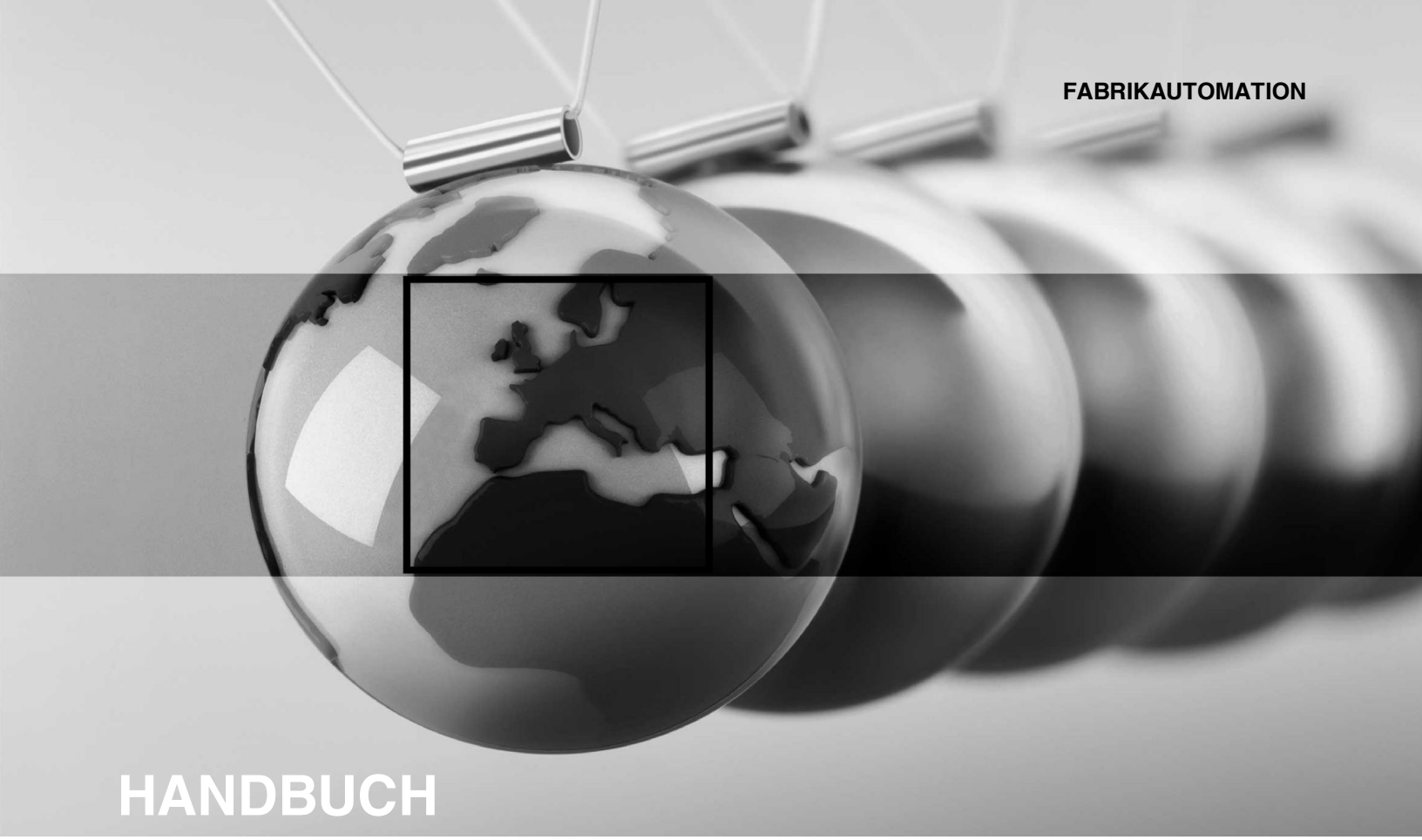


HANDBUCH

RocketLinx

ICRL-M-16RJ45/4CP-G-DIN
ICRL-M-8RJ45/4SFP-G-DIN

PEPPERL+FUCHS
SENSING YOUR NEEDS

Bezüglich der Lieferung von Produkten ist die aktuelle Ausgabe des folgenden Dokuments maßgeblich: Die Allgemeinen Lieferbedingungen für Produkte und Dienstleistungen der Elektroindustrie, veröffentlicht durch den Zentralverband der Elektrotechnik und Elektroindustrie (ZVEI) e.V. einschließlich der Ergänzungsklausel: „Erweiterter Eigentumsvorbehalt“.

Inhaltsverzeichnis

1. Einführung

In diesem Handbuch werden die folgenden Switches behandelt.

- RocketLinx ICRL-M-8RJ45/4SFP-G-DIN
- RocketLinx ICRL-M-16RJ45/4CP-G-DIN

Anmerkung: *Die ICRL-M-16RJ45/4CP-G-DIN und ICRL-M-8RJ45/4SFP-G-DIN werden im Rest dieses Handbuchs einfach als ICRL-M bezeichnet, es sei denn, es gibt Unterschiede zwischen den Modellen.*

1.1. ICRL-M-8RJ45/4SFP-G-DIN-Übersicht

Der RocketLinx ICRL-M-8RJ45/4SFP-G-DIN ist ein vollständig verwalteter Layer-2-Gigabit-Ethernet-Switch mit 12 Ports, der acht 10/100/1000-BASE-T-Kupfer-Ethernet-Ports mit vier 100/1000-BASE-T SFP-Glasfaser-Ports kombiniert und so die Flexibilität bietet, über größere Entfernungen Glasfaser hinzuzufügen, um die einzigartigen Anforderungen jedes Projekts zu erfüllen. Mit einem robusten Metallgehäuse, einem großen Betriebstemperaturbereich sowie erweiterter Sicherheit und Netzwerkleistung ist der ICRL-M-8RJ45/4SFP-G-DIN die ideale Lösung für geschäftskritische industrielle Netzwerkanwendungen.

Der ICRL-M-8RJ45/4SFP-G-DIN bietet:

- Acht RJ45-Gigabit-Ports
- Vier 100/1000-SFP-Steckplätze für Glasfaserverbindungen
- Redundanter Netzeingang mit einem Eingangsstrombereich von 10 bis 36 V DC
- IP31 mit einem extremen Betriebstemperaturbereich von -40 bis 75 °C
- Erfüllt die Anforderungen der Norm EN50121-4 für rollende Lagerschienen

1.2. ICRL-M-16RJ45/4CP-G-DIN-Übersicht

Der RocketLinx ICRL-M-16RJ45/4CP-G-DIN ist ein vollständig verwalteter Layer-2-Gigabit-Ethernet-Switch mit 20 Ports, der 16 10/100/1000-BASE-T-Kupfer-Ethernet-Ports mit vier 100/1000-BASE-T-Kupfer- oder SFP-Glasfaser-Combo-Ports kombiniert. Mit einem robusten Metallgehäuse, einem großen Betriebstemperaturbereich sowie erweiterter Sicherheit und Netzwerkleistung ist der ICRL-M-16RJ45/4CP-G-DIN die ideale Lösung für geschäftskritische industrielle Netzwerkanwendungen.

Der ICRL-M-16RJ45/4CP-G-DIN bietet:

- 16 RJ45-Gigabit-Ports
- Vier kombinierte RJ45-/SFP-Ports
- Redundanter Netzeingang mit einem Eingangsstrombereich von 10 bis 60 V DC
- IP31 mit einem extremen Betriebstemperaturbereich von -40 bis 75 °C
- Erfüllt die Anforderungen der Norm EN50121-4 für rollende Lagerschienen

5/21/20

2. Installation der Hardware

Sie können die folgenden Unterabschnitte verwenden, um den RocketLinx ICRL-M zu installieren.

- *ICRL-M-8RJ45/4SFP-G-DIN – Verfahren* auf Seite 9
- *ICRL-M-16RJ45/4CP-G-DIN – Verfahren* auf Seite 13
- *Montieren des ICRL-M* auf Seite 15
- *Anschließen der Ethernet-Ports* auf Seite 16
- *Anschließen des SFP-Transceivers* auf Seite 17
- *Beschreibung der LED* auf Seite 17
- *Reset-Taste* auf Seite 18

Anmerkung: *Die ICRL-M-16RJ45/4CP-G-DIN und ICRL-M-8RJ45/4SFP-G-DIN werden im Rest dieses Kapitels einfach als ICRL-M bezeichnet, es sei denn, es gibt modellspezifische Informationen.*

2.1. ICRL-M-8RJ45/4SFP-G-DIN – Verfahren

Verwenden Sie die folgenden Unterabschnitte, um mit der Installation des ICRL-M-8RJ45/4SFP-G-DIN zu beginnen.

- *Verbinden von Stromversorgung und Masse (ICRL-M-8RJ45/4SFP-G-DIN)* auf Seite 10
- *Anschließen des Relaisausgangs (ICRL-M-8RJ45/4SFP-G-DIN)* auf Seite 11
- *Anschließen des Digitaleingangs (ICRL-M-8RJ45/4SFP-G-DIN)* auf Seite 12

Gehen Sie wie folgt vor, um die Installation abzuschließen:

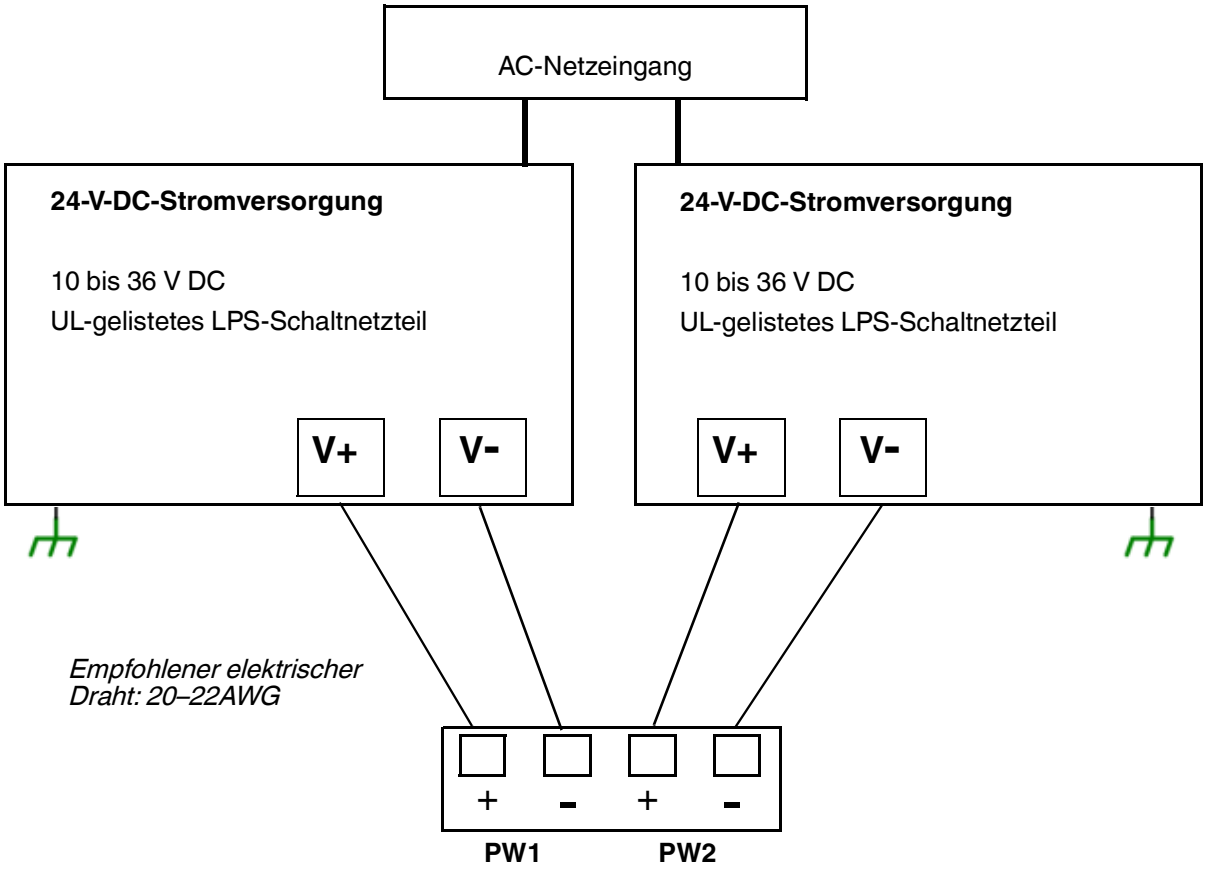
- *Anschließen der Ethernet-Ports* auf Seite 16
- *Anschließen des SFP-Transceivers* auf Seite 17
- *Beschreibung der LED* auf Seite 17
- *Reset-Taste* auf Seite 18

5/21/20

2.1.1. Verbinden von Stromversorgung und Masse (ICRL-M-8RJ45/4SFP-G-DIN)

Gehen Sie wie folgt vor, um ICRL-M-8RJ45/4SFP-G-DIN Stromversorgung und Masse anzuschließen.

1. Schließen Sie die DC-Stromeingänge an, indem Sie die positiven und negativen Drähte (20–22AWG) in die Kontakte PW+ und PW- einführen.
   - PW1 und PW2 unterstützen Stromredundanz und Verpolschutz.
   - Akzeptiert eine positive oder negative Stromquelle, aber PW1 und PW2 müssen für denselben Modus gelten.
   - Wenn beide Stromeingänge angeschlossen sind, wird der ICRL-M-8RJ45/4SFP-G-DIN mit der höchsten angeschlossenen Spannung versorgt.
   - Der ICRL-M-8RJ45/4SFP-G-DIN kann einen Alarm ausgeben, wenn PW1 oder PW2 nicht mehr mit Strom versorgt werden. Informationen zum Konfigurieren eines Alarms finden Sie im Abschnitt *Warnung* auf Seite 143.



Anmerkung: *Trennen Sie das Netzteil von der Spannungsquelle, bevor Sie es an den Schalter anschließen. Andernfalls kann die Klinge des Schraubendrehers unbeabsichtigt zu einem Kurzschluss der Anschlüsse am geerdeten Gehäuse führen. Ziehen Sie die Schrauben der steckbaren Kabelklemmen fest, um zu verhindern, dass sich die Kabel lösen.*

2. Schließen Sie einen Massedraht zwischen dem Gehäuse und der Erdung mit einem 12–24AWG-Draht an, um sicherzustellen, dass der ICRL-M-8RJ45/4SFP-G-DIN nicht durch Rauschen oder Stromschlag beschädigt wird.
   a. Lösen Sie die Masseschrauben an der Gehäuserückseite des ICRL-M-8RJ45/4SFP-G-DIN.
   b. Führen Sie den Massedraht ein.
   c. Ziehen Sie die Masseschraube fest, nachdem der Massedraht angeschlossen wurde.

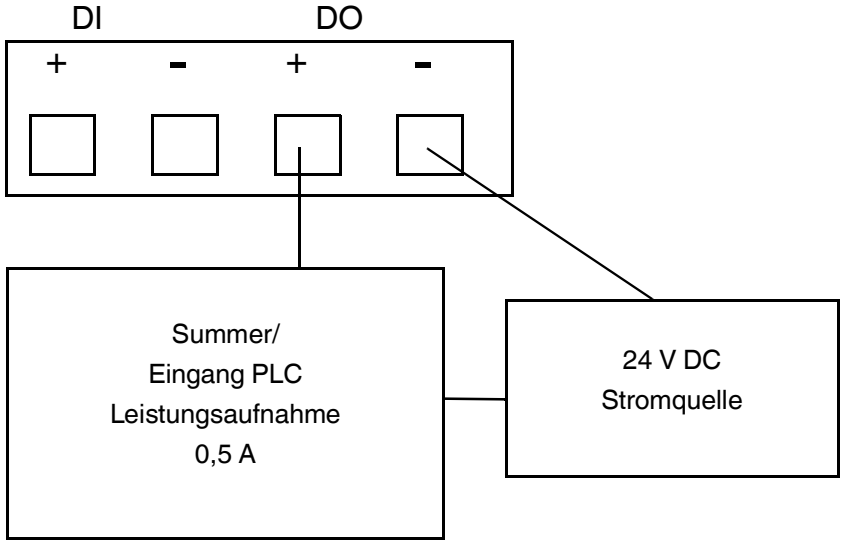
2.1.2. Anschließen des Relaisausgangs (ICRL-M-8RJ45/4SFP-G-DIN)

Falls gewünscht, schließen Sie den Relaisausgang (Digitalausgang) an der Unterseite des ICRL-M-8RJ45/4SFP-G-DIN an. Der Relaisausgang wird durch die vordefinierten Betriebsregeln gesteuert. Zum Aktivieren der Relaisausgangsfunktionen siehe *Fault Relay* auf Seite 143.

Relaiskontakte werden für normalen Betrieb unter Spannung gesetzt (offen) und schließen bei Fehlerbedingungen. Zu den Fehlerbedingungen gehören:

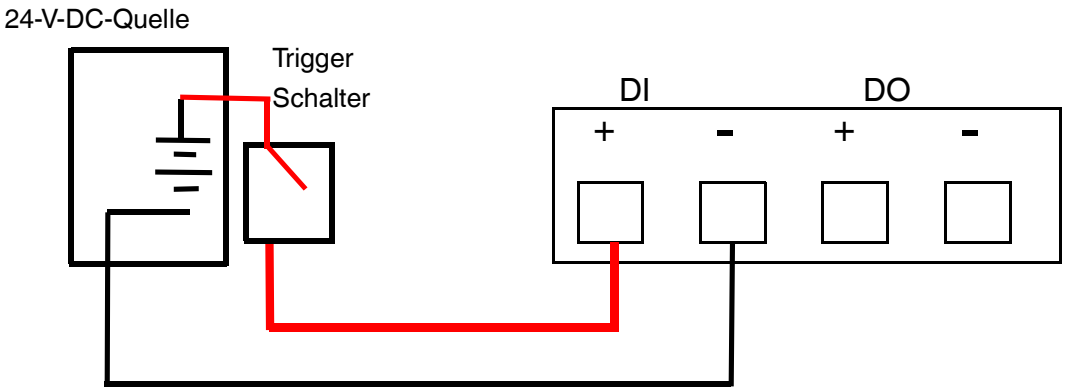
- Stromausfall
- Verbindungsfehler
- Ring
- Ping-Fehler
- Ping-Reset
- Trockene Ausgabe
- DI-Status

Anmerkung: *Der Relaiskontakt (DO) unterstützt 0,5 A bei 24 V DC. Schließen Sie keine Spannung und keinen Strom an, die diese Spezifikationen überschreiten.*



2.1.3. Anschließen des Digitaleingangs (ICRL-M-8RJ45/4SFP-G-DIN)

Die Digitaleingangskontakte befinden sich an der Unterseite des ICRL-M-8RJ45/4SFP-G-DIN. Er akzeptiert einen externen DC-Signaleingang und kann so konfiguriert werden, dass er eine Warnmeldung über Ethernet sendet, wenn das Signal geändert wird. Das Signal kann durch einen externen Spannungswechsel ausgelöst und erzeugt werden, wie z. B. einen Türauslöser für einen Schaltschrank.



Messfühler

1 = Hoher Eingang (11 bis 30 V DC)

0 = Niedriger Eingang (0 bis 10 V DC)

Anmerkung: *DI akzeptiert DC-Signale und unterstützt isolierte Eingangsschaltungen mit digitalem High-Pegel-Eingang von 11 bis 30 V DC und digitalem Low-Pegel-Eingang von 0 bis 10 V DC. Legen Sie keine Spannung an, die die Spezifikation überschreitet, da dies zu einer Beschädigung des internen Stromkreises oder einer falschen Aktion des DI führen kann.*

2.2. ICRL-M-16RJ45/4CP-G-DIN – Verfahren

Verwenden Sie die folgenden Unterabschnitte, um mit der Installation des ICRL-M-16RJ45/4CP-G-DIN zu beginnen.

- *Verbinden von Stromversorgung und Masse (ICRL-M-16RJ45/4CP-G-DIN)* auf Seite 13
- *Anschließen der Relaisausgangskontakte (ICRL-M-16RJ45/4CP-G-DIN)* auf Seite 14

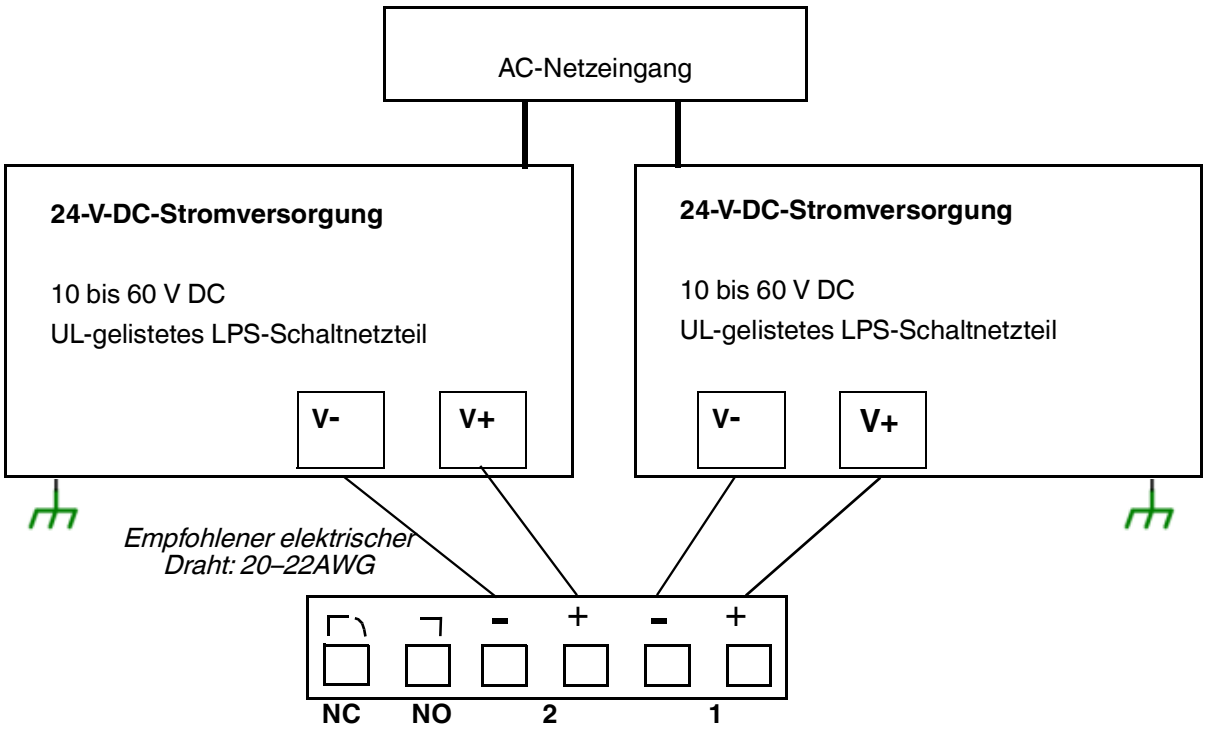
Gehen Sie wie folgt vor, um die Installation abzuschließen:

- *Anschließen der Ethernet-Ports* auf Seite 16
- *Anschließen des SFP-Transceivers* auf Seite 17
- *Beschreibung der LED* auf Seite 17
- *Reset-Taste* auf Seite 18

2.2.1. Verbinden von Stromversorgung und Masse (ICRL-M-16RJ45/4CP-G-DIN)

Gehen Sie wie folgt vor, um ICRL-M-16RJ45/4CP-G-DIN Stromversorgung und Masse anzuschließen.

1. Schließen Sie die DC-Stromeingänge an, indem Sie die positiven und negativen Drähte (20–22AWG) in die Kontakte PW+ und PW- einführen.
   - PW1 und PW2 unterstützen Stromredundanz und Verpolschutz.
   - Akzeptiert eine positive oder negative Stromquelle, aber PW1 und PW2 müssen für denselben Modus gelten.
   - Wenn beide Stromeingänge angeschlossen sind, wird der ICRL-M-16RJ45/4CP-G-DIN mit der höchsten angeschlossenen Spannung versorgt.
   - Der ICRL-M-16RJ45/4CP-G-DIN kann einen Alarm ausgeben, wenn PW1 oder PW2 nicht mehr mit Strom versorgt werden. Informationen zum Konfigurieren eines Alarms finden Sie im Abschnitt *Warnung* auf Seite 143.



5/21/20

Anmerkung: *Trennen Sie das Netzteil von der Spannungsquelle, bevor Sie es an den Schalter anschließen. Andernfalls kann die Klinge des Schraubendrehers unbeabsichtigt zu einem Kurzschluss der Anschlüsse am geerdeten Gehäuse führen. Ziehen Sie die Schrauben der steckbaren Kabelklemmen fest, um zu verhindern, dass sich die Kabel lösen.*

2. Schließen Sie einen Massedraht zwischen dem Gehäuse und der Erdung mit einem 12–24AWG-Draht an, um sicherzustellen, dass der ICRL-M-16RJ45/4CP-G-DIN nicht durch Rauschen oder Stromschlag beschädigt wird.
   a. Lösen Sie die Masseschrauben an der Gehäuserückseite des ICRL-M-16RJ45/4CP-G-DIN.
   b. Führen Sie den Massedraht ein.
   c. Ziehen Sie die Masseschraube fest, nachdem der Massedraht angeschlossen wurde.

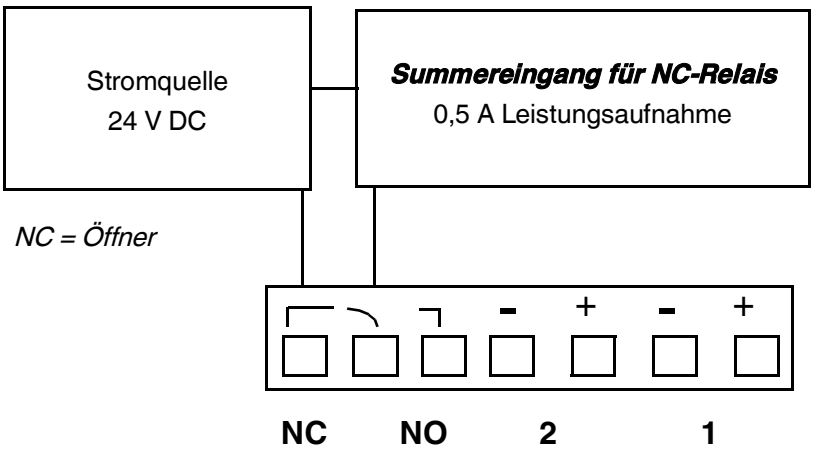
2.2.2. Anschließen der Relaisausgangskontakte (ICRL-M-16RJ45/4CP-G-DIN)

Falls gewünscht, schließen Sie die Relaisausgangskontakte an, die sich auf dem 6-poligen Klemmenblock-Steckverbinder an der Vorderseite des ICRL-M-16RJ45/4CP-G-DIN befinden. Der Relaisausgang wird durch die vordefinierten Betriebsregeln gesteuert. Zum Aktivieren der Relaisausgangsfunktionen siehe *Fault Relay* auf Seite 143.

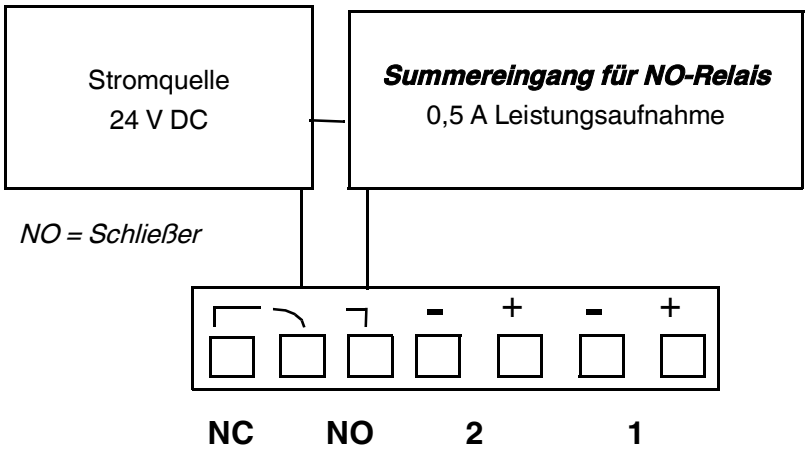
Digitalausgangs-Relaiskontakte werden für normalen Betrieb unter Spannung gesetzt (offen) und schließen bei Fehlerbedingungen. Zu den Fehlerbedingungen gehören:

- Stromausfall
- Verbindungsfehler
- Ring
- Ping-Fehler
- Ping-Reset
- Trockene Ausgabe

Anmerkung: *Der Relaiskontakt unterstützt 0,5 A bei 24 V DC. Schließen Sie keine Spannung und keinen Strom an, die diese Spezifikationen überschreiten.*



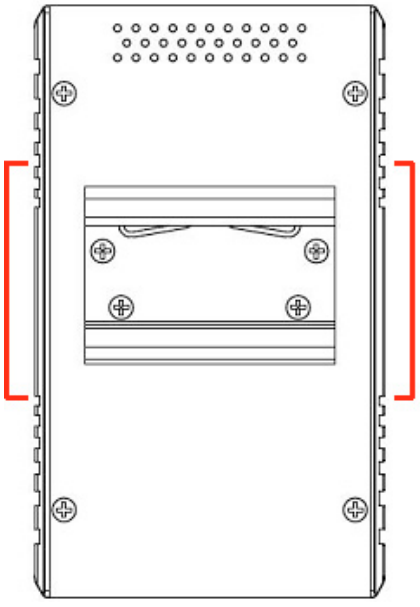
5/21/20



2.3. Montieren des ICRL-M

Gehen Sie wie folgt vor, um den ICRL-M in einer Hutschiene zu installieren.

Der Hutschienenclip ist bereits am ICRL-M befestigt. Wenn der Hutschienenclip nicht auf den ICRL-M geschraubt ist, befolgen Sie die Anweisungen und die Abbildung unten, um den Hutschienenclip am ICRL-M zu befestigen.



Hutschienenmontage

1. Verwenden Sie bei Bedarf die Schrauben, um den DIN-Hutschienenclip an der Rückwand des ICRL-M zu befestigen. (Führen Sie zum Entfernen des Hutschienenclips Schritt 1 in umgekehrter Reihenfolge aus.)
2. Führen Sie das obere Ende des DIN-Hutschienenclips von der Oberseite her in die Rückseite der DIN-Hutschiene.
3. Drücken Sie das untere Ende des DIN-Hutschienenclips sanft in die Schiene.
4. Stellen Sie sicher, dass der DIN-Hutschienenclip fest auf der Schiene sitzt.
5. Um den ICRL-M aus der Schiene zu entfernen, führen Sie die oben genannten Schritte in umgekehrter Reihenfolge aus.

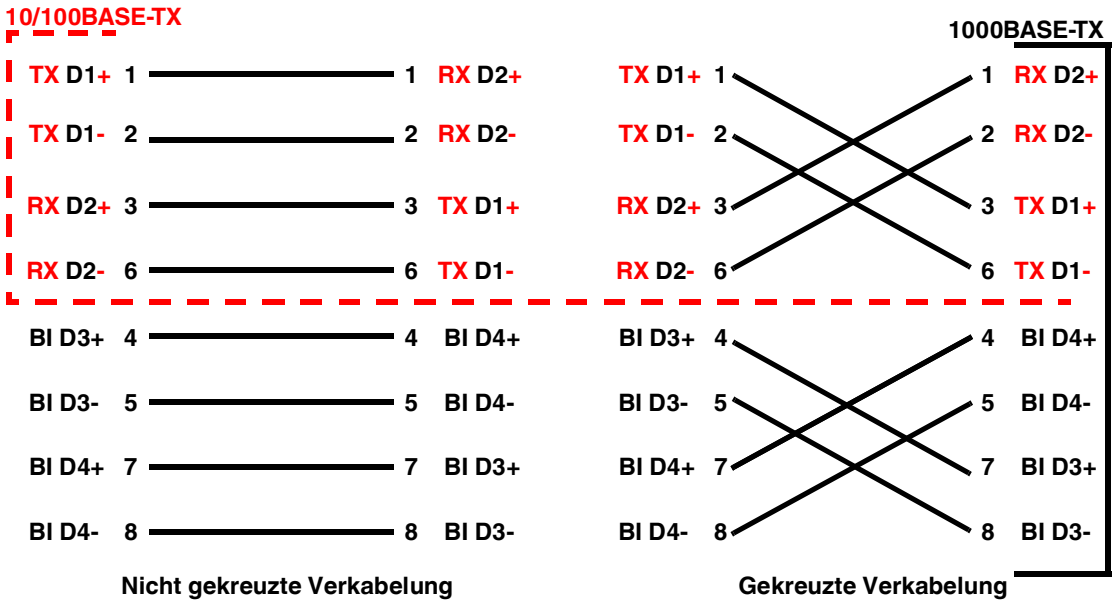
2.4. Anschließen der Ethernet-Ports

Sie können die folgenden Informationen verwenden, um Standard-Netzwerkkabel zwischen den ICRL-M-Ethernet-Ports und den Netzwerkknoten anzuschließen.

- ICRL-M-8RJ45/4SFP-G-DIN: Die Ports 1–8 sind RJ45-Gigabit-Kupfer-Ports und die Ports 9–12 sind Gigabit-SPFs.
- ICRL-M-16RJ45/4CP-G-DIN: Die Ports 1–16 sind RJ45-Gigabit-Kupfer-Ports mit Kombinationsports17–20, die über 4-Gigabit-RJ45-Ports und 4-Gigabit-SFP-Ports verfügen.

Informationen zur SFP-Installation finden Sie unter *Anschließen des SFP-Transceivers* auf Seite 17.

Alle Ethernet-Ports erkennen automatisch das Signal der angeschlossenen Geräte und können Verbindungsgeschwindigkeit und Duplexmodus (Halb- oder Vollduplex) aushandeln. Mit Auto-MDI/MDIX können Sie einen anderen Switch, einen anderen Hub oder eine andere Workstation anschließen, ohne nicht gekreuzte oder Crossover-Kabel austauschen zu müssen. Crossover-Kabel verbinden die Übertragungsleitungen an beiden Enden mit den Empfangsleitungen am gegenüberliegenden Ende.



Schließen Sie eine Seite eines Netzwerkkabels an einen beliebigen Switchport und die andere Seite an das angeschlossene Gerät an. Die LED **LNK/ACT** leuchtet, wenn das Kabel richtig angeschlossen ist. Achten Sie immer darauf, dass die Kabel zwischen den Switches und den angeschlossenen Geräten (z. B. Switch, Hub oder Workstation) weniger als 100 Meter lang sind und diese Anforderungen erfüllen.

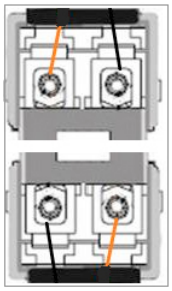
- **10/100BASE-TX**: Category-5-Kabel
- **1000BASE-TX**: Category-5- oder -5e-Kabel

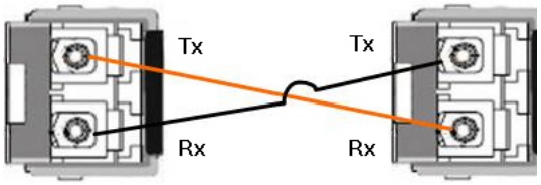
2.5. Anschließen des SFP-Transceivers

Der ICRL-M verfügt über vier SFP-Ports. Die SFP-Ports unterstützen Standard-GBIC-SFP-Transceiver, die 1000BASE-X (1000BASE-SX/LX/LHX/XD/ZX) unterstützen.

Die ICRL-M-16RJ45/4CP-G-DIN-SFP-Ports werden mit den RJ45-Ports 17–20 kombiniert.

Zur Gewährleistung der Systemzuverlässigkeit empfiehlt Pepperl+Fuchs die Verwendung Pepperl+Fuchs-zertifizierter SFPs.





Das SFP-Gehäuse weist ein 2x1-Design auf.

1. Schließen Sie den SFP-Transceiver an den SFP-Glasfaser-Transceiver an.
2. Verbinden Sie den Übertragungskanal an jedem Ende mit dem Empfangskanal.
3. Prüfen Sie die Richtung/den Winkel des Glasfaser-Transceivers und des Glasfaserkabels.

   Anmerkung: *Dies ist ein Laser-/LED-Produkt der Klasse 1. Blicken Sie nicht in den Laser-/LED-Strahl.*

Der SFP-Port funktioniert erst, wenn das Glasfaserkabel mit einem anderen aktiven Gerät verbunden ist.

SFP und entsprechende RJ45-Ports am ICRL-M-16RJ45/4CP-G-DIN arbeiten im exklusiven Modus. Datenverkehr, der über das SFP-Modul gesendet oder empfangen wird, hat Priorität, sodass kein Datenverkehr über die entsprechende RJ45-Verbindung gesendet oder empfangen wird. Um die RJ45-Verbindung zu verwenden, entfernen Sie den entsprechenden SFP.

Multimode-Kabel sollten nicht mehr als 2 km und Singlemode-Kabel nicht mehr als 30 km lang sein.

2.6. Beschreibung der LED

Dieser Unterabschnitt enthält Informationen zu den ICRL-M-LED. Weitere Informationen zur Verwendung der Web-Benutzerschnittstelle zur Remote-Anzeige von LED-Informationen finden Sie unter *Device Front Panel* auf Seite 157.

LED	LED leuchtet	LED blinkt	LED Aus
Sys	System ist bereit	Firmware wird hochgeladen	System ist nicht bereit
PWR 1/2	Gerät ist eingeschaltet	nicht zutreffend	Stromversorgung ist nicht eingeschaltet
RS (Ringstatus)	Grün: Ring ist normal Gelb: Ring ist anormal	Grün: Ring mit falschem Port Gelb: Ringport des Geräts ist ausgefallen	Switch arbeitet im Slave-Modus
DO (Rot)	Relais ist aktiv und Kontakte sind kurzgeschlossen	nicht zutreffend	DO nicht aktiviert
DI (Grün) ICRL-M-8RJ45/4SFP-G-DIN	Hohes digitales Signal erkannt	nicht zutreffend	DI nicht aktiviert
LINK/ACT	Port ist verbunden	Port ist aktiv	Portverbindung wurde unterbrochen oder Port ist nicht verbunden

LED	LED leuchtet	LED blinkt	LED Aus
1000M	Port ist mit 1000 MBit/s verbunden	nicht zutreffend	nicht zutreffend

LED	Funktion	Beschreibung
Link/Act	Zeigt Datenverkehr und Verbindungsstatus an	Ein: Port ist mit einem anderen Gerät verbunden Blinkt: Datenverkehr ist aktiv Aus: Port ist nicht verbunden
Geschwin-digkeit	Zeigt Verbindungsgeschwindigkeit des Kupferports an	Ein: Portverbindung weist 1000 MBit/s auf Aus: Portverbindung weist 100 MBit/s oder 10 MBit/s auf
1000	SFP-Transceiver-Geschwindigkeitsanzeige	Ein: SFP unterstützt 1000 MBit/s Grau: Angeschlossen, aber noch nicht verbunden

2.7. Reset-Taste

Der ICRL-M verfügt über eine Reset-Taste, mit der Sie den ICRL-M neu starten oder die Konfiguration auf die Werkseinstellungen zurücksetzen können.

Reset-Taste	Beschreibung
5 Sekunden lang drücken	Dadurch wird der ICRL-M neu gestartet, ohne die Konfiguration zu ändern.
Über 10 Sekunden lang drücken	Dadurch werden die werkseitigen Konfigurationswerte einschließlich der IP-Adresse auf dem ICRL-M wiederhergestellt.

Die **Reset**-Taste befindet sich an der Vorderseite des ICRL-M-8RJ45/4SFP-G-DIN oberhalb des **Konsolenports**.

3. Verwendung von PortVision DX

Anmerkung: *Die ICRL-M-16RJ45/4CP-G-DIN und ICRL-M-8RJ45/4SFP-G-DIN werden im Rest dieses Kapitels einfach als ICRL-M bezeichnet.*

Es gibt mehrere Möglichkeiten, Netzwerkinformationen zu konfigurieren. Der technische Support von Pepperl+Fuchs empfiehlt, den ICRL-M an einen PC oder Laptop anzuschließen, auf dem Windows ausgeführt wird, und *PortVision DX* für die Erstkonfiguration zu installieren.

In diesem Abschnitt wird die Verwendung von PortVision DX für die Erstkonfiguration des Netzwerks beschrieben. Außerdem wird erläutert, wie Sie folgende Aktionen durchführen können:

- PortVision DX installieren (Seite 20)
- Netzwerkadresse konfigurieren (Seite 23)
- Firmware- und Bootloader-Version auf dem ICRL-M überprüfen, um vor der Konfiguration sicherzustellen, dass die neuesten Versionen geladen sind (Seite 26)
- Die neueste Version von Firmware und Bootloader herunterladen und sie auf den ICRL-M (Seite 27) hochladen
- Andere PortVision DX-Aufgaben ausführen, z. B.:
  - Firmware auf mehrere ICRL-M-Switches hochladen (Seite 28)
  - Einen neuen RocketLinx (verwaltet oder nicht verwaltet) oder ein Drittanbietergerät zu PortVision DX hinzufügen, um Geräteinformationen in Ihrem Netzwerk zu verwalten (Seite 29)
  - Konfigurationsdateien für die Konfiguration mehrerer Installationen mit denselben Funktionen verwenden (Seite 30)
  - Den LED-Tracker verwenden (Seite 31)
- Organisieren, wie PortVision DX Ihre Pepperl+Fuchs Comtrol Ethernet-angeschlossene Produkte anzeigt (Seite 30)

Optional können Sie die Web-Benutzerschnittstelle oder die CLI verwenden, um diese Aufgaben auf dem ICRL-M auszuführen. Verwenden Sie hierzu die folgenden Unterabschnitte:

- *IP Configuration* auf Seite 40
- *Firmware Upgrade* auf Seite 56
- *Grundeinstellungen (CLI)* auf Seite 180

3.1. PortVision DX-Übersicht

PortVision DX erkennt automatisch Pepperl+Fuchs Comtrol Ethernet-angeschlossene Produkte, die physisch mit dem lokalen Netzwerksegment verbunden sind, sodass Sie die Netzwerkadresse konfigurieren, Firmware hochladen und die folgenden Produkte verwalten können:

- RocketLinx ICRL-M-Switches
- ICDM-RX/TCP-Reihe
- ICDM-RX/EN| EN1| MOD| PN| PN1-Industrial-Gateway-Reihe
- IO-Link-Master (ICE2| ICE3)-Reihe

Neben der Identifizierung von Pepperl+Fuchs Comtrol Ethernet-angeschlossenen Produkten können Sie mit PortVision DX beliebige Drittanbieter-Switches und -Hardware anzeigen, die direkt mit diesen Geräten verbunden sein können. Alle Nicht-Pepperl+Fuchs-Produkte und nicht verwalteten RocketLinx-Switches werden als nicht intelligente Geräte behandelt und verfügen nur über begrenzte Funktionsunterstützung. So können Sie beispielsweise die Firmware eines Drittanbieter-Schalters nicht konfigurieren oder aktualisieren.

3.2. PortVision DX-Anforderungen

Verwenden Sie PortVision DX zum Identifizieren, Konfigurieren, Aktualisieren und Verwalten des ICRL-M unter Windows XP SP3- bis Windows 10-Betriebssystemen, einschließlich Windows Server 2019 (zum Zeitpunkt der Veröffentlichung).

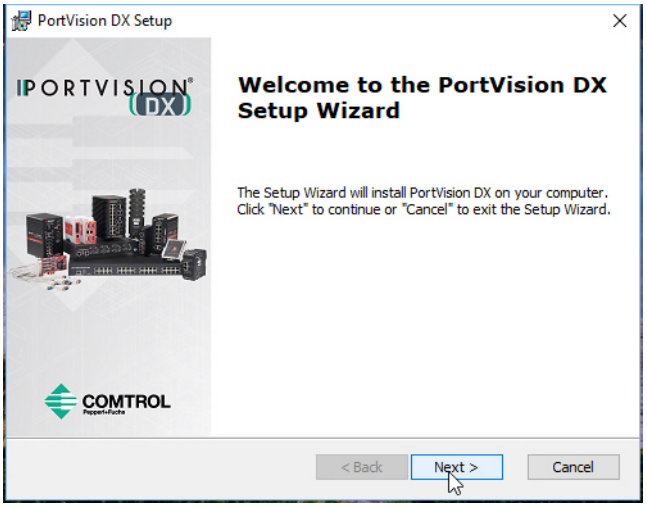
PortVision DX erfordert, dass Sie das Pepperl+Fuchs Comtrol Ethernet-angeschlossene Produkt mit demselben Netzwerksegment verbinden wie das Windows-Hostsystem, wenn Sie es beim Konfigurationsprozess automatisch scannen und lokalisieren möchten.

3.3. Installation von PortVision DX

Während der Erstkonfiguration erkennt und identifiziert PortVision DX automatisch die ICRL-M-Switches, sofern sie sich im selben Netzwerksegment befinden.

Sie können die neueste Version von PortVision DX unter https://www.pepperl-fuchs.com herunterladen.

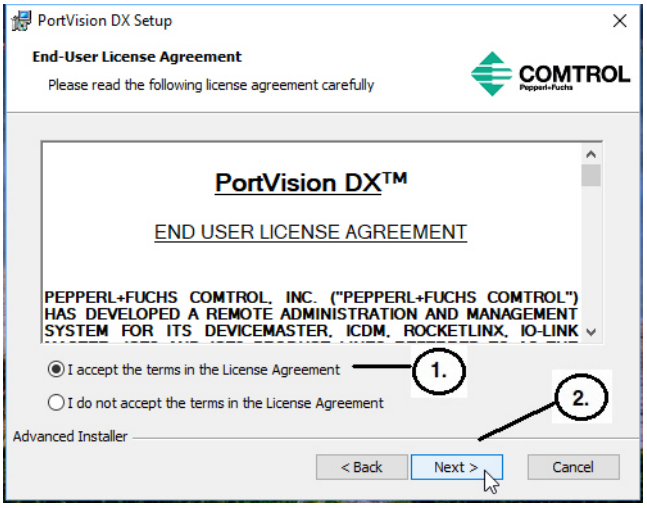
1. Entpacken Sie PortVision DX gegebenenfalls und führen Sie die Datei **PortVision_DX[version].msi** aus.



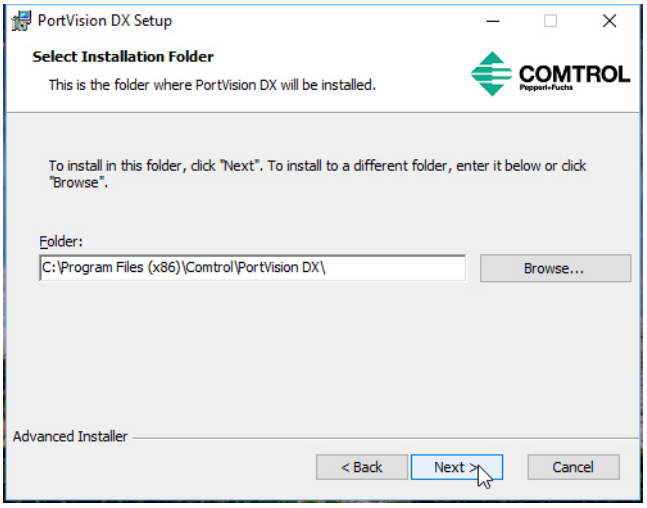
Anmerkung: *Je nach Betriebssystem müssen Sie möglicherweise auf eine Sicherheitswarnung antworten, um den Zugriff zu ermöglichen.*

2. Klicken Sie auf dem Bildschirm *Welcome* auf **Next**.

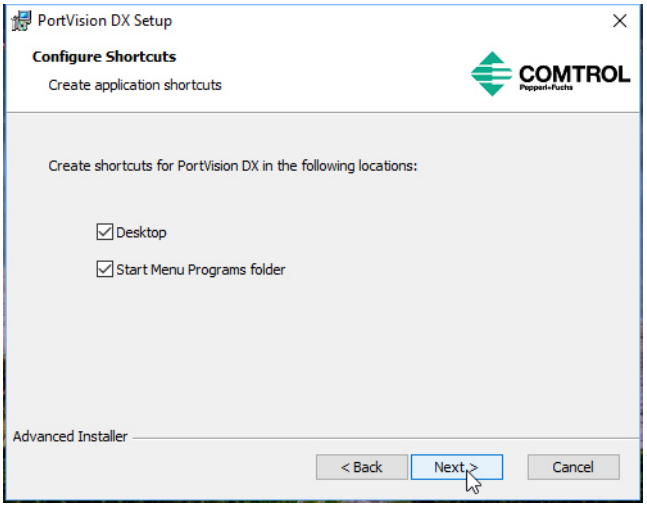
3. Klicken Sie auf **I accept the terms in the License Agreement** und dann auf **Next**.



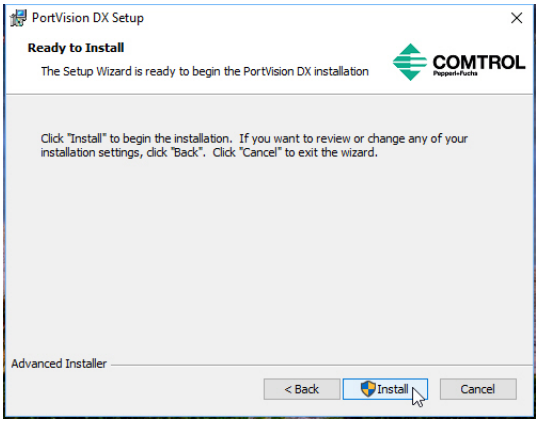
4. Klicken Sie auf **Next** oder navigieren Sie optional zu einem anderen Speicherort und klicken Sie dann auf **Next**.



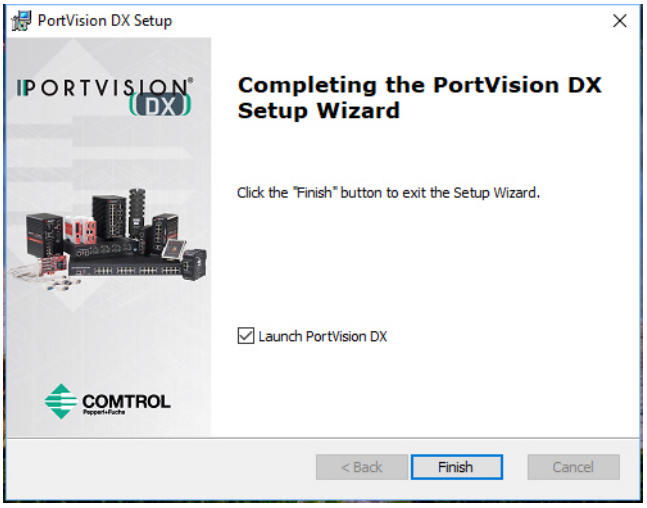
5. Klicken Sie auf **Next**, um die Verknüpfungen zu konfigurieren.



6. Klicken Sie auf **Install**.



7. Je nach Betriebssystem müssen Sie möglicherweise auf **Yes** klicken, um die Frage *Do you want to allow the following program to install software on this computer?* zu beantworten.
8. Klicken Sie auf dem letzten Installationsbildschirm auf **Launch PortVision DX** und auf **Finish**.



9. Je nach Betriebssystem müssen Sie möglicherweise auf **Yes** klicken, um die Frage *Do you want to allow the following program to make changes to this computer?* zu beantworten.
10. Gehen Sie zum nächsten Unterabschnitt, um PortVision DX zur Programmierung der Netzwerkinformationen zu verwenden.

3.4. Konfigurieren der Netzwerkeinstellungen

Der ICRL-M verfügt bei Auslieferung ab Werk über die folgenden Standardwerte:

- IP-Adresse: 192.168.250.250
- Subnetzmaske: 255.255.255.0
- Gateway-Adresse: 192.168.250.1

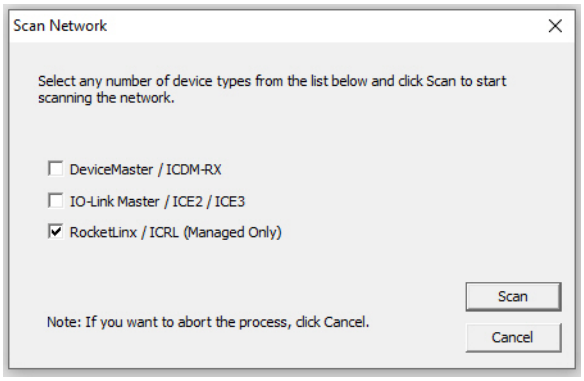
Gehen Sie wie folgt vor, um die Standard-Netzwerkeinstellungen auf dem ICRL-M für Ihr Netzwerk zu ändern.

1. Starten Sie PortVision DX wenn nötig mit der **PortVision DX**-Verknüpfung auf dem Desktop oder klicken Sie unter der Schaltfläche **Start** auf **Pepperl+Fuchs Comtrol > PortVision DX > PortVision DX**.

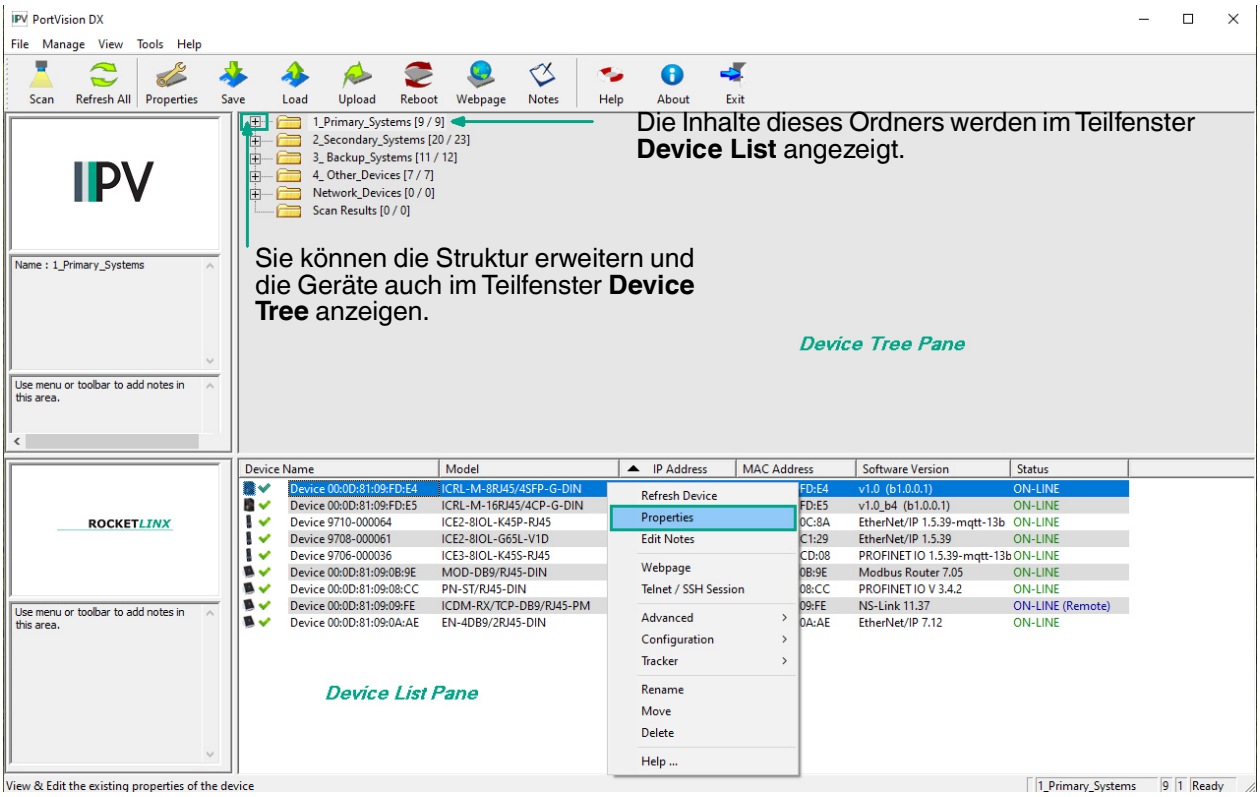
   Anmerkung: *Je nach Betriebssystem müssen Sie möglicherweise die Frage Do you want to allow the following program to make changes to this computer? mit* **Yes** *beantworten.*

2. Klicken Sie in der *Symbolleiste* auf die Schaltfläche **Scan**.
3. Wählen Sie die Pepperl+Fuchs Comtrol Ethernet-angeschlossene Produkte aus, die Sie suchen möchten, und klicken Sie dann auf **Scan**.

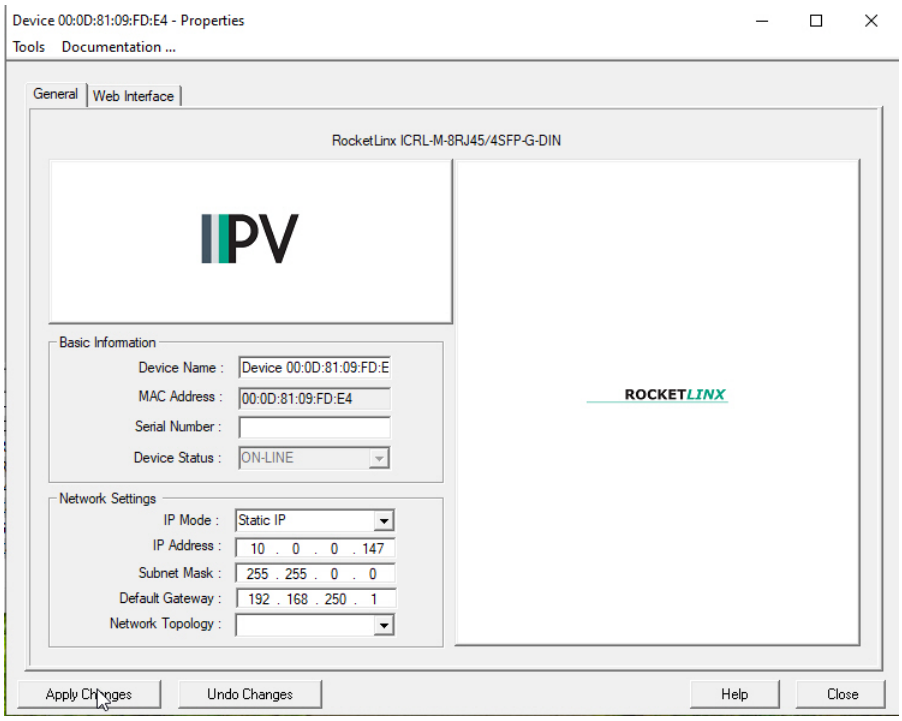
   Anmerkung: *Wenn sich das Pepperl+Fuchs Comtrol Ethernet-angeschlossene Produkt nicht im lokalen Segment befindet und mit einer IP-Adresse programmiert wurde, muss das Pepperl+Fuchs Comtrol Ethernet-angeschlossene Produkt manuell zu PortVision DX hinzugefügt werden.*



4. Markieren Sie den ICRL-M, für den Sie die Netzwerkinformationen programmieren möchten, und öffnen Sie den Bildschirm **Properties** anhand einer der folgenden Methoden.
   - Doppelklicken Sie im Teilfenster *Device Tree* oder *Device List* auf den ICRL-M.
   - Markieren Sie den ICRL-M im Teilfenster *Device Tree* oder *Device List* und klicken Sie auf die Schaltfläche **Properties**.
   - Klicken Sie mit der rechten Maustaste auf den ICRL-M im Teilfenster *Device Tree* oder *Device List* und klicken Sie im Kontextmenü auf **Properties**.
   - Markieren Sie den ICRL-M. Klicken Sie auf das Menü **Manage** und dann auf **Properties**.



5. *Optional:* Benennen Sie den ICRL-M im Feld **Device Name** in einen PortVision DX-Anzeigenamen um. Der Standardname wird als *Device* plus MAC-Adresse angezeigt.



Anmerkung: *Die Felder **MAC Address** und **Device Status** werden automatisch ausgefüllt und Sie können diese Werte nicht ändern.*

6. Geben Sie optional die Seriennummer ein, die auf einem Etikett am ICRL-M steht.
7. Wählen Sie **DHCP IP** oder **Static IP** für den *IP Mode* aus.
   - Wenn Sie **DHCP IP** auswählen, gehen Sie zu Schritt 8.
   - Wenn Sie **Static IP** auswählen:
     - Geben Sie unter **IP Adress** eine eindeutige IP-Adresse für Ihren Standort ein.
     - Geben Sie einen gültigen **Subnet Mask**-Wert für Ihr Netzwerk ein.
     - Geben Sie einen gültigen **Default Gateway**-Wert für Ihr Netzwerk ein.
8. Wählen Sie optional den **Network Topology**-Typ aus, der ein Informationsfeld ist.
9. Klicken Sie auf **Apply Changes**, um die Netzwerkinformationen auf dem ICRL-M zu aktualisieren.

   Anmerkung: *Wenn Sie mehrere ICRL-M-Switches bereitstellen, die gemeinsame Werte verwenden, können Sie die Konfigurationsdatei speichern und diese Konfiguration auf andere ICRL-M-Switches laden. Weitere Informationen finden Sie unter Verwenden von Konfigurationsdateien auf Seite 30.*
10. Klicken Sie auf **Close**, um das Fenster *Properties* zu schließen.
11. Sie sollten überprüfen, ob die neueste Firmware auf dem ICRL-M geladen ist, da eine neuere Version in der Regel Funktionsverbesserungen und Fehlerbehebungen enthält. Siehe *Überprüfen der Firmwareversion* auf Seite 26 und falls erforderlich *Hochladen der neuesten Version von Firmware oder Bootloader* auf Seite 27.
12. Wenn Sie über die neueste Firmware verfügen, können Sie mit der Funktionskonfiguration beginnen. Weitere Informationen finden Sie in einem der folgenden Abschnitte:
    - *Konfiguration – Web-Benutzerschnittstelle* auf Seite 33
    - *Konfiguration – Befehlszeilenschnittstelle (CLI)* auf Seite 162

- Klicken Sie mit der rechten Maustaste auf den ICRL-M im Teilfenster *Device List* und klicken Sie im Pop-up-Menü auf **Webpage**.

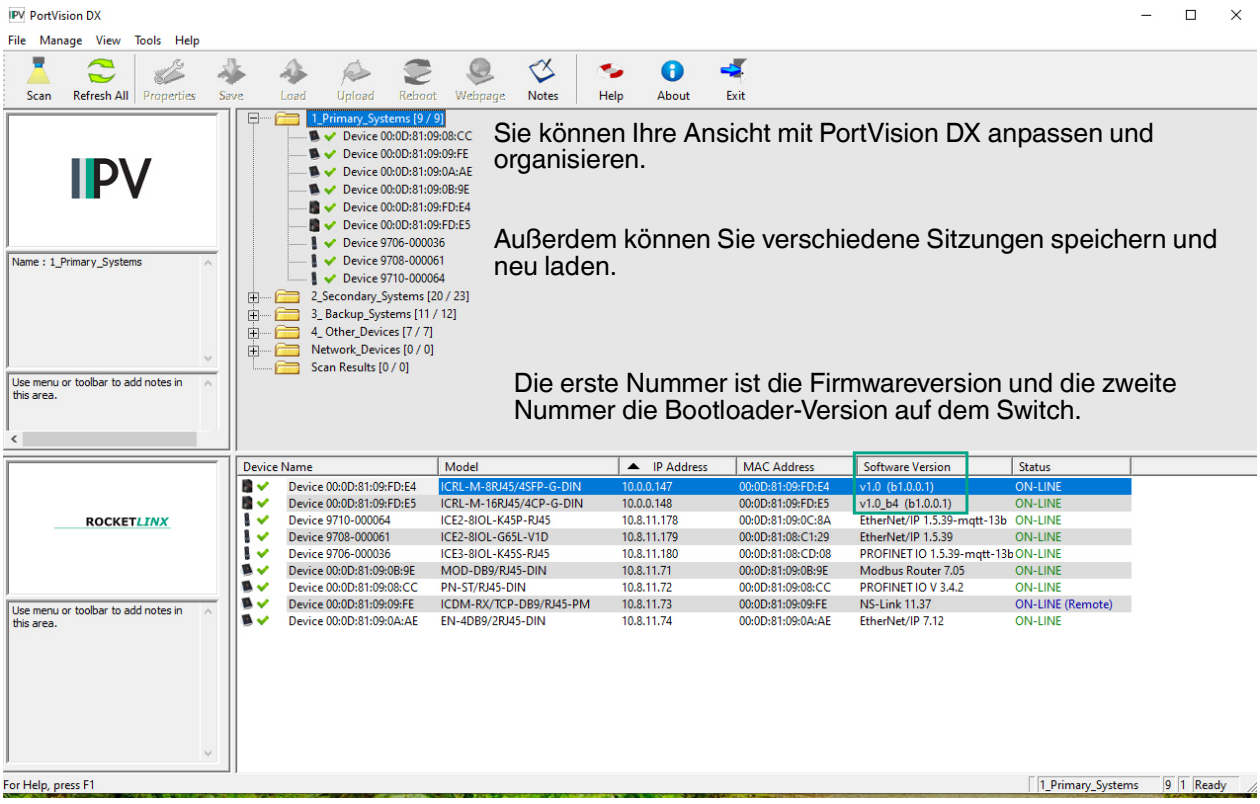
Anmerkung: *Der Standardbenutzername und das -kennwort lauten beide* **admin**.

3.5. Überprüfen der Firmwareversion

Die Überprüfung Ihrer Webschnittstellen- und Bootloader-Versionen ist in PortVision DX ganz einfach.

Pepperl+Fuchs empfiehlt, die neueste Version von Firmware und Bootloader zu laden, damit Sie über die neuesten Funktionsverbesserungen und Fehlerbehebungen verfügen.

1. Wenn der ICRL-M nicht in PortVision DX angezeigt wird, klicken Sie auf die Schaltfläche **Scan**.
2. Wählen Sie den Pepperl+Fuchs Comtrol Ethernet-angeschlossenen Produkt-Typ aus und klicken Sie auf die Schaltfläche **Scan**.
3. Suchen Sie den ICRL-M im Teilfenster *Device List*. Unter *Software Version*: Die erste Zahl gibt die Firmwareversion an, die zweite Zahl zeigt die Bootloader-Version.



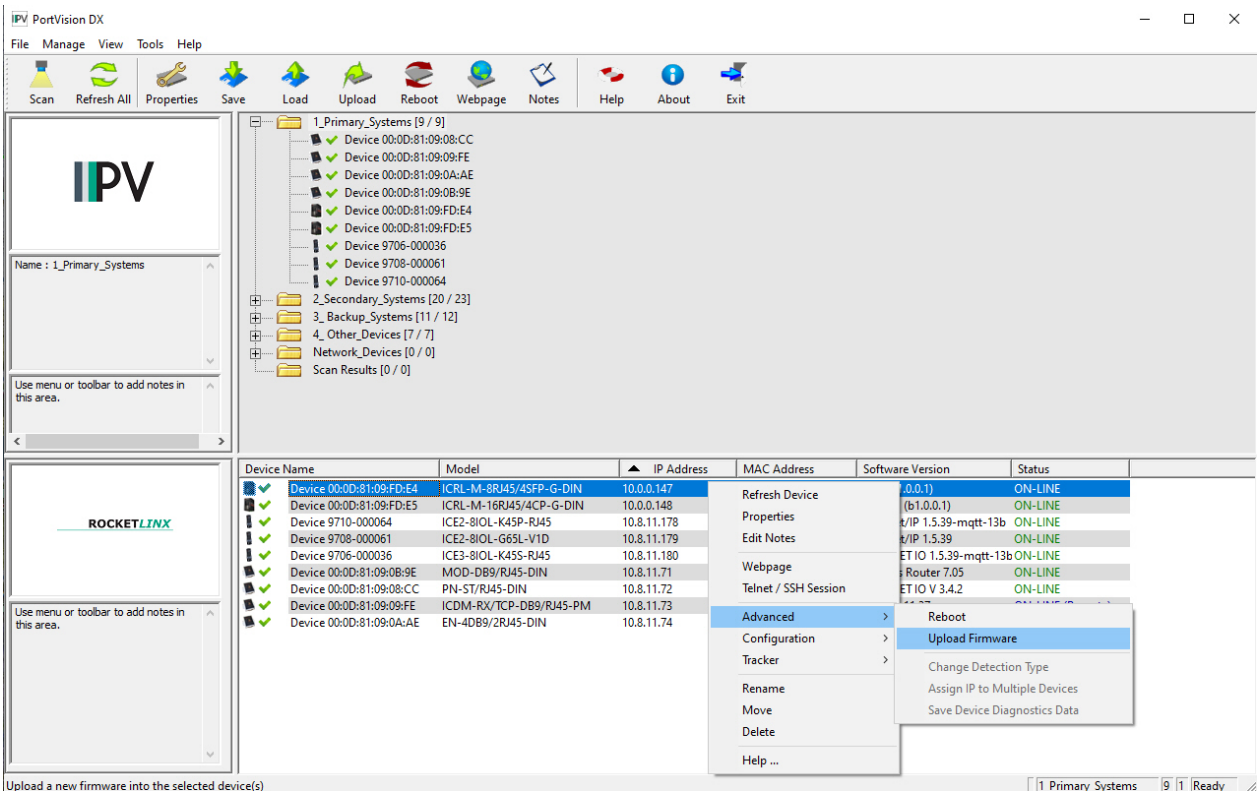
4. Sehen Sie auf https://www.pepperl-fuchs.com nach der neuesten Version von Firmware und Bootloader. Klicken Sie einfach auf Ihren Produkttyp, klicken Sie auf den Link **Software** und vergleichen Sie die aktuelle Version mit der Version auf dem ICRL-M.

Verwenden Sie den nächsten Unterabschnitt für Verfahren zum Hochladen der Firmware (Webschnittstelle) und des Bootloaders.

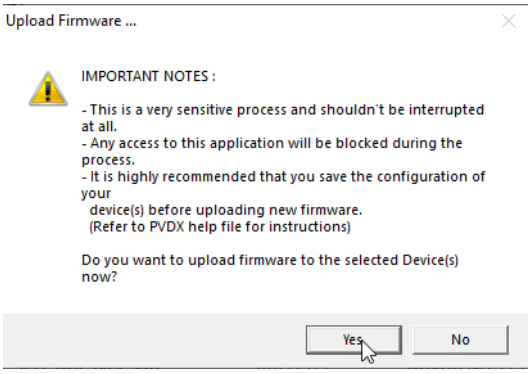
3.6. Hochladen der neuesten Version von Firmware oder Bootloader

Sie können das folgende Verfahren zum Hochladen der neuesten Firmware oder des neuesten Bootloaders verwenden.

1. Wenn Sie dies nicht getan haben, laden Sie die neueste Firmware und den neuesten Bootloader unter Verwendung des vorherigen Unterabschnitts herunter.
2. Klicken Sie im Teilfenster *Device List* mit der rechten Maustaste auf den ICRL-M, den Sie aktualisieren möchten, und klicken Sie auf **Advanced --> Upload Firmware**.



3. Navigieren Sie zum Speicherort der Firmwaredateien, wählen Sie die entsprechende Datei aus und klicken Sie dann auf **Open**.
4. Klicken Sie in der Meldung *Upload Firmware* auf **Yes**.
5. Klicken Sie auf **OK**, um zu bestätigen, dass Sie mit der Verwendung des ICRL-M warten sollen, bis der Status wieder ON-LINE lautet.
6. Klicken Sie mit der rechten Maustaste im Teilfenster *Device List* auf den ICRL-M und dann auf **Refresh**. Optional können Sie auf die Schaltfläche **Refresh** in der *Symbolleiste* klicken, um alle Geräte in PortVision DX zu aktualisieren.
7. Stellen Sie sicher, dass die Versionsänderung unter *Software Version* widergespiegelt wird.



3.7. Hochladen der Firmware auf mehrere ICRL-M-Switches

Sie können dieses Verfahren anwenden, wenn Ihr ICRL-M mit dem Host-PC oder Laptop verbunden ist oder wenn sich der ICRL-M im lokalen Netzwerksegment befindet.

Anmerkung: *Der technische Support empfiehlt nicht, Bootloader auf mehrere ICRL-M-Switches hochzuladen. Denken Sie daran, dass durch das Hochladen der Firmware der ICRL-M neu gestartet wird. Dies kann je nach Netzwerkverbindung dazu führen, dass das Hochladen der Firmware auf einem anderen ICRL-M fehlschlägt.*

1. Wenn der ICRL-M nicht in PortVision DX angezeigt wird, klicken Sie auf die Schaltfläche **Scan**.
2. Wählen Sie den Pepperl+Fuchs Comtrol Ethernet-angeschlossenen Produkt-Typ aus und klicken Sie auf die Schaltfläche **Scan**.
3. Klicken Sie im Bildschirm **Main** bei gedrückter Umschalttaste auf die ICRL-M-Switches, die Sie aktualisieren möchten. Klicken Sie dann mit der rechten Maustaste und anschließend auf **Advanced > Upload Firmware**.
4. Suchen Sie die Firmwaredatei (**.bin**). Klicken Sie auf **Open** (*Please locate the new firmware*) und klicken Sie dann auf **Yes** (*Upload Firmware*).

   Es kann einige Minuten dauern, bis die Firmware auf alle ICRL-M-Switches hochgeladen wurde. Der ICRL-M startet beim Hochladen neu.
5. Klicken Sie in der Hinweismeldung auf **Ok** (gibt vor, dass Sie mit der Verwendung des Geräts warten sollen, bis der Status **ON-LINE** lautet).

Im nächsten Abfragezyklus aktualisiert PortVision DX das Teilfenster *Device List* und zeigt die neue Firmwareversion an.

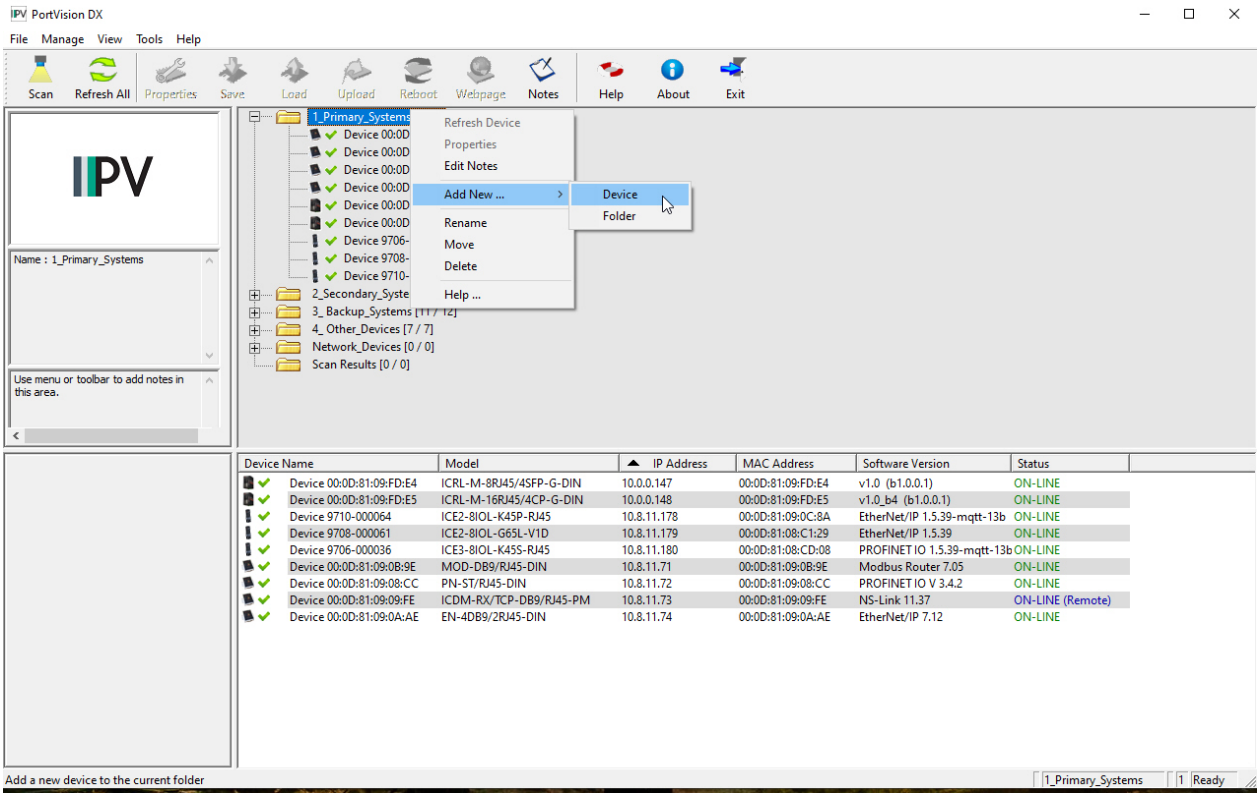
3.8. Neues Gerät in PortVision DX hinzufügen

Sie können einen neuen ICRL-M manuell hinzufügen, wenn Sie das Netzwerk nicht durchsuchen möchten, um ihn zu finden, oder Sie einen ICRL-M vorkonfigurieren möchten, bevor Sie ihn mit dem Netzwerk verbinden. Optional können Sie auch nicht verwaltete Geräte oder RocketLinx-Switches hinzufügen, um Informationen über Geräte im Netzwerk zu verwalten.

Weitere PortVision DX-Informationen zum Hinzufügen von nicht verwalteten RocketLinx-Switches oder Drittanbietergeräten oder -switches finden Sie in der Hilfe.

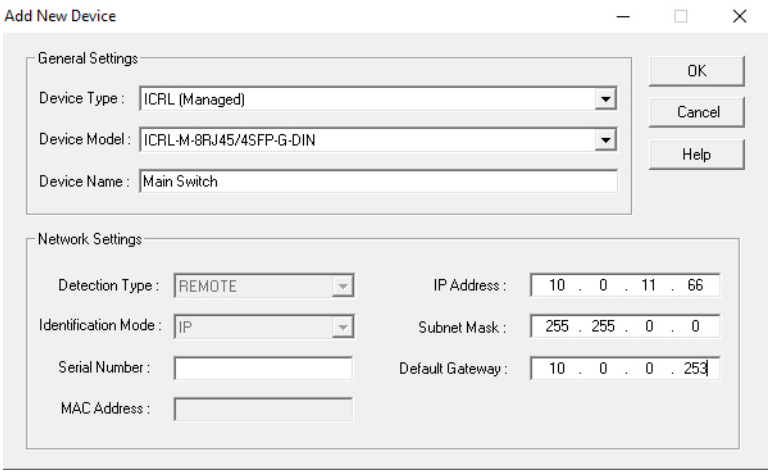
Gehen Sie wie folgt vor, um eine ICRL-M-Remote-Einheit in PortVision DX hinzuzufügen.

1. Öffnen Sie das Fenster *New Device* anhand einer der folgenden Methoden:
   - Klicken Sie im Menü *Manage* auf **Add New > Device**.
   - Klicken Sie mit der rechten Maustaste auf einen Ordner oder RocketLinx-Switch im Teilfenster *Device Tree* und klicken Sie auf **Add New > Device**.



2. Wählen Sie den entsprechenden RocketLinx in der Drop-Down-Liste **Device Type** aus.
3. Wählen Sie das entsprechende Modell in der Drop-Down-Liste **Device Model** aus.
4. Geben Sie einen Gerätenamen in das Listenfeld **Device Name** ein.
5. Geben Sie optional die Seriennummer in das Listenfeld **Serial Number** ein.

6. Geben Sie die IP-Adresse für den ICRL-M ein. Es ist nicht nötig, die Subnetzmaske und das Standard-Gateway einzugeben.
7. Klicken Sie auf **Ok**, um das Fenster *Add New Device* zu schließen. Es kann einige Minuten dauern, bis der ICRL-M gespeichert wird.
8. Klicken Sie bei Bedarf auf **Refresh**, damit der neue RocketLinx im Teilfenster *Device Tree* oder *Device List* angezeigt wird. Der RocketLinx zeigt „OFF-LINE“ an, wenn er nicht mit dem lokalen Netzwerk verbunden ist oder eine falsche IP-Adresse eingegeben wurde.



3.9. Verwenden von Konfigurationsdateien

Wenn Sie mehrere ICRL-M-Switches bereitstellen, die gemeinsame Firmwarewerte verwenden, können Sie die Konfigurationsdatei (.**dc**) über den Bildschirm *Main* in PortVision DX speichern und diese Konfiguration auf andere ICRL-M-Switches laden.

3.9.1. Speichern einer Konfigurationsdatei

Hier wird beschrieben, wie Sie Konfigurationsdateien speichern können.

