Bedienungsanleitung

Managed Switch

Anleitungen werden kontinuierlich weiterentwickelt.
Die jeweils aktuellste Fassung des Dokuments
finden Sie online auf unserer Website.

VIDEOR E. Hartig GmbH | Carl-Zeiss-Straße 8 | 63322 Rödermark | Germany | Tel. +49.6074.888-0 | Fax +49.6074.888-100 |
Amtsgericht Offenbach am Main | HRB 32047 | UIN DE 113592980 |
Geschäftsführer / Managing Directors: Lars Hagenlocher, Dominik Mizdrak

www.eneo-security.com | info@eneo-security.com

CONTENT / INHALT

ÜBER DIESES DOKUMENT

In diesem Dokument finden Sie eine umfassende Beschreibung einer bestimmten Geräteserie, die mit großer Sorgfalt und Genauigkeit erstellt wurde, um Ihnen einen detaillierten Einblick in die allgemeinen Funktionen und Merkmale zu geben, die diese Geräteserie auszeichnen.

Bitte beachten Sie jedoch, dass sich die detaillierte Charakterisierung in diesem Dokument auf die allgemeine Produktlinie bezieht. Der individuelle Funktionsumfang einzelner Modelle oder Ausführungen innerhalb dieser Baureihe kann je nach Konfiguration variieren.

Diese Abweichungen können sich in einem erweiterten oder eingeschränkten Funktions- und Leistungsumfang niederschlagen, so dass die tatsächlichen Spezifikationen einzelner Produkte in mancher Hinsicht von den in diesem Dokument dargestellten Ausführungen abweichen können.

Aus diesem Grund wird dringend empfohlen, das spezifische Datenblatt für das jeweilige Produkt sorgfältig zu lesen. Das Datenblatt enthält spezifische und detaillierte Informationen, die auf das jeweilige Modell zugeschnitten sind. Es ist das primäre Referenzdokument, das die authentischsten und genauesten Informationen über die einzelnen Funktionen und Eigenschaften jedes spezifischen Produkts unserer Geräteserie liefert.

Wir danken Ihnen für Ihr Verständnis und Ihre Bereitschaft, Zeit zu investieren, um genaue Kenntnisse über das von Ihnen ausgewählte Produkt unserer Geräteserie zu erlangen. Bitte zögern Sie nicht, uns zu kontaktieren, wenn Sie weitere Fragen haben oder zusätzliche Informationen benötigen.

SICHERHEITSHINWEISE

Lesen Sie die Sicherheitshinweise und die Bedienungsanleitung vor der Installation des Produkts sorgfältig durch. Je nach Produkttyp können einzelne Punkte entfallen.

Montage und Installation

- Stellen Sie sicher, dass der vorgesehene Montageort für das jeweilige Produkt geeignet ist (z.B. hinsichtlich Gewicht).
- Befestigen Sie die Produkte sicher an den vom Hersteller empfohlenen Stellen und Oberflächen, um Stabilität und Sicherheit zu gewährleisten.
- Stellen Sie sicher, dass die Produkte witterungsbeständig sind, wenn sie im Freien installiert werden, und schützen Sie z.B. Kameras vor direkter Sonneneinstrahlung oder extremen Temperaturen.
- Achten Sie darauf, dass eventuell vorhandene Lüftungsschlitze nicht blockiert werden, um eine ausreichende Luftzirkulation und Kühlung zu gewährleisten.
- Achten Sie darauf, dass Kameras, Schalter usw. mit ausreichendem Sicherheitsabstand zu brennbaren Materialien, Stromquellen, fließendem Wasser usw. installiert werden.
- Montage, Inbetriebnahme und Wartung dürfen nur von autorisiertem Fachpersonal unter Beachtung der einschlägigen Normen und Richtlinien durchgeführt werden.

Stromversorgung & Verkabelung

- Um eine sichere Stromversorgung zu gewährleisten, verwenden Sie nur vom Hersteller empfohlene Netzteile und Kabel.
- Achten Sie darauf, dass die Kabel ordnungsgemäß verlegt und vor Manipulation und Beschädigung (z. B. Knicken) geschützt sind, um Stromausfälle oder Kurzschlüsse (z. B. durch Eindringen von Feuchtigkeit) zu vermeiden.
- Achten Sie darauf, dass die Kabel nicht durch Türen, Fenster oder andere bewegliche Teile geführt werden, um Beschädigungen und Stolperfallen zu vermeiden.
- Um das System von der Stromversorgung zu trennen, ziehen Sie das Kabel nur am Stecker und niemals direkt am Kabel.
- Beim Kürzen von flexiblen Anschlusskabeln sind Aderendhülsen zu verwenden.

Sicherheit

- Verwenden Sie starke Passwörter für alle Kameras und Geräte, um unbefugten Zugriff zu verhindern.
- Halten Sie die Firmware der Geräte auf dem neuesten Stand, um Sicherheitslücken zu minimieren.
- Schützen Sie den (Fern-)Zugriff auf die Geräte durch sichere Methoden wie verschlüsselte Verbindungen oder VPN.

Betrieb

- Die Geräte dürfen nur innerhalb der im Datenblatt angegebenen Temperatur- und Feuchtebereiche betrieben werden.
- Zur Vermeidung von Überhitzung ist für ausreichende Belüftung zu sorgen. Dies gilt insbesondere für Geräte wie Recorder und Switches, die Wärme erzeugen können.
- Stellen Sie sicher, dass keine Sichtlinien blockiert werden und dass das Zubehör keine Bereiche verdeckt, die von anderen Geräten oder Personen genutzt werden.
- Stellen Sie sicher, dass Kameras so ausgerichtet sind, dass sie einen klaren Blick auf den gewünschten Bereich bieten, ohne die Privatsphäre von Personen zu beeinträchtigen.

Reinigung und Wartung

- Reinigen Sie die Linsen und Gehäuse der Kameras regelmäßig, um eine klare Sicht zu gewährleisten.
- Halten Sie die Lüftungsschlitze sauber und frei von Staub, um eine effiziente Kühlung zu gewährleisten.
- Verwenden Sie für die Reinigung ein mildes Reinigungsmittel. Scharfe Reinigungsmittel wie Verdünner oder Benzin können die Oberfläche dauerhaft beschädigen.
- Überprüfen Sie das Produkt regelmäßig auf Beschädigungen und Verschleißerscheinungen.
- Verwenden Sie nur Original-Ersatzteile (z.B. Anschlusskabel) oder Zubehör der Firma VIDEOR E. Hartig GmbH.
- Bei Eingriffen durch nicht autorisierte Personen erlischt jeglicher Garantieanspruch.
- Vor dem Öffnen des Gehäuses ist die Stromversorgung zu unterbrechen.

Warnhinweise, Datenschutz und rechtliche Hinweise

- Machen Sie Besucherinnen und Besucher durch gut sichtbare Hinweise darauf aufmerksam, dass sie aufgezeichnet werden.
- Weisen Sie gegebenenfalls auf Verhaltensregeln hin.
- Stellen Sie sicher, dass die Kameras so ausgerichtet sind, dass die Privatsphäre nicht verletzt wird, z. B. durch Aufnahmen von Nachbarn oder öffentlichen Bereichen.
- Beachten Sie die örtlichen Gesetze und Vorschriften zur Videoüberwachung und zum Datenschutz (DSGVO).

1 – EINFÜHRUNG

1.1 – Technische Daten

Die Frontplatte des Web-Smart-Switches verfügt über 8/16/24 adaptive 10/100M-UTP-Ports und eine LED-Anzeige.

Die 8/16/24 Ports unterstützen Geräte mit einer Bandbreite von 10/100 Mbit/s und Auto-Negotiation.

Jeder Port verfügt über eine LNK/ACT-Anzeige.

1.2 – Vorsichtsmaßnahmen bei der Installation

- Stellen Sie sicher, dass die Oberfläche, auf der das Gerät aufgestellt wird, ausreichend befestigt ist, damit es nicht kippen kann.
- Stellen Sie sicher, dass die Steckdose nicht weiter als 1,8m vom Gerät entfernt ist.
- Stellen Sie sicher, dass das Gerät mit dem Netzkabel sicher an die Steckdose angeschlossen ist.
- Stellen Sie sicher, dass das Gerät gut belüftet ist und die Wärme gut abgeführt werden kann.
- Stellen Sie keine schweren Gegenstände auf das Gerät.
- Benutzen Sie ausschließlich die mitgelieferten Schrauben! So vermeiden Sie Probleme und gewährleisten eine einfache Montage.

1.3 – Stromversorgung

Der Switch kann mit einer Wechselstromversorgung von 100 bis 240 V AC, 50 bis 60 Hz verwendet werden. Das integrierte Stromversorgungssystem des Switches passt die Betriebsspannung automatisch an die tatsächliche Eingangsspannung an. Der Netzanschluss befindet sich auf der Rückseite des Switches.

Trennen Sie das Netzkabel, indem Sie den Stecker am Netzschalter auf der Rückseite ziehen und das andere Ende aus einer Steckdose ziehen.

2 – INBETRIEBNAHME

Sie können die webbrowserbasierte Konfiguration verwenden, um den Web-Smart Switch zu verwalten. Der über einen Webbrowser zu konfigurierende Web-Smart Switch muss über eine Ethernet-Verbindung mit mindestens einem Computer verbunden sein. Dazu kann ein PC/Laptop an einen beliebigen RJ45-Port angeschlossen werden.

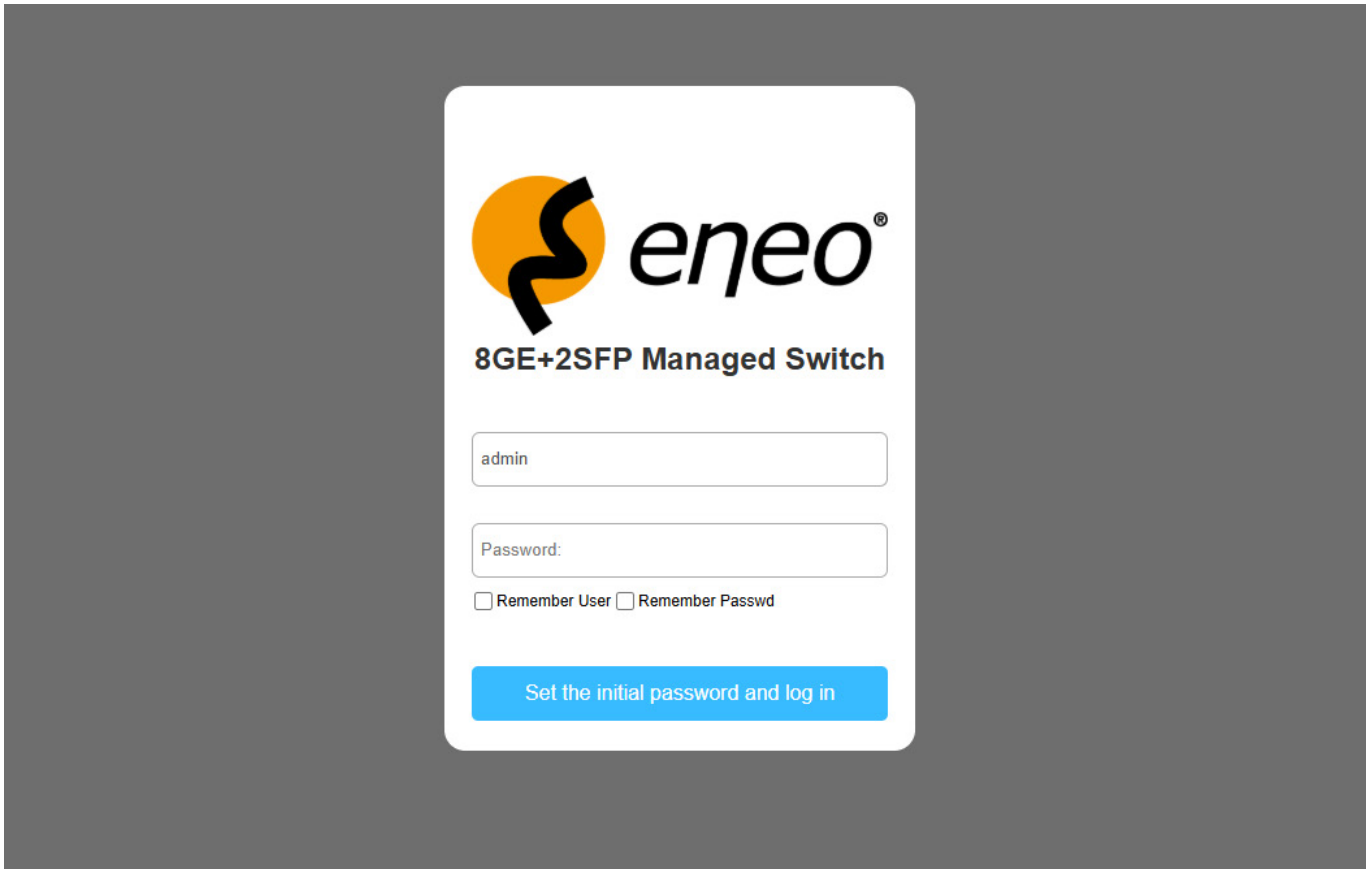
2.1 – Werkseinstellungen und Anmeldung

Die Switches werden mit den folgenden Werkseinstellungen geliefert:

IP-Adresse: 192.168.1.10
Subnetzmaske: 255.255.255.0

Benutzername: admin
Kennwort: Sie müssen zunächst ein Kennwort für die erste Anmeldung festlegen. Dieses muss mindestens acht Zeichen lang sein.

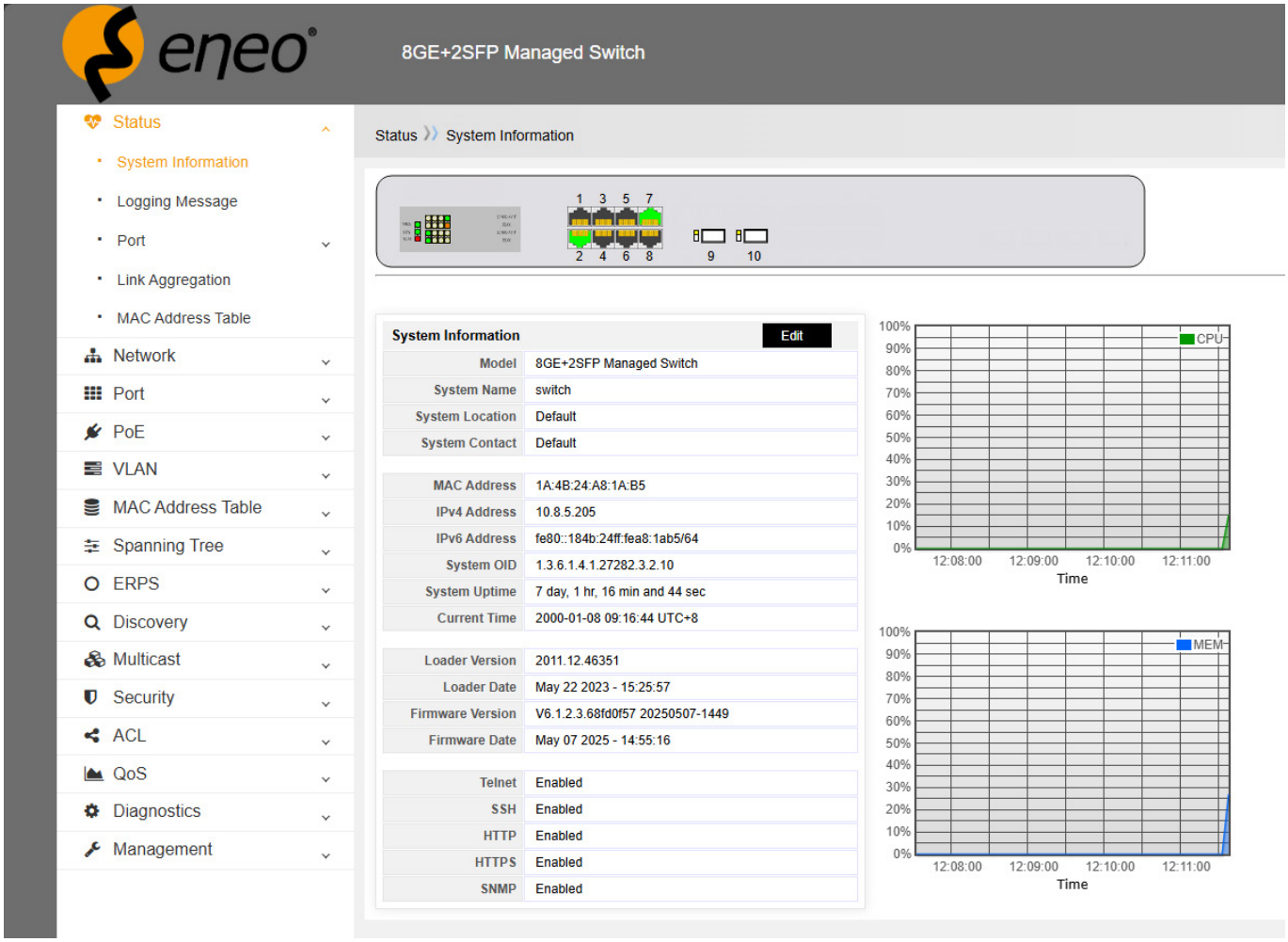
Eine Verbindung zum Switch kann hergestellt werden, indem die IP-Adresse des Switches (192.168.1.10) direkt in einen Webbrowser eingetragen wird. Zur Anmeldung trägt der Benutzer einfach den oben aufgeführten Benutzernamen und das Kennwort ein.



2.2 – System Informationen

Nach erfolgreicher Anmeldung wird automatisch die Seite „Systeminformationen“ angezeigt, auf der die wichtigsten Informationen zum Switch angezeigt werden.

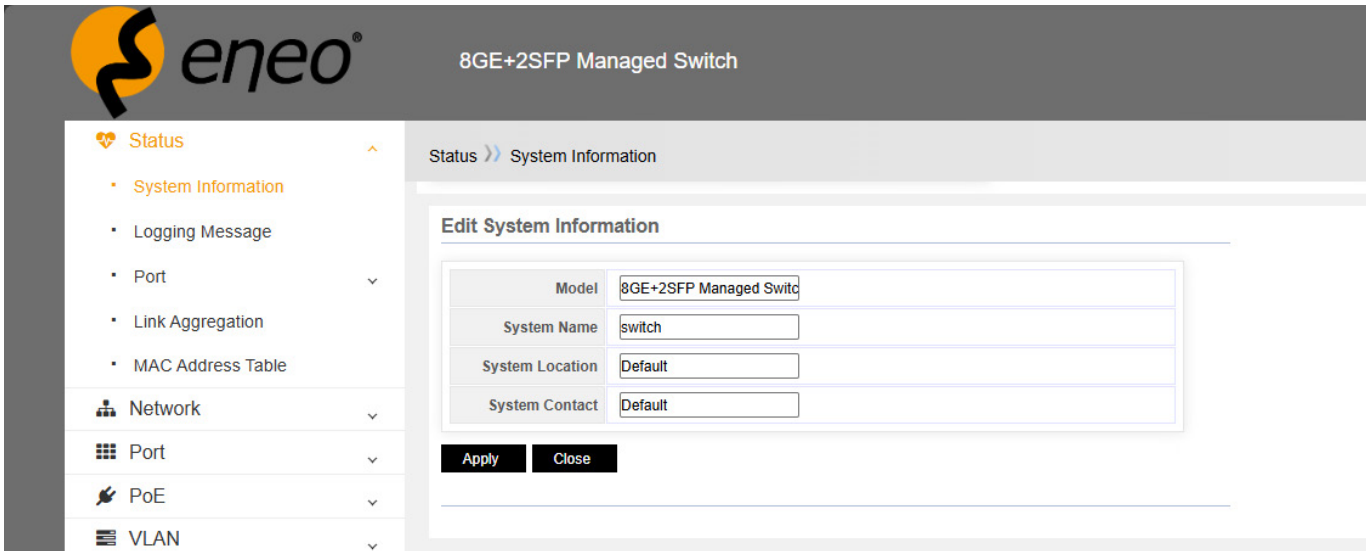
Sie zeigt die Systeminformationen des Switches an, wie z. B. Modellname, MAC-Adresse, IP-Adresse, Hardware- und Softwareversionsinformationen.



Modell: Modellname des Geräts
Systemname: Name des Geräts. Die Standardeinstellung ist „Switch“.
Systemstandort: Standort des Geräts.
Systemkontakt: Kontakt für das System.

2.2.1 – Bearbeiten

Über die Schaltfläche „Edit/Bearbeiten“ haben Sie die Möglichkeit, einige Systeminformationen zu bearbeiten.



2.2.2 – Statische IP-Adresse oder dynamische IP-Adresse festlegen

Statische IP-Adresse

Eine statische IP-Adresse ist eine manuell zugewiesene und feste numerische Kennung, die einem Gerät innerhalb eines Computernetzwerks zugewiesen wird. Sie bleibt unverändert und ändert sich nur, wenn sie manuell neu konfiguriert wird. Statische IP-Adressen werden in der Regel für Geräte verwendet, die einen konsistenten und zuverlässigen Netzwerkzugang erfordern.

Hinweis!

Wenn Sie „Statisch“ auswählen, müssen Sie dem Switch manuell eine IP-Adresse, eine Subnetzmaske, ein Standard-Gateway und einen DNS-Server (optional) zuweisen. Die IP-Adresse und das Gateway müssen sich im selben Netzwerksegment befinden.

Dynamische IP-Adresse

Eine dynamische IP-Adresse ist eine IP-Adresse, die einem Gerät automatisch von einem DHCP-Server (Dynamic Host Configuration Protocol) zugewiesen wird. Im Gegensatz zu einer statischen IP-Adresse kann sich eine dynamische IP-Adresse im Laufe der Zeit ändern. Der DHCP-Server vergibt IP-Adressen aus einem Pool verfügbarer Adressen, wodurch eine effiziente Nutzung der Netzwerkressourcen ermöglicht wird.

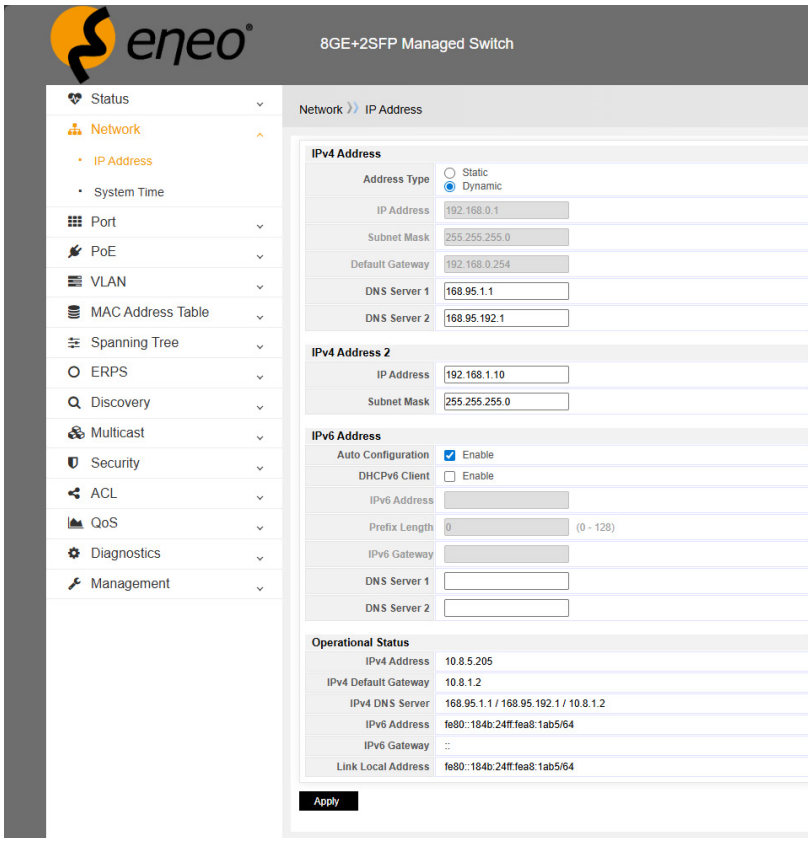
Hinweis!

Wenn Sie „Dynamisch" auswählen, weist der DHCP-Server dem Switch eine IP-Adresse innerhalb des vordefinierten Bereichs zu. Die Subnetzmaske und NMS werden automatisch vom DHCP-Server zugewiesen. Der DNS-Server muss jedoch weiterhin manuell eingerichtet werden.

Auf dieser Seite können Sie die IP-Adresse, die Subnetzmaske, das Gateway und andere Informationen manuell einstellen; Sie können auch Ihr Netzwerk verwenden, unter anderem DHCP Server, der automatisch eine IP-Adresse zuweist.

Hinweis!

DHCP-Server (Dynamic Host Configuration Protocol Server) ist ein Netzwerkserver, der Geräten in einem Netzwerk automatisch IP-Adressen und andere Netzwerkkonfigurationsparameter zuweist.



Die **Standard-IP-Adresse** des Switches lautet: 192.168.1.199

Standard-Subnetzmaske: 255.255.255.0

Standard-Gateway: 192.168.1.254

Wenn Sie die Bearbeitung abgeschlossen haben, klicken Sie auf „Übernehmen", um die IP-Adresseinstellungen abzuschließen.

Hinweis!

Automatische IP-Adressvergabe: Wenn ein Gerät (z. B. ein Computer, Smartphone oder Drucker) eine Verbindung zu einem Netzwerk herstellt, weist der DHCP-Server ihm eine IP-Adresse zu. Diese IP-Adresse ist für das Gerät unerlässlich, um mit anderen Geräten im Netzwerk zu kommunizieren und auf das Internet zuzugreifen.

Hinweis!

Temporäre Leases: Die vom DHCP-Server zugewiesenen IP-Adressen werden in der Regel für einen bestimmten Zeitraum (Lease) vergeben. Nach Ablauf des Leases kann das Gerät eine neue IP-Adresse anfordern oder die bestehende erneuern. Dies trägt zu einer effizienten Verwaltung der begrenzten Anzahl verfügbarer IP-Adressen in einem Netzwerk bei.

Hinweis!

Subnetzmaske: Der DHCP-Server stellt dem Gerät auch die Subnetzmaske zur Verfügung. Die Subnetzmaske hilft dem Gerät zu verstehen, welcher Teil der IP-Adresse sich auf das Netzwerk bezieht und welcher Teil sich auf den Host (das Gerät) innerhalb des Netzwerks bezieht.

Hinweis!

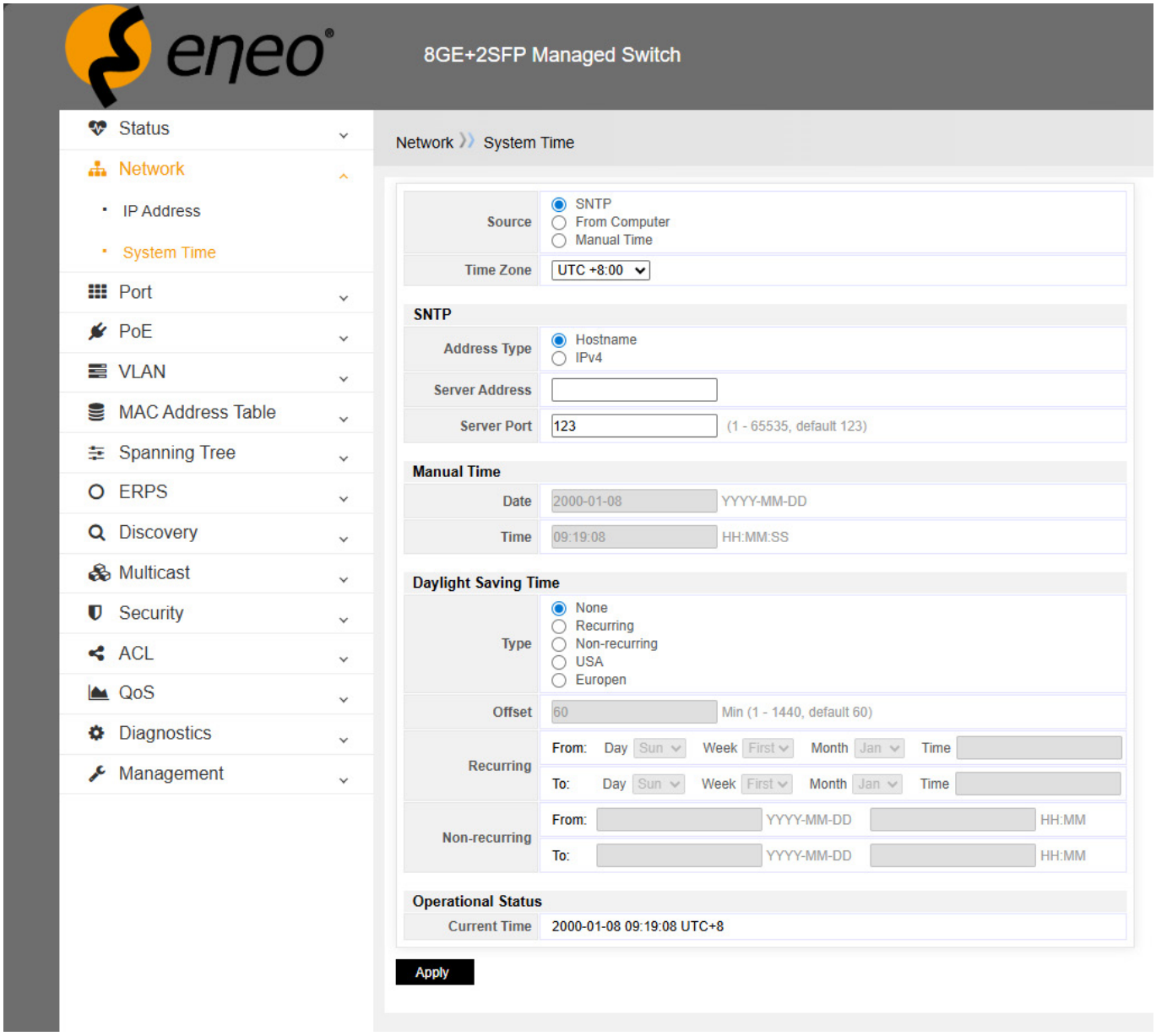
Standard-Gateway: Er weist die Standard-Gateway-Adresse zu. Der Standard-Gateway ist die IP-Adresse des Routers, der das lokale Netzwerk mit anderen Netzwerken (wie dem Internet) verbindet. Geräte verwenden diesen Gateway, um Daten an Ziele außerhalb ihres lokalen Netzwerks zu senden.

Hinweis!

DNS-Server: Der DHCP-Server informiert das Gerät über die DNS-Server (Domain Name System). DNS-Server übersetzen für Menschen lesbare Domänennamen (wie www.example.com) in IP-Adressen, die Geräte verstehen können. Dadurch können Geräte problemlos auf Websites und andere Internetressourcen zugreifen.

2.3 – Zeitkonfiguration

Die Systemzeit des Switches kann über SNTP, den Computer, der auf den Switch zugreift, und durch manuelle Konfiguration abgerufen werden.



2.3.1 – Quelle

2.3.1.1 – SNTP

SNTP (Simple Network Time Protocol) ist eine vereinfachte Version des NTP (Network Time Protocol), das zur Synchronisierung der Uhren von Geräten in einem Netzwerk verwendet wird.

Wenn im eigenen Netzwerk keine Zeitquelle verfügbar ist und die Zeit von einer externen Quelle über das Internet abgerufen werden soll, können die Daten des externen NTP-Servers direkt eingetragen werden, z. B. 213.209.109.45 unter http://www.pool.ntp.org/de/

2.3.1.2 – Vom Computer

Die Systemzeit wird mit der aktuellen Computerzeit synchronisiert.

2.3.1.3 – Manuelle Zeit

Sie können jede beliebige Zeit manuell einstellen.

2.3.2 – Zeitzone

Eine Zeitzone ist ein Bereich der Erde, in dem aus rechtlichen, wirtschaftlichen und sozialen Gründen eine einheitliche Standardzeit gilt. Zeitzonen basieren in der Regel auf der Position der Sonne relativ zur Erde und weichen in der Regel um eine bestimmte Anzahl von Stunden (oder in einigen Fällen um halbe Stunden) von der koordinierten Weltzeit (UTC) ab. Die Standardzeitzone in Deutschland ist beispielsweise UTC+1.

Wenn die Zeit über SNTP bezogen wird, können Sie direkt die IPv4-Adresse des Zeitservers und 123 für den Standardport eintragen. Stellen Sie sicher, dass der Switch die jeweilige IP-Adresse auch tatsächlich erreichen kann.

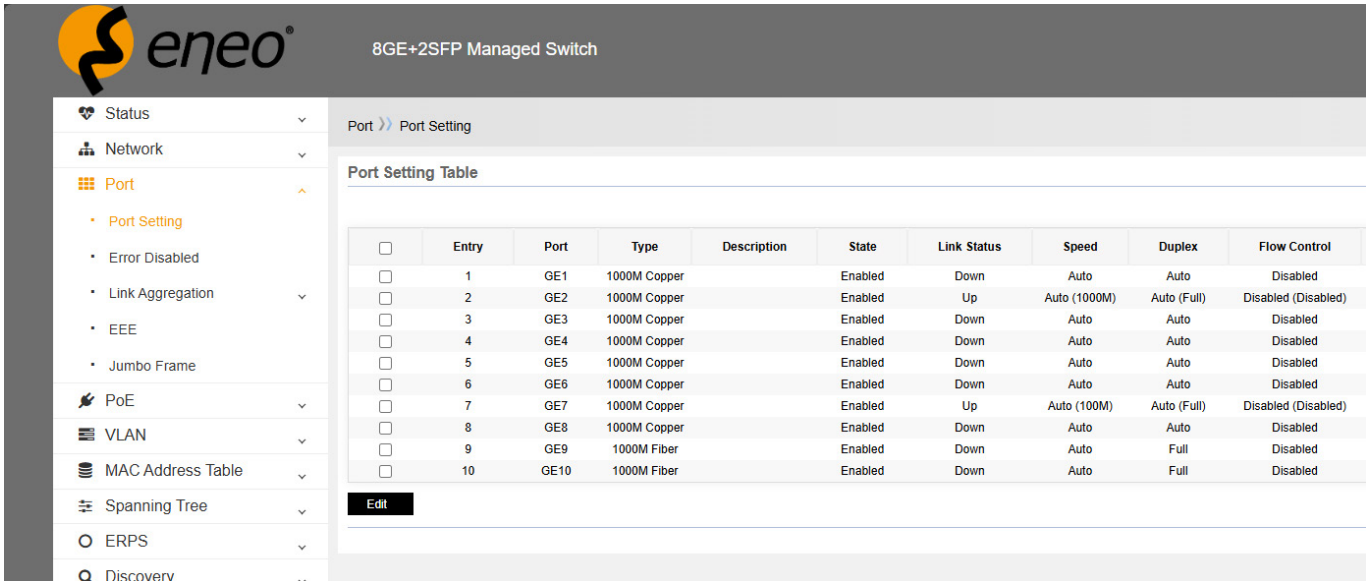
3 – PORT KONFIGURATION

Auf dieser Seite können Sie die Beschreibungen, den Verwaltungsstatus, die Geschwindigkeit, den Duplexmodus und die Flusskontrolle des Ports einstellen. Die Ports sind werkseitig auf den Auto-Modus eingestellt. Die automatische Aushandlung ist ein Verfahren, mit dem zwei verbundene Ethernet-Netzwerkports unabhängig voneinander die höchstmögliche Übertragungsgeschwindigkeit sowie den Duplexmodus aushandeln und konfigurieren können. Dieses Verfahren gilt nur fürTwisted-Pair-Kabel – nicht für Glasfaserverbindungen.

In einigen Fällen kann es jedoch vorkommen, dass das Endgerät nicht richtig erkannt wird. Dies tritt manchmal bei Verwendung einer Kamera mit einer 100-Mbps-Schnittstelle auf. In diesem Fall muss der Port manuell auf 100 Mbps eingestellt werden.

Wenn ein Port aus Sicherheitsgründen nicht verwendet werden soll, kann er vollständig deaktiviert werden.

3.1 – Porteinstellungen



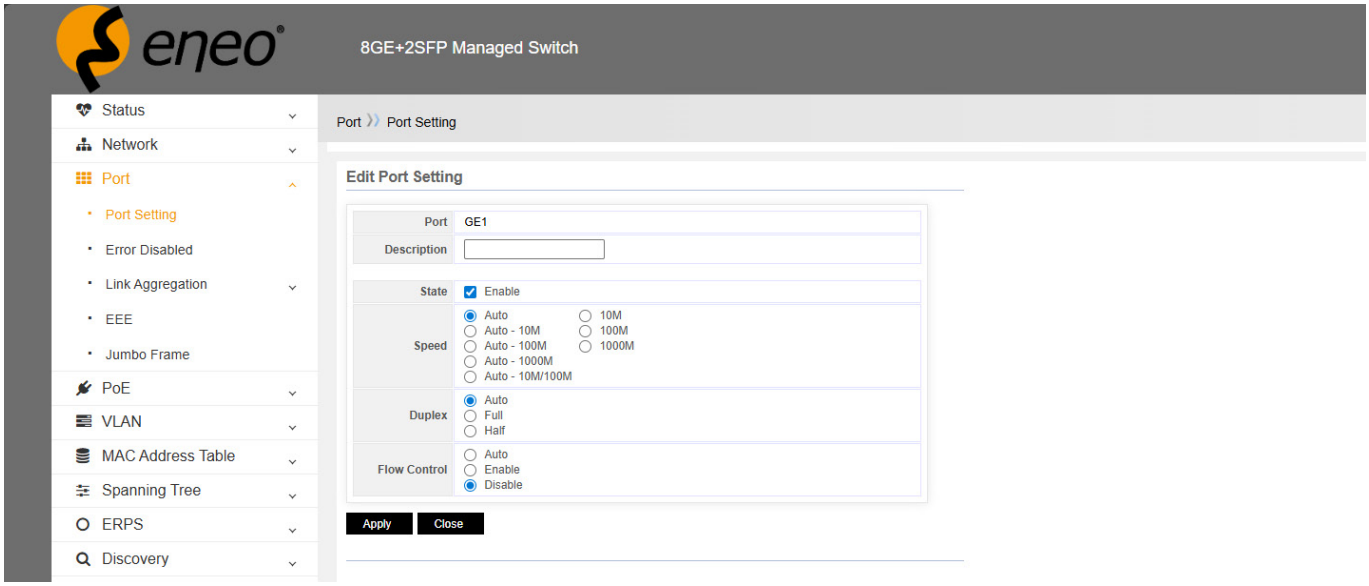
Entry: Eintragsnummer des Ports

Port: Der Name des Ports. GE steht für Gigabit Ethernet und bezieht sich auf eine Netzwerkschnittstelle, die Datenübertragungsraten von bis zu 1 Gigabit pro Sekunde (1 Gbps) unterstützt.

Typ: Typ der Übertragungsrate und des Mediums.

Status: Aktivieren/Deaktivieren. Sie können den Port deaktivieren, indem Sie den Portstatus ändern.

Link Status: Wenn der Port ordnungsgemäß verbunden ist, ist er UP, andernfalls ist er DOWN.



Die folgenden Schritte zeigen, wie Sie die Port-Einstellungen vornehmen.

1. Wählen Sie den Port aus, der konfiguriert werden soll, z. B. Port 1-4.
2. Klicken Sie unten links auf „Edit/Bearbeiten“.
3. Legen Sie die Beschreibung, den Verwaltungsstatus, die Geschwindigkeit, den Duplexmodus und die Flusskontrolle fest.
4. Klicken Sie unten links auf „Übernehmen“.

State: Verbindungsstatus Aktivieren/Deaktivieren. Wenn Sie „Aktivieren“ auswählen, kann dieser Port normal verwendet werden. Wenn Sie „Aktivieren“ deaktivieren, kann dieser Port nicht normal verwendet werden.

Speed: Legen Sie die Standardgeschwindigkeit für die automatische Aushandlung (5 Typen) sowie den erzwungenen Modus (3 Typen) fest.

Duplex: Auswahl aus Auto, Duplex und Halbduplex

Flow Control: Automatische Aushandlung, aktivieren und deaktivieren. Die Flusskontrolle ist ein Mechanismus zur Verwaltung der über ein Netzwerk oder eine Kommunikationsverbindung gesendeten Datenmenge. Sie stellt sicher, dass der Sender den Empfänger nicht mit mehr Daten überlastet, als dieser verarbeiten oder puffern kann. Dies ist entscheidend für die Aufrechterhaltung einer zuverlässigen und effizienten Kommunikation, insbesondere in Umgebungen, in denen Sender und Empfänger unterschiedliche Verarbeitungskapazitäten haben oder die Netzwerkbedingungen variieren.

Halbduplex-Modus: Zwei-Wege-Kommunikation, jedoch nicht gleichzeitig in beide Richtungen.

