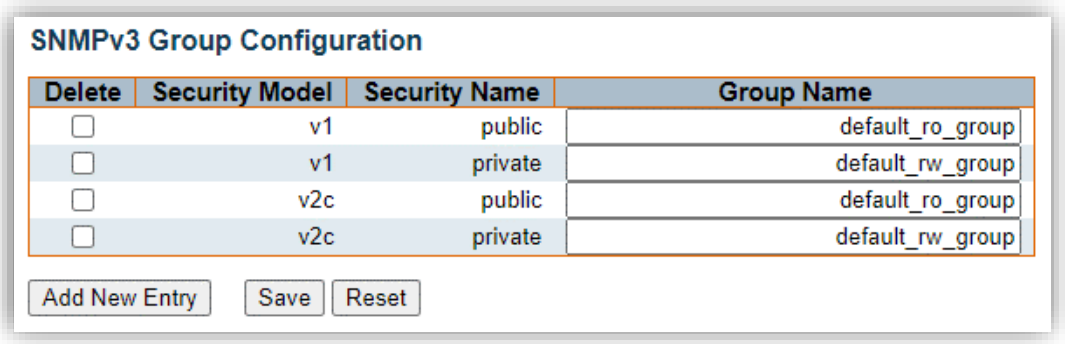
Einstellung	Beschreibung
Löschen	Aktivieren Sie dieses Kontrollkästchen, um den Eintrag zu löschen. Er wird beim nächsten Speichern gelöscht.
Engine-ID	Eine Oktettzeichenfolge, die die Engine-ID identifiziert, zu der dieser Eintrag gehören soll. Die Zeichenfolge muss eine gerade Zahl (im Hexadezimalformat) mit einer Ziffernanzahl zwischen 10 und 64 enthalten, wobei jedoch keine reinen Nullen und keine reinen „F“s zulässig sind. Die SNMPv3-Architektur verwendet das benutzerbasierte Sicherheitsmodell (USM) für die Nachrichtensicherheit und das ansichtsbasierte Zugriffskontrollmodell (VACM) für die Zugriffskontrolle. Bei einem USM-Eintrag sind „usmUserEngineID“ und „usmUserName“ die Schlüssel des Eintrags. Bei einem einfachen Agenten entspricht „usmUserEngineID“ immer dem Wert „snmpEngineID“ dieses Agenten. Der Wert kann auch den Wert der „snmpEngineID“ einer entfernten SNMP-Engine annehmen, mit der dieser Benutzer kommunizieren kann. Mit anderen Worten: Wenn die Benutzer-Engine-ID mit der System-Engine-ID übereinstimmt, handelt es sich um einen lokalen Benutzer; andernfalls um einen entfernten Benutzer.
Benutzername	Eine Zeichenfolge, die den Benutzernamen identifiziert, zu dem dieser Eintrag gehören soll. Die zulässige Zeichenfolgenlänge beträgt 1 bis 32, und der zulässige Inhalt besteht aus ASCII-Zeichen von 33 bis 126.
Sicherheitsstufe	Gibt das Sicherheitsmodell an, zu dem dieser Eintrag gehören soll. Mögliche Sicherheitsmodelle sind: • **NoAuth, NoPriv:** Keine Authentifizierung und keine Privatsphäre. • **Auth, NoPriv:** Authentifizierung und keine Privatsphäre. • **Auth, Priv:** Authentifizierung und Datenschutz. Der Wert der Sicherheitsstufe kann nicht geändert werden, wenn der Eintrag bereits vorhanden ist. Das bedeutet, dass zunächst sichergestellt werden muss, dass der Wert korrekt gesetzt ist.

Authentifizierungsprotokoll	Gibt das Authentifizierungsprotokoll an, zu dem dieser Eintrag gehören soll. Mögliche Authentifizierungsprotokolle sind: • **Keine:** Kein Authentifizierungsprotokoll. • **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. Der Wert der Sicherheitsstufe kann nicht geändert werden, wenn der Eintrag bereits vorhanden ist. Das bedeutet, dass zunächst sichergestellt werden muss, dass der Wert korrekt eingestellt ist.
Authentifizierungskennwort	Eine Zeichenfolge, die die Passwortphrase für die Authentifizierung angibt. Beim MD5-Authentifizierungsprotokoll beträgt die zulässige Zeichenfolgenlänge 8 bis 32. Beim SHA-Authentifizierungsprotokoll beträgt die zulässige Zeichenfolgenlänge 8 bis 40. Zulässig sind ASCII-Zeichen von 33 bis 126.
Datenschutzprotokoll	Gibt das Datenschutzprotokoll an, zu dem dieser Eintrag gehören soll. Mögliche Datenschutzprotokolle sind: • **Keine:** Kein Datenschutzprotokoll. • **DES:** Ein optionales Flag, das angibt, dass dieser Benutzer das DES-Authentifizierungsprotokoll verwendet. • **AES:** Ein optionales Flag, das angibt, dass dieser Benutzer das AES-Authentifizierungsprotokoll verwendet.
Datenschutz-Passwort	Eine Zeichenfolge, die die Datenschutz-Passwortphrase identifiziert. Die zulässige Zeichenfolgenlänge beträgt 8 bis 32 Zeichen, und der zulässige Inhalt besteht aus ASCII-Zeichen von 33 bis 126.

Konfiguration > Sicherheit > Switch > SNMP > Gruppen

SNMPv3-Gruppenkonfiguration

Konfigurieren Sie auf dieser Seite die SNMPv3-Gruppentabelle. Die Indexschlüssel für die Einträge sind **„Sicherheitsmodell“** und **„Sicherheitsname**“.



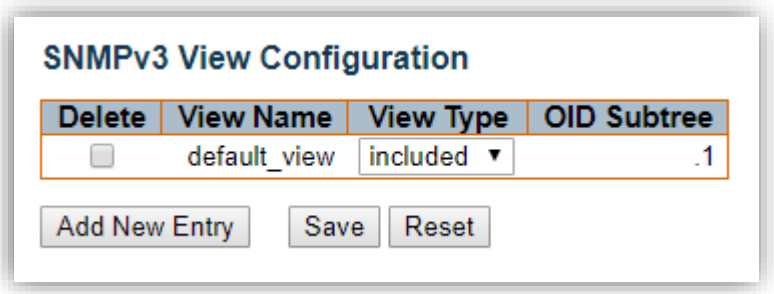
Neuen Eintrag hinzufügen

Einstellung	Beschreibung
Löschen	Aktivieren Sie dieses Kontrollkästchen, um den Eintrag zu löschen. Er wird beim nächsten Speichern gelöscht.
Sicherheitsmodell	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).
Sicherheitsname	Eine Zeichenfolge, die den Sicherheitsnamen identifiziert, zu dem dieser Eintrag gehören soll. Die zulässige Zeichenfolgenlänge beträgt 1 bis 32, und der zulässige Inhalt besteht aus ASCII-Zeichen von 33 bis 126. **HINWEIS:** Der Wert ist im Abschnitt **„Konfiguration > Sicherheit > Switch > SNMP > Communities“** vorkonfiguriert.
Gruppenname	Eine Zeichenfolge, die den Gruppennamen angibt, zu dem dieser Eintrag gehören soll. Die zulässige Zeichenfolgenlänge beträgt 1 bis 32, und der zulässige Inhalt besteht aus ASCII-Zeichen von 33 bis 126.

Konfiguration > Sicherheit > Switch > SNMP > Ansichten

SNMPv3-Ansichtskonfiguration

Konfigurieren Sie auf dieser Seite die SNMPv3-Ansichtstabelle. Die Indexschlüssel für die Einträge sind **„Ansichtsname“** und **„OID-Teilbaum**“.



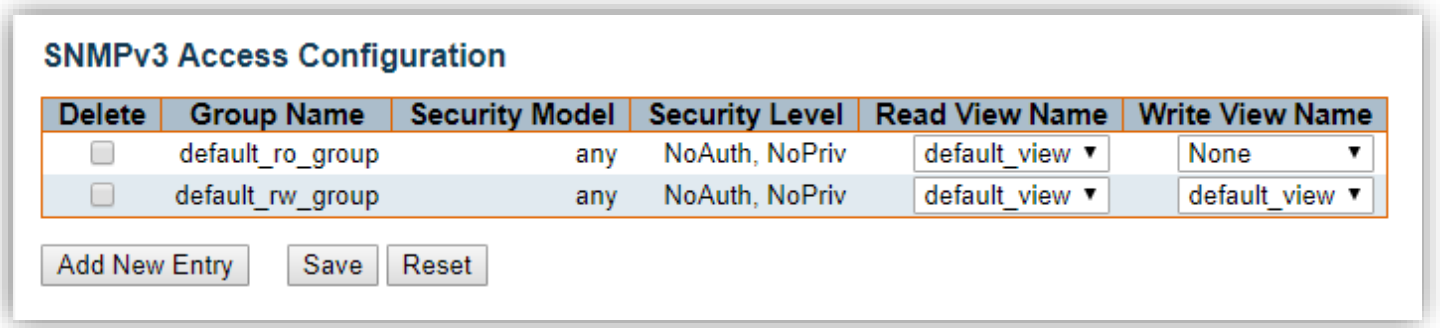
Neuen Eintrag hinzufügen

Einstellung	Beschreibung
Löschen	Aktivieren Sie dieses Kontrollkästchen, um den Eintrag zu löschen. Er wird beim nächsten Speichern gelöscht.
Ansichtsname	Eine Zeichenfolge, die den Namen der Ansicht angibt, zu der dieser Eintrag gehören soll. Die zulässige Zeichenfolgenlänge beträgt 1 bis 32, und der zulässige Inhalt besteht aus ASCII-Zeichen von 33 bis 126.
Ansichtstyp	Gibt den Ansichtstyp an, zu dem dieser Eintrag gehören soll. Mögliche Ansichtstypen sind: • **included:** Ein optionales Flag, das angibt, dass dieser Ansichtsunterbaum einbezogen werden soll. • **excluded:** Ein optionales Flag, das angibt, dass dieser Ansichtsunterbaum ausgeschlossen werden soll. Im Allgemeinen gilt: Wenn der Ansichtstyp eines Ansichtseintrags **„excluded“** ist, sollte ein weiterer Ansichtseintrag mit dem Ansichtstyp „included“ vorhanden sein, dessen OID-Unterbaum den **ausgeschlossenen** Ansichtseintrag überlagert.
OID-Teilbaum	Die OID, die die Wurzel des Teilbaums definiert, der der benannten Ansicht hinzugefügt werden soll. Die zulässige OID-Länge beträgt 1 bis 128. Der zulässige Zeichenfolgeninhalt besteht aus einer digitalen Zahl oder einem Sternchen (*).

Konfiguration > Sicherheit > Switch > SNMP > Zugriff

SNMPv3-Zugriffskonfiguration

Konfigurieren Sie auf dieser Seite die SNMPv3-Zugriffstabelle. Die Indexschlüssel für die Einträge sind **Gruppenname**, **Sicherheitsmodell** und **Sicherheitsstufe**.



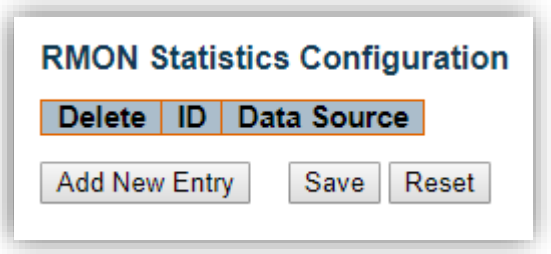
Neuen Eintrag hinzufügen

Einstellung	Beschreibung
Löschen	Aktivieren Sie dieses Kontrollkästchen, um den Eintrag zu löschen. Er wird beim nächsten Speichern gelöscht.
Gruppenname	Eine Zeichenfolge, die den Gruppennamen angibt, zu dem dieser Eintrag gehören soll. Die zulässige Zeichenfolgenlänge beträgt 1 bis 32, und der zulässige Inhalt besteht aus ASCII-Zeichen von 33 bis 126.
Sicherheitsmodell	Gibt das Sicherheitsmodell an, zu dem dieser Eintrag gehören soll. Mögliche Sicherheitsmodelle sind: • **any:** Jedes Sicherheitsmodell wird akzeptiert (v1|v2c|usm). • **v1:** Reserviert für SNMPv1. • **v2c:** Reserviert für SNMPv2c. • **usm:** Benutzerbasiertes Sicherheitsmodell (USM).
Sicherheitsstufe	Gibt das Sicherheitsmodell an, zu dem dieser Eintrag gehören soll. Mögliche Sicherheitsmodelle sind: • **NoAuth, NoPriv:** Keine Authentifizierung und keine Privatsphäre. • **Auth, NoPriv:** Authentifizierung und kein Datenschutz. • **Auth, Priv:** Authentifizierung und Datenschutz.
Name der Leseansicht	Der Name der MIB-Ansicht, die die MIB-Objekte definiert, für die diese Anfrage die aktuellen Werte abfragen darf. Die zulässige Zeichenfolgenlänge beträgt 1 bis 32, und der zulässige Inhalt besteht aus ASCII-Zeichen von 33 bis 126.
Schreibansicht-Name	Der Name der MIB-Ansicht, die die MIB-Objekte definiert, für die diese Anfrage möglicherweise neue Werte festlegen kann. Die zulässige Zeichenfolgenlänge beträgt 1 bis 32, und der zulässige Inhalt besteht aus ASCII-Zeichen von 33 bis 126.

Konfiguration > Sicherheit > Switch > RMON > Statistiken

RMON-Statistiken – Konfiguration

Konfigurieren Sie auf dieser Seite die RMON-Statistiktabelle. Der Indexschlüssel für den Eintrag lautet **„ID**“.



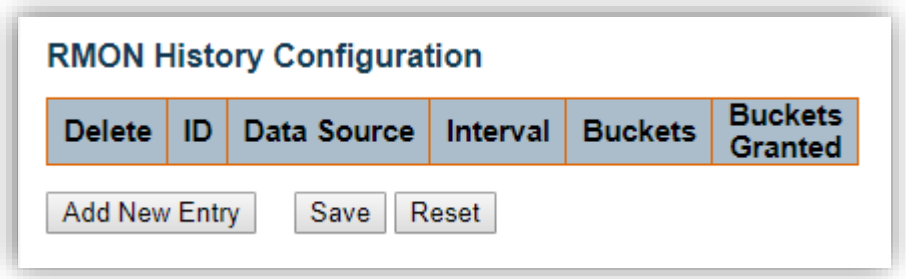
Neuen Eintrag hinzufügen

Einstellung	Beschreibung
Löschen	Aktivieren Sie dieses Kontrollkästchen, um den Eintrag zu löschen. Er wird beim nächsten Speichern gelöscht.
ID	Gibt den Index des Eintrags an. Der Bereich reicht von 1 bis 65535.
Datenquelle	Gibt die Port-ID an, die überwacht werden soll. Bei einem Stacking-Switch muss der Wert um 1000000*(Switch-ID-1) erhöht werden. Wenn es sich beispielsweise um Port 5 von Switch 3 handelt, lautet der Wert 2000005.

Konfiguration > Sicherheit > Switch > RMON > Verlauf

RMON-Verlaufskonfiguration

Konfigurieren Sie auf dieser Seite die RMON-Verlaufstabelle. Der Schlüssel für den Eintragsindex ist **die ID**.



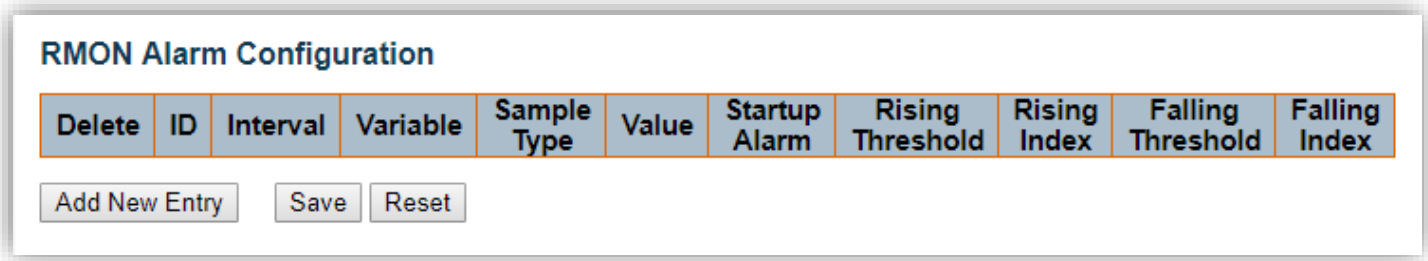
Neuen Eintrag hinzufügen

Einstellung	Beschreibung
Löschen	Aktivieren Sie dieses Kontrollkästchen, um den Eintrag zu löschen. Er wird beim nächsten Speichern gelöscht.
ID	Gibt den Index des Eintrags an. Der Bereich reicht von 1 bis 65535.
Datenquelle	Gibt die Port-ID an, die überwacht werden soll. Bei einem Stacking-Switch muss der Wert um 1000000*(Switch-ID-1) erhöht werden; wenn es sich beispielsweise um Port 5 von Switch 3 handelt, lautet der Wert 2000005.
Intervall	Gibt das Intervall in Sekunden für die Erfassung der historischen Statistikdaten an. Der Wertebereich reicht von 1 bis 3600, der Standardwert beträgt 1800 Sekunden.
Buckets	Gibt die maximale Anzahl der Dateneinträge an, die diesem Verlaufseintrag zugeordnet und in RMON gespeichert sind. Der Bereich reicht von 1 bis 3600, der Standardwert beträgt 50.
Zugewiesene Buckets	Die Anzahl der Datensätze, die in RMON gespeichert werden sollen.

Konfiguration > Sicherheit > Switch > RMON > Alarm

RMON-Alarmkonfiguration

Konfigurieren Sie auf dieser Seite die RMON-Alarmtabelle. Der Indexschlüssel für die Einträge ist **„ID“**.



Neuen Eintrag hinzufügen

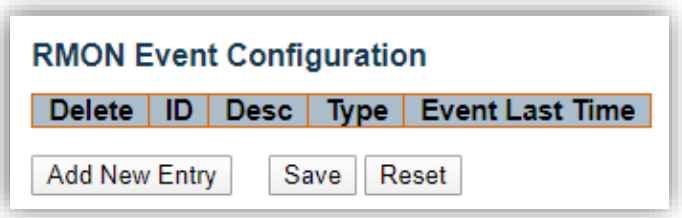
Einstellung	Beschreibung
Löschen	Aktivieren Sie dieses Kontrollkästchen, um den Eintrag zu löschen. Er wird beim nächsten Speichern gelöscht.
ID	Gibt den Index des Eintrags an. Der Bereich reicht von 1 bis 65535.
Intervall	Gibt das Intervall in Sekunden für die Abtastung und den Vergleich des Anstiegs- und Abfallschwellenwerts an. Der Bereich reicht von 1 bis 2^31-1.
Variable	Gibt die jeweilige zu erfassende Variable an. Mögliche Variablen sind: • **InOctets:** Die Gesamtzahl der an der Schnittstelle empfangenen Oktette, einschließlich der Rahmenzeichen. • **InUcastPkts:** Die Anzahl der an ein Protokoll einer höheren Schicht übermittelten Unicast-Pakete. • **InNUcastPkts:** Die Anzahl der Broadcast- und Multicast-Pakete, die an ein Protokoll einer höheren Schicht übergeben wurden. • **InDiscards:** Die Anzahl der eingehenden Pakete, die verworfen wurden, obwohl sie normal waren. • **InErrors:** Die Anzahl der eingehenden Pakete, die Fehler enthielten, die eine Weiterleitung an ein Protokoll einer höheren Schicht verhinderten. • **InUnknownProtos:** Die Anzahl der eingehenden Pakete, die aufgrund eines unbekannten oder nicht unterstützten Protokolls verworfen wurden. • **OutOctets:** Die Anzahl der über die Schnittstelle gesendeten Oktette, einschließlich Rahmenzeichen. • **OutUcastPkts:** Die Anzahl der Unicast-Pakete, für die eine Übertragung angefordert wurde. • **OutNUcastPkts:** Die Anzahl der Broadcast- und Multicast-Pakete, für die eine Übertragung angefordert wurde. • **OutDiscards:** Die Anzahl der ausgehenden Pakete, die verworfen wurden, obwohl die Pakete normal sind. • **OutErrors:** Die Anzahl der ausgehenden Pakete, die aufgrund von Fehlern nicht übertragen werden konnten. • **OutQLen:** Die Länge der Ausgangspaketwarteschlange (in Paketen).

Stichprobenart	Die Methode zur Erfassung der ausgewählten Variablen und zur Berechnung des Werts, der mit den Schwellenwerten verglichen werden soll. Mögliche Erfassungstypen sind: • **Absolut:** Die Stichprobe wird direkt erfasst. • **Delta:** Berechnung der Differenz zwischen den Stichproben (Standard).
Wert	Der Wert der Statistik während des letzten Erfassungszeitraums.
Startalarm	Die Methode zur Abtastung der ausgewählten Variablen und zur Berechnung des Werts, der mit den Schwellenwerten verglichen werden soll. Mögliche Abtasttypen sind: • **Ansteigend:** Alarm auslösen, wenn der erste Wert größer als der ansteigende Schwellenwert ist. • **Fallend:** Alarm auslösen, wenn der erste Wert kleiner als der fallende Schwellenwert ist. • **Steigend oder fallend:** Alarm auslösen, wenn der erste Wert größer als der Schwellenwert für steigende Werte oder kleiner als der Schwellenwert für fallende Werte ist (Standard).
Anstiegsschwelle	Anstiegsschwellenwert (-2147483648–2147483647).
Anstiegsindex	Anstiegs-Ereignisindex (1–65535).
Schwellenwert für fallende Werte	Fallender Schwellenwert (-2147483648–2147483647).
Fallender Index	Fallender Ereignisindex (1–65535).

Konfiguration > Sicherheit > Switch > RMON > Ereignis

RMON-Ereigniskonfiguration

Konfigurieren Sie auf dieser Seite die RMON-Ereignistabelle. Der Schlüssel für den Eintragsindex ist **„ID**“.



Neuen Eintrag hinzufügen

Einstellung	Beschreibung
Löschen	Aktivieren Sie das Kontrollkästchen, um den Eintrag zu löschen. Er wird beim nächsten Speichern gelöscht.
ID	Gibt den Index des Eintrags an. Der Bereich reicht von 1 bis 65535.
Beschreibung	Bezeichnet dieses Ereignis; die Zeichenfolgenlänge liegt zwischen 0 und 127, der Standardwert ist eine leere Zeichenfolge.
Typ	Gibt die Art der Benachrichtigung über das Ereignis an; mögliche Typen sind: **none:** Es wird kein SNMP-Protokoll erstellt und kein SNMP-Trap gesendet. **log:** Erzeugt einen SNMP-Protokolleintrag, wenn das Ereignis ausgelöst wird. **snmptrap:** Es wird ein SNMP-Trap gesendet, wenn das Ereignis ausgelöst wird. **logandtrap:** Bei Auslösung des Ereignisses wird ein SNMP-Protokolleintrag erstellt und ein SNMP-Trap gesendet.
Zeitpunkt des letzten Ereignisses	Gibt den Wert von „sysUpTime“ zu dem Zeitpunkt an, zu dem dieser Ereigniseintrag zuletzt ein Ereignis generiert hat.

Konfiguration > Sicherheit > Netzwerk

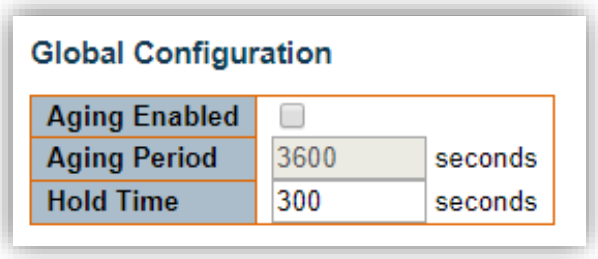
Konfiguration der Port-Sicherheit

Mit der Port-Sicherheitskonfiguration können Sie die globalen und portbezogenen Einstellungen für die Port-Sicherheit konfigurieren.

Die Port-Sicherheit ermöglicht es, die Anzahl der Benutzer an einem bestimmten Port zu begrenzen. Ein Benutzer wird anhand einer MAC-Adresse und einer VLAN-ID identifiziert. Wenn die Port-Sicherheit an einem Port aktiviert ist, legt die Begrenzung die maximale Anzahl von Benutzern an diesem Port fest. Wird diese Anzahl überschritten, wird je nach Verstoßmodus eine Maßnahme ergriffen. Der Verstoßmodus kann einer der drei unten beschriebenen sein.

Die Konfiguration der Port-Sicherheit besteht aus zwei Abschnitten: einem globalen und einem portbezogenen.

Globale Konfiguration

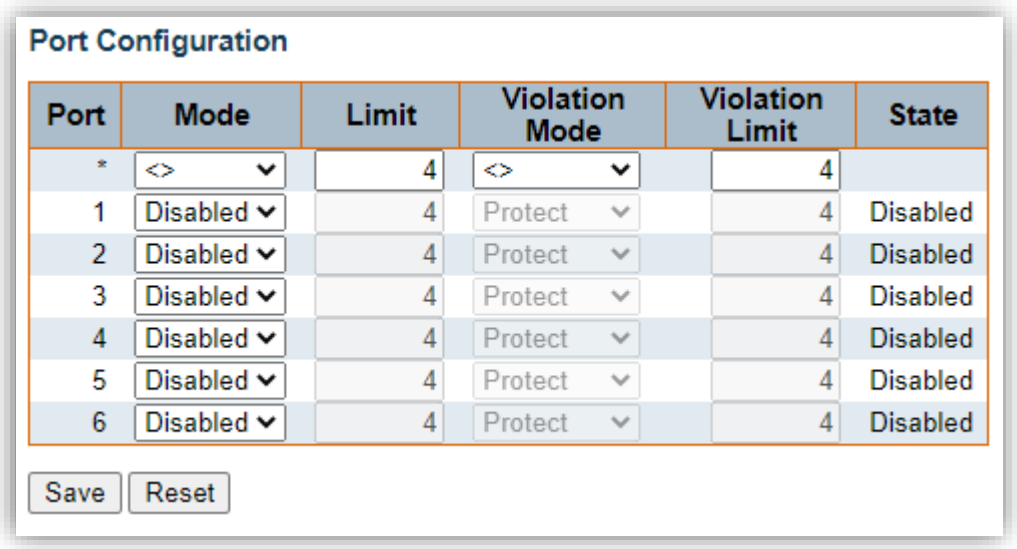


Einstellung	Beschreibung
Aging aktiviert	Wenn diese Option aktiviert ist, unterliegen gesicherte MAC-Adressen dem Aging, wie unter „Aging-Zeitraum“ beschrieben.
Ablaufzeit	Wenn „Aging aktiviert“ aktiviert ist, wird die Aging-Dauer über dieses Eingabefeld gesteuert. Falls andere Module die zugrunde liegende Funktionalität zur Sicherung von MAC-Adressen nutzen, können sie andere Anforderungen an die Aging-Dauer stellen. Die zugrunde liegende Funktionalität verwendet die kürzeste angeforderte Aging-Dauer aller Module, bei denen Aging aktiviert ist. Die „Aging-Dauer“ kann auf einen Wert zwischen 10 und 10000000 Sekunden eingestellt werden, wobei der Standardwert 3600 Sekunden beträgt. Um zu verstehen, warum eine Gültigkeitsdauer wünschenswert sein kann, betrachten Sie das folgende Szenario: Angenommen, ein Endhost ist mit einem Switch oder Hub eines Drittanbieters verbunden, der wiederum an einen Port dieses Switches angeschlossen ist, auf dem Port Security aktiviert ist. Der Endhost darf Daten weiterleiten, solange das Limit nicht überschritten wird. Nehmen wir nun an, der Endhost meldet sich ab oder wird heruntergefahren. Ohne Aging würde der Endhost weiterhin Ressourcen auf diesem Switch beanspruchen und könnte weiterhin Daten weiterleiten. Um diese Situation zu beheben, aktivieren Sie die Aging-Funktion. Bei aktiviertem Aging wird ein Timer gestartet, sobald der Endhost gesichert wurde. Nach Ablauf des Timers beginnt der Switch, nach Frames vom Endhost zu suchen. Werden innerhalb der nächsten Aging-Periode keine solchen Frames erkannt, wird davon ausgegangen, dass der Endhost

	getrennt ist, und die entsprechenden Ressourcen werden auf dem Switch freigegeben.
Haltezeit	Die Haltezeit – gemessen in Sekunden – dient dazu, festzulegen, wie lange eine MAC-Adresse in der MAC-Tabelle gehalten wird, wenn festgestellt wurde, dass sie den Grenzwert überschreitet. Der gültige Bereich liegt zwischen 10 und 10000000 Sekunden, wobei der Standardwert bei 300 Sekunden liegt. Der Grund für das Beibehalten einer regelwidrigen MAC-Adresse in der MAC-Tabelle besteht in erster Linie darin, sicherzustellen, dass dieselbe MAC-Adresse nicht zu fortlaufenden Benachrichtigungen führt (sofern Benachrichtigungen zur Anzahl der Verstöße aktiviert sind).

Port-Konfiguration

Die Tabelle enthält eine Zeile für jeden Port des Switches sowie mehrere Spalten.



Einstellung	Beschreibung
Port	Die Portnummer, für die die nachstehende Konfiguration gilt.
Modus	Legt fest, ob die Port-Sicherheit an diesem Port aktiviert ist. Beachten Sie, dass andere Module die zugrunde liegenden Port-Sicherheitsfunktionen weiterhin nutzen können, ohne dass die Port-Sicherheit an einem bestimmten Port aktiviert ist.
Limit	Die maximale Anzahl von MAC-Adressen, die an diesem Port gesichert werden können. Diese Zahl darf 1023 nicht überschreiten. Wird das Limit überschritten, wird eine dem Verstoßmodus entsprechende Maßnahme ergriffen. Der Switch verfügt über einen festen Pool an MAC-Adressen, aus dem alle Ports schöpfen, sobald eine neue MAC-Adresse an einem Port mit aktivierter Port-Sicherheit erkannt wird. Da alle Ports aus demselben Pool schöpfen, kann es vorkommen, dass ein konfiguriertes Maximum nicht gewährt werden kann, wenn die übrigen Ports bereits alle verfügbaren MAC-Adressen belegt haben. **Standard**: 4

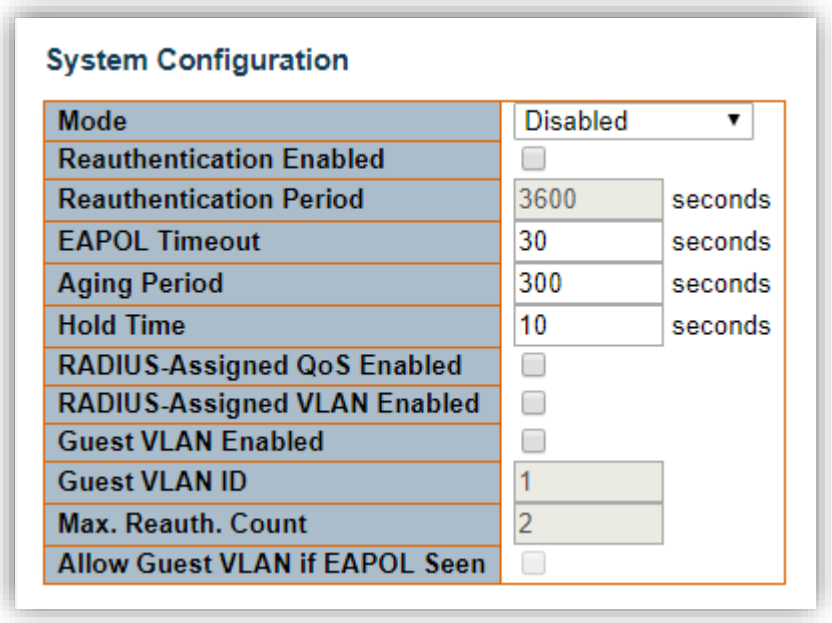
Verstoßmodus	Wenn das Limit erreicht ist, kann der Switch eine der folgenden Maßnahmen ergreifen: **„Protect“**: Es werden nicht mehr als „Limit“ MAC-Adressen am Port zugelassen, es werden jedoch keine weiteren Maßnahmen ergriffen. **Einschränken**: Wenn das Limit erreicht ist, werden nachfolgende MAC-Adressen am Port gezählt und als Verstoß markiert. Solche MAC-Adressen werden aus der MAC-Tabelle entfernt, sobald die Haltezeit abgelaufen ist. Zu jedem Zeitpunkt können höchstens „Verstoßlimit“ MAC-Adressen als Verstoß markiert werden. **Abschaltung**: Wenn der Grenzwert erreicht ist, führt bereits eine weitere MAC-Adresse zur Abschaltung des Ports. Dies bedeutet, dass alle gesicherten MAC-Adressen vom Port entfernt werden und keine neuen Adressen mehr gelernt werden. Es gibt drei Möglichkeiten, den Port wieder zu öffnen: 1. Deaktivieren Sie auf der Seite „Konfiguration→Ports“ in der Spalte „Konfiguriert“ zunächst den Port und stellen Sie anschließend den ursprünglichen Modus wieder her. 2. Nehmen Sie eine Änderung an der Port-Sicherheitskonfiguration für den Port vor. 3. Starten Sie den Switch neu.
Verstoßlimit	Die maximale Anzahl von MAC-Adressen, die an diesem Port als regelwidrig markiert werden können. Diese Zahl darf 1023 nicht überschreiten. Der Standardwert ist 4. Dieser Wert wird nur verwendet, wenn der Verstoßmodus auf **„Restrict“** eingestellt ist.
Status	Diese Spalte zeigt den aktuellen Port-Security-Status des Ports an. Der Status kann einen von vier Werten annehmen: **Deaktiviert**: Die Port-Sicherheit ist an diesem Port deaktiviert. **Bereit**: Das Limit ist noch nicht erreicht. Dies kann für alle Verstoßmodi angezeigt werden. **Limit erreicht**: Zeigt an, dass das Limit an diesem Port erreicht ist. Dies kann bei allen Verstoßmodi angezeigt werden. **Abgeschaltet**: Zeigt an, dass der Port durch die Port-Sicherheit abgeschaltet wurde. Dieser Status kann nur angezeigt werden, wenn der Verstoßmodus auf **„Abgeschaltet“** eingestellt ist.

Konfiguration > Sicherheit > Netzwerk > NAS

Konfiguration des Netzwerkzugriffsservers

Auf dieser Seite können Sie das IEEE 802.1X- und das MAC-basierte Authentifizierungssystem sowie die Port-Einstellungen konfigurieren.
Der IEEE 802.1X-Standard definiert ein portbasiertes Zugriffskontrollverfahren, das unbefugten Zugriff auf ein Netzwerk verhindert, indem Benutzer zunächst Anmeldedaten zur Authentifizierung übermitteln müssen. Ein oder mehrere zentrale Server, die Backend-Server, entscheiden, ob dem Benutzer der Zugriff auf das Netzwerk gewährt wird. Diese Backend-Server (RADIUS-Server) werden auf der Seite „Konfiguration > Sicherheit > AAA“ konfiguriert. Der IEEE 802.1X-Standard definiert einen portbasierten Betrieb, doch nicht standardkonforme Varianten überwinden Sicherheitsbeschränkungen, wie im Folgenden erläutert wird.
Die MAC-basierte Authentifizierung ermöglicht die Authentifizierung von mehr als einem Benutzer am selben Port und erfordert nicht, dass der Benutzer spezielle 802.1X-Supplicant-Software auf seinem System installiert hat. Der Switch verwendet die MAC-Adresse des Benutzers zur Authentifizierung gegenüber dem Backend-Server. Angreifer können gefälschte MAC-Adressen erstellen, wodurch die MAC-basierte Authentifizierung weniger sicher ist als die 802.1X-Authentifizierung.
Die NAS-Konfiguration besteht aus zwei Abschnitten: einem systemweiten und einem portweiten.

Systemkonfiguration



Einstellung	Beschreibung
Modus	Gibt an, ob das NAS auf dem Switch global aktiviert oder deaktiviert ist. Bei globaler Deaktivierung ist die Weiterleitung von Frames an allen Ports zulässig.

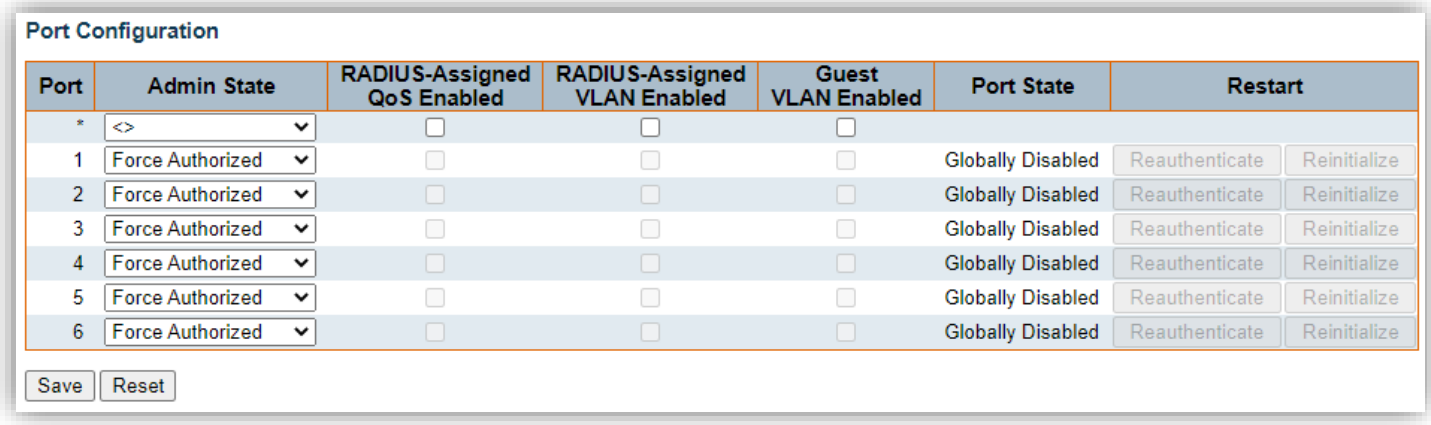
Reauthentifizierung aktiviert	Wenn diese Option aktiviert ist, werden erfolgreich authentifizierte Supplicants/Clients nach dem unter „Reauthentication Period“ festgelegten Intervall erneut authentifiziert. Die erneute Authentifizierung für 802.1X-fähige Ports kann verwendet werden, um zu erkennen, ob ein neues Gerät an einen Switch-Port angeschlossen wurde oder ob ein Supplicant nicht mehr verbunden ist. Bei MAC-basierten Ports ist die erneute Authentifizierung nur dann sinnvoll, wenn sich die Konfiguration des RADIUS-Servers geändert hat. Sie beinhaltet keine Kommunikation zwischen dem Switch und dem Client und bedeutet daher nicht, dass ein Client noch an einem Port vorhanden ist (siehe „Aging-Periode“ weiter unten).
Reauthentifizierungszeitraum	Legt den Zeitraum in Sekunden fest, nach dessen Ablauf ein verbundener Client erneut authentifiziert werden muss. Diese Option ist nur aktiv, wenn das Kontrollkästchen „Reauthentication Enabled“ aktiviert ist. Gültige Werte liegen im Bereich von 1 bis 3600 Sekunden.
EAPOL-Timeout	Legt die Zeit für die erneute Übertragung von „Request Identity“-EAPOL-Frames fest. Gültige Werte liegen im Bereich von 1 bis 65535 Sekunden. Dies hat keine Auswirkungen auf MAC-basierte Ports.
Ablaufzeit	Diese Einstellung gilt für die folgenden Modi, d. h. Modi, die die Port-Security-Funktionalität zur Sicherung von MAC-Adressen nutzen: • **Single 802.1X** • **Multi 802.1X** • **MAC-basierte Authentifizierung** Wenn das NAS-Modul das Port-Security-Modul zur Sicherung von MAC-Adressen verwendet, muss das Port-Security-Modul in regelmäßigen Abständen die betreffende MAC-Adresse auf Aktivität überprüfen und Ressourcen freigeben, wenn innerhalb eines bestimmten Zeitraums keine Aktivität festgestellt wird. Dieser Parameter steuert genau diesen Zeitraum und kann auf einen Wert zwischen 10 und 1000000 Sekunden eingestellt werden. Wenn die erneute Authentifizierung aktiviert ist und sich der Port im 802.1X-basierten Modus befindet, ist dies nicht so kritisch, da Supplicants, die nicht mehr mit dem Port verbunden sind, bei der nächsten erneuten Authentifizierung entfernt werden, die fehlschlagen wird. Ist die erneute Authentifizierung jedoch nicht aktiviert, besteht die einzige Möglichkeit, Ressourcen freizugeben, darin, die Einträge verfallen zu lassen. Bei Ports im MAC-basierten Authentifizierungsmodus führt die Neuauthentifizierung nicht zu einer direkten Kommunikation zwischen dem Switch und dem Client, sodass nicht erkannt wird, ob der Client noch verbunden ist oder nicht; die einzige Möglichkeit, Ressourcen freizugeben, besteht darin, den Eintrag verfallen zu lassen.

Haltezeit	Diese Einstellung gilt für die folgenden Modi, d. h. Modi, die die Port-Security-Funktionalität zur Sicherung von MAC-Adressen nutzen: • **Single 802.1X** • **Multi 802.1X** • **MAC-basierte Authentifizierung** Wird einem Client der Zugriff verweigert – entweder weil der RADIUS-Server dem Client den Zugriff verweigert oder weil die RADIUS-Serveranfrage abläuft (gemäß der auf der Seite **„Konfiguration > Sicherheit > AAA“** festgelegten Zeitüberschreitung) –, wird der Client im Status „Nicht autorisiert“ in die Warteschleife versetzt. Der Wartezeit-Timer läuft während einer laufenden Authentifizierung nicht weiter. Im Modus „MAC-basierte Authentifizierung“ ignoriert der Switch während der Wartezeit neue Frames, die vom Client gesendet werden. Die Wartezeit kann auf einen Wert zwischen 10 und 1000000 Sekunden eingestellt werden
RADIUS-zugewiesene QoS aktiviert	RADIUS-zugewiesenes QoS bietet die Möglichkeit, zentral zu steuern, welcher Verkehrsklasse der von einem erfolgreich authentifizierten Supplicant stammende Datenverkehr auf dem Switch zugewiesen wird. Der RADIUS-Server muss so konfiguriert sein, dass er spezielle RADIUS-Attribute überträgt, damit diese Funktion genutzt werden kann (eine detaillierte Beschreibung finden Sie weiter unten unter „RADIUS-zugewiesenes QoS aktiviert“). Das Kontrollkästchen „RADIUS-Assigned QoS Enabled“ bietet eine schnelle Möglichkeit, die vom RADIUS-Server zugewiesene QoS-Klassenfunktion global zu aktivieren bzw. zu deaktivieren. Ist das Kontrollkästchen aktiviert, bestimmt die entsprechende Einstellung der einzelnen Ports, ob die vom RADIUS-Server zugewiesene QoS-Klasse an diesem Port aktiviert ist. Ist das Kontrollkästchen deaktiviert, ist die vom RADIUS-Server zugewiesene QoS-Klasse an allen Ports deaktiviert.
„RADIUS-Assigned VLAN Enabled“	Das RADIUS-zugewiesene VLAN bietet die Möglichkeit, zentral zu steuern, in welchem VLAN ein erfolgreich authentifizierter Supplicant auf dem Switch platziert wird. Eingehender Datenverkehr wird dem RADIUS-zugewiesenen VLAN zugeordnet und dort weitergeleitet. Der RADIUS-Server muss so konfiguriert sein, dass er spezielle RADIUS-Attribute überträgt, um diese Funktion nutzen zu können (eine detaillierte Beschreibung finden Sie weiter unten unter **„RADIUS-zugewiesenes VLAN aktiviert**“). Das Kontrollkästchen „RADIUS-zugewiesenes VLAN aktiviert“ bietet eine schnelle Möglichkeit, die Funktion des vom RADIUS-Server zugewiesenen VLANs global zu aktivieren bzw. zu deaktivieren. Ist das Kontrollkästchen aktiviert, bestimmt die entsprechende Einstellung der einzelnen Ports, ob das RADIUS-zugewiesene VLAN an diesem Port aktiviert ist. Ist das Kontrollkästchen deaktiviert, ist das vom RADIUS-Server zugewiesene VLAN an allen Ports deaktiviert.
Gast-VLAN aktiviert	Ein Gast-VLAN ist ein spezielles VLAN – in der Regel mit eingeschränktem Netzwerkzugang –, in das 802.1X-unfähige Clients nach Ablauf einer vom Netzwerkadministrator festgelegten Zeitüberschreitung verschoben werden. Der Switch befolgt eine Reihe von Regeln für den Beitritt zum und das Verlassen des Gast-VLANs, wie unten aufgeführt.

	Das Kontrollkästchen **„Gast-VLAN aktiviert“** bietet eine schnelle Möglichkeit, die Gast-VLAN-Funktionalität global zu aktivieren bzw. zu deaktivieren. Ist das Kontrollkästchen aktiviert, bestimmt die entsprechende Einstellung der einzelnen Ports, ob der Port in das Gast-VLAN verschoben werden kann. Ist das Kontrollkästchen deaktiviert, ist die Möglichkeit, in das Gast-VLAN zu wechseln, an allen Ports deaktiviert.
Gast-VLAN-ID	Dies ist der Wert, auf den die Port-VLAN-ID eines Ports gesetzt wird, wenn ein Port in das Gast-VLAN verschoben wird. Er kann nur geändert werden, wenn die Option „Gast-VLAN“ global aktiviert ist. Gültige Werte liegen im Bereich [1; 4095].
Max. Anzahl der Neuauthentifizierungen	Mit dieser Einstellung wird festgelegt, wie oft der Switch einen EAPOL-Request-Identity-Frame ohne Antwort sendet, bevor er den Wechsel in das Gast-VLAN in Betracht zieht. Der Wert kann nur geändert werden, wenn die Option „Gast-VLAN“ global aktiviert ist. Gültige Werte liegen im Bereich [1; 255].
„Guest VLAN zulassen, wenn EAPOL erkannt wird“	Der Switch merkt sich für die gesamte Lebensdauer des Ports, ob an diesem Port ein EAPOL-Frame empfangen wurde. Sobald der Switch prüft, ob er in das Gast-VLAN wechseln soll, überprüft er zunächst, ob diese Option aktiviert oder deaktiviert ist. Ist sie deaktiviert (nicht markiert; Standard), wechselt der Switch nur dann in das Gast-VLAN, wenn an dem Port während seiner gesamten Lebensdauer kein EAPOL-Frame empfangen wurde. Ist die Option aktiviert (markiert), erwägt der Switch den Wechsel in das Gast-VLAN auch dann, wenn während der Lebensdauer des Ports ein EAPOL-Frame an diesem Port empfangen wurde. Der Wert kann nur geändert werden, wenn die Option „Gast-VLAN“ global aktiviert ist.

Port-Konfiguration

Die Tabelle enthält eine Zeile für jeden Port des Switches und mehrere Spalten



Port

Die Portnummer, für die die untenstehende Konfiguration gilt.

Admin-Status
Wenn NAS global aktiviert ist, steuert diese Auswahl den Authentifizierungsmodus des Ports.

Einstellung	Beschreibung
Autorisierung erzwingen	In diesem Modus sendet der Switch einen EAPOL-Success-Frame, sobald die Portverbindung hergestellt ist, und jedem Client an diesem Port wird der Netzwerkzugang ohne Authentifizierung gewährt.
„Force Unauthorized“	In diesem Modus sendet der Switch einen EAPOL-Fehler-Frame, sobald die Portverbindung hergestellt ist, und jedem Client an diesem Port wird der Netzwerkzugang verweigert.
Portbasiertes 802.1X	In der 802.1X-Umgebung wird der Benutzer als „Supplicant“ bezeichnet, der Switch als „Authenticator“ und der RADIUS-Server als Authentifizierungsserver. Der Authenticator fungiert als „Man-in-the-Middle“ und leitet Anfragen und Antworten zwischen dem Supplicant und dem Authentifizierungsserver weiter. Die zwischen dem Supplicant und dem Switch gesendeten Frames sind spezielle 802.1X-Frames, die als EAPOL-Frames (EAP Over LANs) bezeichnet werden. EAPOL-Frames kapseln EAP-PDUs (RFC 3748). Die zwischen dem Switch und dem RADIUS-Server gesendeten Frames sind RADIUS-Pakete. RADIUS-Pakete kapseln ebenfalls EAP-PDUs zusammen mit anderen Attributen wie der IP-Adresse des Switches, seinem Namen und der Portnummer des Supplicants am Switch ein. EAP ist insofern sehr flexibel, als es verschiedene Authentifizierungsmethoden wie MD5-Challenge, PEAP und TLS zulässt. Wichtig ist, dass der Authentifikator (der Switch) nicht wissen muss, welche Authentifizierungsmethode der Supplicant und der Authentifizierungsserver verwenden oder wie viele Frames zum Informationsaustausch für eine bestimmte Methode benötigt werden. Der Switch kapselt einfach den EAP-Teil des Frames in den entsprechenden Typ (EAPOL oder RADIUS) ein und leitet ihn weiter. Nach Abschluss der Authentifizierung sendet der RADIUS-Server ein spezielles Paket, das eine Erfolgsmeldung oder eine Fehlermeldung enthält. Der Switch leitet diese Entscheidung nicht nur an den Supplicant weiter, sondern nutzt sie auch, um den Datenverkehr am mit dem Supplicant verbundenen Switch-Port freizugeben oder zu blockieren. **HINWEIS:** Angenommen, es sind zwei Backend-Server aktiviert und die Server-Zeitüberschreitung ist (über die AAA-Konfigurationsseite) auf X Sekunden eingestellt, und angenommen, der erste Server in der Liste ist derzeit ausgefallen (wird aber nicht als ausgefallen betrachtet). Wenn der Supplicant nun EAPOL-Start-Frames in Abständen von weniger als X Sekunden erneut sendet, wird er niemals authentifiziert, da der Switch laufende Anfragen an den Backend-Authentifizierungsserver abbricht, sobald er einen neuen EAPOL-Start-Frame vom Supplicant empfängt. Und da der Server noch nicht ausgefallen ist (da die X Sekunden noch nicht abgelaufen sind), wird bei der nächsten Anfrage des Switches an den Backend-Authentifizierungsserver derselbe Server kontaktiert. Dieses Szenario wiederholt sich endlos. Daher sollte die Server-Timeout-Zeit kürzer sein als die Wiederholungsrate der EAPOL-Start-Frames des Supplicants.
Einzelnes 802.1X	Bei der portbasierten 802.1X-Authentifizierung wird der gesamte Port für den Netzwerkverkehr freigegeben, sobald ein Supplicant an einem Port erfolgreich authentifiziert wurde. Dies ermöglicht es anderen Clients, die an

	den Port angeschlossen sind (beispielsweise über einen Hub), sich an den erfolgreich authentifizierten Client anzuhängen und Netzwerkzugang zu erhalten, obwohl sie eigentlich nicht authentifiziert sind. Um diese Sicherheitslücke zu schließen, verwenden Sie die Variante „Single 802.1X“. „Single 802.1X“ ist zwar kein IEEE-Standard, weist jedoch viele der gleichen Merkmale auf wie die portbasierte 802.1X-Authentifizierung. Bei „Single 802.1X“ kann jeweils höchstens ein Supplicant am Port authentifiziert werden. Für die Kommunikation zwischen dem Supplicant und dem Switch werden normale EAPOL-Frames verwendet. Sind mehrere Supplicants an einen Port angeschlossen, wird derjenige berücksichtigt, der als Erster erscheint, sobald die Verbindung zum Port hergestellt ist. Wenn dieser Supplicant nicht innerhalb einer bestimmten Zeitspanne gültige Anmeldedaten vorlegt, erhält ein anderer Supplicant eine Chance. Sobald ein Supplicant erfolgreich authentifiziert wurde, erhält nur dieser Supplicant Zugriff. 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 Merkmale aufweist. Bei Multi 802.1X können sich ein oder mehrere Supplicants gleichzeitig am selben Port authentifizieren lassen. Jeder Supplicant wird einzeln authentifiziert und mithilfe des Port-Security-Moduls in der MAC-Tabelle gesichert. Bei 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 Anfragen antworten würden. Stattdessen verwendet der Switch die MAC-Adresse des Supplicants, die aus dem ersten EAPOL-Start- oder EAPOL-Response-Identity-Frame, der vom Supplicant gesendet wurde. Eine Ausnahme bildet der Fall, dass keine Supplicants angeschlossen sind. In diesem Fall sendet der Switch EAPOL-Request-Identity-Frames unter Verwendung der BPDU-Multicast-MAC-Adresse als Zieladresse, um etwaige Supplicants, die sich am Port befinden könnten, zu wecken. Die maximale Anzahl der Supplicants, die an einen Port angeschlossen werden können, lässt sich mithilfe der Funktion „Port Security Limit Control“ begrenzen.
MAC-basierte Authentifizierung.	Im Gegensatz zur portbasierten 802.1X-Authentifizierung ist die MAC-basierte Authentifizierung kein Standard, sondern lediglich eine von der Branche übernommene Best-Practice-Methode. Bei der MAC-basierten Authentifizierung werden die Benutzer als Clients bezeichnet, und der Switch fungiert im Namen der Clients als Supplicant. Der erste vom Client gesendete Frame (egal welcher Art) wird vom Switch abgefangen, der wiederum die MAC-Adresse des Clients sowohl als Benutzernamen als auch als Passwort im anschließenden EAP-Austausch mit dem RADIUS-Server verwendet. Die 6-Byte-MAC-Adresse wird in eine Zeichenkette der folgenden Form „xx-xx-xx-xx-xx-xx“ umgewandelt, d. h., ein Bindestrich (-) dient als Trennzeichen zwischen den Hexadezimalziffern in Klein . Der Switch unterstützt ausschließlich die MD5-Challenge-Authentifizierungsmethode, daher muss der RADIUS-Server entsprechend konfiguriert werden. Nach Abschluss der Authentifizierung sendet der RADIUS-Server eine Erfolgsmeldung oder eine Fehlermeldung, woraufhin der Switch mithilfe des

	Port-Security-Moduls den Datenverkehr für diesen bestimmten Client freigibt oder blockiert. Erst dann werden Frames vom Client über den Switch weitergeleitet. Bei dieser Authentifizierung sind keine EAPOL-Frames beteiligt, weshalb die MAC-basierte Authentifizierung nichts mit dem 802.1X-Standard zu tun hat. 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 einem gültigen RADIUS-Benutzer gehört, können von jedem genutzt werden. Außerdem wird nur die MD5-Challenge-Methode unterstützt. Die maximale Anzahl von Clients, die an einen Port angeschlossen werden können, lässt sich mithilfe der Funktion „Port Security Limit Control“ begrenzen.

RADIUS-zugewiesenes QoS aktiviert
Wenn „RADIUS-Assigned QoS“ sowohl global aktiviert als auch an einem bestimmten Port aktiviert (markiert) ist, reagiert der Switch auf QoS-Klasseninformationen, die im vom RADIUS-Server übertragenen RADIUS-Access-Accept-Paket enthalten sind, sobald ein Supplicant erfolgreich authentifiziert wurde. Sofern vorhanden und gültig, wird der am Port des Supplicants empfangene Datenverkehr der angegebenen QoS-Klasse zugeordnet. Wenn die (Neu-)Authentifizierung fehlschlägt oder das RADIUS-Access-Accept-Paket keine QoS-Klasse mehr enthält oder diese ungültig ist oder der Supplicant aus anderen Gründen nicht mehr am Port vorhanden ist, wird die QoS-Klasse des Ports sofort auf die ursprüngliche QoS-Klasse zurückgesetzt (die in der Zwischenzeit vom Administrator geändert werden kann, ohne dass dies Auswirkungen auf die RADIUS-zugewiesene QoS-Klasse hat).
Diese Option ist nur für Einzel-Client-Modi verfügbar, d. h.

- **portbasiertes 802.1X**
- **Einzel-802.1X**

RADIUS-Attribute zur Identifizierung einer QoS-Klasse:
Das in RFC 4675 definierte Attribut „User-Priority-Table“ bildet die Grundlage für die Identifizierung der QoS-Klasse in einem Access-Accept-Paket.
Es wird nur das erste Vorkommen des Attributs im Paket berücksichtigt, und um gültig zu sein, muss es dieser Regel entsprechen:

- Alle 8 Oktette im Wert des Attributs müssen identisch sein und aus ASCII-Zeichen im Bereich „0“ – „7“ bestehen, was der gewünschten QoS-Klasse im Bereich [0; 7] entspricht.

RADIUS-zugewiesenes VLAN aktiviert
Wenn „RADIUS-Assigned VLAN“ sowohl global aktiviert als auch für einen bestimmten Port aktiviert (markiert) ist, reagiert der Switch auf VLAN-ID-Informationen, die im vom RADIUS-Server übertragenen RADIUS-Access-Accept-Paket enthalten sind, sobald ein Supplicant erfolgreich authentifiziert wurde. Sofern vorhanden und gültig, wird die Port-VLAN-ID des Ports auf diese VLAN-ID geändert, der Port wird als Mitglied dieser VLAN-ID festgelegt und der Port wird in den VLAN-unabhängigen Modus versetzt. Nach der Zuweisung wird der gesamte am Port ankommende Datenverkehr anhand der RADIUS-zugewiesenen VLAN-ID klassifiziert und weitergeleitet.
Wenn die (Neu-)Authentifizierung fehlschlägt oder das RADIUS-„Access-Accept“-Paket keine VLAN-ID mehr enthält oder diese ungültig ist oder der Supplicant aus anderen Gründen nicht mehr am Port vorhanden ist, wird die VLAN-ID des Ports sofort auf die ursprüngliche VLAN-ID

zurückgesetzt (die in der Zwischenzeit vom Administrator geändert werden kann, ohne dass dies Auswirkungen auf die von RADIUS zugewiesene VLAN-ID hat).
Diese Option ist nur für Einzelclient-Modi verfügbar, d. h.

- **portbasiertes 802.1X**
- **Einzel-802.1X**

Zur Fehlerbehebung bei VLAN-Zuweisungen verwenden Sie die Seiten **„Monitor > VLANs > VLAN-Mitgliedschaft**“ und **„VLAN-Port**“. Diese Seiten zeigen an, welche Module die aktuelle Port-VLAN-Konfiguration (vorübergehend) überschrieben haben.

RADIUS-Attribute zur Identifizierung einer VLAN-ID:
RFC 2868 und RFC 3580 bilden die Grundlage für die Attribute, die zur Identifizierung einer VLAN-ID in einem „Access-Accept“-Paket verwendet werden. Es gelten die folgenden Kriterien:

- Die Attribute **„Tunnel-Medium-Type“, „Tunnel-Type“** und **„Tunnel-Private-Group-ID“** müssen alle mindestens einmal im „Access-Accept“-Paket vorhanden sein.
- Der Switch sucht nach dem ersten Satz dieser Attribute, die denselben Tag-Wert haben und die folgenden Anforderungen erfüllen (wenn „Tag == 0“ verwendet wird, muss die **„Tunnel-Private-Group-ID“** keinen Tag enthalten):
    - Der Wert von **„Tunnel-Medium-Type“** muss auf „IEEE-802“ gesetzt sein.
    - Der Wert von **„Tunnel-Type“** muss auf **„VLAN“** gesetzt sein.
    - Der Wert von **„Tunnel-Private-Group-ID“** muss eine Zeichenfolge aus ASCII-Zeichen im Bereich **von 0 bis 9** sein, die als dezimale Zeichenfolge interpretiert wird, die die VLAN-ID darstellt. Führende „0“en werden ignoriert. Der endgültige Wert muss im Bereich [1; 4095] liegen.

Gast-VLAN aktiviert
Wenn das Gast-VLAN sowohl global aktiviert als auch für einen bestimmten Port aktiviert (markiert) ist, erwägt der Switch, den Port gemäß den unten aufgeführten Regeln in das Gast-VLAN zu verschieben.
Diese Option ist nur für EAPOL-basierte Modi verfügbar, d. h.:

- **Portbasiertes 802.1X**
- **Einzelnes 802.1X**
- **Multi-802.1X**

Zur Fehlerbehebung bei VLAN-Zuweisungen verwenden Sie die Seiten „Monitor→VLANs→VLAN-Zugehörigkeit und VLAN-Port“. Auf diesen Seiten wird angezeigt, welche Module die aktuelle Port-VLAN-Konfiguration (vorübergehend) überschrieben haben.

Betrieb des Gast-VLANs:
Wenn die Verbindung eines für das Gast-VLAN aktivierten Ports hergestellt wird, beginnt der Switch mit der Übertragung von EAPOL-Request-Identity-Frames. Übersteigt die Anzahl der Übertragungen solcher Frames den Wert „Max. Reauth. Count“ und wurden in der Zwischenzeit keine EAPOL-Frames empfangen, erwägt der Switch den Beitritt zum Gast-VLAN. Das Intervall zwischen der Übertragung von EAPOL-Request-Identity-Frames wird über „EAPOL Timeout“ konfiguriert. Ist die Option „Allow Guest VLAN if EAPOL Seen“ aktiviert, wird der Port nun in das Gast-VLAN verschoben. Ist sie deaktiviert, überprüft der Switch zunächst seinen Verlauf, um festzustellen, ob zuvor bereits ein EAPOL-Frame an diesem Port empfangen wurde (dieser Verlauf wird gelöscht, wenn die Portverbindung unterbrochen wird oder sich der Admin-Status des Ports ändert); ist dies nicht der Fall, wird der Port in das Gast-VLAN verschoben. Andernfalls wechselt er nicht in das Gast-VLAN, sondern sendet weiterhin EAPOL-Request-Identity-Frames mit der durch das EAPOL-Timeout festgelegten Rate.

Sobald sich der Port im Gast-VLAN befindet, gilt er als authentifiziert, und allen an den Port angeschlossenen Clients wird der Zugriff auf dieses VLAN gewährt. Der Switch sendet beim Eintritt in das Gast-VLAN keinen EAPOL-Success-Frame.
Während sich der Port im Gast-VLAN befindet, überwacht der Switch die Verbindung auf EAPOL-Frames; wird ein solcher Frame empfangen, entfernt der Switch den Port sofort aus dem Gast-VLAN und beginnt mit der Authentifizierung des Supplicants entsprechend dem Port-Modus. Wird ein EAPOL-Frame empfangen, kann der Port niemals wieder in das Gast-VLAN zurückkehren, wenn die Option „Gast-VLAN zulassen, wenn **EAPOL erkannt wird“** deaktiviert ist.

Port-Status
Der aktuelle Status des Ports. Er kann einen der folgenden Werte annehmen:

- **Global deaktiviert:** NAS ist global deaktiviert.
- **Verbindung unterbrochen:** Das NAS ist global aktiviert, aber es besteht keine Verbindung am Port.
- **Autorisiert:** Der Port befindet sich im Modus „Force Authorized“ oder im Einzel-Supplicant-Modus, und der Supplicant ist autorisiert.
- **Nicht autorisiert:** Der Port befindet sich im Modus „Force Unauthorized“ oder im Einzel-Supplicant-Modus, und der Supplicant wurde vom RADIUS-Server nicht erfolgreich autorisiert.
- **X Auth/Y Unauth:** Der Port befindet sich im Multi-Supplicant-Modus. Derzeit sind X Clients autorisiert und Y nicht autorisiert.