1. Markieren Sie den ICRL-M im Teilfenster *Device List* und verwenden Sie eine der folgenden Methoden:
   - Klicken Sie auf die Schaltfläche **Save**.
   - Klicken Sie die rechte Maustaste und klicken Sie dann auf **Configuration > Save**.
2. Navigieren Sie zu dem Speicherort, an dem Sie die Datei speichern möchten, geben Sie einen Dateinamen ein und klicken Sie auf **Save**.
3. Klicken Sie auf **OK**, um die Meldung *Save Configuration Completed* zu schließen.

3.9.2. Laden einer Konfigurationsdatei

Gehen Sie wie folgt vor, um eine zuvor gespeicherte ICRL-M-Konfigurationsdatei zu laden. Laden Sie eine Konfigurationsdatei und wenden Sie sie auf die im Teilfenster *Device List* ausgewählten ICRL-M-Switches an.

Gehen Sie wie folgt vor, um eine Konfigurationsdatei über das Teilfenster *Device List* auf einen oder mehrere ICRL-M-Switches zu laden.

1. Markieren Sie im Teilfenster *Device List* die Geräte, die Sie laden möchten, und verwenden Sie eine der folgenden Methoden:
   - Klicken Sie auf die Schaltfläche **Load**
   - Klicken Sie die rechte Maustaste und klicken Sie dann auf **Configuration > Load**.
2. Klicken Sie in der Warnung, dass es 25 Sekunden pro Gerät dauert und die Geräte außerdem möglicherweise neu gestartet werden können, auf **Yes**.
3. Navigieren Sie zum Speicherort der Konfigurationsdatei, klicken Sie auf den Dateinamen (**.dc**) und dann auf **Open**.
4. Schließen Sie die Pop-up-Meldung *Load Configuration*.

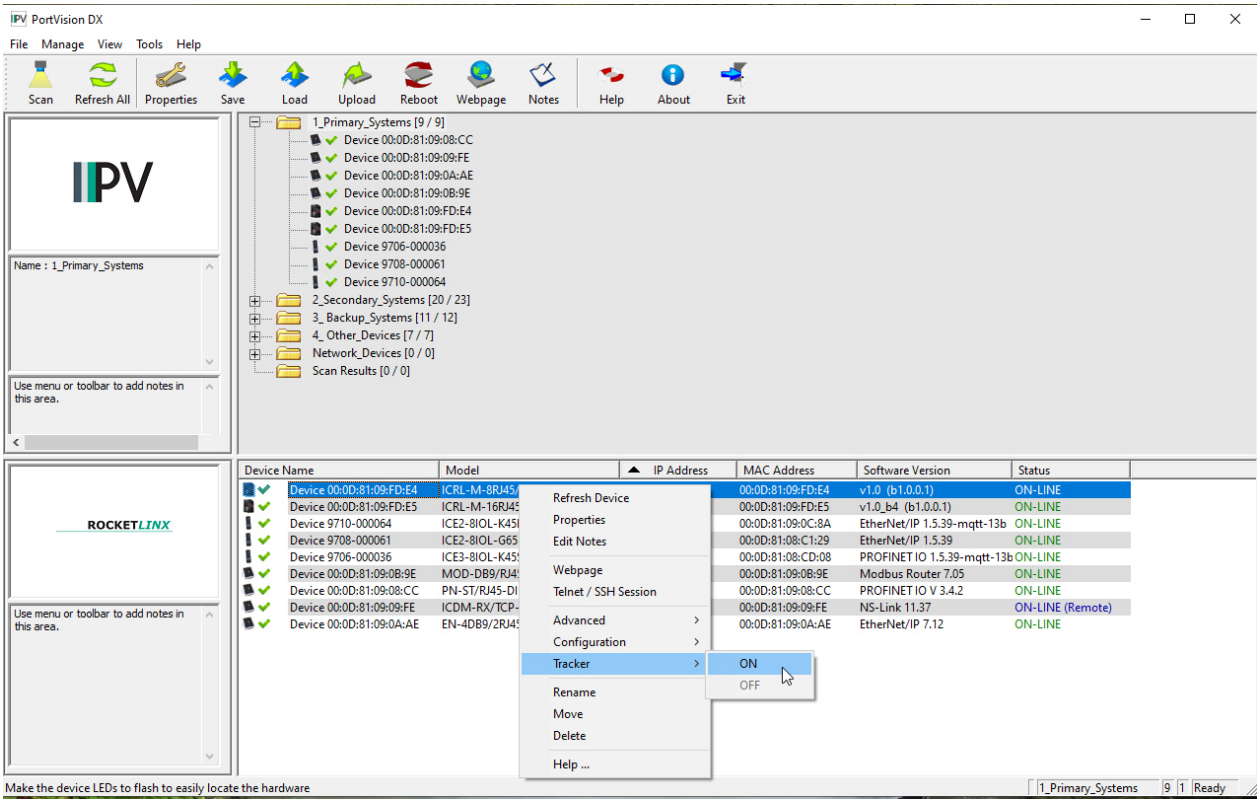
3.10. Verwenden des LED-Trackers

Verwaltete RocketLinx-Switches unterstützen die LED-Tracker-Funktion, mit der Sie die LED an einem bestimmten Gerät ein- und ausschalten können, um die physische Einheit zu lokalisieren.

Gehen Sie wie folgt vor, um die **LED Tracker**-Funktion auf RocketLinx-Switches umzuschalten.

1. Klicken Sie im Teilfenster *Device List* mit der rechten Maustaste auf ICRL-M, klicken Sie auf **Tracker** und dann auf **ON**.

   Die ICRL-M-**SYS**-LED blinkt fünf Sekunden lang.



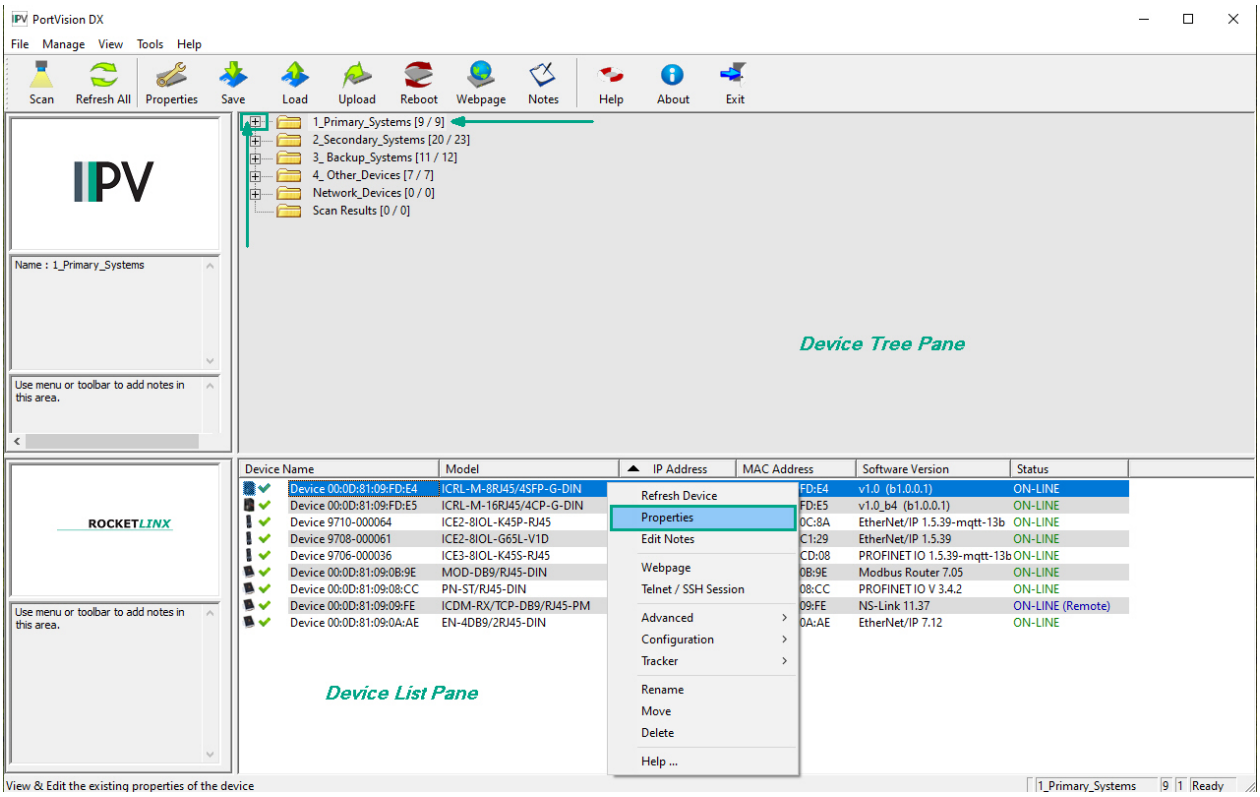
2. Falls erforderlich, müssen Sie möglicherweise mehrmals auf **Tracker** und **ON** klicken, um die blinkende **SYS**-LED zu finden.

3.11. Anpassen von PortVision DX

Sie können anpassen, wie PortVision DX die Geräte anzeigt. Sie können sogar Sitzungen erstellen, die auf bestimmte Zielgruppen zugeschnitten sind. Sie können auch Verknüpfungen zu anderen Anwendungen hinzufügen, indem Sie **Tools > Applications > Customize** wählen.

Im Folgenden wird dargestellt, wie Sie Ihre Ansicht anpassen können.

Ausführliche Informationen zum Ändern der Ansicht finden Sie im PortVision DX-Hilfesystem. Der obige Screenshot zeigt beispielsweise Geräte, die in Ordnern abgelegt sind.



4. Konfiguration – Web-Benutzerschnittstelle

Anmerkung: *Die ICRL-M-16RJ45/4CP-G-DIN und ICRL-M-8RJ45/4SFP-G-DIN werden im Rest dieses Kapitels einfach als ICRL-M bezeichnet.*

Der ICRL-M bietet In-Band- und Out-Band-Konfigurationsmethoden:

- Die In-Band-Verwaltung bedeutet, dass Sie den ICRL-M mithilfe des RS-232-Konsolenkabels und der Befehlszeilenschnittstelle (Command-Line Interface, CLI) für den Zugriff auf den ICRL-M konfigurieren, ohne einen Admin-PC an das Netzwerk anzuschließen. Sie können die Out-Band-Verwaltung verwenden, wenn die Netzwerkverbindung zum ICRL-M unterbrochen wird. CLI und Telnet werden in *Konfiguration – Befehlszeilenschnittstelle (CLI)* auf Seite 162 beschrieben.
- In-Band-Verwaltung bedeutet, dass Sie mittels der ICRL-M-IP-Adresse eine Remote-Verbindung über das Netzwerk herstellen. Sie können eine Remote-Verbindung mit der Web-Benutzerschnittstelle des ICRL-M oder mit einer Telnet-Konsole und der CLI herstellen. Der ICRL-M bietet eine HTTP-Web-Benutzerschnittstelle (Seite 34) für die Webverwaltung.

4.1. Konfigurationsübersicht

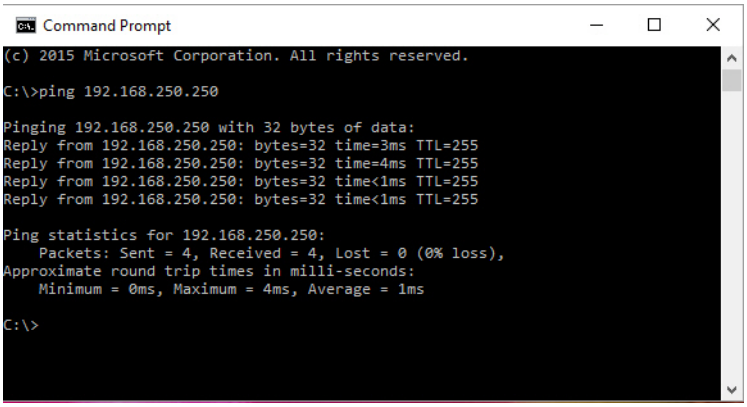
In diesem Unterabschnitt wird die erforderliche Mindestkonfiguration für den Betrieb des ICRL-M beschrieben.

1. Wenn Sie dies nicht bereits getan haben, installieren Sie die Hardware (siehe *Installation der Hardware* auf Seite 9).
2. Wenn Sie die In-Band-Verwaltung verwenden möchten, müssen Sie die ICRL-M-IP-Adresse entsprechend Ihren Netzwerkanforderungen programmieren. Die einfachste Möglichkeit, die IP-Adresse zu konfigurieren, ist die Verwendung eines Windows-Systems sowie PortVision DX (siehe *Konfigurieren der Netzwerkeinstellungen* auf Seite 23).
3. Konfigurieren Sie andere Funktionen nach Bedarf.
   - *Grundeinstellungen* auf Seite 36
   - *Portkonfiguration* auf Seite 60
   - *Netzwerkredundanz* auf Seite 70
   - *VLAN* auf Seite 90 und *Privates VLAN* auf Seite 97
   - *Datenverkehr-Priorisierung* auf Seite 103
   - *Multicast-Filterung* auf Seite 108
   - *SNMP* auf Seite 113
   - *Sicherheit* auf Seite 117
   - *Warnung* auf Seite 143
   - *Überwachung und Diagnose* auf Seite 149
   - *Device Front Panel* auf Seite 157
   - *Speichern (im Flash)* auf Seite 159
   - *Abmelden* auf Seite 160

4.2. Web-Benutzerschnittstelle

Sie können einen beliebigen Standard-Webbrowser verwenden, um den ICRL-M von jedem beliebigen Ort im Netzwerk aus zu konfigurieren und mit ihm zu kommunizieren.

Die Standard-IP-Adresse für den ICRL-M lautet ***192.168.250.250***.



1. Öffnen Sie ein Eingabeaufforderungsfenster und pingen Sie die IP-Adresse des ICRL-M an, um die normale Antwortzeit zu überprüfen.

   Anmerkung: *Wenn Sie die IP-Adresse für Ihr Netzwerk nicht über PortVision DX programmiert haben (Konfigurieren der Netzwerkeinstellungen auf Seite 23), müssen Sie die IP-Adresse Ihres Computers zu* **192.168.250.x** *(Netzwerkmaske: 255.255.255.0) ändern.*

2. Starten Sie den Webbrowser auf dem PC mit einer der folgenden Methoden:
   - Klicken Sie in PortVision DX mit der rechten Maustaste auf den ICRL-M und klicken Sie auf **Webpage**.
   - Öffnen Sie Ihren Browser, geben Sie die IP-Adresse des Switches ein und drücken Sie **Enter**. Beispiel: **http://10.0.0.147**.

   Anmerkung: *Sie müssen ein gültiges Zertifikat laden, um eine HTTPS-Verbindung zu verwenden.*

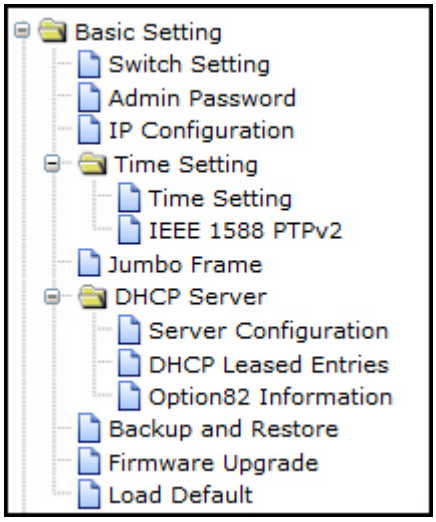
3. Geben Sie den Benutzernamen und das Kennwort ein und klicken Sie auf **OK**. Der Standardbenutzername und das -passwort lauten **admin**.

4. Wenn Sie dies nicht getan haben, können Sie die ICRL-M-IP-Adresse entsprechend Ihrer Netzwerkumgebung ändern.
   a. Doppelklicken Sie auf **Basic Setting**.
   b. Klicken Sie auf **IP Configuration**.
      - Um statische Adressen zu verwenden, geben Sie eine gültige IP-Adresse, Subnetzmaske und ein Standard-Gateway ein.
      - Um DHCP zu verwenden, klicken Sie in der Drop-Down-Liste **DHCP Client** auf **Enable**.
   c. Klicken Sie auf **Apply**.

4.3. Grundeinstellungen

In der Gruppe *Basic Setting* können Sie Switch-Informationen, IP-Adresse und Benutzername/Kennwort des Systems konfigurieren. Außerdem können Sie die Firmware aktualisieren, die Konfiguration sichern und wiederherstellen, die Werkseinstellungen wiederherstellen und das System neu starten.

Die folgenden Webseiten sind in dieser Gruppe enthalten:

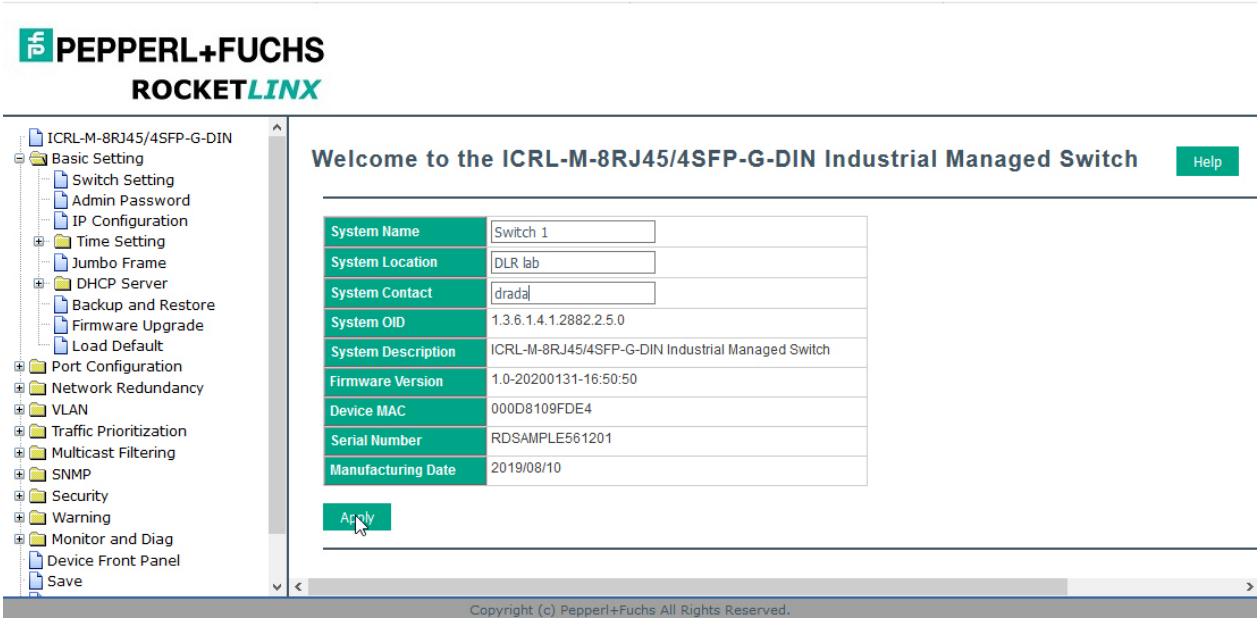


- *Switch Setting* auf Seite 37
- *Admin Password* auf Seite 38
- *IP Configuration* auf Seite 40
- *Time Setting* auf Seite 42
- *Jumbo Frame* auf Seite 46
- *DHCP Server Configuration* auf Seite 48
  - *DHCP Leased Entries* auf Seite 51
  - *Seite „Option82 Information“* auf Seite 52
- *Backup and Restore* auf Seite 54
- *Firmware Upgrade* auf Seite 56
- *Load Default* auf Seite 58

Optional können Sie die Befehlszeilenschnittstelle (Command-Line Interface, CLI) für die Konfiguration verwenden (siehe *Grundeinstellungen (CLI)* auf Seite 180).

4.3.1. Switch Setting

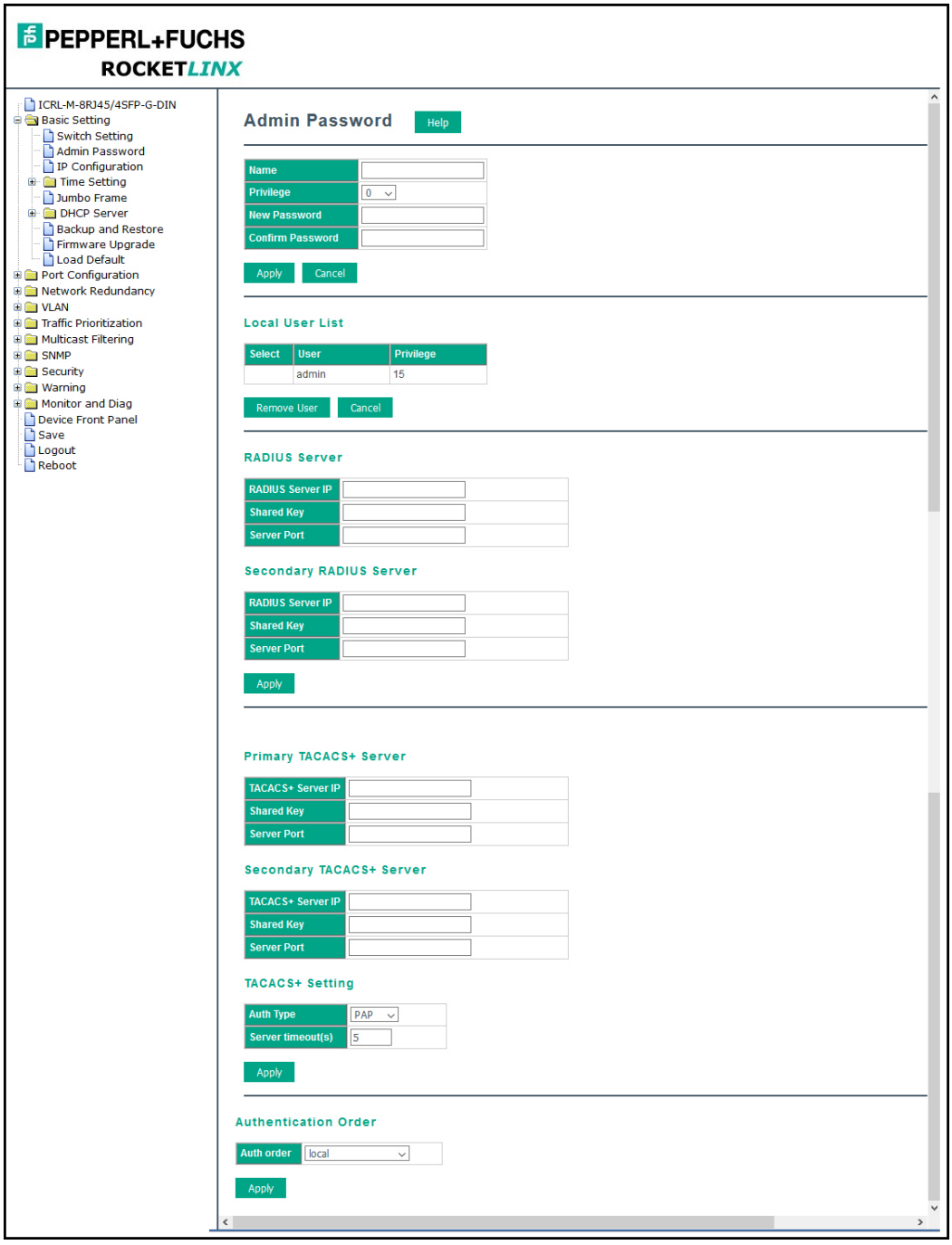
Sie können **Systemname**, **Ort** und **Kontakt** zuweisen und ICRL-M-Informationen anzeigen.



Seite „Switch Setting“	
System Name	Sie können dem ICRL-M einen Namen mit bis zu 64 Zeichen zuweisen. Nachdem Sie den Namen konfiguriert haben, wählt das CLI-System die ersten 12 Zeichen als Namen im CLI-System aus.
System Location	Sie können den physischen Standort des ICRL-M mit bis zu 64 Zeichen angeben.
System Contact	Sie können Kontaktpersonen mit bis zu 64 Zeichen angeben, indem Sie den Namen, die E-Mail-Adresse oder andere Informationen des Administrators eingeben.
System OID	Die SNMP-Objekt-ID des ICRL-M. Sie können dem Pfad folgen, um seine private MIB in einem MIB-Browser zu finden. ***Anmerkung:*** *Wenn Sie versuchen, eine private MIB anzuzeigen, sollten Sie zuerst private MIB-Dateien in Ihren MIB-Browser kompilieren.*
System Description	ICRL-M Industrieller verwalteter Ethernet-Switch
Firmware Version	Zeigt die in diesem ICRL-M installierte Firmwareversion an.
Device MAC	Zeigt eine eindeutige Hardware-Adresse (MAC-Adresse) an, die werkseitig zugewiesen wurde.
Serial Number	Zeigt die Seriennummer des ICRL-M an.
Manufacture Date	Zeigt das Herstellungsdatum an.
Apply	Klicken Sie auf **Apply**, um die Einstellungen anzuwenden. ***Anmerkung:*** *Sie müssen die Einstellungen mit **Save** speichern (Seite 159), wenn Sie diese Einstellungen nach Ausschalten des ICRL-M beibehalten möchten.*

4.3.2. Admin Password

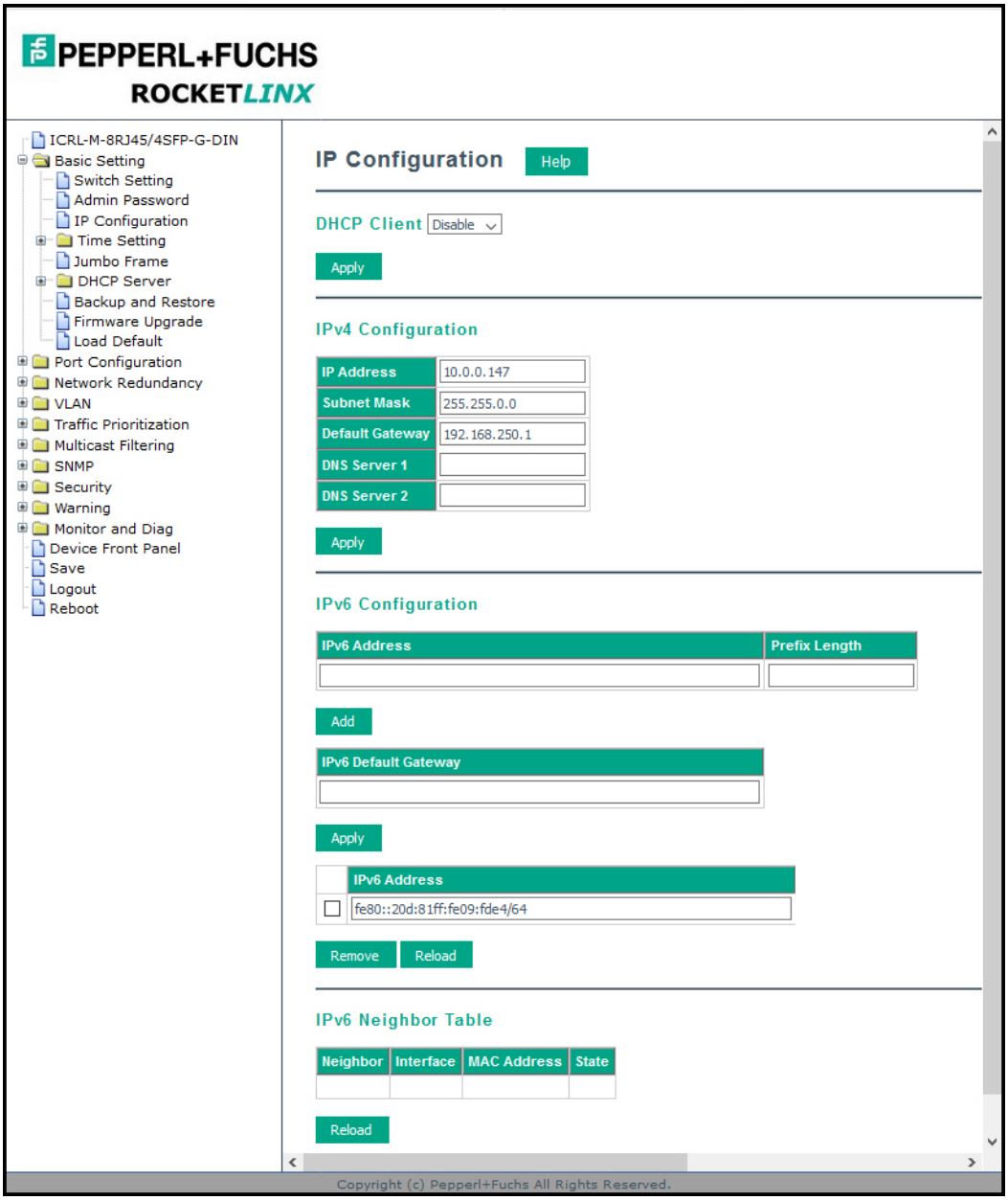
Hier können Sie den Benutzernamen und das Kennwort ändern, um die Sicherheit zu erhöhen.



Seite „Admin Password“	
Administrator	
Name	Hier können Sie einen neuen Benutzernamen eingeben. Der Standardname lautet **admin**.
Privilege	0 oder 15. 0 ist eine schreibgeschützte Berechtigung. 15 ist eine Lese-/Schreibberechtigung.
New Password	Hier können Sie ein neues Kennwort eingeben. Das Passwort im Auslieferungszustand lautet **admin**.
Confirm Password	Sie müssen das neue Kennwort erneut eingeben, um es zu bestätigen.
Local User List	
Select	Klicken Sie auf das Kontrollkästchen und anschließend auf **Remove User**, wenn Sie einen Benutzer entfernen möchten.
RADIUS Server	
RADIUS Server IP	Die IP-Adresse des RADIUS-Servers.
Shared Key	Das Kennwort für die Kommunikation zwischen Switch und RADIUS-Server.
Server Port	Der UDP-Port des RADIUS-Servers.
Secondary RADIUS Server	
RADIUS Server IP	Die IP-Adresse des RADIUS-Servers.
Shared Key	Das Kennwort für die Kommunikation zwischen Switch und RADIUS-Server.
Server Port	Der UDP-Port des RADIUS-Servers.
Primary TACACS+ Server	
TACACS+ Server IP	Die IP-Adresse des primären TACACS+-Servers.
Shared Key	Das Kennwort für die Kommunikation zwischen dem Switch und dem primären TACACS+-Server.
Server Port	Der UDP-Port des primären TACACS+-Servers.
Secondary TACACS+ Server	
TACACS+ Server IP	Die IP-Adresse des sekundären TACACS+-Servers.
Shared Key	Das Kennwort für die Kommunikation zwischen dem Switch und dem sekundären TACACS+-Server.
Server Port	Der UDP-Port des sekundären TACACS+-Servers.
TACACS+ Setting	
Auth Type	Wählen Sie den entsprechenden Authentifizierungstyp aus: ASCII, PAP oder CHAP.
Server timeout(s)	TACACS+-Server-Timeout in Sekunden.
Authentication Order	
Auth Order	Wählen Sie die Reihenfolge für den Benutzeranmeldeprozess: Local, RADIUS --> Local or TACACS+ --> Local. Der Standardwert ist „Local“.
Apply	Klicken Sie auf **Apply**, um die Einstellungen anzuwenden. ***Anmerkung:*** *Sie müssen die Einstellungen mit **Save** speichern (Seite 159), wenn Sie diese Einstellungen nach Ausschalten des ICRL-M beibehalten möchten.*

4.3.3. IP Configuration

Auf dieser Webseite können Sie die IP-Adresseinstellungen des ICRL-M konfigurieren.



Seite „IP Configuration“	
DHCP Client	Sie können die DHCP-Client-Funktion mit **Enable** aktivieren oder mit **Disable** deaktivieren. Wenn die DHCP-Client-Funktion aktiviert ist, wird dem Switch vom DHCP-Server des Netzwerks eine IP-Adresse zugewiesen. In diesem Modus wird die Standard-IP-Adresse durch die vom DHCP-Server zugewiesene IP-Adresse ersetzt. Wenn **DHCP Client** deaktiviert ist, wird die von Ihnen angegebene IP-Adresse verwendet.
IP Address Default: 192.168.250.250	Sie können die IP-Adresse zuweisen, die von Ihrem Netzwerk für den ICRL-M reserviert wurde. Wenn die DHCP-Client-Funktion aktiviert ist, müssen Sie dem ICRL-M keine IP-Adresse zuweisen, da sie vom DHCP-Server überschrieben und hier angezeigt wird.
Subnet Mask Default: 255.255.255.0	Sie können die Subnetzmaske für die IP-Adresse hier zuweisen. Wenn die DHCP-Client-Funktion aktiviert ist, müssen Sie die Subnetzmaske nicht zuweisen. ***Anmerkung:*** *In der Befehlszeilenschnittstelle wird das aktivierte Bit der Subnetzmaske verwendet, um die in der Web-Verwaltungsschnittstelle angezeigte Nummer darzustellen. Beispiel: 8 steht für 255.0.0.0; 16 steht für 255.255.0.0; 24 steht für 255.255.255.0.*
Default Gateway: 192.168.250.1	Sie können das Gateway für den Switch hier zuweisen. ***Anmerkung:*** *Verwenden Sie in der CLI „0.0.0.0/0“, um das Standard-Gateway darzustellen.*
DNS Server 1/2	Das Domain Name System (DNS) ist ein hierarchisches Naming-System, das auf einer verteilten Datenbank für Computer, Dienste oder beliebige andere Ressourcen basiert, die mit dem Internet oder einem privaten Netzwerk verbunden sind. Es ordnet dem Domainnamen, der jeder teilnehmenden Einheit zugewiesen ist, verschiedene Informationen zu. Am wichtigsten ist jedoch, dass Domainnamen in die numerischen Kennungen übersetzt werden, die mit Netzwerkgeräten verbunden sind, um diese Geräte weltweit zu lokalisieren und zu adressieren.
IPv6 Address	Sie können eine IPv6-Adresse für den ICRL-M eingeben. Eine IPv6-Adresse wird in Form von acht Gruppen mit jeweils vier hexadezimalen Ziffern dargestellt, wobei jede Gruppe 16 Bits (zwei Oktette) darstellt. Die Gruppen werden durch Doppelpunkte (:) getrennt und die Länge der IPv6-Adresse beträgt 128 Bits. Die 64-Bit-Schnittstellen-ID wird automatisch aus der MAC-Adresse für den ICRL-M unter Verwendung des geänderten EUI-64-Formats generiert.
Prefix Length	Dieses IPv6-Präfix gibt die Größe eines Netzwerks oder Subnetzes an. Der Standardwert beträgt 64.
IPv6 Default Gateway	Die IPv6-Standard-Gateway-IP-Adresse identifiziert das Gateway (z. B. einen Router), das die Pakete empfängt und weiterleitet, deren Adressen dem lokalen Netzwerk unbekannt sind. Der Agent verwendet die Standard-Gateway-Adresse, wenn er Warnungspakete an die Management-Workstation in einem anderen Netzwerk als dem lokalen Netzwerk sendet.
IPv6 Address	In dieser Tabelle werden die IPv6-Adressen angezeigt, die dem Management-VLAN hinzugefügt wurden. Um einen Eintrag zu entfernen, klicken Sie auf das Kontrollkästchen neben dem Eintrag und anschließend auf die Schaltfläche **Remove**. Um die Liste neu zu laden, klicken Sie auf die Schaltfläche **Reload**.
IPv6 Neighbor Table	
Neighbor	Die *IPv6-Nachbartabelle* listet die Nachbarn des ICRL-M auf.
Interface	Die mit dem Nachbarn verbundene Schnittstelle.
MAC Address	Dies ist die MAC-Adresse des Nachbarn.
State	Dies zeigt den NUD-Status (Neighbor Unreachability Detection) des Nachbareintrags an.
Remove	Klicken Sie auf die Schaltfläche **Remove**, um eine IPv6-Konfiguration oder einen IPv6-Nachbartabelleneintrag zu entfernen.

Seite „IP Configuration“ (Fortsetzung)	
Reload	Klicken Sie auf Schaltfläche **Reload**, um die IPv6-Konfiguration neu zu laden.
Apply	Klicken Sie auf **Apply**, um die Einstellungen anzuwenden. ***Anmerkung:*** *Sie müssen die Einstellungen mit **Save** speichern (Seite 159), wenn Sie diese Einstellungen nach Ausschalten des ICRL-M beibehalten möchten.*

4.3.4. Time Setting

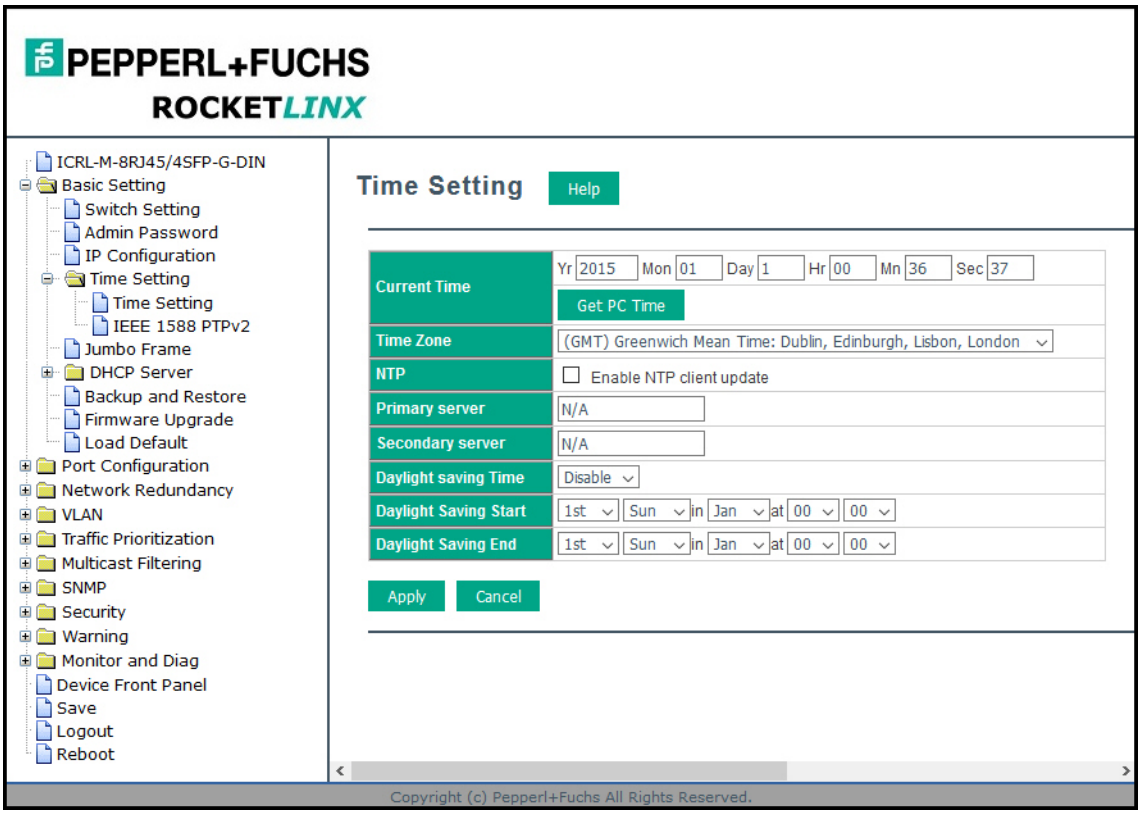
Auf der Seite **Time Setting** können Sie die Uhrzeit manuell oder über den NTP-Server einstellen. Network Time Protocol (NTP) wird verwendet, um Computeruhren im Internet zu synchronisieren. Sie können hier NTP-Einstellungen konfigurieren, um die Uhren mehrerer Switches im Netzwerk zu synchronisieren.

Das IEEE1588 PTP (Precision Time Protocol) unterstützt eine sehr präzise Zeitsynchronisierung in Ethernet-Netzwerken. Es gibt zwei Uhren: Master und Slave. Das Master-Gerät startet in regelmäßigen Abständen einen Austausch von Nachrichten mit Slave-Geräten, damit jeder Slave-Takt die Abweichung zwischen seiner Uhr und der Uhr des Masters neu berechnen kann.

Anmerkung: *Aktivieren Sie nur ein Synchronisierungsprotokoll (PTP/NTP).*

4.3.4.1. Seite „Time Setting“

Mit der Zeiteinstellung können Sie die Uhrzeit manuell oder über einen NTP-Server (Network Time Protocol) einstellen. NTP wird verwendet, um Computeruhren im Internet zu synchronisieren. Sie können hier NTP-Einstellungen konfigurieren, um die Uhren mehrerer Switches im Netzwerk zu synchronisieren. Der ICRL-M bietet auch eine Sommerzeitfunktion.



5/21/20

Seite „Time Setting“	
Current Time	**Manual Setting**: Klicken Sie auf **Get PC Time**, um die Zeiteinstellung des PCs für den ICRL-M abzurufen, oder geben Sie die entsprechenden Informationen in die dafür vorgesehenen Felder ein. **NTP Client**: Klicken Sie auf **Time Setting Source**, wenn Sie möchten, dass der NTP-Client dem ICRL-M die Aktivierung des NTP-Client-Dienstes erlaubt. Der NTP-Client wird automatisch aktiviert, wenn Sie **Time Setting Source** zu **NTP Client** ändern. Das System sendet ein Anfragenpaket, um die aktuelle Uhrzeit vom zugewiesenen NTP-Server abzurufen.
Time Zone	Wählen Sie die Zeitzone aus, in der sich der ICRL-M befindet. In der folgenden Tabelle werden die Zeitzonen für verschiedene Standorte zu Referenzzwecken aufgeführt. Die Standardzeitzone ist GMT (Greenwich Mean Time).
NTP	Klicken Sie auf dieses Kontrollkästchen, um NTP (Network Time Protocol) zu aktivieren.
Primary/Secondary Server	Der primäre Server ist der primäre NTP-Server, für den Sie die Uhrzeit synchronisieren möchten. Der sekundäre Server ist der Backup-NTP-Server, der verwendet werden soll, wenn der primäre Server nicht mehr verfügbar ist.
Daylight Saving Time	Sie können **Daylight Saving Time** aktivieren und dann die **Start**- und **End**-Zeiten für die Sommerzeit festlegen. Während der Sommerzeit liegt die Zeit des ICRL-M eine Stunde vor der tatsächlichen Zeit.
Apply	Klicken Sie auf **Apply**, um die Einstellungen anzuwenden. ***Anmerkung:*** *Sie müssen die Einstellungen mit **Save** speichern (Seite 159), wenn Sie diese Einstellungen nach Ausschalten des ICRL-M beibehalten möchten.*

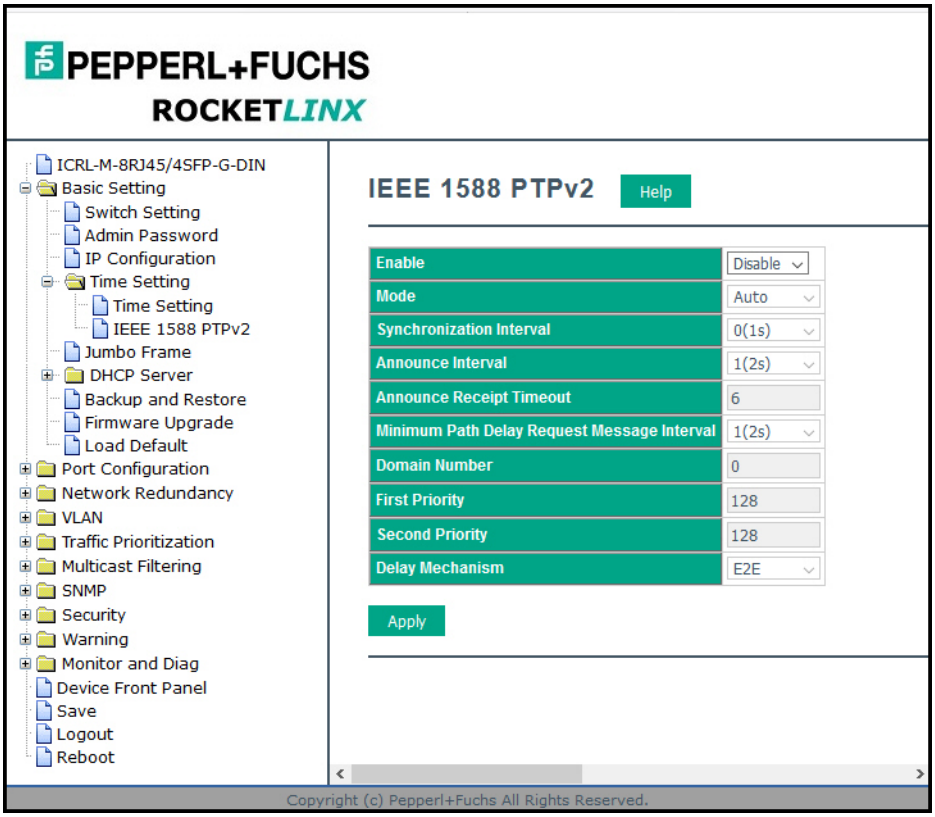
Switch(config)# clock timezone
01 (GMT-12:00) Eniwetok, Kwajalein
02 (GMT-11:00) Midway-Insel, Samoa
03 (GMT-10:00) Hawaii
04 (GMT-09:00) Alaska
05 (GMT-08:00) Pacific Time (USA und Kanada), Tijuana
06 (GMT-07:00) Arizona
07 (GMT-07:00) Mountain Time (USA und Kanada)
08 (GMT-06:00) Mittelamerika
09 (GMT-06:00) Central Time (USA und Kanada)
10 (GMT-06:00) Mexiko-Stadt
11 (GMT-06:00) Saskatchewan
12 (GMT-05:00) Bogota, Lima, Quito
13 (GMT-05:00) Eastern Time (USA und Kanada)
14 (GMT-05:00) Indiana (Ost)
15 (GMT-04:00) Atlantic Time (Kanada)
16 (GMT-04:00) Caracas, La Paz
17 (GMT-04:00) Santiago
18 (GMT-03:00) Neufundland
19 (GMT-03:00) Brasilia
20 (GMT-03:00) Buenos Aires, Georgetown
21 (GMT-03:00) Grönland
22 (GMT-02:00) Mittelatlantik
23 (GMT-01:00) Azoren

24 (GMT-01:00) Kapverdische Inseln
25 (GMT) Casablanca, Monrovia
26 (GMT) Greenwich Mean Time: Dublin, Edinburgh, Lissabon, London
27 (GMT+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien
28 (GMT+01:00) Belgrad, Bratislava, Budapest, Ljubljana, Prag
29 (GMT+01:00) Brüssel, Kopenhagen, Madrid, Paris
30 (GMT+01:00) Sarajevo, Skopje, Sofija, Vilnius, Warschau, Zagreb
31 (GMT+01:00) West-Zentralafrika
32 (GMT+02:00) Athen, Istanbul, Minsk
33 (GMT+02:00) Bukarest
34 (GMT+02:00) Kairo
35 (GMT+02:00) Harare, Pretoria
36 (GMT+02:00) Helsinki, Riga, Tallinn
37 (GMT+02:00) Jerusalem
38 (GMT+03:00) Bagdad
39 (GMT+03:00) Kuwait, Riad
40 (GMT+03:00) Moskau, St. Petersburg, Wolgograd
41 (GMT+03:00) Nairobi
42 (GMT+03:30) Teheran
43 (GMT+04:00) Abu Dhabi, Muscat
44 (GMT+04:00) Baku, Tiflis, Jerewan
45 (GMT+04:30) Kabul
46 (GMT+05:00) Jekaterinburg
47 (GMT+05:00) Islamabad, Karatschi, Taschkent
48 (GMT+05:30) Kalkutta, Chennai, Mumbai, Neu-Delhi
49 (GMT+05:45) Kathmandu
50 (GMT+06:00) Almaty, Nowosibirsk
51 (GMT+06:00) Astana, Dhaka
52 (GMT+06:00) Sri Jayawardenepura
53 (GMT+06:30) Rangun
54 (GMT+07:00) Bangkok, Hanoi, Jakarta
55 (GMT+07:00) Krasnojarsk
56 (GMT+08:00) Peking, Chongqing, Hongkong, Urumqi
57 (GMT+08:00) Irkutsk, Ulan Bator
58 (GMT+08:00) Kuala Lumpur, Singapur
59 (GMT+08:00) Perth
60 (GMT+08:00) Taipeh
61 (GMT+09:00) Osaka, Sapporo, Tokio
62 (GMT+09:00) Seoul
63 (GMT+09:00) Jakutsk
64 (GMT+09:30) Adelaide
65 (GMT+09:30) Darwin
66 (GMT+10:00) Brisbane
67 (GMT+10:00) Canberra, Melbourne, Sydney
68 (GMT+10:00) Guam, Port Moresby
69 (GMT+10:00) Hobart
70 (GMT+10:00) Wladiwostok
71 (GMT+11:00) Magadan, Salomonen, Neukaledonien
72 (GMT+12:00) Auckland, Wellington
73 (GMT+12:00) Fidschi, Kamtschatka, Marshallinseln
74 (GMT+13:00) Nuku'alofa

5/21/20

4.3.5. IEEE 1588 PTPv2

Das IEEE1588 PTP (Precision Time Protocol) unterstützt eine sehr präzise Zeitsynchronisierung in Ethernet-Netzwerken. Es gibt zwei Uhren: Master und Slave. Das Master-Gerät startet in regelmäßigen Abständen einen Austausch von Nachrichten mit Slave-Geräten, damit jeder Slave-Takt die Abweichung zwischen seiner Uhr und der Uhr des Masters neu berechnen kann.

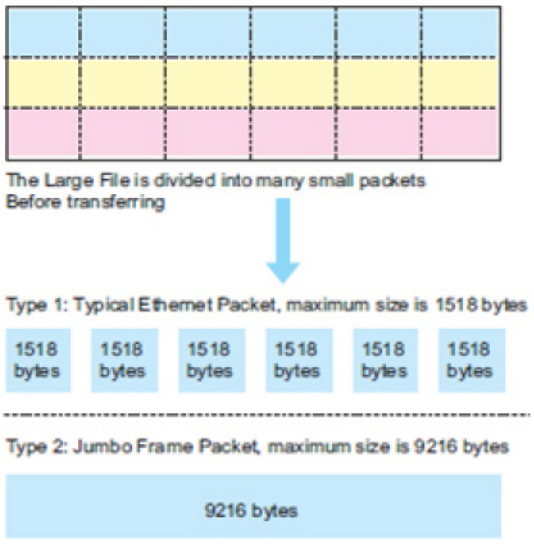


Seite „IEEE 1588 PTPv2“	
Enable	Um IEEE 1588 zu aktivieren, wählen Sie unter **PTP Status** die Option **Enable** und anschließend den Modus **Auto**, **Master** oder **Slave** aus. Nach der Synchronisierung zeigt die Systemzeit die korrekte Zeit des PTP-Servers an.
Mode	• Auto-Modus: Der Switch führt den PTP-Master- und Slave-Modus aus. • Master-Modus: Der Switch agiert nur als PTP-Master. • Slave-Modus: Der Switch agiert nur als PTP-Slave.
Synchronization Interval	Wählen Sie folgende Elemente aus: -3(128ms) -2(256ms) -1(512ms) 0(1s) 1(2s) 2(4s) 3(8s) 4(16s)
Announce Interval	Wählen Sie folgende Elemente aus: 0(1s) 1(2s) 2(4s) 3(8s) 4(16s)
Announce Receipt Timeout	Wählen Sie folgende Werte aus: <2–10>
Minimum Path Delay Request Message Interval	Wählen Sie folgende Werte aus: -1(512ms) 0(1s) 1(2s) 2(4s) 3(8s) 4(16s)
Domain Number	Wählen Sie folgende Werte aus: <0–3>
First Priority	Erste Priorität; wählen Sie folgende Werte aus: <0–255>

Seite „IEEE 1588 PTPv2“ (Fortsetzung)	
Second Priority	Zweite Priorität; wählen Sie folgende Werte aus: <0–255>
Delay Mechanism	E2E: End-to-End PTP: Peer-to-Peer
Apply	Klicken Sie auf **Apply**, um die Einstellungen anzuwenden. ***Anmerkung:*** *Sie müssen die Einstellungen mit **Save** speichern (Seite 159), wenn Sie diese Einstellungen nach Ausschalten des ICRL-M beibehalten möchten.*

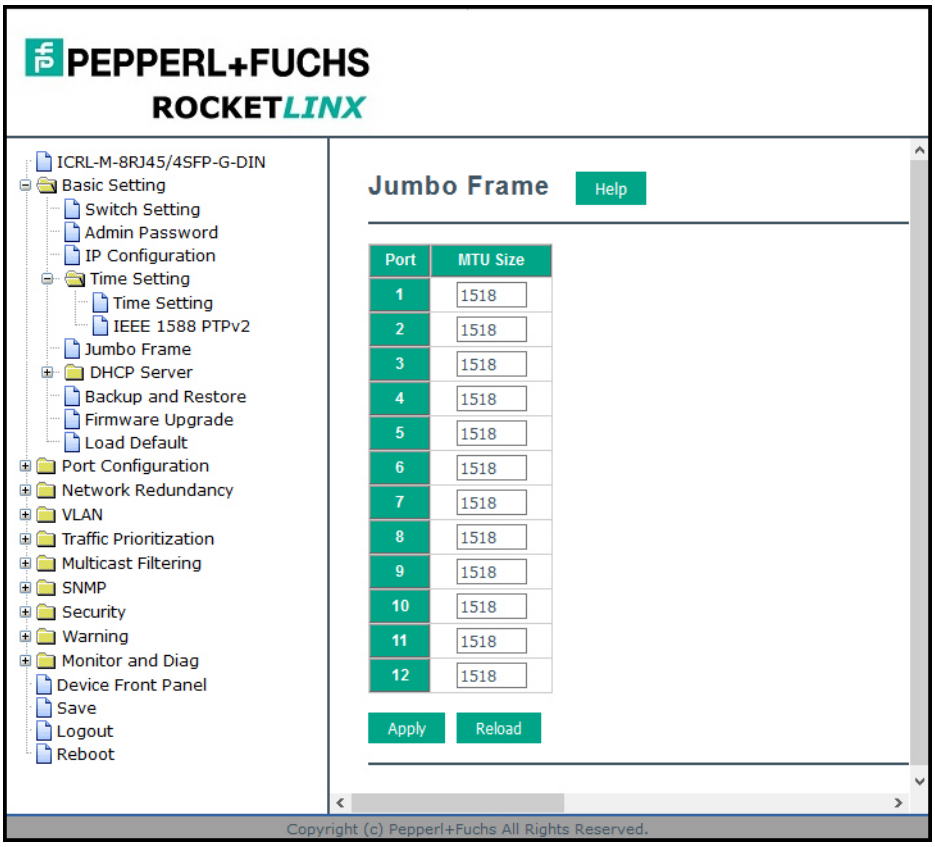
4.3.6. Jumbo Frame

Der typische Ethernet-Frame-Bereich liegt zwischen 64 und 1.500. Mit der Funktion „Jumbo Frame“ kann dieser Switch Ethernet-Frames senden und empfangen, die 64 bis 9.216 Bytes an seinen Schnittstellen verwenden.



Jumbo Frame unterstützt 1.518 (Standard) bis 9.216 Bytes. Dies reicht für allgemeine Anwendungen aus. Wenn Benutzer jedoch große Dateien übertragen möchten, können die Dateien in viele kleine Pakete unterteilt werden. Wenn die Übertragungsgeschwindigkeit langsam wird, kann das Problem durch einen Jumbo-Frame mit langer Größe behoben werden.

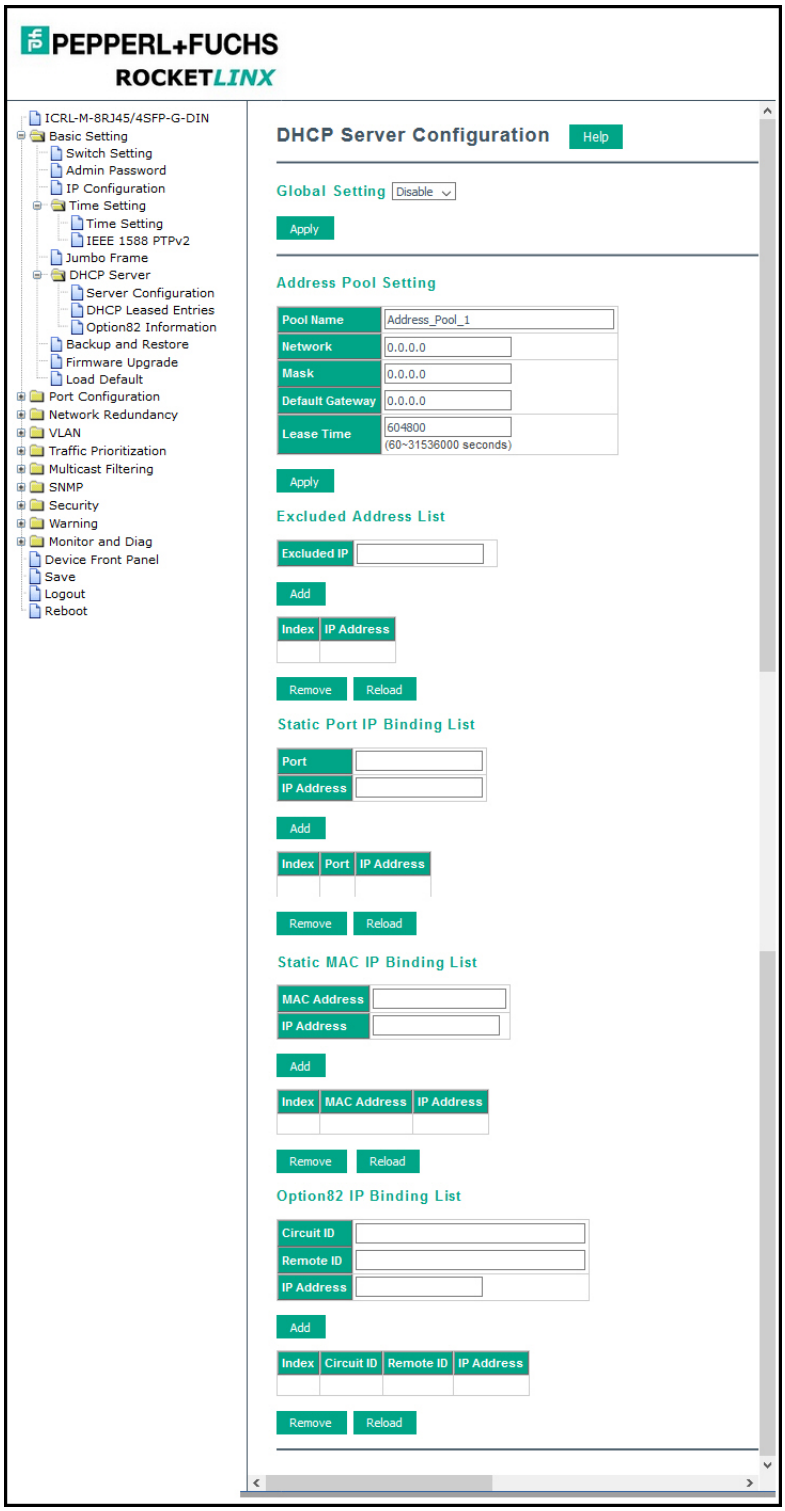
Der ICRL-M ermöglicht Ihnen die Konfiguration der maximalen Übertragungseinheit (Maximal Transmission Unit, MTU). Sie können die MTU-Größe erhöhen, um Jumbo-Frames auf allen Schnittstellen zu unterstützen, indem Sie die Jumbo-Frame-MTU einstellen. Sie können die verfügbare Paketgröße frei ändern.



Jumbo Frame	Beschreibung
MTU Size	Ändern Sie die MTU-Größe für alle Gigabit-Ethernet-Schnittstellen im Switch-Stack. Der Bereich liegt zwischen 1.518 und 9216 Bytes; Standardwert sind 1.518 Bytes.
Apply	Klicken Sie auf **Apply**, um die Einstellungen anzuwenden. ***Anmerkung:*** *Sie müssen die Einstellungen mit **Save** speichern (Seite 159), wenn Sie diese Einstellungen nach Ausschalten des ICRL-M beibehalten möchten.*
Reset	Klicken Sie auf **Reset**, um die MTU auf den Standardwert zurückzusetzen.

4.3.7. DHCP Server Configuration

Auf dieser Seite können Sie DHCP-Serverservices konfigurieren.



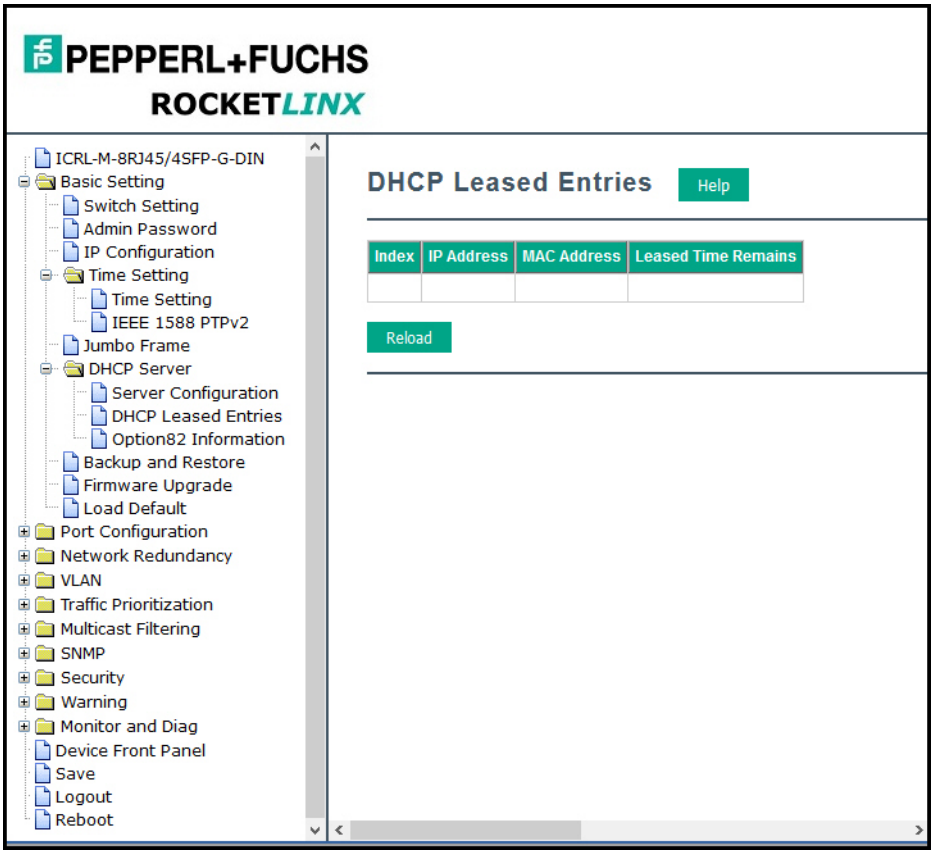
5/21/20

Seite „DHCP Server Configuration“	
Global Setting	Sie können die DHCP-Server-Funktion mit **Enable** aktivieren oder mit **Disable** deaktivieren. Der ICRL-M weist Link-Partnern eine neue IP-Adresse zu.
Apply	Klicken Sie auf **Apply**, um die Einstellungen anzuwenden. ***Anmerkung:*** *Sie müssen die Einstellungen mit **Save** speichern (Seite 159), wenn Sie diese Einstellungen nach Ausschalten des ICRL-M beibehalten möchten.*
Address Pool Setting	
Pool Name	Geben Sie einen Poolnamen ein.
Network	Geben Sie die IPv4-Adresse für den DHCP-Server ein.
Subnet Mask	Geben Sie die Subnetzmaske für den DHCP-Server ein.
Default Gateway	Geben Sie die IP-Gateway-Adresse für den DHCP-Server ein.
Lease Time	Geben Sie die Leasing-Zeit in Sekunden für den Client ein.
Excluded Address List	
Excluded IP	Sie können eine bestimmte Adresse in das Feld **Excluded IP** für die reservierte IP-Adresse des DHCP-Servers eingeben. Die in der **Excluded Address List Table** aufgeführten IP-Adressen sind den Netzwerkgeräten nicht zugewiesen. Fügen Sie eine IP-Adresse zur **Excluded Address List** hinzu, oder entfernen Sie sie, indem Sie auf **Add** oder **Remove** klicken. ***Anmerkung:*** *Standardmäßig wird nur die Überschrift der Tabelle angezeigt, bis eine IP-Adresse in das Feld **Excluded IP** eingegeben und über die Schaltfläche **Add** hinzugefügt wird.*
Static Port/IP Binding List	
Port	Geben Sie die Client-Portnummer für den DHCP-Server ein.
IP Address	Geben Sie die Client-IP-Adresse für den DHCP-Server ein. Nachdem Sie die Portnummer und die IP-Adresse eingegeben haben, klicken Sie auf **Add**. Klicken Sie zum Entfernen eines Ports und der zugehörigen IP-Adresse auf **Remove**. Klicken Sie auf **Reload**, um die ausgewählten Port- und IP-Adresseinträge neu zu laden. ***Anmerkung:*** *Standardmäßig wird nur die Überschrift der Tabelle angezeigt, bis Informationen in die Felder **Port** und **IP Address** eingegeben und über die Schaltfläche **Add** hinzugefügt werden.*
Static MAC/IP Binding List	

Seite „DHCP Server Configuration“ (Fortsetzung)	
IP Address	Der ICRL-M bietet eine Funktion zum Binden und Entfernen von IP-Adressen. Geben Sie die angegebene IP-Adresse ein und klicken Sie dann auf **Add**, um eine neue IP-Bindungsregel für einen bestimmten Link-Partner, wie eine SPS, oder ein beliebiges Gerät ohne **DHCP Client**-Funktion hinzuzufügen. Um eine IP-Adresse aus der Liste der manuellen Bindungen zu entfernen, markieren Sie die Regel und klicken Sie auf **Remove**.
MAC Address	Der ICRL-M bietet eine Funktion zum Binden und Entfernen von MAC-Adressen. Geben Sie die angegebene IP-Adresse ein und klicken Sie dann auf **Add**, um eine neue MAC-Bindungsregel für einen bestimmten Link-Partner, wie eine SPS, oder ein beliebiges Gerät ohne **DHCP Client**-Funktion hinzuzufügen. Das Format der MAC-Adresse lautet **xxxx.xxxx.xxxx**. Um eine MAC-Adresse aus der Liste der statischen MAC-/IP-Bindungen zu entfernen, markieren Sie die Regel und klicken Sie auf **Remove**. ***Anmerkung:*** *Standardmäßig wird nur die Überschrift der Tabelle angezeigt, bis Informationen in die Felder* **IP Address** *und* **MAC Address** *eingegeben und über die Schaltfläche* **Add** *hinzugefügt werden.*
Option82/IP Binding List	
Circuit ID	Die Circuit-ID der IP-Adresskonfiguration von Option82.
Remote ID	Die Remote-ID der IP-Adresskonfiguration von Option82. Klicken Sie nach der Eingabe der IP-Adresse, der Circuit-ID und der Remote-ID auf **Add**. Klicken Sie auf die Schaltfläche **Remove**, um die ausgewählten Einträge in der IP-Adressentabelle von Option82 zu entfernen. Klicken Sie auf die Schaltfläche **Reload**, um die ausgewählten Einträge in der IP-Adressentabelle von Option82 neu zu laden.
IP Address	Konfiguration der Option82-IP-Adresse: unterstützt vollständig die DHCP-Relay-Funktion. Die IP-Adresse der IP-Adresskonfiguration von Option82. ***Anmerkung:*** *Standardmäßig wird nur die Überschrift der Tabelle angezeigt, bis Informationen in die Felder* **Circuit ID, Remote ID** *und* **IP Address** *eingegeben und über die Schaltfläche* **Add** *hinzugefügt werden.*

4.3.8. DHCP Leased Entries

Der ICRL-M stellt eine Tabelle bereit, in der die zugewiesenen IP-Adressen angezeigt werden.

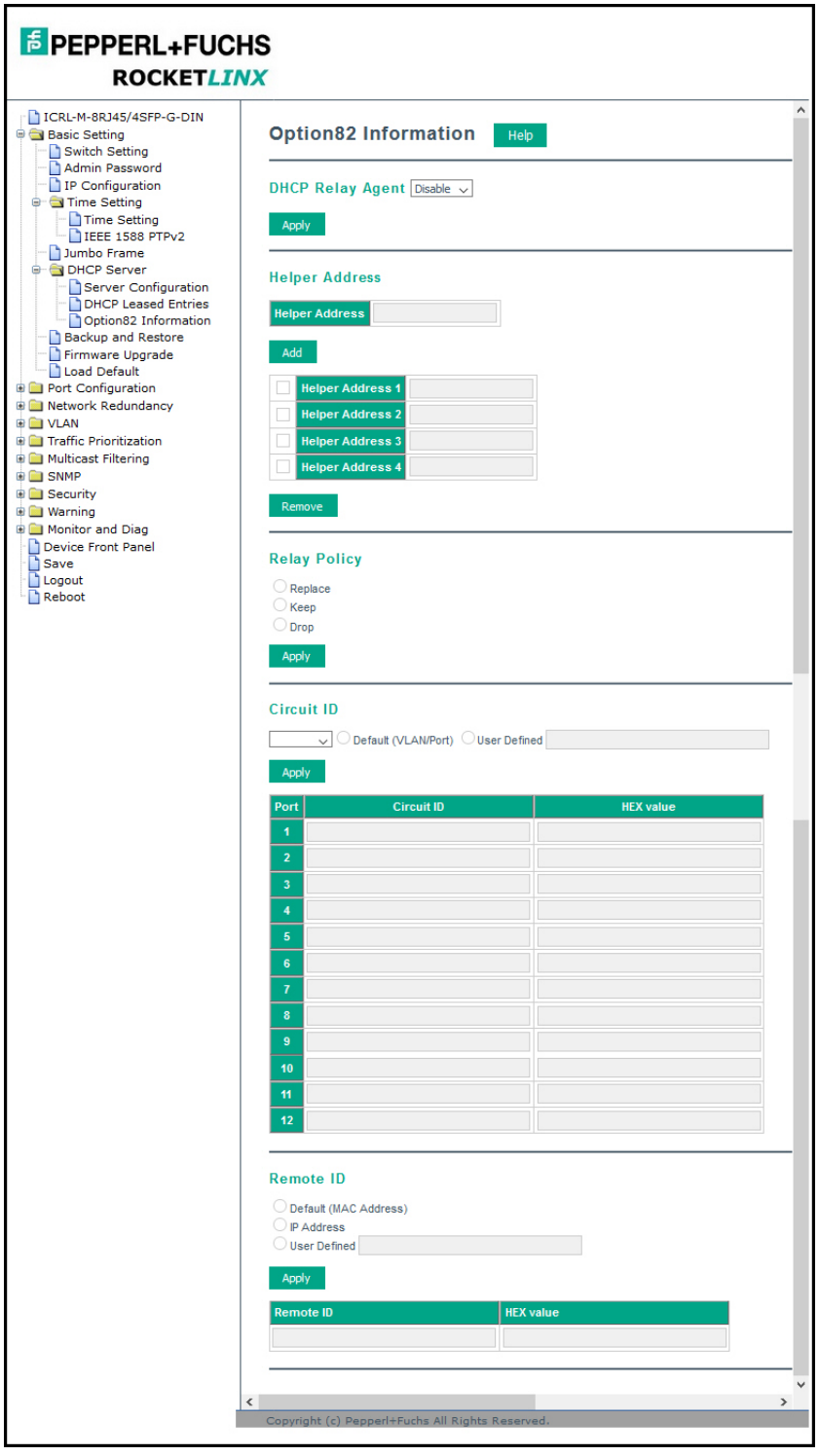


Seite „DHCP Leased Entries“	
Index	Index der DHCP-Lease-Einträge.
IP Address	Die IP-Adresse des Lease-Eintrags.
MAC Address	Die MAC-Adresse des Lease-Eintrags.
Lease Time(s)	Die Lease-Zeit des Lease-Eintrags (in Sekunden).
Reload	Klicken Sie hier, um DHCP-Lease-Einträge neu zu laden.

Anmerkung: *Standardmäßig wird nur die Überschrift der Tabelle angezeigt, bis Daten zur Anzeige verfügbar sind.*

4.3.9. Seite „Option82 Information“

In diesem Unterabschnitt wird die Seite *Option82 Information* behandelt.



5/21/20

Anmerkung: *Sie müssen die Einstellungen mit **Save** speichern (Seite 159), damit diese Einstellungen nach Ausschalten des ICRL-M beibehalten werden.*

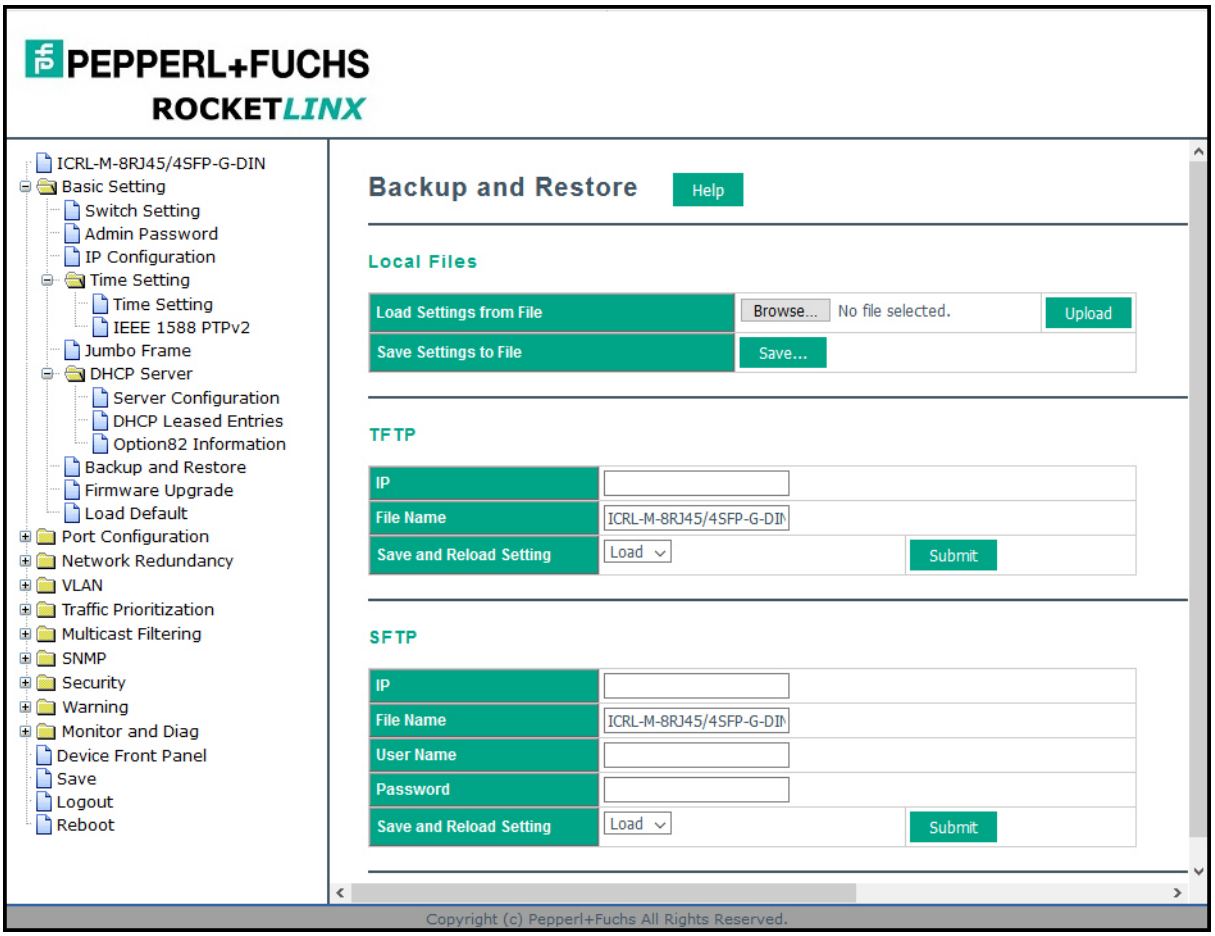
Seite „Option82 Information“	
DHCP Relay Agent	Sie können die Funktion **DHCP Option82 Relay**, die Link-Partnern eine neue IP-Adresse zuweist, mit **Enable** aktivieren oder mit **Disable** deaktivieren.
Helper Address	
Helper Address	Geben Sie die DHCP-Serveradresse für den Relay-Agent ein und klicken Sie auf **Add**. Die Helper-Adressen werden in der folgenden Tabelle angezeigt.
Helper-Address 1–4	DHCP-Serveradressen für den Relay-Agent.
Relay Policy	• **Replace**: Ersetzt das vorhandene Option82-Feld und fügt das neue Option82-Feld hinzu. Dies ist die Standardeinstellung, wenn der DHCP-Relay-Agent aktiviert ist. • **Keep**: Behält das ursprüngliche Option82-Feld bei und leitet es an den Server weiter. • **Drop**: Löscht das Option82-Feld und fügt kein Option82-Feld hinzu.
Circuit ID	• **Default**: Standardwert der Circuit-ID. • **Port**: Port des Switches. • **Circuit ID**: Die Circuit-ID enthält spezifische Informationen zu dem Schaltkreis, über den die Anfrage eingegangen ist. Es handelt sich um eine Kennung, die spezifisch für den Relay-Agent ist, sodass die Art des Anschlusses je nach Relay-Agent variiert.
Remote ID	• **Default**: Standardwert der Remote-ID. • **IP Address**: IP-Adresse des Switches. • **Remote ID**: Die Remote-ID überträgt Informationen über das Ende des Schaltkreises des Remote-Hosts, also die MAC-Adresse des Relays.

4.3.10. Backup and Restore

Sie können die Option **Backup** verwenden, um die aktuelle Konfiguration, die im ICRL-M-Flashspeicher abgelegt ist, auf einem PC oder Laptop, Ihrem TFTP-Server oder einem SFTP-Server zu speichern.

So können Sie die Option **Restore** verwenden, um eine Konfigurationsdatei in den ICRL-M zu laden oder die gespeicherten Einstellungen auf einen anderen ICRL-M zu laden. Bevor Sie eine Konfigurationsdatei wiederherstellen können, müssen Sie zuerst die Backup-Konfigurationsdatei auf einem lokalen System, TFTP- oder SFTP-Server speichern. Der ICRL-M kann diese Datei dann wieder in den Flashspeicher herunterladen.

Die ICRL-M-Konfigurationsdatei ist eine Standardtextdatei. Sie können die Datei mit WordPad oder dem Editor öffnen. Sie können auch die Datei ändern, die Konfigurationseinstellungen hinzufügen/entfernen und dann die Datei wieder in den ICRL-M laden.



Optional können Sie zum Sichern und Wiederherstellen von Konfigurationsdateien PortVision DX verwenden.