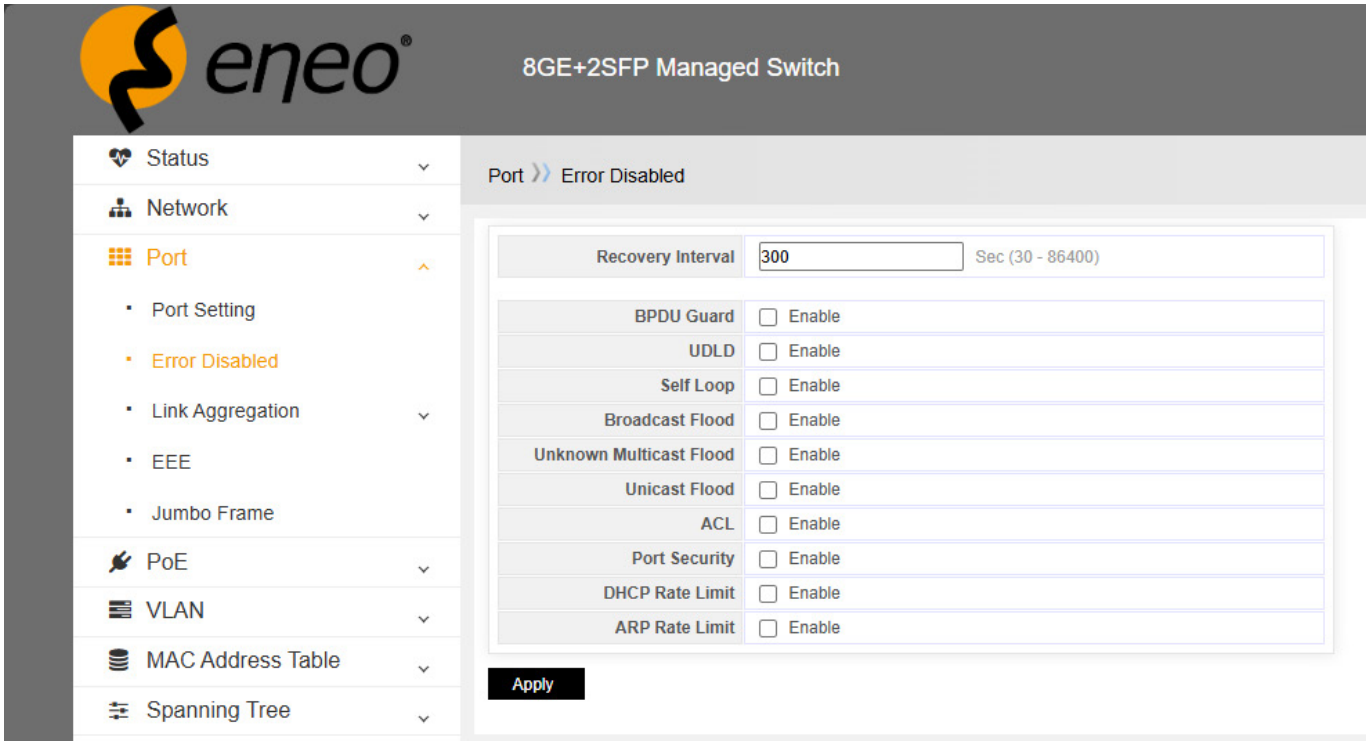
Vollduplex-Modus: Zwei-Wege-Kommunikation, gleichzeitig in beide Richtungen.

3.2 – Fehler deaktiviert

Zur Fehlerbehebung bei einer fehlerbedingten Deaktivierung der Schnittstelle gehören folgende Fehlererscheinungen: Die Leitung ist blockiert, die physische Anzeige ist ausgeschaltet oder leuchtet orange (der Anzeigestatus ist je nach Plattform unterschiedlich).

Das System versucht nach einer bestimmten Zeit (standardmäßig 300 Sekunden) die als fehlerbedingt deaktivierte Schnittstelle wiederherzustellen.

Wenn die Ursache für die Fehlerdeaktivierung jedoch nicht grundlegend behoben wurde, wird die Schnittstelle nach der Wiederherstellung erneut als fehlerbedingt deaktiviert.



Aus der Liste können wir häufige Ursachen wie UDLD, DPUD Guard, Port-Sicherheit und Schleifen erkennen. Sie können das Wiederherstellungsintervall festlegen und die häufigsten Ursachen für die Deaktivierung auswählen.

UDLD

UDLD steht für Unidirectional Link Detection. Es handelt sich um ein Datenverbindungsschichtprotokoll, das von Cisco Systems entwickelt wurde, um die physische Konfiguration von Kabeln zu überwachen und unidirektionale Verbindungen zu erkennen.
Eine unidirektionale Verbindung ist eine Verbindung, die auf beiden Seiten der Verbindung besteht, aber Pakete werden nur von einer Seite empfangen. Dies kann zu Problemen wie Weiterleitungsschleifen und Traffic Blackholing führen.

UDLD funktioniert durch den Austausch von Protokollpaketen zwischen benachbarten Geräten. Jeder für UDLD konfigurierte Switch-Port sendet UDLD-Protokollpakete, die die Geräte- und Port-ID des Ports sowie die von UDLD an diesem Port erkannten Nachbar-Geräte- und Port-IDs enthalten. Wenn ein Port seine eigene Geräte- und Port-ID für einen bestimmten Zeitraum nicht in den eingehenden UDLD-Paketen sieht, wird die Verbindung als unidirektional betrachtet. Sobald eine unidirektionale Verbindung erkannt wird, wird der entsprechende Port deaktiviert.

UDLD ist ein Cisco-eigenes Protokoll, aber ähnliche Funktionen gibt es unter anderen Namen in Produkten anderer Anbieter. HP nennt seine Funktion beispielsweise Device Link Detection Protocol (DLDP), Extreme Networks Extreme Link Status Monitoring (ELSM) und AVAYA Link-State Tracking.

1. BPDU-Schutz:

   Deaktiviert automatisch einen Port, wenn BPDU-Pakete erfasst werden, und verhindert so, dass nicht autorisierte Geräte das Spanning Tree Protocol (STP) stören.

2. UDUL (UniDirectional Link Detection):

   Erkennt und blockiert unidirektionale Glasfaser-/Kupferverbindungen, um Netzwerkinstabilitäten durch Einwegkommunikation zu vermeiden.

3. Selbstschleifenerkennung:

   Identifiziert und blockiert physische Port-Loops (z. B. ein Kabel, das zwei Ports auf demselben Switch verbindet), um Traffic-Stürme zu verhindern.

4. Broadcast-Flood-Control:

   Begrenzt übermäßigen Broadcast-Traffic, um Netzwerküberlastungen und Leistungseinbußen zu vermeiden.

5. Unknown Multicast Flood Control:

   Beschränkt das Flooding unbekannter Multicast-Frames und optimiert so die Bandbreitennutzung.

6. Unicast Flood Control:

   Blockiert übermäßige Fluten von unbekanntem Unicast-Datenverkehr, um das Risiko einer Ressourcenerschöpfung zu verringern.

7. ACL (Access Control List):

Filtert den Datenverkehr anhand vordefinierter Regeln (z. B. IP/MAC-Adressen, Ports), um Sicherheitsrichtlinien durchzusetzen.

8. Port-Sicherheit:

Beschränkt den Portzugriff auf autorisierte MAC-Adressen und verhindert so unbefugte Geräteverbindungen.

9. DHCP-Ratenbegrenzung:

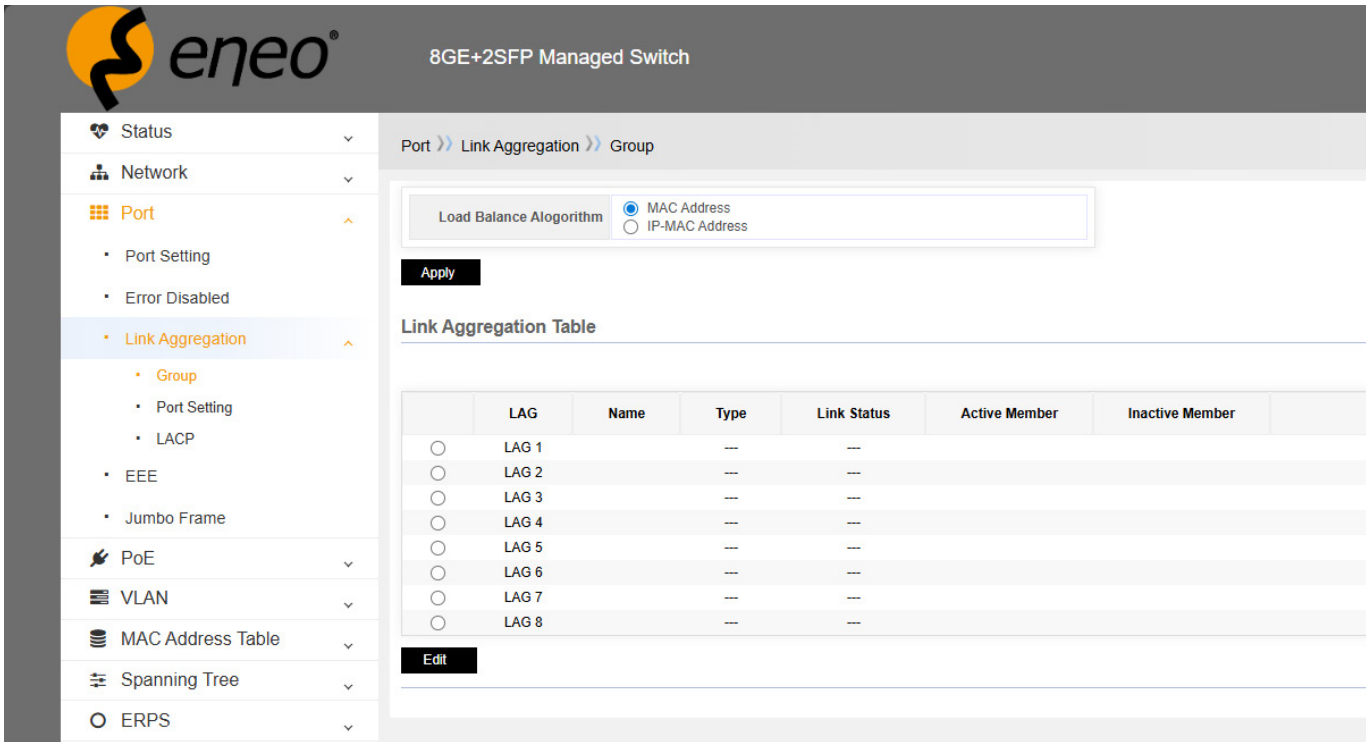
Kontrolliert die Anzahl der DHCP-Anfragen pro Port, um DHCP-Erschöpfungsangriffe zu verhindern.

10. ARP-Ratenbegrenzung:

Drosselt die Häufigkeit von ARP-Paketen, um ARP-Spoofing- oder Flooding-Angriffe abzuwehren.

3.3 – Link-Aggregation

Link-Aggregation kann mehrere Ethernet-Ports zu einer logischen Aggregationsgruppe zusammenfassen. Auf der Schicht-Entität sind alle physischen Verbindungen in einer Aggregationsgruppe eine logische Verbindung. Die Link-Aggregation ist in einer Aggregationsgruppe so konzipiert, dass die Bandbreite durch die Verteilung der Ausgangs-/Eingangslast zwischen den Mitgliedsports erhöht wird. Die Link-Aggregationsgruppe ermöglicht auch Port-Redundanz, um die Verbindungszuverlässigkeit zu gewährleisten. Eine Link-Aggregation besteht aus maximal acht ordnungsgemäß konfigurierten Ethernet-Schnittstellen. Alle Schnittstellen in der Link-Aggregation müssen die gleiche Geschwindigkeit haben und als Layer-2-Schnittstellen konfiguriert sein.



LAG (Link Aggregation Group): LAG bezeichnet eine Gruppe von physischen Ethernet-Ports, die gebündelt werden, um den Durchsatz zu erhöhen und Redundanz zu gewährleisten. Dadurch können mehrere physische Verbindungen als eine einzige logische Verbindung behandelt werden, was die Netzwerkleistung und -zuverlässigkeit verbessert.

TYP: LAG kann als statisch oder LACP eingestellt werden. Statisch ist eine gängige Art der Link-Aggregation. LACP wird in ► „3.3.3 – LACP“ ausführlich beschrieben.

Link-Status: Wenn der Port ordnungsgemäß verbunden ist, ist er UP, andernfalls ist er DOWN.

3.3.1 – Gruppe festlegen und Ports hinzufügen

Lastverteilungsalgorithmus:

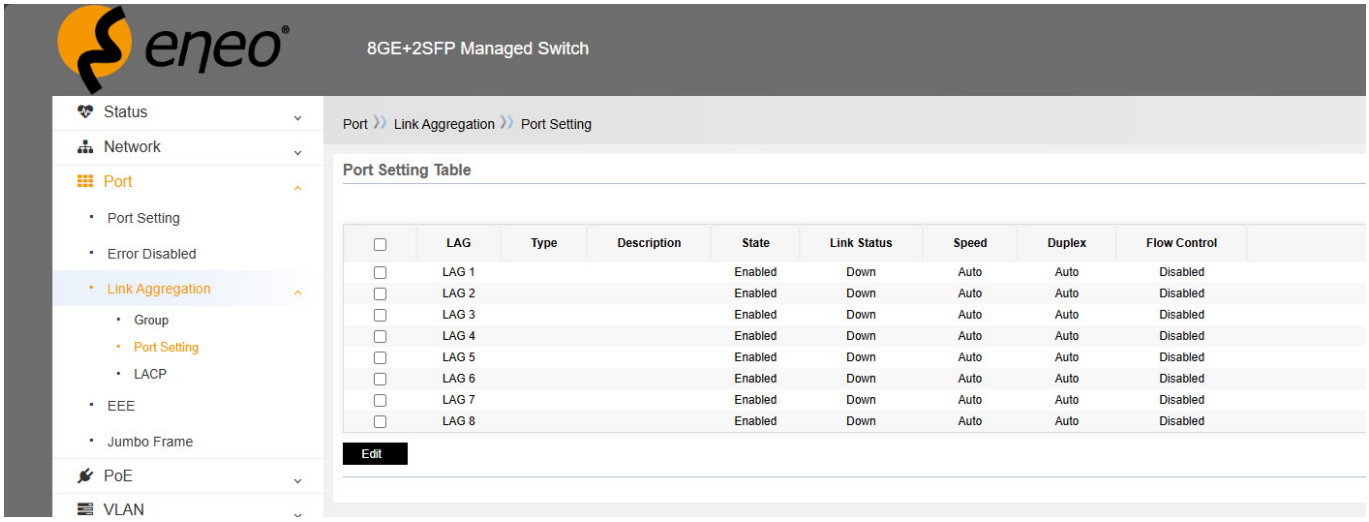
- MAC-Adresse (Quell-MAC + Ziel-MAC)
- IP-MAC-Adresse (Quell-IP + Ziel-IP + Quell-MAC + Ziel-MAC)

Dies ist ein aggregierter Routing-Algorithmus.
Die Route einer Nachricht wird anhand ihrer Adresse ausgewählt

1. Wählen Sie eine Aggregationsgruppe (1-8), LAG 1 ~ LAG 8
2. Klicken Sie auf „Edit/Bearbeiten“
3. Wählen Sie „Statisch“, um den Port aus dem linken Feld zum rechten Feld hinzuzufügen und ihn der Aggregationsgruppe hinzuzufügen. Es werden maximal 8 Aggregationsgruppen und maximal 8 Mitgliedsports pro Aggregationsgruppe unterstützt.

3.3.2 – Einstellungen für Aggregationsport-Eigenschaften

Stellen Sie die Geschwindigkeit, Duplex und Flusssteuerung des Aggregationsports so ein, dass sie mit den Port-Einstellungen in ►„3.1 – Porteinstellungen“ übereinstimmen.



Port: Der Name des LAG.

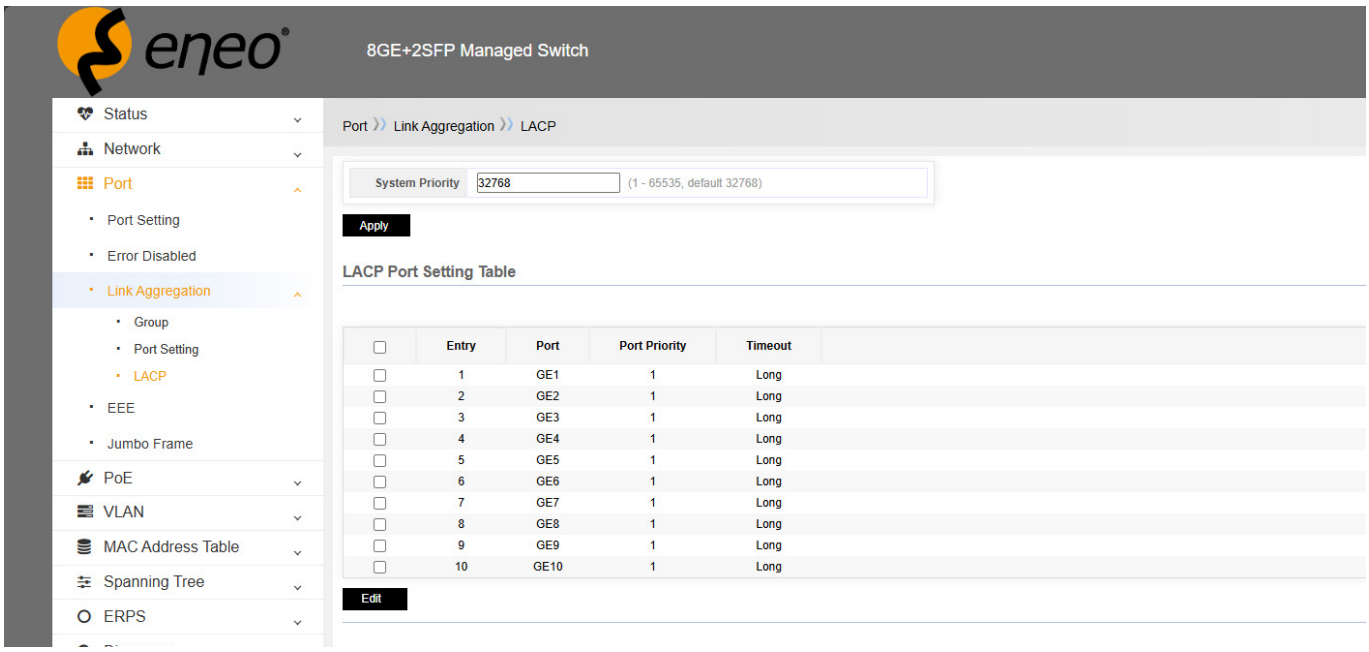
Beschreibung: Kann verwendet werden, um die Verwendung eines LAG-Ports zu beschreiben.

Status: Aktivieren oder deaktivieren. Sie können den Port deaktivieren, indem Sie den Portstatus ändern.

3.3.3 – LACP

LACP (Link Aggregation Control Protocol) ist ein branchenübliches Protokoll, das im Standard IEEE 802.3ad definiert ist. Es wird verwendet, um mehrere physische Verbindungen zu einer einzigen logischen Verbindung zusammenzufassen, die als Link Aggregation Group (LAG) oder EtherChannel bezeichnet wird. Diese Zusammenfassung trägt zur Erhöhung der Bandbreite bei und bietet Redundanz, da der Datenverkehr auf die Mitgliedsverbindungen verteilt werden kann und bei Ausfall einer Verbindung ein Failover erfolgen kann.

LACP arbeitet auf der Datenverbindungsschicht und sendet Link Aggregation Control Protocol Data Units (LACPDUs) zwischen den Geräten. Diese LACPDUs enthalten Informationen wie die LACP-Systempriorität des Geräts, die MAC-Adresse, Schnittstellenprioritäten und Schnittstellennummern. Anhand dieser Informationen verhandeln die Geräte, welche Verbindungen gebündelt werden sollen und welche für die Weiterleitung des Datenverkehrs aktiv sind.



Legen Sie die Systempriorität von LACP und Ports fest.

Der Wert ist standardmäßig konfiguriert und kann von Benutzern nach Bedarf geändert werden.

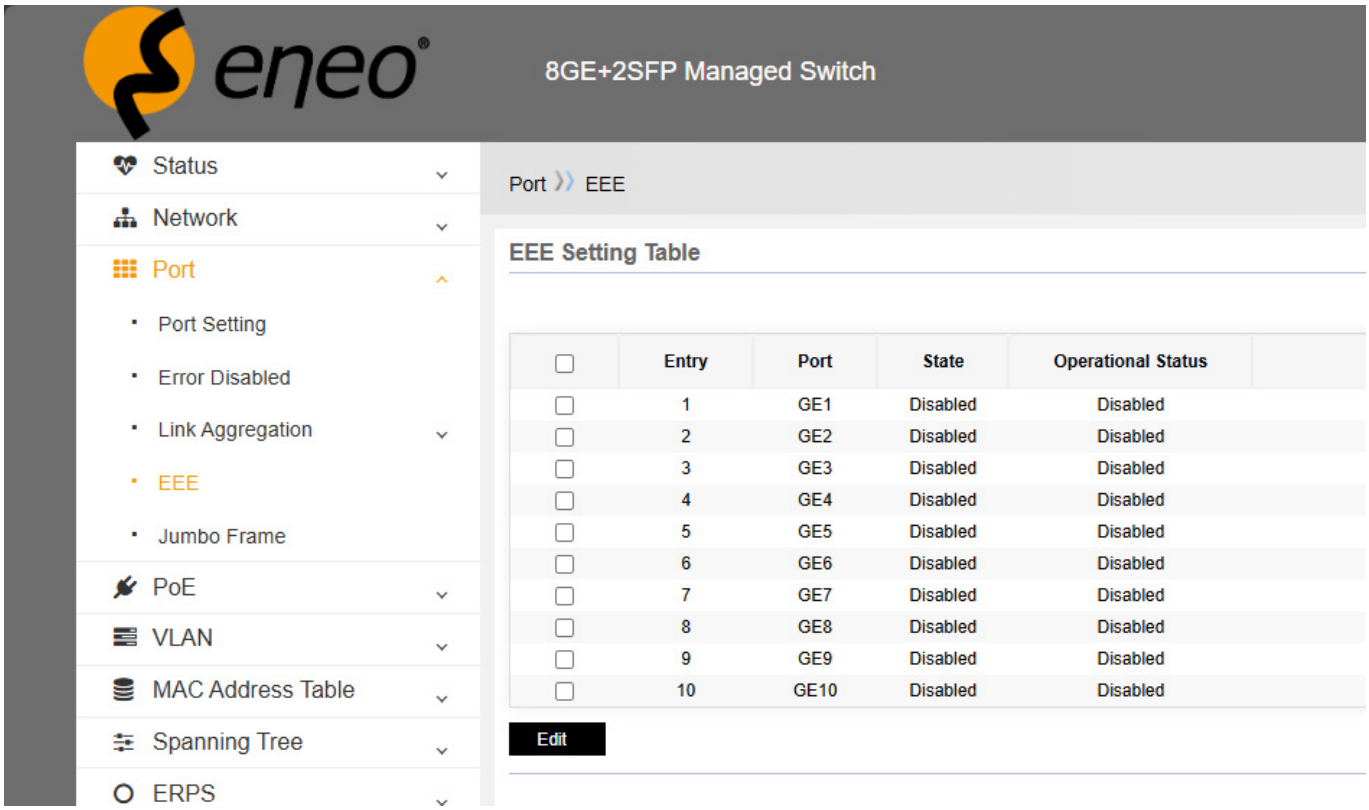
Systempriorität: Dieser Parameter gibt die LACP-Priorität an. Ein kleinerer Parameterwert bedeutet eine höhere LACP-Priorität.

Portpriorität: Dieser Parameter gibt die Priorität für den Beitritt zum LACP pro Port an. Die Priorität kann zwischen 1 und 65535 eingestellt werden, der Standardwert ist 1. Ein kleinerer Parameterwert bedeutet eine höhere Priorität.

Zeitlimit: Kann lang oder kurz eingestellt werden.

3.4 – EEE

Energieeffizientes Ethernet, kurz EEE, bezeichnet „energieeffiziente Ethernet-Technologie“ mit der Funktion, den Stromverbrauch automatisch zu reduzieren, wenn die Netzwerkkarte keinen Datenverkehr hat. Nur bei hoher Netzwerkauslastung kann die maximale Leistungsaufnahme erreicht werden.



Standardmäßig ist EEE für den Port deaktiviert. Wenn Sie diese Funktion benötigen, aktivieren Sie sie einfach für den Port.

3.5 – Jumbo Frame

Ein Jumbo-Frame ist ein Ethernet-Frame mit einer Länge von mehr als 1522 Byte.
Es handelt sich dabei um ein vom Hersteller festgelegtes Standardformat für besonders lange Frames, das speziell für Gigabit-Ethernet entwickelt wurde. Die Länge der Jumbo-Frames variiert je nach Hersteller zwischen 9000 und 64000 Byte.
Der Jumbo-Frame kann die Leistung von Gigabit-Ethernet voll ausschöpfen und die Datenübertragungseffizienz um 50 % bis 100 % verbessern. In der Anwendungsumgebung von Netzwerkspeichern hat der Jumbo-Frame eine außerordentliche Bedeutung.

Solange der Jumbo-Frame aktiviert ist, unterstützt er Übertragungsgeschwindigkeiten von bis zu 10K.

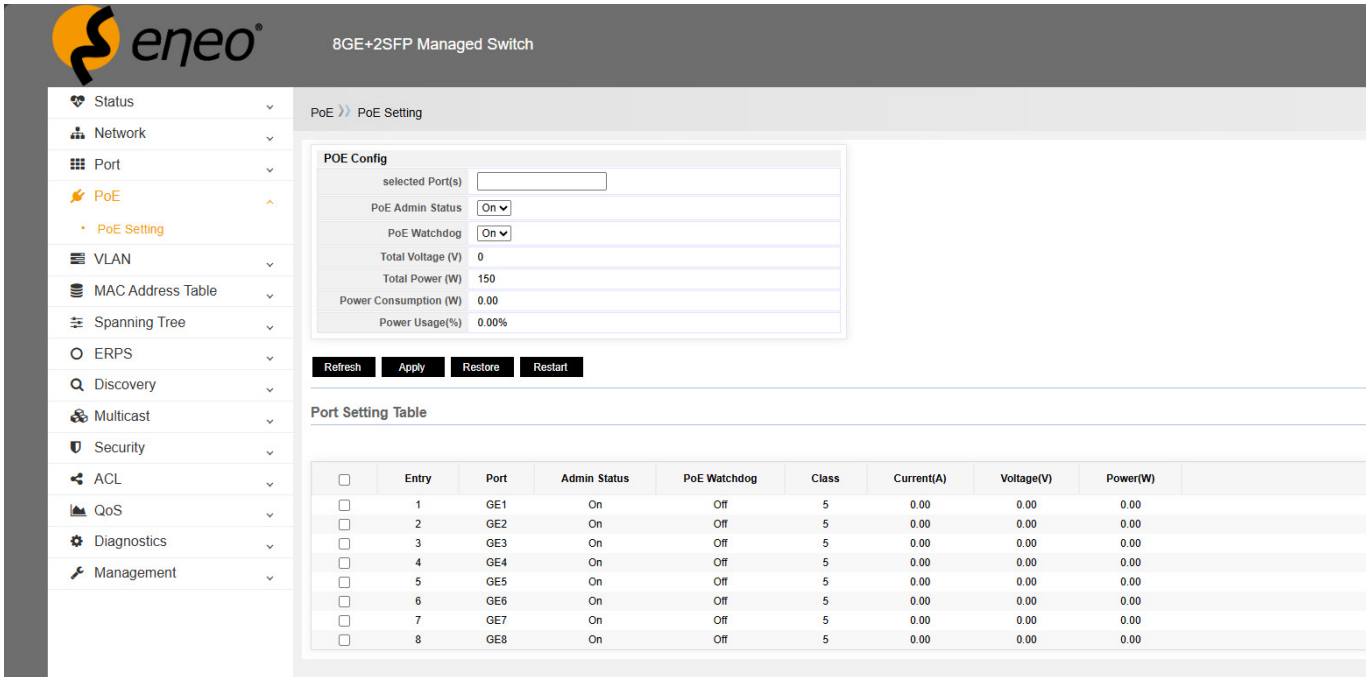
4 – POE

4.1 – PoE Konfiguration

Power over Ethernet (PoE) aktiviert ein Netzwerkgerät, um Terminals über Twisted-Pair-Kabel mit Strom zu versorgen. Das Gerät unterstützt IEEE 802.3af und IEEE 802.3at.

IEEE 802.3af: Ein Standard für Power over Ethernet (PoE), der die Übertragung von Daten und Strom über ein einziges Ethernet-Kabel ermöglicht und eine maximale Ausgangsleistung von 15,4 W pro Port zulässt.

IEEE 802.3at: Auch bekannt als PoE+ (Power over Ethernet Plus), ist ein erweiterter Standard für die Stromversorgung über Ethernet-Kabel. Er ermöglicht eine maximale Ausgangsleistung von 30 Watt pro Port vom Power Sourcing Equipment (PSE). Am Powered Device (PD) stehen mindestens 25,5 Watt zur Verfügung, wobei die Leistungsverluste über das Kabel berücksichtigt sind.



Wählen Sie im Abschnitt „Port-Konfiguration“ die Ports aus, die Sie konfigurieren möchten, und legen Sie die Parameter fest. Klicken Sie auf „Übernehmen“.

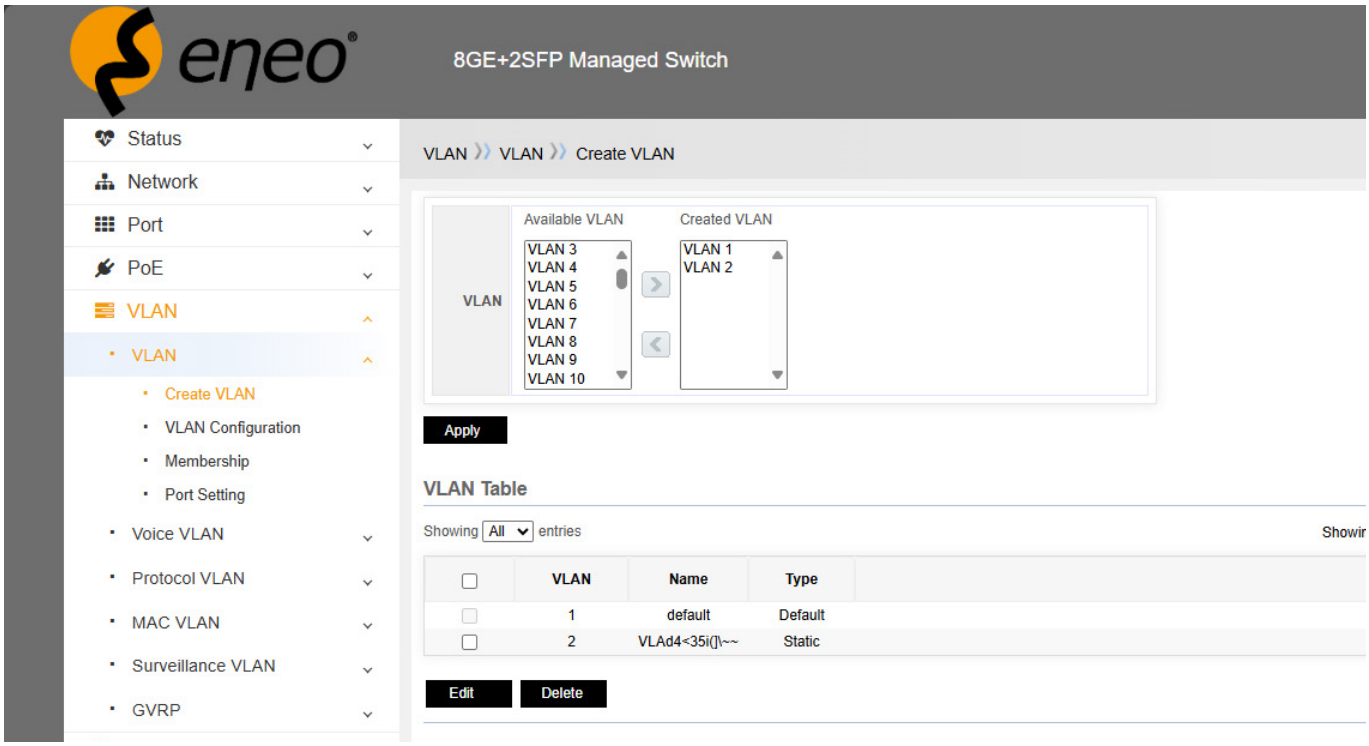
PoE-Admin-Status: Aktivieren oder deaktivieren Sie die PoE-Funktion an den entsprechenden Ports. Ein Port kann das PD mit Strom versorgen, wenn sein Status aktiviert ist.

PoE-Watchdog: Wenn die Switch-Port-Kommunikation fehlschlägt, erkennt der entsprechende Port PoE dies automatisch, startet neu, stellt die Netzwerkkommunikation selbstständig wieder her und reduziert manuelle Eingriffe und Wartungsarbeiten.

5 – VLAN

VLAN (Virtual Local Area Network) ist ein Netzwerkkonzept, das die Einrichtung mehrerer separater logischer Netzwerke innerhalb einer einzigen physischen Netzwerkinfrastruktur ermöglicht.

5.1 – VLAN erstellen



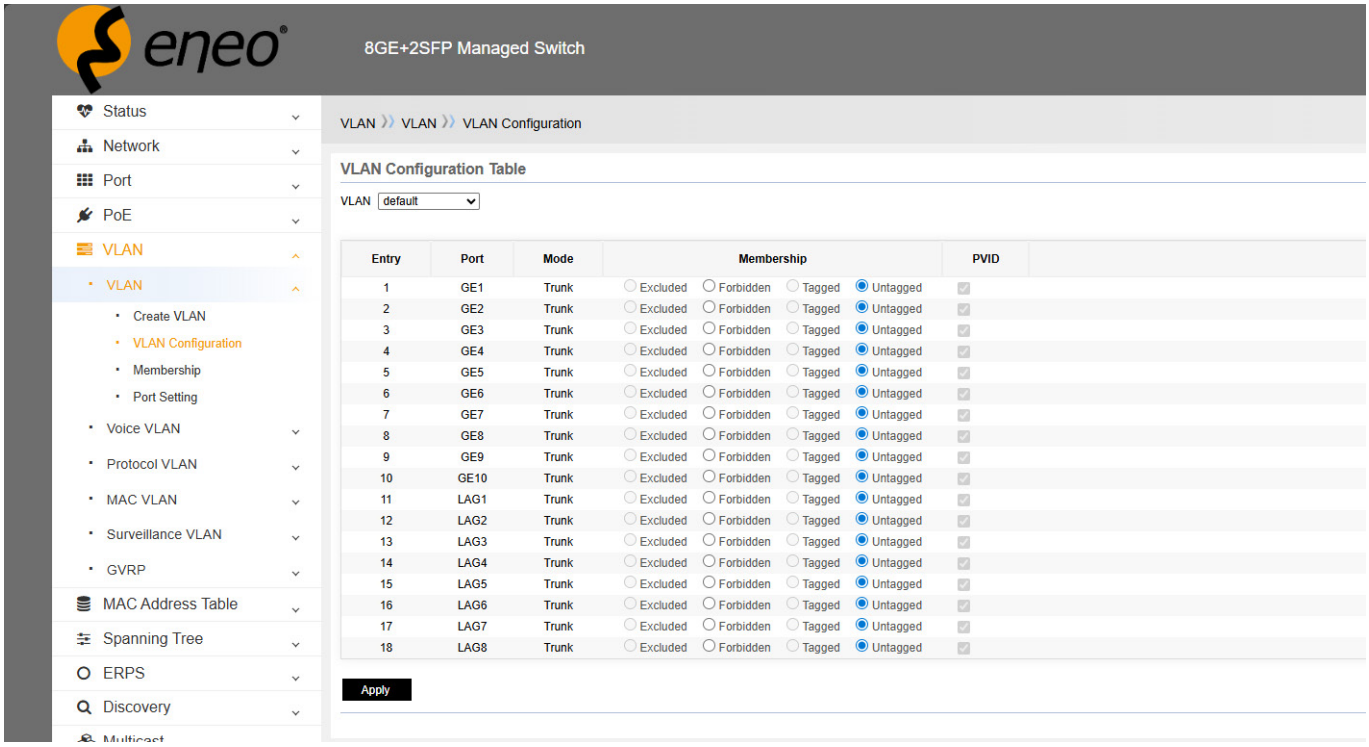
Die Gesamtzahl der VLANs beträgt 1-4094.

Wählen Sie die VLAN-Nummer im linken Feld aus und fügen Sie sie im rechten Feld hinzu, um ein VLAN zu erstellen.

VLAN 1 wird standardmäßig erstellt und kann nicht gelöscht werden. Daher ist der Typ von VLAN 1 standardmäßig „Static“ (Statisch). Sie können das VLAN bearbeiten und benennen.

5.2 – VLAN Konfiguration

Konfigurieren Sie 802.1Q_VLAN für den Switch.

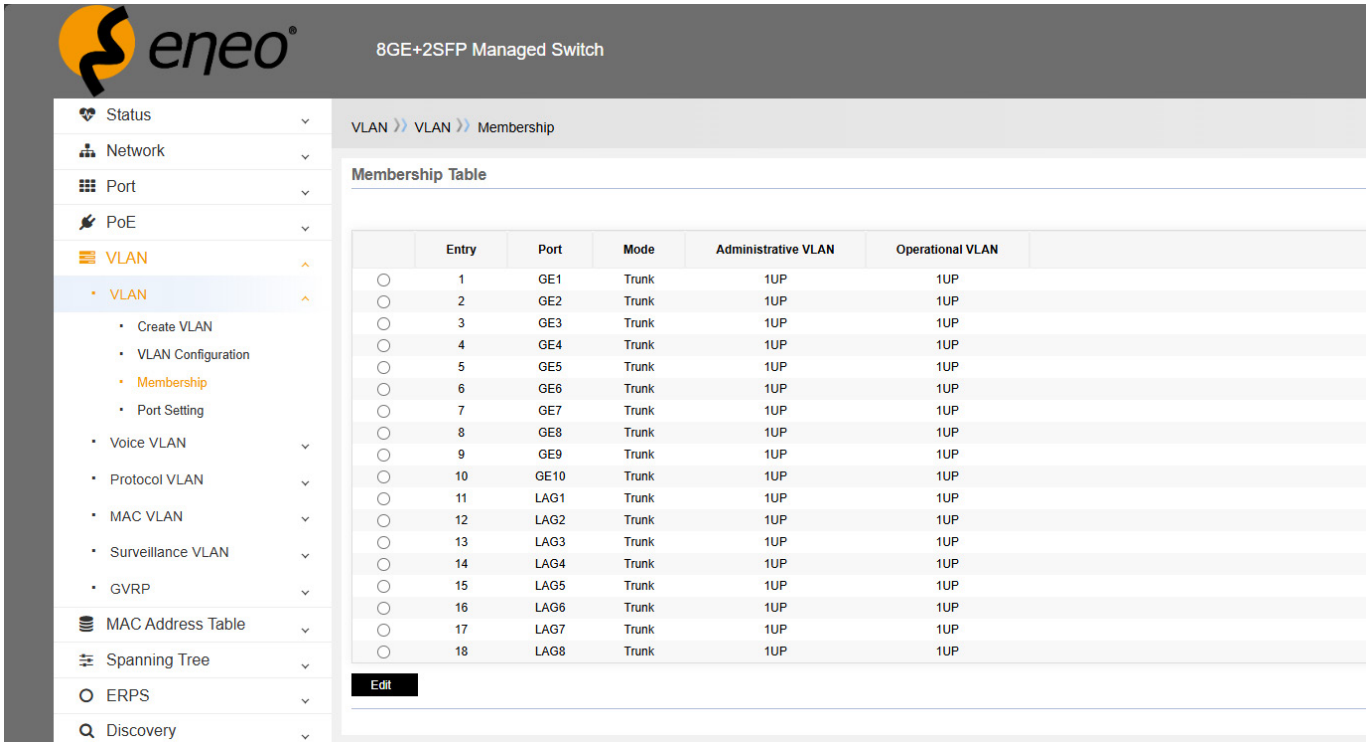


Default: Default bedeutet VLAN 1. Es ist klar, dass alle Ports zu VLAN 1 gehören und nicht getaggt sind, PVID=1.

Wenn VLAN 2 für VLAN ausgewählt ist, gibt es standardmäßig keine Mitglieder, sodass diese manuell festgelegt werden können.

5.3 – Membership

VLAN-Konfiguration des Switches.



Administratives VLAN: VLAN-Einstellung des Ports.

Operatives VLAN: Zeigt das ordnungsgemäß funktionierende VLAN an. Bei korrekten Einstellungen entspricht dies dem administrativen VLAN.

Im nächsten Abschnitt stellen wir den VLAN-Modus des Ports vor.

5.4 – Port-Einstellungen

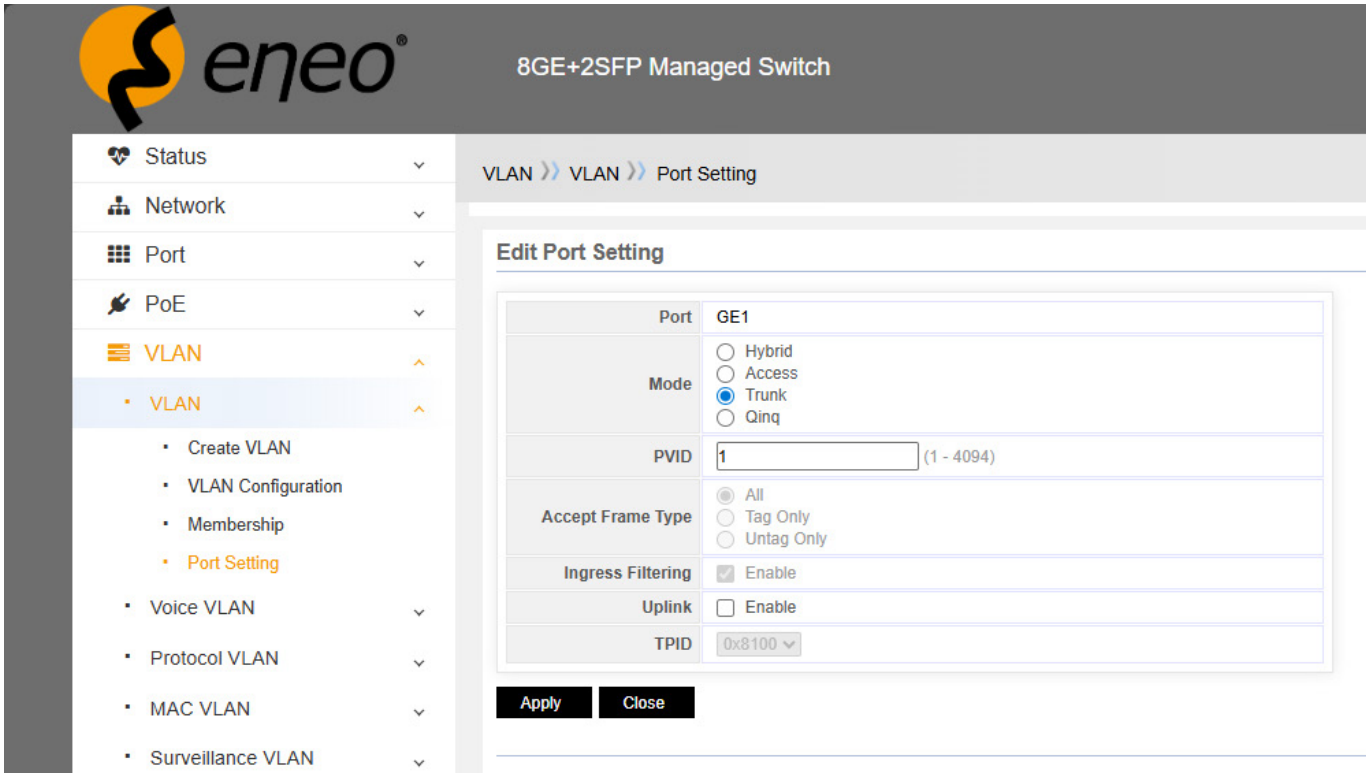
Konfigurieren Sie den Portmodus, die Eingangserfassungsfunktion und die TPID-Funktion.