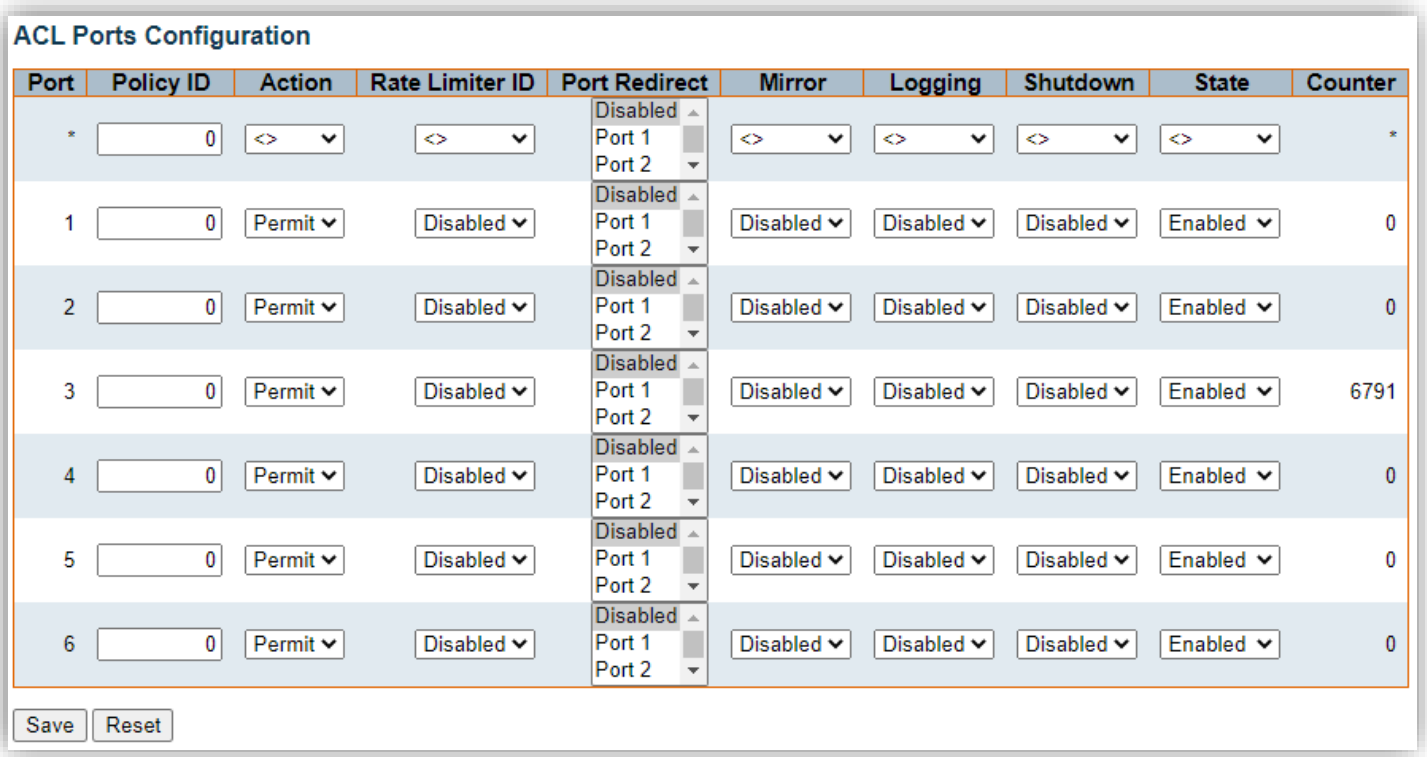
Neustart
Für jede Zeile stehen zwei Schaltflächen zur Verfügung. Die Schaltflächen sind nur aktiviert, wenn die Authentifizierung global aktiviert ist und sich der Admin-Status des Ports im EAPOL-basierten oder MAC-basierten Modus befindet.
Ein Klick auf diese Schaltflächen bewirkt nicht, dass die auf der Seite geänderten Einstellungen wirksam werden.

- **Neuauthentifizieren:** Plant eine Neuauthentifizierung, sobald die Ruhephase des Ports abgelaufen ist (EAPOL-basierte Authentifizierung). Bei der MAC-basierten Authentifizierung wird die Neuauthentifizierung sofort versucht. Die Schaltfläche wirkt sich nur auf erfolgreich authentifizierte Clients am Port aus und führt nicht dazu, dass die Clients vorübergehend nicht autorisiert werden.
- **Neu initialisieren:** Erzwingt eine Neuinitialisierung der Clients am Port und damit eine sofortige erneute Authentifizierung. Die Clients wechseln während der laufenden erneuten Authentifizierung in den nicht autorisierten Zustand.

Konfiguration > Sicherheit > Netzwerk > ACL > Ports

ACL-Port-Konfiguration

Konfigurieren Sie die ACL-Parameter (ACE) jedes Switch-Ports. Diese Parameter wirken sich auf die an einem Port empfangenen Frames aus, sofern der Frame nicht mit einem bestimmten ACE übereinstimmt.



Port
Der logische Port für die in derselben Zeile enthaltenen Einstellungen.

Richtlinien-ID

Einstellung	Beschreibung	Werkseinstellung
0–255	Wählen Sie die Richtlinie aus, die auf diesen Port angewendet werden soll. Die zulässigen Werte liegen zwischen 0 und 255.	0

Aktion

Einstellung	Beschreibung	Werkseinstellung
Zulassen	Die Weiterleitung ist erlaubt.	Zulassen
Verweigern	Die Weiterleitung wird verweigert.	

Rate-Limiter-ID

Einstellung	Beschreibung	Werkseinstellung

Deaktiviert	Der Ratenbegrenzer ist deaktiviert.	Deaktiviert
1–16	Wählen Sie aus, welcher Ratenbegrenzer auf diesen Port angewendet werden soll.	

Port-Umleitung

Einstellung	Beschreibung	Werkseinstellung
Deaktiviert	Die Port-Umleitung ist deaktiviert.	Deaktiviert
Port X	Wählen Sie den Port aus, auf den die Frames umgeleitet werden sollen.	

Spiegeln

Einstellung	Beschreibung	Werkseinstellung
Deaktiviert	Am Port empfangene Frames werden nicht gespiegelt.	Deaktiviert
Aktiviert	Am Port empfangene Frames werden gespiegelt.	

Protokollierung

Legen Sie die Protokollierung für diesen Port fest. Beachten Sie, dass die Protokollmeldung die 4-Byte-CRC nicht enthält.

Einstellung	Beschreibung	Werkseinstellung
Deaktiviert	Am Port empfangene Frames werden nicht protokolliert.	Deaktiviert
Aktiviert	Am Port empfangene Frames werden im Systemprotokoll gespeichert.	
HINWEIS	Die Protokollierungsfunktion funktioniert nur, wenn die Paketlänge weniger als 1518 beträgt (ohne VLAN-Tags), und die Speichergröße des Systemprotokolls sowie die Protokollierungsrate sind begrenzt.	

Herunterfahren

Einstellung	Beschreibung	Werkseinstellung
Deaktiviert	Die Port-Abschaltung ist deaktiviert.	Deaktiviert
Aktiviert	Wenn ein Frame an dem Port empfangen wird, wird der Port deaktiviert.	
HINWEIS	Die Abschaltfunktion funktioniert nur, wenn die Paketlänge weniger als 1518 beträgt (ohne VLAN-Tags).	

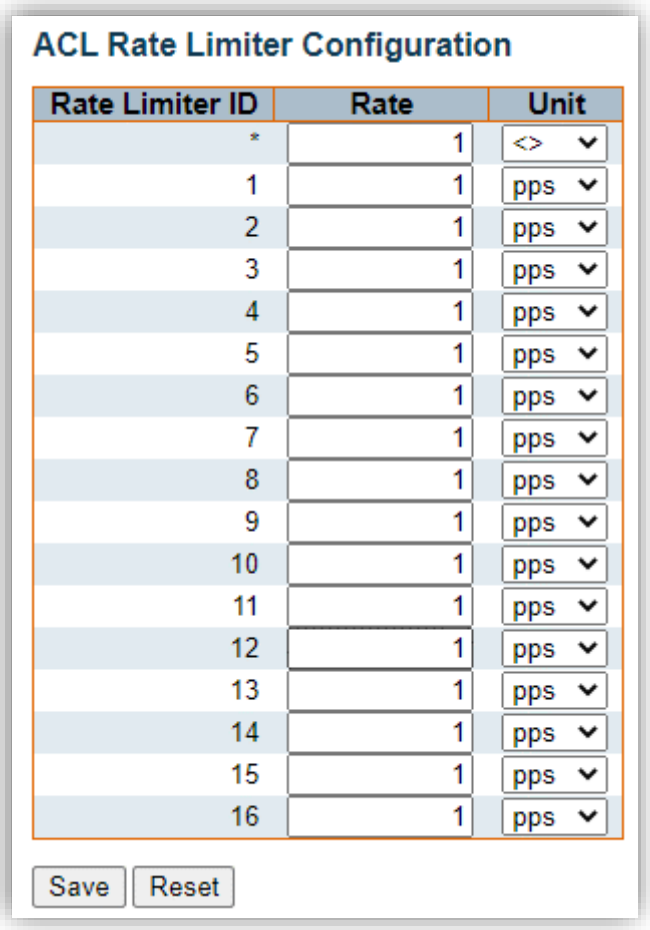
Status

Einstellung	Beschreibung	Werkseinstellung
Deaktiviert	Zum Schließen von Ports durch Ändern der flüchtigen Portkonfiguration des ACL-Benutzermoduls.	Aktiviert
Aktiviert	Zum erneuten Öffnen von Ports durch Ändern der flüchtigen Portkonfiguration des ACL-Benutzermoduls.	

Zähler
Zählt die Anzahl der Frames, die dieser ACE entsprechen.

Konfiguration > Sicherheit > Netzwerk > ACL > Ratenbegrenzer

Konfiguration des ACL-Ratenbegrenzers



Ratenbegrenzer-ID
Die Rate-Limiter-ID für die in derselben Zeile enthaltenen Einstellungen und deren Bereich liegt zwischen 1 und 16.

Rate

Einstellung	Beschreibung	Werkseinstellung
0–3276700	Der gültige Wert liegt im Bereich von 0 bis 3276700 in pps. oder 0, 100, 200, 300, …, 1000000 in kbps	1

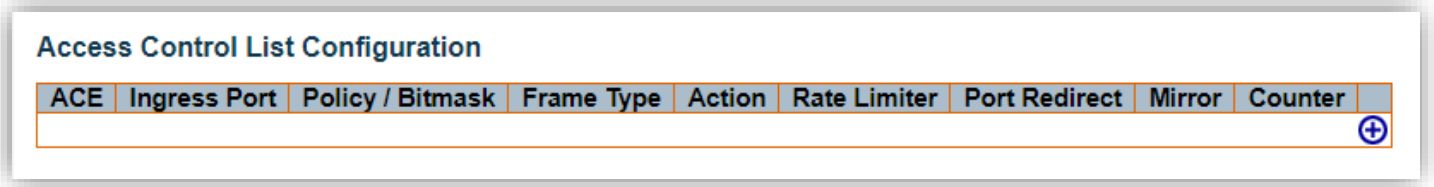
Einheit

Einstellung	Beschreibung	Werkseinstellung
pps	Pakete pro Sekunde	pps
kbps	Kbit pro Sekunde.	

Konfiguration > Sicherheit > Netzwerk > ACL > Zugriffskontrollliste

Konfiguration der Zugriffskontrollliste

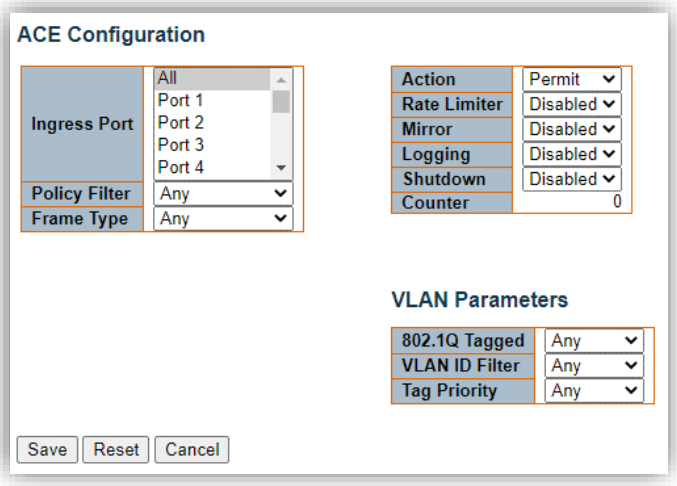
Auf dieser Seite wird die Zugriffskontrollliste (ACL) angezeigt, die sich aus den auf diesem Switch definierten ACEs zusammensetzt. Jede Zeile beschreibt die jeweilige definierte ACE. Die maximale Anzahl von ACEs beträgt 256 pro Switch.



Klicken Sie auf das unterste Pluszeichen, um der Liste einen neuen ACE hinzuzufügen. Die für interne Protokolle reservierten ACEs können weder bearbeitet noch gelöscht werden, ihre Reihenfolge lässt sich nicht ändern und sie haben die höchste Priorität.
Sie können jeden ACE (Access Control Entry) in der Tabelle mithilfe der folgenden Schaltflächen bearbeiten:

- : Fügt einen neuen ACE vor der aktuellen Zeile ein.
- „ “: Bearbeitet die ACE-Zeile.
- : Verschiebt den ACE in der Liste nach oben.
- : Verschiebt den ACE in der Liste nach unten.
- : Löscht den ACE.
- : Das unterste Pluszeichen fügt einen neuen Eintrag am Ende der ACE-Liste hinzu.

ACE-Konfiguration



Ein ACE besteht aus mehreren Parametern. Diese Parameter variieren je nach dem von Ihnen ausgewählten Frame-Typ. Wählen Sie zunächst den Eingangsport für den ACE und anschließend den Frame-Typ aus. Je nach ausgewähltem Frame-Typ werden unterschiedliche Parameteroptionen angezeigt.
Ein Frame, der auf diesen ACE trifft, entspricht der hier definierten Konfiguration.

Eingangsport

Einstellung	Beschreibung	Werkseinstellung
Alle	Die ACE gilt für alle Ports.	Alle
Port n	Die ACE gilt für diese Portnummer, wobei n die Nummer des Switch-Ports ist.	

Richtlinienfilter

Einstellung	Beschreibung	Werkseinstellung
Beliebig	Es ist kein Richtlinienfilter angegeben.	Beliebig
Spezifisch	Wenn Sie mit dieser ACE eine bestimmte Richtlinie filtern möchten, wählen Sie diesen Wert aus. Es erscheinen zwei Felder zur Eingabe eines Richtlinienwerts und einer Bitmaske.	

Richtlinienwert

Einstellung	Beschreibung	Werkseinstellung
0–255	Wenn für den Richtlinienfilter **die Option „Spezifisch“** ausgewählt ist, können Sie einen bestimmten Richtlinienwert eingeben. Der zulässige Bereich liegt zwischen 0 und 255.	0

Richtlinien-Bitmaske

Einstellung	Beschreibung	Werkseinstellung
0x0 bis 0xff	Wenn für den Richtlinienfilter **die Option „Spezifisch“** ausgewählt ist, können Sie eine spezifische Richtlinien-Bitmaske eingeben. Der zulässige Bereich liegt zwischen 0x0 und 0xff. Beachten Sie die Verwendung der Bitmaske: Ist der binäre Bitwert „0“, bedeutet dies, dass dieses Bit „beliebig“ ist. Das tatsächlich abgeglichene Muster lautet [Richtlinienwert & Richtlinien-Bitmaske]. Wenn der Richtlinienwert beispielsweise 3 und die Richtlinien-Bitmaske 0x10 ist (Bit 0 ist ein „beliebiges“ Bit), werden die Richtlinien 2 und 3 auf diese Regel angewendet.	0xff

Frame-Typ

Wählen Sie den Frame-Typ für diese ACE aus. Diese Frame-Typen schließen sich gegenseitig aus.

Einstellung	Beschreibung	Werkseinstellung
Beliebig	Jeder Frame kann dieser ACE entsprechen.	Beliebig
Ethernet-Typ	Nur Frames vom Typ „Ethernet“ können mit dieser ACE übereinstimmen. Die Spezifikation nach IEEE 802.3 schreibt vor, dass der Wert des Längen-/Typfelds größer oder gleich 1536 dezimal (entspricht 0600 hexadezimal) sein muss und nicht gleich 0x800 (IPv4), 0x806 (ARP) oder 0x86DD (IPv6) sein darf.	

ARP	Nur ARP-Frames können mit diesem ACE übereinstimmen. Beachten Sie, dass ARP-Frames nicht mit dem ACE vom Typ „Ethernet“ übereinstimmen.	
IPv4	Nur IPv4-Frames können mit diesem ACE übereinstimmen. Beachten Sie, dass IPv4-Frames nicht mit dem ACE mit dem Ethernet-Typ übereinstimmen.	
IPv6	Nur IPv6-Frames können mit diesem ACE übereinstimmen. Beachten Sie, dass IPv6-Frames nicht mit dem ACE vom Typ „Ethernet“ übereinstimmen.	

Aktion
Geben Sie die Aktion an, die bei einem Frame ausgeführt werden soll, der auf diese ACE trifft.

Einstellung	Beschreibung	Werkseinstellung
Zulassen	Dem Frame, der auf diese ACE trifft, wird die Berechtigung für den ACE-Vorgang erteilt.	Zulassen
Verweigern	Der Frame, der auf diese ACE trifft, wird verworfen.	
Filtern	Frames, die der ACE entsprechen, werden gefiltert.	

Ratenbegrenzer
Geben Sie den Ratenbegrenzer in Anzahl der Basiseinheiten an.

Einstellung	Beschreibung	Werkseinstellung
Deaktiviert	Der Betrieb des Ratenbegrenzers ist deaktiviert.	Deaktiviert
1–16	Geben Sie den Ratenbegrenzer in Basiseinheiten an. Der zulässige Bereich liegt zwischen 1 und 16.	

Port-Umleitung
Frames, die auf den ACE treffen, werden an die hier angegebene Portnummer umgeleitet. Der Ratenbegrenzer wirkt sich auf diese Ports aus. Der zulässige Bereich entspricht dem Bereich der Switch-Portnummern. **„Deaktiviert“** bedeutet, dass die Portumleitung deaktiviert ist und die spezifische Portnummer für „Portumleitung“ nicht festgelegt werden kann, wenn die Aktion zulässig ist.

Einstellung	Beschreibung	Werkseinstellung
Deaktiviert	Die Port-Umleitung ist deaktiviert	Deaktiviert
Aktiviert	Die Portweiterleitung ist aktiviert	

Spiegelung
Legen Sie die Spiegelungsfunktion dieses Ports fest. Frames, die dem ACE entsprechen, werden an den Ziel-Spiegelport gespiegelt. Der Ratenbegrenzer hat keinen Einfluss auf Frames am Spiegelport.

Einstellung	Beschreibung	Werkseinstellung
Aktiviert	Am Port empfangene Frames werden gespiegelt.	Deaktiviert
Deaktiviert	Am Port empfangene Frames werden nicht gespiegelt.	

Protokollierung
Legen Sie die Protokollierung des ACE fest. Beachten Sie, dass die Protokollmeldung die 4-Byte-CRC-Informationen nicht enthält.

Einstellung	Beschreibung	Werkseinstellung
Aktiviert	Frames, die dem ACE entsprechen, werden im Systemprotokoll gespeichert.	Deaktiviert
Deaktiviert	Frames, die der ACE entsprechen, werden nicht protokolliert.	
HINWEIS	Die Protokollierungsfunktion funktioniert nur, wenn die Paketlänge weniger als 1518 beträgt (ohne VLAN-Tags), und die Speichergröße des Systemprotokolls sowie die Protokollierungsrate sind begrenzt.	

Herunterfahren

Einstellung	Beschreibung	Werkseinstellung
Aktiviert	Wenn ein Frame dem ACE entspricht, wird der Eingangsport deaktiviert.	Deaktiviert
Deaktiviert	Die Port-Deaktivierung ist für die ACE deaktiviert.	
HINWEIS	Die Abschaltfunktion funktioniert nur, wenn die Paketlänge weniger als 1518 beträgt (ohne VLAN-Tags).	

Zähler
Der Zähler gibt an, wie oft der ACE von einem Frame getroffen wurde.

MAC-Parameter

SMAC-Filter
(Wird nur angezeigt, wenn der Frame-Typ „Ethernet“ oder „ARP“ ist.)

Einstellung	Beschreibung	Werkseinstellung
Beliebig	Es ist kein SMAC-Filter angegeben.	Beliebig
Spezifisch	Wenn Sie mit dieser ACE eine bestimmte Quell-MAC-Adresse filtern möchten, wählen Sie diesen Wert aus. Es erscheint ein Feld zur Eingabe eines SMAC-Werts.	

SMAC-Wert

Einstellung	Beschreibung	Werkseinstellung
MAC-Adresse	Wenn für den SMAC-Filter die Option „Spezifisch“ ausgewählt ist, können Sie eine bestimmte Quell-MAC-Adresse eingeben. Das zulässige Format lautet **xx-xx-xx-xx-xx-xx** oder **xx.xx.xx.xx.xx.xx** oder **xxxxxxxxxxxx** (x steht für eine Hexadezimalziffer). Ein Frame, der auf diese ACE trifft, entspricht diesem SMAC-Wert.	00-00-00-00-00-01

DMAC-Filter

Einstellung	Beschreibung	Werkseinstellung
Beliebig	Es ist kein DMAC-Filter angegeben.	Beliebig
MC	Frame muss per Multicast übertragen werden.	
BC	-Frame muss als Broadcast gesendet werden.	
UC	Der Frame muss ein Unicast-Frame sein.	
Spezifisch	Wenn Sie mit dieser ACE eine bestimmte Ziel-MAC-Adresse filtern möchten, wählen Sie diesen Wert aus. Es erscheint ein Feld zur Eingabe eines DMAC-Werts.	

DMAC-Wert

Einstellung	Beschreibung	Werkseinstellung
MAC-Adresse	Wenn für den DMAC-Filter **die Option „Spezifisch“** ausgewählt ist, können Sie eine bestimmte Quell-MAC-Adresse eingeben. Das zulässige Format lautet **xx-xx-xx-xx-xx-xx** oder **xx.xx.xx.xx.xx.xx** oder **xxxxxxxxxxxx** (x steht für eine Hexadezimalziffer). Ein Frame, der auf diesen ACE trifft, stimmt mit diesem DMAC-Wert überein.	00-00-00-00-00-02

VLAN-Parameter

802.1Q-getaggt

Einstellung	Beschreibung	Werkseinstellung
Beliebig	Jeder Wert ist zulässig.	Beliebig
Aktiviert	Nur mit Tags versehene Frames.	
Deaktiviert	Nur nicht getaggte Frames.	

VLAN-ID-Filter

Einstellung	Beschreibung	Werkseinstellung
Beliebig	Es ist kein VLAN-ID-Filter festgelegt.	Beliebig
Spezifisch	Wenn Sie mit dieser ACE eine bestimmte VLAN-ID filtern möchten, wählen Sie diesen Wert aus. Es erscheint ein Feld zur Eingabe einer VLAN-ID-Nummer.	

VLAN-ID

Einstellung	Beschreibung	Werkseinstellung
1–4095	Wenn für den VLAN-ID-Filter **die Option „Spezifisch“** ausgewählt ist, können Sie eine bestimmte VLAN-ID eingeben. Der zulässige Bereich liegt zwischen 1 und 4095. Ein Frame, der auf diese ACE trifft, stimmt mit diesem VLAN-ID-Wert überein.	1

Tag-Priorität

Einstellung	Beschreibung	Werkseinstellung
Beliebig	Es ist keine Tag-Priorität angegeben	Beliebig
0–7, 0–1, 2–3, 4–5, 6–7, 0–3, 4–7	Geben Sie die Tag-Priorität für diese ACE an. Ein Frame, der auf diese ACE trifft, entspricht dieser Tag-Priorität.	

ARP-Parameter

Die ARP-Parameter können konfiguriert werden, wenn der Frame-Typ „ARP“ ausgewählt ist.

ARP/RARP

Einstellung	Beschreibung	Werkseinstellung
Beliebig	Es ist kein ARP/RARP-OP-Flag angegeben.	Beliebig
ARP	Der Frame muss den ARP-Opcode „ARP“ enthalten.	
RARP	-Frame muss den RARP-Opcode auf „RARP“ gesetzt haben.	
Andere	Der Frame weist ein unbekanntes ARP/RARP-Opcode-Flag auf.	

Anfrage/Antwort

Einstellung	Beschreibung	Werkseinstellung
Beliebig	Es ist kein OP-Flag für Anfrage/Antwort angegeben	Beliebig
Anfrage	Der Frame muss das OP-Flag „ARP-Anfrage“ oder „RARP-Anfrage“ gesetzt haben.	
Antwort	Der Frame muss das OP-Flag „ARP-Antwort“ oder „RARP-Antwort“ enthalten.	

Absender-IP-Filter

Einstellung	Beschreibung	Werkseinstellung
Beliebig	Es ist kein Filter für die Absender-IP angegeben.	Beliebig
Host	Der Absender-IP-Filter ist auf „Host“ eingestellt. Geben Sie die Absender-IP-Adresse in das angezeigte Feld „SIP-Adresse“ ein.	

Netzwerk	Der Filter für die Absender-IP ist auf „Netzwerk“ eingestellt. Geben Sie die Absender-IP-Adresse und die Absender-IP-Maske in die angezeigten Felder „SIP-Adresse“ und „SIP-Maske“ ein.	

Absender-IP-Adresse

Einstellung	Beschreibung	Werkseinstellung
IP-Adresse	Wenn für den Absender-IP-Filter **„Host“** oder **„Netzwerk“** ausgewählt ist, können Sie eine bestimmte Absender-IP-Adresse in Dezimalschreibweise mit Punkten eingeben. Beachten Sie, dass auch eine ungültige IP-Adresskonfiguration zulässig ist, zum Beispiel 0.0.0.0. Normalerweise fügt ein ACE mit einer ungültigen IP-Adresse explizit eine „Deny“-Aktion hinzu.	0.0.0.0

Absender-IP-Maske

Einstellung	Beschreibung	Werkseinstellung
IP-Adresse	Wenn für den Absender-IP-Filter die Option **„Netzwerk“** ausgewählt ist, können Sie eine bestimmte Absender-IP-Maske in Dezimalschreibweise mit Punkten eingeben.	255.255.255.0

Ziel-IP-Filter

Einstellung	Beschreibung	Werkseinstellung
Beliebig	Es ist kein Ziel-IP-Filter angegeben.	Beliebig
Host	Der Ziel-IP-Filter ist auf „Host“ eingestellt. Geben Sie die Ziel-IP-Adresse in das angezeigte Feld „Ziel-IP-Adresse“ ein.	
Netzwerk	Der Ziel-IP-Filter ist auf „Netzwerk“ eingestellt. Geben Sie die Ziel-IP-Adresse und die Ziel-IP-Maske in die angezeigten Felder „Ziel-IP-Adresse“ und „Ziel-IP-Maske“ ein.	

Ziel-IP-Adresse

Einstellung	Beschreibung	Werkseinstellung
IP-Adresse	Wenn für den Ziel-IP-Filter **„Host“** oder **„Netzwerk“** ausgewählt ist, können Sie eine bestimmte Ziel-IP-Adresse in Dezimalschreibweise mit Punkten eingeben. Beachten Sie, dass auch eine ungültige IP-Adresskonfiguration zulässig ist, zum Beispiel 0.0.0.0. Normalerweise fügt ein ACE mit einer ungültigen IP-Adresse explizit eine „Deny“-Aktion hinzu.	0.0.0.0

Ziel-IP-Maske

Einstellung	Beschreibung	Werkseinstellung
IP-Adresse	Wenn für den Ziel-IP-Filter **„Netzwerk“** ausgewählt ist, können Sie eine bestimmte Ziel-IP-Maske in Dezimalschreibweise mit Punkten eingeben.	255.255.255.0

ARP-Absender-MAC-Übereinstimmung

Legen Sie fest, ob Frames entsprechend den Einstellungen ihres Sender-Hardware-Adressfelds (SHA) die Aktion auslösen können.

Einstellung	Beschreibung	Werkseinstellung
0	ARP-Frames, bei denen die SHA nicht mit der SMAC-Adresse übereinstimmt.	Beliebig
1	ARP-Frames, bei denen SHA mit der SMAC-Adresse übereinstimmt.	
Beliebig	Jeder Wert ist zulässig.	

RARP-Ziel-MAC-Übereinstimmung

Geben Sie an, ob Frames entsprechend den Einstellungen ihres Ziel-Hardware-Adressfelds (THA) die Aktion auslösen können.

Einstellung	Beschreibung	Werkseinstellung
0	RARP-Frames, bei denen das THA-Feld nicht mit der Ziel-MAC-Adresse übereinstimmt.	Beliebig
1	RARP-Frames, bei denen THA mit der Ziel-MAC-Adresse übereinstimmt.	
Beliebig	Jeder Wert ist zulässig.	

IP/Ethernet-Länge

Geben Sie an, ob Frames entsprechend den Einstellungen für die ARP/RARP-Hardwareadresslänge (HLN) und die Protokolladresslänge (PLN) die Aktion auslösen können.

Einstellung	Beschreibung	Werkseinstellung
0	ARP/RARP-Frames, bei denen die HLN nicht mit Ethernet (0x06) übereinstimmt oder die PLN nicht mit IPv4 (0x04) übereinstimmt.	Beliebig

1	ARP-/RARP-Frames, bei denen die HLN mit Ethernet (0x06) übereinstimmt und die PLN mit IPv4 (0x04) übereinstimmt.	
Beliebig	Jeder Wert ist zulässig.	

IP
Legen Sie fest, ob Frames die Aktion entsprechend ihren ARP/RARP-Hardwareadressraum-Einstellungen (HRD) auslösen können.

Einstellung	Beschreibung	Werkseinstellung
0	ARP/RARP-Frames, bei denen der HLD nicht mit Ethernet (1) übereinstimmt.	Beliebig
1	ARP-/RARP-Frames, bei denen der HLD-Wert „Ethernet“ (1) entspricht.	
Beliebig	Jeder Wert ist zulässig.	

Ethernet
Geben Sie an, ob Frames entsprechend ihren Einstellungen für den ARP/RARP-Protokolladressraum (PRO) die Aktion auslösen können.

Einstellung	Beschreibung	Werkseinstellung
0	ARP/RARP-Frames, bei denen der PRO nicht mit IP (0x800) übereinstimmt.	Beliebig
1	ARP-/RARP-Frames, bei denen der PRO-Wert gleich IP (0x800) ist.	
Beliebig	Jeder Wert ist zulässig.	

IP-Parameter

Die IP-Parameter können konfiguriert werden, wenn der Rahmentyp „IPv4“ ausgewählt ist.
IP-Protokollfilter

Einstellung	Beschreibung	Werkseinstellung
Beliebig	Es ist kein IP-Protokollfilter festgelegt	Beliebig
Sonstiges	Wenn Sie mit dieser ACE einen bestimmten IP-Protokollfilter anwenden möchten, wählen Sie diesen Wert aus. Es erscheint ein Feld zur Eingabe eines IP-Protokollfilters.	
ICMP	Wählen Sie „ICMP“ aus, um IPv4-ICMP-Protokoll-Frames zu filtern. Es werden zusätzliche Felder zur Definition von ICMP-Parametern angezeigt. Diese Felder werden später in dieser Hilfedatei erläutert.	
UDP	Wählen Sie „UDP“ aus, um IPv4-UDP-Protokoll-Frames zu filtern. Es werden zusätzliche Felder zur Definition von UDP-Parametern angezeigt. Diese Felder werden später in dieser Hilfedatei erläutert.	
TCP	Wählen Sie „TCP“ aus, um IPv4-TCP-Protokoll-Frames zu filtern. Es werden zusätzliche Felder zur Definition von TCP-Parametern angezeigt. Diese Felder werden später in dieser Hilfedatei erläutert.	

IP-Protokollwert

Einstellung	Beschreibung	Werkseinstellung

0–255	Wenn für den IP-Protokollwert **„Andere“** ausgewählt ist, können Sie einen bestimmten Wert eingeben. Der zulässige Bereich liegt zwischen 0 und 255. Ein Frame, der auf diese ACE trifft, entspricht diesem IP-Protokollwert.	255

IP-TTL
Legen Sie die Time-to-Live-Einstellungen für diese ACE fest.

Einstellung	Beschreibung	Werkseinstellung
Null	IPv4-Frames mit einem Time-to-Live-Feld größer als Null dürfen nicht mit diesem Eintrag übereinstimmen.	Jeder
IPv4-Frames, deren	IPv4-Frames mit einem Time-to-Live-Feld größer als Null müssen mit diesem Eintrag übereinstimmen können.	
Jeder	Beliebiger Wert ist zulässig.	

IP-Fragment
Geben Sie die Fragment-Offset-Einstellungen für diese ACE an. Dazu gehören die Einstellungen für das „More Fragments“ (MF)-Bit und das Feld „Fragment Offset“ (FRAG OFFSET) eines IPv4-Frames.

Einstellung	Beschreibung	Werkseinstellung
Nein	IPv4-Frames, bei denen das MF-Bit gesetzt ist oder das Feld „FRAG OFFSET“ größer als Null ist, dürfen nicht mit diesem Eintrag übereinstimmen.	Beliebig
Ja	IPv4-Frames, bei denen das MF-Bit gesetzt ist oder das Feld „FRAG OFFSET“ größer als Null ist, müssen mit diesem Eintrag übereinstimmen können.	
Beliebig	Jeder Wert ist zulässig.	

IP-Option
Geben Sie die Einstellung des Optionsflags für diese ACE an.

Einstellung	Beschreibung	Werkseinstellung
Nein	IPv4-Frames, bei denen das Options-Flag gesetzt ist, dürfen nicht mit diesem Eintrag übereinstimmen.	Beliebig
Ja	IPv4-Frames, bei denen das Options-Flag gesetzt ist, müssen mit diesem Eintrag übereinstimmen können.	
Beliebiger	Jeder Wert ist zulässig.	

SIP-Filter
Geben Sie den Quell-IP-Filter für diese ACE an.

Einstellung	Beschreibung	Werkseinstellung
Beliebig	Es ist kein Quell-IP-Filter angegeben.	Beliebig
Host	Der Quell-IP-Filter ist auf „Host“ eingestellt. Geben Sie die Quell-IP-Adresse in das angezeigte Feld „SIP-Adresse“ ein.	
Netzwerk	Der Quell-IP-Filter ist auf „Netzwerk“ eingestellt. Geben Sie die Quell-IP-Adresse und die Quell-IP-Maske in die angezeigten Felder „SIP-Adresse“ und „SIP-Maske“ ein.	

SIP-Adresse

Einstellung	Beschreibung	Werkseinstellung
IP-Adresse	Wenn für den Quell-IP-Filter **„Host“** oder **„Netzwerk“** ausgewählt ist, können Sie eine bestimmte SIP-Adresse in Dezimalschreibweise mit Punkten eingeben. Beachten Sie, dass auch eine ungültige IP-Adresskonfiguration zulässig ist, zum Beispiel 0.0.0.0. Normalerweise fügt ein ACE mit einer ungültigen IP-Adresse explizit eine „Deny“-Aktion hinzu.	0.0.0.0

SIP-Maske

Einstellung	Beschreibung	Werkseinstellung
IP-Adresse	Wenn für den Quell-IP-Filter **„Netzwerk“** ausgewählt ist, können Sie eine bestimmte SIP-Maske in Dezimalschreibweise mit Punkten eingeben.	255.255.255.0

DIP-Filter

Geben Sie den Ziel-IP-Filter für diese ACE an.

Einstellung	Beschreibung	Werkseinstellung
Beliebig	Es ist kein Quell-IP-Filter angegeben.	Beliebig
Host	Der Quell-IP-Filter ist auf „Host“ eingestellt. Geben Sie die Quell-IP-Adresse in das angezeigte Feld „SIP-Adresse“ ein.	
Netzwerk	Der Quell-IP-Filter ist auf „Netzwerk“ eingestellt. Geben Sie die Quell-IP-Adresse und die Quell-IP-Maske in die angezeigten Felder „SIP-Adresse“ und „SIP-Maske“ ein.	

DIP-Adresse

Einstellung	Beschreibung	Werkseinstellung
IP-Adresse	Wenn für den Ziel-IP-Filter **„Host“** oder **„Netzwerk“** ausgewählt ist, können Sie eine bestimmte DIP-Adresse in Dezimalschreibweise mit Punkten eingeben. Beachten Sie, dass auch eine ungültige IP-Adresskonfiguration zulässig ist, zum Beispiel 0.0.0.0. Normalerweise fügt ein ACE mit einer ungültigen IP-Adresse explizit eine Verweigerungsaktion hinzu.	0.0.0.0

IP-Maske

Einstellung	Beschreibung	Werkseinstellung
IP-Adresse	Wenn für den Ziel-IP-Filter **„Netzwerk“** ausgewählt ist, können Sie eine bestimmte DIP-Maske in Dezimalschreibweise mit Punkten eingeben.	255.255.255.0

IPv6-Parameter

Die IP-Parameter können konfiguriert werden, wenn als Frame-Typ **„IPv6“** ausgewählt ist.

Nächster Header-Filter

Einstellung	Beschreibung	Werkseinstellung
Beliebig	Es ist kein IPv6-Next-Header-Filter angegeben.	Beliebig
Sonstiges	Wenn Sie mit dieser ACE einen bestimmten IPv6-Next-Header-Filter anwenden möchten, wählen Sie diesen Wert aus. Es erscheint ein Feld zur Eingabe eines IPv6-Next-Header-Filters.	
ICMP	Wählen Sie „ICMP“ aus, um IPv6-ICMP-Protokoll-Frames zu filtern. Es werden zusätzliche Felder zur Definition von ICMP-Parametern angezeigt. Diese Felder werden später in dieser Hilfedatei erläutert.	
UDP	Wählen Sie „UDP“ aus, um IPv6-UDP-Protokollframes zu filtern. Es werden zusätzliche Felder zur Definition von UDP-Parametern angezeigt. Diese Felder werden später in dieser Hilfedatei erläutert.	
TCP	Wählen Sie „TCP“ aus, um IPv6-TCP-Protokollrahmen zu filtern. Es werden zusätzliche Felder zur Definition von TCP-Parametern angezeigt. Diese Felder werden später in dieser Hilfe-Datei erläutert.	

Nächster Kopfzeilenwert

Einstellung	Beschreibung	Werkseinstellung
0–255	Wenn für den IPv6-Wert des nächsten Headers **„Andere“** ausgewählt ist, können Sie einen bestimmten Wert eingeben. Der zulässige Bereich liegt zwischen 0 und 255. Ein Frame, der auf diese ACE trifft, entspricht diesem IPv6-Protokollwert.	255

SIP-Filter

Geben Sie den IPv6-Quellfilter für diese ACE an.

Einstellung	Beschreibung	Werkseinstellung
Beliebig	Es ist kein IPv6-Quellfilter angegeben.	Beliebig
Spezifisch	Der IPv6-Quellfilter ist auf „Netzwerk“ eingestellt. Geben Sie die IPv6-Quelladresse und die IPv6-Quellmaske in die angezeigten SIP-Adressfelder ein.	

SIP-Adresse

Einstellung	Beschreibung	Werkseinstellung
IPv6-Adresse	Wenn für den IPv6-Quellfilter **die Option „Spezifisch“** ausgewählt ist, können Sie eine bestimmte SIPv6-Adresse eingeben. Das Feld unterstützt nur die letzten 32 Bits der IPv6-Adresse.	::

SIP-Bitmaske

Einstellung	Beschreibung	Werkseinstellung
IPv6-Adresse	Wenn für den IPv6-Quellfilter **die Option „Spezifisch“** ausgewählt ist, können Sie eine bestimmte SIPv6-	0xFFFFFFFF

	Maske eingeben. Das Feld unterstützt nur die letzten 32 Bits der IPv6-Adresse.	

Hop-Limit

Einstellung	Beschreibung	Werkseinstellung
0	IPv6-Frames mit einem Hop-Limit-Feld größer als Null dürfen nicht mit diesem Eintrag übereinstimmen.	Beliebig
1	IPv6-Frames mit einem Hop-Limit-Feld größer als Null müssen mit diesem Eintrag übereinstimmen können.	
Beliebig	Jeder Wert ist zulässig.	

ICMP-Parameter

ICMP-Typ-Filter

Einstellung	Beschreibung	Werkseinstellung
Beliebig	Es ist kein ICMP-Filter festgelegt.	Beliebig
Spezifisch	Wenn Sie mit dieser ACE einen bestimmten ICMP-Filter anwenden möchten, können Sie einen bestimmten ICMP-Wert eingeben. Es erscheint ein Feld zur Eingabe eines ICMP-Werts.	

ICMP-Typ Wert

Einstellung	Beschreibung	Werkseinstellung
0–255	Wenn für den ICMP-Filter die **Option „Spezifisch“** ausgewählt ist, können Sie einen bestimmten ICMP-Wert eingeben. Der zulässige Bereich liegt zwischen 0 und 255. Ein Frame, der auf diese ACE trifft, entspricht diesem ICMP-Wert.	255

ICMP-Code-Filter

Einstellung	Beschreibung	Werkseinstellung
Beliebig	Es ist kein ICMP-Code-Filter angegeben	Beliebig
Spezifisch	Wenn Sie mit dieser ACE einen bestimmten ICMP-Code filtern möchten, können Sie einen bestimmten ICMP-Code-Wert eingeben. Es erscheint ein Feld zur Eingabe eines ICMP-Code-Werts.	

ICMP-Code-Wert

Einstellung	Beschreibung	Werkseinstellung
0–255	Wenn für den ICMP-Code-Filter **die Option „Spezifisch“** ausgewählt ist, können Sie einen bestimmten ICMP-Code-Wert eingeben. Der zulässige Bereich liegt zwischen 0 und	255

	255. Ein Frame, der auf diese ACE trifft, stimmt mit diesem ICMP-Code-Wert überein.	

TCP/UDP-Parameter

TCP/UDP-Quellfilter

Einstellung	Beschreibung	Werkseinstellung
Beliebig	Es wurde kein TCP/UDP-Quellfilter angegeben	Beliebig
Bestimmt	Wenn Sie mit dieser ACE einen bestimmten TCP/UDP-Quellfilter filtern möchten, können Sie einen bestimmten TCP/UDP-Quellwert eingeben. Es erscheint ein Feld zur Eingabe eines TCP/UDP-Quellwerts.	
Bereich	Wenn Sie mit dieser ACE einen bestimmten TCP/UDP-Quellbereich filtern möchten, können Sie einen bestimmten TCP/UDP-Quellbereich eingeben. Es erscheint ein Feld zur Eingabe eines TCP/UDP-Quellbereichs.	

TCP/UDP-Quellnummer

Einstellung	Beschreibung	Werkseinstellung
0 bis 65535	Wenn für den TCP/UDP-Quellfilter **die Option „Spezifisch“** ausgewählt ist, können Sie einen bestimmten TCP/UDP-Quellwert eingeben. Der zulässige Bereich liegt zwischen 0 und 65535. Ein Frame, der auf diese ACE trifft, stimmt mit diesem TCP/UDP-Quellwert überein.	0

TCP/UDP-Quellbereich

Einstellung	Beschreibung	Werkseinstellung
0 bis 65535	Wenn für den TCP/UDP-Quellfilter die Option „Bereich“ ausgewählt ist, können Sie einen bestimmten Wert für den TCP/UDP-Quellbereich eingeben. Der zulässige Bereich liegt zwischen 0 und 65535. Ein Frame, der auf diese ACE trifft, entspricht diesem TCP/UDP-Quellwert.	0–65535

TCP/UDP-Zielportfilter

Einstellung	Beschreibung	Werkseinstellung
Beliebig	Es ist kein TCP/UDP-Zielportfilter festgelegt	Beliebig
Spezifisch	Wenn Sie mit dieser ACE einen bestimmten TCP/UDP-Zielfilter anwenden möchten, können Sie einen bestimmten TCP/UDP-Zielwert eingeben. Es erscheint ein Feld zur Eingabe eines TCP/UDP-Zielwerts.	

Bereich	Wenn Sie mit dieser ACE einen bestimmten TCP/UDP-Zielbereich filtern möchten, können Sie einen bestimmten TCP/UDP-Zielbereich eingeben. Es erscheint ein Feld zur Eingabe eines TCP/UDP-Zielbereichs.	

TCP/UDP-Zielportnummer

Einstellung	Beschreibung	Werkseinstellung
0 bis 65535	Wenn für den TCP/UDP-Zielfilter **die Option „Spezifisch“** ausgewählt ist, können Sie einen bestimmten TCP/UDP-Zielwert eingeben. Der zulässige Bereich liegt zwischen 0 und 65535. Ein Frame, der auf diese ACE trifft, stimmt mit diesem TCP/UDP-Zielwert überein.	0

TCP/UDP-Zielbereich

Einstellung	Beschreibung	Werkseinstellung
0 bis 65535	Wenn für den TCP/UDP-Zielfilter die Option „Bereich“ ausgewählt ist, können Sie einen bestimmten Wert für den TCP/UDP-Zielbereich eingeben. Der zulässige Bereich liegt zwischen 0 und 65535. Ein Frame, der auf diese ACE trifft, stimmt mit diesem TCP/UDP-Zielwert überein.	0–65535

TCP FIN

Geben Sie den TCP-Wert „Keine weiteren Daten vom Absender“ (FIN) für diese ACE an.

Einstellung	Beschreibung	Werkseinstellung
0	TCP-Frames, bei denen das FIN-Feld gesetzt ist, dürfen nicht mit diesem Eintrag übereinstimmen.	Beliebig
1	TCP-Frames, bei denen das FIN-Feld gesetzt ist, müssen mit diesem Eintrag übereinstimmen können.	
Beliebig	Beliebiger Wert ist zulässig.	

TCP SYN

Geben Sie den TCP-Wert „Sequenznummern synchronisieren“ (SYN) für diese ACE an.

Einstellung	Beschreibung	Werkseinstellung
0	TCP-Frames, bei denen das SYN-Feld gesetzt ist, dürfen nicht mit diesem Eintrag übereinstimmen.	Beliebig
1	TCP-Frames, bei denen das SYN-Feld gesetzt ist, müssen mit diesem Eintrag übereinstimmen können.	
Beliebig	Beliebiger Wert ist zulässig.	

TCP RST

Geben Sie den TCP-Wert „Verbindung zurücksetzen“ (RST) für diese ACE an.

Einstellung	Beschreibung	Werkseinstellung
0	TCP-Frames, bei denen das RST-Feld gesetzt ist, dürfen nicht mit diesem Eintrag übereinstimmen.	Beliebig
1	TCP-Frames, bei denen das RST-Feld gesetzt ist, müssen mit diesem Eintrag übereinstimmen können.	
Beliebig	Beliebiger Wert ist zulässig.	

TCP PSH

Geben Sie den Wert für die TCP-„Push-Funktion“ (PSH) für diese ACE an.

Einstellung	Beschreibung	Werkseinstellung
0	TCP-Frames, bei denen das PSH-Feld gesetzt ist, dürfen nicht mit diesem Eintrag übereinstimmen.	Jeder
1	TCP-Frames, bei denen das PSH-Feld gesetzt ist, muss mit diesem Eintrag übereinstimmen können.	
Beliebig	Beliebiger Wert ist zulässig.	

TCP ACK

Geben Sie den TCP-Wert für „Acknowledgment field significant“ (ACK) für diese ACE an.

Einstellung	Beschreibung	Werkseinstellung
0	TCP-Frames, bei denen das ACK-Feld gesetzt ist, dürfen nicht mit diesem Eintrag übereinstimmen.	Beliebig
1	TCP-Frames, bei denen das ACK-Feld gesetzt ist, müssen mit diesem Eintrag übereinstimmen können.	
Beliebig	Jeder Wert ist zulässig.	

TCP URG

Geben Sie den TCP-Wert für „Urgent Pointer field significant“ (URG) für diese ACE an.

Einstellung	Beschreibung	Werkseinstellung
0	TCP-Frames, bei denen das URG-Feld gesetzt ist, dürfen nicht mit diesem Eintrag übereinstimmen.	Beliebig
1	TCP-Frames, bei denen das URG-Feld gesetzt ist, müssen mit diesem Eintrag übereinstimmen können.	
Beliebig	Beliebiger Wert ist zulässig.	

Ethernet-Typ-Parameter

Die Ethernet-Typ-Parameter können konfiguriert werden, wenn als Rahmentyp „Ethernet-Typ“ ausgewählt ist.

EtherType-Filter

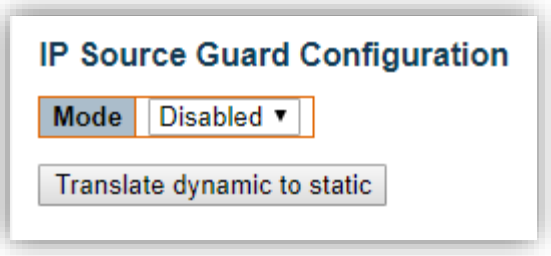
Einstellung	Beschreibung	Werkseinstellung
Beliebig	Es ist kein EtherType-Filter angegeben	Beliebig
Spezifisch	Wenn Sie mit dieser ACE nach einem bestimmten EtherType filtern möchten, können Sie einen bestimmten EtherType-Wert eingeben. Es erscheint ein Feld zur Eingabe eines EtherType-Werts.	

Ethernet-Typ-Wert

Einstellung	Beschreibung	Werkseinstellung
0x600 ~ 0xFFFF ausgenommen 0x800, 0x806, 0x86DD	Wenn für den EtherType-Filter **„Spezifisch“** ausgewählt ist, können Sie einen bestimmten EtherType-Wert eingeben. Der zulässige Bereich liegt zwischen 0x600 und 0xFFFF, wobei jedoch 0x800 (IPv4), 0x806 (ARP) und 0x86DD (IPv6) ausgeschlossen sind. Ein Frame, der auf diese ACE trifft, stimmt mit diesem EtherType-Wert überein.	0xFFFF

Konfiguration > Sicherheit > Netzwerk > IP-Source-Guard > Konfiguration

IP-Source-Guard-Konfiguration

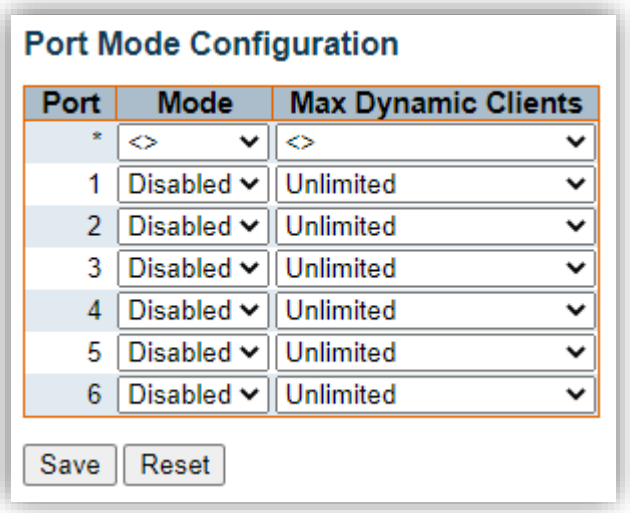


Modus

Einstellung	Beschreibung	Werkseinstellung
Aktiviert	Aktivieren Sie den Global IP Source Guard. Alle konfigurierten ACEs gehen verloren, wenn der Modus aktiviert wird.	Deaktiviert
Deaktiviert	Deaktivieren Sie den globalen IP-Source-Guard.	

Schaltfläche „Dynamisch in statisch umwandeln“
Klicken Sie hier, um alle dynamischen Einträge in statische Einträge umzuwandeln.

Konfiguration des Port-Modus



Modus

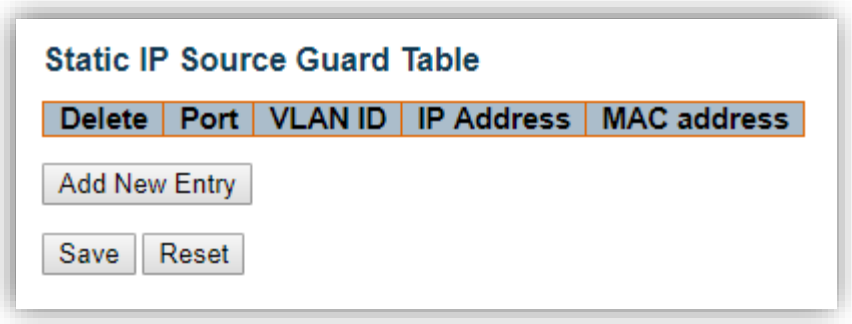
Einstellung	Beschreibung	Werkseinstellung
Aktiviert	Der Port-Modus ist aktiviert	Deaktiviert
Deaktiviert	Der Port-Modus ist deaktiviert	

Max. dynamische Clients

Einstellung	Beschreibung	Werkseinstellung
0, 1, 2, Unbegrenzt	Geben Sie die maximale Anzahl dynamischer Clients an, die an einem bestimmten Port erkannt werden können. Dieser Wert kann 0, 1, 2 oder „unbegrenzt“ betragen. Wenn der Port-Modus aktiviert ist und der Wert für „Max. dynamische Clients“ gleich 0 ist, bedeutet dies, dass nur die Weiterleitung von IP-Paketen erlaubt ist, die mit statischen Einträgen an diesem bestimmten Port übereinstimmen.	Unbegrenzt

Konfiguration > Sicherheit > Netzwerk > IP-Quellschutz > Statische Tabelle

Statische IP-Source-Guard-Tabelle

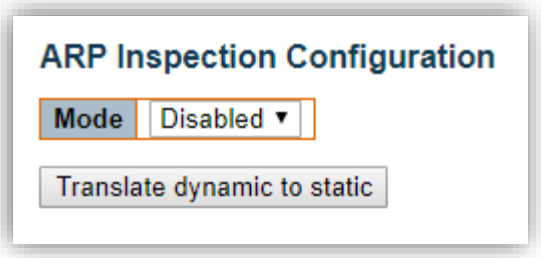


Neuen Eintrag hinzufügen

Einstellung	Beschreibung
Löschen	Aktivieren Sie dieses Kontrollkästchen, um den Eintrag zu löschen. Er wird beim nächsten Speichern gelöscht.
Port	Der logische Port für die Einstellungen.
VLAN-ID	Die VLAN-ID für die Einstellungen.
IP-Adresse	Zulässige Quell-IP-Adresse.
MAC-Adresse	Zulässige Quell-MAC-Adresse.

Konfiguration > Sicherheit > Netzwerk > ARP-Prüfung > Port-Konfiguration

Konfiguration der ARP-Prüfung



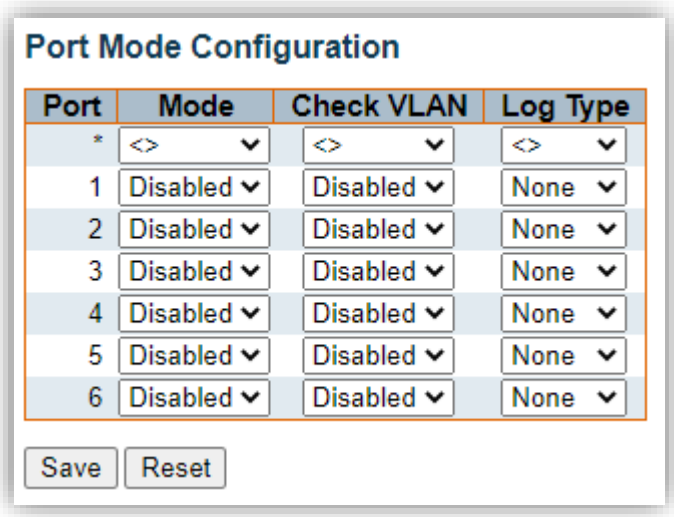
Modus

Einstellung	Beschreibung	Werkseinstellung
Aktiviert	Globale ARP-Prüfung aktivieren	Deaktiviert
Deaktiviert	Globale ARP-Prüfung deaktivieren	

Schaltfläche „Dynamische in statische umwandeln“
Klicken Sie hier, um alle dynamischen Einträge in statische Einträge umzuwandeln.

Konfiguration des Port-Modus

Legen Sie fest, auf welchen Ports die ARP-Prüfung aktiviert ist. Nur wenn sowohl der globale Modus als auch der Port-Modus auf einem bestimmten Port aktiviert sind, ist die ARP-Prüfung auf diesem Port aktiviert.



Modus

Einstellung	Beschreibung	Werkseinstellung
Aktiviert	ARP-Prüfung aktivieren.	Deaktiviert
Deaktiviert	Deaktivieren Sie die ARP-Prüfung.	

VLAN prüfen

Wenn Sie die VLAN-Konfiguration überprüfen möchten, müssen Sie die Einstellung „VLAN prüfen“ aktivieren. Die Standardeinstellung für „VLAN prüfen“ ist deaktiviert. Wenn die Einstellung „VLAN prüfen“ deaktiviert ist, bezieht sich der Protokolltyp der ARP-Prüfung auf die Port-Einstellung. Ist die Einstellung „VLAN prüfen“ aktiviert, bezieht sich der Protokolltyp der ARP-Prüfung auf die VLAN-Einstellung.

Einstellung	Beschreibung	Werkseinstellung
Aktiviert	Aktiviert die VLAN-Prüfung.	Deaktiviert
Deaktiviert	VLAN-Prüfung deaktivieren.	

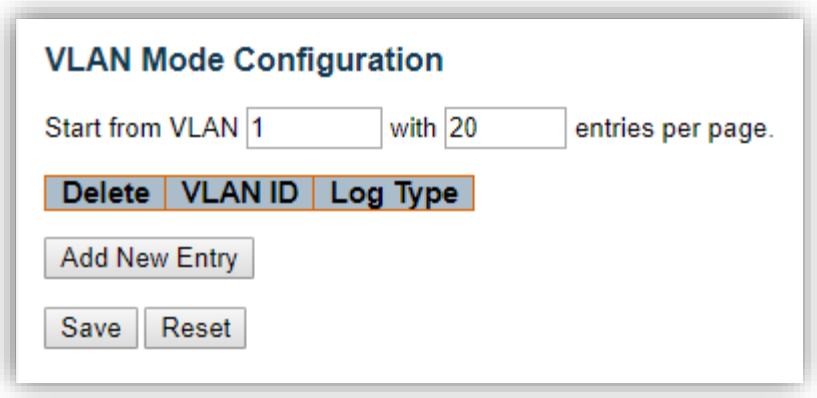
Protokolltyp

Sind an einem bestimmten Port nur der globale Modus und der Port-Modus aktiviert und ist die Einstellung „VLAN-Prüfung“ deaktiviert, bezieht sich der Protokolltyp der ARP-Prüfung auf die Port-Einstellung.

Einstellung	Beschreibung	Werkseinstellung
Keine	Nichts protokollieren.	Keine
Ablehnen	Verweigerte Einträge protokollieren.	
Zulassen	Zulässige Einträge protokollieren.	
ALLE	Alle Einträge protokollieren.	

Konfiguration > Sicherheit > Netzwerk > ARP-Prüfung > VLAN-Konfiguration

Konfiguration des VLAN-Modus



Navigation in der VLAN-Konfiguration
Jede Seite zeigt bis zu 9999 Einträge aus der VLAN-Tabelle an, wobei die Standardeinstellung 20 beträgt und über das Eingabefeld „Einträge pro Seite“ ausgewählt werden kann. Beim ersten Aufruf der Webseite werden die ersten 20 Einträge vom Anfang der VLAN-Tabelle angezeigt. Als erster wird der Eintrag mit der niedrigsten VLAN-ID aus der VLAN-Tabelle angezeigt.

Konfiguration des VLAN-Modus
Legen Sie fest, auf welchen VLANs die ARP-Prüfung aktiviert ist. Zunächst müssen Sie die Port-Einstellung auf der Webseite zur Konfiguration des Port-Modus aktivieren. Nur wenn sowohl der globale Modus als auch der Port-Modus für einen bestimmten Port aktiviert sind, ist die ARP-Prüfung auf diesem Port aktiviert. Anschließend können Sie auf der Webseite zur Konfiguration des VLAN-Modus festlegen, welche VLANs geprüft werden sollen. Der Protokolltyp kann ebenfalls pro VLAN konfiguriert werden.
Mögliche Typen sind:

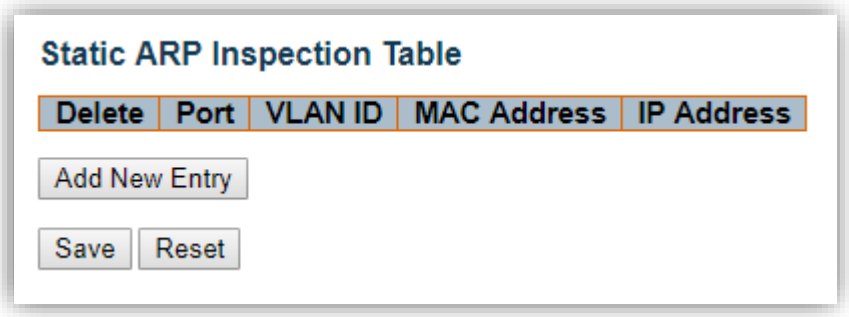
- **Keine:** Es wird nichts protokolliert.
- **„Deny“:** Verweigerte Einträge protokollieren.
- **Zulassen:** Zulässige Einträge protokollieren.
- **ALL:** Alle Einträge protokollieren.

Schaltfläche „Neuen Eintrag hinzufügen“
Klicken Sie hier, um ein neues VLAN zur ARP-Inspektions-VLAN-Tabelle hinzuzufügen.

Konfiguration > Sicherheit > Netzwerk > ARP-Prüfung > Statische Tabelle

Statische ARP-Prüfungstabelle

Auf dieser Seite werden die statischen ARP-Prüfungsregeln angezeigt. Die maximale Anzahl an Regeln beträgt **256** auf dem Switch.



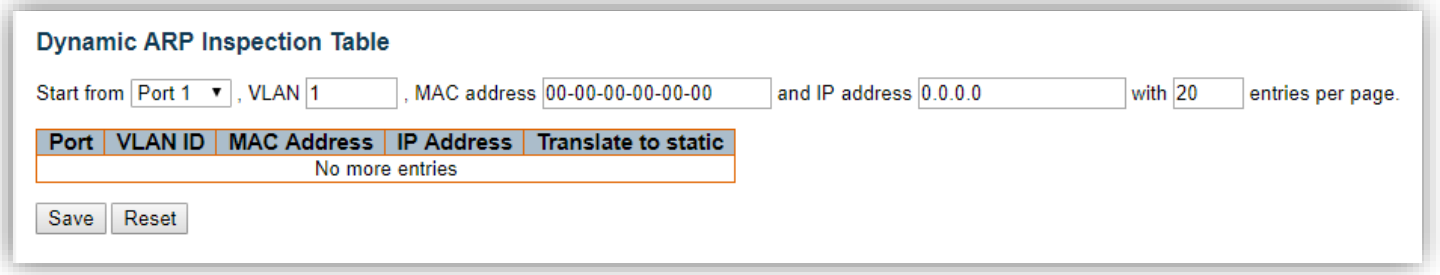
Neuen Eintrag hinzufügen

Einstellung	Beschreibung
Löschen	Aktivieren Sie dieses Kontrollkästchen, um den Eintrag zu löschen. Er wird beim nächsten Speichern gelöscht.
Port	Der logische Port für die Einstellungen.
VLAN-ID	Die VLAN-ID für die Einstellungen.
MAC-Adresse	Zulässige Quell-MAC-Adresse in ARP-Anfragepaketen.
IP-Adresse	Zulässige Quell-IP-Adresse in ARP-Anfragepaketen.

Konfiguration > Sicherheit > Netzwerk > ARP-Prüfung > Dynamische Tabelle

Dynamische ARP-Prüfungstabelle

Auf dieser Seite werden die Einträge in der dynamischen ARP-Prüfungstabelle angezeigt. Die dynamische ARP-Prüfungstabelle enthält bis zu 256 Einträge und ist zunächst nach Port, dann nach VLAN-ID, anschließend nach MAC-Adresse und schließlich nach IP-Adresse sortiert. Alle dynamischen Einträge stammen aus dem DHCP-Snooping.



