



INDRy II-Serie

Verwalteter industrieller Ethernet-Switch

LIG1014A

Betriebsanleitung

Versionsnummer:

Ausgabe: 1.0, September 2014



[INHALT]

1. Das Wichtigste zuerst (Baudrate, Standard-IP-Adresse, Nutzernamen usw.)	3
2. Vorwort (Sicherheit)	4
3. Überblick (Technisches, Steckverbindungen)	5
4. Zubehör	8
5. Installation	9
6. Anleitung für die VLAN-Anwendung	25
7. Anleitung für die Sicherheitsanwendung	32
8. Anleitung für den Ringschutz	49
9. Anleitung für die QoS-Anwendung	60
10. Anleitung für die Link Fail Alarm- Anwendung	79
11. Anleitung für die 802.1x-Authentifizierungs- anwendung	85

Das Wichtigste zuerst

INDRy II benötigt Gleichstrom (DC). Ein AC/DC-Netzadapter wird mit dem Produkt nicht mitgeliefert. Geeignet ist ein DC-Netzadapter zwischen **12 und 58 V DC**. Wenn Sie nicht zu viele und zu langsame oder WDM-SFP-Module verwenden, ist eine Stromquelle mit **2 Ampere** für den Anfang richtig.

Sie können zwei Stromquellen oder DC-Netzadapter anschließen. Zum ersten Starten wählen Sie PWR1 oder PWR2, das ist zum gegenwärtigen Zeitpunkt egal. Achten Sie auf richtige Polarität und schließen Sie den Alarm-Kontakt nirgendwo an. Sorgen Sie dafür, dass nichts unter Strom steht und achten Sie auf die elektrische Sicherheit.

INDRy II braucht einige Sekunden, um hochzufahren. Jetzt können Sie INDRy II entweder über die serielle Verbindung einrichten oder unter Verwendung der **Standard-IP-Adresse 192.0.2.1**. Dafür müssen Sie die LAN-Schnittstelle Ihres PCs manuell auf das gleiche Subnetz konfigurieren, zum Beispiel durch Auswahl von 192.0.2.200.

Wenn Sie das Gerät über die serielle Verbindung einrichten wollen, verwenden Sie das mitgelieferte RJ45-DB9-Kabel mit der RJ45-Terminal-/Konsolverbindung oben auf dem Produkt (gleiche Seite, auf der sich der Netzanschluss befindet). Wenn Sie Hyperterminal (standardmäßig in den neueren Windows-Versionen nicht mehr enthalten) mit **115200bps 8N1** verwenden, erhalten Sie eine Verbindung

Der Standard-Nutzername ist admin, das Passwort-Feld bleibt leer. Wenn Sie in das Passwortfeld etwas hineinschreiben, haben Sie diese Anweisung falsch verstanden. Das gilt sowohl für die Web-Schnittstelle als auch für die serielle Verbindung.

Die Zuweisung der IP-Adresse für INDRy II geschieht auf der **Schnittstellen-/VLAN-Ebene**. Es gibt keine globale Switch-Einstellung für eine IP-Adresse.

Wenn Sie mehr als ein INDRy II mit IP-Adressen konfigurieren, achten Sie auf Mac-Adresstabellen auf Ihrem Computer. Nach der Konfiguration des ersten INDRy II bereinigen Sie entweder Ihren ARP-Cache (`arp -d *`) oder warten ein paar Sekunden und Minuten, bevor Sie den nächsten INDRy II anschließen.

Vorwort

Umfang

Dieses Dokument bietet einen Überblick über INDRy II. Es beinhaltet:

- Materialien zur Installationsanleitung für INDRy II-Hardware.

Zielgruppe

Die Anleitung eignet sich für Systemingenieure oder Betreiber, die ein Grundverständnis von INDRy II haben möchten.

Sicherheitshinweise

Wird eine Steckverbindung während der Installation, eines Tests oder des Betriebs entfernt oder bricht ein Faserkabel, das unter Strom steht, dann entsteht das Risiko, dass das Auge einen Laserstrahl auffängt und dadurch Schaden nimmt, je nach Stärke des Lasers.

Die vorrangigen Schäden, die durch Laserstrahlung entstehen können sind:

- Schäden am Auge durch unbeabsichtigtes Hineinsehen in einen von einer Laserquelle ausgesendeten Strahl.
- Schäden am Auge durch eine Steckverbindung an eine gebrochene oder spannungsführende Faser.

Konventionen in der Dokumentation

In diesem Handbuch werden die folgenden Konventionen verwendet, um Informationen hervorzuheben, die für den Leser von Interesse sind:

Gefahr — Die beschriebene Tätigkeit oder Situation weist auf eine Gefahr hin, die *Verletzungen* verursachen kann oder wird.

Warnung — Die beschriebene Tätigkeit oder Situation weist auf eine Gefahr hin, die Schäden an der Anlage verursachen kann oder wird.

Vorsicht — Die beschriebene Tätigkeit oder Situation weist auf eine Gefahr hin, die einen Betriebsausfall verursachen kann oder wird.

Anmerkung — Enthält Informationen, die den Text ergänzen oder wichtige Punkte herausstellen.

Übersicht

Die serienmäßigen industriellen INDRy II-Ethernet-Lösungen bieten hochwertige Qualität, einen breiten Betriebstemperaturbereich, einen erweiterten Leistungsaufnahmebereich und moderne VLAN- und QoS-Funktionen. Sie eignen sich optimal für den Einsatz unter rauen Umgebungsbedingungen und in unternehmenskritischen Anwendungen.

Bedienbild

Einführung in die Komponenten an der Vorderseite

Vorderseite	
Systemzustands-LED	P1, P2 und Alarm
Gigabit-Ethernet-Kupfer-Ports	RJ45
Gigabit-Ethernet-SFP-Ports	SFP-Slots



Einführung in die Komponenten an der Oberseite

Oberseite	
Leistungsaufnahme (Dual)	6P Reihenklemme
Konsole (RS232)	RJ45
Reset	Schalter



Technische Daten

Ethernet

Betriebsmodus	Store-and-Forward, L2-Leitungsgeschwindigkeit/ nicht-blockierende Umschaltereinheit
MAC-Adressen	8K
Jumbo-Frames	9000 Byte

RJ45 Kupfer-Ports

Geschwindigkeit	10/100/1000 Mbps
MDI/MDIX Auto-Crossover	Unterstützt gerade oder gekreuzt verdrahtete Kabel
Auto-Negotiating	10/100/1000 Mbit/s Geschwindigkeit mit Auto-Negotiation-Funktion; Voll- und Halbduplex
Ethernet-Isolierung	1500 VRMS 1 Minute

(Steckbare) SFP-Ports

Unterstützte Port-Typen	(Steckbare) SFP-Ports 100/1000Base SFP-Slot
-------------------------	---

LWL-Anschluss	Unterstützt 100/1000BaseT SFP-Transceiver
Optimale LWL-Kabel	LC üblicherweise für LWL (je nach Modul) Typisch 50 oder 62,5/125 µm für Multimode (MM); Typisch 8 oder 9/125 µm für Singlemode (SM)

Netzwerkredundanz

Schnelle Failover-Schutzringe	Wiederherstellung einer Verbindung < 20 ms
Spanning Tree Protocol	Unterstützung von Einfach- und Mehrfachringen
Port-Trunking mit LACP	IEEE 802.1D STP, IEEE 802.1w RSTP, IEEE 802.1s MSTP Statischer Trunk oder dynamisch über LACP (Link Aggregation Control Protocol)

Brücke, VLANs und Protokolle

Ablaufsteuerung	IEEE 802.3x (Vollduplex) und Back-Pressure (Halbduplex)
-----------------	---

VLAN-Typen	Port-basierte VLANs IEEE 802.1Q tag-basierte VLANs IEEE 802.1ad Double Tagging (Q in Q)
------------	---

Multicast-Protokolle	IGMP v1, v2 IGMP-Snooping und -Abfragen Sofort verlassen und Proxy verlassen Drosselung und Filterung
LLDP	IEEE 802.1ab Link layer Discovery Protocol (LLDP)

Traffic-Management und QoS

Priorität	IEEE 802.1p QoS
Anzahl der Warteschlangen pro Port	8
Ablaufplanung	SPQ, WRR
Traffic Shaper	port-basiertes Shaping

Sicherheit

Port-Sicherheit	IP- und MAC-basierte Zugriffskontrolle Netzwerkzugriffskontrolle mit IEEE 802.1X-Authentifizierung
Storm Control	Broadcast-, Multicast- und Flut-, Sturm-Control

Stromversorgung

Leistungsaufnahme	Redundante Eingangsklemmen
Eingangsspannungsbereich	12-58 VDC
Max. Leistungsaufnahme	10,5W
Verpolungsschutz	Ja

Anzeigen

Betriebszustandsanzeige	Anzeige des Status der Eingangsleistung
Ethernet-Port-Anzeige	Verbindung und Geschwindigkeit

Management

Schnittstellen zur Benutzerverwaltung	CLI (Command Line Interface) Webbasiertes Management SNMP v1, v2c Telnet (5 Sitzungen)
Management Security	HTTPs, SSH RADIUS Client-Verwaltung
Upgrade und Wiederherstellung	Konfiguration Import/Export Firmware-Upgrade
Diagnose	Syslog Über VLAN-Spiegelung SFP mit DDM (Digital Diagnostic Monitoring)
MIBs	RMON 1,2,3,9; Q-Bridge MIB, RFC 1213 MIB-II, RFC 4188 Bridge MIB
DHCP NTP/SNTP	Client, Server, Relay, Snooping, Option 82 Ja

Umwelt und Richtlinien

Betriebstemperaturbereich	-40 bis +75° C (Kaltstart bei -40° C)
Lagertemperaturbereich	-40 bis +85° C
Feuchte (nicht kondensierend)	5 bis 95% RF
Erschütterung, Stoß und Sturz	IEC68-2-6, -27, -32
Zertifizierung der Bestandteile	CE/FCC; EN-50121-4
Elektrische Sicherheit	CSA C22, EN61010-1, CE
EMC	FCC Teil 15, CISPR 22 (EN55022) Klasse A IEC61000-4-2, -3, -4, -5, -6
RoHS und WEEE	RoHS (bleifrei) und WEEE-konform
MTBF	> 25 Jahre

Mechanik

Schutzart	IP30
Montagemöglichkeit	Hutschienenmontage, Wandmontage
Abmessung	154 mm x 109 mm x 60 mm
Gewicht	1056 g

Zubehör

Netzteile

12 V 40 Watt HUTSCHIENE	MDR-40-12
24 V 40 Watt HUTSCHIENE	MDR-40-24
12 V 60 Watt HUTSCHIENE	MDR-60-12
24 V 60 Watt HUTSCHIENE	MDR-60-24

SFP-Module

INDRy II ermöglicht SFP-Multirate-Funktionalität. Dadurch können 100 Mbps und Gigabit SFP-Module vermischt und kombiniert werden. Bitte beachten, dies gilt für keinen anderen Switch. Sollten Sie also einen SFP-Switch eines anderen Herstellers nutzen, bedeutet dies, dass Sie Gigabit SFPs benötigen, weil der andere Switch nur Gigabit SFP-Module unterstützt. Ziehen Sie LGB5124A/LGB5128A von Black Box in Betracht, um einen 19“ SFP-basierten Backbone-Switch zu erhalten.

100 MBit/s Multimode 1310 nm LC Duplex	LFP402
100 MBit/s Singlemode 1310 nm 30 km LC Duplex	LFP403
100 MBit/s Singlemode 1310 nm 60km LC Duplex	LFP404
1000 MBit/s/Gigabit Multimode 850 nm LC Duplex	LFP411
1000 MBit/s/Gigabit Singlemode 1310 nm 10km LC Duplex	LFP413
1000 MBit/s/Gigabit Singlemode 1310 nm 40km LC Duplex	LFP414
10000 MBit/s RJ45	LFP415
10/100/1000 MBit/s RJ45	LFP416

Extras

RJ45 Staubabdeckungen, rot, abschließbar	PL-AB-RD-25PAK
RJ45 Staubabdeckungen, schwarz, abschließbar	PL-AB-BK-25PAK

Installation

Montage des INDRy II (Hutschiene)

Montage:

1. Schrauben Sie die DIN-Schienen-Halterung mithilfe der Klemme und der Schrauben im Zubehörset an.
2. Haken Sie die Einheit an der DIN-Schiene fest.
3. Drücken Sie das Endstück des Geräts gegen die DIN-Schiene bis es einrastet.

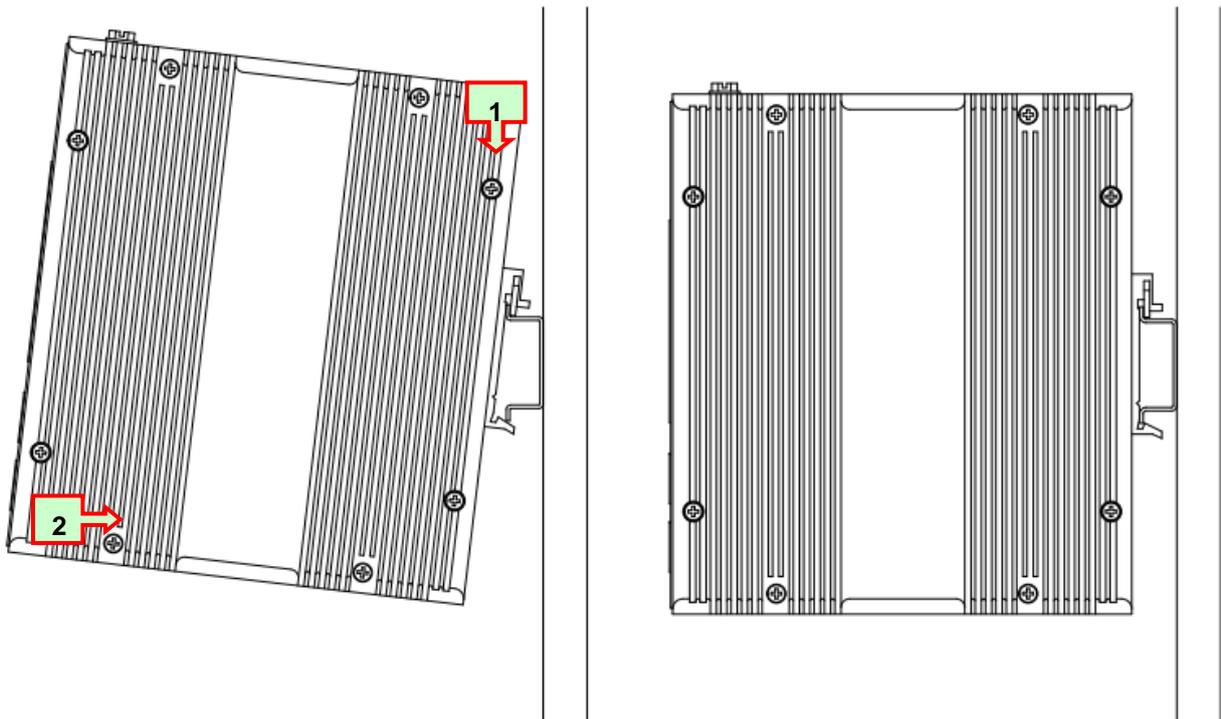


Abbildung 1 INDRy II Hutschienenmontage

Montage des INDRy II (Wandmontage)

Montage:

1. Schrauben Sie die Wandhalterung mithilfe der Platte und der Schrauben im Zubehörset an.

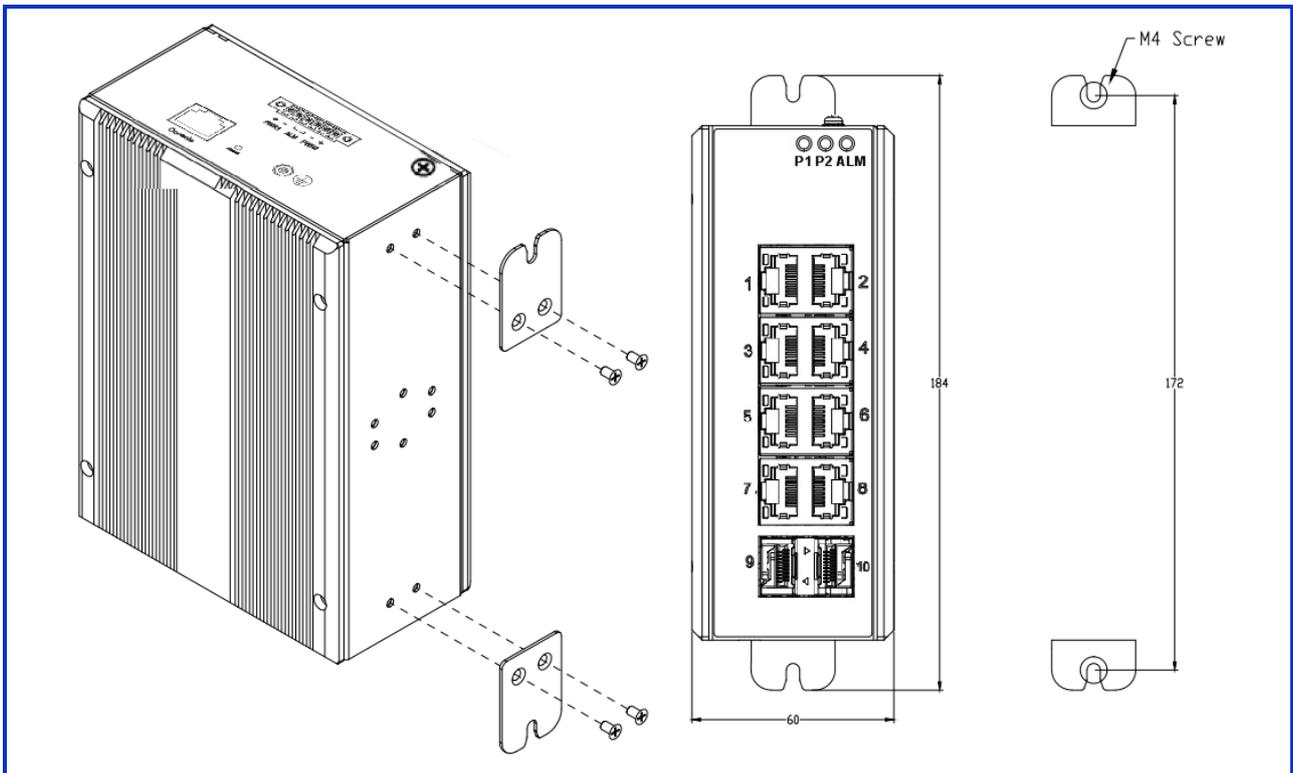
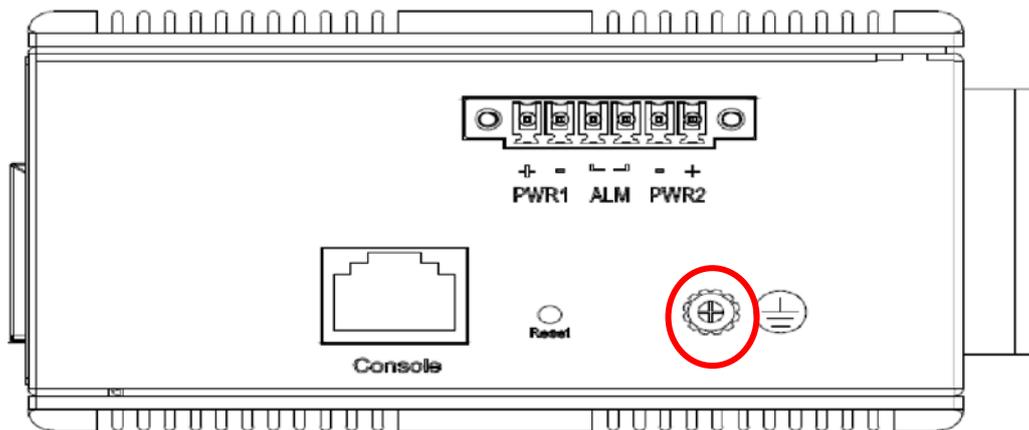


Abbildung 2 INDRy II Wandmontage

Erdungsanschlüsse

Um eine optimale Systemleistung zu gewährleisten, muss der INDRy II richtig geerdet werden.



Anschließen der Ethernet-Schnittstelle (RJ45 Ethernet)

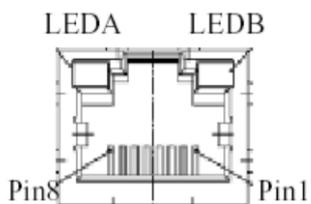
Der INDRy II unterstützt zwei verschiedene Schnittstellen: eine elektrische (RJ45) und eine optische (mini-GBIC).

Der Anschluss an einen PC erfolgt über ein gerade oder ein gekreuzt verdrahtetes Ethernet-Kabel.

- Der INDRy II Kupfer-Port lässt sich mit einem UTP- (Unshielded Twisted Pair) oder STP- (Shielded Twisted Pair) Ethernet-Kabel an ein Ethernet-Gerät anschließen.



Die folgende Abbildung und Tabelle zeigen die Belegung des RJ45-Steckers.



Stecker	Belegung
1,2	T/Rx+,T/Rx-
3,6	T/Rx+,T/Rx-
4,5	T/Rx+,T/Rx-
7,8	T/Rx+,T/Rx-

Anschließen der Ethernet-Schnittstelle (LWL)

Bereiten Sie ein geeignetes SFP-Modul vor, und installieren Sie es in den Optical Port. Danach können Sie die Glasfaserverkabelung, die LC-Stecker oder SC-Stecker (mit optionaler Nutzung eines SC-to-LC-Adapters) an den Glasfaseranschluss anschließen.

Siehe Table 1 für den LED-Status im Normalbetrieb.



Glasfaserkabel mit LC-Duplex-Stecker



Verbinden Sie das Glasfaserkabel an die SFP-Buchse

GEFAHR: Versuchen Sie niemals optische Stecker zu prüfen, weil diese Laserenergie abstrahlen könnten.

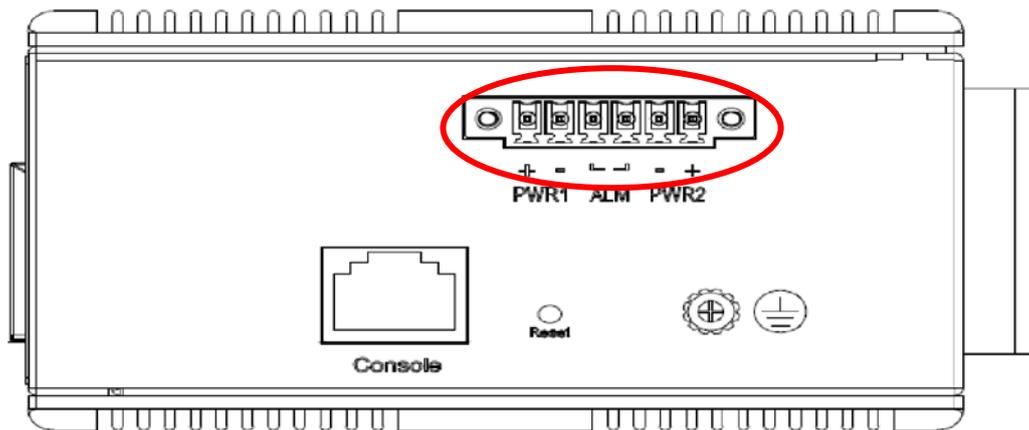
Schalten Sie das Laserprodukt nicht ein, ohne den Laser an das Glasfaserkabel angeschlossen und das Gehäuse in Position gebracht zu haben, weil Laserausgänge an dieser Stelle Infrarotlaserlicht abgeben.

Stromversorgung

Die DC-Stromversorgungsschnittstelle ist eine 6-pol. Klemmleiste mit Polaritätsangabe an der oberen Seite.

Die INDRy II kann über zwei Stromversorgungseingänge gespeist werden (Leistungsaufnahmebereich 12 V – 58 V). Der DC-Stromanschluss besteht aus einer 6-pol. Klemmleiste; an der mittleren Klemmleiste gibt es einen Alarmkontakt.

Siehe Table 1 für den LED-Status im Normalbetrieb.