Eingangserfassung: Wenn es sich bei dem Port um eine Hybridverbindung handelt, können Tag-Nachrichten, Untag-Nachrichten oder alle Nachrichten die Eingangserfassung passieren.

TPID (Tag Protocol Identifier) ist ein Feld im VLAN-Tag. Gemäß dem IEEE 802.1Q-Protokoll ist der Wert dieses Feldes 0x8100. Die Standardeinstellung des Geräts ist der im Protokoll angegebene TPID-Wert (0x8100). Einige Hersteller legen 0x9100 oder andere Werte als TPID-Wert fest, der vom Gerät erkannt werden kann.

Um mit diesen Geräten kompatibel zu sein, bietet das Gerät eine einstellbare Funktion für den TPID-Wert von globalen VLAN-VPN-Nachrichten, und Benutzer können den TPID-Wert selbst konfigurieren. Wenn der VLAN-VPN-Uplink-Port Nachrichten weiterleitet, ersetzt er den TPID-Wert im äußeren VLAN-Tag der Nachricht durch den vom Benutzer festgelegten Wert und sendet sie dann, sodass die an das öffentliche Netzwerk gesendete VLAN-VPN-Nachricht von den Geräten anderer Hersteller erkannt werden kann.

So können diese Parameter entsprechend den Kundenanforderungen konfiguriert werden.



Es gibt drei VLAN-Modi: Access, Trunk, Hybrid

- **Access:** Verbindung zu Endgeräten (wie PC, Kamera, Set-Top-Box usw.) und direkte Einstellung von PVID.
- **Trunk:** Der Port, der zwischen Switches verbunden ist. Im Allgemeinen müssen viele VLANs eingestellt werden, um eine Tagging-Funktion auszuführen.
- **Hybrid:** Gemischter Modus. Er kann Tagging für viele VLANs oder Untagging für andere VLANs ausführen.

PVID: PVID ist die Standard-VLAN-ID, die einem Port auf einem Switch zugewiesen ist. Wenn ein Switch-Port einen nicht getaggten Frame (d. h. einen Frame ohne VLAN-Tag) empfängt, weist er diesem Frame die PVID zu und platziert ihn damit effektiv im entsprechenden VLAN.

ACCEPT FRAME TYPE (FRAMETYP AKZEPTIEREN): Sie können diese Option nur auswählen, wenn Sie den Hybridmodus ausgewählt haben. Legen Sie den Frametyp so fest, dass alle Frametypen oder nur getaggte/nicht getaggte Frames akzeptiert werden.

Wie in der Abbildung oben gezeigt, legen Sie den Zugriffsmodus für Port 5 und 6 gleichzeitig fest und ändern Sie den PVID-Wert auf 5.

Achtung!

Wenn Sie den PVID-Wert festlegen, muss vor der Einstellung VLAN hinzugefügt werden. VLAN2-4 wurde in Kapitel 6.1 hinzugefügt, sodass Sie 5 einstellen können. Wenn der Wert jedoch auf 9 gesetzt ist, meldet das System einen Fehler und die Einstellung ist nicht erfolgreich.
Unter normalen Bedingungen wird weder die Eingangsdetektionsfilterung noch der TPID gesetzt. Übernehmen Sie direkt den Standardwert.

Hinweis!

Wenn Sie die Protokollinformationen kontrollieren müssen, besuchen Sie die Seite „Status-Protokollierungsmeldung".

6 – MAC-ADRESSENTABELLE

6.1 – Einführung in MAC-Adressen

6.1.1 – Einführung in die MAC-Adressentabelle

Die Hauptfunktion eines Ethernet-Switches besteht darin, Nachrichten auf der Datenverbindungsschicht weiterzuleiten, d. h. die Nachricht entsprechend der MAC-Adresse des Empfängers an den entsprechenden Port auszugeben. Die MAC-Adressweiterleitungstabelle ist eine 2-schichtige Weiterleitungstabelle, die die entsprechenden Beziehungen zwischen MAC-Adressen und Weiterleitungsports enthält. Sie ist die Grundlage für die schnelle Weiterleitung von Layer-2-Nachrichten durch den Ethernet-Switch, die wiederum die Grundlage für die schnelle Weiterleitung der oben genannten 2-Layer-Nachrichten durch den Ethernet-Switch ist. Die Einträge in der MAC-Adressweiterleitungstabelle enthalten die folgenden Informationen:

- MAC-Zieladresse
- VLAN-ID des Ports
- Weiterleitungsportnummer auf dem Gerät

Wenn der Ethernet-Switch Nachrichten weiterleitet, wendet er entsprechend den Informationen in der MAC-Adressentabelle die folgenden beiden Weiterleitungsmethoden an:

- **Unicast-Modus:** Wenn die MAC-Adressweiterleitungstabelle einen Tabelleneintrag enthält, der der MAC-Zieladresse der Nachricht entspricht, sendet der Switch die Nachricht direkt vom Weiterleitungsport des Tabelleneintrags.
- **Broadcast-Modus:** Wenn der Switch Nachrichten mit der Zieladresse F empfängt oder die MAC-Adressweiterleitungstabelle keinen Tabelleneintrag für die MAC-Adresse des Nachrichtenempfängers enthält, verwendet der Switch den Broadcast-Modus, um die Nachricht an alle Ports außer dem empfangenden Port weiterzuleiten.

6.1.2 – Einführung in den MAC-Adresslernprozess

Die Einträge in der MAC-Adressweiterleitungstabelle können auf zwei Arten aktualisiert und gepflegt werden:

- Manueller Konfigurationsmodus
- MAC-Adresslernmodus

In der Regel werden die meisten Einträge in der MAC-Adressentabelle über die MAC-Adresslernfunktion erstellt und gepflegt.

6.1.3 – Verwaltung der MAC-Adressweiterleitungstabelle

6.1.3.1 – Aging-Mechanismus der MAC-Adressweiterleitungstabelle

Die MAC-Adressweiterleitungstabelle des Ethernet-Switches hat eine begrenzte Kapazität. Um die Nutzung der Ressourcen der Adressweiterleitungstabelle zu maximieren, verwendet der Ethernet-Switch einen Alterungsmechanismus, um die MAC-Adressweiterleitungstabelle zu aktualisieren, d. h., wenn das System einen Tabelleneintrag dynamisch erstellt, schaltet es den Alterungstimer ein, und wenn es während der Alterungszeit keine MAC-Adressnachrichten von diesem Tabelleneintrag erhält, löscht der Switch diesen MAC-Adress-Tabelleneintrag.

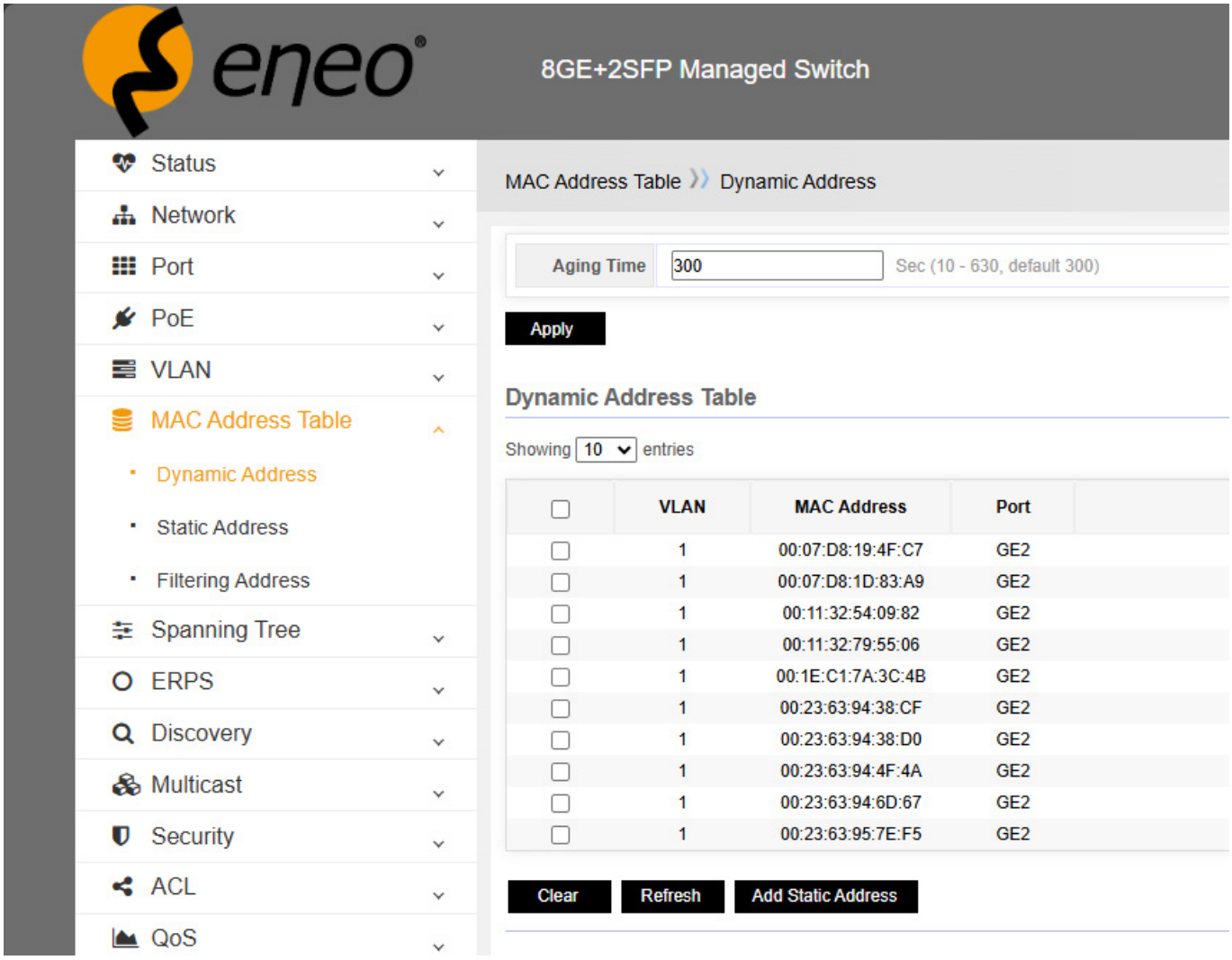
6.1.3.2 – Klassifizierung und Merkmale von MAC-Adress-Tabelleneinträgen

Je nach ihren Merkmalen und Konfigurationsmethoden lassen sich MAC-Adress-Tabelleneinträge in drei Kategorien einteilen:

- **Statischer MAC-Adress-Tabelleneintrag:** Auch als „permanente Adresse“ bezeichnet, wird manuell vom Benutzer hinzugefügt und gelöscht und altert nicht mit der Zeit. In einem Netzwerk mit wenigen Geräteänderungen kann der Broadcast-Verkehr im Netzwerk durch manuelles Hinzufügen statischer Adress-Tabelleneinträge reduziert werden.
- **Dynamischer MAC-Adress-Tabelleneintrag:** Bezieht sich auf den MAC-Adress-Tabelleneintrag, der entsprechend der vom Benutzer festgelegten Alterungszeit veraltet. Der Switch kann dynamische MAC-Adress-Tabelleneinträge über den MAC-Adress-Lernmechanismus oder durch manuelle Einrichtung durch den Benutzer hinzufügen.
- **Black Hole MAC-Adressentrierung:** Auch als „gefilterte MAC-Adressentrierung“ bezeichnet, handelt es sich hierbei um eine spezielle MAC-Adresse, die vom Benutzer manuell konfiguriert wird. Wenn der Switch eine Nachricht empfängt, deren Quell-MAC-Adresse oder Ziel-MAC-Adresse eine Black Hole MAC-Adresse ist, verwirft er diese Nachricht.

6.2 – Dynamische Adresse

Die MAC-Adresse wird von diesem Switch automatisch gelernt, und die Einträge lauten wie folgt:



MAC-Adresse: wird von diesem Switch automatisch gelernt.

Port: überträgt die gelernte MAC-Adresse an einen bestimmten Port.

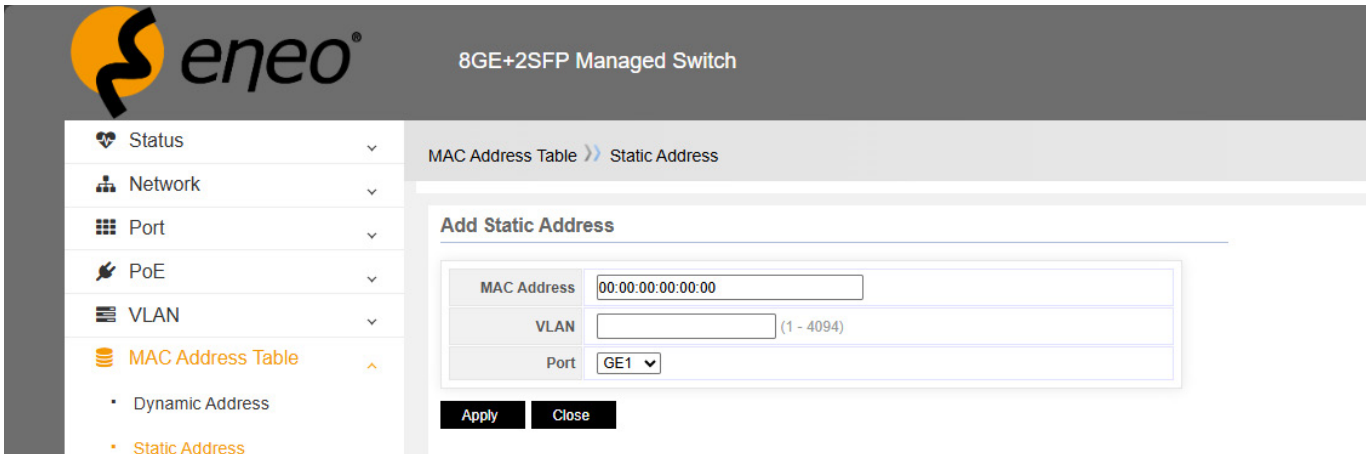
VLAN-ID (1-4094): Übertragung der erlernten MAC-Adresse an ein bestimmtes VLAN.

6.3 – Statische Adresse

6.3.1 – MAC-Adressentrierung festlegen

Je nach tatsächlicher Situation kann der Administrator die Einträge in der MAC-Adressweiterleitungstabelle manuell hinzufügen, ändern oder löschen. Er kann alle MAC-Adress-Tabelleneinträge löschen, die sich auf einen bestimmten Port beziehen, oder bestimmte Arten von MAC-Adress-Tabelleneinträgen löschen, z. B. dynamische Tabelleneinträge und statische Tabelleneinträge.

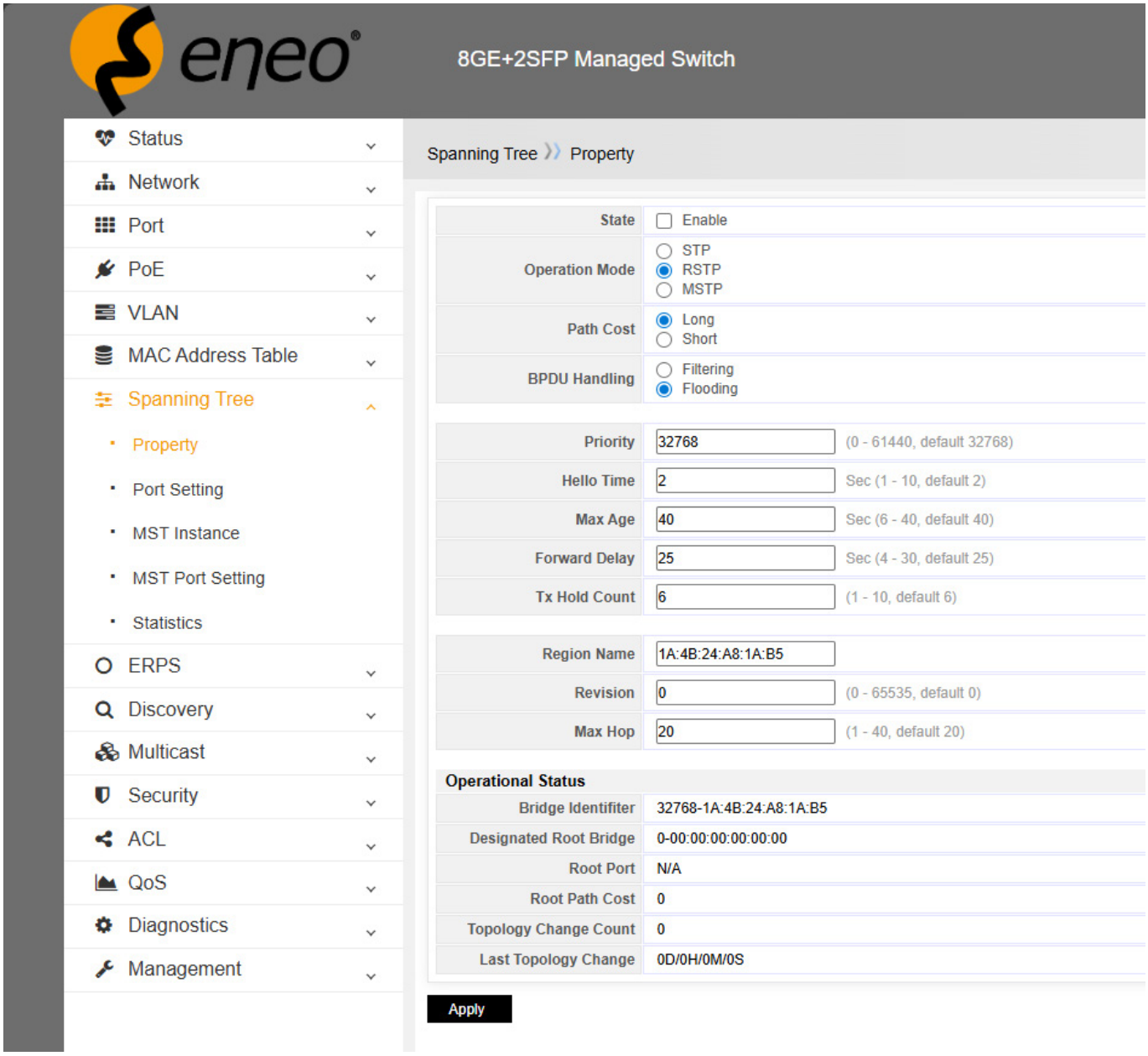
Benutzer können statische MAC-Adress-Tabelleneinträge auf der Seite hinzufügen oder löschen. Dies wird auch als MAC-Adressbindung bezeichnet, d. h. die Verknüpfung von MAC-Adresse, Port und VLAN.



Beispiel

Fügen Sie die statische MAC-Adresse 28:D2:44:80:B2:F0 manuell zum Port GE 2 hinzu.

1. Klicken Sie auf „Hinzufügen“, um das Dialogfeld zum Hinzufügen einer statischen MAC-Adresse zu öffnen.
2. Geben Sie die MAC-Adresse, die VLAN-Nummer und die zu bindende Portnummer ein.
3. Klicken Sie auf „Übernehmen“.



Die Ergebnisse der Bindungskonfiguration sind wie folgt:

1. Diese MAC-Adresse kann nur über Port GE 2 kommunizieren. Wenn diese MAC mit einem anderen Port verbunden ist, kann sie keine Nachrichten empfangen, deren Zieladresse diese MAC ist. Wenn die von diesem Switch empfangene Zieladresse die gebundene MAC-Adresse ist, leitet dieser Switch die Nachricht nur an diesen gebundenen Port weiter.
2. Nach der Konfiguration der statischen MAC-Adresse wird der ursprünglich in der dynamischen MAC vorhandene Adresseintritt gelöscht.

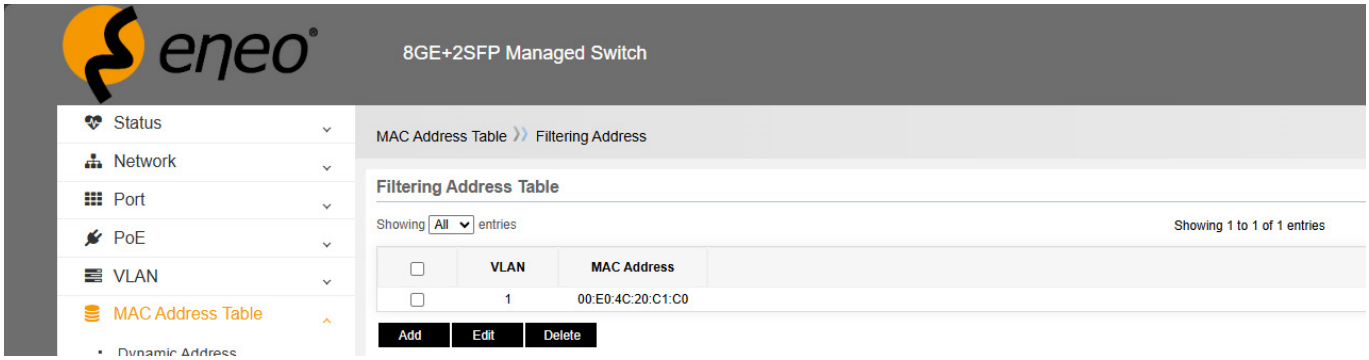
6.4 – MAC-Adressfilterung

Wenn der Eintrag für die MAC-Adressfilterung in diesem Switch festgelegt ist, wird die Nachricht mit dieser MAC-Adresse, unabhängig davon, ob sie sich in der Quell-MAC oder der Ziel-MAC befindet, verworfen, sobald der Switch sie empfängt.

Beispiel

MAC-Adressfilterung hinzufügen: 00:E0:4C:20:C1:C0

1. Klicken Sie auf „Hinzufügen“, um das Dialogfeld zum Hinzufügen einer statischen MAC-Adresse aufzurufen.
2. Geben Sie die MAC-Adresse und das zuzuordnende VLAN ein.
3. Klicken Sie auf „Übernehmen“.

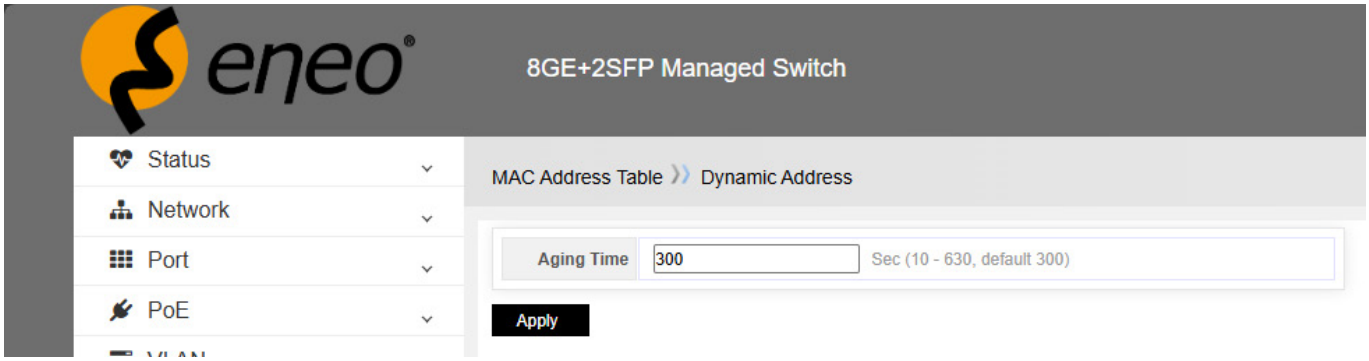


MAC-Adresse: Geben Sie die MAC-Adresse ein, die abgelehnt werden soll.

VLAN-ID (1-4094): Geben Sie das VLAN der abgelehnten MAC-Adresse ein.

6.5 – MAC-Ablaufzeit

Benutzer können die Ablaufzeit für dynamische MAC-Adress-Tabelleneinträge anpassen. Wenn die vom Benutzer konfigurierte Ablaufzeit zu lang ist, speichert das Gerät möglicherweise viele veraltete MAC-Adress-Tabelleneinträge, wodurch die Ressourcen der MAC-Adress-Tabelle erschöpft werden und das Gerät die MAC-Adress-Tabelle nicht mehr entsprechend den Änderungen im Netzwerk aktualisieren kann. Wenn die vom Benutzer konfigurierte Alterungszeit zu kurz ist, löscht das Gerät möglicherweise die gültigen MAC-Adresseneinträge, was dazu führen kann, dass das Gerät eine große Anzahl von Datenpaketen sendet und die Leistung beeinträchtigt wird. Daher müssen Benutzer eine der tatsächlichen Situation entsprechende Alterungszeit konfigurieren, um die MAC-Adressalterungsfunktion effektiv zu nutzen.



Geben Sie die Alterungszeit ein und klicken Sie auf „Übernehmen“.

Die Alterungszeit der dynamischen MAC-Adressentabelle gilt für alle Ports, und die Adressalterung funktioniert nur für dynamische (vom Gerät gelernte oder vom Benutzer dynamisch konfigurierte) Einträge in der MAC-Adressentabelle.

7 – SPANNING TREE PROTOCOL

7.1 – Einführung in STP

7.1.1 – Anwendung von STP

STP (Spanning Tree Protocol) ist ein Protokoll basierend auf dem IEEE 802.1D-Standard, das zur Beseitigung physischer Schleifen auf der Datenverbindungsschicht in LANs verwendet wird. Die Geräte, auf denen dieses Protokoll ausgeführt wird, finden durch gegenseitige Informationen Schleifen im Netzwerk und blockieren selektiv einige Ports. Schließlich wird die Schleifenstruktur des Netzwerks zu einer baumartigen Netzwerkstruktur ohne Schleifen reduziert, um eine kontinuierliche Ausbreitung und endlose Zirkulation von Nachrichten im Schleifennetzwerk zu verhindern und eine Verringerung der Paketverarbeitungskapazität durch wiederholtes Empfangen derselben Nachrichten zu vermeiden.

STP hat zwei Bedeutungen. Im engeren Sinne bezieht sich STP auf das in IEEE 802.1D definierte STP-Protokoll, im weiteren Sinne auf das in IEEE 802.1D definierte STP-Protokoll und verschiedene darauf basierende verbesserte Spanning-Tree-Protokolle.

7.1.2 – STP-Protokollnachrichten

Die Protokollnachricht in STP ist BPDU (Bridge Protocol Data Unit), auch als Konfigurationsnachricht bekannt.

STP kann die Netzwerktopologie durch die Übertragung von BPDUs zwischen Geräten bestimmen. BPDUs enthalten genügend Informationen, um sicherzustellen, dass das Gerät den Berechnungsprozess des Spanning Tree abschließen kann.

BPDU kann im STP-Protokoll in zwei Typen unterteilt werden

- **Konfigurations-BPDU:** Eine Nachricht, die zur Berechnung des Spanning Tree und zur Aufrechterhaltung der Spanning-Tree-Topologie verwendet wird.
- **TCN-BPDU** (Topology Change Notification BPDU): Wenn sich die Topologie ändert, wird diese Nachricht verwendet, um die mit der Netzwerk-Topologie verbundenen Geräte über die Änderungen zu informieren.

7.2 – Grundkonzept von STP

7.2.1 – Root Bridge

Die Baumstruktur eines Netzwerks muss eine Wurzel haben, daher führt STP das Konzept der Root Bridge ein. Es gibt nur eine Root Bridge im gesamten Netzwerk, und die Root Bridge ändert sich mit der Netzwerktopologie, sodass die Root Bridge nicht fest ist.
Nachdem das Netzwerk konvergiert ist, generiert die Root Bridge in bestimmten Zeitintervallen die konfigurierte BPDU und sendet sie. Andere Geräte übertragen die konfigurierte BPDU, um die Stabilität der Topologie sicherzustellen.

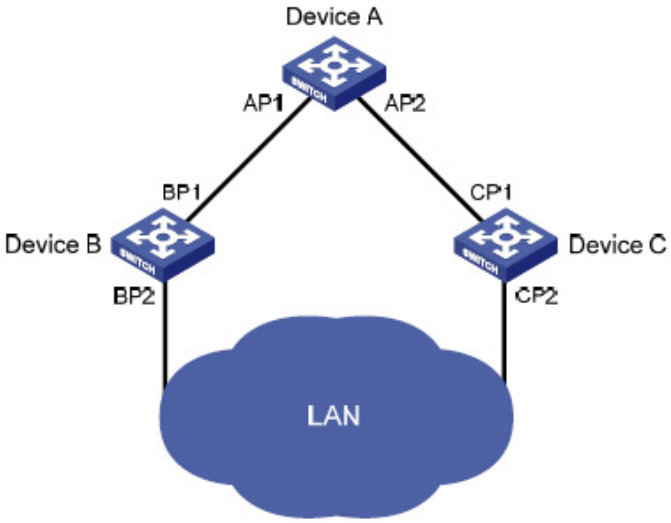
7.2.2 – Root-Port

Der Root-Port ist der Port, der auf einem Nicht-Root-Bridge-Gerät am nächsten zur Root-Bridge liegt. Der Root-Port ist für die Kommunikation mit der Root-Bridge verantwortlich. Auf einem Nicht-Root-Bridge-Gerät gibt es nur einen Root-Port. Auf der Root-Bridge gibt es keinen Root-Port.

7.2.3 – Spezifizierte Bridge und spezifizierter Port

Die Definitionen von spezifizierter Bridge und spezifiziertem Port finden Sie in dieser Tabelle.

Type	Spezifizierte Bridge	Spezifizierter Port
Für ein Gerät	Dieses Gerät ist direkt mit dem lokalen Rechner verbunden und für die Übertragung von Konfigurationsmeldungen an den lokalen Rechner zuständig.	Dieser Port überträgt Konfigurationsmeldungen von der angegebenen Bridge an den lokalen Rechner.
Für LAN	Dieses Gerät ist für die Übertragung von Konfigurationsmeldungen an das lokale Segment zuständig.	Dieser Port überträgt Konfigurationsmeldungen von der angegebenen Bridge an den lokalen Rechner.



Die Abbildung zeigt die angegebene Bridge und den angegebenen Port, wobei AP1, AP2, BP1, BP2, CP1 und CP2 jeweils die Ports von Gerät A, Gerät B und Gerät C sind.

- Wenn Gerät A Konfigurationsnachrichten über Port AP1 an Gerät B sendet, ist die angegebene Bridge von Gerät B Gerät A und der angegebene Port ist AP1.
- Es sind zwei Geräte mit dem LAN verbunden: Gerät B und Gerät C. Wenn Gerät B für die Übertragung von Konfigurationsnachrichten an das LAN zuständig ist, ist die angegebene Bridge des LANs Gerät B und der angegebene Port ist BP2.

7.2.4 – Pfadkosten

Pfadkosten sind der Referenzwert des STP-Protokolls für die Verbindungsauswahl. STP berechnet die Pfadkosten, um die stärkere Verbindung auszuwählen und die redundante Verbindung zu blockieren, sodass das Netzwerk zu einer Baumstruktur ohne Schleifen reduziert wird.

7.3 – Grundprinzip von STP

STP kann die Netzwerktopologie durch die Übertragung von BPDUs zwischen Geräten bestimmen. Die Konfigurationsnachrichten enthalten genügend Informationen, um sicherzustellen, dass das Gerät den Berechnungsprozess zur Erstellung von Bäumen abschließen kann, darunter mehrere wichtige Informationen wie folgt:

- Root Bridge ID: besteht aus der Priorität und der MAC-Adresse der Root Bridge;
- Root Path Cost: Pfadkosten zum Erreichen der Root Bridge;
- Spezifizierte Bridge-ID: Sie besteht aus der Priorität und der MAC-Adresse der spezifizierten Bridge.
- Spezifizierte Port-ID: Sie besteht aus der Priorität und dem Portnamen des spezifizierten Ports.
- Lebensdauer der Konfigurationsnachrichten, die im Netzwerk verbreitet werden: Nachrichtenalter.
- Maximale Lebensdauer der im Gerät gespeicherten Konfigurationsnachrichten: Max. Alter.
- Zyklus der Übertragung von Konfigurationsnachrichten: Hello-Zeit;
- Verzögerung der Port-Statusmigration: Weiterleitungsverzögerung.

7.3.1 – Spezifischer Prozess der STP-Algorithmusimplementierung

- Ausgangszustand

  Zu Beginn generiert jeder Port jedes Geräts eine Konfigurationsnachricht, wobei er sich selbst als Root-Bridge betrachtet. Die Root-Pfadkosten betragen 0. Die angegebene Bridge-ID ist die eigene Geräte-ID und der angegebene Port ist der eigene Port.

- Auswahl der optimalen Konfigurationsnachricht

  Jedes Gerät sendet seine eigenen Konfigurationsnachrichten nach außen und empfängt die von anderen Geräten gesendeten Konfigurationsnachrichten.
  Der Auswahlprozess der optimalen Konfigurationsnachricht ist in der folgenden Tabelle dargestellt.

Schritt	Inhalt
1	Nach Erhalt der Konfigurationsnachricht läuft jeder Port wie folgt ab: • Wenn die Priorität der vom Port empfangenen Konfigurationsnachricht niedriger ist als die der Portkonfigurationsnachricht, verwirft das Gerät die empfangene Konfigurationsnachricht ohne weitere Verarbeitung. • Wenn die Priorität der vom Port empfangenen Konfigurationsnachricht höher ist als die des Ports, ersetzt das Gerät den Inhalt der Portkonfigurationsnachricht durch die empfangene Konfigurationsnachricht.
2	Das Gerät vergleicht die Konfigurationsmeldungen aller Ports, um den optimalen auszuwählen.

7.3.1.1 – Auswahl einer Root-Bridge

Während der Netzwerkinitialisierung betrachten sich alle STP-Geräte im Netzwerk als „Root-Bridge", wobei die Root-Bridge-ID ihrer eigenen Geräte-ID entspricht. Durch den Austausch von Konfigurationsmeldungen werden die Root-Bridge-IDs zwischen den Geräten verglichen und das Gerät mit der kleinsten Root-Bridge-ID im Netzwerk wird als Root-Bridge ausgewählt.

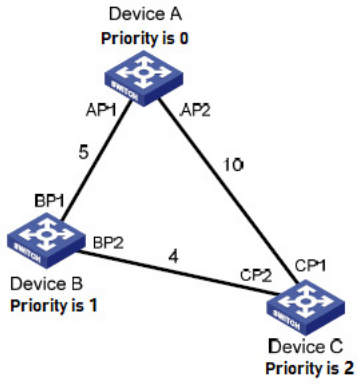
7.3.1.2 – Auswahl eines Root-Ports und eines Designated Port

Der Auswahlprozess für Root-Ports und Designated Ports ist in der folgenden Tabelle dargestellt.

Schritt	Inhalt
1	Das Nicht-Root-Bridge-Gerät legt den Port, der die optimale Konfigurationsmeldung empfängt, als Root-Port fest.
2	Entsprechend der Konfigurationsmeldung und dem Pfad-Overhead des Root-Ports berechnet das Gerät für jeden Port eine bestimmte Port-Konfigurationsmeldung: • Ersetzen Sie die Root-Bridge-ID durch die Root-Bridge-ID in der Konfigurationsmeldung des Root-Ports. • Ersetzen Sie den Root-Pfad-Overhead durch den Root-Pfad-Overhead der Root-Port-Konfigurationsnachricht plus den Pfad-Overhead, der dem Root-Port entspricht. • Ersetzen Sie die festgelegte Bridge-ID durch die eigene Geräte-ID. • Ersetzen Sie die festgelegte Port-ID durch die eigene Port-ID.
3	Das Gerät vergleicht die berechneten Konfigurationsmeldungen mit den Konfigurationsmeldungen an dem Port, dessen Rolle bestimmt werden muss, und wählt auf der Grundlage der Vergleichsergebnisse unterschiedliche Verarbeitungsmethoden: • Wenn die berechnete Konfigurationsmeldung überlegen ist, legt das Gerät den Port als den vorgesehenen Port fest, und die Konfigurationsmeldung an diesem Port wird durch die berechnete Konfigurationsmeldung ersetzt und regelmäßig gesendet. • Wenn die Konfigurationsmeldung am Port überlegen ist, aktualisiert das Gerät die Konfigurationsmeldung dieses Ports nicht und blockiert ihn. Der Port leitet keine Daten mehr weiter, sondern empfängt nur noch die Konfigurationsmeldung, ohne sie zu senden.

Sobald die Root-Bridge, der Root-Port und der angegebene Port erfolgreich ausgewählt wurden, wird die gesamte Baumtopologie aufgebaut.

Das folgende Beispiel veranschaulicht den Berechnungsprozess des STP-Algorithmus. Die Priorität von Gerät A ist 0, die von Gerät B ist 1 und die von Gerät C ist 2. Der Pfad-Overhead aller Verbindungen beträgt 5, 10 bzw. 4.



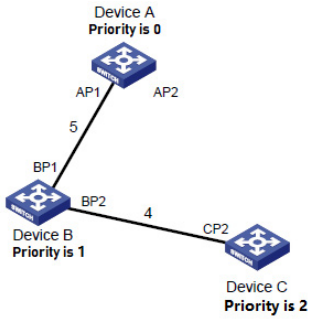
Gerät	Portname	Port-Konfigurationsmeldung
Gerät A	AP1	{0, 0, 0, AP1}
	AP2	{0, 0, 0, AP2}
Gerät B	BP1	{1, 0, 1, BP1}
	BP2	{1, 0, 1, BP2}
Gerät C	CP1	{2, 0, 2, CP1}
	CP2	{2, 0, 2, CP1}

7.3.1.3 – Vergleichsverfahren und Ergebnisse aller Geräte

Gerät	Vergleichsprozess	Port-Konfigurationsmeldung nach Vergleich
Gerät A	• Port AP1 empfängt die Konfigurationsnachricht {1, 0, 1, BP1} von Gerät B. Gerät A stellt fest, dass diese Portkonfigurationsnachricht {0, 0, 0, AP1} der empfangenen Konfigurationsnachricht übergeordnet ist, und verwirft daher die empfangene Nachricht. • Port AP2 empfängt die Konfigurationsnachricht {2, 0, 2, CP1} von Gerät C. Gerät A stellt fest, dass diese Portkonfigurationsnachricht {0, 0, 0, AP1} der empfangenen Konfigurationsnachricht übergeordnet ist, und verwirft daher die empfangene Nachricht. • Wenn Gerät A feststellt, dass die Root-Bridge und die designierte Bridge in der Konfigurationsmeldung seiner eigenen Ports enthalten sind, betrachtet es sich selbst als Root-Bridge, ohne die Konfigurationsmeldungen aller Ports zu ändern, und sendet dann regelmäßig Konfigurationsmeldungen nach außen.	AP1: {0, 0, 0, AP1} AP2: {0, 0, 0, AP2}
Gerät B	• Port BP1 empfängt die Konfigurationsmeldung {0, 0, 0, AP1} von Gerät A. Gerät B stellt fest, dass die empfangene Konfigurationsmeldung besser ist als seine eigene Konfigurationsmeldung {1, 0, 1, BP1} für diesen Port, und aktualisiert daher die Konfigurationsmeldung von Port BP1. • Port BP2 empfängt die Konfigurationsmeldung {2, 0, 2, CP2} von Gerät C. Gerät B stellt fest, dass die Konfigurationsmeldung {1, 0, 1, BP2} dieses Ports besser ist als die empfangene Konfigurationsmeldung, und verwirft daher die empfangene Konfigurationsmeldung.	BP1: {0, 0, 0, AP1} BP2: {1, 0, 1, BP2}
	• Gerät B vergleicht die Konfigurationsmeldungen aller Ports und wählt die Konfigurationsmeldung von Port BP1 als die optimale aus. Anschließend legt es Port BP1 als Root-Port fest, ohne dessen Konfigurationsmeldung zu ändern. • Gerät B berechnet auf der Grundlage der Konfigurationsmeldung und des Pfad-Overheads 5 des Root-Ports BP eine bestimmte Port-Konfigurationsmeldung {0, 5, 1, BP2} für den Port BP2. • Gerät B vergleicht die berechnete Konfigurationsmeldung {0, 5, 1, BP2} mit der Konfigurationsmeldung am Port BP2. Das Vergleichsergebnis ist, dass die berechnete Konfigurationsmeldung besser ist, sodass Gerät B den Port BP2 als den bestimmten Port festlegt und dessen Konfigurationsmeldung durch die berechnete ersetzt und regelmäßig nach außen gesendet wird.	Root-Port BP1: {0, 0, 0, AP1} Designierter Port BP2: {0, 5, 1, BP2}
Gerät C	• Wenn Port CP1 die Konfigurationsmeldung {0, 0, 0, AP2} von Gerät A empfängt, stellt Gerät C fest, dass die empfangene Konfigurationsmeldung besser ist als die Konfigurationsmeldung {2, 0, 2, CP1} dieses Ports, sodass es die Konfigurationsmeldung von Port CP1 aktualisiert. • Port CP2 empfängt vor der Aktualisierung die Konfigurationsmeldung {1, 0, 1, bp2} von BP2 von Gerät B. Gerät C stellt fest, dass die empfangene Konfigurationsmeldung besser ist als die Konfigurationsmeldung {2, 0, 2, CP2} dieses Ports, und aktualisiert daher die Konfigurationsmeldung von Port CP2.	CP1: {0, 0, 0, AP2} CP2: {1, 0, 1, BP2}
	Nach dem Vergleich: • Die Konfigurationsmeldung von Port CP1 wird als optimale Konfigurationsmeldung ausgewählt, und Port CP1 wird ohne Änderung seiner Konfigurationsmeldung als Root-Port festgelegt. • Nach dem Vergleich der berechneten Konfigurationsmeldung {0, 10, 2, CP2} des festgelegten Ports mit der Konfigurationsmeldung von Port CP2 wird Port CP2 in den festgelegten Port umgewandelt und seine Konfigurationsmeldung durch die berechnete Konfigurationsmeldung ersetzt.	Root-Port CP1: {0, 0, 0, AP2} Designierter Port CP2: {0, 10, 2, CP2}

Gerät	Vergleichsprozess	Port-Konfigurationsmeldung nach Vergleich
Gerät C	• Dann empfängt Port CP2 die aktualisierte Konfigurationsmeldung {0, 5, 1, bp2} von Gerät B. Da die empfangene Konfigurationsmeldung besser ist als die ursprüngliche, löst Gerät C den Aktualisierungsprozess aus. • Gleichzeitig empfängt Port CP1 die von Gerät A regelmäßig gesendete Konfigurationsmeldung. Nach dem Vergleich löst Gerät C den Aktualisierungsprozess nicht aus.	CP1: {0, 0, 0, AP2} CP2: {0, 5, 1, BP2}
	Nach dem Vergleich: • Der Root-Pfad-Overhead 9 von Port CP2 (Root-Pfad-Overhead 5 der Konfigurationsnachricht + Pfad-Overhead 4 von Port CP2) ist kleiner als der Root-Pfad-Overhead 10 von Port CP1 (Root-Pfad-Overhead 0 der Konfigurationsnachricht + Pfad-Overhead 10 von Port CP1), daher wird die Konfigurationsnachricht von Port CP2 als optimale ausgewählt und Port CP2 wird ohne Änderung seiner Konfigurationsnachricht als Root-Port festgelegt. • Nach dem Vergleich der Konfigurationsnachricht von Port CP1 mit der berechneten Konfigurationsnachricht des festgelegten Ports wird Port CP1 ohne Änderung seiner Portkonfigurationsnachricht gesperrt und empfängt keine von Gerät A weitergeleiteten Daten, bis eine neue Bedingung die Berechnung des Spanning Tree auslöst, z. B. wenn die Verbindung von Gerät B zu Gerät C unterbrochen ist.	Blockierter Port CP1: {0, 0, 0, AP2} Root-Port CP2: {0, 5, 1, BP2}

Nach dem Vergleich in der obigen Tabelle wird ein Spanning Tree gebildet, der Gerät A als Root Bridge verwendet.