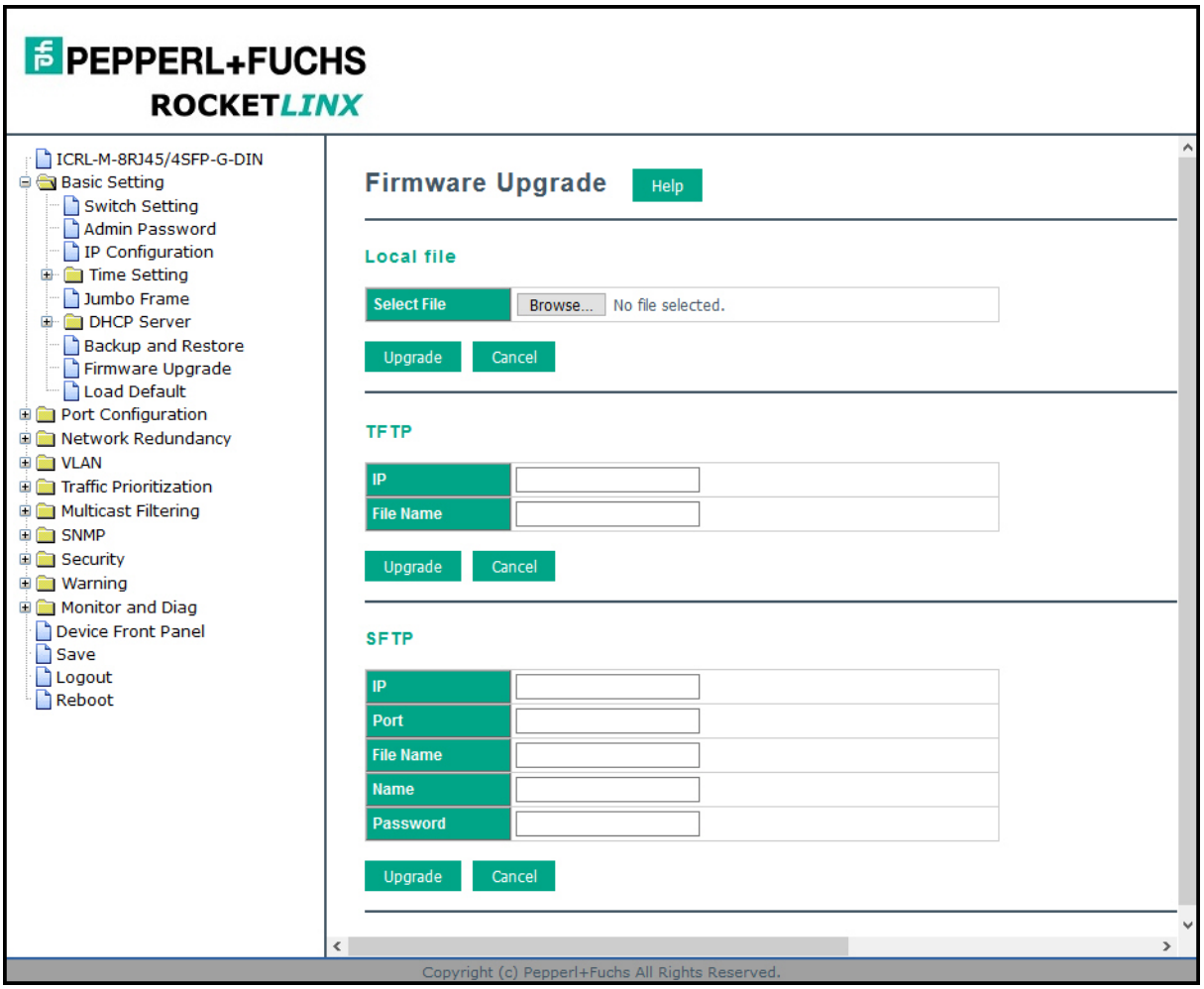
Seite „Backup and Restore“	
Local Files	In diesem Modus fungiert der Switch als Fileserver. Sie können den Zielordner durchsuchen und dann den Dateinamen eingeben, um die Konfiguration zu sichern. Sie können auch den Zielordner durchsuchen und eine vorhandene Konfigurationsdatei auswählen, um die Konfiguration wieder in den ICRL-M zu laden. Dieser Modus wird nur von Web-Benutzerschnittstelle bereitgestellt. **Load Settings from File**: Klicken Sie auf die Schaltfläche **Browse**, um die zuvor gespeicherte Sicherungskonfigurationsdatei auszuwählen. Nachdem Sie die Konfigurationsdatei gefunden haben, klicken Sie auf die Schaltfläche **Upload**. **Save Settings to File**: Klicken Sie auf die Schaltfläche **Save**, um die Konfigurationsdatei zu speichern. ***Anmerkung:*** *Wenn Sie die falsche Datei auswählen, wird die gesamte Konfiguration übersprungen.*
TFTP	In diesem Modus fungiert der ICRL-M als TFTP-Client. Stellen Sie zunächst sicher, dass Ihr TFTP-Server bereit ist. Geben Sie die IP-Adresse des TFTP-Servers und den Namen der Sicherungskonfigurationsdatei ein. Dieser Modus kann sowohl in der CLI als auch über Web-Benutzerschnittstelle verwendet werden. **IP**: Dies ist die IP-Adresse des TFTP-Servers, auf dem Ihre Konfigurationsdatei bereits gespeichert wurde oder gespeichert werden kann. **File Name**: Dies ist der Dateiname der zu speichernden Konfigurationsdatei. **Load/Save Settings**: Wählen Sie **Load**, um die Konfiguration vom TFTP-Server auf den Switch zu laden. Klicken Sie auf **Submit**, um die Konfiguration zu laden oder zu speichern.
SFTP	In diesem Modus fungiert der Switch als SFTP-Client. Stellen Sie zunächst sicher, dass Ihr SFTP-Server bereit ist. Geben Sie die IP-Adresse des SFTP-Servers und den Namen der Sicherungskonfigurationsdatei ein. Dieser Modus kann sowohl in der CLI als auch über Web-Benutzerschnittstelle verwendet werden. **IP**: Dies ist die IP-Adresse des SFTP-Servers, auf dem Ihre Konfigurationsdatei bereits gespeichert wurde oder gespeichert werden kann. **File Name**: Dies ist der Dateiname der zu speichernden Konfigurationsdatei. **User Name**: Fügen Sie den Benutzernamen für SFTP ein. **Password**: Geben Sie das SFTP-Kennwort ein. **Load/Save Settings**: Wählen Sie **Load**, um die Konfiguration vom SFTP-Server auf den Switch zu laden. Klicken Sie auf **Submit**, um die Konfiguration zu laden oder zu speichern.

- Der ICRL-M stellt eine Standardkonfigurationsdatei im ICRL-M bereit. Um die Standardkonfigurationsdatei zu laden, können Sie den Befehl **Reset** auf der Seite *Load Default* auf Seite 58 oder den Befehl **Reload** in der CLI (Seite 185) verwenden.
- Sie können die CLI verwenden, um die neuesten Einstellungen anzuzeigen, die auf dem ICRL-M aktiv sind. Die Informationen sind die Einstellungen, die Sie konfiguriert, aber noch nicht im Flash gespeichert haben. Die Einstellungen müssen im Flash gespeichert werden, damit sie nach dem Wiedereinschalten verfügbar sind. Verwenden Sie den Befehl **running-config**, um die Konfigurationsdatei anzuzeigen (siehe *Aktive Konfiguration anzeigen* auf Seite 185).
- Nachdem Sie die **running-config** im Flash gespeichert haben, werden die neuen Einstellungen beibehalten und funktionieren nach dem Aus- und Wiedereinschalten. Verwenden Sie die Option **show startup-config**, um sie in der CLI anzuzeigen. Mit dem Befehl **Backup** kann nur die Konfigurationsdatei auf Ihrem PC oder TFTP-Server gesichert werden.

4.3.11. Firmware Upgrade

Verwenden Sie diesen Bereich, um die Firmware des ICRL-M auf die neueste Version zu aktualisieren. Pepperl+Fuchs stellt die neueste Firmware auf https://www.pepperl-fuchs.com bereit. Aktualisierte Firmware kann neue Funktionen, Fehlerbehebungen oder andere Softwareänderungen umfassen. Der technische Support von Pepperl+Fuchs empfiehlt Ihnen, die neueste Firmware anzuwenden, bevor Sie den ICRL-M an einem Kundenstandort installieren.

Anmerkung: *Optional können Sie PortVision DX verwenden, um die neueste Firmware hochzuladen. Wenn Sie eine neue Version des Bootloaders hochladen müssen, müssen Sie PortVision DX oder die CLI verwenden. Sie können zum Hochladen des Bootloaders nicht die Web-Benutzerschnittstelle verwenden.*



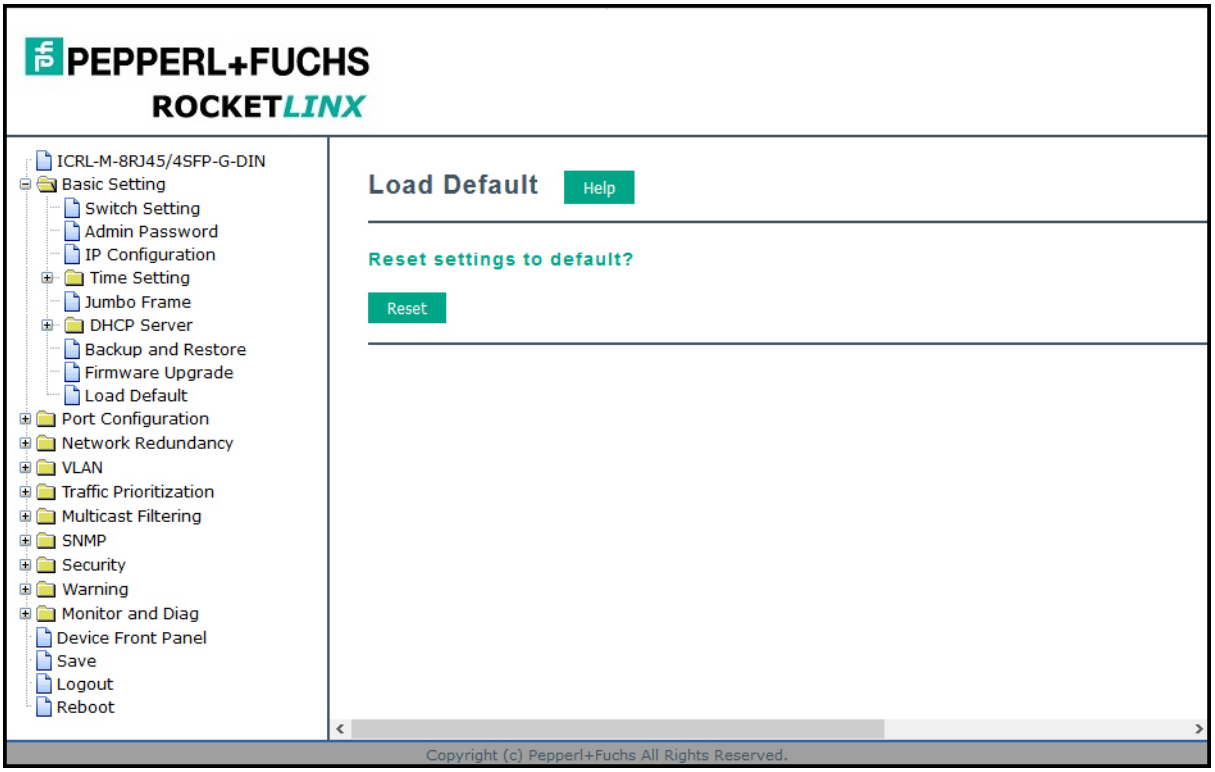
Seite „Firmware Upgrade“	
Local File	Mit dieser Option können Sie ein Firmware-Image hochladen, das lokal auf Ihrem Computer gespeichert ist. **Select File**: Wählen Sie ein Firmware-Image auf Ihrem Computer aus. Klicken Sie auf **Upgrade**, um mit der Aktualisierung der Firmware zu beginnen. Klicken Sie auf **Cancel**, um die ausgewählte Datei zu löschen. Nachdem die Firmware aktualisiert wurde, wird der Switch automatisch neu gestartet. Möglicherweise sollten Sie die verbundenen Netzwerkbenutzer daran erinnern, bevor Sie diese Funktion ausführen.
TFTP	Mit dieser Option können Sie ein Firmware-Image hochladen, das auf einem TFTP-Server gespeichert ist. **IP**: Dies ist die IP-Adresse des TFTP-Servers, auf dem Ihr Firmware-Image gespeichert ist. **File Name**: Dies ist der Dateiname des Firmware-Image. Klicken Sie auf **Upgrade**, um mit der Aktualisierung der Firmware zu beginnen. Klicken Sie auf **Cancel**, um die ausgewählte Datei zu löschen. Nachdem die Firmware aktualisiert wurde, wird der Switch automatisch neu gestartet. Möglicherweise sollten Sie die verbundenen Netzwerkbenutzer daran erinnern, bevor Sie diese Funktion ausführen.
SFTP	Mit dieser Option können Sie ein Firmware-Image hochladen, das auf einem SFTP-Server gespeichert ist. **IP**: Dies ist die IP-Adresse des SFTP-Servers, auf dem Ihr Firmware-Image gespeichert ist. **Port**: Geben Sie die TCP-Portnummer ein. **File Name**: Dies ist der Dateiname des Firmware-Image. **Name**: Fügen Sie den Benutzernamen für SFTP ein. **Password**: Geben Sie das SFTP-Kennwort ein. Klicken Sie auf **Upgrade**, um mit der Aktualisierung der Firmware zu beginnen. Klicken Sie auf **Cancel**, um die ausgewählte Datei zu löschen. Nachdem die Firmware aktualisiert wurde, wird der Switch automatisch neu gestartet. Möglicherweise sollten Sie die verbundenen Netzwerkbenutzer daran erinnern, bevor Sie diese Funktion ausführen.

4.3.12. Load Default

Sie können die ICRL-M-Konfigurationswerte, ausgenommen der Netzwerkinformationen, auf die Standardeinstellungen zurücksetzen. Optional können Sie die *Reset-Taste* auf Seite 18 verwenden, die auch die IP-Adresse auf die Standardkonfigurationswerte zurücksetzt.

Anmerkung: *Sie können auch PortVision DX verwenden, um den Switch auf die Standardkonfigurationswerte zurückzusetzen (mit Ausnahme der Netzwerkeinstellungen).*

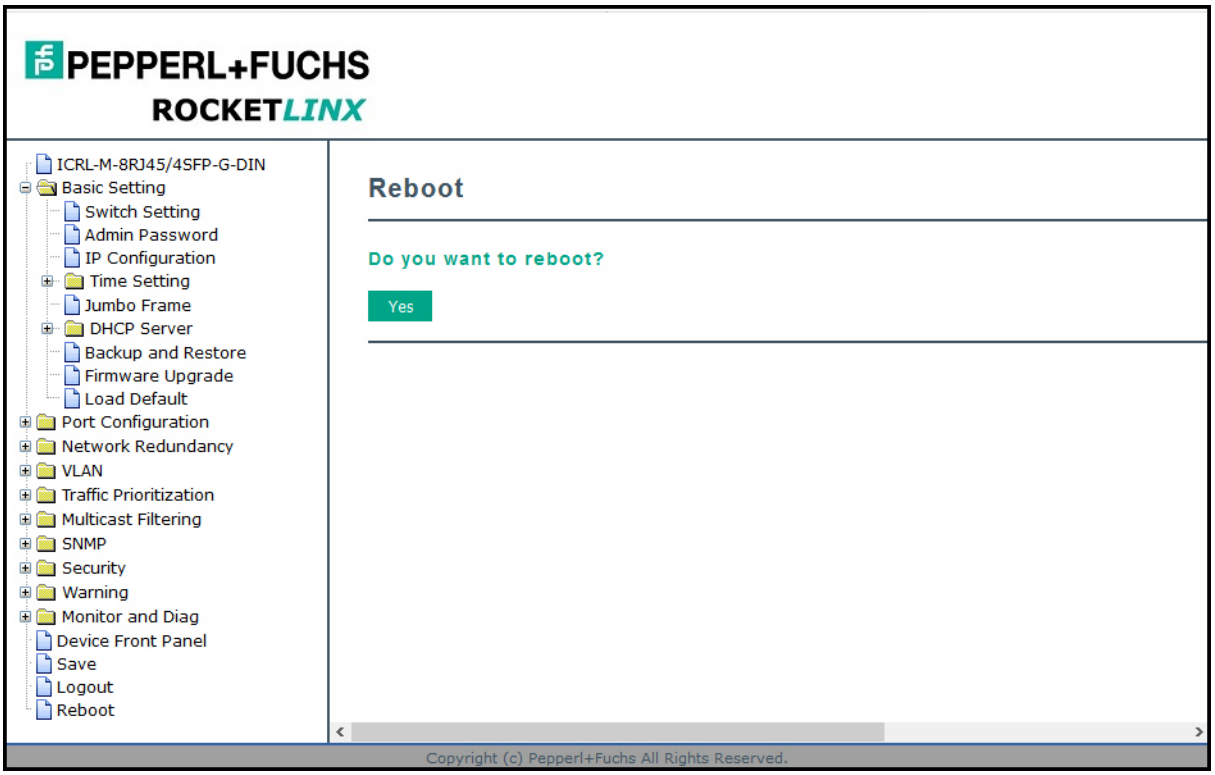
1. Klicken Sie auf die Schaltfläche **Reset**, wenn der ICRL-M alle Konfigurationen auf die Werkseinstellungen zurücksetzen soll.



   Das System zeigt nach Abschluss des Vorgangs ein Popup-Fenster an. Die Standardeinstellungen funktionieren nach dem Neustart des ICRL-M.

2. Klicken Sie in der Popup-Meldung auf **OK**, um die Konfiguration auf die Standardeinstellungen zurückzusetzen.
3. Klicken Sie im Fenster *Please reboot the switch to reload default settings except IP address* auf **OK**.

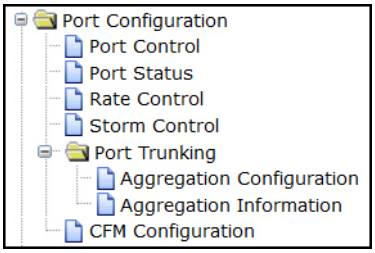
4. Rufen Sie die Seite **Reboot** auf und klicken Sie auf die Schaltfläche **Yes**.



4.4. Portkonfiguration

Mit der Gruppe *Port Configuration* können Sie den Portstatus aktivieren/deaktivieren oder die automatische Portaushandlung, Geschwindigkeit, Duplexfunktion, Flusssteuerung, Port-Aggregationseinstellungen (Port-Trunking) und die Ratenbeschränkung konfigurieren. Außerdem können Sie hier Portstatus- und Aggregationsinformationen anzeigen. Die folgenden Seiten sind in dieser Gruppe enthalten:

- *Port Control*
- *Port status* auf Seite 62
- *Rate Control* auf Seite 64
- *Storm Control* auf Seite 65
- *Port Trunking* auf Seite 66



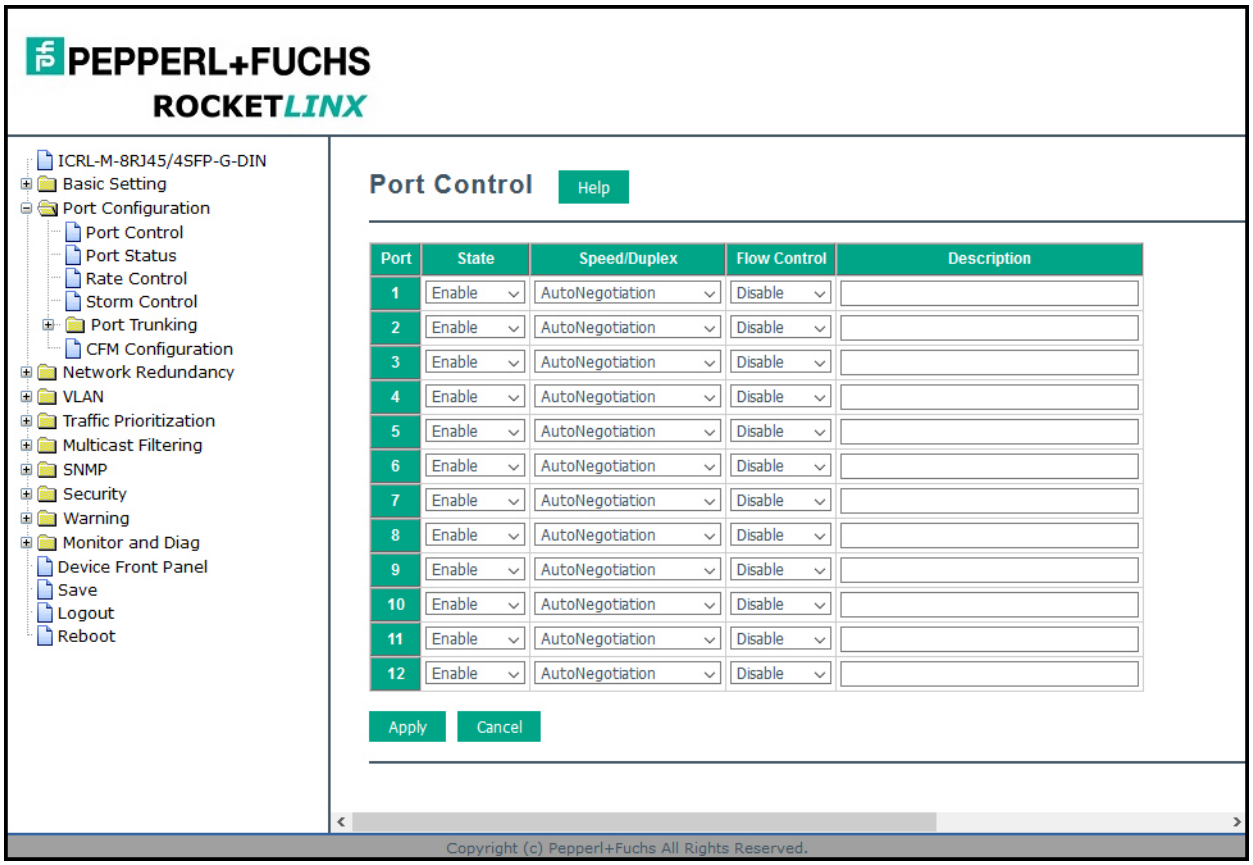
Optional können Sie die Befehlszeilenschnittstelle (Command-Line Interface, CLI) für die Konfiguration verwenden (siehe *Portkonfiguration (CLI)* auf Seite 186).

4.4.1. Port Control

Auf der Seite *Port Control* können Sie den Portstatus aktivieren/deaktivieren oder die automatische Portaushandlung, Geschwindigkeit, Duplexfunktion und Flusssteuerung konfigurieren.

Wählen Sie den Port aus, den Sie konfigurieren möchten, und nehmen Sie Änderungen am Port vor. Die folgende Tabelle enthält Informationen zu den verschiedenen Optionen unter „Port Control“.

Anmerkung: *Wenn beide Enden nicht mit der gleichen Geschwindigkeit verbunden sind, können sie sich nicht miteinander verbinden. Wenn sich beide Enden nicht im selben Duplexmodus befinden, werden sie im Halbduplexmodus verbunden.*

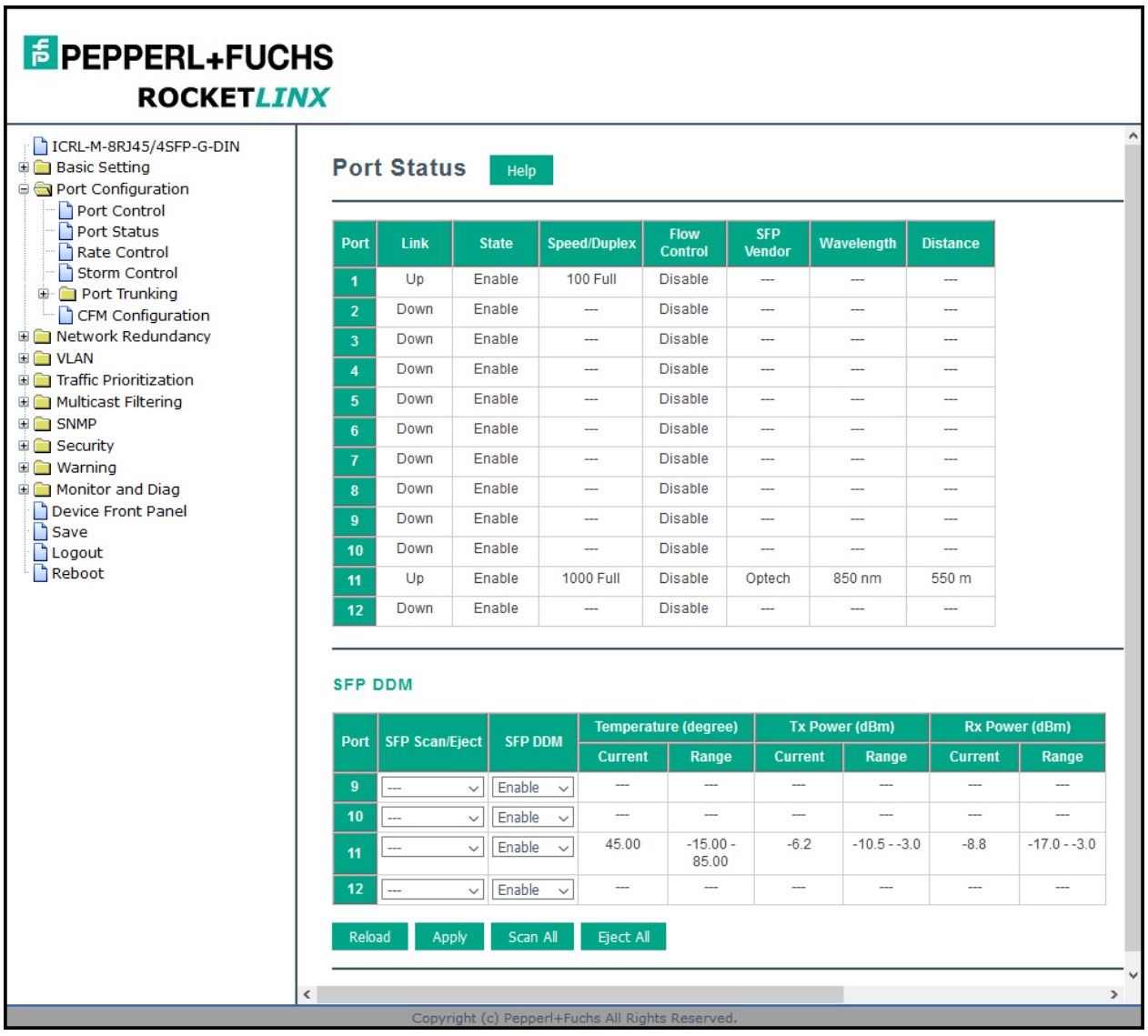


5/21/20

Seite „Port Configuration“	
State	Sie können den Status dieses Ports aktivieren oder deaktivieren. Sobald Sie auf **Disable** klicken, wird der Port angehalten, um eine Verbindung zum anderen Ende herzustellen, und leitet keinen Datenverkehr mehr weiter. Die Standardeinstellung ist **Enable**, d. h., alle Ports können verwendet werden, wenn Sie den ICRL-M erhalten.
Speed/Duplex	Sie können die Portgeschwindigkeit und den Duplexmodus für jeden Gigabit-Port konfigurieren. Nachfolgend finden Sie die Auswahlmöglichkeiten für die RJ45-Ports: • Auto Negotiation (Standard) • 10M full-duplex (10 Vollduplex) • 10M half-duplex (10 Halbduplex) • 100M full-duplex (100 Vollduplex) • 100M half-duplex (100 Halbduplex) Nachfolgend finden Sie die Auswahlmöglichkeiten für die SFP-Ports: • Auto Negotiation (Standard) • 100M full-duplex (100 Vollduplex) ICRL-M-16RJ45/4CP-G-DIN bietet vier RJ45-/SFP-Kombinationsports. Standardmäßig sind die RJ45(C)-Ports deaktiviert. Wenn Sie sowohl die RJ45-Kupferports als auch die SFP(F)-Ports verwenden möchten, müssen Sie den Kupferport aktivieren. Wenn auf beide Ports gleichzeitig zugegriffen wird, hat SFP Priorität. 
Flow Control	**Enable** bedeutet, dass Sie die Flusssteuerungsfunktion des Remote-Netzwerkgeräts aktivieren müssen, damit die Flusssteuerung des entsprechenden Ports auf dem Switch funktioniert. **Disable** (Standard) bedeutet, dass Sie die Flusssteuerungsfunktion des Remote-Netzwerkgeräts nicht aktivieren müssen, da die Flusssteuerung des entsprechenden Ports auf dem Switch funktioniert.
Description	Klicken Sie auf dieses Feld, wenn Sie eine Portbeschreibung eingeben möchten.
Apply	Klicken Sie auf **Apply**, um die Einstellungen anzuwenden. ***Anmerkung:*** *Sie müssen die Einstellungen mit **Save** speichern (Seite 159), wenn Sie diese Einstellungen nach Ausschalten des ICRL-M beibehalten möchten.*

4.4.2. Port status

Anmerkung: Die Seite *Port Status* zeigt den aktuellen Portstatus an, einschließlich SFP-Glasfaser-Transceiver (Small Form Factor) mit DDM-Funktion (Digital Diagnostic Monitoring), die Echtzeitinformationen zum SFP-Transceiver liefert und die Diagnose des empfangenen und gestarteten Glasfasersignals ermöglicht. *Die Web-Benutzerschnittstelle kann den Namen des Anbieters, die Wellenlänge und die Entfernung aller Pepperl+Fuchs-Gigabit-SFP-Transceiver anzeigen. Wenn „Unknown Information“ angezeigt wird, bedeutet dies möglicherweise, dass der Anbieter seine Informationen nicht bereitstellt oder dass die Informationen seines Transceivers nicht gelesen werden können.*

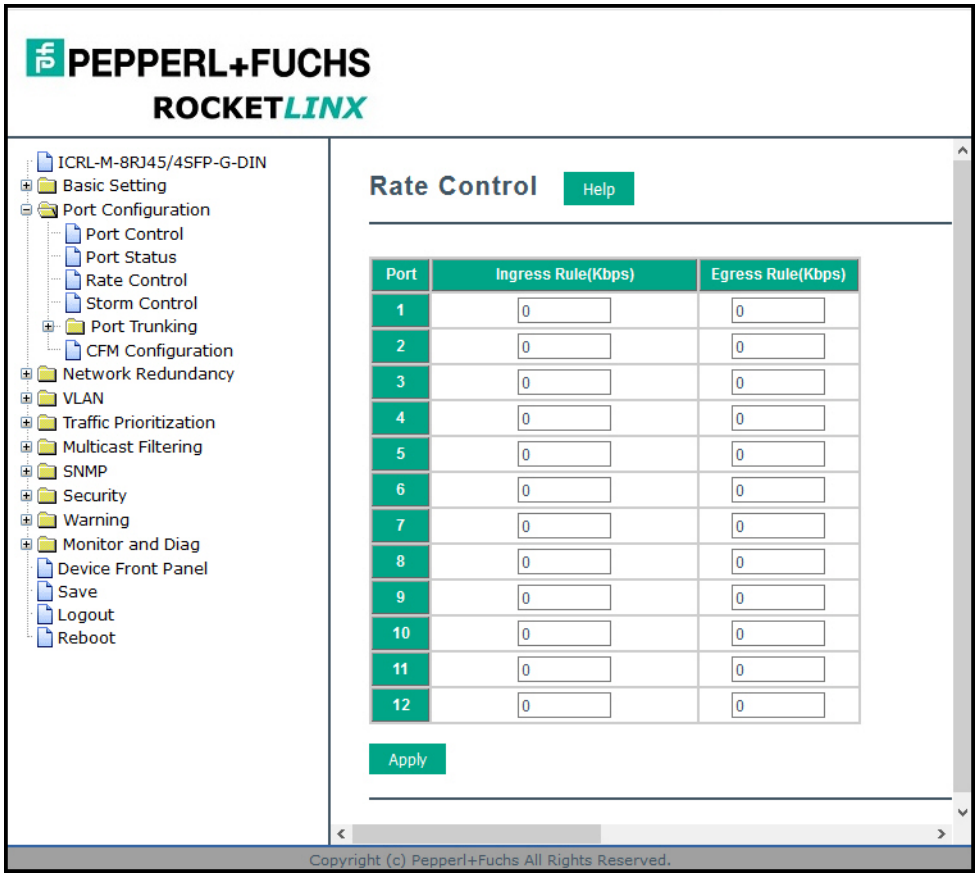


Seite „Port Status“	
Link	Zeigt den Verbindungsstatus an; **Up** bedeutet, dass die Verbindung aktiv ist, und **Down** bedeutet, dass die Verbindung nicht verfügbar ist.
State	Zeigt den Portstatus an. Wenn der Status aktiv ist, wird **Enable** angezeigt. Wenn der Port deaktiviert oder heruntergefahren ist, wird **Disable** angezeigt.
Speed/Duplex	Aktueller Funktionsstatus des Ports.
Flow Control	Der Status der Flusssteuerung.
SFP Vendor	Name des Herstellers des SFP-Transceivers, der an den/die SFP-Port(s) angeschlossen ist.
Wavelength	Wellenlänge des SFP-Transceivers, der an den/die SFP-Port(s) angeschlossen ist.
Distance	Distanz des SFP-Transceivers, der an den/die SFP-Port(s) angeschlossen ist.
SFP Scan/Eject	Sie können aus folgenden Optionen wählen: • **Scan**: Scannen Sie den SFP-Transceiver und zeigen Sie die Informationen an. • **Eject**: Werfen Sie den ausgewählten SFP-Transceiver aus. Sie können einen Port oder mit **Eject All** alle Ports auswerfen.
SFP DDM	Wenn Sie diese Option aktivieren, wird ein SFP-DDM-Transceiver gescannt und die Informationen werden angezeigt.
SFP Scan/Eject	Klicken Sie auf die Schaltfläche **Scan/Eject**, um das SFP zu scannen oder sicher zu entfernen.
SFP DDM	Klicken Sie auf die Schaltfläche **Enable/Disable**, um die SFP-DDM-Funktion zu aktivieren oder zu deaktivieren.
Temperature	Zeigt die aktuell erkannte Temperatur und den zulässigen Temperaturbereich für den DDM-SFP-Transceiver an.
Tx Power (dBm)	Zeigt die aktuell erkannte Übertragungsleistung und den zulässigen Tx-Leistungsbereich für den DDM-SFP-Transceiver an.
Rx Power (dBm)	Zeigt die aktuelle Empfangsleistung und den zulässigen Rx-Leistungsbereich für den DDM-SFP-Transceiver an.
Reload	Klicken Sie hier, um den Portstatus neu zu laden.
Scan All	Klicken Sie auf die Schaltfläche **Scan All**, um nach allen SFPs zu suchen.
Eject All	Sie können einen oder alle DDM-SFP-Transceiver auswerfen. Um alle SFPs auszuwerfen, klicken Sie auf **Eject All**.

Anmerkung: *Die meisten SFP-Transceiver stellen Herstellerinformationen bereit, die der ICRL-M lesen kann. Die Webschnittstelle kann den Herstellernamen, die Wellenlänge und die Entfernung aller Pepperl+Fuchs-SFP-Transceiver-Modelle anzeigen. Wenn „Unknown Info“ angezeigt wird, bedeutet dies möglicherweise, dass der Anbieter seine Informationen nicht bereitstellt oder dass die Informationen seines Transceivers nicht gelesen werden können. Wenn der verstopfte DDM-SFP-Transceiver nicht durch Pepperl+Fuchs zertifiziert ist, wird die DDM-Funktion nicht unterstützt, aber die Kommunikation wird nicht deaktiviert.*

4.4.3. Rate Control

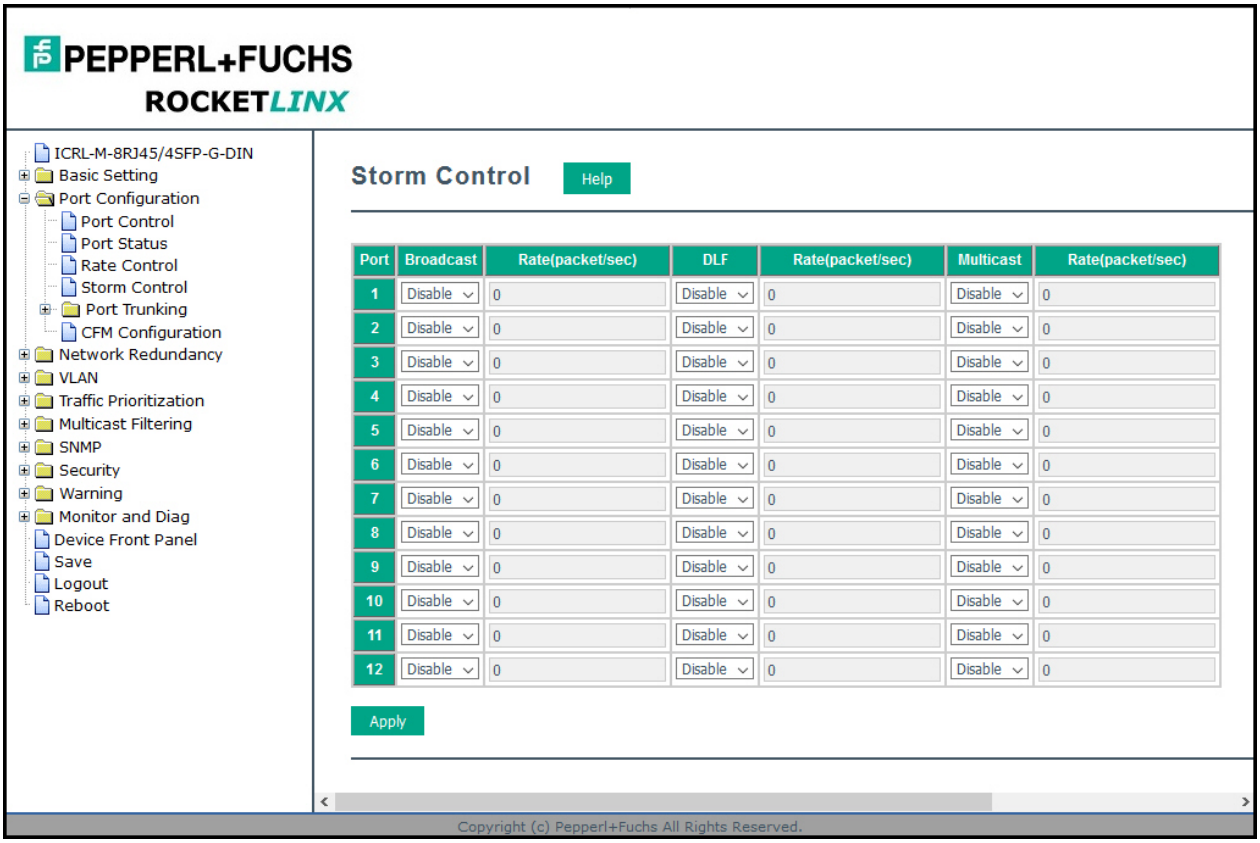
Die Ratenbeschränkung wird verwendet, um die Rate des Datenverkehrs zu steuern, der über eine Netzwerkschnittstelle gesendet oder empfangen wird. Wenn die Eingangsrate beschränkt wird, wird Datenverkehr empfangen, der kleiner oder gleich der angegebenen Rate ist, während Datenverkehr, der die Rate überschreitet, verworfen wird. Wenn die Ausgangsrate beschränkt wird, wird Datenverkehr gesendet, der kleiner oder gleich der angegebenen Rate ist, während Datenverkehr, der die Rate überschreitet, verworfen wird.



Seite „Rate Control“	
Ingress Rule (Kbps)	Eingangsrate in kBit/s; der Ratenbereich liegt zwischen 1 und 1.000.000 kBit/s. Null bedeutet keine Beschränkung. Der Standardwert ist unbeschränkt.
Egress Rule (Kbps)	Ausgangsrate in kBit/s; der Ratenbereich liegt zwischen 1 und 1.000.000 kBit/s. Null bedeutet keine Beschränkung. Der Standardwert ist unbeschränkt. Die Beschränkung der Ausgangsrate hat Auswirkungen auf alle Arten von Pakettypen, einschließlich Unknown Unicast, Multicast und Broadcast.
Apply	Klicken Sie auf **Apply**, um die Einstellungen anzuwenden. ***Anmerkung:*** *Sie müssen die Einstellungen mit **Save** speichern (Seite 159), wenn Sie diese Einstellungen nach Ausschalten des ICRL-M beibehalten möchten.*

4.4.4. Storm Control

Storm Control ähnelt der Ratenbeschränkung. Die Ratenbeschränkung filtert den gesamten Datenverkehr oberhalb des über die Benutzerschnittstelle eingegebenen Schwellenwerts. Mit Storm Control können Sie die Rate für bestimmte Pakettypen definieren.



Seite „Storm Control“	
Broadcast	Aktivieren oder deaktivieren Sie Broadcast Storm Control am entsprechenden Port. Der Wert der Broadcast-Ratenbeschränkung liegt zwischen 2 und 262.142 Paketen/s. Null bedeutet keine Beschränkung.
DLF	Aktivieren oder deaktivieren Sie Destination Lookup Failure Storm Control am entsprechenden Port. Der Wert der DLF-Ratenbeschränkung liegt zwischen 2 und 262.142 Paketen/s. Null bedeutet keine Beschränkung.
Multicast	Aktivieren oder deaktivieren Sie Multicast Storm Control an diesem Port. Der Wert der Multicast-Ratenbeschränkung liegt zwischen 2 und 262.142 Paketen/s. Null bedeutet keine Beschränkung.
Apply	Klicken Sie auf **Apply**, um die Einstellungen anzuwenden. Es kann einige Zeit dauern und die Web-Benutzerschnittstelle wird möglicherweise langsam. Das ist normal. ***Anmerkung:*** *Sie müssen die Einstellungen mit **Save** speichern (Seite 159), wenn Sie diese Einstellungen nach Ausschalten des ICRL-M beibehalten möchten.*

4.4.5. Port Trunking

Mit Port-Trunking können Sie mehrere Ethernet-Ports parallel gruppieren, um die Verbindungsbandbreite zu erhöhen. Die aggregierten Ports können als physischer Port betrachtet werden, der eine Bandbreite aufweist, die der kombinierten Bandbreite jedes Trunk-Ports entspricht. Die Mitgliedsports derselben Trunk-Gruppe können die Last und die Sicherung für einander ausgleichen. Die Port-Trunking-Funktion wird in der Regel verwendet, wenn Sie eine höhere Bandbreite für den Netzwerk-Backbone benötigen. Dies ist eine kostengünstige Möglichkeit für Sie, mehr Daten zu übertragen.

Die aggregierten Ports können mit einem anderen Switch verbunden werden, der auch Port-Trunking unterstützt. Pepperl+Fuchs unterstützt zwei Arten von Port-Trunking:

- Static Trunk
- IEEE 802.3ad

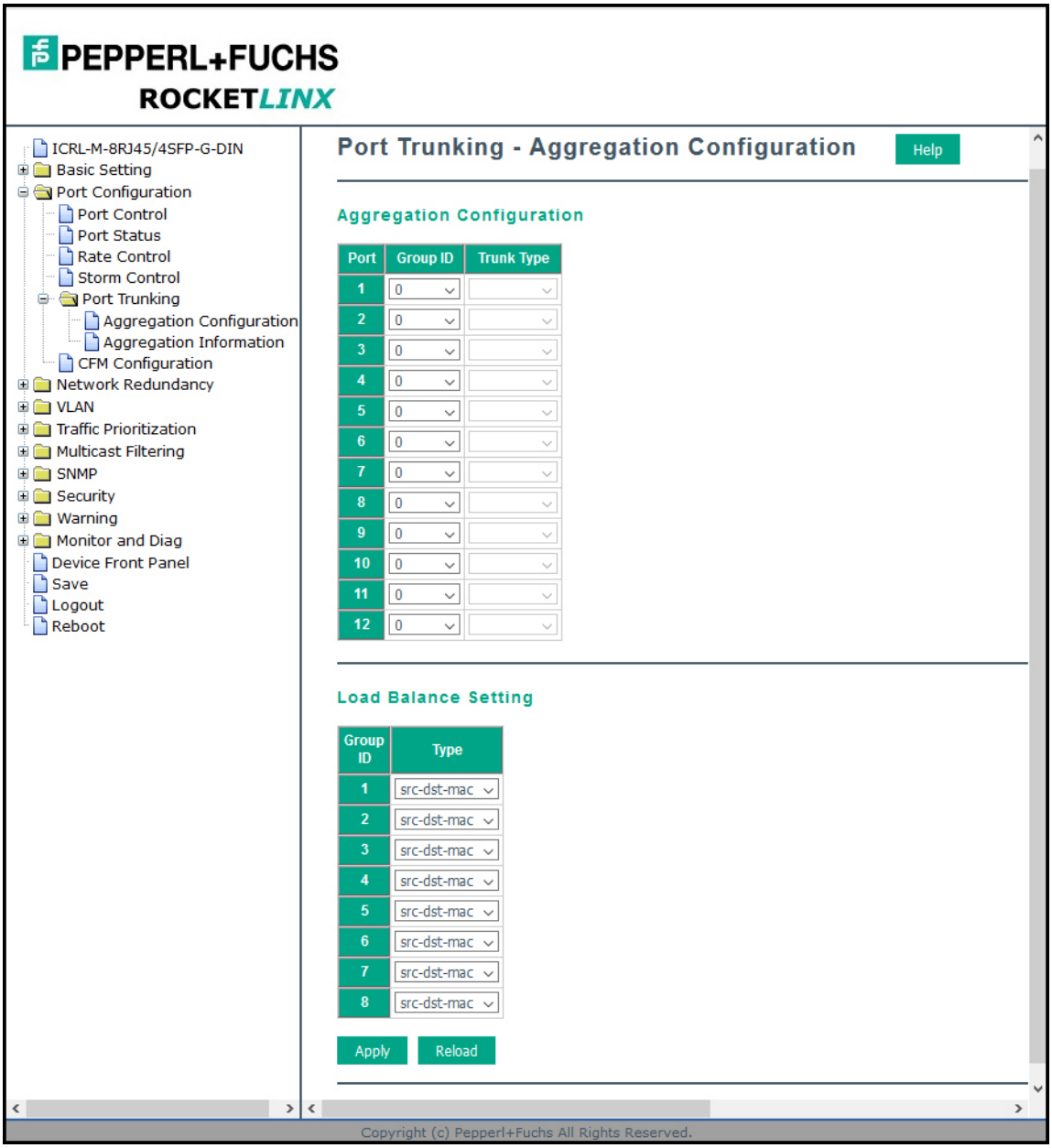
Es gibt verschiedene Beschreibungen für Port-Trunking. Verschiedene Hersteller können unterschiedliche Beschreibungen für ihre Produkte verwenden, z. B. Link Aggregation Group (LAG), Link Aggregation Control Protocol, Ethernet Trunk oder Ether Channel.

Wenn das andere Ende IEEE 802.3ad LACP verwendet, sollten Sie dem Trunk „IEEE 802.3ad LACP“ zuweisen. Wenn das andere Ende nicht 802.3ad verwendet, können Sie „Static Trunk“ verwenden.

Es gibt zwei Seiten für Port-Trunking: *Aggregationskonfiguration* auf Seite 67 und *Aggregationsinformationen* auf Seite 68.

4.4.5.1. Aggregationskonfiguration

Verwenden Sie die Seite *Port Trunk – Aggregation Configuration*, um das Port-Trunking einzurichten.

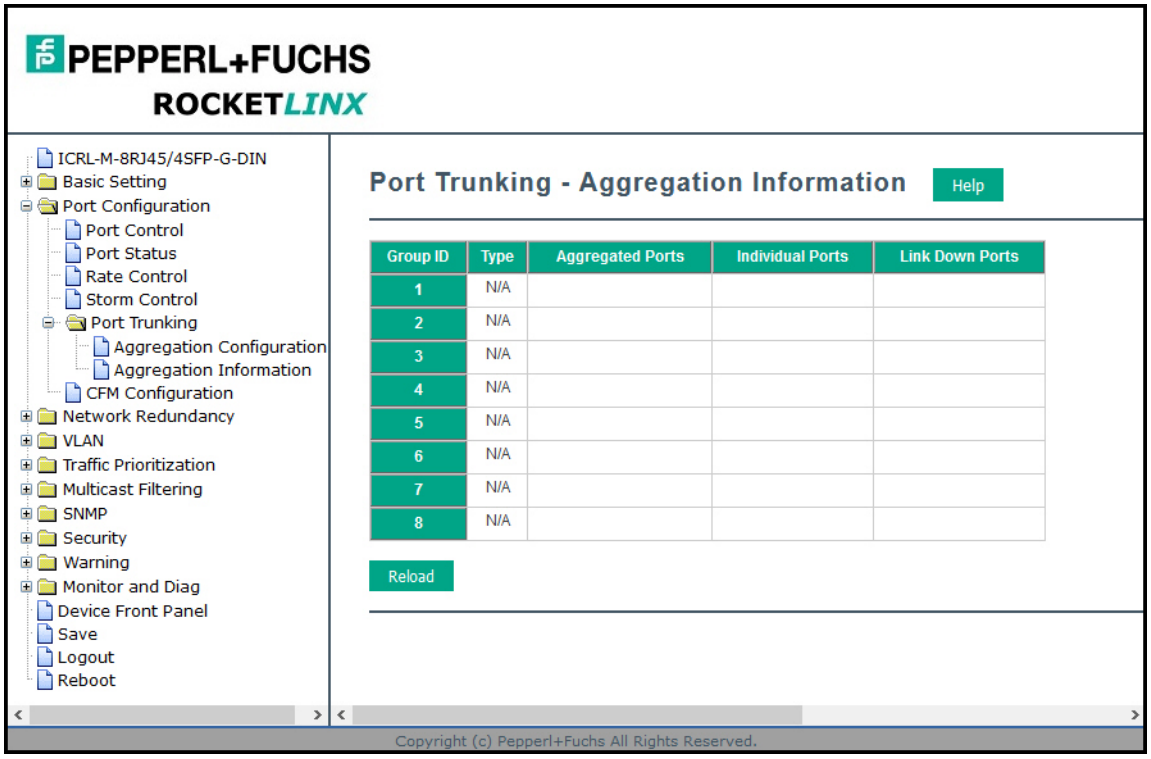


Seite „Aggregation Setting“	
Group ID	Die **Group ID** ist die ID für die Port-Trunking-Gruppe. Ports mit derselben Gruppen-ID befinden sich in derselben Gruppe.
Trunk Type	**Static** oder **LACP**. Jede Trunk-Gruppe kann nur Static oder 802.3ad LACP unterstützen. Nicht aktive Ports können hier nicht eingerichtet werden.

Seite „Aggregation Setting“ (Fortsetzung)	
Load Balance Type	Es gibt mehrere Lastausgleichstypen: • dst-ip (Ziel-IP) • dst-mac (Ziel-MAC) • src-dst-ip (Quell- und Ziel-IP) • src-dst-mac (Quell- und Ziel-MAC) • src-ip (Quell-IP) • src-mac (Quell-MAC)
Apply	Klicken Sie auf **Apply**, um die Einstellungen anzuwenden. ***Anmerkung:*** *Sie müssen die Einstellungen mit **Save** speichern (Seite 159), wenn Sie diese Einstellungen nach Ausschalten des ICRL-M beibehalten möchten.*

4.4.5.2. Aggregationsinformationen

Auf der Seite *Port Trunk – Aggregation Information* wird der Status der Portaggregation angezeigt. Sobald die Aggregationsports verhandelt wurden, wird der folgende Status angezeigt.



Seite „Aggregation Status“	
Group ID	Zeigt die Einrichtung von Trunk 1 bis Trunk 8 an.
Type	Der Typ ist **Static** oder **LACP**. Statisch bedeutet, dass LACP deaktiviert ist und statisch vom Administrator konfiguriert wird.

Seite „Aggregation Status“ (Fortsetzung)	
Aggregated Ports	Bei LACP-Verbindungen können Sie die Mitgliedsports in der Spalte **Aggregated** sehen.
Individual Ports	Wenn **LACP** aktiviert ist, werden Mitgliedsports der LACP-Gruppe, die nicht mit den richtigen LACP-Mitgliedsports verbunden sind, in der Spalte **Individual** angezeigt.
Link Down Ports	Wenn **LACP** aktiviert ist, werden Mitgliedsports der LACP-Gruppe, die nicht verbunden sind, in der Spalte **Link Down** angezeigt.
Reload	Klicken Sie auf **Reload**, um Aggregationseinstellungen neu zu laden.

4.5. Netzwerkredundanz

Für industrielle Anwendungen ist es wichtig, dass das Netzwerk jederzeit läuft. Der ICRL-M unterstützt:

- *Standard Spanning Tree Protocol* (STP) und *Rapid Spanning Tree Protocol* (RSTP)

  Der ICRL-M unterstützt die RSTP-Versionen IEEE 802.1D-2004, IEEE 802.1D-1998 STP und IEEE 802.1w RSTP.

- *Multiple Spanning Tree Protocol* (MSTP)

  MSTP implementiert IEEE 802.1s, das RSTP für schnelle Konvergenz verwendet, und ermöglicht die Gruppierung von VLANs in einer Spanning-Tree-Instanz, wobei jede Instanz über eine Spanning-Tree-Topologie unabhängig von anderen Spanning-Tree-Instanzen verfügt. Diese Architektur bietet mehrere Weiterleitungspfade für Datenverkehr, ermöglicht Lastausgleich und reduziert die Anzahl der Spanning-Tree-Instanzen, die für die Unterstützung einer großen Anzahl von VLANs erforderlich sind. MSTP wurde ursprünglich in IEEE 802.1s definiert und später in die IEEE-802.1Q-2003-Spezifikation integriert.

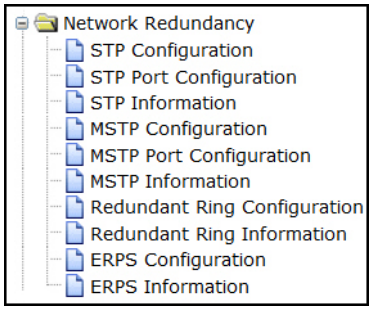
- *Redundanter Ring*

  Der redundante Ring verfügt über 0 ms für die Wiederherstellung und mehrere Millisekunden für das Failover für Kupferkabel.

- *Rapid Dual Homing (RDH)*

  Die fortschrittliche RDH-Technologie ermöglicht dem ICRL-M die einfache Verbindung mit einem zentralen verwalteten Switch. Mit der RDH-Technologie können Sie auch mehrere Rapid Super Rings- oder RSTP-Gruppen verbinden, die auch als automatische Ringkopplung bezeichnet werden.

Die folgenden Seiten sind in dieser Gruppe enthalten:



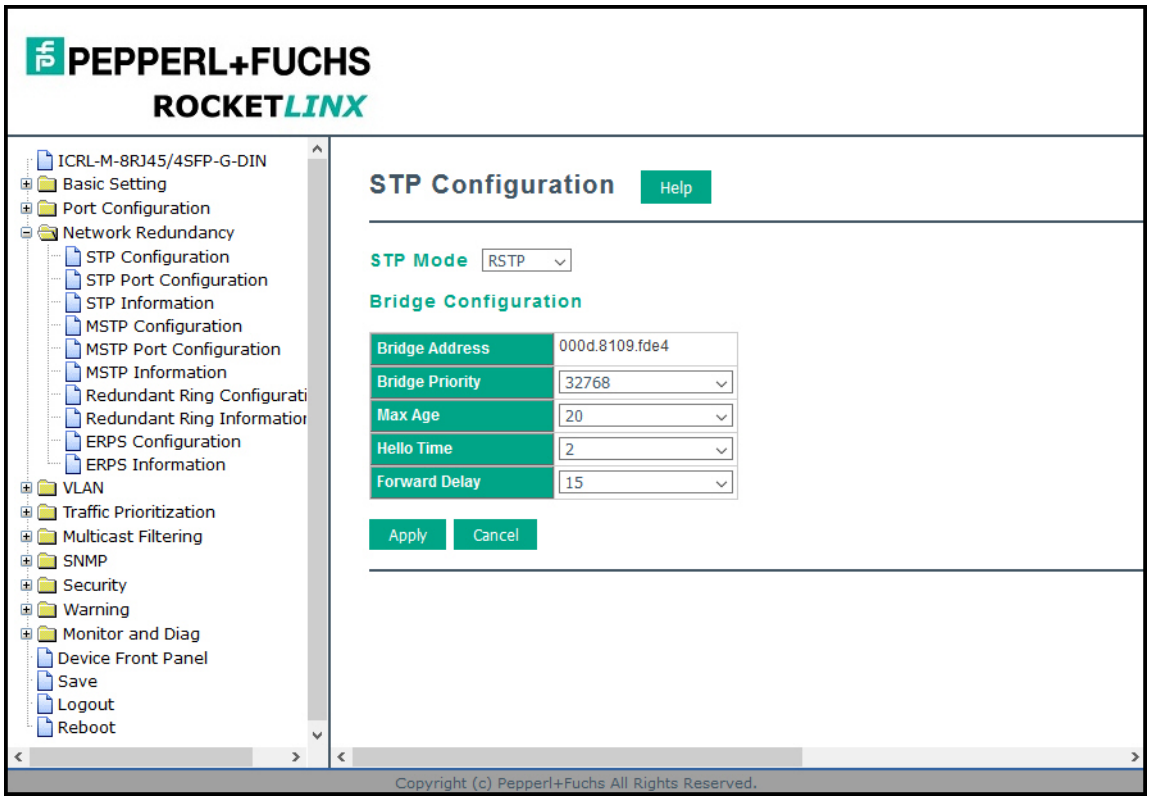
Optional können Sie diese Funktionen über die CLI konfigurieren (siehe *Netzwerkredundanz (CLI)* auf Seite 190).

4.5.1. STP Configuration

Auf dieser Seite können Sie den STP-Modus auswählen und die globale STP-/RSTP-Bridge-Konfiguration festlegen. Das Spanning Tree Protocol (STP; IEEE 802.1D) bietet eine schleifenfreie Topologie für jedes LAN- oder überbrückte Netzwerk.

Das Rapid Spanning Tree Protocol (RSTP; IEEE 802.1w) ist eine Weiterentwicklung des Spanning Tree Protocol (STP). Es wurde mit dem IEEE-802.1w-Standard eingeführt und bietet eine schnellere Spanning-Tree-Konvergenz nach Topologieänderungen. In den meisten Fällen kann IEEE 802.1w auch auf IEEE 802.1D zurückgesetzt werden, um auf Portbasis mit älteren Bridges zu interoperieren. Die neue Ausgabe des IEEE-802.1D-Standards IEEE 802.1D-2004 umfasst die Standards IEEE-802.1t-2001 und IEEE-802.1w.

Multiple Spanning Tree Protocol (MSTP; IEEE 802.1s), das RSTP für schnelle Konvergenz verwendet und die Gruppierung von VLANs in einer Spanning-Tree-Instanz ermöglicht, wobei jede Instanz über eine Spanning-Tree-Topologie unabhängig von anderen Spanning-Tree-Instanzen verfügt. Diese Architektur bietet eine schleifenfreie Topologie mit Lastausgleich bei gleichzeitiger Reduzierung der Anzahl von Spanning-Tree-Instanzen, die zur Unterstützung einer großen Anzahl von VLANs erforderlich sind. MSTP wurde ursprünglich in IEEE 802.1s definiert und später in die IEEE-802.1Q-2003-Spezifikation integriert.

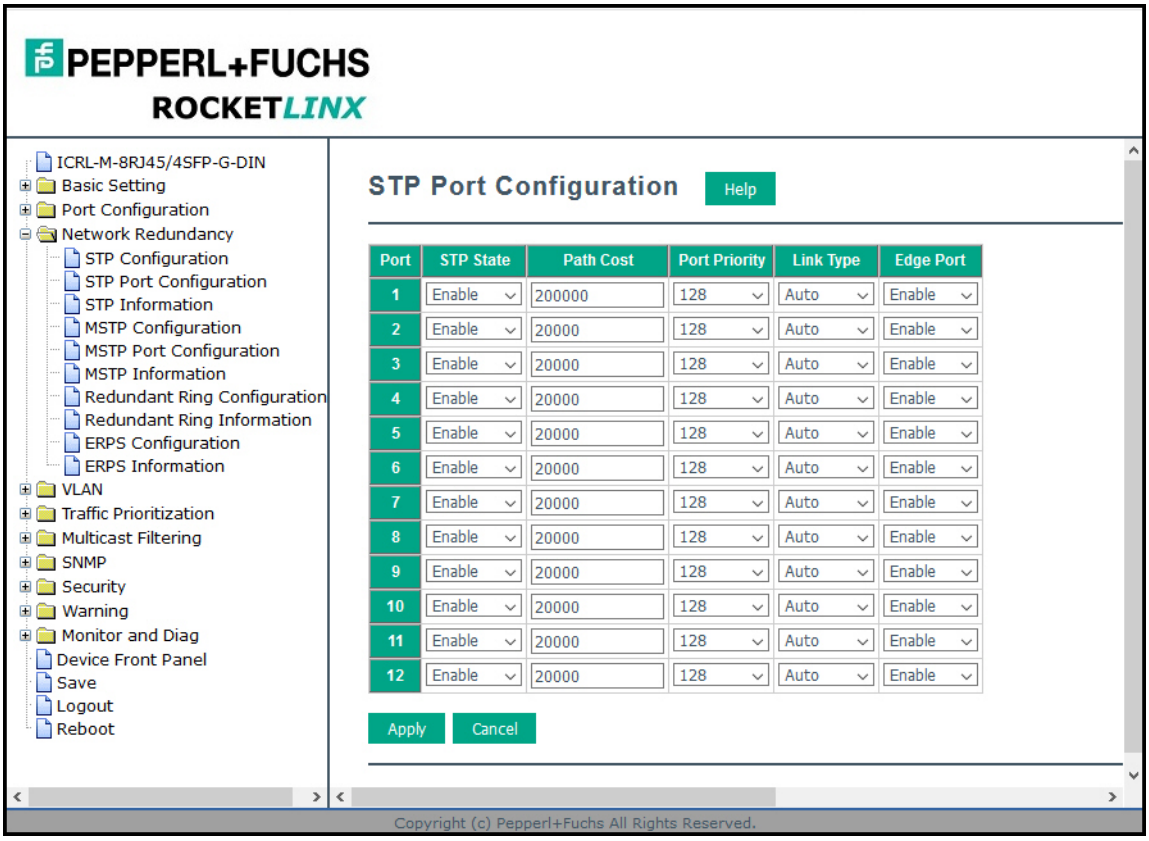


Seite „STP Configuration“	
STP Mode	Wählen Sie das Spanning Tree Protocol (STP, RSTP oder MSTP) oder deaktivieren Sie STP.
Bridge Configuration	
Bridge Address	Ein Wert, der zur Identifizierung der Bridge verwendet wird. Dieses Element kann nicht geändert werden.

Seite „STP Configuration“ (Fortsetzung)	
Bridge Priority	RSTP verwendet eine Bridge-ID, um die Root-Bridge zu bestimmen. Die Bridge mit der höchsten Bridge-ID wird zur Root-Bridge. Die Bridge-ID besteht aus Bridge-Priorität und Bridge-MAC-Adresse. So erhält die Bridge mit der höchsten Priorität die höchste Bridge-ID. Wenn alle Bridge-IDs dieselbe Priorität haben, wird die Bridge mit der niedrigsten MAC-Adresse zur Root-Bridge. ***Anmerkung:*** *Der Bridge-Prioritätswert muss ein Vielfaches von 4096 sein. Ein Gerät mit einer niedrigeren Nummer hat eine höhere Bridge-Priorität. Beispiel: Bei 4096 ist die Priorität höher als bei 32768.* *Über die Web-Benutzerschnittstelle können Sie die Prioritätsnummer direkt auswählen. Wenn Sie den Wert über die CLI oder SNMP konfigurieren, müssen Sie ihn möglicherweise direkt eingeben. Sie müssen die n x 4096 Regeln für die Bridge-Priorität befolgen.*
Max Age (siehe Hinweis)	Dieser Wert stellt die Zeit dar, die eine Bridge wartet, ohne STP-Konfigurationsnachrichten zu empfangen, bevor sie versucht, neu zu konfigurieren. Wenn der ICRL-M nicht die Root-Bridge ist und keine Hello-Nachricht von der Root-Bridge in einem Zeitraum von „Max Age“ empfangen wurde, konfiguriert sich der ICRL-M selbst als Root-Bridge neu. Sobald zwei oder mehr Geräte im Netzwerk als Root-Bridge erkannt werden, verhandeln die Geräte erneut, um eine neue Spanning-Tree-Topologie einzurichten. Der Wert für das maximale Alter wirkt sich auf das maximale Volumen der RSTP-Schleife aus. Im RSTP-BPDU-Paket gibt es das Feld **Message Age**, das bei 0 beginnt. Jedes Mal, nachdem ein Hop in der RSTP-Schleife übergeben wurde, wird 1 hinzugefügt. Wenn das Nachrichtenalter größer als „Max Age“ ist, wird die BPDU ignoriert und die unteren Switches werden in eine separate RSTP-Domain verschoben. Die Switches in einer anderen RSTP-Domain können nicht über den oberen Switch verwaltet werden. Da verschiedene RSTP-fähige Switches über einen eigenen Mechanismus verfügen, um das Nachrichtenalter zu berechnen, kann bei RSTP-fähigen Switches anderer Anbieter ein Problem mit der Interoperabilität auftreten. Das maximale Volumen der RocketLinx-RSTP-Domain ist 23. Stellen Sie daher sicher, dass Sie einen „Max Age“-Wert von unter 23 konfigurieren.
Hello Time (siehe Hinweis)	Dies ist ein periodischer Timer, der den ICRL-M zum Senden eines BPDU-Pakets (Bridge Protocol Data Unit) zum Prüfen des aktuellen STP-Status veranlasst. Geben Sie eine Zahl zwischen 1 und 10 ein.
Forward Delay (siehe Hinweis)	Die Anzahl der Sekunden, die ein Port wartet, bevor er vom STP-Lern- und -Abhörstatus in den Weiterleitungsstatus wechselt. Geben Sie eine Zahl zwischen 4 und 30 ein.
Apply	Klicken Sie auf **Apply**, um die Einstellungen anzuwenden. ***Anmerkung:*** *Sie müssen die Einstellungen mit **Save** speichern (Seite 159), wenn Sie diese Einstellungen nach Ausschalten des ICRL-M beibehalten möchten.*
Anmerkung: *2 x (Weiterleitungsverzögerungszeit - 1 Sekunde) muss größer oder gleich „Max Age“ sein. „Max Age“ muss größer oder gleich 2 x (Hello-Zeit + 1 Sekunde) sein.*	

4.5.2. STP Port Configuration

Auf dieser Seite können Sie den Portparameter konfigurieren, nachdem Sie STP, RSTP oder MSTP aktiviert haben.

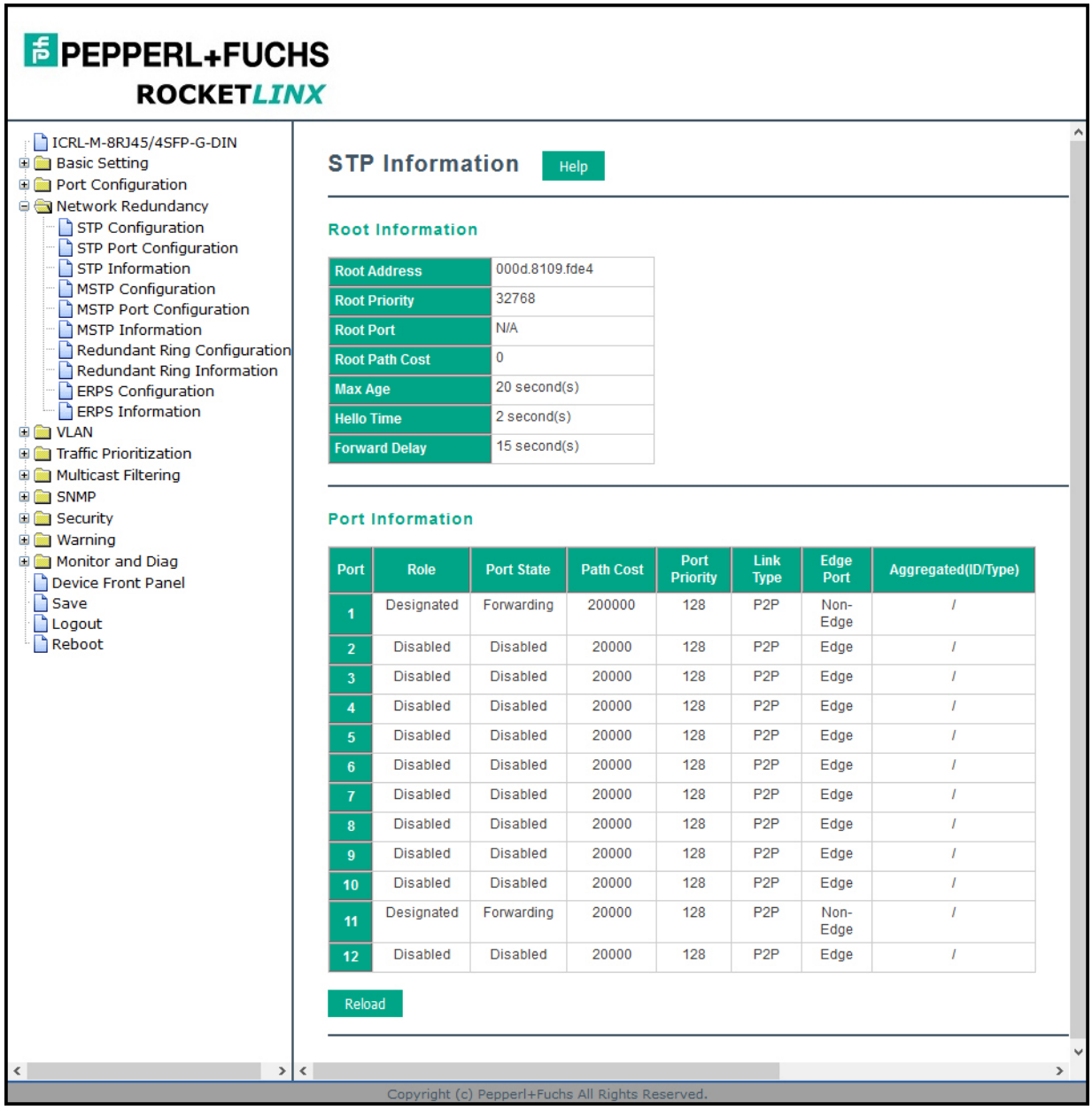


Seite „STP Port Configuration“	
STP State	Sie können STP/RSTP/MSTP auf Portbasis aktivieren/deaktivieren. Sie können den STP-Status deaktivieren, wenn Sie ein Gerät verbinden, um STP-Wartezeiten zu vermeiden.
Path Cost	Die Kosten für den Pfad zur anderen Bridge von dieser Übertragungsbrücke am angegebenen Port. Geben Sie eine Zahl zwischen 1 und 200.000.000 ein.
Port Priority	Entscheiden Sie, welcher Port in Ihrem LAN nach Priorität gesperrt werden soll. Geben Sie eine Zahl zwischen 0 und 240 in Schritten von 16 ein.
Link Type	Einige der schnellen Statustransaktionen, die innerhalb von RSTP möglich sind, hängen davon ab, ob der betreffende Port mit genau einer anderen Bridge verbunden ist (d. h., er wird von einem Punkt-zu-Punkt-LAN-Segment bedient) oder mit zwei oder mehr Brücken verbunden ist (d. h., er wird von einem gemeinsamen mittleren LAN-Segment bedient). Mit dieser Konfiguration kann der P2P-Status der Verbindung von einem Administrator gesteuert werden.
Edge Port	In Implementierungen vorhanden, die die Identifizierung von Edge-Ports unterstützen. Alle Ports, die direkt mit den Endstationen verbunden sind, können keine Bridging-Schleifen im Netzwerk erstellen und können somit direkt in die Weiterleitung übergehen und die Abhör- und Lernphase überspringen. Wenn ein Nicht-Bridge-Gerät einen Edge-Port verbindet, befindet sich dieser Port in einem blockierenden Zustand und wechselt zu einem Weiterleitungsstatus in 2 x Hello-Zeit Sekunden. Wenn das Verbindungsgerät einen Edge-Port verbindet, handelt es sich bei diesem Port automatisch um einen Nicht-Edge-Port.

Seite „STP Port Configuration“ (Fortsetzung)	
Apply	Klicken Sie auf **Apply**, um die Einstellungen anzuwenden. ***Anmerkung:*** *Sie müssen die Einstellungen mit **Save** speichern (Seite 159), wenn Sie diese Einstellungen nach Ausschalten des ICRL-M beibehalten möchten.*

4.5.3. STP Information

Auf der Seite *STP Information* können Sie die Root-Informationen und den Portstatus des ICRL-M anzeigen.



Seite „STP Information“	
Root Information	
Root Address	Root-Bridge-Adresse, bei der es sich um die Bridge mit der kleinsten (niedrigsten) Bridge-ID handelt.
Root Priority	Root-Bridge-Priorität; die Bridge mit dem niedrigsten Wert hat die höchste Priorität und wird als Root ausgewählt.
Root Port	Root-Port dieser Bridge.

Seite „STP Information“ (Fortsetzung)	
Root Path Cost	Root-Pfadkosten.
Max Age	Die Zeit in Sekunden, die eine Bridge wartet, ohne STP-Konfigurationsnachrichten zu empfangen, bevor sie versucht, neu zu konfigurieren.
Hello Time	Die Anzahl der Sekunden zwischen den Übertragungen von STP-Konfigurationsnachrichten.
Forward Delay	Die Anzahl der Sekunden, die ein Port wartet, bevor er vom STP-Lern- und -Abhörstatus in den Weiterleitungsstatus wechselt.
Port Information	
Role	Beschreibende Informationen über die STP-/RSTP-Switchport-Rolle. Role: Root, Designated, Alternate, Backup, Disabled, Unknown.
Port State	Beschreibende Informationen über den STP-/RSTP-Switchport-Status. State: Blocking, Listening, Learning, Forwarding, Disabled, Unknown.
Path Cost	Die Kosten für den Pfad zur anderen Bridge von dieser Übertragungsbrücke am angegebenen Port. Der Pfadkostenbereich liegt zwischen 1 und 200.000.000.
Port Priority	Entscheiden Sie, welcher Port in Ihrem LAN nach Priorität gesperrt werden soll. Der Bereich liegt zwischen 0 und 240 in Schritten von 16.
Link Type	Betriebsverbindungstyp. Einige der schnellen Statustransaktionen, die innerhalb von RSTP möglich sind, hängen davon ab, ob der betreffende Port mit genau einer anderen Bridge verbunden (d. h., er wird von einem Punkt-zu-Punkt-LAN-Segment bedient) oder mit zwei oder mehr Brücken verbunden werden kann (d. h., er wird von einem gemeinsamen mittleren LAN-Segment bedient).
Edge Port	Betriebs-Edge-Port-Status. In Implementierungen vorhanden, die die Identifizierung von Edge-Ports unterstützen. Alle Ports, die direkt mit den Endstationen verbunden sind, können keine Bridging-Schleifen im Netzwerk erstellen und können somit direkt in die Weiterleitung übergehen und die Abhör- und Lernphase überspringen. Wenn das Nicht-Bridge-Gerät einen Edge-Port verbindet, befindet sich dieser Port in einem blockierenden Zustand und wechselt zu einem Weiterleitungsstatus in 2 x Hello-Zeit Sekunden. Wenn das Verbindungsgerät einen Edge-Port verbindet, handelt es sich bei diesem Port automatisch um einen Nicht-Edge-Port.
Aggregated (ID/Typ)	Dies sind die aggregierten Portinformationen. Die ID ist die Aggregations-ID (Trunk-ID) und der Typ ist entweder „Static“ oder „LACP“.
Reload	Klicken Sie auf die Schaltfläche **Reload**, um die STP-Informationen neu zu laden.

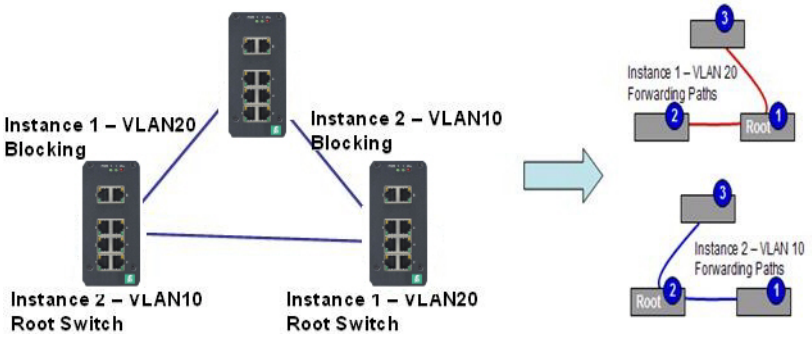
4.5.4. MSTP Configuration

Multiple Spanning Tree Protocol (MSTP) ist eine direkte Erweiterung von RSTP. Es kann einen unabhängigen Spanning-Tree für verschiedene VLANs bereitstellen. Es vereinfacht die Netzwerkverwaltung, schafft eine schnellere Konvergenz als RSTP, indem die Größe jeder Region begrenzt wird, und verhindert, dass VLAN-Mitglieder von den anderen Gruppen segmentiert werden (wie es manchmal bei IEEE 802.1D STP der Fall ist).

Bei der Verwendung von MSTP gibt es einige neue Konzepte der Netzwerkarchitektur. Ein Switch kann zu verschiedenen Gruppen gehören, als Root oder designierter Switch fungieren oder BPDU-Pakete generieren, damit das Netzwerk die Weiterleitungstabelle des Spanning-Baums beibehalten kann. MSTP kann auch einen Lastausgleich zwischen Switches bereitstellen.

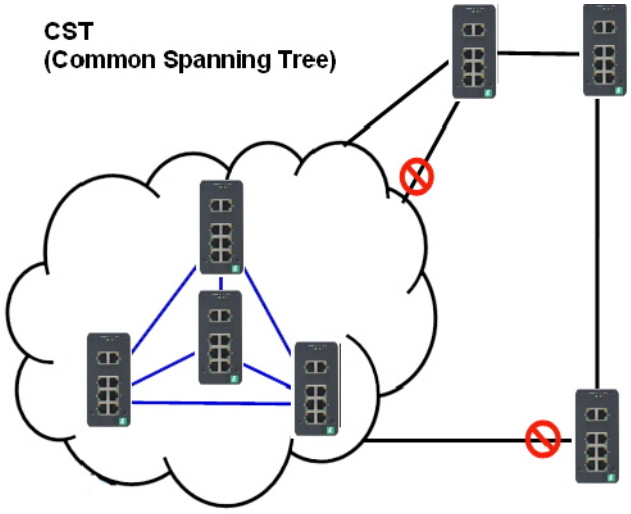
Ein VLAN kann einer Multiple Spanning Tree Instance (MSTI) zugeordnet werden. Die maximale Anzahl von Instanzen, die vom ICRL-M unterstützt werden, beträgt 16, mit einem Bereich von 0 bis 15. Das MSTP erstellt für jede Instanz einen separaten Multiple Spanning Tree (MST), um die Konnektivität zwischen jeder der zugewiesenen VLAN-Gruppen aufrechtzuerhalten. Ein interner Spanning Tree (IST) wird verwendet, um alle MSTP-Switches innerhalb einer MST-Region zu verbinden. Eine MST-Region kann mehrere MSTP-Instanzen enthalten.

Die folgende Abbildung zeigt eine MSTP-Instanz mit zwei VLANs. Jede Instanz verfügt über einen Root-Knoten und Weiterleitungspfade.

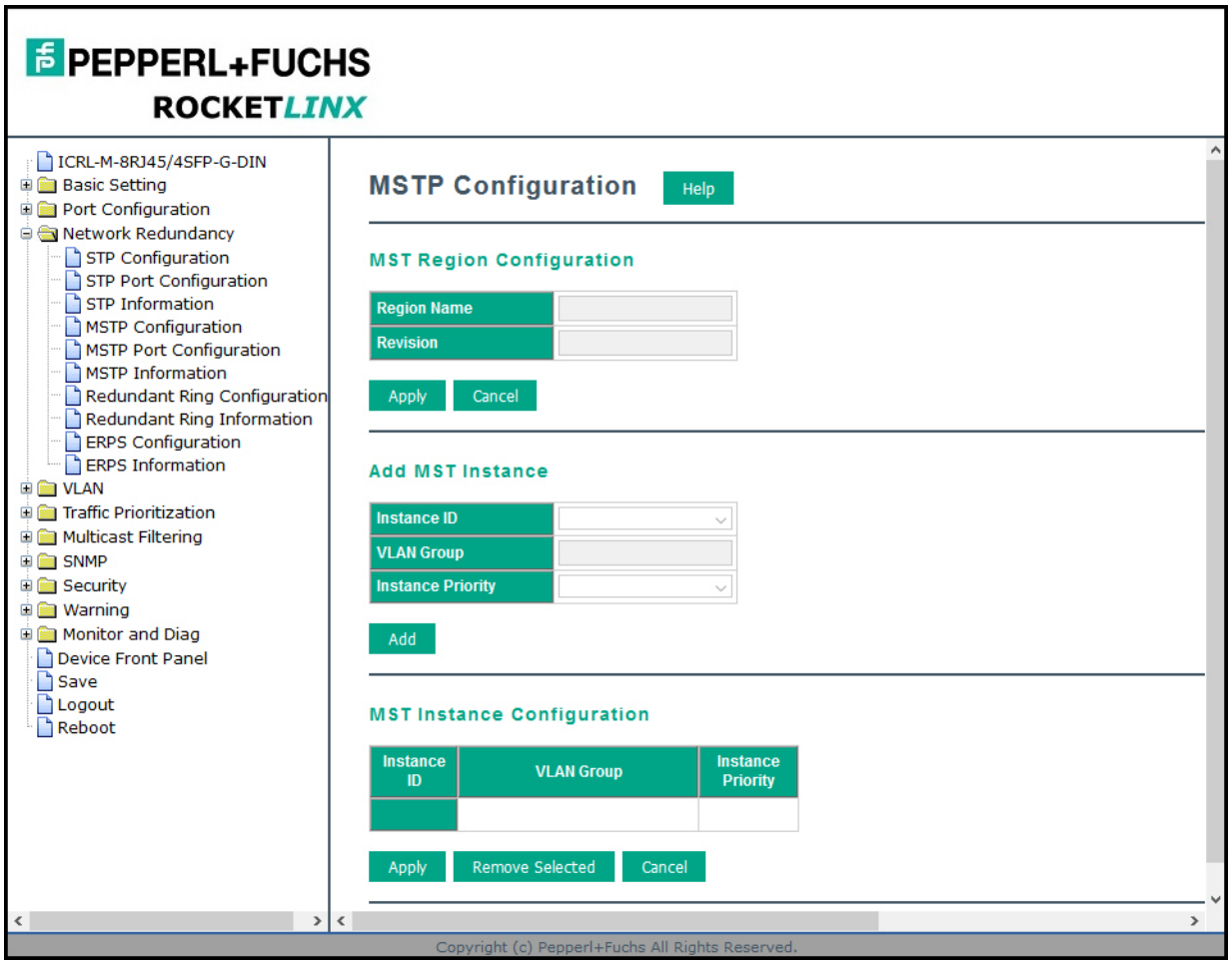


Ein Common Spanning Tree (CST) verbindet alle benachbarten MST-Regionen und fungiert als virtueller Brückenknoten für die Kommunikation mit STP- oder RSTP-Knoten im globalen Netzwerk. MSTP verbindet alle Bridges und LAN-Segmente mit einem einzigen Common Internal Spanning Tree (CIST). Der CIST wird durch den ausgeführten Spanning-Tree-Algorithmus zwischen Switches gebildet, die die STP-, RSTP- oder MSTP-Protokolle unterstützen.