Steckanschluss (6P Reihenklemme)

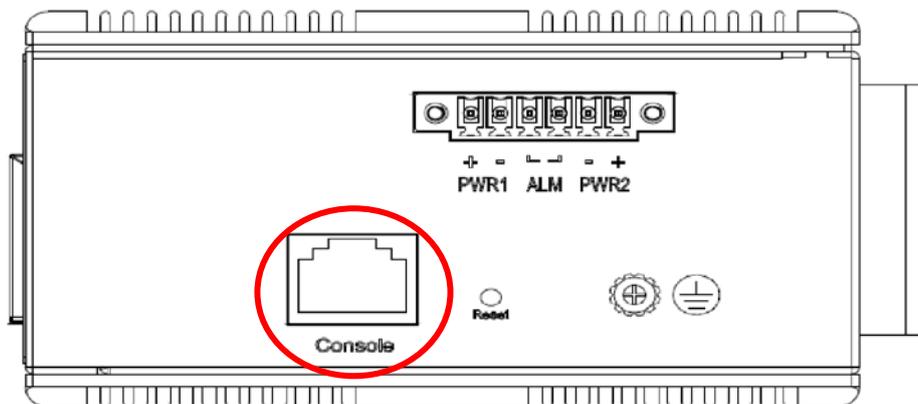
Input	DC 12-58 V
PWR1 +/-	Leistungsaufnahme 1 +/-
PWR2 +/-	Leistungsaufnahme 2 +/-
ALM	Alarmrelaisausgang

Hinweis: 1. Der DC-Stromanschluss muss an eine gut gesicherte Stromversorgung angeschlossen werden.

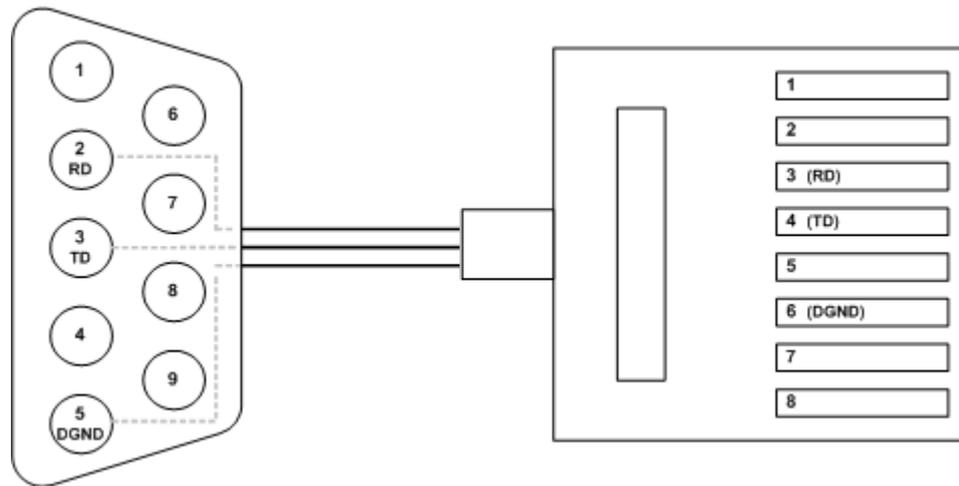
Konsolenverbindung

Der Konsolenport ist für die lokale Verwaltung mithilfe eines Terminalemulators oder eines Computers mit Terminalemulationssoftware.

- DB9-Stecker an den Computer-COM Port anschließen
- Baudrate: 115200bps
- 8 Datenbits, 1 Stoppbit
- Keine Priorität
- Keine Datenflusskontrolle



Um den Host-PC an den Konsolenport anzuschließen, wird der mitgelieferte - und nur der mitgelieferte RJ45 (männliche) Stecker für das RS232 DB9 (weibliche) Anschlusskabel benötigt. Der RJ45-Stecker des Kabels wird nicht an den Konsolenport des INDRY II angeschlossen; der DB9-Stecker des Kabels wird an den PC COM-Port angeschlossen. Steckerbelegung des Konsolenkabels siehe unten:



Initialisierung der Webschnittstelle (optional)

Webbrowser-Unterstützung

Internet Explorer 7 (oder neuere Version) mit den folgenden Standardeinstellungen wird empfohlen:

Zeichensatz	Lateinisch
Schriftart für Webseiten	Times New Roman
Schriftart für Klartext	Courier New
Codierung	Unicode (UTF-8)
Schriftgröße	Mittel

Firefox mit den folgenden Standardeinstellungen wird empfohlen:

Schriftart für Webseiten	Times New Roman
Codierung	Unicode (UTF-8)
Schriftgröße	16

Google Chrome mit den folgenden Standardeinstellungen wird empfohlen:

Schriftart für Webseiten	Times New Roman
Codierung	Unicode (UTF-8)
Schriftgröße	Mittel

Anschließen und Anmelden an INDRY II

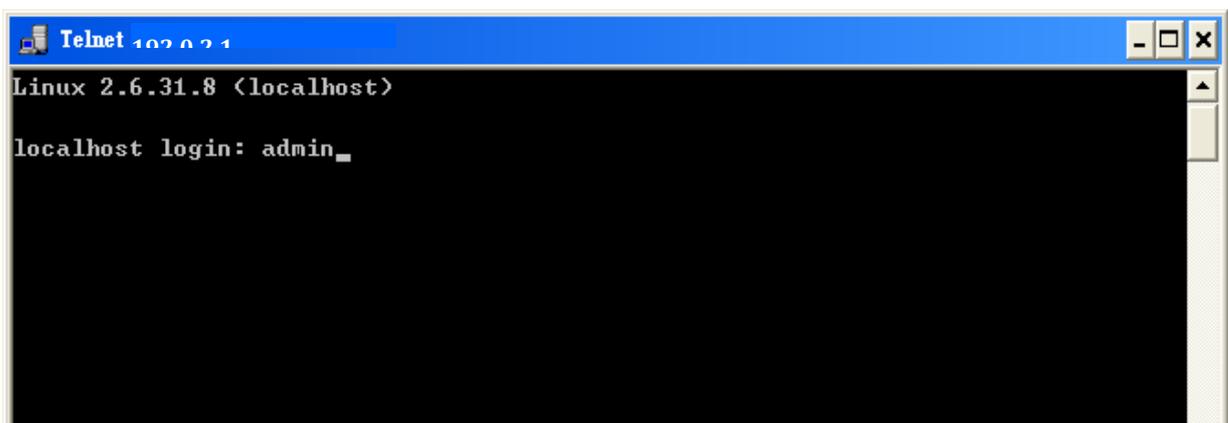
1. Anschließen an den INDRY II-Ethernet-Port (RJ45 Ethernet-Port).
2. **Werkseitig voreingestellte IP-Adresse: 192.0.2.1**
3. Anmeldung mit dem Standard-Konto und Passwort.
Benutzername: admin
Passwort: (ohne)

CLI-Initialisierung und -Konfiguration (optional)

1. Anschließen an den INDRY II-Ethernet-Port (RJ45 Ethernet-Port).
2. Befehl unter Telnet eingeben: **telnet 192.0.2.1**
3. Anmeldung mit dem Standard-Konto und Passwort.

Benutzername: admin

Passwort: (ohne)

A screenshot of a Telnet window titled "Telnet 192.0.2.1". The window shows a terminal session with the following text:

```
Linux 2.6.31.8 <localhost>
localhost login: admin_
```

4. Die IP-Adresse mithilfe der nachstehend aufgeführten Befehle ändern:

CLI-Befehl:

```
enable
configure terminal
interface vlan 1
ip address xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx
exit
```

Überwachen der Ethernet-Schnittstelle (RJ45 Ethernet)

Zur Überwachung eines 8 Gigabit-Ethernets mit Kupfer-Stecker (RJ45) siehe Figure 3. Siehe auch Table 1 für den LED-Status im Normalbetrieb.

Überwachen der Ethernet-Schnittstelle (SFP)

Zur Überwachung eines 4 Gigabit-Ethernets mit SFP-Stecker siehe Figure 3. Siehe auch Table 1 für den LED-Status im Normalbetrieb.

LED-STATUSANZEIGEN

Tabelle 1 LED-Statusanzeigen

LED	Status	Beschreibung
P1	Ein Grün	P1 Stromversorgung ist eingeschaltet
	Aus	P1-Stromversorgung nicht angeschlossen oder ausgeschaltet
P2	Ein Grün	P2 Stromversorgung ist eingeschaltet
	Aus	P2-Stromversorgung nicht angeschlossen oder ausgeschaltet
Alarm	Ein Rot	Auftreten eines Alarmereignisses
	Aus	Kein Alarm
Kupfer-Ports Link/Act	Ein Grün	Ethernet verbunden, aber keine Datenübertragung erkannt
	Blinkt grün	Ethernet verbunden und Datenübertragung erkannt
	Aus	Ethernet nicht verbunden
Kupfer-Ports Geschwindigkeit	Ein Gelb	Verbindung mit 100 Mbit/s oder 1000 Mbit/s entdeckt
	Aus	Keine Verbindung oder es wurde eine 10 Mbps-Verbindung erkannt
SFP-Port Link/Act	Ein Grün	Ethernet verbunden
	Aus	Ethernet nicht verbunden
SFP-Port Geschwindigkeit	Ein Gelb	SFP-Port-Geschwindigkeit 1000 Mbps-Verbindung erkannt.
	Aus	SFP-Port-Geschwindigkeit 100 Mbps-Verbindung erkannt.

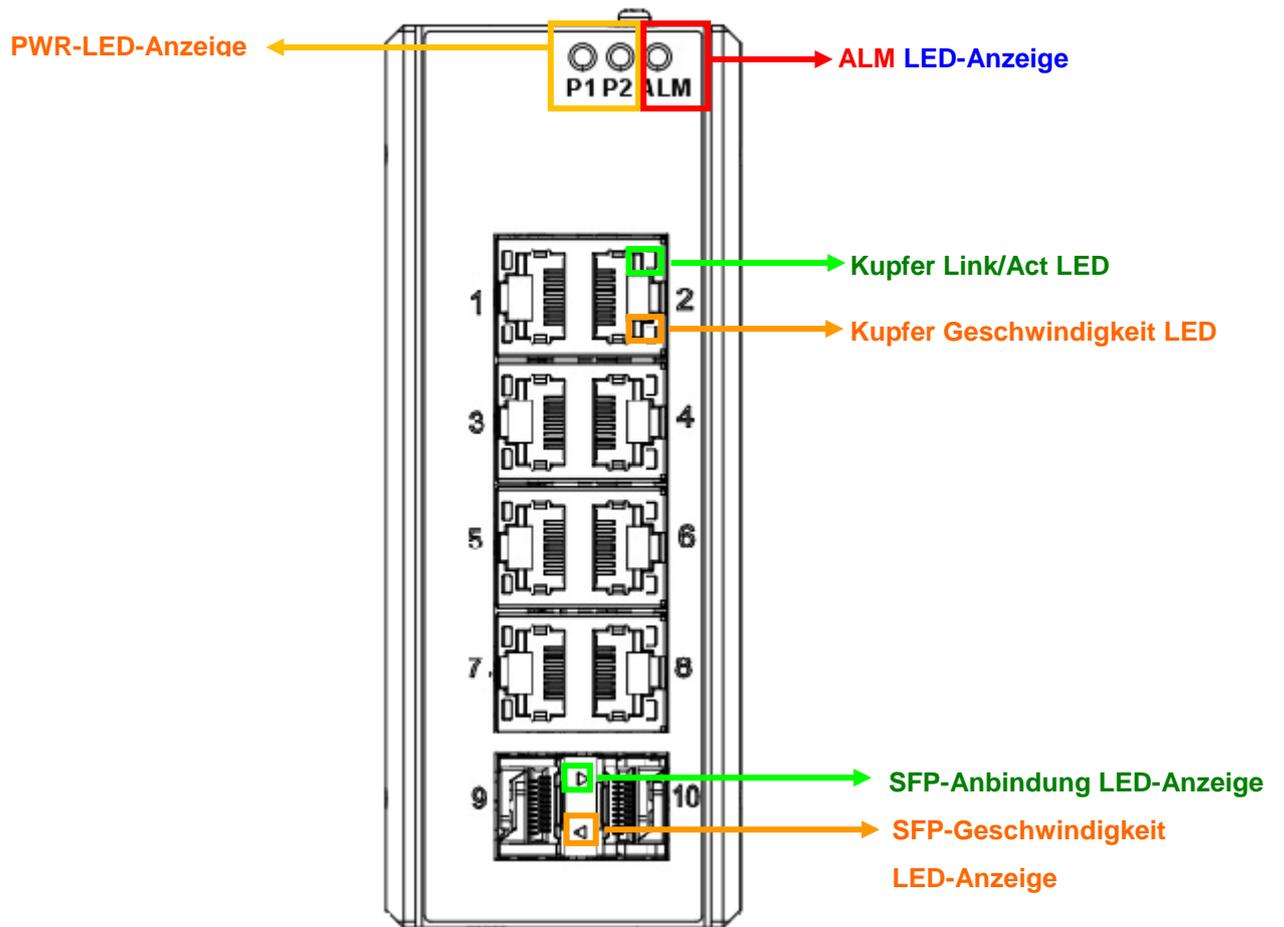
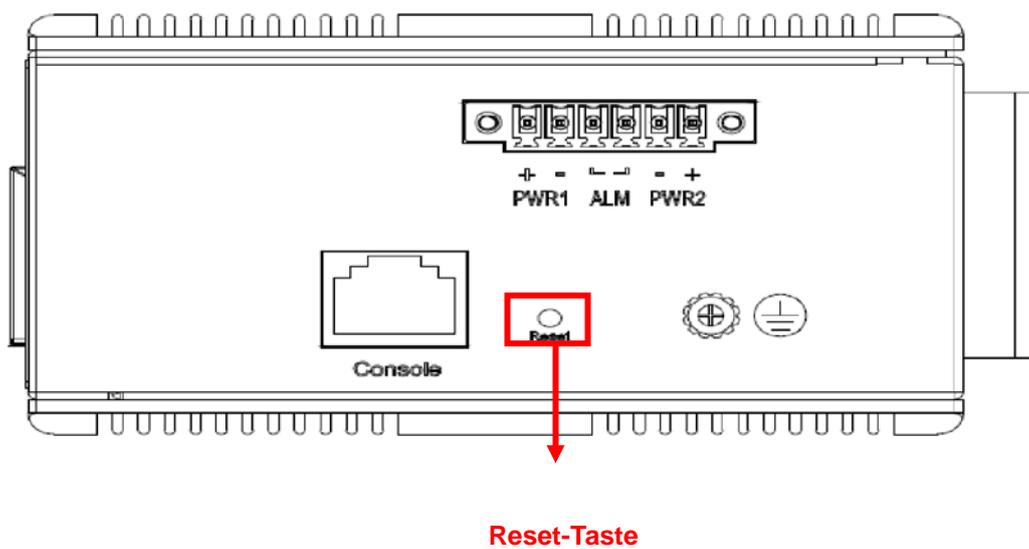


Abbildung 3 LED-Anzeigen, Modell INDRy II L hat mehr Anschlüsse, hier nur zur Erläuterung

ZURÜCKSETZEN DES SYSTEMS

Die Reset-Taste dient der Zurücksetzung des Systems, ohne Abschalten der Stromversorgung. Unter normalen Umständen werden Sie diese nicht benötigen. Trotzdem kann es in seltenen Fällen vorkommen, dass der INDRY II nicht reagiert; dann drücken Sie die Reset-Taste.



Anwendungshilfe

Leitfaden zum VLAN

Leitfaden zur Sicherheit

Ring Protection Anwendungshilfe

Leitfaden zum QoS

Leitfaden zum Link Fail Alarm

802.1x Authentifizierungs-

Anwendungshilfe

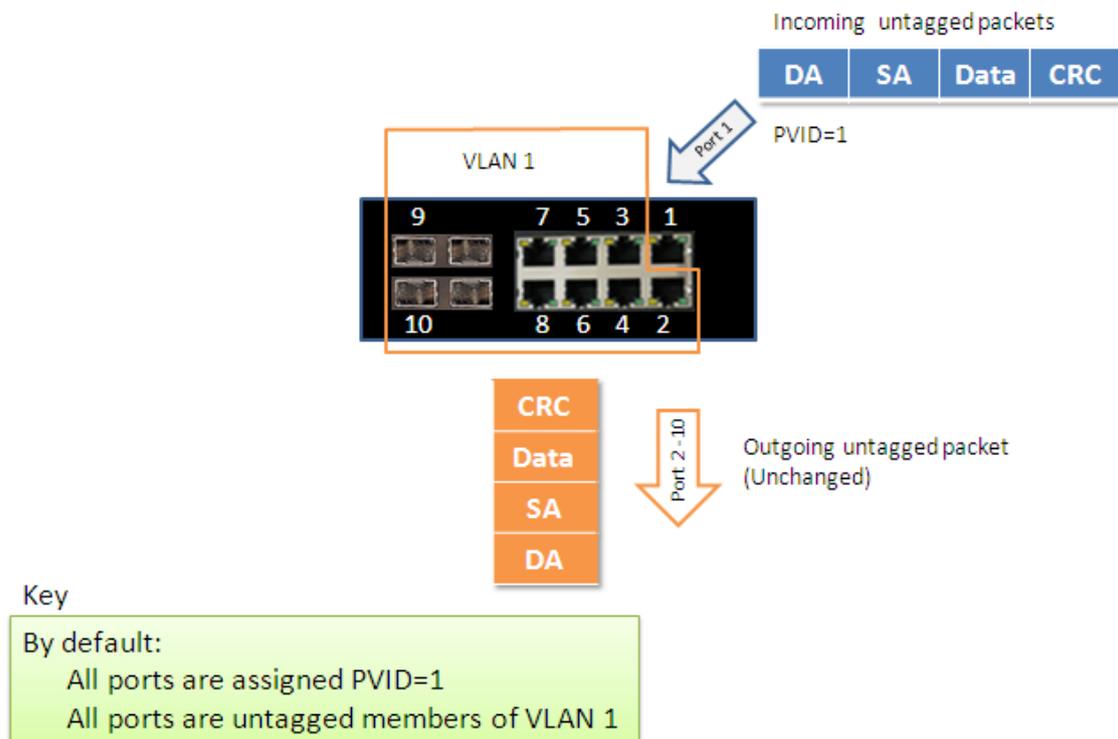
Leitfaden zum VLAN

Dieses Kapitel beschreibt, wie man Virtual LANs (VLANs) in INDRY II konfiguriert. Der INDRY II unterstützt bis zu 2048 VLANs. Ports werden in Broadcast-Domänen gruppiert, indem sie demselben VLAN zugeordnet werden. Bei VLAN eingehende Frames können nur in diesem VLAN weitergeleitet werden, und Multicast-Frames und unbekannte Unicast-Frames werden nur an Ports im selben VLAN weitergegeben.

Beispiel 1: Standardmäßige VLAN-Einstellungen

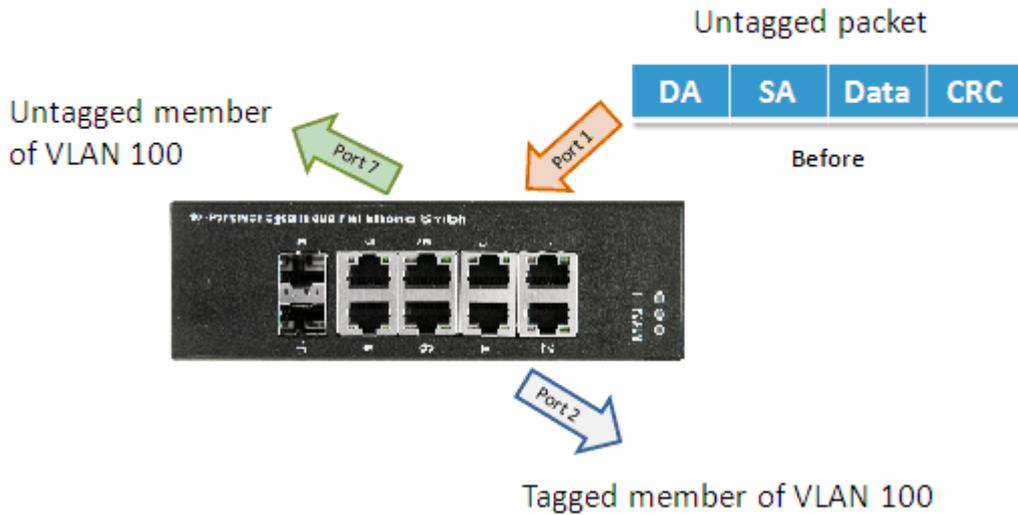
Jeder Port in INDRY II hat eine konfigurierbare VLAN-Standardnummer, bekannt als ihre PVID. Diese platziert alle Ports grundsätzlich an denselben VLAN, auch wenn jede Port-PVID für jede VLAN-Nummer zwischen 1 und 4094 konfigurierbar ist.

Bei den standardmäßigen Konfigurationseinstellungen für INDRY II sind alle Ports als unmarkierte Teile von VLAN 1 und alle Port als PVID=1 eingestellt. Im Beispiel der Standardkonfiguration in der folgenden Abbildung werden alle eingehenden Pakete über den standardmäßigen VLAN-Porterkenner (PVID=1) an VLAN 1 geschickt.



Beispiel 2: Port-basierte VLANs

Wenn INDRY II ein unmarkiertes VLAN-Paket erhält, wird es dem Frame entsprechend der PVID-Einstellung an dem Port mit einem VLAN-Tag versehen. Wie in der folgenden Abbildung dargestellt, wird das unmarkierte Paket markiert (mit einem Tag versehen), als es INDRY II über Port 2 verlässt, welcher als markiertes Teil des VLAN100 konfiguriert ist. Das unmarkierte Paket bleibt unverändert, als es INDRY II über Port 7 verlässt, welcher als unmarkiertes Teil des VLAN100 konfiguriert ist.



Konfiguration:

Step 1. Gehen Sie über Konfiguration -> VLANs -> Port VLAN-Konfiguration und konfigurieren Sie PVID 100 für Port 1, Port 2 und Port 7.

The screenshot shows the network configuration interface. The 'Global VLAN Configuration' section has 'Allowed Access VLANs' set to 1,100 and 'Ethertype for Custom S-ports' set to 88A8. The 'Port VLAN Configuration' table is as follows:

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	1	<>	<input type="checkbox"/>	<>	<>	1	
1	Trunk	100	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1-4095	
2	Trunk	100	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1-4095	
3	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
4	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
5	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
6	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
7	Trunk	100	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1-4095	
8	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	

Step 2. Wählen Sie den Menüpunkt Konfiguration -> VLAN -> Statisches VLAN. Erstellen Sie ein VLAN mit VLAN ID 100. Geben Sie in das Feld **Name** eine Bezeichnung für das VLAN ein.

The screenshot shows the 'Configuration / VLAN' page. The left sidebar has a red arrow pointing to the 'VLAN' menu item. The main area shows a table of VLAN configurations:

VID	Name	GE-1	GE-2	GE-3	GE-4	GE-5	GE-6	GE-7	GE-8	GE-9	GE-10	Modify
1	default	U	U	U	U	U	U	U	U	U	U	Modify
100	V100	T	T	-	-	-	-	U	-	-	-	Modify

Step 3. Weisen Sie VLAN eine Tag-Einstellung zu oder löschen Sie diese von einem Port, indem Sie die Kontrollbox unter einer individuellen Portnummer umschalten. Die Tag-Einstellungen bestimmen, ob vom Port übertragene Pakete mit VLAN ID versehen oder nicht versehen werden. Die Möglichkeiten für die Tag-Einstellungen sind:

- Tag All** Gibt an, dass ausgehende Pakete mit einer Port-Kennung versehen werden.
- Untag port vlan** Gibt an, dass ausgehende Pakete mit keiner Port-Kennung versehen werden.
- Untag All** Gibt an, dass alle Frames, unabhängig davon, ob sie einem portbasierten VLAN zugeordnet sind, ohne Kennung versendet werden.

In diesem Fall wird das getaggte VLAN100 für Port 1 und Port 2 eingerichtet und das ungetaggte VLAN100 für Port 7 konfiguriert.