7.3.2 – Übertragungsmechanismus der SPT-Konfigurationsnachricht

- Bei der Initialisierung des Netzwerks betrachten alle Geräte sich selbst als Root-Bridge und generieren Konfigurationsnachrichten, in denen sie sich selbst als Root angeben, um diese in regelmäßigen Abständen mit der Hello Time zu versenden.
- Wenn der Port, der die Konfigurationsnachricht empfängt, der Root-Port ist und die empfangene Konfigurationsnachricht besser ist als die des Ports, erhöht das Gerät die Message Age in der Konfigurationsnachricht nach bestimmten Regeln, startet einen Timer, um die Zeit für die Konfigurationsnachricht zu berechnen, und leitet sie vom festgelegten Port des Geräts weiter.
- Wenn die Priorität der vom vorgesehenen Port empfangenen Konfigurationsnachricht niedriger ist als die des Ports, sendet dieser sofort seine eigene bessere Konfigurationsnachricht als Antwort.
- Wenn ein Pfad ausfällt, empfängt der Root-Port auf diesem Pfad keine neuen Konfigurationsnachrichten mehr, und die alten werden aufgrund einer Zeitüberschreitung verworfen. Das Gerät generiert die Konfigurationsnachricht neu, wobei es sich selbst als Root verwendet, und sendet sie nach außen, wodurch eine Neuberechnung des Spanning Tree erfolgt, um einen neuen Pfad zu erhalten, der die ausgefallene Verbindung ersetzt und das Netzwerk wiederherstellt.

Die neu berechnete Konfigurationsmeldung wird jedoch nicht sofort an das gesamte Netzwerk übertragen, sodass der alte Root-Port und der designierte Port weiterhin Daten über den ursprünglichen Pfad weiterleiten, da sie die Änderung in der Netzwerktopologie nicht erkennen. Wenn der neu ausgewählte Root-Port und der designierte Port sofort mit der Weiterleitung von Daten beginnen, kann dies zu einer vorübergehenden Schleife führen.

7.3.3 – STP-Timer

Bei der STP-Berechnung müssen drei wichtige Zeitparameter verwendet werden: Vorwärtsverzögerung, Hello Timeund Max Age.

- Die Vorwärtsverzögerung bezieht sich auf die Verzögerungszeit der Gerätezustandsmigration. Ein Verbindungsausfall führt dazu, dass das Netzwerk den Spanning Tree neu berechnet und seine Struktur entsprechend ändert. Die neu berechnete Konfigurationsmeldung wird jedoch nicht sofort an das gesamte Netzwerk übertragen. Wenn der neu ausgewählte Root-Port und der designierte Port sofort mit der Weiterleitung von Daten beginnen, kann dies zu einer vorübergehenden Schleife führen. Aus diesem Grund verwendet STP einen Mechanismus zur Zustandsänderung. Der neu ausgewählte Root-Port und der designierte Port können Daten erst nach zweimaliger Vorwärtsverzögerung weiterleiten, wodurch sichergestellt wird, dass die neue Konfigurationsmeldung im gesamten Netzwerk übertragen wurde.
- Die Hello Time wird verwendet, um zu erfassen, ob eine Verbindung zum Gerät besteht. In jedem Hello-Zeitintervall sendet das Gerät eine Hello-Nachricht an die umliegenden Geräte, um zu bestätigen, ob die Verbindung besteht.
- Der Parameter „Max Age“ wird verwendet, um zu bestimmen, ob die Speicherdauer von Konfigurationsnachrichten im Gerät „abgelaufen“ ist. Das Gerät verwirft die abgelaufenen Konfigurationsnachrichten.

7.4 – MSTP Einführung

7.4.1 – MSTP-Hintergrund

7.4.1.1 – Mängel von STP und RSTP

STP kann nicht schnell migrieren. Selbst bei einer Punkt-zu-Punkt-Verbindung oder einem Edge-Port (d. h. dieser Port ist direkt mit dem Benutzerendgerät verbunden, ohne Verbindung zu anderen Geräten oder einem gemeinsamen Netzwerksegment) muss er zweimal die Vorwärtsverzögerungszeit abwarten, bevor er in den Weiterleitungszustand migriert.

RSTP (Rapid Spanning Tree Protocol) ist eine optimierte Version des STP-Protokolls, bei der „schnell" bedeutet, dass bei der Auswahl eines Ports als Root-Port und Designated Port die Verzögerungszeit für das Eintragen in den Weiterleitungszustand unter bestimmten Bedingungen erheblich verkürzt wird, um die Zeit zu verkürzen, die das Netzwerk benötigt, um die endgültige topologische Stabilität zu erreichen.

- In RSTP ist die Bedingung für den schnellen Wechsel des Root-Port-Status, dass der alte Root-Port auf diesem Gerät die Weiterleitung von Daten eingestellt hat und der vorgelagerte designierte Port mit der Weiterleitung von Daten begonnen hat.
- In RSTP ist die Bedingung für den schnellen Wechsel des Status des designierten Ports, dass der designierte Port ein Edge-Port oder ein designierter Port ist, der mit der Punkt-zu-Punkt-Verbindung verbunden ist. Wenn der designierte Port ein Edge-Port ist, kann dieser Port direkt in den Weiterleitungsstatus eintreten; wenn der designierte Port mit einer Punkt-zu-Punkt-Verbindung verbunden ist, kann dieses Gerät eine Verbindung mit dem nachgeschalteten Gerät herstellen und sofort nach Empfang der Antwort in den Weiterleitungsstatus eintreten.

RSTP kann schnell konvergieren, weist jedoch ähnliche Mängel wie STP auf: Alle Bridges im LAN teilen sich einen Spanning Tree, sodass redundante Verbindungen nicht gemäß VLAN blockiert werden können und alle VLAN-Pakete entlang eines Spanning Tree weitergeleitet werden.

7.4.1.2 – Merkmale von MSTP

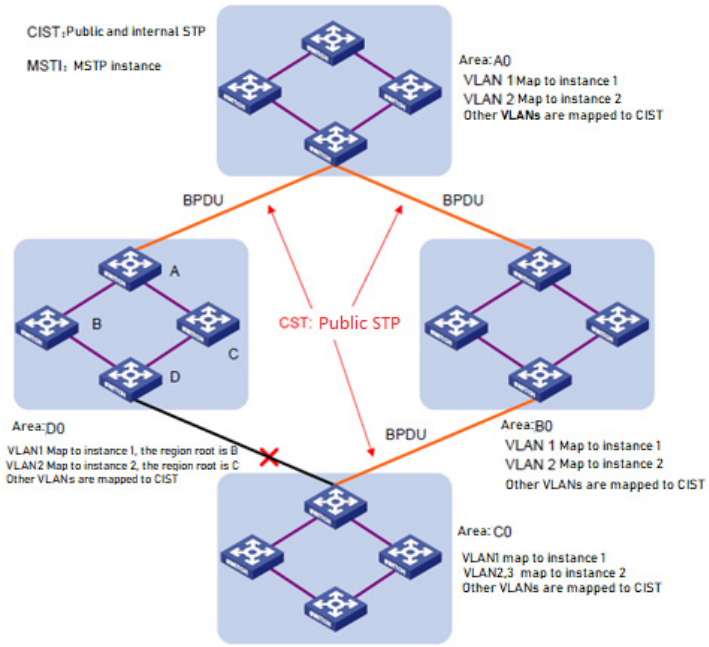
MSTP (Multiple Spanning Tree Protocol) kann die Mängel von STP und RSTP ausgleichen. Es kann schnell konvergieren und den Datenverkehr in verschiedenen VLANs über ihre eigenen Pfade weiterleiten, wodurch ein besserer Lastverteilungsmechanismus für redundante Verbindungen bereitgestellt wird. Informationen zur Einführung von VLAN finden Sie unter „VLAN-Konfiguration" im Abschnitt „Zugriffsvolumen".

- MSTP kann eine VLAN-Zuordnungstabelle (eine Tabelle mit den entsprechenden Beziehungen zwischen VLAN und Spanning Tree) festlegen, um VLAN und Spanning Tree zu verbinden. Durch Hinzufügen des Konzepts „Instanz" (Integration vieler VLANs in einen Satz) werden viele VLANs in einer Instanz gebündelt, um Kommunikationsaufwand und Ressourcenauslastung zu reduzieren. MSTP unterteilt ein Switched-Netzwerk in viele Bereiche, in denen es viele unabhängige Spanning Trees gibt.

- MSTP beschneidet das Ringnetzwerk zu einem Baumnetzwerk ohne Schleifen, um die Verbreitung und endlose Zirkulation von Paketen im Ringnetzwerk zu vermeiden. Gleichzeitig werden viele redundante Pfade für die Datenweiterleitung bereitgestellt, um die Lastverteilung der VLAN-Daten während der Datenweiterleitung zu realisieren.
- MSTP ist kompatibel mit STP und RSTP.

7.4.2 – Grundkonzept von MSTP

In dieser Abbildung führt jedes Gerät MSTP aus. Einige grundlegende Konzepte von MSTP werden anhand der folgenden Grafiken erläutert.



7.4.2.1 – MST-Bereich

Der MST-Bereich (Multiple Spanning Tree-Bereich) besteht aus vielen Geräten in einem Switched-Netzwerk und den Netzwerksegmenten zwischen ihnen. Diese Geräte haben die folgenden Merkmale:

- Sie haben denselben Bereichsnamen.
- Sie haben dieselbe Zuordnungskonfiguration von VLAN zu Spanning Tree-Instanz.
- Sie haben dieselbe MSTP-Revisionskonfiguration.
- Sie sind physisch miteinander verbunden.

Beispielsweise haben in Bereich A0 in der vorherigen Abbildung alle Geräte in diesem Bereich dieselbe MST-Bereichskonfiguration:

- Gleicher Bereichsname;

- Gleiche Zuordnungsbeziehung zwischen VLAN und Spanning-Tree-Instanz (VLAN 1 ist der Spanning-Tree-Instanz 1 zugeordnet, VLAN 2 ist der Spanning-Tree-Instanz 2 zugeordnet und andere VLANs sind CIST zugeordnet, wobei CIST die Spanning-Tree-Instanz 0 ist);
- Gleiche MSTP-Revisionsstufe (in der obigen Abbildung nicht dargestellt).

In einem geswitchten Netzwerk gibt es viele MST-Bereiche. Benutzer können viele Geräte mithilfe von MSTP-Konfigurationsbefehlen in einen MST-Bereich unterteilen.

7.4.2.2 – WLAN-Zuordnungstabelle

Die VLAN-Zuordnungstabelle ist ein Attribut des MST-Bereichs, das zur Beschreibung der Zuordnungsbeziehung zwischen VLAN und Spanning-Tree-Instanz verwendet wird.

In der vorherigen Abbildung lautet die VLAN-Zuordnungstabelle für den Bereich A0 beispielsweise wie folgt: VLAN 1 wird der Spanning-Tree-Instanz 1 zugeordnet, VLAN 2 wird der Spanning-Tree-Instanz 2 zugeordnet und andere VLANs werden CIST zugeordnet. MSTP kann auf der Grundlage der VLAN-Zuordnungstabelle eine Lastverteilung erreichen.

7.4.2.3 – IST

IST (Internal Spanning Tree) ist ein Spanning Tree in einem MST-Bereich.

IST und CST (Common Spanning Tree) bilden den Spanning Tree CIST (Common and Internal Spanning Tree) des gesamten Switched-Netzwerks. IST ist das Fragment von CIST im MST-Bereich.
In der Abbildung hat CIST beispielsweise in jedem MST-Bereich einen Fragment, der dem IST in dem jeweiligen Bereich entspricht.

7.4.2.4 – CST

CST ist ein einzelner Spanning Tree, der alle MST-Bereiche in einem vermittelten Netzwerk verbindet. Wenn jeder MST-Bereich als „Gerät" betrachtet wird, ist CST ein Spanning Tree, der von diesen „Geräten" durch STP-Protokoll und RSTP-Protokollberechnung generiert wird.

Die rote Linie in der Abbildung ist beispielsweise CST.

7.4.2.5 – CIST

CIST ist ein einzelner Spanning Tree, der alle Geräte in einem Switched Network verbindet und aus IST und CST besteht.
In der Abbildung bilden beispielsweise die IST in jedem MST-Bereich und die CST zwischen den MST-Bereichen das CIST des gesamten Netzwerks.

7.4.2.6 – MSTI

Ein MST-Bereich kann über MSTP viele Spanning Trees generieren, die voneinander unabhängig sind. Jeder Spanning Tree wird als MSTI (Multiple Spanning Tree Instance) bezeichnet.
In der Abbildung gibt es beispielsweise in jedem Bereich viele Spanning Trees, wobei jeder Spanning Tree dem entsprechenden VLAN entspricht. Diese Spanning Trees werden als MSTI bezeichnet.

7.4.2.7 – Bereichswurzel

Die Root-Bridge von IST und MSTI im MST-Bereich ist die Bereichswurzel. Die Topologie jedes Spanning Trees im MST-Bereich ist unterschiedlich, sodass auch die Bereichswurzel unterschiedlich sein kann.
In der Abbildung ist beispielsweise die Bereichswurzel der Spanning-Tree-Instanz 1 im Bereich D0 das Gerät B und die Bereichswurzel der Spanning-Tree-Instanz 2 das Gerät C.

7.4.2.8 – Gemeinsame Root-Bridge

Die gemeinsame Root-Bridge bezeichnet die Root-Bridge von CIST.
In der Abbildung ist die gemeinsame Root-Bridge beispielsweise ein Gerät in Bereich A0.

7.4.2.9 – Bereichsgrenzport

Der Bereichsgrenzport ist der Port am Rand des MST-Bereichs, über den verschiedene MST-Bereiche, MST-Bereiche und Bereiche, in denen STP ausgeführt wird, sowie MST-Bereiche und Bereiche, in denen RSTP ausgeführt wird, miteinander verbunden werden.
Wenn beispielsweise in der Abbildung ein Gerät der Region A0 mit dem ersten Port eines Geräts in der Region D0 verbunden ist und sich die gemeinsame Root des gesamten geswitchten Netzwerks in A0 befindet, ist der erste Port dieses Geräts in der Region D0 der Bereichsgrenzenport der Region D0.
Die Rolle des Bereichsgrenzports auf der Spanning-Tree-Instanz entspricht der des CIST, mit Ausnahme des Master-Ports, dessen Rolle auf dem CIST Root-Port ist, auf anderen Instanzen jedoch Master-Port.

7.4.2.10 – Port-Rolle

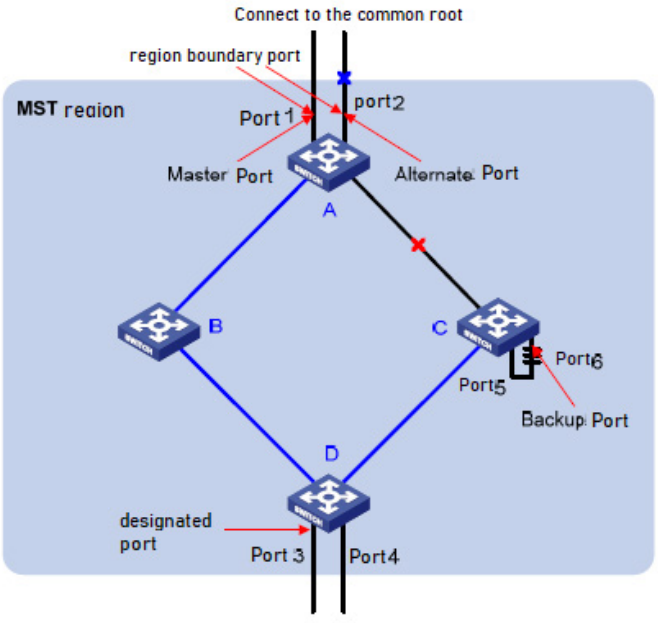
Im MSTP-Berechnungsprozess umfassen die Port-Rollen hauptsächlich Root-Port, Designated Port, Master-Port, Alternate Port, Backup-Port und so weiter.

- Root-Port: Weiterleitung von Daten an die Root-Bridge.
- Designated Port: Weiterleitung von Daten an nachgeschaltete Netzwerksegmente oder Geräte.
- Master-Port: Verbindet den MST-Bereich mit dem gemeinsamen Root, der sich auf dem kürzesten Weg vom gesamten Bereich zum gemeinsamen Root befindet. Aus der Perspektive von CST ist der Master-Port ein „Root-Port" des Bereichs (wenn man den Bereich als Knoten betrachtet). Die Rolle des Master-Ports in IST/CIST ist Root-Port, in anderen Instanzen ist es Master-Port.
- Alternativer Port: Backup-Port des Root-Ports und des Master-Ports. Wenn der Root-Port oder der Master-Port blockiert ist, wird der alternative Port zum neuen Root-Port oder Master-Port.
- Backup-Port: Designierter Port des Backup-Ports. Wenn der designierte Port blockiert ist, wird der Backup-Port schnell zu einem neuen designierten Port und leitet Daten ohne Verzögerung weiter. Wenn zwei Ports eines Geräts mit MSTP offen und miteinander verbunden sind, entsteht eine Schleife. In diesem Fall blockiert das Gerät einen der Ports, und der Backup-Port ist der blockierte Port.

Ports spielen in verschiedenen Spanning-Tree-Instanzen unterschiedliche Rollen.

Die obigen Konzepte werden in der folgenden Abbildung veranschaulicht.

- Die Geräte A, B, C und D bilden einen MST-Bereich.
- Der Port 1 und der Port 2 des Geräts A sind mit dem gemeinsamen Root verbunden.
- Der Port 5 und der Port 6 des Geräts C bilden eine Schleife.
- Der Port 3 und der Port 4 des Geräts D sind mit anderen MST-Bereichen nach unten verbunden.



7.4.2.11 – Portstatus

In MSTP kann der Status eines Ports je nachdem, ob er MAC-Adressen lernt und den Datenverkehr des Benutzers weiterleitet, in die folgenden drei Typen unterteilt werden:

- **Weiterleitungsstatus:** MAC-Adressen werden gelernt und der Datenverkehr des Benutzers wird weitergeleitet.
- **Lernstatus:** MAC-Adressen werden gelernt, aber der Datenverkehr des Benutzers wird nicht weitergeleitet.
- **Verwerfungsstatus:** Weder MAC-Adressen werden gelernt noch wird der Datenverkehr des Benutzers weitergeleitet.

Es besteht kein notwendiger Zusammenhang zwischen dem Portstatus und seiner Rolle. Die folgende Tabelle zeigt den Portstatus verschiedener Portrollen („√" bedeutet, dass diese Portrolle diesen Status haben kann; „--" bedeutet, dass diese Portrolle diesen Status nicht haben kann).

Port Rolle Port Status	Root-Port/ Master-Port	Bestimmter Port	Alternativer Port	Backup Port
Weiterleitung	√	√	--	--
Lernen	√	√	--	--
Verwerfen	√	√	√	√

7.4.3 – Grundprinzip von MSTP

MSTP unterteilt das gesamte zweischichtige Netzwerk in mehrere MST-Bereiche, und CST wird durch Berechnung zwischen den Bereichen generiert; mehrere Spanning Trees werden durch Berechnung im Bereich generiert, und jeder Spanning Tree wird als mehrere Spanning Tree-Instanzen bezeichnet, wobei Instanz 0 IST ist und andere mehrere Spanning Tree-Instanzen MSTI sind. MSTP verwendet wie STP Konfigurationsmeldungen zur Berechnung des Spanning Trees, aber die Konfigurationsmeldung enthält die Konfigurationsinformationen des MSTP-Geräts.

7.4.3.1 – Berechnung des CIST-Spanning-Tree

Nach dem Vergleich der Konfigurationsmeldungen wird ein Gerät mit der höchsten Priorität im gesamten Netzwerk als Root-Bridge des CIST ausgewählt. In jedem MST-Bereich generiert MSTP durch Berechnung einen IST. Gleichzeitig behandelt MSTP jeden MST-Bereich als einzelnes Gerät und generiert durch Berechnung einen CST zwischen den Bereichen. CST und IST bilden den CIST des gesamten Netzwerks.

7.4.3.2 – Berechnung von MSTI

In einem MST-Bereich generiert MSTP verschiedene Spanning-Tree-Instanzen für verschiedene VLANs entsprechend der Zuordnungsbeziehung zwischen VLAN und Spanning-Tree-Instanzen. Jeder Spanning Tree wird unabhängig berechnet. Der Berechnungsprozess ähnelt dem von STP.

In MSTP wird eine VLAN-Nachricht über den folgenden Pfad übertragen:

- Im MST-Bereich wird sie entlang des entsprechenden MSTI übertragen.
- Zwischen MST-Bereichen wird sie entlang des CST übertragen.

7.4.4 – Realisierung von MSTP auf Geräten

MSTP ist kompatibel mit STP und RSTP. Nachrichten der STP- und RSTP-Protokolle können von MSTP-Geräten identifiziert und zur Berechnung des Spanning Tree verwendet werden.

Zusätzlich zu den Grundfunktionen von MSTP bietet dieses Gerät viele spezielle Funktionen, die aus Sicht des Benutzers für die Verwaltung praktisch sind, darunter:

- Wartung der Root-Bridge
- Sicherung der Root-Bridge
- Root-Schutzfunktion
- BPDU-Schutzfunktion
- Loop-Schutzfunktion
- Schutz vor Angriffen durch TC-BPDU-Nachrichten

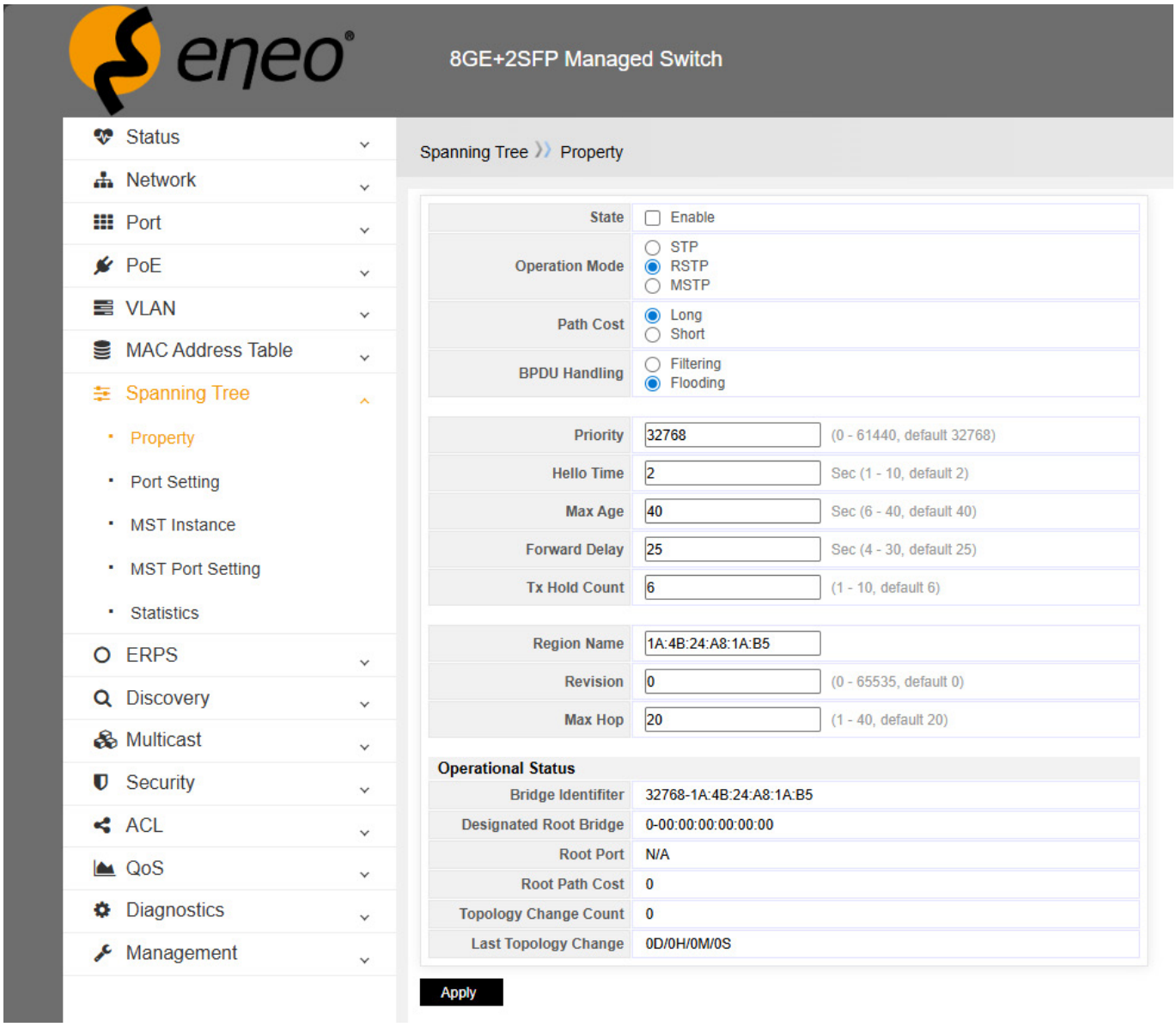
7.5 – Protokoll

Relevante Protokolle:

- **IEEE 802.1D:** Spanning Tree Protocol (STP)
- **IEEE 802.1w:** Rapid Spanning Tree Protocol (RSTP)
- **IEEE 802.1s:** Multiple Spanning Tree Protocol (MSTP)

7.6 – Property

Status: Aktivieren (vollständige Switch-Spanning-Tree-Konfiguration, zum Aktivieren markieren, zum Deaktivieren nicht markieren)



Vorgangsmodus: STP/RSTP/MSTP (drei Modi zur Auswahl)

Pfadkosten: Lang/Kurz (der Wertebereich ist eine kurze Ganzzahl (kurz: 1-65535) (lang: 1-200000000))

BPDU-Behandlung: Filtering/Flooding (Filtern oder Fluten von BPDU-Nachrichten)

Priorität: Konfigurieren Sie die Priorität für den Switch. Der Wertebereich liegt zwischen 0 und 61440. Er wird um ein Vielfaches von 4096 erhöht. Der Standardwert ist 32768.

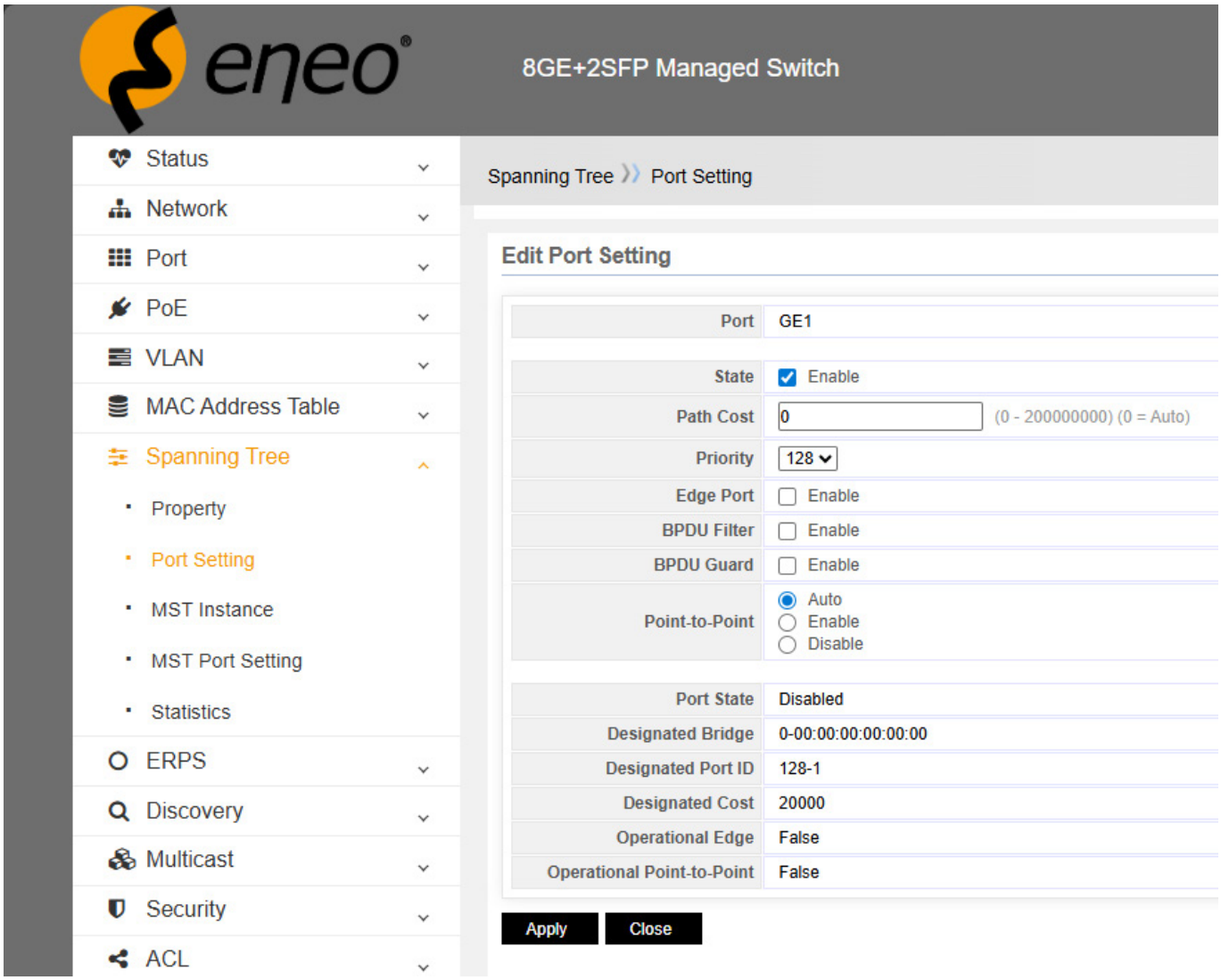
Hell Time: Konfigurieren Sie das Zeitintervall für die Übertragung von BPDU-Nachrichten für den Switch. Der Standardwert beträgt 2 Sekunden.

Maximale Lebensdauer: Konfigurieren Sie die maximale Lebensdauer von BPDU-Nachrichten. Der Standardwert beträgt 20 Sekunden.

Weiterleitungsverzögerung: Konfigurieren Sie das Zeitintervall für die Änderung des Portstatus. Der Standardwert beträgt 15 Sekunden.

TX-Halteanzahl: Konfigurieren Sie die maximale Anzahl der pro Sekunde übertragenen BPDUs. Der Standardwert beträgt 3.

7.7 – Port-Einstellungen



Status: Aktivieren (Als Spanning-Tree-Konfiguration des Switch-Ports, zum Aktivieren markieren, zum Deaktivieren nicht markieren)

Pfadkosten: Lang/Kurz (der Wertebereich ist eine kurze Ganzzahl (kurz: 1-65535) (lang: 1-200000000))

Priorität: Konfigurieren Sie die Priorität des Switch-Ports im Bereich von 0 bis 240.

Edge-Port: Ein als Edge-Port konfigurierter Port kann den Portstatus direkt auf „Weiterleitung“ ändern, wenn er aktiv ist.

BPDU-Filter: Wenn der BPDU-Filter auf dem Port konfiguriert ist, sendet und empfängt die Schnittstelle keine BPDU-Nachrichten mehr.

BPDU-Schutz: Wenn der BPDU-Schutz auf dem Port konfiguriert ist, wird die Schnittstelle direkt getrennt, sobald ein BPDU-Paket, das nicht vorhanden sein sollte, auf einer bestimmten Schnittstelle empfangen wird, sodass sie in den Zustand „Soft Close Err deaktiviert" versetzt wird. Im Vergleich zum BPDU-Filter ist diese Methode robuster.

Punkt zu Punkt: Wenn der BPDU-Filter auf dem Port konfiguriert ist, sendet und empfängt die Schnittstelle keine BPDU-Nachrichten mehr.

8 – ERPS (G.8032)

Ethernet Ring Protection Switching (ERPS) ist ein Protokoll, das von der International Telecommunication Union - Telecommunication Standardization Sector (ITU-T) definiert wurde, um Schleifen auf Layer 2 zu eliminieren. Es implementiert die Konvergenz von Zuverlässigkeitsstandards der Carrier-Klasse und ermöglicht die Kommunikation aller ERPS-fähigen Geräte in einem Ringnetzwerk.

8.1 – Einführung

8.1.1 – Definition

Da die Standardnummer ITU-T G.8032/Y1344 lautet, wird ERPS auch als G.8032 bezeichnet.
ERPS definiert Ring Auto Protection Switching (RAPS) Protocol Data Units (PDUs) und Schutzumschaltmechanismen.

ERPS gibt es in zwei Versionen: ERPSv1, veröffentlicht von ITU-T im Juni 2008, und ERPSv2, veröffentlicht im August 2010. EPRSv2 ist vollständig kompatibel mit ERPSv1 und bietet die folgenden erweiterten Funktionen:

- Mehrringtopologien, wie z. B. sich kreuzende Ringe
- RAPS-PDU-Übertragung auf virtuellen Kanälen (VCs) und nicht-virtuellen Kanälen (NVCs) in Unterringen
- Forced Switch (FS) und Manual Switch (MS)
- Revertive und nicht-revertive Umschaltung

8.1.2 – Zweck

Im Allgemeinen werden redundante Links in einem Ethernet-Switching-Netz, z. B. in einem Ringnetz, verwendet, um ein Link-Backup zu bieten und die Zuverlässigkeit des Netzes zu erhöhen.
Die Verwendung redundanter Verbindungen kann jedoch zu Schleifen führen, die Broadcast-Stürme verursachen und die MAC-Adresstabelle instabil machen.
Infolgedessen verschlechtert sich die Kommunikationsqualität, und die Kommunikationsdienste können sogar unterbrochen werden. Die folgende Tabelle beschreibt die von den Geräten unterstützten Ringnetzwerkprotokolle.

Ring-Netzwerkprotokoll	Vorteil	Nachteil
STP / RSTP / MSTP	• Gilt für alle Layer-2-Netzwerke. • Ist ein Standard-IEEE-Protokoll, das die Kommunikation zwischen Huawei-Geräten und Geräten anderer Hersteller ermöglicht.	• Bietet eine geringe Konvergenz in einem großen Netzwerk, das die Anforderungen an die Zuverlässigkeit der Carrier-Klasse nicht erfüllen kann.
ERPS	• Bietet schnelle Konvergenz und Zuverlässigkeit der Carrier-Klasse. • Ist ein Standardprotokoll nach ITU-T, das die Kommunikation von Huawei-Geräten mit Geräten anderer Hersteller ermöglicht. • Unterstützt Single-Ring- und Multi-Ring-Topologien in ERPSv2.	• Die Netzwerktopologie muss im Voraus geplant werden. • Die Konfiguration ist komplex.

Ethernet-Netzwerke erfordern eine schnellere Schutzumschaltung. STP erfüllt die Anforderungen an eine schnelle Konvergenz nicht. RRPP und SEP sind proprietäre Ringprotokolle von Huawei, die nicht für die Kommunikation zwischen Huawei- und Nicht-Huawei-Geräten in einem Ringnetzwerk verwendet werden können.

ERPS, ein Standardprotokoll der ITU-T, verhindert Schleifen in Ringnetzwerken. Es optimiert die Erfassung und sorgt für eine schnelle Konvergenz. ERPS ermöglicht die Kommunikation aller ERPS-fähigen Geräte in einem Ringnetzwerk.

8.1.3 – Vorteile

- Verhindert Broadcast-Stürme und implementiert eine schnelle Verkehrsüberleitung in einem Netzwerk mit Schleifen.
- Bietet schnelle Konvergenz und Zuverlässigkeit der Carrier-Klasse.
- Ermöglicht die Kommunikation aller ERPS-fähigen Geräte in einem Ringnetzwerk.

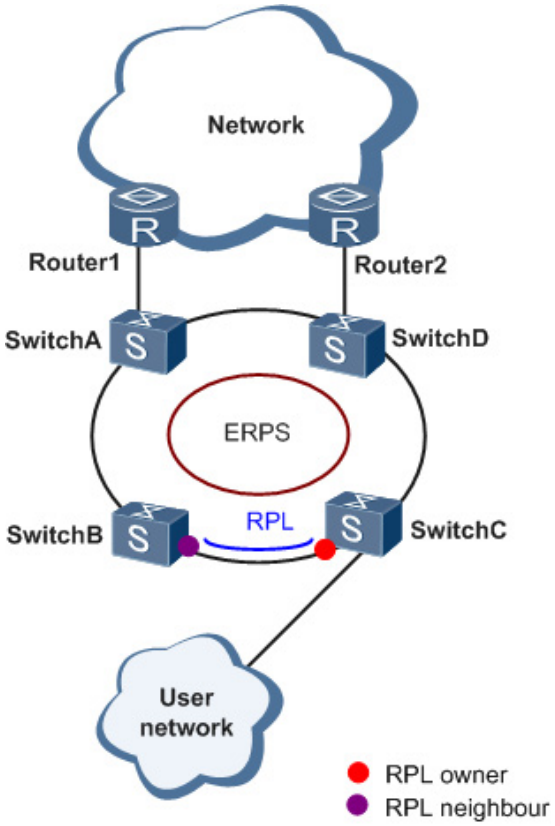
8.2 – Grundsätze

In diesem Abschnitt wird die Umsetzung von ERPS beschrieben.

8.2.1 – Grundlegende ERPS-Konzepte

ERPS eliminiert Schleifen auf der Verbindungsschicht eines Ethernet-Netzwerks. ERPS funktioniert für ERPS-Ringe. In einem ERPS-Ring gibt es mehrere Knoten. ERPS blockiert den RPL-Eigentümer-Port und steuert gemeinsame Ports, um den Port-Status zwischen Weiterleitung und Verwerfung zu wechseln und Schleifen zu vermeiden. ERPS verwendet das Steuer-VLAN, das Daten-VLAN und die Ethernet Ring Protection (ERP)-Instanz.

In dem in der folgenden Abbildung dargestellten Netzwerk bilden SwitchA bis SwitchD einen Ring und sind mit dem Upstream-Netzwerk doppelt gebündelt. Dieser Zugriffsmodus führt zu einer Schleife im gesamten Netzwerk. Um redundante Verbindungen zu eliminieren und die Konnektivität der Verbindungen zu gewährleisten, wird ERPS verwendet, um Schleifen zu verhindern.



8.2.1.1 – ERPS-Ring

Ein ERPS-Ring besteht aus miteinander verbundenen Layer-2-Switching-Geräten, die mit demselben Kontroll-VLAN konfiguriert sind.

8.2.1.2 – Port-Rolle

ERPS definiert drei Port-Rollen: RPL-Eigentümer-Port, RPL-Nachbar-Port (nur in ERPSv2) und gemeinsamer Port.