Das folgende Diagramm zeigt ein CST, das an ein größeres Netzwerk angeschlossen ist. In diesem Netzwerk kann eine Region unterschiedliche Instanzen und ihren eigenen Weiterleitungspfad und ihre eigene Tabelle aufweisen, das CST fungiert jedoch als einzelne Bridge.



Dies ist die Seite *MSTP Configuration*.

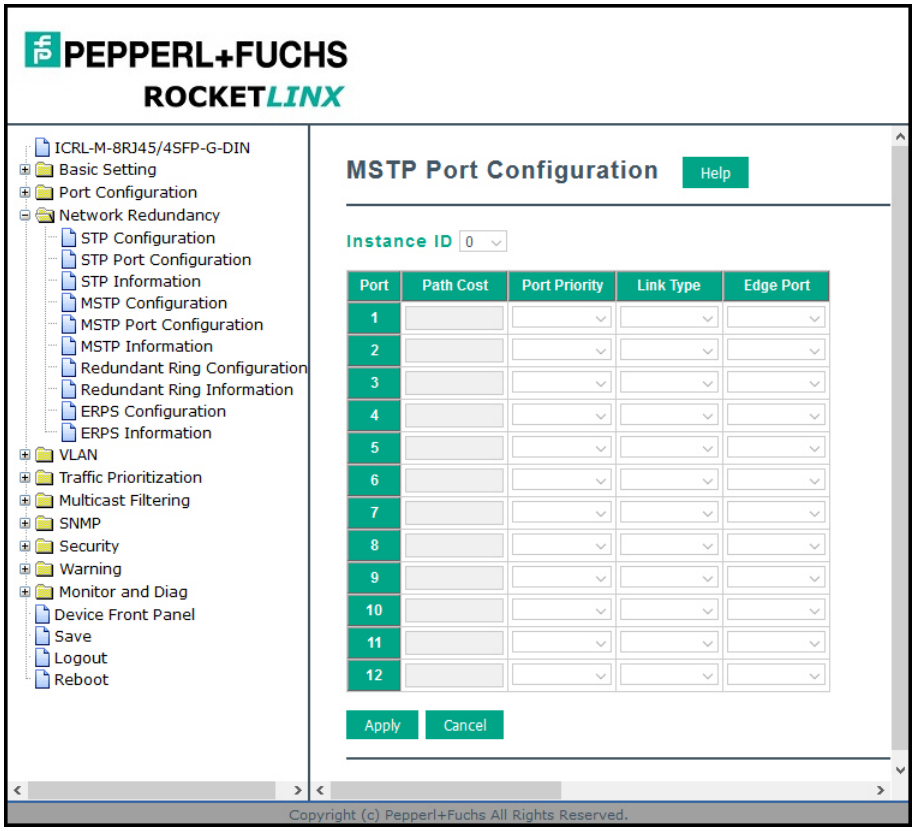


Seite „MSTP Configuration“	
MST Region Configuration	
Region Name	Ein Name zur Identifizierung der MST-Region. Maximale Länge: 32 Zeichen.
Revision	Ein Wert zur Identifizierung der MST-Region. Bereich: 0–65535 (Standard: 0).
Apply	Klicken Sie auf die Schaltfläche **Apply**, um die **MST Region Configuration** anzuwenden.
New MST Instance	
Instance ID	Ein Wert, der zur Identifizierung der MST-Instanz verwendet wird. Gültige Werte sind 1 bis 15. Instanz 0 (CIST, Common Internal Spanning Tree) ist eine spezielle Instanz von Spanning Tree, bekannt als IST oder Internal Spanning Tree (=MSTI00).
VLAN Group	Geben Sie eine VLAN-Gruppe an, um diese MST-Instanz zuzuordnen. Verwenden Sie eine VLAN-Nummer (z. B. 10), einen Bereich (z. B. „1-10“) oder ein Mischformat (z. B.: „2,4,6,4-7,10“).
Instance Priority	Ein Wert zur Identifizierung der MST-Instanz. Die MST-Instanz mit dem niedrigsten Wert hat die höchste Priorität und wird als Root ausgewählt. Geben Sie eine Zahl zwischen 0 und 61.440 in Schritten von 4096 ein.

Seite „MSTP Configuration“ (Fortsetzung)	
Add	Klicken Sie auf die Schaltfläche **Add**, um **New MST Instance** hinzuzufügen.
Current MST Instance Configuration	
Instance ID	Ein Wert zur Identifizierung der MST-Instanz. Instanz 0 (CIST, Common Internal Spanning Tree) ist eine spezielle Instanz von Spanning Tree, bekannt als IST oder Internal Spanning Tree (=MSTI00).
VLAN Group	Geben Sie eine VLAN-Gruppe an, um diese MST-Instanz zuzuordnen. Verwenden Sie die VLAN-Nummer, z. B.: 10. Sie können einen Bereich (z. B. „1-10“) oder bestimmte VLANs festlegen (z. B. „2,4,6,4-7“).
Instance Priority	Ein Wert zur Identifizierung der MST-Instanz. Die MST-Instanz mit dem niedrigsten Wert hat die höchste Priorität und wird als Root ausgewählt. Geben Sie eine Zahl zwischen 0 und 61.440 in Schritten von 4096 ein.
Apply	Klicken Sie auf die Schaltfläche **Apply**, um die aktuelle **MST Instance Configuration** anzuwenden. ***Anmerkung:*** *Sie müssen die Einstellungen mit **Save** speichern (Seite 159), wenn Sie diese Einstellungen nach Ausschalten des ICRL-M beibehalten möchten.*

4.5.5. MSTP Port Configuration

Auf dieser Seite können Sie die Porteinstellungen konfigurieren. Wählen Sie die Instanz-ID, die Sie konfigurieren möchten.

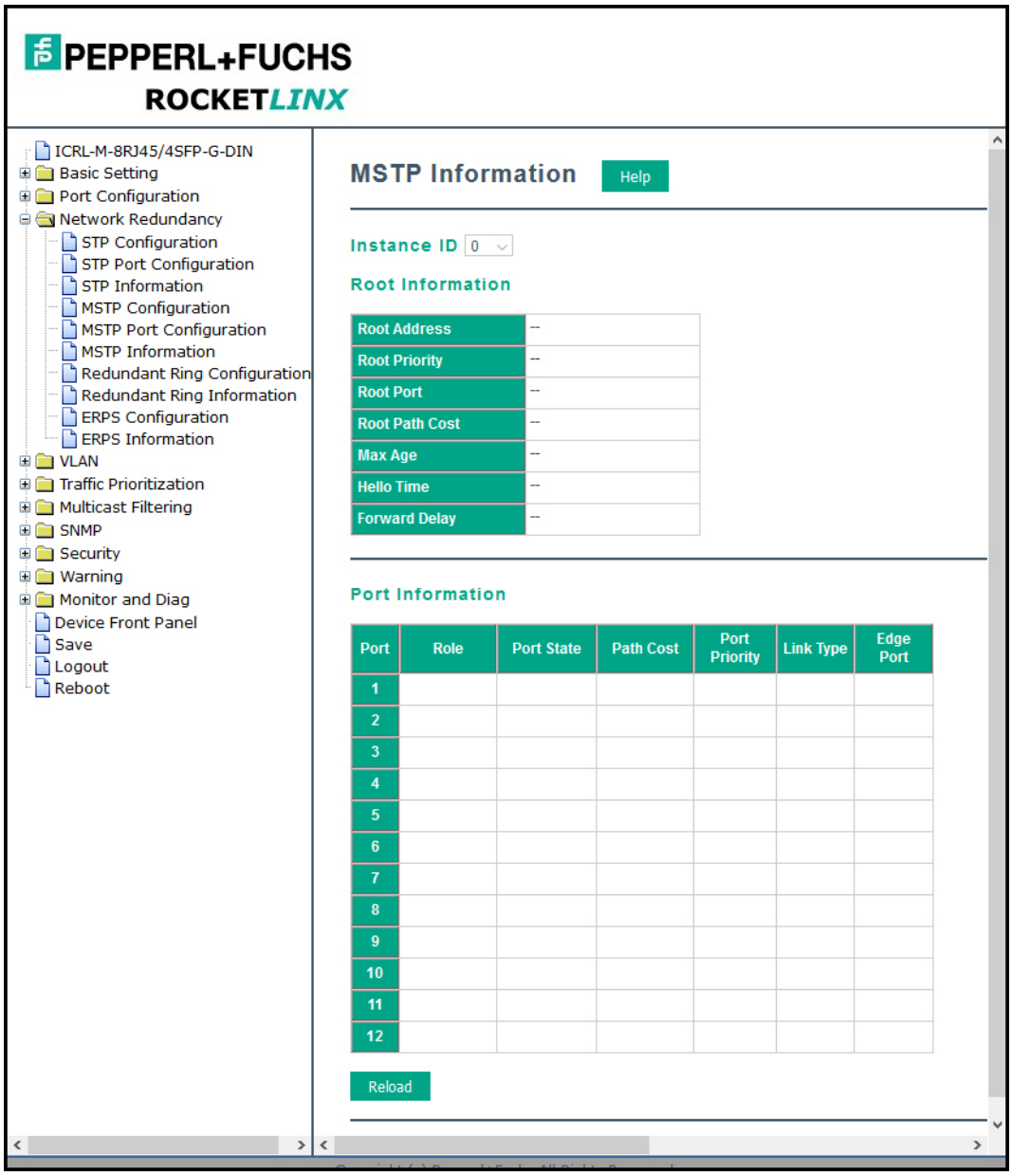


Seite „MSTP Port Configuration“	
Instance ID	Wählen Sie eine Instanz-ID aus, um die MSTP-Instanzeinstellung anzuzeigen und zu ändern.
Portkonfiguration	
Path Cost	Die Kosten für den Pfad zur anderen Bridge von dieser Übertragungsbrücke am angegebenen Port. Geben Sie eine Zahl zwischen 1 und 200.000.000 ein.
Port Priority	Entscheiden Sie, welcher Port in Ihrem LAN nach Priorität gesperrt werden soll. Geben Sie eine Zahl zwischen 0 und 240 in Schritten von 16 ein.
Link Type	Einige der schnellen Statustransaktionen, die innerhalb von RSTP möglich sind, hängen davon ab, ob der betreffende Port mit genau einer anderen Bridge verbunden ist (d. h., er wird von einem Punkt-zu-Punkt-LAN-Segment bedient) oder mit zwei oder mehr Brücken verbunden ist (d. h., er wird von einem gemeinsamen mittleren LAN-Segment bedient). Mit dieser Konfiguration kann der P2P-Status der Verbindung von einem Administrator gesteuert werden.
Edge Port	In Implementierungen vorhanden, die die Identifizierung von Edge-Ports unterstützen. Alle Ports, die direkt mit den Endstationen verbunden sind, können keine Bridging-Schleifen im Netzwerk erstellen und können somit direkt in die Weiterleitung übergehen und die Abhör- und Lernphase überspringen. Wenn das Nicht-Bridge-Gerät einen Edge-Port verbindet, befindet sich dieser Port in einem blockierenden Zustand und wechselt zu einem Weiterleitungsstatus in 2 x Hello-Zeit Sekunden. Wenn das Verbindungsgerät einen Edge-Port verbindet, handelt es sich bei diesem Port automatisch um einen Nicht-Edge-Port.

Seite „MSTP Port Configuration“ (Fortsetzung)	
Apply	Klicken Sie auf die Schaltfläche **Apply**, um die Konfiguration anzuwenden. ***Anmerkung:*** *Sie müssen die Einstellungen mit **Save** speichern (Seite 159), damit diese Einstellungen nach Ausschalten des ICRL-M beibehalten werden.*

4.5.6. MSTP Information

Auf dieser Seite können Sie die aktuellen MSTP-Informationen anzeigen. Wählen Sie zuerst die Instanz-ID aus. Wenn die Instanz nicht hinzugefügt wird, bleiben die Informationen leer.

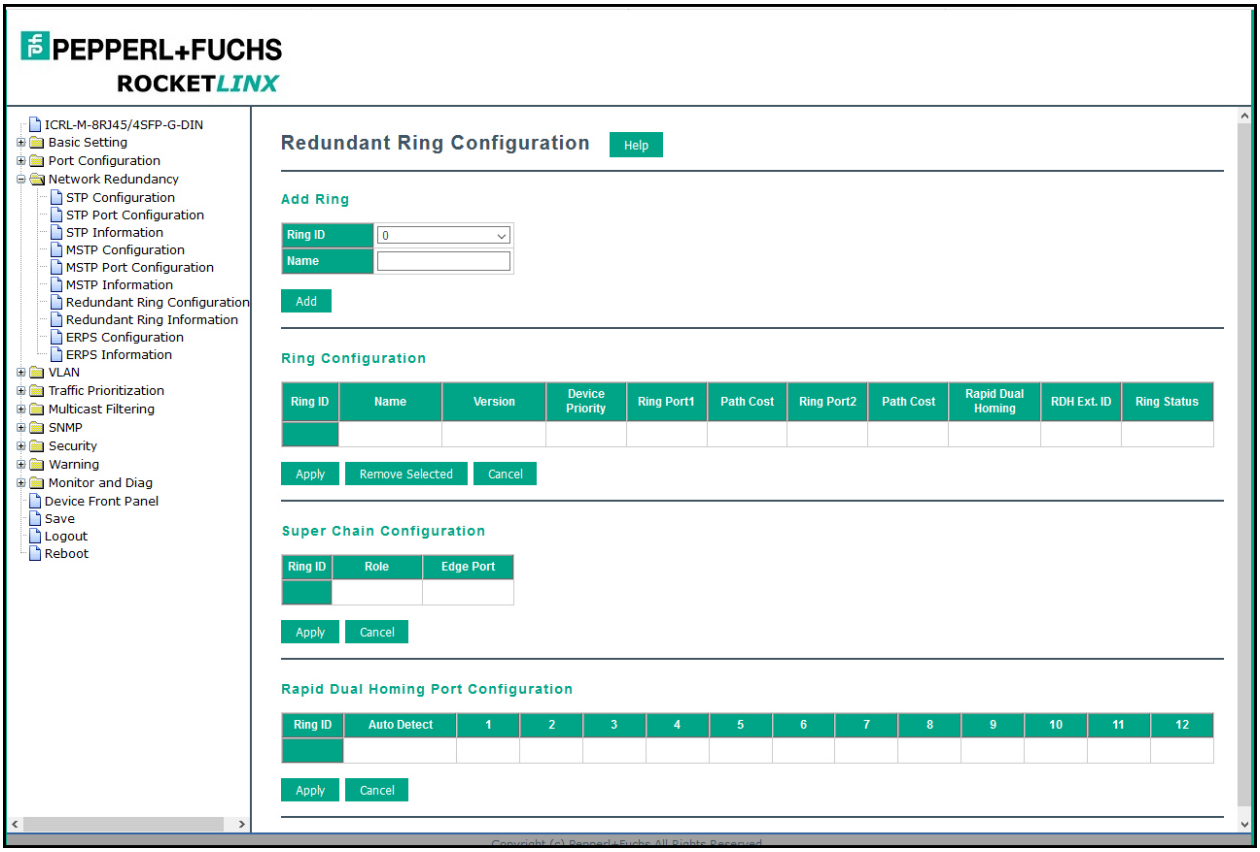


5/21/20

Seite „MSTP Information“	
Instance ID	Wählen Sie eine Instanz-ID, um MSTP-Instanzinformationen anzuzeigen. Instanz 0 (CIST, Common Internal Spanning Tree) ist eine spezielle Instanz von Spanning Tree, bekannt als IST oder Internal Spanning Tree (=MSTI00).
Root Information	
Root Address	Root-Bridge-Adresse, bei der es sich um die Bridge mit der kleinsten (niedrigsten) Bridge-ID handelt.
Root Priority	Root-Bridge-Priorität; die Bridge mit dem niedrigsten Wert hat die höchste Priorität und wird als Root ausgewählt.
Root Port	Root-Port dieser Bridge.
Root Path Cost	Root-Pfadkosten.
Max Age	Die Zeit in Sekunden, die eine Bridge wartet, ohne STP-Konfigurationsnachrichten zu empfangen, bevor sie versucht, neu zu konfigurieren.
Hello Time	Die Anzahl der Sekunden zwischen den Übertragungen von STP-Konfigurationsnachrichten.
Forward Delay	Die Anzahl der Sekunden, die ein Port wartet, bevor er vom STP-Lern- und -Abhörstatus in den Weiterleitungsstatus wechselt.
Port Information	
Port Role	Beschreibende Informationen über die MSTP-Switchport-Rolle. Role: Master, Root, Designated, Alternate, Backup, Boundary, Disabled, Unknown.
Port State	Beschreibende Informationen über den MSTP-Switchport-Status. State: Blocking, Listening, Learning, Forwarding, Disabled, Unknown.
Path Cost	Die Kosten für den Pfad zur anderen Bridge von dieser Übertragungsbrücke am angegebenen Port. Der Pfadkostenbereich liegt zwischen 1 und 200.000.000.
Port Priority	Entscheiden Sie, welcher Port in Ihrem LAN nach Priorität gesperrt werden soll. Der Bereich liegt zwischen 0 und 240 in Schritten von 16.
Link Type	Betriebsverbindungstyp. Einige der schnellen Statustransaktionen, die innerhalb von MSTP möglich sind, hängen davon ab, ob der betreffende Port mit genau einer anderen Bridge verbunden (d. h., er wird von einem Punkt-zu-Punkt-LAN-Segment bedient) oder mit zwei oder mehr Brücken verbunden werden kann (d. h., er wird von einem gemeinsamen mittleren LAN-Segment bedient).
Edge Port	Betriebs-Edge-Port-Status. In Implementierungen vorhanden, die die Identifizierung von Edge-Ports unterstützen. Alle Ports, die direkt mit den Endstationen verbunden sind, können keine Bridging-Schleifen im Netzwerk erstellen und können somit direkt in die Weiterleitung übergehen und die Abhör- und Lernphase überspringen. Wenn das Nicht-Bridge-Gerät einen Edge-Port verbindet, befindet sich dieser Port in einem blockierenden Zustand und wechselt zu einem Weiterleitungsstatus in 2 x Hello-Zeit Sekunden. Wenn das Verbindungsgerät einen Edge-Port verbindet, handelt es sich bei diesem Port automatisch um einen Nicht-Edge-Port.
Reload	Klicken Sie auf die Schaltfläche **Reload**, um die MSTP-Instanzinformationen neu zu laden.

4.5.7. Redundant Ring Configuration

Die gängigste Redundanz im industriellen Netzwerk besteht darin, einen Ring oder eine Schleife zu bilden. In der Regel werden verwaltete Switches in Reihe geschaltet und der letzte Switch wird wieder an den ersten angeschlossen. In einer solchen Verbindung können Sie die Ringredundanz-Technologie implementieren.

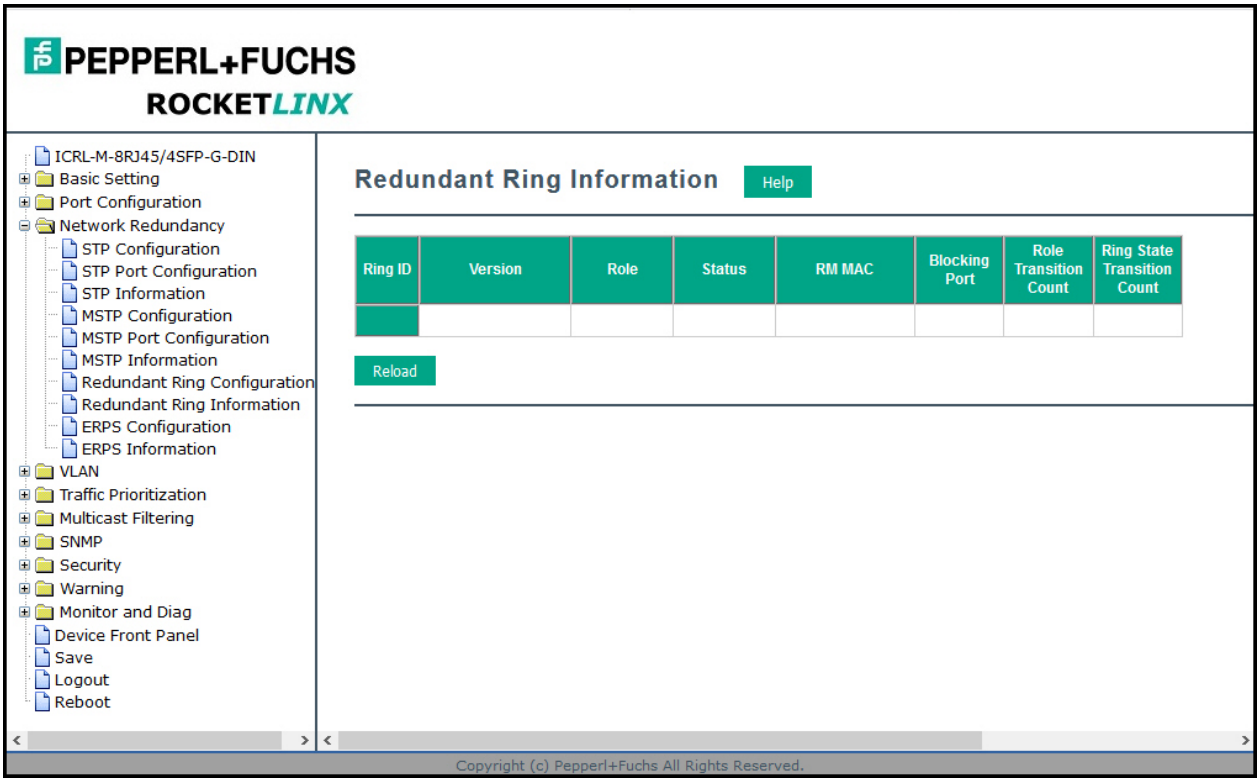


Seite „Redundant Ring“	
Ring ID/Name	Um einen redundanten Ring zu erstellen, wählen Sie die Ring-ID aus, die zwischen 0 und 31 liegt. Wenn das Namensfeld leer bleibt, wird der Name dieses Rings automatisch mit der Ring-ID benannt. Die maximale Anzahl der Ringe beträgt 32. ***Anmerkung:*** *Nachdem ein Ring erstellt wurde, können Sie ihn nicht mehr ändern.*
Ring Configuration	
Ring ID	Nachdem ein Ring erstellt wurde, wird die Ring-ID angezeigt und kann nicht mehr geändert werden. In Umgebungen mit mehreren Ringen kann der Datenverkehr nur unter derselben Ring-ID weitergeleitet werden. Denken Sie daran, die Ring-ID zu prüfen, wenn mehr als ein Ring vorhanden ist.
Name	In diesem Feld wird der Name des Rings angezeigt. Wenn dieser Wert beim Erstellen nicht eingegeben wird, wird er automatisch von der Regel *RingID* benannt.
Version	Die Version des Rings kann hier geändert werden. Zur Auswahl stehen **Rapid Super Ring** oder **Super Chain**.

Seite „Redundant Ring“ (Fortsetzung)	
Device Priority	Der Switch mit der höchsten Priorität (höchster Wert) wird automatisch als **Ring Master** (RM) ausgewählt. Wenn einer der Ringanschlüsse auf diesem Switch zu einem Weiterleitungsport wird und der andere zu einem blockierenden Port wird. Wenn alle Switches dieselbe Priorität haben, wird der Switch mit der höchsten MAC-Adresse als Ring Master ausgewählt.
Ring Port1	In einer **Rapid Super Ring**-Umgebung sollten Sie zwei Ringports haben. Gibt an, ob dieser Switch ein Ring Master ist oder nicht. Bei der Konfiguration von **Rapid Super Rings** sollten zwei Ports als Ringports ausgewählt werden. Bei einem Ringmaster wird einer der Ringports zum Weiterleitungsport und der andere zum blockierenden Port.
Path Cost	Ändern Sie den **Path Cost**-Wert von „Ring Port1“. Wenn dieser Switch der Ring Master eines Rings ist, dann bestimmt er den blockierenden Port. Der Port mit höherem **Path Cost**-Wert unter den beiden Ringports wird zum blockierenden Port. Wenn die **Path Cost**-Werte identisch sind, wird der Port mit der höheren Portnummer zum blockierenden Port.
Ring Port2	Weisen Sie einen anderen Port für die Ringverbindung zu.
Path Cost	Ändern Sie den **Path Cost**-Wert von „Ring Port2“.
Rapid Dual Homing	Rapid Dual Homing ist eine wichtige Funktion der Rapid Super Ring-Redundanztechnologie. Wenn Sie mehrere RSR-Verbindungen herstellen oder eine redundante Topologie mit anderen Anbietern erstellen möchten, können Sie mit RDH ohne Probleme maximal sieben Mehrfachverbindungen für Redundanz bereitstellen. In RDH müssen Sie keinen bestimmten Port konfigurieren, um eine Verbindung zu einem anderen Protokoll herzustellen. RDH wählt die schnellste Verbindung für die primäre Verbindung und blockiert alle anderen Verbindungen, um eine Schleife zu vermeiden. Wenn die primäre Verbindung fehlgeschlagen ist, leitet RDH automatisch an die sekundäre Verbindung für eine redundante Netzwerkverbindung weiter. Wenn mehr Verbindungen vorhanden sind, sind diese Standbyverbindungen und werden wiederhergestellt, wenn sowohl primäre als auch sekundäre Links unterbrochen sind.
RDH Ext ID	Dies ist die Rapid Dual Homing-Erweiterungs-ID. Die Erweiterungs-ID und die Ring-ID dürfen nicht identisch sein, wenn zwei Heimnetzwerke mit demselben externen Netzwerk verbunden sind. Der Erweiterungs-ID-Bereich liegt zwischen 0 und 7. Mit der Kombination aus Erweiterungs-ID (0 bis 7) und Ring-ID (0 bis 31) unterstützt der ICRL-M bis zu 256 (8 x 32) verschiedene Dual-Homing-Ringe.
Ring Status	Um den Ring mit **Enable**/**Disable** zu (de-)aktivieren, denken Sie daran, den Ring erst zu aktivieren, nachdem Sie ihn hinzugefügt haben.
Super Chain Configuration	
ID	Die Ring-ID, die sich auf diesen Ring (Chain) bezieht.
Role	Super Chain hat zwei Knotenrollen: **Border** und **Member**. **Border** ist der Knoten, der eine Verbindung zu einem externen Netzwerk herstellt. **Member** sind die Knoten (mit Ausnahme des **Border**-Knotens) in der Super Chain.
Edge Port	**Edge Port** ist einer der Ringports des **Border**-Knotens. Er wird für die Verbindung mit einem externen Netzwerk verwendet.
Rapid Dual Homing Port Configuration	
Ring ID	Die Ring-ID, die sich auf diesen Ring bezieht.
Auto Detect	Aktivieren Sie den RDH-Portmodus (Rapid Dual Homing) mit automatischer Erkennung.
Apply	Klicken Sie auf **Apply**, um die Einstellungen anzuwenden. ***Anmerkung:*** *Sie müssen die Einstellungen mit **Save** speichern (Seite 159), wenn Sie diese Einstellungen nach Ausschalten des ICRL-M beibehalten möchten.*

4.5.8. Redundant Ring Information

Auf dieser Seite werden Informationen zum redundanten Ring angezeigt.

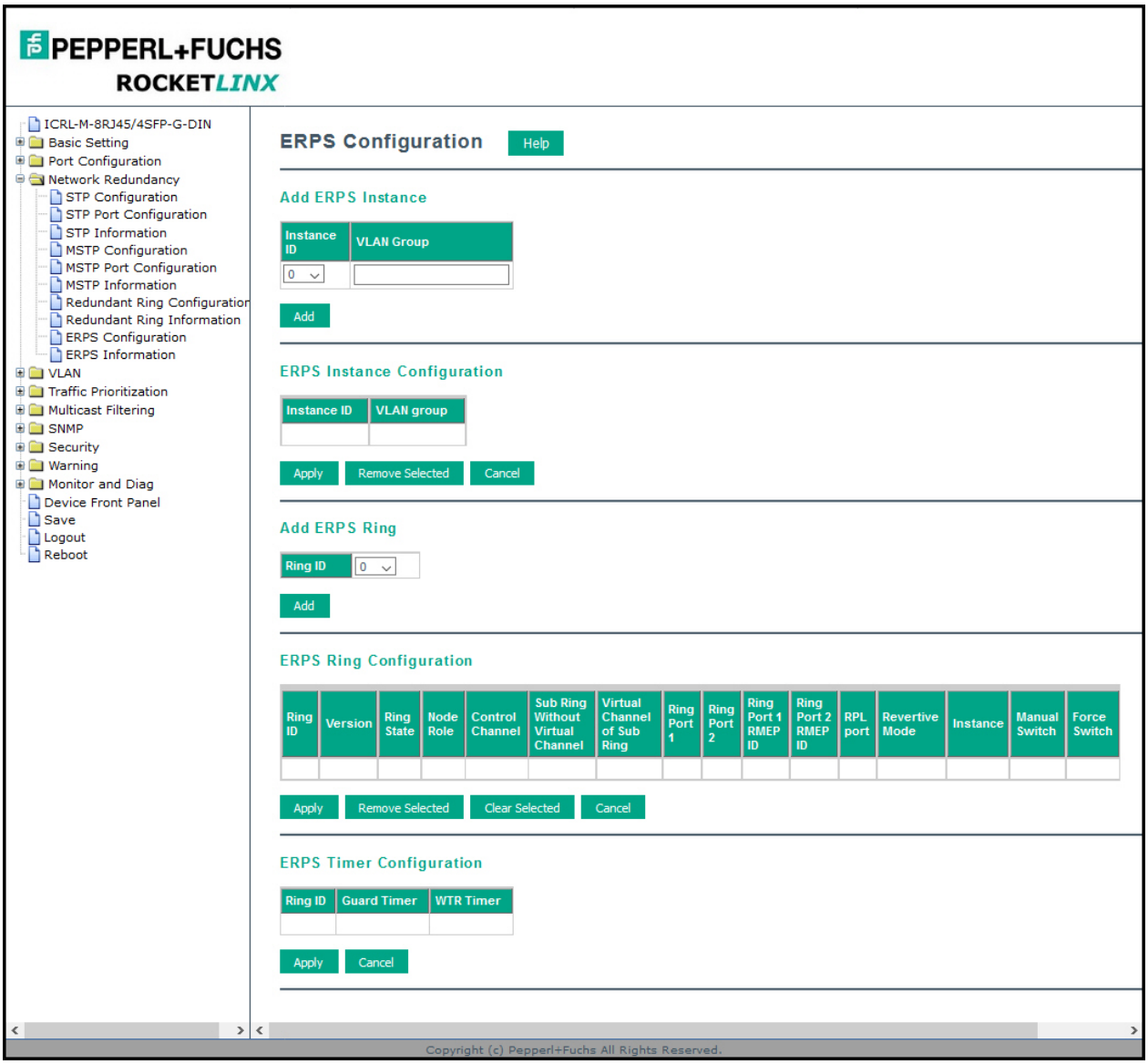


Seite „Redundant Ring Information“	
Ring ID	Die Ring-ID.
Version	Zeigt die Ringversion an. Dieses Feld kann „Rapid Super Ring“ oder „Super Chain“ enthalten.
Role	Dieser ICRL-M ist RM (Ring Master) oder nonRM (nicht Ring Master).
Zustand	Wenn dieses Feld **Normal** lautet, bedeutet dies, dass die Redundanz genehmigt wurde. Wenn eine der Verbindungen in diesem Ring defekt ist, lautet der Status **Abnormal**.
RM MAC	Die MAC-Adresse des Ring Master dieses Rings, die hilft, den redundanten Pfad zu finden.
Blocking Port	Zeigt an, welcher der blockierende Port des RM ist.
Role Transition Count	Zeigt an, wie oft dieser ICRL-M seine Rolle von nonRM zu RM oder von RM zu nonRM geändert hat.
Ring State Transition Count	Zeigt an, wie oft der Ringstatus zwischen **Normal** und **Abnormal** geändert wurde.
Reload	Klicken Sie hier, um die Informationen zum redundanten Ring erneut zu laden.

4.5.9. ERPS Configuration

Ethernet Ring Protection Switching (ERPS) implementiert die ITU-T-Empfehlung (G.8032), um eine Wiederherstellung des Ethernet-Datenverkehrs in einer Ringtopologie im Bereich von unter 50 ms zu ermöglichen und gleichzeitig sicherzustellen, dass sich keine Schleifen auf Ethernet-Ebene bilden.

Der Hauptvorteil dieser Funktion ist, dass es sich um eine Ringtechnologie nach Industriestandard handelt, mit der Sie den ICRL-M mit den Switches anderer Hersteller in einen G.8032-Ring schalten können.

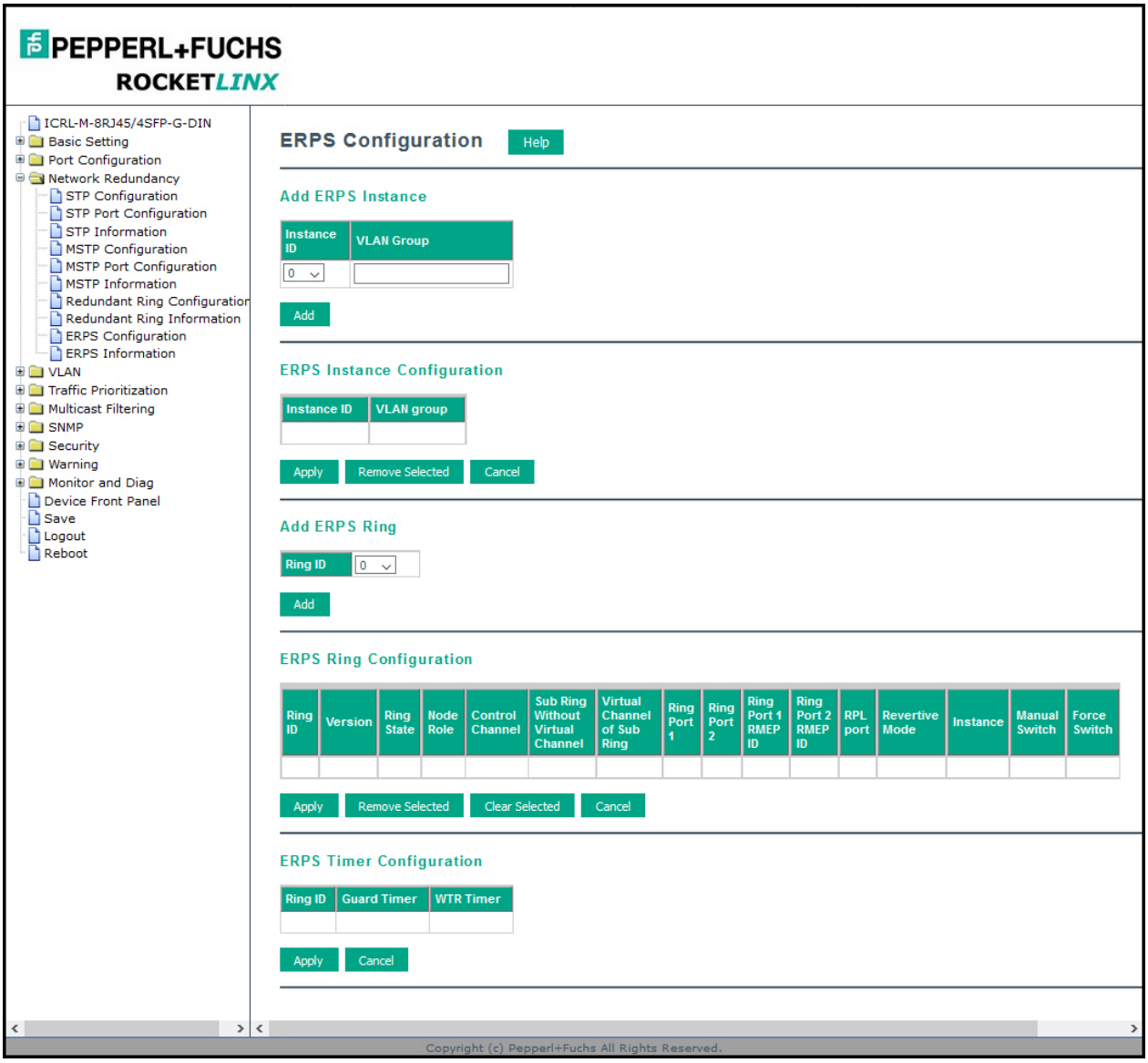


Seite „ERPS Configuration“	
Add ERPS Instance	
Instance ID	Die ERPS-Instanzidentität. Gültige Werte liegen zwischen 0 und 15.
VLAN Group	Die VLAN-ID-Mitglieder der Instanz-ID. Klicken Sie auf die Schaltfläche **Add**, um diese ERPS-Instanz hinzuzufügen.
ERPS Instance Configuration	
Instance ID	Die ERPS-Instanzidentität. Gültige Werte liegen zwischen 0 und 15.
VLAN Group	Die VLAN-ID-Mitglieder der Instanz-ID. • Klicken Sie auf die Schaltfläche **Add**, um die ERPS-Instanz hinzuzufügen. • Um eine MST-Instanz zu entfernen, aktivieren Sie das Kontrollkästchen der Instanz-ID, die Sie entfernen möchten, und klicken Sie auf die Schaltfläche **Remove Selected**. • Klicken Sie auf die Schaltfläche **Cancel**, um die aktuellen Einstellungen neu zu laden.
Add ERPS Ring	
Ring ID	Die ERPS-Ring-Identität. Gültige Werte sind 0 bis 31. Klicken Sie auf **Add**, um den ERPS-Ring hinzuzufügen.
ERPS Ring Configuration	
Ring ID	Die ERPS-Ring-Identität.
Version	ERPs weist Version 1 und 2 auf.
Ring State	Der aktuelle Status des Rings: Disable, Major oder Sub.
Node Role	Die Rolle des Knotens: **RPL Owner** und **Ring Node**. Der **RPL Owner** ist ein Ethernet-Ringknoten neben dem RPL.
Control Channel	Steuerungskanal zur Bereitstellung eines Kommunikationskanals für die Übertragung von automatischen Ring-Schutzschaltungen (R-APS).
Sub Ring Without Virtual Channel	Wählen Sie diese Option, um den virtuellen Kanal für die Übertragung des automatischen Sub-Ring-Schutzschalters (R-APS) zu verwenden.
Virtual Channel of Sub Ring	Steuerungskanal zur Bereitstellung eines Kommunikationskanals für die Übertragung von automatischen Sub-Ring-Schutzschaltungen (R-APS).
Ring Port	Eine Ringverbindung wird von zwei benachbarten Knoten begrenzt und ein Port für eine Ringverbindung wird als Ringport bezeichnet.
RMEP ID	Die Endpunkt-ID der Remote-Wartungsverknüpfung (MEP) des Ringports.
RPL Port	Die Ringschutzverbindung (Ring Protection Link, RPL) ist die Ringverbindung, die unter normalen Bedingungen, d. h. ohne Ausfall oder Anfrage, für den Verkehrskanal blockiert wird, um die Bildung von Schleifen zu verhindern.
Revertive Mode	Im Revertive-Modus wurden alle Ringverbindungen und Knoten wiederhergestellt. Die blockierende Verbindung wird auf die RPL-Verbindung zurückgesetzt. Im nicht umkehrenden Modus kehrt der Ring nicht automatisch zurück.
Instance	Wählen Sie eine ERPS-Instanz, um sie zu steuern.
Manual Switch	Ermöglicht es dem Betreiber, einen bestimmten Ringport manuell zu blockieren.

Seite „ERPS Configuration“	
Force Switch	Ermöglicht es dem Betreiber, die Blockierung eines bestimmten Ringports zu erzwingen.
Apply	Klicken Sie auf **Apply**, um die Einstellungen anzuwenden. ***Anmerkung:*** *Sie müssen die Einstellungen mit **Save** speichern (Seite 159), wenn Sie diese Einstellungen nach Ausschalten des ICRL-M beibehalten möchten.*
Remove Selected	Wählen Sie den Ring aus und klicken Sie dann auf diese Schaltfläche, um einen Ring zu entfernen.
Clear Selected	Wählen Sie den Ring aus und klicken Sie dann auf diese Schaltfläche, um einen vorhandenen FS- oder MS-Befehl am Ringport abzubrechen.
Cancel	Klicken Sie auf diese Schaltfläche, um diese Änderung abzubrechen.
ERPS Ring Configuration	
Ring ID	Die ERPS-Ring-Identität.
Guard Timer	Der Guard-Timer. Gültige Werte sind 10 bis 2000 ms, Standard sind 100 ms.
WTR Timer	Der WTR-Timer (Wait-to-Restore). Gültige Werte sind 1 bis 12 Minuten, Standard sind 5 Minuten.
Cancel	Klicken Sie auf diese Schaltfläche, um diese Änderung abzubrechen.
Apply	Klicken Sie auf **Apply**, um die Einstellungen anzuwenden. ***Anmerkung:*** *Sie müssen die Einstellungen mit **Save** speichern (Seite 159), wenn Sie diese Einstellungen nach Ausschalten des ICRL-M beibehalten möchten.*

4.5.10. ERPS Information

Diese Seite enthält Informationen zu ERPS.

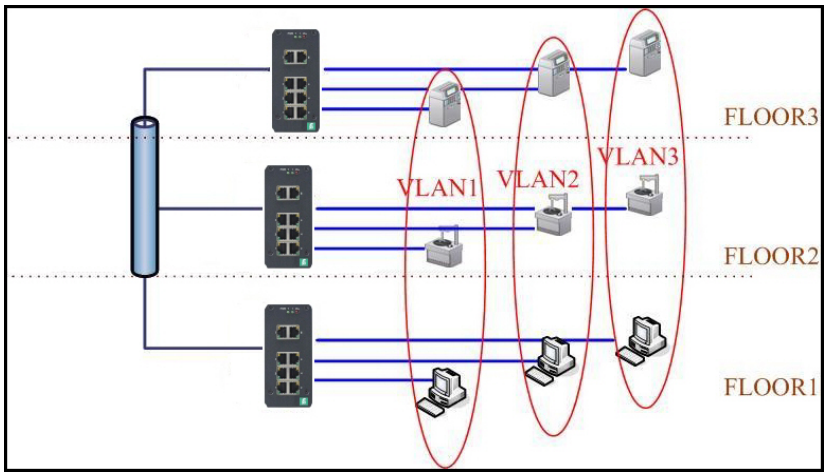


4.6. VLAN

Ein virtuelles LAN (VLAN) ist eine logische Gruppierung von Knoten, um eine Broadcast-Domain auf bestimmte Mitglieder einer Gruppe zu beschränken, ohne die Mitglieder physisch zu gruppieren. Das VLAN ermöglicht es Ihnen, den Netzwerkverkehr so zu isolieren, dass nur Mitglieder des VLAN Datenverkehr von Mitgliedern desselben VLAN empfangen können. Im Grunde ist die Erstellung eines VLAN über einen Switch das logische Äquivalent zur physischen Neuverbindung einer Gruppe von Netzwerkgeräten mit einem anderen Layer-2-Switch, ohne diese Geräte tatsächlich von ihren ursprünglichen Switches zu trennen.

Der ICRL-M unterstützt IEEE-802.1Q-VLAN, das auch als Tag-Based VLAN bezeichnet wird. Dieses Tag-Based VLAN ermöglicht die Erstellung eines VLAN über verschiedene Switches hinweg. IEEE 802.1Q Tag-Based VLANs nutzen VLAN-Steuerungsinformationen, die in einem VLAN-Header gespeichert sind, der an IEEE-802.3-Paketframes angehängt ist. Dieses Tag enthält eine VLAN-Kennung (VID), die angibt, zu welchem VLAN ein Frame gehört. Da jeder Switch nur das Tag eines Frames prüfen muss, ohne den Inhalt des Frames zu untersuchen, spart dies eine Menge Rechenressourcen innerhalb des ICRL-M.

Die folgende Abbildung zeigt ein IEEE-802.1Q-VLAN.

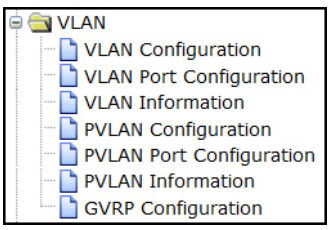


Der ICRL-M unterstützt VLAN-Tunneling (QinQ), wodurch die Anzahl der VLANs durch Hinzufügen eines Tags zu den 802.1Q-Paketen erweitert wird. Das ursprüngliche VLAN wird normalerweise als Kunden-VLAN (C-VLAN) identifiziert, und das neue VLAN als Service-VLAN (S-VLAN). Durch Hinzufügen des zusätzlichen Tags erhöht QinQ die mögliche Anzahl von VLANs. Nachdem QinQ aktiviert wurde, kann der ICRL-M bis zu 256 x 256 VLANs erreichen. Mit verschiedenen Standard-Tags wird auch die Netzwerksicherheit verbessert.

802.1Q Tunnel

802.1Q Tunnel Uplink

Auf den Seiten unter „VLAN Configuration“ können Sie ein VLAN hinzufügen und entfernen, Ingress-/Egress-Parameter des Ports konfigurieren und die VLAN-Tabelle anzeigen. Die folgenden Seiten sind in dieser Gruppe enthalten:

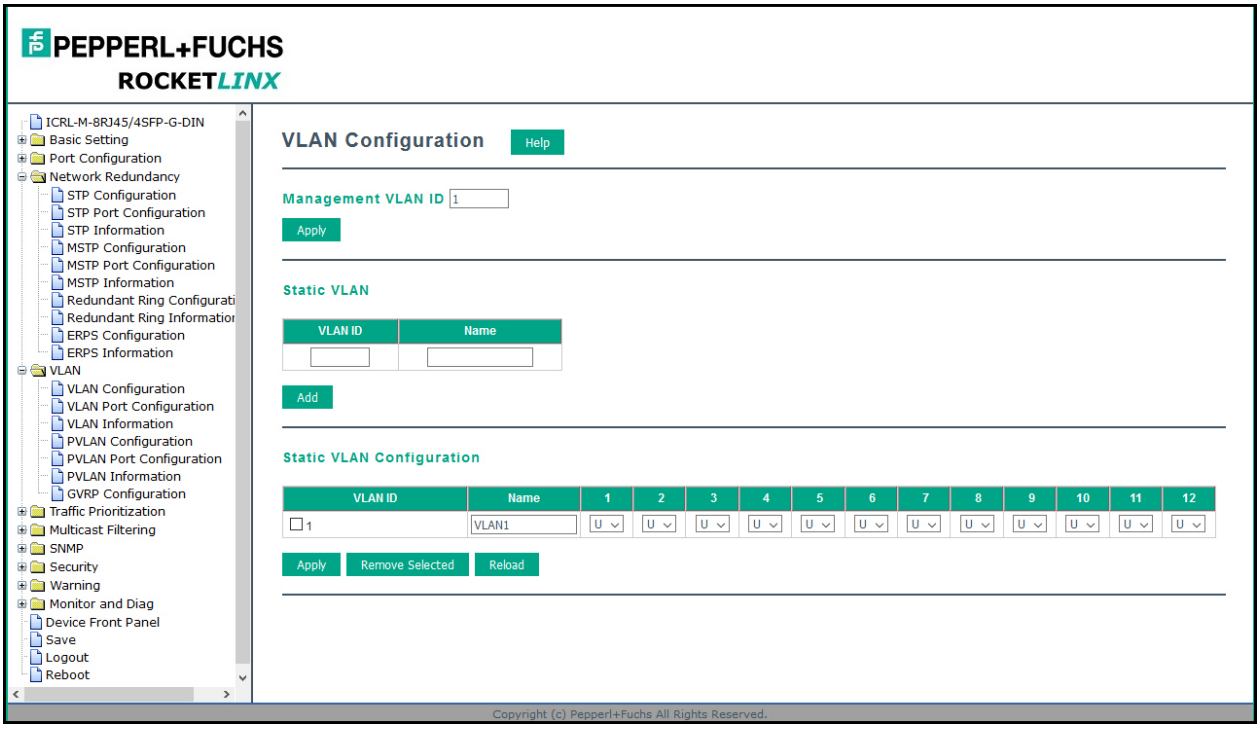


- *PVLAN Port Configuration* auf Seite 99
- *PVLAN Information* auf Seite 100
- *GVRP Configuration* auf Seite 101

Optional können Sie die Befehlszeilenschnittstelle (Command-Line Interface, CLI) für die Konfiguration verwenden (siehe *VLAN (CLI)* auf Seite 197).

4.6.1. VLAN Configuration

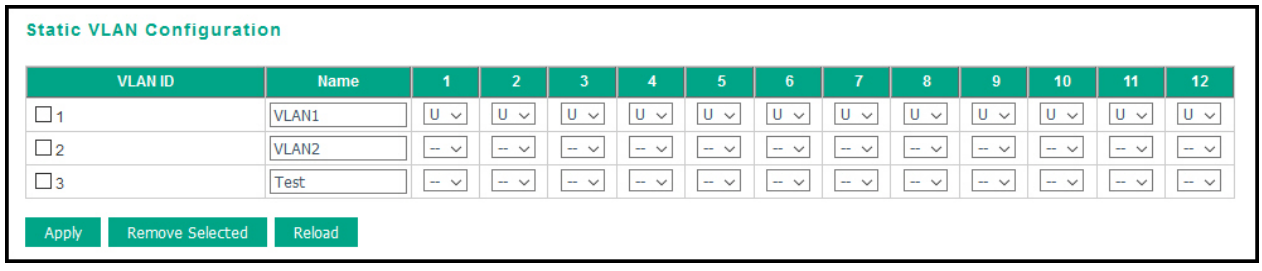
Verwenden Sie diese Seite, um das Management-VLAN zuzuweisen, das statische VLAN zu erstellen und die Egress-Regel für die Mitgliedsports des VLAN zuzuweisen.



Seite „VLAN Configuration“	
Management VLAN ID	Die Management-VLAN-ID ist die VLAN-ID der CPU-Schnittstelle, sodass nur Mitgliedsports des Verwaltungs-VLAN Ping-Befehle an den Switch senden und darauf zugreifen können. Die standardmäßige Management-VLAN-ID ist **1**. Klicken Sie nach der Eingabe der VLAN-ID auf **Apply**.
Static VLAN	Sie können dem neuen statischen VLAN eine VLAN-ID und einen VLAN-Namen zuweisen. • **VLAN ID**: Diese wird vom Switch verwendet, um verschiedene VLANs zu identifizieren. Eine gültige VLAN-ID liegt zwischen 1 und 4094; 1 ist das Standard-VLAN. • **VLAN Name**: Dies ist eine Referenz für den Netzwerkadministrator, um verschiedene VLANs zu identifizieren. Der VLAN-Name kann bis zu 12 Zeichen lang sein. Wenn Sie keinen VLAN-Namen angeben, weist das System automatisch einen VLAN-Namen zu. Die Regel ist „VLAN (VLAN-ID)“. Klicken Sie auf **Add**, um ein neues VLAN zu erstellen. Das neue VLAN wird in der Tabelle *Static VLAN Configuration* angezeigt. Nach der Erstellung des VLAN bleibt der Status des VLAN „Unused“, bis Sie dem VLAN Ports hinzufügen. ***Anmerkung:*** *Bevor Sie die Management-VLAN-ID per Web oder Telnet ändern, denken Sie daran, dass der vom Administrator verbundene Port ein Mitgliedsport des Management-VLAN sein sollte. Andernfalls kann der Administrator nicht über das Netzwerk auf den Switch zugreifen. Der ICRL-M unterstützt maximal 256 VLANs.*

Static VLAN Configuration	• **VLAN ID**: Die VLAN-ID für dieses VLAN.
	• **Name**: Der Name des VLAN.
	• 1–20: Die entsprechende Portnummer auf dem VLAN.
	  • **--** Nicht verfügbar
	  • **U** Tag aufheben: Gibt an, dass ausgehende Frames nicht VLAN-getaggt sind.
	  • **T** Taggen: Zeigt an, dass ausgehende Frames mit einem LAN-Tag versehen sind.
	• Klicken Sie auf **Apply**, um die Einstellungen anzuwenden.
	Anmerkung: *Sie müssen die Einstellungen mit **Save** speichern (Seite 159), wenn Sie diese Einstellungen nach Ausschalten des ICRL-M beibehalten möchten.*
	• Klicken Sie auf **Remove Selected**, um das ausgewählte statische VLAN zu entfernen.
	• Klicken Sie auf **Reload**, um die statische VLAN-Konfiguration neu zu laden.

Die folgende Abbildung zeigt eine Konfigurationstabelle für statische VLANs. Es wurden zwei neue VLANs erstellt („VLAN2“ und „Test“). Egress-Regeln der Ports sind nicht konfiguriert.

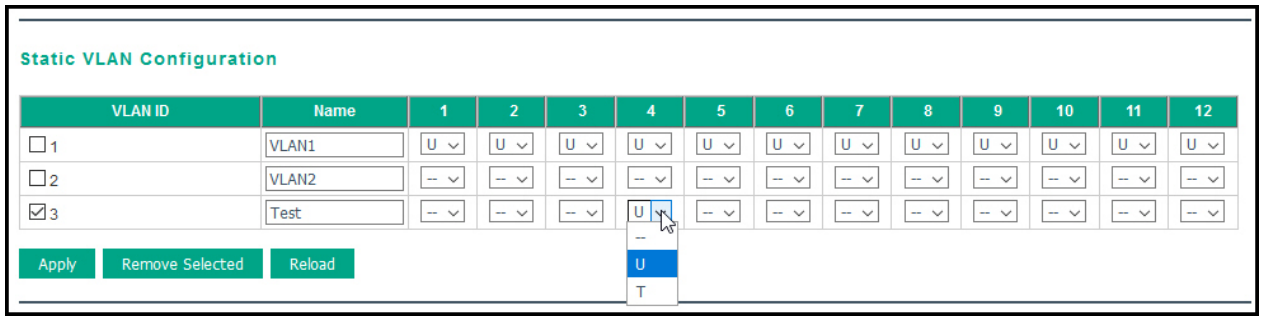


5/21/20

Die folgende Abbildung zeigt, wie die Egress-Regel der Ports konfiguriert wird.

Gehen Sie wie folgt vor, um Egress-Regeln zu konfigurieren:

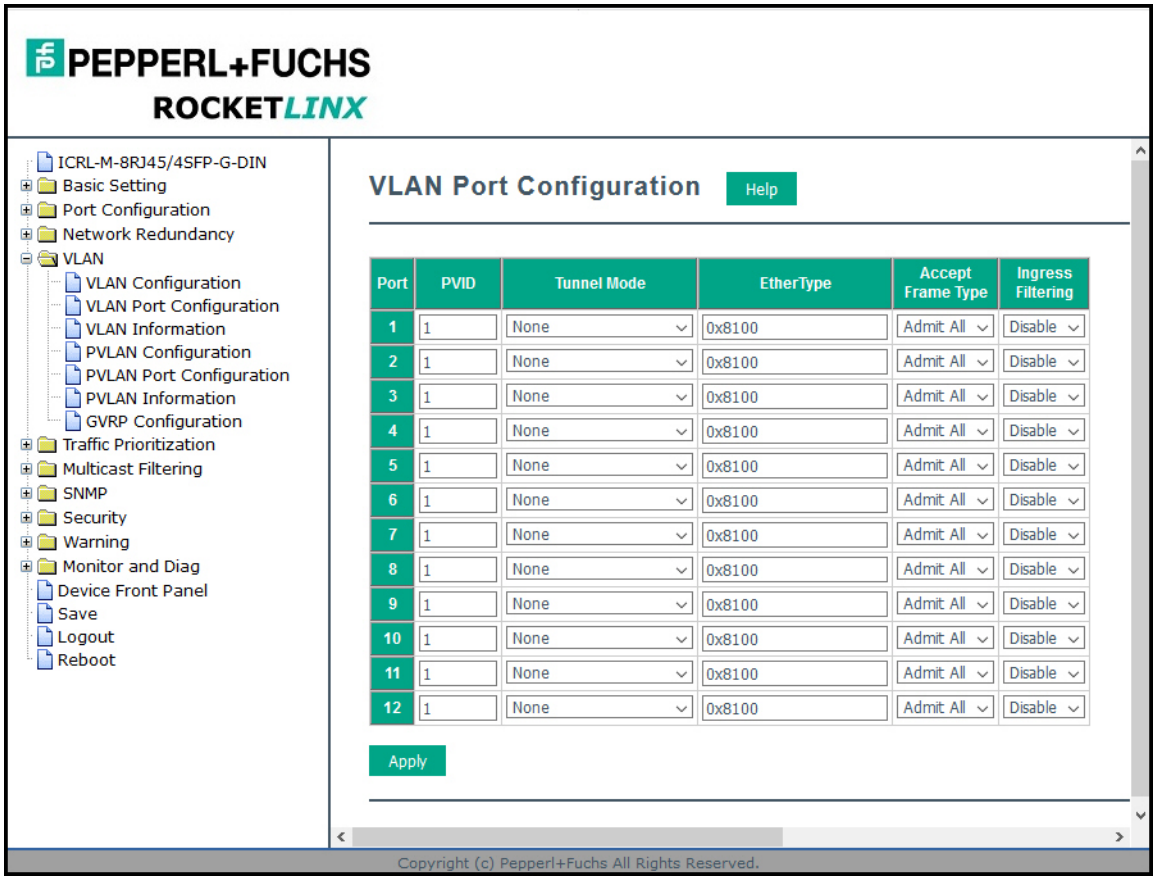
1. Weisen Sie die Egress-Regel der Ports **U** oder **T** zu.
2. Klicken Sie auf **Apply**, um die Einstellung zu übernehmen.



Wenn Sie ein VLAN entfernen möchten, wählen Sie den VLAN-Eintrag aus und klicken Sie dann auf die Schaltfläche **Remove**.

4.6.2. VLAN Port Configuration

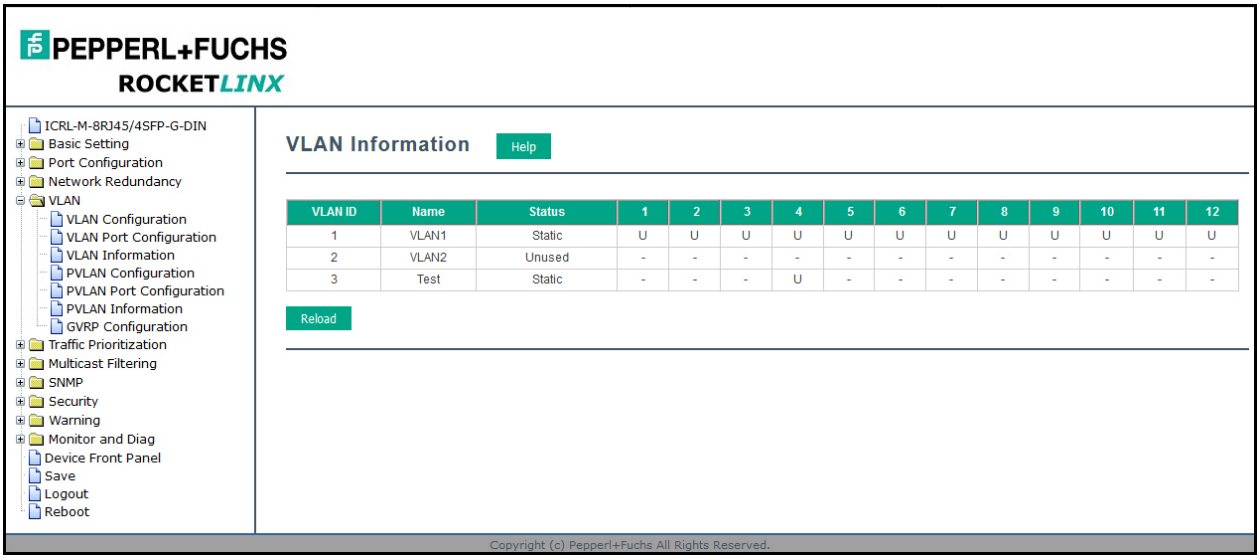
Auf der Seite *VLAN Port Configuration* können Sie VLAN-Portparameter an einem bestimmten Port konfigurieren. Tag-Based VLANs basieren auf der IEEE-802.1Q-Spezifikation. Datenverkehr wird an VLAN-Mitgliedsports weitergeleitet, basierend auf VLAN-Tags in den Datenpaketen. Sie können den Switch auch so konfigurieren, dass er mit vorhandenen Tag-Based-VLAN-Netzwerken und älteren Nicht-Tag-Netzwerken interoperiert.



Seite „VLAN Port Configuration“	
PVID	Geben Sie die Port-VLAN-ID (PVID) ein. Mit der PVID können die Switches identifizieren, welcher Port zu welchem VLAN gehört. Um die Dinge einfach zu halten, wird empfohlen, dass die PVID den VLAN-IDs entspricht. Die standardmäßige Port-VID: die VLAN-ID, die einem am Port empfangenen nicht getaggten oder nur mit der Priorität gekennzeichneten Frame zugewiesen ist. Der gültige Bereich liegt zwischen 1 und 4094. Geben Sie die PVID ein, die Sie konfigurieren möchten.
Tunnel Mode	**None**: IEEE-802.1Q-Tunnelmodus ist deaktiviert. **802.1Q Tunnel**: QinQ wird auf die Ports angewendet, die eine Verbindung zum C-VLAN herstellen. Der Port empfängt einen getaggten Frame vom C-VLAN. Sie müssen ein neues Tag (Port VID) als S-VLAN-VID hinzufügen. Wenn die Pakete an das C-VLAN weitergeleitet werden, wird das S-VLAN-Tag entfernt. Nachdem der **802.1Q Tunnel**-Modus einem Port zugewiesen wurde, sollte die Ausgangseinstellung für den Port *Untag* lauten. Dies weist darauf hin, dass das Ausgangspaket immer ungetaggt ist. Dies wird in der Tabelle **Static VLAN Configuration** (Seite 91) konfiguriert. **802.1Q Tunnel Uplink**: QinQ wird auf die Ports angewendet, die eine Verbindung zum S-VLAN herstellen. Der Port empfängt einen getaggten Frame vom S-VLAN. Wenn die Pakete an das S-VLAN weitergeleitet werden, wird das S-VLAN-Tag beibehalten. Nachdem der **802.1Q Tunnel Uplink**-Modus einem Port zugewiesen wurde, sollte die Ausgangseinstellung für den Port *Tag* lauten. Dies weist darauf hin, dass das Ausgangspaket immer getaggt ist. Dies wird in der Tabelle **Static VLAN Configuration** (Seite 91) konfiguriert. Beispiel: Wenn die VID von „S-VLAN/Tunnel Uplink“ 10 ist, ist die VID von „C-VLAN/Tunnel“ 5. Der 802.1Q-Tunnelport empfängt Tag 5 vom C-VLAN und fügt Tag 10 zum Paket hinzu. Wenn die Pakete an das S-VLAN weitergeleitet werden, wird Tag 10 beibehalten.
EtherType	Hierüber können Sie den EtherType manuell definieren. Dies ist ein erweiterter QinQ-Parameter, mit dem Sie den Übertragungspakettyp definieren können.
Accept Frame Type	Wenn Sie **Tag Only** auswählen, verwirft das Gerät nicht markierte Frames oder nur mit Priorität gekennzeichnete Frames, die an diesem Port empfangen werden. Wenn Sie **Admit All** festlegen, werden nicht getaggte oder nur mit Priorität gekennzeichnete Frames, die an diesem Port empfangen werden, akzeptiert und der PVID für diesen Frame zugewiesen. Diese Steuerung wirkt sich nicht auf VLAN-unabhängige BPDU-Frames aus, wie STP, GVRP und LACP. Sie wirkt sich auf VLAN-abhängige BPDU-Frames aus, wie z. B. GMRP.
Ingress Filtering	Die Ingress-Filterung weist die VLAN-Engine an, unerwünschten Datenverkehr an einem Port herauszufiltern. • Wenn Sie **Enable Ingress Filtering** festlegen, prüft der Port, ob die eingehenden Frames zu dem vom Frame angegebenen VLAN gehören oder nicht. Der Port bestimmt dann, ob die Frames verarbeitet werden können oder nicht. Wenn beispielsweise ein getaggter Frame vom *TEST VLAN* empfangen wird und die Eingangsfilterung aktiviert ist, bestimmt der ICRL-M, ob der Port in der *TEST VLAN*-Egress-Liste enthalten ist. Ist dies der Fall, kann der Frame bearbeitet werden. Ist dies nicht der Fall, wird der Frame verworfen. • Wenn Sie **Disable** auswählen, akzeptiert der Port alle eingehenden Frames unabhängig von ihrer VLAN-Klassifizierung. Diese Steuerung wirkt sich nicht auf VLAN-unabhängige BPDU-Frames aus, wie Super Ring, STP, GVRP und LACP. Sie wirkt sich auf VLAN-abhängige BPDU-Frames aus, wie z. B. GMRP.
Apply	Klicken Sie auf **Apply**, um die Einstellungen anzuwenden. ***Anmerkung:*** *Sie müssen die Einstellungen mit **Save** speichern (Seite 159), wenn Sie diese Einstellungen nach Ausschalten des ICRL-M beibehalten möchten.*

4.6.3. VLAN Information

Die Seite *VLAN Information* zeigt die aktuellen Einstellungen Ihrer VLAN-Tabelle an, einschließlich VLAN-ID, Name, Status und Egress-Regel der Ports.

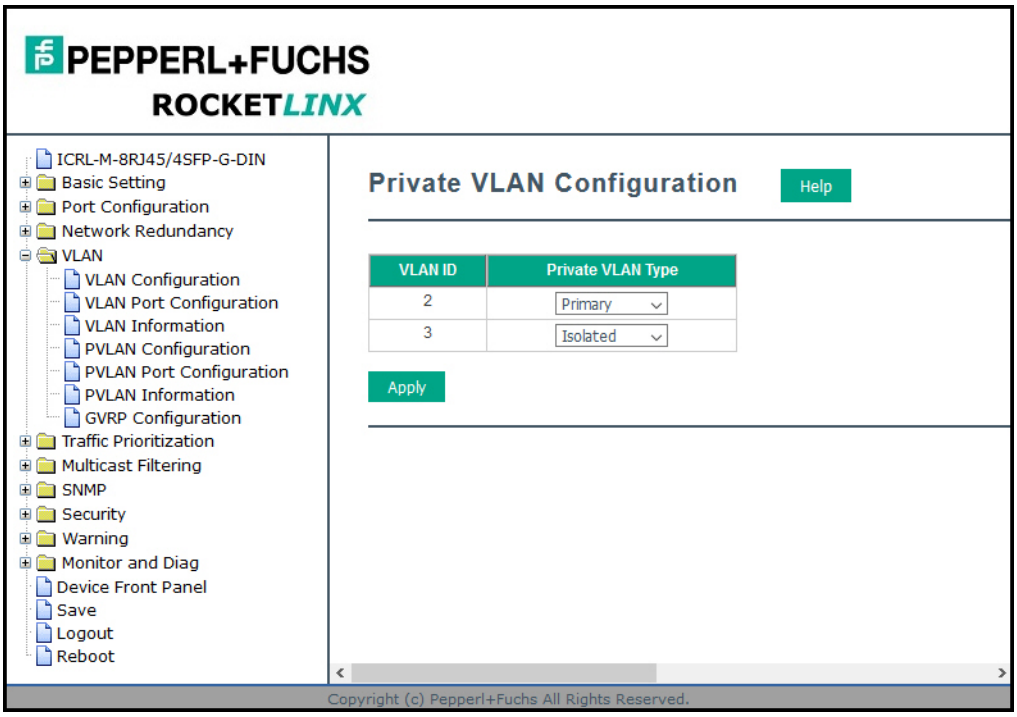


Seite „VLAN Information“	
VLAN ID	Die ID des VLAN.
Name	Der Name des VLAN.
Status	**Static** bedeutet, dass es sich um ein manuell konfiguriertes statisches VLAN handelt. **Unused** bedeutet, dass dieses VLAN über die Web-Benutzerschnittstelle/CLI erstellt wurde, aber noch nicht über Mitgliedsports verfügt und noch nicht funktioniert. **Dynamic** bedeutet, dass dieses VLAN von GVRP gelernt wurde. • **--** Keine VLAN-Einstellung. • **T** Ein Trunk-Link ist ein LAN-Segment, das für das Multiplexing von VLANs zwischen VLAN-Bridges verwendet wird. Alle Geräte, die eine Verbindung zu einem Trunk-Link herstellen, müssen IEEE-802.1Q-VLAN-fähig sein, da hier Frames mit IEEE-802.1Q-Tags gesendet und empfangen werden. • **U** Ein Access-Link ist ein LAN-Segment für nicht IEEE-802.1Q-VLAN-fähige Geräte an einem Port einer VLAN-Bridge. Geräte, die mit einem Access-Link verbunden sind, senden und empfangen Frames ohne IEEE-802.1Q-Tagging, d. h. ohne Identifizierung des VLAN, zu dem der Frame gehört.

4.7. Privates VLAN

Ein privates VLAN hilft bei der Behebung von Problemen mit der primären VLAN-ID, der Isolierung der Clientports und der Netzwerksicherheit. Die Private-VLAN-Funktionen bieten primäre und sekundäre VLANs innerhalb eines einzigen Switches.

Primäres VLAN: Der Uplink-Port ist in der Regel Mitglied des primären VLAN. Ein primäres VLAN enthält promiskuitive Ports, die mit sekundären VLANs kommunizieren können.



Sekundäres VLAN: Die Clientports werden in der Regel innerhalb des sekundären VLAN definiert. Das sekundäre VLAN umfasst isolierte und Community-VLANs. Die Clientports können isolierte VLANs sein oder im selben Community-VLAN gruppiert werden. Die Ports innerhalb desselben Community-VLAN können miteinander kommunizieren, die isolierten VLAN-Ports können jedoch nicht miteinander kommunizieren.

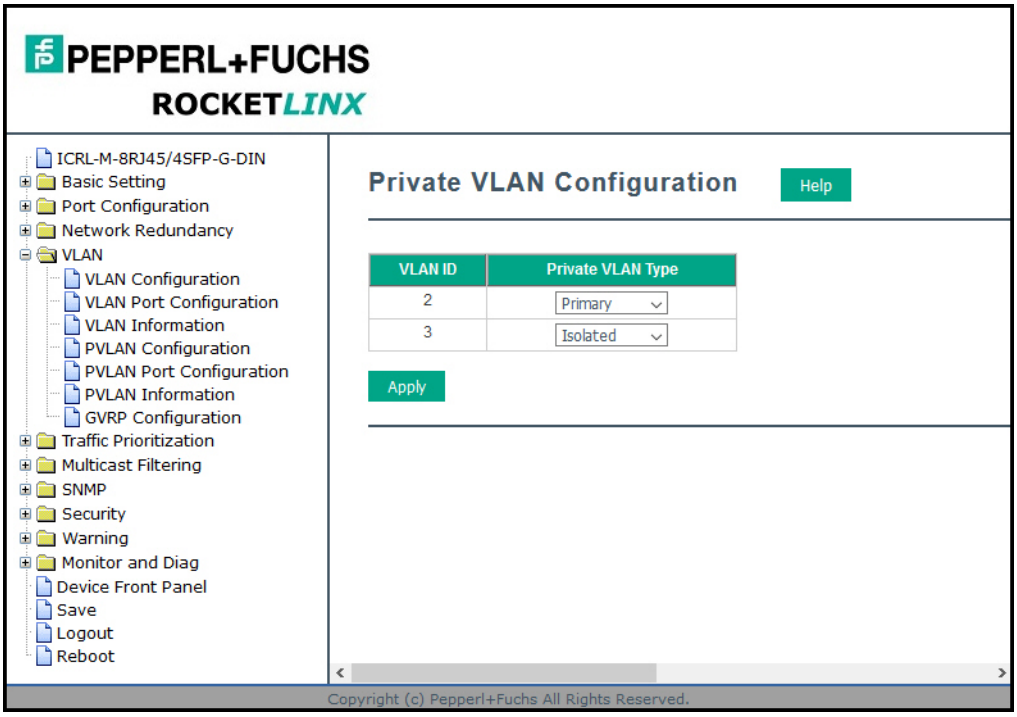
Diese Abbildung zeigt ein typisches privates VLAN. Ein SCADA/Public Server oder eine NMS-Workstation befindet sich in der Regel in einem primären VLAN. Client-PCs und -Ringe befinden sich in der Regel im sekundären VLAN.

Optional können Sie die Befehlszeilenschnittstelle (Command-Line Interface, CLI) für die Konfiguration verwenden (siehe *Privates VLAN (CLI)* auf Seite 201).

4.7.1. PVLAN Configuration

Mit der PVLAN-Konfiguration können Sie einen Private-VLAN-Typ zuweisen. Wählen Sie die Private-VLAN-Typen für jedes VLAN aus, das Sie konfigurieren möchten.

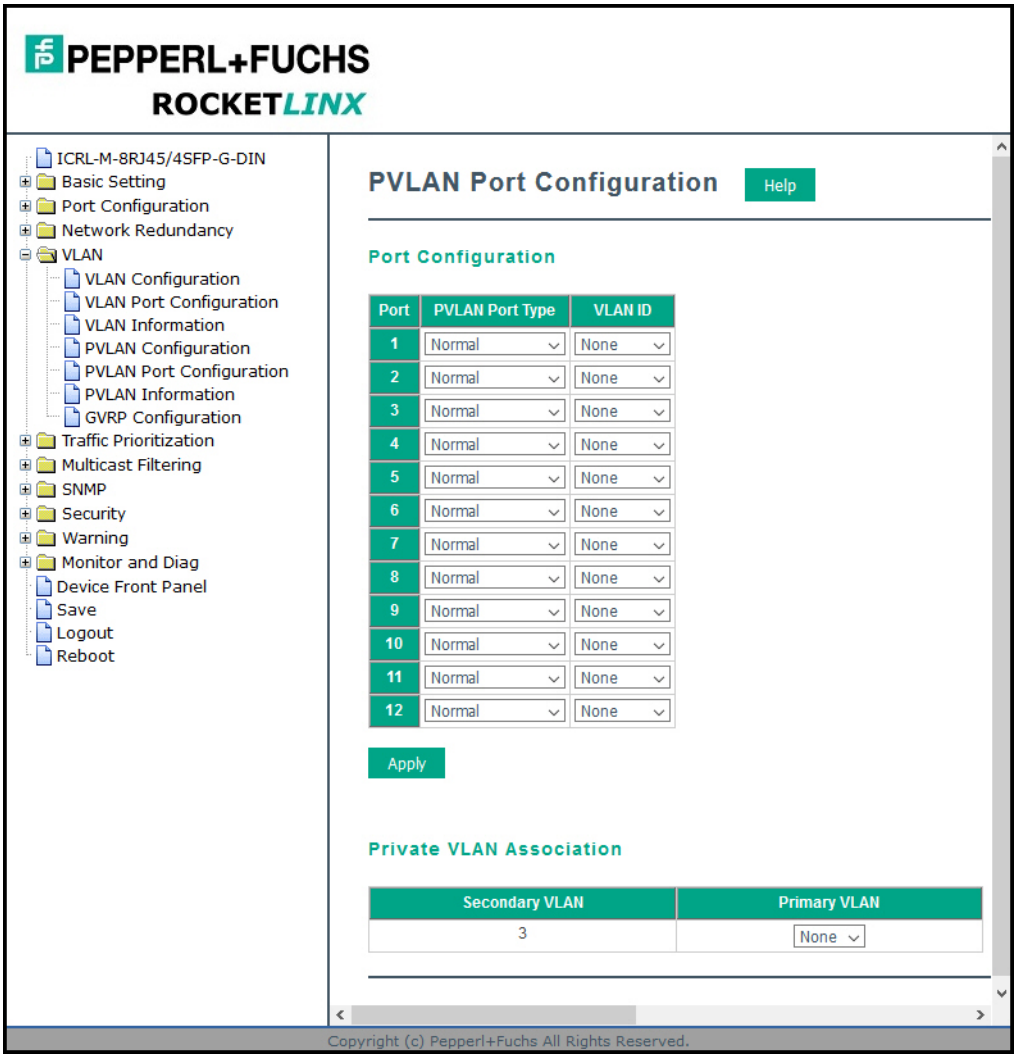
Anmerkung: *Sie müssen zuvor ein VLAN im Bildschirm „VLAN Configuration“ konfiguriert haben. Nähere Informationen finden Sie unter VLAN Configuration auf Seite 91.*



Seite „Private VLAN Configuration“	
VLAN ID	• *Primary VLAN*: Der Uplink-Port ist in der Regel das primäre VLAN. Ports innerhalb eines primären VLAN können mit Ports in einem sekundären VLAN kommunizieren • *Secondary VLAN*: Die Clientports werden in der Regel innerhalb des sekundären VLAN definiert. Das sekundäre VLAN umfasst isolierte und Community-VLANs. Die Clientports können isolierte VLANs sein oder im selben Community-VLAN gruppiert werden. Die Ports innerhalb desselben Community-VLAN können miteinander kommunizieren. Das gilt nicht für die isolierten VLAN-Ports.
Private VLAN Type	• **None**: Das VLAN ist nicht im privaten VLAN enthalten. • Primary: Ein primäres VLAN enthält promiskuitive Ports, die mit den sekundären VLANs kommunizieren können. • **Isolated**: Die Mitgliedsports des VLAN sind isoliert. • **Community**: Die Mitgliedsports des VLAN können miteinander kommunizieren.
Apply	Klicken Sie auf **Apply**, um die Einstellungen anzuwenden. ***Anmerkung:*** *Sie müssen die Einstellungen mit **Save** speichern (Seite 159), wenn Sie diese Einstellungen nach Ausschalten des ICRL-M beibehalten möchten.*

4.7.2. PVLAN Port Configuration

Auf der Seite *PVLAN Port Configuration* können Sie die Portkonfiguration und Private-VLAN-Verbindungen konfigurieren.

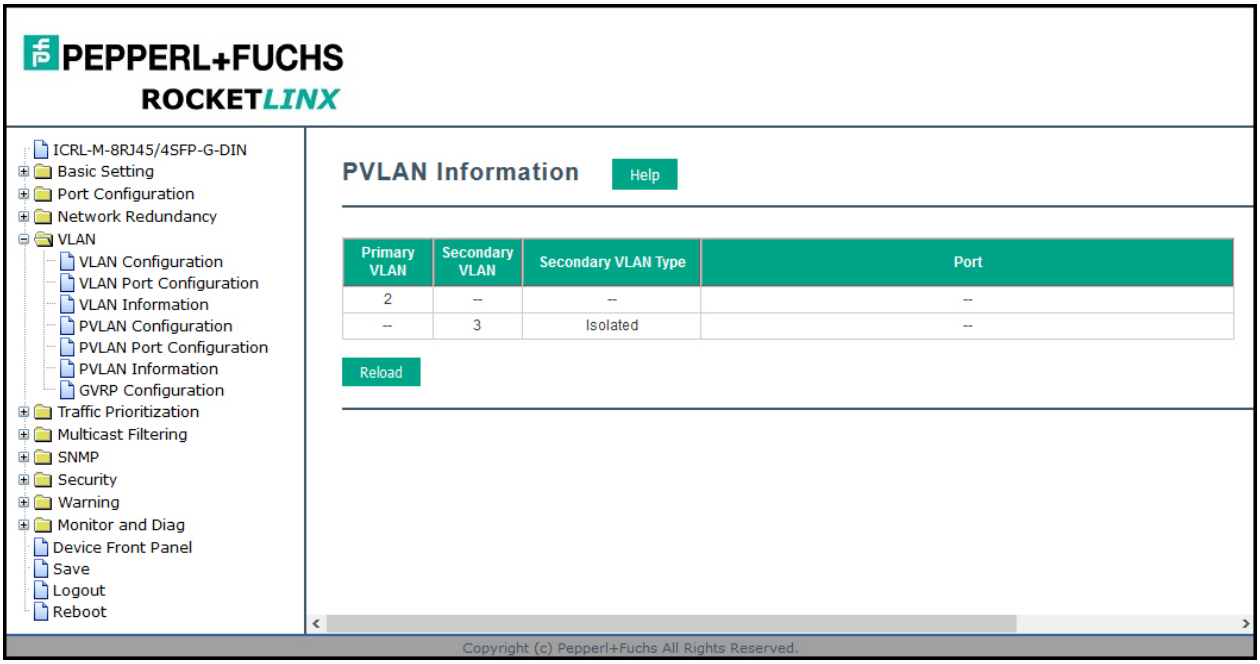


Seite „Private VLAN Port Configuration“	
PVLAN Port Type	Die folgenden Optionen stehen zur Verfügung: **Normal**: Normale Ports verbleiben in ihrer ursprünglichen VLAN-Konfiguration. **Host**: Hostports können dem sekundären VLAN zugeordnet werden. **Promiscuous**: Promiskuitive Ports können dem primären VLAN zugeordnet werden.
VLAN ID	Nach der Zuweisung des Porttyps wird die verfügbare VLAN-ID angezeigt, der der Port zugeordnet werden kann.