The screenshot shows the 'Global VLAN Configuration' and 'Port VLAN Configuration' pages. The 'Port VLAN Configuration' table is as follows:

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	100	<>	<input checked="" type="checkbox"/>	<>	<>	1-4095	
1	Trunk	100	C-Port	<input checked="" type="checkbox"/>	Tagged Only	Tag All	1,100	
2	Trunk	100	C-Port	<input checked="" type="checkbox"/>	Tagged Only	Tag All	1,100	
3	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
4	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
5	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
6	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
7	Trunk	100	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1,100	
8	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	

Step 4. Ungetaggte Unicast-Pakete werden von Port 1 auf Port 2 und Port 7 weitergeleitet. Das Paket sollte am Switch mit der VID 100 versehen werden. Das Paket hat Zugriff auf Port 2 und Port 7. Die Kennung wird vom ausgehenden Paket entfernt, das Port 7 wieder als ungetaggttes Paket verlässt. Bei Port 2 wird das ausgehende Paket mit VID 100 als getaggtes Paket verschickt.

Step 5. Ungetaggte Unicast-Pakete werden von Port 2 auf Port 1 und Port 7 weitergeleitet. Das Paket sollte am Switch mit der VID 100 versehen werden. Das Paket hat Zugriff auf Port1 und Port 7 Die Kennung wird vom ausgehenden Paket entfernt, das Port 7 wieder als ungetaggttes Paket verlässt. Bei Port 1 wird das ausgehende Paket mit VID 100 als getaggtes Paket verschickt.

Step 6. Ungetaggte Unicast-Pakete werden von Port 7 auf Port 1 und Port 2 weitergeleitet. Das Paket sollte am Switch mit der VID 100 versehen werden. Das Paket hat Zugriff auf Port1 und Port 2 Bei Port 1 und Port 2 wird das ausgehende Paket mit VID 100 als getaggttes Paket verschickt.

Step 7. Wiederholen Sie Schritt 4 unter Anwendung von Broadcast- und Multicast-Paketen.

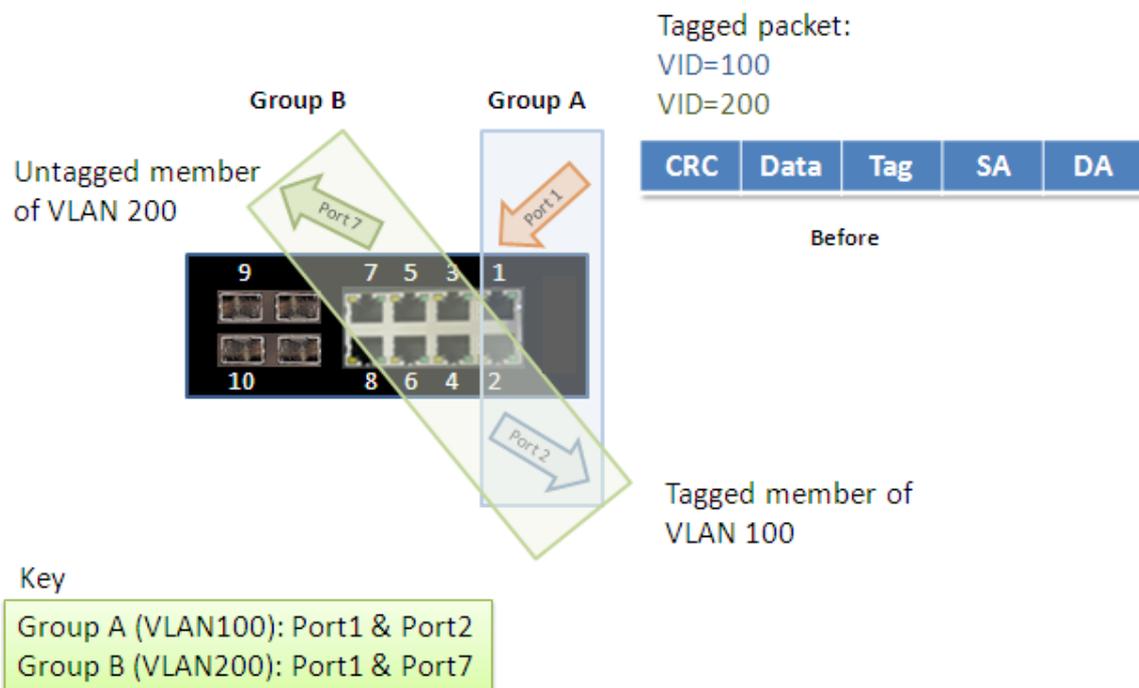
CLI-Befehl:

```
Schnittstellen-Gigabit 1
Standardmäßige VLAN-Einstellung 100
VLAN 100 getaggt
exit
Schnittstellen-Gigabit 2
Standardmäßige VLAN-Einstellung 100
VLAN 100 getaggt
exit
Schnittstellen-Gigabit 7
Standardmäßige VLAN-Einstellung 100
VLAN 100 ungetaggt
exit
```

Beispiel 3: IEEE 802.1Q Tagging

INDRY II ist in der Lage, auf 2 Ebenen Broadcast-Domänen zu generieren, durch Identifizierung der auf IEEE 802.1Q bestimmten VLAN ID. Es sendet einen Frame zwischen Brückenports, die der gleichen VLAN ID zugewiesen sind und kann mehrere VLANs für jeden Brückenport einstellen.

In der folgenden Abbildung werden die getaggten, eingehenden Pakete direkt an VLAN 100 und VLAN 200 geschickt, aufgrund der Tag-Zuordnung des Pakets. Port 2 ist als ein getaggtes Teil von VLAN 100 konfiguriert, und Port 7 ist als ein ungetaggtes Teil von VLAN 200 konfiguriert. Hosts im gleichen VLAN kommunizieren miteinander, als wenn sie in einem LAN wären. Allerdings können Hosts in verschiedenen VLANs nicht direkt miteinander kommunizieren.



In diesem Fall:

1. Die Hosts von Gruppe A können miteinander kommunizieren.
2. Die Hosts von Gruppe B können miteinander kommunizieren.
3. Die Hosts von Gruppe A und Gruppe B können nicht miteinander kommunizieren.
4. Sowohl Gruppe A als auch Gruppe B können über IVS514F ins Internet gehen.

Konfiguration:

Step 1. Gehen Sie zu Konfiguration -> VLANs -> Port VLAN-Konfiguration und spezifizieren Sie die VLAN-Teile wie folgt:

The screenshot shows the configuration interface for a network switch. On the left is a navigation menu with categories like Configuration, Monitor, Diagnostics, and Maintenance. The main area is titled 'Global VLAN Configuration' and contains two input fields: 'Allowed Access VLANs' with the value '1,100,200' and 'Ethertype for Custom S-ports' with the value '88A8'. Below this is the 'Port VLAN Configuration' section, which contains a table with 8 rows and 9 columns.

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
1	Trunk	1	C-Port	<input checked="" type="checkbox"/>	Tagged Only	Tag All	1,100,200	
2	Trunk	1	C-Port	<input checked="" type="checkbox"/>	Tagged Only	Tag All	1,100	
3	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
4	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
5	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
6	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
7	Trunk	1	C-Port	<input checked="" type="checkbox"/>	Tagged Only	Tag All	1,200	
8	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	

At the bottom of the configuration area are 'Save' and 'Reset' buttons.

Step 2. Übertragen Sie Unicast-Pakete mit VLAN-Tag 100 von Port 1 zu Port 2 und Port 7. Das Paket sollte am Switch mit der VID 100 versehen werden. Das Paket hat nur Zugang zu Port 2. Bei Port 2 wird das ausgehende Paket mit VID 100 als getaggttes Paket verschickt.

Step 3. Übertragen Sie Unicast-Pakete mit VLAN-Tag 200 von Port 1 zu Port 2 und Port 7. Das Paket sollte am Switch mit der VID 200 versehen werden. Das Paket hat nur Zugang zu Port 7. Das an Port 7 ausgehende Paket ist von seinem Tag als ungetaggttes Paket isoliert.

Step 4. Übertragen Sie Unicast-Pakete mit VLAN-Tag 100 von Port 2 zu Port 1 und Port 7. Das Paket sollte am Switch mit der VID 100 versehen werden. Das Paket hat nur Zugang zu Port 1. Bei Port 1 wird das ausgehende Paket mit VID 100 als getaggttes Paket verschickt.

Step 5. Übertragen Sie Unicast-Pakete mit VLAN-Tag 200 von Port 7 zu Port 1 und Port 2. Das Paket sollte am Switch mit der VID 200 versehen werden. Das Paket hat nur Zugang zu Port 1. Das an Port 1 ausgehende Paket wird als mit VID 200 getaggttes Paket weitergeleitet.

Step 6. Wiederholen Sie die oben genannten Schritte unter Anwendung von Broadcast- und Multicast-Paketen.

CLI-Befehl:

```
VLAN 100 v100
VLAN 200 v200
Schnittstellen-Gigabit 1
VLAN 100 getaggt
VLAN 200 getaggt
exit
Schnittstellen-Gigabit 2
VLAN 100 getaggt
exit
Schnittstellen-Gigabit 7
VLAN 200 ungetaggt
exit
```


Leitfaden zur Sicherheit

Die ACL-Funktion unterstützt die Zugangssteuerungssicherung für MAC-Adresse, IP-Adresse, Layer4 Port und Servicetyp. Jede hat fünf Aktionen: Deny, Permit, Queue Mapping, CoS Marking und Copy Frame. Anwender können standardmäßige ACL-Regeln zum Zulassen bzw. Verweigern einstellen (Permit oder Deny). Um diese ACL-Funktion zu verdeutlichen, siehe die folgende Tabelle.

Standardmäßige ACL-Regel	Aktionen				
	Verweigern	Zulassen	Queue Mapping	CoS Marking	Copy Frame
Zulassen	(a)	(b)	(c)	(d)	(e)
Verweigern	(f)	(g)	(h)	(i)	(j)

Kurzbeschreibungen der obigen Tabelle:

- (a): Alle Frames zulassen, aber die in ACL eingestellten Frames verweigern.
- (b): Alle Frames zulassen.
- (c): Alle Frames und Queue Mapping der übertragenen Frames zulassen.
- (d): Alle Frames und Änderung des CoS-Werts der übertragenen Frames zulassen.
- (e): Alle Frames und das Kopieren der in ACL für einen bestimmten GE-Port eingestellten Frames zulassen.
- (f): Keine Frames zulassen.
- (g) Nur die in ACL voreingestellten Frames zulassen.
- (h): Keine Frames zulassen.
- (i): Keine Frames zulassen.
- (j): Keine Frames zulassen, aber das Kopieren von Frames, die in ACL für einen bestimmten GE-Port eingestellt sind, zulassen.

Fall 1: ACL für MAC-Adresse

Um ACL an Mac zu adressieren, kann nach Mac-Adressquelle oder -ziel gefiltert werden, oder beides. Wenn beide Filter eingesetzt werden, werden Pakete konform beider Regeln behandelt. Mit anderen Worten, gefiltert wird nur, wenn beide Regeln zutreffen.

Wenn der Benutzer nur eine MAC-Zieladresse filtern will, muss die andere MAC-Adresse auf Null eingestellt werden. Das bedeutet, dass diese nicht geteilt werden kann. Neben der MAC-Adresse können auch VLAN und Ethernet für weitere Filter genutzt werden. Bestimmte VLAN- oder Ethernet-Typen generieren unter der MAC-Adresse ein Ergebnis. Wenn der Benutzer kein VLAN oder Ethernet handhabt, kann er einfach Nullwerte einstellen. Im Folgenden geht es um Beispiele aus der oben stehenden Tabelle:

- **Fall 1: (a)**

Der Anwender kann standardmäßige ACL-Regeln für GE-Ports eingeben, um Aktionen „Zulassen“ oder „zu verweigern“. Das bedeutet, dass der GE-Port alle Pakete bis auf die, die im ACL beschrieben werden, durchlassen kann.

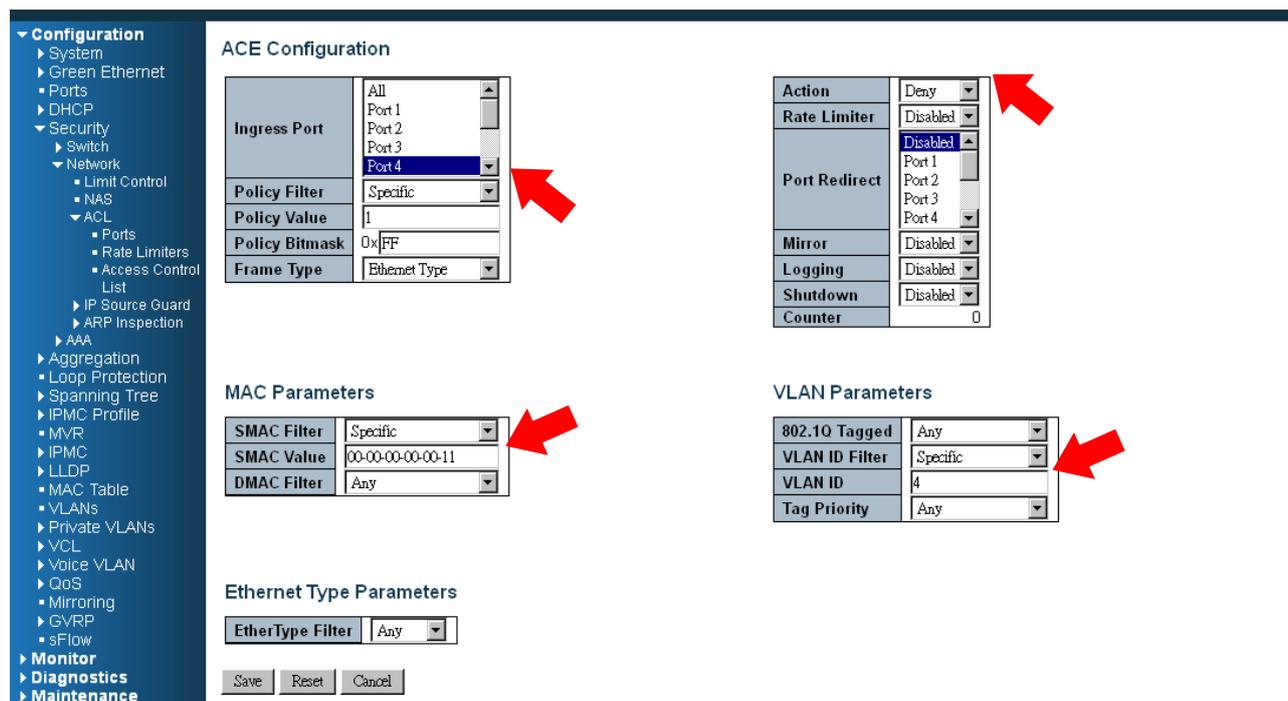
© Eine MAC-Zieladresse mit einer VLAN-Verbotsfiltrierung.

Schritt 1: Erstellen Sie ein neues ACL-Profil. (Profilname: DenySomeMac)

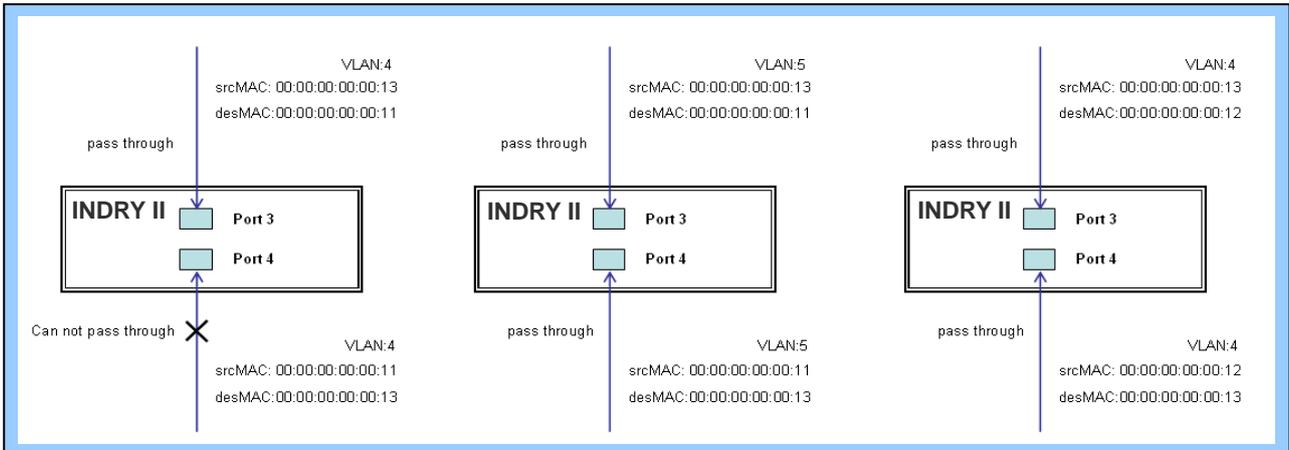


Schritt 2: Geben Sie eine neue ACL-Regel für dieses ACL-Profil ein. (Verweigern MAC: 11 und VLAN: 4)

Schritt 3: Verknüpfen Sie dieses ACL-Profil mit einem GE-Port. (PORT-4)



Schritt 4: Versenden Sie Frames zwischen PORT-3 und PORT-4, und prüfen Sie die Testergebnisse.



CLI-Befehl:

```
Zugangsliste Ace 1 Eingangsschnittstelle GigabitEthernet 1/4 policy
1 vid 4 Frametyp smac 00-00-00-00-00-11 Aktion verweigern
exit
Schnittstelle GigabitEthernet 1/3
  Amt-Switchport zugelassen für VLAN 4,5
  Amt-Switchport VLAN Tag native
!
Schnittstelle GigabitEthernet 1/4
  Amt-Switchport zugelassen für VLAN 4,5
  Amt-Switchport VLAN Tag nativevlan 4
exit
```

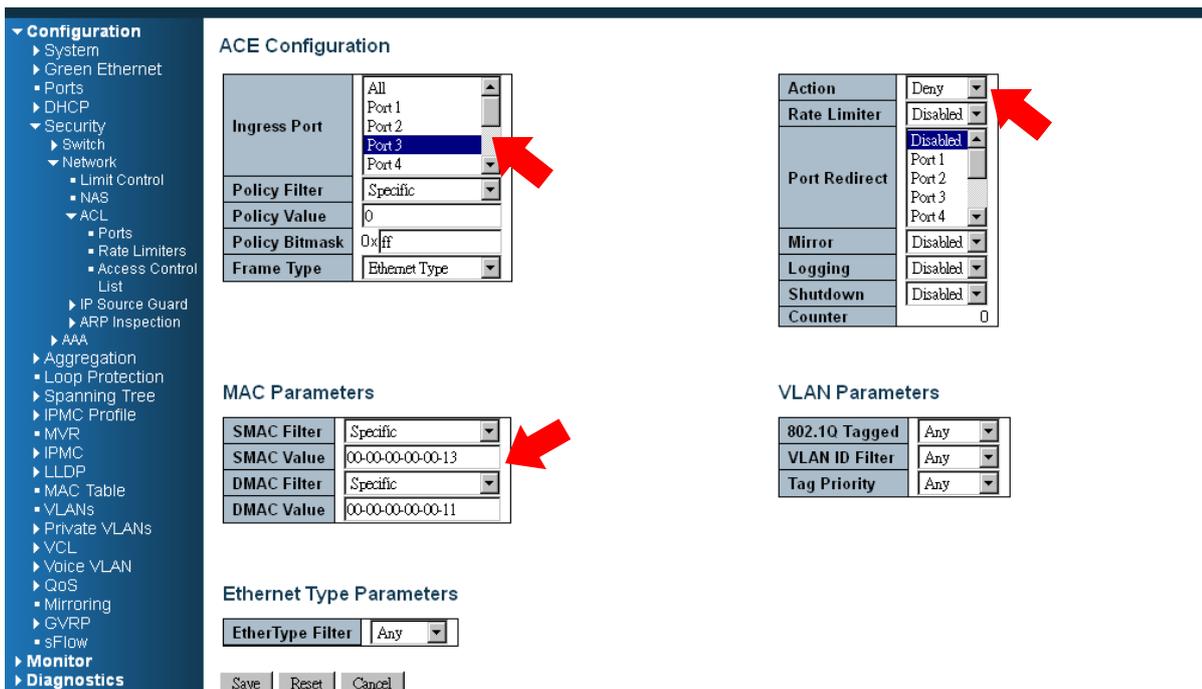
© Zwei MAC-Zieladressen mit Verbotsfiltrierung für alle VLANs.

Schritt 1: Erstellen Sie ein neues ACL-Profil. (Profilname: DenySomeMac)

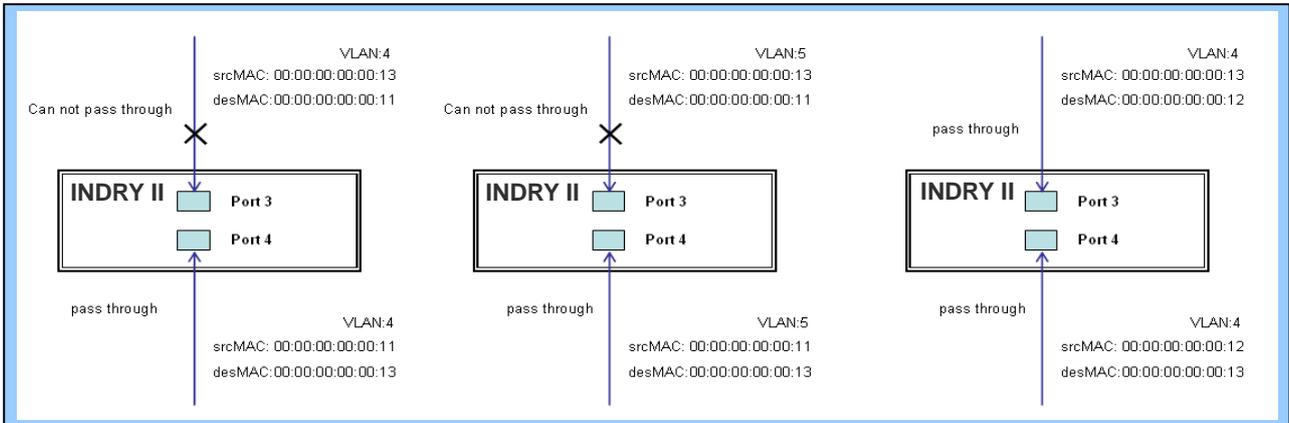


Schritt 2: Geben Sie eine neue ACL-Regel für dieses ACL-Profil ein. (Verweigern SrcMAC: 13 und DesMAC: 11)

Schritt 3: Verknüpfen Sie dieses ACL-Profil mit einem GE-Port. (PORT-3)



Schritt 4: Versenden Sie Frames zwischen PORT-3 und PORT-4, und prüfen Sie die Testergebnisse.



CLI-Befehl:

```
Zugangsliste Ace 2 Eingangsschnittstelle GigabitEthernet 1/3 policy 0 Frametyp etype
smac 00-00-00-00-00-13 dmac 00-00-00-00-00-11 Aktion verweigern
exit
Schnittstelle GigabitEthernet 1/3
  Amt-Switchport zugelassen für VLAN 4,5
  Amt-Switchport VLAN Tag native
!
Schnittstelle GigabitEthernet 1/4
  Amt-Switchport zugelassen für VLAN 4,5
  Amt-Switchport VLAN Tag nativevlan 4
exit
```

- **Fall 1: (b)**

In diesem Fall wird keine ACL-Funktion gehandhabt. Das bedeutet, alle Frames durchgelassen werden.

- **Fall 1: (c)**

Der Anwender kann standardmäßige ACL-Regeln für GE-Ports eingeben, um Aktionen „Zuzulassen“ oder ein geeignetes Profil mit „Queue Mapping“-Aktion für einige ACL-Funktionen zu verknüpfen. Das bedeutet, dass der GE-Port Queue Mapping 0~7 des von diesem Port erhaltenen Frames ausführen kann.

- **Fall 1: (d)**

Der Anwender kann standardmäßige ACL-Regeln für GE-Ports eingeben, um Aktionen „Zuzulassen“ oder ein geeignetes Profil mit „CoS Marking“-Aktion für einige ACL-Funktionen zu verknüpfen. Das bedeutet, dass der GE-Port CoS des von diesem Port erhaltenen VLAN-Frames erkennen kann.