- **RPL-Eigentümer-Port**

  Ein RPL-Eigentümer-Port ist für die Blockierung des Datenverkehrs über die Ring Protection Link (RPL) verantwortlich, um Schleifen zu verhindern. Ein ERPS-Ring hat nur einen RPL-Eigentümer-Port.
  Wenn der Knoten, auf dem sich der RPL-Eigentümerport befindet, eine RAPS-PDU empfängt, die einen Link- oder Knotenfehler in einem ERPS-Ring anzeigt, hebt der Knoten die Sperrung des RPL-Eigentümerports auf. Anschließend kann der RPL-Eigentümerport Datenverkehr senden und empfangen, um eine unterbrechungsfreie Weiterleitung des Datenverkehrs zu gewährleisten.
  Der Link, auf dem sich der RPL-Eigentümerport befindet, ist der RPL.

- **RPL-Nachbar-Port**

  Ein RPL-Nachbarport ist direkt mit einem RPL-Eigentümerport verbunden.
  Sowohl der RPL-Eigentümerport als auch die RPL-Nachbarports sind in normalen Situationen gesperrt, um Schleifen zu verhindern.
  Wenn ein ERPS-Ring ausfällt, werden sowohl der RPL-Eigentümerport als auch die Nachbarports entsperrt.
  Der RPL-Nachbarport trägt dazu bei, die Anzahl der FDB-Eintragaktualisierungen auf dem Gerät zu reduzieren, auf dem sich der RPL-Nachbarport befindet.

- **Gemeinsamer Port**

  Gemeinsame Ports sind Ringports, die keine RPL-Besitzer- oder Nachbarports sind.
  Ein gemeinsamer Port überwacht den Status der direkt verbundenen ERPS-Verbindung und sendet RAPS-PDUs, um die anderen Ports über Änderungen des Verbindungsstatus zu informieren.

8.2.1.3 – Portstatus

In einem ERPS-Ring hat ein ERPS-aktivierter Port zwei Status:

- **Weiterleitung:** Leitet den Benutzerdatenverkehr weiter und sendet und empfängt RAPS-PDUs.
- **Verwerfen:** Sendet und empfängt nur RAPS-PDUs.

8.2.1.4 – Steuerungs-VLAN

Ein Steuerungs-VLAN wird in einem ERPS-Ring konfiguriert, um RAPS-PDUs zu übertragen. Jeder ERPS-Ring muss mit einem Steuer-VLAN konfiguriert werden. Nachdem ein Port zu einem ERPS-Ring hinzugefügt wurde, der mit einem Steuer-VLAN konfiguriert ist, wird der Port automatisch zum Steuer-VLAN hinzugefügt. Verschiedene ERPS-Ringe müssen unterschiedliche Steuer-VLANs verwenden.

8.2.1.5 – Daten-VLAN

Im Gegensatz zu Steuer-VLANs werden Daten-VLANs zur Übertragung von Datenpaketen verwendet.

8.2.1.6 – ERP-Instanz

Auf einem Layer-2-Gerät, auf dem ERPS läuft, muss das VLAN, in dem RAPS-PDUs und Datenpakete übertragen werden, einer Ethernet Ring Protection (ERP)-Instanz zugeordnet werden, damit ERPS die Pakete auf der Grundlage von konfigurierten Regeln weiterleitet oder blockiert. Wenn die Zuordnung nicht konfiguriert ist, können die vorangehenden Pakete Broadcast-Stürme im Ringnetzwerk verursachen. Dies führt dazu, dass das Netzwerk nicht mehr verfügbar ist.

8.2.1.7 – Timer

- **Guard-Timer**

  Nachdem eine fehlerhafte Verbindung oder ein fehlerhafter Knoten wiederhergestellt oder ein Löschvorgang ausgeführt wurde, sendet das Gerät RAPS No Request (NR)-Nachrichten, um die anderen Knoten über die Wiederherstellung der Verbindung oder des Knotens zu informieren, und startet den Guard-Timer. Vor Ablauf des Guard-Timers verarbeitet das Gerät keine RAPS (NR)-Nachrichten, um den Empfang veralteter RAPS (NR)-Nachrichten zu vermeiden. Wenn das Gerät nach Ablauf des Guard-Timers immer noch eine RAPS (NR)-Nachricht empfängt, trägt sich der lokale Port in den Forwarding-Zustand ein.

- **WTR-Timer**

  Wenn ein RPL-Eigentümer-Port aufgrund eines Verbindungs- oder Knotenfehlers entsperrt wird, kann der betroffene Port nicht sofort nach der Wiederherstellung der Verbindung oder des Knotens nach oben gehen. Die Blockierung des RPL-Eigentümer-Ports kann zu Netzwerkflapping führen. Um dieses Problem zu vermeiden, startet der Knoten, in dem sich der RPL-Eigentümer-Port befindet, nach dem Empfang einer RAPS (NR)-Nachricht den WTR-Timer (Wait to Restore). Wenn der Knoten eine RAPS Signal Fail (SF) Nachricht empfängt, bevor der Timer abläuft, beendet er den WTR Timer. Empfängt der Knoten keine RAPS (SF)-Nachricht, bevor der Zeitgeber abläuft, blockiert er den RPL-Eigentümerport, wenn der Zeitgeber abläuft, und sendet eine RAPS (no request, root blocked)-Nachricht. Nach Erhalt dieser RAPS (NR, RB)-Nachricht versetzen die Knoten ihre wiederhergestellten Ports im Ring in den Weiterleitungszustand.

- **Holdoff-Timer**

  In Schicht-2-Netzen, in denen EPRS eingesetzt wird, können unterschiedliche Anforderungen an das Wechseln des Schutzes bestehen. In einem Netzwerk, in dem mehrschichtige Dienste bereitgestellt werden, benötigen die Benutzer nach dem Ausfall eines Servers möglicherweise eine gewisse Zeit, um den Serverfehler zu beheben, damit die Clients den Fehler nicht erfassen. Sie können den Holdoff-Timer einstellen. Tritt der Fehler auf, wird er erst nach Ablauf des Holdoff-Timers an ERPS gesendet.

8.3 – Konfigurationsbeispiele

Dieser Abschnitt enthält Konfigurationsbeispiele für ERPS, einschließlich der Netzwerkvoraussetzungen, der Konfigurations-Roadmap, der Konfigurationsvorgehensweise und der Konfigurationsdateien.

8.3.1 – Beispiel für die Konfiguration von ERPS Multi-Instance

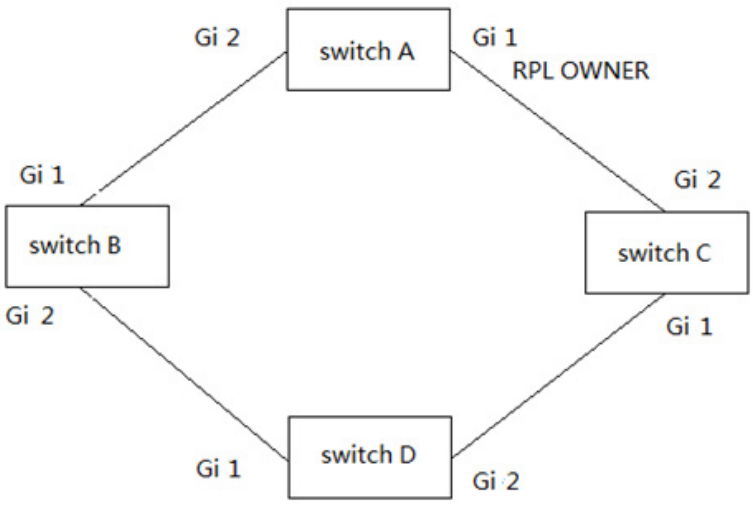
Dieser Abschnitt enthält ein Beispiel zur Konfiguration mehrerer Instanzen von ERPS.

8.3.1.1 – Netzwerkvoraussetzungen

Im Allgemeinen werden redundante Links in einem Ethernet-Switching-Netzwerk verwendet, um ein Link-Backup zu bieten und die Zuverlässigkeit des Netzwerks zu erhöhen. Die Verwendung redundanter Links kann jedoch zu Schleifen führen, die Broadcast Storms verursachen und die MAC-Adresstabelle instabil machen. Infolgedessen verschlechtert sich die Kommunikationsqualität, und die Kommunikationsdienste können sogar unterbrochen werden.

Um durch redundante Links verursachte Schleifen zu verhindern, aktivieren Sie ERPS auf den Knoten des Ringnetzes. ERPS ist ein Layer-2-Schleifenunterbrechungsprotokoll, das von der ITU-T definiert wurde und eine schnelle Konvergenz von Zuverlässigkeitsstandards der Carrier-Klasse ermöglicht.

Die folgende Abbildung zeigt ein Netzwerk, in dem ein ERPS-Ring mit mehreren Instanzen verwendet wird. SwitchA bis SwitchD bilden ein Ringnetz auf der Aggregationsschicht, um die Dienstaggregation auf Schicht 2 zu implementieren und Schicht-3-Dienste zu verarbeiten. ERPS wird in dem Ringnetz verwendet, um Schutzschaltungen für redundante Verbindungen der Schicht 2 bereitzustellen. ERPS Ring 1 und ERPS Ring 2 sind auf SwitchA bis SwitchD konfiguriert. P1 auf SwitchB ist ein gesperrter Port in ERPS-Ring 1, und P2 auf SwitchA ist ein gesperrter Port in ERPS-Ring 2, wodurch Lastausgleich und Link-Backup implementiert werden.



8.3.1.2 – Konfigurations-Roadmap

Die Konfigurations-Roadmap sieht wie folgt aus:

1. Konfigurieren Sie den Verbindungstyp aller Ports, die zu ERPS-Ringen hinzugefügt werden sollen, als Trunk.
2. Erstellen Sie ERPS-Ringe und konfigurieren Sie Steuer-VLANs und Ethernet Ring Protection (ERP)-Instanzen in den ERPS-Ringen.
3. Fügen Sie Layer-2-Ports zu ERPS-Ringen hinzu und legen Sie Port-Rollen fest.
4. Konfigurieren Sie die Guard-Timer und WTR-Timer in den ERPS-Ringen.
5. Konfigurieren Sie die Layer-2-Weiterleitung auf SwitchA bis SwitchD.

8.3.1.3 – Hinzufügen eines Layer-2-Ports zu einem ERPS-Ring und Konfigurieren der Portrolle

Nachdem ERPS konfiguriert wurde, fügen Sie Layer-2-Ports zu einem ERPS-Ring hinzu und konfigurieren Sie die Portrollen, damit ERPS ordnungsgemäß funktioniert.
Sie können einen Layer-2-Port auf eine der folgenden Arten zu einem ERPS-Ring hinzufügen:

- Fügen Sie in der ERPS-Ringansicht einen bestimmten Port zum ERPS-Ring hinzu und konfigurieren Sie die Portrolle.
- Fügen Sie in der Schnittstellenansicht den aktuellen Port zum ERPS-Ring hinzu und konfigurieren Sie die Portrolle.

Die Webseitenkonfiguration lautet wie folgt:

1. Konfigurieren Sie Port 1 und Port 2, die beide mit dem Tag „VLAN200“ versehen sind.
2. Konfigurieren Sie SwitchA, um ERP zu aktivieren, konfigurieren Sie dann die VLAN-ID des Kontroll-VLAN auf 200 und konfigurieren Sie anschließend Port 1 für den RTL-Besitzer-Modus und Port 2 für den Ring-Modus.
3. Klicken Sie auf die Schaltfläche „Übernehmen“, um die Konfiguration von SwitchA abzuschließen.
4. Wenn Sie SwitchB~D konfigurieren müssen, ist alles andere gleich, konfigurieren Sie lediglich den Portmodus auf „Ring“.

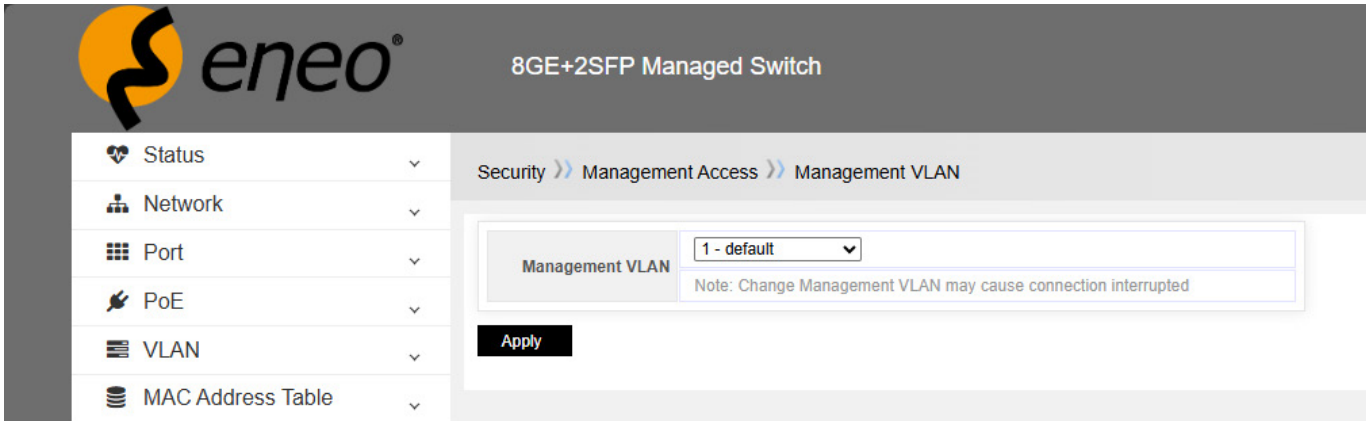
9 – SICHERHEIT

9.1 – Managementzugriff

9.1.1 – VLAN-Management

VLAN-Management bedeutet, dass nur das VLAN am Port mit der CPU des Switches kommunizieren und das Switch-System verwalten kann.

Standardmäßig können die Mitglieder-Ports von VLAN1 Mitglieder-Ports Switches verwalten.

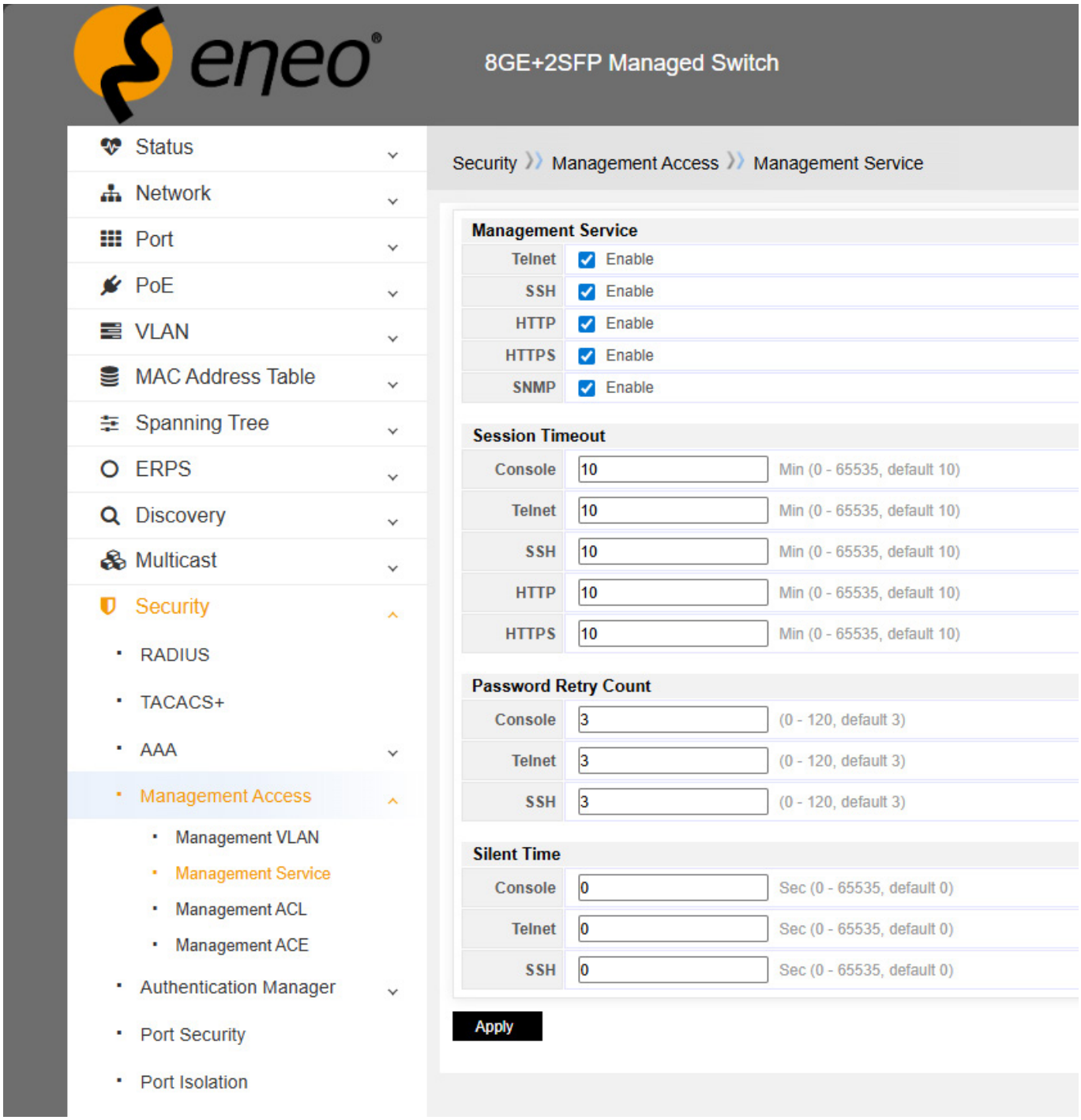


Je nach den Anforderungen des Benutzers können Sie ein beliebiges VLAN zur Verwaltung des Switch-Systems auswählen. Voraussetzung ist jedoch, dass das ausgewählte VLAN zuvor eingerichtet wurde.

Beispiel

1. Fügen Sie ein VLAN hinzu, z. B. VLAN100
2. Fügen Sie Port 5 zu VLAN 100 hinzu
3. Legen Sie VLAN100 als verwaltendes VLAN fest
4. Verbinden Sie den PC mit Port 5, um den Switch zu verwalten.

9.1.2 – Management Service



Telnet: Telnet ist ein Netzwerkprotokoll, das im Internet oder in lokalen Netzwerken verwendet wird, um eine bidirektionale, interaktive, textorientierte Kommunikation über eine virtuelle Terminalverbindung zu ermöglichen, mit der Netzwerkadministratoren aus der Ferne auf Netzwerkgeräte wie Router, Switches und Server zugreifen und diese verwalten können. So kann sich ein Administrator beispielsweise von einem entfernten Standort aus über Telnet bei einem Router anmelden und dessen Einstellungen wie IP-Adressen, Routing-Protokolle und Zugriffskontrolllisten konfigurieren.

SSH (Secure Shell): SSH ist ein kryptografisches Netzwerkprotokoll für den sicheren Betrieb von Netzwerkdiensten über ein ungesichertes Netzwerk. Der Standard-TCP-Port für SSH ist 22. Ähnlich wie Telnet wird SSH für die Fernanmeldung und -verwaltung von Netzwerkgeräten verwendet. Es bietet jedoch ein wesentlich höheres Maß an Sicherheit. Wenn ein Administrator SSH verwendet, um sich bei einem Gerät anzumelden, werden die zwischen dem Client (dem Rechner, auf dem der Administrator arbeitet) und dem Server (dem Netzwerkgerät) übertragenen Daten verschlüsselt. Diese Verschlüsselung schützt sensible Informationen wie Kennwörter und Konfigurationsdetails vor der Preisgabe.

HTTP (Hypertext Transfer Protocol): HTTP ist die Grundlage der Datenkommunikation im World Wide Web. Es ist ein Anwendungsschichtprotokoll zur Übertragung von Hypermedia-Dokumenten wie HTML. Über diese Schnittstelle kann der Administrator den Gerätestatus anzeigen, Einstellungen konfigurieren und verschiedene Verwaltungsaufgaben wie die Aktualisierung der Firmware durchführen.

HTTPS (Hypertext Transfer Protocol Secure): HTTPS ist eine Erweiterung von HTTP. Die Daten, die zwischen dem Webbrowser und dem Netzwerkgerät übertragen werden, werden mit SSL/TLS-Protokollen (Secure Sockets Layer/Transport Layer Security) verschlüsselt. Dadurch wird sichergestellt, dass sensible Informationen wie Anmeldedaten und Konfigurationsänderungen vor Abhören und Manipulationen geschützt sind.

SNMP (Simple Network Management Protocol): SNMP ist ein Internet-Standardprotokoll für die Verwaltung von Geräten in IP-Netzen. Es wird verwendet, um Netzwerkgeräte auf Zustände zu überwachen, die administrative Aufmerksamkeit erfordern.SNMP wird häufig in Netzwerkmanagementsystemen verwendet, um Informationen von Netzwerkgeräten zu sammeln. Netzwerkgeräte wie Router, Switches und Server können so konfiguriert werden, dass sie als SNMP-Agenten fungieren. Diese Agenten sammeln Daten über die Leistung des Geräts, z. B. CPU-Nutzung, Speichernutzung, Schnittstellenstatus und Verkehrsstatistiken. Der SNMP-Manager, bei dem es sich in der Regel um eine Netzwerkverwaltungssoftware handelt, kann dann die Agenten abfragen, um diese Informationen zu erhalten. Beispielsweise kann ein Netzwerkadministrator SNMP verwenden, um die Bandbreitennutzung der verschiedenen Netzwerkschnittstellen eines Routers in Echtzeit zu überwachen.

Zeitlimit: Je nach den Anforderungen der Benutzer können Sie die zu unterstützenden Switches auswählen.

Sitzungs-Timeout: z.B. nach dem Einloggen auf der Webseite, wenn 10 Sekunden lang kein Vorgang stattfindet, wird das System die Webseite automatisch verlassen. Der Benutzer muss seinen Namen und sein Kennwort erneut eingeben, um den Switch zu verwalten.

Anzahl der Passwortwiederholungen: Wenn die Anzahl der Eingaben eines falschen Kennworts den eingestellten Wert überschreitet, wartet der Benutzer einige Zeit und gibt das Kennwort erneut ein, um Brute-Force zu verhindern.

10 – MULTICAST

10.1 – Einführung in Multicast

Das Multicast-Verfahren, das neben Unicast und Broadcast existiert, ist eine wirksame Lösung für das Problem der Punkt-zu-Mehrpunkt-Datenübertragung. Durch die hocheffiziente Punkt-zu-Mehrpunkt-Datenübertragung über ein Netz spart Multicast erheblich an Netzbandbreite und verringert die Netzbelastung.

Mit der Multicast-Technologie kann ein Netzbetreiber problemlos neue Mehrwertdienste anbieten, z. B. Live-Webcasting, Web-TV, Fernunterricht, Telemedizin, Webradio, Echtzeit-Videokonferenzen und andere bandbreiten- und zeitkritische Informationsdienste.

10.2 – IGMP-Snooping – Übersicht

Internet Group Management Protocol Snooping (IGMP Snooping) ist ein Multicast-Einschränkungsmechanismus, der auf Layer-2-Geräten zur Verwaltung und Kontrolle von Multicast-Gruppen läuft.

10.2.1 – Beim Empfang einer allgemeinen Abfrage

Der IGMP-Abfrager sendet in regelmäßigen Abständen allgemeine IGMP-Abfragen an alle Hosts und Router (224.0.0.1) im lokalen Subnetz, um herauszufinden, ob es im Subnetz aktive Multicast-Gruppenmitglieder gibt.

Nach dem Empfang einer allgemeinen IGMP-Abfrage leitet der Switch diese über alle Ports im VLAN mit Ausnahme des empfangenden Ports weiter und führt für den empfangenden Port Folgendes aus:

- Wenn der empfangende Port ein Router-Port ist, der in seiner Router-Port-Liste vorhanden ist, setzt der Switch den Alterungstimer dieses Router-Ports zurück.
- Wenn der empfangende Port kein Router-Port ist, der in seiner Router-Port-Liste vorhanden ist, fügt der Switch ihn seiner Router-Port-Liste hinzu und setzt einen Aging-Timer für diesen Router-Port.

10.2.2 – Beim Empfang eines Membership-Berichts

Ein Host sendet unter den folgenden Umständen einen IGMP-Bericht an den Multicast-Router:

- Nach dem Empfang einer IGMP-Abfrage antwortet ein Host, der Mitglied einer Multicast-Gruppe ist, mit einem IGMP-Bericht.
- Wenn ein Host einer Multicast-Gruppe beitreten möchte, sendet er einen IGMP-Bericht an den Multicast-Router, um mitzuteilen, dass er an den für diese Gruppe bestimmten Multicast-Informationen interessiert ist.

Nach dem Empfang eines IGMP-Berichts leitet der Switch diesen über alle Router-Ports im VLAN weiter, löst die Adresse der gemeldeten Multicast-Gruppe auf und führt Folgendes aus:

- Wenn für die gemeldete Gruppe kein Eintrag in der Weiterleitungstabelle vorhanden ist, erstellt der Switch einen Eintrag, fügt den Port als Mitgliedspfort zur Liste der ausgehenden Ports hinzu und startet einen Mitgliedspfort-Aging-Timer für diesen Port.
- Wenn ein Eintrag in der Weiterleitungstabelle für die gemeldete Gruppe vorhanden ist, der Port jedoch nicht in der Liste der ausgehenden Ports für diese Gruppe enthalten ist, fügt der Switch den Port als Mitgliedspfort zur Liste der ausgehenden Ports hinzu und startet einen Mitgliedspfort-Aging-Timer für diesen Port.
- Wenn ein Eintrag in der Weiterleitungstabelle für die gemeldete Gruppe vorhanden ist und der Port in der Liste der ausgehenden Ports enthalten ist, was bedeutet, dass dieser Port bereits ein Mitgliedsport ist, setzt der Switch den Member Port Aging Timer für diesen Port zurück.

10.2.3 – Beim Empfang einer Leave-Group-Nachricht

Wenn ein IGMPv2- oder IGMPv3-Host eine Multicast-Gruppe verlässt, sendet der Host eine IGMP-Leave-Group-Nachricht an den Multicast-Router.

Wenn der Switch eine gruppenspezifische IGMP-Leave-Group-Nachricht an einem Mitglied-Port empfängt, kontrolliert er zunächst, ob ein Eintrag für diese Gruppe in der Weiterleitungstabelle vorhanden ist, und wenn ja, ob die ausgehende Portliste diesen Port enthält.

- Wenn der Eintrag in der Weiterleitungstabelle nicht vorhanden ist oder wenn die Liste der ausgehenden Ports diesen Port nicht enthält, verwirft der Switch die IGMP-Leave-Group-Nachricht, anstatt sie an einen Port weiterzuleiten.
- Wenn der Eintrag in der Weiterleitungstabelle vorhanden ist und die Liste der ausgehenden Ports den Port enthält, leitet der Switch die Leave-Group-Nachricht an alle Router-Ports im VLAN weiter. Da der Switch nicht weiß, ob andere an den Port angeschlossene Hosts noch auf diese Gruppenadresse hören, entfernt er den Port nicht sofort aus der Liste der ausgehenden Ports des Eintrags in der Weiterleitungstabelle für diese Gruppe, sondern setzt den Member-Port-Aging-Timer für den Port zurück.

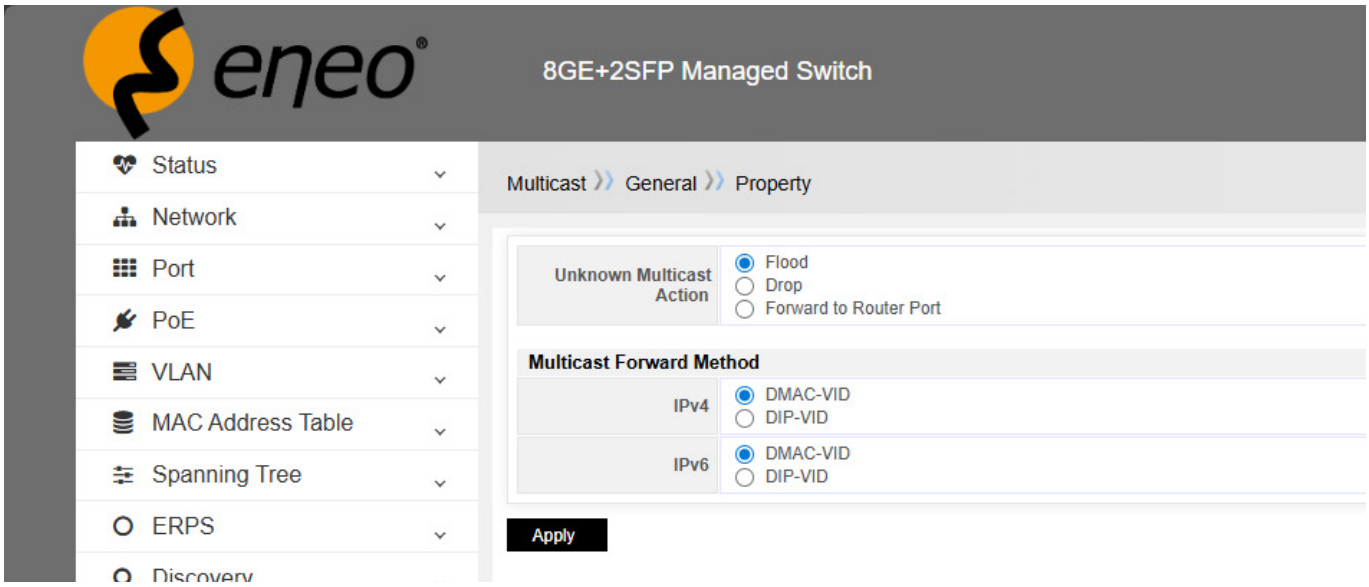
Nach dem Empfang der IGMP-Leave-Group-Nachricht von einem Host ermittelt der IGMP-Querier aus der Nachricht die Adresse der Multicast-Gruppe, die der Host gerade verlassen hat, und sendet eine IGMP-gruppenspezifische Abfrage an diese Multicast-Gruppe über den Port, der die Leave-Group-Nachricht empfangen hat. Nach dem Empfang der IGMP-gruppenspezifischen Abfrage leitet der Switch diese über alle seine Router-Ports im VLAN und alle Mitgliedsports für diese Multicast-Gruppe weiter und führt Folgendes aus:

- Wenn vor Ablauf des Aging-Timers auf einem Mitgliedsport ein IGMP-Bericht als Antwort auf die gruppenspezifische Abfrage empfangen wird, bedeutet dies, dass ein an den Port angeschlossener Host Multicast-Daten für diese Multicast-Gruppe empfängt oder erwartet. Der Switch setzt den Aging-Timer des Mitgliedsports zurück.
- Wenn vor Ablauf des Aging-Timers kein IGMP-Bericht als Antwort auf die gruppenspezifische Abfrage an einem Mitgliedsport empfangen wird, bedeutet dies, dass keine an den Port angeschlossenen Hosts mehr auf diese Gruppenadresse hören: Der Switch entfernt den Port aus der Liste der ausgehenden Ports des Eintrags in der Weiterleitungstabelle für diese Multicast-Gruppe, wenn der Aging-Timer abläuft.

10.3 – IGMP-Snooping-Konfiguration

10.3.1 – Verarbeitung unbekannter Multicast-Pakete

Für die Verarbeitung unbekannter Multicast-Pakete können Sie wählen, ob Sie diese als Flooding behandeln, verwerfen oder an den Routing-Port weiterleiten möchten.



IGMP (Internet Group Management Protocol) wird zur Verwaltung von Multicast-Gruppenmitgliedschaften verwendet. Im Zusammenhang mit IGMP beziehen sich die Begriffe „flood“, ‚drop‘ und „forward“ auf bestimmte Aktionen, die von Netzwerkgeräten (z. B. Switches) beim Umgang mit Multicast-Verkehr durchgeführt werden. Hier eine Erklärung der einzelnen Begriffe:

Hier finden Sie eine Erklärung der einzelnen Begriffe:

Flood

Definition: Wenn ein Switch Multicast-Datenverkehr „flutet“, sendet er die Multicast-Pakete an alle Ports innerhalb eines VLAN, mit Ausnahme des Ports, von dem das Paket empfangen wurde. Dies ähnelt der Verarbeitung von Broadcast-Paketen.

Szenario: Dies geschieht, wenn der Switch nicht weiß, welche Ports Empfänger für eine bestimmte Multicast-Gruppe haben. Wenn beispielsweise „Flood Unknown Multicast“ aktiviert ist und der Switch keine IGMP-Berichte für eine Multicast-Gruppe empfangen hat, wird der Multicast-Verkehr an alle Ports im VLAN weitergeleitet.

Drop

Definition: „Dropping“ von Multicast-Verkehr bedeutet, dass der Switch die Multicast-Pakete verwirft, ohne sie an einen Port weiterzuleiten.

Szenario: Dies kann auftreten, wenn der Switch keine IGMP-Berichte für eine Multicast-Gruppe empfangen hat und „Flood Unknown Multicast” deaktiviert ist. In diesem Fall geht der Switch davon aus, dass keine interessierten Empfänger vorhanden sind, und verwirft den Multicast-Datenverkehr.

Weiterleiten

Definition: „Weiterleiten” von Multicast-Datenverkehr bedeutet, dass der Switch die Multicast-Pakete nur an die Ports sendet, an denen er interessierte Empfänger kennt.

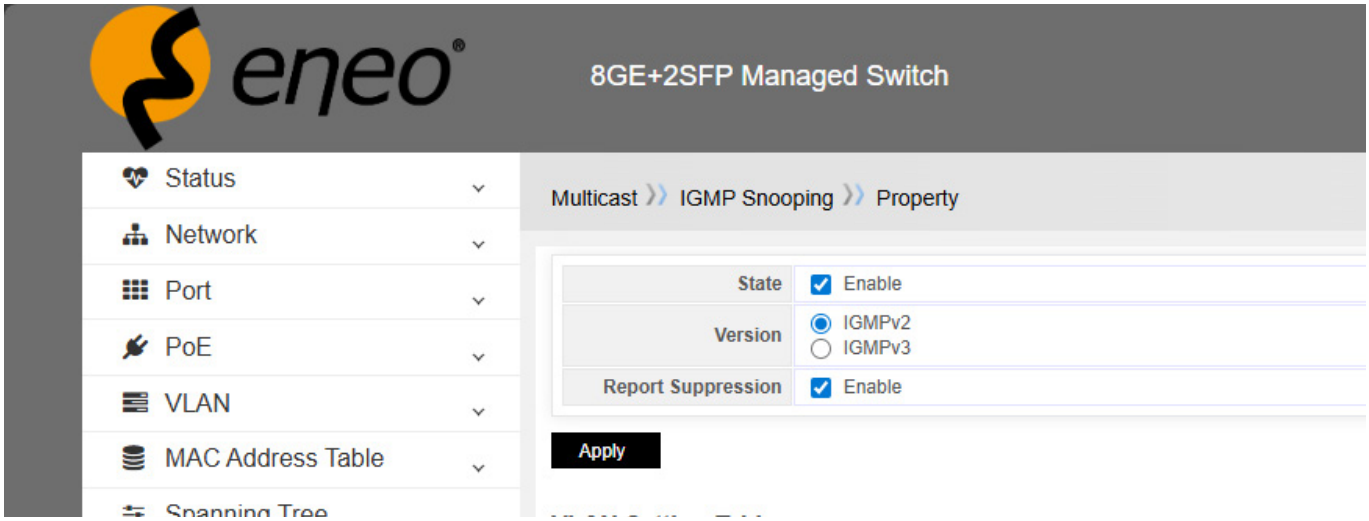
Szenario: Dies geschieht, wenn der Switch IGMP-Berichte von Hosts empfangen hat, die ihr Interesse an einer Multicast-Gruppe signalisieren. Der Switch leitet den Multicast-Verkehr dann nur an diese Ports weiter. Wenn ein Switch beispielsweise einen IGMP-Bericht von einem Host an einem bestimmten Port empfängt, leitet er den Multicast-Verkehr für diese Gruppe an diesen Port weiter.

10.3.2 – IGMP-Snooping aktivieren

Der Standardstatus von IGMP Snooping auf dem Switch ist aktiviert, was als globaler Toggle zum Aktivieren oder Deaktivieren von IGMP Snooping auf dem Switch dient. Standardmäßig unterstützt der Switch IGMPv2, das auf dem Markt überwiegend in den Versionen v1 und v2 eingesetzt wird. Natürlich unterstützt dieser Switch auch v3.

Der Standardstatus von IGMP Snooping für VLANs auf dem Switch ist jedoch deaktiviert, so dass IGMP Snooping für jedes einzelne VLAN aktiviert werden muss, damit es wirksam wird.

So aktivieren Sie die IGMP-Snooping-Funktion von VLAN1:



Status: Aktivieren oder deaktivieren Sie IGMP-Snooping.

Version: Wählen Sie IGMPv2 oder IGMPv3. Im Folgenden finden Sie einen Vergleich der Funktionen:

IGMP v2:

- Verwaltet die Mitgliedschaft in Multicast-Gruppen.
- Ermöglicht Hosts das Beitreten zu oder Verlassen von Multicast-Gruppen.
- Führt einen expliziten Austrittsmechanismus ein, um unnötigen Datenverkehr zu reduzieren.
- Bietet effiziente Abfrage- und Berichtsmechanismen zur Verwaltung der Gruppenmitgliedschaft.

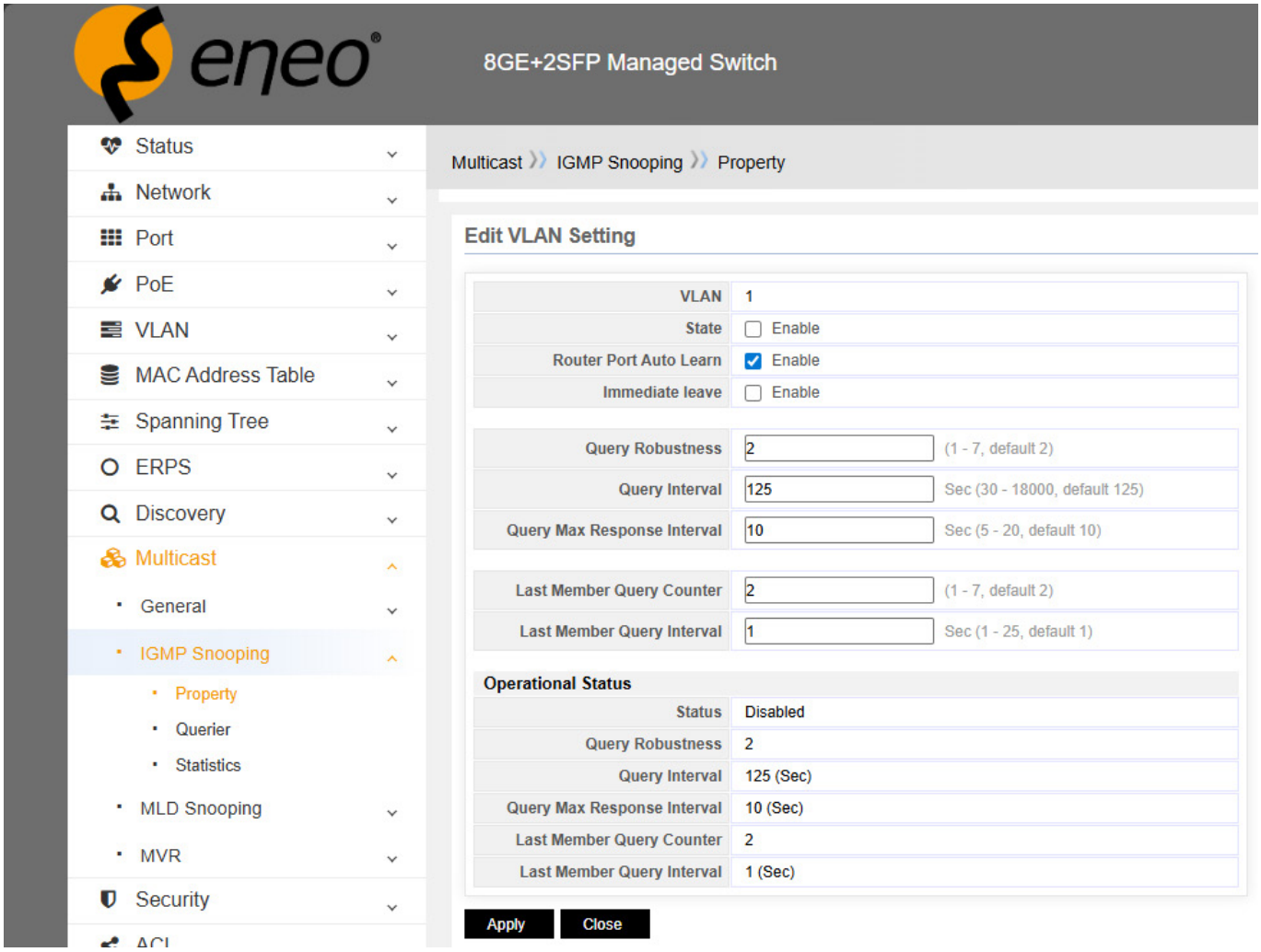
IGMP v3:

Alle Funktionen von IGMP v2 plus:

- Unterstützt Source-Specific Multicast (SSM), wodurch Hosts sowohl die Multicast-Gruppe als auch die gewünschten Quellen angeben können.
- Bietet eine detailliertere Kontrolle über den Multicast-Datenverkehr durch verbesserte Berichte zur Mitgliedschaft und quellenspezifische Abfragen.

Unterdrückung von Berichten:

Die Unterdrückung von Berichten ist ein Mechanismus, der die Anzahl der IGMP-Berichtsnachrichten in einem Netzwerk reduziert. Dies trägt dazu bei, Netzwerküberlastungen und die Verarbeitungslast auf den Geräten zu minimieren.



VLAN: Die zu konfigurierende VLAN-ID (hier VLAN 1).

Status: Mit diesem Kontrollkästchen können Sie das VLAN aktivieren oder deaktivieren. Wenn „Aktivieren" aktiviert ist, ist das VLAN aktiviert; wenn es deaktiviert ist, ist das VLAN deaktiviert.

Router Port Auto Learn: Wenn diese Option aktiviert ist, kann der Switch automatisch Geräte erkennen und erfassen, die an als Router-Ports konfigurierte Ports angeschlossen sind.