Seite „Private VLAN Port Configuration“ (Fortsetzung)	
Private VLAN Association	
Secondary VLAN	Nachdem die isolierten und Community-VLANs auf der Seite *Private VLAN Configuration* konfiguriert wurden, werden die VLANs angezeigt, die zum zweiten VLAN gehören.
Primary VLAN	Nachdem der primäre VLAN-Typ auf der Seite *Private VLAN Configuration* zugewiesen wurde, kann das sekundäre VLAN der primären VLAN-ID zugeordnet werden. ***Anmerkung:*** *Vor der Konfiguration des PVLAN-Porttyps sollte zuerst die private VLAN-Zuordnung durchgeführt werden.*

4.7.3. PVLAN Information

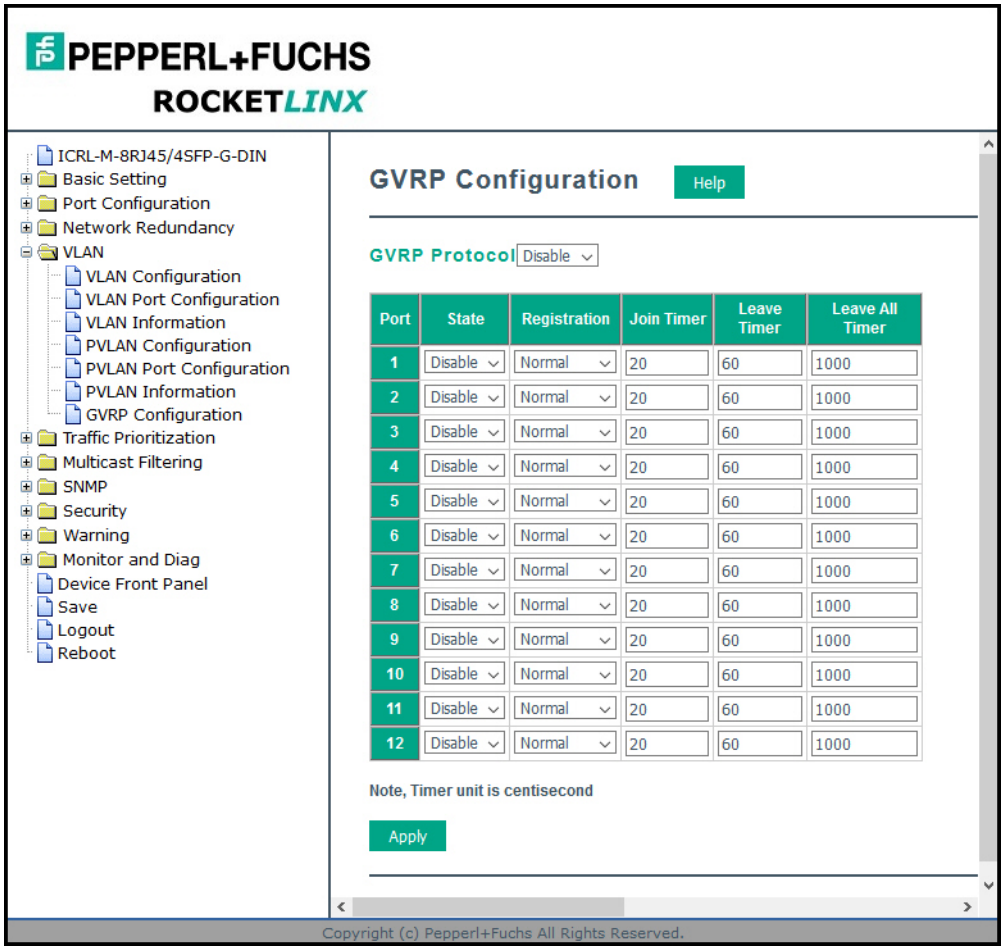
Auf der Seite *PVLAN Information* können Sie die Private-VLAN-Informationen anzeigen. Klicken Sie auf **Reload**, um den Seiteninhalt zu aktualisieren.



4.7.4. GVRP Configuration

Das GARP VLAN Registration Protocol (GVRP) ermöglicht Ihnen die automatische Einrichtung von VLANs anstelle einer manuellen Konfiguration an jedem Port auf jedem Switch im Netzwerk. GVRP entspricht der IEEE-802.1Q-Spezifikation. Diese definiert eine Methode zum Tagging von Frames mit VLAN-Konfigurationsdaten, mit der Netzwerkgeräte VLAN-Konfigurationsinformationen dynamisch mit anderen Geräten austauschen können.

GARP (Generic Attribute Registration Protocol), ein Protokoll, das Verfahren definiert, mit denen die Endstationen und Switches in einem LAN (Local Area Network) Attribute, wie IDs oder Adressen, registrieren und deregistrieren können. Jede Endstation und jeder Switch verfügt somit über eine aktuelle Aufzeichnung aller anderen Endstationen und Schalter, die erreicht werden können. GVRP verhindert, wie GARP, unnötigen Netzwerkverkehr, indem Versuche vermieden werden, Informationen an nicht registrierte Benutzer zu übertragen. Außerdem muss nur ein Switch manuell konfiguriert werden und alle anderen Switches werden entsprechend konfiguriert.



Seite „GVRP Configuration“	
GVRP Protocol	(De-)Aktivieren Sie GVRP mit **Enable**/**Disable** global.
State	Nach der globalen Aktivierung von GVRP können Sie GVRP mit **Enable**/**Disable** auch für einzelne Ports (de-)aktivieren.
Registration	Dieser Wert legt den Registrierungsmodus von GVRP fest (Standard ist der Normalmodus).

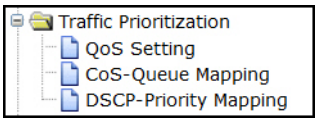
Seite „GVRP Configuration“ (Fortsetzung)	
Join Timer	Steuert das Intervall für das Senden der GVRP-Join-BPDU (Bridge Protocol Data Unit). Eine Instanz dieses Timers ist pro Port und pro GARP-Teilnehmer erforderlich.
Leave Timer	Steuert die Zeit für die Freigabe der GVRP-Reservierung nach Erhalt der GVRP-Leave-BPDU. Eine Instanz des Timers ist für jede Zustandsmaschine erforderlich, die sich im LV-Zustand befindet.
Leave All Timer	Steuert den Zeitraum, in dem die Garbage Collection des registrierten VLAN initiiert wird. Der Timer ist pro Port und GARP-Teilnehmer erforderlich.
Apply	Klicken Sie auf **Apply**, um die Einstellungen anzuwenden. ***Anmerkung:*** *Sie müssen die Einstellungen mit **Save** speichern (Seite 159), wenn Sie diese Einstellungen nach Ausschalten des ICRL-M beibehalten möchten.*

4.7. Datenverkehr-Priorisierung

Quality of Service (QoS) bietet einen Mechanismus zur Priorisierung des Datenverkehrs, mit dem Sie einen besseren Service für bestimmte Datenflüsse bereitstellen können. QoS kann auch dazu beitragen, Überlastungsprobleme zu beseitigen und sicherzustellen, dass Datenverkehr mit hoher Priorität zuerst bereitgestellt wird. In diesem Abschnitt können Sie die *Traffic Prioritization*-Einstellungen für jeden Port konfigurieren, um Prioritäten festzulegen.

ICRL-M QoS unterstützt vier physische Warteschlangen, WRR (Weighted Fair Queuing) und das Strict Priority Scheme, das dem IEEE-802.1p-CoS-Tag und den IPv4-TOS/DiffServ-Informationen folgt, um den Datenverkehr Ihres industriellen Netzwerks zu priorisieren.

Die folgenden Webseiten sind in dieser Gruppe enthalten:

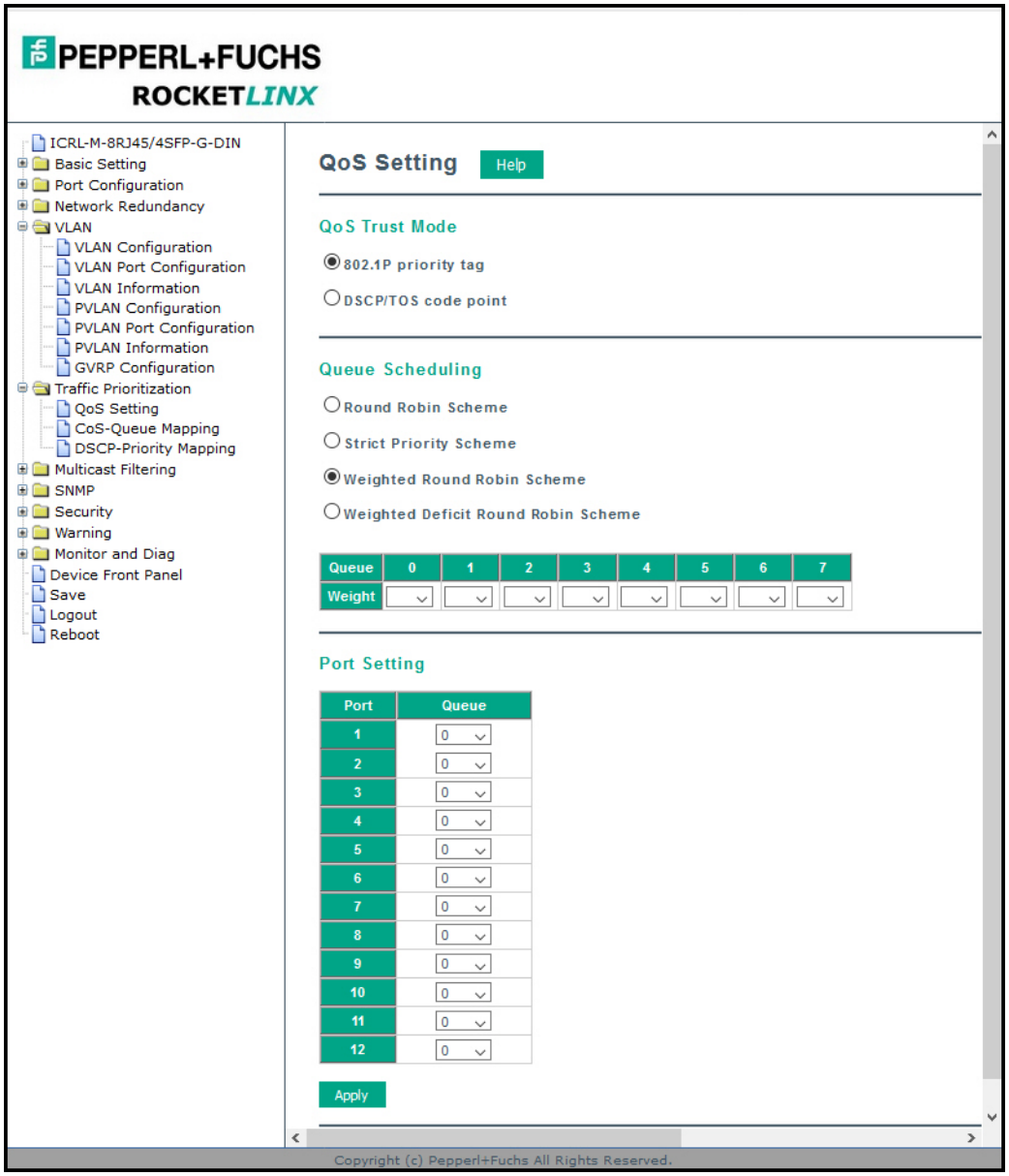


- *QoS Setting*
- *CoS-Queue Mapping* auf Seite 106
- *DSCP-Priority Mapping* auf Seite 107

Optional können Sie die Befehlszeilenschnittstelle (Command-Line Interface, CLI) für die Konfiguration verwenden (siehe *Datenverkehr-Priorisierung (CLI)* auf Seite 205).

4.7.1. QoS Setting

Verwenden Sie diesen Unterabschnitt, um die QoS-Einstellungen für den ICRL-M einzurichten.



Seite „QoS Setting“	
Queue Trust Mode	
802.1P Priority Tag	Wenn 802.1P ausgewählt ist, nutzt der ICRL-M die CoS-Informationen eines Pakets, um die Priorität zu bestimmen. Dies hängt mit den Einstellungen auf der Seite *CoS-Queue Mapping* zusammen.
DSCP/TOS Code Point	Bei Auswahl von DSCP/TOS verlässt sich der Switch zur Bestimmung der Priorität auf Codepunktinformationen für differenzierte Pakete. Dies hängt mit den Einstellungen auf der Seite *DSCP-Priority Mapping* zusammen.
Queue Scheduling	
Round Robin Scheme	Das Round-Robin-Schema bedeutet, dass alle Prioritäten die gleiche Berechtigung haben und der Datenverkehr wird zyklisch weitergeleitet, vom höchsten zum niedrigsten.
Strict Priority Scheme	Pakete mit einer höheren Priorität in der Warteschlange werden immer zuerst verarbeitet, es gibt jedoch kein Paket mit höherer Priorität.
Use Weighted Round Robin scheme	Mit diesem Schema können Benutzer jeder Klasse ein neues Gewichtungsverhältnis zuweisen. 10 ist die höchste Gewichtung. Die Gewichtung der einzelnen Klasse lautet wie folgt: Wx/W0 + W1 + W2 + W3 + W4 + W5 + W6 + W7 (Gesamtvolumen Warteschlangen 0–7)
Weighted Deficit Round Robin Scheme	Mit diesem Schema können Sie jeder Klasse ein neues Gewichtungsverhältnis zuweisen. Die Gewichtung 2032 ist das Maximum; die Gewichtung 0 ist das Minimum; der Wert muss gerade sein. Die Einstellung 0 legt die reine Prioritätsplanung fest. Die programmierbare Gewichtungseinstellung reicht von 1 bis 127. Gesamtvolumen der Warteschlangen 0–7.
Port Setting	
Queue	Wählen Sie den Warteschlangenwert für die einzelnen Ports aus. Der Port weist daraufhin seine Standardpriorität auf. Warteschlange 7 ist die höchste portbasierte Warteschlange, 0 die niedrigste. Der am Port eingespeiste Datenverkehr folgt bei der Weiterleitung der Warteschlangenebene. Der ausgehende Datenverkehr nimmt die Warteschlangenebene jedoch nicht zum nächsten Switch mit.
Apply	Klicken Sie auf **Apply**, um die Einstellungen anzuwenden. ***Anmerkung:*** *Sie müssen die Einstellungen mit **Save** speichern (Seite 159), wenn Sie diese Einstellungen nach Ausschalten des ICRL-M beibehalten möchten.*

4.7.2. CoS-Queue Mapping

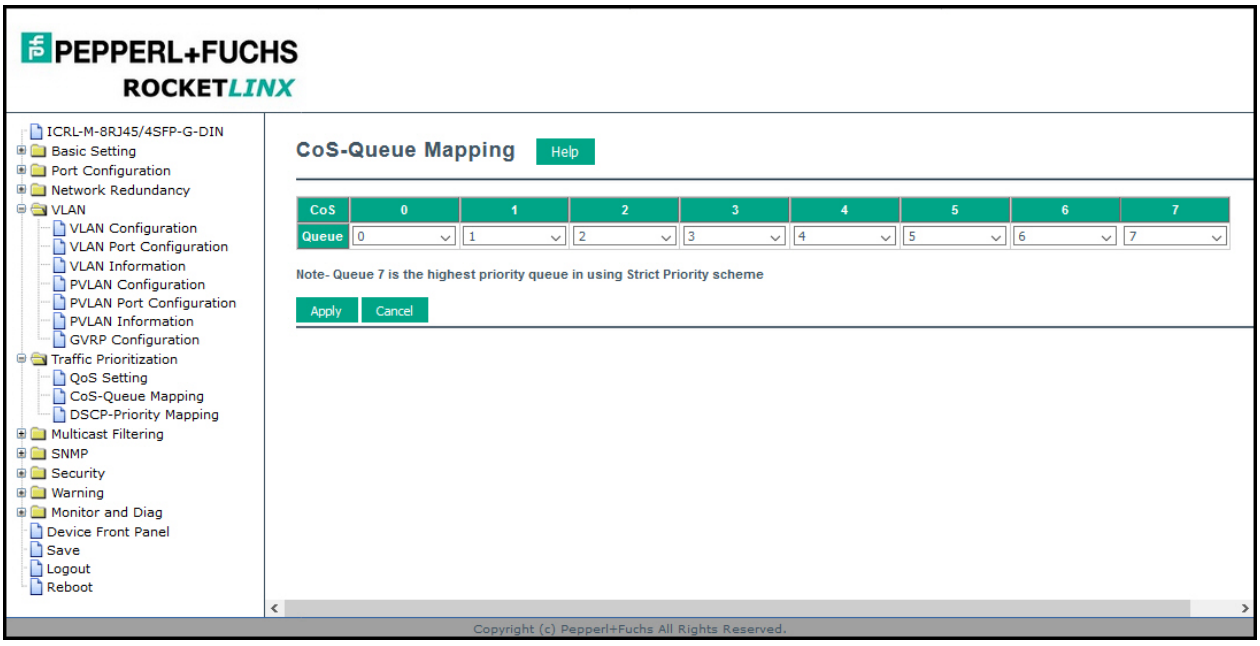
Auf dieser Seite können Sie die CoS-Werte in der Zuordnungstabelle der physischen Warteschlange ändern. Da die Switch-Struktur von ICRL-M vier Warteschlangen (Lowest, Low, Middle und High) unterstützt, sollten Benutzer festlegen, wie der CoS-Wert der Ebene der physischen Warteschlange zugeordnet werden soll.

Sie können die Zuordnungstabelle zuweisen oder den Vorschlag des IEEE-802.1p-Standards befolgen. Der ICRL-M verwendet die IEEE-802.1p-Vorschläge als Standardwerte. CoS-Werte 1 und 2 werden der physischen Warteschlange 0, der niedrigsten Warteschlange, zugeordnet. CoS-Werte 0 und 3 werden der physischen Warteschlange 1, der niedrigen/normalen physischen Warteschlange, zugeordnet. CoS-Werte 4 und 5 werden der physischen Warteschlange 2, der mittleren physischen Warteschlange, zugeordnet. CoS-Werte 6 und 7 werden der physischen Warteschlange 3, der hohen physischen Warteschlange, zugeordnet.

Class of Service (CoS) ist ein 3-Bit-Feld innerhalb eines Layer-2-Ethernet-Frame-Headers, der durch IEEE 802.1p definiert wird, wenn IEEE-802.1Q-Tagging verwendet wird. Das Feld gibt einen Prioritätswert zwischen 0 und 7 an, der von QoS-Mechanismen (Quality of Service) zur Unterscheidung des Datenverkehrs verwendet werden kann.

Während CoS nur bei Ethernet auf der Datenverbindungsebene arbeitet, werden andere QoS-Mechanismen (wie DiffServ) auf der Netzwerkebene und höher ausgeführt. Andere arbeiten auf anderen physischen Ebenen. Obwohl IEEE-802.1Q-Tagging aktiviert sein muss, um Prioritätsinformationen von Switch zu Switch zu kommunizieren, verwenden einige Switches CoS zur internen Klassifizierung des Datenverkehrs für QoS-Zwecke.

Differentiated Services (DiffServ) ist ein Modell, bei dem der Datenverkehr von Zwischensystemen mit relativen Prioritäten basierend auf dem Diensttyp (ToS) verarbeitet wird. Der in RFC2474 und RFC2475 definierte DiffServ-Standard ersetzt die ursprüngliche Spezifikation zur Definition der Paketpriorität, wie in RFC791 beschrieben. DiffServ erhöht die Anzahl der definierbaren Prioritätsebenen durch Neuzuweisung von Bits eines IP-Pakets für die Prioritätskennzeichnung. Die DiffServ-Architektur definiert das DiffServ-Feld, das das ToS-Feld in IPv4 ersetzt, um PHB-Entscheidungen (Per-Hop Behavior) über Funktionen zur Paketklassifizierung und Datenverkehr-Aufbereitung zu treffen, wie z. B. Erfassung, Kennzeichnung, Gestaltung und Richtlinienüberwachung.



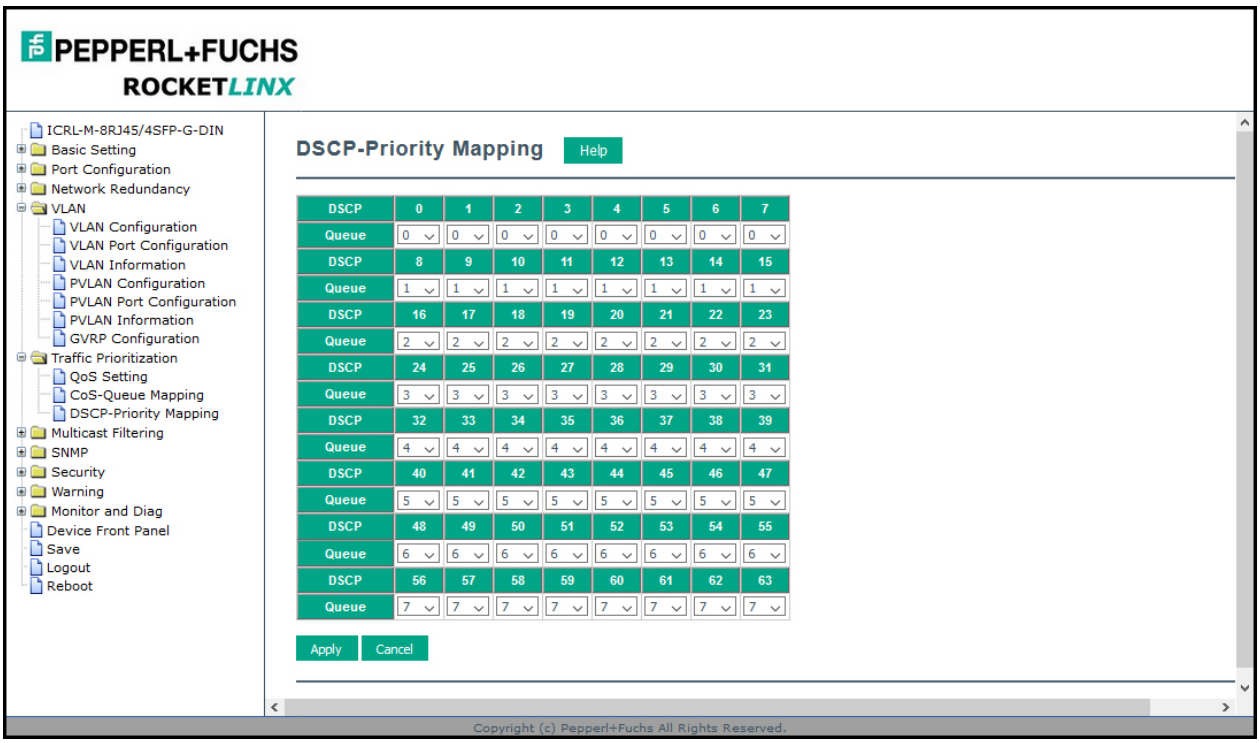
Klicken Sie nach der Konfiguration auf **Apply**, um die Einstellungen zu aktivieren.

Anmerkung: *Sie müssen die Einstellungen mit **Save** speichern (Seite 159), wenn Sie diese Einstellungen nach Ausschalten des ICRL-M beibehalten möchten.*

4.7.3. DSCP-Priority Mapping

Auf dieser Seite können Sie die DSCP-Werte in die Zuordnungstabelle der physischen Warteschlange ändern. Da die Switch-Struktur des ICRL-M nur vier Warteschlangen (Lowest, Low, Middle und High) unterstützt, sollten Benutzer festlegen, wie DSCP-Werte der Ebene der physischen Warteschlange zugeordnet werden sollen. Sie sollten daher festlegen, wie der DSCP-Wert der Warteschlangenebene zugeordnet wird. Sie können die Zuordnungstabelle so ändern, dass sie dem oberen Layer-3-Switch oder der DSCP-Einstellung des Routers folgt.

Klicken Sie nach der Konfiguration auf **Apply**, um die Einstellungen zu aktivieren.



Anmerkung: *Sie müssen die Einstellungen mit* **Save** *speichern (Seite 159), wenn Sie diese Einstellungen nach Ausschalten des ICRL-M beibehalten möchten.*

4.8. Multicast-Filterung

Für die Multicast-Filterung verwendet der ICRL-M die IGMP-Snooping-Technologie (Internet Group Management Protocol). IGMP ist ein Internetprotokoll, mit dem das Internetgerät seine Multicast-Gruppenmitgliedschaft an benachbarte Router melden kann. Multicasting ermöglicht es einem Computer im Netzwerk, Daten an eine Vielzahl von anderen Computern zu senden, die sich selbst als interessiert am Empfang der Daten des ursprünglichen Computers identifiziert haben.

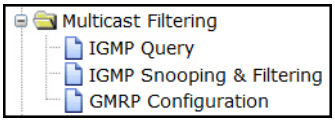
Multicasting ist nützlich für Anwendungen, bei denen dieselben Daten an mehrere Ziele gesendet werden müssen, z. B. Multimedia-Streaming oder unternehmensweite Softwareupdates.

IGMP-Snooping verwaltet den Multicast-Datenverkehr durch die Verwendung von Switches, Routern und Hosts, die IGMP unterstützen. Durch Aktivieren von IGMP-Snooping können die Ports IGMP-Abfragen erkennen, Pakete melden und Multicast-Datenverkehr über den Switch verwalten. IGMP verfügt über drei grundlegende Meldungstypen, wie in der folgenden Tabelle dargestellt.

Nachrichten	
Abfrage	Eine vom Querier (IGMP-Router oder -Switch) gesendete Nachricht, die eine Antwort von jedem Host anfordert, der zu der Multicast-Gruppe gehört
Melden	Eine Nachricht, die von einem Host an den Querier gesendet wird, um anzugeben, dass der Host ein Mitglied der in der Meldenachricht angegebenen Gruppe sein möchte oder ist
Gruppe verlassen	Eine Nachricht, die von einem Host an den Querier gesendet wird, um anzugeben, dass die Mitgliedschaft des Hosts in einer bestimmten Multicast-Gruppe beendet wurde

Sie können die Funktionen **IGMP Snooping** und **IGMP Query** aktivieren. In diesem Abschnitt werden die Informationen der IGMP-Snooping-Funktion erläutert, einschließlich der VIDs und Mitgliederports verschiedener Multicast-Gruppen und der IP-Multicast-Adressen im Bereich von 224.0.0.0 bis 239.255.255.255.

Die folgenden Webseiten sind in dieser Gruppe enthalten:



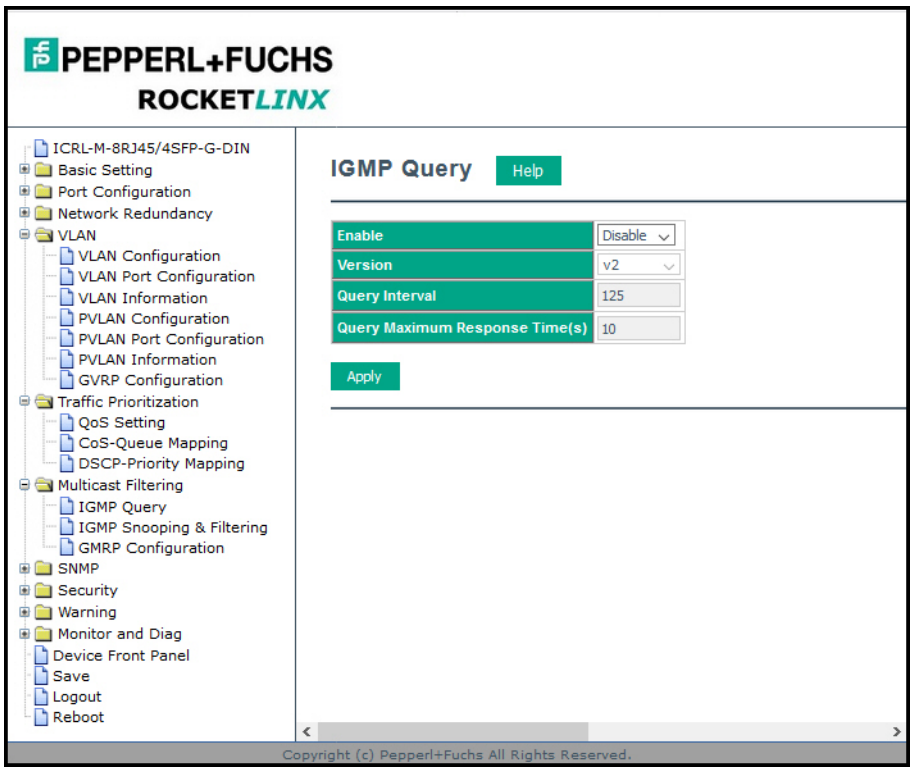
- *IGMP Query* auf Seite 109
- *IGMP Snooping & Filtering* auf Seite 110
- *GMRP Configuration* auf Seite 112

Optional können Sie die Befehlszeilenschnittstelle (Command-Line Interface, CLI) für die Konfiguration verwenden (siehe *Multicast-Filterung (CLI)* auf Seite 208).

4.8.1. IGMP Query

Auf dieser Seite können Sie die *IGMP Query*-Funktion konfigurieren. Da der ICRL-M nur von Mitgliedsports des Management-VLAN konfiguriert werden kann, kann IGMP Query nur im Management-VLAN aktiviert werden. Wenn Sie die IGMP-Snooping-Funktion in mehreren VLANs ausführen möchten, überprüfen Sie zunächst, ob jedes VLAN über einen eigenen IGMP-Querier verfügt.

Der IGMP-Querier sendet in regelmäßigen Abständen Abfragepakete an alle Endstationen in den LANs oder VLANs, die mit ihm verbunden sind. Bei Netzwerken mit mehr als einem IGMP-Querier wird der Switch mit der niedrigsten IP-Adresse zum IGMP-Querier.

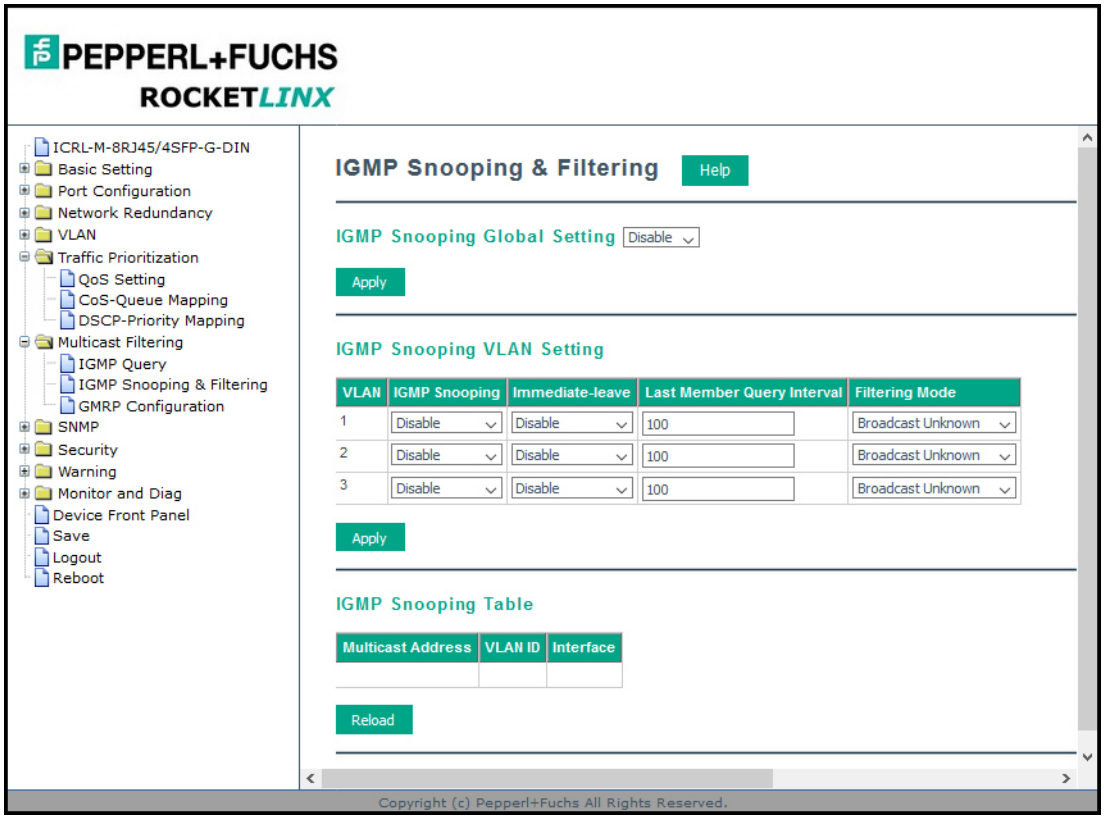


Seite „IGMP Query“	
Enable	Standardmäßig ist die IGMP-Abfrage deaktiviert.
Version	Wählen Sie **Version 1**, **Version 2** oder **Disable**. • **Version 1** steht für IGMP V1 General Query. • **Version 2** steht für IGMP V2 General Query. Die Abfrage wird an alle Multicast-Gruppen im VLAN weitergeleitet. • Mit **Disable** können Sie die IGMP-Abfrage deaktivieren.
Query Interval(s)	Der Zeitraum zwischen den vom Querier gesendeten Abfragen (Sekunden). Geben Sie eine Zahl zwischen 1 und 65.535 ein.
Query Maximum Response Time	Diese Option ist verfügbar, wenn Sie **Version 2** auswählen. Der Span-Querier erkennt (Sekunden), um zu bestätigen, dass keine direkt verbundenen Gruppenmitglieder mehr in einem LAN vorhanden sind. Geben Sie eine Zahl zwischen 1 und 25 ein.

Seite „IGMP Query“ (Fortsetzung)	
Apply	Klicken Sie auf **Apply**, um die Einstellungen anzuwenden. ***Anmerkung:*** *Sie müssen die Einstellungen mit **Save** speichern (Seite 159), wenn Sie diese Einstellungen nach Ausschalten des ICRL-M beibehalten möchten.*

4.8.2. IGMP Snooping & Filtering

Verwenden Sie diese Seite, um die IGMP-Snooping-Funktion zu aktivieren, IGMP-Snooping bestimmten VLANs zuzuweisen und die *IGMP-Snooping-Tabelle* einer von Ihnen bereitgestellten dynamischen erlernten oder statischen Adresse anzuzeigen.

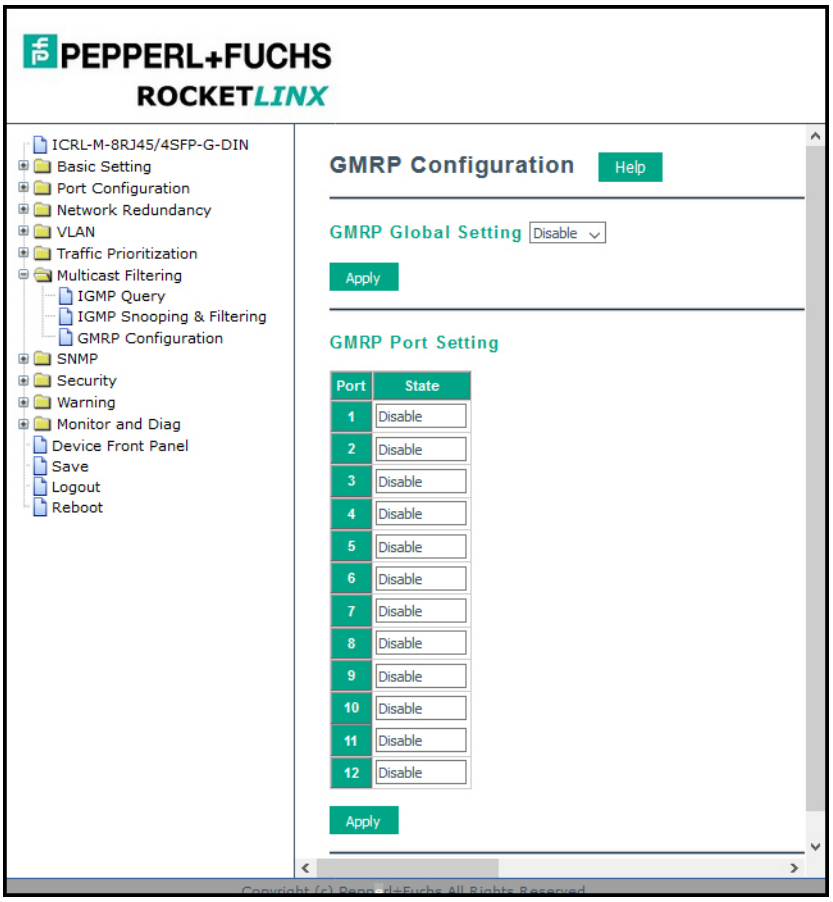


Seite „IGMP Snooping“	
IGMP Snooping Global Setting	Sie können IGMP-Snooping mit **Enable** aktivieren oder mit **Disable** deaktivieren. Nach der Aktivierung von IGMP-Snooping können Sie IGMP-Snooping mithilfe von *IGMP Snooping VLAN Setting* für ein bestimmtes VLAN aktivieren.
IGMP Snooping VLAN Setting	
VLAN	Bezieht sich auf die VLAN-Nummer, die auf der Seite *VLAN Configuration* konfiguriert wurde.
IGMP Snooping	Wählen Sie **Enable**, um IGMP-Snooping auf dem ausgewählten VLAN zu starten.
Immediate-leave	Verlassen Sie die Gruppe, wenn Sie eine Leave-Nachricht erhalten.
Last Member Query Interval (Hundertstelsekunden)	Das Intervall, das der Switch abwartet, bevor der Tabelleneintrag aktualisiert wird.
Filtering Mode	Die verfügbaren Filtermodi sind: • **Broadcast-Unknown**: Der unbekannte Multicast wird an alle Ports gesendet, selbst wenn es sich nicht um Mitgliedsports der Gruppen handelt. • **Discard-Unknown**: Der unbekannte Multicast wird verworfen. Ports, die keine Mitglieder sind, empfangen die unbekannten Multicast-Streams nicht. • **Source-only-learning**: Hierbei wird unbekannter Multicast-Datenverkehr an alle Ports weitergeleitet, die bereits Mitglieder einer Multicast-Gruppe sind.
IGMP Snooping Table	In dieser Tabelle werden die IP-Adresse der Multicast-Gruppe, die VLAN-ID, zu der sie gehört, und die Mitgliedsports der Multicast-Gruppe angezeigt. Der ICRL-M unterstützt 256 Multicast-Gruppen. Klicken Sie auf **Reload**, um die Tabelle neu zu laden.

Anmerkung: *Sie müssen die Einstellungen mit **Save** speichern (Seite 159), wenn Sie diese Einstellungen nach Ausschalten des ICRL-M beibehalten möchten.*

4.8.3. GMRP Configuration

GARP Multicast Registration Protocol (GMRP) ist eine GARP-Anwendung (Generic Registration Protocol), die eine Verwaltungsfunktion für Multicast-Datenverkehr auf Layer 2 bereitstellt, ähnlich wie IGMP auf Layer 3. GMRP und GARP sind branchenübliche Protokolle, die erstmals im Rahmen von IEEE 802.1D eingeführt wurden.



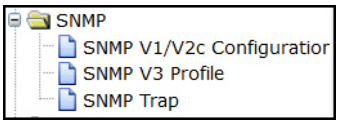
GMRP Configuration	
GMRP Global Setting	(De-)Aktivieren Sie das GMRP mit **Enable**/**Disable**.
State	Der Status des GMRP-Vorgangs an einem ausgewählten Port. Der Wert „Enabled“ gibt an, dass GMRP an diesem Port aktiviert ist, solange das GMRP für dieses Gerät ebenfalls aktiviert ist. Wenn diese Option deaktiviert ist, aber das GMRP für das Gerät noch aktiviert ist, wird das GMRP am ausgewählten Port deaktiviert.
Apply	Klicken Sie auf **Apply**, um die Einstellungen anzuwenden. ***Anmerkung:*** *Sie müssen die Einstellungen mit **Save** speichern (Seite 159), wenn Sie diese Einstellungen nach Ausschalten des ICRL-M beibehalten möchten.*

4.9. SNMP

Das Simple Network Management Protocol (SNMP) ist ein Protokoll, das für den Austausch von Verwaltungsinformationen zwischen Netzwerkgeräten verwendet wird. SNMP ist Mitglied der TCP/IP-Protokollsuite. Der ICRL-M unterstützt SNMP v1, v2c und v3.

Ein SNMP-verwaltetes Netzwerk besteht aus zwei Hauptkomponenten: Agents und einem Manager. Ein Agent ist ein Management-Softwaremodul, das sich in einem verwalteten Switch befindet. Ein Agent übersetzt die lokalen Verwaltungsinformationen vom verwalteten Gerät in ein SNMP-kompatibles Format. Der Manager ist die Konsole im Netzwerk.

Die folgenden Webseiten sind in dieser Gruppe enthalten:

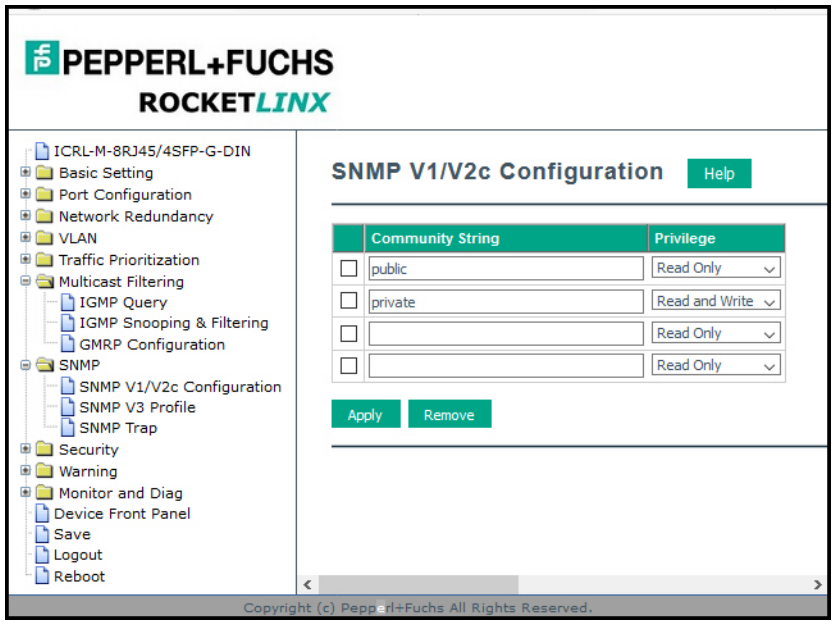


- *SNMP Configuration*
- *SNMP V3 Profile* auf Seite 114
- *SNMP Trap* auf Seite 115

Optional können Sie die Befehlszeilenschnittstelle (Command-Line Interface, CLI) für die Konfiguration verwenden (siehe *SNMP (CLI)* auf Seite 212).

4.9.1. SNMP Configuration

Auf dieser Seite können Sie die SNMP-v1/v2c-Community konfigurieren. Die Communityzeichenfolge kann als Kennwort angesehen werden, da SNMP v1/v2c Sie nicht zur Eingabe eines Kennworts auffordert, bevor Sie versuchen, auf den SNMP-Agent zuzugreifen.



Die Community verfügt über zwei Berechtigungen:

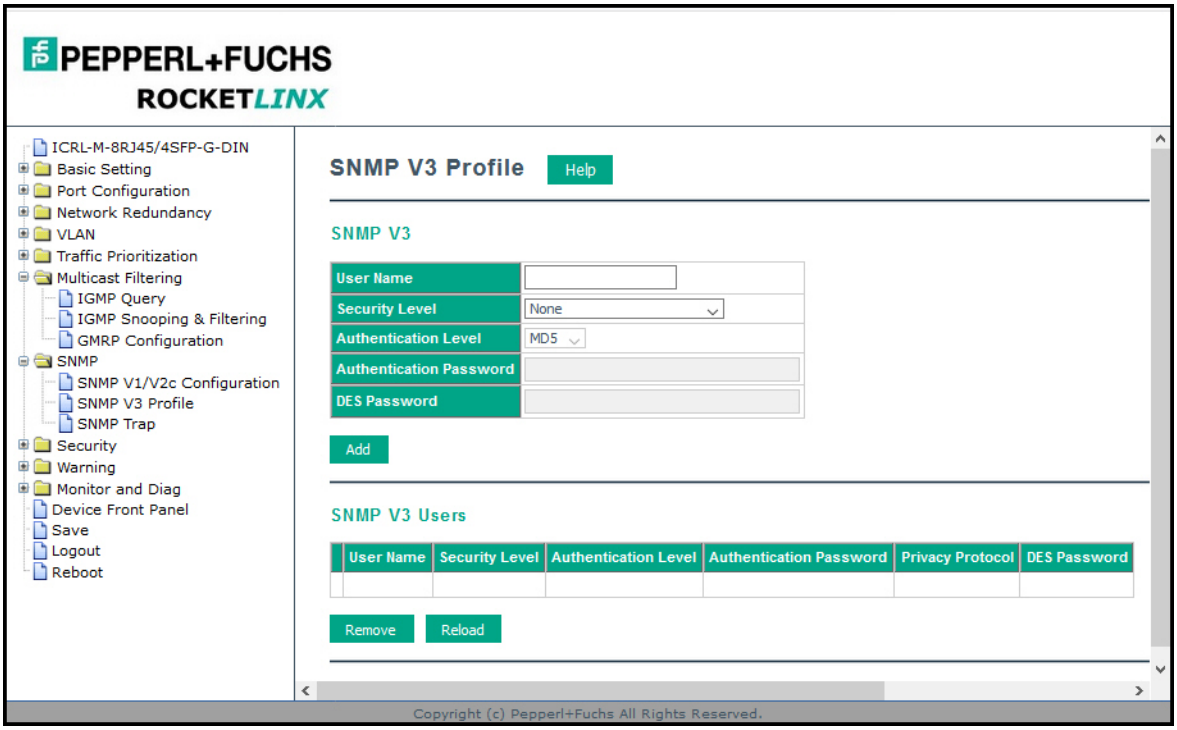
- **Read Only**-Berechtigung: Sie haben nur die Möglichkeit, die Werte von MIB-Tabellen zu lesen. Die Standard-Communityzeichenfolge ist **public**.
- **Read and Write**-Berechtigung: Sie haben die Möglichkeit, die Werte von MIB-Tabellen zu lesen und Werte festzulegen. Die Standard-Communityzeichenfolge ist **private**.

Mit dem ICRL-M können Sie vier Communityzeichenfolgen zuweisen. Geben Sie die Communityzeichenfolge ein, wählen Sie die Berechtigung aus und klicken Sie dann auf **Apply**.

Anmerkung: *Wenn Sie das Gerät zum ersten Mal in Ihrem Netzwerk installieren, empfehlen wir, die Communityzeichenfolge zu ändern. Die meisten SNMP-Verwaltungsanwendungen verwenden „public“ und „private“ als Standard-Communitynamen. Dies kann eine Sicherheitsschwachstelle für Ihr Netzwerk bedeuten.*

4.9.2. SNMP V3 Profile

SNMP v3 kann mehr Sicherheitsfunktionen bieten, wenn Sie die Remote-Verwaltung über das SNMP-Protokoll durchführen. Sie liefert dem Administrator SNMP-Informationen mit Benutzerauthentifizierung; alle Daten zwischen dem ICRL-M und dem Administrator werden verschlüsselt, um eine sichere Kommunikation zu gewährleisten.



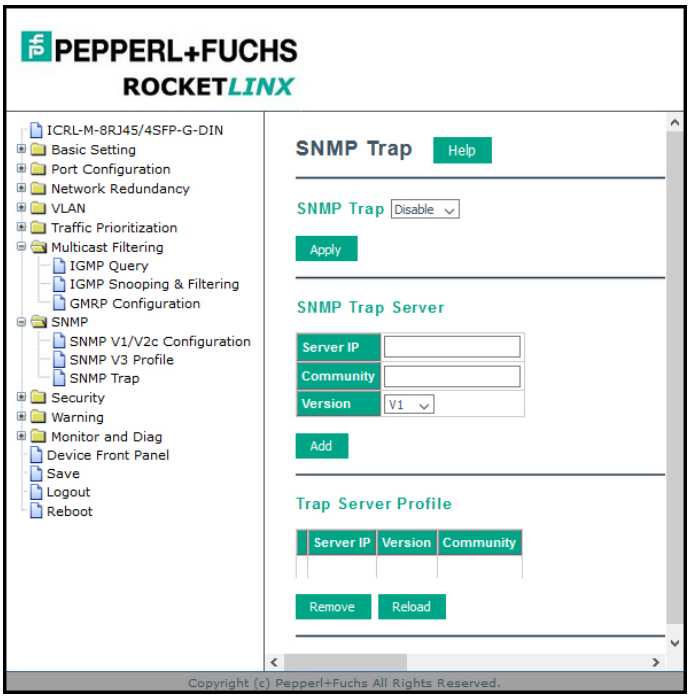
Seite „SNMP V3 Profile“	
User Name	SNMP-v3-Benutzername.
Security Level	Wählen Sie die folgenden Sicherheitsstufen aus: **None**, **Authentication** oder **Authentication and Privacy**.
Authentication Level	Wählen Sie **MD5** (Message-Digest Algorithm 5) oder **SHA** (Secure Hash Algorithm) aus. • **MD5** ist eine weit verbreitete kryptografische Hashfunktion mit einem 128-Bit-Hash-Wert. • **SHA**-Funktionen beziehen sich auf fünf durch Federal Information Processing Standard genehmigte Algorithmen zur Berechnung einer komprimierten digitalen Darstellung. Der ICRL-M bietet zwei Protokolle zur Benutzerauthentifizierung in MD5 und SHA. Sie müssen SNMP-v3-Parameter für Ihr SNMP-Tool mit derselben Authentifizierungsmethode konfigurieren.
Authentication Password	Geben Sie das SNMP-v3-Benutzer-Authentifizierungskennwort ein.
DES Password	Geben Sie das Kennwort für die SNMP-v3-Benutzer-DES-Verschlüsselung ein.
Add	Klicken Sie hier, um einen SNMP-v3-Benutzer hinzuzufügen.
SNMP V3 Users	Diese Tabelle enthält SNMP-v3-Benutzerinformationen. Klicken Sie auf **Remove**, um einen ausgewählten SNMP-v3-Benutzer zu entfernen. Klicken Sie auf **Reload**, um die SNMP-v3-Benutzerinformationen neu zu laden.

Anmerkung: *Sie müssen die Einstellungen mit **Save** speichern (Seite 159), wenn Sie diese Einstellungen nach Ausschalten des ICRL-M beibehalten möchten.*

4.9.3. SNMP Trap

„SNMP Trap“ ist die vom SNMP-Protokoll definierte Benachrichtigungsfunktion. Alle SNMP-Verwaltungsanwendungen können solche Trap-Informationen verstehen. Daher müssen Sie keine neuen Anwendungen installieren, um die Benachrichtigungsinformationen zu lesen.

Sie können die Änderung der vordefinierten SNMP-Standard-Traps und vordefinierten Pepperl+Fuchs-Traps sehen. Die vordefinierten Traps finden Sie in der MIB-Datei für Ihren ICRL-M unter https://www.pepperl-fuchs.com.

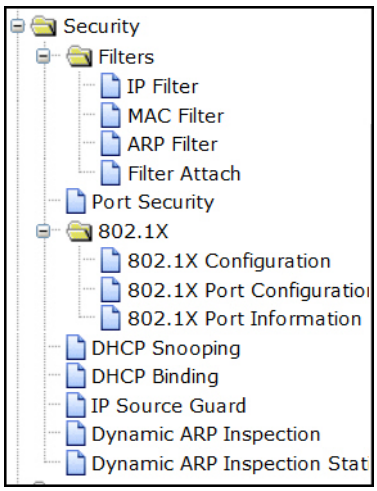


Seite „SNMP Trap“	
SNMP-Trap	(De-)Aktivieren Sie die SNMP-Trap-Funktion mit **Enable**/**Disable**.
Apply	Klicken Sie auf **Apply**, um die Einstellungen anzuwenden. ***Anmerkung:*** *Sie müssen die Einstellungen mit **Save** speichern (Seite 159), wenn Sie diese Einstellungen nach Ausschalten des ICRL-M beibehalten möchten.*
SNMP Trap Server	
Server IP	Die IP-Adresse des SNMP-Trap-Servers.
Community	Die Communityzeichenfolge des SNMP-Trap-Servers.
Version	Die SNMP-Trap-Version: V1 oder V2c.
Add	Klicken Sie auf die Schaltfläche **Add**, um einen SNMP-Server hinzuzufügen.
Trap Server Profile	
Server IP	Die IP-Adresse des SNMP-Trap-Servers.
Community	Die Communityzeichenfolge des SNMP-Trap-Servers.
Version	Die SNMP-Trap-Version: V1 oder V2c.
Remove	Klicken Sie auf **Remove**, um den ausgewählten SNMP-Server zu entfernen.
Reload	Klicken Sie auf die Schaltfläche **Reload**, um die SNMP-Serverinformationen neu zu laden.

Anmerkung: *Sie müssen die Einstellungen mit **Save** speichern (Seite 159), wenn Sie diese Einstellungen nach Ausschalten des ICRL-M beibehalten möchten.*

4.10. Sicherheit

Der ICRL-M bietet verschiedene Sicherheitsfunktionen, mit denen Sie Ihre Verbindung schützen können. Die folgenden Seiten sind in dieser Gruppe enthalten:



- *Filtersatz (Zugriffskontrollliste)*
  - *IP Filter* auf Seite 119
  - *MAC Filter (Portsicherheit)* auf Seite 121
  - *ARP Filter*
  - *Filter Attach* auf Seite 125
- *Port Security*
- *802.1X Configuration* auf Seite 128
- *802.1X Port Configuration* auf Seite 130
- *802.1X Port Information* auf Seite 132
- *DHCP Snooping* auf Seite 133
- *DHCP Binding Configuration* auf Seite 135
- *IP Source Guard* auf Seite 137
- *Dynamic ARP Inspection* auf Seite 139
- *Dynamic ARP Inspection Status* auf Seite 141

Optional können Sie die Befehlszeilenschnittstelle (Command-Line Interface, CLI) für die Konfiguration verwenden (siehe *Sicherheit (CLI)* auf Seite 213).

4.10.1. Filtersatz (Zugriffskontrollliste)

Der Filtersatz wird als ACL-Funktion (Access Control List) bezeichnet. Es gibt zwei Haupttypen:

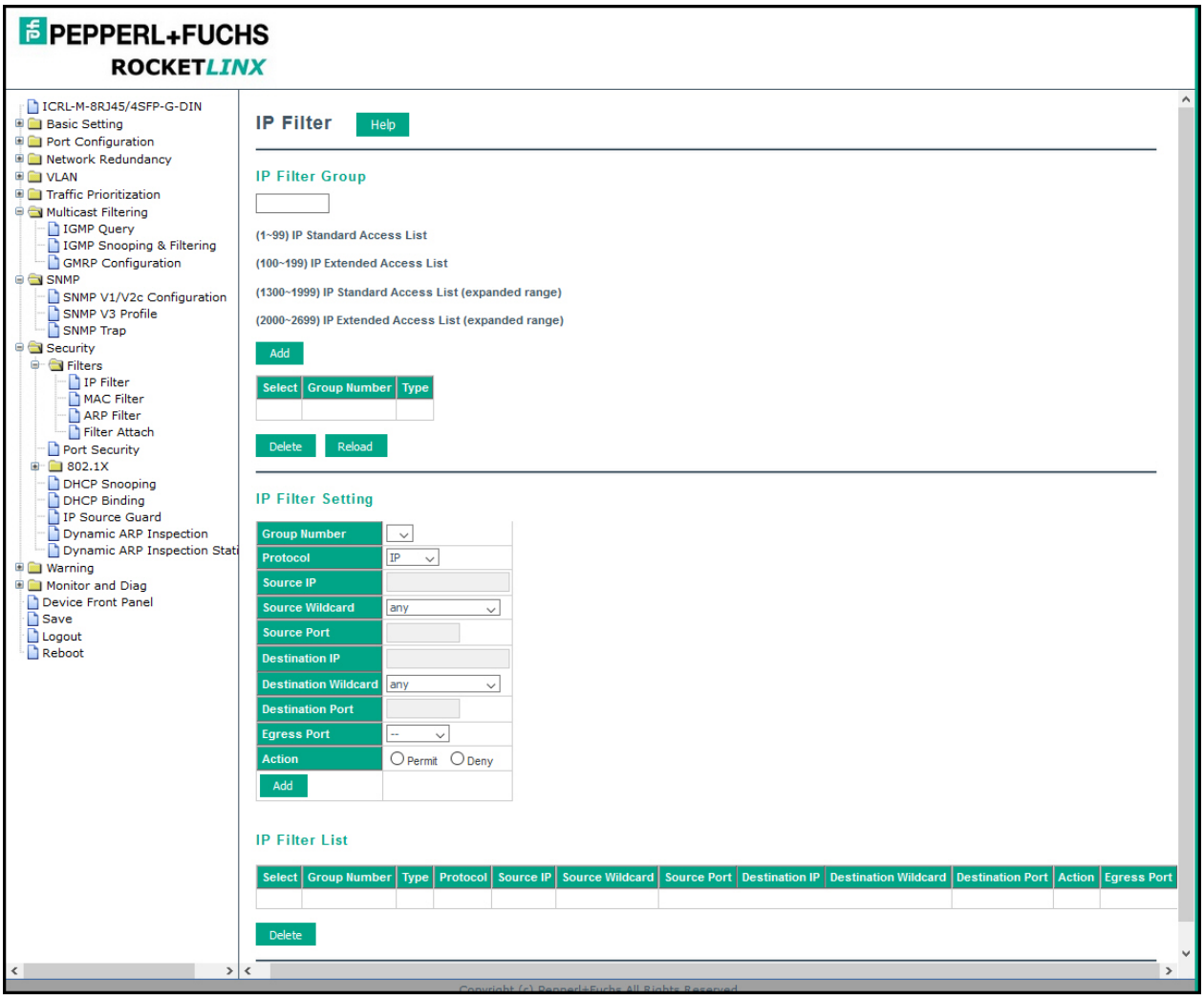
- *IP Filter* auf Seite 119, der in anderen RocketLinx-Modellen als IP-Sicherheit bezeichnet wird und die Zugriffsliste nach IP-Standard und erweiterte IP-basierte Zugriffslisten unterstützt.
- *MAC Filter (Portsicherheit)* auf Seite 121, der in anderen RocketLinx-Switches als Portsicherheit bezeichnet wird. Sie können die Zugriffsregel basierend auf der MAC-Adresse definieren.

Sie können Access Control Entry (ACE) verwenden, um eine Genehmigungs- oder Ablehnungsregel für bestimmte IP- oder MAC-Adressen oder IP-Gruppen nach Netzwerkmaske in jedem ACE zu definieren. Eine ACL kann mehrere ACEs enthalten. Das System prüft nacheinander die ACEs und leitet die Daten basierend auf dem Ergebnis weiter.

Bei Regelkonflikten wird der älteste Eintrag ausgewählt.

4.10.1.1. IP Filter

Klicken Sie auf **IP Filter** und geben Sie **ID/Name** ein, um die Sicherheit mithilfe von IP-Adressen zu konfigurieren. Klicken Sie auf **Reload**, um die Einstellungen zu aktualisieren, und auf **Delete**, um einen der Einträge zu entfernen.



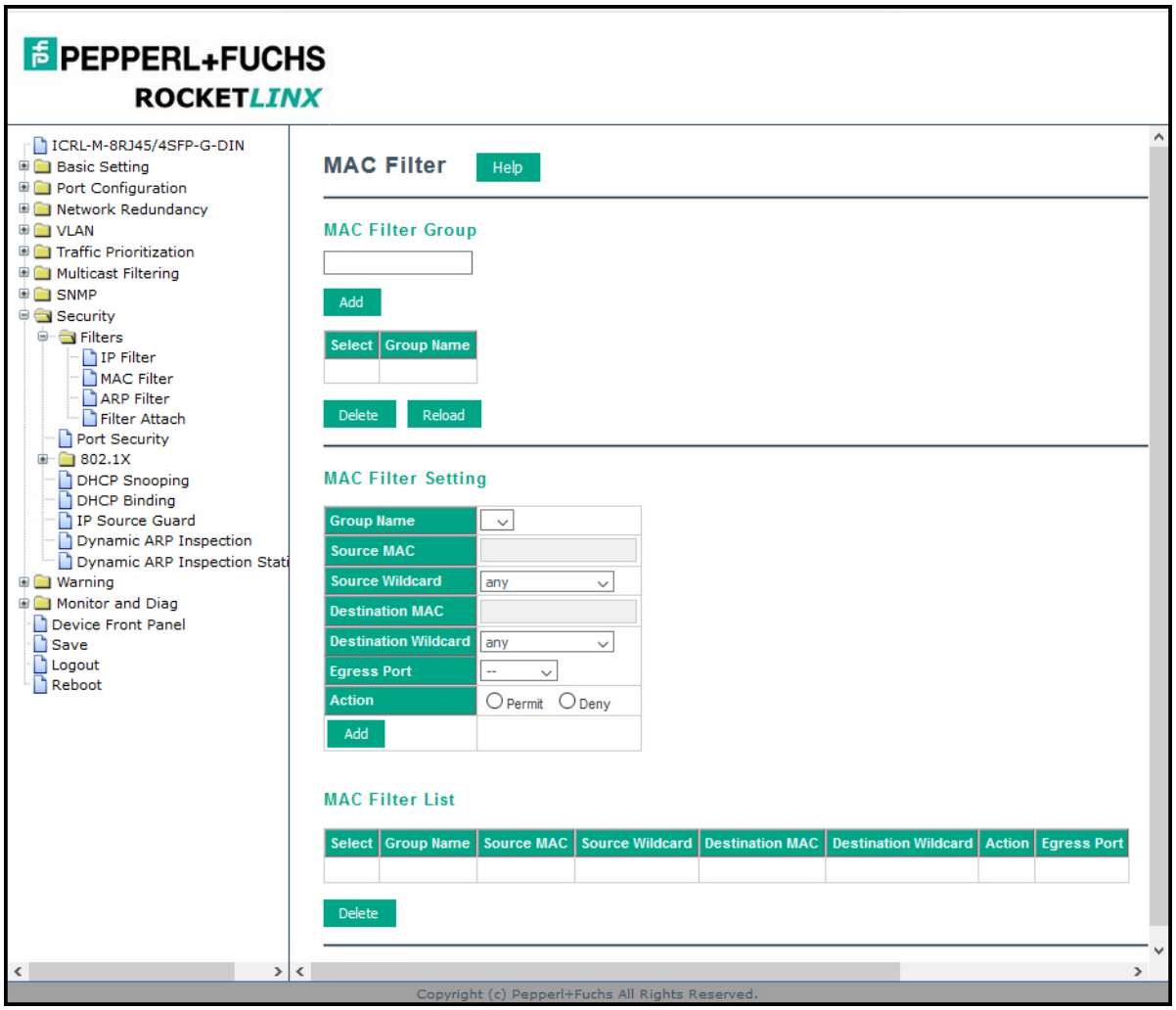
Seite „IP Filter“	
IP Filter Group	
IP Filter Group	Geben Sie eine entsprechende Gruppennummer ein, um anzugeben, ob es sich um eine IP-Standard- oder eine erweiterte IP-Zugriffsliste handelt. • IP Standard Access List Mit diesem ACL-Typ können Sie Filterregeln gemäß der IP-Quelladresse definieren. • IP Extended Access List Mit diesem ACL-Typ können Sie Filterregeln gemäß IP-Quelladresse, IP-Zieladresse, TCP/UDP-Quellport, TCP/UDP-Zielport und ICMP-Typ und -Code definieren.
Add	Klicken Sie nach der Eingabe einer IP-Filtergruppennummer auf **Add**.
Select	Wählen Sie dieses Feld aus, um diesen Eintrag zu löschen oder neu zu laden.
Group Number	Dies ist die Zahl, die die Filtergruppe darstellt.
Type	Dies ist der Filtergruppentyp (Standard oder erweitert).
Delete	Löscht die ausgewählte Regeltabelle.
Reload	Lädt die Regeltabelle neu.

Markieren Sie eine(n) IP-Filter-ID/-Namen und klicken Sie auf **Edit**, um die IP-Filterregeln zu konfigurieren.

IP Filter Setting	
Group Number	Dies ist die Filtergruppennummer.
Protokoll	Dies ist das Internet Protocol (IP) oder das L4-Protokoll (TCP/UDP/ICMP).
Source IP	Geben Sie die Quell-IP-Adresse des Pakets ein.
Source Wildcard	Dies ist die Maske der Quell-IP-Adresse.
Source Port	Dies ist der Quellport des L4-Protokolls (TCP/UDP).
Destination IP	Dies ist die Ziel-IP-Adresse des Pakets.
Destination Wildcard	Dies ist die Maske der Ziel-IP-Adresse.
Destination Port	Dies ist der Zielport des L4-Protokolls (TCP/UDP).
Egress Port	Dies ist die Nummer des ausgehenden Ports.
Action	Dies ist die Filteraktion, mit der das Paket abgelehnt oder zugelassen wird.
Add	Fügt die Regel dem Filter hinzu.
IP Filter List	
Delete	Entfernt die ausgewählte Regel aus dem Filter.

4.10.1.2. MAC Filter (Portsicherheit)

Mit dem MAC-Filter können Sie die Zugriffssteuerungsliste für eine bestimmte MAC-Adresse oder eine Gruppe von MAC-Adressen definieren. Die Paketfilterung kann dazu beitragen, den Netzwerkverkehr zu begrenzen und die Netzwerknutzung durch bestimmte Benutzer oder Geräte einzuschränken. Die Funktion **Add Filters** filtert den Datenverkehr, während er durch einen Switch geleitet wird, und erlaubt oder verweigert Pakete, die bestimmte Schnittstellen überschreiten. MAC-Filter können Layer-2-Datenverkehr filtern.



Seite „MAC Filter“	
MAC Filter Group	Der Name für diesen MAC-Filtereintrag.
Select	Wenn Sie diese Option auswählen und auf die Schaltfläche **Delete** klicken, wird die entsprechende Filtergruppe gelöscht.
Group Name	Dies ist der MAC-Gruppenname.
Reload	Klicken Sie auf **Reload**, um die Filtergruppentabelle neu zu laden.
MAC Filter Setting	
Group Name	Dies ist der Name der MAC-Filtergruppe.
Source MAC	Geben Sie die zu konfigurierende MAC-Adresse ein. Das Format ist AABB.CCDD.EEFF.
Source Wildcard	Sie können einen einzelnen Host oder eine Gruppe von Hosts basierend auf dem Platzhalter definieren. Einige Beispiele für Erlaubnisse sind in der folgenden Tabelle aufgeführt.
Destination MAC	Geben Sie die zu konfigurierende MAC-Adresse ein. Das Format ist AABB.CCDD.EEFF.
Destination Wildcard	Sie können einen einzelnen Host oder eine Gruppe von Hosts basierend auf dem Platzhalter definieren. Einige Beispiele für Erlaubnisse sind in der folgenden Tabelle aufgeführt.
Egress Port	Dies ist die Nummer des ausgehenden Ports.
Action	Wählen Sie **Permit** aus, um Datenverkehr aus bestimmten Quellen zuzulassen, oder **Deny**, um Datenverkehr aus diesen Quellen zu verweigern.
MAC Filter List	
Group Name	Dies ist die Filtergruppennummer.
Source MAC	Geben Sie die Quell-MAC-Adresse des Pakets ein.
Source Wildcard	Dies ist die Maske der MAC-Adresse.
Destination MAC	Dies ist die Ziel-MAC-Adresse des Pakets.
Destination Wildcard	Dies ist die Maske der Ziel-MAC-Adresse.
Action	Dies ist die Filteraktion, mit der das Paket abgelehnt oder zugelassen wird.
Egress Port	Dies ist die Nummer des ausgehenden Ports.
Delete	Entfernt die ausgewählte Regel aus dem Filter.

Wenn Sie die Konfiguration der MAC-Einstellungen abgeschlossen haben, klicken Sie auf **Add**, um die Konfiguration anzuwenden.

Anmerkung: *Sie müssen die Einstellungen mit **Save** speichern (Seite 159), wenn Sie diese Einstellungen nach Ausschalten des ICRL-M beibehalten möchten.*

Geben Sie im Feld **Source MAC/Destination MAC** die MAC-Adresse ein, die Sie konfigurieren möchten. Das Format lautet **AABB.CCDD.EEFF**. Beispiel: **Source to Destination** ist **0012.7700.0000 to 0012.7700.0002**. Im Feld **Wildcard/Destination Wildcard** können Sie einen einzelnen Host oder eine Gruppe von Hosts basierend auf dem Platzhalter definieren. Einige Beispiele für Erlaubnisse sind unten dargestellt:

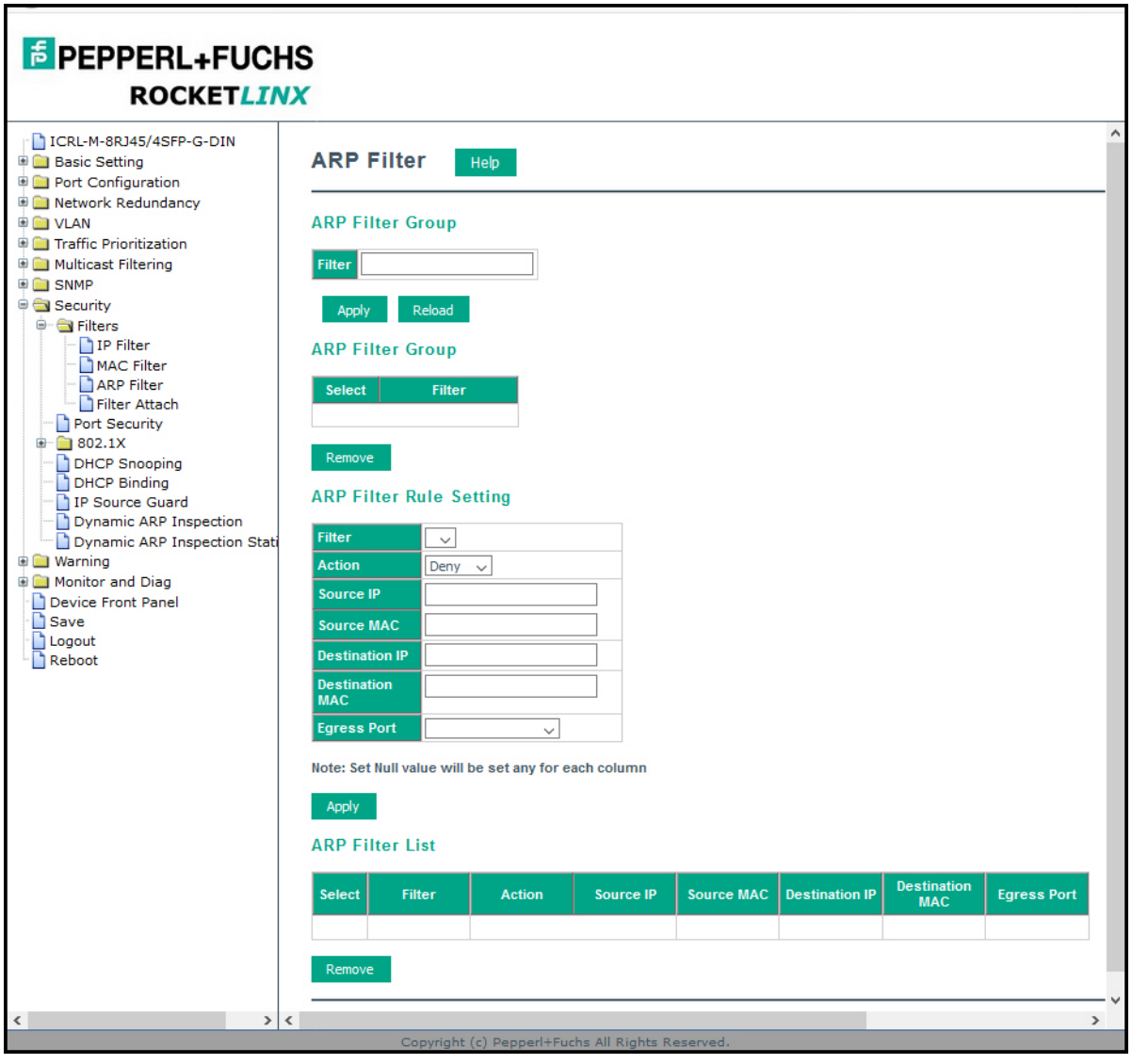
Platzhalter	Bit	Anzahl Erlaubnisse	Hinweis
Ein evtl.	1111.1111.1111	All	
Host		1	Nur Quelle oder Ziel
0000.0000.0003	0000.0000.000(00000011)	3	

5/21/20

Platzhalter	Bit	Anzahl Erlaubnisse	Hinweis
0000.0000.0007	0000.0000.000(00000111)	7	
0000.0000.000F	0000.0000.000(11111111)	15	
....			

4.10.1.3. ARP Filter

Die ARP-Filterung kann dazu beitragen, den ARTP-Datenverkehr zu begrenzen und die Netzwerknutzung durch bestimmte Benutzer oder Geräte einzuschränken. Die Funktion **Add Filters** filtert den Datenverkehr, während er durch einen Switch geleitet wird, und erlaubt oder verweigert Pakete, die bestimmte Schnittstellen überschreiten.



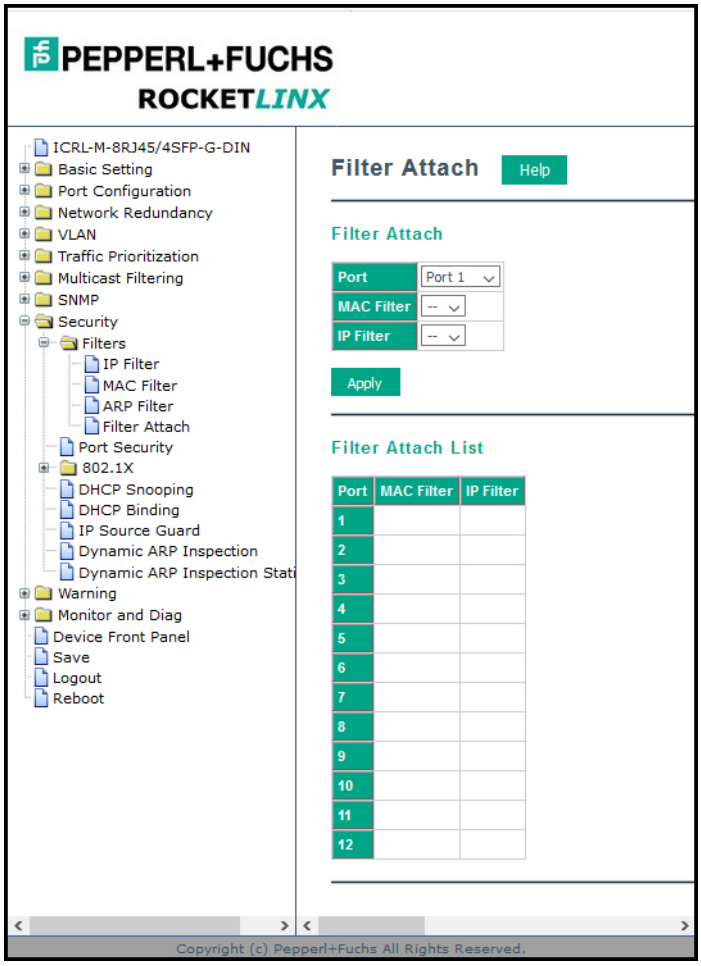
Seite „ARP Filter“
ARP Filter Group

5/21/20

Seite „ARP Filter“ (Fortsetzung)	
Filter	Dieser Name stellt die Filtergruppe dar.
Apply	Dadurch wird die Filtergruppe gespeichert.
Reload	Dadurch wird die ausgewählte Filtergruppe neu geladen.
ARP Filter Group	
Select	Wählen Sie dieses Feld aus, um den Eintrag zu löschen, und klicken Sie dann auf die Schaltfläche **Remove**.
Filter	Dieser Name stellt die Filtergruppe dar.
Remove	Klicken Sie auf die Schaltfläche **Remove**, um die Filtergruppe zu entfernen.
ARP Filter Rule Setting	
Filter	Name der Filtergruppe.
Action	Dies ist die Filteraktion, mit der das Paket abgelehnt oder zugelassen wird.
Source IP	Dies ist die Quell-IP-Adresse des Pakets.
Source MAC	Dies ist die Quell-MAC-Adresse des Pakets.
Destination IP	Dies ist die Ziel-IP-Adresse des Pakets.
Destination MAC	Dies ist die Ziel-MAC-Adresse des Pakets.
Egress Port	Dies ist der ausgehende Port.
Apply	Klicken Sie auf die Schaltfläche **Apply**, um eine neue ARP-Filterregel hinzuzufügen.
ARP Filter List	
Select	Zum Löschen ausgewählt.
Filter	Name der Filtergruppe.
Action	Dies ist die Filteraktion, mit der das Paket abgelehnt oder zugelassen wird.
Source IP	Dies ist die Quell-IP-Adresse des Pakets.
Source MAC	Dies ist die Quell-MAC-Adresse des Pakets.
Destination IP	Dies ist die Ziel-IP-Adresse des Pakets.
Destination MAC	Dies ist die Ziel-MAC-Adresse des Pakets.
Egress Port	Dies ist die Nummer des ausgehenden Ports.
Remove	Klicken Sie auf die Schaltfläche **Remove**, um den ausgewählten Filter zu entfernen.

4.10.1.4. Filter Attach

Auf dieser Seite können Sie Filter, die auf den Seiten „IP Filter“ und „MAC Filter“ erstellt wurden, an Ports auf dem Switch anschließen.