- ◎ Eine MAC-Zieladresse mit CoS Marking-Aktion. (Ein VLAN, und Don't-Care-Ethernettyp)

Schritt 1: Erstellen Sie ein neues ACL-Profil. (Profilname: CoSMarkingTest)

Schritt 2: Geben Sie eine neue ACL-Regel für dieses ACL-Profil ein.
(Filter SrcMAC: 11 und VLAN ID: 4 Frame zu CoS: 2)

Schritt 3: Verknüpfen Sie dieses ACL-Profil mit einem GE-Port. (PORT-4)

The screenshot displays the configuration interface for an ACL profile named 'CoSMarkingTest'. The left sidebar shows the navigation tree with 'Security' > 'ACL' selected. The main area is divided into three sections:

- ACE Configuration:**

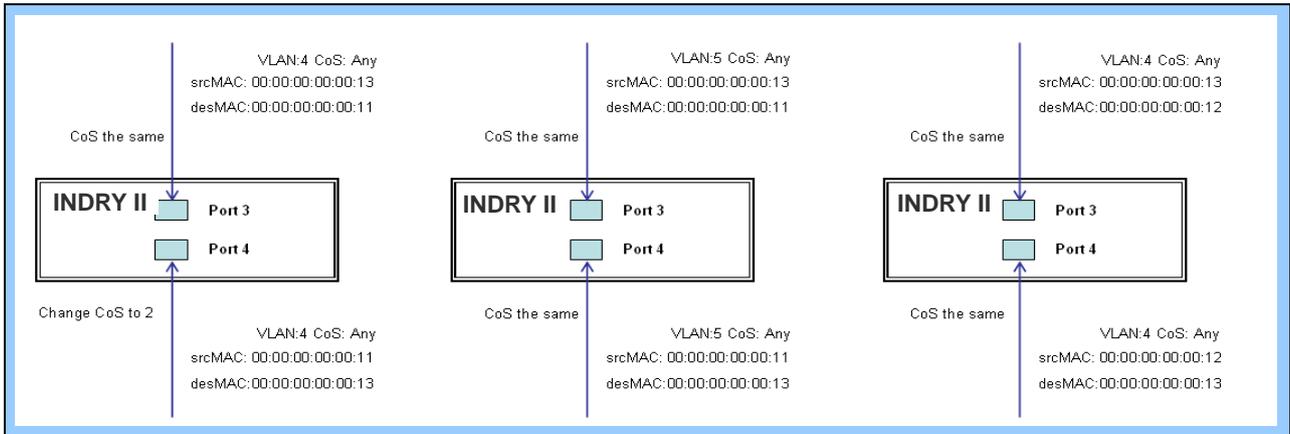
Ingress Port	All
Policy Filter	Specific
Policy Value	2
Policy Bitmask	0xfff
Frame Type	Ethernet Type
- MAC Parameters:**

SMAC Filter	Specific
SMAC Value	00-00-00-00-00-11
DMAC Filter	Any
- VLAN Parameters:**

802.1Q Tagged	Enabled
VLAN ID Filter	Specific
VLAN ID	4
Tag Priority	2

Additional configuration options on the right include Action (Deny), Rate Limiter (Disabled), Port Redirect (Disabled), Mirror (Disabled), Logging (Disabled), Shutdown (Disabled), and Counter (0). A red arrow points to the '802.1Q Tagged' field in the VLAN Parameters section.

Schritt 4: Versenden Sie Frames zwischen PORT-3 und PORT-4, und prüfen Sie die Testergebnisse.



CLI-Befehl:

```
Zugangsliste Ace 1 neben 2 Eingangsschnittstelle GigabitEthernet 1/4 policy 1 vid 4 Frametyp
etype smac 00-00-00-00-00-11 Aktion verweigern
exit
Schnittstelle GigabitEthernet 1/3
  Amt-Switchport zugelassen für VLAN 4,5
  Amt-Switchport VLAN Tag native
!
Schnittstelle GigabitEthernet 1/4
  Amt-Switchport zugelassen für VLAN 4,5
  Amt-Switchport VLAN Tag native
exit
```

● Fall 1: (e)

Der Anwender kann standardmäßige ACL-Regeln für GE-Ports eingeben, um Aktionen „Zuzulassen“ oder ein geeignetes Profil mit „Copy Frame“-Aktion für den Mirror Analyzer zu verknüpfen. Das bedeutet, dass das System Frames vom verknüpften GE-Port zum Analyse-Port kopiert.

© Zwei MAC-Zieladressen mit „Copy Frame“-Aktion.
(Don't care VLAN ID, Ethernettyp)

Schritt 1: Erstellen Sie ein neues ACL-Profil. (Profilname: CopyFrameTest)

Schritt 2: Geben Sie eine neue ACL-Regel für dieses ACL-Profil ein. (SrcMAC: 13 und DesMAC: 11)

Schritt 3: Stellen Sie den Analyse-Port ein, um den Analyse-Port zu aktivieren und zu kopieren.

Schritt 4: Verknüpfen Sie dieses ACL-Profil mit einem GE-Port. (PORT-3)

- ▼ Configuration
 - ▶ System
 - ▶ Green Ethernet
 - Ports
 - ▶ DHCP
 - ▼ Security
 - ▶ Switch
 - ▼ Network
 - Limit Control
 - NAS
 - ▼ ACL
 - Ports
 - Rate Limiters
 - Access Control List
 - ▶ IP Source Guard
 - ▶ ARP Inspection
 - ▶ AAA
 - ▶ Aggregation
 - Loop Protection
 - ▶ Spanning Tree
 - ▶ IPMC Profile
 - MVR
 - ▶ IPMC
 - ▶ LLDP
 - MAC Table
 - VLANs
 - ▶ Private VLANs
 - ▶ VCL
 - ▶ Voice VLAN
 - ▶ QoS
 - Mirroring
 - ▶ GVRP
 - sFlow
 - ▶ Monitor
 - ▶ Diagnostics
 - ▶ Maintenance

ACE Configuration

Ingress Port	All Port 1 Port 2 Port 3 Port 4
Policy Filter	Specific
Policy Value	0
Policy Bitmask	0x FF
Frame Type	Ethernet Type

MAC Parameters

SMAC Filter	Specific
SMAC Value	00-00-00-00-00-13
DMAC Filter	Specific
DMAC Value	00-00-00-00-00-11

Ethernet Type Parameters

EtherType Filter	Any
------------------	-----

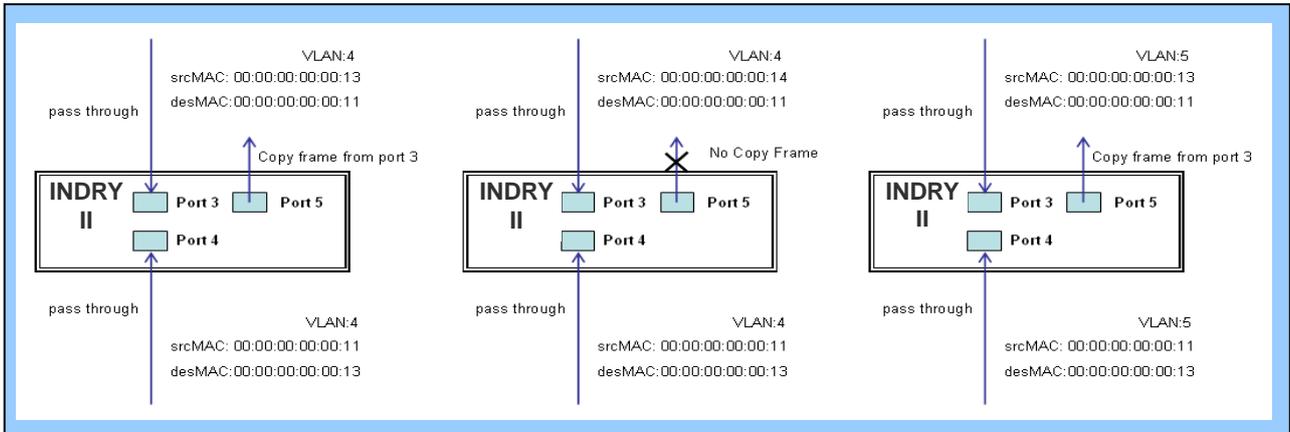
Action	Deny
Rate Limiter	Disabled
Port Redirect	Port 2 Port 3 Port 4 Port 5 Port 6 Port 7
Mirror	Enabled
Logging	Disabled
Shutdown	Disabled
Counter	0

VLAN Parameters

802.1Q Tagged	Any
VLAN ID Filter	Any
Tag Priority	Any



Schritt 5: Versenden Sie Frames zwischen PORT-3 und PORT-4, und prüfen Sie die Testergebnisse.



CLI-Befehl:

```
Zugangsliste Ace 2 neben 3 Eingangsschnittstelle GigabitEthernet 1/3 policy 0 Frametyp etype
smac 00-00-00-00-00-13 dmac 00-00-00-00-00-11 Aktion verweigern auf Spiegel umleiten
Schnittstelle GigabitEthernet 1/5
exit
Schnittstelle GigabitEthernet 1/3
  Amt-Switchport zugelassen für VLAN 4,5
  Amt-Switchport VLAN Tag native
!
Schnittstelle GigabitEthernet 1/4
  Amt-Switchport zugelassen für VLAN 4,5
  Amt-Switchport VLAN Tag native
exit
```

- **Fall 1: (f)**

Das bedeutet, dass keine Frames durchgelassen werden.

- **Fall 1: (g)**

Der Anwender kann standardmäßige ACL-Regeln für GE-Ports eingeben, um Aktionen „zu verweigern“ oder mit einem bestimmten Profil in ACL zu verknüpfen, um die Aktion „zuzulassen“. Das bedeutet, dass der GE-Port keine Pakete bis auf die, die im ACL beschrieben werden, durchlassen kann.

© Eine MAC-Zieladresse mit einem VLAN-Zulassungsfiler.

Schritt 1: Erstellen Sie ein neues ACL-Profil. (Profilname: AllowSomeMac)

Schritt 2: Geben Sie eine neue ACL-Regel für dieses ACL-Profil ein. (Zulassen MAC: 11 und VLAN: 4)

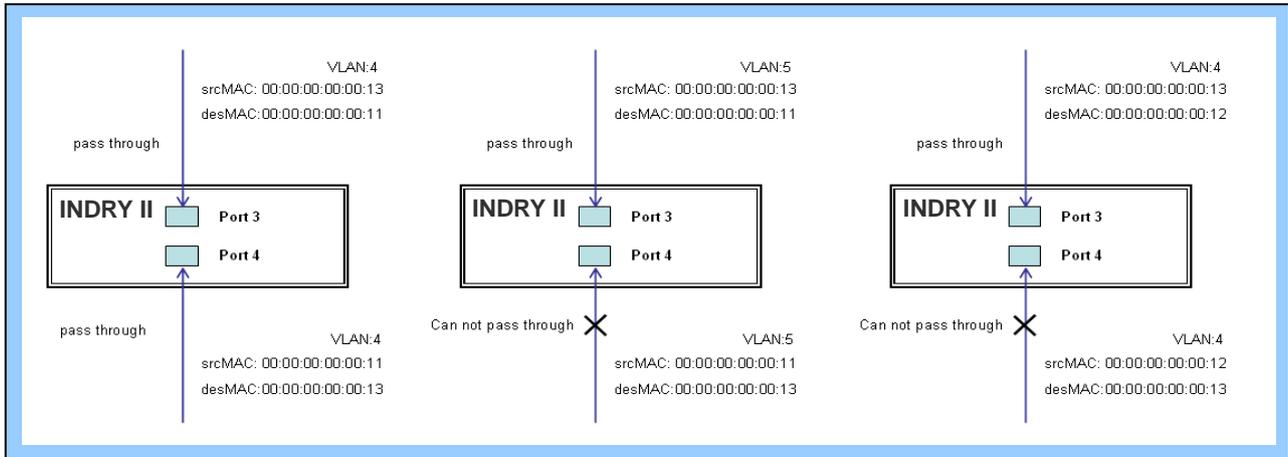
Schritt 3: Verknüpfen Sie dieses ACL-Profil mit einem GE-Port. (PORT-4)

The screenshot displays the configuration interface for an Access Control Entry (ACE). On the left is a navigation tree with categories like Configuration, Monitor, Diagnostics, and Maintenance. The main area is divided into several sections:

- ACE Configuration:** A table with fields: Ingress Port (All, Port 1, Port 2, Port 3, Port 4), Policy Filter (Specific), Policy Value (3), Policy Bitmask (0x0fff), and Frame Type (Ethernet Type).
- MAC Parameters:** A table with fields: SMAC Filter (Specific), SMAC Value (00-00-00-00-00-01), and DMAC Filter (Any).
- Ethernet Type Parameters:** A table with field: EtherType Filter (Any).
- VLAN Parameters:** A table with fields: 802.1Q Tagged (Enabled), VLAN ID Filter (Specific), VLAN ID (4), and Tag Priority (Any).
- Action Parameters:** A table with fields: Action (Permit), Rate Limiter (Disabled), Mirror (Disabled), Logging (Disabled), Shutdown (Disabled), and Counter (0). A red arrow points to the Action dropdown.

At the bottom of the configuration area are buttons for Save, Reset, and Cancel.

Schritt 4: Versenden Sie Frames zwischen PORT-3 und PORT-4, und prüfen Sie die Testergebnisse.



CLI-Befehl:

```
Zugangsliste Ace 4 Eingangsschnittstelle GigabitEthernet 1/4 policy 3 Tag getaggt vid 4 Frametyp
etype smac 00-00-00-00-00-11
exit
Schnittstelle GigabitEthernet 1/3
Amt-Switchport zugelassen für VLAN 4,5
Amt-Switchport VLAN Tag native
!
Schnittstelle GigabitEthernet 1/4
Amt-Switchport zugelassen für VLAN 4,5
Amt-Switchport VLAN Tag native
exit
```

© Zwei MAC-Adressen mit allen VLAN-Zulassungsfiltren.

Schritt 1: Erstellen Sie ein neues ACL-Profil. (Profilname: AllowSomeMac)

Schritt 2: Geben Sie eine neue ACL-Regel für dieses ACL-Profil ein. (Zulassen SrcMAC: 13 und DesMAC: 11)

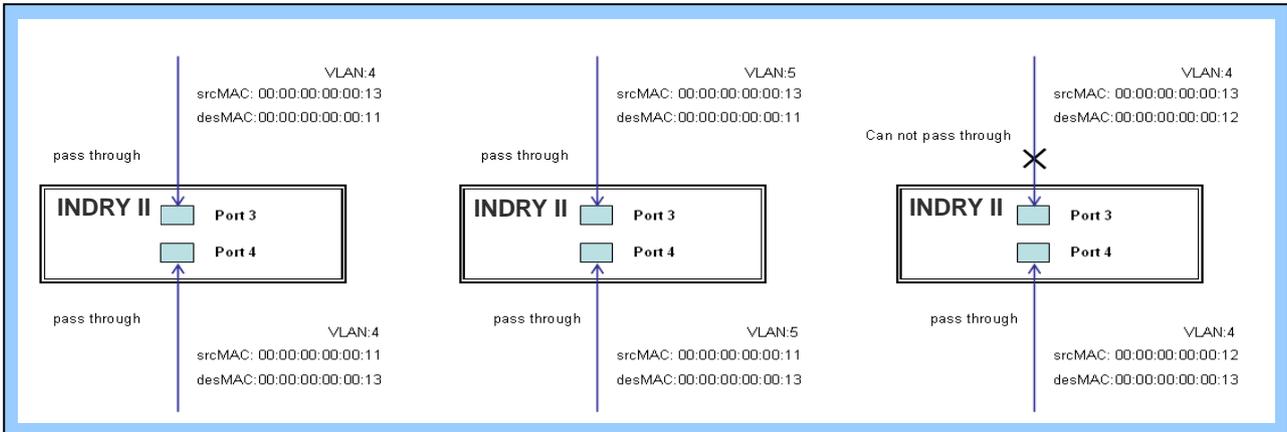
Schritt 3: Verknüpfen Sie dieses ACL-Profil mit einem GE-Port. (PORT-3)

The screenshot shows a network configuration interface with a sidebar on the left and a main configuration area on the right. The sidebar is titled 'Configuration' and includes sections for System, Green Ethernet, Ports, DHCP, Security, Network Control, AAA, Aggregation, and Monitor/Diagnostics/Maintenance. The main area is titled 'ACE Configuration' and contains several sections:

- ACE Configuration:** A table with fields: Ingress Port (dropdown menu with options All, Port 1, Port 2, Port 3, Port 4; Port 3 is selected), Policy Filter (Specific), Policy Value (5), Policy Bitmask (0x0fff), and Frame Type (Ethernet Type).
- MAC Parameters:** A table with fields: SMAC Filter (Specific), SMAC Value (00-00-00-00-00-13), DMAC Filter (Specific), and DMAC Value (00-00-00-00-00-11).
- Ethernet Type Parameters:** A table with field: EtherType Filter (Any).
- Action Parameters:** A table with fields: Action (Permit), Rate Limiter (Disabled), Mirror (Disabled), Logging (Disabled), Shutdown (Disabled), and Counter (0).
- VLAN Parameters:** A table with fields: 802.1Q Tagged (Any), VLAN ID Filter (Any), and Tag Priority (Any).

At the bottom of the ACE Configuration section, there are buttons for 'Save', 'Reset', and 'Cancel'.

Schritt 4: Versenden Sie Frames zwischen PORT-3 und PORT-4, und prüfen Sie die Testergebnisse.



CLI-Befehl:

```
Zugangsliste Ace 5 Eingangsschnittstelle GigabitEthernet 1/3 policy 5 Frametyp etype smac  
00-00-00-00-00-13 dmac 00-00-00-00-00-11  
exit  
Schnittstelle GigabitEthernet 1/3  
  Amt-Switchport zugelassen für VLAN 4,5  
  Amt-Switchport VLAN Tag native  
!  
Schnittstelle GigabitEthernet 1/4  
  Amt-Switchport zugelassen für VLAN 4,5  
  Amt-Switchport VLAN Tag native  
exit
```

- **Fall 1: (h)**

Aufgrund der voreingestellten ACL-Regel von GE, ist der Port „verweigert“, Queue Mapping-Aktion macht keinen Sinn. Wir führen diesen Fall nicht durch.

- **Fall 1: (i)**

Aufgrund der voreingestellten ACL-Regel von GE, ist der Port „verweigert“, CoS Marking-Aktion macht keinen Sinn. Wir führen diesen Fall nicht durch.

- **Fall 1: (j)**

Der Anwender kann standardmäßige ACL-Regeln für GE-Ports eingeben, um Aktionen „zu verweigern“ oder ein geeignetes Profil mit „Copy Frame“-Aktion für den Mirror Analyzer zu verknüpfen. Das bedeutet, dass das System Frames vom verknüpften GE-Port zum Analyse-Port kopiert. Es wurde kein Frame von dem verweigerten GE-Port, sondern vom Mirror Analyzer empfangen.

© Eine MAC-Zieladresse mit „Copy Frame“-Aktion. (Don't care VLAN, Ethertyp)

Schritt 1: Erstellen Sie ein neues ACL-Profil. (Profilname: CopyFrameTest)

Schritt 2: Geben Sie eine neue ACL-Regel für dieses ACL-Profil ein. (SrcMAC: 13 und DesMAC: 11)

ACE Configuration

Ingress Port	All Port 1 Port 2 Port 3 Port 4
Policy Filter	Specific
Policy Value	4
Policy Bitmask	0xfff
Frame Type	Ethernet Type

MAC Parameters

SMAC Filter	Specific
SMAC Value	00-00-00-00-00-13
DMAC Filter	Specific
DMAC Value	00-00-00-00-00-11

Ethernet Type Parameters

EtherType Filter	Any
------------------	-----

VLAN Parameters

802.1Q Tagged	Any
VLAN ID Filter	Any
Tag Priority	Any

Action

Action	Permit
Rate Limiter	Disabled
Mirror	Enabled
Logging	Disabled
Shutdown	Disabled
Counter	0

Save Reset Cancel

Schritt 3: Verknüpfen Sie dieses ACL-Profil mit einem GE-Port. (PORT-3)

Schritt 4: Stellen Sie den Analyse-Port ein, um den Analyse-Port zu aktivieren und zu kopieren.



- ▼ Configuration
 - ▶ System
 - ▶ Green Ethernet
 - ▶ Ports
 - ▶ DHCP
 - ▼ Security
 - ▶ Switch
 - ▼ Network
 - Limit Control
 - NAS
 - ▼ ACL
 - Ports
 - Rate Limiters
 - Access Control List
 - ▶ IP Source Guard
 - ▶ ARP Inspection
 - ▶ AAA
 - ▶ Aggregation
 - ▶ Loop Protection
 - ▶ Spanning Tree
 - ▶ IPMC Profile
 - MVR
 - ▶ IPMC
 - ▶ LLDP
 - MAC Table
 - VLANs
 - ▶ Private VLANs
 - ▶ VCL
 - ▶ Voice VLAN
 - ▶ QoS
 - Mirroring
 - ▶ GVRP
 - sFlow
 - ▶ Monitor
 - ▶ Diagnostics
 - ▶ Maintenance

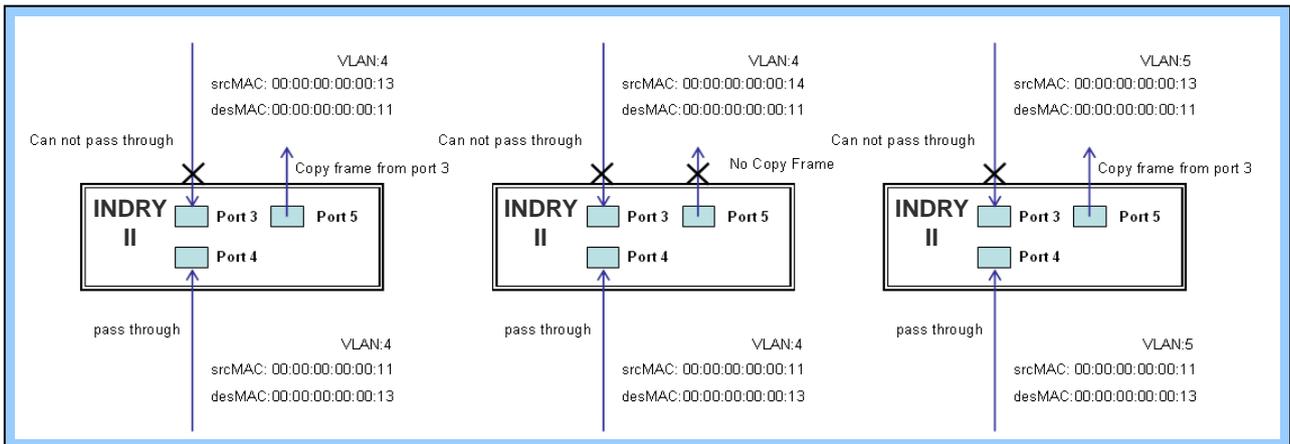
Mirror Configuration

Port to mirror to:

Mirror Port Configuration

Port	Mode
*	<input type="text" value=""/>
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled
CPU	Enabled

Schritt 5: Versenden Sie Frames zwischen PORT-3 und PORT-4, und prüfen Sie die Testergebnisse.



CLI-Befehl:

```
Zugangsliste Ace 5 neben 6 Eingangsschnittstelle GigabitEthernet 1/3 policy 5 Frametyp etype smac
00-00-00-00-00-13 dmac 00-00-00-00-00-11
Beenden
Zielschnittstelle GigabitEthernet 1/5 überwachen
Quelle cpu überwachen, beide
exit
Schnittstelle GigabitEthernet 1/3
  Amt-Switchport zugelassen für VLAN 4,5
  Amt-Switchport VLAN Tag native
!
Schnittstelle GigabitEthernet 1/4
  Amt-Switchport zugelassen für VLAN 4,5
  Amt-Switchport VLAN Tag native
exit
```

Fall 2: ACL für IP-Adresse

Um ACL an IP zu adressieren, kann nach IP-Adressquelle oder -ziel gefiltert werden, oder beides. Es ist auch möglich einen IP-Bereich in ACL einzustellen. Wenn beide Filter eingesetzt werden, werden Pakete konform beider Regeln behandelt. Mit anderen Worten, gefiltert wird nur, wenn beide Regeln zutreffen.