Immediate leave: Wenn diese Option aktiviert ist, sendet der Switch sofort eine Leave-Nachricht an den Router, wenn ein Gerät eine Multicast-Gruppe verlässt, anstatt bis zum Ende des Abfrageintervalls zu warten.

Query Robustness: Dieser Wert gibt die Robustheit von IGMP-Abfragen an, d. h. die Toleranz des Systems gegenüber verlorenen IGMP-Abfragen aufgrund von Netzwerkproblemen. Ein höherer Wert bedeutet eine größere Toleranz gegenüber Verlusten.

Query Interval: Dieser Wert definiert das Zeitintervall zwischen den vom Router gesendeten IGMP-Abfragen in Sekunden. Ein kürzeres Intervall ermöglicht eine schnellere Erkennung von Änderungen in der Multicast-Gruppenmitgliedschaft, erhöht jedoch den Netzwerkverkehr.

Query Max Response Interval: Dieser Wert definiert die maximale Zeit, die ein Mitglied einer Multicast-Gruppe nach dem Empfang einer IGMP-Abfrage zum Antworten hat, gemessen in Sekunden.

Last Member Query Counter: Dieser Wert definiert, wie oft der Router IGMP-Abfragen sendet, nachdem das letzte Mitglied einer Multicast-Gruppe die Gruppe verlassen hat. Dieser Mechanismus stellt sicher, dass alle Mitglieder die Gruppe tatsächlich verlassen haben.

Last Member Query Interval: Dieser Wert definiert das Zeitintervall zwischen IGMP-Abfragen, die vom Router gesendet werden, nachdem der letzte Teilnehmer einer Multicast-Gruppe die Gruppe verlassen hat, gemessen in Sekunden.

Abschnitt „Betriebsstatus“

Status: Zeigt den aktuellen Status des VLAN an, der in diesem Fall „Deaktiviert“ lautet und angibt, dass das VLAN derzeit nicht aktiv ist.

Query Robustness: Zeigt den aktuellen Wert der IGMP-Abfrage-Robustheit an, der 2 beträgt.

Query Interval: Zeigt das aktuelle Zeitintervall zwischen IGMP-Abfragen an, das 125 Sekunden beträgt.

Query Max Response Interval: Zeigt die maximale Zeit an, die ein Mitglied einer Multicast-Gruppe nach dem Empfang einer IGMP-Abfrage zum Antworten hat, die 10 Sekunden beträgt.

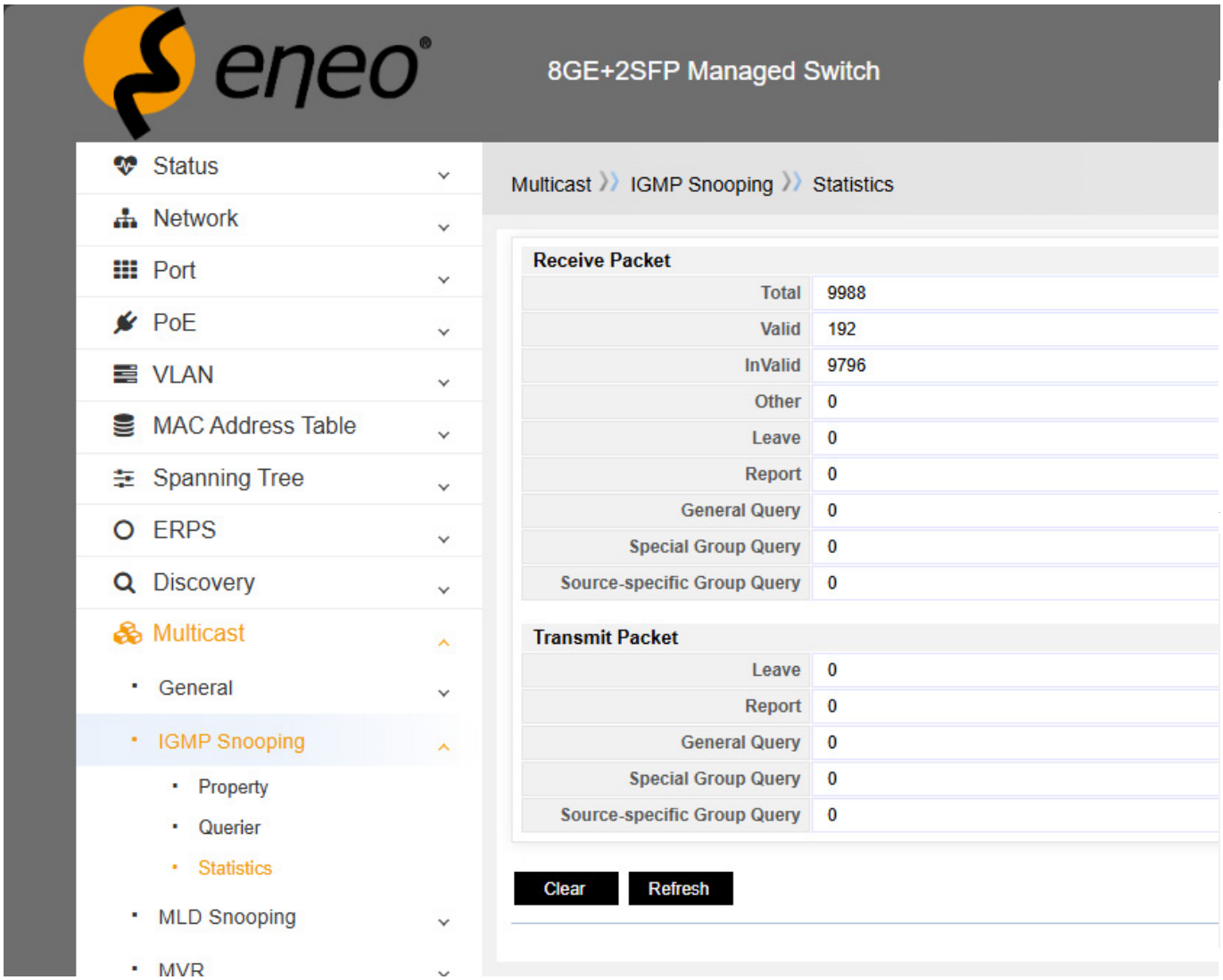
Last Member Query Counter: Zeigt an, wie oft der Router IGMP-Abfragen sendet, nachdem das letzte Mitglied einer Multicast-Gruppe verlassen hat. Der Wert ist 2.

Last Member Query Interval: Zeigt das Zeitintervall zwischen den IGMP-Abfragen an, die der Router sendet, nachdem das letzte Mitglied einer Multicast-Gruppe verlassen hat. Der Wert ist 1 Sekunde.

Hinweis!

Die Alterungszeit für Multicast beträgt standardmäßig 260 Sekunden. Wenn sie erhöht werden muss, kann die Abfrageintervallzeit auf 18000 geändert werden, die Alterungszeit beträgt dann 36010 Sekunden.

10.3.3 – IGMP-Protokollpaketstatistik



10.3.3.1 – Paket empfangen

Total: Die Gesamtzahl der vom Switch empfangenen IGMP-Pakete.

Valid: Die Anzahl der empfangenen gültigen IGMP-Pakete. Gültige Pakete sind solche, die ordnungsgemäß formatiert sind und vom Switch korrekt verarbeitet werden.

InValid: Die Anzahl der empfangenen ungültigen IGMP-Pakete. Dies sind Pakete, die entweder fehlerhaft formatiert sind oder nicht korrekt verarbeitet werden können.

Other: Die Anzahl der IGMP-Pakete, die nicht in die Kategorien „Gültig“ oder „Ungültig“ fallen. Dazu können Pakete gehören, die für die aktuelle IGMP-Snooping-Konfiguration nicht relevant sind.

Leave: Die Anzahl der empfangenen IGMP-Leave-Group-Meldungen. Diese Meldungen werden von Hosts gesendet, wenn sie eine Multicast-Gruppe verlassen möchten.

Report: Die Anzahl der empfangenen IGMP-Membership-Report-Meldungen. Diese Meldungen werden von Hosts gesendet, um anzuzeigen, dass sie Multicast-Datenverkehr von einer bestimmten Gruppe empfangen möchten.

General Query: Die Anzahl der empfangenen IGMP-Allgemeinen-Abfrage-Nachrichten. Diese werden von Multicast-Routern gesendet, um festzustellen, welche Hosts Mitglieder welcher Multicast-Gruppen sind.

Special Group Query: Die Anzahl der empfangenen IGMP-Spezielle-Gruppenabfrage-Nachrichten. Diese werden an bestimmte Multicast-Adressen gesendet, um Mitglieder dieser Gruppen zu ermitteln.

Source-specific Group Query: Die Anzahl der empfangenen IGMP-Nachrichten zur quellen-spezifischen Gruppenabfrage. Diese werden in der quellen-spezifischen Multicast-Übertragung (SSM) verwendet, um Mitglieder abzufragen, die an Datenverkehr von bestimmten Quellen zu einer Multicast-Gruppe interessiert sind.

10.3.3.2 – Paket übertragen

Leave: Die Anzahl der vom Switch übertragenen IGMP-Leave-Group-Meldungen.

Report: Die Anzahl der vom Switch übertragenen IGMP-Mitgliedschaftsberichts-Meldungen.

General Query: Die Anzahl der vom Switch übertragenen IGMP-Allgemeinen Abfrage-Meldungen.

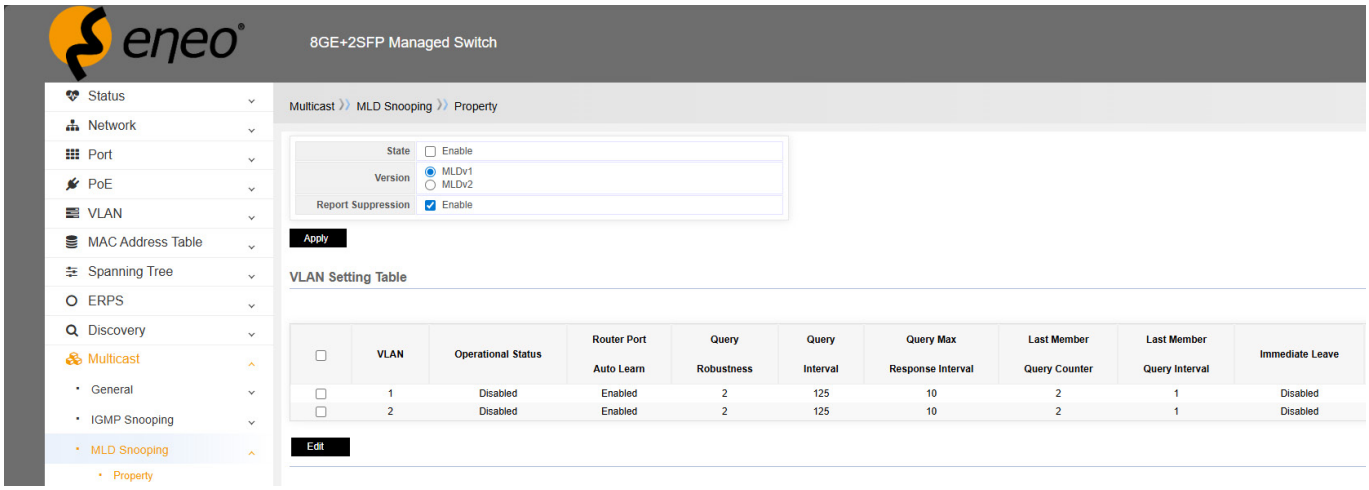
Special Group Query: Die Anzahl der vom Switch übertragenen IGMP-Spezielle Gruppenabfrage-Meldungen.

Source-specific Group Query: Die Anzahl der vom Switch übertragenen IGMP-Quellenspezifische Gruppenabfrage-Meldungen.

- **Problemquelle lokalisieren:** Bei einem Netzwerkfehler kann die IGMP-Protokollnachrichtenstatistik detaillierte Informationen zu den Nachrichten liefern und Netzwerkadministratoren dabei helfen, die Ursache des Problems schnell zu finden.
- **Protokollinteraktionen analysieren:** Durch die statistische Analyse der Interaktionen von IGMP-Protokollnachrichten können wir die Kompatibilität und Stabilität zwischen Netzwerkprotokollen bewerten und so Kommunikationsprobleme beheben, die durch Protokollinkompatibilitäten entstehen.

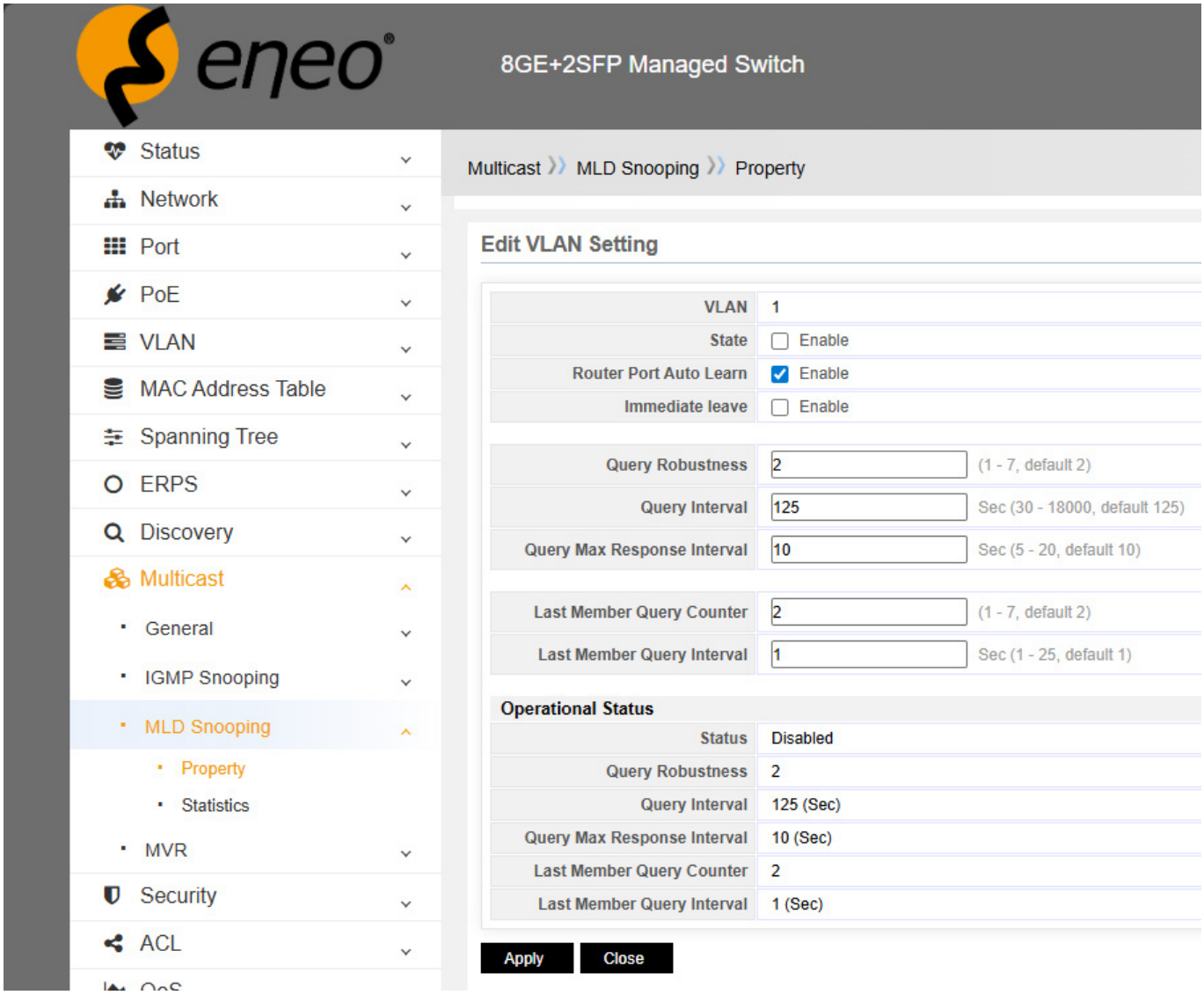
10.3.4 – MLD-Snooping

MLD Snooping, kurz für Multicast Listener Discovery Snooping, ist eine Funktion, die vor allem auf Layer-2-Geräten in IPv6-Multicast-Netzwerken zum Einsatz kommt. Sie dient als Mechanismus zur Verwaltung und Steuerung von IPv6-Multicast-Gruppen durch Analyse der empfangenen MLD-Nachrichten (Multicast Listener Discovery). Konkret wird eine Zuordnung zwischen Ports und MAC-Multicast-Adressen hergestellt und IPv6-Multicast-Daten auf Basis dieser Zuordnung weitergeleitet.



- Benutzer müssen den MLD-Snooping-Status auf „aktiviert“ setzen und auswählen, ob die Version MLDv1 oder MLDv2 unterstützt werden soll.
- Zusätzlich muss das VLAN-basierte MLD-Snooping auf „aktiviert“ gesetzt werden.

Kontrollieren Sie die Option MLD-Snooping-Eintrag für VLAN1 und klicken Sie auf die Schaltfläche „Edit/Bearbeiten“.

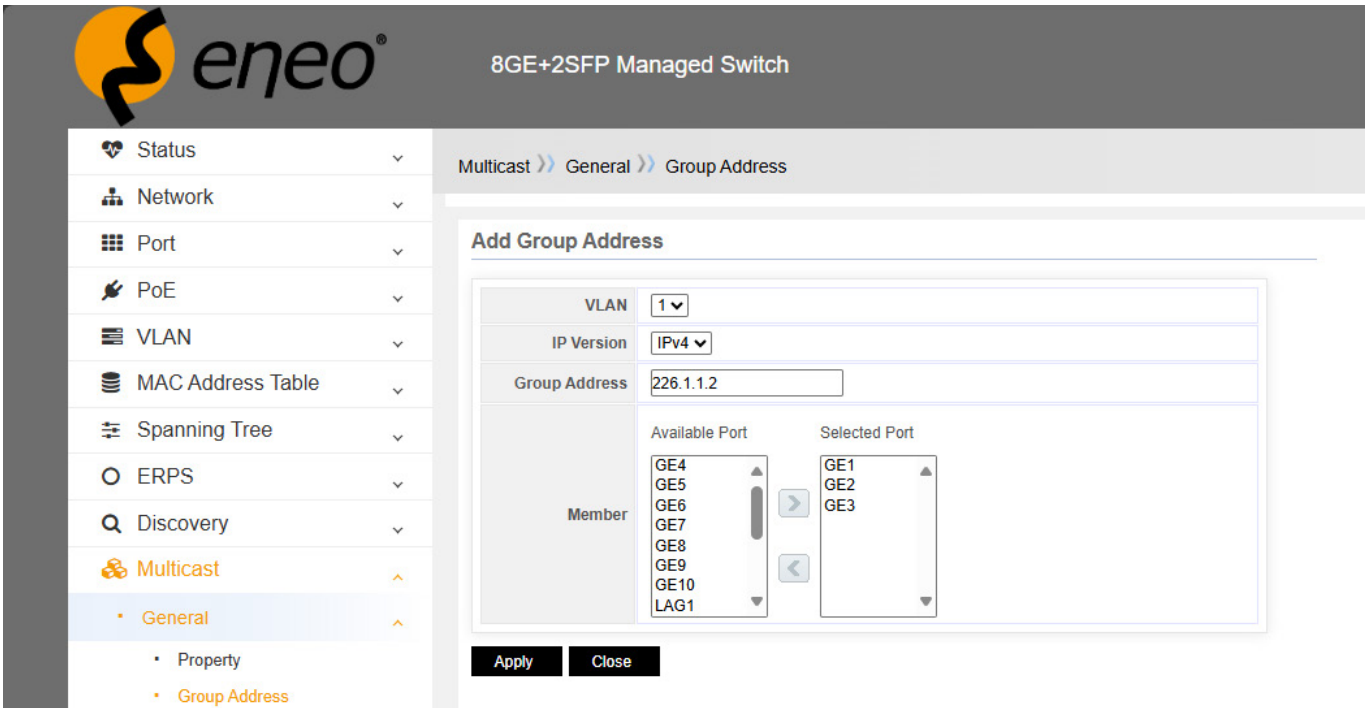


- **MLD-Snooping-Status:** Legen Sie den IGMP-Snooping-Status fest, aktivieren oder deaktivieren Sie ihn (muss aktiviert sein).
- **Automatisches Erlernen von Routing-Ports:** Legt fest, ob der Switch einen Port beim Empfang einer IGMP-Abfrage als Routing-Port lernt (muss aktiviert sein).
- **Sofortiges Verlassen:** Legt fest, ob der Switch ein Mitglied bei Empfang einer IGMP-Leave-Nachricht sofort aus der Multicast-Gruppe entfernt und ob das schnelle Verlassen aktiviert werden soll (gemäß den Anforderungen des Benutzers festlegen).

10.3.5 – IGMP-Gruppenadressentabelle

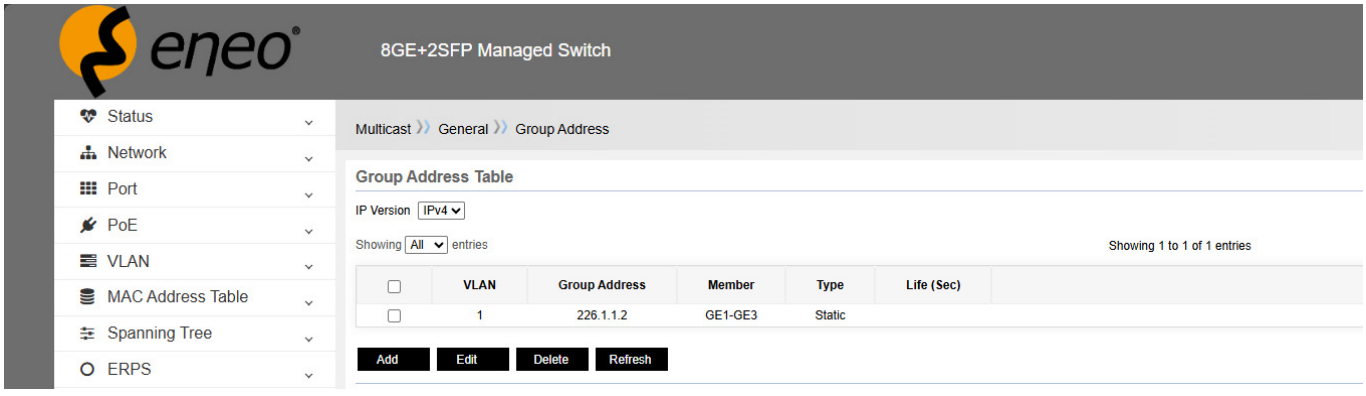
Wenn der entsprechende Port des Switches eine IGMP-Protokollnachricht empfängt, erstellt er basierend auf dem Inhalt eine Multicast-Adressentabelle.

Bei Bedarf kann der Benutzer auch manuell eine Multicast-Adressentabelle hinzufügen, indem er auf die Schaltfläche „Hinzufügen“ klickt und dann die Konfigurationsoberfläche einträgt.



Nachdem Sie das VLAN, die IP-Version, die Multicast-Adresse und die Mitgliedsports eingerichtet haben, klicken Sie auf die Schaltfläche „Übernehmen“, um die Konfiguration abzuschließen.

Schließlich sehen Sie in der Gruppenadressentabelle, dass die statische Multicast-Gruppe für 226.1.1.2 mit den Mitgliedsports 1-3 eingerichtet wurde.



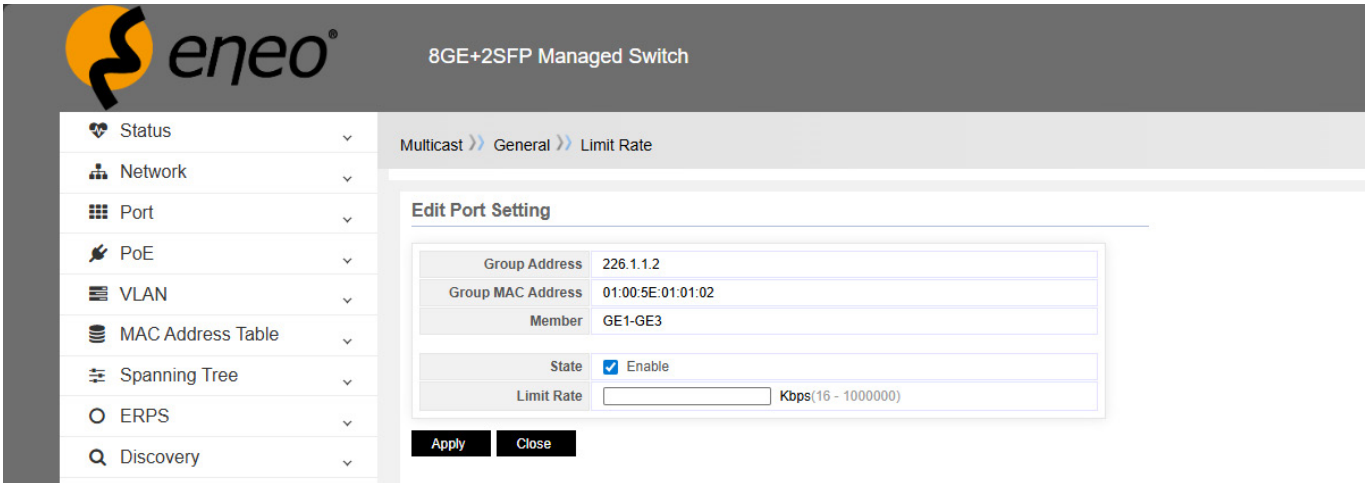
10.3.6 – IGMP-Multicast-Begrenzungsrate

Es gibt mehrere Vorteile:

- **Fein abgestimmte Verkehrssteuerung:** Mit der Funktion zur Begrenzung der Übertragungsrate können Netzwerkadministratoren den Datenverkehr bestimmter Multicast-Gruppen präzise steuern und die Bandbreitenzuweisung an den tatsächlichen Bedarf anpassen, um unterschiedlichen Netzwerkanforderungen in verschiedenen Anwendungsszenarien gerecht zu werden.
- **Verbesserte Benutzererfahrung:** Durch die Implementierung angemessener Ratenbegrenzungen können kritische Anwendungen oder Dienste für die Datenübertragung priorisiert werden, wodurch die Benutzererfahrung verbessert wird.
- **Abwehr bösartiger Datenverkehrangriffe:** Die Ratenbegrenzung von Multicast-Gruppen kann auch als Abwehrmechanismus gegen bösartige Datenverkehrangriffe dienen, indem die von Angriffsdatenverkehr verbrauchte Bandbreite begrenzt und somit dessen Auswirkungen auf das Netzwerk reduziert werden.

Wählen Sie die Multicast-Gruppe aus, für die eine Ratenbegrenzung erforderlich ist, klicken Sie auf die Schaltfläche „Edit/Bearbeiten“ und fahren Sie mit der Konfiguration fort.

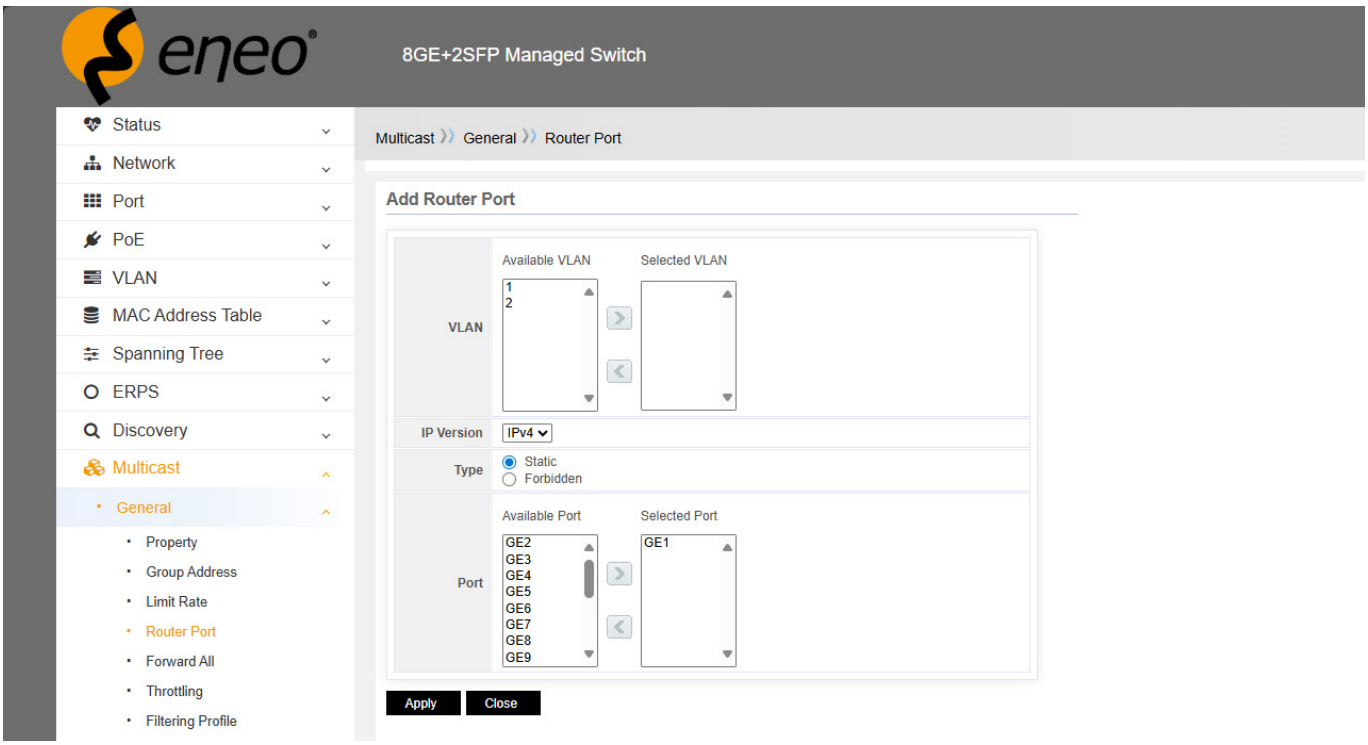
Aktivieren Sie das Kontrollkästchen, um den Status auszuwählen, geben Sie dann den Wert für die Ratenbegrenzung ein und klicken Sie abschließend auf „Übernehmen“, um den Vorgang abzuschließen.



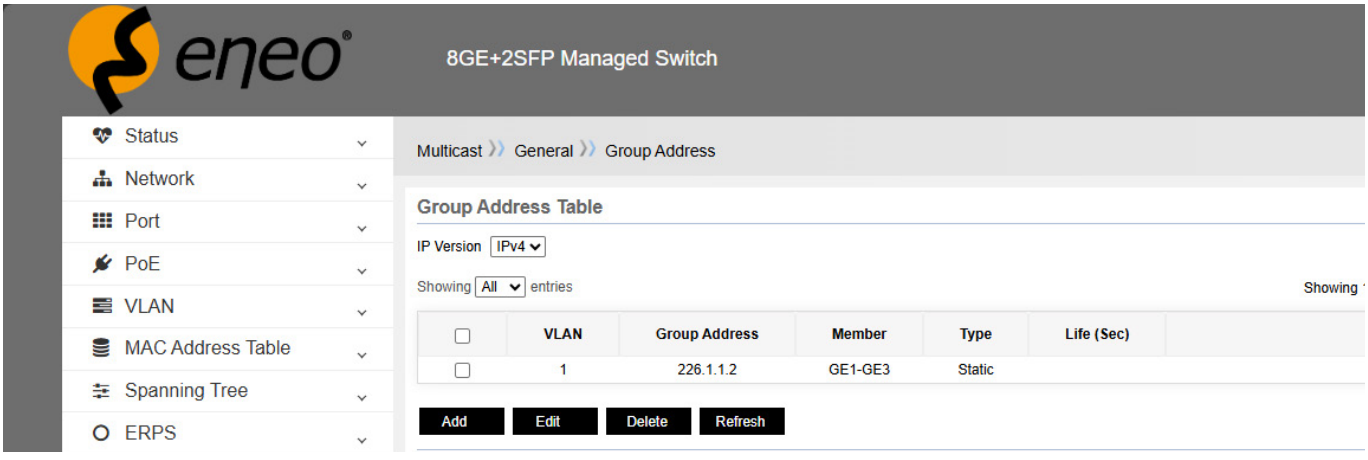
10.3.7 – IGMP-Router-Port

IGMP-Routing-Ports werden in zwei Typen unterteilt: dynamisch und statisch. Wenn ein Switch eine IGMP-Abfrage empfängt, erkennt er diesen Port automatisch als dynamischen Routing-Port. Benutzer können auch statische Routing-Ports manuell konfigurieren, die dieselbe Funktion wie dynamisch erkannte Routing-Ports haben.

Um beispielsweise den GE1-Port als ausgewählten Port festzulegen, klicken Sie auf die Schaltfläche „Übernehmen“ und schon sind Sie fertig.

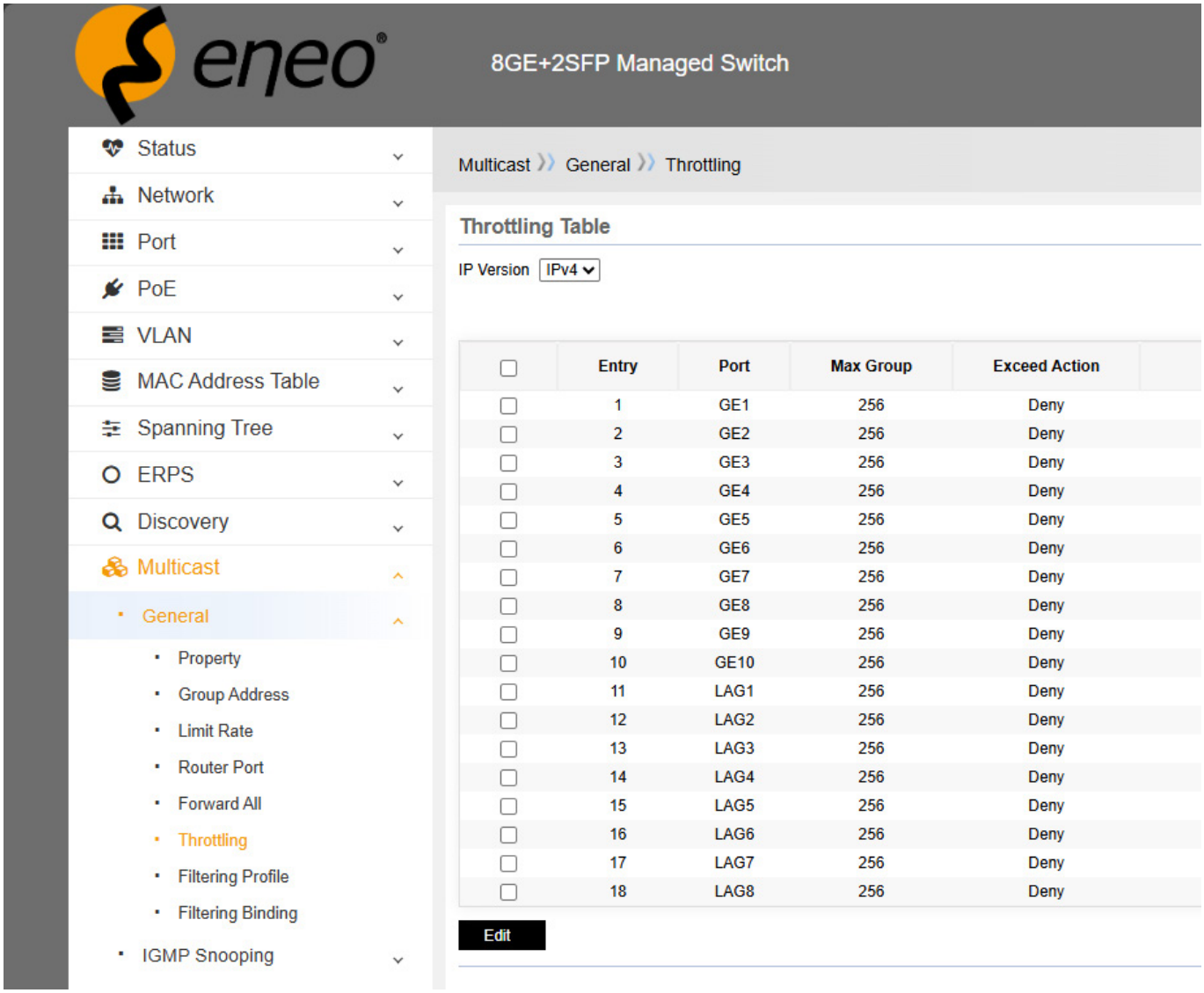


Wie Sie sehen können, wurde GE1 als Routing-Port konfiguriert, und es wird auch angezeigt, dass GE1 ein statischer Routing-Port ist.

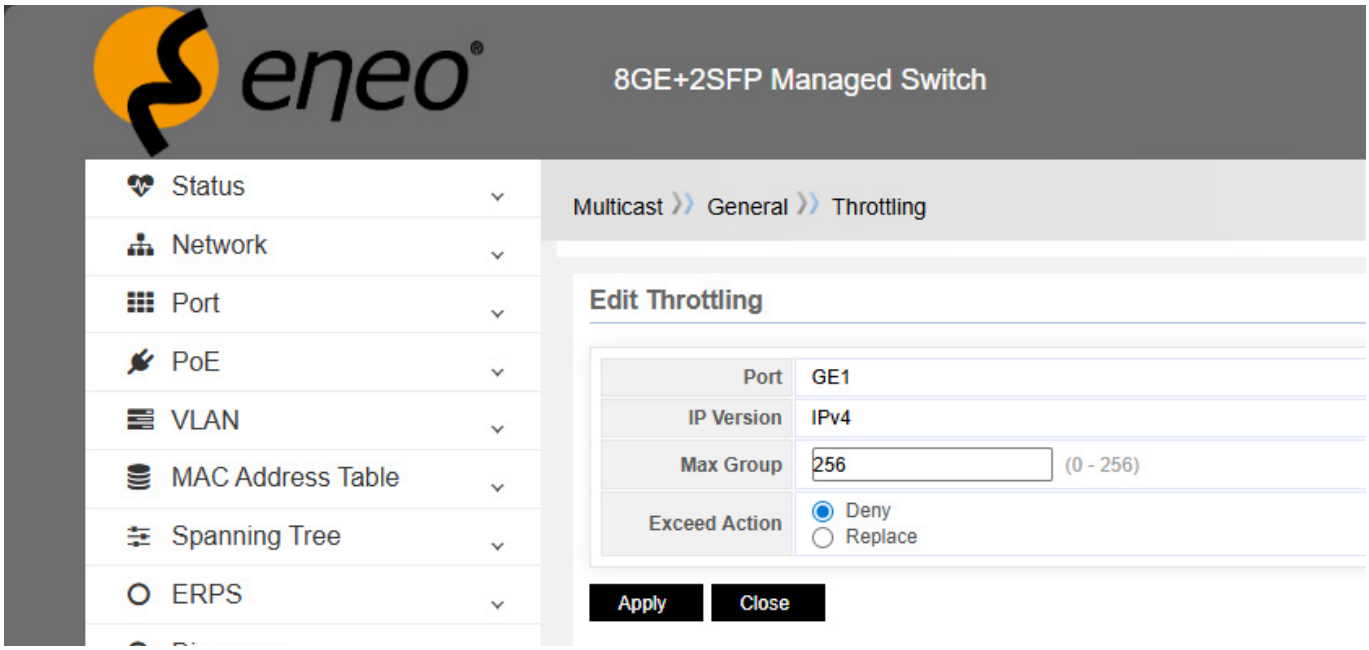


10.3.8 – Maximale Anzahl von Ports, die zu Multicast-Gruppen hinzugefügt werden können

Standardmäßig kann ein IGMP-Mitgliedsport bis zu 512 Multicast-Gruppen beitreten, aber Benutzer können die Anzahl der Multicast-Gruppen, denen er beitreten kann, begrenzen. Ein Benutzer kann beispielsweise den Port so einschränken, dass er nur einer Multicast-Gruppe beitreten kann.



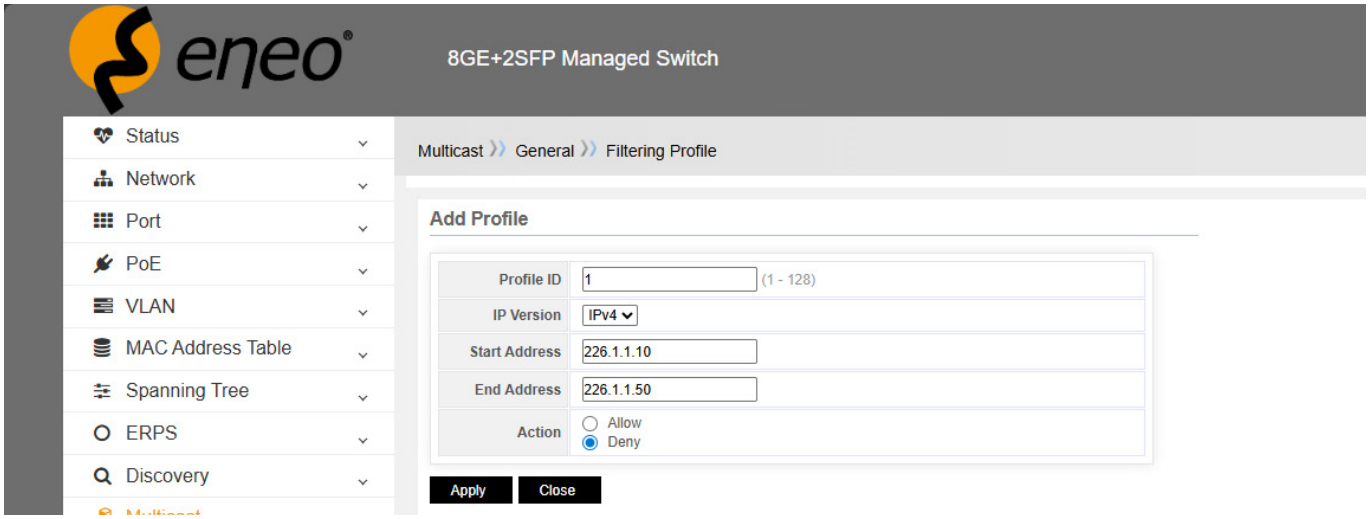
Wählen Sie den Port aus, der eingeschränkt werden soll. Wenn beispielsweise die maximale Gruppengrenze auf 1 festgelegt ist, kann dieser Port nur einer Multicast-Gruppe beitreten. Für alle weiteren Multicast-Gruppen haben Sie die Möglichkeit, diese entweder abzulehnen oder zu ersetzen. Ablehnen bedeutet, dass keine neuen Gruppen beigetreten werden, während Ersetzen bedeutet, dass die vorhandene Multicast-Gruppe durch eine neue ersetzt wird, der Port jedoch weiterhin nur Mitglied einer Multicast-Gruppe zu einem bestimmten Zeitpunkt ist.