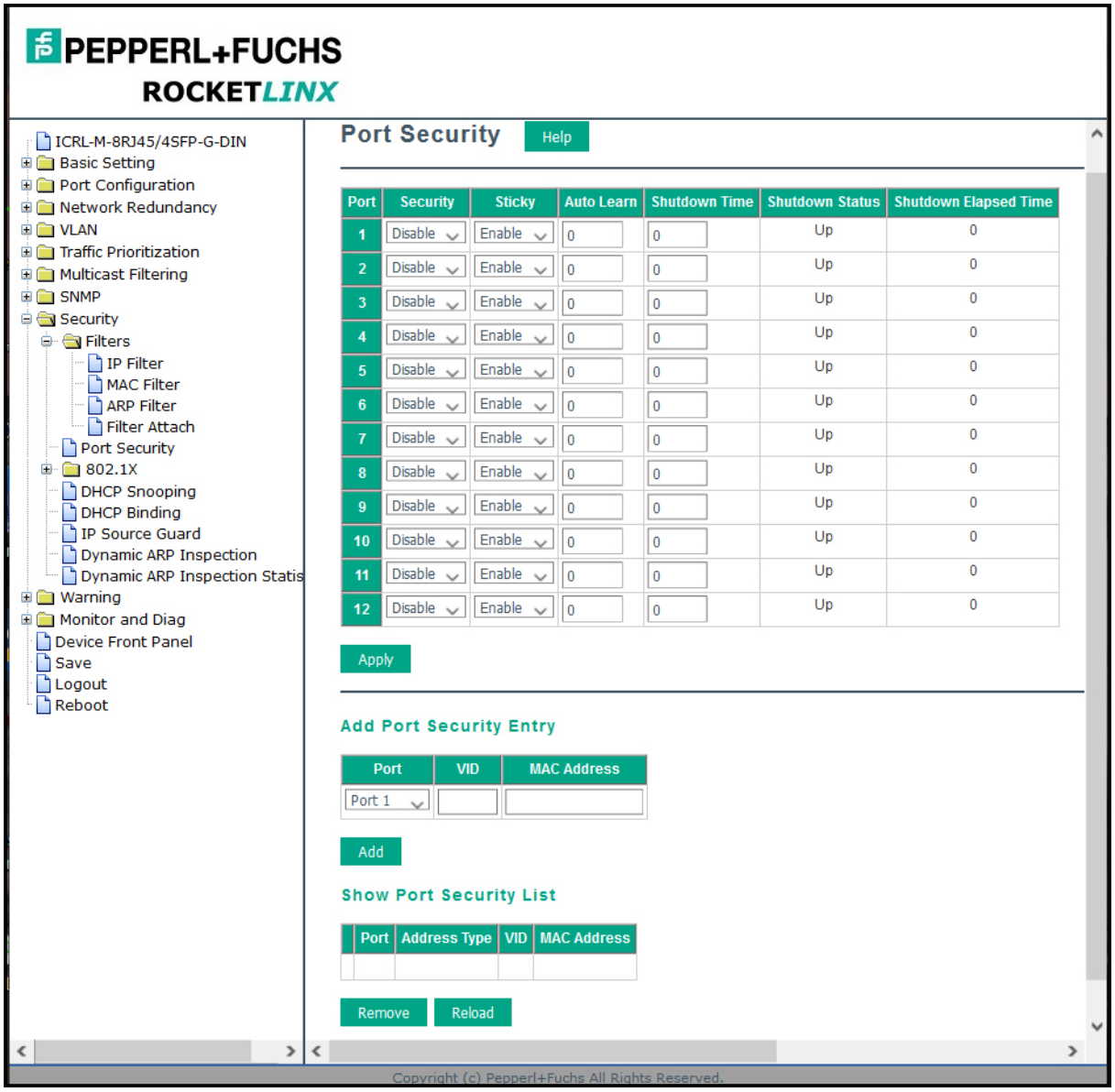


Seite „Filter Attach“	
Port	Der Port, an den Sie einen Filter anschließen möchten.
MAC Filter	Wählen Sie einen MAC-adressbasierten Filter aus, der an die Schnittstelle angeschlossen werden soll. Wählen Sie „--“ aus, um einen angeschlossenen MAC-Adressfilter zu entfernen.
IP Filter	Wählen Sie einen IP-adressbasierten Filter aus, der an die Schnittstelle angeschlossen werden soll. Wählen Sie „--“ aus, um einen angeschlossenen IP-Adressfilter zu entfernen.
Apply	Klicken Sie auf die Schaltfläche **Apply**, um die Filterkonfigurationen anzuwenden.

Anmerkung: *Sie müssen die Einstellungen mit **Save** speichern (Seite 159), wenn Sie diese Einstellungen nach Ausschalten des ICRL-M beibehalten möchten.*

4.10.2. Port Security

Verwenden Sie die Seite *Port Security*, um die Sicherheit Port für Port zu konfigurieren.

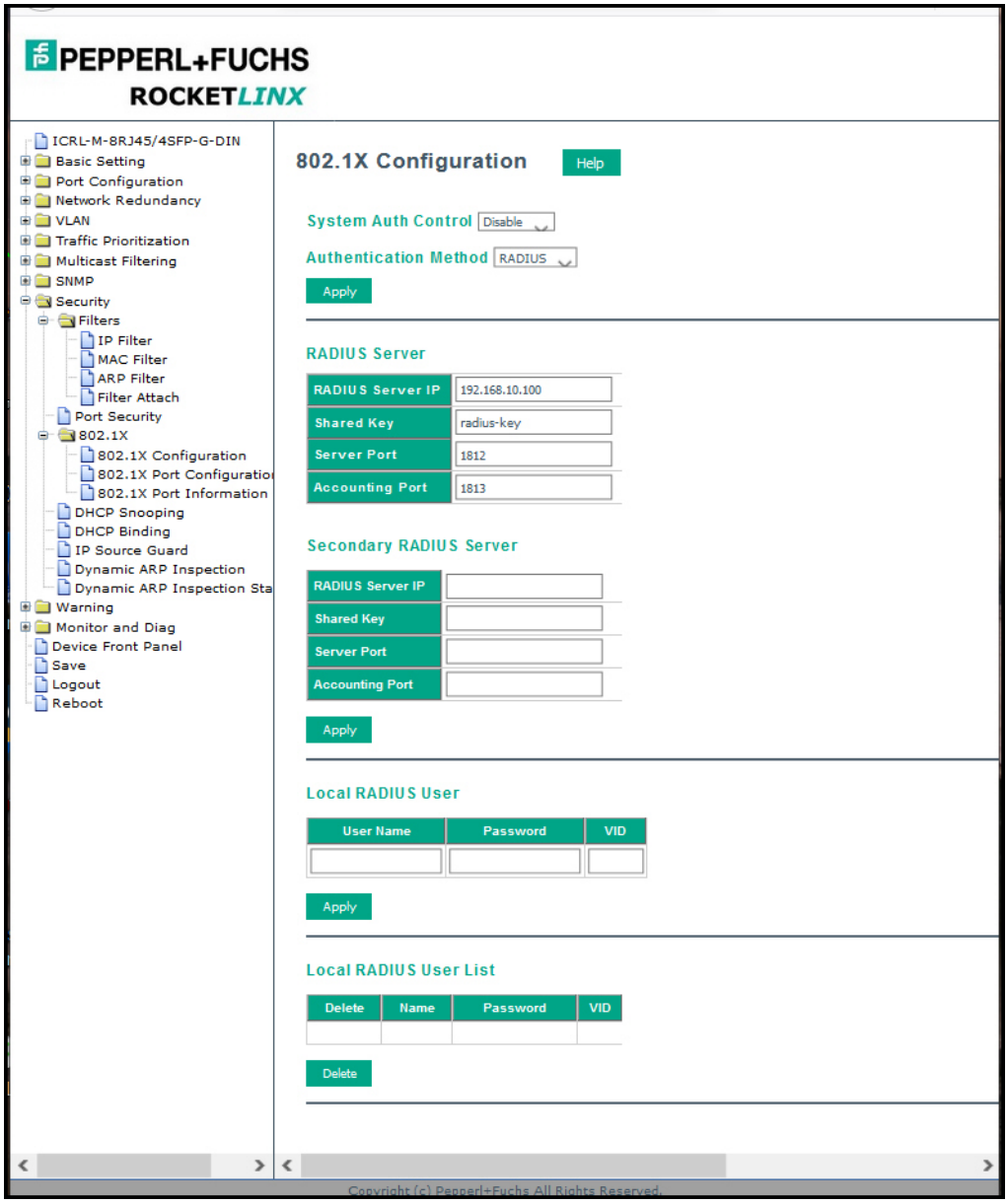


Seite „Port Security“	
Port	Die Port-ID.
Security	Aktivieren oder deaktivieren Sie die Portsicherheit an diesem Port.
Sticky	Aktivieren oder deaktivieren Sie die Stickiness an diesem Port.
Auto Learn	Gibt die maximale Anzahl von MAC-Adressen an, die dynamisch am Port ermittelt werden können. Der gültige Bereich ist 0–10.
Shutdown Time	Gibt an, wie lange der Port abgeschaltet werden soll. Der gültige Bereich liegt bei einer Sicherheitsverletzung zwischen 0 und 86.400 Sekunden.

Seite „Port Security“ (Fortsetzung)	
Shutdown Status	Zeigt an, ob der Port abgeschaltet ist oder nicht.
Shutdown Elapsed Time	Zeigt die abgelaufene Zeit für das Abschalten des Ports an.
Apply	Klicken Sie auf die Schaltfläche **Apply**, um „Port Security State“-Konfigurationen anzuwenden.
Add Port Security Entry	
Port	Die Port-ID; wenn Sie einen neuen MAC-Eintrag einfügen möchten, muss die Port-ID beim Erstellen eines neuen Eintrags korrekt sein.
VID	Die VLAN-ID; wenn Sie einen neuen MAC-Eintrag einfügen möchten, muss die VLAN-ID beim Erstellen eines neuen Eintrags korrekt sein.
MAC Address	MAC-Adresse des Eintrags.
Add	Klicken Sie auf die Schaltfläche **Add**, um einen Portsicherheitseintrag hinzuzufügen.
Show Port Security List	
Port	Die Port-ID des Eintrags.
Address Type	Typ der Sicherheits-MAC-Adresse. Sicherheit ist statische Sicherheits-MAC-Adresse. Sicherheit ist automatisch gelernte MAC-Adresse.
VID	Die VLAN-ID des Eintrags.
MAC Address	MAC-Adresse des Eintrags.
Remove	Klicken Sie auf die Schaltfläche **Remove**, um den ausgewählten Portsicherheitseintrag zu entfernen.

4.10.3. 802.1X Configuration

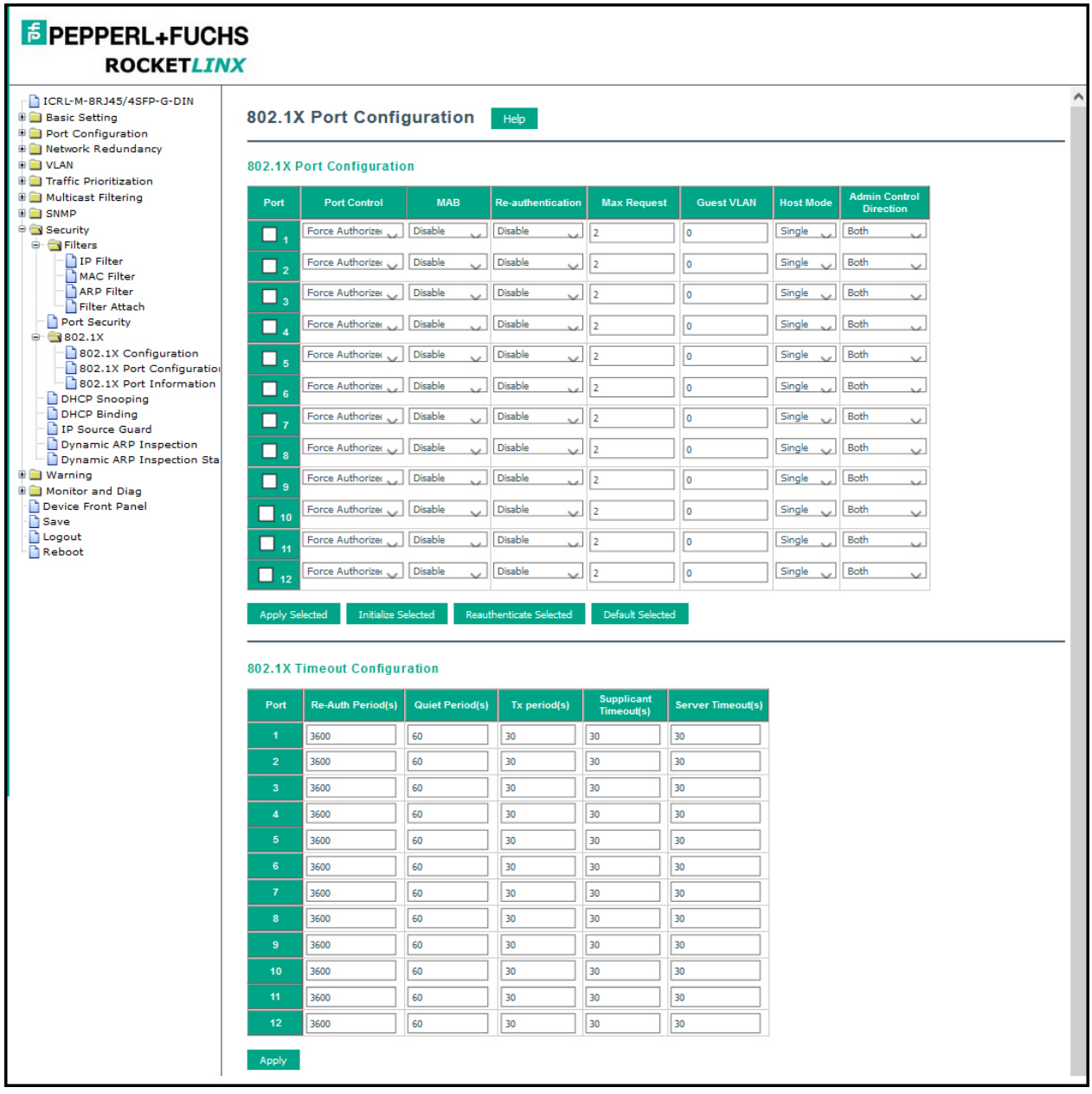
IEEE 802.1X ist das Protokoll, das eine Authentifizierung durchführt, um Zugriff auf IEEE-802-LANs zu erhalten. Es handelt sich um eine Netzwerkzugriffskontrolle auf Portbasis. Mit dieser Funktion kann der ICRL-M steuern, welche Verbindung verfügbar ist oder nicht.



Seite „IEEE 802.1x“	
System Auth Control	(De-)Aktivieren Sie mit **Enable**/**Disable** die IEEE-802.1x-Authentifizierung.
Authentication Method	**RADIUS** ist ein Authentifizierungsserver, der einen Schlüssel für die Authentifizierung bereitstellt. Wenn Sie diese Methode verwenden, müssen Sie den Switch mit dem Server verbinden. Wenn Sie die Authentifizierungsmethode **Local** auswählen, verwendet der Switch die lokale Benutzerdatenbank, die auf dieser Seite zur Authentifizierung erstellt werden kann.
RADIUS Server	
RADIUS Server IP	Die IP-Adresse des RADIUS-Servers.
Shared Key	Das Kennwort, das für die Kommunikation zwischen dem ICRL-M und dem RADIUS-Server verwendet wird.
Server Port	Der UDP-Port des RADIUS-Servers.
Accounting Port	Der Port für Pakete, die die Anmelde- oder Abmeldeinformationen für das Konto enthalten.
Secondary RADIUS Server	
RADIUS Server IP	Sie können einen sekundären RADIUS-Server einrichten, wenn der primäre RADIUS-Server ausfällt.
Shared Key	Das Kennwort, das für die Kommunikation zwischen dem ICRL-M und dem sekundären RADIUS-Server verwendet wird.
Server Port	Der UDP-Port des sekundären RADIUS-Servers.
Accounting Port	Der Port für Pakete, die die Anmelde- oder Abmeldeinformationen des Kontos für den sekundären Server enthalten.
Local RADIUS User	
User Name	Der Benutzername des lokalen RADIUS-Benutzers.
Password	Das Kennwort des lokalen RADIUS-Benutzers.
VID	Das Kennwort des lokalen RADIUS-Benutzers.
Apply	Klicken Sie auf die Schaltfläche **Apply**, um einen lokalen RADIUS-Benutzer hinzuzufügen.
Local RADIUS User List	
Delete	Dies ist das Auswahlelement für das Löschen des lokalen RADIUS-Benutzers.
Name	Dies ist der Name des lokalen RADIUS-Benutzers.
Password	Dies ist das Kennwort des lokalen RADIUS-Benutzers.
VID	Dies ist die VLAN-ID des lokalen RADIUS-Benutzers.
Delete	Klicken Sie auf die Schaltfläche **Remove**, um ausgewählte lokale RADIUS-Benutzer zu entfernen.

4.10.4. 802.1X Port Configuration

Nach der Konfiguration von **RADIUS Server** oder **Local RADIUS User List** müssen Sie auch den Authentifizierungsmodus, das Authentifizierungsverhalten, das angewendete VLAN für jeden Port und die zulässige Kommunikation konfigurieren.

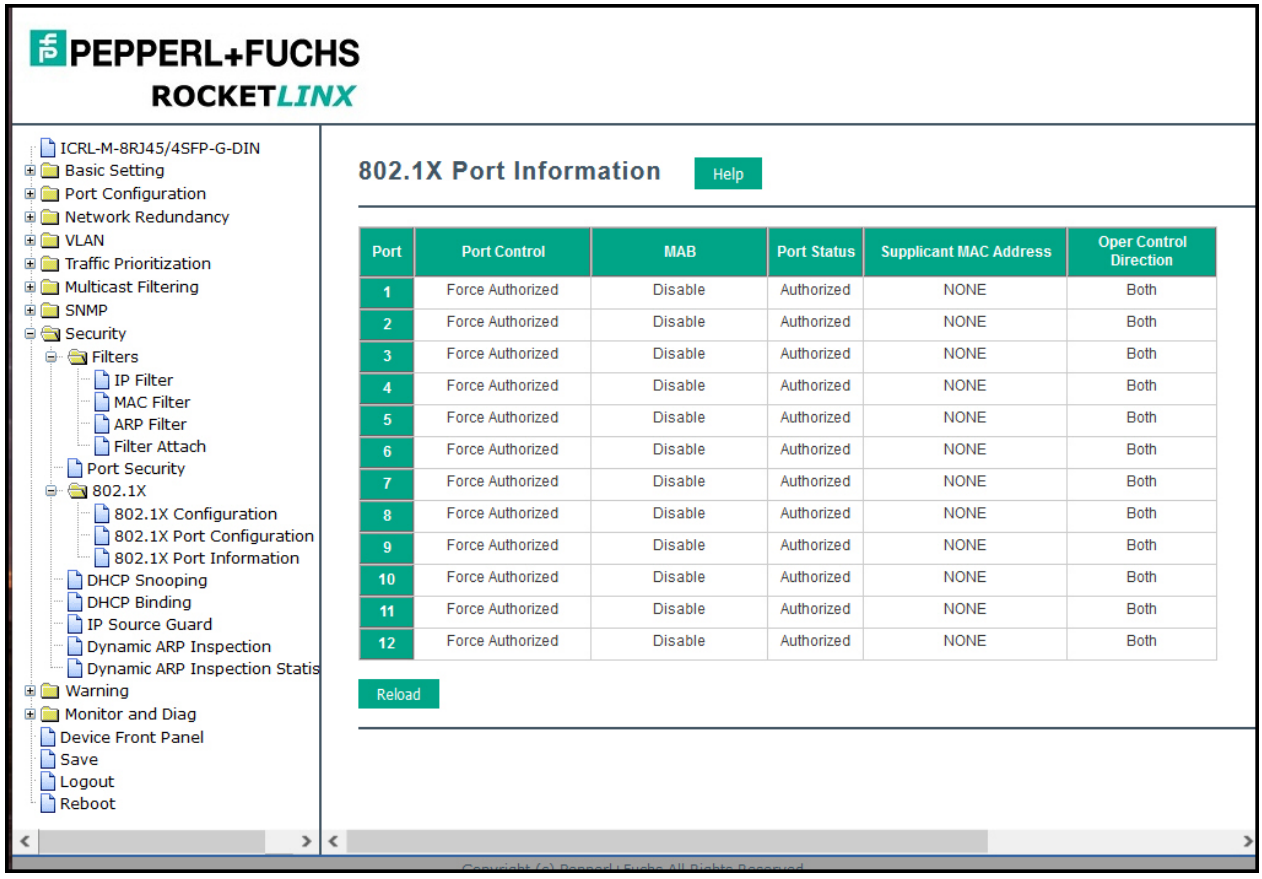


5/21/20

Seite „802.1x Port Configuration“	
802.1X Port Configuration	
Port Control	**Force Authorized** bedeutet, dass dieser Port autorisiert ist; die Daten können frei empfangen/gesendet werden. **Force Unauthorized** bedeutet genau das Gegenteil: Der Port ist blockiert. Um diesen Port mit einem RADIUS-Server zu steuern, wählen Sie **Auto** für die Portsteuerung aus.
MAB	Wenn dieses Feld aktiviert ist, wird die funktionale MAC-Adresse zur Authentifizierung an den RADIUS-Server übergeben.
Reauthentication	Wenn dieses Feld aktiviert ist, fordert der ICRL-M den Client zur erneuten Authentifizierung auf. Das Standardzeitintervall beträgt 3600 Sekunden.
Max Request	Dies ist die maximale Anzahl von Clientanfragen, die der ICRL-M zulässt.
Guest VLAN	Der zulässige Bereich für dieses Feld ist 0 bis 4094. Wenn dieses Feld auf 0 gesetzt ist, bedeutet dies, dass der Port nach einem Authentifizierungsfehler blockiert wird. Andernfalls ist der Port auf Gast-VLAN eingestellt.
Host Mode	Wenn mehr als ein Gerät mit diesem Port verbunden ist, stellen Sie den Hostmodus auf **Single** ein, d. h., nur der erste PC, der erfolgreich authentifiziert wird, kann auf diesen Port zugreifen. Wenn dieser Port auf **Multi** gesetzt ist, können alle Geräte auf diesen Port zugreifen, sobald einer von ihnen die Authentifizierung erfolgreich abschließt.
Admin Control Direction	Verwenden Sie diese Option, um zu bestimmen, welche Geräte nur Daten senden oder sowohl Daten senden als auch empfangen können.
Apply	Klicken Sie auf **Apply**, um die Einstellungen anzuwenden.
Initialize Selected	Klicken Sie hier, um den Autorisierungsstatus des ausgewählten Ports auf den Initialisierungsstatus festzulegen.
Reauthenticate Selected	Klicken Sie hier, um eine EAP-Anfrage an den Anfragesender zu senden, um eine erneute Authentifizierung anzufordern.
Default Selected	Klicken Sie hier, um die konfigurierbaren IEEE-802.1x-Parameter des ausgewählten Ports auf die Standardwerte zurückzusetzen.
802.1x Timeout Configuration	
Re-Auth Period(s)	Steuert das Zeitintervall für die erneute Authentifizierung (Sekunden). Sie können einen Bereich zwischen 1 und 65.535 eingeben.
Quiet Period(s)	Wenn die Authentifizierung fehlschlägt, wartet der ICRL-M eine gewisse Zeit ab und versucht dann erneut, mit dem RADIUS-Server zu kommunizieren.
Tx Period(s)	Das Zeitintervall der Authentifizierungsanfrage.
Supplicant Timeout(s)	Das Timeout für die Clientauthentifizierung.
Sever Timeout(s)	Das Timeout für die Serverantwort auf die Authentifizierung.
Apply	Klicken Sie auf **Apply**, um die Einstellungen anzuwenden. ***Anmerkung:*** *Sie müssen die Einstellungen mit **Save** speichern (Seite 159), wenn Sie diese Einstellungen nach Ausschalten des ICRL-M beibehalten möchten.*

4.10.5. 802.1X Port Information

Auf der Seite *802.1X Port Information* können Sie den Portstatus für **Port Control Status**, **Authorize Status**, **Authorized Supplicant** und **Oper Control Direction** für jeden Port anzeigen.

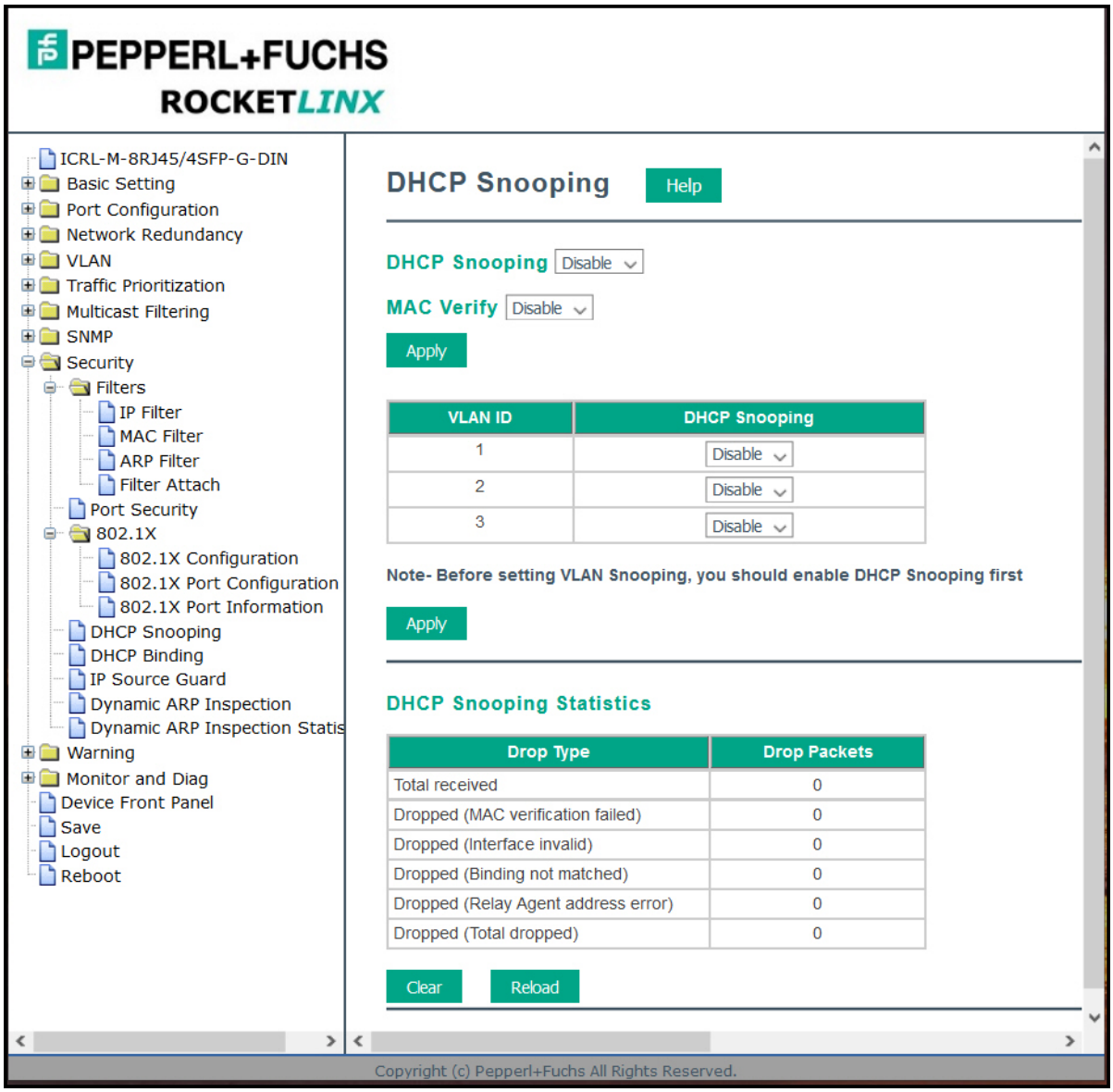


Seite „802.1X Port Information“	
Port	Die Port-ID.
Port Control	„Force Authorized“ bedeutet, dass dieser Port autorisiert ist und die Daten frei empfangen/gesendet werden können. „Force Unauthorized“ bedeutet genau das Gegenteil: Der Port ist blockiert.
Authorized Status	Der Autorisierungsstatus des Ports.
Authorized Supplicant	Die MAC-Adresse des autorisierten Supplicants.
Oper Control Direction	Gibt an, ob ein nicht authentifizierter Port eingehenden und ausgehenden Datenverkehr oder nur eingehenden Datenverkehr deaktiviert. „Both“ bedeutet, dass eingehender und ausgehender Datenverkehr blockiert werden. „In“ bedeutet, dass eingehender Datenverkehr blockiert wird.
Reload	Klicken Sie auf **Reload**, um den 802.1X-Portstatus neu zu laden

4.10.6. DHCP Snooping

DHCP-Snooping umfasst eine Reihe von Techniken, die auf die Sicherheit eines vorhandenen DHCP-Netzwerks angewendet werden. Mit der DHCP-Snooping-Funktion verwaltet der DHCP-Server den Netzwerkzugriff und ermöglicht den Zugriff mit einer bestimmten IP- und MAC-Adresse von einem bestimmten ICRL-M-Port, der auf das Netzwerk zugreifen kann. Sie bietet außerdem Schutz, um das Hinzufügen gefälschter DHCP-Server in einem sicheren Netzwerk durch Angreifer zu verhindern, die versuchen, den DHCP-Prozess zu übernehmen. Sobald der ICRL-M das Problem erkannt hat, wird der Port, mit dem der Eindringling verbunden ist, gesperrt, um den Netzwerkzugriff zu schützen.

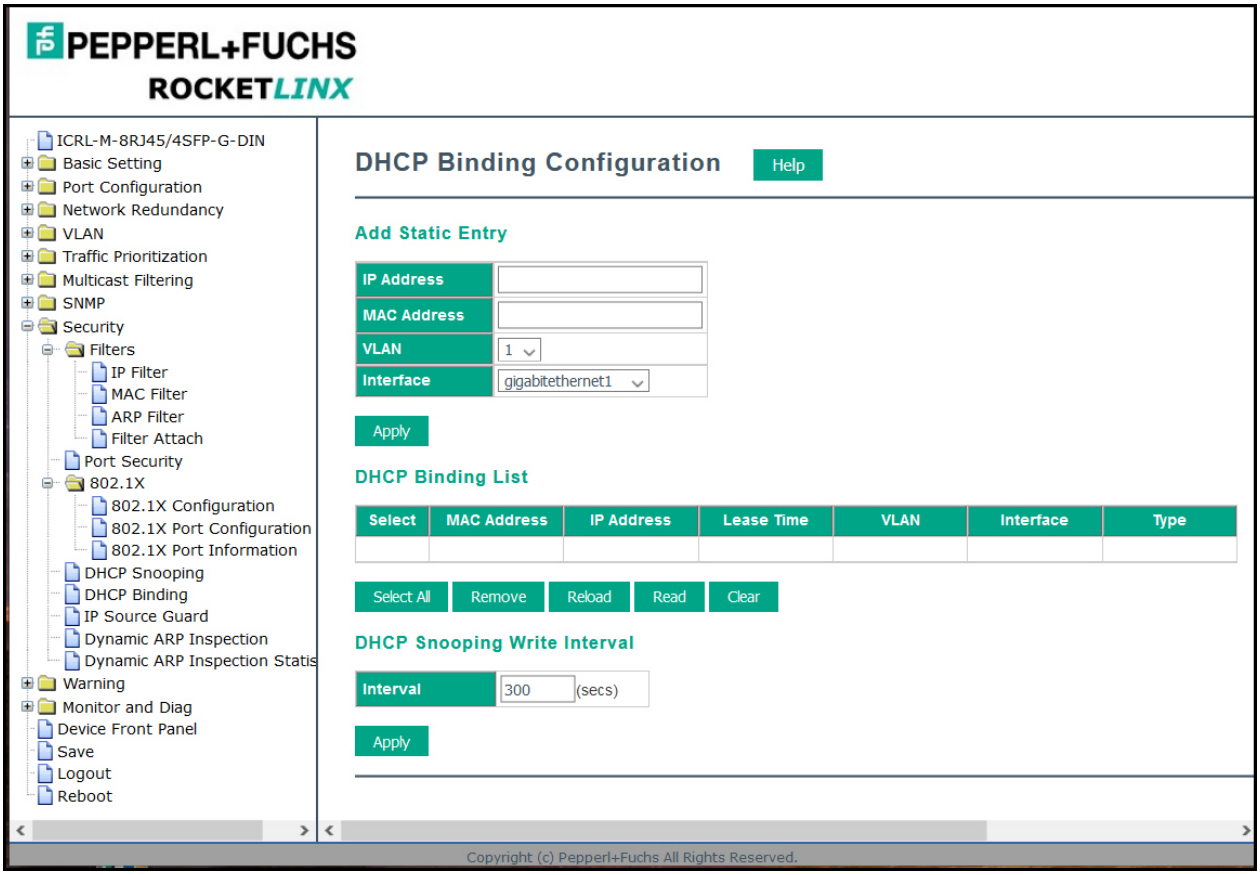
Anmerkung: *DHCP-Snooping bietet eine wertvolle Sicherheitsfunktion und ist für die Unterstützung von IP Source Guard erforderlich.*



Seite „DHCP Snooping“	
DHCP Snooping	Aktiviert/deaktiviert DHCP-Snooping global.
MAC Verify	Aktiviert/deaktiviert MAC-Überprüfung global. Wenn diese Option aktiviert ist, überprüft das Layer-2-DHCP-Snooping-Modul die MAC-Quelladresse anhand der Hardwareadresse des Clients in den empfangenen DHCP-Paketen.
Apply	Klicken Sie auf die Schaltfläche **Apply**, um die Konfigurationen anzuwenden.
DHCP Snooping Statistics	
Total received	Die Anzahl der empfangenen Snooping-Pakete.
MAC verification failed	Die Anzahl der fehlgeschlagenen Pakete für die MAC-Überprüfung.
Interface invalid	Anfragepaket stimmt nicht mit seiner Schnittstelle überein.
Binding not matched	Zählt die Pakete, bei denen die Bindung nicht übereinstimmt.
Relay Agent address error	Zählt die Pakete mit fehlerhafter Relay-Agent-Adresse.
Total dropped	Die Anzahl der verworfenen Snooping-Pakete.
Clear	Klicken Sie auf die Schaltfläche **Clear**, um die Anzahl der Pakete zu löschen.
Reload	Klicken Sie auf die Schaltfläche **Reload**, um die Anzahl der Pakete zu aktualisieren.

4.10.7. DHCP Binding Configuration

„DHCP Binding Configuration“ zeigt die Snooping-Bindungstabelle an. Darüber hinaus können Sie einen statischen Eintrag hinzufügen.

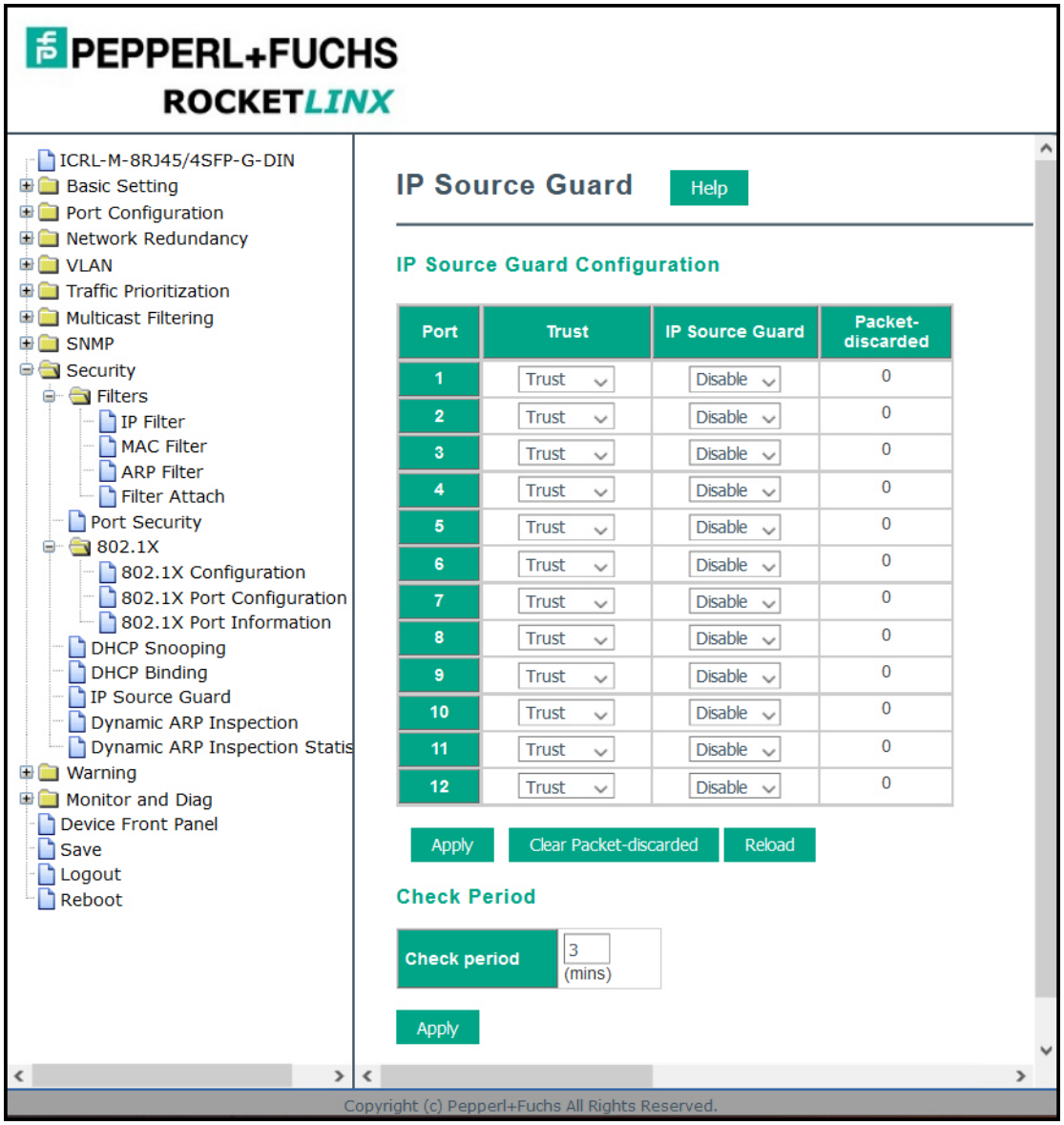


Seite „DHCP Binding Configuration“	
Add Static Entry	
IP Address	IP des Eintrags.
MAC Address	MAC-Adresse des Eintrags.
VLAN	VLAN des Eintrags.
Schnittstelle	Schnittstelle des Eintrags.
Apply	Klicken Sie auf die Schaltfläche **Apply**, um einen statischen Eintrag hinzuzufügen.
DHCP Binding List	
MAC Address	Zeigt die MAC-Adresse des Eintrags an.
IP Address	Zeigt die IP-Adresse des Eintrags an.
Lease Time	Die Lease-Zeit des Eintrags.
VLAN	Der Eintrag gehört zur VLAN-ID.
Schnittstelle	Schnittstelle des Eintrags.

Seite „DHCP Binding Configuration“ (Fortsetzung)	
Type	Der Eintragstyp: Static/Dynamic.
Select All	Klicken Sie auf die Schaltfläche **Select All**, um alle Einträge auszuwählen.
Remove	Klicken Sie auf die Schaltfläche **Remove**, um die ausgewählten Einträge zu entfernen.
Reload	Klicken Sie auf die Schaltfläche **Reload**, um die temporären Einträge zu laden.
Read	Klicken Sie auf die Schaltfläche **Read**, um die Einträge der DHCP-Bindungsdatenbank zu laden.
Clear	Klicken Sie auf die Schaltfläche **Clear**, um alle Einträge und die Bindungsdatenbank zu löschen.
DHCP Snooping Write Interval:	
Interval	Schreibt die aktuelle Bindungstabelle in das System. (Sek.)
Apply	Klicken Sie auf die Schaltfläche **Apply**, um die Änderung am Schreibintervall anzuwenden.

4.10.8. IP Source Guard

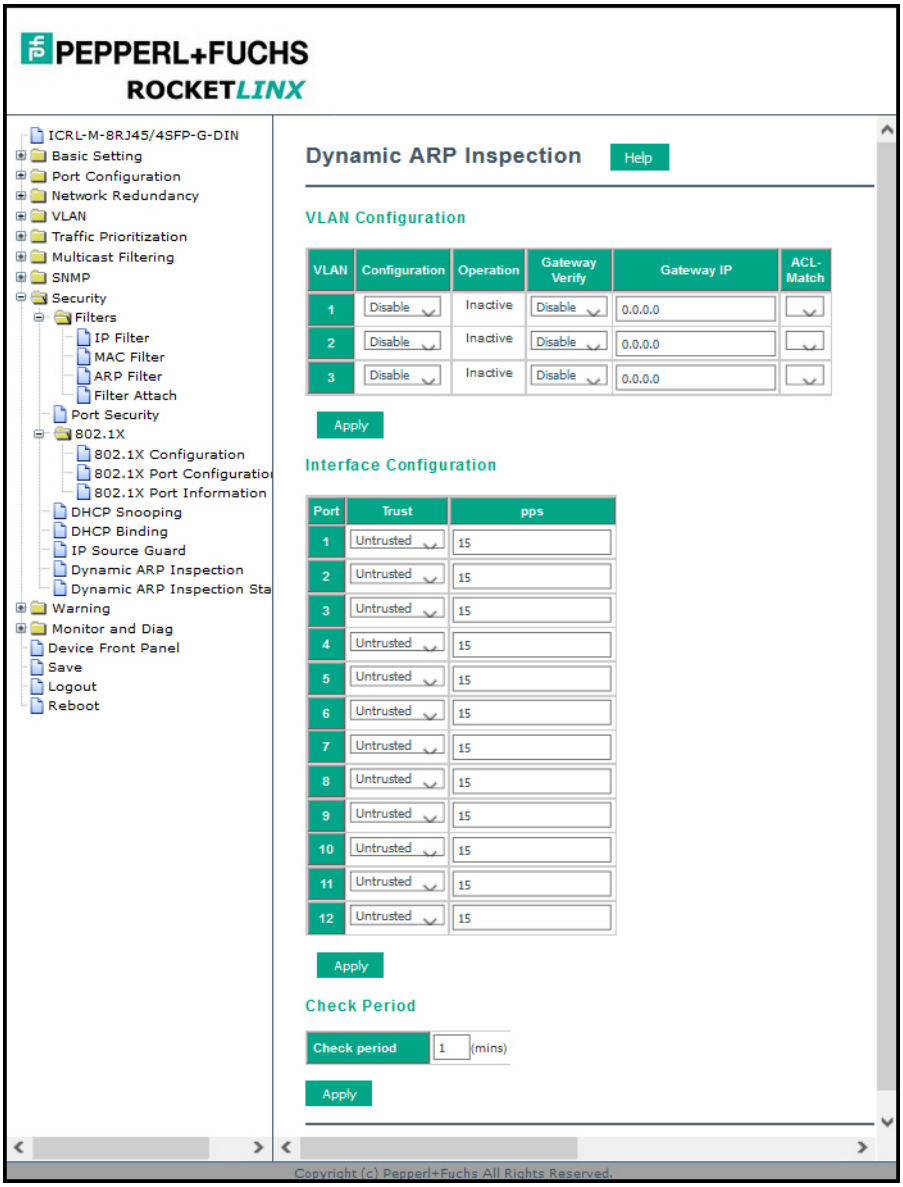
IP Source Guard ist eine Sicherheitsfunktion, die den IP-Datenverkehr an einem nicht vertrauenswürdigen Switch-Layer-2-Port beschränkt, indem der Datenverkehr basierend auf der DHCP-Snooping-Bindungsdatenbank oder den manuell konfigurierten IP-Quellbindungen gefiltert wird. Diese Funktion verhindert IP-Spoofing-Angriffe, bei denen ein Host versucht, die IP-Adresse eines anderen Hosts zu spoofen und zu verwenden.



Seite „IP Source Guard“	
IP Source Guard Configuration	
Trust	Aktiviert/deaktiviert Vertrauensstellung am jeweiligen Port.
IP Source Guard	Konfigurieren Sie die Schnittstelle als „Enables IPSG“ oder „Disables IPSG“. Wenn IP Source Guard auf einer Schnittstelle aktiviert ist, wird eingehender IP-Datenverkehr an einer Schnittstelle zugelassen, wenn ein übereinstimmender Eintrag in der IP-Quell-Bindungsdatenbank vorhanden ist. Andernfalls ist der gesamte eingehende IP-Datenverkehr an einer Schnittstelle unabhängig von der IP-Bindungsdatenbank zulässig.
Packet-discarded	Zeigt verworfene Pakete für den jeweiligen Port an.
Apply	Klicken Sie auf die Schaltfläche **Apply**, um die Konfigurationen anzuwenden.
Clear Packet-discarded	Klicken Sie auf die Schaltfläche **Clear Packet-discarded**, um die Anzahl verworfener Pakete zu löschen.
Check Period	
Check Period	Der Timer für die Aktualisierung verworfener Pakete. Dieser bestimmt, über welche Dauer die verworfenen Pakete berechnet werden.
Apply	Klicken Sie auf die Schaltfläche **Apply**, um die Konfigurationen für den Überprüfungszeitraum anzuwenden.

4.10.9. Dynamic ARP Inspection

Die dynamische ARP-Überprüfung (Dynamic ARP Inspection, DAI) ist eine Sicherheitsfunktion, die ARP-Angriffe verhindert. Der ICRL-M empfängt ein ARP-Paket an einem nicht vertrauenswürdigen Port und vergleicht die IP-zu-MAC-Adressen-Bindung mit Einträgen aus der DHCP-Snooping-Datenbank oder den ARP-Zugriffslisten. Wenn keine Übereinstimmung vorhanden ist, wird das ARP-Paket vom ICRL-M gelöscht, um die Netzwerk-Performance sicherzustellen.

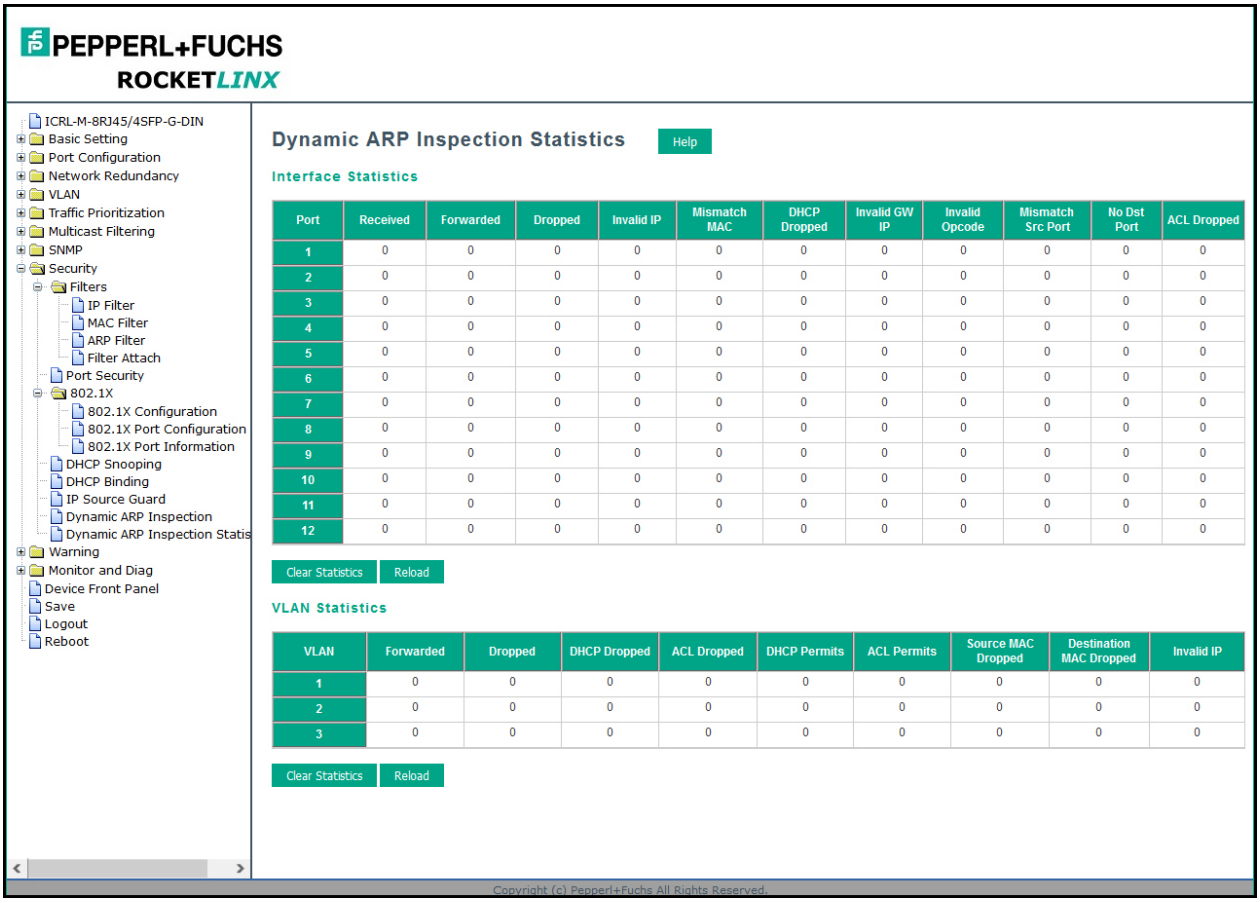


5/21/20

Seite „Dynamic ARP Inspection“	
VLAN Configuration	
VLAN	Zeigt den VLAN-Index an.
Configuration	Aktivieren oder deaktivieren Sie DAI für die einzelnen VLANs.
Operation	Zeigt den DAI-Betriebszustand an.
Gateway Verify	Aktivieren/deaktivieren Sie die Gateway-Überprüfung.
Gateway IP	Gateway-IP-Adresse.
ACL-Match	Wählen Sie eine der ARP-Filterregeln aus. Die leere Spalte dient nicht zum Festlegen der APR-Regel.
Interface Configuration	
Trust	Legen Sie für jeden Port „Trust“ oder „Untrust“ für DAI fest.
pps	Pakete pro Sekunde.
Apply	Klicken Sie auf die Schaltfläche **Apply**, um die Konfigurationsänderung anzuwenden.
Check Period	
Check Period	Der Timer für die Aktualisierung verworfener Pakete. Dieser bestimmt, über welche Dauer die verworfenen Pakete berechnet werden.
Apply	Klicken Sie auf die Schaltfläche **Apply**, um die Konfigurationen für den Überprüfungszeitraum anzuwenden.

4.10.10. Dynamic ARP Inspection Status

Auf dieser Seite werden DAI-Statistiken für das angegebene VLAN und den angegebenen Port angezeigt.



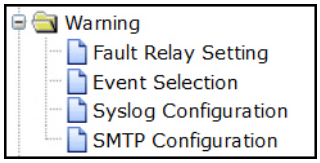
Seite „Dynamic ARP Inspection Statistics“	
Interface statistics	
Port	Dies ist die Port-ID.
Received	Die Anzahl der empfangenen ARP-Pakete.
Forwarded	Die Anzahl der weitergeleiteten ARP-Pakete.
Dropped	Die Anzahl der verworfenen ARP-Pakete.
Invalid IP	Die Anzahl der Pakete mit IP-Zieladressen ohne Übereinstimmung mit der DHCP-Bindungstabelle.
Mismatch MAC	Die MAC-Quelladresse des Ethernet-Headers stimmt nicht mit der MAC-Absenderadresse überein.
DHCP Dropped	Die Anzahl der ARP-Pakete, die durch fehlende Übereinstimmung mit der DHCP-Bindungstabelle verworfen wurden.
Invalid GW IP	Die Anzahl der ungültigen Gateway-IP-Adressen.
Invalid Opcode	Die Anzahl der empfangenen ungültigen Opcodes.

Seite „Dynamic ARP Inspection Statistics“ (Fortsetzung)	
Mismatch Src Port	Die Anzahl der Quellports ohne Übereinstimmung mit der DHCP-Bindungstabelle.
No Dst Port	Die Anzahl der aufgrund nicht gefundener Zielports verworfenen Pakete.
ACL Dropped	Die Anzahl der ARP-Pakete, die durch die ACL-Einstellung verworfen wurden.
Clear	Klicken Sie auf die Schaltfläche **Clear Statistics**, um die Schnittstellenstatistiken zu löschen.
Reload	Klicken Sie auf die Schaltfläche **Reload**, um die Statistiken neu zu laden.
VLAN Statistics	
VLAN	Dies ist die VLAN-ID.
Forwarded	Die Anzahl der weitergeleiteten ARP-Pakete.
Dropped	Die Anzahl der verworfenen ARP-Pakete.
DHCP Dropped	Die Anzahl der ARP-Pakete, die durch fehlende Übereinstimmung mit der DHCP-Bindungstabelle verworfen wurden.
ACL Dropped	Die Anzahl der ARP-Pakete, die durch die ACL-Einstellung verworfen wurden.
DHCP Permits	Die Anzahl der ARP-Paketgenehmigungen nach DHCP-Bindungstabelle.
ACL Permits	Die Anzahl der ARP-Paketgenehmigungen nach ACL-Einstellung.
Src MAC Dropped	Die MAC-Quelladresse des Ethernet-Headers stimmt nicht mit der MAC-Absenderadresse überein.
Dest MAC Dropped	Die Anzahl der ARP-Pakete, die aufgrund nicht übereinstimmender MAC-Zieladresse verworfen wurden.
Invalid IP	Die Anzahl der Pakete mit IP-Zieladressen ohne Übereinstimmung mit der DHCP-Bindungstabelle.
Clear Statistics	Klicken Sie auf die Schaltfläche **Clear Statistics**, um die VLAN-Statistiken zu löschen.
Reload	Klicken Sie auf die Schaltfläche **Reload**, um die Statistiken neu zu laden.

4.11. Warnung

Der ICRL-M bietet verschiedene Arten von Warnfunktionen, mit denen Sie den Status der angeschlossenen Geräte oder Änderungen in Ihrem Netzwerk remote überwachen können. Zu den Funktionen gehören Fehlerrelais, Systemprotokoll und SMTP-E-Mail-Warnung.

Die folgenden Webseiten sind in dieser Gruppe enthalten:

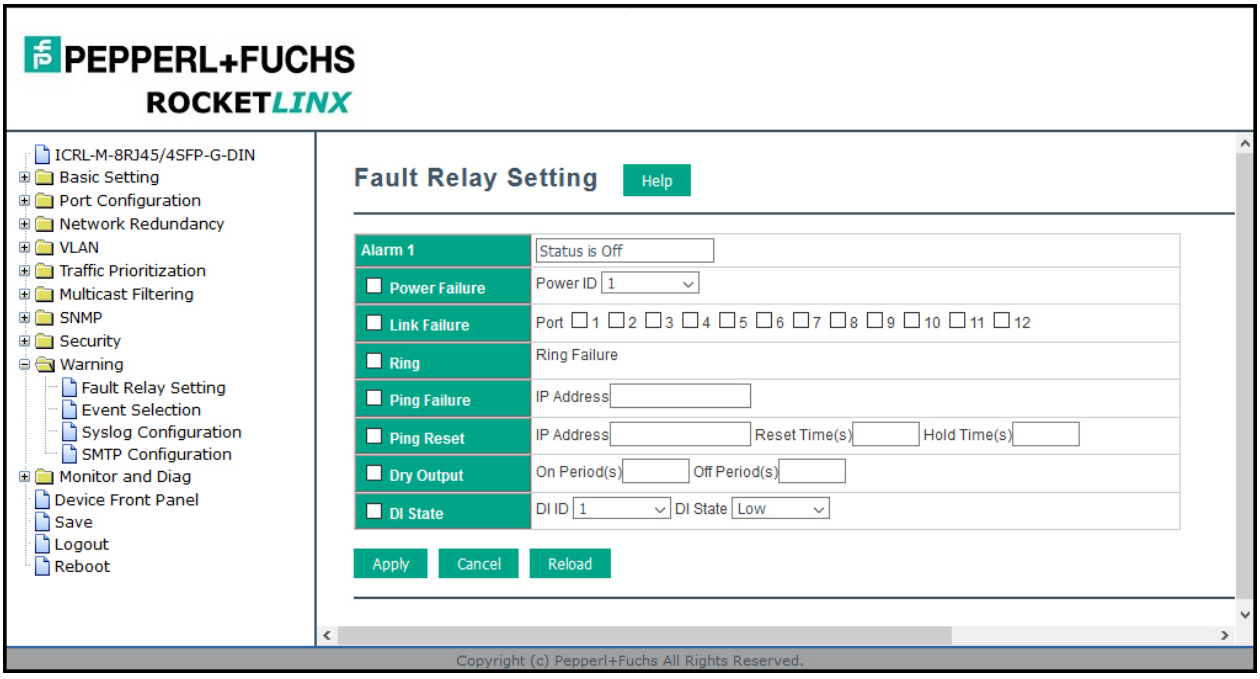


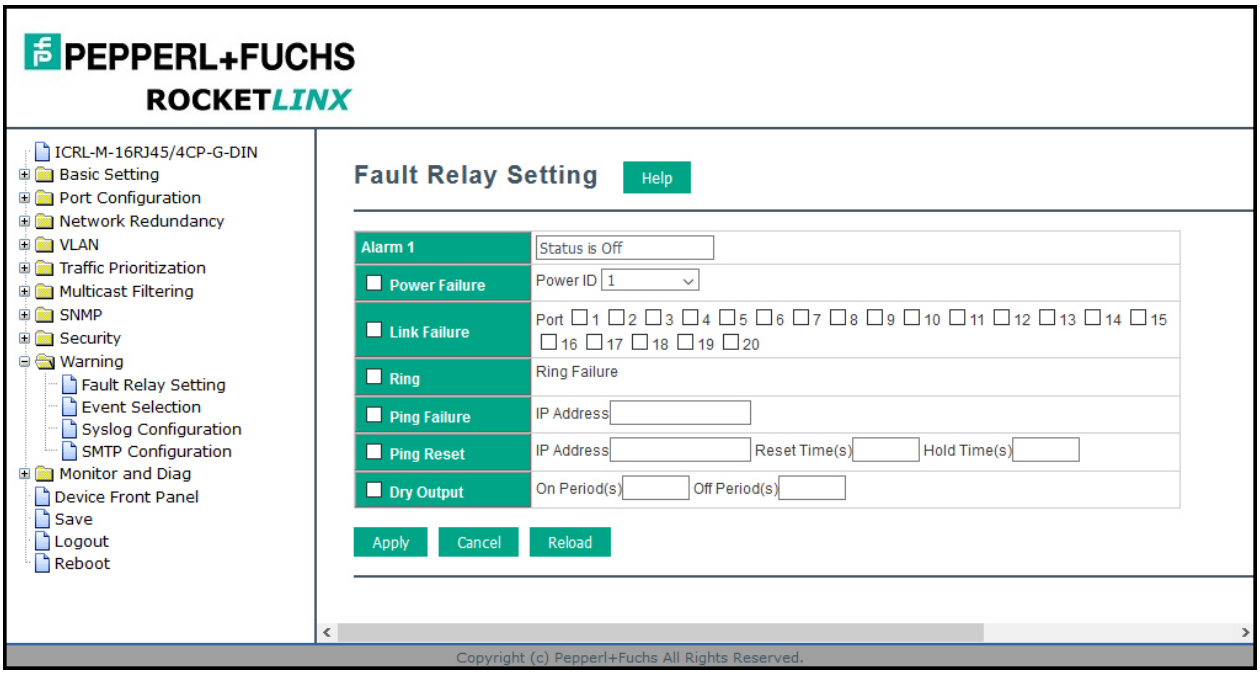
- *Fault Relay*
- *Event Selection* auf Seite 145
- *SysLog Configuration* auf Seite 147
- *SMTP Configuration* auf Seite 148

Optional können Sie die Befehlszeilenschnittstelle (Command-Line Interface, CLI) für die Konfiguration verwenden (siehe *Warnungen (CLI)* auf Seite 217).

4.11.1. Fault Relay

Der ICRL-M bietet einen Alarmrelaisausgang (DO), der mehrere Fehlerzustände unterstützen kann. Die Relaiskontakte werden für normalen Betrieb unter Spannung gesetzt (offen) und schließen unter Fehlerbedingungen. Zu den Fehlerbedingungen gehören Stromausfall, Ethernet-Portverbindungsfehler, Ringtopologieänderungen, Ping-Fehler, DI-Statusänderungen oder Remote-IP-Ping-Fehler.





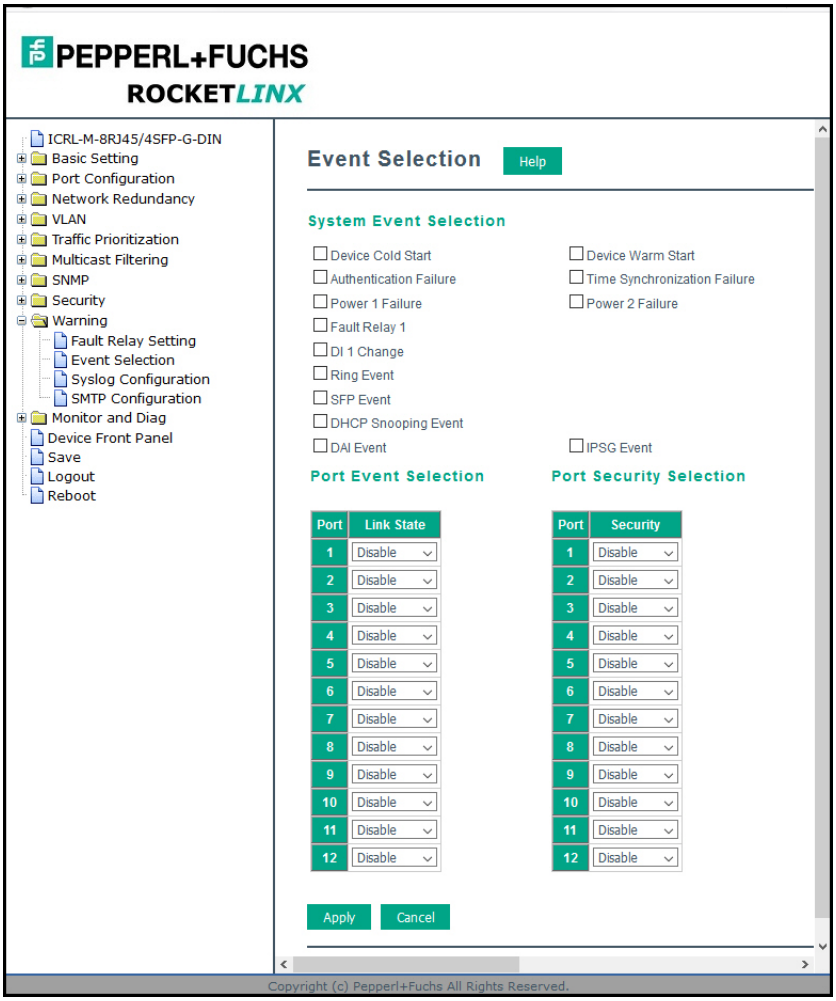
Die folgende Tabelle beschreibt die Fehlerrelaisbedingungen.

Seite „Fault Relay“	
Alarm 1	Zeigt an, ob der Alarmstatus ein- oder ausgeschaltet ist. Sie müssen eine Fehlerrelaisoption auswählen und auf **Apply** klicken, damit der Status als aktiviert angezeigt wird.
Power Failure	Erkennt den Stromeingangsstatus der ausgewählten Stromquelle oder -quellen.
Link Failure	Überwacht Ereignisse zu ausgefallenen Verbindungen für die ausgewählten Ports.
Ring	Überwacht Ringtopologieänderungen.
Ping Failure	Wenn die Ziel-IP-Adresse nicht auf die Ping-Anfrage antwortet, wird das Fehlerrelais aktiviert.
Ping Reset	Pingt das Zielgerät an und bringt das Relais dazu, ein Zurücksetzen des Stroms auf dem Remote-Gerät zu emulieren, wenn das Remote-System abstürzt. • **IP Address**: IP-Adresse des Remote-Geräts, dessen Stromversorgungsverdrahtung mit dem Relaisausgang verbunden ist. • **Reset Time (Sec)**: Dauer, über die der Relaiskontakt geöffnet wird, um das Ausschalten des Netzschalters zu emulieren. Nach dem Zurücksetzen schließt sich das Relais, um zu emulieren, dass der Netzschalter eingeschaltet ist. • **Hold Time (Sec)**: Die vom Remote-Gerät benötigte Startzeit. Nach dem Schließen des Relaiskontakts beginnt der ICRL-M nach der Haltezeit mit dem Anpingen.
Dry Output	Das Relais öffnet und schließt ständig die Kontakte. Der verfügbare Bereich beträgt 0–65.535 Sekunden. ***Anmerkung:*** *Verwenden Sie diese Funktion nicht mit anderen Ereignissen.* • **On Period**: Dauer des Kurzschlusses des Relaisausgangs (geschlossen). • **Off Period**: Dauer des Öffnungsvorgangs des Relaisausgangs.

Seite „Fault Relay“ (Fortsetzung)	
DI State (ICRL-M-8RJ45/4SFP-G-DIN)	Relais wird ausgelöst, wenn DI den Status zu „high“ oder „low“ ändert.
Apply	Klicken Sie auf **Apply**, um die Einstellungen anzuwenden. ***Anmerkung:*** *Sie müssen die Einstellungen mit **Save** speichern (Seite 159), wenn Sie diese Einstellungen nach Ausschalten des ICRL-M beibehalten möchten.*

4.11.2. Event Selection

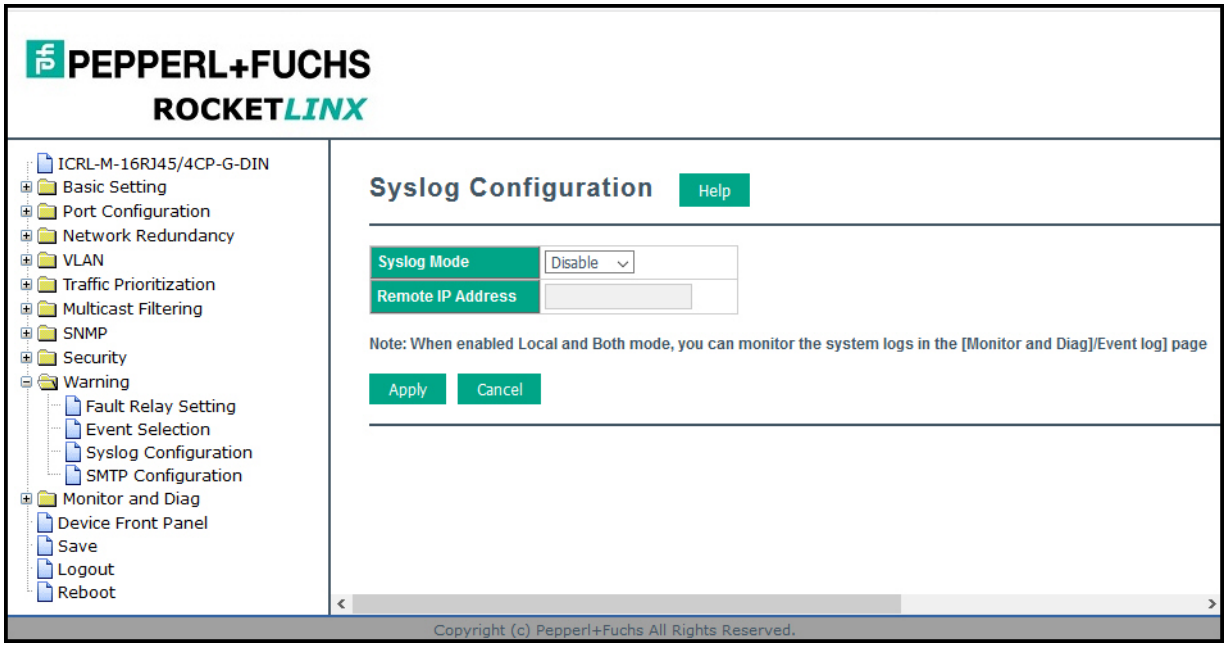
Ereignistypen können in zwei Basisgruppen unterteilt werden: Systemereignisse und Portereignisse. Systemereignisse beziehen sich auf die Gesamtfunktion des Switches, während Portereignisse mit der Aktivität bestimmter Ports in Zusammenhang stehen.



Seite „Event Selection“	
System Event Selection	**Warning is sent when….**
Device Cold Start	Die Stromversorgung wird unterbrochen und dann wieder angeschlossen.
Device Warm Start	Das Gerät wird über die CLI oder die Web-Benutzerschnittstelle neu gestartet.
Authentication failure	Ein falsches Kennwort oder eine falsche SNMP-Communityzeichenfolge wurde eingegeben.
Time Synchronize Failure	Der Zugriff auf den NTP-Server ist fehlgeschlagen.
Power 1 Failure	PW1-Stromausfall.
Power 2 Failure	PW2-Stromausfall.
Fault Relay 1	Ein Fehlerrelais wurde aktiviert.
DI 1 Change	Der Status des Digitaleingangs 1 wurde geändert.
Ring Event	Ein Ringereignis ist aufgetreten.
SFP Event	Die vom DDM-SFP-Transceiver gelesenen Informationen liegen über der Temperatur oder außerhalb des Bereichs der TX-/RX-Leistung.
DHCP Snooping Event	Wenn diese Option ausgewählt ist, generiert der Switch eine Benachrichtigung, wenn sich der Status eines DHCP-Snoopings ändert.
DAI Event	Wenn diese Option ausgewählt ist, generiert der Switch eine Benachrichtigung, wenn sich der Status einer DAI-Statistik ändert.
IPSG Event	Wenn diese Option ausgewählt ist, generiert der Switch eine Benachrichtigung, wenn sich der Status einer IPSG-Statistik ändert.
Port Event Selection	**Warning is sent when…..**
Link-Up	Der Port ist mit einem anderen Gerät verbunden.
Link-Down	Der Port ist getrennt. Beispielsweise wurde das Kabel herausgezogen oder das gegenüberliegende Gerät ist ausgefallen.
Both	Der Verbindungsstatus hat sich geändert.
Port Security Selection	**Warning is sent when…..**
Port	Die zugehörige Portnummer.
Security	Wählen Sie **Disable** oder **Enable**, um ein Portsicherheitsereignis zu generieren. Wenn dieses Ereignis eintritt, sendet der Switch eine Benachrichtigung.
Both	Der Verbindungsstatus hat sich geändert.
Apply	Klicken Sie auf **Apply**, um die Einstellungen anzuwenden. ***Anmerkung:*** *Sie müssen die Einstellungen mit **Save** speichern (Seite 159), wenn Sie diese Einstellungen nach Ausschalten des ICRL-M beibehalten möchten.*

4.11.3. SysLog Configuration

Die Seite *System Log* enthält den ICRL-M-Ereignisverlauf für den Systemadministrator. Der ICRL-M bietet zwei Systemprotokollmodi: **Local** und **Remote**.

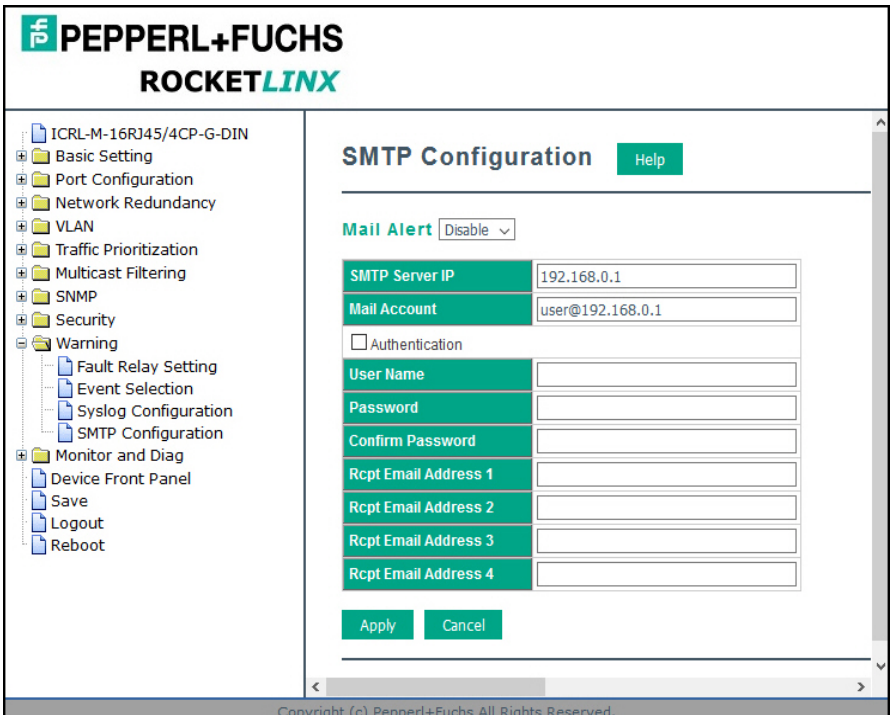


Seite „Warning – SysLog Configuration“	
Syslog Mode	Es sind zwei Systemprotokolle verfügbar: • **Local Mode**: Der ICRL-M druckt die Ereignisse, die auf der Seite *Event Selection* ausgewählt wurden, in die Tabelle *System Log* des ICRL-M. Sie können die Systemprotokolle auf der Seite *Monitor and Diag/Event Log* überwachen. • **Remote Mode**: Weisen Sie die IP-Adresse des Systemprotokollservers zu. Der ICRL-M sendet aufgetretene Ereignisse auf der Seite *Event Selection* an den Systemprotokollserver, den Sie zuweisen. • **Both**: Dadurch werden sowohl **Local**- als auch **Remote**-Modi aktiviert.
Remote IP Address	Die IP-Adresse des Systemprotokollservers.
Apply	Klicken Sie auf **Apply**, um die Einstellungen anzuwenden. ***Anmerkung:*** *Sie müssen die Einstellungen mit **Save** speichern (Seite 159), wenn Sie diese Einstellungen nach Ausschalten des ICRL-M beibehalten möchten.*

Wenn Sie die Modi **Local** oder **Both** aktivieren, können Sie die Systemprotokolle auf *Monitor and Diag/Event Log* überwachen.

4.11.4. SMTP Configuration

Der ICRL-M unterstützt eine E-Mail-Warnungsfunktion. Der ICRL-M sendet die aufgetretenen Ereignisse an einen Remote-E-Mail-Server. Die E-Mail-Warnung entspricht dem SMTP-Standard. Auf der Seite *E-Mail Alert* können Sie die SMTP-Server-IP, Absender-E-Mail und Empfänger-E-Mail zuweisen Wenn der SMTP-Server eine Authentifizierung anfordert, können Sie den Benutzernamen und das Kennwort einrichten.

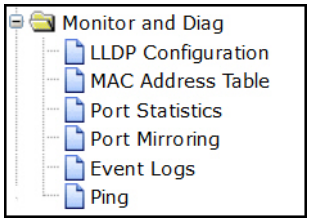


Seite „SMTP Configuration“	
SMTP Server IP Address	Geben Sie die IP-Adresse des E-Mail-Servers ein.
Mail Account	Das E-Mail-Konto für den SMTP-Server.
Authentication	Klicken Sie auf das Kontrollkästchen, um das Kennwort zu aktivieren.
User Name	Geben Sie einen E-Mail-Kontonamen ein (maximal 40 Zeichen).
Password	Geben Sie das Kennwort des E-Mail-Kontos ein.
Confirm Password	Geben Sie das Kennwort des E-Mail-Kontos erneut ein.
Sie können bis zu vier E-Mail-Adressen für den Empfang von E-Mail-Alarmen vom ICRL-M einrichten.	
Rcpt E-mail Address 1	Die erste E-Mail-Adresse, an die eine E-Mail-Benachrichtigung vom ICRL-M gesendet wird (maximal 40 Zeichen).
Rcpt E-mail Address 2	Die zweite E-Mail-Adresse, an die eine E-Mail-Benachrichtigung vom ICRL-M gesendet wird (maximal 40 Zeichen).
Rcpt E-mail Address 3	Die dritte E-Mail-Adresse, an die eine E-Mail-Benachrichtigung vom ICRL-M gesendet wird (maximal 40 Zeichen).
Rcpt E-mail Address 4	Die vierte E-Mail-Adresse, an die eine E-Mail-Benachrichtigung vom ICRL-M gesendet wird (maximal 40 Zeichen).
Apply	Klicken Sie auf **Apply**, um die Einstellungen anzuwenden. ***Anmerkung:*** *Sie müssen die Einstellungen mit **Save** speichern (Seite 159), wenn Sie diese Einstellungen nach Ausschalten des ICRL-M beibehalten möchten.*

4.12. Überwachung und Diagnose

Der ICRL-M bietet mehrere Seiten der Web-Benutzerschnittstelle, auf denen Sie den Status des Switches überwachen oder Probleme mit dem ICRL-M untersuchen können. Zu den Funktionen gehören MAC-Adresstabelle, Portstatistiken, Portspiegelung, Ereignisprotokoll und Ping.

Die folgenden Webseiten sind in dieser Gruppe enthalten:



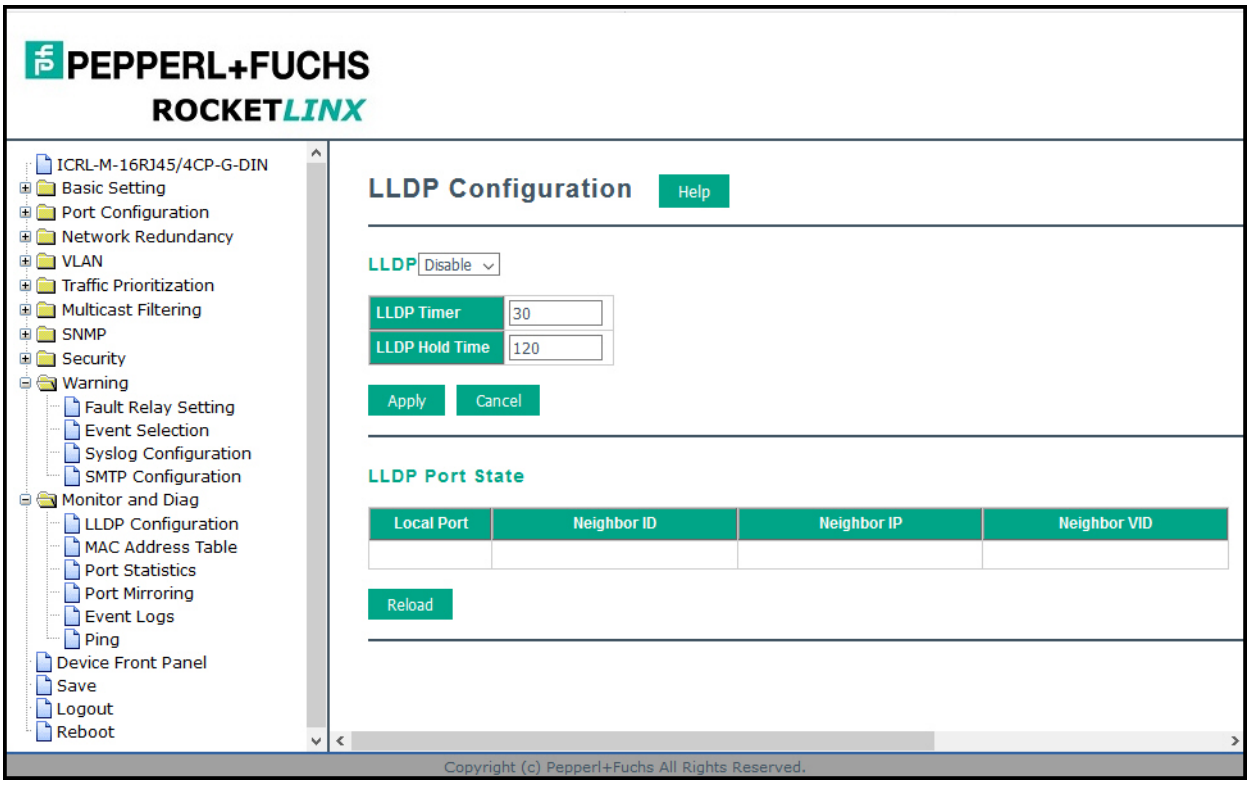
- *LLDP Configuration* auf Seite 149
- *MAC Address Table*
- *Port Statistics* auf Seite 153
- *Port Mirroring* auf Seite 154
- *Event Logs* auf Seite 155
- *Ping* auf Seite 156

Optional können Sie die Befehlszeilenschnittstelle (Command-Line Interface, CLI) für die Konfiguration verwenden (siehe *Überwachung und Diagnose (CLI)* auf Seite 220).

4.12.1. LLDP Configuration

Der ICRL-M unterstützt die Topologieerkennung mit LLDP (IEEE 802.1AB Link Layer Discovery Protocol). LLDP ermöglicht es Netzwerkgeräten, ihre Identitäten und Funktionen auf anderen Geräten im gleichen Netzwerksegment zu veröffentlichen.

LLDP ermöglicht Netzwerküberwachungssystemen, die Netzwerktopologie zu erlernen und Informationen über verwaltete Switches wie Portbeschreibungen und VLAN-IDs anzuzeigen. .