Wenn der Benutzer nur eine IP-Zieladresse filtern will, muss die andere IP-Adresse auf Null eingestellt werden. Das bedeutet, dass diese nicht geteilt werden kann. Neben der IP-Adresse können auch Protokolle für weitere Filter genutzt werden. (TCP=6, UDP=17, etc.) Ein bestimmtes Protokoll unter diesen IP-Adressen hat eine Wirkung. Wenn der Benutzer kein Protokoll handhabt, kann er einfach einen Nullwert einstellen. Hinsichtlich des Detailtests, siehe MAC ACL oben.

Fall 3: ACL für L4 Port

Für Layer4 Port ACL, kann der Filter nach (1) IP-Quellenadresse, (2) L4 Quellen-Port, (3) IP-Zieladresse, (4) L4 Ziel-Port, und (5) UDP oder TCP-Protokoll suchen. Der Benutzer kann wählen, ob er den Filter (1)~(4) für alle oder spezielle Werte nutzen möchte, aber es muss genau ein Protokoll aus UDP oder TCP ausgewählt werden.

Wenn beide Filter (IP-Zieladresse und L4-Port) eingesetzt werden, werden Pakete konform beider Regeln behandelt. Mit anderen Worten, gefiltert wird nur, wenn beide Regeln zutreffen.

Wenn der Benutzer nur eine IP-Zieladresse oder einen L4-Port filtern will, müssen die andere IP-Adresse und der L4-Port auf Null eingestellt werden. Das bedeutet, dass diese nicht geteilt werden kann. Hinsichtlich des Detailtests, siehe MAC ACL oben.

Fall 4: ACL für ToS

Für den Servicetyp (ToS) kann nach (1) IP-Quellenadresse mit ToS-Typ oder (2) IP-Zieladresse mit ToS-Typ oder beidem (3) oder (4) keinem von beidem (nur Filter ToS) gefiltert werden. Wenn beide Filter eingesetzt werden, werden Pakete konform beider Regeln behandelt. Mit anderen Worten, gefiltert wird nur, wenn beide Regeln zutreffen.

Wenn der Benutzer nur eine IP-Zieladresse filtern will, muss die andere IP-Adresse auf Null eingestellt werden. Das bedeutet, dass diese nicht geteilt werden kann. Hinsichtlich des Detailtests, siehe Fall 1 MAC ACL oben.

Gültige Werte: Präzedenz: 0~7, ToS: 0~15, DSCP: 0~63

0	1	2	3	4	5	6	7
Precedence				Type of Service			

0	1	2	3	4	5	6	7
DS field				ECN field			

Dieser Wert (7) ist belegt und auf 0 eingestellt.

Ex: Pre (001) bedeutet 1

Pre (100) bedeutet 4

ToS (00010) bedeutet 1

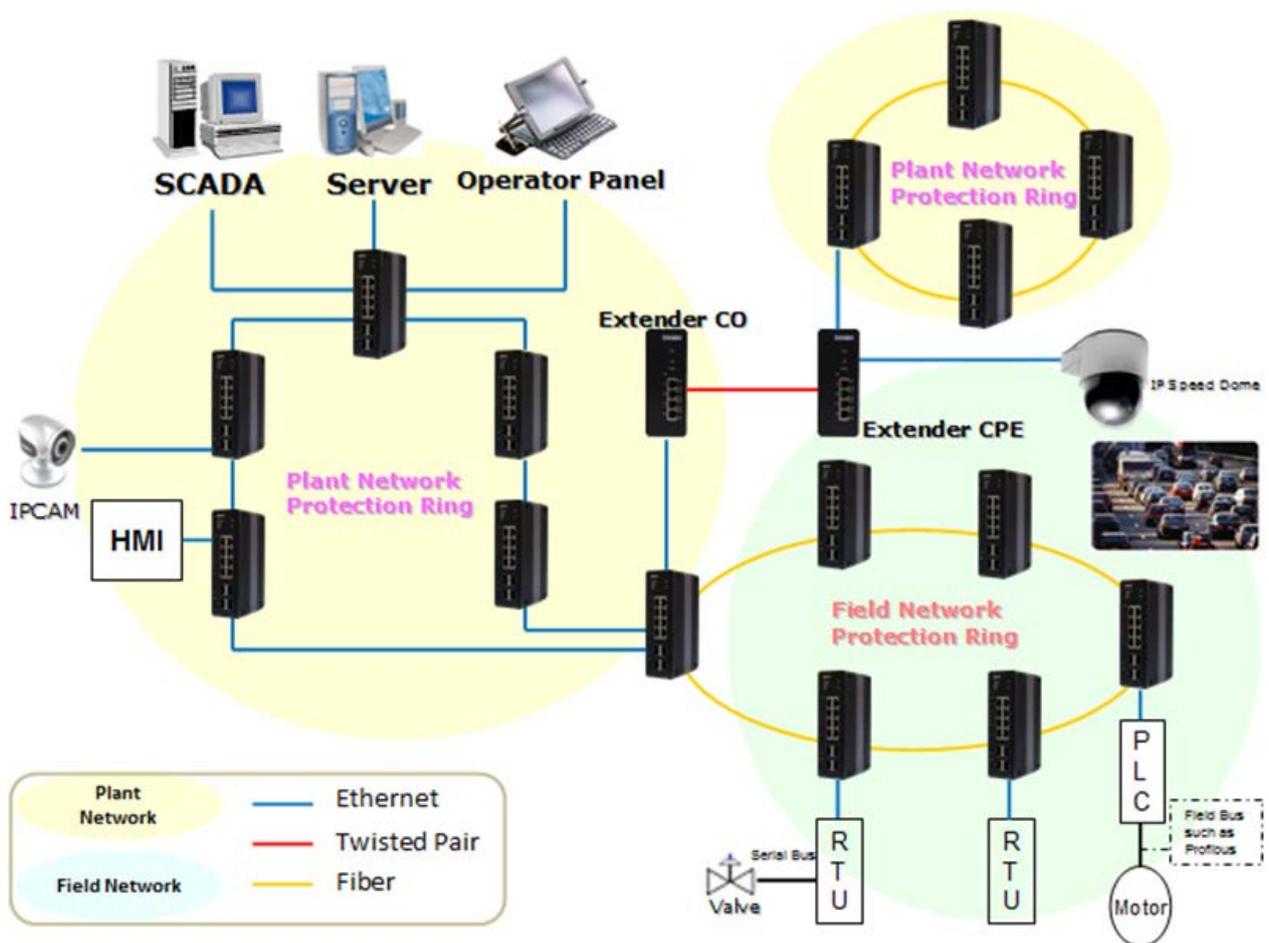
ToS (10000) bedeutet 8

DSCP (000001) bedeutet 1

DSCP (100000) bedeutet 32

Ring Protection Anwendungshilfe

Für Ethernetanwendungen ist es sehr wichtig, über ein zuverlässiges Netzwerk zu verfügen, insbesondere innerhalb der Industrie. INDRY II liefert einen zweiten Ausfallschutz; diese Funktion bietet ein reibungslos funktionierendes Betriebsnetz, auch wenn es Verbindungsprobleme gibt. Dies kann mit Ethernet- und Glasfaserkabel angewandt werden.



Konfiguration (Konsole)

Um das Ring-Protection-System im seriellen Schalter in INDRY II zu konfigurieren,

1. Loggen Sie sich in der Konsole über „**admin**“ ein
2. Gehen Sie über „**Terminal konfigurieren**“ in den Konfigurationsmodus
3. Gehen Sie mithilfe des Befehls „**Ring protect**“ zur Konfiguration der Ring Protection
4. Gehen Sie mithilfe des Befehls „**Gruppe1**“ zur Konfiguration des Ring Protection-Systems der Gruppe 1
5. Vor der Konfiguration muss der Ring Protection-Status mithilfe des Befehls „**Modus deaktivieren**“ deaktiviert werden.
6. Stellen Sie alle benötigten Parameter ein:
 - Knotenpunkt 1 und Knotenpunkt 2, wählen Sie die Ports, die Sie mit einem anderem Schalter verbinden
 - Zum Beispiel, wählen Sie PORT-1 und PORT-2, was bedeutet, dass PORT-1 einer der Ports ist, die an einen anderen Schalter angeschlossen sind, ebenso wie PORT-2.
 - Dann wählen Sie eine der Ringschaltungseinrichtungen als „Master“, wobei Sie den „Knotenpunkt 2-Port als Sperrport akzeptieren können“.

id 1

Knotenpunkt 1 Schnittstelle GigabitEthernet 1/1

Knotenpunkt 2 Schnittstelle GigabitEthernet 1/2

Masterfunktion Knotenpunkt 1 Schnittstelle GigabitEthernet 1/1

Knotenpunkt 2 Schnittstelle GigabitEthernet 1/2

- Um die Konfiguration abzuschließen, muss der Ring Protection-Status mittels des Befehls „**Modus aktivieren**“ aktiviert werden.

Hinweis: Bitte achten Sie nach jeder Aktion auf den Status der „Letzten Befehlsausführung“.

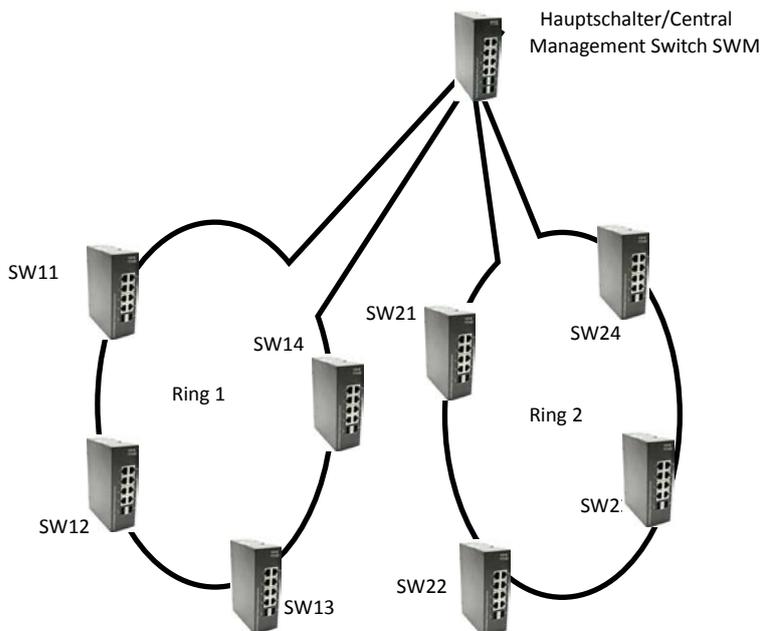
```
configure terminal
Ring Protection ausgeführt
```

```
group1
Modus deaktiviert
id 1
Knotenpunkt 1 Schnittstelle GigabitEthernet 1/1
Knotenpunkt 2 Schnittstelle GigabitEthernet 1/2
Masterfunktion zugeteilt
Modus aktiviert
```

```
exit
```

Konfiguration (Web UI)

Multi Single Ring



Step 1: RSTP am Hauptschalter einstellen
Entsprechend der oben genannten Feldtopologie muss der Administrator den STP-Modus am Hauptschalter „SWM“ konfigurieren.

- ▼ Configuration
 - ▶ System
 - ▶ Green Ethernet
 - Ports
 - ▶ DHCP
 - ▶ Security
 - ▶ Aggregation
 - Loop Protection
 - ▼ Spanning Tree (1)
 - Bridge Settings (2)
 - MSTI Mapping
 - MSTI Priorities
 - CIST Ports
 - MSTI Ports
 - ▶ IPMC Profile
 - MVR
 - ▶ IPMC
 - ▶ LLDP
 - MAC Table
 - VLANs
 - ▶ Private VLANs
 - ▶ VCL
 - ▶ Voice VLAN
 - ▶ QoS
 - Mirroring
 - ▶ GVRP
 - sFlow
 - Ring
- ▶ Monitor
- ▶ Diagnostics
- ▶ Maintenance

STP Bridge Configuration

Basic Settings

Protocol Version	RSTP (2)
Bridge Priority	32768
Forward Delay	15
Max Age	20
Maximum Hop Count	20
Transmit Hold Count	6

Advanced Settings

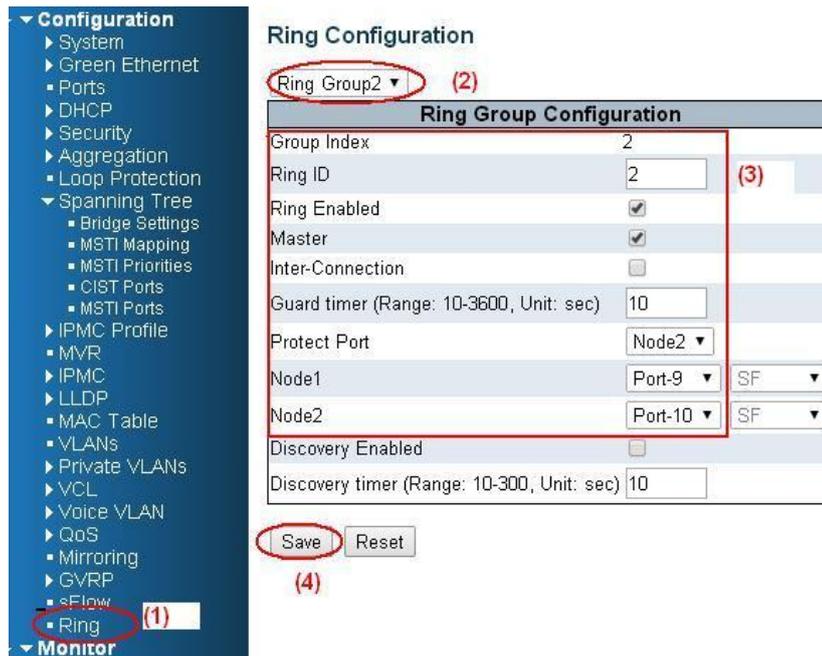
Edge Port BPDU Filtering	<input type="checkbox"/>
Edge Port BPDU Guard	<input type="checkbox"/>
Port Error Recovery	<input type="checkbox"/>
Port Error Recovery Timeout	<input style="width: 100%;" type="text"/>

1. Gehen Sie zu „Konfiguration→Spanning Tree→ Bridge Setting“ Website.
2. Selektieren Sie „RSTP“ als „Protokollversion“
3. Klicken Sie auf „Speichern“.

1. Gehen Sie zu „Konfiguration→Spanning Tree→ CIST-Ports“ Website
2. Aktivieren Sie nicht Port 7, 8, prüfen Sie das Feld für Ring 1
3. Aktivieren Sie nicht Port 9, 10, prüfen Sie das Feld für Ring 2
4. Prüfen Sie „Auto Edge“ an Port 11, 12.
5. Klicken Sie auf „Speichern“.

Step 2: Stellen Sie am Hauptschalter das Ring Protection-System ein

1. Gehen Sie zu „Konfiguration→Ring“ Website
2. Wählen Sie „Ring Gruppe 1“ aus
3. Ring ID→1
Prüfen Sie „Ring aktivieren“ und „Master“.
Knotenpunkt 1 ist „Port-7“, und Knotenpunkt 2 ist „Port-8“
4. Klicken Sie auf „Speichern“.



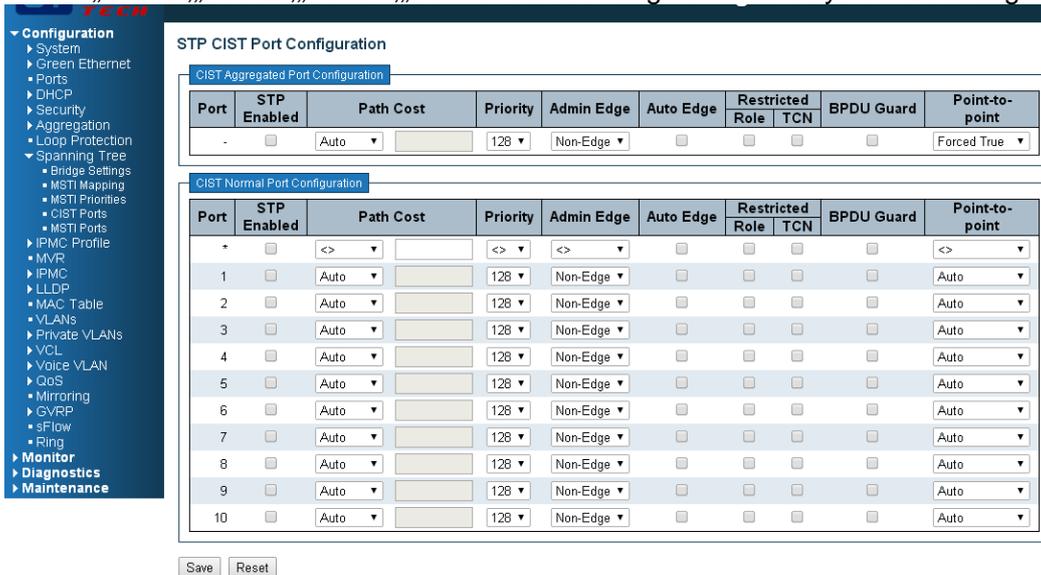
1. Gehen Sie zu „Konfiguration→Ring“ Website
2. Wählen Sie „Ring Gruppe 2“ aus
3. Ring ID→2
Prüfen Sie „Ring aktivieren“ und „Master“.
Knotenpunkt 1 ist „Port-9“, und Knotenpunkt 2 ist „Port-10“
4. Klicken Sie auf „Speichern“.

Danach befolgen Sie die unten stehende Abbildung, um die aktuelle Konfiguration zu speichern.

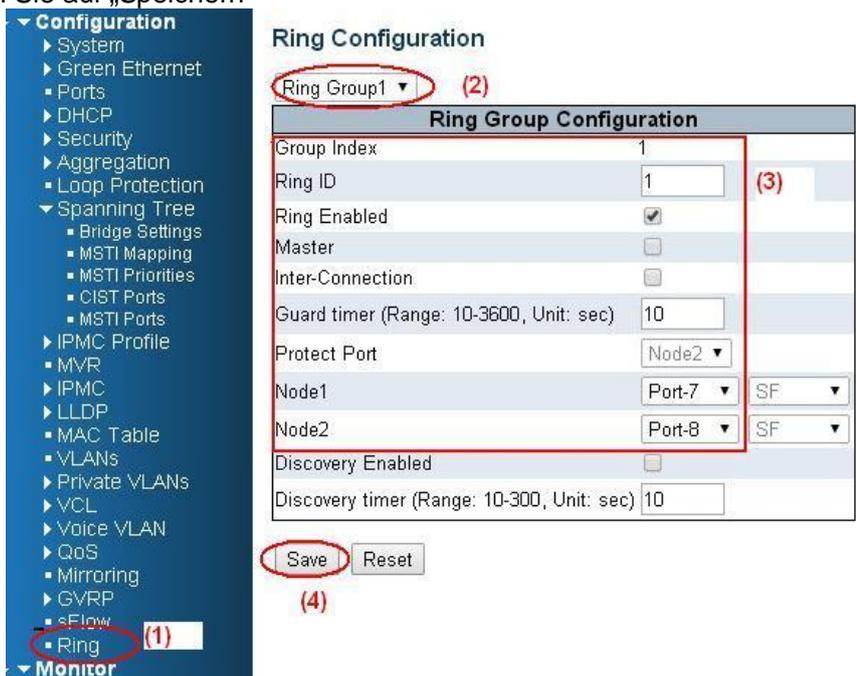


=====

Step 3: An Gerät „SW11“, „SW12“, „SW13“, „SW14“ um das Ring Protection-System zu konfigurieren



1. Gehen Sie zu „Konfiguration→Spanning Tree→ CIST-Ports“ Website
2. Aktivieren Sie auf keinen Fall STP. Prüfen Sie das Feld der Ring-Konfiguration
3. Klicken Sie auf „Speichern“



1. Gehen Sie zu „Konfiguration→Ring“ Website
2. Wählen Sie „Ring Gruppe 1“ aus
3. Ring ID→1
Prüfen Sie „Ring aktivieren“.
Knotenpunkt 1 ist „Port-7“, und Knotenpunkt 2 ist „Port-8“
4. Klicken Sie auf „Speichern“.

Danach speichern Sie die Betriebskonfiguration.

Step 4: An Gerät „SW21“ „SW22“ „SW23“ „SW24“ um das Ring Protection-System zu konfigurieren

Port	STP Enabled	Path Cost	Priority	Admin Edge	Auto Edge	Restricted Role	TCN	BPDU Guard	Point-to-point
-	<input type="checkbox"/>	Auto	128	Non-Edge	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Forced True
*	<input type="checkbox"/>	<>	<>	<>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<>
1	<input type="checkbox"/>	Auto	128	Non-Edge	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
2	<input type="checkbox"/>	Auto	128	Non-Edge	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
3	<input type="checkbox"/>	Auto	128	Non-Edge	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
4	<input type="checkbox"/>	Auto	128	Non-Edge	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
5	<input type="checkbox"/>	Auto	128	Non-Edge	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
6	<input type="checkbox"/>	Auto	128	Non-Edge	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
7	<input type="checkbox"/>	Auto	128	Non-Edge	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
8	<input type="checkbox"/>	Auto	128	Non-Edge	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
9	<input type="checkbox"/>	Auto	128	Non-Edge	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
10	<input type="checkbox"/>	Auto	128	Non-Edge	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto

1. Gehen Sie zu „Konfiguration→Spanning Tree→ CIST-Ports“ Website
2. Aktivieren Sie auf keinen Fall STP. Prüfen Sie das Feld der Ring-Konfiguration
3. Klicken Sie auf „Speichern“

Ring Group Configuration	
Group Index	2
Ring ID	2
Ring Enabled	<input checked="" type="checkbox"/>
Master	<input type="checkbox"/>
Inter-Connection	<input type="checkbox"/>
Guard timer (Range: 10-3600, Unit: sec)	10
Protect Port	Node2
Node1	Port-9 SF
Node2	Port-10 SF
Discovery Enabled	<input type="checkbox"/>
Discovery timer (Range: 10-300, Unit: sec)	10

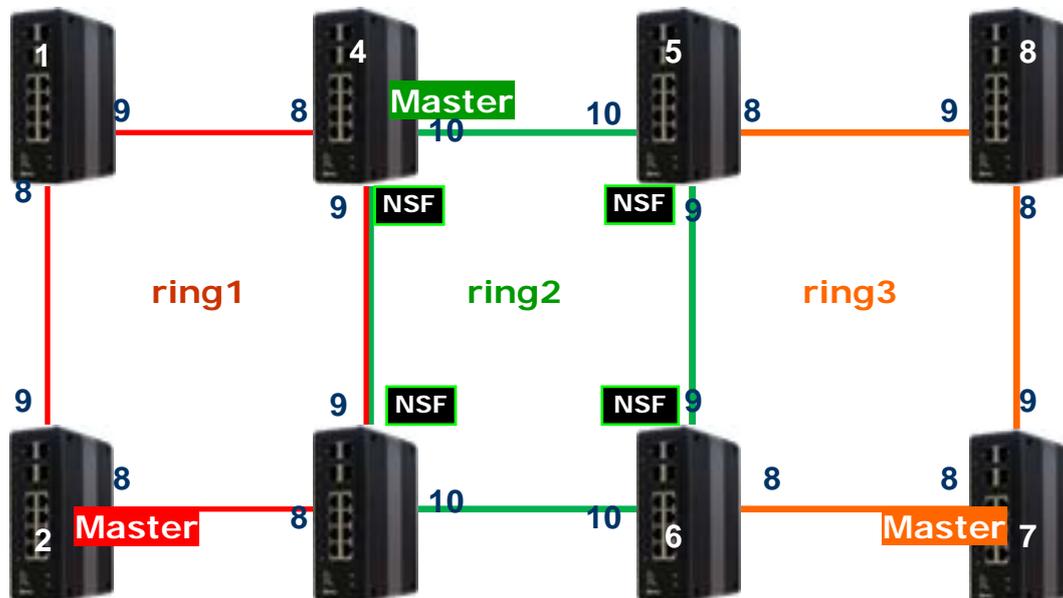
1. Gehen Sie zu „Konfiguration→Ring“ Website
2. Wählen Sie „Ring Gruppe 2“ aus
3. Ring ID→2
Prüfen Sie „Ring aktivieren“.
Knotenpunkt 1 ist „Port-9“, und Knotenpunkt 2 ist „Port-10“
4. Klicken Sie auf „Speichern“.