10.3.9 – IGMP-Filtertabelle

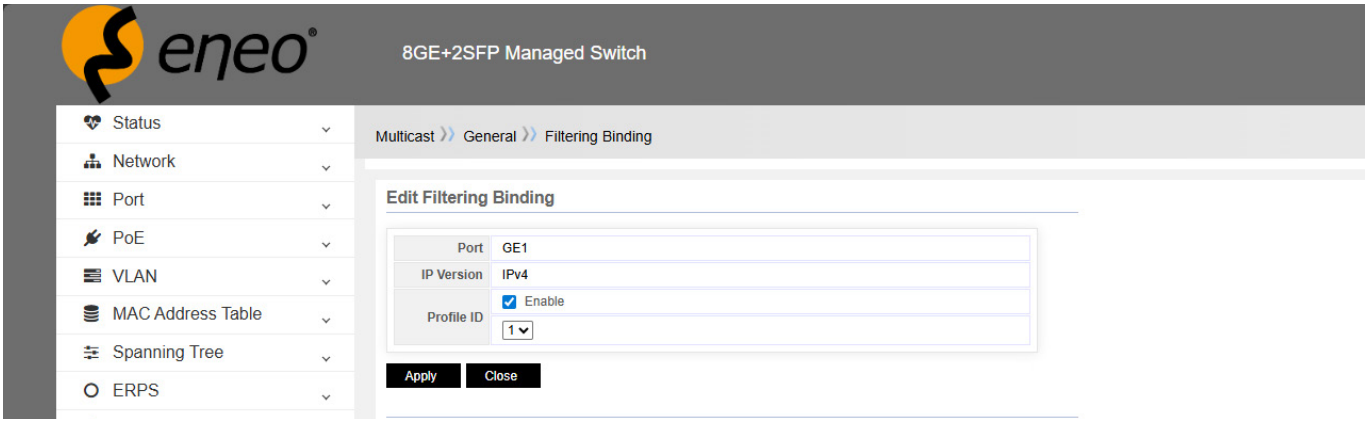
Die Funktion der IGMP-Filterung besteht in der Regel darin, einen bestimmten Port oder mehrere Ports, die der Multicast-Gruppe beigetreten sind, zu filtern. Benutzer können einige Multicasts und einige Ports entsprechend ihren tatsächlichen Anforderungen filtern, um den Anforderungen der Benutzer gerecht zu werden.

Daher müssen die IGMP-Filtertabelle und der IGMP-Filterport zusammen verwendet werden.



Um beispielsweise eine Filterregel hinzuzufügen, wählen Sie als IP-Versionsinformation „IPv4“, legen Sie die Startadresse auf „226.1.1.10“ und die Endadresse auf „226.1.1.50“ fest und setzen Sie die Aktion auf „Ablehnen“.

Binden Sie die Filterregel an die angegebenen Ports, wie in der folgenden Abbildung dargestellt:



Binden Sie diese Regel dann an Port 1 und Port 3. Dadurch wird der vom Server gesendete Multicast-Stream dieser Gruppe nicht an die Ports 1 und 3 weitergeleitet, selbst wenn Port 1 und 3 der Multicast-Gruppe 226.1.1.22 beigetreten sind.

10.3.10 – MVR

Die MVR-Funktion (Multicast VLAN Registration) ist eine wesentliche Komponente für Multicast-Umgebungen. Sie erleichtert in erster Linie die Replikation von Multicast-Streams über VLANs hinweg.

Mit MVR können Client-PCs in ihren individuellen VLANs verbleiben und dennoch auf gemeinsam genutzte Multicast-Streams zugreifen. Dies ist besonders nützlich in Szenarien, in denen Multicast-Ressourcen über verschiedene VLANs hinweg gemeinsam genutzt werden müssen, z. B. bei Videokonferenzen oder Live-Fernsehübertragungen über das Netzwerk.

Funktionsprinzip von MVR

In einem Multicast-Szenario werden Multicast-Daten, die von einer Multicast-Quelle gesendet werden, an alle Hosts repliziert, die an dieser Multicast-Gruppe interessiert sind. In herkömmlichen VLAN-Konfigurationen sind VLANs jedoch voneinander isoliert, sodass Multicast-Daten nicht direkt über VLANs übertragen werden können.

MVR löst dieses Problem durch einen Registrierungsmechanismus. Wenn ein Host innerhalb eines VLANs Interesse an einer bestimmten Multicast-Gruppe bekundet, registriert dieses VLAN sein Interesse beim Switch. Der Switch repliziert dann die Multicast-Daten für diese Gruppe an alle VLANs, die Interesse bekundet haben, und aktiviert so die VLAN-übergreifende Freigabe von Multicast-Daten.

Anwendungsszenarien für MVR

MVR ist in Szenarien entscheidend, die eine groß angelegte Bereitstellung von Multicast-Anwendungen erfordern. In Unternehmensnetzwerken kann es beispielsweise erforderlich sein, Videokonferenzen oder Live-Fernsehübertragungen über verschiedene Abteilungen oder Etagen hinweg gemeinsam zu nutzen. Durch Aktivieren von MVR können diese Ressourcen problemlos über VLANs hinweg gemeinsam genutzt werden, ohne dass separate Multicast-Quellen in jedem VLAN bereitgestellt werden müssen.

MVR konfigurieren

Bei der Konfiguration der MVR-Funktion gibt es zwei Arten von MVR-Ports: Quellports und Empfangsports.

- **Quellport:** Ein Quellport ist der Port, über den Multicast-Streams in einem Multicast-VLAN übertragen werden.
- **Empfangsport:** Dies ist der Port eines Switches, der mit einem Multicast-hörenden Host verbunden ist. Er kann in jedem anderen VLAN als dem Multicast-VLAN oder in einem VLAN-losen Zustand platziert werden (VLAN-los bezieht sich normalerweise auf VLAN1, wo der Datenverkehr nicht getaggt ist). Dies bedeutet, dass der Switch mit aktiviertem MVR einen VLAN-Tag-Austausch durchführt und den VLAN-Tag des Multicast-Empfangsportes durch den VLAN-Tag des Quellportes ersetzt.

Multicast-VLAN bezieht sich auf ein dediziertes VLAN für MVR, das manuell in einem bestimmten Netzwerk konfiguriert werden muss. Es muss für alle Quellports explizit konfiguriert werden.
Es wird häufig verwendet, um Multicast-Streams im Netzwerk zu übertragen und gleichzeitig die Duplizierung von Multicast-Streams in verschiedenen VLANs zu vermeiden.

MVR verfügt über zwei Konfigurationsmodi: den kompatiblen Modus und den dynamischen Modus

- **Kompatibler Modus:** Im kompatiblen Modus leitet die CPU des MVR-Switches normalerweise Abfragen von Routern weiter und verarbeitet Berichtsnachrichten von Clients, um eine dynamisch erlernte Multicast-Weiterleitungstabelle zu erstellen. Die CPU leitet jedoch keine Berichtsnachrichten an Router-Ports weiter, sodass der übergeordnete Router die zugrunde liegenden Berichtsnachrichten nicht empfängt, was dazu führt, dass die Routerdaten nicht normal an den Switch weitergeleitet werden können. In diesem Modus muss die Multicast-Weiterleitungstabelle des Routers manuell konfiguriert werden, um Daten an den Switch weiterzuleiten.
- **Dynamischer Modus:** Der einzige Unterschied zwischen dem dynamischen Modus und dem kompatiblen Modus besteht darin, dass im dynamischen Modus die CPU Berichtsnachrichten an Router-Ports weiterleiten kann, sodass übergeordnete Router die Multicast-Weiterleitungstabelle dynamisch lernen können, ohne dass die Multicast-Weiterleitungstabelle des Routers manuell konfiguriert werden muss, um Daten an den Switch weiterzuleiten.

11 – ACL

11.1 – ACL Übersicht

Aufgrund des zunehmenden Umfangs und Datenverkehrs von Netzwerken spielen Sicherheitskontrollen und Bandbreitenzuweisung eine immer wichtigere Rolle im Netzwerkmanagement. Durch das Filtern von Paketen kann der Zugriff unbefugter Benutzer auf das Netzwerk wirksam verhindert, der Netzwerkverkehr gesteuert und Netzwerkressourcen gespart werden. Zugriffskontrolllisten (ACLs) werden häufig verwendet, um Übereinstimmungsregeln für die Paketfilterung zu konfigurieren.

Wenn eine Nachricht empfangen wird, vergleicht der Switch die Nachricht mit den ACL-Regeln, die auf den aktuellen Port angewendet werden, um die Nachricht zuzulassen oder zu verwerfen.

Eine ACL-Regel kann von anderen IP- und MAC-Typ-Klassifizierungsreferenzen verwendet werden. Eine ACL verwendet eine Reihe von Bedingungen, die als Regeln bezeichnet werden, um Pakete zu klassifizieren. Bedingungen können auf dem Pakettyp, der Quelladresse, der Zieladresse und der Portnummer basieren, die das Paket enthält.

ACL wird entsprechend ihrem Anwendungszweck in die folgenden drei Typen unterteilt:

- **MAC-basierte ACL:** Regeln werden nur auf der Grundlage der Quell-MAC-Adresse und der Ziel-MAC-Adresse erstellt.
- **ACL basierend auf IPv4:** Regeln werden basierend auf Informationen der Schichten 3 und 4 erstellt, wie z. B. Quell- und Ziel-IP-Adressen, vom IP transportierter Protokolltyp, detaillierte Protokollmerkmale usw.;
- **IPv6-basierte ACL:** Regeln werden basierend auf Informationen der Schichten 3 und 4 erstellt, wie z. B. Quell- und Ziel-IP-Adressen, vom IP transportierter Protokolltyp, detaillierte Protokollmerkmale usw.;

11.2 – Zugriffskontrollparameter verstehen

Bevor Sie eine ACL auf einem Switch konfigurieren, müssen Sie die Zugriffskontrollparameter (ACP) gut verstehen. ACP in der CLI-Ausgabe eines Switches umfasst Masken.

Jeder ACE verfügt über eine Maske und eine Regel. Die Klassifizierungsdomäne oder Maske ist die Domäne, in der Sie eine Aktion ausführen möchten. Die Angabe eines Werts und einer bestimmten Maske wird als Regel bezeichnet.

Nachrichten können in diesen Domänen der Schichten 2, 3 und 4 klassifiziert werden:

Layer 2:

- Quell-MAC-Adresse (alle 48 Bits angeben)
- Zweck-MAC-Adresse (alle 48 Bits angeben)
- Ether-Typ (16-Bit-Ether-Typ-Feld)

Sie können einen Teil oder alle diese Domänen verwenden, um einen Stream zu definieren.

Layer 3:

- **IP-Quelladresse**

  (Geben Sie alle 32-Bit-IP-Quelladressen an, um den Stream zu definieren, oder geben Sie ein benutzerdefiniertes Subnetz an. Es gibt keine Einschränkungen für das angegebene IP-Subnetz.)

- **IP-Zieladresse**

  (Gibt alle 32-Bit-IP-Zieladressbits an, um den Stream zu definieren, oder gibt ein benutzerdefiniertes Subnetz an. Es gibt keine Einschränkungen für das angegebene IP-Subnetz.)

Sie können einen Stream mit einem Teil oder allen dieser Domänen definieren.

Layer 4:

- TCP (Sie können TCP, Quellport, Zielport oder beides angeben)
- UDP (Sie können UDP, Quelle, Zielportnummer oder beides angeben)

11.3 – Beispielkonfiguration von ACL

ACL benennen

Beim Erstellen von MAC-ACL, IPv4-ACL und IPv6-ACL müssen Benutzer zunächst einen Namen für die ACL angeben. Jeder ACL-Typ kann mehrere Namen haben. Benannte ACLs ermöglichen es Benutzern, eine ACL anhand ihres Namens zu identifizieren und entsprechende Vorgänge auszuführen. Beim Erstellen einer ACL müssen Benutzer zunächst den Namen konfigurieren. Nachdem eine ACL erstellt wurde, können Benutzer sie löschen, aber nicht mehr ändern.

ACL-Übereinstimmungsreihenfolge

Eine ACL kann mehrere Regeln enthalten, wobei jede Regel unterschiedliche Optionen für die Paketübereinstimmung festlegt. Diese Regeln können doppelt vorhanden oder widersprüchlich sein. Welche Regeln sollten verwendet werden, wenn ein Paket mit den Regeln einer ACL übereinstimmt? Die Reihenfolge der übereinstimmenden Regeln muss festgelegt werden.

Die folgenden Grundsätze gelten für die Festlegung der Priorität einer ACL

Konfigurationsreihenfolge: Die Regeln werden in der Reihenfolge der Benutzerkonfigurationsregeln und auch in der Reihenfolge der ACL-Seriennummern abgeglichen.

Anzahl der ACL-Einträge

Basierend auf MAC, IPv4 und IPv6 beträgt die Gesamtzahl der Einträge 1000, die von Benutzern zugewiesen werden können.

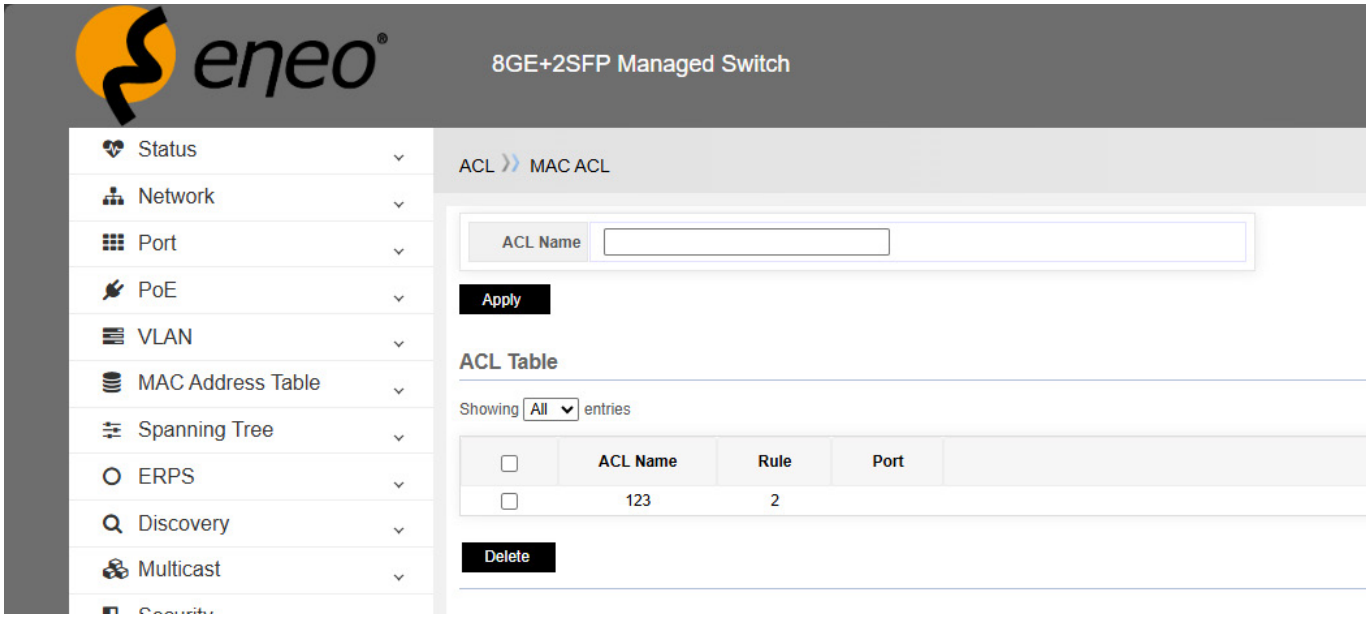
Für Port-Bindungs-ACL-Eintragregeln

ACL-Einträge können an einen bestimmten Port gebunden werden, der einzeln mit MAC, IPv4 und IPv6 ACL übereinstimmen kann. Wenn sie jedoch gleichzeitig übereinstimmen, kann nur MAC ACL + IPv4 ACL oder MAC ACL + IPv6 ACL übereinstimmen.

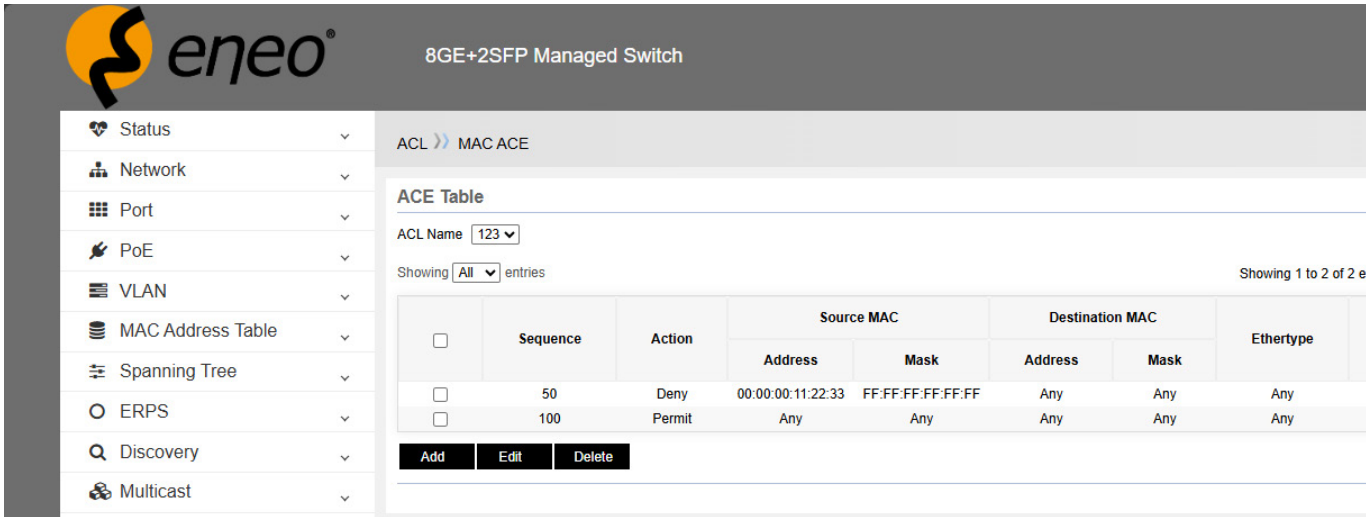
Das heißt, IPv4 kann beispielsweise mehrere Namens-ACL-Regeln festlegen, Port 1 kann mit einer davon übereinstimmen, Port 2 kann mit einer anderen Regel übereinstimmen.

MAC ACL

Ein Eintrag mit ACL 123 ist konfiguriert



Anschließend wurden zwei Regeln zu den MAC ACE-Regeln hinzugefügt

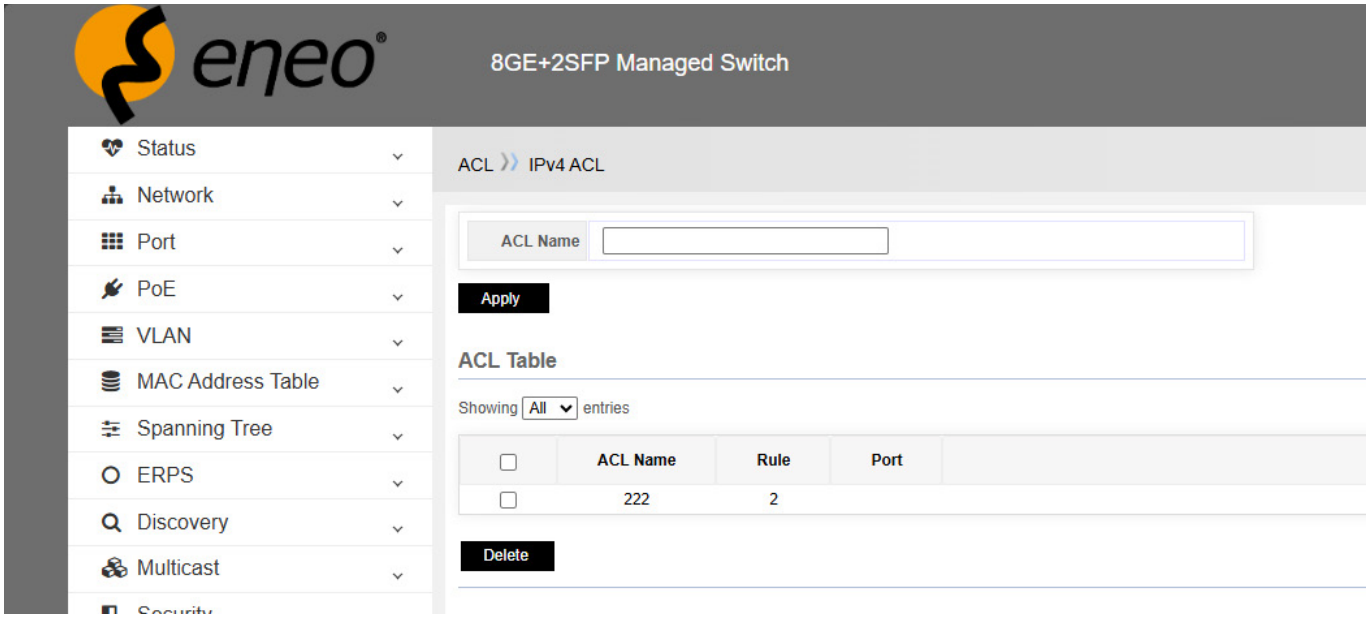


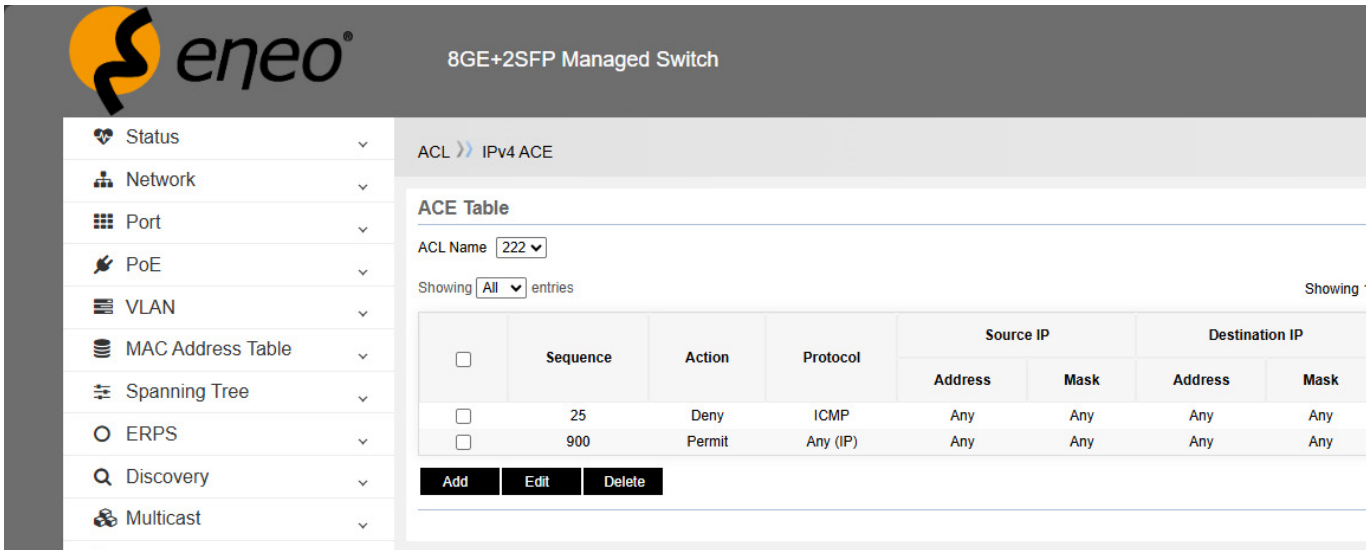
Konfiguration der MAC-ACL-Regeln

- Die erste Regel lehnt Nachrichten mit der MAC-Adresse 00:00:00:11:22:33 ab.
- Die zweite Regel lässt alle Nachrichten basierend auf der MAC-Adresse durch.

IPv4 ACL

Ein Eintrag mit ACL 222 ist konfiguriert.



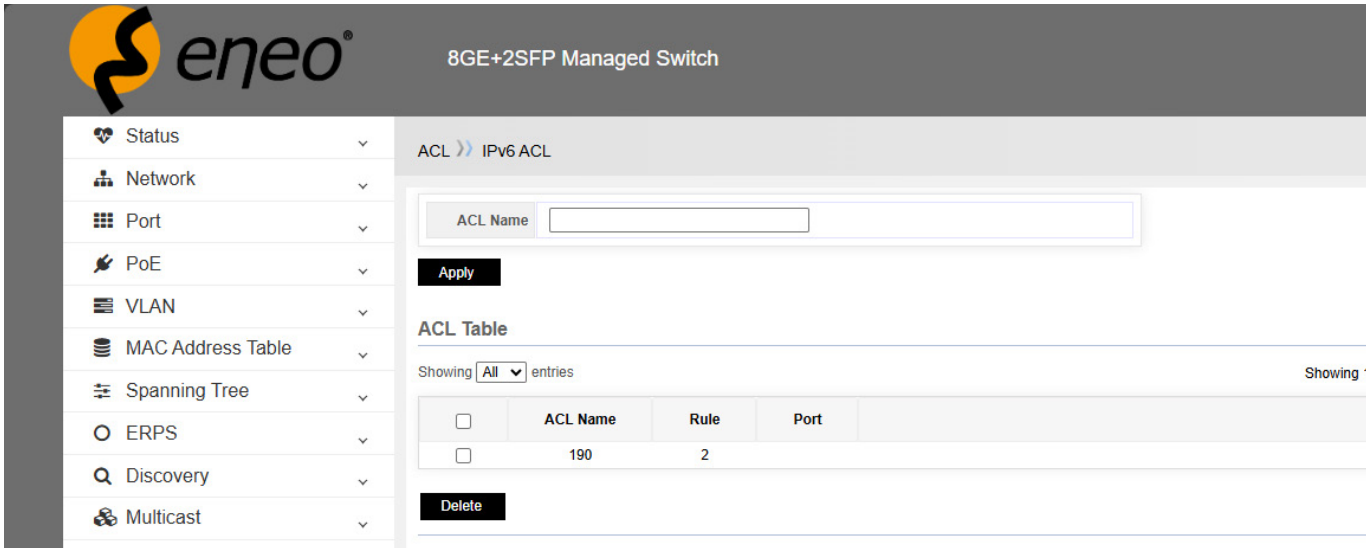


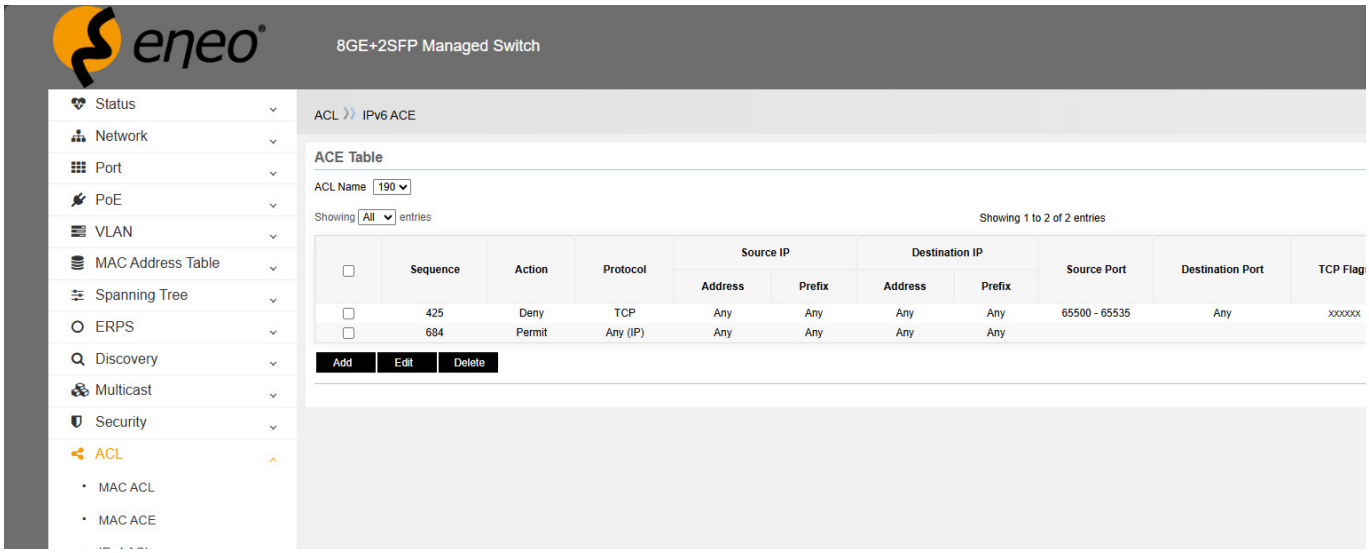
Konfiguration der IPv4-ACL-Regeln

- Die erste Regel lehnt ICMP-IPv4-Pakete ab.
- Die zweite Regel lässt alle IPv4-basierten Pakete durch.

IPv6 ACL

Ein Eintrag mit ACL 333 ist konfiguriert.



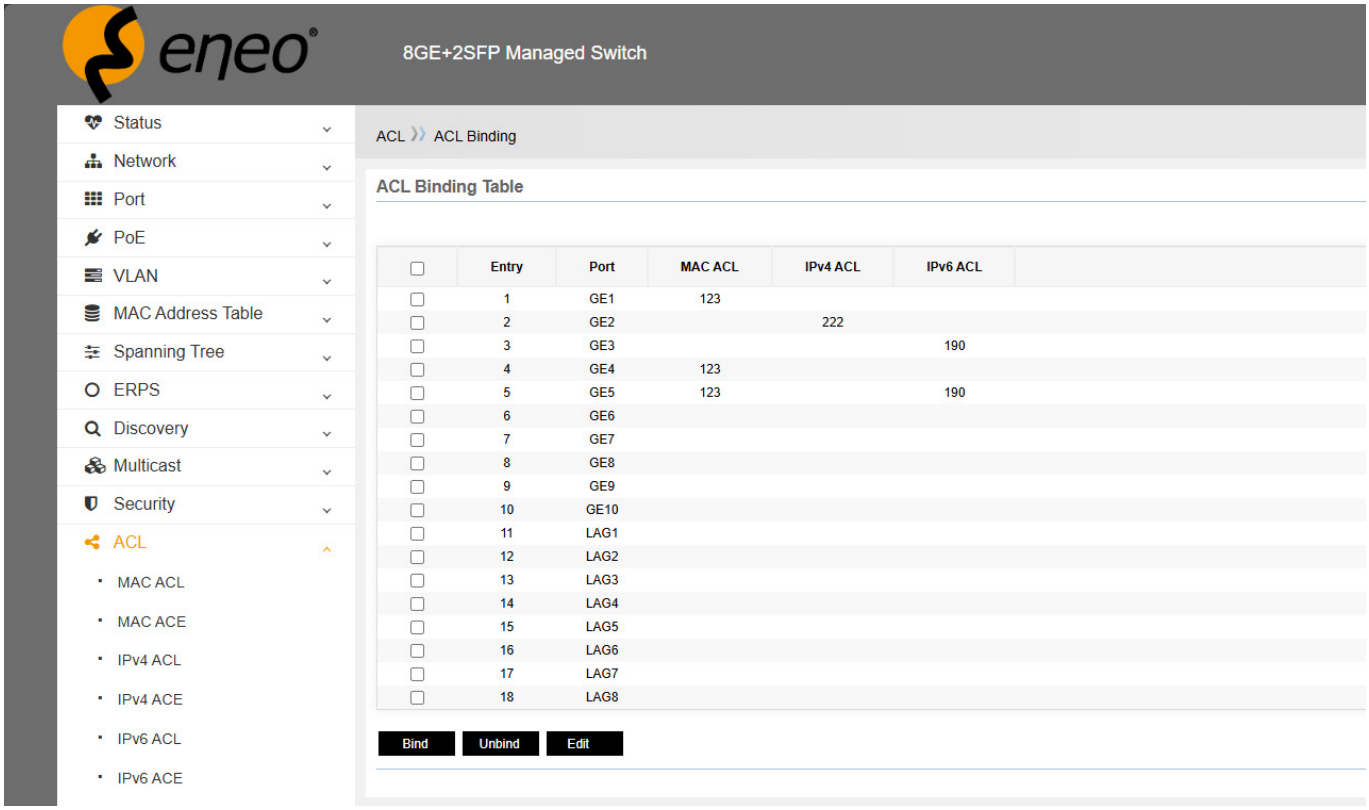


Konfiguration der IPv6-ACL-Regeln

- Die erste Regel lehnt IPv6-Pakete ab, deren TCP-Portnummer zwischen 65500 und 65535 liegt.
- Die zweite Regel lässt alle IPv6-basierten Pakete durch.

ACL-Binding

Binden Sie ACL-Regeln an die entsprechenden Ports.



Wie hier zu sehen ist:

- Die 1 ist an die Regel 123 gebunden
- Die 2 ist an die Regel 222 gebunden
- Die 3 ist an die Regel 190 gebunden
- Die 4 ist an die Regeln 123+222 gebunden
- Die 5 ist an die Regeln 123+190 gebunden

Regeln können je nach den Anforderungen des Benutzers auf vielfältige Weise definiert und dann an den entsprechenden Port gebunden werden. Beispielsweise können Sie in MAC ACL einen Regeleintrag mit dem Wert 111 definieren und diesen dann an einen anderen Port binden.

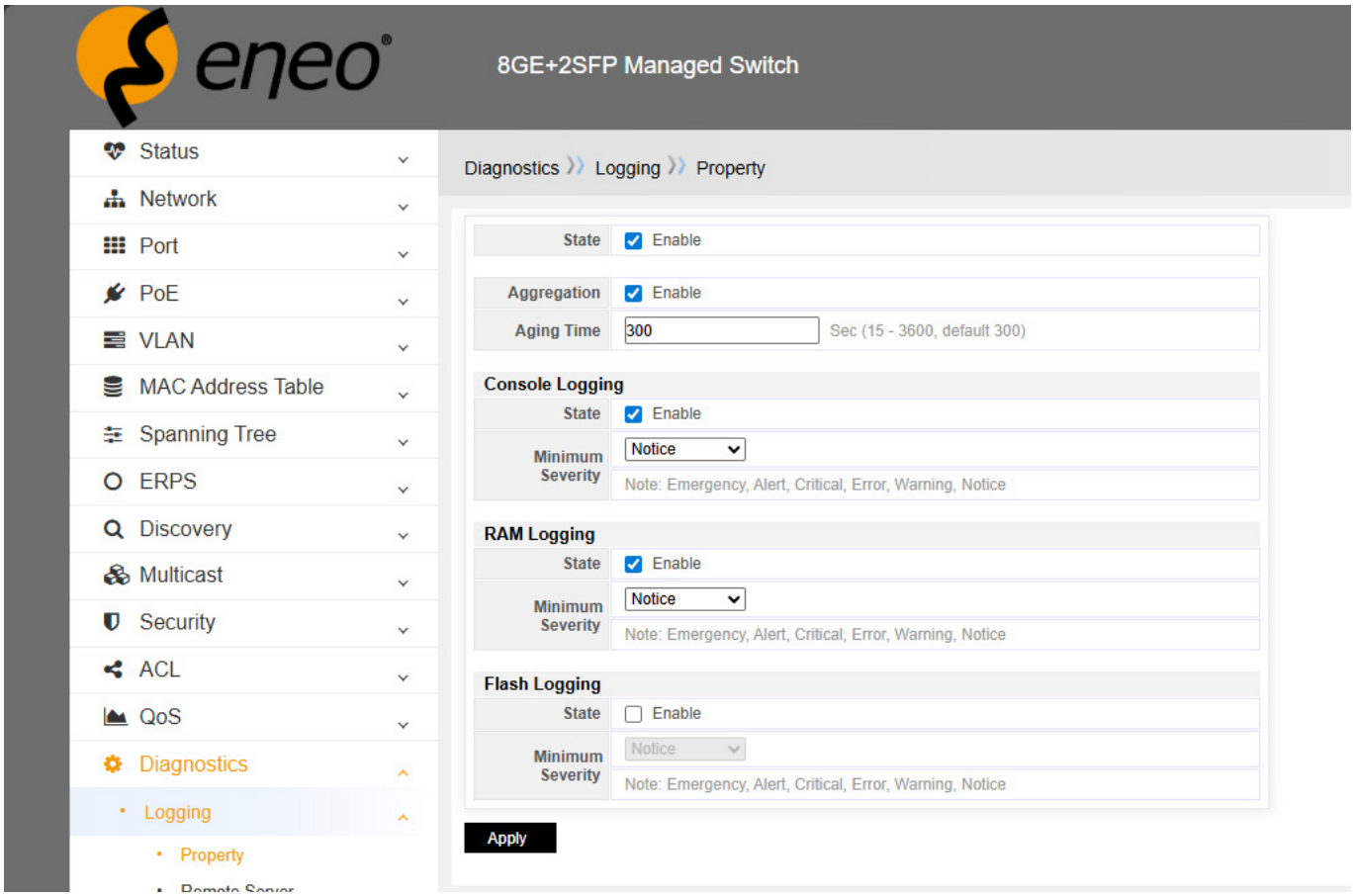
Hinweis!

Wenn Sie eine ACL-Eintragregel löschen möchten, müssen Sie sie zuerst aufheben, bevor Sie sie löschen können. Wenn dieser Eintrag bereits mit dem Port verknüpft ist, können Sie ihn nicht löschen.

12 – DIAGNOSTIK

12.1 – Protokollierung

12.1.1 – Property



Status: Informationen zur Aufzeichnung des Protokolls, ein/aus.

Aggregation: Gibt an, ob Protokolleinträge kombiniert angezeigt werden, ein/aus.

Aging Time: Wie oft die Protokollinformationen aktualisiert werden. Der Standardwert ist 300 Sekunden.

Konsolenprotokollierung: Protokollinformationen auf der Konsole anzeigen.

RAM-Protokollierung: Protokollinformationen im RAM anzeigen.

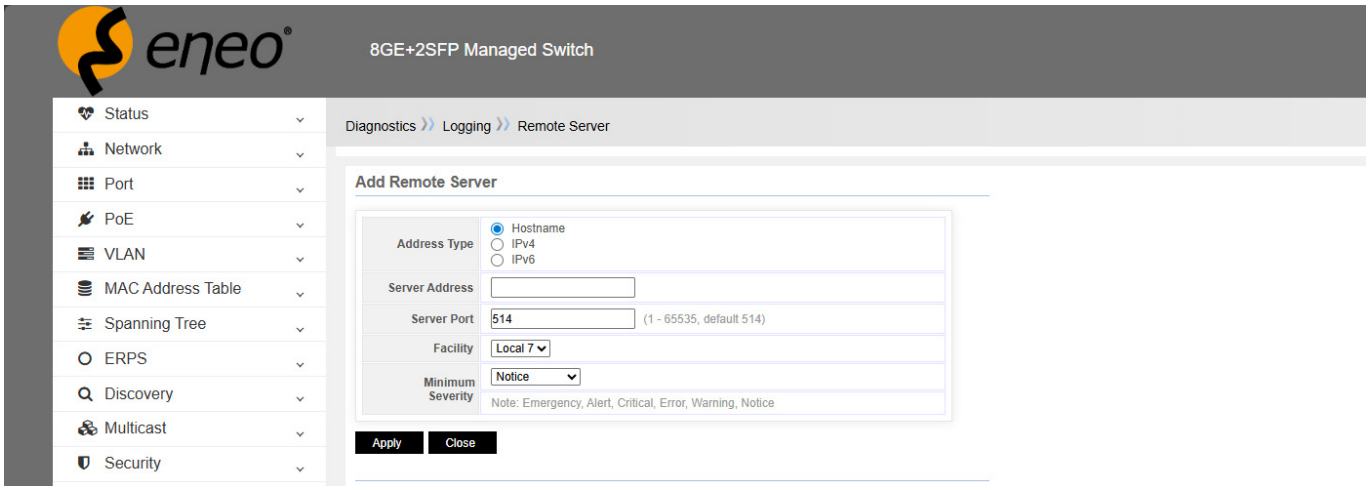
Flash-Protokollierung: Protokollinformationen im Flash anzeigen.

Mindestschweregrad: Protokollstufe, unterteilt in 8 Typen: Notfall, Warnung, Kritisch, Fehler, Hinweis, Information, Debug.