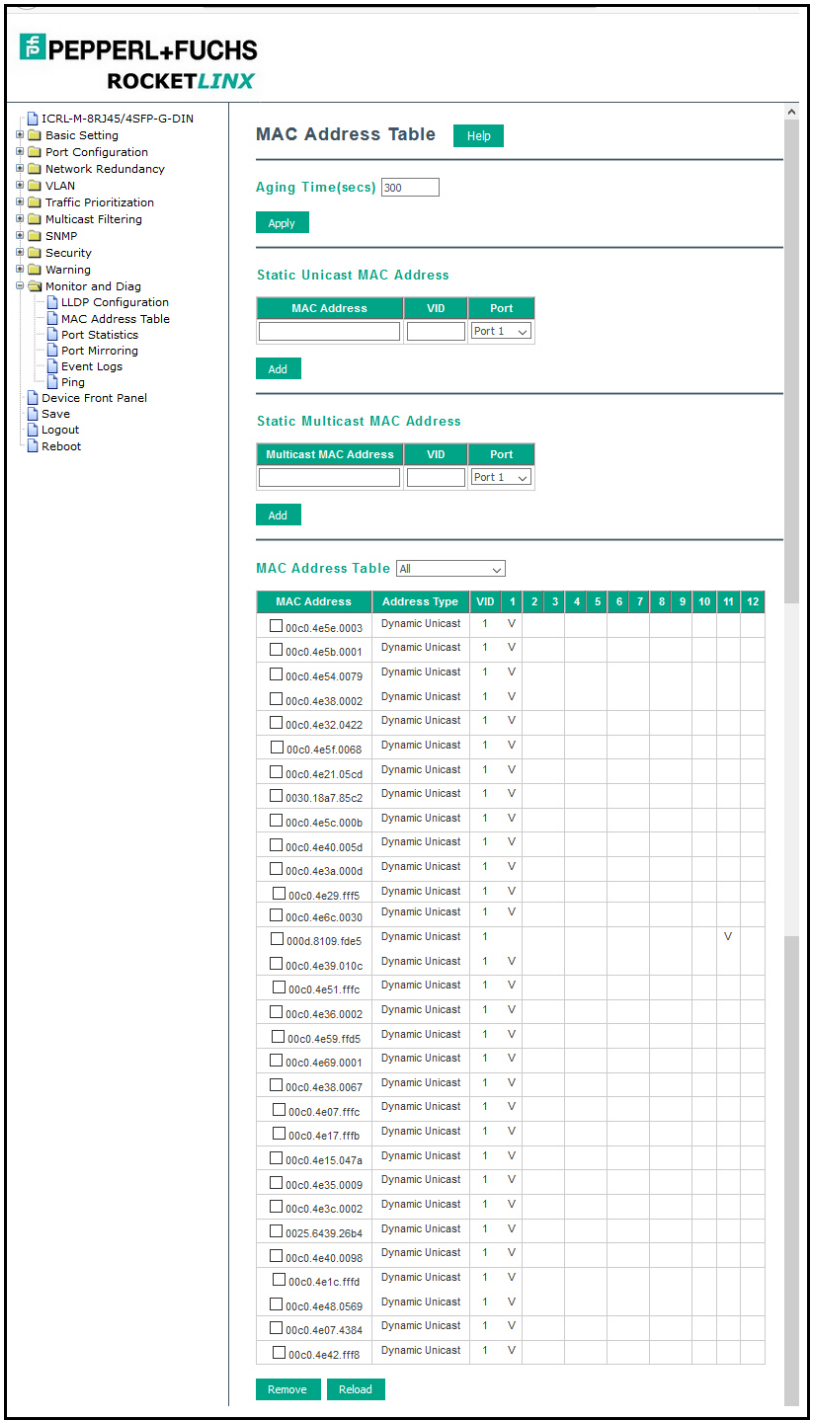


5/21/20

Seite „LLDP Configuration“	
LLDP Configuration	
LLDP	Wählen Sie **Enable**/**Disable** aus, um die LLDP-Funktion zu (de-)aktivieren.
LLDP Timer	Dies ist die Intervallzeit jedes LLDP in Sekunden; gültige Werte liegen zwischen 5 und 254. Der Standardwert ist Sekunden, wenn LLDP aktiviert ist.
LLDP Hold Time	Die Time-to-Live (TTL) des Timers. Der LLDP-Status läuft ab, wenn LLDP nicht innerhalb der Haltezeit empfangen wird. Der Standardwert beträgt 120 Sekunden, wenn das LLDP aktiviert ist. Der Bereich liegt zwischen 10 und 255.
Apply	Klicken Sie auf **Apply**, um die Einstellungen anzuwenden. ***Anmerkung:*** *Sie müssen die Einstellungen mit **Save** speichern (Seite 159), wenn Sie diese Einstellungen nach Ausschalten des ICRL-M beibehalten möchten.*
LLDP Port State	
Local Port	Die aktuelle Portnummer, die mit dem Nachbarnetzwerkgerät verknüpft ist.
Neighbor ID	Die MAC-Adresse des Nachbargeräts im gleichen Netzwerksegment.
Neighbor IP	Die IP-Adresse des Nachbargeräts im gleichen Netzwerksegment.
Neighbor VID	Die VLAN-ID des Nachbargeräts im gleichen Netzwerksegment.
Reload	Klicken Sie auf **Reload**, um die LLDP-Portstatustabelle neu zu laden.

4.12.2. MAC Address Table

Der ICRL-M stellt in der *MAC-Adresstabelle* 16.000 Einträge bereit. Sie können die Aging-Zeit ändern, statische Unicast-MAC-Adressen hinzufügen, die MAC-Adresse überwachen oder nach verschiedenen Pakettypen und Ports sortieren.



Seite „MAC Address Table“	
Aging Time (Sec)	Jede Switch-Struktur hat eine Größenbeschränkung zum Schreiben der gelernten MAC-Adresse. Um mehr Einträge für eine neue MAC-Adresse zu speichern, altert die Switch-Struktur einen nicht verwendeten MAC-Adresseintrag gemäß des „Aging Time“-Timeouts. Dieser Wert bestimmt das Intervall, in dem ein automatisch erlernter MAC-Adresseintrag in der Weiterleitungsdatenbank seit dem letzten Zugriff als Quelladresse gültig bleibt, bevor er gelöscht wird. Der Wert sollte in Schritten von 15 Sekunden angegeben werden. Das Mindestalter beträgt 15 Sekunden. Das maximale Alter beträgt 3.825 Sekunden oder fast 64 Minuten. Die standardmäßige **Aging Time** beträgt 300 Sekunden. Wenn der Wert auf 0 gesetzt ist, wird die Aging-Funktion deaktiviert und alle erlernten Adressen bleiben für immer in der Datenbank.
Static Unicast MAC Address	Bei einigen Anwendungen ist es möglicherweise erforderlich, dass Sie die statische Unicast-MAC-Adresse in die MAC-Adressentabelle eingeben. Geben Sie die MAC-Adresse (Format: xxxx.xxxx.xxxx) ein, wählen Sie die VID und die Port-ID aus und klicken Sie dann auf **Add**, um sie der MAC-Adresstabelle hinzuzufügen.
Static Multicast MAC Address	In diesem Abschnitt können Sie dem FIB manuell Multicast-MAC-Adressen hinzufügen. Manuell eingegebene Adressen laufen nicht wie automatisch erlernte Adressen ab. • Multicast MAC Address: Die Multicast-MAC-Adresse, die Sie manuell in das FIB eingeben möchten. • VID: Das VLAN, dem Sie die MAC-Adresse hinzufügen möchten. • Port: Der Port, dem die MAC-Adresse zugeordnet werden soll. Klicken Sie auf die Schaltfläche **Add**, um die statische Multicast-MAC-Adresse dem FIB hinzuzufügen.
MAC Address Table	Hierdurch werden alle MAC-Adressen angezeigt, die von der Switch-Struktur erlernt wurden. Zu den Pakettypen gehören Management Unicast, Static Unicast, Dynamic Unicast, Static Multicast und Dynamic Multicast. In der Tabelle können Sie die Adresse nach Pakettypen und Port sortieren.
Address Types	• **Management Unicast** bezeichnet die MAC-Adresse des Switches. Er gehört nur zum CPU-Port. • **Static Unicast**-MAC-Adressen können hinzugefügt und gelöscht werden. • **Dynamic Unicast MAC** ist eine MAC-Adresse, die von der Switch-Struktur erlernt wurde. • **Static Multicast** kann von der CLI hinzugefügt und über die Web-Benutzerschnittstelle und CLI gelöscht werden. • **Dynamic Multicast** wird angezeigt, nachdem Sie IGMP aktiviert haben und der Switch den IGMP-Bericht erlernt hat. • **Management-Multicast** ist eine Multicast-Adresse, die für Verwaltungszwecke konfiguriert ist, z. B. GVRP usw. Verwaltungseinträge sind schreibgeschützt. Dynamische und statische Einträge können entfernt werden.
Remove	Klicken Sie hier, um die statische Unicast-/Multicast-MAC-Adresse zu entfernen.
Reload	Klicken Sie hier, um die Tabelle neu zu laden. Die neu erlernte Unicast-/Multicast-MAC-Adresse wird in der *MAC-Adresstabelle* aktualisiert.

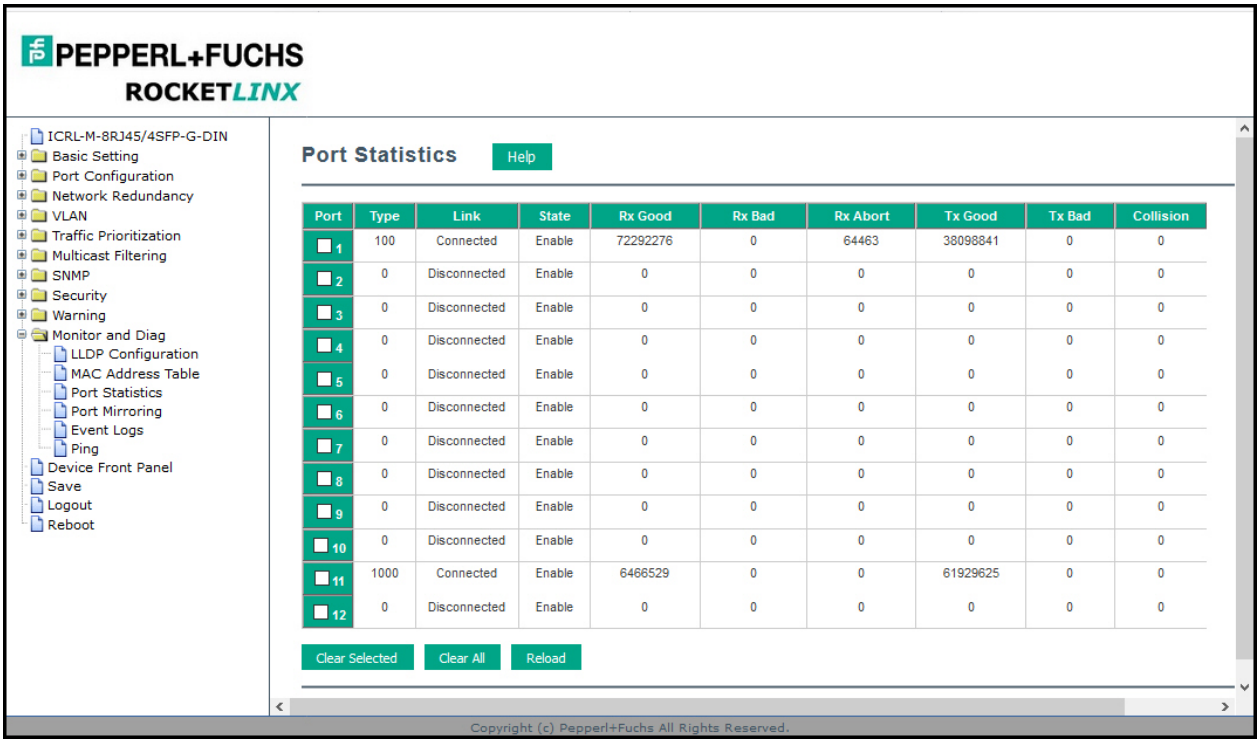
Seite „MAC Address Table“ (Fortsetzung)	
Apply	Klicken Sie auf **Apply**, um die Einstellungen anzuwenden. ***Anmerkung:*** *Sie müssen die Einstellungen mit **Save** speichern (Seite 159), wenn Sie diese Einstellungen nach Ausschalten des ICRL-M beibehalten möchten.*

4.12.3. Port Statistics

Auf dieser Seite können Sie die Betriebsstatistiken für jeden Port anzeigen. Zu den Statistiken, die angezeigt werden können, gehören **Link Type**, **Link State**, **Rx Good**, **Rx Bad**, **Rx Abort**, **Tx Good**, **Tx Bad** und **Collisions**.

Anmerkung: *Wenn Sie eine Zunahme von **Bad**, **Abort** oder **Collision** sehen, kann dies bedeuten, dass das Netzwerkkabel nicht richtig angeschlossen ist oder die Netzwerkleistung des Ports schlecht ist. Überprüfen Sie das Netzwerkkabel, die Netzwerkkarte des angeschlossenen Geräts und die Netzwerkanwendung oder weisen Sie den Netzwerkverkehr neu zu.*

Die folgenden Informationen bieten eine Übersicht der aktuellen Port-Statistikinformationen.

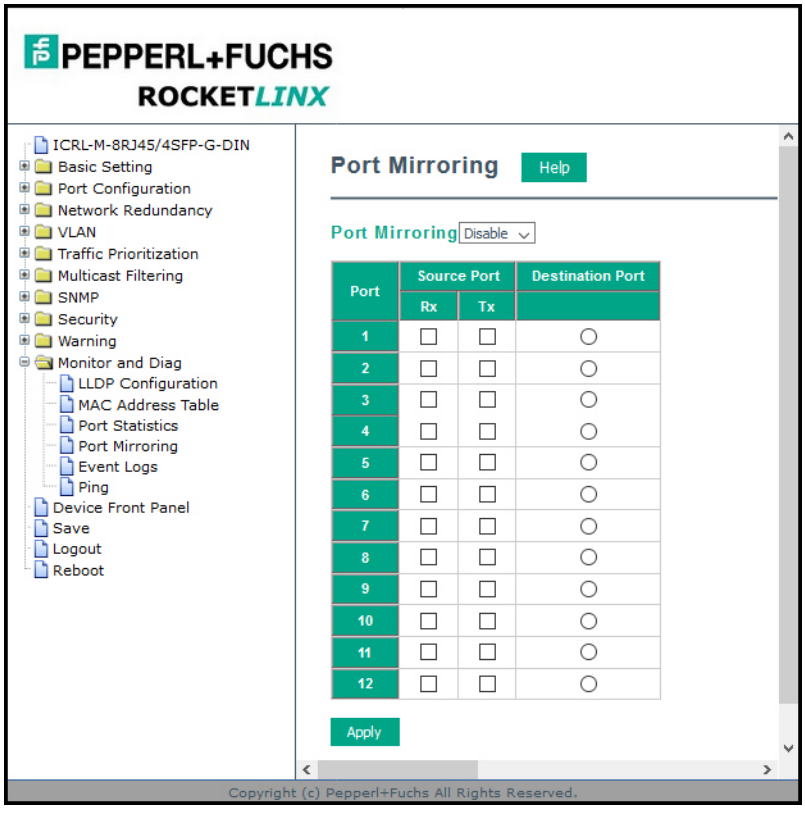


Seite „Port Statistics“	
Type	Zeigt den Porttyp an.
Link	Zeigt den Verbindungsstatus an: **Up** oder **Down**.
State	Zeigt den Verbindungsstatus an: **Enable** oder **Disable**.
Rx Good	Die Anzahl der empfangenen guten Frames, also die Gesamtzahl der empfangenen Unicast-, Broadcast-, Multicast- und Pause-Frames.

Seite „Port Statistics“ (Fortsetzung)	
Rx Bad	Die Anzahl der empfangenen fehlerhaften Frames, also die Gesamtanzahl der unter-/überdimensionierten Frames bzw. der Fragment-, Jabber- und Empfangsfehler (**RxErr**) sowie Frame-Prüfsequenzfehler (**FCSErr**).
Rx Abort	Die Anzahl der empfangenen abgebrochenen Frames, also die Gesamtzahl der verworfenen und gefilterten Frames.
Tx Good	Die Anzahl der gesendeten guten Frames, also die Gesamtzahl der gesendeten Unicast-, Broadcast-, Multicast- und Pause-Frames.
Tx Bad	Die Anzahl der gesendeten **FCSErr**-Frames.
Collision	Die Anzahl der Kollisionsframes, einschließlich einzelner, mehrerer, übermäßiger und verspäteter Kollisionen.
Clear Selected	Klicken Sie hier, um die Zahlen der ausgewählten Ports zu löschen.
Clear All	Klicken Sie hier, um alle Zahlen zu löschen.
Reload	Klicken Sie hier, um alle Zahlen neu zu laden.

4.12.4. Port Mirroring

Die Portspiegelung (auch *Port Spanning* genannt) ist ein Tool, mit dem Sie den Datenverkehr von einem oder mehreren Ports auf einen anderen Port spiegeln können, ohne den Datenverkehrsfluss auf dem ursprünglichen Port zu unterbrechen. Jeder Datenverkehr, der in die oder aus den **Quellports** übertragen wird, wird an den **Zielports** dupliziert. Dieser Datenverkehr kann dann am Zielport mithilfe eines Überwachungsgeräts oder einer Überwachungsanwendung analysiert werden. Der Netzwerkadministrator verwendet dieses Tool in der Regel für Diagnose, Debugging oder Angriffsabwehr.

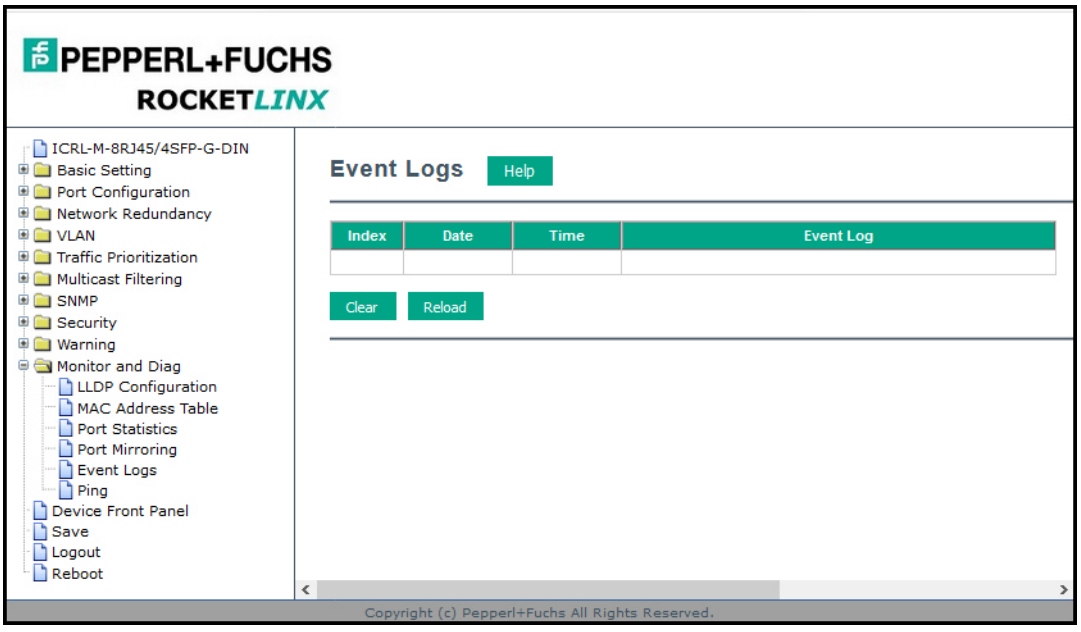


5/21/20

Seite „Port Mirroring Mode“	
Port Mirror Mode	Wählen Sie **Enable** oder **Disable**, um die Portspiegelung zu aktivieren/deaktivieren.
Source Port	Dieser wird auch als *Überwachungsport* bezeichnet. Dies sind die Ports, die Sie überwachen möchten. Der Datenverkehr aller Quell-/Überwachungsports wird zu Ziel-/Analyseports kopiert. Sie können einen einzelnen Port oder eine beliebige Kombination von Ports auswählen, aber Sie können sie nur in RX oder TX überwachen. Klicken Sie auf das Kontrollkästchen **Port ID**, **Rx, Tx** oder beides, um die Quellports auszuwählen.
Destination Port	Dieser wird auch als *Analyseport* bezeichnet. Sie können den Datenverkehr aller überwachten Ports an diesem Port analysieren, ohne den Datenverkehr an den überwachten Ports zu beeinträchtigen. Es kann nur eine RX/TX des Zielports ausgewählt werden. Der Netzwerkadministrator verbindet in der Regel einen LAN-Analysator oder ein Netxray-Gerät mit diesem Port.
Apply	Klicken Sie auf **Apply**, um die Einstellungen anzuwenden. ***Anmerkung:*** *Sie müssen die Einstellungen mit **Save** speichern (Seite 159), wenn Sie diese Einstellungen nach Ausschalten des ICRL-M beibehalten möchten.*

4.12.5. Event Logs

Die Systemprotokollfunktion wird in *SysLog Configuration* auf Seite 147 vorgestellt. Wenn der Modus **System Log Local** ausgewählt ist, zeichnet der ICRL-M die Ereignisse auf, die in der lokalen Protokolltabelle aufgetreten sind. Auf dieser Seite wird die Protokolltabelle angezeigt. Der Eintrag enthält den Index, das Auftrittsdatum und die -uhrzeit sowie den Inhalt der Ereignisse.

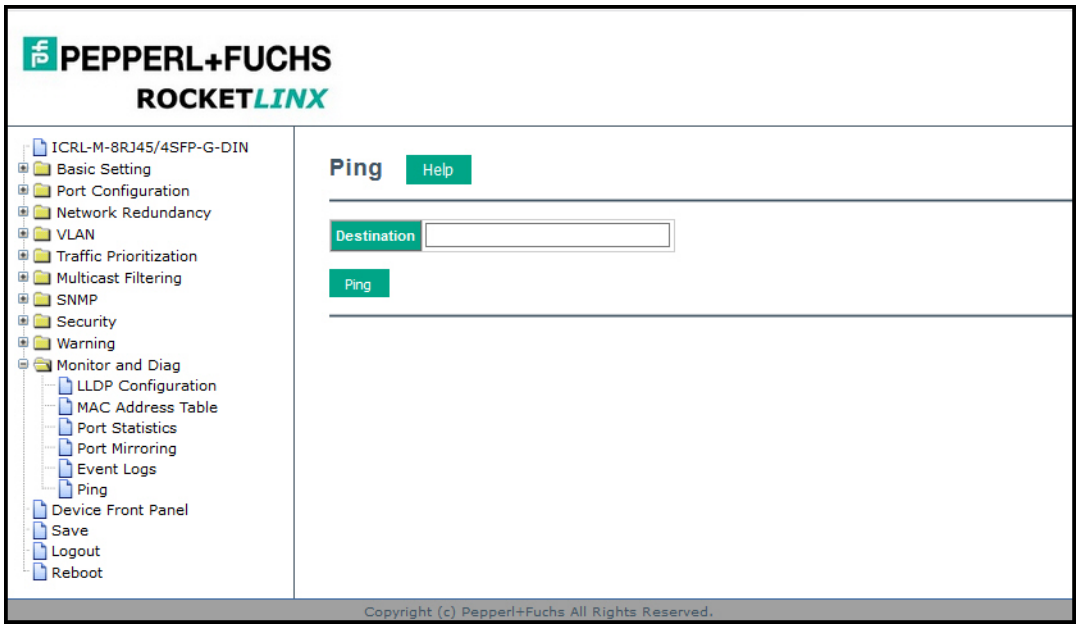


Klicken Sie auf **Clear**, um die Einträge zu löschen. Klicken Sie auf **Reload**, um die Tabelle neu zu laden.

4.12.6. Ping

Auf dieser Seite finden Sie das Tool **Ping Utility**, mit dem Sie ein Ping-Signal an ein Remote-Gerät senden und überprüfen können, ob das Gerät aktiv ist oder nicht.

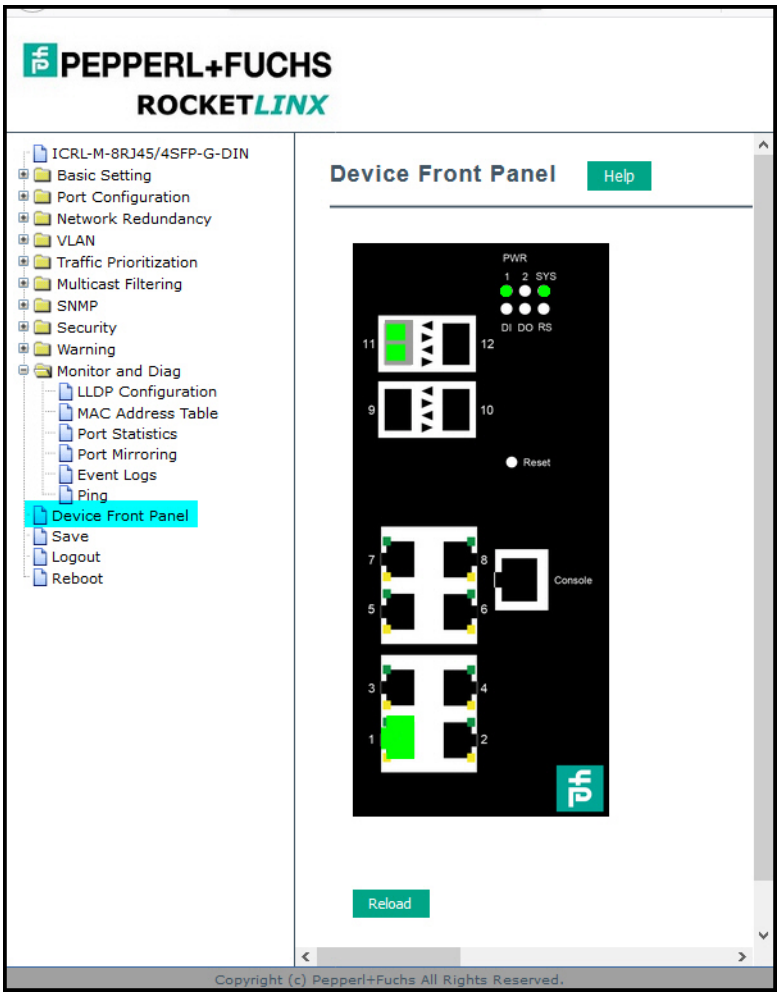
Geben Sie die **Target IP**-Adresse des Zielgeräts ein und klicken Sie auf **Start**, um den Ping zu starten.



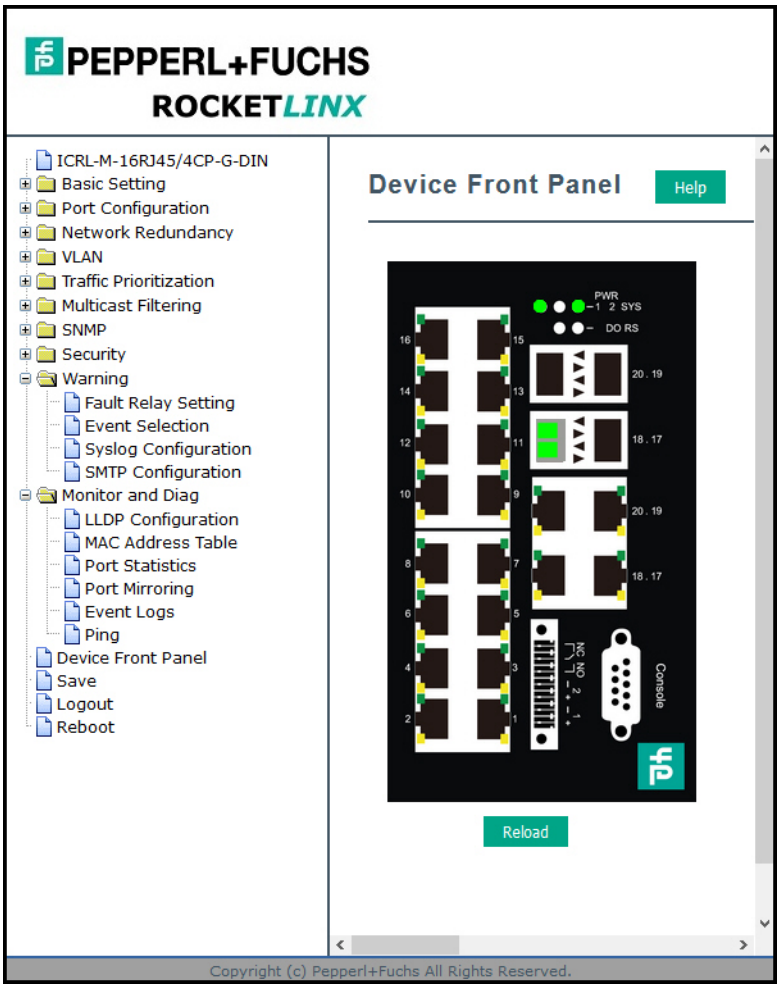
Nach einigen Sekunden wird das Ergebnis im Feld **Result** angezeigt.

4.13. Device Front Panel

Unter **Device Front Panel** können Sie den LED-Status des ICRL-M einsehen.



Anmerkung: *Für diese Funktion ist kein CLI-Befehl vorhanden. Wenn Sie die physischen LED sehen können, finden Sie unter Beschreibung der LED auf Seite 17 detaillierte LED-Informationen. Wenn Sie den ICRL-M in einem Rack lokalisieren müssen, können Sie die LED-Tracker-Funktion in PortVision DX verwenden.*

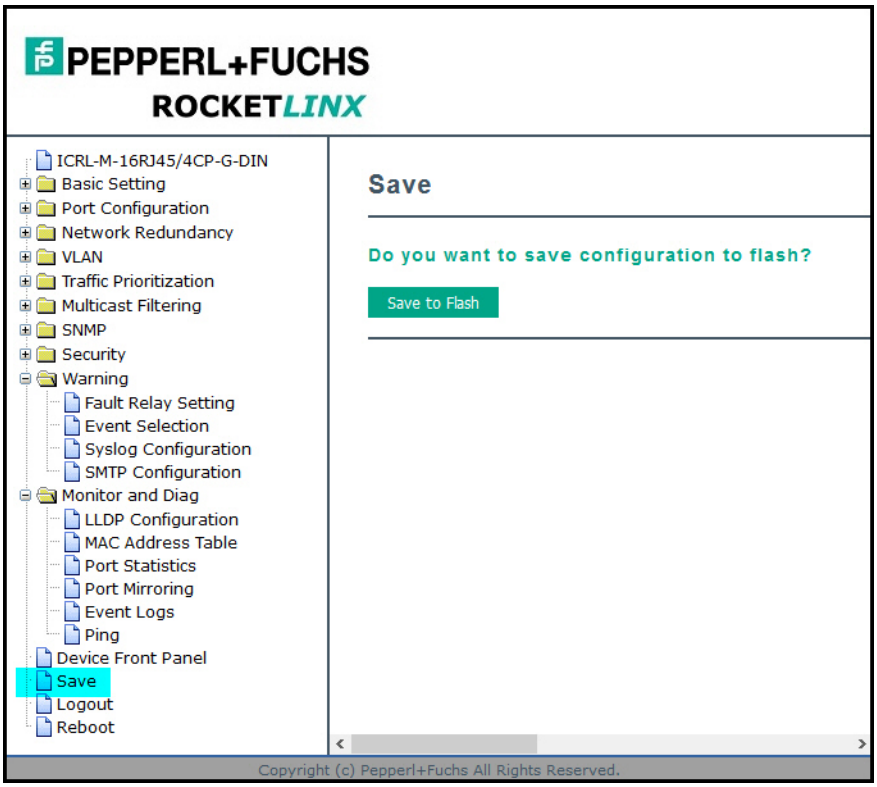

PEPPERL+FUCHS
ROCKETLINX
ICRL-M-16RJ45/4CP-G-DIN
Basic Setting
Port Configuration
Network Redundancy
VLAN
Traffic Prioritization
Multicast Filtering
SNMP
Security
Warning
Fault Relay Setting
Event Selection
Syslog Configuration
SMTP Configuration
Monitor and Diag
LLDP Configuration
MAC Address Table
Port Statistics
Port Mirroring
Event Logs
Ping
Device Front Panel
Save
Logout
Reboot
Device Front Panel
Help
PWR
1 2 SYS
DO RS
20. 19
18. 17
20. 19
18. 17
Console
Reload
Copyright (c) Pepperl+Fuchs All Rights Reserved.

4.14. Speichern (im Flash)

Auf der Seite **Save** werden alle Änderungen an der Konfiguration im Flash gespeichert.

Änderungen, die an der Konfiguration eines Switches vorgenommen werden, werden zunächst im flüchtigen Speicher gespeichert, wodurch sie verloren gehen, wenn der Switch die Stromversorgung verliert oder neu gestartet wird. Beim Speichern der Einstellungen im Flash werden sie in einem nicht flüchtigen Speicher gespeichert, wodurch sie beibehalten werden, wenn der Switch die Stromversorgung verliert oder neu gestartet wird.

Klicken Sie nach Auswahl von **Save Configuration** auf **Save to Flash**, um die neue Konfiguration zu speichern.

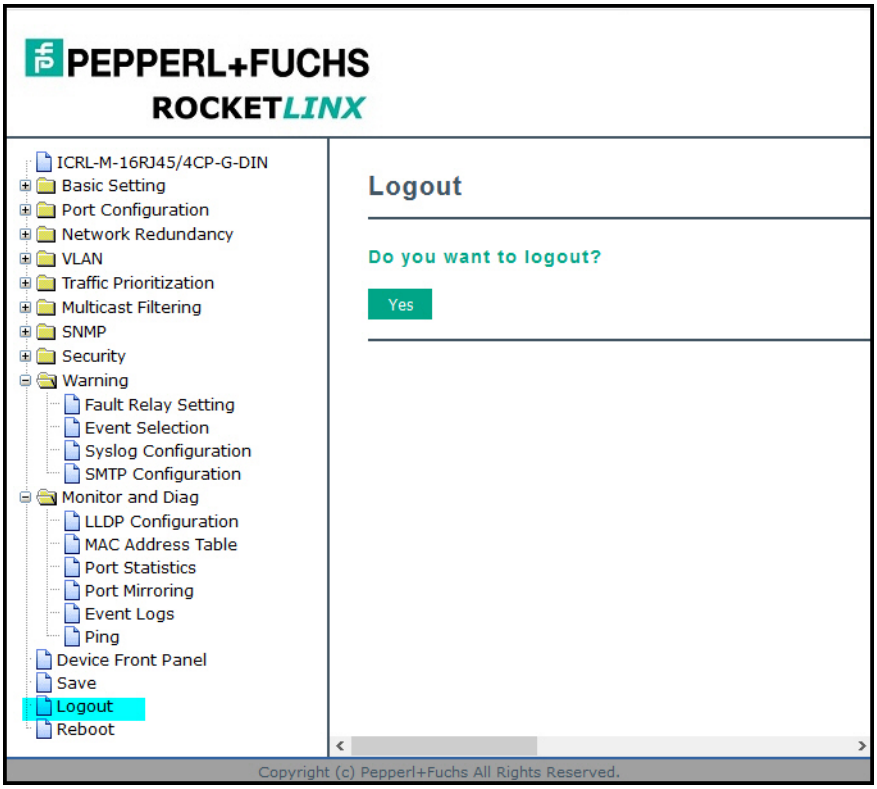


Optional können Sie die CLI verwenden (siehe *Speichern im Flash (CLI)* auf Seite 223).

4.15. Abmelden

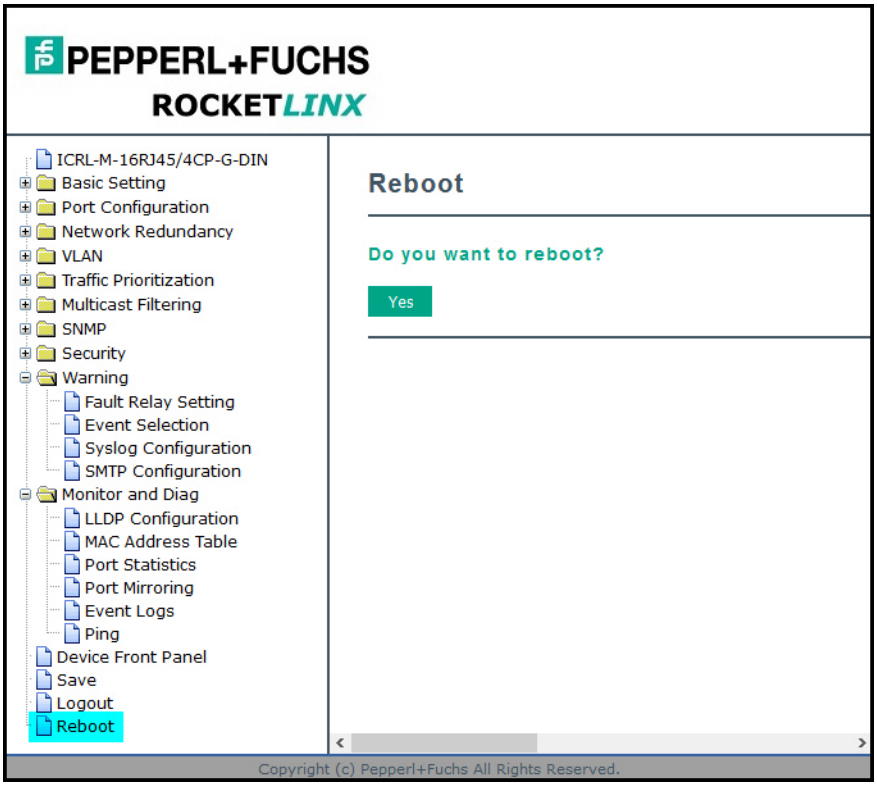
Klicken Sie in der Web-Benutzerschnittstelle auf die Option **Logout**, um die Webverbindung manuell abzumelden.

Klicken Sie auf **Yes**, um sich abzumelden.



4.16. Reboot

Verwenden Sie diese Seite, um den ICRL-M neu zu starten. Stellen Sie sicher, dass Sie Ihre Änderungen gespeichert haben, da sie sonst verloren gehen.



5. Konfiguration – Befehlszeilenschnittstelle (CLI)

5.1. Übersicht

Der ICRL-M bietet In-Band- und Out-Band-Konfigurationsmethoden:

- Die In-Band-Verwaltung bedeutet, dass Sie den ICRL-M mithilfe des RS-232-Konsolenkabels und der Befehlszeilenschnittstelle (Command-Line Interface, CLI) für den Zugriff auf den ICRL-M konfigurieren, ohne einen Admin-PC an das Netzwerk anzuschließen. Sie können die Out-Band-Verwaltung verwenden, wenn die Netzwerkverbindung zum ICRL-M unterbrochen wird.
- In-Band-Verwaltung bedeutet, dass Sie mittels der ICRL-M-IP-Adresse eine Remote-Verbindung über das Netzwerk herstellen. Sie können eine Remote-Verbindung mit der im ICRL-M integrierten Web-Benutzerschnittstelle oder einer Telnet-Konsole und der CLI herstellen.

Wenn Sie die In-Band-Verwaltung verwenden möchten, müssen Sie die ICRL-M-IP-Adresse entsprechend Ihren Netzwerkanforderungen programmieren. Die einfachste Möglichkeit, die IP-Adresse zu konfigurieren, ist die Verwendung eines Windows-Systems sowie PortVision DX (siehe *Konfigurieren der Netzwerkeinstellungen* auf Seite 23).

Wenn Sie die Web-Benutzerschnittstelle für die Konfiguration verwenden möchten, finden Sie entsprechende Informationen unter *Konfiguration – Web-Benutzerschnittstelle* auf Seite 33.

Gehen Sie wie folgt vor, um über die CLI auf den ICRL-M zuzugreifen:

- *Verwenden der seriellen Konsole*
- *Verwenden einer Telnet-/SSH-Konsole*

Dieser Abschnitt enthält Informationen zu den folgenden Befehlsgruppen:

5.1.1. Verwenden der seriellen Konsole

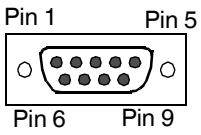
Pepperl+Fuchs bietet ein RS-232-RJ45- (ICRL-M-8RJ45/4SFP-G-DIN) und ein RS-232-DB9-Konsolenkabel (ICRL-M-16RJ45/4CP-G-DIN).

Anmerkung: *Für die Verwendung einer seriellen Konsolenverbindung ist ein System-COM-Port erforderlich. Wenn kein COM-Port verfügbar ist, gehen Sie wie unter Verwenden einer Telnet-/SSH-Konsole auf Seite 166 beschrieben vor.*

1. Schließen Sie den RS-232-Steckverbinder (RJ45- oder DB9-Buchse) an den COM-Port Ihres PCs an und verbinden Sie das andere Ende mit dem **Konsolenport** des ICRL-M. Wenn das Kabel nicht mehr vorhanden ist, können Sie die entsprechende Pin-Belegung des Konsolenkabels verwenden oder ein Nullmodemkabel erwerben. Wenn Sie ein Ersatzkabel erstellen, müssen Sie mindestens Tx-, Rx- und Erdungssignale anschließen.

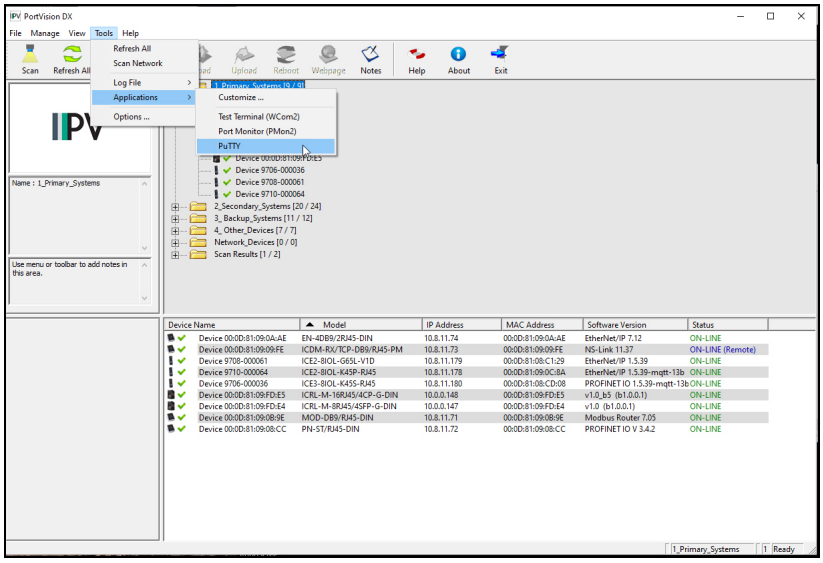
RJ45-Pin	RJ45-Signal
5	DTR
7	Tx
6	Rx
3	DSR
4	GND
1	CTS
8	RTS
2	CD

DB9F-Pin	DB9-Signal
1	CD
2	Rx
3	Tx
4	DTR
5	GND
6	Nicht belegt
7	RTS
8	CTS
9	RI

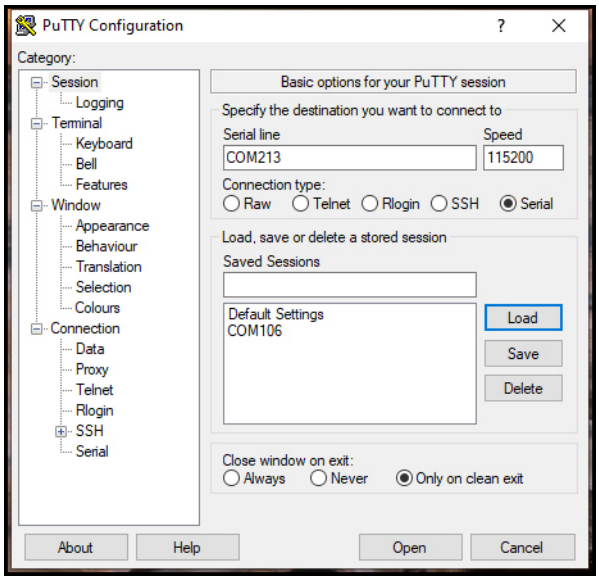
Serielles Ende


2. Starten Sie ein Terminalprogramm wie HyperTerminal oder verwenden Sie PuTTY, das in PortVision DX enthalten ist. Das folgende Beispiel veranschaulicht die Verwendung von PuTTY.

3. Öffnen Sie PortVision DX und klicken Sie auf **Tools** I **Applications** I **PuTTY**.



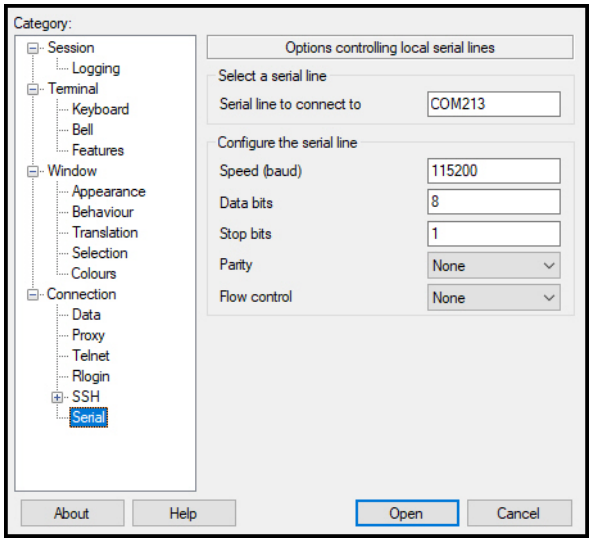
4. Klicken Sie beim **Connection Type** auf **Serial**.
5. Geben Sie unter **Host Name** den Hostnamen ein, der den COM-Port darstellt.



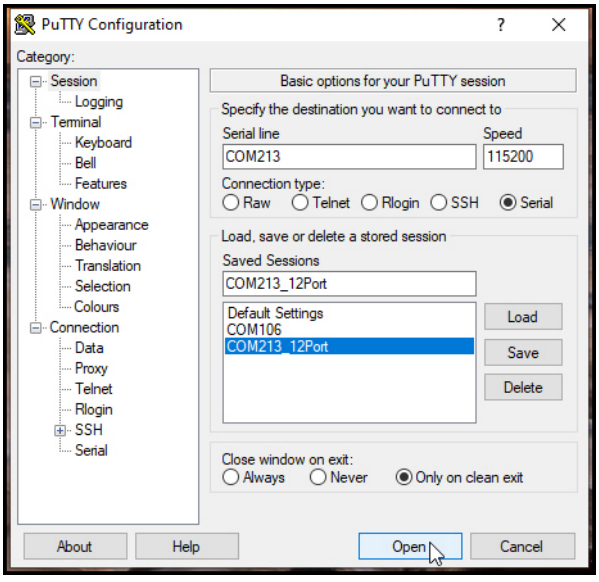
6. Klicken Sie auf der linken Seite unter **Category** auf **Serial**.

7. Konfigurieren Sie die serielle Verbindung mit den folgenden Eigenschaften.

Serielle Einstellungen	Value
Baud Rate	115200
Data bits	8
Stop Bit	1
Parity	None
Flow Control	None



8. Klicken Sie unter **Category** im Menü auf **Sessions**.
9. Geben Sie einen geeigneten **Saved Session**-Namen ein und klicken Sie auf **Save**.



10. Klicken Sie auf **Open**.
11. Drücken Sie **Enter**.

12. Melden Sie sich beim Switch an. Der Standardbenutzername lautet **admin**, und das Kennwort **admin**.
    a. Geben Sie den Anmeldenamen ein und drücken Sie **Enter**.
    b. Geben Sie das Kennwort ein und drücken Sie **Enter**.

```
Switch-Anmeldename: admin
Password:


ICRL-M-8RJ45/4SFP-G-DIN (Version 1.0-20200131-16:50:50).
Copyright Pepperl+Fuchs
```

Anmerkung: *Die folgenden Beispiele veranschaulichen den ICRL-M-8RJ45/4SFP-G-DIN. Beachten Sie jedoch, dass der ICRL-M-16RJ45/4CP-G-DIN ähnlich ist.*

13. Konfigurieren Sie bei Bedarf die IP-Adresse für Ihr Netzwerk. Das folgende Beispiel zeigt, wie die IP-Adresse 192.168.11.252 mit einer Subnetzmaske der Klasse B (255.255.0.0) programmiert wird.

```
Switch> enable
Switch# configure terminal
Switch(config)# int vlan1
Switch(config-if)# ip address 192.168.11.252/16
```

Weitere Informationen zur Verwendung der CLI finden Sie unter *Einführung zur Befehlszeilenschnittstelle* auf Seite 169.

5.1.2. Verwenden einer Telnet-/SSH-Konsole

Der ICRL-M unterstützt eine Telnet- oder SSH-Konsole mit der Befehlszeilenschnittstelle (CLI), die mit der Verwendung des RS-232-Konsolenports identisch ist. Die SSH-Verbindung kann alle Konfigurationsbefehle sichern, die Sie an den ICRL-M senden.

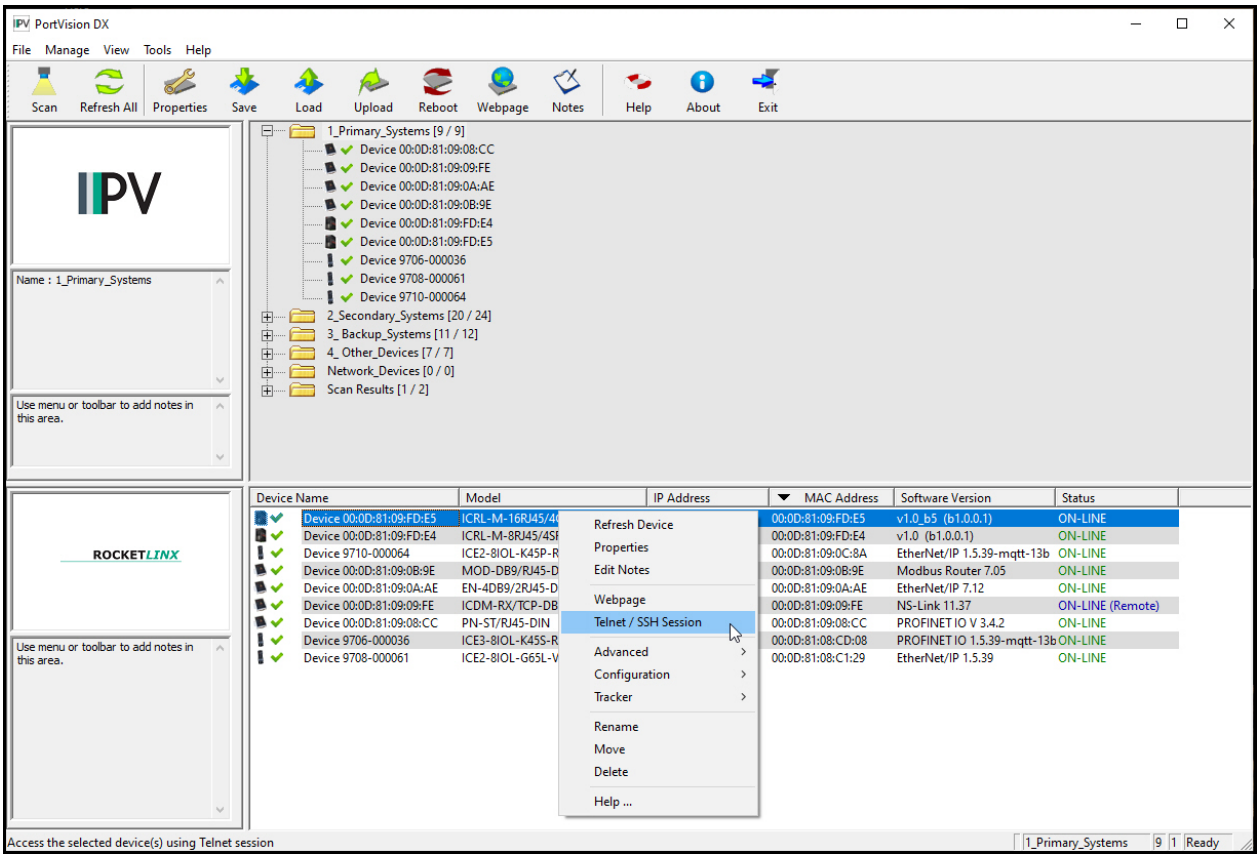
SSH ist eine Client-/Server-Architektur, in der der ICRL-M der SSH-Server ist. Wenn Sie eine SSH-Verbindung mit dem ICRL-M herstellen möchten, können Sie PortVision DX verwenden oder ein SSH-Client-Tool herunterladen.

Im nächsten Abschnitt werden Verfahren zur Verwendung von PortVision DX mit einer Telnet- oder SSH-Verbindung beschrieben.

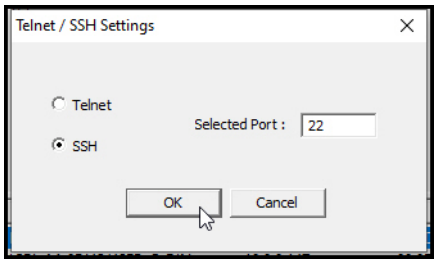
Sie können PortVision DX verwenden, um auf die CLI zuzugreifen, indem Sie das folgende Verfahren anwenden.

1. Gegebenenfalls müssen Sie PortVision DX installieren (*Installation von PortVision DX* auf Seite 20).
2. Starten Sie PortVision DX.

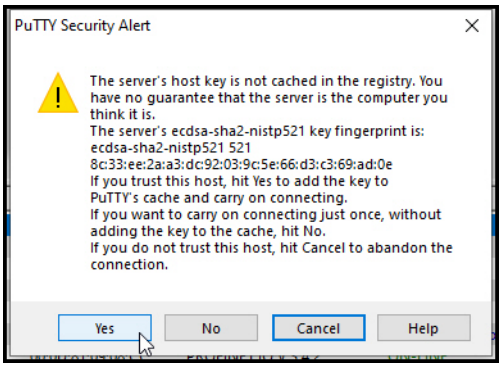
3. Klicken Sie mit der rechten Maustaste auf den ICRL-M im Teilfenster *Device List* (unten) und klicken Sie auf **Telnet/SSH**.



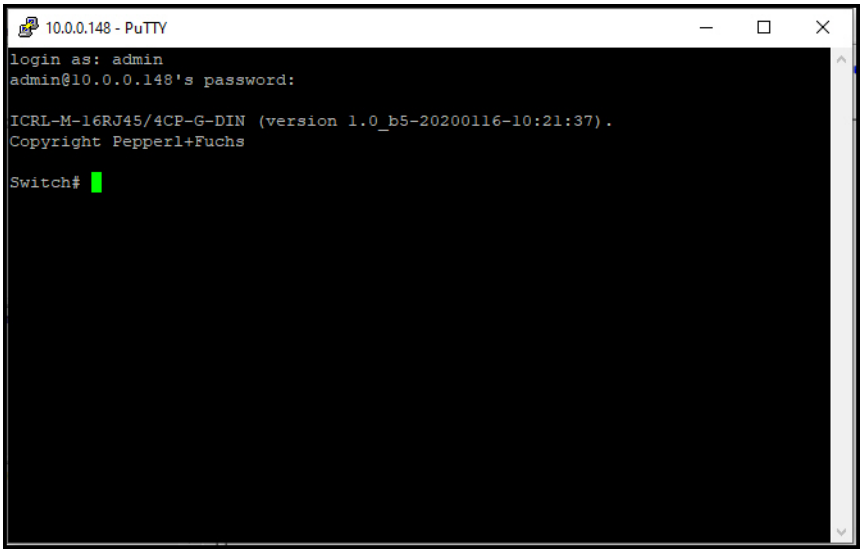
4. Wählen Sie entweder Telnet oder SSH aus und behalten Sie die Standardportnummer bei.



Wenn Sie **SSH** ausgewählt haben, klicken Sie auf **Yes**.



- Geben Sie den Benutzernamen ein (Standard: **admin**).
- Geben Sie das Kennwort ein (Standard: **admin**).



Wenn Sie **Telnet** ausgewählt haben:

- Geben Sie den Benutzernamen ein (Standard: **admin**).
- Geben Sie das Kennwort ein (Standard: **admin**).

Alle Befehle, die Sie in SSH sehen, sind identisch mit den CLI-Befehlen, die über die RS-232-Konsole angezeigt werden.

Weitere Informationen zur Verwendung der CLI finden Sie unter *Einführung zur Befehlszeilenschnittstelle* auf Seite 169.

5.2. Einführung zur Befehlszeilenschnittstelle

Die Befehlszeilenschnittstelle (Command-Line Interface, CLI) ist die Benutzerschnittstelle für die im ICRL-M integrierte Software. Sie können Systeminformationen und Status anzeigen, den Switch konfigurieren und eine Antwort vom System erhalten, indem Sie einen Befehl eingeben.

Es gibt verschiedene Befehlsmodi. Jeder Befehlsmodus verfügt über eigene Zugriffsfähigkeiten und verfügbare Befehlszeilen und verwendet verschiedene Befehlszeilen zur Eingabe und zum Verlassen. Diese Modi lauten:

- *User EXEC-Modus* auf Seite 173, der Ping- und Telnet-Befehle für Remote-Geräte sowie Befehle zur Anzeige einiger grundlegender Informationen und zum Zugriff auf den *Privileged EXEC*-Modus enthält
- *Privileged EXEC-Modus* auf Seite 174, über den Sie die aktuelle Konfiguration anzeigen, die Standardeinstellungen wiederherstellen, den Switch neu laden, Systeminformationen anzeigen, die Konfiguration speichern und auf den *Global Configuration*-Modus zugreifen können
- *Global Configuration-Modus* auf Seite 174, den Sie verwenden können, um alle ICRL-M-Funktionen zu konfigurieren und auf einen der *Interface Configuration*-Modi zuzugreifen
- *(Port) Interface Configuration* auf Seite 176, der zum Konfigurieren der Porteinstellungen verwendet werden kann
- *(VLAN) Interface Configuration* auf Seite 177, der zur Konfiguration der Einstellungen für ein bestimmtes VLAN verwendet werden kann

Weitere Informationen zum Zugriff auf die CLI finden Sie unter *Konfiguration – Befehlszeilenschnittstelle (CLI)* auf Seite 162.

5.3. Zugriff auf die Optionen für einen Befehl

Das folgende Beispiel zeigt, wie die Beschreibung und die Optionen für einen Befehl angezeigt werden. Dieses Beispiel veranschaulicht den Befehl **show** und die angezeigte Firmwareversion entspricht möglicherweise nicht Ihrer Version.

Anmerkung: *Das **?** wird nicht auf dem Bildschirm angezeigt.*

1. Wenn Sie **show?** eingeben (ohne Leerzeichen zwischen **show** und **?**; drücken Sie nicht **Enter**), stellt der ICRL-M eine grundlegende Beschreibung dieses Befehls bereit.

```
Switch-Anmeldename: admin
Password:

ICRL-M-8RJ45/4SFP-G-DIN (Version 1.0-20200131-16:50:50).
Copyright Pepperl+Fuchs

switch# show
  show  Show running system information
```

Anmerkung: *Die Firmwareversion entspricht möglicherweise nicht Ihrem RocketLinx-Modell.*

2. Wenn Sie **show ?** eingeben (mit Leerzeichen zwischen **show** und **?**; drücken Sie nicht **Enter**), stellt der ICRL-M Informationen zu den Optionen für diesen Befehl bereit.

```
switch# show
  acceptable          Get the information of acceptable frame type
  arp                 Address Resolution Protocol
  auth                Authentication
  cfm                 IEEE 802.1ag - Connectivity Fault Management
  clock               Display time-of-day clock
  debugging           Debugging functions (see also 'undebug')
  dot1q-tunnel        802.1Q tunnel characteristics
  dot1x               Get IEEE 802.1x information
  erps                Ethernet Ring Protection Switching (ITU-T G.8032)
  ethernet-ip         Show Ethernet/IP information
  event-log           Event log
  garp                General Attribute Registration Protocol
  gmrp                GMRP
  gvrp                GARP VLAN Registration Protocol information
  hardware            Hardware information
  ingress             Get the information of ingress filtering
  interface           Interface status and configuration
  ip                  IP interface commands
  ipv6                IPv6
  l2_interface        Interface status and configuration
  lacp                Link Aggregation Control Protocol
  lldp                Show LLDP information
  mac                 MAC interface commands
  mac-address-table   MAC address table
  memory              Memory statistics
  mirror              Port mirroring
  modbus              Modbus TCP Slave
  nameserver          DNS Server
  ntp                 Network time protocol
  port-security       Port Security
  process             Process
  ptp                 IEEE1588 Precision Time Protocol
  qos                 Quality of Service (QoS)
  rate-limit          Rate limit configuration
  redundant-ring      The Redundant Ring protocol
  relay               relay output type information
  rmon                Remote monitoring
  running-config      Current operating configuration
  service             System service
  sfp                 Small form factor pluggable information
  smtp-server         SMTP server configuration
  snmp-server         The SNMP server
  spanning-tree       The spanning-tree protocol
  startup-config      Contentes of startup configuration
  storm-control       Enables packets flooding rate limiting features
  tftp                Show tftp status
  trunk               Trunk group information
  users               Users information
  version             Displays ISS version
  vlan                vlan
  warning-event       Warning event
```

3. Geben Sie **show IP ?** ein (mit Leerzeichen zwischen **show** und **?**; drücken Sie nicht **Enter**), um die Optionen für **ip** anzuzeigen.

```
switch# show ip
  access-group      IP access-group configuration commands
  access-list       List IP access lists
  arp               Address Resolution Protocol
  dhcp              DHCP Protocol
  forwarding        IP forwarding status
  igmp              IGMP information
  route             IP routing table
  verify            Verify
```

4. Geben Sie **show ip route** ein und drücken Sie **Enter**, um die IP-Routingtabellen für den ICRL-M anzuzeigen.

```
Switch> show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       IA - OSPF inter area, E1 - OSPF external type 1,
       E2 - OSPF external type 2,
       B - BGP, > - selected route, * - FIB route

S   0.0.0.0/0 [1/10] via 192.168.250.1 inactive
C>* 10.0.0.0/16 is directly connected, vlan1
```

5. Wenn Sie **list** eingeben und **Enter** drücken, zeigt der ICRL-M die Informationen zu allen Befehlen und Optionen für einen Modus an. Das folgende Beispiel zeigt die verfügbaren Befehle und ihre Optionen für den *User EXEC*-Modus.

```
switch# disable
switch> list
  enable
  exit
  list
  ping A.B.C.D
  ping WORD
  ping X:X::X:X
  quit
  show gvrp statistics [IFNAME]
  show ip forwarding
  show ip route
  show ip route A.B.C.D
  show ip route A.B.C.D/M
  show ip route supernets-only
  show memory
  show users
  show version
  telnet WORD
  telnet WORD PORT
  traceroute WORD
switch>
```

5.3.1. *User EXEC*-Modus

Wenn Sie sich mit der CLI beim ICRL-M anmelden, befinden Sie sich im *Privileged EXEC*-Modus. Um auf den *User EXEC*-Modus zuzugreifen, müssen Sie „disable“ eingeben.

Im *User EXEC*-Modus können Sie ein Ping-/Telnet-Signal an ein Remote-Gerät senden und einige grundlegende Informationen anzeigen.

Geben Sie den folgenden Befehl ein und drücken Sie **Enter**:

- **enable**, um auf den *Privileged EXEC*-Modus zuzugreifen (*Privileged EXEC-Modus* auf Seite 174)
- **exit**, um sich abzumelden
- **?**, um die Befehlsliste anzuzeigen
- **list**, um die Befehle im *User EXEC*-Modus und ihre Optionen anzuzeigen

```
switch# disable
switch>
  enable      Privileged-Modus aktivieren
  exit        Aktuellen Modus beenden und zum vorherigen Modus   zurückkehren
  list        Befehlsliste anzeigen
  ping        Echo-Meldungen senden
  quit        Aktuellen Modus beenden und zum vorherigen Modus zurückkehren
  show        Informationen zum laufenden System anzeigen
  telnet      Telnet-Verbindung öffnen
  traceroute  Route zum Ziel nachverfolgen
```

Eine vollständige Liste der Befehle und ihrer Optionen finden Sie unter *User EXEC-Modus* auf Seite 224.

5.3.2. *Privileged EXEC*-Modus

In diesem Modus (Standardmodus bei der Anmeldung) können Sie auf dem ICRL-M die aktuelle Konfiguration anzeigen, die Standardeinstellungen wiederherstellen, den Switch neu laden, Systeminformationen anzeigen, die Konfiguration speichern und zum *Global Configuration*-Modus wechseln.

Geben Sie die folgenden Befehle ein und drücken Sie **Enter**.

- **configure terminal**, um auf den *Global Configuration*-Modus zuzugreifen (*Global Configuration-Modus* auf Seite 174).
- **exit**, um die CLI zu schließen
- **?**, um die Befehlsliste anzuzeigen
- **list**, um die Befehle im *Privileged EXEC*-Modus und ihre Optionen anzuzeigen

Eine vollständige Liste der Befehle und ihrer Optionen finden Sie unter *Privileged EXEC-Modus* auf Seite 225.

```
switch#
  archive      Archivdateien verwalten
  clear        Funktionen zurücksetzen
  clock        Uhrzeit konfigurieren
  configure    Konfiguration über VTY-Schnittstelle
  copy         Von einer Datei zu einer anderen kopieren
  debug        Debugging-Funktionen (siehe auch „undebug“)
  disable      Privileged-Modus deaktivieren
  dot1x        IEEE-802.1x-Standard-Zugriffskontrolle
  end          Aktuellen Modus beenden und zum Aktivierungsmodus wechseln
  exit         Aktuellen Modus beenden und zum vorherigen Modus zurückkehren
  list         Befehlsliste anzeigen
  mac          MAC-Schnittstellenbefehle
  no           Befehl negieren oder Standard wiederherstellen
  pager        Terminal-Pager
  ping         Echo-Meldungen senden
  quit         Aktuellen Modus beenden und zum vorherigen Modus zurückkehren
  read         Aus Flash lesen
  reboot       System neu starten
  reload       Standard-Konfigurationsdatei kopieren, um die aktuelle zu ersetzen
  show         Informationen zum laufenden System anzeigen
  telnet       Telnet-Verbindung öffnen
  traceroute   Route zum Ziel nachverfolgen
  write        Aktive Konfiguration in Speicher, Netzwerk oder Terminal schreiben
```

5.3.3. *Global Configuration*-Modus

Wenn Sie **configure terminal** im *Privileged EXEC*-Modus eingeben, können Sie daraufhin auf den *Global Configuration*-Modus zugreifen. Im *Global Configuration*-Modus können Sie alle ICRL-M-Funktionen konfigurieren. Geben Sie die folgenden Befehle ein und drücken Sie **Enter**.

- **interface IFNAME/VLAN**, um auf den entsprechenden *Interface Configuration*-Modus zuzugreifen.
- **exit**, um zum *Privileged EXEC*-Modus zurückzukehren.
- **?**, um die Befehlsliste anzuzeigen
- **list**, um die Befehle im *Global Configuration*-Modus und ihre Optionen anzuzeigen

Im Folgenden finden Sie eine Liste der verfügbaren Befehle für den *Global Configuration*-Modus. Eine vollständige Liste der Befehle und ihrer Optionen finden Sie unter *Global Configuration-Modus* auf Seite 232.

```
switch# config term
switch(config)#
```

access-list	Listeneintrag hinzufügen
arp	ARP
auth	Authentifizierung
cfm	IEEE 802.1ag – Connectivity-Fehlermanagement
clock	Uhrzeit konfigurieren
default	Befehl auf Standard zurücksetzen
dot1x	IEEE-802.1x-Standard-Zugriffskontrolle
end	Aktuellen Modus beenden und zum Aktivierungsmodus wechseln
erps	Ethernet-Ring-Schutzschalter (ITU-T G.8032)
ethernet-ip	Ethernet-/IP-Protokoll
exit	Aktuellen Modus beenden und zum vorherigen Modus zurückkehren
gmrp	GARP Multicast Registration Protocol
gvrp	GARP VLAN Registration Protocol
hostname	Netzwerkname des Systems festlegen
interface	Schnittstelle zur Konfiguration auswählen
ip	Globale Unterbefehle zur IP-Konfiguration
ipv6	IP-Informationen
lacp	Link Aggregation Control Protocol
list	Befehlsliste anzeigen
lldp	Link Layer Discovery Protocol
log	Protokollierungssteuerung
mac	Globale Unterbefehle zur MAC-Konfiguration
mac-address-table	MAC-Adresstabelle
mirror	Portspiegelung
modbus	Modbus-TCP-Slave
nameserver	DNS-Server
no	Befehl negieren oder Standard wiederherstellen
ntp	NTP konfigurieren
ptp	IEEE1588 PTPv2
qos	Quality of Service (QoS)
redundant-ring	Ringredundanz konfigurieren
relay	Informationen zum Relay-Ausgangstyp
router	Routingprozess aktivieren
service	Systemservice
sfp	Small Form-Factor Pluggable
smtp-server	SMTP-Serverkonfiguration
snmp-server	SNMP-Server
spanning-tree	Spanning-Tree-Algorithmus
tftp	TFTP (de-)aktivieren
trunk	Trunk-Gruppen-Konfiguration
username	Neue Benutzerkonten, Kennwörter oder Berechtigungen hinzufügen oder bestehende einrichten
vlan	Virtual LAN
warning-event	Warnereignis-Auswahl
write-config	Konfigurationsdateien für Schreibvorgang angeben

5.3.4. (Port) Interface Configuration

Wenn Sie **interface IFNAME** im *Global Configuration*-Modus eingeben, können Sie auf den *Interface Configuration*-Modus zugreifen. In diesem Modus können Sie Porteinstellungen konfigurieren.

Geben Sie den Schnittstellennamen ein, z. B. „gi1“, wenn Sie einen bestimmten *Interface Configuration*-Modus aufrufen möchten. Geben Sie die folgenden Befehle ein und drücken Sie **Enter**.

- **exit**, um zum *Privileged EXEC*-Modus zurückzukehren.
- **?**, um die Befehlsliste anzuzeigen
- **list**, um die Befehle im *Interface Configuration*-Modus und ihre Optionen anzuzeigen Die folgende Liste enthält die verfügbaren Befehle für den *Port Interface Configuration*-Modus.

Eine vollständige Liste der Befehle und ihrer Optionen finden Sie unter ***Port Interface Configuration-Modus*** auf Seite 240.

```
switch(config)# interface gi1
switch(config-if)#
 acceptable          Konfiguriert die 802.1Q-zulässigen Frametypen eines Ports
 description         Schnittstellenspezifische Beschreibung
 dot1x               IEEE-802.1x-Standard-Zugriffskontrolle
 duplex              Gibt die Duplex-Betriebsart für einen Port an
 end                 Aktuellen Modus beenden und zum Aktivierungsmodus wechseln
 ethertype           EtherType
 exit                Aktuellen Modus beenden und zum vorherigen Modus zurückkehren
 flowcontrol         Legt den Flusssteuerungswert für eine Schnittstelle fest
 garp                General Attribute Registration Protocol
 ingress             802.1Q-Ingress-Filterfunktionen
 ip                  Konfigurationsbefehle für das Internet Protocol der Schnittstelle
 lacp                Link Aggregation Control Protocol
 list                Befehlsliste anzeigen
 loopback            Gibt die Loopback-Betriebsart für einen Port an
 mac                 MAC-Schnittstellenbefehle
 media-type          Medientyp angeben
 mtu                 Gibt die MTU an einem Port an
 no                  Befehl negieren oder Standard wiederherstellen
 qos                 Quality of Service (QoS)
 quit                Aktuellen Modus beenden und zum vorherigen Modus zurückkehren
 rate-limit          Konfiguration der Ratenbeschränkung
 sfp                 Small Form-Factor Pluggable
 shutdown            Ausgewählte Schnittstelle abschalten
 spanning-tree       Spanning Tree Protocol
 speed               Gibt die Geschwindigkeit eines Fast Ethernet- oder Gigabit
                     Ethernet-Ports an
 storm-control       Aktiviert Funktionen zur Beschränkung der Paket-Flooding-Rate
 switchport          Verhalten des Switching-Modus festlegen
```

5.3.5. (VLAN) Interface Configuration

Wenn Sie **interface VLAN VLAN-ID** im *Global Configuration*-Modus eingeben, können Sie auf den *VLAN Interface Configuration*-Modus zugreifen. In diesem Modus können Sie die Einstellungen für das spezifische VLAN konfigurieren.

Der VLAN-Schnittstellenname von VLAN 1 lautet „VLAN 1“, der von VLAN 2 „VLAN 2“.

Geben Sie **exit** ein, um zum vorherigen Modus zurückzukehren. Geben Sie **?** ein, um die verfügbare Befehlsliste anzuzeigen.

```
switch# config term
switch(config)# interface vlan 1
switch(config-if)#
```

description	Schnittstellenspezifische Beschreibung
end	Aktuellen Modus beenden und zum Aktivierungsmodus wechseln
exit	Aktuellen Modus beenden und zum vorherigen Modus zurückkehren
ip	Konfigurationsbefehle für das Internet Protocol der Schnittstelle
ipv6	Konfigurationsbefehle für das Internet Protocol der Schnittstelle
list	Befehlsliste anzeigen
no	Befehl negieren oder Standard wiederherstellen
quit	Aktuellen Modus beenden und zum vorherigen Modus zurückkehren
shutdown	Ausgewählte Schnittstelle abschalten

Eine vollständige Liste der Befehle und ihrer Optionen finden Sie unter *VLAN Interface Configuration-Modus* auf Seite 243.

5.4. Zusammenfassung der Befehlsmodi

Diese Tabelle enthält eine Zusammenfassung der fünf Befehlsmodi.

Modus: Hauptfunktion	Modus aufrufen und verlassen	Eingabeaufforderung
User EXEC: Dies ist die erste Zugriffsebene. Sie können ein Ping-/Telnet-Signal an ein Remote-Gerät senden und einige grundlegende Informationen anzeigen.	• Zugriff auf den *User EXEC*-Modus: Melden Sie sich erfolgreich an und geben Sie „disable“ ein, um auf den *User EXEC*-Modus zuzugreifen. • Beenden: Geben Sie **exit** ein, um sich abzumelden. • Nächster Modus: Geben Sie **enable** ein, um erneut den *Privileged EXEC*-Modus aufzurufen.	Switch>
Privileged EXEC: Hier können Sie die aktuelle Konfiguration anzeigen, die Standardeinstellungen wiederherstellen, den Switch neu laden, Systeminformationen anzeigen, die Konfiguration speichern und auf den *Global Configuration*-Modus zugreifen.	• Zugriff auf den *Privileged EXEC*-Modus: Melden Sie sich erfolgreich an. Geben Sie **enable** ein, wenn Sie vom *User EXEC*-Modus zurückkehren. • Beenden: Geben Sie **disable** ein, um den *User EXEC*-Modus zu beenden. • Geben Sie **exit** ein, um sich abzumelden. • Nächster Modus: Geben Sie **configure terminal** ein, um zum *Global Configuration*-Modus zu wechseln.	Switch#

Modus: Hauptfunktion	Modus aufrufen und verlassen	Eingabeaufforderung
Global Configuration: Konfigurieren Sie alle Funktionen, die der ICRL-M bereitstellt.	• Zugriff auf den *Global Configuration*-Modus: Geben Sie im *Privileged EXEC*-Modus **configure terminal** ein. • Beenden: Geben Sie **exit** oder **end** ein oder drücken Sie **Strg+Z**, um den Vorgang zu beenden. • Nächster Modus: Geben Sie **interface IFNAME/ VLAN VID** ein, um zum *Interface Configuration*-Modus zu gelangen.	Switch(config)#
Port Interface Configuration: Konfigurieren Sie portbezogene Einstellungen.	• Zugriff auf den *Port Interface Configuration*-Modus: Geben Sie im *Global Configuration*-Modus **interface IFNAME** ein. • Beenden: Geben Sie **exit** ein oder drücken Sie **Strg+Z**, um zum *Global Configuration*-Modus zurückzukehren. • Geben Sie **end** ein, um zum *Privileged EXEC*-Modus zurückzukehren.	Switch(config-if)#
VLAN Interface Configuration: Konfigurieren Sie die Einstellungen für ein bestimmtes VLAN.	• Zugriff auf den *VLAN Interface Configuration*-Modus: Geben Sie im *Global Configuration*-Modus **interface VLAN ID** ein. • Beenden: Geben Sie **exit** ein oder drücken Sie **Strg+Z**, um zum *Global Configuration*-Modus zurückzukehren. • Geben Sie **end** ein, um zum *Privileged EXEC*-Modus zurückzukehren.	Switch (config-vlan)#

Die folgenden Befehle sind nützlich, um Zeit bei der Eingabe zu sparen und Tippfehler zu vermeiden.

Drücken Sie **?**, um alle verfügbaren Befehle in einem Modus anzuzeigen. Das hilft Ihnen dabei, den nächsten Befehl anzuzeigen, den Sie eingeben können.

```
switch(config)# interface (?)
  IFNAME        Interface's name
  vlan          Select a vlan to configure
```

Geben Sie *Zeichen***?** ein (siehe unten), um alle verfügbaren Befehle anzuzeigen, die mit diesem Zeichen beginnen.

```
switch(config)# a?
  access-list       Add an access list entry
  administrator     Administrator account setting
  auth              Authentication
```

Drücken Sie die **Tabulatortaste**, um den Befehl schneller einzugeben. Wenn nur ein nächster Befehl verfügbar ist, können Sie mit der **Tabulatortaste** die Eingabe abschließen.

```
switch# co (tab) (tab)
switch# configure terminal

switch(config)# ad (tab)
switch(config)# administrator
```

Tastenkombination	Funktion
Strg+C	Beendet die Ausführung des unvollendeten Befehls.
Strg+S	Sperrt den Bildschirm des Terminals, sodass kein Befehl eingegeben werden kann.
Strg+Q	Entsperrt den Bildschirm, wenn dieser mit **Strg+S** gesperrt wurde.
Strg+Z	Beendet den *Configuration*-Modus.

5.5. Grundeinstellungen (CLI)

In der Gruppe *Basic Setting* können Sie Switch-Informationen, IP-Adresse und Benutzername/Kennwort des Systems konfigurieren. Außerdem können Sie die Firmware aktualisieren, die Konfiguration sichern und wiederherstellen, die Werkseinstellungen wiederherstellen und das System neu starten.

Sie können optional die Web-Benutzerschnittstelle für die Konfiguration verwenden. Informationen hierzu finden Sie unter *Grundeinstellungen* auf Seite 36.

Diese Tabelle enthält detaillierte Informationen zu den CLI-Befehlen für Grundeinstellungen.

Switch-Einstellung	
System Name	Switch(config)# hostname DWORD Netzwerkname des Systems Switch(config)# hostname ICRL-M Switch(config)#
Systemstandort	Switch(config)# snmp-server location Minnesota
Systemkontakt	Switch(config)# snmp-server contact info@de.pepperl-fuchs.com
Anzeige	Switch# show snmp-server name ICRL-M Switch# show snmp-server location DLR lab Switch# show snmp-server contact drada switch# show version Hardware Information : Product Name : ICRL-M-8RJ45/4SFP-G-DIN Serial Number : RDSAMPLE561201 MAC Address : 000D8109FDE4 Manufacturing Date : 2019/08/10 HW Code : 20 Software Information : Loader Version : 1.0.0.1 Firmware Version : 1.0-20200131-16:50:50 System OID : 1.3.6.1.4.1.2882.2.5.0 Switch# show hardware mac MAC Address: 00:0D:81:09:FD:E4
Admin Password	
Benutzername und Kennwort	Switch(config)# administrator NAME Name des Administratorkontos Switch(config)# administrator admin PASSWORD Kennwort des Administratorkontos Switch(config)# administrator admin admin Change administrator account admin and password admin success.
Anzeige	Switch# show administrator Administrator account information name: admin password: admin

IP-Konfiguration	
IP-Adresse/Maske (192.168.250.250, 255.255.255.0) Das aktivierte Bit der Subnetzmaske wird verwendet, um die in der Web-Benutzerschnittstelle angezeigte Nummer darzustellen. Beispiel: 8 steht für 255.0.0.0, 16 steht für 255.255.0.0, 24 steht für 255.255.255.0.	Switch(config)# int vlan 1 Switch(config-if)# ip address dhcp Switch(config-if)# ip address 192.168.250.8/24 Switch(config-if)# ip dhcp client Switch(config-if)# ip dhcp client renew Switch(config-if)# ipv6 address ; IPv6 configuration X:X::X:X/M IPv6 address (e.g. 3ffe:506::1/48) Switch(config-if)# ipv6 address 3ffe:506::1/48
Gateway	Switch(config)# ip route 0.0.0.0/0 192.168.250.254/24
Remove Gateway	Switch(config)# no ip route 0.0.0.0/0 192.168.250.254/24
Anzeige	Switch# show running-config …… ! interface vlan1 ip address 192.168.250.8/24 no shutdown ! ip route 0.0.0.0/0 192.168.250.254/24 !
Zeiteinstellung	
NTP Server	Switch(config)# ntp peer enable disable primary secondary Switch(config)# ntp peer primary IPADDR Switch(config)# ntp peer primary 192.168.250.250
Time Zone	Switch(config)# clock timezone 26 Sun Jan 1 04:13:24 2006 (GMT) Greenwich Mean Time: Dublin, Edinburgh, Lissabon, London ***Anmerkung:*** *Wenn Sie die Zeitzone der Uhr eingeben, wird die Zeitzonenliste angezeigt. Wählen Sie dann die Nummer der Zeitzone aus, die Sie festlegen möchten.*

Zeiteinstellung (Fortsetzung)	
Anzeige	Switch # sh ntp associations Network time protocol Status: Deaktiviert Primary peer: N/A Secondary peer: N/A Switch # show clock Sun Jan 1 04:14:19 2006 (GMT) Greenwich Mean Time: Dublin, Edinburgh, Lissabon, London Switch # show clock timezone clock timezone (26) (GMT) Greenwich Mean Time: Dublin, Edinburgh, Lissabon, London
Jumbo Frame	
Jumbo Frame	Switch(config-if)# mtu 9216
DHCP-Server	
DHCP Server configuration	DHCP-Server auf ICRL-M-Switch aktivieren Switch# Switch# configure terminal Switch(config)# router dhcp Switch(config-dhcp)# service dhcp Configure DHCP network address pool Switch(config-dhcp)#network 50.50.50.0/4 -(network/mask) Switch(config-dhcp)#default-router 50.50.50.1
Lease time configure	Switch(config-dhcp)#lease 300 (300 Sek.)