Auf jeder Seite werden bis zu 99 Einträge aus der dynamischen ARP-Prüfungstabelle angezeigt, wobei die Standardeinstellung 20 beträgt und über das Eingabefeld „Einträge pro Seite“ ausgewählt werden kann. Beim ersten Aufruf der Webseite werden die ersten 20 Einträge vom Anfang der dynamischen ARP-Prüfungstabelle angezeigt.
Über die Eingabefelder „Ab Port-Adresse beginnen“, „VLAN“, „MAC-Adresse“ und „IP-Adresse“ kann der Benutzer den Startpunkt in der Dynamic-ARP-Inspection-Tabelle auswählen.

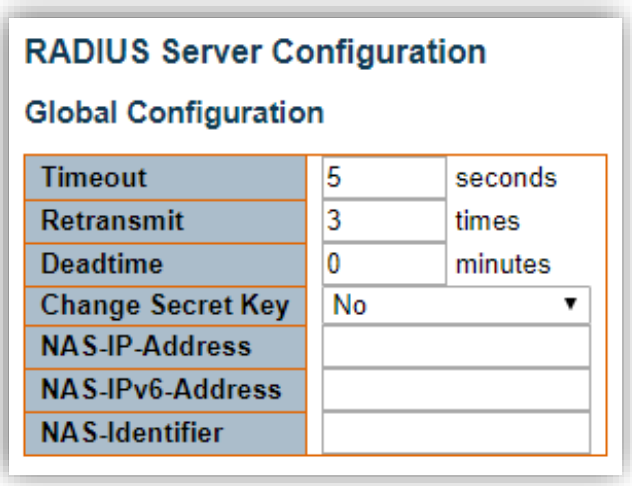
Spalten der ARP-Inspektions-Tabelle

Element	Beschreibung
Port	Switch-Port-Nummer, für die die Einträge angezeigt werden.
VLAN-ID	VLAN-ID, in der der ARP-Verkehr zugelassen ist.
MAC-Adresse	MAC-Adresse des Benutzers für diesen Eintrag.
IP-Adresse	Benutzer-IP-Adresse des Eintrags.
In statischen Eintrag umwandeln	Aktivieren Sie das Kontrollkästchen, um den Eintrag in einen statischen Eintrag umzuwandeln.

Konfiguration > Sicherheit > AAA > RADIUS

RADIUS-Server-Konfiguration

Globale Konfiguration

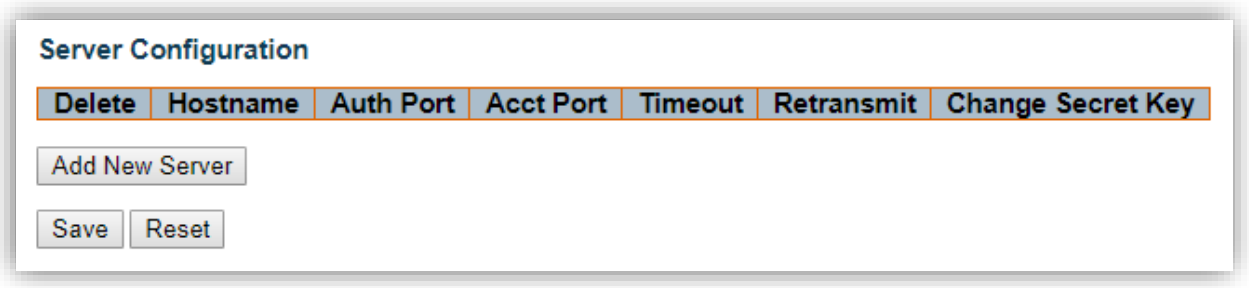


Einstellung	Beschreibung	Werkseinstellung
Zeitlimit	Das Timeout ist die Anzahl der Sekunden im Bereich von 1 bis 1000, die auf eine Antwort vom RADIUS-Server gewartet wird, bevor die Anfrage erneut gesendet wird.	5
Wiederholung	Die Wiederholungsanzahl gibt an, wie oft (im Bereich von 1 bis 1000) eine RADIUS-Anfrage an einen Server, der nicht antwortet, erneut gesendet wird. Wenn der Server nach der letzten Wiederholung nicht geantwortet hat, gilt er als ausgefallen.	3
Deadtime	Die Deadtime, die auf einen Wert zwischen 0 und 1440 Minuten eingestellt werden kann, ist der Zeitraum, in dem der Switch keine neuen Anfragen an einen Server sendet, der auf eine vorherige Anfrage nicht geantwortet hat. Dadurch wird verhindert, dass der Switch weiterhin versucht, einen Server zu kontaktieren, den er bereits als ausgefallen eingestuft hat. Durch Einstellen der Deadtime auf einen Wert größer als 0 (Null) wird diese Funktion aktiviert, jedoch nur, wenn mehr als ein Server konfiguriert wurde.	0
Geheimschlüssel ändern	Geben Sie an, ob der geheime Schlüssel geändert werden soll oder nicht. Wenn für diese Option „Ja“ ausgewählt ist, können Sie den geheimen Schlüssel – mit einer Länge von bis zu 63 Zeichen – ändern, der zwischen dem RADIUS-Server und dem Switch ausgetauscht wird.	Nein
NAS-IP-Adresse	Die IPv4-Adresse, die als Attribut 4 in RADIUS-Access-Request-Paketen verwendet werden soll. Wenn dieses Feld leer gelassen wird, wird die IP-Adresse der ausgehenden Schnittstelle verwendet.	Keine
NAS-IPv6-Adresse	Die IPv6-Adresse, die als Attribut 95 in RADIUS-Access-Request-Paketen verwendet werden soll. Wenn dieses Feld leer gelassen wird, wird die IP-Adresse der ausgehenden Schnittstelle verwendet.	Keine
NAS-Identifier	Die Kennung – mit einer Länge von bis zu 253 Zeichen –, die als Attribut 32 in RADIUS-Access-Request-Paketen verwendet werden	Keine

	soll. Wenn dieses Feld leer gelassen wird, wird der NAS-Identifier nicht in das Paket aufgenommen.	

Serverkonfiguration

Die Tabelle enthält eine Zeile für jeden RADIUS-Server und mehrere Spalten.



Einstellung	Beschreibung
Löschen	Um einen RADIUS-Server-Eintrag zu löschen, aktivieren Sie dieses Kontrollkästchen. Der Eintrag wird beim nächsten Speichern gelöscht.
Hostname	Die IP-Adresse oder der Hostname des RADIUS-Servers.
Auth-Port	Der UDP-Port, der auf dem RADIUS-Server für die Authentifizierung verwendet werden soll. Setzen Sie den Wert auf 0, um die Authentifizierung zu deaktivieren.
Abrechnungsport	Der UDP-Port, der auf dem RADIUS-Server für die Abrechnung verwendet werden soll. Setzen Sie den Wert auf 0, um die Abrechnung zu deaktivieren.
Zeitlimit	Diese optionale Einstellung überschreibt den globalen Timeout-Wert. Wird das Feld leer gelassen, wird der globale Timeout-Wert verwendet.
Wiederholungsversuche	Diese optionale Einstellung überschreibt den globalen Wert für die Wiederholung. Wird das Feld leer gelassen, wird der globale Wert für die Wiederholung verwendet.
Geheimschlüssel ändern	Geben Sie an, ob der geheime Schlüssel geändert werden soll oder nicht. Wenn das Kontrollkästchen aktiviert ist, können Sie die Einstellung ändern, die den globalen Schlüssel überschreibt. Wenn das Feld leer bleibt, wird der globale Schlüssel verwendet.

Schaltfläche „Neuen Server hinzufügen“

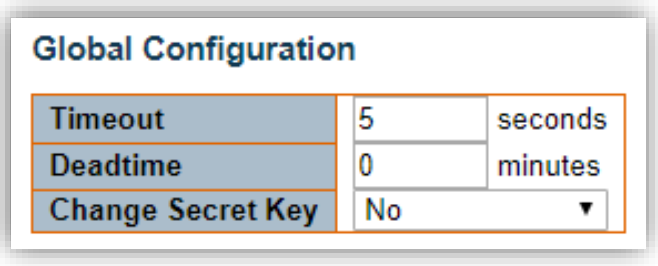
Klicken Sie auf die Schaltfläche „Neuen Server hinzufügen“, um einen neuen RADIUS-Server hinzuzufügen. Der Tabelle wird eine leere Zeile hinzugefügt, und der RADIUS-Server kann nach Bedarf konfiguriert werden. Es werden bis zu 5 Server unterstützt.

Mit der Schaltfläche „Löschen“ können Sie das Hinzufügen des neuen Servers rückgängig machen.

Konfiguration > Sicherheit > AAA > TACACS+

TACACS+-Serverkonfiguration

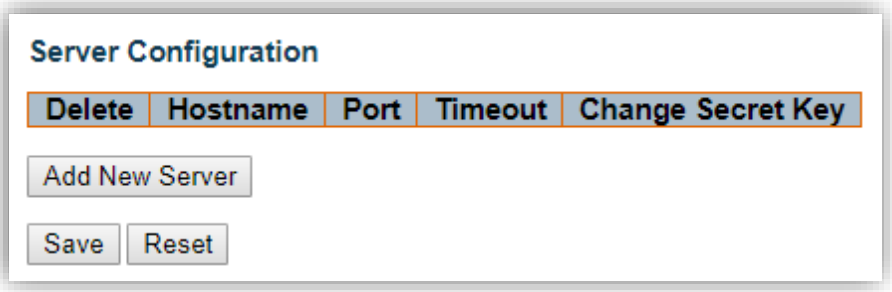
Globale Konfiguration



Einstellung	Beschreibung
Zeitlimit	Das Timeout ist die Anzahl der Sekunden im Bereich von 1 bis 1000, die auf eine Antwort von einem TACACS+-Server gewartet wird, bevor dieser als ausgefallen gilt.
Ausfallzeit	Die Deadtime, die auf einen Wert zwischen 0 und 1440 Minuten eingestellt werden kann, ist der Zeitraum, in dem der Switch keine neuen Anfragen an einen Server sendet, der auf eine vorherige Anfrage nicht geantwortet hat. Dadurch wird verhindert, dass der Switch weiterhin versucht, einen Server zu kontaktieren, den er bereits als ausgefallen identifiziert hat. Durch Einstellen der Deadtime auf einen Wert größer als 0 (Null) wird diese Funktion aktiviert, jedoch nur, wenn mehr als ein Server konfiguriert wurde.
Geheimschlüssel ändern	Geben Sie an, ob der geheime Schlüssel geändert werden soll oder nicht. Wenn für diese Option „Ja“ ausgewählt ist, können Sie den geheimen Schlüssel – mit einer Länge von bis zu 63 Zeichen – ändern, der zwischen dem TACACS+-Server und dem Switch gemeinsam genutzt wird.

Serverkonfiguration

Die Tabelle enthält eine Zeile für jeden TACACS+-Server und mehrere Spalten.



Einstellung	Beschreibung
Löschen	Um einen TACACS+-Server-Eintrag zu löschen, aktivieren Sie dieses Kontrollkästchen. Der Eintrag wird beim nächsten Speichern gelöscht.
Hostname	Die IP-Adresse oder der Hostname des TACACS+-Servers.
Port	Der TCP-Port, der auf dem TACACS+-Server für die Authentifizierung verwendet werden soll.
Zeitlimit	Diese optionale Einstellung überschreibt den globalen Timeout-Wert. Wird das Feld leer gelassen, wird der globale Timeout-Wert verwendet.
Geheimschlüssel ändern	Geben Sie an, ob der geheime Schlüssel geändert werden soll oder nicht. Wenn das Kontrollkästchen aktiviert ist, können Sie die Einstellung ändern, die den globalen Schlüssel überschreibt. Wenn das Feld leer bleibt, wird der globale Schlüssel verwendet.

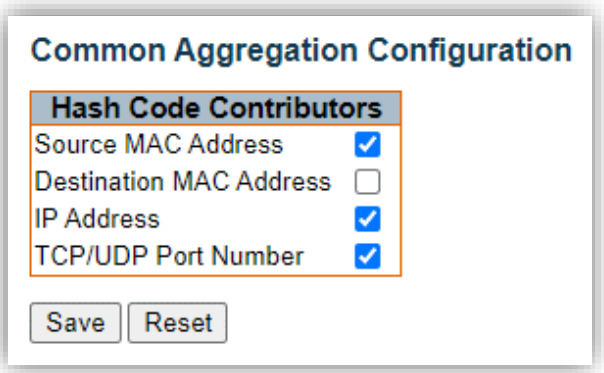
Schaltfläche „Neuen Server hinzufügen“

Klicken Sie auf die Schaltfläche „Neuen Server hinzufügen“, um einen neuen TACACS+-Server hinzuzufügen. Der Tabelle wird eine leere Zeile hinzugefügt, und der TACACS+-Server kann nach Bedarf konfiguriert werden. Es werden bis zu 5 Server unterstützt.

Mit der Schaltfläche „Löschen“ können Sie das Hinzufügen des neuen Servers rückgängig machen.

Konfiguration > Aggregation > Allgemein

Allgemeine Aggregationskonfiguration

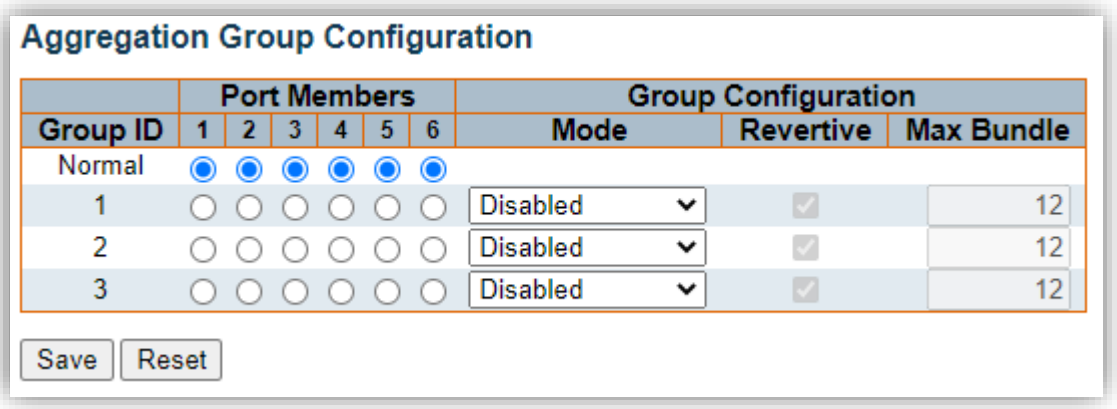


Beiträge zum Hash-Code

Einstellung	Beschreibung	Werkseinstellung
Quell-MAC-Adresse	Die Quell-MAC-Adresse kann zur Berechnung des Zielports für den Frame verwendet werden. Aktivieren Sie das Kontrollkästchen, um die Verwendung der Quell-MAC-Adresse zu aktivieren, oder deaktivieren Sie es, um sie zu deaktivieren.	Aktiviert
Ziel-MAC-Adresse	Die Ziel-MAC-Adresse kann zur Berechnung des Zielports für den Frame verwendet werden. Aktivieren Sie das Kontrollkästchen, um die Verwendung der Ziel-MAC-Adresse zu aktivieren, oder deaktivieren Sie es, um sie zu deaktivieren.	Deaktiviert
IP-Adresse	Die IP-Adresse kann zur Berechnung des Zielports für den Frame verwendet werden. Aktivieren Sie das Kontrollkästchen, um die Verwendung der IP-Adresse zu aktivieren, oder deaktivieren Sie es, um sie zu deaktivieren.	Aktiviert
TCP/UDP-Portnummer	Die TCP/UDP-Portnummer kann zur Berechnung des Zielports für den Frame verwendet werden. Aktivieren Sie das Kontrollkästchen, um die Verwendung der TCP/UDP-Portnummer zu aktivieren, oder deaktivieren Sie es, um sie zu deaktivieren.	Aktiviert

Konfiguration > Aggregation > Gruppen

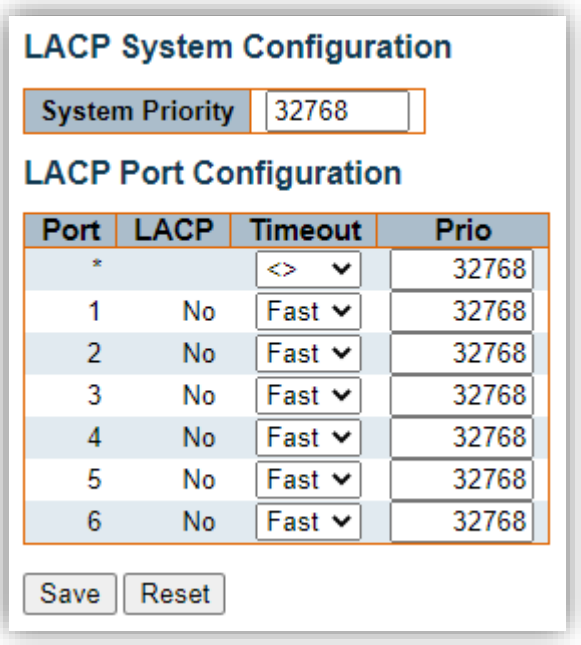
Konfiguration der Aggregationsgruppe



Einstellung	Beschreibung
Gruppen-ID	Gibt die Gruppen-ID für die in derselben Zeile enthaltenen Einstellungen an. Die Gruppen-ID „Normal“ bedeutet, dass keine Aggregation stattfindet. Pro Port ist nur eine Gruppen-ID gültig.
Port-Mitglieder	Für jede Gruppen-ID werden die einzelnen Switch-Ports aufgelistet. Wählen Sie ein Optionsfeld aus, um einen Port in eine Aggregation aufzunehmen, oder deaktivieren Sie das Optionsfeld, um den Port aus der Aggregation zu entfernen. Standardmäßig gehört kein Port zu einer Aggregationsgruppe. Nur Vollduplex-Ports können einer Aggregation beitreten, und die Ports müssen in jeder Gruppe die gleiche Geschwindigkeit aufweisen.
Modus	Dieser Parameter legt den Modus für die Aggregationsgruppe fest. ● **Deaktiviert**: Die Gruppe ist deaktiviert. ● **Statisch**: Die Gruppe arbeitet im statischen Aggregationsmodus. ● **LACP (Aktiv)**: Die Gruppe arbeitet im aktiven LACP-Aggregationsmodus. Weitere Informationen finden Sie in IEEE 801.AX-2014, Abschnitt 6.4.1. ● **LACP (passiv)**: Die Gruppe arbeitet im passiven LACP-Aggregationsmodus. Weitere Informationen finden Sie in IEEE 801.AX-2014, Abschnitt 6.4.1.
Revertive	Dieser Parameter gilt nur für LACP-fähige Gruppen. Er legt fest, ob die Gruppe eine automatische (Neu-)Berechnung der Verbindungen durchführt, sobald Verbindungen mit höherer Priorität verfügbar werden.
Max. Bündel	Dieser Parameter gilt nur für LACP-fähige Gruppen. Er legt die maximale Anzahl aktiver gebündelter LACP-Ports fest, die in einer Aggregation zulässig sind.

Konfiguration > Aggregation > LACP

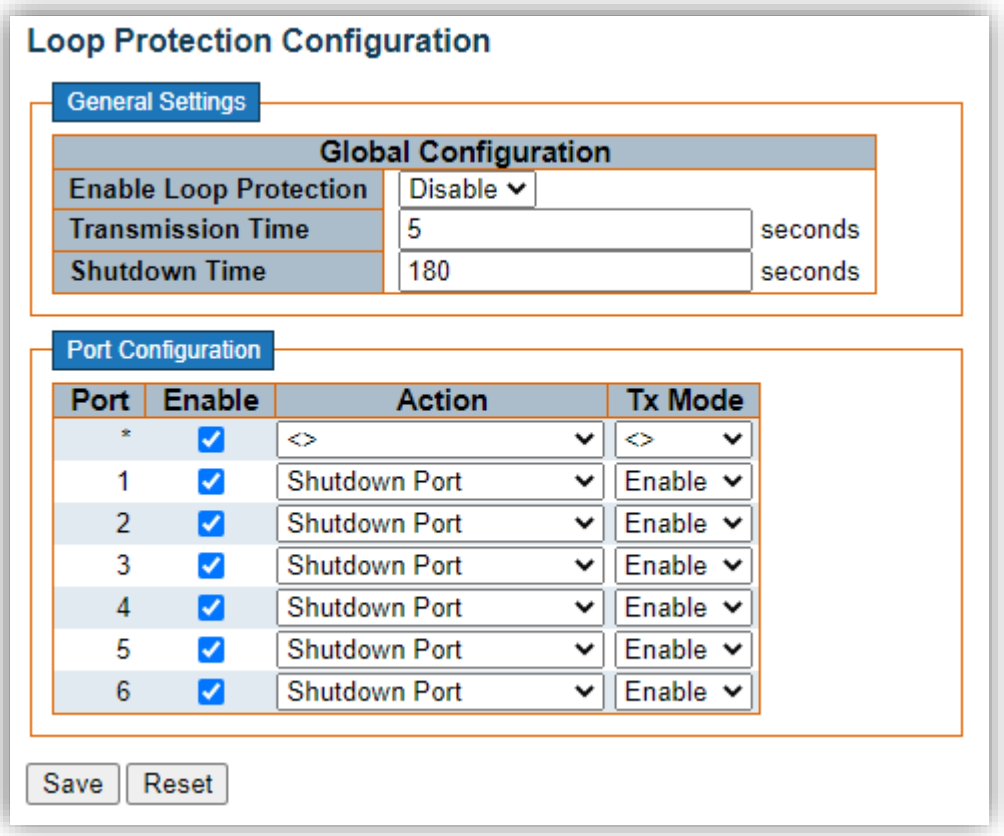
LACP-Port-Konfiguration



Einstellung	Beschreibung
Port	Die Nummer des Switch-Ports.
LACP	Zeigt an, ob LACP derzeit an diesem Switch-Port aktiviert ist.
Timeout	Das **Timeout** steuert den Zeitraum zwischen den BPDU-Übertragungen. Bei der Einstellung **„Fast“** werden LACP-Pakete jede Sekunde gesendet, während bei der Einstellung **„Slow“** 30 Sekunden gewartet wird, bevor ein LACP-Paket gesendet wird.
Prio	**Die Priorität (Prio)** bestimmt die Priorität des Ports im Bereich von 1 bis 65535. Wenn der LACP-Partner eine größere Gruppe bilden möchte, als von diesem Gerät unterstützt wird, legt dieser Parameter fest, welche Ports aktiv sind und welche Ports eine Backup-Rolle übernehmen. Eine niedrigere Zahl bedeutet eine höhere Priorität.

Konfiguration > Schleifenschutz

Konfiguration des Schleifenschutzes



Allgemeine Einstellungen

Einstellung	Beschreibung	Werkseinstellung
Schleifenschutz aktivieren	Legt fest, ob der Schleifenschutz (insgesamt) aktiviert ist.	Deaktiviert
Übertragungszeit	Das Intervall zwischen den einzelnen Loop-Schutz-PDUs, die an jedem Port gesendet werden.	5
Abschaltzeit	Der Zeitraum (in Sekunden), für den ein Port deaktiviert bleibt, wenn eine Schleife erkannt wird (und die Port-Aktion den Port abschaltet). Gültige Werte liegen zwischen 0 und 604800 Sekunden (7 Tage). Bei einem Wert von Null bleibt ein Port deaktiviert (bis zum nächsten Neustart des Geräts).	180

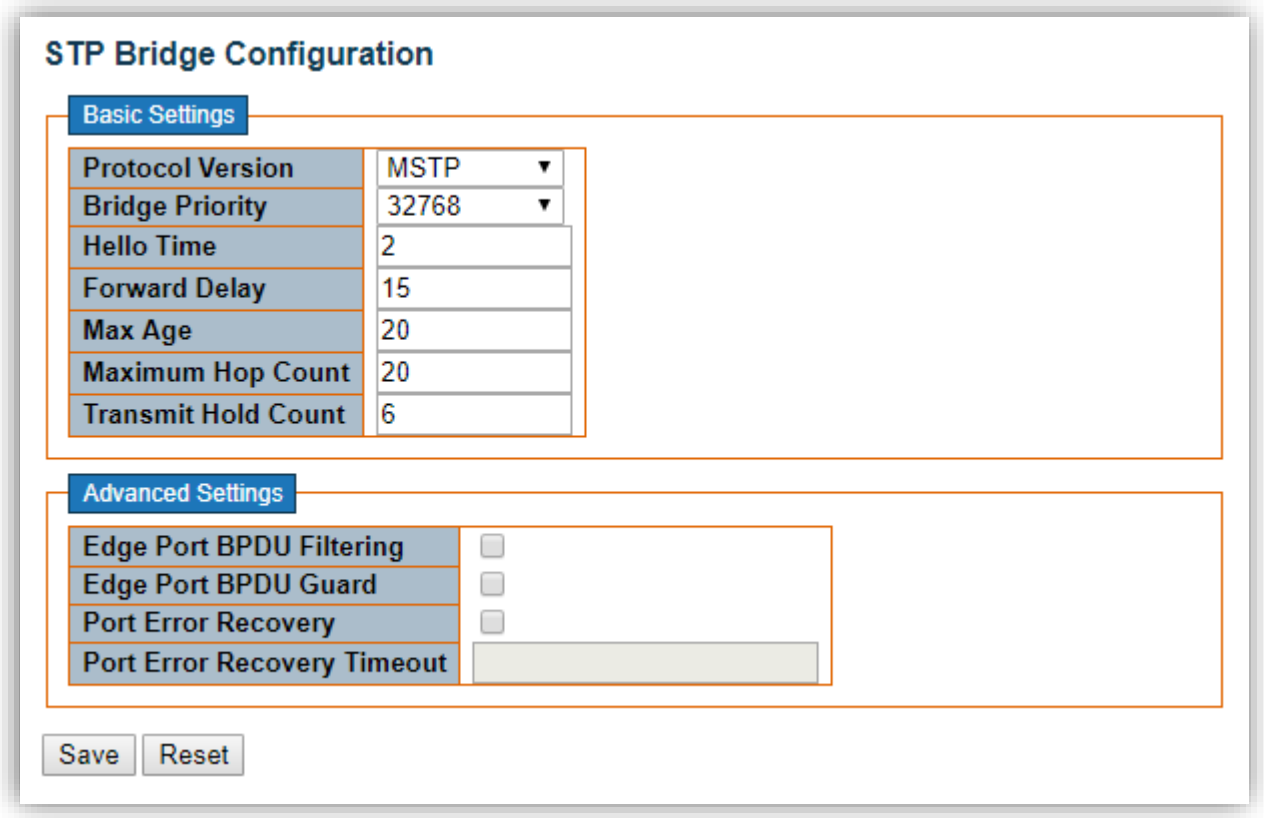
Portkonfiguration

Einstellung	Beschreibung
Port	Die Switch-Port-Nummer des Ports.
Aktivieren	Legt fest, ob der Schleifenschutz an diesem Switch-Port aktiviert ist.
Aktion	Konfiguriert die Aktion, die ausgeführt wird, wenn an einem Port eine Schleife erkannt wird. Gültige Werte sind **„Port abschalten“**, **„Port abschalten und protokollieren“** oder **„Nur protokollieren“**.
Tx-Modus	Legt fest, ob der Port aktiv PDUs zur Schleifensicherung generiert oder ob er lediglich passiv nach PDUs in einer Schleife sucht.

Konfiguration > Spanning Tree > Bridge-Einstellungen

STP-Bridge-Konfiguration

Auf dieser Seite können Sie die STP-Systemeinstellungen konfigurieren. Die Einstellungen gelten für alle STP-Bridge-Instanzen im Switch.



Grundeinstellungen

Einstellung	Beschreibung	Werkseinstellung
Protokollversion	Die Einstellung für die MSTP-/RSTP-/STP-Protokollversion. Gültige Werte sind **STP**, **RSTP** und **MSTP**.	MSTP
Brückenpriorität	Steuert die Brückenpriorität. Niedrigere numerische Werte haben eine höhere Priorität. Die Brückenpriorität zusammen mit der MSTI-Instanznummer, verkettet mit der 6-Byte-MAC-Adresse des Switches, bildet eine Brückenkennung. Im **MSTP**-Betrieb entspricht dies der Priorität des CIST. Andernfalls entspricht dies der Priorität der STP/RSTP-Brücke.	32768
Hello-Zeit	Das Intervall zwischen dem Senden von STP-BPDUs. Gültige Werte liegen im Bereich von 1 bis 10 Sekunden. **HINWEIS:** Es wird nicht empfohlen, diesen Parameter vom Standardwert abzuweichen, da dies negative Auswirkungen auf Ihr Netzwerk haben kann.	2
Weiterleitungsverzögerung	Die Verzögerung, die von STP-Brücken verwendet wird, um Root- und Designated-Ports in den Weiterleitungsmodus zu versetzen (wird im STP-kompatiblen Modus verwendet). Gültige Werte liegen im Bereich von 4 bis 30 Sekunden.	15

MaxAge	Die maximale Lebensdauer der Informationen, die von der Bridge übertragen werden, wenn sie als Root-Bridge fungiert. Gültige Werte liegen im Bereich von 6 bis 40 Sekunden, und MaxAge muss <= (FwdDelay-1)*2 sein.	20
Maximale Hop-Anzahl	Dies definiert den Anfangswert der verbleibenden Hops für MSTI-Informationen, die an der Grenze einer MSTI-Region generiert werden. Es legt fest, an wie viele Bridges eine Root-Bridge ihre BPDU-Informationen verteilen kann. Gültige Werte liegen im Bereich von 6 bis 40 Hops.	20
Übertragungs-Warteanzahl	Die Anzahl der BPDUs, die ein Brückenport pro Sekunde senden kann. Bei Überschreitung dieser Grenze wird die Übertragung der nächsten BPDU verzögert. Gültige Werte liegen im Bereich von 1 bis 10 BPDUs pro Sekunde.	6

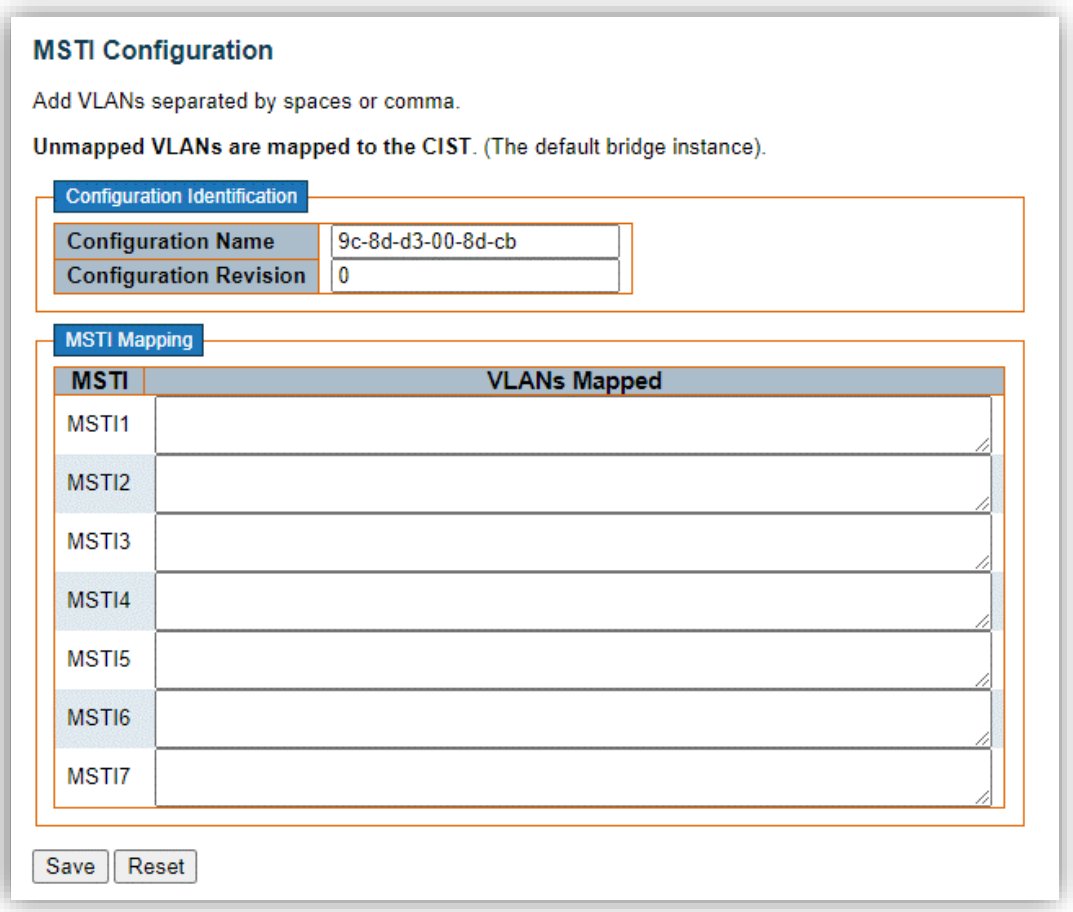
Erweiterte Einstellungen

Einstellung	Beschreibung
BPDU-Filterung für Edge-Ports	Legt fest, ob ein explizit als **Edge** konfigurierter Port BPDUs sendet und empfängt.
BPDU-Schutz für Edge-Port	Legen Sie fest, ob sich ein explizit als **Edge** konfigurierter Port beim Empfang eines BPDU selbst deaktiviert. Der Port wechselt in den Fehler-Deaktivierungszustand und wird aus der aktiven Topologie entfernt.
Port-Fehlerbehebung	Legen Sie fest, ob ein Port im fehlerbedingten deaktivierten Zustand nach einer bestimmten Zeit automatisch wieder aktiviert wird. Ist die Wiederherstellung nicht aktiviert, müssen die Ports für den normalen STP-Betrieb deaktiviert und erneut aktiviert werden. Der Zustand wird auch durch einen Systemneustart zurückgesetzt.
Zeitlimit für die Port-Fehlerbehebung	Die Zeit, die vergehen muss, bevor ein Port im fehlerbedingten deaktivierten Zustand wieder aktiviert werden kann. Gültige Werte liegen zwischen 30 und 86.400 Sekunden (24 Stunden).

Konfiguration > Spanning Tree > MSTI-Zuordnung

MSTI-Konfiguration

Auf dieser Seite kann der Benutzer die aktuellen Prioritätskonfigurationen der STP-MSTI-Bridge-Instanzen einsehen.



Konfigurationskennung

Einstellung	Beschreibung
Konfigurationsname	Der Name, der die Zuordnung von VLAN zu MSTI identifiziert. Brücken müssen denselben Namen und dieselbe Revision (siehe unten) sowie die Konfiguration der VLAN-zu-MSTI-Zuordnung aufweisen, um Spanning Trees für MSTIs (innerhalb einer Region) gemeinsam nutzen zu können. Der Name darf maximal 32 Zeichen lang sein.
Konfigurationsrevision	Die Revision der oben genannten MSTI-Konfiguration. Dies muss eine ganze Zahl zwischen 0 und 65535 sein.

MSTI-Zuordnung

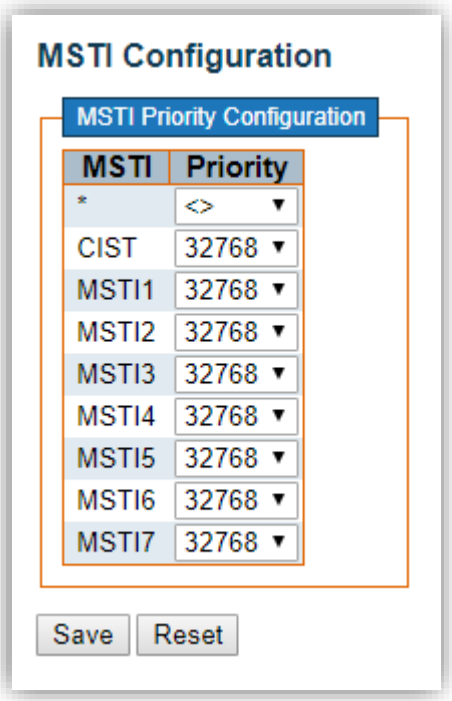
Einstellung	Beschreibung
MSTI	Die Bridge-Instanz. Das CIST steht für eine explizite Zuordnung nicht zur Verfügung, da es die nicht explizit zugeordneten VLANs erhält.
Zugeordnete VLANs	Die Liste der VLANs, die der MSTI zugeordnet sind. Die VLANs können als einzelnes VLAN (**xx**, wobei xx zwischen 1 und 4094 liegt) oder als Bereich (**xx-yy**) angegeben werden, wobei die einzelnen Einträge durch Kommas und/oder Leerzeichen voneinander getrennt werden müssen. Ein VLAN kann nur einer MSTI zugeordnet werden. Eine ungenutzte MSTI sollte einfach leer

	gelassen werden (d. h., es sollten keine VLANs ihr zugeordnet sein). Beispiel: **2,5,20-40**.

Konfiguration > Spanning Tree > MSTI-Prioritäten

MSTI-Konfiguration

Auf dieser Seite kann der Benutzer die aktuellen Prioritätskonfigurationen der STP-MSTI-Bridge-Instanzen einsehen.



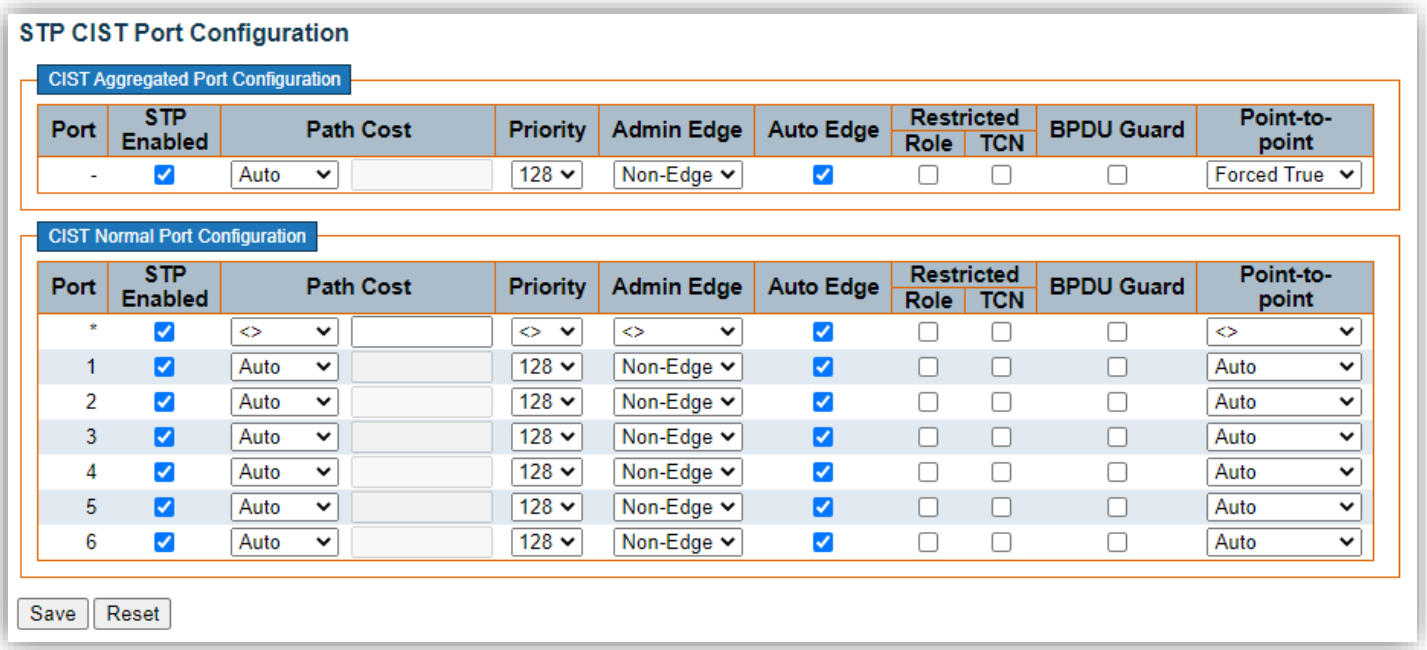
MSTI-Prioritätskonfiguration

Einstellung	Beschreibung
MSTI	Die Bridge-Instanz. Die CIST ist die Standardinstanz, die stets aktiv ist.
Priorität	Steuert die Priorität der Bridge. Niedrigere numerische Werte haben eine höhere Priorität. Die Bridge-Priorität sowie die MSTI-Instanznummer, verkettet mit der 6-Byte-MAC-Adresse des Switches, bilden eine Bridge-Kennung.

Konfiguration > Spanning Tree > CIST-Ports

STP-CIST-Port-Konfiguration

Auf dieser Seite kann der Benutzer die aktuellen STP-CIST-Port-Konfigurationen einsehen und gegebenenfalls ändern.
Diese Seite enthält Einstellungen für physische und aggregierte Ports.



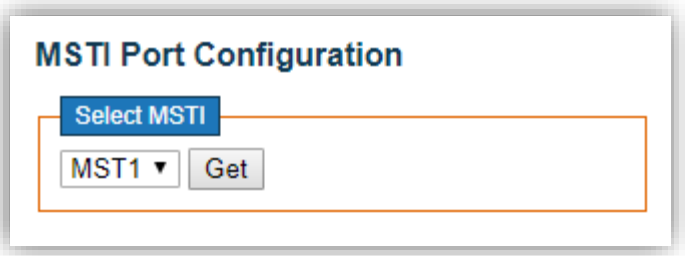
Konfiguration von aggregierten/normalen CIST-Ports

Einstellung	Beschreibung
Port	Die Switch-Port-Nummer des logischen STP-Ports.
STP aktiviert	Legt fest, ob STP an diesem Switch-Port aktiviert ist.
Pfadkosten	Steuert die vom Port verursachten Pfadkosten. Bei der Einstellung **„Auto“** werden die Pfadkosten entsprechend der physikalischen Verbindungsgeschwindigkeit unter Verwendung der in 802.1D empfohlenen Werte festgelegt. Bei der Einstellung **„Spezifisch“** kann ein benutzerdefinierter Wert eingegeben werden. Die Pfadkosten werden beim Aufbau der aktiven Topologie des Netzwerks herangezogen. Ports mit niedrigeren Pfadkosten werden gegenüber Ports mit höheren Pfadkosten als Weiterleitungsports bevorzugt. Gültige Werte liegen im Bereich von 1 bis 200000000.
Priorität	Steuert die Portpriorität. Damit lässt sich die Priorität von Ports mit identischen Portkosten steuern.
operEdge (Statusflag)	Betriebsflag, das angibt, ob der Port direkt mit Edge-Geräten verbunden ist. (Keine Brücken angeschlossen.) Der Übergang in den Weiterleitungszustand erfolgt bei Edge-Ports (bei denen operEdge auf „true“ gesetzt ist) schneller als bei anderen Ports. Der Wert dieses Flags basiert auf den Feldern „AdminEdge“ und „AutoEdge“. Dieses Flag wird unter „Monitor > Spanning Tree > STP Detailed Bridge Status“ als „Edge“ angezeigt.
AdminEdge	Steuert, ob das operEdge-Flag zu Beginn gesetzt oder gelöscht sein soll. (Der anfängliche operEdge-Zustand bei der Initialisierung eines Ports).

AutoEdge	Steuert, ob die Bridge die automatische Edge-Erkennung am Bridge-Port aktivieren soll. Dadurch kann „operEdge“ daraus abgeleitet werden, ob BPDUs am Port empfangen werden oder nicht.
Eingeschränkte Rolle	Wenn diese Option aktiviert ist, wird der Port nicht als Root-Port für das CIST oder ein MSTI ausgewählt, selbst wenn er den besten Spanning-Tree-Prioritätsvektor aufweist. Ein solcher Port wird nach der Auswahl des Root-Ports als Alternate-Port ausgewählt. Wenn diese Option gesetzt ist, kann dies zu einer Unterbrechung der Spanning-Tree-Konnektivität führen. Sie kann von einem Netzwerk -Administrator festgelegt werden, um zu verhindern, dass Brücken außerhalb eines Kernbereichs des Netzwerks die aktive Spanning-Tree-Topologie beeinflussen, möglicherweise weil diese Brücken nicht vollständig unter der Kontrolle des Administrators stehen. Diese Funktion wird auch als „Root Guard“ bezeichnet.
Eingeschränkte TCN	Wenn diese Option aktiviert ist, führt dies dazu, dass der Port empfangene Topologieänderungsbenachrichtigungen und Topologieänderungen nicht an andere Ports weiterleitet. Wenn diese Option aktiviert ist, kann es nach Änderungen an der aktiven Topologie eines Spanning-Tree-Netzwerks zu einem vorübergehenden Verbindungsverlust kommen, da die erlernten Standortinformationen der Stationen dauerhaft falsch sind. Sie wird von einem Netzwerkxml-ph-0000@deepl.internalen festgelegt, um zu verhindern, dass Brücken außerhalb eines Kernbereichs des Netzwerks ein Adress-Flushing in diesem Bereich verursachen – möglicherweise, weil diese Brücken nicht vollständig unter der Kontrolle des Administrators stehen oder sich der physikalische Verbindungsstatus der angeschlossenen LANs häufig ändert.
BPDU-Wächter	Wenn diese Option aktiviert ist, deaktiviert sich der Port beim Empfang gültiger BPDUs. Im Gegensatz zur ähnlichen Bridge-Einstellung hat der **Edge**-Status des Ports keinen Einfluss auf diese Einstellung. Ein Port, der aufgrund dieser Einstellung in den Fehler-Deaktivierungszustand wechselt, unterliegt ebenfalls der Bridge-Einstellung „Port Error Recovery“.
Punkt-zu-Punkt	Legt fest, ob der Port eine Verbindung zu einem Punkt-zu-Punkt-LAN statt zu einem gemeinsam genutzten Medium herstellt. Dies kann automatisch ermittelt oder zwangsweise auf „true“ oder „false“ gesetzt werden. Der Übergang in den Weiterleitungszustand erfolgt bei Punkt-zu-Punkt-LANs schneller als bei gemeinsam genutzten Medien.

Konfiguration > Spanning Tree > MSTI-Ports

MSTI-Port-Konfiguration



MSTI auswählen
Wählen Sie **die MSTI-Portnummer** aus und klicken Sie zur Konfiguration auf die Schaltfläche **„Abrufen**“.

(MSTn) MSTI-Port-Konfiguration

Ein MSTI-Port ist ein virtueller Port, der für jeden aktiven CIST-Port (physischen Port) separat instanziiert wird, und zwar für jede auf dem Port konfigurierte und für diesen geltende MSTI-Instanz. Die MSTI-Instanz muss ausgewählt werden, bevor die eigentlichen Konfigurationsoptionen für den MSTI-Port angezeigt werden.
Diese Seite enthält MSTI-Port-Einstellungen für physische und aggregierte Ports.

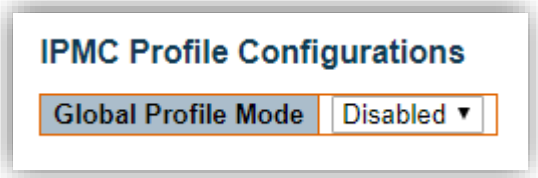
Konfiguration von aggregierten/normalen MSTI-Ports

Einstellung	Beschreibung
Port	Die Switch-Port-Nummer des entsprechenden STP-CIST- (und MSTI-)Ports.
Pfadkosten	Steuert die vom Port verursachten Pfadkosten. Bei der Einstellung **„Auto“** werden die Pfadkosten entsprechend der physikalischen Verbindungsgeschwindigkeit unter Verwendung der in 802.1D empfohlenen Werte festgelegt. Bei der Einstellung **„Spezifisch**“ kann ein benutzerdefinierter Wert eingegeben werden. Die Pfadkosten werden beim Aufbau der aktiven Topologie des Netzwerks herangezogen. Ports mit niedrigeren Pfadkosten werden gegenüber Ports mit höheren Pfadkosten als Weiterleitungsports bevorzugt. Gültige Werte liegen im Bereich von 1 bis 200000000.
Priorität	Steuert die Portpriorität. Damit lässt sich die Priorität von Ports mit identischen Portkosten steuern.

Konfiguration > IPMC-Profil > Profiltabelle

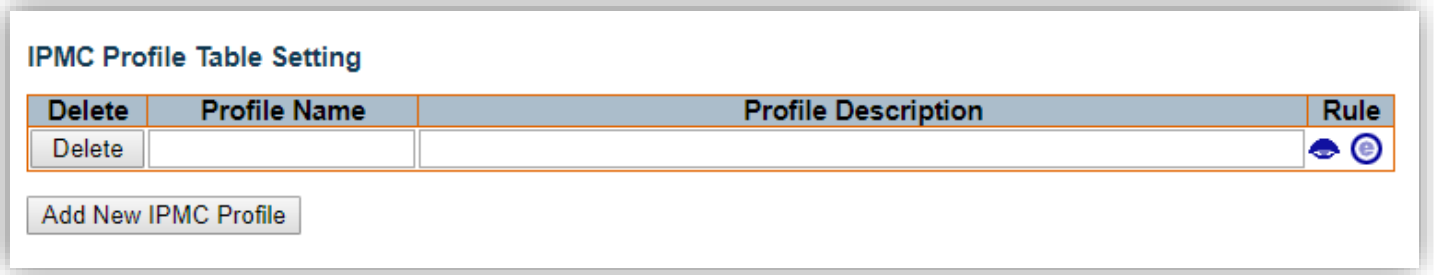
IPMC-Profil-Konfigurationen

Auf dieser Seite werden Konfigurationen im Zusammenhang mit IPMC-Profilen bereitgestellt. Das IPMC-Profil wird verwendet, um die Zugriffskontrolle für IP-Multicast-Streams zu implementieren. Es können maximal 64 Profile mit jeweils maximal 128 entsprechenden Regeln erstellt werden.



Globaler Profilmodus
Aktivieren/Deaktivieren Sie das globale IPMC-Profil.

Einstellungen für die IPMC-Profil-Tabelle



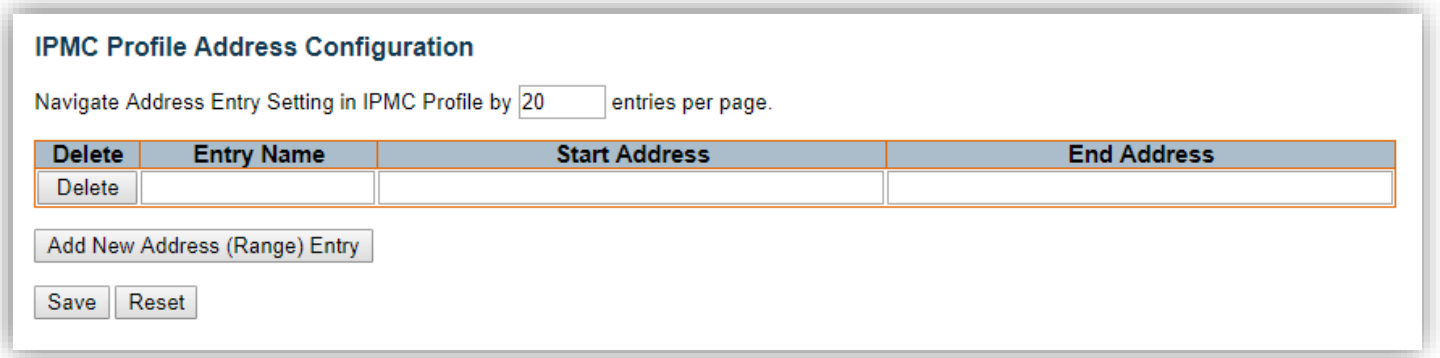
Schaltfläche „Neues IPMC-Profil hinzufügen“
Klicken Sie hier, um ein neues IPMC-Profil hinzuzufügen. Geben Sie den Namen an und konfigurieren Sie den neuen Eintrag.

Einstellung	Beschreibung
Löschen	Aktivieren Sie dieses Kontrollkästchen, um den Eintrag zu löschen. Er wird beim nächsten Speichern gelöscht.
Profilname	Der Name, der für die Indizierung der Profiltabelle verwendet wird. Jeder Eintrag hat einen eindeutigen Namen, der aus maximal 16 alphanumerischen Zeichen besteht. Mindestens ein Buchstabe muss enthalten sein.
Profilbeschreibung	Zusätzliche Beschreibung des Profils, bestehend aus maximal 64 alphanumerischen Zeichen. Leerzeichen sind in der Beschreibung nicht zulässig. Verwenden Sie „_“ oder „-“ zur Trennung der Beschreibungssätze.
Regel	Wenn das Profil erstellt wurde, klicken Sie auf die Schaltfläche „Bearbeiten“, um die Seite mit den Regeleinstellungen des ausgewählten Profils aufzurufen. Durch Klicken auf die Schaltfläche „Anzeigen“ wird eine Zusammenfassung des ausgewählten Profils angezeigt. Mit den folgenden Schaltflächen können Sie die Regeln des ausgewählten Profils verwalten oder überprüfen: : Listet die mit dem ausgewählten Profil verknüpften Regeln auf. : Passen Sie die mit dem ausgewählten Profil verknüpften Regeln an.

Konfiguration > IPMC-Profil > Adresseneingabe

IPMC-Profil – Adresskonfiguration

Auf dieser Seite werden die Adressbereichseinstellungen für das IPMC-Profil vorgenommen. Der Adresseintrag dient zur Angabe des Adressbereichs, der dem IPMC-Profil zugeordnet wird. Es dürfen maximal 128 Adresseinträge im System angelegt werden.



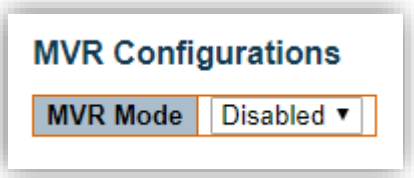
Schaltfläche „Neuen Adresseintrag (Bereich) hinzufügen“

Einstellung	Beschreibung
Löschen	Aktivieren Sie dieses Kontrollkästchen, um den Eintrag zu löschen. Er wird beim nächsten Speichern gelöscht.
Eintragsname	Der Name, der zur Indizierung der Adresseintragstabelle verwendet wird. Jeder Eintrag hat einen eindeutigen Namen, der aus maximal 16 alphanumerischen Zeichen besteht. Mindestens ein Buchstabe muss enthalten sein.
Startadresse	Die Startadresse der IPv4/IPv6-Multicast-Gruppe, die als Adressbereich verwendet wird.
Endadresse	Die Endadresse der IPv4/IPv6-Multicast-Gruppe, die als Adressbereich verwendet wird.

Konfiguration > MVR

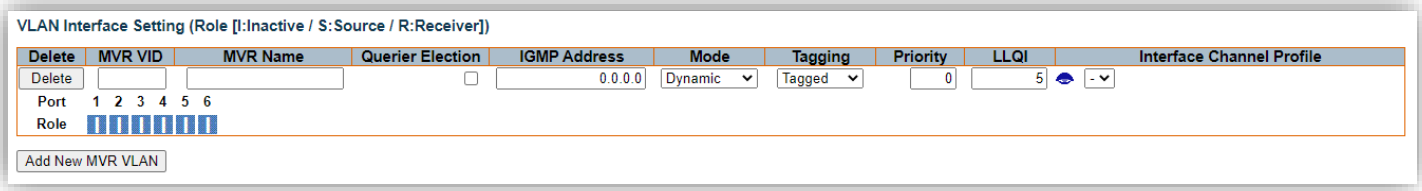
MVR-Konfigurationen

Die MVR-Funktion ermöglicht die Weiterleitung von Multicast-Datenverkehr in den Multicast-VLANs.
In einer Multicast-Fernsehanwendung kann ein PC, ein Netzwerkfernseher oder eine Set-Top-Box den Multicast-Stream empfangen. An einen Teilnehmeranschluss – einen als MVR-Empfängerport konfigurierten Switch-Port – können mehrere Set-Top-Boxen oder PCs angeschlossen werden. Wenn ein Teilnehmer einen Kanal auswählt, sendet die Set-Top-Box oder der PC eine IGMP/MLD-Meldung an Switch A, um der entsprechenden Multicast-Gruppenadresse beizutreten. Uplink-Ports, die Multicast-Daten an das Multicast-VLAN senden und von diesem empfangen, werden als MVR-Quellports bezeichnet.
Der Querier sollte eine Verbindung zum Quellport herstellen. Durch die Zuweisung einer statischen Mitgliedschaft im MVR-VLAN leitet das Gerät lediglich die IGMP-Berichte von den Downstream-Ports (Empfängerports) zu den Upstream-Ports (Quellports) weiter, während das aus dem Downstream kommende Abfragepaket stillschweigend ignoriert wird.
Nachdem die MVR-VLAN-Mitglieder ordnungsgemäß konfiguriert wurden, muss dem jeweiligen MVR-VLAN ein IPMC-Profil zugeordnet werden, das als erwarteter Kanal dienen soll. Das Kanalprofil wird durch das IPMC-Profil definiert, das die Filterbedingungen festlegt. Beachten Sie, dass das Profil nur funktioniert, wenn der globale Profilmodus aktiviert ist. Es dürfen maximal 4 MVR-VLANs mit entsprechenden Kanalprofilen angelegt werden.



MVR-Modus
Aktivieren/Deaktivieren des globalen MVR.
Die Steuerung des „Unregistered Flooding“ hängt von der aktuellen Konfiguration im IGMP/MLD-Snooping ab.
Es wird empfohlen, die „Unregistered Flooding“-Steuerung zu aktivieren, wenn die MVR-Gruppentabelle voll ist.

VLAN-Schnittstelleneinstellung



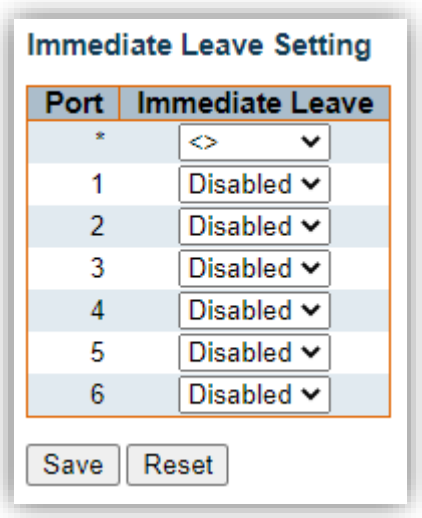
Schaltfläche „Neues MVR-VLAN hinzufügen“

Einstellung	Beschreibung
Löschen	Aktivieren Sie dieses Kontrollkästchen, um den Eintrag zu löschen. Er wird beim nächsten Speichern gelöscht.
MVR-VID	Geben Sie die Multicast-VLAN-ID an. **Achtung:** Es wird nicht empfohlen, MVR-Quellports mit Management-VLAN-Ports zu überlappen.

MVR-Name	Der MVR-Name ist ein optionales Attribut zur Angabe des Namens des jeweiligen MVR-VLANs. Die maximale Länge der Zeichenfolge für den MVR-VLAN-Namen beträgt 16. Der MVR-VLAN-Name darf nur Buchstaben oder Ziffern enthalten. Wenn der optionale MVR-VLAN-Name angegeben wird, muss er mindestens einen Buchstaben enthalten. Der MVR-VLAN-Name kann für bestehende MVR-VLAN-Einträge bearbeitet oder neuen Einträgen hinzugefügt werden.
Querier-Wahl	Aktivieren Sie diese Option, um an der IGMP-Querier-Wahl im VLAN teilzunehmen. Deaktivieren Sie diese Option, um als IGMP-Non-Querier zu fungieren.
IGMP-Adresse	Legen Sie die IPv4-Adresse als Quelladresse fest, die im IP-Header für IGMP-Steuerrahmen verwendet wird. Die Standard-IGMP-Adresse ist nicht festgelegt (0.0.0.0). Wenn die IGMP-Adresse nicht festgelegt ist, verwendet das System die IPv4-Verwaltungsadresse der diesem VLAN zugeordneten IP-Schnittstelle. Ist die IPv4-Verwaltungsadresse nicht festgelegt, verwendet das System die erste verfügbare IPv4-Verwaltungsadresse. Andernfalls verwendet das System einen vordefinierten Wert. Standardmäßig lautet dieser Wert 192.0.2.1.
Modus	Geben Sie den MVR-Betriebsmodus an. Im dynamischen Modus ermöglicht MVR dynamische MVR-Mitgliedschaftsmeldungen an Quellports. Im kompatiblen Modus sind MVR-Mitgliedschaftsmeldungen an Quellports untersagt. Standardmäßig ist der dynamische Modus eingestellt.
Tagging	Legen Sie fest, ob die durchlaufenden IGMP/MLD-Steuerrahmen als „Untagged“ oder mit MVR-VID „Tagged“ gesendet werden sollen. Die Standardeinstellung ist „Tagged“.
Priorität	Legen Sie fest, wie die durchlaufenden IGMP/MLD-Steuerrahmen priorisiert gesendet werden sollen. Die Standardpriorität ist 0.
LLQI	Legen Sie die maximale Wartezeit für IGMP/MLD-Berichte zur Mitgliedschaft an einem Empfängerport fest, bevor der Port aus der Multicast-Gruppenmitgliedschaft entfernt wird. Der Wert wird in Zehntelsekunden angegeben. Der Bereich reicht von 0 bis 31744. Der Standardwert für LLQI beträgt 5 Zehntelsekunden bzw. eine halbe Sekunde.
Schnittstellenkanalprofil	Wenn das MVR-VLAN erstellt wird, wählen Sie das IPMC-Profil als Kanalfilterbedingung für das jeweilige MVR-VLAN aus. Eine Zusammenfassung zur Schnittstellenkanalprofilierung (des MVR-VLANs) wird durch Klicken auf die Schaltfläche „Anzeigen“ angezeigt. Das für den festgelegten Schnittstellenkanal ausgewählte Profil darf keine überlappenden Zulassungsgruppenadressen enthalten.
 **Schaltfläche „Profilverwaltung“**	Listet die Regeln auf, die mit dem ausgewählten Profil verknüpft sind.
Port	Der logische Port für die Einstellungen.
Port-Rolle	Konfigurieren Sie einen MVR-Port des angegebenen MVR-VLANs für eine der folgenden Rollen. **Inaktiv:** Der zugewiesene Port nimmt nicht an MVR-Vorgängen teil. **Quelle:** Konfigurieren Sie Uplink-Ports, die Multicast-Daten empfangen und senden, als Quellports. Teilnehmer können nicht direkt an Quellports angeschlossen werden.

	Empfänger: Konfigurieren Sie einen Port als Empfängerport, wenn es sich um einen Teilnehmerport handelt, der ausschließlich Multicast-Daten empfangen soll. Er empfängt keine Daten, es sei denn, er wird durch das Senden von IGMP-/MLD-Nachrichten Mitglied der Multicast-Gruppe. **Achtung:** Es wird nicht empfohlen, MVR-Quellports mit Management-VLAN-Ports zu überlappen. Wählen Sie die Portrolle aus, indem Sie auf das Rollensymbol klicken, um die Einstellung zu ändern. I steht für „Inaktiv“; S steht für „Quelle“; R steht für „Empfänger“. Die Standardrolle ist „Inaktiv“.