Danach speichern Sie die Betriebskonfiguration.

=====

Dual Ring

Funktion: Zwischenverbindungs-Ports können zu zwei Nachbargruppen gehören
 Vorteil: Das Gerät der mittleren Ringgruppe konnte auf einen Port für die Ringfunktion reduziert werden.



Schritte konfigurieren:

1. RSTP an allen Ringports deaktivieren
2. Selektieren Sie in jeder Ringgruppe einen Masterport
3. Konfigurieren Sie das Ring Protection-System für die Ring 2-Gruppe
4. Gehen Sie zum anderen Ringgruppen-Gerät, um das Ring Protection-System zu konfigurieren

Anm

Regeln:

- Kein Gerät mit Masterport kann an ein anderes Gerät mit Masterport angeschlossen werden
- Die NSF-Ports gehören zur mittleren Ringgruppe
- Die Ringgruppen können im dualen Ringszenario bis 3 gehen.
- Jedes Gerät, das zu zwei Ringgruppen gehört, ist eine Zwischenverbindung.

Konfigurieren Sie das Ring Protection-System der mittleren Ringgruppe (Ring 2)

An Gerät 4 (Ring 2 Master)

1. Gehen Sie zu „Konfiguration◇Ring“ Website
2. Wählen Sie „Ring Gruppe 2“ aus
3. Ring ID◇2
 Prüfen Sie „Ring aktivieren“, „Zwischenverbindung“ und „Master“.
 Sicherung von Port und NSF ist an „Knotenpunkt 1 (Port 9)“,
 Knotenpunkt 1 ist „Port-9“, and Knotenpunkt 2 ist „Port-10“
4. Klicken Sie auf „Speichern“.

▼ **Configuration**

- ▶ System
- ▶ Green Ethernet
- Ports
- ▶ DHCP
- ▶ Security
- ▶ Aggregation
- Loop Protection
- ▶ Spanning Tree
- ▶ IPMC Profile
- MVR
- ▶ IPMC
- ▶ LLDP
- MAC Table
- VLANs
- ▶ Private VLANs
- ▶ VCL
- ▶ Voice VLAN
- ▶ QoS
- Mirroring
- ▶ GVRP
- sFlow
- **Ring**

▼ **Monitor**

Ring Configuration

Ring Group2 ▼

Ring Group Configuration	
Group Index	2
Ring ID	2
Ring Enabled	<input checked="" type="checkbox"/>
Master	<input checked="" type="checkbox"/>
Inter-Connection	<input checked="" type="checkbox"/>
Guard timer (Range: 10-3600, Unit: sec)	10
Protect Port	Node1 ▼
Node1	Port-9 ▼ Non-SF ▼
Node2	Port-10 ▼ SF ▼
Discovery Enabled	<input type="checkbox"/>
Discovery timer (Range: 10-300, Unit: sec)	10

An Gerät 3, 5 und 6 (Ring 2 slave)

1. Wählen Sie „Ring Gruppe 2“ aus
2. Ring ID=2
Prüfen Sie „Ring aktivieren“ und „Zwischenverbindung“
NSF ist an „Knotenpunkt 1 (Port 9)“,
Node 1 be „Port-9“, and node 2 be „Port-10“
3. Klicken Sie auf „Speichern“.

▼ **Configuration**

- ▶ System
- ▶ Green Ethernet
- Ports
- ▶ DHCP
- ▶ Security
- ▶ Aggregation
- Loop Protection
- ▶ Spanning Tree
- ▶ IPMC Profile
- MVR
- ▶ IPMC
- ▶ LLDP
- MAC Table
- VLANs
- ▶ Private VLANs
- ▶ VCL
- ▶ Voice VLAN
- ▶ QoS
- Mirroring
- ▶ GVRP
- sFlow
- **Ring**

▼ **Monitor**

Ring Configuration

Ring Group2 ▼

Ring Group Configuration	
Group Index	2
Ring ID	2
Ring Enabled	<input checked="" type="checkbox"/>
Master	<input type="checkbox"/>
Inter-Connection	<input checked="" type="checkbox"/>
Guard timer (Range: 10-3600, Unit: sec)	10
Protect Port	Node2 ▼
Node1	Port-9 ▼ Non-SF ▼
Node2	Port-10 ▼ SF ▼
Discovery Enabled	<input type="checkbox"/>
Discovery timer (Range: 10-300, Unit: sec)	10

Konfigurieren Sie das Ring Protection-System an der seitlichen Ringgruppe (Ring 1 und 3)

An Gerät 2 und 7 (Master)

1. Selektieren Sie „Ringgruppe 1 (oder 3)“
2. Ring ID→1 (oder 3)
Prüfen Sie „Ring aktivieren“ und „Master“.
Portsicherung ist an „Knotenpunkt 1 (Port 9)“
Knotenpunkt 1 ist „Port-9“ und Knotenpunkt 2 ist „Port-10“
3. Klicken Sie auf „Speichern“.

An Gerät 1 und 8 (slave)

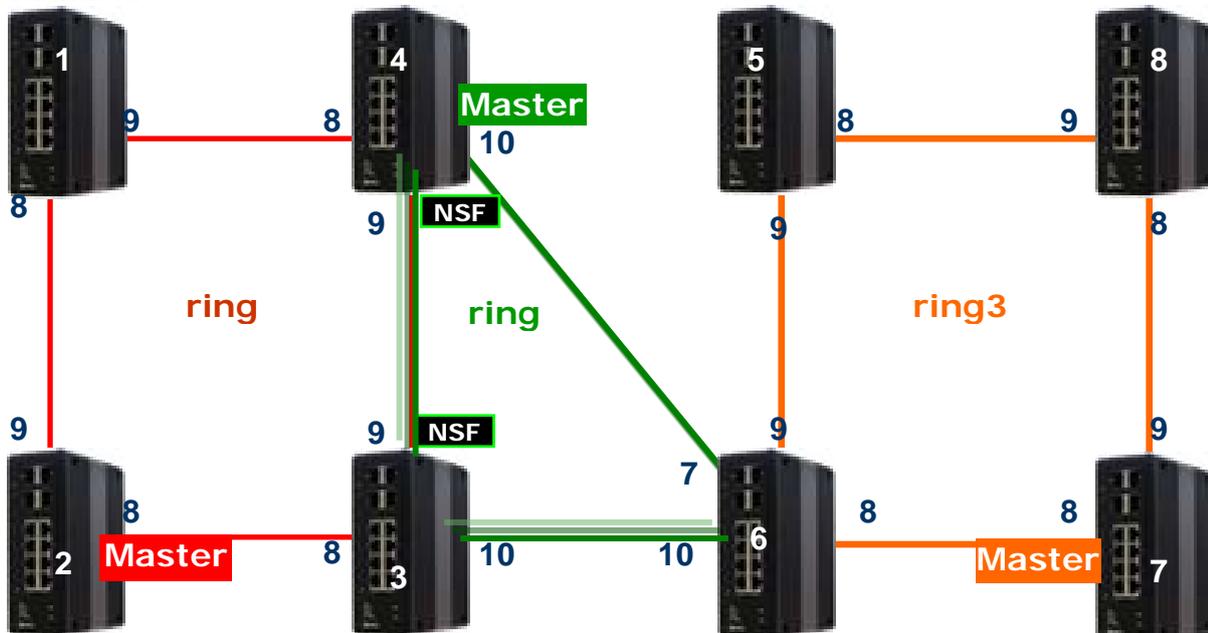
1. Selektieren Sie „Ringgruppe 1 (oder 3)“
2. Ring ID→1 (oder 3)
Prüfen Sie „Ring aktivieren“
Knotenpunkt 1 ist „Port-9“, und Knotenpunkt 2 ist „Port-8“
3. Klicken Sie auf „Speichern“.

An Gerät 3~6 (slave)+Zwischenverbindung

1. Selektieren Sie „Ringgruppe 1 (oder 3)“
2. Ring ID→1 (oder 3)
3. Prüfen Sie „Ring aktivieren“ und „Zwischenverbindung“
Knotenpunkt 1 ist „Port-9“ und Knotenpunkt 2 ist „Port-8“
4. Klicken Sie auf „Speichern“.

Dual Homing

Funktion: Dual Homing-Geräte (Switch 6) müssen zwei Ringgruppen aktivieren.
Vorteil: Die Erholungszeit ist kürzer als beim „Dual Ring“ und könnte zwei Dual-Ringe verbinden.



Schritte konfigurieren:

1. RSTP an allen Ringports deaktivieren
2. Selektieren Sie in jeder Ringgruppe einen Masterport
3. Konfigurieren Sie das Ring Protection-System für die Ring 2-Gruppe
4. Gehen Sie zum anderen Ringgruppen-Gerät, um das Ring Protection-System zu konfigurieren

Im Vergleich zum „Dual Ring“, müssen nur gerät 5 und 6 modifiziert werden

An Gerät 5 (slave)

1. Wählen Sie „Ring Gruppe 3“ aus
2. Ring ID◇ 3
Prüfen Sie „Ring aktivieren“
Knotenpunkt 1 ist „Port-9“, und Knotenpunkt 2 ist „Port-8“
3. Klicken Sie auf „Speichern“.

An Gerät 6 (slave)

1. Wählen Sie „Ring Gruppe 3“ aus
2. Ring ID◇ 3
Prüfen Sie „Ring aktivieren“
3. Knotenpunkt 1 ist „Port-9“, und Knotenpunkt 2 ist „Port-8“
4. Wählen Sie „Ring Gruppe 2“ aus
5. Ring ID◇ 2
Prüfen Sie „Ring aktivieren“
Knotenpunkt 1 ist „Port-7“, und Knotenpunkt 2 ist „Port-10“
6. Klicken Sie auf „Speichern“.

Leitfaden zum QoS

Quality of Service (QoS)-Funktionen ermöglichen Ihnen, Netzwerkressourcen erfolgskritischen Anwendungen erweiterte Anwendungen zuzuordnen, die weniger anfällig für Faktoren wie Zeitverzögerung oder Netzüberlastung sind. Sie können Ihr Netzwerk konfigurieren, um spezielle Übertragungstypen zu priorisieren, um zu gewährleisten, dass jeder Typ das angemessene Quality of Service (QoS)-Niveau erreicht.

SP/SPWRR/WRR

INDRY II kann so konfiguriert werden, dass es über 8 Class of Service (CoS)-Ausgangswarteschleifen (Q0–Q7) pro Port verfügt, in die jedes Paket platziert wird. Q0 ist die Warteschleife mit größter Dringlichkeit. Die 802.1p-Dringlichkeit jedes Pakets bestimmt seine CoS-Warteschleife. Der Benutzer muss ein VLAN Prioritäts-/Queue Mapping-Profil für jeden Port erstellen, für jede VLAN-Priorität muss ein Traffic Descriptor zugewiesen werden. Der Traffic Descriptor definiert die Grenzparameter jeder VLAN-Priorität für die Ethernet-Schnittstelle. Aktuell unterstützt INDRY II Strict Priority (SP)/SPWRR (SP+WRR)/WRR (Weighted Round Robin)-Methoden an jedem Port. In Bezug auf weitere Referenzen siehe das Bedienungshandbuch von INDRY II.

Standardmäßig eingestelltes Prioritäts- und Queue Mapping wie folgt:

Priority0	Priority1	Priority2	Priority3	Priority4	Priority5	Priority6	Priority7
Queue0	Queue1	Queue2	Queue3	Queue4	Queue5	Queue6	Queue7
WRR	WRR	WRR	WRR	SPQ	SPQ	SPQ	SPQ

Anwendungsbeispiele

Nachfolgend geben wir einige Beispiele für verschiedene QoS-Kombinationen, die das webbasierte Verwaltungssystem, CLI (Command Line Interface) oder SNMP nutzen.

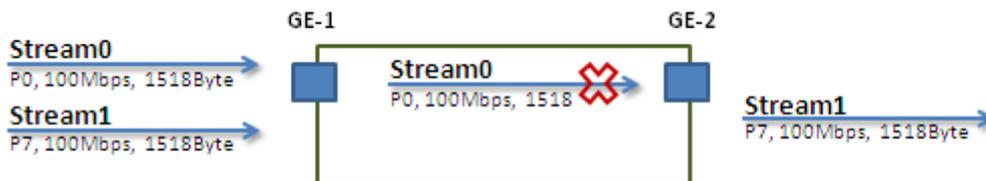
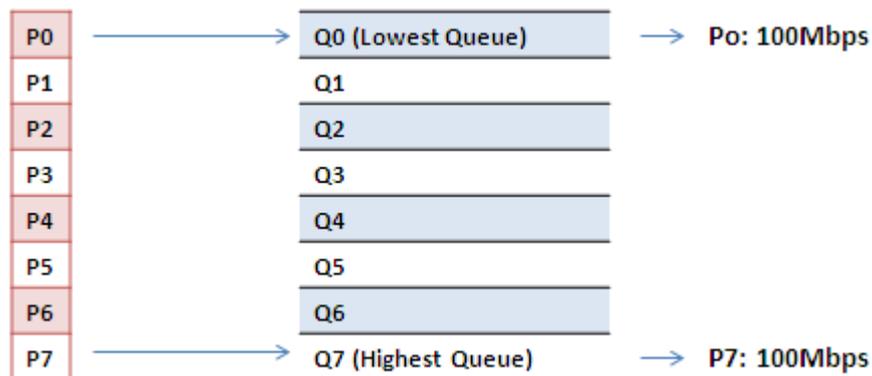
Beispiel 1: SPQ ohne Grenzwerte (Standardprofil)

Wir senden 2 Streams (Stream0, Stream1) von PORT-1 zu PORT-2. Beide Streams haben jeweils 100 Mbps. Stream0 umfasst VLAN-Priorität 0, Stream1 umfasst VLAN Priorität 7. Stellen Sie die PORT-2-Verbindungsgeschwindigkeit auf 100 Mbps ein.

Erwartetes Ergebnis:

Wir erwarten, dass PORT-2 nur 100 Mbps von Stream1 erhalten kann und Stream0 gelöscht wird. Dieser Fall hilft Anwendern, zu verstehen, wie SPQ beim INDRY II funktioniert.

Gigabit-Port VLAN Priorität und Queue Mapping:



- **Stream0 :**
 Dst Mac : 00:00:00:00:20:01
 Src Mac : 00:00:00:00:10:01
 Vlan : 100
 Vlan prio : 0
 Gesendete Rate : 100Mbps
 Paketlänge: 1518bytes
- **Stream1:**
 Dst Mac : 00:00:00:00:20:02
 Src Mac : 00:00:00:00:10:02
 Vlan : 100
 Vlan prio : 7
 Gesendete Rate : 100Mbps
 Paketlänge: 1518bytes

Webmanagement:

Step 1. Gehen Sie zu Konfiguration -> Ports -> Stellen Sie die Port 2-Verbindungsgeschwindigkeit auf 100 Mbps Vollduplex.

Port	Link	Speed		Flow Control			Maximum Frame Size	Excessive Collision Mode
		Current	Configured	Current Rx	Current Tx	Configured		
*						<input type="checkbox"/>	9600	
1	Down		Auto	X	X	<input type="checkbox"/>	9600	Discard
2	100fdx		100Mbps FDX	X	X	<input type="checkbox"/>	9600	Discard
3	Down		Auto	X	X	<input type="checkbox"/>	9600	Discard
4	Down		Auto	X	X	<input type="checkbox"/>	9600	Discard
5	Down		Auto	X	X	<input type="checkbox"/>	9600	Discard
6	100fdx		Auto	X	X	<input type="checkbox"/>	9600	Discard
7	Down		Auto	X	X	<input type="checkbox"/>	9600	Discard
8	Down		Auto	X	X	<input type="checkbox"/>	9600	Discard
9	Down		Auto	X	X	<input type="checkbox"/>	9600	Discard
10	Down		Auto	X	X	<input type="checkbox"/>	9600	Discard
11	Down		Auto	X	X	<input type="checkbox"/>	9600	Discard
12	Down		Auto	X	X	<input type="checkbox"/>	9600	Discard
13	Down		Auto	X	X	<input type="checkbox"/>	9600	Discard
14	Down		Auto	X	X	<input type="checkbox"/>	9600	Discard

Step 2. Selektieren Sie Konfiguration -> VLANs -> Erstellen Sie ein VLAN mit VLAN ID 100. Geben Sie in das Feld **Name** eine Bezeichnung für das VLAN ein. Hier stellen wir ein getaggttes VLAN100 für PORT-1 und PORT-2 ein.

Global VLAN Configuration

Allowed Access VLANs: 1,100
 Ethertype for Custom S-ports: 88A8

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*		1		<input type="checkbox"/>				
1	Trunk	100	C-Port	<input checked="" type="checkbox"/>	Tagged Only	Tag All	1,100	
2	Trunk	100	C-Port	<input checked="" type="checkbox"/>	Tagged Only	Tag All	1,100	
3	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
4	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
5	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
6	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
7	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
8	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
9	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
10	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
11	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
12	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
13	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
14	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	

CLI-Konfigurationsbefehl:

```
Schnittstelle GigabitEthernet 1/2
Geschwindigkeit 100
Vollduplex
exit
vlan 100
```

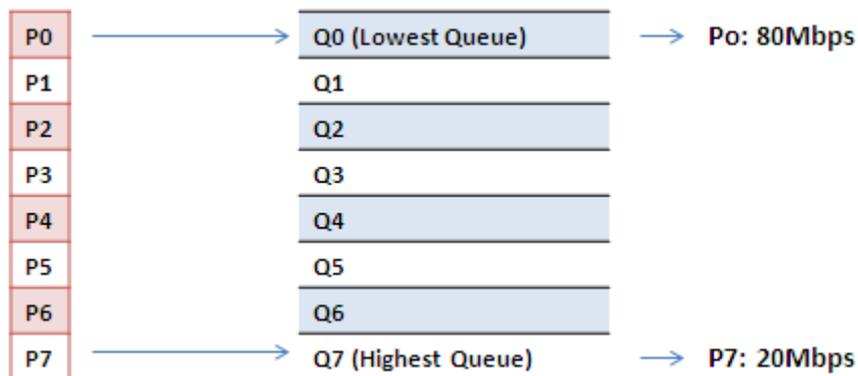
Beispiel 2: SPQ mit Grenzwerten

Wir senden 2 Streams (Stream0, Stream1) von Port 1 zu Port 2. Beide Streams haben jeweils 100 Mbps. Stream0 umfasst VLAN-Priorität 0, Stream1 umfasst VLAN Priorität 7. Stream3 und Stream4 nur zur Überprüfung, dass keine Datenübertragung vorliegt.

Erwartetes Ergebnis:

Wir erwarten, dass PORT-2 nur 20 Mbps von Stream1 und 80 Mbps von Stream0 erhalten kann. Dieser Fall hilft Anwendern, zu verstehen, wie SPQ beim INDRY II funktioniert.

VDSL-Port VLAN Priorität und Queue Mapping:



- **Stream0 :**
 Dst Mac : 00:00:00:00:20:01
 Src Mac : 00:00:00:00:10:01
 Vlan : 100
 Vlan prio : 0
 Gesendete Rate : 100Mbps
 Paketlänge: 1518bytes
- **Stream1:**
 Dst Mac : 00:00:00:00:20:02
 Src Mac : 00:00:00:00:10:02
 Vlan : 100
 Vlan prio : 7
 Gesendete Rate : 100Mbps
 Paketlänge: 1518bytes

● **Stream3 : (Zur Überprüfung)**

Dst Mac : 00:00:00:00:10:01
 Src Mac : 00:00:00:00:20:01
 Vlan : 100
 Vlan prio : 0
 Gesendete Rate : 10Mbps
 Paketlänge: 1518bytes

● **Stream4 : (Zur Überprüfung)**

Dst Mac : 00:00:00:00:10:02
 Src Mac : 00:00:00:00:20:02
 Vlan : 100
 Vlan prio : 0
 Gesendete Rate : 10Mbps
 Paketlänge: 1518bytes

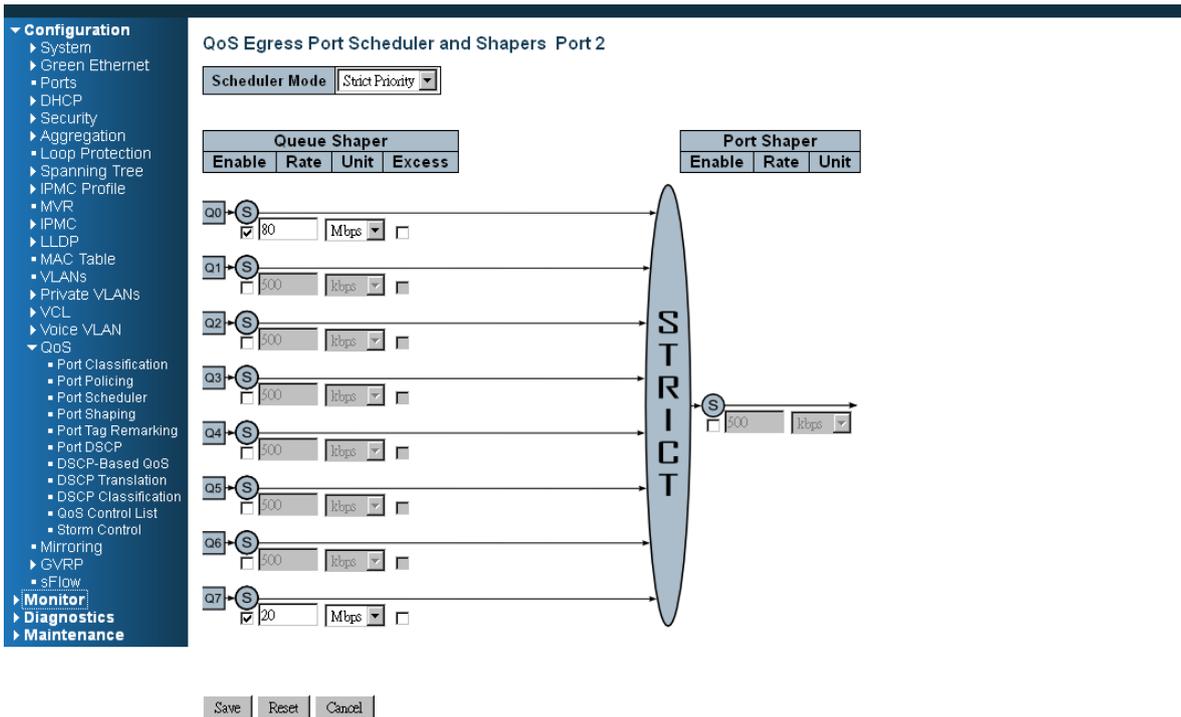
Webmanagement:

Step 1. Gehen Sie zu Konfiguration -> Qos-> Port Grenzwerte, um ein Qos-Profil für Port-2 zu erstellen.

- ▼ Configuration
 - ▶ System
 - ▶ Green Ethernet
 - ▶ Ports
 - ▶ DHCP
 - ▶ Security
 - ▶ Aggregation
 - ▶ Loop Protection
 - ▶ Spanning Tree
 - ▶ IPMC Profile
 - ▶ MVR
 - ▶ IPMC
 - ▶ LLDP
 - ▶ MAC Table
 - ▶ VLANs
 - ▶ Private VLANs
 - ▶ VCL
 - ▶ Voice VLAN
 - ▼ QoS
 - Port Classification
 - Port Policing
 - Port Scheduler
 - Port Shaping
 - Port Tag Remarking
 - Port DSCP
 - DSCP-Based QoS
 - DSCP Translation
 - DSCP Classification
 - QoS Control List
 - Storm Control
 - ▶ Mirroring
 - ▶ GVRP
 - sFlow
- ▶ Monitor
- ▶ Diagnostics

QoS Egress Port Shapers

Port	Shapers								Port	
	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7		
1	disabled									
2	80 Mbps	disabled	disabled	disabled	disabled	disabled	disabled	20 Mbps	disabled	disabled
3	disabled									
4	disabled									
5	disabled									
6	disabled									
7	disabled									
8	disabled									
9	disabled									
10	disabled									
11	disabled									
12	disabled									
13	disabled									
14	disabled									



Step 2. Selektieren Sie „Strikte Priorität“ und stellen Sie den Grenzwertbereich für Warteschleife 0 und Warteschleife 7 wie folgt ein.