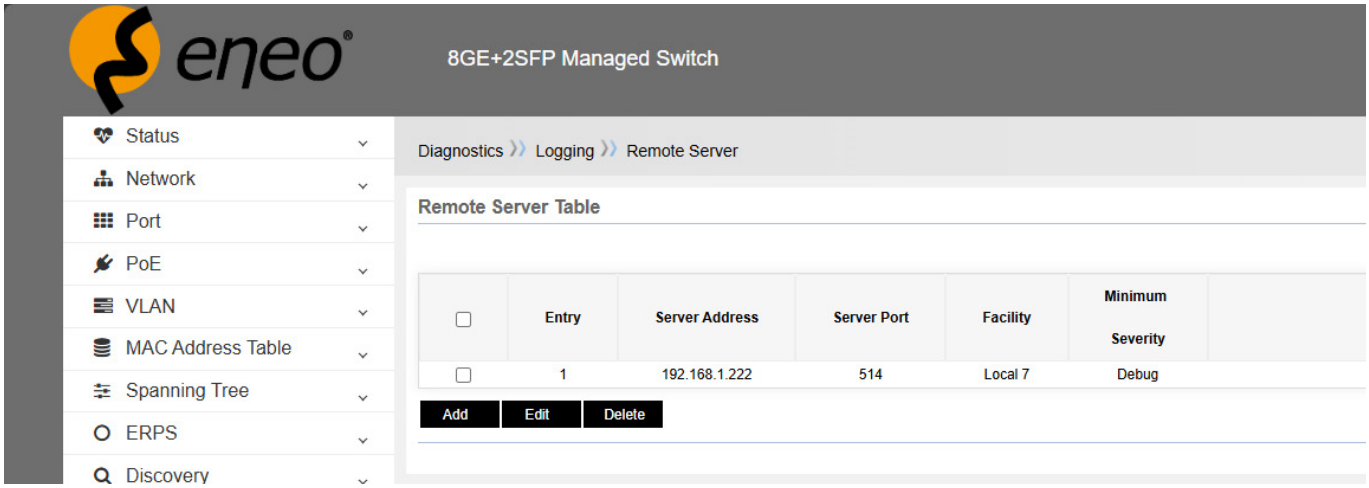
12.1.2 – Einstellung für die Ausgabe von Informationen zum Wechseln zu einem Log-Server

Die Protokollinformationen des Switches können an den Protokollserver gesendet werden, der alle Protokollinformationen lückenlos speichert. Praktisch für Benutzer zum Abfragen.

Fügen Sie Informationen zum Protokollserver hinzu, einschließlich Serveradresse und Option für Mindestschweregrad.



Nach Abschluss der Konfiguration sieht es wie in der folgenden Abbildung aus:



Der Log-Server kann die vom Switch gesendeten Log-Datensätze empfangen und detaillierte Log-Informationen anzeigen.

12.2 – Spiegelung

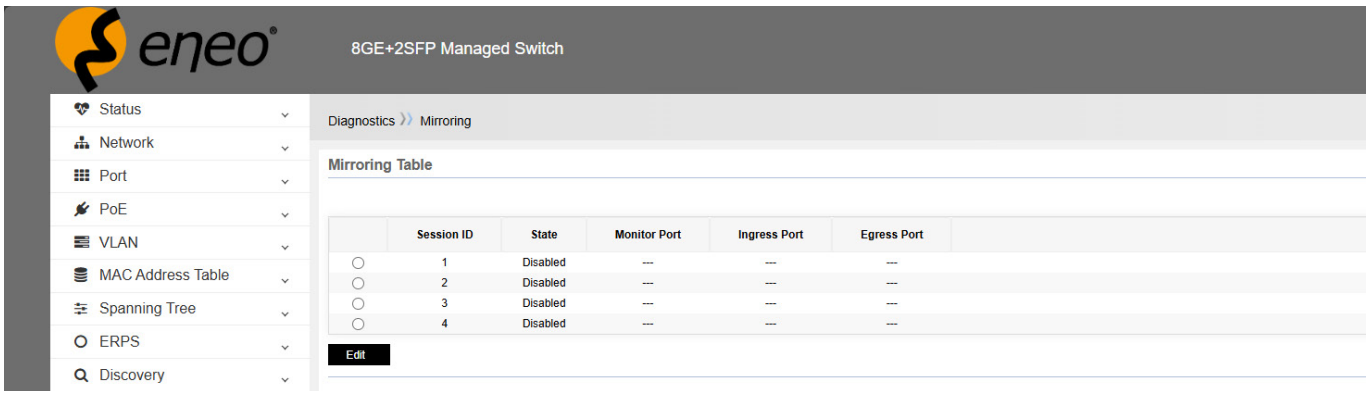
Unterstützt 4 Spiegelungssitzungen.

Einstellung der Datenerfassung:

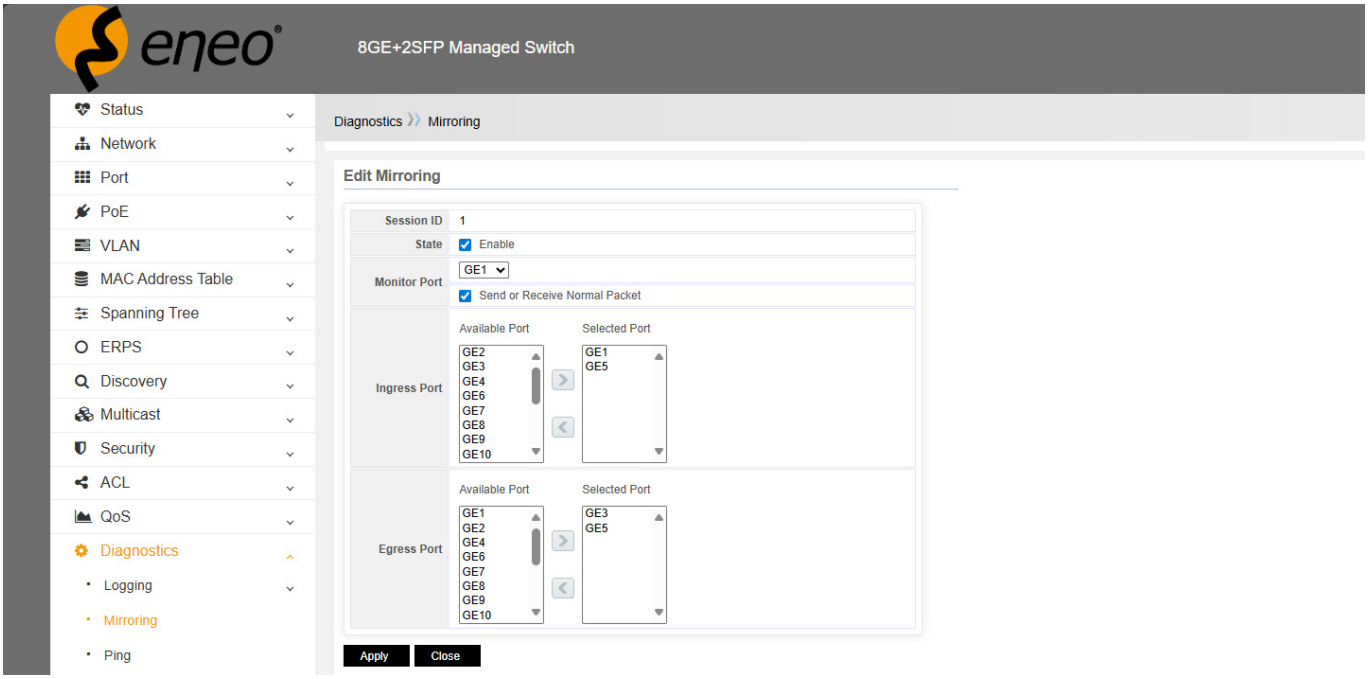
Aufnahmestatus: Status der Portspiegelung einstellen, ein/aus

Aufnahmeport: einen Aufnahmeport auswählen, d. h. die auf dem aufgenommenen Port empfangenen Nachrichten an diesen Port spiegeln

Aufgenommener Port: eingehende Nachrichten, ausgehende Nachrichten oder alle Nachrichten aufnehmen.



Wählen Sie eine Spiegelungssitzung aus und klicken Sie auf „Edit/Bearbeiten“.



Status: Aktivieren

Monitor-Port: Wählen Sie einige Ports aus, deren Meldungen auf diesem Port gespiegelt werden sollen.

Hinweis!

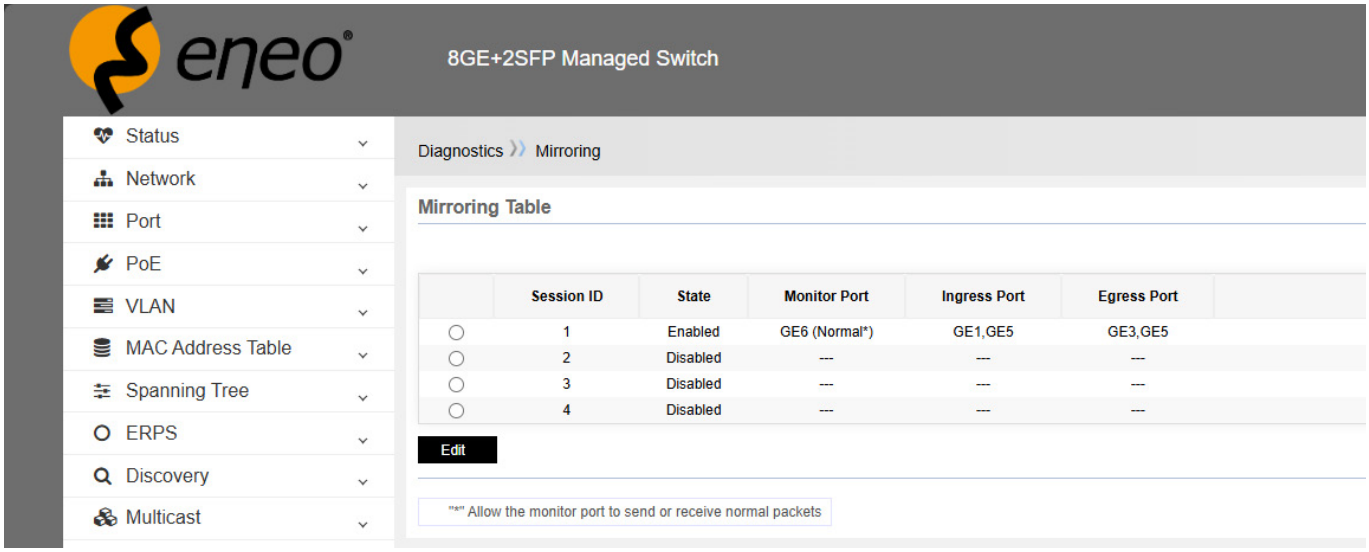
Aktivieren Sie „Normales Paket senden oder empfangen", um den Switch nach der Konfiguration über den mit diesem Port verbundenen PC zu steuern. Andernfalls kann dieser Port nicht zur Steuerung des Switches verwendet werden.

Eingangsport: Nachrichten, die an diesen Port gesendet werden

Fortschrittsport: Nachrichten, die von diesem Port gesendet werden

Wie im Beispiel gezeigt:

- Spiegeln Sie die Eingangsnachrichten des GE2-Ports auf den GE6-Port
- Spiegeln Sie die Ausgangsnachrichten des GE3-Ports auf den GE6-Port
- Spiegeln Sie die Eingangs- und Ausgangsnachrichten des GE5-Ports auf den GE6-Port

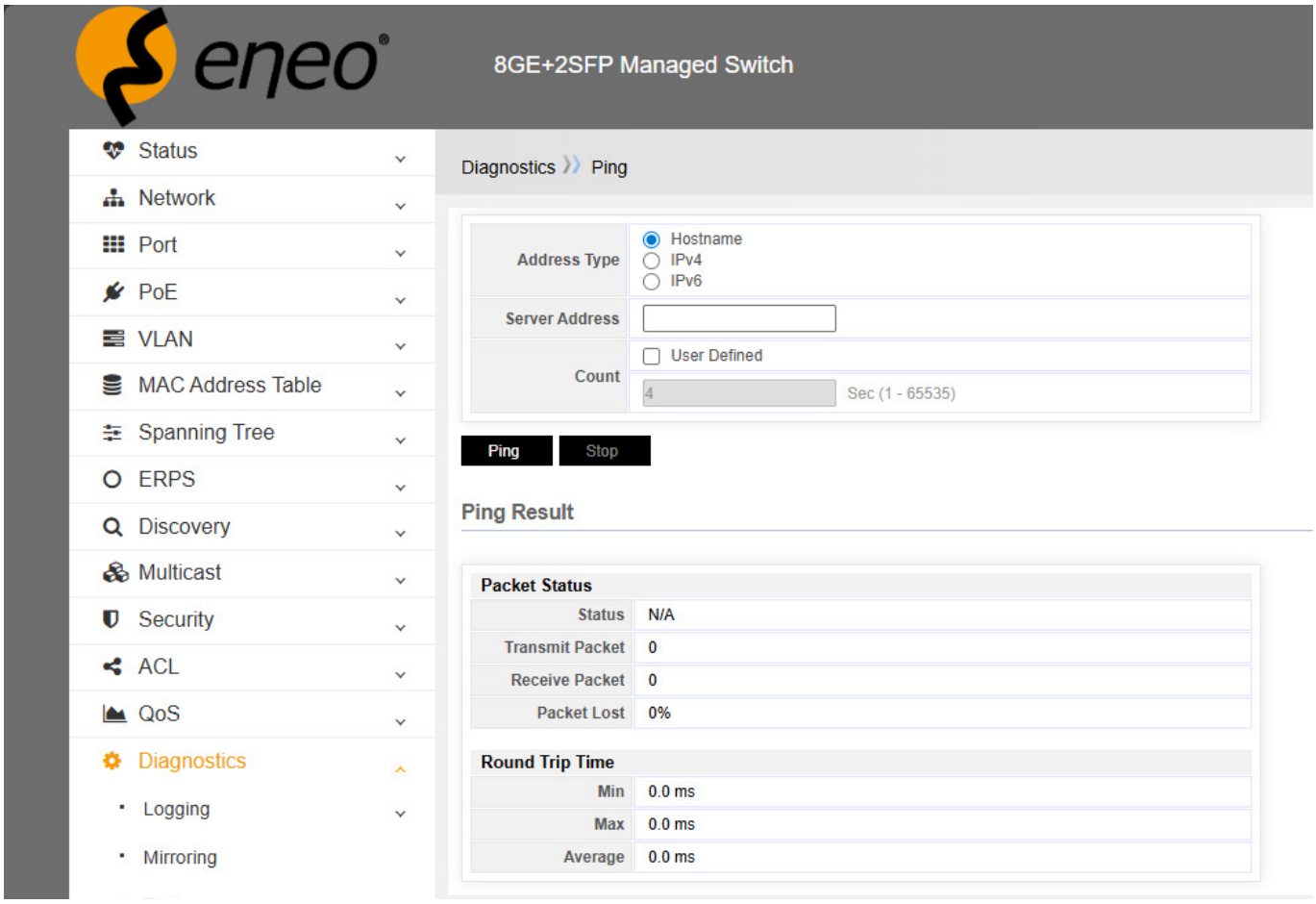


Kontrollieren Sie die Details der Spiegelkonfiguration.

12.3 – PING

PING (Packet Internet Groper) wird verwendet, um die Netzwerkverbindung zu testen. Ping ist ein Dienstbefehl, der in der Anwendungsschicht der TCP/IP-Netzwerkarchitektur ausgeführt wird und hauptsächlich dazu dient, eine ICMP-ECHO-Anforderungsnachricht an einen bestimmten Zielhost zu senden, um zu testen, ob dieser Zielhost erreichbar ist, und um seinen relevanten Status zu verstehen.

PING wird verwendet, um sicherzustellen, dass der lokale Host erfolgreich Pakete mit einem anderen Host austauschen (senden und empfangen) kann. Anhand der zurückgesendeten Informationen können wir ableiten, ob die TCP/IP-Parameter korrekt eingestellt sind, der Vorgang normal verläuft und das Netzwerk frei von Störungen ist.



Adresstyp: Hostname, IPv4, IPv6

Dienstadresse: Hier muss die Zieladresse für PING eingegeben werden.

Anzahl: Die Anzahl der Nachrichten für PING in Folge. Der Standardwert ist 4. Sie können die Anzahl der Nachrichten für PING auch manuell eingeben.

Ping-Ergebnis

Status: Bestanden oder fehlgeschlagen

Paket übertragen: Wie viele Ping-Nachrichten wurden gesendet?

Paket empfangen: Wie viele Ping-Nachrichten wurden empfangen?

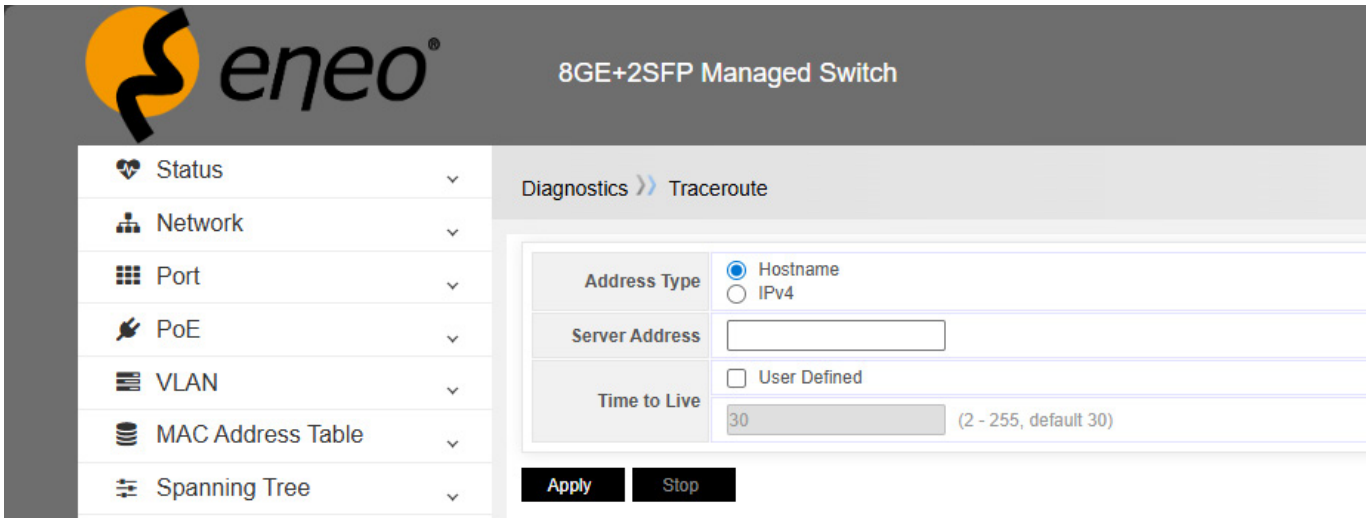
Paket verloren: Vergleichen Sie die Daten der gesendeten und empfangenen Nachrichten, um den Prozentsatz der verlorenen Nachrichten zu ermitteln.

12.4 – Traceroute

Der Befehl Traceroute verwendet das ICMP-Protokoll, um alle Router zwischen Endgerät und Zielendgerät zu lokalisieren. Der TTL-Wert kann die Anzahl der Router oder Gateways widerspiegeln, die das Datenpaket passiert hat. Durch die Steuerung des unabhängigen ICMP, um den TTL-Wert von Nachrichten abzurufen und die verworfenen Rückinformationen dieser Nachricht zu beobachten, kann der Traceroute-Befehl alle Router auf dem Paketübertragungspfad durchlaufen.

Dieses Programm wird den TTL-Wert erhöhen, um seine Funktionen zu realisieren. Das Programm realisiert seine Funktion durch die Erhöhung des TTL-Wertes. Jedes Mal, wenn ein Paket einen Router durchläuft, wird seine Lebensdauer um 1 verringert. Wenn seine Lebensdauer 0 ist, bricht der Host das Paket ab und sendet ein ICMP-TTL-Paket an den Absender des ursprünglichen Pakets.

Die TTL-Werte der ersten drei vom Programm gesendeten Pakete sind 1, die der nächsten drei sind 2 usw., so dass das Programm eine Reihe von Paketpfaden erhält. Beachten Sie, dass IP nicht garantiert, für jedes Paket den gleichen Weg zu nehmen.

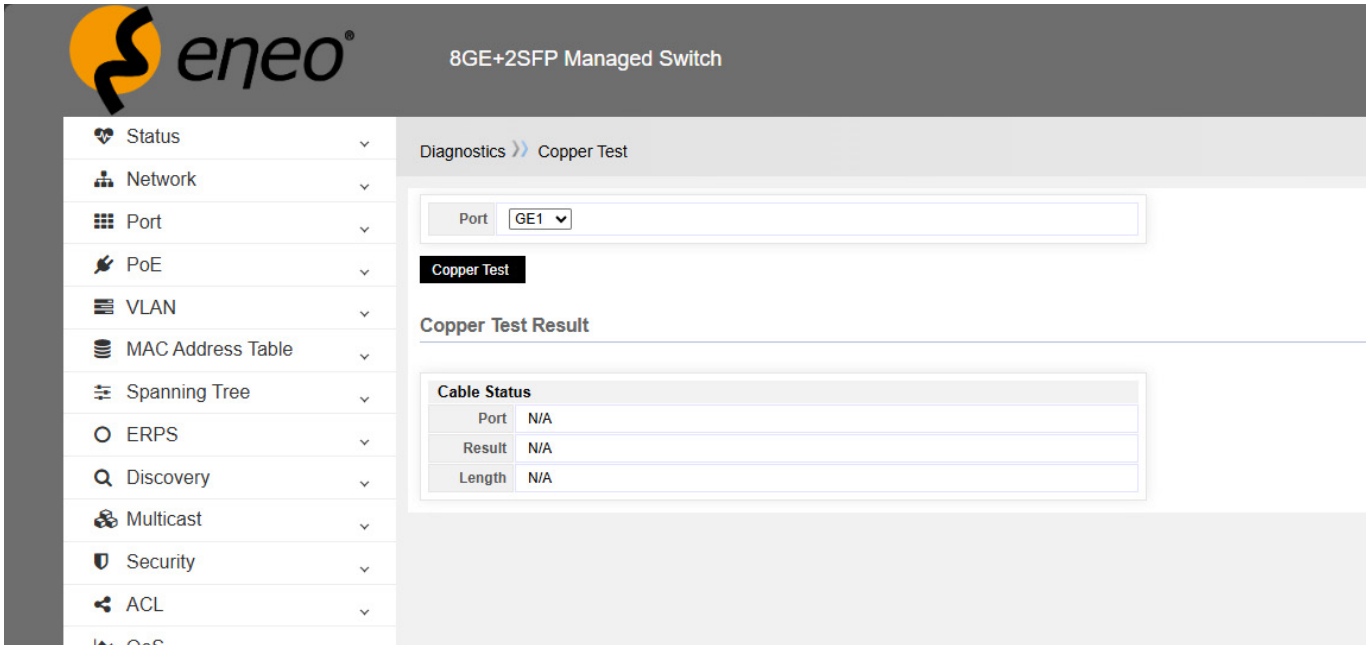


12.5 – Kupfertest

VCT ist die Abkürzung für Virtual Cable Test (Virtueller Kabeltest), eine gängige Funktion in Netzwerkkommunikationsgeräten.
VCT verwendet TDR (Time Domain Reflectometry), um den physikalischen Zustand von Netzwerkkabeln zu erfassen.

Das Prinzip der TDR-Erfassung ähnelt dem des Radars. Die Arbeitsweise besteht darin, ein Impulssignal durch eine aktive Führungslinie zu senden und das Ergebnis der Reflexion des gesendeten Impulssignals zu erfassen, um den Kabelfehler zu erkennen. Wenn das gesendete Impulssignal das Kabelende oder den Fehlerpunkt des Kabels durchläuft, wird ein Teil oder die gesamte Impulsenergie zurück zur ursprünglichen Sendequelle reflektiert. Die VCT-Technologie ermittelt die Zeit, zu der das Signal am Fehlerpunkt ankommt oder zurückkehrt, je nach seinem Übertragungsstatus im Kabel, und wandelt dann die entsprechende Zeit in den Entfernungswert gemäß der Formel um. VCT kann den Kabelzustand, die Fehlerentfernung, den Polaritätswechsel, die Dämpfung des Einfügungssignals, die Dämpfung des Rücksignals usw. erfassen.

Der Benutzer kann die VCT-Eigenschaften zur Erfassung von Ethernet-Verbindungskabeln verwenden und das System zur Erfassung von Ethernet-Kabeln einschalten. Die Erfassung umfasst Kurzschluss und Unterbrechung in der Empfangs- und Senderichtung des Kabels sowie die fehlerhafte Position des Kabels.



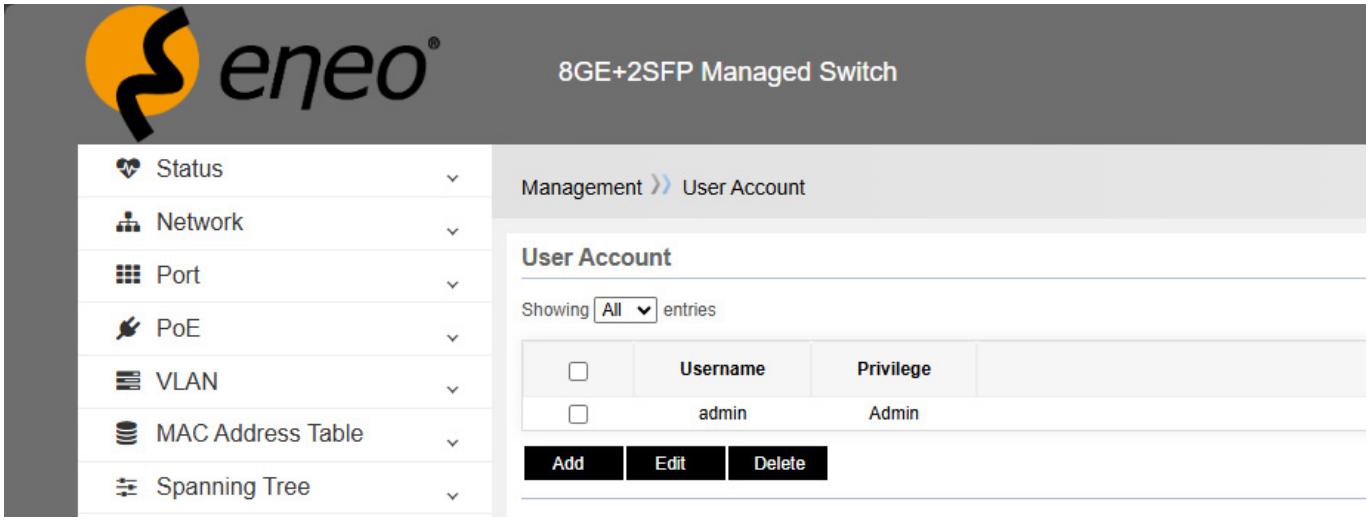
Wählen Sie einen Port und klicken Sie auf die Schaltfläche „Kupfertest“.

Wenn das Netzwerkkabel getrennt ist, wird ein Testergebnis angezeigt, das die Länge angibt, d. h. wie viele Meter das Kabel getrennt ist. Die Fehlerquote beträgt etwa 1 Meter, sodass diese Funktion zum Kontrollieren von Netzwerkkabelfehlern verwendet werden kann.

13 – MANAGEMENT

13.1 – Benutzerkonto

Klicken Sie auf „Hinzufügen“, um einen neuen Benutzer hinzuzufügen.



Geben Sie den Benutzernamen und das Kennwort ein und bestätigen Sie das Kennwort.

Es gibt zwei Ebenen: Admin und Benutzer.

Der Administrator kann alle Funktionen des Switch-Systems verwalten.

Der Benutzer kann nur einige Funktionen des Switches verwalten.

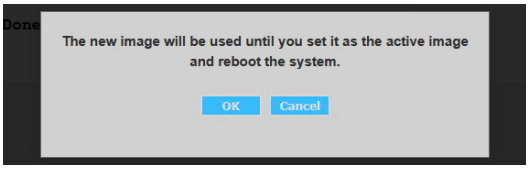
13.2 – Firmware

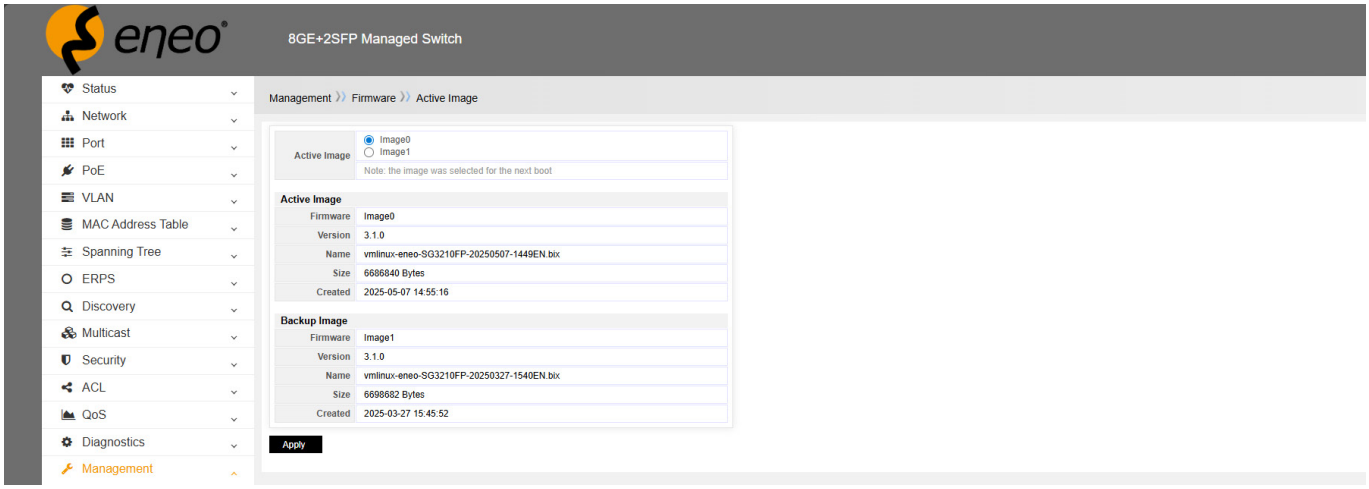
13.2.1 – Upgrade / Backup

Das Softwaresystem kann über TFTP oder HTTP aktualisiert und gesichert werden.

Wenn Sie eine Aktualisierung durchführen möchten, wählen Sie „Upgrade“ oder „HTTP“, wählen Sie anschließend die Systemaktualisierungsdatei aus und klicken Sie abschließend auf „Übernehmen“.

Nach dem Upgrade werden die folgenden Informationen angezeigt. Klicken Sie auf OK.





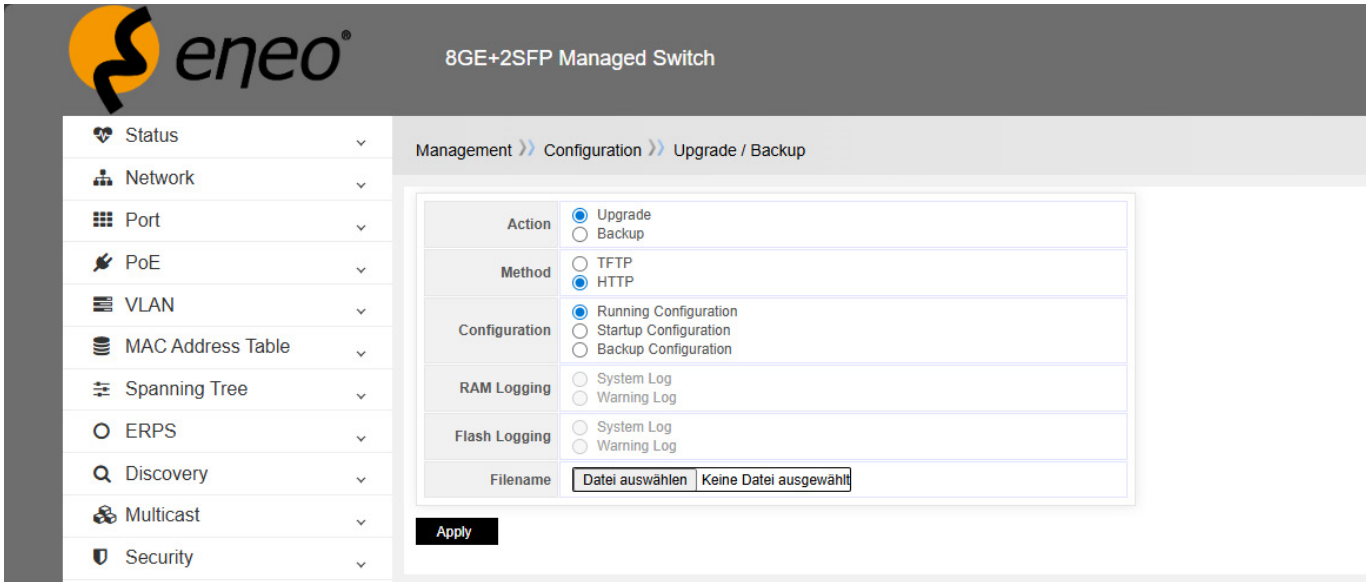
Nach dem Upgrade können Sie feststellen, dass die soeben verwendete Upgrade-Datei dem aktualisierten Image1 entspricht. Wählen Sie nun Image1 in der Option „Aktives Image” aus, klicken Sie auf „Übernehmen”, um das Upgrade abzuschließen, und klicken Sie abschließend auf die Schaltfläche „Neustart”.

Hinweis!

Der Switch ist ein duales IMG-System. Wenn derzeit Image1 ausgeführt wird, wird Image0 aktualisiert. Wenn hingegen Image0 ausgeführt wird, wird Image1 aktualisiert.

13.3 – Konfiguration

13.3.1 – Upgrade / Backup / Werkseinstellungen



Aktion: Aktualisieren/Sichern

Aktualisieren: Parameter aktualisieren

Sichern: Parameter sichern

Methode: TFTP/HTTP

Konfiguration:

Laufende Konfiguration: Parameter, die das System ausführt

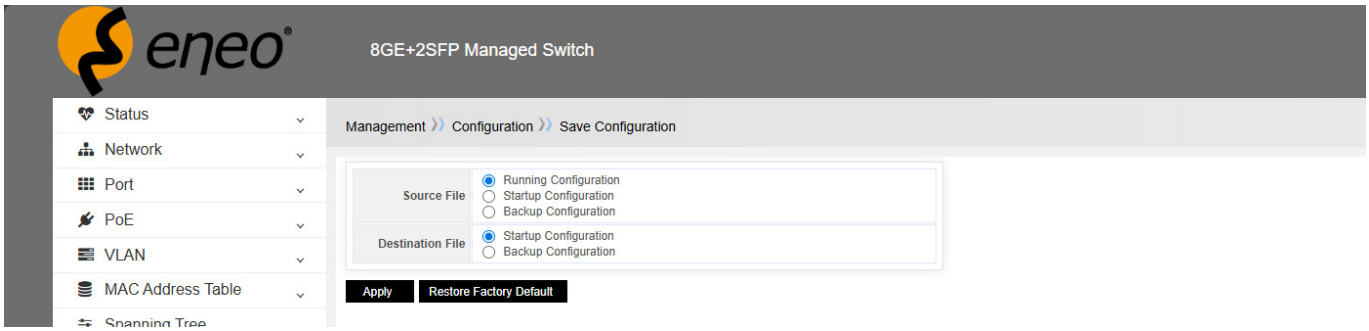
Startkonfiguration: Parameter, die beim Systemstart geladen werden

Sicherungskonfiguration: Parameter, die gesichert wurden

Hinweis!

Wählen Sie beim Importieren von Parametern die Option „Startkonfiguration“ aus. Klicken Sie anschließend auf „Neustart“, um den Import der Parameter abzuschließen.
Wählen Sie beim Exportieren von Parametern die Option „Laufende Konfiguration“ aus.

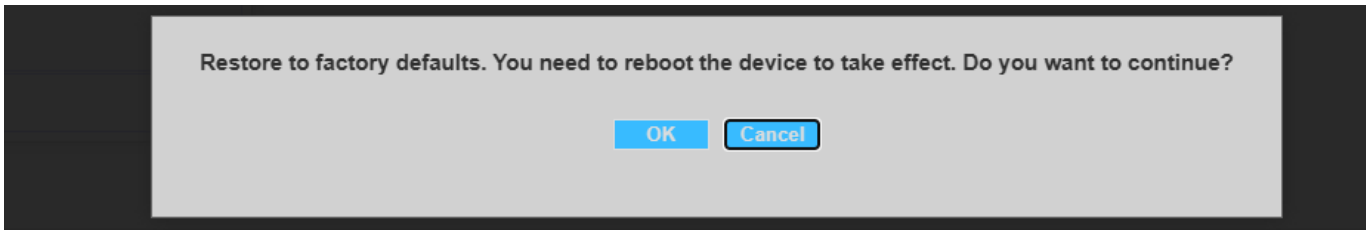
13.3.2 – Konfiguration speichern

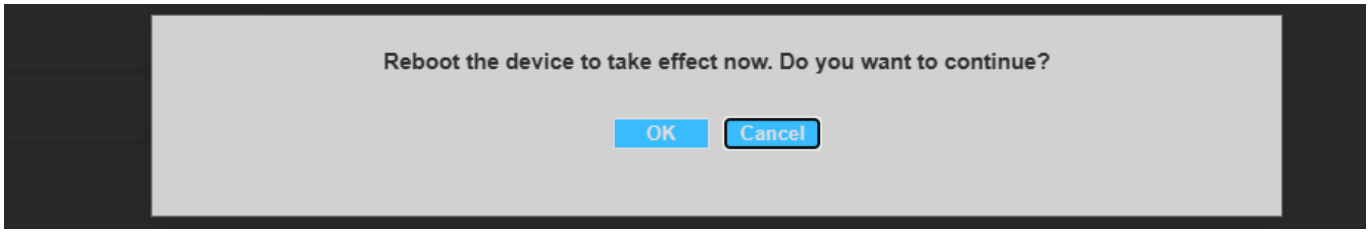


Kopieren Sie die Quelldatei in die Zieldatei, um die Parameter zu speichern.
Am einfachsten ist es, hierfür oben rechts auf die Schaltfläche „Speichern/Save“ zu klicken.

Auf Werkseinstellungen zurücksetzen

Wenn Sie das Gerät auf die Werkseinstellungen zurücksetzen möchten, klicken Sie auf „Restore Factory Default“ und folgen Sie den Anweisungen.





Um zu verhindern, dass diese Einstellung versehentlich vorgenommen wird, muss sie zweimal bestätigt werden.

Klicken Sie dazu jeweils auf „OK”.

14 – FAQ

14.1 – Anzeigestörung der Verbindungsstatusanzeige (Verbindungsfehler)

Kontrollieren Sie, ob das Verbindungsende mit der PC-Netzwerkkarte oder einer anderen Ethernet-Schnittstelle verbunden ist.

Kontrollieren Sie, ob der Verbindungszugangspunkt rostig oder beschädigt ist.

Kontrollieren Sie über das WEB die Konfiguration dieses Ports (Duplex und Geschwindigkeit) und stellen Sie sicher, dass die Konfiguration mit der des anderen Endes der Verbindung übereinstimmt.

Hinweis!

Wenn Duplex und Geschwindigkeit dieses Ports zwingend festgelegt sind, muss die Konfiguration einer Verbindung mit der der anderen übereinstimmen, da sonst keine Verbindung hergestellt werden kann.

14.2 – Normale Anzeige der Verbindungsstatusanzeige, aber keine Kommunikation

Kontrollieren Sie über die WEB-Seite, ob der Port gestoppt ist (geben Sie „Portkonfiguration" ein). Wenn der Port gestoppt ist, aktivieren Sie ihn bitte.

Kontrollieren Sie über die WEB-Seite, ob der Port durch VLAN isoliert ist. Zum Vergleich mit anderen Ports: Nur wenn der Port im selben VLAN auf „Zugriff" eingestellt ist, können sie miteinander kommunizieren.

14.3 – Anmeldung am Switch nicht möglich

Kontrollieren Sie, ob der Switch eingeschaltet ist.

Wenn die Verbindung fehlgeschlagen ist, kontrollieren Sie die Antwort des Switches mit „Ping". Wenn keine Antwort erfolgt, kontrollieren Sie die IP-Adresskonfiguration des PCs und des Switches. Ermitteln Sie die Ursache des Problems anhand der Rückmeldung der HTTP-Verbindung.

Kontrollieren Sie die IP-Adresseinstellungen

1. Kontrollieren Sie, ob die IP-Adresse und die Subnetzmaske des PCs richtig eingestellt sind. Tragen Sie „ipconfig" in das Befehlszeilenfenster ein und drücken Sie die Eingabetaste, um die IP-Adresskonfiguration des PCs zu kontrollieren.
2. Kontrollieren Sie, ob die IP-Adresse, die Subnetzmaske und der Standard-Gateway des Switches richtig eingestellt sind.
3. Kontrollieren Sie, ob die IP-Adresse des Switches von anderen Geräten belegt ist.

Kontrollieren Sie das Login-Konto

Wenn beim Einloggen in WEB der Switch den Benutzer kontinuierlich auffordert, das Konto und das Kennwort einzutragen, kann dies bedeuten, dass dieses Konto nicht existiert oder dieses Kennwort ungültig ist.

14.4 – Switch startet nicht

1. Kontrollieren Sie, ob die Nummer der seriellen Schnittstelle falsch ist, normalerweise ist dies COM1 oder COM2.
2. Stellen Sie sicher, dass die Software wie folgt konfiguriert ist: 115200 bps, 8 Datenbits, 1 Stoppbit, keine Paritätsprüfung und keine Datenflusskontrolle.
3. Kontrollieren Sie, ob die serielle Schnittstelle des PCs normal funktioniert: Sie können mit der Maus überprüfen, ob die serielle Schnittstelle funktioniert.
4. Stellen Sie sicher, dass kein anderes Programm diesen seriellen Anschluss verwendet: Unter Windows kann ein serieller Anschluss nicht von mehreren Programmen gleichzeitig verwendet werden.

14.5 – Stromausfall

Kontrollieren Sie die Betriebsanzeige. Wenn die Anzeige nicht leuchtet, ist möglicherweise die Stromverbindung beschädigt. Stellen Sie sicher, dass die Stromversorgung normal ist, und überprüfen Sie, ob die Verbindung zwischen dem Switch und seiner Stromversorgung stabil und zuverlässig ist.

Version: 07 / 2025

VIDEOR E. Hartig GmbH | Carl-Zeiss-Straße 8 | 63322 Rödermark | Germany | Tel. +49.6074.888-0 | Fax +49.6074.888-100 |
Amtsgericht Offenbach am Main | HRB 32047 | UIN DE 113592980 |
Geschäftsführer / Managing Directors: Lars Hagenlocher, Dominik Mizdrak

www.eneo-security.com | info@eneo-security.com