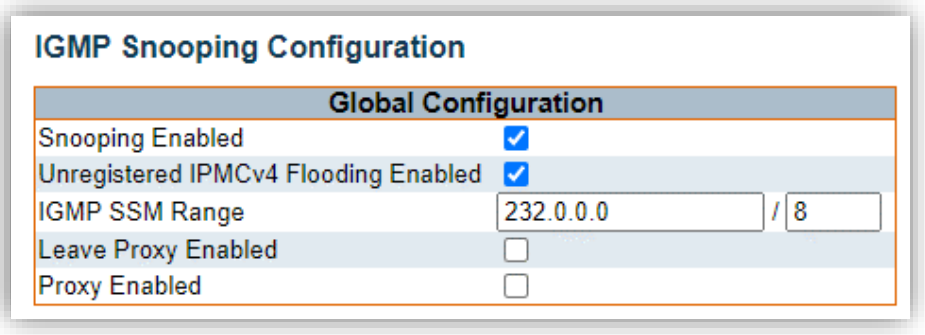
Einstellung „Sofortiges Verlassen“



Einstellung	Beschreibung	Werkseinstellung
Aktiviert	Aktiviert das schnelle Verlassen am Port. Das System entfernt den Gruppeneintrag und beendet die Datenweiterleitung nach Empfang der IGMPc2/MLDv1-Leave-Nachricht, ohne „Last Member Query“-Nachrichten zu senden. Es wird empfohlen, diese Funktion nur zu aktivieren, wenn ein einzelner IGMPv2/MLDv1-Host an den jeweiligen Port angeschlossen ist.	Deaktiviert
Deaktiviert	Deaktivieren Sie „Fast Leave“ an diesem Port.	

Konfiguration > IPMC > IGMP-Snooping > Grundkonfiguration

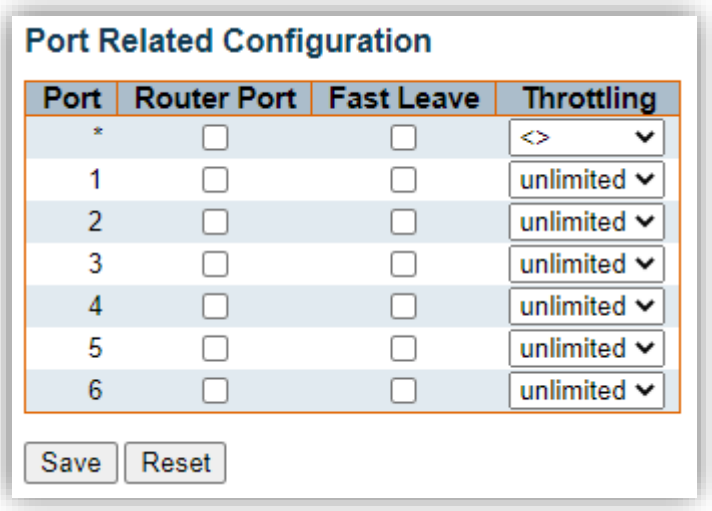
IGMP-Snooping-Konfiguration



Globale Konfiguration

Einstellung	Beschreibung
Snooping aktiviert	Aktivieren Sie das globale IGMP-Snooping.
Flooding von nicht registriertem IPMCv4 aktiviert	Aktivieren Sie das Flooding von nicht registriertem IPv4-Datenverkehr. Die Flooding-Steuerung greift nur, wenn IGMP-Snooping aktiviert ist. Wenn das IGMP-Snooping deaktiviert ist, ist das Flooding von nicht registriertem IPv4-Verkehr ungeachtet dieser Einstellung immer aktiv.
IGMP-SSM-Bereich	Der SSM-Bereich (Source-Specific Multicast) ermöglicht es SSM-fähigen Hosts und Routern, das SSM-Dienstmodell für die Gruppen im Adressbereich auszuführen. Weisen Sie dem Bereich eine gültige IPv4-Multicast-Adresse als Präfix mit einer Präfixlänge (von 4 bis 32) zu.
Leave-Proxy aktiviert	Aktivieren Sie „IGMP Leave Proxy“. Diese Funktion kann verwendet werden, um die Weiterleitung unnötiger Leave-Nachrichten an den Router zu vermeiden.
Proxy aktiviert	Aktivieren Sie den IGMP-Proxy. Mit dieser Funktion kann vermieden werden, dass unnötige „Join“- und „Leave“-Nachrichten an den Router weitergeleitet werden.

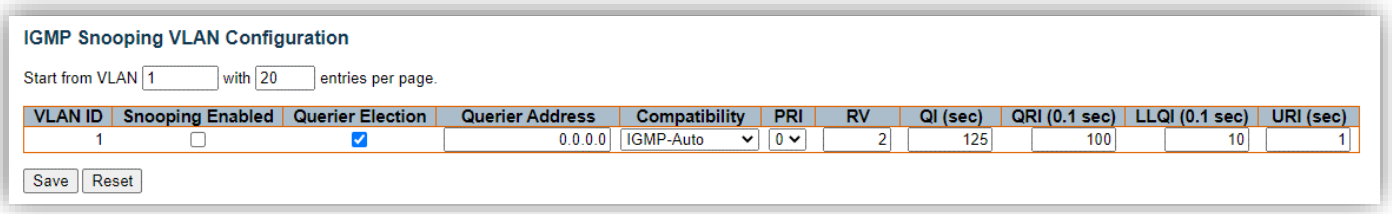
Portbezogene Konfiguration



Einstellung	Beschreibung
Router-Port	Geben Sie an, welche Ports als Router-Ports fungieren sollen. Ein Router-Port ist ein Port am Ethernet-Switch, der zum Layer-3-Multicast-Gerät oder zum IGMP-Querier führt. Wenn ein Port eines Aggregationsmitglieds als Router-Port ausgewählt wird, fungiert die gesamte Aggregation als Router-Port.
Schnelles Verlassen	Aktivieren Sie die Funktion „Fast Leave“ für den Port. Das System entfernt den Gruppeneintrag und stellt die Datenweiterleitung ein, sobald es die IGMPv2-Leave-Nachricht empfängt, ohne letzte Member-Query-Nachrichten zu senden. Es wird empfohlen, diese Funktion nur zu aktivieren, wenn ein einzelner IGMPv2-Host an den jeweiligen Port angeschlossen ist.
Drosselung	Aktivieren Sie diese Option, um die Anzahl der Multicast-Gruppen zu begrenzen, denen ein Switch-Port angehören kann.

Konfiguration > IPMC > IGMP-Snooping > VLAN-Konfiguration

IGMP-Snooping-VLAN-Konfiguration



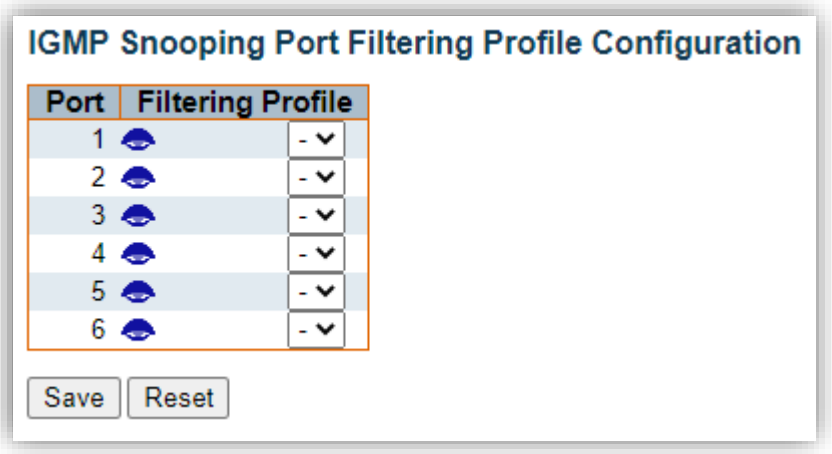
Navigieren in der IGMP-Snooping-VLAN-Tabelle
Jede Seite zeigt bis zu 99 Einträge aus der VLAN-Tabelle an, wobei die Standardeinstellung 20 beträgt und über das Eingabefeld „Einträge pro Seite“ ausgewählt werden kann. Beim ersten Aufruf der Webseite werden die ersten 20 Einträge vom Anfang der VLAN-Tabelle angezeigt. Als erster wird der Eintrag mit der niedrigsten VLAN-ID aus der VLAN-Tabelle angezeigt.

Einstellung	Beschreibung
VLAN-ID	Die VLAN-ID des Eintrags.
IGMP-Snooping aktiviert	Aktivieren Sie das VLAN-spezifische IGMP-Snooping. Für das IGMP-Snooping können bis zu **8** VLANs ausgewählt werden.
Querier-Wahl	Aktivieren, um an der IGMP-Querier-Wahl im VLAN teilzunehmen. Deaktivieren, um als IGMP-Non-Querier zu fungieren.
Querier-Adresse	Legen Sie die IPv4-Adresse als Quelladresse fest, die im IP-Header für die Wahl des IGMP-Queriers verwendet wird. Wenn die Querier-Adresse nicht festgelegt ist, verwendet das System die IPv4-Verwaltungsadresse der diesem VLAN zugeordneten IP-Schnittstelle. Wenn die IPv4-Verwaltungsadresse nicht festgelegt ist, verwendet das System die erste verfügbare IPv4-Verwaltungsadresse. Andernfalls verwendet das System einen vordefinierten Wert. Standardmäßig lautet dieser Wert 192.0.2.1.
Kompatibilität	Die Kompatibilität wird dadurch gewährleistet, dass Hosts und Router je nach den auf den Hosts und Routern innerhalb eines Netzwerks verwendeten IGMP-Versionen entsprechende Maßnahmen ergreifen. Zur Auswahl stehen **„IGMP-Auto“**, **„Forced IGMPv1“**, **„Forced IGMPv2**“ und **„Forced IGMPv3**“; der Standardwert für die Kompatibilität ist „IGMP-Auto“.
PRI	Priorität der Schnittstelle. Sie gibt die vom System generierte Prioritätsstufe für IGMP-Steuerrahmen an. Diese Werte können verwendet werden, um verschiedenen Verkehrsklassen Priorität zuzuweisen. Der zulässige Bereich reicht von **0** (Best-Effort) bis **7** (höchste Priorität); der Standardwert für die Schnittstellenpriorität ist 0.
RV	Robustheitsvariable. Die Robustheitsvariable ermöglicht die Anpassung an den erwarteten Paketverlust in einem Netzwerk. Der zulässige Bereich liegt zwischen **1** und **255**; der Standardwert der Robustheitsvariable ist 2.
QI	Abfrageintervall. Das Abfrageintervall ist der Zeitraum zwischen den vom Abfragenden gesendeten allgemeinen Abfragen. Der zulässige Bereich liegt zwischen **1** und **31744** Sekunden, das Standard-Abfrageintervall beträgt 125 Sekunden.

QRI	Abfrage-Antwort-Intervall. Die maximale Antwortverzögerung, die zur Berechnung des maximalen Antwortcodes verwendet wird, der in die periodischen allgemeinen Abfragen eingefügt wird. Der zulässige Bereich liegt zwischen **0** und **31744** in Zehntelsekunden; das Standard-Abfrageantwortintervall beträgt 100 in Zehntelsekunden (10 Sekunden).
LLQI (LMQI für IGMP)	Last Member Query Interval. Die Zeit für die letzte Mitgliederabfrage ist der Zeitwert, der durch das Intervall für die letzte Mitgliederabfrage dargestellt wird, multipliziert mit der Anzahl der letzten Mitgliederabfragen. Der zulässige Bereich liegt zwischen **0** und **31744** in Zehntelsekunden; das Standardintervall für die letzte Mitgliederabfrage beträgt 10 in Zehntelsekunden (1 Sekunde).
URI	Unsolicited Report Interval. Das Intervall für unaufgeforderte Berichte ist die Zeit zwischen den Wiederholungen des ersten Berichts eines Hosts über seine Mitgliedschaft in einer Gruppe. Der zulässige Bereich liegt zwischen **0** und **31744** Sekunden; das Standardintervall für unaufgeforderte Berichte beträgt 1 Sekunde.

Konfiguration > IPMC > IGMP-Snooping > Port-Filterprofil

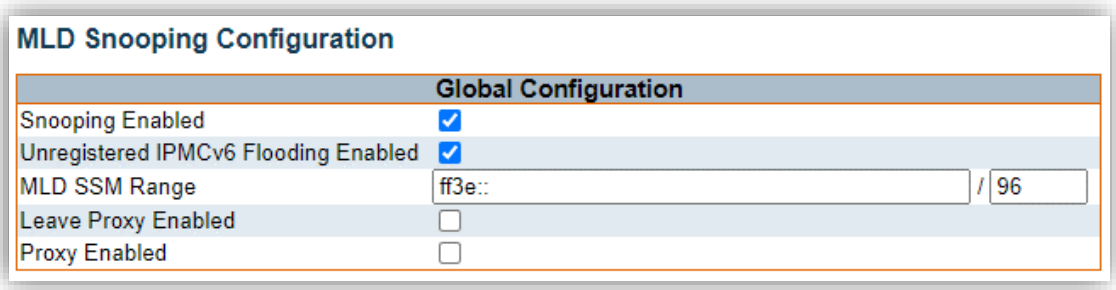
Konfiguration des IGMP-Snooping-Portfilterprofils



Einstellung	Beschreibung
Port	Der logische Port für die Einstellungen.
Filterprofil	Wählen Sie das IPMC-Profil als Filterbedingung für den jeweiligen Port aus. Durch Klicken auf die Schaltfläche „Anzeigen“ wird eine Zusammenfassung des ausgewählten Profils angezeigt.
Schaltfläche „Profilverwaltung“	Listet die Regeln auf, die mit dem ausgewählten Profil verknüpft sind.

Konfiguration > IPMC > MLD-Snooping > Grundkonfiguration

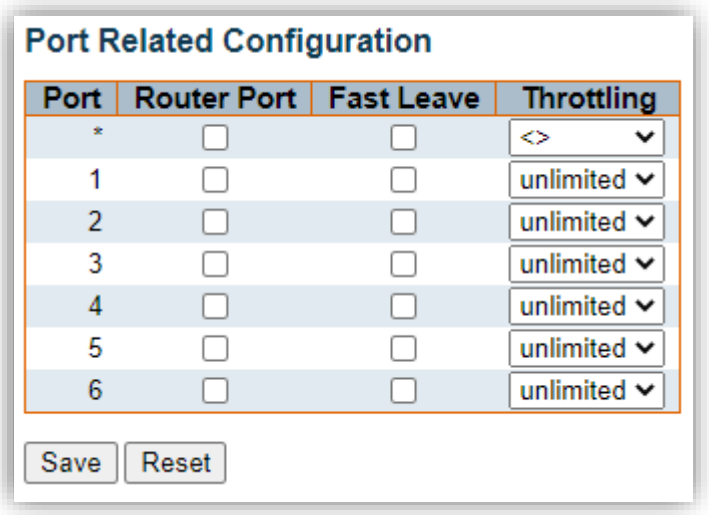
MLD-Snooping-Konfiguration



Globale Konfiguration

Einstellung	Beschreibung
Snooping aktiviert	Aktivieren Sie das globale MLD-Snooping.
Flooding von nicht registriertem IPv6-Verkehr aktiviert	Aktivieren Sie das Flooding von nicht registriertem IPMCv6-Datenverkehr. Die Flooding-Steuerung greift nur, wenn MLD-Snooping aktiviert ist. Wenn MLD-Snooping deaktiviert ist, ist das Flooding von nicht registriertem IPMCv6-Datenverkehr ungeachtet dieser Einstellung immer aktiv.
MLD-SSM-Bereich	Der SSM-Bereich (Source-Specific Multicast) ermöglicht es SSM-fähigen Hosts und Routern, das SSM-Dienstmodell für die Gruppen im Adressbereich auszuführen. Weisen Sie dem Bereich eine gültige IPv6-Multicast-Adresse als Präfix mit einer Präfixlänge (von 8 bis 128) zu.
Leave-Proxy aktiviert	Aktivieren Sie „MLD Leave Proxy“. Diese Funktion kann verwendet werden, um die Weiterleitung unnötiger Leave-Nachrichten an den Router zu vermeiden.
Proxy aktiviert	Aktivieren Sie den MLD-Proxy. Diese Funktion kann verwendet werden, um die Weiterleitung unnötiger „Join“- und „Leave“-Nachrichten an den Router zu vermeiden.

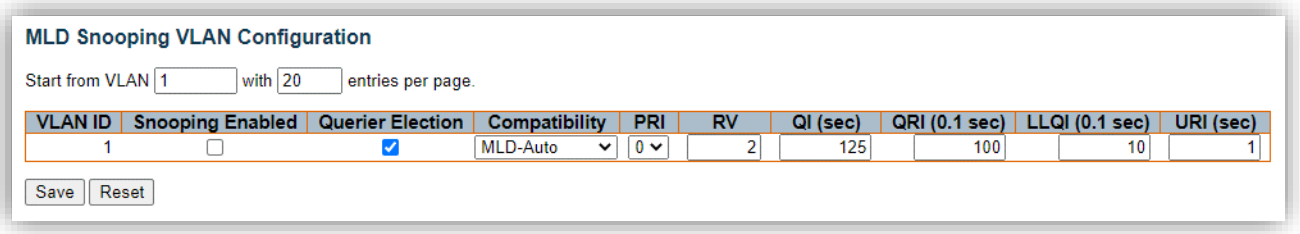
Portbezogene Konfiguration



Einstellung	Beschreibung
Router-Port	Geben Sie an, welche Ports als Router-Ports fungieren sollen. Ein Router-Port ist ein Port am Ethernet-Switch, der zum Layer-3-Multicast-Gerät oder zum MLD-Querier führt. Wird ein Port eines Aggregationsmitglieds als Router-Port ausgewählt, fungiert die gesamte Aggregation als Router-Port.
Schnelles Verlassen	Aktivieren Sie die Funktion „Fast Leave“ für den Port. Das System entfernt den Gruppeneintrag und stellt die Datenweiterleitung ein, sobald es die MLDv1-Leave-Nachricht empfängt, ohne letzte Member-Query-Nachrichten zu senden. Es wird empfohlen, diese Funktion nur zu aktivieren, wenn ein einzelner MLDv1-Host an den jeweiligen Port angeschlossen ist.
Drosselung	Aktivieren Sie diese Option, um die Anzahl der Multicast-Gruppen zu begrenzen, denen ein Switch-Port angehören kann.

Konfiguration > IPMC > MLD-Snooping > VLAN-Konfiguration

MLD-Snooping-VLAN-Konfiguration



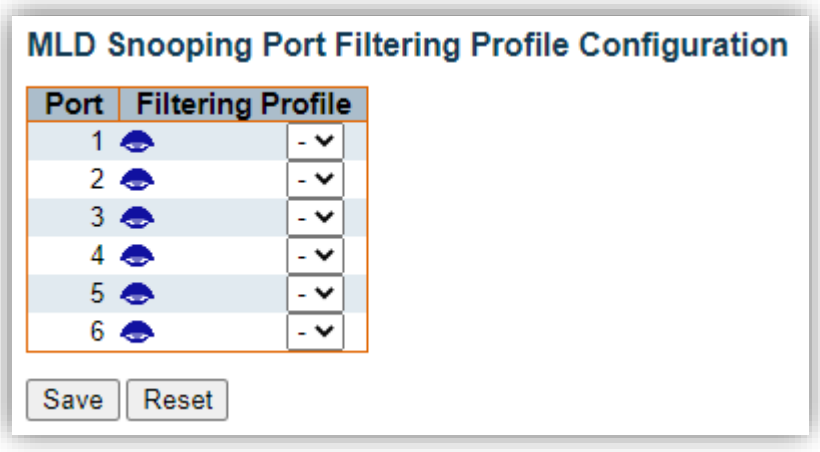
Navigieren in der MLD-Snooping-VLAN-Tabelle
Auf jeder Seite werden bis zu 99 Einträge aus der VLAN-Tabelle angezeigt, standardmäßig sind es 20, die über das Eingabefeld „Einträge pro Seite“ ausgewählt werden können. Beim ersten Aufruf der Webseite werden die ersten 20 Einträge vom Anfang der VLAN-Tabelle angezeigt. Als erster wird der Eintrag mit der niedrigsten VLAN-ID aus der VLAN-Tabelle angezeigt.

Einstellung	Beschreibung
VLAN-ID	Die VLAN-ID des Eintrags.
Snooping aktiviert	Aktiviert das MLD-Snooping pro VLAN. Für das MLD-Snooping können bis zu **8** VLANs ausgewählt werden.
Querier-Wahl	Aktivieren, um an der MLD-Querier-Wahl im VLAN teilzunehmen. Deaktivieren, um als MLD-Non-Querier zu fungieren.
Kompatibilität	Die Kompatibilität wird dadurch gewährleistet, dass Hosts und Router je nach den auf den Hosts und Routern innerhalb eines Netzwerks verwendeten MLD-Versionen entsprechende Maßnahmen ergreifen. Zur Auswahl stehen **„MLD-Auto“**, **„Forced MLDv1**“ und **„Forced MLDv2**“; der Standardwert für die Kompatibilität ist „MLD-Auto“.
PRI	Priorität der Schnittstelle. Sie gibt die vom System generierte Prioritätsstufe für MLD-Steuerrahmen an. Diese Werte können verwendet werden, um verschiedenen Verkehrsklassen Priorität zuzuweisen. Der zulässige Bereich reicht von **0** (Best-Effort) bis **7** (höchste Priorität); der Standardwert für die Schnittstellenpriorität ist 0.
RV	Robustheitsvariable. Die Robustheitsvariable ermöglicht die Anpassung an den erwarteten Paketverlust auf einer Verbindung. Der zulässige Bereich liegt zwischen **1** und **255**; der Standardwert der Robustheitsvariable ist 2.
QI	Abfrageintervall. Das Abfrageintervall ist der Zeitraum zwischen den vom Abfrager gesendeten allgemeinen Abfragen. Der zulässige Bereich liegt zwischen **1** und **31744** Sekunden, das Standard-Abfrageintervall beträgt 125 Sekunden.
QRI	Abfrage-Antwort-Intervall. Die maximale Antwortverzögerung, die zur Berechnung des maximalen Antwortcodes verwendet wird, der in die periodischen allgemeinen Abfragen eingefügt wird. Der zulässige Bereich liegt zwischen **0** und **31744** in Zehntelsekunden; das Standard-Abfrageantwortintervall beträgt 100 in Zehntelsekunden (10 Sekunden).

LLQI	Abfrageintervall für den letzten Listener. Das Abfrageintervall für den letzten Listener ist die maximale Antwortverzögerung, die zur Berechnung des maximalen Antwortcodes verwendet wird, der in Multicast-Adress-spezifische Abfragen eingefügt wird, die als Antwort auf „Version 1 Multicast Listener Done“-Nachrichten gesendet werden. Es ist auch die maximale Antwortverzögerung, die zur Berechnung des maximalen Antwortcodes verwendet wird, der in Multicast-Adress- und Quell-spezifische Abfragen eingefügt wird. Der zulässige Bereich liegt zwischen **0** und **31744** in Zehntelsekunden; das Standardintervall für die letzte Listener-Abfrage beträgt 10 in Zehntelsekunden (1 Sekunde).
URI	Intervall für unaufgeforderte Berichte. Das Intervall für unaufgeforderte Berichte ist die Zeit zwischen den Wiederholungen des ersten Berichts eines Knotens über sein Interesse an einer Multicast-Adresse. Der zulässige Bereich liegt zwischen **0** und **31744** Sekunden; das Standardintervall für unaufgeforderte Berichte beträgt 1 Sekunde.

Konfiguration > IPMC > MLD-Snooping > Port-Filterprofil

Konfiguration des MLD-Snooping-Portfilterprofils

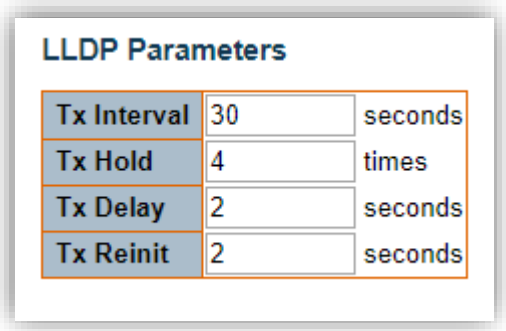


Einstellung	Beschreibung
Port	Der logische Port für die Einstellungen.
Filterprofil	Wählen Sie das IPMC-Profil als Filterbedingung für den jeweiligen Port aus. Durch Klicken auf die Schaltfläche „Anzeigen“ wird eine Zusammenfassung des ausgewählten Profils angezeigt.
Schaltfläche „Profilverwaltung“	Listet die Regeln auf, die mit dem ausgewählten Profil verknüpft sind.

Konfiguration > LLDP > LLDP

LLDP-Konfiguration

LLDP-Parameter



Sendeintervall

Einstellung	Beschreibung	Werkseinstellung
5 ~ 32768	Der Switch sendet in regelmäßigen Abständen LLDP-Frames an seine Nachbarn, um die Informationen zur Netzwerkerkennung auf dem neuesten Stand zu halten. Das Intervall zwischen den einzelnen LLDP-Frames wird durch den Wert für **das Tx-Intervall** bestimmt. Gültige Werte liegen im Bereich von 5 bis 32768 Sekunden.	30

Tx Hold

Einstellung	Beschreibung	Werkseinstellung
2 bis 10	Jeder LLDP-Frame enthält Informationen darüber, wie lange die Informationen im LLDP-Frame als gültig gelten sollen. Die Gültigkeitsdauer der LLDP-Informationen entspricht dem Wert von **„Tx Hold“** multipliziert mit dem Wert von **„Tx Interval“** in Sekunden. Gültige Werte sind auf das 2- bis 10-fache beschränkt.	4

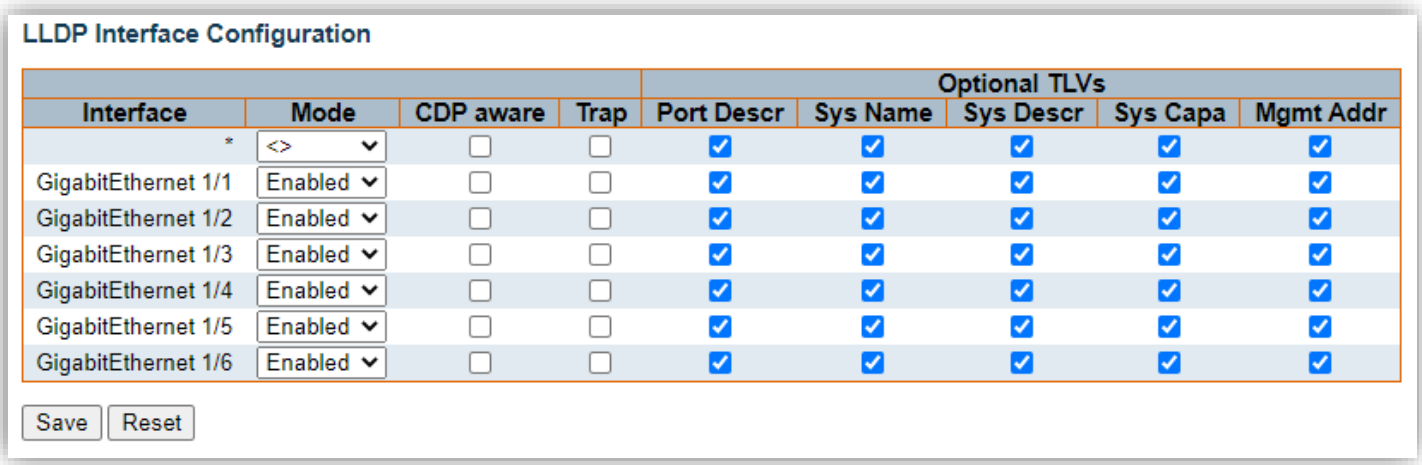
Tx-Verzögerung

Einstellung	Beschreibung	Werkseinstellung
1 ~ 8192	Wenn eine Konfiguration geändert wird (z. B. die IP-Adresse), wird ein neuer LLDP-Frame gesendet, wobei der Zeitabstand zwischen den LLDP-Frames jedoch immer mindestens dem Wert von **„Tx Delay“** in Sekunden entspricht. **„Tx Delay“** darf nicht größer sein als 1/4 des Werts für **„Tx Interval**“. Gültige Werte sind auf 1 bis 8192 Sekunden beschränkt.	2

Tx Reinit

Einstellung	Beschreibung	Werkseinstellung
1 ~ 10	Wenn eine Schnittstelle deaktiviert wird, LLDP deaktiviert wird oder der Switch neu gestartet wird, wird ein LLDP-Shutdown-Frame an die benachbarten Geräte gesendet, der signalisiert, dass die LLDP-Informationen nicht mehr gültig sind. **Tx Reinit** steuert die Zeitspanne in Sekunden zwischen dem Shutdown-Frame und einer neuen LLDP-Initialisierung. Gültige Werte sind auf 1 – 10 Sekunden.	2

LLDP-Schnittstellenkonfiguration



Einstellung	Beschreibung
Schnittstelle	Der Switch-Schnittstellenname der logischen LLDP-Schnittstelle.
Modus	Wählen Sie den LLDP-Modus aus. **Nur Empfang:** Der Switch sendet keine LLDP-Informationen aus, analysiert jedoch LLDP-Informationen von benachbarten Geräten. **Nur Tx:** Der Switch verwirft von Nachbarn empfangene LLDP-Informationen, sendet jedoch selbst LLDP-Informationen. **Deaktiviert:** Der Switch sendet keine LLDP-Informationen und verwirft von benachbarten Geräten empfangene LLDP-Informationen. **Aktiviert:** Der Switch sendet LLDP-Informationen und analysiert die von benachbarten Geräten empfangenen LLDP-Informationen.

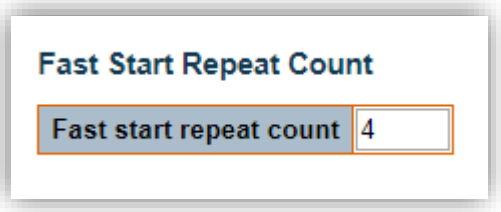
CDP-Unterstützung	Wählen Sie die CDP-Unterstützung aus. Der CDP-Betrieb beschränkt sich auf die Dekodierung eingehender CDP-Frames (der Switch sendet keine CDP-Frames). CDP-Frames werden nur dekodiert, wenn LLDP auf der Schnittstelle aktiviert ist. Es werden nur CDP-TLVs dekodiert, die einem entsprechenden Feld in der LLDP-Nachbartabelle zugeordnet werden können. Alle anderen TLVs werden verworfen (nicht erkannte CDP-TLVs und verworfene CDP-Frames werden in den LLDP-Statistiken nicht angezeigt). CDP-TLVs werden wie unten dargestellt der LLDP-Nachbartabelle zugeordnet. Die CDP-TLV „Device ID“ wird dem Feld „LLDP Chassis ID“ zugeordnet. Das CDP-TLV „Adresse“ wird dem Feld „LLDP-Verwaltungsadresse“ zugeordnet. Das CDP-TLV „Adresse“ kann mehrere Adressen enthalten, jedoch wird in der LLDP-Nachbartabelle nur die erste Adresse angezeigt. Die CDP-TLV-Port-ID wird dem Feld „LLDP-Port-ID“ zugeordnet. Die CDP-TLV-Felder „Version“ und „Plattform“ werden dem LLDP-Feld „Systembeschreibung“ zugeordnet. Sowohl CDP als auch LLDP unterstützen Systemfunktionen, doch die CDP-Funktionen umfassen auch Funktionen, die nicht Teil von LLDP sind. Diese Funktionen werden in der LLDP-Nachbartabelle als „Sonstige“ angezeigt. Wenn die CDP-Erkennung auf allen Schnittstellen deaktiviert ist, leitet der Switch die von Nachbargeräten empfangenen CDP-Frames weiter. Ist die CDP-Erkennung auf mindestens einer Schnittstelle aktiviert, werden alle CDP-Frames vom Switch beendet. **HINWEIS:** Wenn die CDP-Erkennung auf einer Schnittstelle deaktiviert ist, werden die CDP-Informationen nicht sofort entfernt, sondern erst, wenn die Haltezeit überschritten ist.
Portbeschreibung	Optionaler TLV: Wenn diese Option aktiviert ist, wird die Portbeschreibung in die übertragenen LLDP-Informationen aufgenommen.
Systemname	Optionales TLV: Wenn diese Option aktiviert ist, wird der Systemname in die übertragenen LLDP-Informationen aufgenommen.
Systembeschreibung	Optionales TLV: Wenn diese Option aktiviert ist, wird die Systembeschreibung in die übertragenen LLDP-Informationen aufgenommen.
Systemkapazität	Optionales TLV: Wenn diese Option aktiviert ist, wird die Systemkapazität in die übertragenen LLDP-Informationen aufgenommen.
Verwaltungsadresse	Optionales TLV: Wenn diese Option aktiviert ist, wird die Verwaltungsadresse in die übertragenen LLDP-Informationen aufgenommen.

Konfiguration > LLDP > LLDP-MED

LLDP-MED-Konfiguration

Auf dieser Seite können Sie LLDP-MED konfigurieren. Diese Funktion gilt für VoIP-Geräte, die LLDP-MED unterstützen.

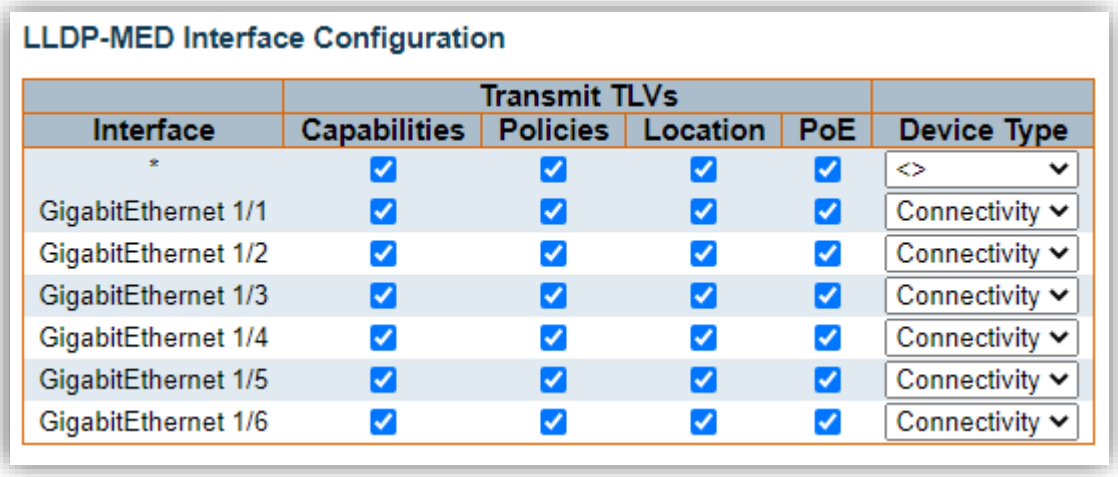
Anzahl der Schnellstart-Wiederholungen



Schnellstart und Standortidentifizierung für Notrufdienste Die Erkennung von Endpunkten ist ein äußerst wichtiger Aspekt von VoIP-Systemen im Allgemeinen. Darüber hinaus ist es ratsam, nur jene Informationen zu übermitteln, die für bestimmte Endpunkttypen spezifisch relevant sind (z. B. die Sprachnetzwerkrichtlinie nur an zugelassene sprachfähige Geräte zu übermitteln), um sowohl den begrenzten LLDPU-Speicherplatz zu schonen als auch Sicherheits- und Systemintegritätsprobleme zu verringern, die durch unangemessene Kenntnis der Netzwerkrichtlinie entstehen können.
Vor diesem Hintergrund definiert LLDP-MED eine LLDP-MED-Fast-Start-Interaktion zwischen der Protokollschicht und den darüber liegenden Anwendungsschichten, um diese Eigenschaften zu erreichen. Zu Beginn überträgt ein Netzwerkverbindungsgerät ausschließlich LLDP-TLVs in einer LLDPDU. Erst nachdem ein LLDP-MED-Endgerät erkannt wurde, beginnt ein LLDP-MED-fähiges Netzwerkverbindungsgerät, LLDP-MED-TLVs in ausgehenden LLDPDUs auf der zugehörigen Schnittstelle zu übertragen. Die LLDP-MED-Anwendung beschleunigt vorübergehend die Übertragung der LLDPDU, sodass diese innerhalb einer Sekunde beginnt, sobald ein neuer LLDP-MED-Nachbar erkannt wurde, um LLDP-MED-Informationen so schnell wie möglich an neue Nachbarn weiterzugeben.
Da das Risiko besteht, dass ein LLDP-Frame während der Übertragung zwischen Nachbarn verloren geht, wird empfohlen, die „Fast Start“-Übertragung mehrmals zu wiederholen, um die Wahrscheinlichkeit zu erhöhen, dass die Nachbarn den LLDP-Frame empfangen. Mit **der „Fast Start Repeat Count“** lässt sich festlegen, wie oft die „Fast Start“-Übertragung wiederholt werden soll. Der empfohlene Wert beträgt 4 Mal, da bei Empfang eines LLDP-Frames mit neuen Informationen 4 LLDP-Frames im Abstand von jeweils 1 Sekunde übertragen werden.
Es ist zu beachten, dass LLDP-MED und der LLDP-MED-Fast-Start-Mechanismus ausschließlich für den Einsatz auf Verbindungen zwischen LLDP-MED-Netzwerkverbindungsgeräten und Endgeräten vorgesehen sind und daher nicht für Verbindungen zwischen Elementen der LAN-Infrastruktur – einschließlich Netzwerkverbindungsgeräten – oder anderen Verbindungstypen gelten.

LLDP-MED-Schnittstellenkonfiguration

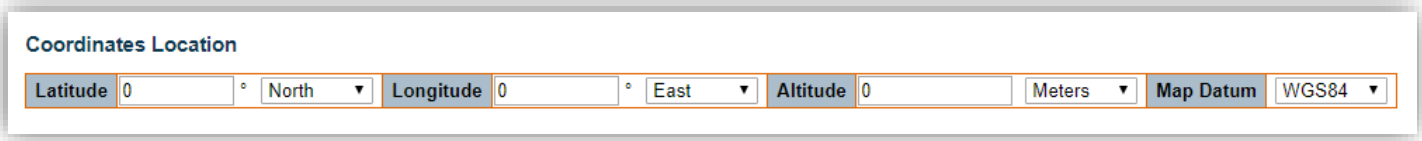
Es ist möglich auszuwählen, welche LLDP-MED-Informationen an die Nachbarn übertragen werden sollen. Wenn das Kontrollkästchen aktiviert ist, werden die Informationen in den an den Nachbarn übertragenen Frame aufgenommen.



Einstellung	Beschreibung
Schnittstelle	Der Name der Schnittstelle, für die die Konfiguration gilt.
TLVs übertragen – Funktionen	Wenn diese Option aktiviert ist, werden die Funktionen des Switches in die übertragenen LLDP-MED-Informationen aufgenommen.
TLVs senden – Richtlinien	Wenn diese Option aktiviert ist, werden die für die Schnittstelle konfigurierten Richtlinien in die übertragenen LLDP-MED-Informationen aufgenommen.
TLVs senden – Standort	Wenn diese Option aktiviert ist, werden die konfigurierten Standortinformationen des Switches in die übertragenen LLDP-MED-Informationen aufgenommen.
TLVs senden – PoE	Wenn diese Option aktiviert ist, werden die für die Schnittstelle konfigurierten PoE-Informationen (Power Over Ethernet) in die übertragenen LLDP-MED-Informationen aufgenommen.
Gerätetyp	Jedes LLDP-MED-Gerät arbeitet als ein bestimmter Typ von LLDP-MED-Gerät, bei dem es sich entweder um ein Netzwerkverbindungsgerät oder um eine bestimmte Klasse von Endgeräten handeln kann, wie unten definiert. Ein Netzwerkverbindungsgerät ist ein LLDP-MED-Gerät, das LLDP-MED-Endgeräten den Zugriff auf die IEEE-802-basierte LAN-Infrastruktur ermöglicht. Ein LLDP-MED-Netzwerkverbindungsgerät ist ein LAN-Zugangsgerät, das auf einer der folgenden Technologien basiert: 1. LAN-Switch/Router 2. IEEE 802.1-Bridge 3. IEEE 802.3-Repeater (aus historischen Gründen enthalten) 4. IEEE 802.11-WLAN-Zugangspunkt 5. Jedes Gerät, das die IEEE 802.1AB- und MED-Erweiterungen unterstützt und IEEE 802-Frames auf beliebige Weise weiterleiten kann. Ein Endgerät ist ein LLDP-MED-Gerät, das am Netzwerkrand angesiedelt ist und bestimmte Aspekte von IP-Kommunikationsdiensten auf Basis der IEEE 802-LAN-Technologie bereitstellt.

	Der Hauptunterschied zwischen einem Netzwerkverbindungsgerät und einem Endpunktgerät besteht darin, dass nur ein Endpunktgerät den LLDP-MED-Informationsaustausch initiieren kann. Auch wenn ein Switch grundsätzlich immer ein Netzwerkverbindungsgerät sein sollte, ist es möglich, ihn so zu konfigurieren, dass er als Endgerät fungiert und dadurch den LLDP-MED-Informationsaustausch „ “ initiiert (im Fall, dass zwei Netzwerkverbindungsgeräte miteinander verbunden sind).

Koordinaten Standort



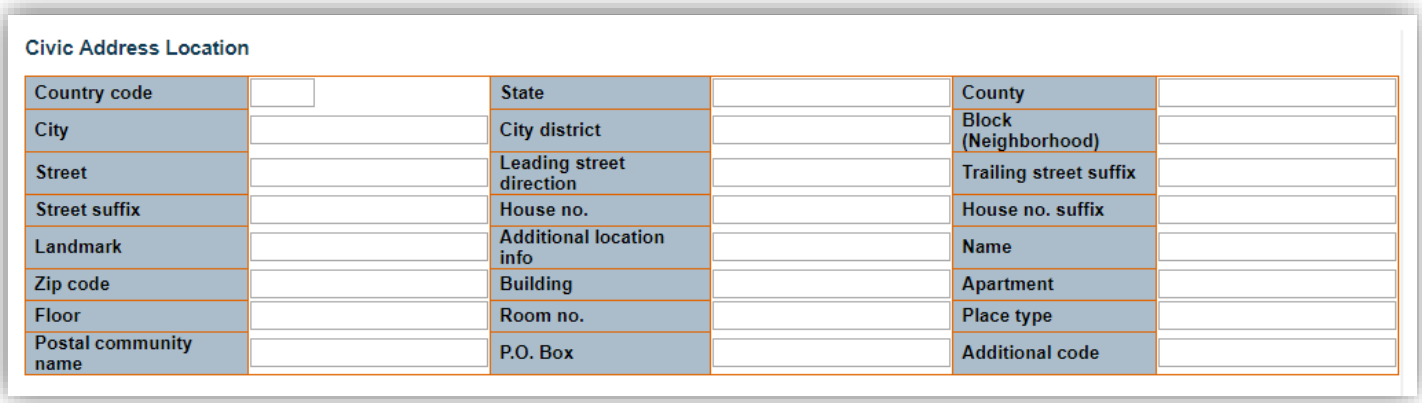
Einstellung	Beschreibung
Breitengrad	**Der Breitengrad** SOLLTE auf einen Wert zwischen 0 und 90 Grad mit maximal 4 Stellen normiert werden. Es ist möglich, die Richtung entweder nördlich oder **südlich** des Äquators anzugeben.
Längengrad	**Die Längengradangabe** SOLLTE auf einen Wert zwischen 0 und 180 Grad normiert werden und maximal 4 Ziffern umfassen. Es ist möglich, die Richtung entweder **östlich** oder **westlich** des Nullmeridians anzugeben.
Höhe	**Die Höhe** SOLLTE auf einen Wert zwischen -2097151,9 und 2097151,9 normiert werden, wobei maximal 1 Stelle angegeben werden darf. Es kann zwischen zwei Höhenangaben (Stockwerke oder Meter) gewählt werden. • **Meter:** Die Höhe wird in Metern angegeben, definiert durch den festgelegten vertikalen Bezugspunkt. • **Stockwerke:** Die Höhe wird in einer Form angegeben, die für Gebäude mit unterschiedlichen Abständen zwischen den Stockwerken relevanter ist. Eine Höhe von 0,0 ist auch außerhalb eines Gebäudes aussagekräftig und entspricht dem Bodenniveau bei den angegebenen Breiten- und Längengraden. Innerhalb eines Gebäudes entspricht 0,0 dem Stockwerk, das dem Bodenniveau am Haupteingang zugeordnet ist.
Kartensystem	Das **Kartendatum** wird für die in diesen Optionen angegebenen Koordinaten verwendet: • **WGS84:** (Geografisch 3D) – World Geodetic System 1984, CRS-Code 4327, Name des Nullmeridians: Greenwich. • **NAD83/NAVD88:** North American Datum 1983, CRS-Code 4269, Name des Nullmeridians: Greenwich; das zugehörige vertikale Bezugssystem ist das North American Vertical Datum von 1988 (NAVD88). Dieses Bezugssystempaar ist zu verwenden, wenn Standorte an Land referenziert werden, nicht in der Nähe von Gezeitengewässern (wo das Bezugssystem NAD83/MLLW verwendet würde). • **NAD83/MLLW:** North American Datum 1983, CRS-Code 4269, Name des Nullmeridians: Greenwich; das zugehörige vertikale Bezugssystem ist der mittlere Niedrigwasserstand (MLLW). Dieses Bezugssystempaar ist zu verwenden, wenn Standorte auf Gewässern/im Meer/im Ozean angegeben werden.

Standort anhand der Anschrift

IETF Geopriv-Konfigurationsinformationen für den Standort basierend auf der Anschrift (Civic Address LCI). Die Gesamtzahl der Zeichen für die kombinierten Anschriftangaben darf 250 Zeichen nicht überschreiten.

Einige Anmerkungen zur Beschränkung auf 250 Zeichen.

1. Ein nicht leerer Standort mit ziviler Anschrift benötigt zusätzlich zum Text der zivilen Anschrift 2 weitere Zeichen.
2. Der zweistellige Ländercode ist nicht Teil der Beschränkung auf 250 Zeichen.


Civic Address Location

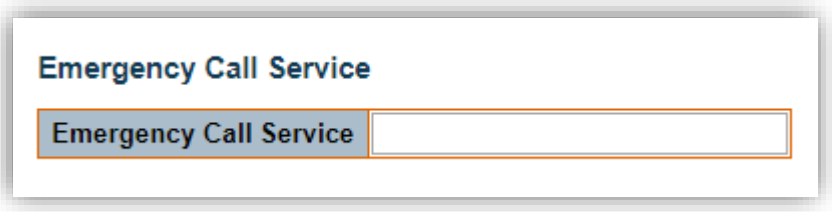
Country code		State		County	
City		City district		Block (Neighborhood)	
Street		Leading street direction		Trailing street suffix	
Street suffix		House no.		House no. suffix	
Landmark		Additional location info		Name	
Zip code		Building		Apartment	
Floor		Room no.		Place type	
Postal community name		P.O. Box		Additional code	

Einstellung	Beschreibung
Ländercode	Der zweistellige ISO 3166-Ländercode in Großbuchstaben (ASCII) – Beispiel: DK, DE oder US.
Bundesland	Nationale Untereinheiten (Bundesstaat, Kanton, Region, Provinz, Präfektur).
Landkreis	Landkreis, Gemeinde, Gun (Japan), Bezirk.
Stadt	Stadt, Gemeinde, Shi (Japan) – Beispiel: Kopenhagen.
Stadtbezirk	Stadtbezirk, Stadtteil, Stadtviertel, Bezirk, Chō (Japan).
Block (Stadtviertel)	Nachbarschaft, Block.
Straße	Straße – Beispiel: Poppelvej.
Richtung der Hauptstraße	Richtung der Hauptstraße – Beispiel: N.
Suffix am Ende der Straße	Endung der Straße – Beispiel: SW.
Straßenname-Endung	Straßensuffix – Beispiel: Ave, Platz.
Hausnummer	Hausnummer – Beispiel: 21.
Hausnummer-Suffix	Hausnummer-Suffix – Beispiel: A, 1/2.
Orientierungspunkt	Orientierungspunkt oder Sonderadresse – Beispiel: Columbia University.
Zusätzliche Standortangaben	Zusätzliche Standortangaben – Beispiel: Südflügel.
Name	Name (Bewohner und Büronutzer) – Beispiel: Flemming Jahn.
Postleitzahl	Postleitzahl – Beispiel: 2791.
Gebäude	Gebäude (Gebäude) – Beispiel: Low Library.
Wohnung	(Wohnung, Suite) – Beispiel: Apt 42.
Etage	Etage – Beispiel: 4.
Zimmer-Nr.	Zimmernummer – Beispiel: 450F.

Ortsart	Ortsart – Beispiel: Büro.
Name der Postgemeinde	Name der Postgemeinde – Beispiel: Leonia.
Postfach	Postfach (P.O. BOX) – Beispiel: 12345.
Zusatzcode	Zusatzcode – Beispiel: 1320300003.

Notrufdienst

Das Datenformat für die ELIN-Kennung des Notrufdienstes ist so definiert, dass die ELIN-Kennung, wie sie beim Aufbau eines Notrufs verwendet wird, an eine herkömmliche CAMA- oder ISDN-Trunk-basierte Notrufzentrale (PSAP) übermittelt wird. Dieses Format besteht aus einer numerischen Ziffernfolge, die der für Notrufe zu verwendenden ELIN entspricht.



Richtlinien

Die Netzwerkrichtlinienerkennung ermöglicht die effiziente Erkennung und Diagnose von Inkonsistenzen bei der VLAN-Konfiguration sowie der zugehörigen Layer-2- und Layer-3-Attribute, die für eine Reihe spezifischer Protokollanwendungen an diesem Port gelten. Falsche Netzwerkrichtlinienkonfigurationen stellen in VoIP-Umgebungen ein sehr großes Problem dar, das häufig zu einer Verschlechterung der Sprachqualität oder zu Dienstausfällen führt.
Richtlinien sind ausschließlich für die Verwendung mit Anwendungen vorgesehen, die spezifische „Echtzeit“-Anforderungen an die Netzwerkrichtlinien stellen, wie beispielsweise interaktive Sprach- und/oder Videodienste.
Die bekannt gegebenen Netzwerkrichtlinienattribute sind:

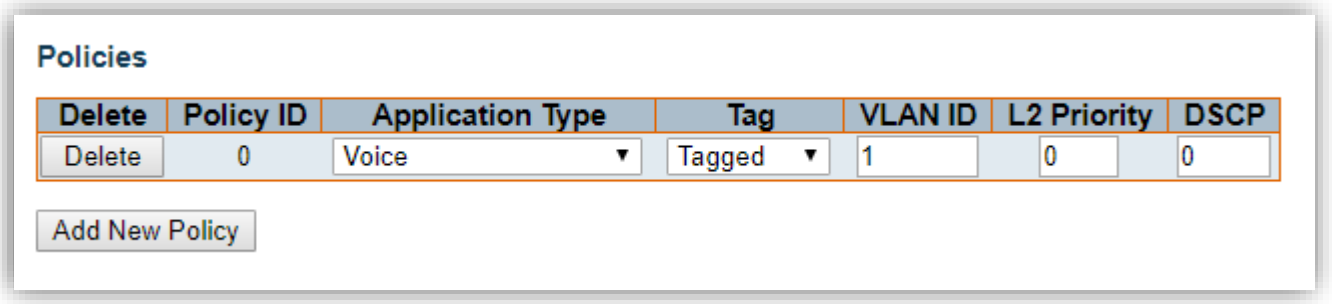
1. Layer-2-VLAN-ID (IEEE 802.1Q-2003)
2. Layer-2-Prioritätswert (IEEE 802.1D-2004)
3. Layer-3-Diffserv-Codepunkt (DSCP)-Wert (IETF RFC 2474)

Diese Netzwerkrichtlinie wird potenziell bekannt gegeben und mit mehreren Sätzen von Anwendungstypen verknüpft, die an einem bestimmten Port unterstützt werden. Die konkret angesprochenen Anwendungstypen sind:

1. Sprache
2. Gast-Sprachverkehr
3. Softphone-Sprachübertragung
4. Videokonferenzen
5. Streaming-Video
6. Steuerung/Signalisierung (unterstützt unter bestimmten Voraussetzungen eine separate Netzwerkrichtlinie für die oben genannten Medientypen)

Ein großes Netzwerk kann mehrere VoIP-Richtlinien unternehmensweit sowie unterschiedliche Richtlinien je nach Anwendungstyp unterstützen. LLDP-MED ermöglicht es, pro Port mehrere Richtlinien zu veröffentlichen, die jeweils einem anderen Anwendungstyp entsprechen. Verschiedene Ports desselben Netzwerkverbindungsgeräts können je nach authentifizierter Benutzeridentität oder Portkonfiguration unterschiedliche Richtliniensätze veröffentlichen.
Es ist zu beachten, dass LLDP-MED nicht dafür vorgesehen ist, auf anderen Verbindungen als denen zwischen Netzwerkverbindungsgeräten und Endpunkten zu laufen, und daher nicht die

Vielzahl von Netzwerkrichtlinien bekanntgeben muss, die häufig auf einer aggregierten Verbindung innerhalb des LANs laufen.



Einstellung	Beschreibung
Löschen	Aktivieren Sie dieses Kontrollkästchen, um die Richtlinie zu löschen. Sie wird beim nächsten Speichern gelöscht.
Richtlinien-ID	ID der Richtlinie. Diese wird automatisch generiert und muss bei der Auswahl der Richtlinien verwendet werden, die den jeweiligen Schnittstellen zugeordnet werden sollen.
Anwendungstyp	Verwendungszweck der Anwendungstypen: 1. **Sprache** – zur Verwendung mit dedizierten IP-Telefon-Endgeräten und anderen ähnlichen Geräten, die interaktive Sprachdienste unterstützen. Diese Geräte werden in der Regel in einem separaten VLAN bereitgestellt, um die Bereitstellung zu vereinfachen und die Sicherheit durch Isolierung von Datenanwendungen zu erhöhen. 2. **Sprachsignalisierung (bedingt)** – zur Verwendung in Netzwerktopologien, die für die Sprachsignalisierung eine andere Richtlinie erfordern als für die Sprachmedien. Dieser Anwendungstyp sollte nicht bekannt gegeben werden, wenn dieselben Netzwerkrichtlinien gelten wie die in der Sprach-Anwendungsrichtlinie bekannt gegebenen. 3. **Gast-Sprachverkehr** – unterstützt einen separaten Sprachdienst mit „eingeschränktem Funktionsumfang“ für Gastnutzer und Besucher mit eigenen IP-Telefon-Endgeräten und anderen ähnlichen Geräten, die interaktive Sprachdienste unterstützen. 4. **Gast-Sprachsignalisierung (bedingt)** – zur Verwendung in Netzwerktopologien, die eine andere Richtlinie für die Gast-Sprachsignalisierung erfordern als für die Gast-Sprachmedien. Dieser Anwendungstyp sollte nicht bekannt gegeben werden, wenn dieselben Netzwerkrichtlinien gelten wie die in der Richtlinie für die Gast-Sprach-Anwendung bekannt gegebenen. 5. **Softphone-Sprachdienst** – zur Verwendung durch Softphone-Anwendungen auf typischen datenzentrierten Geräten wie PCs oder Laptops. Diese Klasse von Endgeräten unterstützt häufig, wenn überhaupt, keine mehreren VLANs und ist in der Regel für die Nutzung eines „untagged“ VLANs oder eines einzelnen „tagged“ datenspezifischen VLANs konfiguriert. Wenn eine Netzwerkrichtlinie für die Verwendung mit einem „untagged“ VLAN definiert ist (siehe „Tagged“-Flag weiter unten), wird das L2-Prioritätsfeld ignoriert und nur der DSCP-Wert ist relevant. 6. **Videokonferenzen** – zur Nutzung durch dedizierte Videokonferenzgeräte und andere ähnliche Geräte, die interaktive Video-/Audio-Dienste in Echtzeit unterstützen.

	7. **Streaming-Video** – zur Nutzung für die Verteilung von Videoinhalten über Broadcast oder Multicast sowie für andere ähnliche Anwendungen, die Streaming-Videodienste unterstützen, die eine spezifische Behandlung im Rahmen der Netzwerkrichtlinien erfordern. Videoanwendungen, die auf TCP mit Pufferung basieren, fallen nicht unter die vorgesehene Nutzung dieses Anwendungstyps. 8. **Videosignalisierung (bedingt)** – zur Verwendung in Netzwerktopologien, die eine separate Richtlinie für die Videosignalisierung erfordern, die sich von der für die Videomedien unterscheidet. Dieser Anwendungstyp sollte nicht bekannt gegeben werden, wenn dieselben Netzwerkrichtlinien gelten wie die in der Anwendungsrichtlinie „Videokonferenzen“ bekannt gegebenen.
Tag	**Tag,** das angibt, ob der angegebene Anwendungstyp ein „getaggtes“ oder ein „ungetaggtes“ VLAN verwendet. **„Untagged“** gibt an, dass das Gerät ein untagged Frame-Format verwendet und daher keinen Tag-Header gemäß der Definition in IEEE 802.1Q-2003 enthält. In diesem Fall werden sowohl die VLAN-ID als auch die Layer-2-Prioritätsfelder ignoriert, und nur der DSCP-Wert ist relevant. **„Tagged“** gibt an, dass das Gerät das getaggte Frame-Format gemäß IEEE 802.1Q verwendet und dass sowohl die VLAN-ID als auch die Layer-2-Prioritätswerte sowie der DSCP-Wert verwendet werden. Das getaggte Format enthält ein zusätzliches Feld, das als Tag-Header bezeichnet wird. Das getaggte Frame-Format umfasst auch prioritätsgetaggte Frames gemäß der Definition in IEEE 802.1Q-2003.
VLAN-ID	VLAN-Kennung (VID) für die Schnittstelle gemäß der Definition in IEEE 802.1Q-2003.
L2-Priorität	Die L2-Priorität ist die Layer-2-Priorität, die für den angegebenen Anwendungstyp verwendet werden soll. Die L2-Priorität kann eine von acht Prioritätsstufen (0 bis 7) angeben, wie sie in der Norm IEEE 802.1D-2004 definiert sind. Der Wert 0 steht für die Verwendung der in IEEE 802.1D-2004 definierten Standardpriorität.
DSCP	DSCP-Wert, der verwendet wird, um das Diffserv-Knotenverhalten für den angegebenen Anwendungstyp gemäß der Definition in IETF RFC 2474 bereitzustellen. DSCP kann einen von 64 Codepunktwerten (0 bis 63) enthalten. Der Wert 0 steht für die Verwendung des Standard-DSCP-Werts gemäß der Definition in RFC 2475.
Hinzufügen einer neuen Richtlinie	Klicken Sie auf die Schaltfläche „**Neue** Richtlinie hinzufügen“, um eine neue Richtlinie hinzuzufügen. Geben Sie den Anwendungstyp, das Tag, die VLAN-ID, die L2-Priorität und den DSCP-Wert für die neue Richtlinie an. Klicken Sie auf „Speichern“. Es werden 32 Richtlinien unterstützt

Konfiguration der Richtlinien-Schnittstelle

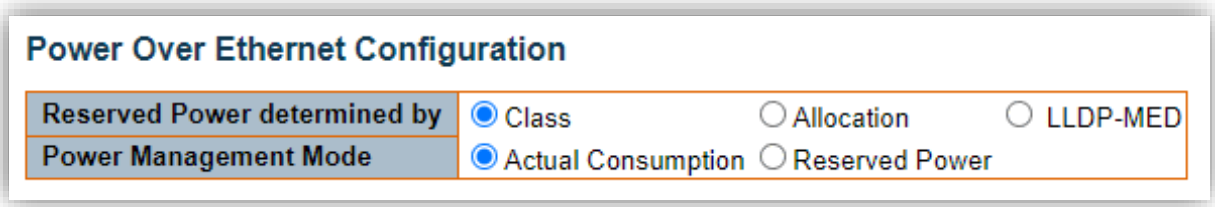
Jede Schnittstelle kann je nach authentifizierter Benutzeridentität oder Schnittstellenkonfiguration einen eindeutigen Satz von Netzwerkrichtlinien oder unterschiedliche Attribute für dieselben Netzwerkrichtlinien bekanntgeben.

Einstellung	Beschreibung
Schnittstelle	Der Name der Schnittstelle, für die die Konfiguration gilt.

Richtlinien-ID	Die Gruppe von Richtlinien, die für eine bestimmte Schnittstelle gelten sollen. Die Gruppe von Richtlinien wird durch Aktivieren der entsprechenden Kontrollkästchen ausgewählt.

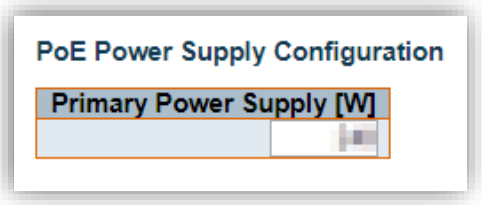
Konfiguration > PoE > Leistungsbudget

Power-over-Ethernet-Konfiguration



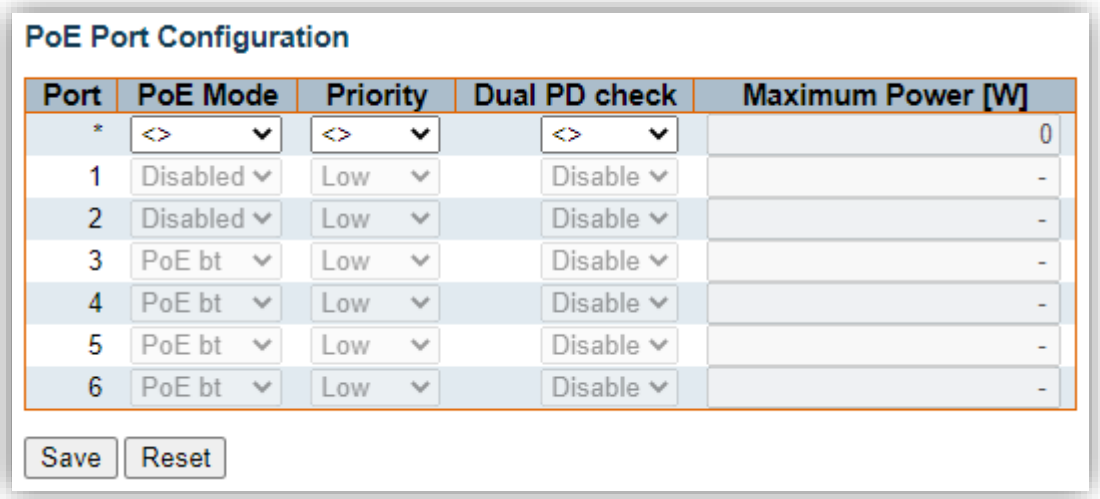
Einstellung	Beschreibung
Reservierte Leistung, bestimmt durch	Es gibt drei Modi zur Konfiguration der Leistungsreservierung für Ports/PDs. 1. **Zuweisungsmodus:** In diesem Modus legt der Benutzer fest, wie viel Leistung jeder Port reservieren darf. Die zugewiesene/reservierte Leistung für jeden Port/jedes PD wird in den Feldern „Maximale Leistung“ angegeben. 2. **Modus „Class“:** In diesem Modus bestimmt jeder Port automatisch, wie viel Leistung entsprechend der Klasse, zu der das angeschlossene PD gehört, reserviert werden soll, und reserviert die Leistung entsprechend. Es gibt vier verschiedene Portklassen: jeweils eine für 4, 7, 15,4 oder 30 Watt. In diesem Modus haben die Felder „Maximale Leistung“ keine Auswirkung. 3. **LLDP-MED-Modus:** Dieser Modus ähnelt dem Klassenmodus, mit dem Unterschied, dass jeder Port die zu reservierende Leistung durch den Austausch von PoE-Informationen über das LLDP-Protokoll ermittelt und die Leistung entsprechend reserviert. Sind für einen Port keine LLDP-Informationen verfügbar, reserviert der Port die Leistung im Klassenmodus. In diesem Modus haben die Felder „Maximale Leistung“ keine Auswirkung **Für alle Modi** gilt**:** Verbraucht ein Port mehr Leistung als die für ihn reservierte, wird der Port abgeschaltet.
Energieverwaltungsmodus	Es gibt zwei Modi zur Konfiguration, wann die Ports abgeschaltet werden sollen: 1. **Tatsächlicher Verbrauch:** In diesem Modus werden die Ports abgeschaltet, wenn der tatsächliche Stromverbrauch aller Ports die von der Stromversorgung lieferbare Leistung übersteigt oder wenn der tatsächliche Stromverbrauch eines bestimmten Ports die für diesen Port reservierte Leistung übersteigt. Die Ports werden entsprechend ihrer Priorität abgeschaltet. Haben zwei Ports dieselbe Priorität, wird der Port mit der höheren Portnummer abgeschaltet. 2. **Reservierte Leistung:** In diesem Modus werden die Ports abgeschaltet, wenn die insgesamt reservierte Leistung die vom Netzteil lieferbare Leistung übersteigt. In diesem Modus wird die Stromversorgung des Ports nicht eingeschaltet, wenn das PD mehr Leistung anfordert, als vom Netzteil zur Verfügung steht.