CLI-Konfigurationsbefehl:

```
VLAN 100 v100
Schnittstellen-Gigabit 1
VLAN 100 getaggt
exit
Schnittstellen-Gigabit 2
qos Grenzwert 100000
qos Warteschleifen-Grenzwert 0 80000
qos Warteschleifen-Grenzwert 7 20000
exit
```

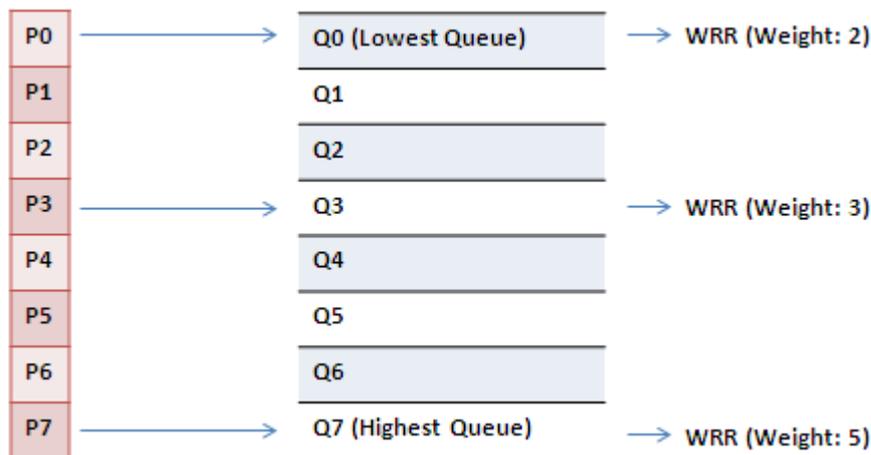
Beispiel 3: WRR

Wir senden 3 Streams (Stream0, Stream1 und Stream2) von PORT-1 zu PORT-2. Diese Streams umfassen jeweils 100 Mbps. Stream0 hat VLAN-Priorität 0, Stream1 hat VLAN-Priorität 3, Stream2 hat VLAN-Priorität 7. Stream3, Stream4 und Stream5 dienen nur zur Überprüfung, dass keine Datenübertragung vorliegt. WRR unterstützt die Gewichtzuweisung, der Gewichtsbereich geht von 1 bis 255. Darüber hinaus wendet INDRY II WRR und Gewicht 1 für alle Gigabit-Ethernet-Ports an. Im folgenden Fall, weisen wir Gewicht 2 Priorität 0, Gewicht 3 Priorität 3 und Gewicht 5 Priorität 7 zu.

Erwartetes Ergebnis:

Wir erwarten, dass PORT-2 ca. 20 Mbps von Stream0, 30 Mbps von Stream1 und 50 Mbps von Stream2 erhält. Dieser Fall hilft den Anwendern, zu verstehen, wie WRR beim INDRY II funktioniert.

Gigabit-Port VLAN Priorität und Queue Mapping:



- **Stream0 :**
Dst Mac : 00:00:00:00:20:01
Src Mac : 00:00:00:00:10:01
Vlan : 100
Vlan prio : 0
Gesendete Rate : 100Mbps
Paketlänge: 1518bytes
- **Stream1:**
Dst Mac : 00:00:00:00:20:04
Src Mac : 00:00:00:00:10:04
Vlan : 100
Vlan prio : 3
Gesendete Rate : 100Mbps
Paketlänge: 1518bytes
- **Stream2:**
Dst Mac : 00:00:00:00:20:08
Src Mac : 00:00:00:00:10:08
Vlan : 100
Vlan prio : 7
Gesendete Rate : 100Mbps
Paketlänge: 1518bytes
- **Stream3 : (Zur Überprüfung)**
Dst Mac : 00:00:00:00:10:01
Src Mac : 00:00:00:00:20:01
Vlan : 100
Vlan prio : 0
Gesendete Rate : 10Mbps
Paketlänge: 1518bytes
- **Stream4 : (Zur Überprüfung)**
Dst Mac : 00:00:00:00:10:04
Src Mac : 00:00:00:00:20:04
Vlan : 100
Vlan prio : 0
Gesendete Rate : 10Mbps
Paketlänge: 1518bytes
- **Stream5 : (Zur Überprüfung)**
Dst Mac : 00:00:00:00:10:08
Src Mac : 00:00:00:00:20:08
Vlan : 100
Vlan prio : 0
Gesendete Rate : 10Mbps
Paketlänge: 1518bytes

Webmanagement:

- ▼ Configuration
 - ▶ System
 - ▶ Green Ethernet
 - ▶ Ports
 - ▶ DHCP
 - ▶ Security
 - ▶ Aggregation
 - ▶ Loop Protection
 - ▶ Spanning Tree
 - ▶ IPMC Profile
 - ▶ IPMC
 - ▶ LLDP
 - ▶ MAC Table
 - ▶ VLANs
 - ▶ Private VLANs
 - ▶ VCL
 - ▶ Voice VLAN
 - ▶ QoS
 - Port Classification
 - Port Policing
 - Port Scheduler
 - Port Shaping
 - Port Tag Remarking
 - Port DSCP
 - DSCP-Based QoS
 - DSCP Translation
 - DSCP Classification
 - QoS Control List
 - Storm Control
 - Mirroring
 - ▶ GVRP
 - sFlow
- ▶ Monitor
- ▶ Diagnostics
- ▶ Maintenance

QoS Egress Port Shapers

Port	Shapers								
	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Port
1	disabled								
2	disabled	50 Mbps							
3	disabled								
4	disabled								
5	disabled								
6	disabled								
7	disabled								
8	disabled								
9	disabled								
10	disabled								
11	disabled								
12	disabled								
13	disabled								
14	disabled								

Step 1. Gehen Sie zu Konfiguration -> Qos -> Port-Grenzwerte, und klicken Sie auf PORT-2, um ein Qos-Profil zu erstellen.

Step 2. Selektieren Sie „Gewogen“ aus, und stellen Sie den Gewichtswert für Warteschlange 0, Warteschlange 3 und Warteschlange 7 wie folgt ein.

- ▼ Configuration
 - ▶ System
 - ▶ Green Ethernet
 - ▶ Ports
 - ▶ DHCP
 - ▶ Security
 - ▶ Aggregation
 - ▶ Loop Protection
 - ▶ Spanning Tree
 - ▶ IPMC Profile
 - ▶ MVR
 - ▶ IPMC
 - ▶ LLDP
 - ▶ MAC Table
 - ▶ VLANs
 - ▶ Private VLANs
 - ▶ VCL
 - ▶ Voice VLAN
 - ▶ QoS
 - Port Classification
 - Port Policing
 - Port Scheduler
 - Port Shaping
 - Port Tag Remarking
 - Port DSCP
 - DSCP-Based QoS
 - DSCP Translation
 - DSCP Classification
 - QoS Control List
 - Storm Control
 - Mirroring
 - ▶ GVRP
 - sFlow
- ▶ Monitor
- ▶ Diagnostics
- ▶ Maintenance

QoS Egress Port Scheduler and Shapers Port 2

Scheduler Mode: Weighted

	Queue Shaper				Queue Scheduler		Port Shaper		
	Enable	Rate	Unit	Excess	Weight	Percent	Enable	Rate	Unit
Q0	<input type="checkbox"/>	500	kbps	<input checked="" type="checkbox"/>	2	22%	D W R R I C T	S T R I C T	<input checked="" type="checkbox"/> 100 Mbps
Q1	<input type="checkbox"/>	500	kbps	<input checked="" type="checkbox"/>	1	11%			
Q2	<input type="checkbox"/>	500	kbps	<input checked="" type="checkbox"/>	1	11%			
Q3	<input type="checkbox"/>	500	kbps	<input checked="" type="checkbox"/>	3	33%			
Q4	<input type="checkbox"/>	500	kbps	<input checked="" type="checkbox"/>	1	11%			
Q5	<input type="checkbox"/>	500	kbps	<input checked="" type="checkbox"/>	1	11%			
Q6	<input checked="" type="checkbox"/>	50	Mbps	<input checked="" type="checkbox"/>					
Q7	<input checked="" type="checkbox"/>	50	Mbps	<input checked="" type="checkbox"/>					

Save Reset Cancel

CLI-Konfigurationsbefehl:

```
Schnittstelle GigabitEthernet 1/1
Amt-Switchport zugelassen für VLAN 1.100
Hybrid-Switchport erlaubt VLAN 1.100
Amt-Switchport VLAN Tag native
Switchport Amtsmodus
exit
Schnittstelle GigabitEthernet 1/2
Amt-Switchport zugelassen für VLAN 1.100
Amt-Switchport VLAN Tag native
Switchport Amtsmodus
qos Grenzwert 100000
qos queue-Grenzwerte 6 50000 Exzess
qos queue-Grenzwerte 7 50000 Exzess
qos wrr 2 1 1 3 1 1
exit
```

Beispiel 4 SP-WRR

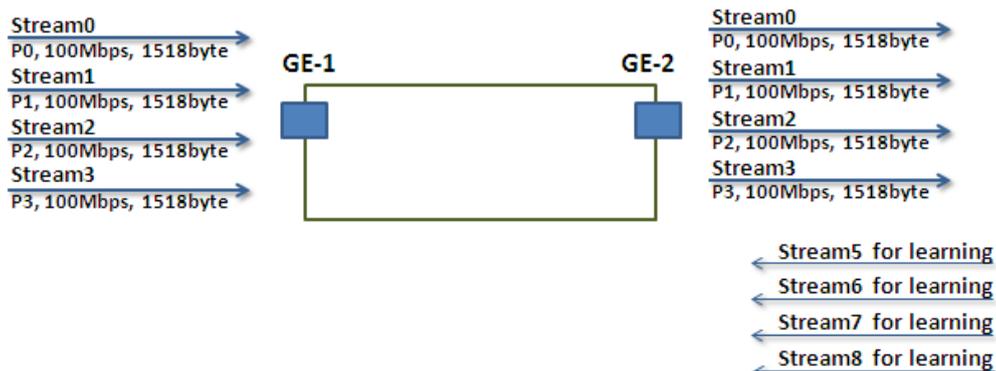
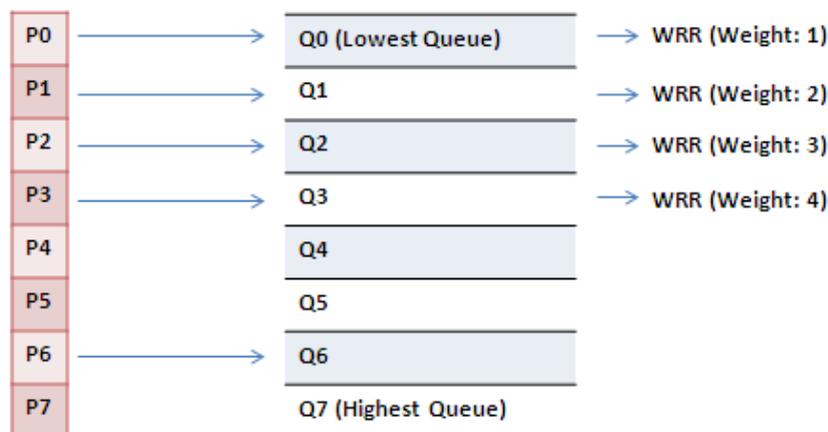
Wir senden 4 Streams (Stream0, Stream1, Stream2 und Stream3) von PORT-1 an PORT-2. Diese Streams umfassen jeweils 100 Mbps. Stream0 hat VLAN Priorität 0, Stream1 hat VLAN Priorität 1, Stream2 hat VLAN Priorität 2, Stream3 hat VLAN Priorität 3 und Stream4 hat VLAN Priorität 6. Stream5, Stream6, Stream7, Stream8 und Stream9 dienen nur zu Überprüfungs Zwecken, ob keine Datenübertragung vorliegt. WRR unterstützt die Gewichtzuweisung, der Gewichtsbereich geht von 1 bis 255. Darüber hinaus wendet INDRY II WRR und Gewicht 1 für alle Gigabit-Ethernet-Ports an. Im folgenden Fall ordnen wir Gewicht 1 Priorität 0, Gewicht 2 Priorität 1, Gewicht 3 Priorität 2 und Gewicht 4 Priorität 3 zu. Im SP-WRR-Modus, Warteschlange 0 bis Warteschlange 3 gehört zu WRR, Warteschlange 4 gehört zu SP.

Erwartetes Ergebnis:

Im Fall 1 erwarten wir, dass PORT-2 ca. 10 Mbps von Stream0, 20 Mbps von Stream1, 30 Mbps oder Stream2 und 40 Mbps von Stream3 empfängt, wenn wir Stream0 bis Stream3 zu PORT-1 senden. Im Fall 2 erwarten wir, dass PORT-2 nur 100 Mbps von Stream6 empfangen kann und Stream0 bis Stream3 in einen anderen Fall einsortiert werden. Dieser Fall hilft den Anwendern, zu verstehen, wie SP-WRR beim INDRY II funktioniert.

Fall 1:

Gigabit-Port VLAN Priorität und Queue Mapping:



- **Stream0 :**
Dst Mac : 00:00:00:00:20:01
Src Mac : 00:00:00:00:10:01
Vlan : 100
Vlan prio : 0
Gesendete Rate : 100Mbps
Paketlänge: 1518bytes

- **Stream1:**
Dst Mac : 00:00:00:00:20:02
Src Mac : 00:00:00:00:10:02
Vlan : 100
Vlan prio : 3
Gesendete Rate : 100Mbps
Paketlänge: 1518bytes

- **Stream2:**
Dst Mac : 00:00:00:00:20:03
Src Mac : 00:00:00:00:10:03
Vlan : 100
Vlan prio : 7
Gesendete Rate : 100Mbps
Paketlänge: 1518bytes

- **Stream3:**
Dst Mac : 00:00:00:00:20:04
Src Mac : 00:00:00:00:10:04
Vlan : 100
Vlan prio : 7
Gesendete Rate : 100Mbps
Paketlänge: 1518bytes

- **Stream5 : (Zur Überprüfung)**
Dst Mac : 00:00:00:00:10:01
Src Mac : 00:00:00:00:20:01
Vlan : 100
Vlan prio : 0
Gesendete Rate : 10Mbps
Paketlänge: 1518bytes

- **Stream6 : (Zur Überprüfung)**
Dst Mac : 00:00:00:00:10:02
Src Mac : 00:00:00:00:20:02
Vlan : 100
Vlan prio : 0
Gesendete Rate : 10Mbps
Paketlänge: 1518bytes

- **Stream7 : (Zur Überprüfung)**
Dst Mac : 00:00:00:00:10:03
Src Mac : 00:00:00:00:20:03
Vlan : 100
Vlan prio : 0
Gesendete Rate : 10Mbps
Paketlänge: 1518bytes

● **Stream8 : (Zur Überprüfung)**

Dst Mac : 00:00:00:00:10:04
 Src Mac : 00:00:00:00:20:04
 Vlan : 100
 Vlan prio : 0
 Gesendete Rate : 10Mbps
 Paketlänge: 1518bytes

Webmanagement:

Step 1. Gehen Sie zu Konfiguration -> Qos -> Port-Grenzwerte, und klicken Sie auf PORT-2, um ein Qos-Profil zu erstellen.

Port	Shapers							Port	
	Q0	Q1	Q2	Q3	Q4	Q5	Q6		Q7
1	disabled								
2	disabled	50 Mbps							
3	disabled								
4	disabled								
5	disabled								
6	disabled								
7	disabled								
8	disabled								
9	disabled								
10	disabled								
11	disabled								
12	disabled								
13	disabled								
14	disabled								

Step 2. Selektieren Sie „Gewogen“ aus, und stellen Sie den Gewichtswert für Warteschlange 0, Warteschlange 0 ~ Warteschlange 3 wie folgt ein.

Queue Shaper				Queue Scheduler		Port Shaper		
Enable	Rate	Unit	Excess	Weight	Percent	Enable	Rate	Unit
<input checked="" type="checkbox"/>	500	kbps	<input type="checkbox"/>	1	8%	<input checked="" type="checkbox"/>	100	Mbps
<input checked="" type="checkbox"/>	500	kbps	<input type="checkbox"/>	2	17%	<input checked="" type="checkbox"/>	100	Mbps
<input checked="" type="checkbox"/>	500	kbps	<input type="checkbox"/>	3	25%	<input checked="" type="checkbox"/>	100	Mbps
<input checked="" type="checkbox"/>	500	kbps	<input type="checkbox"/>	4	33%	<input checked="" type="checkbox"/>	100	Mbps
<input type="checkbox"/>	500	kbps	<input checked="" type="checkbox"/>	1	8%	<input type="checkbox"/>	100	Mbps
<input type="checkbox"/>	500	kbps	<input checked="" type="checkbox"/>	1	8%	<input type="checkbox"/>	100	Mbps
<input type="checkbox"/>	50	Mbps	<input checked="" type="checkbox"/>			<input type="checkbox"/>	100	Mbps
<input type="checkbox"/>	50	Mbps	<input checked="" type="checkbox"/>			<input type="checkbox"/>	100	Mbps

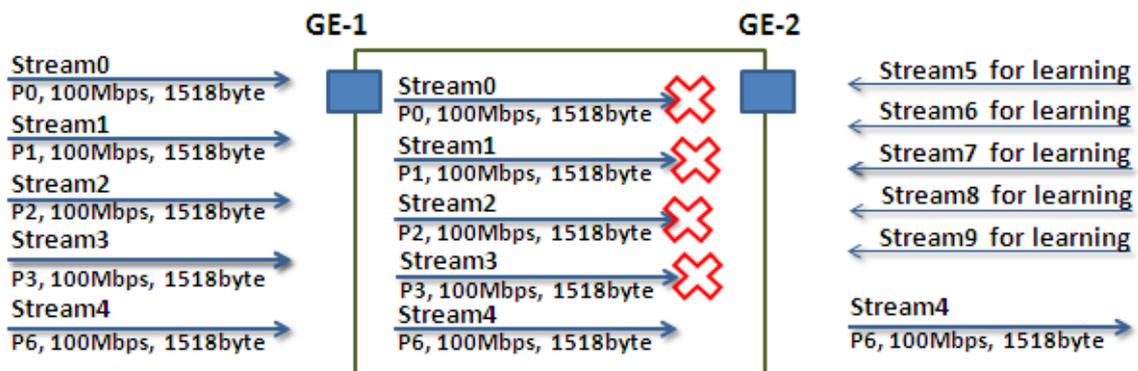
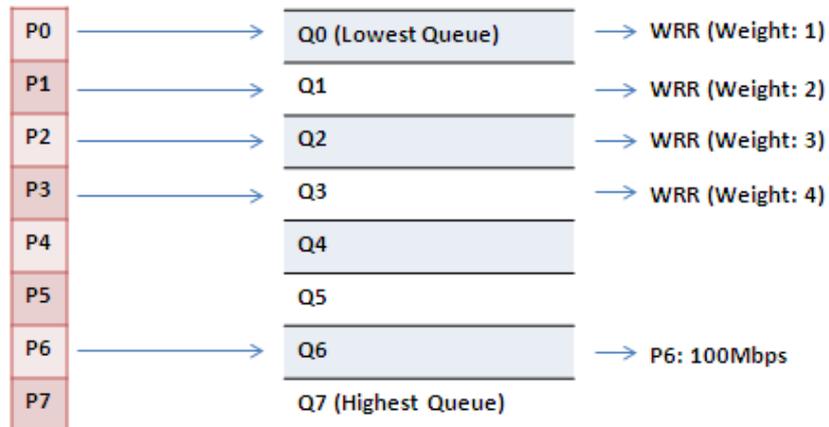
Step 3. Gehen Sie zu Konfiguration-> Queue und Planung-> Verknüpfung, und verknüpfen Sie Profil 2 mit PORT-2.

CLI-Konfigurationsbefehl:

```
Schnittstelle GigabitEthernet 1/2
  Amt-Switchport zugelassen für VLAN 1.100
  Hybrid-Switchport erlaubt VLAN 100,4095
  Amt-Switchport VLAN Tag native
  Switchport Amtsmodus
  qos Grenzwert 100000
  qos Warteschleifen-Grenzwert 0 500
  qos Warteschleifen-Grenzwert 1 500
  qos Warteschleifen-Grenzwert 2 500
  qos Warteschleifen-Grenzwert 3 500
  qos wrr 1 2 3 4 1 1
exit
```

Fall 2:

Gigabit-Port VLAN Priorität und Queue Mapping



- Stream0 :**
 Dst Mac : 00:00:00:00:20:01
 Src Mac : 00:00:00:00:10:01
 Vlan : 100
 Vlan prio : 0
 Gesendete Rate : 100Mbps
 Paketlänge: 1518bytes
- Stream1:**
 Dst Mac : 00:00:00:00:20:02
 Src Mac : 00:00:00:00:10:02
 Vlan : 100
 Vlan prio : 3
 Gesendete Rate : 100Mbps
 Paketlänge: 1518bytes

- **Stream2:**
Dst Mac : 00:00:00:00:20:03
Src Mac : 00:00:00:00:10:03
Vlan : 100
Vlan prio : 7
Gesendete Rate : 100Mbps
Paketlänge: 1518bytes
- **Stream3:**
Dst Mac : 00:00:00:00:20:04
Src Mac : 00:00:00:00:10:04
Vlan : 100
Vlan prio : 7
Gesendete Rate : 100Mbps
Paketlänge: 1518bytes
- **Stream4:**
Dst Mac : 00:00:00:00:20:07
Src Mac : 00:00:00:00:10:07
Vlan : 100
Vlan prio : 7
Gesendete Rate : 100Mbps
Paketlänge: 1518bytes
- **Stream5 : (Zur Überprüfung)**
Dst Mac : 00:00:00:00:10:01
Src Mac : 00:00:00:00:20:01
Vlan : 100
Vlan prio : 0
Gesendete Rate : 10Mbps
Paketlänge: 1518bytes
- **Stream6 : (Zur Überprüfung)**
Dst Mac : 00:00:00:00:10:02
Src Mac : 00:00:00:00:20:02
Vlan : 100
Vlan prio : 0
Gesendete Rate : 10Mbps
Paketlänge: 1518bytes
- **Stream7 : (Zur Überprüfung)**
Dst Mac : 00:00:00:00:10:03
Src Mac : 00:00:00:00:20:03
Vlan : 100
Vlan prio : 0
Gesendete Rate : 10Mbps
Paketlänge: 1518bytes
- **Stream8 : (Zur Überprüfung)**
Dst Mac : 00:00:00:00:10:04
Src Mac : 00:00:00:00:20:04
Vlan : 100
Vlan prio : 0
Gesendete Rate : 10Mbps
Paketlänge: 1518bytes

- **Stream9 : (Zur Überprüfung)**
 Dst Mac : 00:00:00:00:10:07
 Src Mac : 00:00:00:00:20:07
 Vlan : 100
 Vlan prio : 0
 Gesendete Rate : 10Mbps
 Paketlänge: 1518bytes

Webmanagement:

Step 1. Gehen Sie zu Konfiguration -> Qos -> Port-Grenzwerte, und klicken Sie auf PORT-2, um ein Qos-Profil zu erstellen.

Port	Shapers								Port	
	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7		
1	disabled									
2	disabled	50 Mbps								
3	disabled									
4	disabled									
5	disabled									
6	disabled									
7	disabled									
8	disabled									
9	disabled									
10	disabled									
11	disabled									
12	disabled									
13	disabled									
14	disabled									

Step 2. Selektieren Sie „Gewogen“ aus, und stellen Sie den Gewichtswert für Warteschlange 0, Warteschlange 0 ~ Warteschlange 3 wie folgt ein.

Queue Shaper				Queue Scheduler		Port Shaper		
Enable	Rate	Unit	Excess	Weight	Percent	Enable	Rate	Unit
<input checked="" type="checkbox"/>	500	kbps	<input type="checkbox"/>	1	8%	<input checked="" type="checkbox"/>	100	Mbps
<input checked="" type="checkbox"/>	500	kbps	<input type="checkbox"/>	2	17%	<input checked="" type="checkbox"/>	100	Mbps
<input checked="" type="checkbox"/>	500	kbps	<input type="checkbox"/>	3	25%	<input checked="" type="checkbox"/>	100	Mbps
<input checked="" type="checkbox"/>	500	kbps	<input type="checkbox"/>	4	33%	<input checked="" type="checkbox"/>	100	Mbps
<input type="checkbox"/>	500	kbps	<input checked="" type="checkbox"/>	1	8%	<input checked="" type="checkbox"/>	100	Mbps
<input type="checkbox"/>	500	kbps	<input checked="" type="checkbox"/>	1	8%	<input checked="" type="checkbox"/>	100	Mbps
<input type="checkbox"/>	50	Mbps	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>	100	Mbps
<input type="checkbox"/>	50	Mbps	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>	100	Mbps

CLI-Konfigurationsbefehl:

```
Schnittstelle GigabitEthernet 1/2
  Amt-Switchport zugelassen für VLAN 1.100
  Hybrid-Switchport erlaubt VLAN 100,4095
  Amt-Switchport VLAN Tag native
  Switchport Amtsmodus
  qos Grenzwert 100000
  qos wrr 1 2 3 4 1 1
exit
```

Leitfaden zum Link Fail Alarm

Einführung der Alarmfunktion

INDRY II unterstützt ein Alarmprofil, um spezielle Alarmschablonen zu konfigurieren.

Wenn ein spezieller Alarm ausgeführt wurde, wenn die Alarmeingabe demaskiert ist, generiert das System einen Eintrag in die aktuelle Alarmtabelle und einen Eintrag in der Alarmverlauftabelle, SNMP-Alarm-Traps und löst darüber hinaus die Alarmausgangsverzögerung aus.

Im aktuellen Design unterstützt INDRY II nur den Verbindungsfehleralarm. Bitte beachten Sie die folgende Beschreibung.

Verbindungsfehleralarm in INDRY II

INDRY II unterstützt die folgenden Alarmtypen:

- PORT-1 Port Verbindungsausfall
- PORT-2 Port Verbindungsausfall
- PORT-3 Port Verbindungsausfall
- PORT-4 Port Verbindungsausfall
- PORT-5 Port Verbindungsausfall
- PORT-6 Port Verbindungsausfall
- PORT-7 Port Verbindungsausfall
- PORT-8 Port Verbindungsausfall
- PORT-9 Port Verbindungsausfall
- PORT-10 Port Verbindungsausfall

Konfiguration und Anwendung im Alarmzustand

(1) Jeder Typ kann als maskiert oder demaskiert konfiguriert werden. Die Standardwerte sind demaskiert für alle Alarmtypen.

Configuration
 Status
 System
[Restart](#)
[Save & Restore](#)
[Firmware](#)
Alarm Profile
[CLI Options](#)
[HTTP\(HTTPS\)](#)
[SNTP](#)
[Syslog](#)
[User Administration](#)
SNMP
[Options](#)
[Community](#)
[Trap Target](#)
[User](#)
[Group](#)
[View](#)

System / Alarm Profile
 Modify
 Previous Command Result: Normal

<input type="checkbox"/>	ID	Description	Level	Mask
<input type="checkbox"/>	101	GE-1 Port Link Down	Minor	Unmask
<input type="checkbox"/>	102	GE-2 Port Link Down	Major Minor	Unmask
<input type="checkbox"/>	103	GE-3 Port Link Down	Minor	Unmask
<input type="checkbox"/>	104	GE-4 Port Link Down	Minor	Unmask
<input type="checkbox"/>	105	GE-5 Port Link Down	Minor	Mask
<input type="checkbox"/>	106	GE-6 Port Link Down	Minor	Mask
<input type="checkbox"/>	107	GE-7 Port Link Down	Minor	Mask
<input type="checkbox"/>	108	GE-8 Port Link Down	Minor	Mask
<input type="checkbox"/>	109	GE-9 Port Link Down	Minor	Mask
<input type="checkbox"/>	110	GE-10 Port Link Down	Minor	Mask

(2) INDRY II unterstützt die aktuelle Alarmtabelle, um den aktuellen Alarm anzuzeigen.

Status / Alarm Current
 Refresh
 Related: [Alarm Profile](#) [Alarm History](#) [Event Log](#)
 Previous Command Result: Normal

[Alarm Current](#) [Alarm History](#) [Event Log](#)

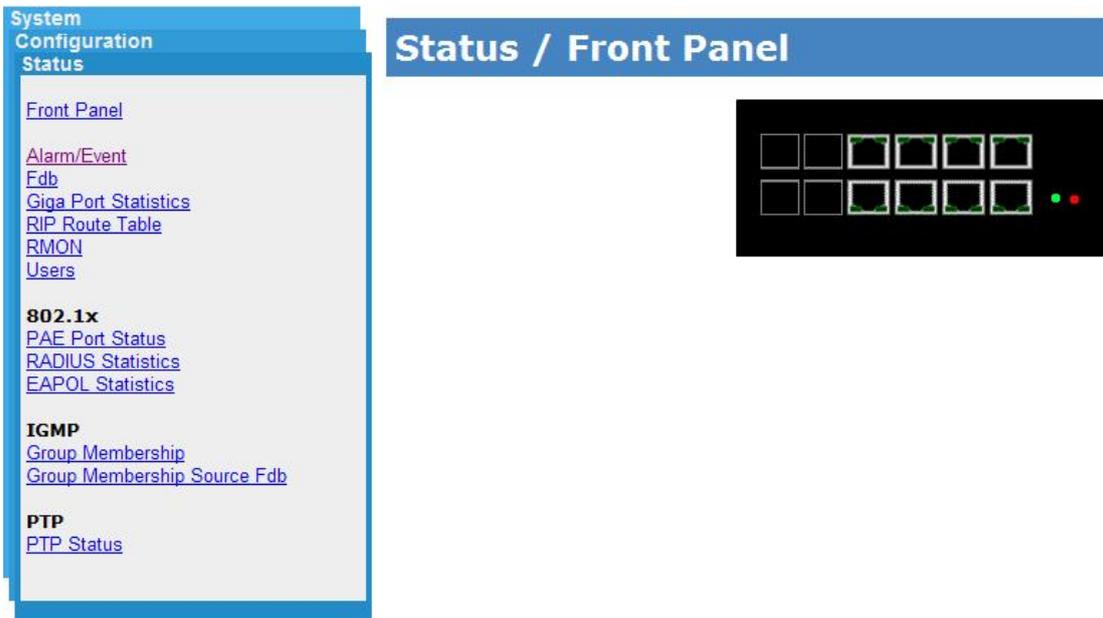
SeqNo	ID	Description	Level	State	Time
37	106	GE-6 Port Link Down	Minor	Set	01/16/2000 06:05:28
36	105	GE-5 Port Link Down	Minor	Set	01/16/2000 06:05:28
1	102	GE-2 Port Link Down	Minor	Set	01/16/2000 04:17:01

(3) INDRY II unterstützt die Alarmverlauffabelle, um die Alarmverlaufaufzeichnungen zu erfassen und zu speichern.

Die Erfassung umfasst das Löschen/Einstellen des Alarms. Die Alarmverlauffabelle kann max. 256 Einträge aufnehmen. Wenn die Alarmverlauffabelle voll ist, überschreibt ein neuer Eintrag die alten.

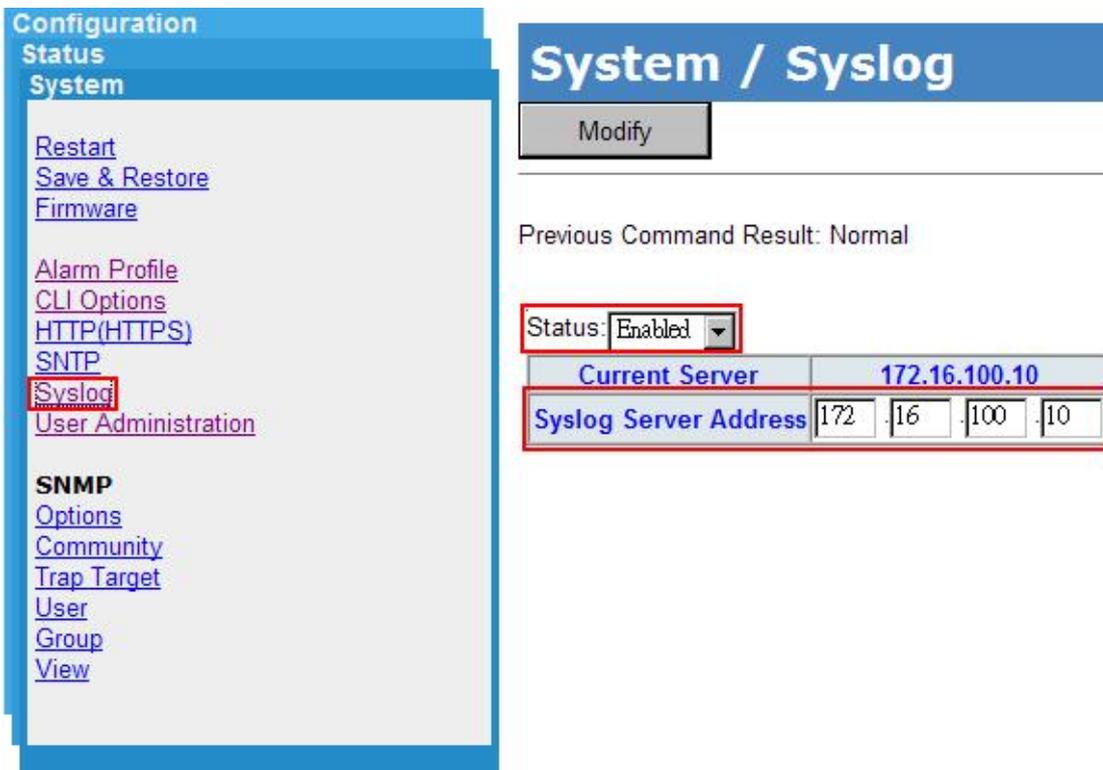
(4) INDRY II unterstützt den Befehl Alarmverlauffabelle löschen.

- (5) Wenn das System einen der Alarme der aktuellen Tabelle hat, müssen die Relaisausgangs- und Alarm-LED-Anzeigen eingeschaltet werden.



Wenn die aktuelle Alarmtabelle leer ist, müssen die Relaisausgangs- und die Alarm-LED ausgeschaltet werden.

- (6) Wenn ein Alarm eingestellt/gelöscht wurde, muss INDRY II einen Eintrag in die Alarmverlauftabelle generieren und eine SNMP-Trap für den Verwaltungsserver.



(7) Am Host mit IP: 172.16.100.10 geht eine Alarm-Trap welche Verbindungs-/Ausfall-Informationen aufzeichnet.

No.	Time.	Source	Destination	Protocol	Info
2	0.00	172.16.100.36	172.16.100.10	Syslog	LOCAL1.ALERT: Jan 16 05:51:08 oamp: Alarm Set: GE-3 Port Link Down: GE-3
3	0.01	172.16.100.36	172.16.100.10	Syslog	LOCAL1.ALERT: Jan 16 05:51:08 oamp: Event: GE Port Link Down: GE-4
4	0.01	172.16.100.36	172.16.100.10	Syslog	LOCAL1.ALERT: Jan 16 05:51:08 oamp: Alarm Set: GE-4 Port Link Down: GE-4
5	2.33	172.16.100.36	172.16.100.10	Syslog	LOCAL1.ALERT: Jan 16 05:51:10 oamp: Event: GE Port Link Up: GE-3
6	2.34	172.16.100.36	172.16.100.10	Syslog	LOCAL1.ALERT: Jan 16 05:51:10 oamp: Alarm Clear: GE-3 Port Link Down: GE-3

[x] Frame 2 (105 bytes on wire, 105 bytes captured)
 [x] Ethernet II, Src: Cimsys_33:44:55 (00:11:22:33:44:55), Dst: PlanetCo_e9:36:98 (00:90:cc:e9:36:98)
 [x] Internet Protocol, Src: 172.16.100.36 (172.16.100.36), Dst: 172.16.100.10 (172.16.100.10)
 [x] User Datagram Protocol, Src Port: 47212 (47212), Dst Port: syslog (514)
 [x] Syslog message: LOCAL1.ALERT: Jan 16 05:51:08 oamp: Alarm Set: GE-3 Port Link Down: GE-3
 1000 1... = Facility: LOCAL1 - reserved for local use (17)
 001 = Level: ALERT - action must be taken immediately (1)
 Message: Jan 16 05:51:08 oamp: Alarm Set: GE-3 Port Link Down: GE-3

No.	Time.	Source	Destination	Protocol	Info
3	0.01	172.16.100.36	172.16.100.10	Syslog	LOCAL1.ALERT: Jan 16 05:51:08 oamp: Event: GE Port Link Down: GE-4
4	0.01	172.16.100.36	172.16.100.10	Syslog	LOCAL1.ALERT: Jan 16 05:51:08 oamp: Alarm Set: GE-4 Port Link Down: GE-4
5	2.33	172.16.100.36	172.16.100.10	Syslog	LOCAL1.ALERT: Jan 16 05:51:10 oamp: Event: GE Port Link Up: GE-3
6	2.34	172.16.100.36	172.16.100.10	Syslog	LOCAL1.ALERT: Jan 16 05:51:10 oamp: Alarm Clear: GE-3 Port Link Down: GE-3
7	2.34	172.16.100.36	172.16.100.10	Syslog	LOCAL1.ALERT: Jan 16 05:51:10 oamp: Event: GE Port Link Up: GE-4

[x] Frame 6 (107 bytes on wire, 107 bytes captured)
 [x] Ethernet II, Src: Cimsys_33:44:55 (00:11:22:33:44:55), Dst: PlanetCo_e9:36:98 (00:90:cc:e9:36:98)
 [x] Internet Protocol, Src: 172.16.100.36 (172.16.100.36), Dst: 172.16.100.10 (172.16.100.10)
 [x] User Datagram Protocol, Src Port: 47212 (47212), Dst Port: syslog (514)
 [x] Syslog message: LOCAL1.ALERT: Jan 16 05:51:10 oamp: Alarm Clear: GE-3 Port Link Down: GE-3
 1000 1... = Facility: LOCAL1 - reserved for local use (17)
 001 = Level: ALERT - action must be taken immediately (1)
 Message: Jan 16 05:51:10 oamp: Alarm Clear: GE-3 Port Link Down: GE-3

802.1x Authentifizierungs- Anwendungshilfe

Einführung von 802.1x Authentifizierungsfunktion

IEEE 802.1x erlangt Schlüssel, die genutzt werden können, um eine PaketAuthentifizierung, Integrität und Vertraulichkeit zu erreichen. Typischerweise in Kombination mit bekannten Algorithmen-Verschlüsselungen verwendet (z.B. TLS, SRP, MD5-Challenge usw.). In unserem industriellen Switch (INDRY II) unterstützen wir die 802.1x-Authentifizierungsfunktion pro Port (Port1~Port10). Sie müssen die 802.1x-Funktion des Systems aktivieren und Ports und typen auswählen, die Sie anwenden möchten. Wenn INDRY II die 802.1x-Authentifizierungsprüfung für bestimmte Ethernet-Ports aktiviert, sollte dieser Port authentifiziert werden, bevor irgendeine Netzwerkleistung genutzt wird. Bitte beachten Sie die folgende Beschreibung.

802.1x Timer in INDRY II

Gegenstand	Parameter (sec)	Beschreibung
1	ReAuth-Zeit	INDRY II startet die Authentifizierung nach jeder ReAuth-Zeit neu, wenn der Authentifizierungserfolg und die ReAuth-Option aktiviert wurden.
2	Ruhezeit	INDRY II wartet eine gewisse Ruhezeit ab, um den Authentifizierungsprozess neu zu starten, nachdem die Authentifizierung vorher fehlgeschlagen ist.
3	Tx Zeit	INDRY II sendet jede Tx Zeit eine EAP-Anfrage an den Antragsteller, wenn die Authentifizierung läuft und die Ruhezeit nicht läuft.
4	Antragsteller-Pause	INDRY II wartet die Antragsteller-Pause ab, um eine Reaktion vom Antragsteller zu erhalten.
5	Server Timeout	INDRY II wartet das ServerTimeout ab, um eine Reaktion vom RADIUS-Server zu erhalten.

Konfiguration in RADIUS-Server

Schritt 1: Installieren Sie einen RADIUS-Server auf einen Linux-PC.

Schritt 2: Geheimen Schlüssel für RADIUS-Server bearbeiten.

Einstellung:

```
client 20.20.20.0/24 {  
    secret = a1b2c3d4  
}
```



Der geheime Schlüssel in
INDRY II sollte mit diesem
identisch sein.

Schritt 3: Benutzernamen und Kennwort für Supplicant zur Authentifizierung beim Server bearbeiten.

Einstellung:

	Benutzername		Benutzerkennwort
test123		Cleartext-Password := "test123"	
aaaa		Cleartext-Password := "aaaa"	

Schritt 4: Statische IP-Adresse für diesen RADIUS-Server festlegen.

Einstellung: 20.20.20.20

Schritt 5: RADIUS-Server starten

Beispiel

Als Beispiel dient im Folgenden die 802.1x-Authentifizierung über INDRY II zur Authentifizierung durch den RADIUS-Server. In diesem einfachen Beispiel dient Port 1 als Testport, der 802.1x in INDRY II aktiviert.

Bei Standardkonfiguration folgende Web UI-Einstellung verwenden.

Step 1. Configuration -> Security -> Networks -> NAS aufrufen.

Modus „Enable“ zur Aktivierung der Authentifizierung auswählen und bei Port-1 bzw. Port-2 „Port Base 802.1x“ eingeben.

Configuration

- System
 - Information
 - IP
 - NTP
 - Time
 - Log
- Green Ethernet
- Ports
- DHCP
- Security
 - Switch
 - Network
 - Limit Control
 - NAS
 - ACL
 - IP Source Guard
 - ARP Inspection
 - AAA
 - RADIUS
 - TACACS+
 - Aggregation
 - Loop Protection
 - Spanning Tree
 - IPMC Profile
 - MVR
 - IPMC
 - LLDP
 - MAC Table
 - VLANs
 - Private VLANs
 - VCL
 - Voice VLAN
 - QoS
 - Mirroring
 - GVRP
 - sFlow
- Monitor
- Diagnostics
- Maintenance

Network Access Server Configuration

System Configuration

Mode	Enabled
Reauthentication Enabled	<input checked="" type="checkbox"/>
Reauthentication Period	3600 seconds
EAPOL Timeout	30 seconds
Aging Period	300 seconds
Hold Time	10 seconds
RADIUS-Assigned QoS Enabled	<input type="checkbox"/>
RADIUS-Assigned VLAN Enabled	<input type="checkbox"/>
Guest VLAN Enabled	<input type="checkbox"/>
Guest VLAN ID	1
Max. Reauth. Count	2
Allow Guest VLAN if EAPOL Seen	<input type="checkbox"/>

Port Configuration

Port	Admin State	RADIUS-Assigned QoS Enabled	RADIUS-Assigned VLAN Enabled	Guest VLAN Enabled	Port State	Restart
*	◇	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
1	Port-based 802.1X	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Link Down	Reauthenticate Reinitialize
2	Port-based 802.1X	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Link Down	Reauthenticate Reinitialize
3	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Link Down	Reauthenticate Reinitialize
4	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Link Down	Reauthenticate Reinitialize
5	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Link Down	Reauthenticate Reinitialize
6	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Link Down	Reauthenticate Reinitialize
7	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Link Down	Reauthenticate Reinitialize
8	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Link Down	Reauthenticate Reinitialize
9	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Authorized	Reauthenticate Reinitialize
10	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Link Down	Reauthenticate Reinitialize
11	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Link Down	Reauthenticate Reinitialize
12	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Link Down	Reauthenticate Reinitialize
13	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Link Down	Reauthenticate Reinitialize
14	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Link Down	Reauthenticate Reinitialize

Save Reset

Step 1. Configuration -> Security -> AAA -> Radius aufrufen.

Auf „Add New Server“ klicken, beim Server „20.20.20.20“ und beim geheimen Schlüssel „a1b2c3d4“ eingeben.

Anschließend auf die Schaltfläche „Save“ klicken.

Configuration

- System
 - Information
 - IP
 - NTP
 - Time
 - Log
- Green Ethernet
- Ports
- DHCP
- Security
 - Switch
 - Network
 - Limit Control
 - NAS
 - ACL
 - IP Source Guard
 - ARP Inspection
 - AAA
 - RADIUS
 - TACACS+
 - Aggregation
 - Loop Protection
 - Spanning Tree
 - IPMC Profile
 - MVR
 - IPMC
 - LLDP

RADIUS Server Configuration

Global Configuration

Timeout	5 seconds
Retransmit	3 times
Deadtime	0 minutes
Key	a1b2c3d4
NAS-IP-Address	
NAS-IPv6-Address	
NAS-Identifier	

Server Configuration

Delete	Hostname	Auth Port	Acct Port	Timeout	Retransmit	Key
<input type="checkbox"/>	10.10.10.199	1812	1813	5	3	a1b2c3d4

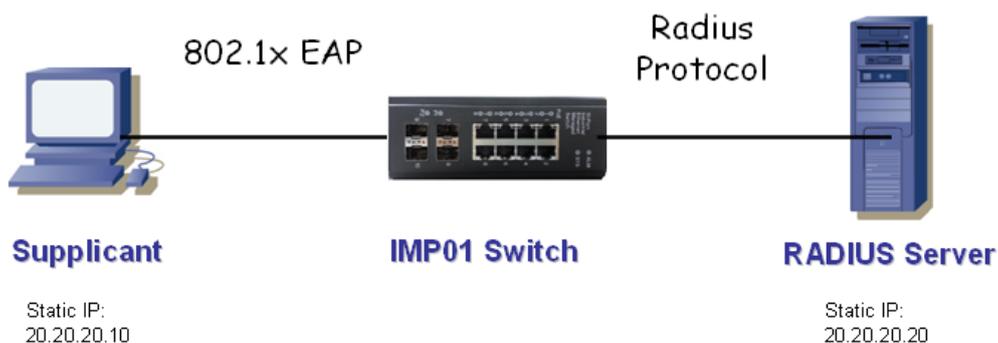
Add New Server

Save Reset

CLI-Befehl:

```
configure
Schnittstelle VLAN1
ip address 20.20.20.120 255.0.0.0exit
exit
radius-server host 20.20.20.20 timeout 5 retransmit 3 key a1b2c3d4
dot1x re-authentication
dot1x system-auth-control
exit
Schnittstelle GigabitEthernet 1/1
dot1x auth-port-control auto
```

Konfiguration



NIC-Einstellung des Supplicants

Schritt 1: Statische IP-Adresse 20.20.20.10 und Netzmaske 255.255.255.0 für Supplicanten konfigurieren.

(Soll ein DHCP-Server eine IP-Adresse für den Supplicanten zuweisen, kann dieser Schritt ignoriert werden.)

Schritt 2: Kontrollkästchen bei IEEE802.1x Authentication Enable aktivieren und dann bei EAP Type MD5-Challenge festlegen.

Nach dem Festlegen dieser Funktion in NIC sollte der Supplicant ein korrektes Paar von Konto und Kennwort eingeben, um diesen Ethernet-Portdienst von INDRY II aus zu verwenden.

Verhalten bei der Authentifizierung

Der Supplicant sollte den Authentifizierungsprozess durchlaufen, um beliebige Dienste nutzen zu können. Nach der Eingabe des korrekten Kontos und Kennworts, die im RADIUS-Server gespeichert sind, ist eine erfolgreiche Authentifizierung möglich. Der Authentifizierungsprozess ist folgendermaßen aufgebaut.