Konfiguration des PoE-Netzteils



Einstellung	Beschreibung
Primäres Netzteil [W]	Um die von dem PD nutzbare Leistung bestimmen zu können, muss festgelegt werden, wie viel Leistung eine Stromquelle liefern kann. Gültige Werte liegen im Bereich von 0 bis 240 Watt.

PoE-Port-Konfiguration



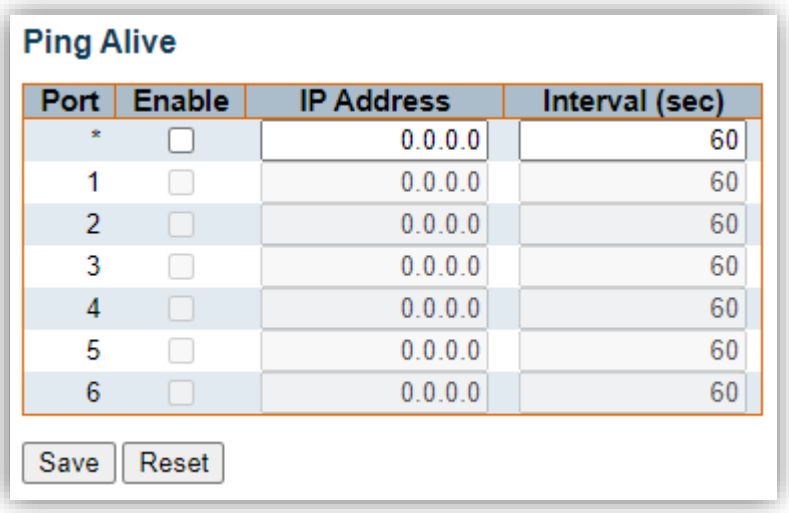
Einstellung	Beschreibung
PoE-Modus	Der PoE-Modus gibt den PoE-Betriebsmodus für den Port an. • **Deaktiviert:** PoE ist für den Port deaktiviert. • **PoE:** Aktiviert PoE nach IEEE 802.3af (PDs der Klasse 4 auf 15,4 W begrenzt) • **PoE+:** Aktiviert PoE+ nach IEEE 802.3at (PDs der Klasse 4 auf 30 W begrenzt) • **PoE bt:** Aktiviert PoE bt nach IEEE 802.3bt (PDs der Klasse 8 auf 90 W begrenzt)
Priorität	Die Priorität gibt die Priorität des Ports an. Es gibt drei Stufen der Stromversorgungspriorität: **„Low“, „High“** und **„Critical**“. Die Priorität kommt zum Einsatz, wenn die Remote-Geräte mehr Strom benötigen, als das Netzteil liefern kann. In diesem Fall wird der Port mit der niedrigsten Priorität abgeschaltet, beginnend mit dem Port mit der höchsten Portnummer.
Dual-PD-Prüfung	Wenn **die Dual-PD-Prüfung** aktiviert ist und auf einem der Kanäle eine ungültige Erkennungssignatur festgestellt wird, führt Port n keine Klassifizierung durch und gewährt keine Einschaltanfragen. Wenn die Dual-PD-Prüfung deaktiviert ist, erkennt, klassifiziert und bedient Port n Einschaltanfragen für jeden Kanal, unabhängig vom Erkennungsergebnis auf dem anderen Kanal.

Maximale Leistung	Der Wert „Maximale Leistung“ gibt die maximale Leistung in Watt an, die an ein Remote-Gerät geliefert werden kann. Der maximal zulässige Wert beträgt 90 W.

Konfiguration > PoE > Ping Alive

Ping Alive

Auf dieser Seite kann der Benutzer die Fehlerüberprüfung für die mit Strom versorgten Geräte des Systems steuern.



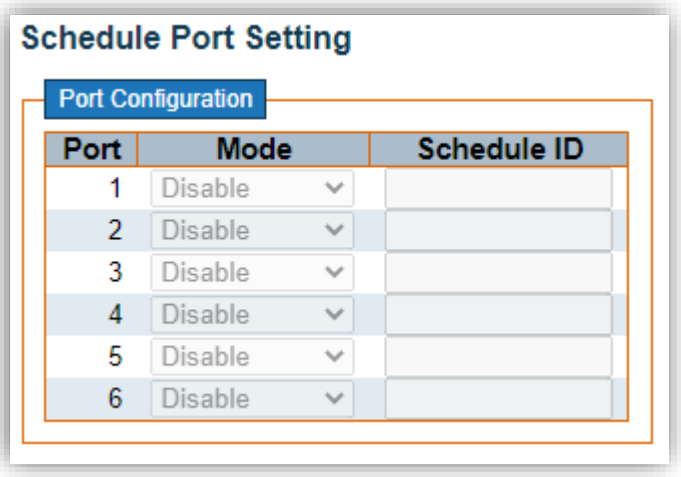
Port-Konfiguration

Einstellung	Beschreibung
Port	Die Switch-Portnummer des Ports.
Aktivieren	Legt fest, ob „Poe Ping Alive“ an diesem Switch-Port aktiviert ist.
IP-Adresse	Die IP-Adresse des mit Strom versorgten Geräts.
Intervall	Die Zeitspanne für die IP-Überprüfung.

Konfiguration > PoE > Zeitplan

Zeitplan-Port-Einstellungen

Diese Seite ist in die Bereiche „Port-Konfiguration“ und „Zeitplan-Einstellungen“ unterteilt. Über die Port-Konfiguration kann der Benutzer für jeden PoE-Port eine PoE-Zeitplan-ID und einen PoE-Zeitplanmodus festlegen. Über die Zeitplan-Einstellungen kann der Benutzer neue Zeitpläne hinzufügen.



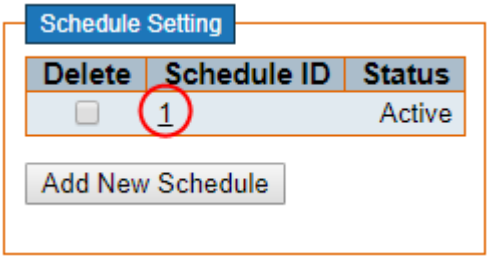
Port-Konfiguration

Einstellung	Beschreibung
Port	Die Switch-Portnummer des Ports.
Modus	**Deaktivieren:** Deaktiviert den Zeitplanbetrieb. **Zeitplan ein:** Liegt die aktuelle Uhrzeit innerhalb des Zeitplanbereichs, versorgt die PSE das PD mit Strom. **Zeitplan aus:** Liegt die aktuelle Uhrzeit innerhalb des Zeitplanbereichs, versorgt die PSE das PD nicht mit Strom.
Zeitplan-ID	Legt fest, ob der Zeitplan ausgeführt werden soll. Die Zeitplan-ID liegt im Bereich von 1 bis 32.

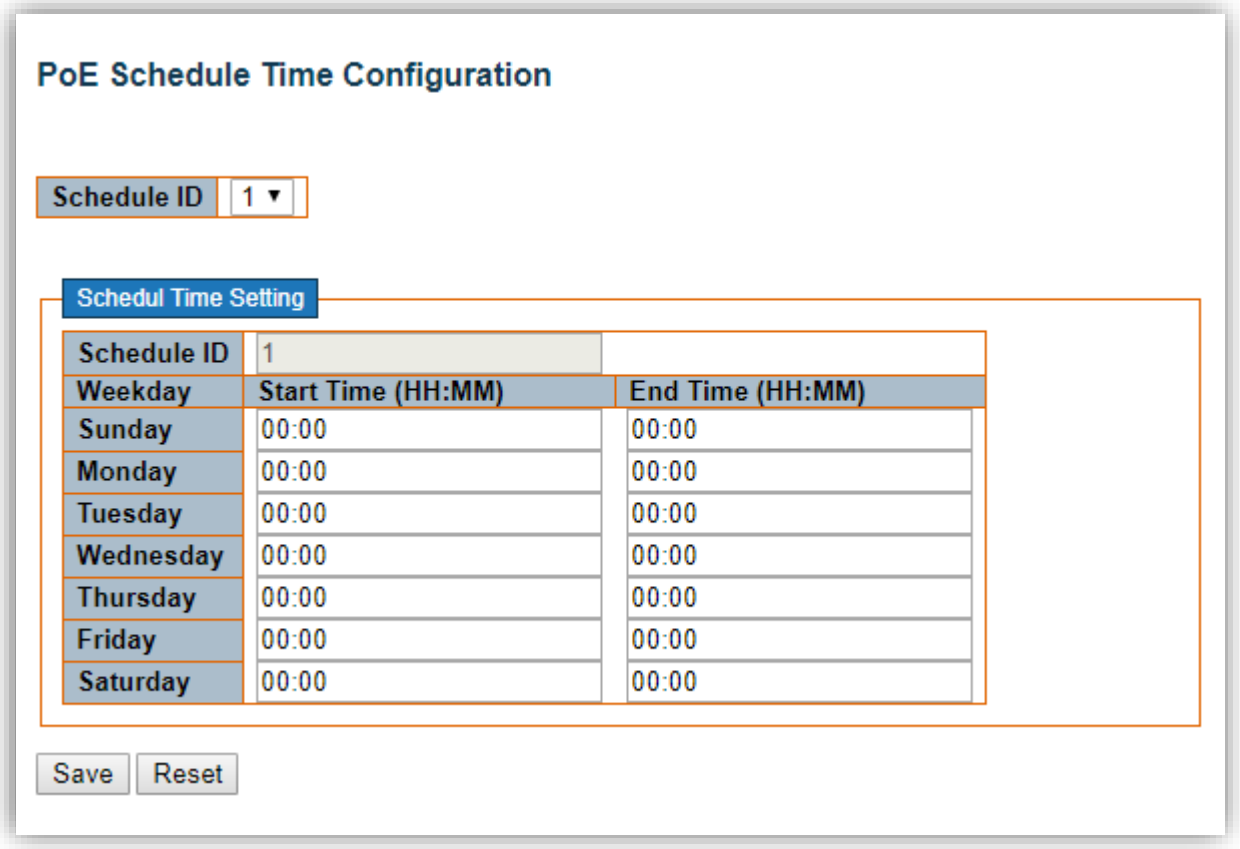
Zeitplan-Einstellung

Einstellung	Beschreibung
Zeitplan-ID	PoE-Zeitplan-ID. Die Zeitplan-ID liegt im Bereich von 1 bis 32.
Status	Status des PoE-Zeitplans.

Konfiguration der PoE-Zeitplanung



Klicken Sie auf die Zeitplan-ID **unter „Zeitplan-Einstellungen“,** um die Konfiguration der PoE-Zeitpläne zu bearbeiten

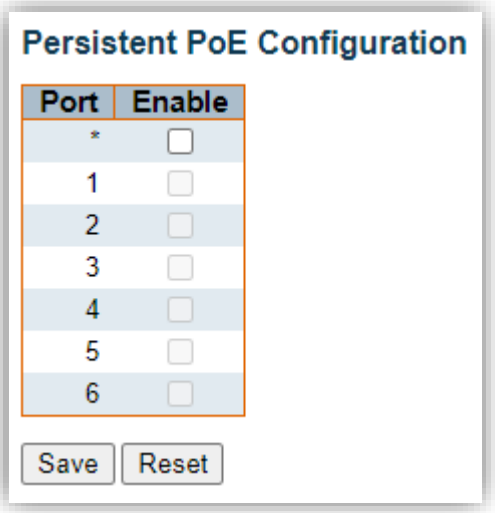


Einstellung	Beschreibung
Zeitplan-ID	Die ID-Nummer des Zeitplans.
Zeit	**Startzeit:** Startzeit des Zeitplans. Format: hh:mm; hh: 00 bis 24, mm: 00 bis 59. **Endzeit:** Endzeit des Zeitplans. Format: hh:mm; hh: 00 bis 24, mm: 00 bis 59.

Konfiguration > PoE > Persistentes PoE

Persistente PoE-Konfiguration

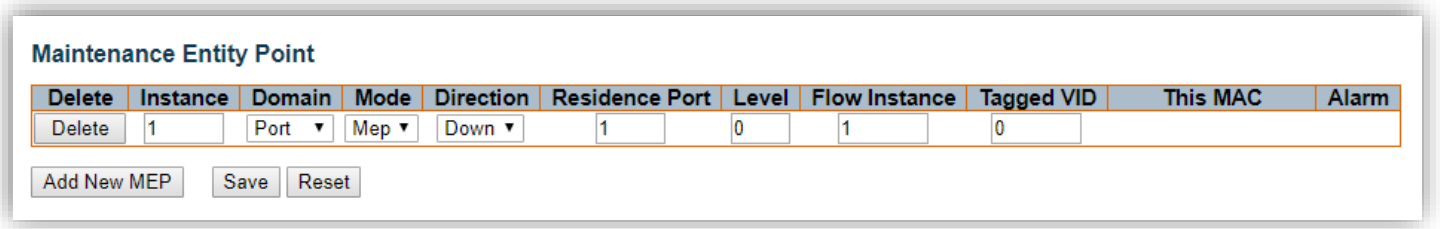
Wenn der Switch einen Reset durchführt und ein Firmware-Upgrade erhält, kann der PSE (PoE-Switch) die PoE-Stromversorgung für das PD weiterhin aufrechterhalten.



Einstellung	Beschreibung	Werkseinstellung
Aktiviert	Aktiviert den dauerhaften PoE-Betrieb.	Deaktiviert
Deaktiviert	Deaktivieren Sie den permanenten PoE-Betrieb.	

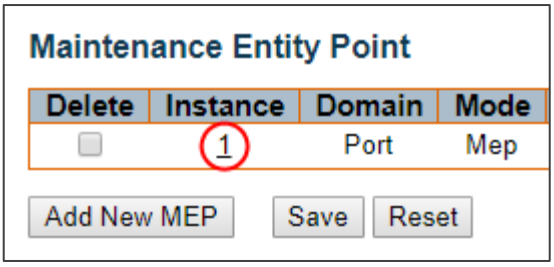
Konfiguration > MEP

Wartungs-Entitätspunkt



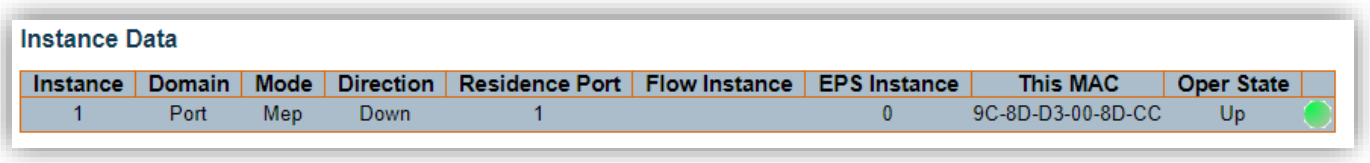
Einstellung	Beschreibung
Löschen	Dieses Kontrollkästchen dient dazu, einen MEP für die Löschung beim nächsten Speichervorgang zu markieren.
Instanz	Die ID des MEP. Klicken Sie auf die ID eines MEP, um die Konfigurationsseite aufzurufen. Der Bereich reicht von **1** bis **100**.
Domäne	**Port:** Dies ist ein MEP in der Port-Domäne.
Modus	**MEP:** Dies ist ein Wartungsentitäts-Endpunkt. **MIP:** Dies ist ein Zwischenpunkt der Wartungseinheit.
Richtung	**Down:** Dies ist ein Down-MEP – Überwachung des eingehenden OAM und des Datenverkehrs am Residence-Port. **Up:** Dies ist ein Up-MEP – Überwachung des ausgehenden OAM und des Datenverkehrs am „Residence Port“.
Residence-Port	Der Port, den der MEP überwacht – siehe „Richtung“. Bei einem EVC-MEP muss es sich um einen Port im EVC handeln. Bei einem VLAN-MEP muss der Port Mitglied eines VLANs sein.
Ebene	Die MEG-Ebene dieses MEP.
Flow-Instanz	Das MEP ist mit diesem Flow verknüpft – siehe „Domäne“. Dies ist bei einem Port-MEP nicht relevant und wird daher nicht angezeigt.
Getaggte VID	**Port-MEP:** Ein äußeres C/S-Tag (abhängig vom VLAN-Porttyp) wird mit dieser VID hinzugefügt. Die Eingabe von „0“ bedeutet, dass kein Tag hinzugefügt wird. **EVC-MEP:** Dies wird nicht verwendet. **VLAN-MEP:** Dies wird nicht verwendet. **EVC-MIP:** Bei Serval handelt es sich hierbei um die Teilnehmer-VID, die den Teilnehmer-Datenfluss in diesem EVC identifiziert, in dem das MIP aktiv ist.
Diese MAC-Adresse	Die MAC-Adresse dieses MEP – kann von anderen MEPs verwendet werden, wenn Unicast ausgewählt ist (nur zur Information).
Alarm	Auf dem MEP liegt ein aktiver Alarm vor.

MEP-Konfiguration



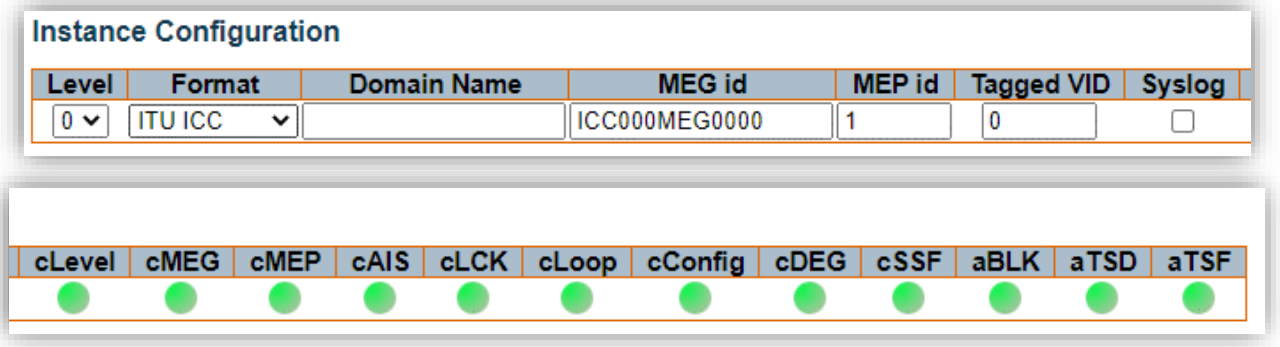
Klicken Sie auf die Instanznummer **des „Maintenance Entity Point“,** um die MEP-Konfiguration zu bearbeiten

Instanzdaten



Einstellung	Beschreibung
Instanz	Die ID des MEP.
Domäne	**Port:** Dies ist ein MEP in der Port-Domäne.
Modus	**MEP:** Dies ist ein Wartungsentitäts-Endpunkt. **MIP:** Dies ist ein Zwischenpunkt der Wartungseinheit.
Richtung	**Down:** Dies ist ein Down-MEP – Überwachung des eingehenden OAM-Verkehrs und des Datenverkehrs am Residence-Port. **Up:** Dies ist ein Up-MEP
Residence-Port	Der Port, den der MEP überwacht – siehe „Richtung“. Bei einem EVC-MEP muss es sich um einen Port im EVC handeln. Bei einem VLAN-MEP muss der Port Mitglied eines VLANs sein.
Flow-Instanz	Das MEP steht in Zusammenhang mit diesem Datenfluss – siehe „Domäne“. Dies ist im Falle eines Port-MEP nicht relevant und wird daher nicht angezeigt.
Getaggte VID	**Port-MEP:** Ein äußeres C/S-Tag (abhängig vom VLAN-Porttyp) wird mit dieser VID hinzugefügt. Die Eingabe von „0“ bedeutet, dass kein Tag hinzugefügt wird. **EVC-MEP:** Dies wird nicht verwendet. **VLAN-MEP:** Dies wird nicht verwendet. **EVC-MIP:** Bei Serval handelt es sich hierbei um die Teilnehmer-VID, die den Teilnehmer-Datenfluss in diesem EVC identifiziert, in dem das MIP aktiv ist.
Diese MAC-Adresse	Die MAC-Adresse dieses MEP – kann von anderen MEPs verwendet werden, wenn Unicast ausgewählt ist (nur zur Information).
Betriebsstatus	Betriebsstatus, der einen der folgenden Werte annehmen kann: **Up**: Die Instanz ist UP, d. h., sie ist physisch konfiguriert und betriebsbereit. **Down**: Die Instanz ist DOWN, d. h., sie ist NICHT physisch konfiguriert und betriebsbereit. **Config**: Die Instanz ist aufgrund einer ungültigen Konfiguration DOWN. **HW**: Die Instanz ist DOWN, da die OAM-unterstützenden Hardware-Ressourcen ausgefallen sind. **MCE**: Die Instanz ist aufgrund ausgefallener MCE-Ressourcen „DOWN“.

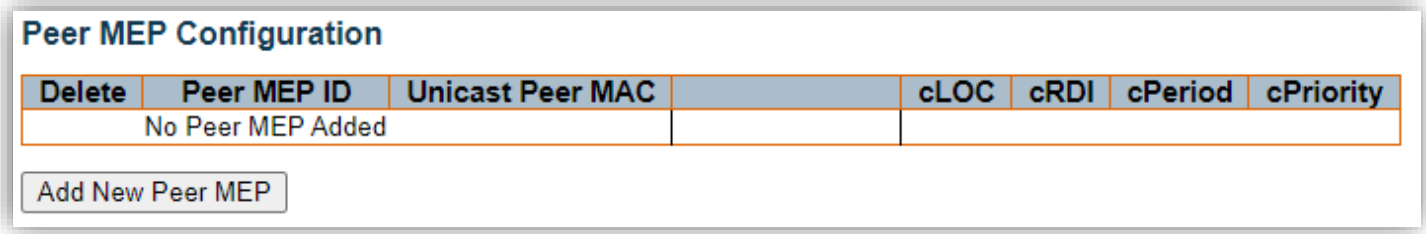
Instanzkonfiguration



Einstellung	Beschreibung
Ebene	Die MEG-Stufe dieses MEP.
Format	Dies ist die Konfiguration der beiden möglichen Formate für den Maintenance Association Identifier. • **ITU ICC:** Dies ist durch die ITU definiert (Y1731 Abb. A3). „Domain Name“ wird nicht verwendet. „MEG id“ darf maximal 13 Zeichen lang sein. • **IEEE-Zeichenkette:** Diese ist durch IEEE (802.1ag Abschnitt 21.6.5) definiert. „Domain Name“ darf maximal 16 Zeichen lang sein. „MEG id“ (kurzer MA-Name) darf maximal 16 Zeichen lang sein. • **ITU CC ICC:** Dies ist durch die ITU definiert (Y1731, Abb. A5). „Domain Name“ wird nicht verwendet. „MEG id“ darf maximal 15 Zeichen lang sein.
Domänenname	Dies ist der IEEE-Wartungsdomänenname und wird nur im Falle des Formats „IEEE-Zeichenkette“ verwendet. Diese Zeichenkette kann leer sein, was dem Format 1 für den Wartungsdomänennamen entspricht – nicht vorhanden. Sie darf maximal 16 Zeichen lang sein.
MEG-ID	Dies ist entweder die ITU-MEG-ID oder der IEEE-Kurzname der MA – abhängig vom „Format“. Siehe „Format“. Beim ITU-ICC-Format muss diese 13 Zeichen lang sein. Beim ITU-CC-ICC-Format muss diese 15 Zeichen lang sein. Beim IEEE-String-Format darf diese maximal 16 Zeichen lang sein.
MEP-ID	Dieser Wert wird zur übertragenen zweibytigen CCM-MEP-ID.
Tagged VID	Dieser Wert ist die VID eines TAGs, das der OAM-PDU hinzugefügt wurde.
Syslog	Wenn diese Option aktiviert ist, werden Benachrichtigungen im Syslog protokolliert.
cLevel	Fehlerursache, die darauf hinweist, dass ein CCM mit einer niedrigeren Stufe als der für dieses MEP konfigurierten empfangen wurde.
cMEG	Fehlerursache, die darauf hinweist, dass ein CCM mit einer MEG-ID empfangen wurde, die von der für diesen MEP konfigurierten abweicht.
cMEP	Fehlerursache, die anzeigt, dass ein CCM mit einer MEP-ID empfangen wurde, die sich von allen für diesen MEP konfigurierten „Peer-MEP-IDs“ unterscheidet.
cAIS	Fehlerursache, die anzeigt, dass eine AIS-PDU empfangen wurde.
cLCK	Fehlerursache, die anzeigt, dass eine LCK-PDU empfangen wurde.
cLoop	Fehlerursache, die anzeigt, dass eine Schleife erkannt wurde, da ein CCM mit der eigenen MEP-ID und dem eigenen SMAC empfangen wurde.
cConfig	Fehlerursache, die anzeigt, dass ein Konfigurationsfehler erkannt wurde, da ein CCM mit der eigenen MEP-ID empfangen wurde.
cDEG	Fehlerursache, die anzeigt, dass die Server-Ebene einen Signalabfall meldet.

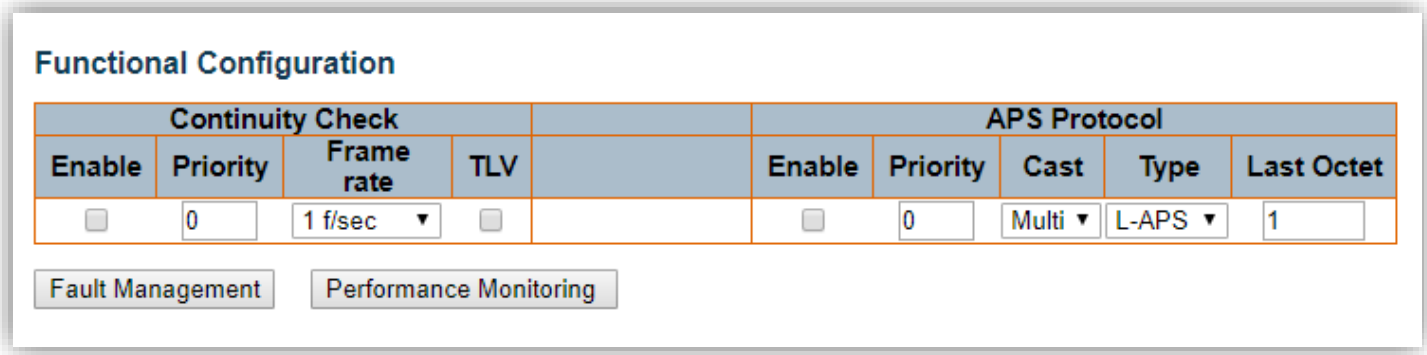
cSSF	Fehlerursache, die darauf hinweist, dass die Server-Ebene einen Signalausfall meldet.
aBLK	Die daraus resultierende Maßnahme, Service-Frames in diesem Datenfluss zu blockieren, ist aktiv.
aTSD	Die Folgeaktion zur Meldung einer Verschlechterung des Trail-Signals wird berechnet.
aTSF	Die Folgeaktion zur Anzeige eines „Trail Signal Fail“ in Richtung Schutz ist aktiv.

Peer-MEP-Konfiguration



Einstellung	Beschreibung
Löschen	Dieses Kontrollkästchen dient dazu, ein Peer-MEP für die Löschung beim nächsten Speichervorgang zu markieren.
Peer-MEP-ID	Dieser Wert wird zur erwarteten MEP-ID in einem empfangenen CCM – siehe „cMEP“.
Unicast-Peer-MAC	Diese MAC-Adresse wird verwendet, wenn bei diesem Peer-MEP Unicast ausgewählt ist. Außerdem wird diese MAC-Adresse verwendet, um eine Hardware-Prüfung der von diesem MEP empfangenen CCM-PDU (LOC-Erkennung) durchzuführen.
cLOC	Fehlerursache, die anzeigt, dass kein CCM (innerhalb von 3,5 Perioden) von diesem Peer-MEP empfangen wurde.
cRDI	Fehlerursache, die anzeigt, dass ein CCM mit einer Remote-Fehleranzeige empfangen wurde – von diesem Peer-MEP.
cPeriod	Fehlerursache, die anzeigt, dass ein CCM mit einer Periode empfangen wurde, die von der für diesen MEP konfigurierten Periode abweicht – von diesem Peer-MEP.
cPriority	Fehlerursache, die anzeigt, dass ein CCM mit einer Priorität empfangen wurde, die von der für diesen MEP konfigurierten Priorität abweicht – von diesem Peer-MEP.

Funktionskonfiguration

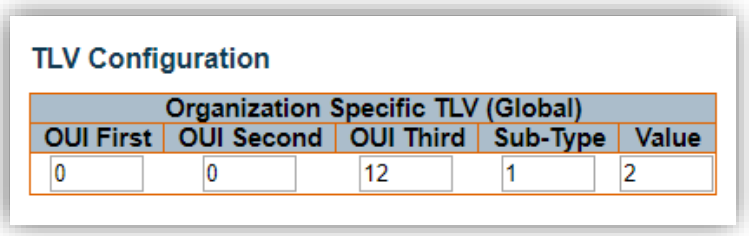


Einstellung	Beschreibung

Kontinuitätsprüfung	• **Aktivieren:** Die Kontinuitätsprüfung auf Basis der Übertragung/des Empfangs von CCM-PDUs kann aktiviert oder deaktiviert werden. Die CCM-PDU wird immer als Multicast-Klasse 1 übertragen. • **Priorität:** Die Priorität, die als PCP-Bits in den TAG eingefügt werden soll (falls vorhanden). Wenn sowohl die Kontinuitätsprüfung als auch die Verlustmessung aktiviert sind und beide auf einem softwarebasierten CCM implementiert sind, muss die „Priorität“ identisch sein. • **Rahmenrate:** Auswahl der Rahmenrate der CCM-PDU. Dies ist der Kehrwert der Übertragungsperiode gemäß Y.1731. Dieser Wert hat folgende Verwendungszwecke: a. Die Übertragungsrate der CCM-PDU. b. Die Fehlerursache „cLOC“ wird gemeldet, wenn innerhalb von 3,5 Perioden keine CCM-PDU empfangen wurde – siehe „cLOC“. c. Die Fehlerursache „cPeriod“ wird gemeldet, wenn eine CCM-PDU mit einer abweichenden Periode empfangen wurde – siehe „cPeriod“. Durch die Auswahl von 300 f/s oder 100 f/s wird (sofern möglich) ein hardwarebasiertes CCM konfiguriert. Bei Auswahl anderer Bildraten wird ein softwarebasiertes CCM konfiguriert. Bei Aktivierung von Kontinuitätsprüfung und Verlustmessung, die beide auf dem softwarebasierten CCM implementiert sind, muss die „Bildrate“ identisch sein. • **TLV:** Aktivieren/Deaktivieren der TLV-Einfügung in die CCM-PDU.
APS-Protokoll	• **Aktivieren:** Die Übertragung von Informationen zum Automatic Protection Switching-Protokoll auf Basis der Übertragung/des Empfangs von R-APS-/L-APS-PDUs kann aktiviert/deaktiviert werden. Muss aktiviert sein, um ERPS/ELPS mit APS-Implementierung zu unterstützen. Dies gilt nur, wenn ein Peer-MEP konfiguriert ist. • **Priorität:** Die Priorität, die als PCP-Bits in den TAG eingefügt werden soll (falls vorhanden). • **Übertragungsart:** Auswahl, ob die APS-PDU als Unicast oder Multicast übertragen wird. Die Unicast-MAC wird aus der Konfiguration „Unicast-Peer-MAC“ übernommen. Unicast ist nur für L-APS gültig – siehe „Typ“. Die R-APS-PDU wird immer mit der in G.8032 beschriebenen Multicast-MAC übertragen. • **Typ:** a. ***R-APS:*** Die APS-PDU wird als R-APS übertragen – dies gilt für ERPS. b. ***L-APS:*** Die APS-PDU wird als L-APS übertragen – dies gilt für ELPS. • **Letztes Oktett:** Dies ist das letzte Oktett der übertragenen und erwarteten RAPS-Multicast-MAC-Adresse. In G.8031 (03/2010) ist eine RAPS-Multicast-MAC-Adresse als 01-19-A7-00-00-XX definiert. Im aktuellen Standard lautet der Wert für dieses letzte Oktett „01“, die Verwendung anderer Werte ist Gegenstand weiterer Untersuchungen.

TLV-Konfiguration

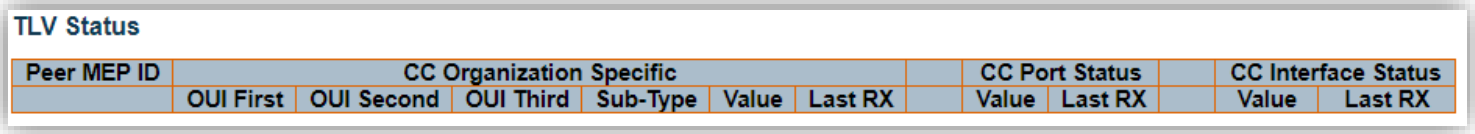
Konfiguration des OAM-PDU-TLV. Derzeit wird nur das TLV im CCM unterstützt.



Einstellung	Beschreibung
Organisationsspezifisch – OUI zuerst	Der als Erstes übertragene Wert im OUI-Feld des OS-TLV.
Organisationsspezifisch – Zweiter OUI-Wert	Der übertragene zweite Wert im OUI-Feld des OS-TLV.
Organisationsspezifisch – OUI, dritter Wert	Der im OUI-Feld des OS-TLV übertragene dritte Wert.
Organisationsspezifisch – Subtyp	Der im Feld „Sub-Type“ des OS-TLV übertragene Wert.
Organisationsspezifisch – Wert	Der im OS-TLV-Feld „Wert“ übertragene Wert.

TLV-Status

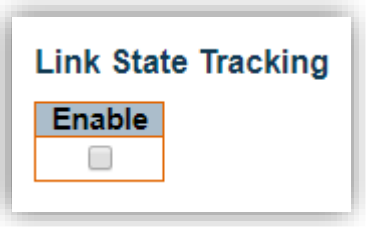
Anzeige des zuletzt empfangenen TLV. Derzeit wird nur TLV im CCM unterstützt.



Einstellung	Beschreibung
CC-organisationsspezifisch – OUI zuerst	Der zuletzt empfangene erste Wert im OUI-Feld.
CC-organisationsspezifisch – OUI, zweiter Wert	Der zuletzt empfangene zweite Wert im OUI-Feld des OS-TLV.
CC-organisationsspezifisch – OUI, dritter Wert	Der zuletzt empfangene dritte Wert im OUI-Feld des OS-TLV.
CC organisationsspezifisch – Subtyp	Der zuletzt empfangene Wert im Feld „Sub-Type“ des OS-TLV.
CC Organisationsspezifisch – Wert	Der zuletzt empfangene Wert im Feld „Value“ des OS-TLV.
CC organisationsspezifisch – Letzte Empfangene	Das OS-TLV wurde in der zuletzt empfangenen CCM-PDU empfangen.
CC Portstatus – Wert	Der zuletzt empfangene Wert im Feld „PS TLV Value“.
CC-Port-Status – Letzter Empfang	PS-TLV wurde in der zuletzt empfangenen CCM-PDU empfangen.

CC-Schnittstellenstatus – Wert	Der zuletzt empfangene Wert im Feld „IS TLV-Wert“.
CC-Schnittstellenstatus – Letzter Empfang	Das IS-TLV wurde in der zuletzt empfangenen CCM-PDU empfangen.

Verfolgung des Verbindungszustands

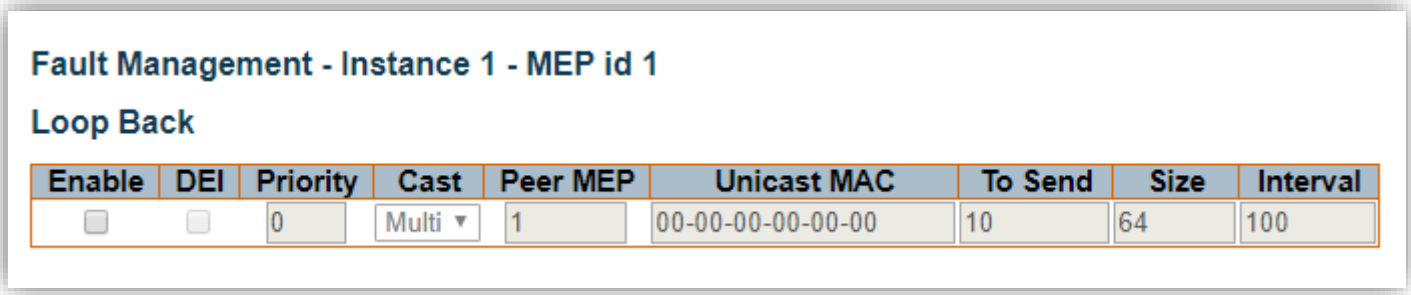


Einstellung	Beschreibung
Aktivieren	Wenn LST in einer Instanz aktiviert ist, führt ein lokaler SF oder ein im CCM-Schnittstellenstatus-TLV empfangenes „isDown“ zum Herunterfahren des Residenzports. Gilt nur im Up-MEP. Die CCM-Rate muss 1 f/s oder höher sein.

Fehlermanagement

Auf dieser Seite kann der Benutzer das Fehlermanagement der aktuellen MEP-Instanz überprüfen und konfigurieren.

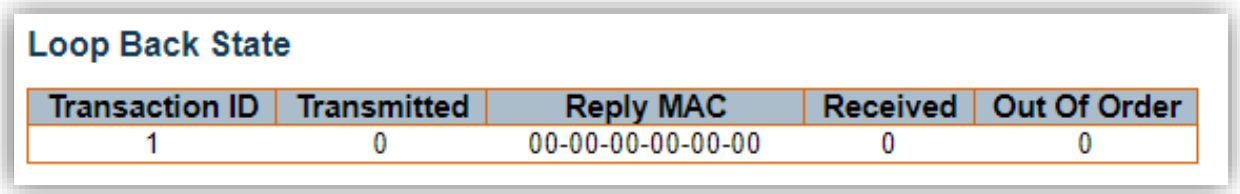
Loopback



Einstellung	Beschreibung
Aktivieren	Loopback auf Basis der Übertragung/des Empfangs von LBM-/LBR-PDUs kann aktiviert/deaktiviert werden. Loopback wird automatisch deaktiviert, wenn alle „To Send“-LBM-PDUs übertragen wurden – es wird 5 Sekunden gewartet, bis alle LBR vom Ende eingegangen sind.
DEI	Der DEI, der als PCP-Bits in den TAG eingefügt werden soll (falls vorhanden).
Priorität	Die Priorität, die als PCP-Bits in den TAG eingefügt werden soll (falls vorhanden).
Übertragungsart	Auswahl, ob die LBM-PDU als Unicast oder Multicast übertragen wird. Die Unicast-MAC-Adresse wird über „Peer MEP“ oder „Unicast Peer MAC“ konfiguriert. In Richtung MIP ist nur Unicast-Loopback möglich.
Peer-MEP	Dies wird nur verwendet, wenn die „Unicast-MAC“ auf ausschließlich Nullen konfiguriert ist. Die LBM-Unicast-MAC wird aus der „Unicast Peer MAC“-Konfiguration dieses Peers übernommen.
Unicast-MAC	Diese Option wird nur verwendet, wenn sie NICHT auf „alle Nullen“ konfiguriert ist. Diese Adresse wird als Unicast-MAC der LBM-PDU verwendet. Dies ist die einzige Möglichkeit, Loopback in Richtung eines MIP zu konfigurieren.
Zu senden	Die Anzahl der LBM-PDUs, die in einem Loop-Test gesendet werden sollen. Der Wert 0 bedeutet unendliche Übertragung (Testverhalten). Hierbei handelt es sich um hardwarebasiertes LBM/LBR, das VOE erfordert.

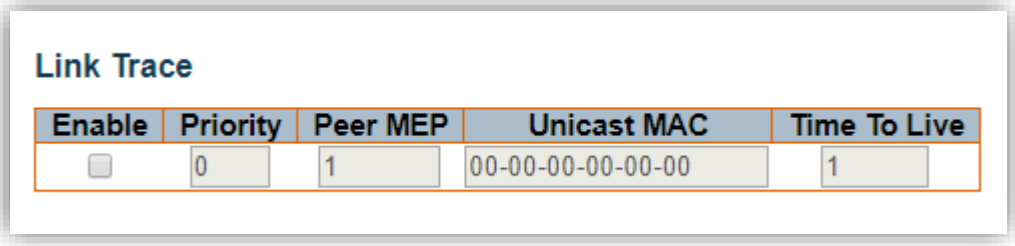
Größe	Die LBM-Frame-Größe. Hier wird die gewünschte Größe (in Byte) eines ungetaggten Frames eingegeben, der eine LBM-OAM-PDU enthält – einschließlich CRC (vier Byte). Beispiel bei „Größe“ = 64 => Größe des nicht getaggten Frames = DMAC(6) + SMAC(6) + TYPE(2) + LBM-PDU-LÄNGE(46) + CRC(4) = 64 Byte Der gesendete Frame wird für jedes hinzugefügte Tag um vier Bytes länger – im Falle eines Tunnel-EVC um 8 Bytes. Es sind zwei maximale Rahmengrößen zu berücksichtigen. • **Maximale Rahmengröße beim Switch-Empfang:** Die maximale Rahmengröße (alles inklusive), die am Switch-Port akzeptiert wird, beträgt 9600 Bytes • **Maximale Frame-Größe beim Empfang durch die CPU:** Die maximale Frame-Größe (alles inklusive), die an die CPU kopiert werden kann, beträgt 9600 Bytes Beachten Sie, dass der Peer-MEP in der Lage sein muss, die ausgewählte Rahmengröße zu verarbeiten. Beachten Sie, dass bei einem softwarebasierten MEP die empfangene LBR-PDU in die CPU kopiert werden muss. Es wird eine Warnung ausgegeben, wenn die ausgewählte Frame-Größe die maximale CPU-Empfangs-Frame-Größe überschreitet. Die Mindestgröße beträgt 64 Byte.
Intervall	Das Intervall zwischen der Übertragung von LBM-PDUs. In 10 ms, falls „To Send“ != 0 (max. 100 – „0“ bedeutet so schnell wie möglich). In 1 µs, falls „To Send“ == 0 (max. 10.000)“,

Loopback-Status



Einstellung	Beschreibung
Transaktions-ID	Die Transaktions-ID der ersten gesendeten LBM. Für jede gesendete LBM wird die Transaktions-ID in der PDU erhöht.
Gesendet	Die Gesamtzahl der übertragenen LBM-PDUs.
Antwort-MAC	Die MAC-Adresse des antwortenden MEP/MIP. Bei einem Multicast-LBM können Antworten von allen Peer-MEPs in der Gruppe empfangen werden. Diese MAC-Adresse wird nicht angezeigt, wenn „To Send“ == 0 ist.
Empfangen	Die Gesamtzahl der von dieser „Antwort-MAC“-Adresse empfangenen LBR-PDUs.
In der falschen Reihenfolge	Die Anzahl der von dieser „Antwort-MAC“-Adresse empfangenen LBR-PDUs mit einer falschen „Transaktions-ID“.

Link-Trace



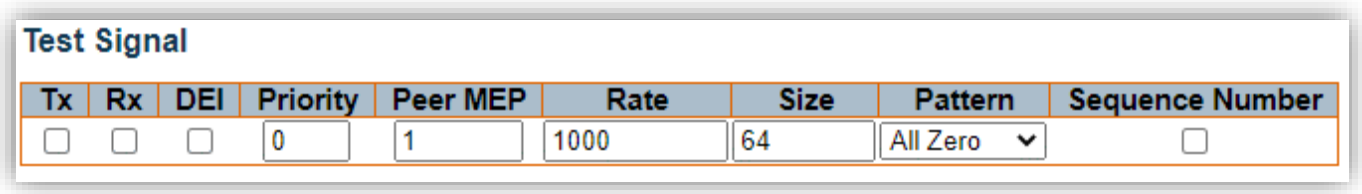
Einstellung	Beschreibung
Aktivieren	Die Link-Trace-Funktion basierend auf dem Senden/Empfangen von LTM-/LTR-PDUs kann aktiviert oder deaktiviert werden. Die Link-Trace-Funktion wird automatisch deaktiviert, wenn alle 5 Transaktionen im Abstand von 5 Sekunden abgeschlossen sind – wobei am Ende 5 Sekunden auf alle LTR gewartet wird. Die LTM-PDU wird immer als Multicast-Klasse 2 gesendet.
Priorität	Die Priorität, die (falls vorhanden) als PCP-Bits in den TAG einzufügen ist.
Peer-MEP	Dies wird nur verwendet, wenn die „Unicast-MAC“ auf ausschließlich Nullen konfiguriert ist. Die Link-Trace-Ziel-MAC wird aus der „Unicast-Peer-MAC“-Konfiguration dieses Peers übernommen.
Unicast-MAC	Dies wird nur verwendet, wenn es NICHT auf „alle Nullen“ konfiguriert ist. Diese Adresse wird als Link-Trace-Ziel-MAC verwendet. Dies ist die einzige Möglichkeit, eine MIP als Ziel-MAC zu konfigurieren.
Time To Live	Dies ist der LTM-PDU-TTL-Wert gemäß Y.1731. Dieser Wert wird bei jeder Weiterleitung durch einen MIP um eins verringert. Bei Erreichen des Werts Null erfolgt keine weitere Weiterleitung.

Link-Trace-Status

Einstellung	Beschreibung
Transaktions-ID	Die Transaktions-ID wird bei jedem LTM-Versand erhöht. Dieser Wert wird in die gesendete LTM-PDU eingefügt und soll in der LTR-PDU empfangen werden. Eine empfangene LTR mit falscher Transaktions-ID wird ignoriert. In einem aktivierten Link Trace gibt es fünf Transaktionen.
Time To Live	Dies ist der TTL-Wert aus dem LTM, das von dem MIP/MEP empfangen wurde, der diese LTR sendet – dekrementiert, als ob es weitergeleitet worden wäre.
Modus	Gibt an, ob diese LTR von einem MEP/MIP gesendet wurde.
Richtung	Gibt an, ob der MEP/MIP, der diese LTR sendet, eingehend oder ausgehend ist.
Weitergeleitet	Gibt an, ob der MEP/MIP, der diese LTR sendet, die LTM weitergeleitet hat.
Weiterleitung	Die Relay-Aktion kann eine der folgenden sein • **MAC:** Es gab einen Treffer bei der LT-Ziel-MAC-Adresse

	• **FDB:** Das LTM wird aufgrund eines Treffers in der Filterdatenbank weitergeleitet • **MFDB:** Das LTM wird aufgrund eines Treffers in der MIP-CCM-Datenbank weitergeleitet
Letzter MAC	Die MAC-Adresse, die den letzten Absender des LBM identifiziert, der diesen LTR ausgelöst hat – initiierendes MEP oder vorherige MIP-Weiterleitung.
Nächster MAC	Die MAC-Adresse, die den nächsten Absender des LBM identifiziert, der diesen LTR verursacht – MIP-Weiterleitung oder beendendes MEP.

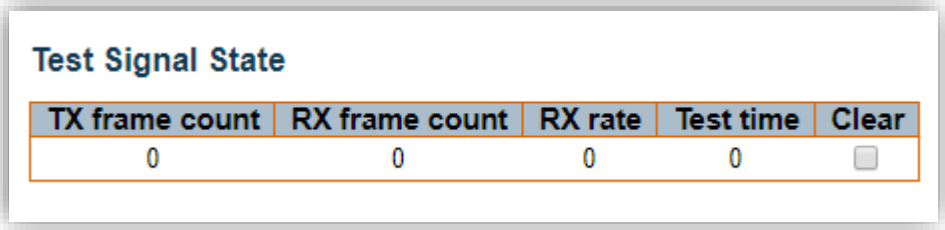
Testsignal



Einstellung	Beschreibung
Aktivieren	Das Testsignal, das auf der Übertragung einer TST-PDU basiert, kann aktiviert/deaktiviert werden.
DEI	Die DEI, die als PCP-Bits in den TAG eingefügt werden soll (falls vorhanden).
Priorität	Die Priorität, die als PCP-Bits in den TAG eingefügt werden soll (falls vorhanden).
Peer-MEP	Die Ziel-MAC-Adresse des TST-Frames wird aus der Konfiguration „Unicast Peer MAC“ dieses Peers übernommen.
Rate	Die Übertragungsbitrate des TST-Frames – in Kilobit pro Sekunde. Begrenzt auf 10 Gbit/s. Dies ist die Bitrate eines Standard-Frames ohne jegliche Kapselung. Wenn in einem EVC-MEP eine Rate von 1 Mbit/s ausgewählt wird, führt das hinzugefügte Tag zu einer höheren Bitrate auf der Leitung.
Größe	Die Größe des TST-Frames. Hier wird die gewünschte Größe (in Byte) eines nicht getaggten Frames eingegeben, der eine TST-OAM-PDU enthält – einschließlich CRC (vier Byte). Beispiel bei „Größe“ = 64 => Größe des nicht getaggten Frames = DMAC(6) + SMAC(6) + TYPE(2) + TST-PDU-LÄNGE(46) + CRC(4) = 64 Byte Der gesendete Frame wird für jedes hinzugefügte Tag um vier Bytes länger – im Falle eines Tunnel-EVC um 8 Bytes. Es sind zwei maximale Rahmengrößen zu berücksichtigen. • **Maximale Frame-Größe beim Switch-Empfang:** Die maximale Frame-Größe (alles inklusive), die am Switch-Port akzeptiert wird, beträgt 10240 Bytes • **Maximale Frame-Größe bei CPU-Empfang:** Die maximale Frame-Größe (alles inklusive), die auf die CPU kopiert werden kann, beträgt 10240 Bytes Beachten Sie, dass der Peer-MEP in der Lage sein muss, die ausgewählte Rahmengröße zu verarbeiten. Beachten Sie, dass zur Berechnung der „Empfangsrate“ eine empfangene TST-PDU in die CPU kopiert werden muss. Es wird eine Warnung ausgegeben, wenn die ausgewählte Frame-Größe die maximale CPU-Empfangs-Frame-Größe überschreitet. Die minimale Frame-Größe beträgt 64 Byte.
Muster	Die „leere“ TST-PDU hat eine Größe von 12 Byte. Um die konfigurierte Frame-Größe zu erreichen, wird ein Daten-TLV mit einem Muster hinzugefügt.

	Beispiel bei „Size“ = 64 => Größe des ungetaggten Frames = DMAC(6) + SMAC(6) + TYPE(2) + TST-PDU-LÄNGE(46) + CRC(4) = 64 Byte Die TST-PDU muss 46 Byte groß sein, daher wird ein Muster von 46–12 = 34 Byte hinzugefügt. **Nur Nullen:** Das Muster lautet „00000000“ **Nur Einsen:** Das Muster lautet „11111111“ **10101010:** Das Muster lautet „10101010“

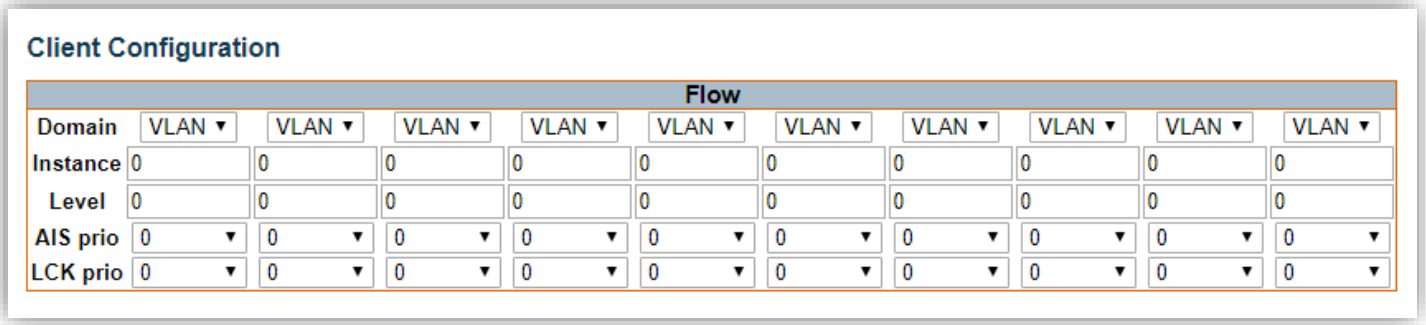
Zustand des Testsignals



Schauplatz	Beschreibung
Anzahl der TX-Frames	Die Anzahl der seit dem letzten „Clear“ gesendeten TST-Frames.
Anzahl der empfangenen TST-Frames	Die Anzahl der empfangenen TST-Frames seit dem letzten „Clear“.
Empfangsrate	Die aktuelle Bitrate der empfangenen TST-Frames in kbps. Diese wird auf einer 1-Sekunden-Basis berechnet, beginnend mit dem Empfang des ersten TST-Frames nach „Clear“. Die für diese Berechnung verwendete Frame-Größe ist die des ersten nach „Clear“ empfangenen Frames.
Testdauer	Die Anzahl der Sekunden, die seit dem Empfang des ersten TST-Frames nach dem letzten „Clear“ vergangen sind.
„Clear“	Dadurch werden alle Testsignalzustände gelöscht. Die Übertragung von TST-Frames wird neu gestartet. Die Berechnung von „Rx-Frame-Zählung“, „RX-Rate“ und „Testzeit“ beginnt mit dem Empfang des ersten TST-Frames.

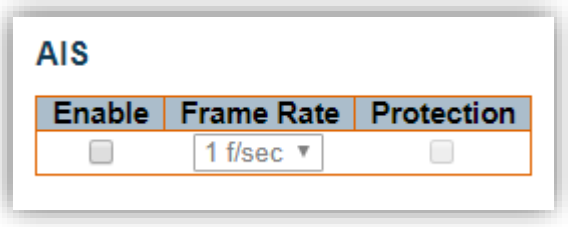
Client-Konfiguration

Nur ein Port-MEP kann als Server-MEP mit Flusskonfiguration fungieren. Die Priorität im Client-Fluss entspricht immer der höchsten im EVC konfigurierten Priorität.



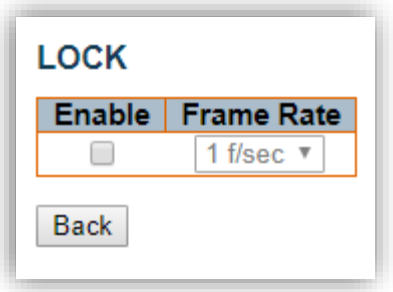
Einstellung	Beschreibung
Domäne	Die Domäne des Client-Layer-Flows.
Instanz	Instanznummern des Client-Layer-Flows.
Ebene	Client-Schicht-Ebene – AIS- und LCK-PDUs, die in diesem Client-Schicht-Flow übertragen werden, befinden sich auf dieser Ebene.
AIS-Priorität	Die Priorität, die bei der Übertragung von AIS in jedem Client-Flow verwendet werden soll. Es kann die Priorität ausgewählt werden, die den höchstmöglichen PCP ergibt.
LCK-Priorität	Die Priorität, die bei der Übertragung von LCK in jedem Client-Datenstrom verwendet werden soll. Es kann die Priorität ausgewählt werden, die den höchstmöglichen PCP ergibt.

AIS



Einstellung	Beschreibung
Aktivieren	Das Einfügen eines AIS-Signals (AIS-PDU-Übertragung) in Client-Layer-Flows kann aktiviert oder deaktiviert werden.
Bildrate	Auswahl der Bildrate der AIS-PDU. Dies ist der Kehrwert der Übertragungsperiode gemäß Y.1731.
Schutz	Wird diese Option ausgewählt, werden die ersten 3 AIS-PDUs so schnell wie möglich übertragen – falls dies zum Schutz am Endpunkt genutzt wird.

Sperren

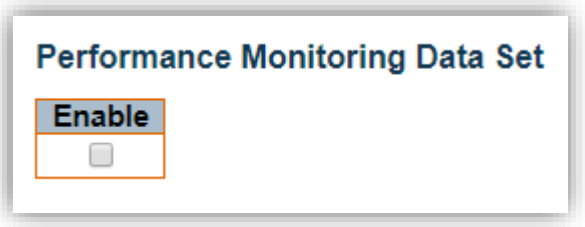


Einstellung	Beschreibung
Aktivieren	Einfügen eines LOCK-Signals (LCK-PDU-Übertragung) in Client-Layer-Flows; kann aktiviert/deaktiviert werden.
Bildrate	Auswahl der Rahmenrate der LCK-PDU. Dies ist der Kehrwert der Übertragungsperiode gemäß Y.1731.

Leistungsüberwachung

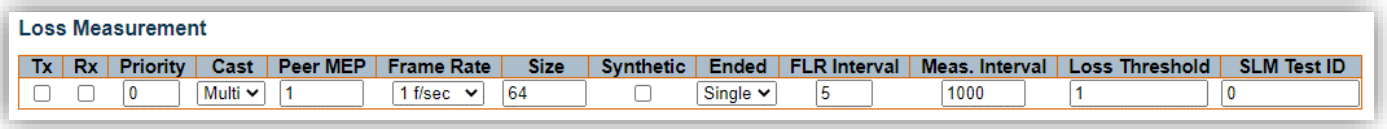
Auf dieser Seite kann der Benutzer den Leistungsmonitor der aktuellen MEP-Instanz einsehen und konfigurieren.

Datensatz zur Leistungsüberwachung



Einstellung	Beschreibung
Aktivieren	Wenn diese Option aktiviert ist, trägt diese MEP-Instanz zum „PM-Datensatz“ bei, der von der PM-Sitzung erfasst wird.

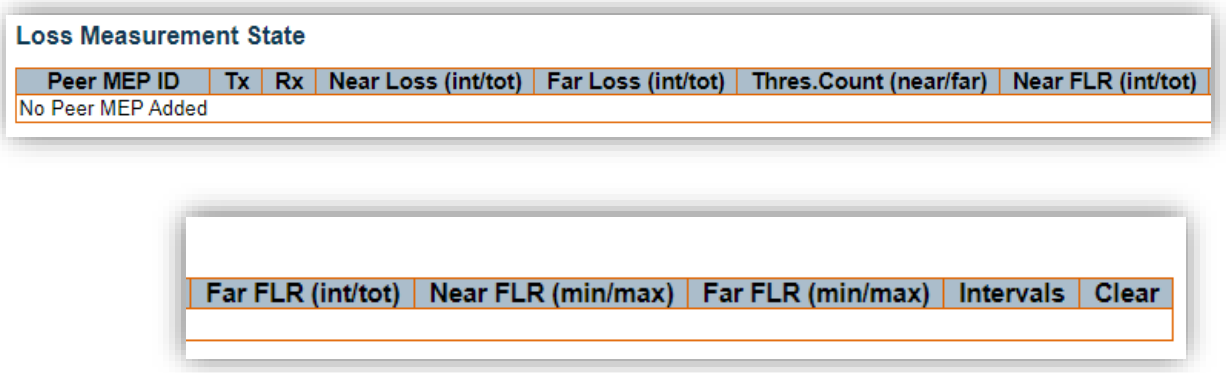
Verlustmessung



Einstellung	Beschreibung
Tx	Senden/Empfangen von CCM- oder LMM/LMR- oder SLM/SLR/1SL-PDUs – siehe „Synthetic“ und „Ended“. Der Service-Frame-LM (nicht „Synthetic“) ist nur zulässig, wenn ein Peer-MEP konfiguriert ist. Ein synthetischer LM-Frame ist bei Konfiguration mehrerer Peer-MEPs zulässig.
Rx	Aktiviert die Verlustberechnung beim Empfang von LM-PDUs (LMM/SLM/1SL). Diese wird ignoriert, wenn der LM-Initiator aktiviert ist.
Priorität	Die Priorität, die als PCP-Bits in den TAG eingefügt werden soll (falls vorhanden). Bei Aktivierung von Kontinuitätsprüfung und Verlustmessung, die beide auf einem softwarebasierten CCM implementiert sind, muss die „Priorität“ identisch sein.
Cast	Auswahl, ob die LM-PDU als Unicast oder Multicast übertragen wird. Die Unicast-MAC wird aus der Datenbank „Unicast Peer MAC“ entnommen. Sind sowohl die Kontinuitätsprüfung als auch die beidseitige Verlustmessung aktiviert und beide auf einem softwarebasierten CCM implementiert, muss der Wert für „Cast“ identisch sein.
Peer-MEP	Peer-MEP-ID für Unicast-LM. Die MAC-Adresse wird aus der Datenbank „Unicast Peer MAC“ entnommen. Wird nur bei mehreren Peers („Synthetic“-LM) verwendet.
Rate	Auswahl der Framerate der LM-PDU. Dies ist der Kehrwert der Übertragungsperiode gemäß Y.1731. Die Auswahl von 100 f/s ist nur bei „synthetischer“ LM gültig. Die Auswahl von 6 f/min ist bei einem beidseitigen „Service Frame“-LM (auf Basis der CCM-PDU) nicht zulässig. Wenn sowohl die Kontinuitätsprüfung als auch die Verlustmessung aktiviert sind und beide auf einem softwarebasierten CCM implementiert sind, muss die „Bildrate“ identisch sein.

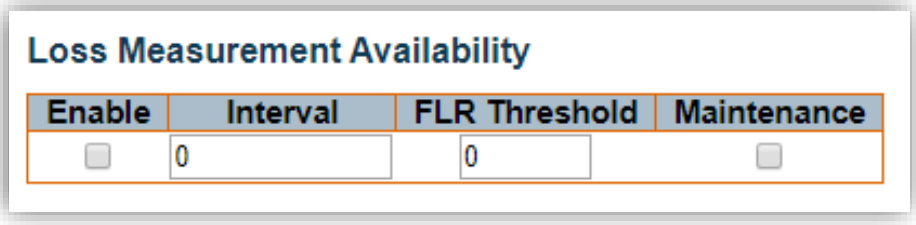
Größe	Die „synthetische“ SLM/1SL-Frame-Größe. Hier wird die gewünschte Größe (in Byte) eines ungetaggten Frames eingegeben, der eine LM-OAM-PDU enthält – einschließlich CRC (vier Byte). Beispiel bei „Größe“ = 64 => Größe des ungetaggten Frames = DMAC(6) + SMAC(6) + TYPE(2) + LBM-PDU-LÄNGE(46) + CRC(4) = 64 Byte Der gesendete Frame wird für jedes hinzugefügte Tag um vier Bytes länger – im Falle eines Tunnel-EVC um 8 Bytes. Es sind zwei maximale Rahmengrößen zu berücksichtigen. • **Maximale Frame-Größe beim Switch-Empfang:** Die maximale Frame-Größe (alles inklusive), die am Switch-Port akzeptiert wird, in Bytes • **Maximale CPU-Empfangsrahmengröße:** Die maximale Rahmengröße (alles inklusive), die an die CPU kopiert werden kann, in Bytes Beachten Sie, dass der Peer-MEP in der Lage sein muss, die ausgewählte Frame-Größe zu verarbeiten. Beachten Sie, dass die empfangene SLR-PDU in die CPU kopiert werden muss. Es wird eine Warnung ausgegeben, wenn die ausgewählte Frame-Größe die maximale CPU-Empfangs-Frame-Größe überschreitet. Die minimale Frame-Größe beträgt 64 Bytes.
Synthetisch	Synthetische Frame-LM ist aktiviert. Hierbei handelt es sich um eine auf SLM/SLR/1SL-PDUs basierende LM.
Beendet	**Single:** Single-Ended-Verlustmessung, implementiert auf LMM/LMR oder SLM/SLR. **Dual:** Die Messung der Verluste auf beiden Seiten wurde auf SW-basiertem CCM oder 1SL implementiert.
FLR-Intervall	Dies ist das Intervall in Anzahl der Messintervalle, über das die Intervall-Frame-Verlustquote berechnet wird.
Messintervall	Dies ist das „synthetische“ LM-Messintervall in Millisekunden. Es muss eine ganze Zahl des LM-PDU-Übertragungsintervalls (Kehrwert von „Rate“) sein. Dies ist das Zeitintervall, in dem der Verlust und die FLR auf der Grundlage der gezählten Anzahl von SL-OAM-PDUs berechnet werden. In diesem Intervall wird die berechnete FLR anhand der Schwellenwerte für Verfügbarkeit, hohen Verlust und verschlechterte FLR überprüft. Beispiel: „Rate“ = 100 f/s => „Messintervall“ = N × 10 Millisekunden. Beispiel: „Rate“ = 10 f/s => „Meas Interval“ = N × 100 Millisekunden. Bei einem auf Service-Frames basierenden LM wird dieses Attribut nicht verwendet, und das Messintervall entspricht stets dem LM-PDU-Übertragungsintervall.
Verlustschwelle	Der Zählwert für den Verlustschwellenwert am entfernten Ende wird erhöht, wenn eine Verlustmessung diesen Schwellenwert überschreitet.
SLM-Test-ID	Der in SLM-PDUs zu verwendende Test-ID-Wert (siehe G.8013, Abschnitt 9.22.1). Der Standardwert ist 0.

Verlustmessungsstatus



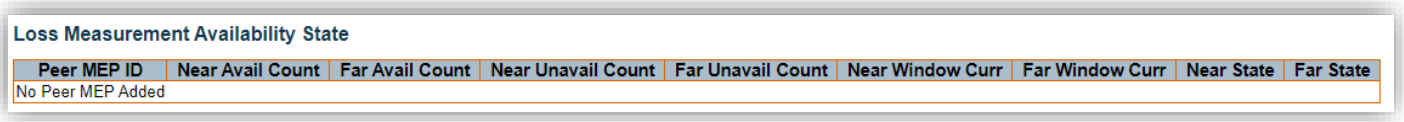
Einstellung	Beschreibung
Peer-MEP	Die Peer-MEP-ID, auf die sich der folgende Status bezieht.
Tx	Die kumulierten gesendeten LM-PDUs – seit dem letzten „Clear“.
Rx	Die kumulierten empfangenen LM-PDUs – seit dem letzten „Clear“.
Nahseitiger Verlust	Dieses Feld enthält sowohl die Anzahl der Messintervalle, die zum Frame-Verlust am nahen Ende beigetragen haben, als auch die Gesamtzahl der Frame-Verluste am nahen Ende – seit dem letzten „Clear“.
Verlust am entfernten Ende	Dieses Feld enthält sowohl die Anzahl der Messintervalle, die zum Frame-Verlust am nahen Ende beigetragen haben, als auch die Gesamtzahl der Frame-Verluste am fernen Ende – seit dem letzten „Clear“.
Schwellenwertanzahl (nahes/fernes Ende)	Die Anzahl der Fälle, in denen die Schwellenwerte für den Frame-Verlust am nahen und am fernen Ende überschritten wurden.
Nah-FLR (int/tot)	Die Intervall- und Gesamt-Rahmenverlustrate auf der nahen Seite, berechnet auf der Grundlage der Anzahl der Rahmenverluste auf der nahen Seite und der übertragenen Rahmen auf der entfernten Seite. Das Ergebnis wird in Prozent angegeben.
Far FLR (int/tot)	Die Intervall- und Gesamt-Frame-Verlustquote auf der Gegenstelle, berechnet auf der Grundlage der Anzahl der Frame-Verluste auf der Gegenstelle und der auf der Nahseite übertragenen Frames. Das Ergebnis wird in 100 * Prozent angegeben.
Nah-FLR (min/max)	Die minimalen und maximalen von Null verschiedenen Rahmenverlustraten auf der nahen Seite, berechnet auf der Grundlage der Anzahl der Rahmenverluste auf der nahen Seite und der übertragenen Rahmen auf der entfernten Seite. Das Ergebnis wird in 100 * Prozent angegeben. Ein Wert von Null bedeutet, dass seit dem letzten „Clear“ kein Verlust aufgetreten ist.
FLR auf der Gegenstelle (min/max)	Die minimalen und maximalen nicht-null-Werte der Rahmenverlustrate am entfernten Ende, berechnet auf der Grundlage der Anzahl der Rahmenverluste am entfernten Ende und der übertragenen Rahmen am nahen Ende. Das Ergebnis wird in 100 * Prozent angegeben. Ein Wert von Null bedeutet, dass seit dem letzten „Clear“ kein Verlust aufgetreten ist.
Intervalle	Die Anzahl der abgelaufenen FLR-Intervalle.
Zurücksetzen	Durch Aktivieren dieser Option und Speichern werden die akkumulierten Zähler zurückgesetzt und die Berechnung der Verlustrate neu gestartet.

Verfügbarkeit der Schadensbewertung



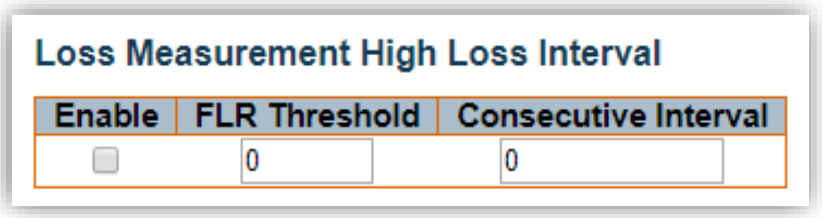
Einstellung	Beschreibung
Aktivieren	Aktivieren/Deaktivieren der Verfügbarkeit der Verlustmessung.
Intervall	Verfügbarkeitsintervall – Anzahl der Messungen mit derselben Verfügbarkeit, die erforderlich sind, um den Verfügbarkeitsstatus zu ändern. Der gültige Bereich liegt zwischen 1 und 1000.
FLR-Schwellenwert	Schwellenwert für die Verfügbarkeits-Frame-Verlustquote in Promille.
Wartung	Aktivieren/Deaktivieren der Wartung der Verfügbarkeit der Verlustmessung.

Verfügbarkeitsstatus der Verlustmessung



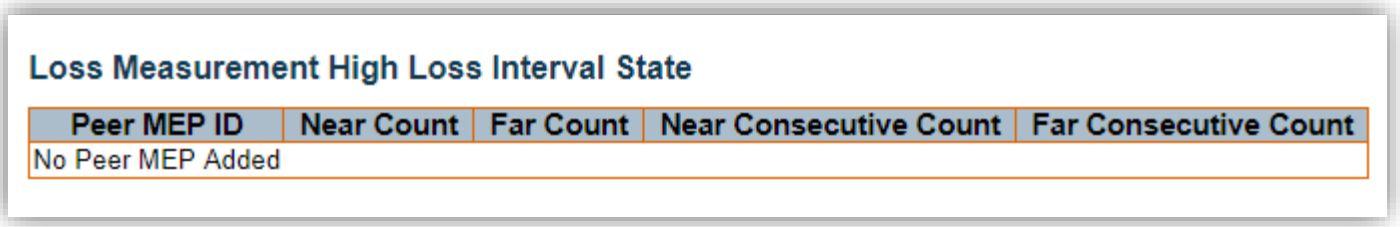
Einstellung	Beschreibung
Peer-MEP	Die Peer-MEP-ID, auf die sich der folgende Status bezieht.
Anzahl der „Near Avail“-Messungen	Die Anzahl der Messungen, die durchgeführt wurden, während sich das nahe Ende im Status „Avail“ befand.
Anzahl der „Far Avail“-Messungen	Die Anzahl der Messungen, die durchgeführt wurden, während sich das entfernte Ende im Zustand „Avail“ befand.
Anzahl der „Near Unavail“-Messungen	Die Anzahl der Messungen, die durchgeführt wurden, während sich die nahe Seite im Zustand „Unavail“ befand.
Anzahl der „Far Unavail“-Messungen	Die Anzahl der Messungen, die durchgeführt wurden, während sich die Gegenstelle im Zustand „Unavail“ befand.
Aktuelle Größe des Nah-Verfügbarkeitsfensters	Die aktuelle Größe des Verfügbarkeitsfensters auf der **nahen** Seite. Wenn **der Status der nahen Seite** „Verfügbar“ ist, gibt dieser Wert die aktuelle Anzahl aufeinanderfolgender Messungen an, die über dem definierten Schwellenwert für die Rahmenverlustrate liegen. Wenn **der Status der nahen Seite** „Nicht verfügbar“ ist, gibt dieser Wert die aktuelle Anzahl aufeinanderfolgender Messungen an, die dem definierten Schwellenwert für die Rahmenverlustrate entsprechen oder darunter liegen. Sobald dieser Wert den definierten „Intervall“-Wert (auch bekannt als „Fenstergröße“) erreicht, ändert sich der Verfügbarkeitsstatus.
Aktuelle Fenstergröße (Fernseite)	Die aktuelle Größe des Verfügbarkeitsfensters am entfernten Ende. Weitere Details finden Sie in der Beschreibung zu **„Near Window Curr“**.
Near-Status	Der aktuelle Verfügbarkeitsstatus auf der Nahseite.
Fernstatus	Der aktuelle Verfügbarkeitsstatus am entfernten Ende.

Verlustmessung – Intervall mit hohem Verlust



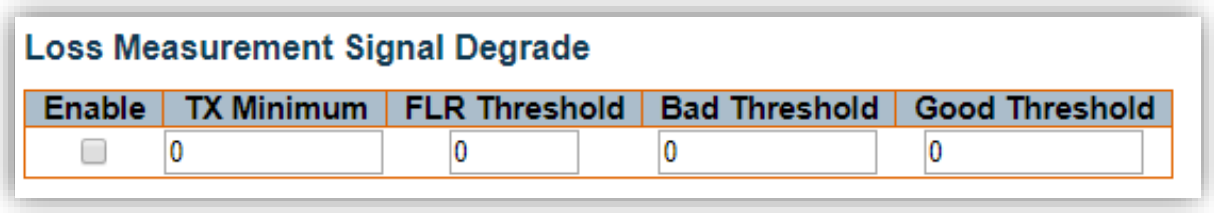
Einstellung	Beschreibung
Aktivieren	Aktivieren/Deaktivieren des Intervalls für hohe Verluste bei der Verlustmessung.
FLR-Schwellenwert	Schwellenwert für die Frame-Loss-Rate im Intervall mit hohem Verlust in Promille.
Aufeinanderfolgendes Intervall	Aufeinanderfolgendes Intervall für das Intervall mit hohem Verlust (Anzahl der Messungen).

Status des Intervalls mit hohem Verlust bei der Verlustmessung



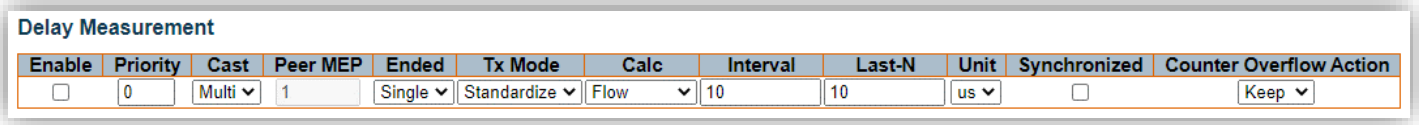
Einstellung	Beschreibung
Anzahl der „Near“-Zählungen	Zählwert für Intervalle mit hohem Verlust am nahen Ende (Anzahl der Messungen, bei denen der Verfügbarkeitsstatus „verfügbar“ ist und der FLR-Wert über dem Schwellenwert für den FLR bei Intervallen mit hohem Verlust liegt).
Zählwert am entfernten Ende	Anzahl der Intervalle mit hohen Verlusten am entfernten Ende (Anzahl der Messungen, bei denen der Verfügbarkeitsstatus vorliegt und der FLR-Wert über dem Schwellenwert für Intervalle mit hohen Verlusten liegt).
Anzahl aufeinanderfolgender Intervalle auf der nahen Seite	Anzahl aufeinanderfolgender Intervalle mit hohem Verlust auf der nahen Seite.
Anzahl aufeinanderfolgender Intervalle am entfernten Ende	Anzahl aufeinanderfolgender Intervalle mit hohem Verlust am entfernten Ende.

Signalverschlechterung bei Verlustmessung



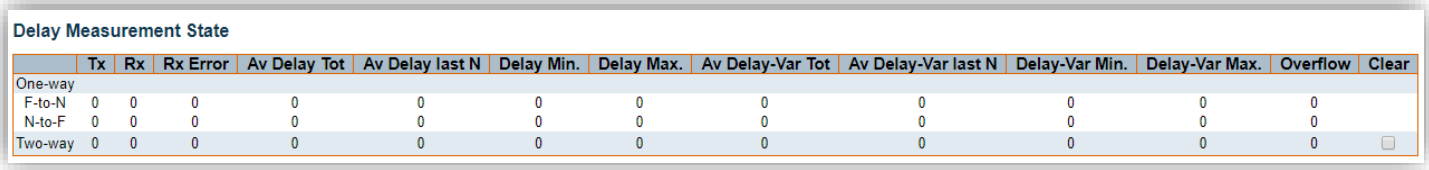
Einstellung	Beschreibung
Aktivieren	Aktivieren/Deaktivieren der Signalverschlechterung bei der Verlustmessung.
TX-Minimum	Mindestanzahl an Frames, die bei einer Messung übertragen werden müssen, bevor die Frame-Verlustquote anhand des Schwellenwerts für die Verlustquote geprüft wird.
FLR-Schwellenwert	Schwellenwert für die Frame-Verlustquote bei Signalverschlechterung in pro Meile.
Schwellenwert für fehlerhafte Intervalle	Anzahl aufeinanderfolgender Messungen mit fehlerhaften Intervallen, die erforderlich sind, um den Degradationszustand auszulösen.
Schwellenwert „Gut“	Anzahl der aufeinanderfolgenden gültigen Intervallmessungen, die erforderlich sind, um den Degradationszustand aufzuheben.

Verzögerung bei der Messung



Einstellung	Beschreibung
Aktivieren	Die Verzögerungsmessung auf Basis der Übertragung von 1DM/DMM-PDUs kann aktiviert oder deaktiviert werden. Die Verzögerungsmessung auf Basis des Empfangs und der Verarbeitung von 1DM/DMR-PDUs ist immer aktiviert.
Priorität	Die Priorität, die als PCP-Bits in den TAG eingefügt werden soll (falls vorhanden).
Übertragungsart	Auswahl, ob die 1DM/DMM-PDU als Unicast oder Multicast übertragen wird. Der Unicast-MAC wird über „Peer MEP“ konfiguriert.
Peer-MEP	Dies wird nur verwendet, wenn „Cast“ auf „Uni“ konfiguriert ist. Die 1DM/DMR-Unicast-MAC-Adresse wird aus der Konfiguration „Unicast Peer MAC“ dieses Peers übernommen.
Ended	**Single:** Einseitige Verzögerungsmessung, implementiert auf DMM/DMR. **Dual:** Auf 1DM implementierte Dual-Ended-Verzögerungsmessung.
Tx-Modus	**Standardisiert:** Standardisierte Methode gemäß Y.1731 zur Übertragung von 1DM/DMR. **Proprietär:** Vitesse-eigene Methode mit Folgepaketen zur Übertragung von 1DM/DMR.
Berechnung	Dies wird nur verwendet, wenn „Ended“ auf „Single Ended“ konfiguriert ist. **Hin- und Rücklauf:** Die Rahmenverzögerung, berechnet anhand der Sende- und Empfangszeitstempel der Initiatoren. Rahmenverzögerung = RxTimeb – TxTimeStampf **Flow:** Die Rahmenverzögerung, berechnet anhand der Sende- und Empfangszeitstempel von Initiatoren und Remotes. Rahmenverzögerung = (RxTimeb – TxTimeStampf) – (TxTimeStampb – RxTimeStampf)
Intervall	Das Intervall zwischen dem Senden von 1DM/DMM-PDUs in 10 ms. Der Bereich liegt zwischen 10 und 65535.
Last-N	Die letzten N Verzögerungsmessungen, die für die Berechnung des Durchschnitts der letzten N verwendet werden. Der Mindestwert beträgt 10. Der Höchstwert beträgt 100.
Einheit	Die Zeitauflösung.
Synchronisiert	Aktivieren Sie diese Option, um DMM/DMR-Pakete zur Berechnung der beidseitigen Verzögerung (Dual-Ended-DM) zu verwenden. Wenn die Option aktiviert ist, werden folgende Maßnahmen ergriffen: Beim Empfang von DMR werden die bidirektionale Verzögerung (Roundtrip oder Flow) sowie sowohl die Einwegverzögerung vom nahen zum entfernten Ende als auch die Einwegverzögerung vom entfernten zum nahen Ende berechnet. Beim Empfang von DMM oder 1DM wird nur die Einwegverzögerung vom entfernten zum nahen Ende berechnet.
Maßnahme bei Zählerüberlauf	Die Aktion, die bei einem Zählerüberlauf ausgeführt werden soll.

Status der Verzögerungsmessung



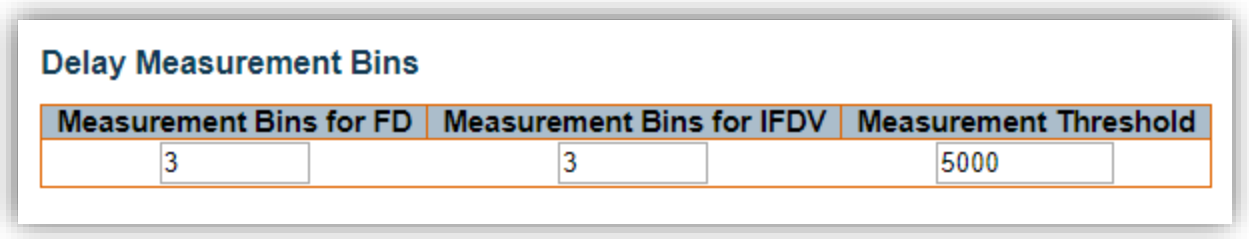
Delay Measurement State

	Tx	Rx	Rx Error	Av Delay Tot	Av Delay last N	Delay Min.	Delay Max.	Av Delay-Var Tot	Av Delay-Var last N	Delay-Var Min.	Delay-Var Max.	Overflow	Clear
One-way													
F-to-N	0	0	0	0	0	0	0	0	0	0	0	0	
N-to-F	0	0	0	0	0	0	0	0	0	0	0	0	
Two-way	0	0	0	0	0	0	0	0	0	0	0	0	☐

Einstellung	Beschreibung
Tx	Die kumulierte Anzahl der Übertragungen – seit dem letzten „Clear“.
Rx	Die kumulierte Anzahl der Empfangsvorgänge – seit dem letzten „Clear“.
Rx-Fehler	Die kumulierte Anzahl der Empfangsfehler – seit dem letzten „Clear“. Diese wird gezählt, wenn die Rahmenverzögerung größer als 1 Sekunde ist oder wenn die Verweildauer am entfernten Ende größer als die Umlaufzeit ist.
Gesamtverzögerung	Die durchschnittliche Gesamtverzögerung – seit dem letzten „Clear“.
Durchschnittliche Verzögerung der letzten N	Die durchschnittliche Verzögerung der letzten n Pakete – seit dem letzten „Clear“.
Min. Verzögerung	Die minimale Verzögerung – seit dem letzten „Clear“.
Max. Verzögerung	Die maximale Verzögerung – seit dem letzten „Clear“.
Durchschnittliche Gesamtverzögerungsschwankung	Die durchschnittliche Gesamtverzögerungsschwankung – seit dem letzten „Clear“.
Durchschnittliche Verzögerungsschwankung der letzten N	Die durchschnittliche Verzögerungsschwankung der letzten n Pakete – seit dem letzten „Clear“.
Verzögerungsschwankung Min.	Die minimale Verzögerungsschwankung – seit dem letzten „Clear“.
Verzögerungsschwankung Max.	Die maximale Verzögerungsschwankung – seit dem letzten „Clear“.
Überlauf	Die Anzahl der Zählerüberläufe – seit dem letzten „Clear“.
Löschen	Wenn Sie diese Option aktivieren und speichern, werden die akkumulierten Zähler zurückgesetzt.
Einwegverzögerung vom entfernten zum nahen Ende	Die Einwegverzögerung bezieht sich auf die Übertragung von den entfernten Geräten zu den lokalen Geräten. Hier sind die Bedingungen für die Berechnung dieser Verzögerung: 1. 1DM empfangen. 2. DMM empfangen, wobei „Synchronisiert“ aktiviert ist. 3. DMR empfangen, wobei „Synchronisiert“ aktiviert ist.
Einwegverzögerung vom nahen zum entfernten Ende	Die Einwegverzögerung erfolgt von den lokalen Geräten zu den entfernten Geräten. Der einzige Fall, in dem diese Verzögerung berechnet wird, ist der folgende: DMR-Empfang bei aktivierter Synchronisierung.

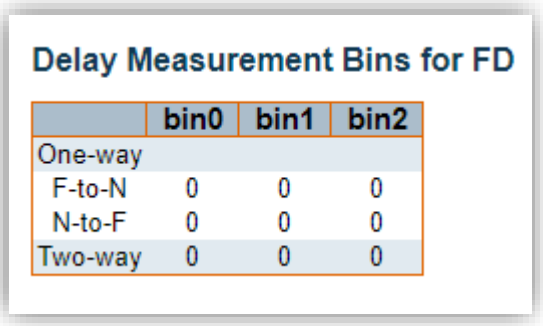
Verzögerungsmess-Bins

Ein Messbereich ist ein Zähler, der die Anzahl der Verzögerungsmessungen speichert, die während eines Messintervalls in einen bestimmten Bereich fallen.



Einstellung	Beschreibung	Werkseinstellung
Messbins für FD	Konfigurierbare Anzahl von Frame-Delay-Messbins pro Messintervall. Die Mindestanzahl der unterstützten FD-Messfenster pro Messintervall beträgt 2. Die maximal unterstützte Anzahl an FD-Messfenstern pro Messintervall beträgt 10.	3
Messfenster für IFDV	Konfigurierbare Anzahl von Messfenstern für die Inter-Frame-Delay-Variation pro Messintervall. Die Mindestanzahl der unterstützten FD-Messfenster pro Messintervall beträgt 2. Die maximal unterstützte Anzahl von FD-Messfenstern pro Messintervall beträgt 10.	3
Messschwellenwert	Der Messschwellenwert ist für jeden Messbereich konfigurierbar. Die Einheit für einen Messschwellenwert ist Mikrosekunden (us).	5000

Verzögerungsmessbereiche für FD



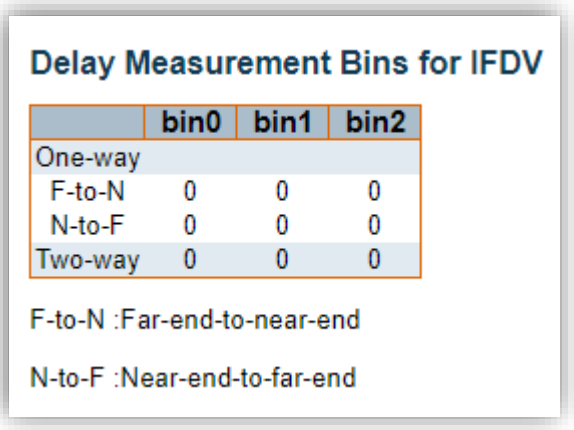
Delay Measurement Bins for FD

	bin0	bin1	bin2
One-way			
F-to-N	0	0	0
N-to-F	0	0	0
Two-way	0	0	0

Ein Messbereich ist ein Zähler, der die Anzahl der Verzögerungsmessungen speichert, die während eines Messintervalls in einen bestimmten Bereich fallen.
Wenn der Messschwellenwert 5000 us beträgt und die Gesamtzahl der Messfächer vier beträgt, lässt sich dies wie folgt veranschaulichen.

Bin	Schwellenwert	Bereich
Bin0	0 µs	0 us <= Messwert < 5.000 us
Bin1	5.000 us	5.000 us <= Messwert < 10.000 us
bin2	10.000 us	10.000 us <= Messwert < 15.000 us
bin3	15.000 us	15.000 us <= Messwert < unendlich us

Verzögerungsmess-Bins für IFDV



Delay Measurement Bins for IFDV

	bin0	bin1	bin2
One-way			
F-to-N	0	0	0
N-to-F	0	0	0
Two-way	0	0	0

F-to-N :Far-end-to-near-end

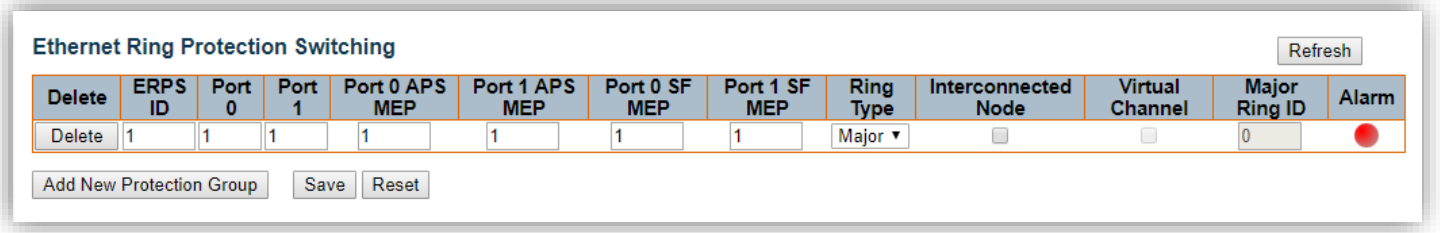
N-to-F :Near-end-to-far-end

Ein Messbereich ist ein Zähler, der die Anzahl der Verzögerungsmessungen speichert, die während eines Messintervalls in einen bestimmten Bereich fallen.
Wenn der Messschwellenwert 5.000 us beträgt und die Gesamtzahl der Messbins vier beträgt, lässt sich dies wie folgt veranschaulichen.

Bin	Schwellenwert	Bereich
Bin0	0 µs	0 us <= Messwert < 5.000 us
Bin1	5.000 us	5.000 us <= Messwert < 10.000 us
bin2	10.000 us	10.000 us <= Messwert < 15.000 us
bin3	15.000 us	15.000 us <= Messwert < unendlich us

Konfiguration > ERPS

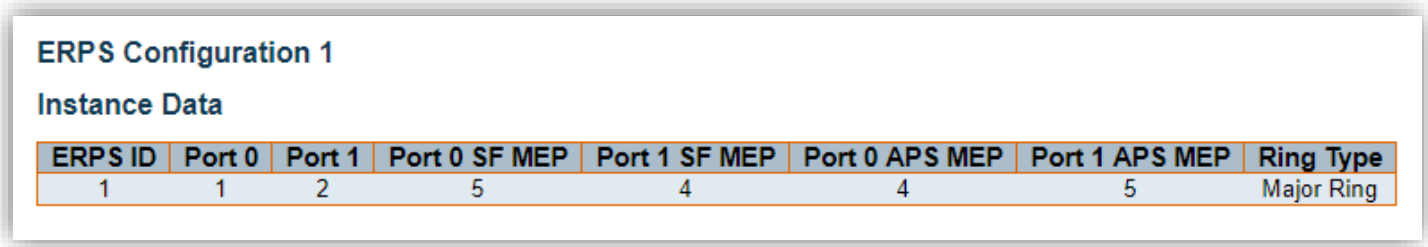
Ethernet-Ring-Schutzumschaltung



Einstellung	Beschreibung
Löschen	Dieses Kontrollkästchen dient dazu, ein ERPS für die Löschung beim nächsten Speichervorgang zu markieren.
ERPS-ID	Die ID der erstellten Schutzgruppe. Es muss sich um eine ganze Zahl zwischen 1 und 64 handeln. Es können maximal 64 ERPS-Schutzgruppen erstellt werden. Klicken Sie auf die ID einer Schutzgruppe, um die Konfigurationsseite aufzurufen.
Port 0	Dadurch wird ein Port 0 des Switches im Ring erstellt.
Port 1	Hiermit wird Port 1 des Switches im Ring erstellt. Da ein miteinander verbundener Subring nur einen Ringport hat, wird Port 1 für den miteinander verbundenen Subring auf 0 konfiguriert. Die Eingabe 0 in diesem Feld bedeutet, dass dieser Instanz kein Port 1 zugeordnet ist.
Port 0 SF MEP	Das MEP zur Meldung eines Signalausfalls an Port 0.
Port 1 SF MEP	Das MEP zur Meldung eines Signalausfalls an Port 1. Da dem miteinander verbundenen Teilring ohne virtuellen Kanal nur ein SF-MEP zugeordnet ist, wird es für solche Ringinstanzen auf 0 konfiguriert. Der Wert 0 in diesem Feld bedeutet, dass dieser Instanz kein SF-MEP für Port 1 zugeordnet ist.
Port 0 APS MEP	Die APS-PDU an Port 0, die MEP verarbeitet.
Port 1 APS MEP	Die Port 1 APS-PDU, die MEP verarbeitet. Da nur eine APS-MEP mit einem miteinander verbundenen Subring ohne virtuellen Kanal verknüpft ist, wird sie für solche Ringinstanzen auf 0 gesetzt. Der Wert 0 in diesem Feld bedeutet, dass dieser Instanz keine Port 1 APS-MEP zugeordnet ist.
Ringtyp	Typ des Schutzrings. Es kann sich entweder um einen Hauptring oder einen Unterring handeln.
Verbundener Knoten	„Verbundener Knoten“ gibt an, dass die Ringinstanz verbunden ist. Klicken Sie auf das Kontrollkästchen, um dies zu konfigurieren. „Ja“ bedeutet, dass es sich bei dieser Instanz um einen verbundenen Knoten handelt. „Nein“ bedeutet, dass die konfigurierte Instanz nicht verbunden ist.
Virtueller Kanal	Unterringe können am miteinander verbundenen Knoten entweder über einen virtuellen Kanal verfügen oder nicht. Dies wird über das Kontrollkästchen „Virtueller Kanal“ konfiguriert. „Ja“ bedeutet, dass es sich um einen Unterring mit virtuellem Kanal handelt. „Nein“ bedeutet, dass der Unterring keinen virtuellen Kanal hat.
Hauptring-ID	Hauptringgruppen-ID für den miteinander verbundenen Unterring. Sie wird verwendet, um Aktualisierungen von Topologieänderungen im Hauptring zu senden. Ist der Ring ein Hauptring, entspricht dieser Wert der Schutzgruppen-ID dieses Rings.
Alarm	Auf dem ERPS liegt ein aktiver Alarm vor.

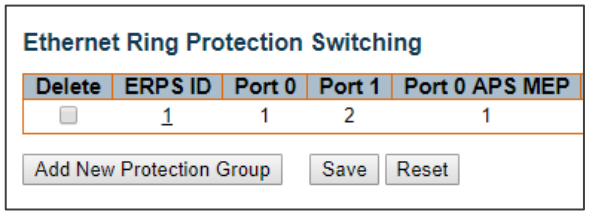
ERPS-Konfiguration n

Instanzdaten

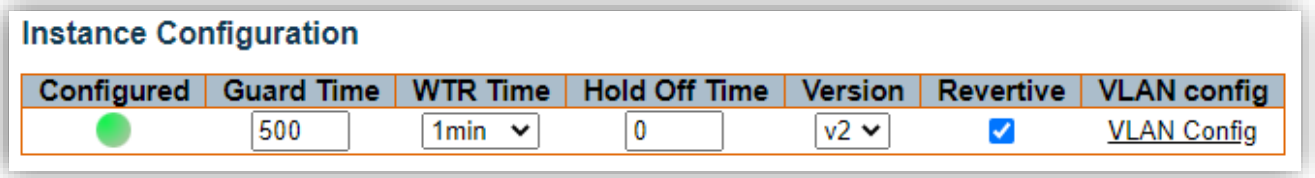


Einstellung	Beschreibung
ERPS-ID	Die ID der Schutzgruppe.
Port 0	Dies ist Port 0 des Switches im Ring.
Port 1	Dies ist Port 1 des Switches im Ring.
Port 0 SF MEP	Der MEP, der einen Signalausfall an Port 0 meldet.
Port 1 SF MEP	Der MEP zur Meldung eines Signalausfalls an Port 1.
Port 0 APS-MEP	Der MEP zur Verarbeitung der APS-PDU für Port 0.
Port 1 APS-MEP	Der MEP für die APS-PDU-Verarbeitung an Port 1.
Ringtyp	Art des Schutzrings. Es kann sich entweder um einen Hauptring oder einen Unterring handeln.

Instanzkonfiguration



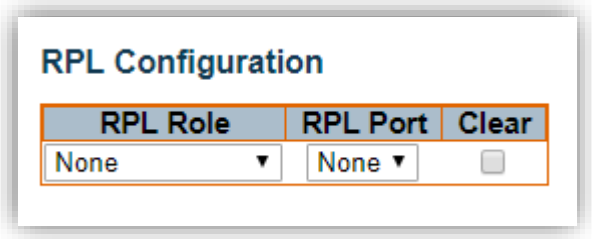
Klicken Sie auf die ERPS-ID-Nummer unter **„Ethernet-Ring-Schutzumschaltung“,** um die Instanz zu konfigurieren



Einstellung	Beschreibung	Werkseinstellung
Konfiguriert	• **Rot:** Dieser ERPS wurde nur erstellt und noch nicht konfiguriert – er ist nicht aktiv. • **Grün:** Dieses ERPS ist konfiguriert – es ist aktiv.	Keine
Wartezeit	Guard-Timeout-Wert, der verwendet wird, um zu verhindern, dass Ringknoten veraltete R-APS-Nachrichten empfangen. Die Dauer des Guard-Timers kann in 10-ms-Schritten zwischen 10 ms und 2 Sekunden konfiguriert werden.	500
WTR-Zeit	Der Wert für die „Wait To Restore“-Zeit, der bei der Rückumschaltung verwendet wird. Die Dauer der WTR-Zeit kann vom Betreiber in 1-Minuten-Schritten zwischen 1 und 12 Minuten konfiguriert werden.	1 min

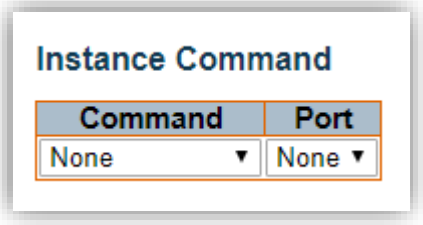
Wartezeit	Der Zeitwert, der verwendet wird, um vor der Umschaltung eine dauerhafte Überprüfung auf Signalausfall durchzuführen. Der Bereich des Hold-Off-Timers reicht von 0 bis 10 Sekunden in Schritten von 100 ms	0
Version	ERPS-Protokollversion – v1 oder v2	v2
Revertive	Im Revertive-Modus wird der Verkehrskanal, nachdem die Bedingungen, die zu einer Schutzumschaltung geführt haben, beseitigt sind, wieder auf die funktionierende Transporteinheit zurückgesetzt, d. h., auf dem RPL gesperrt. Im nicht-revertiven Modus nutzt der Verkehrskanal nach dem Wegfall einer Schutzumschaltbedingung weiterhin das RPL, sofern dieses nicht ausgefallen ist.	Aktiviert
VLAN-Konfiguration	VLAN-Konfiguration der Schutzgruppe. Klicken Sie auf den Link „VLAN-Konfiguration“, um VLANs für diese Schutzgruppe zu konfigurieren.	Keine

RPL-Konfiguration



Einstellung	Beschreibung
RPL-Rolle	Es kann sich entweder um den RPL-Eigentümer oder um einen RPL-Nachbarn handeln.
RPL-Port	Hiermit kann der Ost- oder West-Port als RPL-Block ausgewählt werden.
Löschen	Wenn der Eigentümer geändert werden muss, können Sie über das Kontrollkästchen „Löschen“ den RPL-Eigentümer für diesen ERPS-Ring löschen.

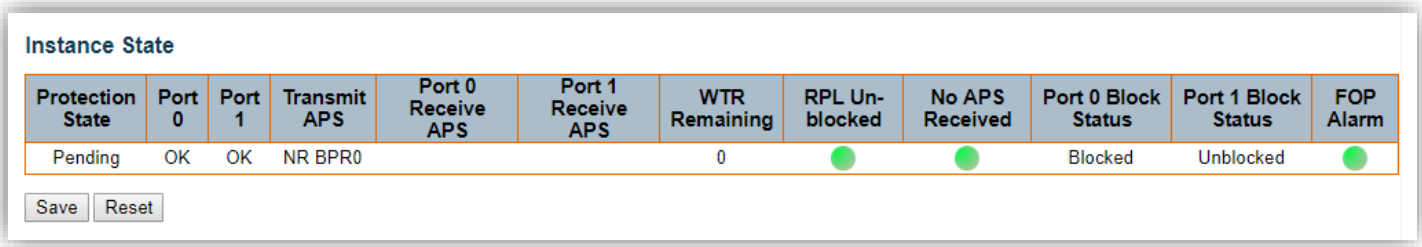
Instanzbefehl



Einstellung	Beschreibung
Befehl	Verwaltungsbefehl. Ein Port kann administrativ so konfiguriert werden, dass er sich entweder im manuellen oder im erzwungenen Switch-Zustand befindet.
Erzwungener Wechsel	Der Befehl „Erzwungener Wechsel“ erzwingt eine Sperrung des Ring-Ports, an dem der Befehl ausgegeben wird.
Manueller Wechsel	Sofern kein Fehler vorliegt und kein erzwungener Wechsel (FS) aktiv ist, erzwingt der Befehl „Manueller Wechsel“ eine Sperrung an dem Ring-Port, an dem der Befehl ausgegeben wird.

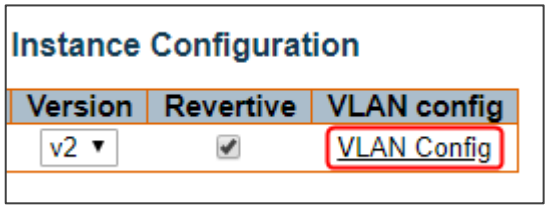
Löschen	Der Befehl „Clear“ dient zum Löschen eines aktiven lokalen Verwaltungsbefehls (z. B. „Forced Switch“ oder „Manual Switch“).
Port	Portauswahl – Port0 oder Port1 der Schutzgruppe, auf die der Befehl angewendet wird.

Instanzstatus

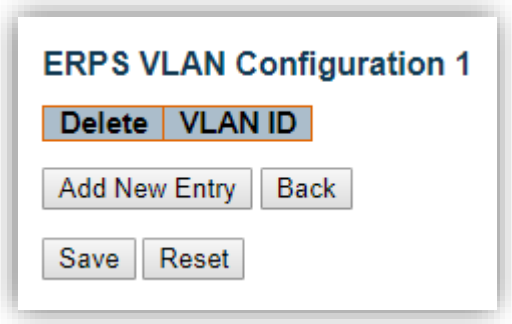


Einstellung	Beschreibung
Schutzstatus	ERPS-Zustand gemäß den Zustandsübergangstabellen in G.8032.
Port 0	**OK:** Der Zustand des östlichen Ports ist in Ordnung **SF:** Der Zustand des Ost-Ports ist „Signalausfall“
Port 1	**OK:** Der Zustand des westlichen Ports ist in Ordnung **SF:** Der Status des westlichen Ports ist „Signalausfall“
APS senden	Das gesendete APS gemäß den Zustandsübergangstabellen in G.8032.
Port 0 – Empfangene APS	Das an Port 0 empfangene APS gemäß den Zustandsübergangstabellen in G.8032.
Port 1 – Empfang APS	Das empfangene APS an Port 1 gemäß den Zustandsübergangstabellen in G.8032.
Verbleibende WTR	Verbleibende WTR-Zeitüberschreitung in Millisekunden.
RPL Nicht blockiert	APS wird im Arbeitsfluss empfangen.
Kein APS empfangen	RAPS-PDU wurde von der Gegenstelle nicht empfangen.
Blockstatus von Port 0	Blockstatus für Port 0 (sowohl für den Datenverkehr als auch für den R-APS-Blockstatus). Der R-APS-Kanal wird auf Subringen ohne virtuellen Kanal niemals blockiert.
Blockstatus von Port 1	Blockstatus für Port 1 (sowohl Datenverkehr als auch R-APS-Blockstatus). Der R-APS-Kanal wird auf Subringen ohne virtuellen Kanal niemals blockiert.
FOP-Alarm	Status „Failure of Protocol Defect“ (FOP). Wird ein FOP erkannt, leuchtet die rote LED; andernfalls leuchtet die grüne LED.

ERPS-VLAN-Konfiguration n



Klicken Sie **unter „Instanzkonfiguration“** auf „VLAN-Konfiguration“, um die ERPS-VLAN-ID-Nummer festzulegen



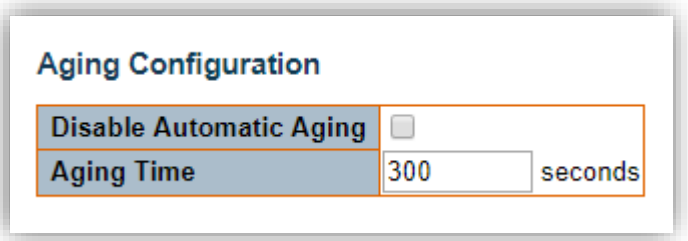
Einstellung	Beschreibung
Löschen	Um einen VLAN-Eintrag zu löschen, aktivieren Sie dieses Kontrollkästchen. Der Eintrag wird beim nächsten Speichern gelöscht.
VLAN-ID	Gibt die ID dieses bestimmten VLANs an.
Neues VLAN hinzufügen	Klicken Sie auf die Schaltfläche „**Neuen Eintrag** hinzufügen“, um eine neue VLAN-ID hinzuzufügen. Zulässige Werte für eine VLAN-ID sind 1 bis 4095. Das VLAN wird aktiviert, sobald Sie auf „Speichern“ klicken. Ein VLAN ohne zugehörige Ports wird gelöscht, sobald Sie auf „Speichern“ klicken. Mit der Schaltfläche „Löschen“ können Sie das Hinzufügen neuer VLANs rückgängig machen.

Konfiguration > MAC-Tabelle

Konfiguration der MAC-Adressentabelle

Auf dieser Seite wird die MAC-Adressentabelle konfiguriert. Legen Sie hier die Timeouts für Einträge in der dynamischen MAC-Tabelle fest und konfigurieren Sie die statische MAC-Tabelle.

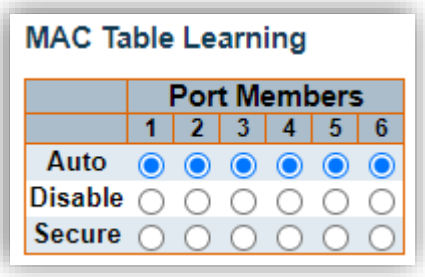
Aging-Konfiguration



Einstellung	Beschreibung
Automatisches Aging deaktivieren	Deaktivieren Sie das automatische Verfallen dynamischer Einträge, indem Sie das Kontrollkästchen „Automatisches Verfallen deaktivieren“ aktivieren.
Aging-Zeit	Standardmäßig werden dynamische Einträge nach 300 Sekunden aus der MAC-Tabelle entfernt. Dieser Vorgang wird auch als „Aging“ bezeichnet. Konfigurieren Sie die Verfallszeit, indem Sie hier einen Wert in Sekunden eingeben. Der zulässige Bereich liegt zwischen 10 und 1000000 Sekunden.

MAC-Tabellen-Lernmodus

Wenn der Lernmodus für einen bestimmten Port ausgegraut ist, wird dieser Modus von einem anderen Modul gesteuert, sodass er vom Benutzer nicht geändert werden kann. Ein Beispiel für ein solches Modul ist die MAC-basierte Authentifizierung unter 802.1X.



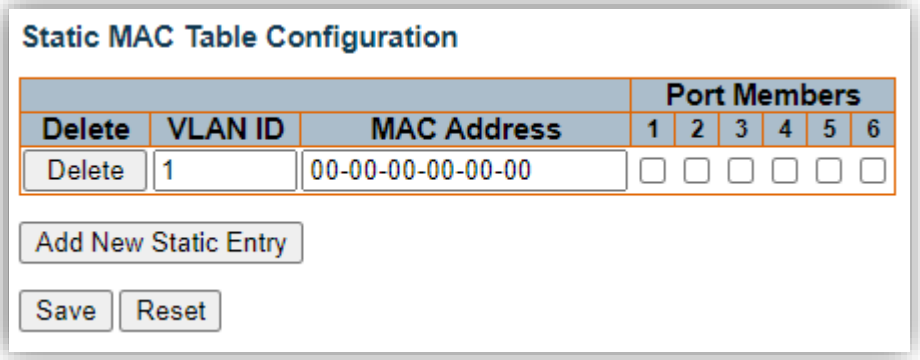
Einstellung	Beschreibung
Auto	Das Erlernen erfolgt automatisch, sobald ein Frame mit unbekanntem SMAC empfangen wird.
Deaktiviert	Es findet kein Einlernen statt.
Sicher	Es werden nur statische MAC-Einträge gelernt, alle anderen Frames werden verworfen. **HINWEIS:** Stellen Sie sicher, dass die für die Verwaltung des Switches verwendete Verbindung zur statischen MAC-Tabelle hinzugefügt wurde, bevor Sie in den sicheren Lernmodus wechseln; andernfalls geht die Verwaltungsverbindung verloren und kann nur über einen anderen, nicht gesicherten Port oder durch eine Verbindung zum Switch über die serielle Schnittstelle wiederhergestellt werden.

Konfiguration des VLAN-Lernens

Einstellung	Beschreibung
VLANs mit deaktiviertem Lernmodus	Dieses Feld zeigt die VLANs an, für die das Lernen deaktiviert ist. Wenn eine NEUE MAC-Adresse in einem VLAN mit deaktiviertem Lernen eintrifft, wird diese MAC-Adresse nicht gelernt. Standardmäßig ist das Feld leer. Es können weitere VLANs mithilfe einer Listensyntax erstellt werden, bei der die einzelnen Elemente durch Kommas getrennt sind. Bereiche werden durch einen Bindestrich zwischen der unteren und oberen Grenze angegeben. Das folgende Beispiel erstellt die VLANs 1, 10, 11, 12, 13, 200 und 300: **1,10-13,200,300**. Zwischen den Trennzeichen sind Leerzeichen zulässig.

Konfiguration der statischen MAC-Tabelle

Die statischen Einträge in der MAC-Tabelle sind in dieser Tabelle aufgeführt. Die statische MAC-Tabelle kann 64 Einträge enthalten. Die MAC-Tabelle ist zunächst nach VLAN-ID und anschließend nach MAC-Adresse sortiert.

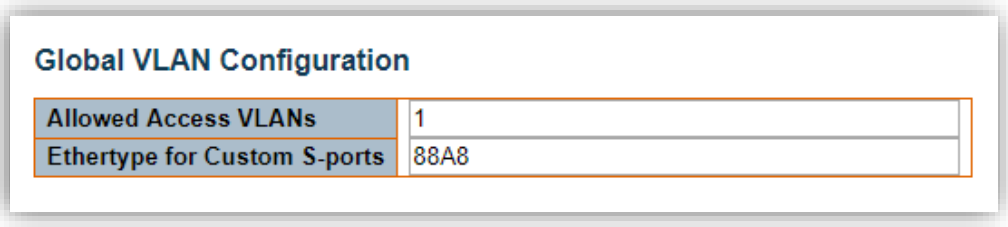


Einstellung	Beschreibung
Löschen	Aktivieren Sie dieses Kontrollkästchen, um den Eintrag zu löschen. Er wird beim nächsten Speichern gelöscht.
VLAN-ID	Die VLAN-ID des Eintrags.
MAC-Adresse	Die MAC-Adresse des Eintrags.
Port-Mitglieder	Häkchen zeigen an, welche Ports zu dem Eintrag gehören. Setzen oder entfernen Sie die Häkchen nach Bedarf, um den Eintrag zu ändern.

Konfiguration > VLANs

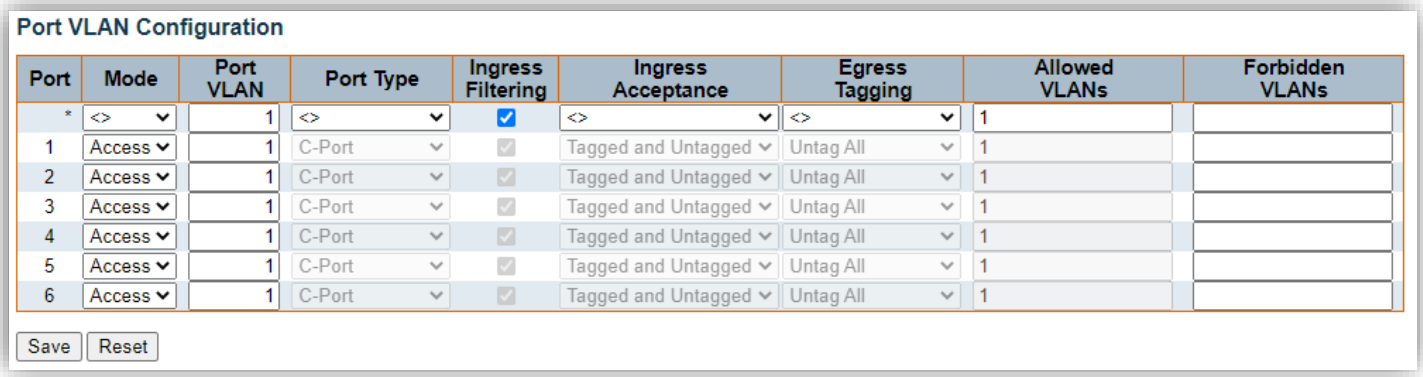
Auf dieser Seite können Sie die VLAN-Konfiguration am Switch steuern.
Die Seite ist in einen globalen Bereich und einen Bereich für die portbezogene Konfiguration unterteilt.

Globale VLAN-Konfiguration



Einstellung	Beschreibung
Zulässige Access-VLANs	Dieses Feld zeigt die zulässigen Access-VLANs an, d. h., es wirkt sich nur auf Ports aus, die als Access-Ports konfiguriert sind. Ports in anderen Modi gehören zu den VLANs, die im Feld „Zulässige VLANs“ angegeben sind. Standardmäßig ist nur VLAN 1 aktiviert. Weitere VLANs können mithilfe einer Listensyntax erstellt werden, bei der die einzelnen Elemente durch Kommas getrennt sind. Bereiche werden durch einen Bindestrich zwischen der unteren und oberen Grenze angegeben. Das folgende Beispiel erstellt die VLANs 1, 10, 11, 12, 13, 200 und 300: **1,10-13,200,300**. Zwischen den Trennzeichen sind Leerzeichen zulässig.
Ethertype für benutzerdefinierte S-Ports	Dieses Feld gibt den Ethertyp/die TPID (in Hexadezimalzahlen angegeben) an, der/die für benutzerdefinierte S-Ports verwendet wird. Die Einstellung gilt für alle Ports, deren Porttyp auf „S-Custom-Port“ gesetzt ist.

Port-VLAN-Konfiguration



Einstellung	Beschreibung
Modus	Der Port-Modus (Standard ist „Access“) bestimmt das grundlegende Verhalten des betreffenden Ports. Ein Port kann sich in einem der drei unten beschriebenen Modi befinden. Wenn ein bestimmter Modus ausgewählt wird, werden die übrigen Felder in dieser Zeile je nach Modus entweder ausgegraut oder können bearbeitet werden. Ausgegraute Felder zeigen den Wert an, den der Port erhält, wenn der Modus angewendet wird. **„Access“:** Zugangsports werden normalerweise für die Verbindung zu Endgeräten verwendet. Dynamische Funktionen wie Voice-VLAN können den Port im Hintergrund möglicherweise weiteren VLANs hinzufügen. Zugangsports weisen die folgenden Merkmale auf: • Mitglied genau eines VLANs, des Port-VLANs (auch bekannt als Access-VLAN), das standardmäßig 1 ist • Akzeptiert untagged und C-getaggte Frames • Verwirft alle Frames, die nicht dem Access-VLAN zugeordnet sind • Beim Ausgang werden alle Frames ungetaggt übertragen **Trunk:** Trunk-Ports können Datenverkehr über mehrere VLANs gleichzeitig übertragen und werden normalerweise zur Verbindung mit anderen Switches verwendet. Trunk-Ports weisen die folgenden Eigenschaften auf: • Standardmäßig ist ein Trunk-Port Mitglied aller VLANs (1–4095) • Die VLANs, denen ein Trunk-Port angehört, können durch die Verwendung von „Allowed VLANs“ eingeschränkt werden • Frames, die einem VLAN zugeordnet sind, dem der Port nicht angehört, werden verworfen • Standardmäßig werden alle Frames außer denen, die dem Port-VLAN (auch als „Native VLAN“ bezeichnet) zugeordnet sind, beim Ausgang getaggt. Frames, die dem Port-VLAN zugeordnet sind, erhalten beim Ausgang kein C-Tag • Die Tagging-Einstellung beim Ausgang kann so geändert werden, dass alle Frames getaggt werden; in diesem Fall werden beim Eingang nur getaggte Frames akzeptiert **Hybrid:** Hybrid-Ports ähneln in vielerlei Hinsicht Trunk-Ports, bieten jedoch zusätzliche Konfigurationsmöglichkeiten. Zusätzlich zu den für Trunk-Ports beschriebenen Eigenschaften verfügen Hybrid-Ports über folgende Funktionen: • Sie können so konfiguriert werden, dass sie VLAN-Tags ignorieren, C-Tags, S-Tags oder benutzerdefinierte S-Tags unterstützen • Die Eingangsfilterung kann gesteuert werden • Die Annahme von Frames am Eingang und die Konfiguration des Egress-Taggings können unabhängig voneinander konfiguriert werden

Port-VLAN	Legt die VLAN-ID des Ports (auch bekannt als PVID) fest. Zulässige VLANs liegen im Bereich von 1 bis 4095, wobei der Standardwert 1 ist. Beim Eingang werden Frames dem Port-VLAN zugeordnet, wenn der Port als „VLAN-unabhängig“ konfiguriert ist, der Frame nicht getaggt ist oder die VLAN-Erkennung am Port aktiviert ist, der Frame jedoch mit einer Prioritätskennzeichnung versehen ist (VLAN-ID = 0). Beim Ausgang werden Frames, die dem Port-VLAN zugeordnet wurden, nicht getaggt, wenn die Konfiguration für das Ausgangstagging auf „Port-VLAN nicht taggen“ eingestellt ist. Das Port-VLAN wird für Ports im Access-Modus als „Access-VLAN“ und für Ports im Trunk- oder Hybrid-Modus als „Native-VLAN“ bezeichnet.
Porttyp	Ports im Hybrid-Modus ermöglichen die Änderung des Port-Typs, d. h., ob ein VLAN-Tag eines Frames verwendet wird, um den Frame beim Eingang einem bestimmten VLAN zuzuordnen, und wenn ja, auf welche TPID er reagiert. Ebenso bestimmt der Port-Typ beim Ausgang die TPID des Tags, falls ein Tag erforderlich ist. **Unaware:** Beim Eingang werden alle Frames, unabhängig davon, ob sie ein VLAN-Tag tragen oder nicht, dem Port-VLAN zugeordnet, und eventuelle Tags werden beim Ausgang nicht entfernt. **C-Port:** Beim Eingang werden Frames mit einem VLAN-Tag mit TPID = 0x8100 dem im Tag eingebetteten VLAN-ID zugeordnet. Ist ein Frame ungetaggt oder mit einem Prioritäts-Tag versehen, wird er dem Port-VLAN zugeordnet. Müssen Frames beim Ausgang getaggt werden, erhalten sie ein C-Tag. **S-Port:** Müssen Frames beim Ausgang getaggt werden, werden sie mit einem S-Tag versehen. Beim Eingang werden Frames mit einem VLAN-Tag mit TPID = 0x88A8 dem im Tag eingebetteten VLAN zugeordnet. Frames mit Prioritäts-Tag werden dem Port-VLAN zugeordnet. Ist der Port so konfiguriert, dass er nur getaggte Frames akzeptiert (siehe „Akzeptanz beim Eingang“ weiter unten), werden Frames ohne diese TPID verworfen. ***Hinweis:*** Ist der S-Port so konfiguriert, dass er sowohl getaggte als auch ungetaggte Frames akzeptiert (siehe „Eingangsakzeptanz“ weiter unten), werden Frames mit einem C-Tag wie Frames mit einem S-Tag behandelt. Ist der S-Port so konfiguriert, dass er nur „Untagged“-Frames akzeptiert, werden S-getaggte Frames verworfen (mit Ausnahme von prioritätsgetaggten S-Frames). C-getaggte Frames werden zunächst als untagged betrachtet und daher nicht verworfen. Im weiteren Verlauf des Eingangs-Klassifizierungsprozesses werden sie dem im Tag eingebetteten VLAN zugeordnet, anstatt der Port-VLAN-ID. **S-Custom-Port:** Müssen Frames beim Ausgang getaggt werden, werden sie mit dem benutzerdefinierten S-Tag versehen. Beim Eingang werden Frames mit einem

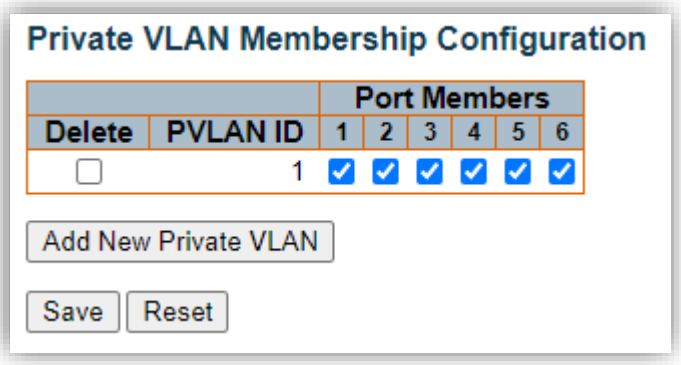
	VLAN-Tag, dessen TPID dem für Custom-S-Ports konfigurierten Ethertype entspricht, dem im Tag eingebetteten VLAN zugeordnet. Frames mit Prioritäts-Tag werden dem Port-VLAN zugeordnet. Ist der Port so konfiguriert, dass er nur getaggte Frames akzeptiert (siehe „Eingangsakzeptanz“ weiter unten), werden Frames ohne diese TPID verworfen. ***Hinweis:*** Wenn der benutzerdefinierte S-Port so konfiguriert ist, dass er sowohl getaggte als auch untaggte Frames akzeptiert (siehe „Eingangsakzeptanz“ weiter unten), werden Frames mit einem C-Tag wie Frames mit einem benutzerdefinierten S-Tag behandelt. Ist der benutzerdefinierte S-Port so konfiguriert, dass er ausschließlich „Untagged“-Frames akzeptiert, werden Frames mit benutzerdefiniertem S-Tag verworfen (mit Ausnahme von Frames mit benutzerdefiniertem S-Tag und Priorität). Frames mit C-Tag gelten zunächst als „Untagged“ und werden daher nicht verworfen. Im weiteren Verlauf des Eingangs-Klassifizierungsprozesses werden sie dem im Tag eingebetteten VLAN zugeordnet, anstatt der Port-VLAN-ID.
Eingangsfilterung	Hybrid-Ports ermöglichen eine anpassbare Eingangsfilterung. Bei Access- und Trunk-Ports ist die Eingangsfilterung immer aktiviert. Wenn die Eingangsfilterung aktiviert ist (Kontrollkästchen ist markiert), werden Frames verworfen, die einem VLAN zugeordnet wurden, dem der Port nicht angehört. Wenn die Eingangsfilterung deaktiviert ist, werden Frames, die einem VLAN zugeordnet sind, dem der Port nicht angehört, akzeptiert und an die Switch-Engine weitergeleitet. Der Port sendet jedoch niemals Frames, die VLANs zugeordnet sind, denen er nicht angehört.
Akzeptanz bei eingehenden Frames	Hybrid-Ports ermöglichen es, die Art der Frames zu ändern, die beim Eingang akzeptiert werden. **Getaggt und ungetaggt:** Sowohl getaggte als auch ungetaggte Frames werden akzeptiert. Eine Beschreibung, wann ein Frame als getaggt gilt, finden Sie unter „Porttyp“. **Nur getaggt:** Beim Eingang werden nur Frames akzeptiert, die mit dem entsprechenden Port-Typ-Tag versehen sind. **Nur ohne Tag:** Beim Eingang werden nur Frames ohne Tag akzeptiert. Eine Beschreibung, wann ein Frame als ohne Tag gilt, finden Sie unter „Porttyp“.
Tagging beim Ausgang	Ports im Trunk- und Hybrid-Modus können das Tagging von Frames beim Ausgang steuern. **Port-VLAN ohne Tagging:** Frames, die dem Port-VLAN zugeordnet sind, werden ohne Tagging übertragen. Andere Frames werden mit dem entsprechenden Tag übertragen. **Alle mit Tag versehen:** Alle Frames, unabhängig davon, ob sie dem Port-VLAN zugeordnet sind oder nicht, werden mit einem Tag übertragen. **Alle ohne Tag:** Alle Frames, unabhängig davon, ob sie dem Port-VLAN zugeordnet sind oder nicht, werden ohne Tag übertragen. Diese Option ist nur für Ports im Hybrid-Modus verfügbar.

Zulässige VLANs	Ports im Trunk- und Hybrid-Modus können steuern, welchen VLANs sie beitreten dürfen. Access-Ports können nur Mitglied eines einzigen VLANs sein, nämlich des Access-VLANs. Die Syntax des Feldes entspricht der im Feld „Aktivierte VLANs“ verwendeten Syntax. Standardmäßig wird ein Trunk- oder Hybrid-Port Mitglied aller VLANs und ist daher auf **1–4095** eingestellt. Das Feld kann leer gelassen werden, was bedeutet, dass der Port Mitglied in keinem VLAN wird.
Verbotene VLANs	Ein Port kann so konfiguriert werden, dass er niemals Mitglied eines oder mehrerer VLANs wird. Dies ist besonders nützlich, wenn verhindert werden soll, dass dynamische VLAN-Protokolle wie MVRP und GVRP Ports dynamisch zu VLANs hinzufügen. Der Trick besteht darin, solche VLANs auf dem betreffenden Port als verboten zu kennzeichnen. Die Syntax ist identisch mit der im Feld „Enabled VLANs“ verwendeten Syntax. Standardmäßig bleibt das Feld leer, was bedeutet, dass der Port Mitglied aller möglichen VLANs werden kann.

Konfiguration > Private VLANs > Mitgliedschaft

Konfiguration der Mitgliedschaft in privaten VLANs

Hier können die Konfigurationen der Private-VLAN-Mitgliedschaft für den Switch überwacht und geändert werden. Hier können Private-VLANs hinzugefügt oder gelöscht werden. Hier können Port-Mitglieder jedes Private-VLANs hinzugefügt oder entfernt werden.
Private VLANs basieren auf der Quellportmaske, und es bestehen keine Verbindungen zu VLANs. Das bedeutet, dass VLAN-IDs und Private-VLAN-IDs identisch sein können.
Ein Port muss sowohl Mitglied eines VLANs als auch eines privaten VLANs sein, um Pakete weiterleiten zu können. Standardmäßig sind alle Ports VLAN-unabhängig und Mitglieder von VLAN 1 sowie des privaten VLANs 1.
Ein VLAN-unabhängiger Port kann nur Mitglied eines einzigen VLANs sein, jedoch Mitglied mehrerer privater VLANs.

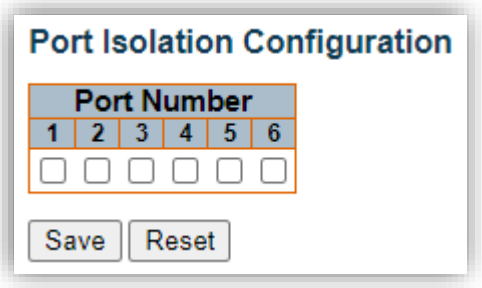


Einstellung	Beschreibung
Löschen	Um einen Private-VLAN-Eintrag zu löschen, aktivieren Sie dieses Kontrollkästchen. Der Eintrag wird beim nächsten Speichern gelöscht.
Private-VLAN-ID	Gibt die ID dieses bestimmten privaten VLANs an.
Port-Mitglieder	Für jede private VLAN-ID wird eine Reihe von Kontrollkästchen für jeden Port angezeigt. Um einen Port in ein privates VLAN aufzunehmen, aktivieren Sie das Kontrollkästchen. Um den Port aus dem privaten VLAN zu entfernen oder auszuschließen, stellen Sie sicher, dass das Kontrollkästchen deaktiviert ist. Standardmäßig sind keine Ports Mitglieder, und alle Kontrollkästchen sind deaktiviert.

Konfiguration > Private VLANs > Port-Isolation

Konfiguration der Port-Isolation

Auf dieser Seite können Sie die Portisolierung für Ports in einem privaten VLAN aktivieren oder deaktivieren.
Ein Port, der Mitglied eines VLANs ist, kann gegenüber anderen isolierten Ports im selben VLAN und privaten VLAN isoliert werden.



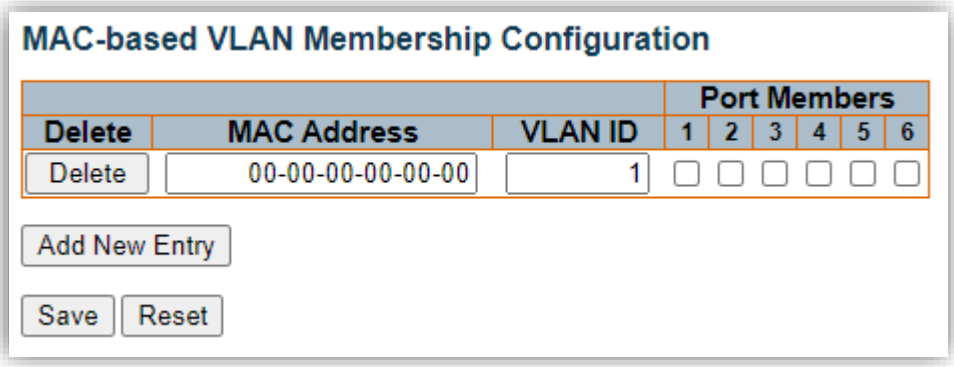
Portnummer

Einstellung	Beschreibung	Werkseinstellung
Aktiviert	Die Portisolierung ist an diesem Port aktiviert.	Nicht markiert
Nicht markiert	Die Port-Isolation ist an diesem Port deaktiviert.	

Konfiguration > VCL > MAC-basiertes VLAN

Konfiguration der MAC-basierten VLAN-Zugehörigkeit

Hier können die Zuordnungen von MAC-Adressen zu VLAN-IDs konfiguriert werden. Auf dieser Seite können Sie Einträge zur MAC-basierten VLAN-Klassifizierungsliste hinzufügen und löschen sowie die Einträge verschiedenen Ports zuweisen.



Einstellung	Beschreibung
Löschen	Um einen Eintrag für die Zuordnung von MAC-Adressen zu VLAN-IDs zu löschen, aktivieren Sie dieses Kontrollkästchen und klicken Sie auf „Speichern“. Der Eintrag wird im Stack gelöscht.
MAC-Adresse	Gibt die MAC-Adresse der Zuordnung an.
VLAN-ID	Gibt die VLAN-ID an, der die oben genannte MAC-Adresse zugeordnet wird.
Port-Mitglieder	Für jeden Eintrag der Zuordnung von MAC-Adresse zu VLAN-ID wird eine Reihe von Kontrollkästchen für jeden Port angezeigt. Um einen Port in die Zuordnung aufzunehmen, aktivieren Sie das Kontrollkästchen. Um den Port aus der Zuordnung zu entfernen oder auszuschließen, stellen Sie sicher, dass das Kontrollkästchen deaktiviert ist. Standardmäßig sind keine Ports Mitglieder, und alle Kontrollkästchen sind deaktiviert.

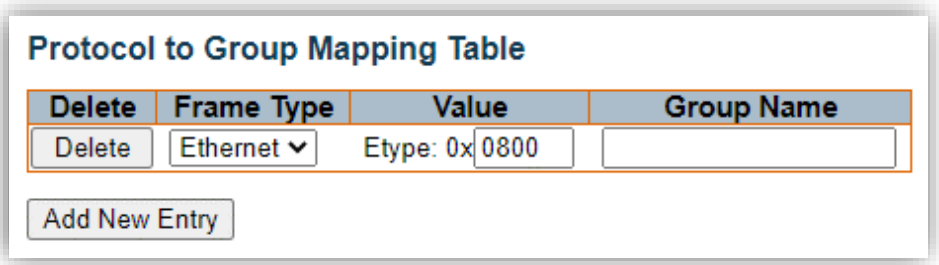
Schaltfläche „Neuen Eintrag hinzufügen“

Klicken Sie auf die Schaltfläche „Neuen Eintrag hinzufügen“, um einen neuen Eintrag für die Zuordnung von MAC-Adressen zu VLAN-IDs hinzuzufügen. Der Tabelle wird eine leere Zeile hinzugefügt, und die Zuordnung kann nach Bedarf konfiguriert werden. Zur Konfiguration der Zuordnung kann jede Unicast-MAC-Adresse verwendet werden. Broadcast- oder Multicast-MAC-Adressen sind nicht zulässig. Gültige Werte für eine VLAN-ID liegen zwischen **1** und **4095**.
Der Eintrag für die Zuordnung von MAC-Adressen zu VLAN-IDs wird aktiviert, wenn Sie auf „Speichern“ klicken. Eine Zuordnung ohne zugehörige Ports wird beim Klicken auf „Speichern“ nicht hinzugefügt. Die maximal mögliche Anzahl an Zuordnungseinträgen von MAC-Adressen zu VLAN-IDs ist auf 256 begrenzt.

Konfiguration > VCL > Protokollbasiertes VLAN > Protokoll-zu-Gruppe

Zuordnungstabelle „Protokoll zu Gruppe“

Auf dieser Seite können Sie neue Zuordnungseinträge für „Protokoll zu Gruppenname“ hinzufügen (jedes Protokoll kann nur Teil einer einzigen Gruppe sein) sowie bereits zugeordnete Einträge für den Switch anzeigen und löschen.



Einstellung	Beschreibung
Löschen	Um einen Zuordnungseintrag für „Protokoll zu Gruppenname“ zu löschen, aktivieren Sie dieses Kontrollkästchen. Der Eintrag wird beim nächsten Speichern vom Switch gelöscht.
Frame-Typ	Der Frame-Typ kann einen der folgenden Werte annehmen: • **Ethernet** • **LLC** • **SNAP** **HINWEIS:** Wenn Sie das Feld „Rahmentyp“ ändern, variieren die gültigen Werte des folgenden Textfelds je nach dem von Ihnen ausgewählten neuen Rahmentyp.
Wert	Der gültige Wert, der in dieses Textfeld eingegeben werden kann, hängt von der im vorhergehenden Auswahlmenü „Frame-Typ“ gewählten Option ab. Nachfolgend sind die Kriterien für die drei verschiedenen Rahmentypen aufgeführt: • **Ethernet:** Der Wert im Textfeld, wenn „Ethernet“ als Rahmentyp ausgewählt ist, wird als „etype“ bezeichnet. Gültige Werte für „etype“ liegen im Bereich von 0x0600 bis 0xffff • **LLC:** Der gültige Wert setzt sich in diesem Fall aus zwei verschiedenen Teilwerten zusammen. a. ***DSAP:*** 1 Byte lange Zeichenfolge (0x00–0xff) b. ***SSAP:*** 1-Byte-Zeichenkette (0x00–0xff) • **SNAP:** Der gültige Wert setzt sich in diesem Fall ebenfalls aus zwei verschiedenen Teilwerten zusammen. a. ***OUI:*** OUI (Organizationally Unique Identifier) ist ein Parameter im Format xx-xx-xx, wobei jedes Paar (xx) in der Zeichenfolge ein Hexadezimalwert im Bereich von 0x00 bis 0xff ist. b. ***PID:*** PID (Protocol ID). Wenn die OUI den Hexadezimalwert 000000 hat, entspricht die Protokoll-ID dem Wert des Felds „EtherType“ für das auf SNAP aufbauende Protokoll; wenn die OUI eine OUI für eine bestimmte Organisation ist, ist die Protokoll-ID ein Wert, der von dieser Organisation dem auf SNAP aufbauenden Protokoll zugewiesen wurde. Mit anderen Worten: Wenn der Wert des OUI-Feldes 00-00-00 ist, dann ist der Wert der

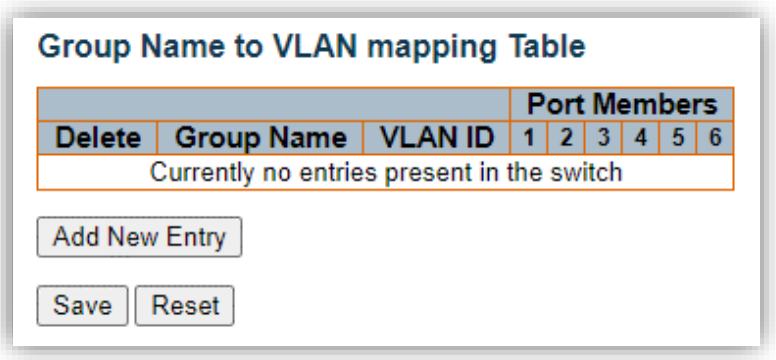
	PID „etype“ (0x0600–0xffff), und wenn der Wert der OUI nicht 00-00-00 ist, dann sind gültige Werte für die PID beliebige Werte zwischen 0x0000 und 0xffff.
Gruppenname	Ein gültiger Gruppenname ist eine 16 Zeichen lange Zeichenfolge, die für jeden Eintrag eindeutig ist und aus einer Kombination von Buchstaben (a–z oder A–Z) und Ziffern (0–9) besteht. **HINWEIS:** Sonderzeichen und Unterstriche (_) sind nicht zulässig.

Schaltfläche „Neuen Eintrag hinzufügen“
Klicken Sie **auf „Neuen Eintrag hinzufügen“**, um einen neuen Eintrag in die Zuordnungstabelle aufzunehmen. Der Tabelle wird eine leere Zeile hinzugefügt, in der Frame-Typ, Wert und Gruppenname nach Bedarf konfiguriert werden können. Die maximal mögliche Anzahl an Protokoll-zu-Gruppe-Zuordnungen ist auf 128 begrenzt.

Konfiguration > VCL > Protokollbasiertes VLAN > Zuordnung von Gruppe zu VLAN

Zuordnungstabelle „Gruppenname zu VLAN“

Auf dieser Seite können Sie einen Gruppennamen (der bereits konfiguriert ist oder später konfiguriert werden soll) einem VLAN für den Switch zuordnen.



Einstellung	Beschreibung
Löschen	Um eine Zuordnung von Gruppennamen zu VLANs zu löschen, aktivieren Sie dieses Kontrollkästchen. Der Eintrag wird beim nächsten Speichern vom Switch gelöscht.
Gruppenname	Ein gültiger Gruppenname ist eine Zeichenfolge mit einer Länge von maximal 16 Zeichen, die aus einer Kombination von Buchstaben (a–z oder A–Z) und Ziffern (0–9) besteht, wobei keine Sonderzeichen zulässig sind. Sie können entweder eine Gruppe verwenden, die bereits ein oder mehrere Protokolle enthält (siehe Zuordnungen von Protokollen zu Gruppen), oder eine Zuordnung von Gruppen zu VLAN-IDs erstellen, die in dem Moment aktiv wird, in dem Sie ein oder mehrere Protokolle zu dieser Gruppe hinzufügen. Darüber hinaus ist die Zuordnung von Gruppe zu VLAN-ID nicht eindeutig, solange sich die Portlisten dieser Zuordnungen nicht überschneiden (z. B. kann Gruppe 1 auf Port Nr. 1 der VID 1 und auf Port Nr. 2 der VID 2 zugeordnet werden).
VLAN-ID	Gibt die VLAN-ID an, der der Gruppenname zugeordnet wird. Eine gültige VLAN-ID liegt im Bereich von 1 bis 4095.
Port-Mitglieder	Für jede Zuordnung von Gruppennamen zu VLAN-IDs wird eine Reihe von Kontrollkästchen für jeden Port angezeigt. Um einen Port in die Zuordnung aufzunehmen, aktivieren Sie das Kontrollkästchen. Um den Port aus der Zuordnung zu entfernen oder auszuschließen, stellen Sie sicher, dass das Kontrollkästchen deaktiviert ist. Standardmäßig sind keine Ports Mitglieder, und alle Kontrollkästchen sind deaktiviert.

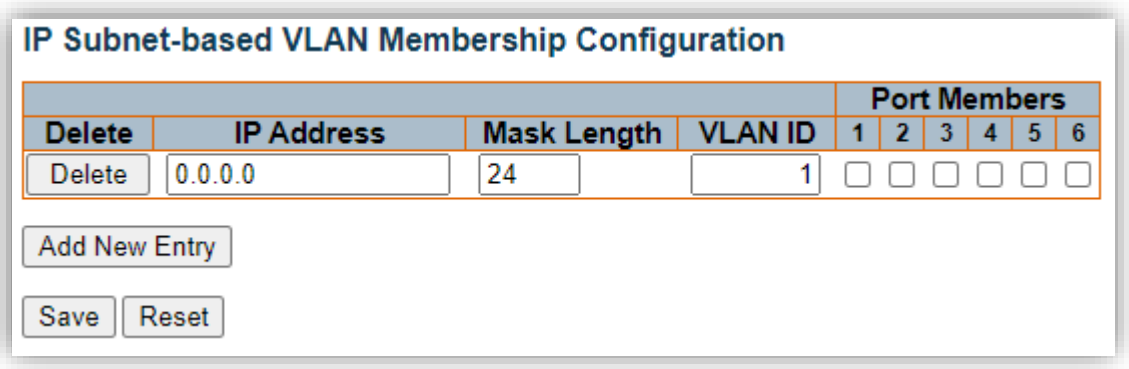
Schaltfläche „Neuen Eintrag hinzufügen“

Klicken Sie auf die Schaltfläche „Neuen Eintrag hinzufügen“, um einen neuen Eintrag in die Zuordnungstabelle aufzunehmen. Der Tabelle wird eine leere Zeile hinzugefügt, und der Gruppenname, die VLAN-ID sowie die Port-Mitglieder können nach Bedarf konfiguriert werden. Zulässige Werte für eine VLAN-ID liegen zwischen **1** und **4095**. Die maximal mögliche Anzahl an Zuordnungen von Gruppen zu VLANs ist auf 256 begrenzt.

Konfiguration > VCL > IP-Subnetz-basiertes VLAN

Konfiguration der VLAN-Zugehörigkeit auf Basis von IP-Subnetzen

Hier können die Zuordnungen von IP-Subnetzen zu VLAN-IDs konfiguriert werden. Auf dieser Seite können Sie Einträge für die Zuordnung von IP-Subnetzen zu VLAN-IDs hinzufügen, aktualisieren und löschen sowie diese verschiedenen Ports zuweisen.



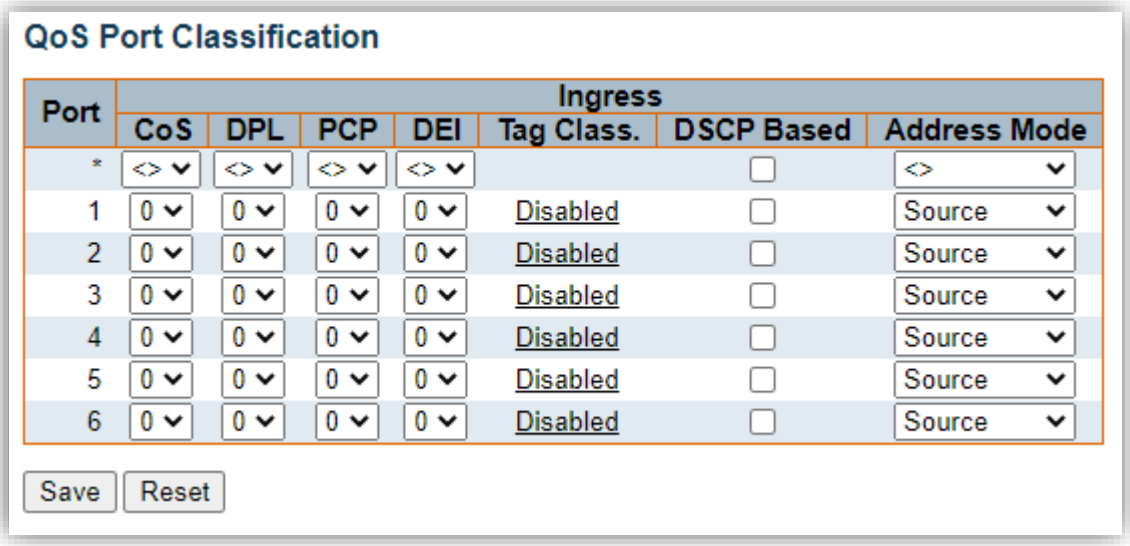
Einstellung	Beschreibung
Löschen	Um eine Zuordnung zu löschen, aktivieren Sie dieses Kontrollkästchen und klicken Sie auf „Speichern“. Der Eintrag wird im Stack gelöscht.
IP-Adresse	Gibt die IP-Adresse des Subnetzes an (hier kann auch eine beliebige Host-Adresse des Subnetzes angegeben werden; die Anwendung konvertiert diese automatisch).
Maskenlänge	Gibt die Maskenlänge des Subnetzes an.
VLAN-ID	Gibt die VLAN-ID an, der das Subnetz zugeordnet wird. Die Zuordnung von IP-Subnetz zu VLAN-ID ist eindeutig.
Port-Mitglieder	Für jeden Eintrag der Zuordnung von IP-Subnetzen zu VLAN-IDs wird eine Reihe von Kontrollkästchen für jeden Port angezeigt. Um einen Port in eine Zuordnung aufzunehmen, aktivieren Sie einfach das Kontrollkästchen. Um den Port aus der Zuordnung zu entfernen oder auszuschließen, stellen Sie sicher, dass das Kontrollkästchen deaktiviert ist. Standardmäßig sind keine Ports Mitglieder und alle Kontrollkästchen sind deaktiviert.

Schaltfläche „Neuen Eintrag hinzufügen“

Klicken Sie auf die Schaltfläche „Neuen Eintrag hinzufügen“, um einen neuen Zuordnungseintrag für ein IP-Subnetz zu einer VLAN-ID hinzuzufügen. Der Tabelle wird eine leere Zeile hinzugefügt, und die Zuordnung kann nach Bedarf konfiguriert werden. Für die Zuordnung können beliebige IP-Adressen und Subnetzmasken konfiguriert werden. Zulässige Werte für die VLAN-ID liegen zwischen **1** und **4095**. Der Eintrag für die Zuordnung von IP-Subnetzen zu VLAN-IDs wird aktiviert, wenn Sie auf „Speichern“ klicken. Die maximal mögliche Anzahl an Zuordnungen von IP-Subnetzen zu VLAN-IDs ist auf 128 begrenzt.

Konfiguration > QoS > Port-Klassifizierung

QoS-Eingangsport-Klassifizierung



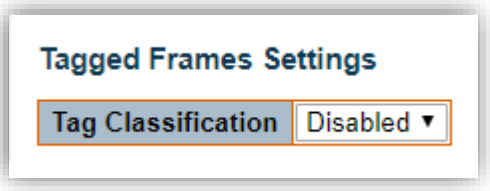
Einstellung	Beschreibung
Port	Die Portnummer, für die die folgende Konfiguration gilt.
CoS	Steuert den Standard-CoS-Wert. Alle Frames werden einer CoS zugeordnet. Es besteht eine Eins-zu-Eins-Zuordnung zwischen CoS, Warteschlange und Priorität. Eine CoS von 0 (Null) hat die niedrigste Priorität. Wenn der Port VLAN-fähig ist, der Frame getaggt ist und „Tag Class.“ aktiviert ist, wird der Frame einer CoS zugeordnet, die anhand der PCP- und DEI-Werte im Tag ermittelt wird. Andernfalls wird der Frame der Standard-CoS zugeordnet. Der zugewiesene CoS kann durch einen QCL-Eintrag überschrieben werden. **Hinweis**: Wenn der Standard-CoS dynamisch geändert wurde, wird der tatsächliche Standard-CoS in Klammern hinter dem konfigurierten Standard-CoS angezeigt.
DPL	Steuert den Standard-DPL-Wert. Alle Frames werden einer Drop-Precedence-Stufe zugeordnet. Wenn der Port VLAN-fähig ist, der Frame getaggt ist und „Tag Class.“ aktiviert ist, wird der Frame einer DPL zugeordnet, die anhand der PCP- und DEI-Werte im Tag ermittelt wird. Andernfalls wird der Frame der Standard-DPL zugeordnet. Die zugewiesene DPL kann durch einen QCL-Eintrag außer Kraft gesetzt werden.
PCP	Steuert den Standard-PCP-Wert. Alle Frames werden einem PCP-Wert zugeordnet. Wenn der Port VLAN-fähig ist und der Frame getaggt ist, wird der Frame dem im Tag enthaltenen PCP-Wert zugeordnet. Andernfalls wird der Frame dem Standard-PCP-Wert zugeordnet.

DEI	Steuert den Standard-DEI-Wert. Alle Frames werden einem DEI-Wert zugeordnet. Wenn der Port VLAN-fähig ist und der Frame getaggt ist, wird der Frame dem im Tag enthaltenen DEI-Wert zugeordnet. Andernfalls wird der Frame dem Standard-DEI-Wert zugeordnet.
Tag-Klasse.	Zeigt den Klassifizierungsmodus für getaggte Frames an diesem Port an. • **Deaktiviert:** Verwendet Standard-CoS und -DPL für getaggte Frames. • **Aktiviert:** Verwendet zugeordnete Versionen von PCP und DEI für getaggte Frames. Klicken Sie auf den Modus, um den Modus und/oder die Zuordnung zu konfigurieren. **HINWEIS:** Diese Einstellung hat keine Auswirkung, wenn der Port VLAN-unabhängig ist. An VLAN-unabhängigen Ports empfangene getaggte Frames werden immer der Standard-CoS und dem Standard-DPL zugeordnet.
DSCP-basiert	Klicken Sie hier, um die DSCP-basierte QoS-Klassifizierung am Eingangsport zu aktivieren.
Adressmodus	Der IP/MAC-Adressmodus legt fest, ob die QCL-Klassifizierung auf Quelladressen (SMAC/SIP) oder Zieladressen (DMAC/DIP) an diesem Port basieren soll. Die zulässigen Werte sind: • **Quelle:** SMAC/SIP-Abgleich aktivieren. • **Ziel:** Aktiviert den DMAC/DIP-Abgleich.

QoS-Eingangsport-Tag-Klassifizierung Port n

Auf dieser Seite wird der Klassifizierungsmodus für getaggte Frames konfiguriert.

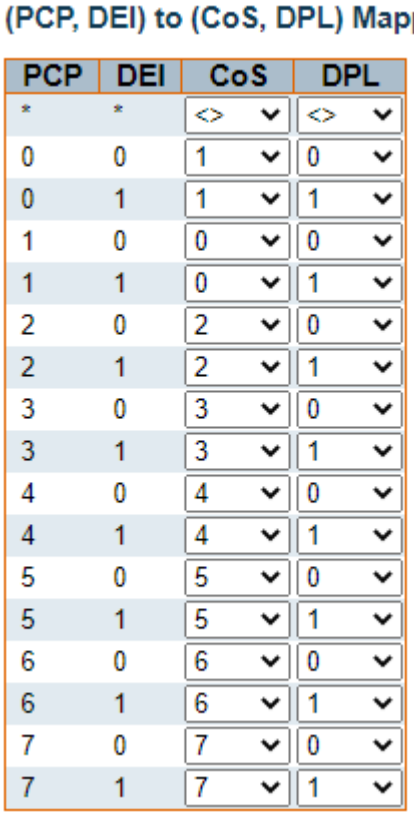
Einstellungen für getaggte Frames



Einstellung	Beschreibung	Werkseinstellung
Aktiviert	Verwendet zugeordnete Versionen von PCP und DEI für getaggte Frames.	Deaktiviert
Deaktiviert	Verwenden Sie die Standard-QoS-Klasse und die Drop-Prioritätsstufe für getaggte Frames.	

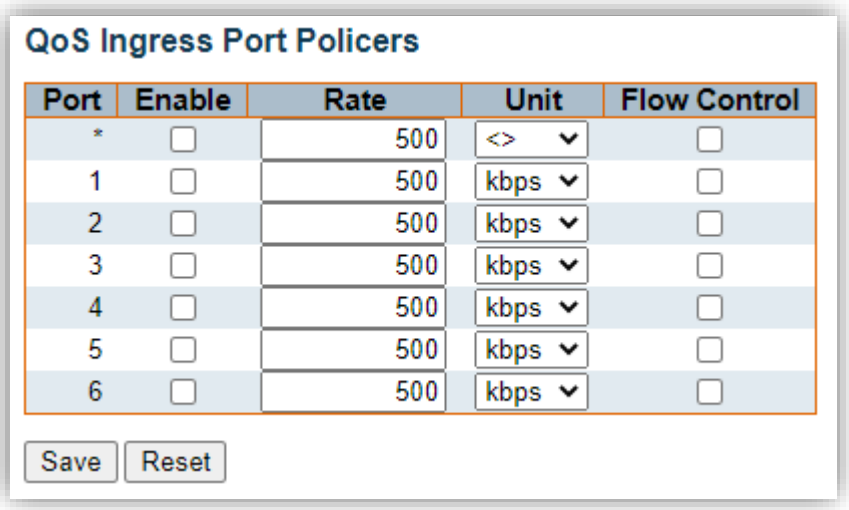
Zuordnung von (PCP, DEI) zu (QoS-Klasse, DP-Level)

Steuert die Zuordnung der klassifizierten Werte von (PCP, DEI) zu (QoS-Klasse, DP-Level), wenn die Tag-Klassifizierung auf **„Aktiviert“** gesetzt ist.



Konfiguration > QoS > Port-Policing

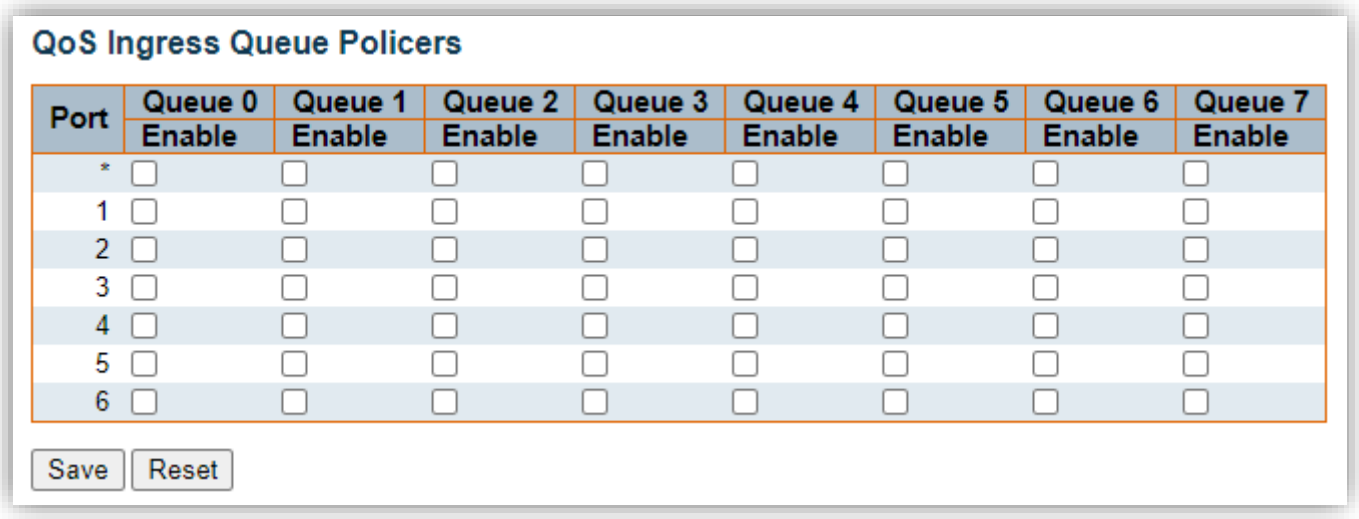
QoS-Ingress-Port-Policer



Einstellung	Beschreibung
Port	Die Portnummer, für die die folgende Konfiguration gilt.
Aktivieren	Aktivieren oder deaktivieren Sie den Port-Policer für diesen Switch-Port.
Rate	Steuert die Rate für den Port-Policer. Dieser Wert ist auf 100–3276700 beschränkt, wenn „Unit“ auf kbps oder fps eingestellt ist, und auf 1–3276, wenn „Unit“ auf Mbps oder kfps eingestellt ist. Die Rate wird intern auf den nächsten vom Port-Policer unterstützten Wert aufgerundet.
Einheit	Legt die Maßeinheit für die Port-Policer-Rate fest: kbps, Mbps, fps oder kfps.
Flusskontrolle	Wenn die Flusssteuerung aktiviert ist und sich der Port im Flusssteuerungsmodus befindet, werden Pausen-Frames gesendet, anstatt Frames zu verwerfen.

Konfiguration > QoS > Warteschlangen-Policing

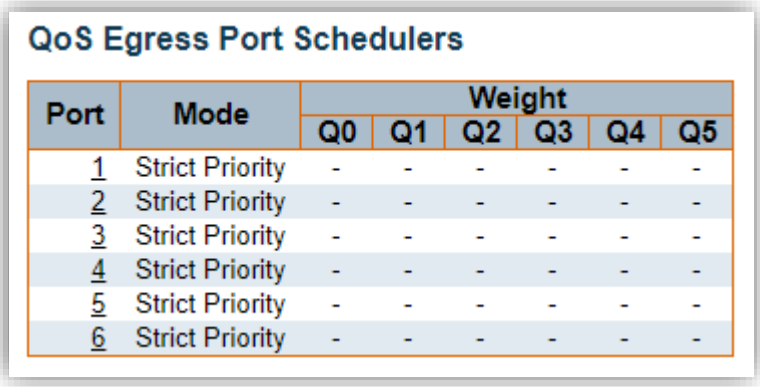
QoS-Ingress-Queue-Policer



Einstellung	Beschreibung
Port	Die Portnummer, für die die folgende Konfiguration gilt.
Aktivieren	Aktivieren oder deaktivieren Sie den Queue-Policer für diesen Switch-Port.
Rate	Steuert die Rate für den Port-Policer. Dieser Wert ist auf 100–3276700 beschränkt, wenn „Einheit“ kbps oder fps ist, und auf 1–3276, wenn „Einheit“ Mbps oder kfps ist. Die Rate wird intern auf den nächsten vom Port-Policer unterstützten Wert aufgerundet. Steuert die Rate für den Queue-Policer. Dieser Wert ist auf 100–3276700 beschränkt, wenn „Unit“ auf kbps eingestellt ist, und auf 1–3276, wenn „Unit“ auf Mbps eingestellt ist. Die Rate wird intern auf den nächsten vom Queue-Policer unterstützten Wert aufgerundet. Dieses Feld wird nur angezeigt, wenn mindestens einer der Queue-Policer aktiviert ist.
Einheit	Legt die Maßeinheit für die Rate des Warteschlangen-Policers fest (kbps oder Mbps). Dieses Feld wird nur angezeigt, wenn mindestens einer der Warteschlangen-Policer aktiviert ist.

Konfiguration > QoS > Port-Scheduler

QoS-Ausgangs-Port-Scheduler



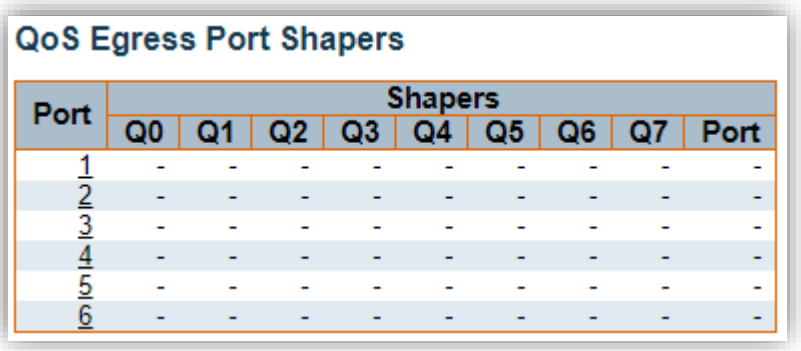
QoS Egress Port Schedulers

Port	Mode	Weight					
		Q0	Q1	Q2	Q3	Q4	Q5
1	Strict Priority	-	-	-	-	-	-
2	Strict Priority	-	-	-	-	-	-
3	Strict Priority	-	-	-	-	-	-
4	Strict Priority	-	-	-	-	-	-
5	Strict Priority	-	-	-	-	-	-
6	Strict Priority	-	-	-	-	-	-

Einstellung	Beschreibung
Port	Der logische Port für die Einstellungen in derselben Zeile. Klicken Sie auf die Portnummer, um die Scheduler zu konfigurieren.
Modus	Zeigt den Planungsmodus für diesen Port an.
Qn	Zeigt die Gewichtung für diese Warteschlange und diesen Port an.

Konfiguration > QoS > Port-Shaping

QoS-Egress-Port-Shaper

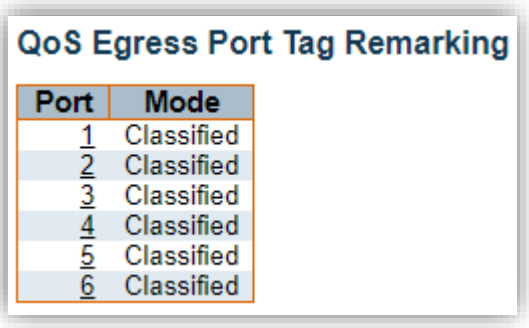

QoS Egress Port Shapers

Port	Shapers								
	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Port
1	-	-	-	-	-	-	-	-	-
2	-	-	-	-	-	-	-	-	-
3	-	-	-	-	-	-	-	-	-
4	-	-	-	-	-	-	-	-	-
5	-	-	-	-	-	-	-	-	-
6	-	-	-	-	-	-	-	-	-

Einstellung	Beschreibung
Port	Der logische Port für die Einstellungen in derselben Zeile. Klicken Sie auf die Portnummer, um die Shaper zu konfigurieren.
Qn	Zeigt „-“ für deaktiviert oder die aktuelle Shaper-Rate an – z. B. „800 Mbps“.
Port	Zeigt „-“ für deaktiviert oder die aktuelle Port-Shaper-Rate an – z. B. „800 Mbps“.

Konfiguration > QoS > Port-Tag-Umbenennung

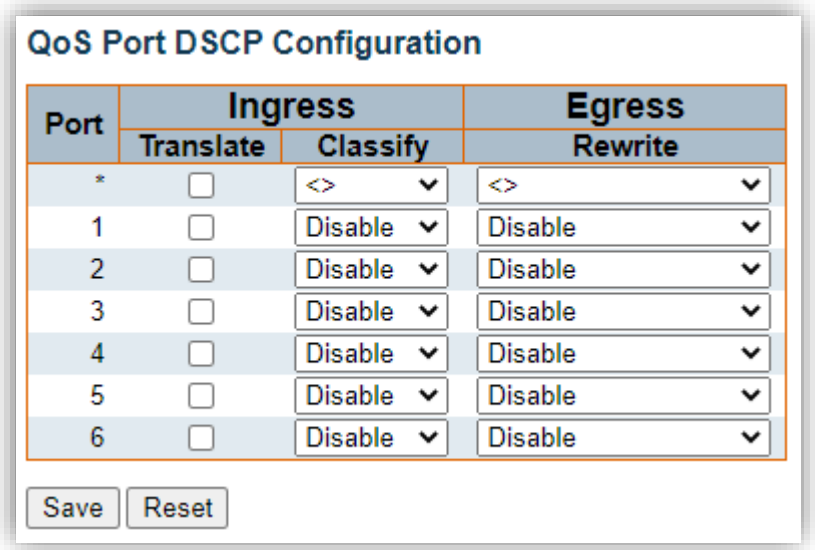
QoS-Port-Tag-Neuvergabe für ausgehenden Datenverkehr



Einstellung	Beschreibung
Port	Der logische Port für die Einstellungen in derselben Zeile. Klicken Sie auf die Portnummer, um die Tag-Neuvergabe zu konfigurieren.
Modus	Zeigt den Tag-Remarking-Modus für diesen Port an. • **Klassifiziert:** Verwenden Sie klassifizierte PCP/DEI-Werte. • **Standard:** Verwenden Sie Standard-PCP/DEI-Werte. • **Zugeordnet:** Verwenden Sie zugeordnete Versionen der QoS-Klasse und der DP-Stufe.

Konfiguration > QoS > Port-DSCP

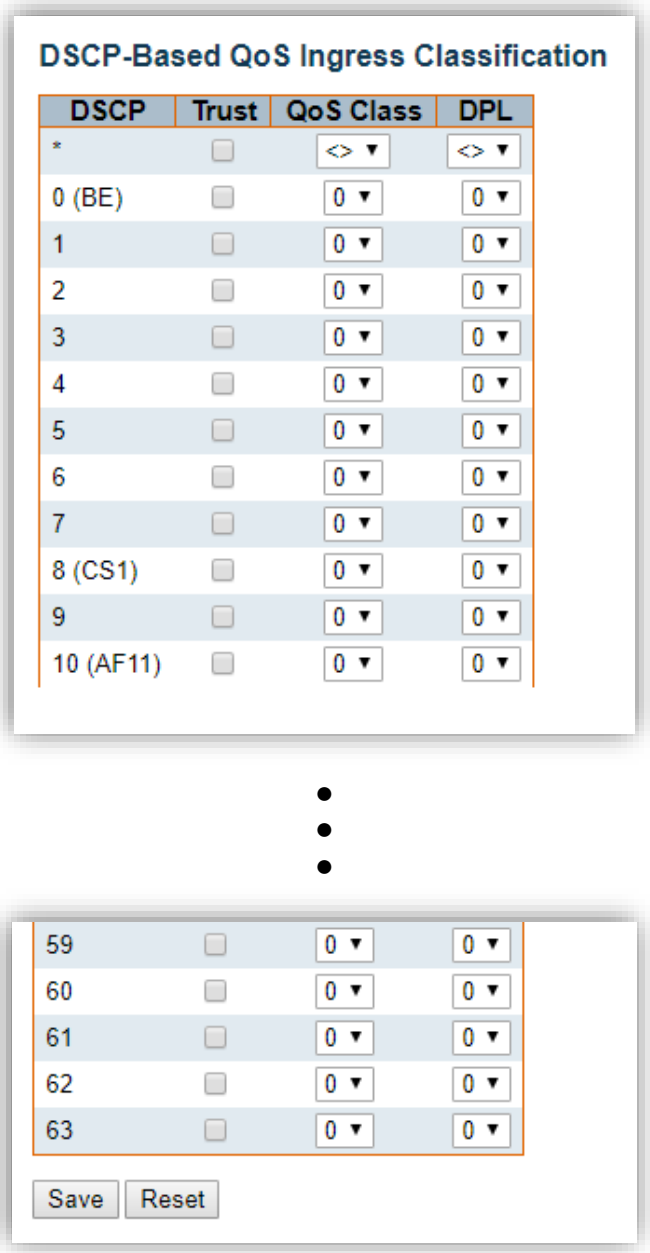
QoS-Port-DSCP-Konfiguration



Einstellung	Beschreibung
Port	Die Spalte „Port“ zeigt die Liste der Ports an, für die Sie DSCP-Einstellungen für den eingehenden und ausgehenden Datenverkehr konfigurieren können.
Eingangs	**Übersetzen:** Um die Ingress-Übersetzung zu aktivieren, klicken Sie auf das Kontrollkästchen. **Klassifizieren:** Die Klassifizierung für einen Port kann 4 verschiedene Werte annehmen. 1. **Deaktivieren:** Keine DSCP-Klassifizierung für eingehenden Datenverkehr. 2. **DSCP=0:** Klassifizieren, wenn der eingehende (oder, falls aktiviert, übersetzte) DSCP-Wert 0 ist. 3. **Ausgewählt:** Nur ausgewählte DSCP klassifizieren, für die die Klassifizierung aktiviert ist, wie im Fenster „DSCP-Übersetzung“ für den jeweiligen DSCP angegeben. 4. **Alle:** Alle DSCP klassifizieren.
Ausgang	**Deaktivieren:** Keine Umschreibung beim Ausgang. **Aktivieren:** Umschreibung am Ausgang ohne Neuzuordnung aktiviert. **DP neu zuordnen (ohne DP-Erkennung):** Der DSCP-Wert vom Analysator wird neu zugeordnet, und der Frame wird mit dem neu zugeordneten DSCP-Wert versehen. Der neu zugeordnete DSCP-Wert wird immer aus der Tabelle „DSCP-Übersetzung -> Ausgangs-Neuzuordnung DP0“ entnommen. **DP-bewusst neu zuordnen:** Der DSCP-Wert vom Analysator wird neu zugeordnet und der Frame mit dem neu zugeordneten DSCP-Wert versehen. Je nach DP-Ebene des Frames wird der neu zugeordnete DSCP-Wert entweder aus der Tabelle „DSCP-Übersetzung -> Egress Remap DP0“ oder aus der Tabelle „DSCP-Übersetzung -> Egress Remap DP1“ entnommen.

Konfiguration > QoS > DSCP-basiertes QoS

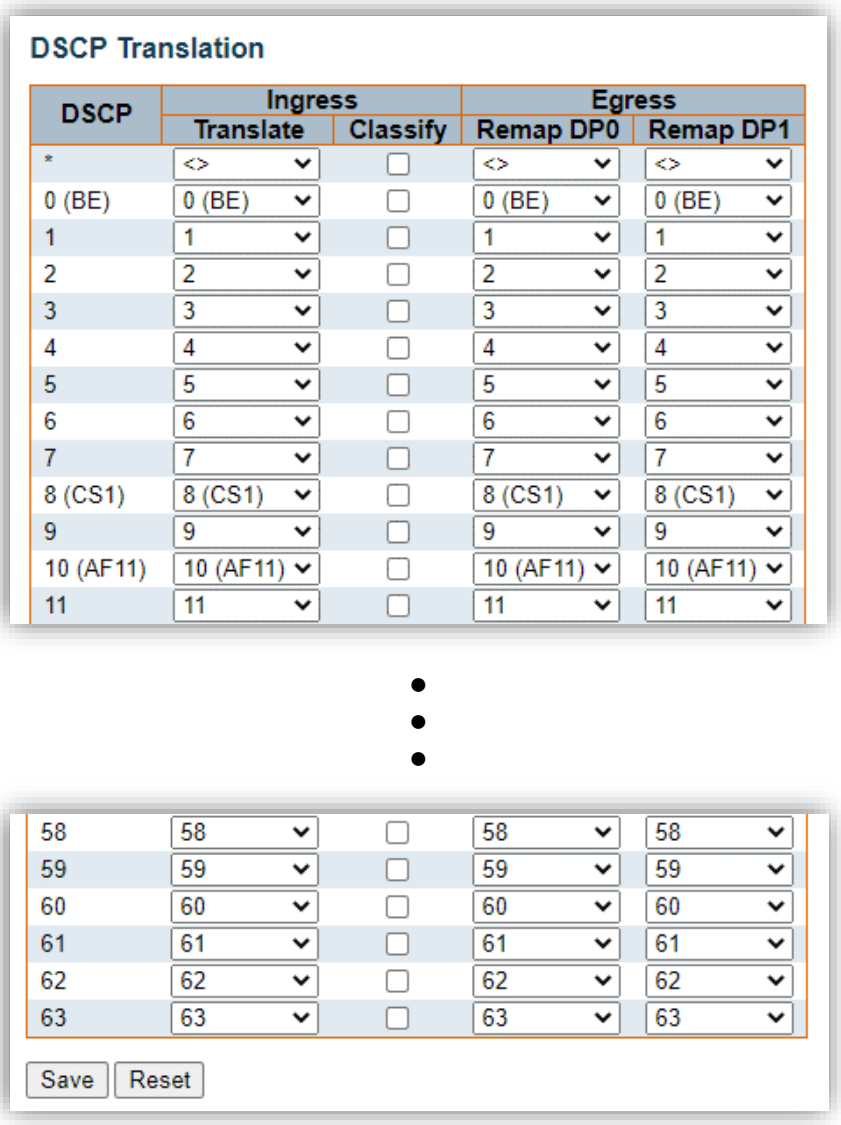
DSCP-basierte QoS-Eingangs-Klassifizierung



Einstellung	Beschreibung
DSCP	Die maximale Anzahl der unterstützten DSCP-Werte beträgt 64.
Vertrauen	Legt fest, ob ein bestimmter DSCP-Wert als vertrauenswürdig eingestuft wird. Nur Frames mit vertrauenswürdigen DSCP-Werten werden einer bestimmten QoS-Klasse und einer bestimmten Drop-Prioritätsstufe zugeordnet. Frames mit nicht vertrauenswürdigen DSCP-Werten werden als Nicht-IP-Frames behandelt.
QoS-Klasse	Der Wert für die QoS-Klasse kann eine beliebige Zahl zwischen 0 und 7 sein.
DPL	Drop-Prioritätsstufe (0–3)

Konfiguration > QoS > DSCP-Übersetzung

DSCP-Übersetzung

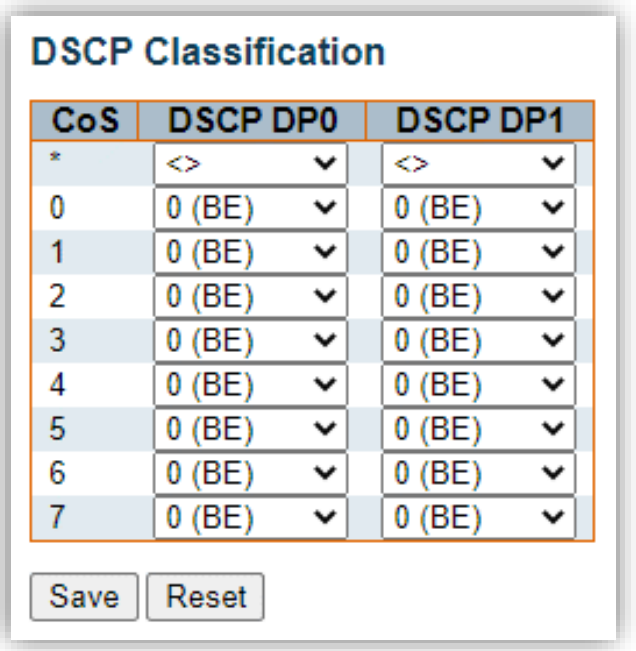


Einstellung	Beschreibung
DSCP	Die maximale Anzahl der unterstützten DSCP-Werte beträgt 64, und gültige DSCP-Werte liegen im Bereich von 0 bis 63.
Eingangsseite	Der DSCP-Wert auf der Eingangsseite kann zunächst in einen neuen DSCP-Wert umgewandelt werden, bevor dieser für die QoS-Klasse und die DPL-Zuordnung verwendet wird. • **Konvertieren:** Der DSCP-Wert auf der Eingangsseite kann in einen beliebigen DSCP-Wert im Bereich von 0 bis 63 konvertiert werden. • **Klassifizieren:** Klicken Sie hier, um die Klassifizierung auf der Eingangsseite zu aktivieren.
Ausgang	• **DP0 neu zuordnen:** Wählen Sie aus dem Auswahlmenü den DSCP-Wert aus, auf den Sie neu zuordnen möchten. Der DSCP-Wert liegt im Bereich von 0 bis 63.

	• **DP1 neu zuordnen:** Wählen Sie aus dem Auswahlmenü den DSCP-Wert aus, auf den Sie neu zuordnen möchten. Der DSCP-Wert liegt im Bereich von 0 bis 63.

Konfiguration > QoS > DSCP-Klassifizierung

DSCP-Klassifizierung

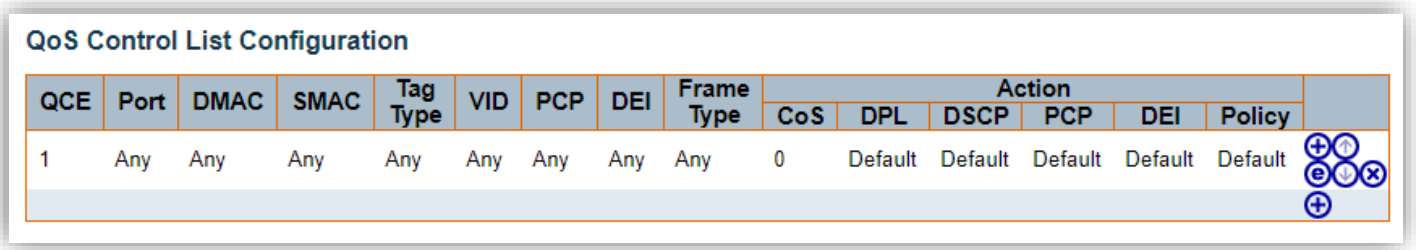


Einstellung	Beschreibung
QoS-Klasse	Tatsächliche QoS-Klasse.
DSCP DP0	Wählen Sie den klassifizierten DSCP-Wert (0–63) für die Drop-Prioritätsstufe 0 aus.
DSCP DP1	Wählen Sie den klassifizierten DSCP-Wert (0–63) für die Drop-Prioritätsstufe 1 aus.

Konfiguration > QoS > QoS-Steuerliste

Konfiguration der QoS-Steuerliste

Auf dieser Seite wird die QoS-Steuerliste (QCL) angezeigt, die aus den QCEs besteht. Jede Zeile beschreibt ein definiertes QCE. Die maximale Anzahl an QCEs beträgt **256** pro Switch.
Klicken Sie auf das unterste Pluszeichen, um der Liste einen neuen QCE hinzuzufügen.



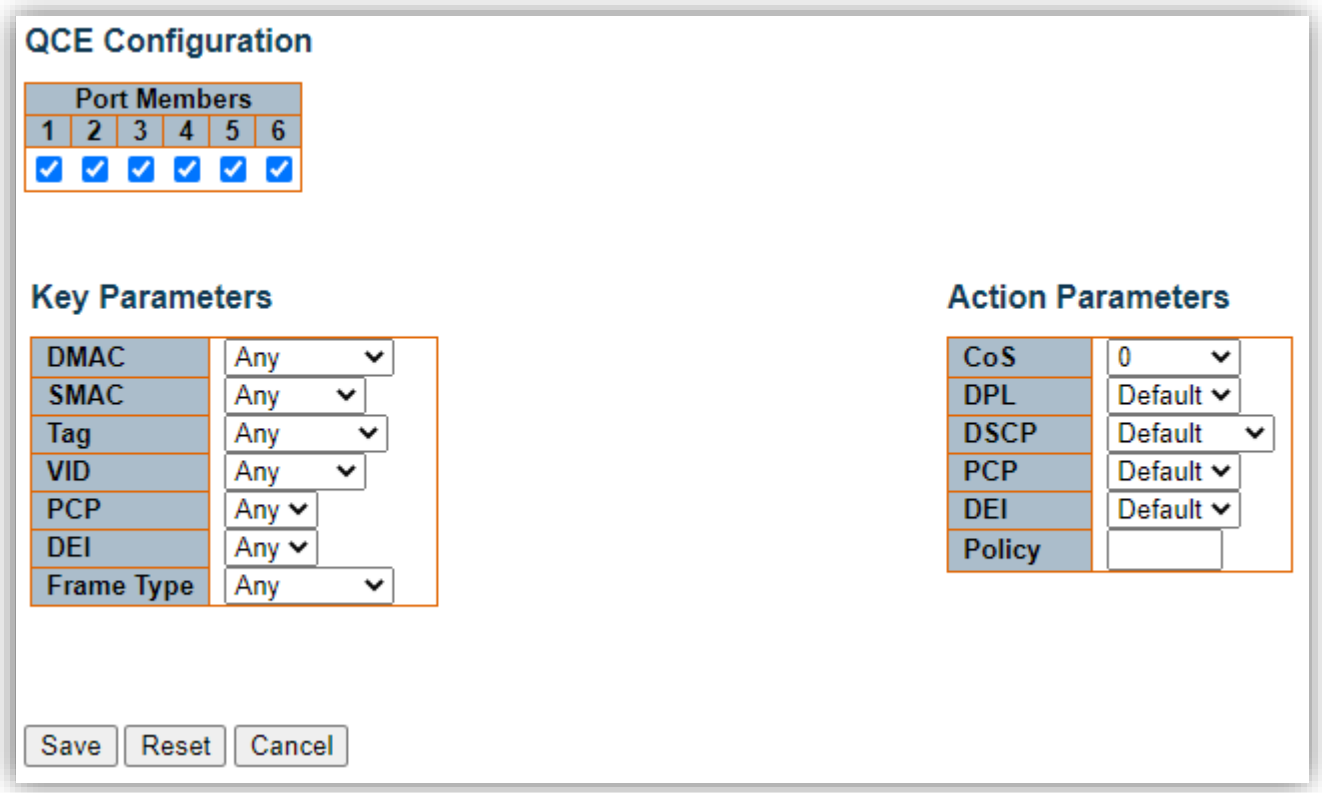
Sie können jeden QCE (QoS-Steuerungseintrag) in der Tabelle mithilfe der folgenden Schaltflächen bearbeiten: „ “: Fügt einen neuen QCE vor der aktuellen Zeile ein.
: Bearbeitet den QCE.
: Verschiebt den QCE in der Liste nach oben.
: Verschiebt den QCE in der Liste nach unten.
: Löscht den QCE.
: Das unterste Pluszeichen fügt einen neuen Eintrag am Ende der QCE-Liste hinzu.

Einstellung	Beschreibung
QCE	Gibt die QCE-ID an.
Port	Gibt die Liste der mit dem QCE konfigurierten Ports oder „Any“ an.
DMAC	Gibt die Ziel-MAC-Adresse an. Mögliche Werte sind: • **Any:** Übereinstimmung mit einer beliebigen DMAC. • **Unicast:** Entspricht einer Unicast-DMAC. • **Multicast:** Übereinstimmung mit einer Multicast-DMAC. • **Broadcast:** Übereinstimmung mit einer Broadcast-DMAC. Der Standardwert ist „Any“.
SMAC	Übereinstimmung mit einer bestimmten Quell-MAC-Adresse oder „Any“. Wenn ein Port so konfiguriert ist, dass er auf Zieladressen abgleichen soll, gibt dieses Feld den DMAC an
Tag-Typ	Gibt den Tag-Typ an. Mögliche Werte sind: • **Any:** Übereinstimmung mit getaggten und ungetaggten Frames. • **„Untagged“:** Übereinstimmung mit nicht getaggten Frames. • **Tagged:** Tagged-Frames abgleichen. Der Standardwert ist „Any“.
VID	Gibt die VLAN-ID (VID) an, entweder eine bestimmte VID oder einen VID-Bereich. Die VID kann im Bereich von 1 bis 4095 oder „Any“ liegen
PCP	Priority Code Point: Gültige Werte für PCP sind bestimmte Werte (0, 1, 2, 3, 4, 5, 6, 7) oder Bereiche (0–1, 2–3, 4–5, 6–7, 0–3, 4–7) oder „Any“.
DEI	Drop Eligible Indicator: Gültige Werte für DEI sind 0, 1 oder „Any“.
Frame-Typ	Gibt den Rahmentyp an. Mögliche Werte sind: 1. **Any:** Übereinstimmung mit jedem Frame-Typ.

	2. **Ethernet:** Übereinstimmung mit EtherType-Frames. 3. **LLC:** Übereinstimmung mit (LLC)-Frames. 4. **SNAP:** Passt auf (SNAP)-Frames. 5. **IPv4:** Passt auf IPv4-Frames. 6. **IPv6:** Sucht nach IPv6-Frames.
Aktion	Gibt die Klassifizierungsaktion an, die für den eingehenden Frame durchgeführt wird, wenn die konfigurierten Parameter mit dem Inhalt des Frames übereinstimmen. Mögliche Aktionen sind: 1. **CoS:** Dienstklasse klassifizieren. 2. **DPL:** Drop-Prioritätsstufe klassifizieren. 3. **DSCP:** DSCP-Wert klassifizieren. 4. **PCP:** Klassifizierung des PCP-Werts. 5. **DEI:** DEI-Wert klassifizieren. 6. **Policy:** Klassifizierung der ACL-Richtliniennummer.

QCE-Konfiguration

Auf dieser Seite können Sie jeweils einen einzelnen QoS-Steuereintrag bearbeiten oder einfügen. Ein QCE besteht aus mehreren Parametern. Diese Parameter variieren je nach dem von Ihnen ausgewählten Frame-Typ.



Port-Mitglieder
Aktivieren Sie das Kontrollkästchen, um den Port in den QCL-Eintrag aufzunehmen. Standardmäßig sind alle Ports enthalten.

Wichtige Parameter

Einstellung	Beschreibung
DMAC	Ziel-MAC-Adresse: Mögliche Werte sind **„Unicast“**, **„Multicast“**, **„Broadcast“** oder **„Any“**.
SMAC	Quell-MAC-Adresse: **xx-xx-xx-xx-xx-xx** oder **„Any“**.
Tag	Der Wert des Tag-Feldes kann **„Untagged“, „Tagged“, „C-Tagged“, „S-Tagged“** oder **„Any“** sein.
VID	Gültige Werte für die VLAN-ID können beliebige Werte im Bereich **von 1 bis 4095** oder **„Any“** sein; der Benutzer kann entweder einen bestimmten Wert oder einen Bereich von VIDs eingeben.
PCP	Gültige Werte für PCP sind bestimmte Werte (**0, 1, 2, 3, 4, 5, 6, 7**), Bereiche (**0–1, 2–3, 4–5, 6–7, 0–3, 4–7**) oder **„Any“**.
DEI	Gültige Werte für DEI sind **0**, **1** oder **„Any“**.
Rahmentyp	Der Rahmentyp kann einen der folgenden Werte annehmen. 1. **Beliebig** 2. **EtherType** 3. **LLC** 4. **SNAP** 5. **IPv4** 6. **IPv6**

Alle Frame-Typen werden im Folgenden erläutert.

1. **Any:** Alle Frame-Typen zulassen.
2. **EtherType:** Ether-Typ. Gültige Ether-Typen sind 0x600–0xFFFF, ausgenommen 0x800 (IPv4) und 0x86DD (IPv6), oder „Any“.
3. **LLC:**
   - ***DSAP-Adresse:*** Gültige DSAP-Adressen (Destination Service Access Point) können zwischen 0x00 und 0xFF liegen oder „Any“ lauten.
   - ***SSAP-Adresse:*** Gültige SSAP-Werte (Source Service Access Point) können zwischen 0x00 und 0xFF oder „Any“ liegen.
   - ***Steuerung:*** Das gültige Steuerungsfeld kann zwischen 0x00 und 0xFF oder „Beliebig“ liegen.
4. **SNAP:** PID: Eine gültige PID (auch bekannt als Ether-Typ) kann zwischen 0x0000 und 0xFFFF oder „Any“ liegen.
5. **IPv4:**
   - ***Protokoll:*** IP-Protokollnummer: (0–255, „TCP“ oder „UDP“) oder „Beliebig“.
   - ***Quell-IP:*** Spezifische Quell-IP-Adresse im Wert-/Maskenformat oder „Beliebig“. IP und Maske haben das Format x.y.z.w, wobei x, y, z und w Dezimalzahlen zwischen 0 und 255 sind. Wenn die Maske in eine 32-Bit-Binärzeichenfolge umgewandelt und von links nach rechts gelesen wird, müssen alle Bits nach der ersten Null ebenfalls Null sein. Wenn ein Port so konfiguriert ist, dass er auf DMAC/DIP abgeglichen wird, ist dieses Feld die Ziel-IP-Adresse.

- ***IP-Fragment:*** Option zur Fragmentierung von IPv4-Frames: „Ja“, „Nein“ oder „Beliebig“.
- ***DSCP:*** Diffserv-Code-Point-Wert (DSCP): Dies kann ein bestimmter Wert, ein Wertebereich oder „Beliebig“ sein. DSCP-Werte liegen im Bereich von 0 bis 63, einschließlich BE, CS1–CS7, EF oder AF11–AF43.
- ***Sport:*** Quell-TCP/UDP-Port: (0–65535) oder „Beliebig“, spezifisch oder Portbereich, anwendbar für das IP-Protokoll UDP/TCP.
- ***Dport:*** Ziel-TCP/UDP-Port: (0–65535) oder „Any“, spezifisch oder Portbereich, anwendbar für das IP-Protokoll UDP/TCP.

6. **IPv6**
   - ***Protokoll:*** IP-Protokollnummer: (0–255, „TCP“ oder „UDP“) oder „Beliebig“.
   - ***Quell-IP:*** 32 LS-Bits der IPv6-Quelladresse im Wert-/Maskenformat oder „Beliebig“. Wenn ein Port so konfiguriert ist, dass er auf DMAC/DIP abgeglichen wird, ist dieses Feld die Ziel-IP-Adresse.
   - ***DSCP:*** Diffserv-Code-Point-Wert (DSCP): Dies kann ein bestimmter Wert, ein Wertebereich oder „Any“ sein. DSCP-Werte liegen im Bereich von 0 bis 63, einschließlich BE, CS1–CS7, EF oder AF11–AF43.
   - ***Port:*** Quell-TCP/UDP-Port: (0–65535) oder „Any“, spezifisch oder Portbereich, anwendbar für das IP-Protokoll UDP/TCP.
   - ***Dport:*** Ziel-TCP/UDP-Port: (0–65535) oder „Any“, ein bestimmter Port oder ein Portbereich, der für das IP-Protokoll UDP/TCP gilt.

Aktionsparameter

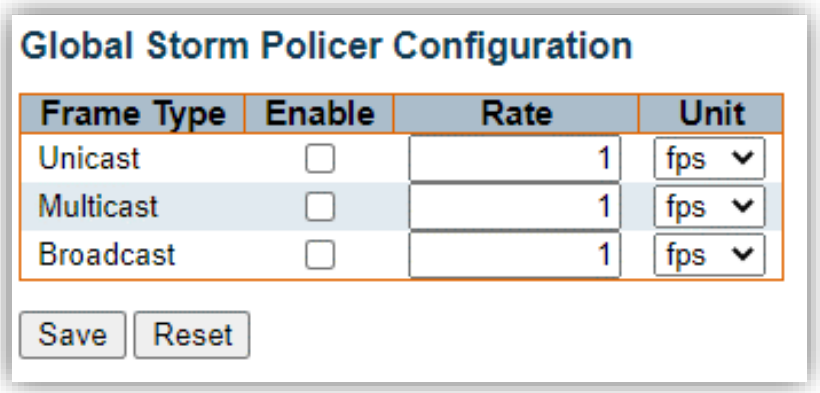
Einstellung	Beschreibung
CoS	Serviceklasse: (**0–7**) oder **„Default**“.
DPL	Drop-Prioritätsstufe: (**0–1**) oder **Standard**.
DSCP	DS1CP: (**0–63, BE, CS1–CS7, EF** oder **AF11–AF43**) oder **Standard**.
PCP	PCP: (**0–7**) oder **Standard**. Hinweis: PCP und DEI können nicht einzeln eingestellt werden.
DEI	DEI: (**0–1**) oder **Standard**.
Richtlinie	ACL-Richtliniennummer: (**0–255**) oder **Standard** (leeres Feld).

Hinweis: „Standard“ bedeutet, dass der standardmäßige Klassifizierungswert durch dieses QCE nicht geändert wird.

Konfiguration > QoS > Storm Policing

Globale Storm-Policer-Konfiguration

Es gibt einen Unicast-Storm-Policer, einen Multicast-Storm-Policer und einen Broadcast-Storm-Policer.
Diese wirken sich nur auf geflutete Frames aus, d. h. auf Frames mit einem (VLAN-ID, DMAC)-Paar, das nicht in der MAC-Adressentabelle vorhanden ist.



Einstellung	Beschreibung
Frame-Typ	Der Frame-Typ, für den die folgende Konfiguration gilt.
Aktivieren	Aktivieren oder deaktivieren Sie den globalen Storm-Policer für den angegebenen Rahmentyp.
Rate	Steuert die Bildrate für den globalen Storm Policer. Dieser Wert ist auf 1–1.024.000 beschränkt, wenn „Unit“ auf „fps“ gesetzt ist, und auf 1–1.024, wenn „Unit“ auf „kfps“ gesetzt ist. Die Bildrate wird intern auf den nächsten vom globalen Storm Policer unterstützten Wert aufgerundet. Unterstützte Raten sind 1, 2, 4, 8, 16, 32, 64, 128, 256 und 512 fps für Raten ≤ 512 fps sowie 1, 2, 4, 8, 16, 32, 64, 128, 256, 512 und 1024 kfps für Raten > 512 fps.
Einheit	Legt die Maßeinheit für die globale Storm-Policer-Rate fest: fps, kfps, kbps oder Mbps.

Konfiguration > Spiegelung

Konfiguration von Mirroring und Remote-Mirroring

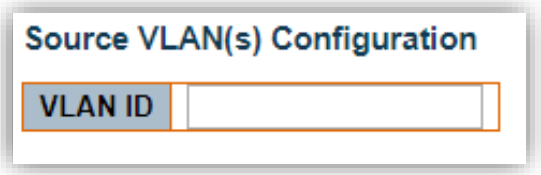
Mirroring ist eine Funktion für den Switched-Port-Analysator. Der Administrator kann das Mirroring zur Fehlerbehebung bei Netzwerkproblemen nutzen. Der ausgewählte Datenverkehr kann auf einen Zielport gespiegelt oder kopiert werden, an den ein Netzwerkanalysator angeschlossen werden kann, um den Netzwerkverkehr zu analysieren.
Remote-Spiegelung ist eine erweiterte Funktion der Spiegelung. Sie ermöglicht die Erweiterung des Zielports auf einen anderen Switch. So kann der Administrator den Netzwerkverkehr auf den anderen Switches analysieren.
Wenn Sie den getaggten gespiegelten Datenverkehr erhalten möchten, müssen Sie die VLAN-Ausgangs-Tagging-Einstellung am Reflektor-Port auf **„Tag All“** setzen. Wenn Sie hingegen den ungetaggten gespiegelten Datenverkehr erhalten möchten, müssen Sie die VLAN-Ausgangs-Tagging-Einstellung am Reflektor-Port auf **„Untag ALL“** setzen.

Einstellung	Beschreibung
Sitzung	Wählen Sie die zu konfigurierende Sitzungs-ID aus.
Modus	Zum Aktivieren/Deaktivieren der Spiegelungs- oder Remote-Spiegelungsfunktion.
Typ	Wählen Sie den Switch-Typ aus. • **Mirror:** Der Switch läuft im Mirror-Modus. Die Quellports und der Zielport befinden sich auf diesem Switch. • **Rmirror-Quelle:** Der Switch ist ein Quellknoten für den Überwachungsdatenfluss. Der/die Quellport(s) und der Reflektorport befinden sich auf diesem Switch. • **Rmirror-Ziel:** Der Switch ist ein Endknoten für den Überwachungsdatenfluss. Der/die Zielport(s) befindet/befinden sich auf diesem Switch.
VLAN-ID	Die VLAN-ID gibt an, wohin das Überwachungspaket kopiert wird. Die Standard-VLAN-ID ist 200.
Reflektor-Port	Der Reflektor-Port dient dazu, den Datenverkehr in das Remote-Mirroring-VLAN umzuleiten. Jedes Gerät, das an einen als Reflektor-Port festgelegten Port angeschlossen ist, verliert die Verbindung, bis das Remote-Mirroring deaktiviert wird. Im Stacking-Modus müssen Sie die Switch-ID auswählen, um das richtige Gerät zu ermitteln. Wenn Sie einen Port deaktivieren, kann dieser nicht mehr als Reflektorport fungieren. Wenn Sie einen Port deaktivieren, der als Reflektor-Port fungiert, funktioniert die Remote-Mirroring-Funktion nicht mehr. **Hinweis 1:** Der Reflektor-Port muss nur auf dem Quell-Switch ausgewählt werden. **Hinweis 2:** Für den Reflektor-Port müssen das MAC-Tabellen-Lernen und STP deaktiviert werden.

	Hinweis 3: Der Reflektorport wird nur an reinen Kupferports unterstützt.

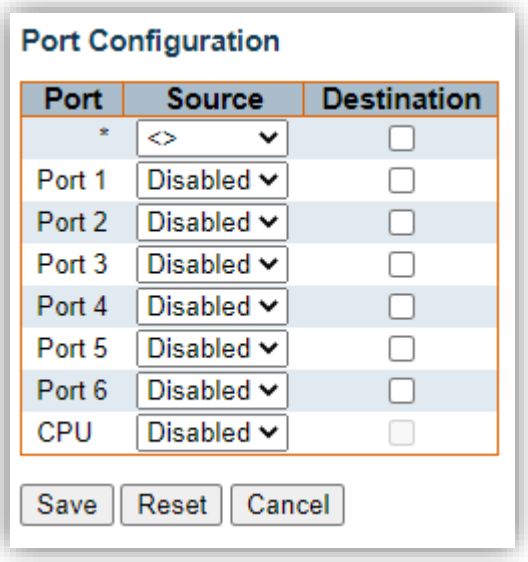
Konfiguration der Quell-VLANs

Der Switch unterstützt VLAN-basiertes Mirroring. Wenn Sie bestimmte VLANs auf dem Switch überwachen möchten, können Sie die ausgewählten VLANs in diesem Feld festlegen.



HINWEIS	Die Spiegelungssitzung darf entweder Ports oder VLANs als Quellen haben, jedoch nicht beides.

Port-Konfiguration



Einstellung	Beschreibung
Port	Der logische Port für die Einstellungen in derselben Zeile.
Quelle	Wählen Sie den Spiegelungsmodus aus. • **Deaktiviert:** Weder gesendete noch empfangene Frames werden gespiegelt. • **Beides:** Sowohl empfangene als auch gesendete Frames werden auf den Zielport gespiegelt. • **Nur Empfang:** An diesem Port empfangene Frames werden am Zielport gespiegelt. Gesendete Frames werden nicht gespiegelt. • **Nur Tx:** An diesem Port gesendete Frames werden am Zielport gespiegelt. Empfangene Frames werden nicht gespiegelt.
Ziel	Zielport auswählen. Dieses Kontrollkästchen ist für die Spiegelung oder Remote-Spiegelung vorgesehen. Der Zielport ist ein Switch-Port, an dem Sie eine Kopie des Datenverkehrs vom Quellport empfangen. **Hinweis 1:** Im Spiegelungsmodus unterstützt das Gerät nur einen Zielport. **Hinweis 2:** Für den Zielport muss das Erlernen der MAC-Tabelle deaktiviert sein.

Konfigurationsrichtlinie für alle Funktionen

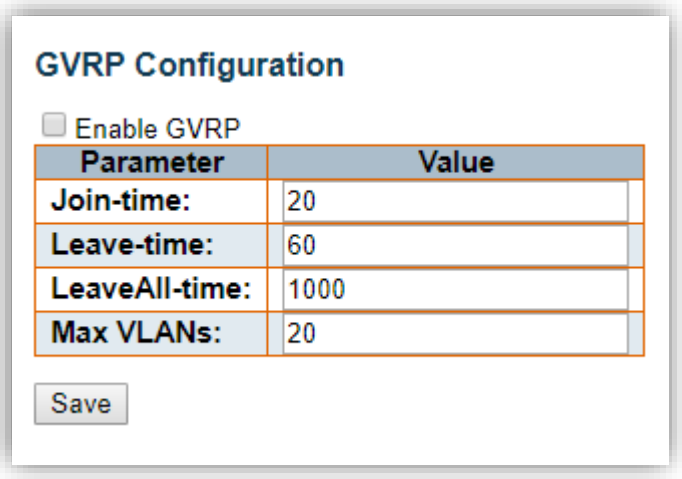
Wenn der Switch im Remote-Mirroring-Modus läuft, muss der Administrator außerdem überprüfen, ob andere Funktionen aktiviert oder deaktiviert sind.
Wenn der Administrator beispielsweise MSTP am Reflektorport nicht deaktiviert hat, wird der gesamte Monitor-Datenverkehr am Reflektorport blockiert.
Alle empfohlenen Einstellungen werden im Folgenden beschrieben.

	Auswirkung	Quellport	Reflektor-Port	Zwischenport	Ziel-Port	Remote-Mirroring-VLAN
arp_inspection	Hoch		* deaktiviert	* deaktiviert		
acl	Kritisch		* deaktiviert	* deaktiviert	* deaktiviert	
dhcp_relay	Hoch		* deaktiviert	* deaktiviert		
dhcp_snooping	Hoch		* deaktiviert	* deaktiviert		
ip_source_guard	Kritisch		* deaktiviert	* deaktiviert	* deaktiviert	
ipmc/igmpsnp	Kritisch					kein Konflikt
ipmc/mldsnp	Kritisch					Konfliktfrei
lacp	Niedrig				o deaktiviert	
LLDP	Niedrig				o deaktiviert	
MAC-Lernmodus	Kritisch		* deaktiviert	* deaktiviert	* deaktiviert	
mstp	Kritisch		* deaktiviert		o deaktiviert	
mvr	Kritisch					Konfliktfrei
nas	Kritisch		* autorisiert	* autorisiert	* autorisiert	
psec	Kritisch		* deaktiviert	* deaktiviert	* deaktiviert	
qos	Kritisch		* unbegrenzt	* unbegrenzt	* unbegrenzt	
UPnP	Niedrig				o deaktiviert	
MAC-basiertes VLAN	Kritisch		* deaktiviert	* deaktiviert		
protokollbasiertes VLAN	Kritisch		* deaktiviert	* deaktiviert		
VLAN-Übersetzung	Kritisch		* deaktiviert	* deaktiviert	* deaktiviert	
voice_vlan	Kritisch		* deaktiviert	* deaktiviert		
mrp	Niedrig				o deaktiviert	
mvrp	Niedrig				o deaktiviert	

Hinweis:
* -- muss
o -- optional
Auswirkung: Kritisch/Hoch/Gering
Kritisch 5 Pakete -> 0 Pakete
Hoch 5 Pakete -> 4 Pakete
Niedrig 5 Pakete -> 6 Pakete

Konfiguration > GVRP > Globale Konfiguration

GVRP-Konfiguration



GVRP aktivieren
Die GVRP-Funktion wird global aktiviert, indem Sie das Kontrollkästchen „GVRP aktivieren“ markieren und auf die Schaltfläche „Speichern“ klicken.

Beitrittszeitpunkt

Einstellung	Beschreibung	Werkseinstellung
1 bis 20	Die Join-Zeit ist ein Wert im Bereich von 1–20 cs, d. h. in Einheiten von Hundertstelsekunden.	20

Verlasszeit

Einstellung	Beschreibung	Werkseinstellung
60 ~ 300	Die Verweilzeit ist ein Wert im Bereich von 60 bis 300 cs, d. h. in Einheiten von einem Hundertstel einer Sekunde.	60

LeaveAll-Zeit

Einstellung	Beschreibung	Werkseinstellung
1000 ~ 5000	„LeaveAll-time“ ist ein Wert im Bereich von 1000 bis 5000 cs, d. h. in Einheiten von einem Hundertstel einer Sekunde. Der Standardwert beträgt 1000 cs.	1000

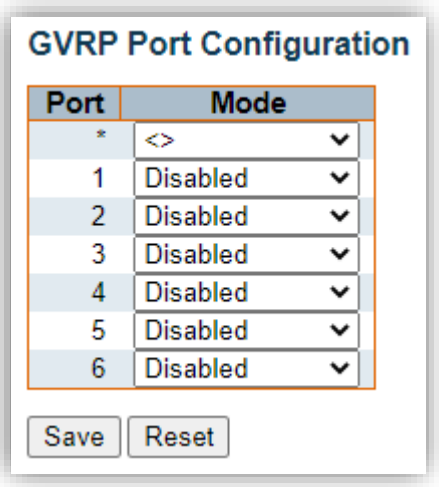
Max. VLANs

Einstellung	Beschreibung	Werkseinstellung
1 bis 4094	Wenn GVRP aktiviert ist, wird die maximale Anzahl der von GVRP unterstützten VLANs festgelegt. Diese Zahl kann nur geändert werden, wenn GVRP deaktiviert ist.	20

Konfiguration > GVRP > Port-Konfiguration

GVRP-Portkonfiguration

Diese Konfiguration kann entweder vor oder nach der globalen GVRP-Konfiguration vorgenommen werden – die Funktionsweise des Protokolls bleibt dabei unverändert.

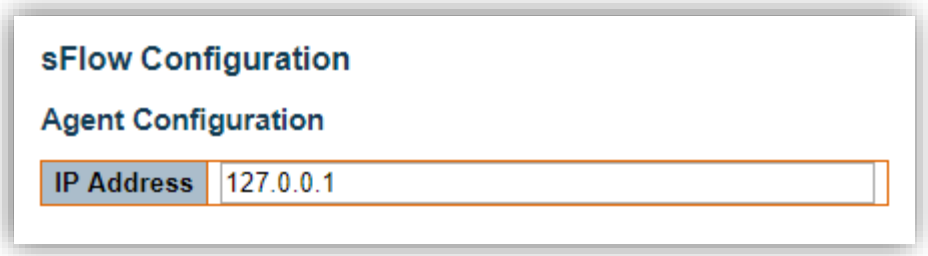


Einstellung	Beschreibung
Port	Der logische Port, der konfiguriert werden soll.
Modus	Der Modus kann entweder **„Deaktiviert“** oder **„GVRP aktiviert“** sein. Diese Werte deaktivieren bzw. aktivieren die GVRP-Funktion für den betreffenden Port.

Konfiguration > sFlow

Auf dieser Seite kann sFlow konfiguriert werden. Die Konfiguration ist in zwei Teile gegliedert: die Konfiguration des sFlow-Empfängers (auch sFlow-Collector genannt) und die Konfiguration der portbezogenen Flow- und Zähler-Sampler.
Die sFlow-Konfiguration wird nicht in einem nichtflüchtigen Speicher gespeichert, was bedeutet, dass ein Neustart die sFlow-Erfassung deaktiviert.

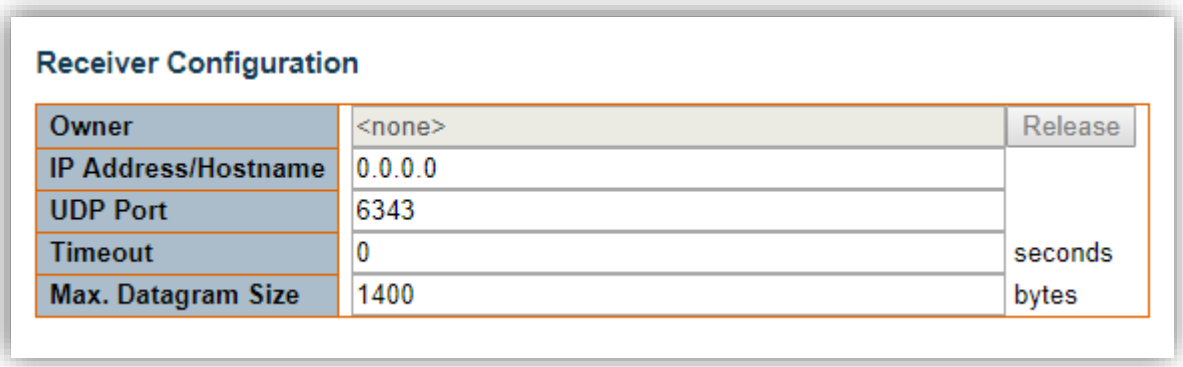
Agentenkonfiguration



IP-Adresse

Einstellung	Beschreibung	Werkseinstellung
IP-Adresse	Die IP-Adresse, die in sFlow-Datagrammen als Agent-IP-Adresse verwendet wird. Sie dient als eindeutiger Schlüssel, der diesen Agenten über einen längeren Zeitraum hinweg identifiziert. Es werden sowohl IPv4- als auch IPv6-Adressen unterstützt.	127.0.0.1

Empfängerkonfiguration



Eigentümer
Grundsätzlich kann sFlow auf zwei Arten konfiguriert werden: über die lokale Verwaltung mithilfe der Web- oder CLI-Schnittstelle oder über SNMP. Dieses schreibgeschützte Feld zeigt den Eigentümer der aktuellen sFlow-Konfiguration an und nimmt folgende Werte an:

- Wenn sFlow derzeit nicht konfiguriert ist oder noch keinem Benutzer zugewiesen wurde, enthält das Feld „Eigentümer“ **den Wert „none**“.
- Wenn sFlow derzeit über das Web oder die CLI konfiguriert ist, enthält „Eigentümer“ den Eintrag **„Über lokale Verwaltung konfiguriert**“.
- Wenn sFlow derzeit über SNMP konfiguriert ist, enthält „Eigentümer“ eine Zeichenfolge, die den sFlow-Empfänger identifiziert.

Wenn sFlow über SNMP konfiguriert ist, sind alle Steuerelemente – mit Ausnahme der Schaltfläche „Freigeben“ – deaktiviert, um eine versehentliche Neukonfiguration zu vermeiden.

Über die Schaltfläche **„Freigeben“** können Sie den aktuellen Eigentümer freigeben und die sFlow-Erfassung deaktivieren. Die Schaltfläche ist deaktiviert, wenn sFlow derzeit nicht zugewiesen ist. Bei einer Konfiguration über SNMP muss die Freigabe bestätigt werden (es erscheint eine Bestätigungsaufforderung).

IP-Adresse/Hostname

Einstellung	Beschreibung	Werkseinstellung
IP-Adresse	Die IP-Adresse oder der Hostname des sFlow-Empfängers. Es werden sowohl IPv4- als auch IPv6-Adressen unterstützt.	0.0.0.0

UDP-Port

Einstellung	Beschreibung	Werkseinstellung
Portnummer	Der UDP-Port, auf dem der sFlow-Empfänger auf sFlow-Datagramme wartet. Bei der Einstellung 0 wird der Standardport (6343) verwendet.	6343

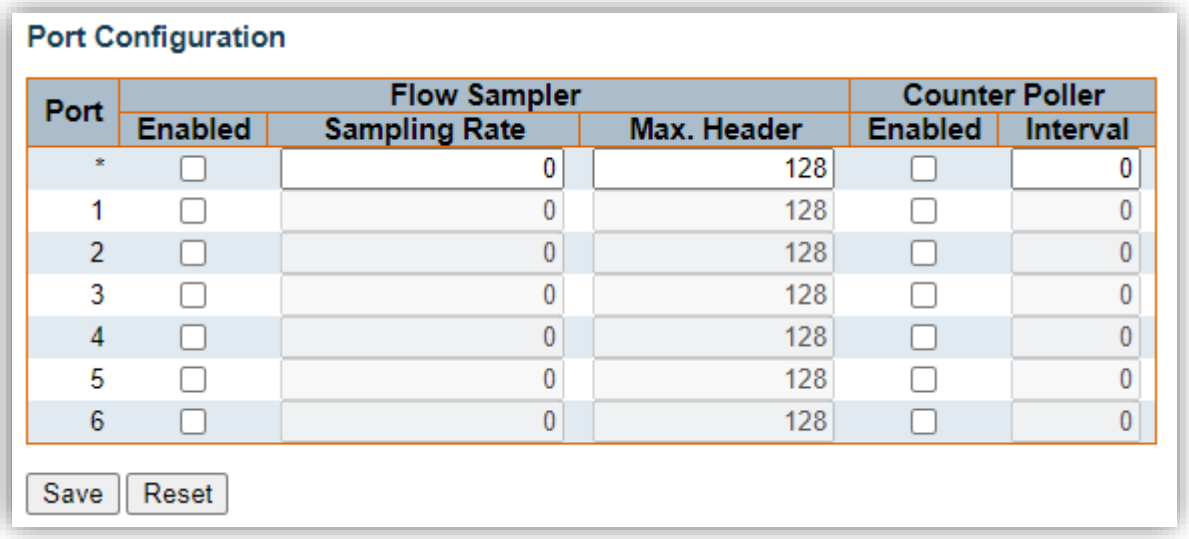
Zeitlimit

Einstellung	Beschreibung	Werkseinstellung
0 ~ 2147483647	Die verbleibende Zeit in Sekunden, bis die Erfassung beendet und der aktuelle sFlow-Eigentümer freigegeben wird. Solange diese Funktion aktiv ist, kann die verbleibende Zeit durch Klicken auf die Schaltfläche „Aktualisieren“ aktualisiert werden. Bei lokaler Verwaltung kann das Timeout im laufenden Betrieb geändert werden, ohne dass andere Einstellungen davon betroffen sind. Der gültige Bereich liegt zwischen 0 und 2147483647 Sekunden.	0

Max. Datagrammgröße

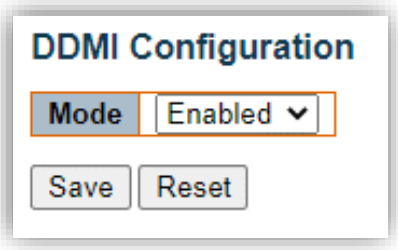
Einstellung	Beschreibung	Werkseinstellung
200 ~ 1468	Die maximale Anzahl an Datenbytes, die in einem einzelnen Sample-Datagramm gesendet werden können. Dieser Wert sollte so gewählt werden, dass eine Fragmentierung der sFlow-Datagramme vermieden wird. Der gültige Bereich liegt zwischen 200 und 1468 Bytes.	1400

Port-Konfiguration



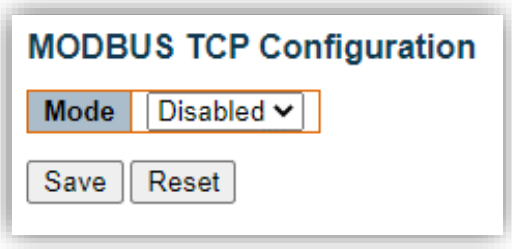
Einstellung	Beschreibung
Port	Die Portnummer, für die die folgende Konfiguration gilt.
Flow-Sampler aktiviert	Aktiviert bzw. deaktiviert die Datenflusserfassung an diesem Port.
Abtastrate des Flow-Samplers	Die statistische Abtastrate für die Paketabtastung. Stellen Sie den Wert auf „N“ ein, um durchschnittlich jedes N-te der an diesem Port gesendeten/empfangenen Pakete zu erfassen. Nicht alle Erfassungsraten sind realisierbar. Wird eine nicht unterstützte Abtastrate angefordert, passt der Switch diese automatisch an die nächstgelegene erreichbare an. Dies wird in diesem Feld gemeldet. Der gültige Bereich liegt zwischen 1 und 4294967295.
Max. Header des Flow-Samplers	Die maximale Anzahl an Bytes, die aus einem erfassten Paket in das sFlow-Datagramm kopiert werden sollen. Der gültige Bereich liegt zwischen 14 und 200 Bytes, wobei der Standardwert 128 Bytes beträgt. Um Platz für jeden Frame zu haben, sollte die maximale Datagrammgröße etwa 100 Bytes größer sein als die maximale Header-Größe. Wenn die maximale Datagrammgröße die maximale Header-Größe nicht berücksichtigt, können Samples verloren gehen.
Zählerabfrage aktiviert	Aktiviert/deaktiviert die Zählerabfrage an diesem Port.
Intervall des Zähler-Pollers	Bei aktiviertem Zähler-Polling gibt dieser Wert das Intervall – in Sekunden – zwischen den Abtastungen des Zähler-Pollers an. Der gültige Bereich liegt zwischen 1 und 3600 Sekunden.

Konfiguration > DDMI



Einstellung	Beschreibung	Werkseinstellung
Modus	Gibt den DDMI-Betriebsmodus an. Mögliche Modi sind: **Aktiviert**: Aktiviert den DDMI-Modus. **Deaktiviert**: Deaktiviert den DDMI-Modus.	Aktiviert

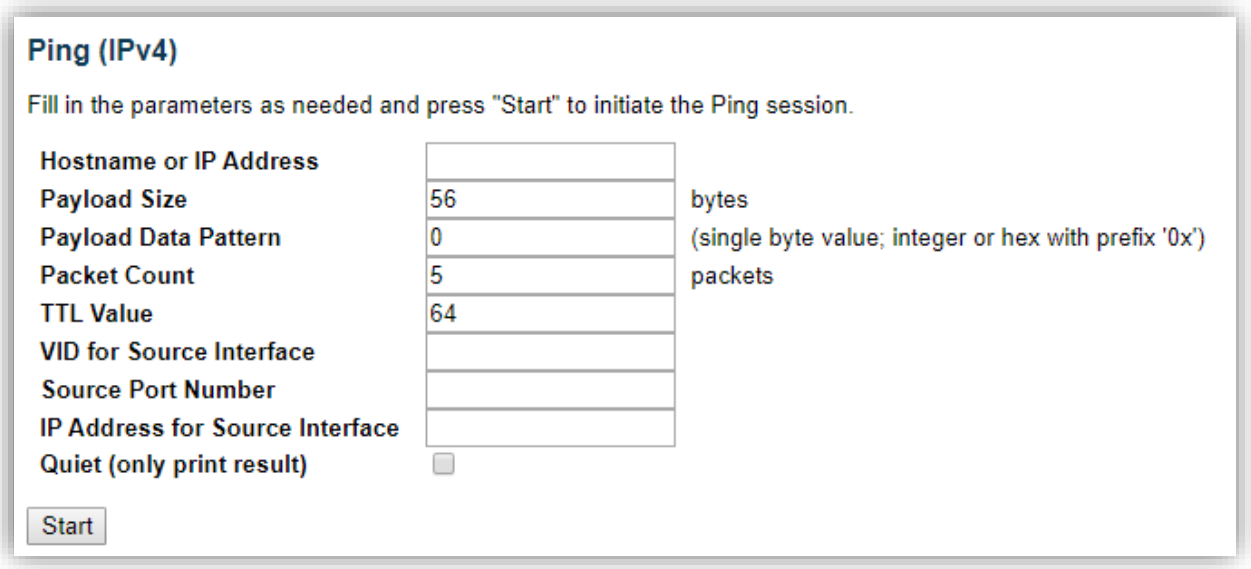
Konfiguration > MODBUS TCP



Einstellung	Beschreibung	Werkseinstellung
Modus	Gibt den Betriebsmodus von MODBUS TCP an. Mögliche Modi sind: **Aktiviert**: Aktiviert den Betrieb im MODBUS-TCP-Modus. **Deaktiviert**: Deaktiviert den Betrieb im MODBUS-TCP-Modus.	Deaktiviert

Diagnose

Diagnose > Ping (IPv4)



Einstellung	Beschreibung
Hostname oder IP-Adresse	Die Adresse des Zielhosts, entweder als symbolischer Hostname oder als IP-Adresse.
Nutzdatengröße	Legt die Größe der ICMP-Nutzdaten in Byte fest (ohne die Größe der Ethernet-, IP- und ICMP-Header). Der Standardwert beträgt 56 Byte. Der gültige Bereich liegt zwischen 2 und 1452 Byte.
Nutzdatenmuster	Legt das Muster fest, das in der ICMP-Datenlast verwendet wird. Der Standardwert ist 0. Der gültige Bereich liegt zwischen 0 und 255.
Paketanzahl	Legt die Anzahl der gesendeten PING-Anfragen fest. Der Standardwert beträgt 5. Der gültige Bereich liegt zwischen 1 und 60.
TTL-Wert	Legt den Wert des Time-To-Live-Feldes (TTL) im IPv4-Header fest. Der Standardwert ist 64. Der gültige Bereich liegt zwischen 1 und 255.
VID für Quellschnittstelle	Mit diesem Feld kann festgelegt werden, dass der Test eine bestimmte lokale VLAN-Schnittstelle als Quellschnittstelle verwendet. Lassen Sie dieses Feld leer, damit die automatische Auswahl auf Basis der Routing-Konfiguration erfolgt. Hinweis: Sie können für die Quellschnittstelle entweder die VID oder die IP-Adresse angeben.
Quellportnummer	Mit diesem Feld können Sie festlegen, dass der Test eine bestimmte lokale Schnittstelle mit der angegebenen Portnummer als Quellschnittstelle verwendet. Der angegebene Port muss mit einer geeigneten IP-Adresse konfiguriert sein. Lassen Sie dieses Feld leer, um die automatische Auswahl basierend auf der Routing-Konfiguration zu ermöglichen. Hinweis: Sie können für die Quellschnittstelle entweder die Quellportnummer oder die IP-Adresse angeben.
Adresse für die Quellschnittstelle	Mit diesem Feld können Sie festlegen, dass der Test eine bestimmte lokale Schnittstelle mit der angegebenen IP-Adresse als Quellschnittstelle verwendet. Die angegebene IP-Adresse muss auf einer lokalen Schnittstelle konfiguriert sein. Lassen Sie dieses Feld leer, damit die automatische Auswahl auf Basis der Routing-Konfiguration erfolgt.

	Hinweis: Sie können für die Quellschnittstelle entweder die VID oder die IP-Adresse angeben.
Quiet (nur Ergebnis ausgeben)	Wenn Sie diese Option aktivieren, wird nicht das Ergebnis jeder einzelnen Ping-Anfrage ausgegeben, sondern nur das Endergebnis angezeigt.

Nachdem Sie auf die Schaltfläche **„Start“** geklickt haben, werden ICMP-Pakete gesendet, und nach dem Empfang einer Antwort werden die Sequenznummer und die Round-Trip-Zeit angezeigt.

Die Datenmenge, die in einem IP-Paket vom Typ ICMP ECHO_REPLY empfangen wird, ist immer um 8 Byte größer als die angeforderte Nutzdatengröße (die Differenz entspricht dem ICMP-Header).

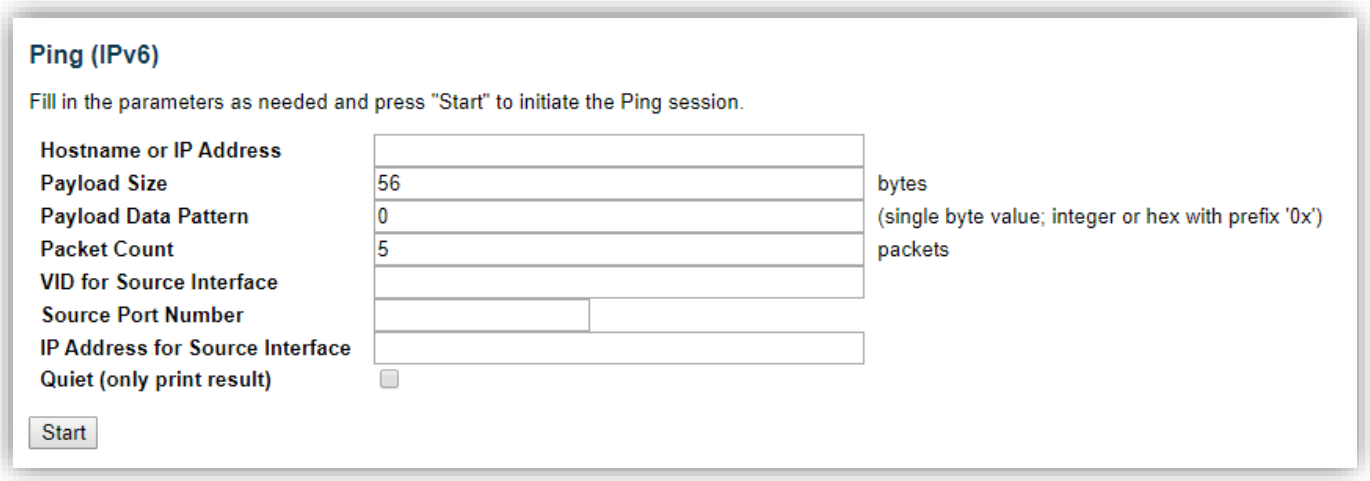
Die Seite wird automatisch aktualisiert, bis Antworten auf alle Pakete empfangen wurden oder bis ein Timeout eintritt.

Die Ausgabe des Befehls sieht wie folgt aus:

PING 172.16.1.1 (172.16.1.1) von 172.16.1.10: 56 Datenbytes
64 Bytes von 172.16.1.1: seq=0 ttl=64 time=2,034 ms
64 Bytes von 172.16.1.1: seq=1 ttl=64 time=1,729 ms
64 Bytes von 172.16.1.1: seq=2 ttl=64 Zeit=1,954 ms
64 Bytes von 172.16.1.1: seq=3 ttl=64 Zeit=1,699 ms
64 Bytes von 172.16.1.1: seq=4 ttl=64 Zeit=1,916 ms

--- Ping-Statistik für 172.16.1.1 ---
5 Pakete gesendet, 5 Pakete empfangen, 0 % Paketverlust
Hin- und Rücklauf min/Durchschnitt/max = 1,699/1,866/2,034 ms

Diagnose > Ping (IPv6)



Einstellung	Beschreibung
Hostname oder IP-Adresse	Die Adresse des Zielhosts, entweder als symbolischer Hostname oder als IP-Adresse.
Nutzdatengröße	Legt die Größe der ICMP-Nutzdaten in Byte fest (ohne die Größe der Ethernet-, IP- und ICMP-Header). Der Standardwert beträgt 56 Byte. Der gültige Bereich liegt zwischen 2 und 1452 Byte.
Nutzdatenmuster	Legt das Muster fest, das in der ICMP-Datenlast verwendet wird. Der Standardwert ist 0. Der gültige Bereich liegt zwischen 0 und 255.
Paketanzahl	Legt die Anzahl der gesendeten PING-Anfragen fest. Der Standardwert beträgt 5. Der gültige Bereich liegt zwischen 1 und 60.
VID für Quellschnittstelle	Mit diesem Feld kann festgelegt werden, dass der Test eine bestimmte lokale VLAN-Schnittstelle als Quellschnittstelle verwendet. Lassen Sie dieses Feld leer, um die automatische Auswahl basierend auf der Routing-Konfiguration zu ermöglichen. Hinweis: Sie können für die Quellschnittstelle entweder die VID oder die IP-Adresse angeben.
Quellportnummer	Mit diesem Feld können Sie festlegen, dass der Test eine bestimmte lokale Schnittstelle mit der angegebenen Portnummer als Quellschnittstelle verwendet. Der angegebene Port muss mit einer geeigneten IP-Adresse konfiguriert sein. Lassen Sie dieses Feld leer, um die automatische Auswahl basierend auf der Routing-Konfiguration zu ermöglichen. Hinweis: Sie können für die Quellschnittstelle entweder die Quellportnummer oder die IP-Adresse angeben.
Adresse für die Quellschnittstelle	Mit diesem Feld können Sie festlegen, dass der Test eine bestimmte lokale Schnittstelle mit der angegebenen IP-Adresse als Quellschnittstelle verwendet. Die angegebene IP-Adresse muss auf einer lokalen Schnittstelle konfiguriert sein. Lassen Sie dieses Feld leer, um die automatische Auswahl basierend auf der Routing-Konfiguration zu ermöglichen. Hinweis: Sie können für die Quellschnittstelle entweder die VID oder die IP-Adresse angeben.
Quiet (nur Ergebnis ausgeben)	Wenn Sie diese Option aktivieren, wird nicht das Ergebnis jeder einzelnen Ping-Anfrage ausgegeben, sondern nur das Endergebnis angezeigt.

Nachdem Sie auf die Schaltfläche **„Start“** geklickt haben, werden ICMP-Pakete gesendet, und die Sequenznummer sowie die Round-Trip-Zeit werden nach Empfang einer Antwort angezeigt.

Die Datenmenge, die in einem IP-Paket vom Typ „ICMP ECHO_REPLY“ empfangen wird, ist immer um 8 Byte größer als die angeforderte Nutzdatengröße (die Differenz entspricht dem ICMP-Header).

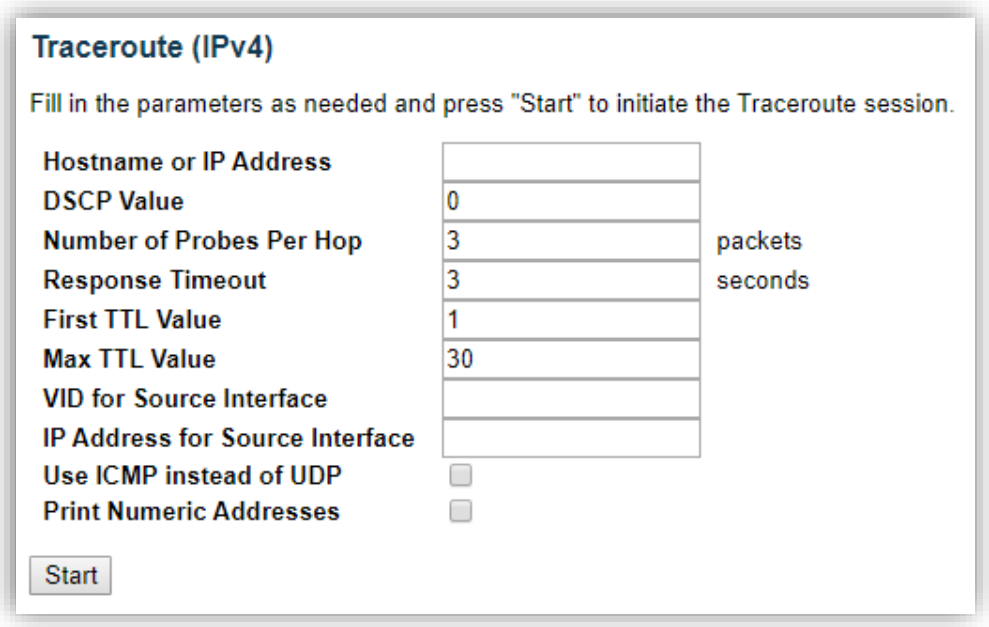
Die Seite wird automatisch aktualisiert, bis Antworten auf alle Pakete empfangen wurden oder bis ein Timeout eintritt.

Die Ausgabe des Befehls sieht wie folgt aus:

PING 2001::01 (2001::1) von 2001::3: 56 Datenbytes
64 Bytes von 2001::1: seq=0 ttl=64 time=2,118 ms
64 Bytes von 2001::1: seq=1 ttl=64 time=2,009 ms
64 Bytes von 2001::1: seq=2 ttl=64 time=1,852 ms
64 Bytes von 2001::1: seq=3 ttl=64 Zeit=2,869 ms
64 Bytes von 2001::1: seq=4 ttl=64 Zeit=1,845 ms

--- 2001::01 Ping-Statistik ---
5 Pakete gesendet, 5 Pakete empfangen, 0 % Paketverlust
Hin- und Rücklauf min/Durchschnitt/max = 1,845/2,138/2,869 ms

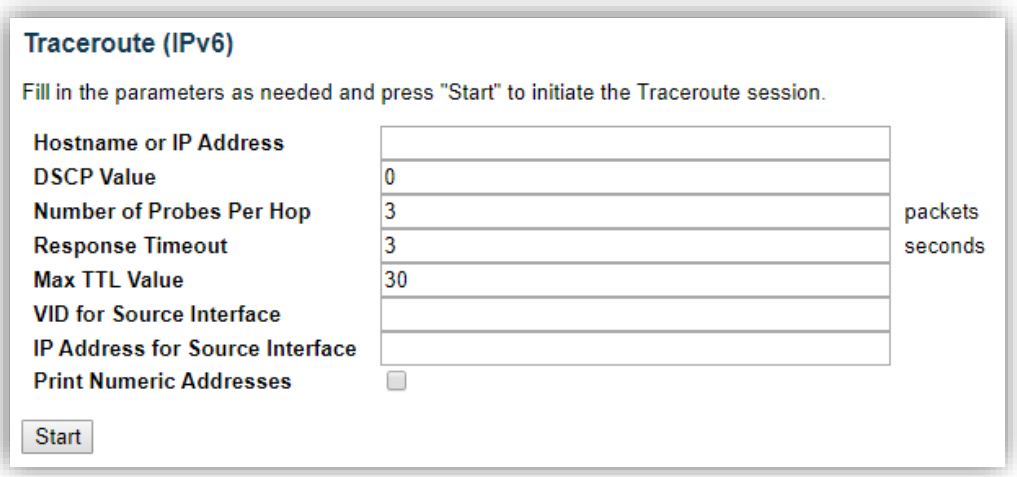
Diagnose > Traceroute (IPv4)



Einstellungen	Beschreibung
Hostname oder IP-Adresse	Die Ziel-IP-Adresse.
DSCP-Wert	Dieser Wert wird für den DSCP-Wert im IPv4-Header verwendet. Der Standardwert ist 0. Der gültige Bereich liegt zwischen 0 und 63.
Anzahl der Probes pro Hop	Legt die Anzahl der Probes (Pakete) fest, die pro Hop gesendet werden. Der Standardwert ist 3. Der gültige Bereich liegt zwischen 1 und 60.
Zeitlimit für die Antwort	Legt fest, wie viele Sekunden auf eine Antwort auf eine gesendete Anfrage gewartet werden soll. Der Standardwert beträgt 3. Der gültige Bereich liegt zwischen 1 und 86400.
Erster TTL-Wert	Legt den Wert des Time-To-Live-Feldes (TTL) im IPv4-Header des ersten gesendeten Pakets fest. Der Standardwert ist 1. Der gültige Bereich liegt zwischen 1 und 30.
Maximaler TTL-Wert	Legt den maximalen Wert des „Time-To-Live“-Feldes (TTL) im IPv4-Header fest. Wird dieser Wert erreicht, bevor der angegebene Remote-Host erreicht wird, wird der Test abgebrochen. Der Standardwert ist 30. Der gültige Bereich liegt zwischen 1 und 255.
VID für Quellschnittstelle	Über dieses Feld kann festgelegt werden, dass der Test eine bestimmte lokale VLAN-Schnittstelle als Quellschnittstelle verwendet. Lassen Sie dieses Feld leer, um die automatische Auswahl basierend auf der Routing-Konfiguration zu ermöglichen. Hinweis: Sie können für die Quellschnittstelle entweder die VID oder die IP-Adresse angeben.
Adresse für die Quellschnittstelle	Mit diesem Feld können Sie festlegen, dass der Test eine bestimmte lokale Schnittstelle mit der angegebenen IP-Adresse als Quellschnittstelle verwendet. Die angegebene IP-Adresse muss auf einer lokalen Schnittstelle konfiguriert sein. Lassen Sie dieses Feld leer, um die automatische Auswahl basierend auf der Routing-Konfiguration zu ermöglichen. Hinweis: Sie können für die Quellschnittstelle entweder die VID oder die IP-Adresse angeben, jedoch nicht beides.

ICMP anstelle von UDP verwenden	Standardmäßig verwendet der Befehl „traceroute“ UDP-Datagramme. Durch Auswahl dieser Option wird stattdessen die Verwendung von ICMP-ECHO-Paketen erzwungen.
Numerische Adressen ausgeben	Standardmäßig gibt der Befehl „traceroute“ Hop-Informationen unter Verwendung einer Reverse-DNS-Abfrage für die erfassten Host-IP-Adressen aus. Dies kann die Anzeige verlangsamen, wenn die DNS-Informationen nicht verfügbar sind. Durch Auswahl dieser Option wird die Reverse-DNS-Abfrage unterbunden und der Befehl „traceroute“ dazu gezwungen, stattdessen numerische IP-Adressen auszugeben.

Diagnose > Traceroute (IPv6)



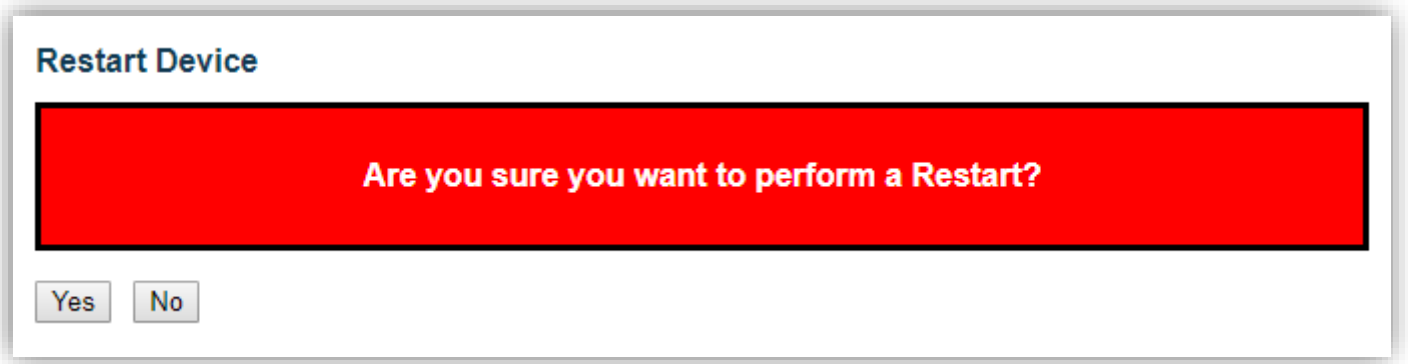
Einstellung	Beschreibung
Hostname oder IP-Adresse	Die Ziel-IP-Adresse.
DSCP-Wert	Dieser Wert wird für den DSCP-Wert im IPv4-Header verwendet. Der Standardwert ist 0. Der gültige Bereich liegt zwischen 0 und 255.
Anzahl der Probes pro Hop	Legt die Anzahl der Probes (Pakete) fest, die pro Hop gesendet werden. Der Standardwert ist 3. Der gültige Bereich liegt zwischen 1 und 60.
Zeitlimit für die Antwort	Legt fest, wie viele Sekunden auf eine Antwort auf eine gesendete Anfrage gewartet werden soll. Der Standardwert beträgt 3. Der gültige Bereich liegt zwischen 1 und 86400.
Maximaler TTL-Wert	Legt den maximalen Wert des Time-To-Live-Feldes (TTL) im IPv4-Header fest. Wird dieser Wert erreicht, bevor der angegebene Remote-Host erreicht wird, wird der Test abgebrochen. Der Standardwert beträgt 30. Der gültige Bereich liegt zwischen 1 und 255.
VID für Quellschnittstelle	Über dieses Feld kann festgelegt werden, dass der Test eine bestimmte lokale VLAN-Schnittstelle als Quellschnittstelle verwendet. Lassen Sie dieses Feld leer, um die automatische Auswahl basierend auf der Routing-Konfiguration zu ermöglichen. Hinweis: Sie können für die Quellschnittstelle entweder die VID oder die IP-Adresse angeben.
Adresse für die Quellschnittstelle	Mit diesem Feld können Sie festlegen, dass der Test eine bestimmte lokale Schnittstelle mit der angegebenen IP-Adresse als Quellschnittstelle verwendet. Die angegebene IP-Adresse muss auf einer lokalen Schnittstelle konfiguriert sein. Lassen Sie dieses Feld leer, um die

	automatische Auswahl basierend auf der Routing-Konfiguration zu ermöglichen. Hinweis: Sie können für die Quellschnittstelle entweder die VID oder die IP-Adresse angeben, jedoch nicht beides.
Numerische Adressen ausgeben	Standardmäßig gibt der Befehl „traceroute“ Hop-Informationen unter Verwendung einer Reverse-DNS-Abfrage für die erfassten Host-IP-Adressen aus. Dies kann die Anzeige verlangsamen, wenn die DNS-Informationen nicht verfügbar sind. Durch Auswahl dieser Option wird die Reverse-DNS-Abfrage unterbunden und der Befehl „traceroute“ dazu gezwungen, stattdessen numerische IP-Adressen auszugeben.

Wartung > Gerät neu starten

Gerät neu starten

Auf dieser Seite können Sie den Switch neu starten. Nach dem Neustart bootet der Switch wie gewohnt. Klicken Sie auf **„Ja“**, um das Gerät neu zu starten.
Klicken Sie auf **„Nein“,** um ohne Neustart zur Seite „Portstatus“ zurückzukehren.



Wartung > Werkseinstellungen

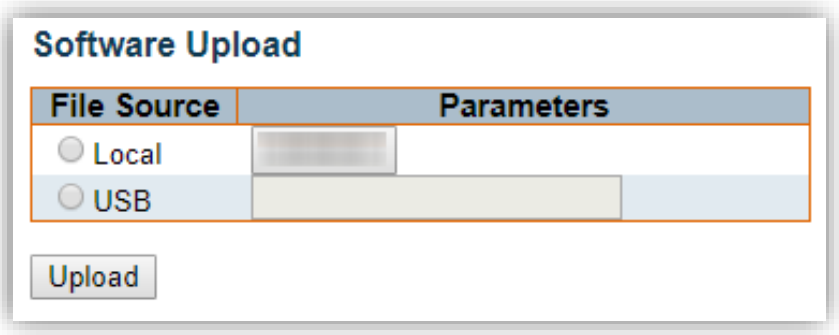
Werkseinstellungen

Auf dieser Seite können Sie die Konfiguration des Switches zurücksetzen. Nur die IP-Konfiguration bleibt erhalten. Die neue Konfiguration ist sofort verfügbar, sodass kein Neustart erforderlich ist.
Klicken Sie auf **„Ja“,** um die Konfiguration auf die Werkseinstellungen zurückzusetzen.
Klicken Sie auf **„Nein“,** um zur Seite „Portstatus“ zurückzukehren, ohne die Konfiguration zurückzusetzen.

Wartung > Software > Hochladen

Software-Upload

Auf dieser Seite können Sie die Firmware des Switches aktualisieren. Klicken Sie auf **„Datei auswählen“,** um den Speicherort eines Software-Images anzugeben, und klicken Sie anschließend auf **„Hochladen**“.
Nachdem das Software-Image hochgeladen wurde, erscheint eine Seite mit der Meldung, dass das Firmware-Update gestartet wurde. Nach etwa einer Minute ist die Firmware aktualisiert und der Switch startet neu.



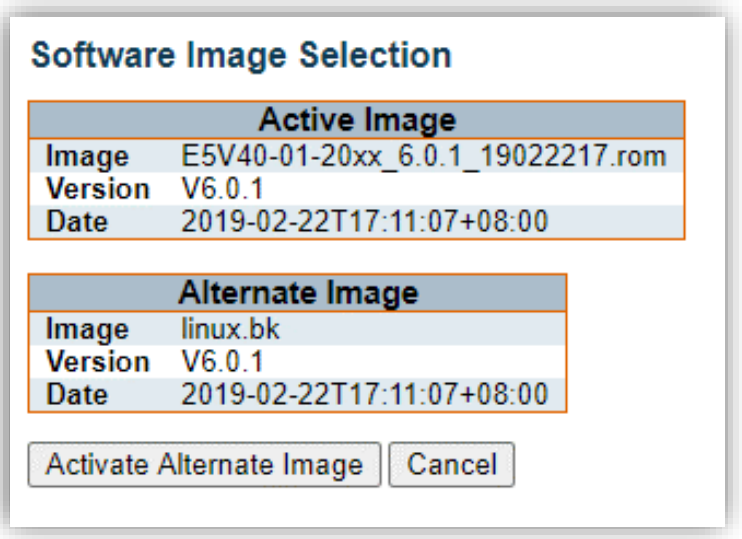
WARNUNG:

Während der Aktualisierung der Firmware ist der Webzugriff vorübergehend nicht verfügbar. Die vordere LED blinkt während der Aktualisierung mit einer Frequenz von 10 Hz grün/aus. Starten Sie das Gerät zu diesem Zeitpunkt nicht neu und schalten Sie es nicht aus, da der Switch sonst anschließend möglicherweise nicht mehr funktioniert.

Wartung > Software > Image-Auswahl

Auswahl des Software-Images

Diese Seite enthält Informationen zu den aktiven und alternativen (Backup-)Firmware-Images im Gerät und ermöglicht es Ihnen, zum alternativen Image zurückzukehren.



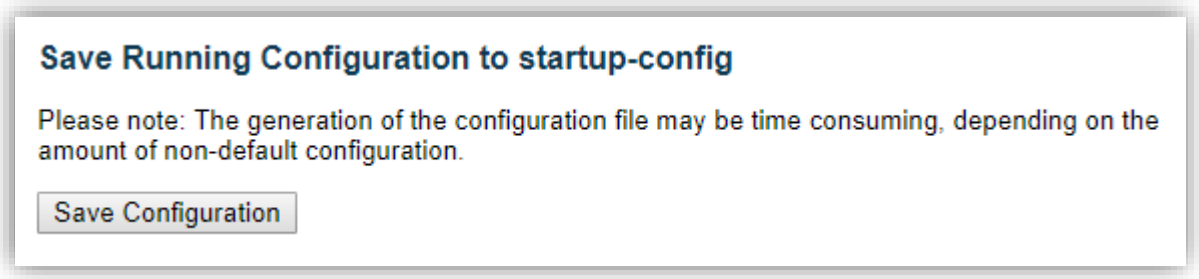
HINWEIS	Falls das aktive Firmware-Image das alternative Image ist, wird nur die Tabelle „Aktives Image“ angezeigt. In diesem Fall ist die Schaltfläche „Alternatives Image aktivieren“ ebenfalls deaktiviert. Ist das alternative Image aktiv (aufgrund einer Beschädigung des primären Images oder durch manuelles Eingreifen), wird beim Hochladen eines neuen Firmware-Images auf das Gerät automatisch der Speicherplatz für das primäre Image verwendet und dieses aktiviert. Bei älteren Firmware-Versionen können die Angaben zur Firmware-Version und zum Datum leer sein. Dies stellt keinen Fehler dar.

Klicken Sie **auf „Alternatives Image aktivieren“,** um das alternative Image zu verwenden. Diese Schaltfläche ist je nach Systemstatus möglicherweise deaktiviert.
Klicken Sie auf **„Abbrechen“,** um das Backup-Image zu aktivieren. Sie verlassen diese Seite.

Wartung > Konfiguration > „startup-config“ speichern

Laufende Konfiguration in „startup-config“ speichern

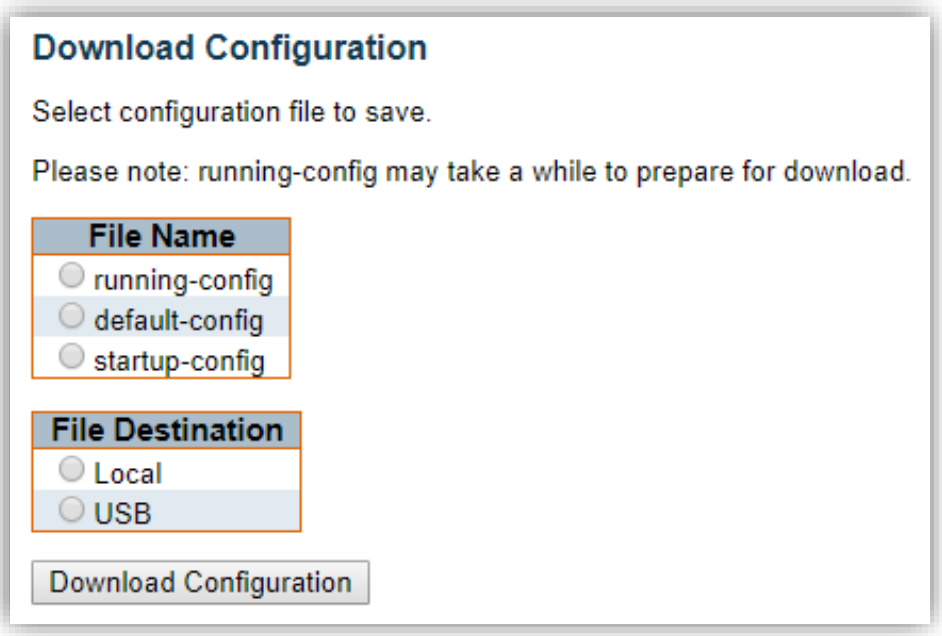
Dadurch wird die „running-config“ in die „startup-config“ kopiert, wodurch sichergestellt wird, dass die derzeit aktive Konfiguration beim nächsten Neustart verwendet wird.



Wartung > Konfiguration > Herunterladen

Konfiguration herunterladen

Der Switch speichert seine Konfiguration in mehreren Textdateien im CLI-Format. Die Dateien sind entweder virtuell (RAM-basiert) oder im Flash-Speicher des Switches abgelegt.

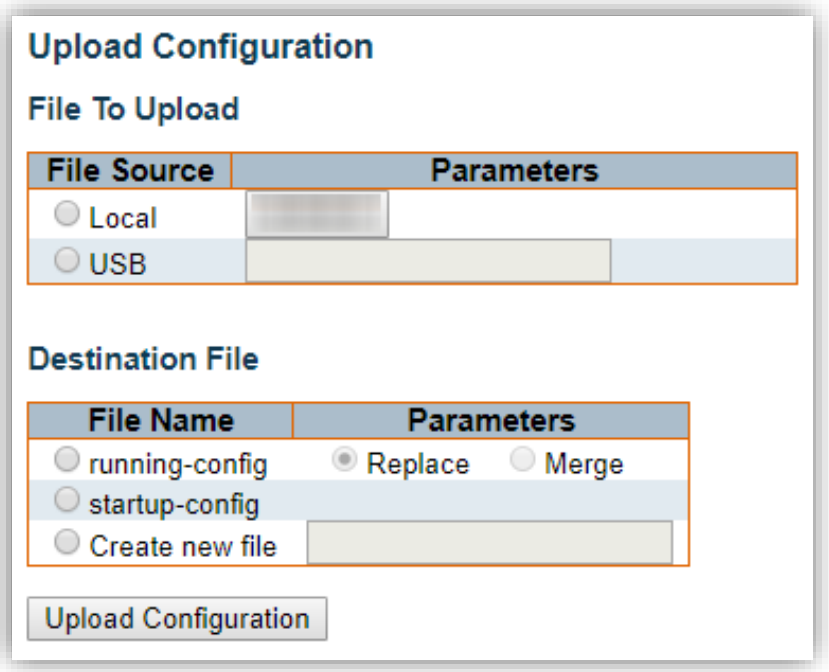


- **„running-config“:** Eine virtuelle Datei, die die aktuell aktive Konfiguration auf dem Switch darstellt. Diese Datei ist flüchtig.
- **default-config:** Eine schreibgeschützte Datei mit herstellerspezifischer Konfiguration. Diese Datei wird gelesen, wenn das System auf die Standardeinstellungen zurückgesetzt wird.
- **startup-config:** Die Startkonfiguration für den Switch, die beim Systemstart eingelesen wird. Wenn diese Datei beim Systemstart nicht vorhanden ist, startet der Switch mit der Standardkonfiguration.
- Bis zu 31 weitere Dateien, die in der Regel für Konfigurationssicherungen oder alternative Konfigurationen verwendet werden.

Es ist möglich, jede der Dateien auf dem Switch in den Webbrowser herunterzuladen. Wählen Sie die Datei aus und klicken Sie auf **„Konfiguration herunterladen**“.
Das Herunterladen der „running-config“ kann eine Weile dauern, da die Datei für den Download vorbereitet werden muss

Wartung > Konfiguration > Hochladen

Konfiguration hochladen



Es ist möglich, eine Datei über den Webbrowser auf alle Dateien auf dem Switch hochzuladen, mit Ausnahme der „default-config“, die schreibgeschützt ist.
Wählen Sie die hochzuladende Datei aus, wählen Sie die Zieldatei auf dem Zielsystem aus und klicken Sie anschließend auf **„Konfiguration hochladen**“.
Wenn das Ziel „running-config“ ist, wird die Datei auf die Switch-Konfiguration angewendet. Dies kann auf zwei Arten erfolgen:

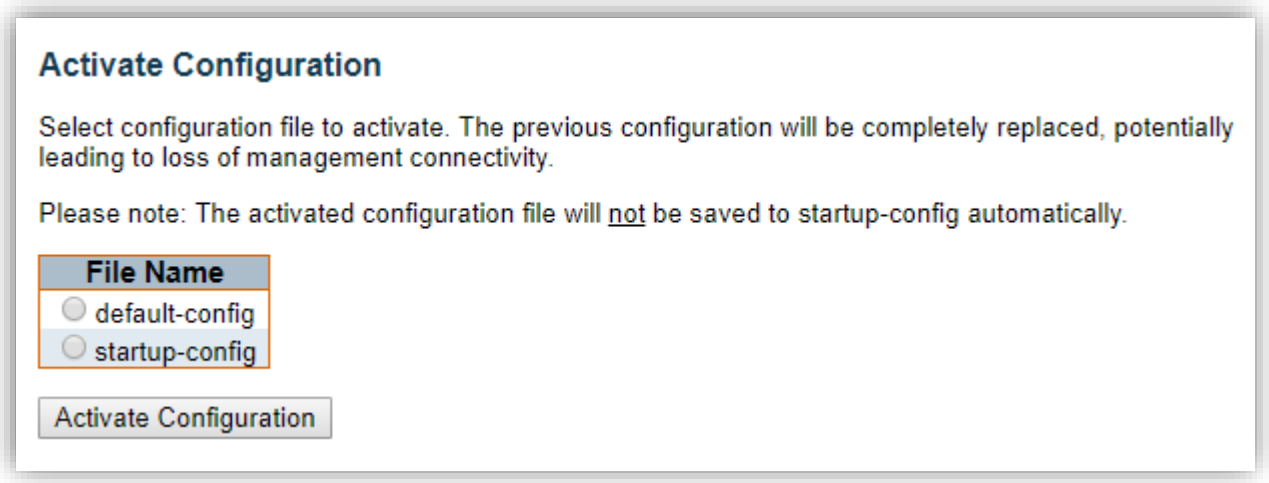
- **Ersetzungsmodus:** Die aktuelle Konfiguration wird vollständig durch die Konfiguration in der hochgeladenen Datei ersetzt.
- **Zusammenführungsmodus:** Die hochgeladene Datei wird in die „running-config“ integriert.

Wenn das Flash-Dateisystem voll ist (d. h. die „default-config“ und 32 weitere Dateien enthält, darunter in der Regel auch die „startup-config“), können keine neuen Dateien erstellt werden. Stattdessen muss eine vorhandene Datei überschrieben oder eine andere Datei gelöscht werden.

Wartung > Konfiguration > Aktivieren

Konfiguration aktivieren

Es ist möglich, jede der auf dem Switch vorhandenen Konfigurationsdateien zu aktivieren, mit Ausnahme der „running-config“, die die derzeit aktive Konfiguration darstellt.
Wählen Sie die zu aktivierende Datei aus und klicken Sie auf „Konfiguration aktivieren“. Dadurch wird der Vorgang gestartet, bei dem die vorhandene Konfiguration vollständig durch die der ausgewählten Datei ersetzt wird.



Wartung > Konfiguration > Löschen

Konfigurationsdatei löschen

Es ist möglich, jede der im Flash-Speicher abgelegten beschreibbaren Dateien zu löschen, einschließlich „startup-config“. Wenn dies geschieht und der Switch ohne vorherigen Speichervorgang neu gestartet wird, wird der Switch dadurch effektiv auf die Standardkonfiguration zurückgesetzt.