DHCP-Server (Fortsetzung)	
DHCP Relay Agent	DHCP-Relay-Agent aktivieren Switch# Switch# configure terminal Switch(config)# router dhcp Switch(config-dhcp)# service dhcp Switch(config-dhcp)# ip dhcp relay information option Enable DHCP Relay policy Switch(config-dhcp)# ip dhcp relay information policy replace drop Relay-Richtlinie keep Option82-Feld verwerfen/behalten/ersetzen Switch(config-dhcp)# ip dhcp relay information option <cr> circuit-id Circuit-ID konfigurieren remote-id Remote-ID konfigurieren Switch(config-dhcp)# ip dhcp relay information option option Option82 Switch(config-dhcp)# ip dhcp relay information option
Show DHCP server information	Switch# show ip dhcp server statistics DHCP Server ON Address Pool 1 network:192.168.17.0/24 default-router:192.168.17.254 lease time:300 Excluded Address List IP Address ---------- (Ausgeschlossene Adressen auflisten) Manual Binding List IP Address MAC Address ---------- ---------- (IP- und MAC-Bindungseinträge auflisten) Leased Address List IP Address MAC Address Leased Time Remains ---------- ---------- ---------- (Lease-Zeit für jeden Eintrag auflisten)

DHCP-Server (Fortsetzung)	
DHCP-Befehle	Switch(config)# router dhcp Switch(config-dhcp)# default-router DHCP-Standardrouter end Aktuellen Modus beenden und zum vorherigen Aktivierungsmodus zurückkehren exit Aktuellen Modus beenden und zum vorherigen Modus zurückkehren ip Internet Protocol lease DHCP-Lease-Zeit list Befehlsliste anzeigen network DHCP-Netzwerk no Entfernen quit Aktuellen Modus beenden und zum vorherigen Modus zurückkehren service Service aktivieren
DHCP Server Enable	Switch(config-dhcp)# service dhcp
DHCP Server IP Pool (Network/Mask)	Switch(config-dhcp)# network A.B.C.D/M network/mask ex. 10.10.1.0/24 Switch(config-dhcp)# network 192.168.10.0/24
DHCP Server – Default Gateway	Switch(config-dhcp)# default-router A.B.C.D address Switch(config-dhcp)# default-router 192.168.10.254
DHCP Server – lease time	Switch(config-dhcp)# lease TIME Sekunden Switch(config-dhcp)#lease 1000 (1000 Sek.)
DHCP Server – Static IP and MAC binding	Switch(config-dhcp)# ip dhcp static MACADDR MAC address Switch(config-dhcp)# ip dhcp static 00:0D:81:09:FD:E4 .0001 A.B.C.D leased IP address Switch(config-dhcp)# ip dhcp static 00:0D:81:09:FD:E4 .0001 192.168.10.99
DHCP Relay – Enable DHCP Relay	Switch(config-dhcp)# ip dhcp relay information option Option82 policy Option82 Switch(config-dhcp)# ip dhcp relay information option
DHCP Relay – DHCP policy	Switch(config-dhcp)# ip dhcp relay information policy drop Relay-Richtlinie keep Option82-Feld verwerfen/behalten/ersetzen replace Switch(config-dhcp)# ip dhcp relay information policy drop Switch(config-dhcp)# ip dhcp relay information policy keep Switch(config-dhcp)# ip dhcp relay information policy replace
DHCP Relay – IP Helper Address	Switch(config-dhcp)# ip dhcp helper-address A.B.C.D Switch(config-dhcp)# ip dhcp helper-address 192.168.10.200
Reset DHCP Settings	Switch(config-dhcp)# ip dhcp reset

Sichern und Wiederherstellen	
Startkonfigurationsdatei sichern	Switch# copy startup-config tftp: 192.168.250.33/default.conf Writing Configuration [OK] ***Anmerkung:*** *Um die neueste Startkonfigurationsdatei zu sichern, sollten Sie zuerst die aktuellen Einstellungen im Flash speichern. Weitere Informationen zum Speichern von Einstellungen im Flash finden Sie unter Speichern (im Flash) auf Seite 159.* *Im obigen Beispiel ist 192.168.250.33 die IP-Adresse des TFTP-Servers und „default.conf“ der Name der Konfigurationsdatei. In Ihrer Umgebung können unterschiedliche IP-Adressen oder andere Dateinamen verwendet werden. Geben Sie die IP-Adresse des TFTP-Zielservers oder den Dateinamen in diesen Befehl ein.*
Konfiguration wiederherstellen	Switch# copy tftp: 192.168.250.33/default.conf startup-config
Startkonfiguration anzeigen	Switch# show startup-config
Aktive Konfiguration anzeigen	Switch# show running-config
Firmware-Upgrade	
Firmware-Upgrade	Switch# archive download-sw /overwrite tftp 192.168.11.33 ICRL-M.bin Firmware upgrading, don't turn off the switch! Tftping file ICRL-M.bin Firmware upgrading .... Firmware upgrade success!! Rebooting.....
Standard laden	
Standard laden	Switch# reload default-config file Reload OK! Switch# reboot
Systemneustart	
Reboot	Switch# reboot

5.6. Portkonfiguration (CLI)

Mit der Gruppe „Port Configuration“ können Sie den Portstatus aktivieren/deaktivieren oder die Porteinstellungen für Auto-Negotiation, Geschwindigkeit, Duplexfunktion, Flusssteuerung, Ratenbeschränkung und Portaggregation konfigurieren. Außerdem können Sie hier Portstatus- und Aggregationsinformationen anzeigen.

Gigabit-Ports werden als gi1, gi2, gi3 usw. bezeichnet.

Sie können optional die Web-Benutzerschnittstelle für die Konfiguration verwenden. Informationen hierzu finden Sie unter *Portkonfiguration* auf Seite 60.

Diese Tabelle enthält detaillierte Informationen zu den CLI-Befehlen für die Portkonfiguration.

Portsteuerung	
Port Control – State	Switch(config-if)# shutdown -> Portstatus deaktivieren Port1 Link Change to DOWN interface gigabitethernet1 is shutdown now. Switch(config-if)# no shutdown -> Portstatus aktivieren Port1 Link Change to DOWN Port1 Link Change to UP interface gigabitethernet1 is up now. Switch(config-if)# Port1 Link Change to UP Switch(config)# sfp ddm Digitale Diagnose und Überwachung eject SFP auswerfen scan SFP scannen Switch(config)# sfp ddm enable DDM aktivieren disable DDM deaktivieren
Port Control – Auto Negotiation	Switch(config)# interface gi1 Switch(config-if)# auto-negotiation Auto-negotiation of port 1 is enabled!
Port Control – Force Speed/ Duplex	Switch(config-if)# speed 100 Port1 Link Change to DOWN set the speed mode ok! Switch(config-if)# Port1 Link Change to UP Switch(config-if)# duplex full set the duplex mode ok!
Port Control – Flow Control	Switch(config-if)# flowcontrol on Flowcontrol on for port 1 set ok! Switch(config-if)# flowcontrol off Flowcontrol off for port 1 set ok!

Portstatus	
Portstatus	ICRL-M# show interface gi1 Interface gigabitethernet1 Description : N/A Administrative Status : Enable Operating Status : Connected Duplex : Auto (Full) Speed : Auto (100) MTU : 1518 Flow Control : off Default Port VLAN ID: 1 Ingress Filtering : Disabled Acceptable Frame Type : All Port Security : Disabled Auto Negotiation : Enable Loopback Mode : None STP Status : Forwarding Default CoS Value for untagged packets is 0. Medium mode is Copper. ICRL-M# show sfp ddm Port 9 Admin status : Enabled Temperature : N/A Tx power : N/A Rx power : N/A Port 10 Admin status : Enabled Temperature : N/A Tx power : N/A Rx power : N/A Port 11 Admin status : Enabled Temperature : 45.00 C (Range : -15.00 - 85.00) Tx power : -6.2 dBm (Range : -10.5 - -3.0) Rx power : -9.0 dBm (Range : -17.0 - -3.0) Port 12 Admin status : Enabled Temperature : N/A Tx power : N/A Rx power : N/A ***Anmerkung:*** *Administrative Status -> Portstatus des Ports Operating Status -> Aktueller Status des Ports Duplex -> Duplexmodus des Ports Speed -> Geschwindigkeitsmodus des Ports Flow Control -> Status der Flusssteuerung des Ports*

Portstatus (Fortsetzung)	
Rate Control – Ingress or Egress	Switch(config-if)# rate-limit egress Ausgehende Pakete ingress Eingehende Pakete ***Anmerkung:*** *Um die Ratenbeschränkung zu aktivieren, müssen Sie zuerst die Ingress- oder Egress-Regel auswählen und dann den Pakettyp und die Bandbreite zuweisen.*
Rate Control – Filter Packet Type	Switch(config-if)# rate-limit ingress bandwidth Informationsparameter zur Bandbreite festlegen Switch(config-if)# rate-limit ingress bandwidth Switch(config-if)# rate-limit ingress bandwidth 800 Ingress-Ratenbeschränkung für Port 1 mit 800 KBit/s festlegen
Storm Control	
Storm Control – Packet Type	Switch(config-if)# storm-control broadcast: Broadcast-Pakete dlf: Destination Lookup Failure multicast: Multicast-Pakete

Storm Control – Rate	Switch(config)# storm-control broadcast
	<0–100000> Ratenbeschränkungswert von 0~262143 Paketen/Sek.
	Switch(config)# storm-control broadcast 10000
	limit_rate = 10000 Pakete/Sek.
	Ratenbeschränkung für Broadcast-Pakete festlegen
	Switch(config)# storm-control multicast 10000
	limit_rate = 10000 Pakete/Sek.
	Ratenbeschränkung für Multicast-Pakete festlegen
	Switch(config)# storm-control dlf 10000
	limit_rate = 10000 Pakete/Sek.
	Ratenbeschränkung für Destination Lookup Failures festlegen

Port-Trunking	
Anzeige – LACP	Switch# show lacp internal LACP group 1 is inactive LACP group 2 is inactive LACP group 3 is inactive LACP group 4 is inactive LACP group 5 is inactive LACP group 6 is inactive LACP group 7 is inactive LACP group 8 is inactive
LACP	Switch(config)# lacp group 1 gi8-10 Group 1 based on LACP(802.3ad) is enabled!

Port-Trunking (Fortsetzung)	
LACP – Portein-stellung	SWITCH(config-if)# lacp port-priority LACP-Priorität für physische Schnittstellen timeout weist einen administrativen LACP-Timeout zu SWITCH(config-if)# lacp port-priority <1–65535> Gültiger Portprioritätsbereich 1 – 65535 (Standard ist 32768) SWITCH(config-if)# lacp timeout long gibt einen langen Timeoutwert an (Standard) short gibt einen kurzen Timeoutwert an SWITCH(config-if)# lacp timeout short Set lacp port timeout ok.
Anzeige – LACP	Switch# show lacp counters LACP-statistische Informationen group LACP-Gruppe internal Interne LACP-Informationen neighbor LACP-Nachbarinformationen port-setting LACP-Einstellung für physische Schnittstellen system-id LACP-Systemidentifizierung system-priority LACP-Systempriorität SWITCH# show lacp port-setting LACP Port Setting : Port Priority Timeout ----- --------- -------- 1 32768 Long 2 32768 Long 3 32768 Long ……. Switch# show lacp internal LACP group 1 internal information: LACP Port Admin Oper Port Port Priority Key Key State ----- ----------- -------- -------- ------- 8 1 8 8 0x45 9 1 9 9 0x45 10 1 10 10 0x45 LACP group 2 is inactive LACP group 3 is inactive LACP group 4 is inactive
Anzeige – Trunk	Switch# show trunk group 1 FLAGS: I -> Individual P -> In channel D -> Port Down Trunk Group TGID Protocol Load-Balance Ports -----+---------+------------+----------------------------------- 1 Static src-dst-mac 11(D) 12(P)

5/21/20

5.7. Netzwerkredundanz (CLI)

Für industrielle Anwendungen ist es wichtig, dass das Netzwerk jederzeit läuft. Der ICRL-M unterstützt:

- Standard Spanning Tree Protocol (STP) und Rapid Spanning Tree Protocol (RSTP)

  Der ICRL-M unterstützt die RSTP-Versionen IEEE 802.1D-2004, IEEE 802.1D-1998 STP und IEEE 802.1w RSTP.

- MSTP (Multiple Spanning Tree Protocol)

  MSTP implementiert IEEE 802.1s, das RSTP für schnelle Konvergenz verwendet, und ermöglicht die Gruppierung von VLANs in einer Spanning-Tree-Instanz, wobei jede Instanz über eine Spanning-Tree-Topologie unabhängig von anderen Spanning-Tree-Instanzen verfügt. Diese Architektur bietet mehrere Weiterleitungspfade für Datenverkehr, ermöglicht Lastausgleich und reduziert die Anzahl der Spanning-Tree-Instanzen, die für die Unterstützung einer großen Anzahl von VLANs erforderlich sind. MSTP wurde ursprünglich in IEEE 802.1s definiert und später in die IEEE-802.1Q-2003-Spezifikation integriert.

- Redundant Ring

  Der redundante Ring verfügt über 0 ms für Wiedereinlagerung und ca.

- Rapid Dual Homing (RDH)

  Die fortschrittliche RDH-Technologie ermöglicht dem ICRL-M die einfache und komfortable Verbindung mit einem zentralen verwalteten Switch. Mit der RDH-Technologie können Sie auch mehrere Rapid Super Rings- oder RSTP-Gruppen verbinden, die auch als automatische Ringkopplung bezeichnet werden.

Sie können optional die Web-Benutzerschnittstelle für die Konfiguration verwenden. Informationen hierzu finden Sie unter *Netzwerkredundanz* auf Seite 70.

Diese Tabelle enthält detaillierte Informationen zu den CLI-Befehlszeilen für Netzwerkredundanz.

Global (STP, RSTP und MSTP)	
Aktivieren	Switch(config)# spanning-tree enable
Deaktivieren	Switch(config)# spanning-tree disable
Modus	Switch(config)# spanning-tree mode rst Rapid Spanning Tree Protocol (802.1w) stp Spanning Tree Protocol (802.1d) mst Multiple Spanning Tree Protocol (802.1s) Switch(config)# spanning-tree mode Switch(config)# spanning-tree mode mst Änderung des Spanning-Tree-Modus zu MSTP (802.1s) Switch(config)# spanning-tree mode stp Änderung des Spanning-Tree-Modus zu STP (802.1d) Switch(config)# spanning-tree mode rst Änderung des Spanning-Tree-Modus zu RSTP (802.1w) Switch(config)# spanning-tree mode mst Änderung des Spanning-Tree-Modus zu MSTP (802.1s)
Bridge-Priorität	Switch(config)# spanning-tree priority <0–61440> Wert der Bridge-Priorität als Vielfaches von 4096 Switch(config)# spanning-tree priority 4096
Bridge-Zeiten	Switch(config)# spanning-tree bridge-times (Weiterleitungsverzögerung) (max. Alter) (Hello-Zeit) Switch(config)# spanning-tree bridge-times 15 20 2 Mit diesem Befehl können Sie das gesamte Timing auf einmal konfigurieren.

Global (STP, RSTP und MSTP) (Fortsetzung)	
Weiterleitungs-verzögerung	Switch(config)# spanning-tree forward-time <4–30> Wert der Weiterleitungsverzögerung in Sekunden Switch(config)# spanning-tree forward-time 15
Max. Alter	Switch(config)# spanning-tree max-age <6–40> Wert des maximalen Nachrichtenalters in Sekunden Switch(config)# spanning-tree max-age 20
Hello-Zeit	Switch(config)# spanning-tree hello-time <1–10> Wert der Hello-Zeit in Sekunden Switch(config)# spanning-tree hello-time 2
MSTP	

MSTP-Konfigurati-onsbaum aufrufen	Switch(config)# spanning-tree mst
	  MSTMAP MST-Instanznummer oder -bereich
	  configuration Zu MST-Konfigurationsmodus wechseln
	  forward-time Zeit der Weiterleitungsverzögerung
	  hello-time Hello-Zeit
	  max-age Maximales Alter der Nachricht
	  max-hops Maximale Hops
	  sync Portstatus des vorhandenen VLAN-Eintrags synchronisieren
	Switch(config)# spanning-tree mst configuration
	Switch(config)# spanning-tree mst configuration
	Switch(config-mst)#
	  abort Aktuellen Modus beenden und alle Änderungen verwerfen
	  end Aktuellen Modus beenden, zum Aktivierungsmodus wechseln und alle Änderungen übernehmen
	  exit Aktuellen Modus beenden und alle Änderungen übernemen
	  instance MST-Instanz
	  list Befehlsliste anzeigen
	  name Name der MST-Region
	  no Befehl negieren oder Standard wiederherstellen
	  quit Aktuellen Modus beenden und alle Änderungen übernehmen
	  revision Revision der MST-Region
	  show MST-Konfiguration anzeigen

Regionskonfigu-ration	Regionsname: Switch(config-mst)# name NAME Namenszeichenfolge Switch(config-mst)# name Pepperl+Fuchs Regionsrevision: Switch(config-mst)# revision <0–65535> Revisionswert Switch(config-mst)# revision 65535
Instanz zu VLAN zuordnen (Bsp.: VLAN 2 zu Instanz 1 zuordnen)	Switch(config-mst)# instance <1–15> Zielinstanznummer Switch(config-mst)# instance 1 vlan VLANMAP target vlan number(z. B. 10) or range(z. B. 1–10) Switch(config-mst)# instance 1 vlan 2

MSTP (Fortsetzung)	
Aktuelle MST-Konfiguration anzeigen	Switch(config-mst)# show current Current MST configuration Name [Pepperl+Fuchs] Revision 65535 Instance Vlans Mapped -------- ---------- 0 1,4-4094 1 2 2 3 ---------- Config HMAC-MD5 Digest: 0xB41829F9030A054FB74EF7A8587FF58D ----------
Regionsname entfernen	Switch(config-mst)# no name Name konfigurieren revision Revision konfigurieren instance MST-Instanz Switch(config-mst)# no name
Beispiel für das Entfernen einer Instanz	Switch(config-mst)# no instance <1–15> Zielinstanznummer Switch(config-mst)# no instance 2
Ausstehende MST-Konfiguration anzeigen	Switch(config-mst)# show pending Pending MST configuration Name [] (->Der Name wird durch „no name“ entfernt.) Revision 65535 Instance Vlans Mapped -------- ---------- 0 1,3-4094 1 2 (->Instanz 2 wird durch „no instance 2“ entfernt.) ---------- Config HMAC-MD5 Digest: 0x3AB68794D602FDF43B21C0B37AC3BCA8 ----------
Einstellung anwenden und zum Konfigurationsmodus wechseln	Switch(config-mst)# quit Alle Änderungen an der MST-Konfiguration übernehmen Switch(config)#
Einstellung anwenden und zum Global-Modus wechseln	Switch(config-mst)# end Alle Änderungen an der MST-Konfiguration übernehmen Switch#

MSTP (Fortsetzung)	
Einstellung abbrechen und zum Konfigurationsmodus wechseln „Pending“ anzeigen, um zu sehen, wo die neuen Einstellungen nicht angewendet werden	Switch(config-mst)# abort Alle Änderungen an der MST-Konfiguration verwerfen Switch(config)# spanning-tree mst configuration Switch(config-mst)# show pending Pending MST configuration Name [Pepperl+Fuchs] (->Der Name wird nach dem Abbrechen der Einstellungen nicht übernommen.) Revision 65535 Instance Vlans Mapped -------- ---------- 0 1,4-4094 1 2 2 3 (->Die Instanz wird nach dem Abbrechen der Einstellungen nicht übernommen.) --- Config HMAC-MD5 Digest: 0xAC36177F50283CD4B83821D8AB26DE62 ---
RSTP	
System-RSTP-Einstellung	Der Modus sollte RSTP lauten. Die Timings können in den vorherigen Beispielen aufgeführten globalen Einstellungen konfiguriert werden.
Port Configuration-Modus	
Portkonfiguration	Switch(config)# interface gi1 Switch(config-if)# spanning-tree bdufilter sicherer BPDU-Prozess an der Edge-Port-Schnittstelle bpduguard sichere Antwort auf ungültige Konfigurationen (von sich selbst gesendete BPDU empfangen) cost Änderung der Kosten für den Spanning-Tree-Portpfad einer Schnittstelle edge-port Schnittstelle, die an ein LAN-Segment am Ende eines überbrückten LAN oder an einen Endknoten angeschlossen ist link-type Verbindungstyp für den Rapid Spanning Tree mst Multiple Spanning Tree port-priority Spanning-Tree-Priorität stp-state STP-Bridge-Port-Status
Portpfadkosten	Switch(config-if)# spanning-tree cost <1–200000000> 16-Bit-basierter Wertebereich von 1–65535, 32-Bit-basierter Wertebereich von 1–200.000.000 Switch(config-if)# spanning-tree cost 200000
Portpriorität	Switch(config-if)# spanning-tree port-priority <0–240> Zahl von 0 bis 240, Vielfaches von 16 Switch(config-if)# spanning-tree port-priority 128
Verbindungstyp – Automatisch	Switch(config-if)# spanning-tree link-type auto
Verbindungstyp – P2P	Switch(config-if)# spanning-tree link-type point-to-point

Port Configuration-Modus (Fortsetzung)	
Verbindungstyp – Freigabe	Switch(config-if)# spanning-tree link-type shared
Edge-Port	Switch(config-if)# spanning-tree edge-port enable Switch(config-if)# spanning-tree edge-port disable
MSTP-Portkonfiguration	Switch(config-if)# spanning-tree mst MSTMAP cost <1–200000000> Wert der Kosten für den MST-Instanzport Switch(config-if)# spanning-tree mst MSTMAP port-priority <0–240> Wert der Priorität des MST-Instanzports als Vielfaches von 16
Globale Informationen	
Aktive Informationen	Switch# show spanning-tree active Spanning-Tree : Enabled Protocol : RSTP Root Address : 000d.8109.fde4 Priority : 32768 Root Path Cost : 0 Root Port : N/A Root Times : max-age 20, hello-time 2, forward-delay 15 Bridge Address : 000d.8109.fde4 Priority : 32768 Bridge Times : max-age 20, hello-time 2, forward-delay 15 BPDU transmission-limit : 3 Port Role State Cost Prio.Nbr Type Aggregated ------ ---------- ---------- -------- ---------- ------------ ------------ gi1 Designated Forwarding 200000 128.1 P2P(RSTP) N/A gi11 Designated Forwarding 20000 128.11 P2P(RSTP) N/A
RSTP-Zusammenfassung	Switch# show spanning-tree summary Spanning-Tree : Enabled Protocol : RSTP Root Address : 000d.8109.fde4 Priority : 32768 Root Path Cost : 0 Root Port : N/A Root Times : max-age 20, hello-time 2, forward-delay 15 Bridge Address 000d.8109.fde4 Priority : 32768 Bridge Times : max-age 20, hello-time 2, forward-delay 15 BPDU transmission-limit : 3 BPDU Skewing Detection : Disabled Backbonefast : Disabled Topology Change Flag : False Topology Change Detected Flag : False Topology Change Count : 75 Last Topology Change from : 0000.0000.0000 Timers: hello 1, topology change 0 Summary of connected spanning tree ports : Port-State Summary Blocking Listening Learning Forwarding Disabled -------- --------- -------- ---------- -------- 0 0 0 2 10 Port Link-Type Summary AutoDetected PointToPoint SharedLink EdgePort ------------ ------------ ---------- -------- 12 0 0 10

5/21/20

Globale Informationen (Fortsetzung)	
Portinformationen	Switch# show spanning-tree interface gi1 Interface gigabitethernet1 of Bridge is Enabled Port Role : Designated Port State : Forwarding Edge Port : Edge (Non-Edge) BPDU Filter : Disabled Link Type : Auto (Point-to-point) BPDU Guard : Disabled Timers : message-age 0, forward-delay 0 BPDUs : sent 390718, received 91 TCNs : sent 0, received 0 Message Expired Count : 0 Forward Transition Count : 1 Aggregation Group: N/A Type: N/A Aggregated with : N/A Port information port id 128.1 priority 128 cost 200000 Designated root address 000d.8109.fde4 priority 32768 cost 200000 Designated bridge address 000d.8109.fde4 priority 32768 port id 128.1
MSTP-Informationen	
MSTP-Konfiguration	Switch# show spanning-tree mst configuration Current MST configuration (MSTP is Stopped) Name [] Revision 0 Instance Vlans Mapped -------- ---------- 0 1-4094 ---------- Config HMAC-MD5 Digest: 0xAC36177F50283CD4B83821D8AB26DE62 ---------- ----------

MSTP-Informationen (Fortsetzung)	
Ring erstellen oder konfigurieren	Switch(config)# redundant-ring 1 Ring 1 created Switch(config-redundant-ring)# ***Anmerkung:*** *1 ist die Ziel-Ring-ID, die erstellt oder konfiguriert wird.*
Super-Ring-Version	Switch(config-redundant-ring)# version default Standard auf „Redundanter Ring“ festlegen rapid-super-ring Rapid Super Ring super-ring Super Ring Switch(config-redundant-ring)# version rapid-super-ring
Priorität	Switch(config-redundant-ring)# priority <0–255> Der gültige Bereich liegt zwischen 0 und 255. default Standard festlegen Switch(config-redundant-ring)# super-ring priority 100
Ringport	Switch(config-redundant-ring)# port IFLIST Schnittstellenliste, Bsp.: gi1,gi3–5,gi8–10 cost Pfadkosten Switch(config-redundant-ring)# port 1,2
Ringinformationen	Switch# show redundant-ring [Ring-ID] [Ring1] Ring1 Current Status : Disabled Role : Disabled Ring Status : Abnormal Ring Manager : 0000.0000.0000 Blocking Port : N/A Giga Copper : N/A Configuration : Version : Super Ring Priority : 128 Ring Port : gi1, gi2 Path Cost : 100, 200 Dual-Homing II : Disabled Statistics : Watchdog sent 0, received 0, missed 0 Link Up sent 0, received 0 Link Down sent 0, received 0 Role Transition count 0 Ring State Transition count 1 *Ring-ID* ist optional. Wenn die Ring-ID eingegeben wird, zeigt dieser Befehl nur die Informationen des Zielrings an.

5.8. VLAN (CLI)

Ein virtuelles LAN (VLAN) ist eine logische Gruppierung von Knoten, um eine Broadcast-Domain auf bestimmte Mitglieder einer Gruppe zu beschränken, ohne die Mitglieder physisch zu gruppieren. Das VLAN ermöglicht es Ihnen, den Netzwerkverkehr so zu isolieren, dass nur Mitglieder des VLAN Datenverkehr von Mitgliedern desselben VLAN empfangen können. Im Grunde ist die Erstellung eines VLAN über einen Switch das logische Äquivalent zur physischen Neuverbindung einer Gruppe von Netzwerkgeräten mit einem anderen Layer-2-Switch, ohne diese Geräte tatsächlich von ihren ursprünglichen Switches zu trennen.

Der ICRL-M unterstützt IEEE-802.1Q-VLAN, das auch als Tag-Based VLAN bezeichnet wird. Dieses Tag-Based VLAN ermöglicht die Erstellung eines VLAN über verschiedene Switches hinweg. IEEE 802.1Q Tag-Based VLANs nutzen VLAN-Steuerungsinformationen, die in einem VLAN-Header gespeichert sind, der an IEEE-802.3-Paketframes angehängt ist. Dieses Tag enthält eine VLAN-Kennung (VID), die angibt, zu welchem VLAN ein Frame gehört. Da jeder Switch nur das Tag eines Frames prüfen muss, ohne den Inhalt des Frames zu untersuchen, spart dies auch eine Menge Rechenressourcen innerhalb des Switches.

Sie können optional die Web-Benutzerschnittstelle für die Konfiguration verwenden. Informationen hierzu finden Sie unter *VLAN* auf Seite 90.

Die folgende Tabelle enthält detaillierte Informationen über Befehlszeilen für das VLAN.

VLAN-Portkonfiguration	
VLAN-Port-PVID	Switch(config-if)# switchport trunk native vlan 2 Set port default vlan id to 2 success
An Port zulässiger Frametyp	Switch(config)# inter gi1 Switch(config-if)# acceptable frame type all any kind of frame type is accepted! Switch(config-if)# acceptable frame type vlantaggedonly only vlan-tag frame is accepted!
Ingress-Filterung (für Fast-Ethernet-Port 1)	Switch(config)# interface gi1 Switch(config-if)# ingress filtering enable ingress filtering enable Switch(config-if)# ingress filtering disable ingress filtering disable
Egress-Regel – Nicht getaggt (für VLAN 2)	Switch(config-if)# switchport access vlan 2 switchport access vlan - success
Egress-Regel – Getaggt (für VLAN 2)	Switch(config-if)# switchport trunk allowed vlan add 2

VLAN-Portkonfiguration (Fortsetzung)	
Anzeige – Port-Ingress-Regel (PVID, Ingress-Filterung, zulässiger Frametyp)	ICRL-M# show interface gi1 Interface gigabitethernet1 Description : N/A Administrative Status : Enable Operating Status : Connected Duplex : Auto (Full) Speed : Auto (100) MTU : 1518 Flow Control : off Default Port VLAN ID: 1 Ingress Filtering : Disabled Acceptable Frame Type : All Port Security : Disabled Auto Negotiation : Enable Loopback Mode : None STP Status : Forwarding Default CoS Value for untagged packets is 0. Medium mode is Copper.
Anzeige – Port-Egress-Regel (Egress-Regel, IP-Adresse, Status)	Switch# show running-config …… ! interface gigabitethernet1 switchport access vlan 1 switchport access vlan 3 switchport trunk native vlan 2 ……. interface vlan1 ip address 192.168.250.8/24 no shutdown
VLAN-Konfiguration	
VLAN (2) erstellen	Switch(config)# vlan 2 vlan 2 success Switch(config)# interface vlan 2 Switch(config-if)# ***Anmerkung:*** *In der CLI-Konfiguration sollten Sie zuerst eine VLAN-Schnittstelle erstellen. Dann können Sie Ports hinzufügen/entfernen. Der Standardstatus des erstellten VLAN wird erst verwendet, wenn Sie ihm Mitgliedsports hinzufügen.*
VLAN entfernen	Switch(config)# no vlan 2 no vlan success ***Anmerkung:*** *Sie können das VLAN nur entfernen, wenn es nicht verwendet wird.*

VLAN-Konfiguration (Fortsetzung)	
VLAN-Name	Switch(config)# vlan 2 vlan 2 exists Switch(config-vlan)# name v2 Switch(config-vlan)# no name ***Anmerkung:*** *Verwenden Sie „no name“, um den Namen zum Standardnamen „VLAN VID“ zu ändern.*
VLAN-Beschreibung	Switch(config)# interface vlan 2 Switch(config-if)# Switch(config-if)# description Das ist VLAN2 Switch(config-if)# no description ->Beschreibung löschen
IP-Adresse des VLAN	Switch(config)# interface vlan 2 Switch(config-if)# Switch(config-if)# ip address 192.168.250.18/24 Switch(config-if)# no ip address 192.168.250.8/24 ->IP-Adresse löschen
Mehrere VLANs erstellen (VLAN 5–8)	Switch(config)# interface vlan 5-8
VLAN abschalten	Switch(config)# interface vlan 2 Switch(config-if)# shutdown Switch(config-if)# no shutdown ->VLAN einschalten
Anzeige – VLAN-Tabelle	Switch# sh vlan VLAN Name Status Trunk Ports Access Ports ---- ---- ------ ------------ -------------------------- 1 VLAN1 Static - gi1-12 2 VLAN2 Unused -
Anzeige – VLAN-Schnittstelleninformationen	Switch# show interface vlan1 Interface vlan1 Description : N/A Administrative Status : Enable Operating Status : Up DHCP Client : Disable Primary IP Address : 10.0.0.147/16 IPv6 Address : fe80::20d:81ff:fe09:fde4/64

GVRP-Konfiguration	
GVRP aktivieren/ deaktivieren	Switch(config)# gvrp mode disable GVRP-Funktion global auf dem Switch deaktivieren enable GVRP-Funktion global auf dem Switch aktivieren Switch(config)# gvrp mode enable Gvrp is enabled on the switch!
GVRP-Timer konfigurieren Timer beitreten/ Timer verlassen/Alle Timer verlassen	Switch(config)# inter gi1 Switch(config-if)# garp timer <10–10000> Switch(config-if)# garp timer 20 60 1000 ***Anmerkung:*** *Die Einheit dieses Timers ist Hundertstelsekunden.*
Management-VLAN	
Management-VLAN	Switch(config)# int vlan 1 (Zu Management-VLAN gehen) Switch(config-if)# no shutdown
Anzeige	Switch# show running-config …. ! interface vlan1 ip address 192.168.250.17/24 ip igmp no shutdown ! ….

5.9. Privates VLAN (CLI)

Ein privates VLAN hilft bei der Behebung von Problemen mit der primären VLAN-ID, der Isolierung der Clientports und der Netzwerksicherheit. Die Private-VLAN-Funktionen bieten primäre und sekundäre VLANs innerhalb eines einzigen Switches.

Primäres VLAN: Der Uplink-Port ist in der Regel Mitglied des primären VLAN. Ein primäres VLAN enthält promiskuitive Ports, die mit sekundären VLANs kommunizieren können.

Sekundäres VLAN: Die Clientports werden in der Regel innerhalb des sekundären VLAN definiert. Das sekundäre VLAN umfasst isolierte und Community-VLANs. Die Clientports können isolierte VLANs sein oder im selben Community-VLAN gruppiert werden. Die Ports innerhalb desselben Community-VLAN können miteinander kommunizieren, die isolierten VLAN-Ports können jedoch nicht miteinander kommunizieren.

Sie können optional die Web-Benutzerschnittstelle für die Konfiguration verwenden. Informationen hierzu finden Sie unter *Privates VLAN* auf Seite 97.

Die folgende Tabelle enthält detaillierte Informationen über Befehlszeilen für die private Private-VLAN-Konfiguration, VLAN-Konfiguration und VLAN-Tabellenanzeige.

Private-VLAN-Konfiguration	
VLAN erstellen	Switch(config)# vlan 2 vlan 2 success Switch(config-vlan)# end Aktuellen Modus beenden und zum Aktivierungsmodus wechseln exit Aktuellen Modus beenden und zum vorherigen Modus zurückkehren list Befehlsliste anzeigen name VLAN einen Namen zuweisen no Nein private-vlan Privates VLAN konfigurieren
Private-VLAN-Typ	Wechseln Sie zu dem VLAN, das Sie zuerst konfigurieren möchten. Switch(config)# vlan (VID)
Typen auswählen	Switch(config-vlan)# private-vlan community VLAN als privates Community-VLAN konfigurieren isolated VLAN als isoliertes privates VLAN konfigurieren primary VLAN als primäres privates VLAN konfigurieren
Typ „Primär“	Switch(config-vlan)# private-vlan primary <cr>
Typ „Isoliert“	Switch(config-vlan)# private-vlan isolated <cr>
Typ „Community“	Switch(config-vlan)# private-vlan community <cr>
Zur Portkonfiguration gehen	Switch(config)# interface (port_number, Bsp.: gi1) Switch(config-if)# switchport private-vlan host-association Host-Verknüpfung des privaten VLAN festlegen mapping Primäres VLAN dem sekundären zuordnen
Private-VLAN-Porttyp	Switch(config-if)# switchport mode private-vlan Private-VLAN-Modus festlegen Switch(config-if)# switchport mode private-vlan host Modus auf Private-VLAN-Host festlegen promiscuous Modus auf promiskuitives privates VLAN festlegen

Private-VLAN-Konfiguration (Fortsetzung)	
Promiskuitiver Porttyp	Switch(config-if)# switchport mode private-vlan promiscuous <cr>
Host-Porttyp	Switch(config-if)# switchport mode private-vlan host <cr>
Private-VLAN-Portkonfiguration PVLAN-Porttyp	Switch(config)# interface gi1 Switch(config-if)# switchport mode private-vlan host
Hostverknüpfung primär zu sekundär (Der Befehl ist nur für den Hostport verfügbar.)	Switch(config-if)# switchport private-vlan host-association <2–4094> Primäre Bereichs-VLAN-ID der Private-VLAN-Portzuordnung Switch(config-if)# switchport private-vlan host-association 2 <2–4094> Sekundäre Bereichs-VLAN-ID der Private-VLAN-Portzuordnung Switch(config-if)# switchport private-vlan host-association 2 3
Zuordnung primäres zu sekundärem VLAN (Der Befehl ist nur für promiskuitive Ports verfügbar.)	Switch(config)# interface gi1 Switch(config-if)# switchport mode private-vlan promiscuous Switch(config-if)# switchport private-vlan mapping 2 add 3 Switch(config-if)# switchport private-vlan mapping 2 add 4 Switch(config-if)# switchport private-vlan mapping 2 add 5
Private-VLAN-Informationen	
Private-VLAN-Informationen	Switch# show vlan private-vlan FLAGS: I -> Isolated P -> Promiscuous C -> Community Primary Secondary Type Ports ------- --------- ----------------- ---------- 2 3 Isolated gi1(P),gi2(I) 2 4 Community gi2(P),gi3(C) 2 5 Community gi2(P),gi1(C),gi3(I) 10 - - -

Private-VLAN-Informationen (Fortsetzung)	
Informationen zur aktiven Konfiguration Private-VLAN-Typ Private-VLAN-Portinformationen	Switch# show run Building configuration... Current configuration: hostname Switch vlan learning independent ! vlan 1 ! vlan 2 private-vlan primary ! vlan 3 private-vlan isolated ! vlan 4 private-vlan community ! vlan 5 private-vlan community ! …….. …….. interface gigabitethernet7 switchport access vlan add 2,5 switchport trunk native vlan 5 switchport mode private-vlan host switchport private-vlan host-association 2 5 ! interface gigabitethernet switchport access vlan add 2,4 switchport trunk native vlan 4 switchport mode private-vlan host switchport private-vlan host-association 2 4 ! interface gigabitethernet9 switchport access vlan add 2,5 switchport trunk native vlan 5 switchport mode private-vlan host switchport private-vlan host-association 2 3 ! interface gigabitethernet10 switchport access vlan add 2,5 switchport trunk native vlan 2 switchport mode private-vlan promiscuous switchport private-vlan mapping 2 add 3-5 …… ……..

Private-VLAN-Informationen (Fortsetzung)	
PVLAN-Typ	Switch# show vlan private-vlan type Vlan Type Ports ---- ----------- ---------- 2 primary gi3 3 isolated gi2 4 community gi1 5 community gi4,gi5 10 primary -
Hostliste	Switch# show vlan private-vlan port-list Ports Mode Vlan ----- ----------- ---- 1 normal - 2 normal - 3 normal - 4 normal - 5 normal - 6 normal - 7 host 5 8 host 4 9 host 3 10 promiscuous 2

5.10. Datenverkehr-Priorisierung (CLI)

Quality of Service (QoS) bietet einen Mechanismus zur Priorisierung des Datenverkehrs, mit dem Sie einen besseren Service für bestimmte Datenflüsse bereitstellen können. QoS kann auch dazu beitragen, Überlastungsprobleme zu beseitigen und sicherzustellen, dass Datenverkehr mit hoher Priorität zuerst bereitgestellt wird. In diesem Abschnitt können Sie die Einstellungen für die Datenverkehr-Priorisierung für jeden Port konfigurieren, um Prioritäten festzulegen.

ICRL-MQoS unterstützt vier physische Warteschlangen, WRR (Weighted Fair Queuing) und das Strict Priority Scheme, das dem IEEE-802.1p-CoS-Tag und den IPv4-TOS/DiffServ-Informationen folgt, um den Datenverkehr Ihres industriellen Netzwerks zu priorisieren.

Sie können optional die Web-Benutzerschnittstelle für die Konfiguration verwenden. Informationen hierzu finden Sie unter *Datenverkehr-Priorisierung* auf Seite 103. Diese Tabelle enthält detaillierte Informationen über Befehlszeilen für die Konfiguration der Datenverkehr-Priorisierung

QoS-Einstellung	
Warteschlangenplanung – Strenge Priorität	Switch(config)# qos queue-sched sp Strenge Priorität wrr Weighted Round Robin Switch(config)# qos queue-sched sp The queue scheduling scheme is setting to Strict Priority.
Warteschlangenplanung – WRR	Switch(config)# qos queue-sched wrr <1–10> Gewichtungen für CoS-Warteschlange 0 (queue_id 0) Switch(config)# qos queue-sched wrr 10 <1–10> Gewichtungen für CoS-Warteschlange 1 (queue_id 1) …….. Switch(config)# qos queue-sched wrr 1 2 3 4 The queue scheduling scheme is setting to Weighted Round Robin. Weisen Sie das Verhältnis für die 4 Serviceklassen zu.
Porteinstellung – CoS (Standard-Portpriorität)	Switch(config)# interface **gi1** Switch(config-if)# qos priority <0–3> Prioritätswarteschlange zuweisen Switch(config-if)# qos priority 3 The priority queue is set 3 ok.
QoS-Prioritätsmodus	Switch(config)# qos priority cos CoS dscp DSCP/TOS port-based Portbasiert Switch(config)# qos priority dscp Switch# show qos priority QoS Priority Mode: DSCP

QoS-Einstellung (Fortsetzung)	
Anzeige – Port-Prioritätseinstellung (Port-Standardpriorität)	Switch# show qos port-priority Port Default Priority : Port Priority Queue -----+---- 1 7 2 0 3 0 4 0 5 0 ……... 205 0 26 0 27 0 28 0
CoS-Warteschlangenzuordnung	
Format	Switch(config)# qos cos-map PRIORITY Priorität zuweisen (höchste ist 3) Switch(config)# qos cos-map 1 QUEUE Warteschlange zuweisen (0–3) ***Anmerkung:*** *Format: qos cos-map Priorität_Wert Warteschlange_Wert.*
CoS 0 zu Warteschlange 1 zuordnen	Switch(config)# qos cos-map 0 1 The CoS to queue mapping is set ok.
CoS 1 zu Warteschlange 0 zuordnen	Switch(config)# qos cos-map 1 0 The CoS to queue mapping is set ok.
CoS 2 zu Warteschlange 0 zuordnen	Switch(config)# qos cos-map 2 0 The CoS to queue mapping is set ok.
CoS 3 zu Warteschlange 1 zuordnen	Switch(config)# qos cos-map 3 1 The CoS to queue mapping is set ok.
CoS 4 zu Warteschlange 2 zuordnen	Switch(config)# qos cos-map 4 2 The CoS to queue mapping is set ok.
CoS 5 zu Warteschlange 2 zuordnen	Switch(config)# qos cos-map 5 2 The CoS to queue mapping is set ok.
CoS 6 zu Warteschlange 3 zuordnen	Switch(config)# qos cos-map 6 3 The CoS to queue mapping is set ok.
CoS 7 zu Warteschlange 3 zuordnen	Switch(config)# qos cos-map 7 3 The CoS to queue mapping is set ok.

CoS-Warteschlangenzuordnung (Fortsetzung)	
Anzeige – CoS-Warteschlangenzu-ordnung	Switch# sh qos cos-map CoS to Queue Mapping : CoS Queue ---- + ------ 0 1 1 0 2 0 3 1 4 2 5 2 6 3 7 3
DSCP-Warteschlangenzuordnung	
Format	Switch(config)# qos dscp-map <0–63> Priorität zuweisen (höchste ist 63) Switch(config)# qos dscp-map 0 <0–3> Warteschlange zuweisen (0–3) **Format**: qos dscp-map Priorität_Wert Warteschlange_Wert.
DSCP 0 zu Warteschlange 1 zuordnen	Switch(config)# qos dscp-map 0 1 The TOS/DSCP to queue mapping is set ok.
Anzeige – DSCP-Warteschlangenzu-ordnung	Switch# show qos dscp-map DSCP to Queue Mapping : (dscp = d1 d2) d2| 0 1 2 3 4 5 6 7 8 9 d1 | -----+---------- 0 | 1 1 1 1 1 1 1 1 0 0 1 | 0 0 0 0 0 0 0 0 0 0 2 | 0 0 0 0 1 1 1 1 1 1 3 | 1 1 2 2 2 2 2 2 2 2 4 | 2 2 2 2 2 2 2 2 3 3 5 | 3 3 3 3 3 3 3 3 3 3 6 | 3 3 3 3

5.11. Multicast-Filterung (CLI)

Für die Multicast-Filterung verwendet der ICRL-M die IGMP-Snooping-Technologie (Internet Group Management Protocol). IGMP ist ein Internetprotokoll, mit dem das Internetgerät seine Multicast-Gruppenmitgliedschaft an benachbarte Router melden kann. Multicasting ermöglicht es einem Computer im Internet, Daten an eine Vielzahl von anderen Computern zu senden, die sich selbst als interessiert am Empfang der Daten des ursprünglichen Computers identifiziert haben.

Multicasting ist nützlich für Anwendungen wie das Aktualisieren der Adressbücher von mobilen Computerbenutzern vor Ort, das Versenden von Newslettern an eine Verteilerliste und das Übertragen von Streaming-Medien an eine Zielgruppe, die bei dem Ereignis durch Einrichten der Multicast-Gruppenmitgliedschaft einschaltet.

IGMP-Snooping verwaltet den Multicast-Datenverkehr durch die Verwendung von Switches, Routern und Hosts, die IGMP unterstützen. Durch Aktivieren von IGMP-Snooping können die Ports IGMP-Abfragen erkennen, Pakete melden und Multicast-Datenverkehr über den Switch verwalten. IGMP verfügt über drei grundlegende Meldungstypen, wie in der folgenden Tabelle dargestellt.

Meldung	
Abfrage	Eine vom Querier (IGMP-Router oder -Switch) gesendete Nachricht, die eine Antwort von jedem Host anfordert, der zu der Multicast-Gruppe gehört
Melden	Eine Nachricht, die von einem Host an den Querier gesendet wird, um anzugeben, dass der Host ein Mitglied der in der Meldenachricht angegebenen Gruppe sein möchte oder ist
Gruppe verlassen	Eine Nachricht, die von einem Host an den Querier gesendet wird, um anzugeben, dass die Mitgliedschaft des Hosts in einer bestimmten Multicast-Gruppe beendet wurde

Sie können die Funktionen **IGMP Snooping** und **IGMP Query** aktivieren. In diesem Abschnitt werden die Informationen der IGMP-Snooping-Funktion erläutert, einschließlich der VIDs und Mitgliederports verschiedener Multicast-Gruppen und der IP-Multicast-Adressen im Bereich von 224.0.0.0 bis 239.255.255.255.

Sie können optional die Web-Benutzerschnittstelle für die Konfiguration verwenden. Informationen hierzu finden Sie unter *Multicast-Filterung* auf Seite 108.

Die folgende Tabelle enthält detaillierte Informationen zu Befehlszeilen für die Multicast-Filterkonfiguration.

IGMP-Snooping	
IGMP-Snooping – Global	Switch(config)# ip igmp snooping IGMP snooping is enabled globally. Specify on which vlans IGMP snooping enables
IGMP-Snooping – VLAN	Switch(config)# ip igmp snooping vlan VLANLIST Liste zulässiger VLANs all Alle vorhandenen VLANs Switch(config)# ip igmp snooping vlan 1-2 IGMP snooping is enabled on VLAN 1-2.
IGMP Snooping deaktivieren – Global	Switch(config)# no ip igmp snooping IGMP snooping is disabled globally ok.
IGMP Snooping deaktivieren – VLAN	Switch(config)# no ip igmp snooping vlan 3 IGMP snooping is disabled on VLAN 3.

IGMP-Snooping (Fortsetzung)	
Anzeige – IGMP-Snooping-Einstellungen	Switch# sh ip igmp interface vlan1 enabled: Yes version: IGMPv1 query-interval; 125s query-max-response-time: 10s Switch# sh ip igmp snooping IGMP snooping is globally enabled Vlan1 is IGMP snooping enabled Vlan2 is IGMP snooping enabled Vlan3 is IGMP snooping disabled
Anzeige – IGMP-Tabelle	Switch# sh ip igmp snooping multicast all VLAN IP Address Type Ports ---- --------------- ------- ------------------------ 1 239.192.8.0 IGMP gi6, 1 239.255.255.250 IGMP gi6,
IGMP-Abfrage	
IGMP-Abfrage – V1	Switch(config)# int vlan 1 Switch(config-if)# ip igmp v1
IGMP-Abfrage – V2	Switch(config)# int vlan 1 Switch(config-if)# ip igmp
IGMP-Abfrage – Version	Switch(config-if)# ip igmp version 1 Switch(config-if)# ip igmp version 2

IGMP-Abfrage – Intervall	Switch(config)# int vlan 1 (Zu Management-VLAN gehen)
	Switch(config-if)# ip igmp
	Switch(config-if)# ip igmp query-interval 60 (Abfrageintervall auf 60 Sekunden ändern, Standardwert sind 125 Sekunden)

IGMP-Abfrage – Max. Antwortzeit	Switch(config)# int vlan 1 (Zu Management-VLAN gehen)
	Switch(config-if)# ip igmp
	Switch(config-if)# ip igmp query-max-response-time 15 (Max. Abfrageantwortzeit auf 15 Sekunden ändern, Standardwert sind 10 Sekunden)

Disable	Switch(config)# int vlan 1 Switch(config-if)# ip igmp

IGMP-Abfrage (Fortsetzung)	
Anzeige	Switch# sh ip igmp interface vlan1 enabled: Yes version: IGMPv2 query-interval: 125s query-max-response-time: 10s Switch# show running-config …. ! interface vlan1 ip address 192.168.250.17/24 ip igmp no shutdown ! …….
Unbekanntes Multicast	
„Unknown Multicast“ an Abfrageports senden	Switch(config)# ip igmp snooping source-only-learning IGMP Snooping Source-Only-Learning enabled
„Unknown Multicast“ an alle Ports senden	Switch(config)# no ip igmp snooping source-only-learning IGMP Snooping Source-Only-Learning disabled Switch(config)# no mac-address-table multicast filtering Flooding unknown multicast addresses ok!
Alle Unknown Multicasts verwerfen	Switch(config)# mac-address-table multicast filtering Filtering unknown multicast addresses ok!

GMRP-Konfiguration	
GMRP global aktivieren	Switch(config)# gmrp mode enable Gmrp is enabled on the switch!
GMRP global deaktivieren	Switch(config)# gmrp mode disable Gmrp is disabled on the switch!
GMRP an einem Port aktivieren	Switch(config)# gmrp mode enable gi1 Gmrp enabled on port 1 !
GMRP an einem Port deaktivieren	Switch(config)# gmrp mode disable gi2 Gmrp disabled on port 2 !
Anzeige	Switch# sh gmrp GMRP global enabled port 1 : enabled port 2 : enabled port 3 : disabled port 4 : disabled port 5 : disabled port 6 : disabled port 7 : disabled port 8 : disabled port 9 : disabled port 10 : disabled
Filterung erzwingen	
Aktivieren	Switch(config)# mac-address-table force filtering Filtering unknown multicast addresses ok!
Deaktivieren	Switch(config)# no mac-address-table force filtering Flooding unknown multicast addresses ok!

5.12. SNMP (CLI)

Das Simple Network Management Protocol (SNMP) ist ein Protokoll, das für den Austausch von Verwaltungsinformationen zwischen Netzwerkgeräten verwendet wird. SNMP ist Mitglied der TCP/IP-Protokollsuite. Der ICRL-M unterstützt SNMP v1, v2c und V3.

Ein SNMP-verwaltetes Netzwerk besteht aus zwei Hauptkomponenten: Agents und einem Manager. Ein Agent ist ein Management-Softwaremodul, das sich in einem verwalteten Switch befindet. Ein Agent übersetzt die lokalen Verwaltungsinformationen vom verwalteten Gerät in ein SNMP-kompatibles Format. Der Manager ist die Konsole im Netzwerk.

Sie können optional die Web-Benutzerschnittstelle für die Konfiguration verwenden. Informationen hierzu finden Sie unter *SNMP* auf Seite 113.

Die folgende Tabelle enthält detaillierte Informationen über Befehlszeilen für die SNMP-Konfiguration.

SNMP-Community	
Schreibgeschützte Community	Switch(config)# snmp-server community public ro community string add ok
Lese-/Schreib-Community	Switch(config)# snmp-server community private rw community string add ok
SNMP-Trap	
Trap aktivieren	Switch(config)# snmp-server enable trap Set SNMP trap enable ok.
SNMP-Trap-Server-IP ohne spezifischen Community-Namen	Switch(config)# snmp-server host 192.168.250.33 SNMP trap host add OK.
SNMP-Trap-Server-IP mit Version 1 und Community	Switch(config)# snmp-server host 192.168.250.33 version 1 private SNMP trap host add OK. ***Anmerkung:*** *„private“ ist der Community-Name, „version 1“ ist die SNMP-Version.*
SNMP-Trap-Server-IP mit Version 2 und Community	Switch(config)# snmp-server host 192.168.250.33 version 2 private SNMP trap host add OK.
SNMP-Trap deaktivieren	Switch(config)# no snmp-server enable trap Set SNMP trap disable ok.
Anzeige	Switch# sh snmp-server trap SNMP trap: Enabled SNMP trap community: public Switch# show running-config ..... snmp-server community public ro snmp-server community private rw snmp-server enable trap snmp-server host 192.168.250.33 version 2 admin snmp-server host 192.168.250.33 version 1 admin ……..

5.13. Sicherheit (CLI)

Der ICRL-M bietet verschiedene Sicherheitsfunktionen, mit denen Sie Ihre Verbindung schützen können.

Sie können optional die Web-Benutzerschnittstelle für die Konfiguration verwenden. Informationen hierzu finden Sie unter *Sicherheit* auf Seite 117.

Diese Tabelle enthält Informationen über die Befehlszeilen für die Sicherheitskonfiguration.

Schutz von Schnittstellen	
Anzeige	Switch# show service Telnet : Disabled Http : Disabled
Telnet	Switch(config)# service telnet enable
HTTP	Switch(config)# service http enable
Portsicherheit	
MAC-Zugriffsliste hinzufügen	Switch(config)# mac access-list extended NAME Name der Zugriffsliste Switch(config)# mac access-list extended server1 Switch(config-ext-macl)# permit Pakete angeben, die weitergeleitet werden sollen deny Pakete angeben, die abgelehnt werden sollen end Aktuellen Modus beenden und zum aktivierten Modus wechseln exit Aktuellen Modus beenden und zum vorherigen Modus zurückkehren list Befehlsliste anzeigen no Befehl negieren oder Standard wiederherstellen quit Aktuellen Modus beenden und zum vorherigen Modus zurückkehren
IP-Standardzugriffsliste hinzufügen	Switch(config)# ip access-list extended Erweiterte Zugriffsliste standard Standardzugriffsliste Switch(config)# ip access-list standard <1–99> Standard-IP-Zugriffslistennummer <1300–1999> Standard-IP-Zugriffslistennummer (erweiterter Bereich) WORD Name der Zugriffsliste Switch(config)# ip access-list standard 1 Switch(config-std-acl)# deny Pakete angeben, die abgelehnt werden sollen permit Pakete angeben, die weitergeleitet werden sollen end Aktuellen Modus beenden und zum aktivierten Modus wechseln exit Aktuellen Modus beenden und zum vorherigen Modus zurückkehren list Befehlsliste anzeigen no Befehl negieren oder Standard wiederherstellen quit Aktuellen Modus beenden und zum vorherigen Modus zurückkehren remark Kommentar Zugriffslisteneintrag

Portsicherheit (Fortsetzung)	

Erweiterte IP-Zugriffsliste hinzufügen	Switch(config)# ip access-list extended
	  <100–199> Erweiterte IP-Zugriffslistennummer
	  <2000–2699> Erweiterte IP-Zugriffslistennummer (erweiterter Bereich)
	  WORD Name der Zugriffsliste
	Switch(config)# ip access-list extended 100
	Switch(config-ext-acl)#
	  deny Pakete angeben, die abgelehnt werden sollen
	  permit Pakete angeben, die weitergeleitet werden sollen
	  end Aktuellen Modus beenden und zum vorherigen Modus zurückkehren
	  exit Aktuellen Modus beenden und zum vorherigen Modus zurückkehren
	  list Befehlsliste anzeigen
	  no Befehl negieren oder Standard wiederherstellen
	  quit Aktuellen Modus beenden und zum vorherigen Modus zurückkehren
	  remark Kommentar Zugriffslisteneintrag

Beispiel 1: MAC-Zugriffsliste bearbeiten	Switch(config-ext-macl)#permit
	  MACADDR MAC-Quelladresse xxxx.xxxx.xxxx
	  any Beliebige MAC-Quelladresse
	  host Einzelner Quellhost
	Switch(config-ext-macl)#permit host
	  MACADDR MAC-Quelladresse xxxx.xxxx.xxxx
	Switch(config-ext-macl)#permit host 00:0D:81:09:FD:E4 .2233
	  MACADDR MAC-Zieladresse xxxx.xxxx.xxxx
	  any Beliebige MAC-Zieladresse
	  host Einzelner Zielhost
	Switch(config-ext-macl)#permit host 00:0D:81:09:FD:E4 .2233 host
	  MACADDR MAC-Zieladresse xxxx.xxxx.xxxx
	Switch(config-ext-macl)#permit host 00:0D:81:09:FD:E4 .2233 host 00:0D:81:09:FD:E4 .2234
	  [IFNAME] Name der Egress-Schnittstelle
	Switch(config-ext-macl)#permit host 00:0D:81:09:FD:E4 .2233 host 00:0D:81:09:FD:E4 .2234 gi25
	MAC-Regel: Permit/Deny Platzhalter Quell_MAC Platzhalter Ziel_MAC Egress_Schnittstelle.

Portsicherheit (Fortsetzung)	
Beispiel 1: Erweiterte IP-Zugriffsliste bearbeiten	Switch(config)# ip access-list extended 100 Switch(config-ext-acl)#permit ip Jedes Internetprotokoll tcp Transmission Control Protocol udp User Datagram Protocol icmp Internet Control Message Protocol Switch(config-ext-acl)#permit ip A.B.C.D Quelladresse any Beliebiger Quellhost host Einzelner Quellhost Switch(config-ext-acl)#permit ip 192.168.10.1 A.B.C.D Quell-Platzhalterbits Switch(config-ext-acl)#permit ip 192.168.10.1 0.0.0.1 A.B.C.D Zieladresse any Beliebiger Zielhost host Einzelner Zielhost Switch(config-ext-acl)#permit ip 192.168.10.1 0.0.0.1 192.168.10.100 0.0.0.1 [IFNAME] Name der Egress-Schnittstelle Switch(config-ext-acl)#permit ip 192.168.10.1 0.0.0.1 192.168.10.100 0.0.0.1 gi26 ***Anmerkung:*** *Befolgen Sie die folgenden Regeln, um die erweiterte IP-Zugriffsliste zu konfigurieren.* **IP-Regel**: Permit/Deny Quell_IP Platzhalter Ziel_IP Platzhalter Egress_Schnittstelle **TCP-Regel**: Permit/Deny tcp Quell_IP Platzhalter Ziel_IP Platzhalter Jeweilige_Port_Nummer Egress_Schnittstelle **UDP-Regel**: Permit/Deny udp Quell_IP Platzhalter Ziel_IP Platzhalter Jeweilige_Port_Nummer Egress_Schnittstelle **ICMP-Regel**: Permit/Deny icmp Quell_IP Platzhalter Ziel_IP Platzhalter ICMP-Nachrichtentyp ICMP-Nachrichtencode Egress_Schnittstelle
MAC hinzufügen	Switch(config)# mac-address-table static 00:0D:81:09:FD:E4 vlan 1 interface gi1 mac-address-table unicast static set ok!
Portsicherheit	Switch(config)# interface gi1 Switch(config-if)# switchport port-security Disables new MAC addresses learning and aging activities! **Regel:** Fügen Sie zuerst die statische MAC-, VLAN- und Portbindung hinzu und aktivieren Sie dann die Portsicherheit, um neue MAC-Lernvorgänge zu stoppen**.**
Portsicherheit deaktivieren	Switch(config-if)# no switchport port-security Enable new MAC addresses learning and aging activities!
Anzeige	Switch# show mac-address-table static Destination Address Address Type Vlan Destination Port ---------- ---------- ------- ---------- 00:0D:81:09:FD:E4 Static 1 gi1

802.1x	
enable disable	Switch(config)# dot1x system-auth-control Switch(config)# Switch(config)# no dot1x system-auth-control Switch(config)#
authentic-method	Switch(config)# dot1x authentic-method local Lokale Benutzernamen-Datenbank zur Authentifizierung verwenden RADIUS RADIUS-Server (Remote Authentication Dial-In User Service) zur Authentifizierung verwenden Switch(config)# dot1x authentic-method RADIUS Switch(config)#
RADIUS server-ip	Switch(config)# dot1x RADIUS Switch(config)# dot1x RADIUS server-ip 192.168.10.120 key 1234 RADIUS Server Port number NOT given. (default=1812) RADIUS Accounting Port number NOT given. (default=1813) RADIUS Server IP : 192.168.10.120 RADIUS Server Key : 1234 RADIUS Server Port : 1812 RADIUS Accounting Port : 1813 Switch(config)#
RADIUS server-ip	Switch(config)# dot1x RADIUS Switch(config)# dot1x RADIUS server-ip 192.168.10.120 key 1234 RADIUS Server Port number NOT given. (default=1812) RADIUS Accounting Port number NOT given. (default=1813) RADIUS Server IP : 192.168.10.120 RADIUS Server Key : 1234 RADIUS Server Port : 1812 RADIUS Accounting Port : 1813 Switch(config)#
RADIUS secondary-server-ip	Switch(config)# dot1x RADIUS secondary-server-ip 192.168.10.250 key 5678 Port number NOT given. (default=1812) RADIUS Accounting Port number NOT given. (default=1813) Secondary RADIUS Server IP : 192.168.10.250 Secondary RADIUS Server Key : 5678 Secondary RADIUS Server Port : 1812 Secondary RADIUS Accounting Port : 1813
Benutzername/Kennwort für Authentifizierung	Switch(config)# dot1x username Pepperl+Fuchs passwd Pepperl+Fuchs vlan 1

5.14. Warnungen (CLI)

Der ICRL-M bietet verschiedene Arten von Warnfunktionen, mit denen Sie den Status der angeschlossenen Geräte oder Änderungen in Ihrem Netzwerk remote überwachen können. Zu den Funktionen gehören Fehlerrelais, Systemprotokoll und SMTP-E-Mail-Warnung.

Sie können optional die Web-Benutzerschnittstelle für die Konfiguration verwenden. Informationen hierzu finden Sie unter *Warnung* auf Seite 143.

Diese Tabelle enthält detaillierte Informationen über die Befehlszeilen der Warnungskonfiguration.

Fehlerrelaisausgang	
Relaisausgang	Switch(config)# relay 1 di DI-Status dry Trockene Ausgabe ping Ping-Fehler port Portverbindungsfehler power Stromausfall ring Ringfehler
DI-Status	Switch(config)# relay 1 di 1 DI-Nummer Switch(config)# relay 1 di 1 high Hoch ist anormal low Niedrig ist anormal Switch(config)# relay 1 di 1 high
Trockene Ausgabe	Switch(config)# relay 1 dry <0–65535> Einschaltdauer in Sekunden Switch(config)# relay 1 dry 5 <0–65535> Ausschaltdauer in Sekunden Switch(config)# relay 1 dry 5 5
Ping-Fehler	Switch(config)# relay 1 ping 192.168.250.33 <cr> reset Gerät zurücksetzen Switch(config)# relay 1 ping 192.168.250.33 reset <1–65535> Rücksetzzeit Switch(config)# relay 1 ping 192.168.250.33 reset 60 <0–65535> Wartezeit für Neuversuch Switch(config)# relay 1 ping 192.168.250.33 reset 60 60
Portverbindungsfehler	Switch(config)# relay 1 port PORTLIST Portliste Switch(config)# relay 1 port gi1-5
Stromausfall	Switch(config)# relay 1 power <1–2> Power-ID any Jeder Stromausfall aktiviert Relais Switch(config)# relay 1 power 1 Switch(config)# relay 1 power 2
Ringfehler	Switch(config)# relay 1 ring

Fehlerrelaisausgang (Fortsetzung)	
Relais deaktivieren	Switch(config)# no relay 1-2 Relais-ID Switch(config)# no relay 1 <cr>
Anzeige	Switch# show relay 1 Relaisausgangstyp: Port Link Port : 1, 2, 3, 4
Ereignisauswahl	Switch(config)# warning-event coldstart Switch-Kaltstartereignis warmstart Switch-Warmstartereignis linkdown Ereignis für unterbrochene Switchverbindung linkup Ereignis für verfügbare Switchverbindung authentication Ereignis für Authentifizierungsfehler ring Ereignis für Ringwechsel time-sync Ereignis für Zeitsynchronisierungsereignis
Beispiel: Kaltstartereignis	Switch(config)# warning-event coldstart Set cold start event enable ok.
Beispiel: Ereignis für verfügbare Verbindung	Switch(config)# warning-event linkup [IFNAME] Schnittstellenliste, Bsp.: Switch(config)# warning-event linkup Set 5 link up event enable ok.
Anzeige	Switch# show warning-event Warning Event: Cold Start: Enabled Warm Start: Disabled Authentication Failure: Disabled Link Down: gi4-5 Link Up: gi4-5 Power Failure: Ring: Disabled Fault Relay: Disabled Time synchronize Failure: Disabled SFP: Enabled DI: Disabled DHCP Snooping: Disabled DAI Statistics Changed: Disabled IPSG Statistics Changed: Disabled Port Security: Disabled

SysLog-Konfiguration	
Lokaler Modus	Switch(config)# log syslog local
Servermodus	Switch(config)# log syslog remote 192.168.250.33
Beides	Switch(config)# log syslog local Switch(config)# log syslog remote 192.168.250.33
Deaktivieren	Switch(config)# no log syslog local
SMTP-Konfiguration	
SMTP aktivieren	Switch(config)# smtp-server enable email-alert SMTP Email Alert set enable ok.
Absender-E-Mail	Switch(config)# smtp-server server 192.168.250.100 ACCOUNT SMTP-Server-E-Mail-Konto, Bsp.: Admin@Pepperl+Fuchs.com Switch(config)# smtp-server server 192.168.250.100 admin@Pepperl+Fuchs.com SMTP Email Alert set Server: 192.168.250.100, Account: admin@Pepperl+Fuchs.com ok.
Empfänger-E-Mail	Switch(config)# smtp-server receipt 1 abc@Pepperl+Fuchs.com SMTP Email Alert set receipt 1: abc@Pepperl+Fuchs.com ok.
Authentifizierung mit Benutzername und Kennwort	Switch(config)# smtp-server authentication username admin password admin SMTP Email Alert set authentication Username: admin, Password: admin ***Anmerkung:*** *Sie können dem Benutzernamen und dem Kennwort eine Zeichenfolge zuweisen.*
SMTP deaktivieren	Switch(config)# no smtp-server enable email-alert SMTP Email Alert set disable ok.
Authentifizierung deaktivieren	Switch(config)# no smtp-server authentication SMTP Email Alert set Authentication disable ok.
Anzeige	Switch# sh smtp-server SMTP Email Alert is Enabled Server: 192.168.250.100, Account: admin@Pepperl+Fuchs.com Authentication: Enabled Username: admin, Password: admin SMTP Email Alert Receipt: Receipt 1: abc@Pepperl+Fuchs.com Receipt 2: Receipt 3: Receipt 4:

5.15. Überwachung und Diagnose (CLI)

Der ICRL-M bietet verschiedene Arten von Funktionen, mit denen Sie den Status des Switches überwachen oder Probleme mit dem Switch untersuchen können. Zu den Funktionen gehören MAC-Adresstabelle, Portstatistiken, Portspiegelung, Ereignisprotokoll und Ping.

Sie können optional die Web-Benutzerschnittstelle für die Konfiguration verwenden. Informationen hierzu finden Sie unter *Überwachung und Diagnose* auf Seite 149.

Diese Tabelle enthält detaillierte Informationen über die Befehlszeilen der Überwachungs- und Diagnosekonfiguration.

MAC-Adresstabelle	
Aging-Zeit	Switch(config)# mac-address-table aging-time 350 mac-address-table aging-time set ok! ***Anmerkung:*** *Der voreingestellte Aging-Timeout-Wert ist 300.*
Statische Unicast-MAC-Adresse hinzufügen	Switch(config)# mac-address-table static 00:0D:81:09:FD:E4 vlan 1 interface gigabitethernet5 mac-address-table ucast static set ok! **Regel**: mac-address-table static MAC_Adresse VLAN VID interface Schnittstelle_Name
Multicast-MAC-Adresse hinzufügen	Switch(config)# mac-address-table multicast 00:0D:81:09:FD:E4 vlan 1 interface gi3-4 Adds an entry in the multicast table ok! **Regel**: mac-address-table multicast MAC_Adresse VLAN VID Schnittstellen_Liste Schnittstelle_Name/Bereich
MAC-Adresstabelle anzeigen – Alle Typen	Switch# show mac-address-table ***** UNICAST MAC ADDRESS ***** Destination Address Address Type Vlan Destination Port ---------- ---------- ---- ---------- 00:0D:81:09:FD:E4 .ca3b Dynamic 1 gi1 00:0D:81:09:FD:E4 .0386 Dynamic 1 gi2 00:0D:81:09:FD:E4 .0101 Static 1 gi3 00:0D:81:09:FD:E4 .0102 Static 1 gi3 00:0D:81:09:FD:E4 .0100 Management 1 ***** MULTICAST MAC ADDRESS ***** Vlan Mac Address COS Status Ports ---- ---------- ---- ------- ---------- 1 00:0D:81:09:FD:E4 .0800 0 gi6 1 00:0D:81:09:FD:E4 .fffa 0 gi4,gi6
MAC-Adresstabelle anzeigen – Dynamische erlernte MAC-Adressen	Switch# show mac-address-table dynamic Destination Address Address Type Vlan Destination Port ---------- ---------- ---- ---------- 00:0D:81:09:FD:E4 .ca3b Dynamic 1 gi4 00:0D:81:09:FD:E4 .0386 Dynamic 1 gi6

MAC-Adresstabelle (Fortsetzung)	
MAC-Adresstabelle anzeigen – Multicast-MAC-Adressen	Switch# show mac-address-table multicast Vlan Mac Address COS Status Ports ---- --------------- ---- ------- --------------------------- 1 00:0D:81:09:FD:E4 .0800 0 gi5-6 1 00:0D:81:09:FD:E4 .fffa 0 gi3,gi5-6
MAC-Adresstabelle anzeigen – Statische MAC-Adressen	Switch# show mac-address-table static Destination Address Address Type Vlan Destination Port ------------------- --------------- ------- ------------------- 00:0D:81:09:FD:E4 Static 1 gi4 000D.8109.FDE5 Static 1 gi5
Aging-Timeout-Zeit anzeigen	Switch# show mac-address-table aging-time the mac-address-table aging-time is 300 sec.
Portstatistiken	
Portstatistiken	Switch# show rmon statistics gi4 (select interface) Interface gigabitethernet4 is enable connected, which has Inbound: Good Octets: 178792, Bad Octets: 0 Unicast: 598, Broadcast: 1764, Multicast: 160 Pause: 0, Undersize: 0, Fragments: 0 Oversize: 0, Jabbers: 0, Discards: 0 Filtered: 0, RxError: 0, FCSError: 0 Outbound: Good Octets: 330500 Unicast: 602, Broadcast: 1, Multicast: 2261 Pause: 0, Deferred: 0, Collisions: 0 SingleCollision: 0, MultipleCollision: 0 ExcessiveCollision: 0, LateCollision: 0 Filtered: 0, FCSError: 0 Number of frames received and transmitted with a length of: 64: 2388, 65to127: 142, 128to255: 11 256to511: 64, 512to1023: 10, 1024toMaxSize: 42
Portspiegelung	
Portspiegel aktivieren	Switch(config)# mirror en Mirror set enable ok.
Portspiegel deaktivieren	Switch(config)# mirror disable Mirror set disable ok.
Quellport auswählen	Switch(config)# mirror source gi1-2 both Empfangener und gesendeter Datenverkehr rx Empfangener Datenverkehr tx Gesendeter Datenverkehr Switch(config)# mirror source gi1-2 both Mirror source gi1-2 both set ok. ***Anmerkung:*** *Wählen Sie die Quellportliste und den Modus TX/RX/Both aus.*

Portspiegelung (Fortsetzung)	
Zielport auswählen	Switch(config)# mirror destination gi6 Mirror destination gi6 set ok
Anzeige	Switch# show mirror Mirror Status : Enabled Ingress Monitor Destination Port : gi6 Egress Monitor Destination Port : gi6 Ingress Source Ports :gi1,gi2, Egress Source Ports :gi1,gi2,
Ereignisprotokoll	
Anzeige	Switch# show event-log <1>Jan 1 02:50:47 snmpd[101]: Event: Link 4 Down. <2>Jan 1 02:50:50 snmpd[101]: Event: Link 5 Up. <3>Jan 1 02:50:51 snmpd[101]: Event: Link 5 Down. <4>Jan 1 02:50:53 snmpd[101]: Event: Link 4 Up.
Topologieerkennung (LLDP)	
Enable LLDP	Switch(config)# lldp holdtime Haltezeit von LLDP in Sekunden run LLDP aktivieren timer Übertragungsfrequenz von LLDP in Sekunden einstellen Switch(config)# lldp run LLDP is enabled!
LLDP-Timer ändern	Switch(config)# lldp holdtime <10–255> Der gültige Bereich beträgt 10~255. Switch(config)# lldp timer <5-254> Der gültige Bereich beträgt 5~254.
Ping	
IP anpingen	Switch# ping 192.168.11.14 PING 192.168.11.14 (192.168.11.14): 56 data bytes 64 bytes from 192.168.11.14: icmp_seq=0 ttl=128 time=0.0 ms 64 bytes from 192.168.11.14: icmp_seq=1 ttl=128 time=0.0 ms 64 bytes from 192.168.11.14: icmp_seq=2 ttl=128 time=0.0 ms 64 bytes from 192.168.11.14: icmp_seq=3 ttl=128 time=0.0 ms 64 bytes from 192.168.11.14: icmp_seq=4 ttl=128 time=0.0 ms --- 192.168.11.14 ping statistics --- packets transmitted, 5 packets received, 0% packet loss round-trip min/avg/max = 1.3/1.3/1.4 ms

5.16. Speichern im Flash (CLI)

Mit **Save Configuration** können Sie jede Konfiguration speichern, die Sie gerade am Flash vorgenommen haben. Wenn der Switch ausgeschaltet wird, ohne die Konfiguration zu speichern, gehen die neuen Einstellungen verloren.

Im Flash speichern	
Im Flash speichern	SWITCH# write Building Configuration… [OK] Switch# copy running-config startup-config Building Configuration... [OK]

5.17. Abmelden (CLI)

Die CLI-Verbindung meldet sich aus dem Terminalkonfigurationsmodus ab, wenn Sie 30 Sekunden lang keinen Befehl eingeben.

Abmelden	
Abmelden	SWITCH> exit SWITCH# exit

5.18. Service (CLI)

Mit dem Servicebefehl können Sie HTTP und Telnet deaktivieren.

Anmerkung: *Für den Servicebefehl ist keine Web-Benutzerschnittstellenseite vorhanden.*

Service	
HTTP deaktivieren	Switch(config)# service http disable Switch(config)#
HTTP aktivieren	Switch(config)# service http enable Switch(config)#
Telnet deaktivieren	Switch(config)# service telnet disable Switch(config)#
Telnet aktivieren	Switch(config)# service telnet enable Switch(config)#

6. Vollständige CLI-Liste

In diesem Abschnitt finden Sie eine vollständige Liste der RocketLinx ICRL-M-Befehle mit den unterstützenden Optionen:

- *User EXEC-Modus*
- *Privileged EXEC-Modus* auf Seite 225
- *Global Configuration-Modus* auf Seite 232
- *Port Interface Configuration-Modus* auf Seite 240
- *VLAN Interface Configuration-Modus* auf Seite 243

6.1. *User EXEC*-Modus

Weitere Informationen zum Zugriff auf den *User EXEC*-Modus finden Sie unter *User EXEC-Modus* auf Seite 224.

```
ICRL-M> list
  enable
  exit
  list
  ping A.B.C.D
  ping WORD
  ping X:X::X:X
  quit
  show gvrp statistics [IFNAME]
  show ip forwarding
  show ip route
  show ip route A.B.C.D
  show ip route A.B.C.D/M
  show ip route supernets-only
  show memory
  show users
  show version
  telnet WORD
  telnet WORD PORT
  traceroute WORD
```

6.2. *Privileged EXEC*-Modus

Weitere Informationen zum Zugriff auf den *Privileged EXEC*-Modus finden Sie unter *Privileged EXEC-Modus* auf Seite 225.

ICRL-M# list
archive download-boot /overwrite scp ACCOUNT PASSWORD IMAGE IPADDRESS [PORT]
archive download-boot /overwrite sftp ACCOUNT PASSWORD IMAGE IPADDRESS [PORT]
archive download-boot /overwrite tftp IPADDRESS IMAGE
archive download-sw /overwrite scp ACCOUNT PASSWORD IMAGE IPADDRESS [PORT]
archive download-sw /overwrite sftp ACCOUNT PASSWORD IMAGE IPADDRESS [PORT]
archive download-sw /overwrite tftp IPADDRESS IMAGE
clear erps statistics [0–31]
clear event-log
clear gvrp statistics [IFNAME]
clear ip arp inspection statistics interface [IFNAME]
clear ip arp inspection statistics vlan [VLANID]
clear ip dhcp snooping binding (all|dynamic|static)
clear ip dhcp snooping statistics
clear lacp counters
clear mac-address-table dynamic
clear mac-address-table dynamic address MACADDR
clear mac-address-table dynamic interface IFNAME
clear mac-address-table dynamic vlan VLANID
clear mac-address-table security interface IFNAME
clear redundant-ring statistics [0–31]
clear rmon statistics [IFNAME]
clear spanning-tree counters
clear spanning-tree counters interafce IFNAME
clear spanning-tree detected-protocols
clear spanning-tree detected-protocols interface IFNAME
clock set TIME MONTH DAY YEAR
configure terminal
copy running-config startup-config
copy sftp: URL startup-config ACCOUNT PASSWD
copy startup-config sftp: URL ACCOUNT PASSWD
copy startup-config tftp: URL
copy tftp: URL (ssh-dss|ssh-rsa)
copy tftp: URL ssl-cert
copy tftp: URL startup-config
debug cfm (pdu|trace|debug|all)
debug dot1x all
debug dot1x errors

debug dot1x events
debug dot1x packets
debug dot1x registry
debug dot1x state-machine
debug erps (pdu|trace|debug|all) <0–31>
debug gmrp
debug gvrp (all|rcv|tx|gvrp_event|vlan_event)
debug ip arp inspection
debug ip dhcp (all|event)
debug ip dhcp snooping
debug ip dhcp snooping packet
debug ip igmp
debug ip igmp snooping (all|group|management|router|timer)
debug l2 mac (all|trace|debug)
debug lacp (all|event|fsm|misc|packet)
debug lldp
debug mirror
debug misc [type] [sub]
debug proto pdu
debug qos
debug rate-limit
debug redundant-ring (pdu|trace|debug|rapid-dual-homing|rstp|multi-ring|all) <0–31>
debug snmp
debug spanning-tree (all|bpdu|config|events|general|root|sync|tc)
debug sw-rate-limit get (IFLIST|all) <0–64>
debug sw-rate-limit ioctl_dump
debug sw-rate-limit pkt_dump
debug sw-rate-limit set (IFLIST|all) <0–64> <0–1000>
debug sw-rate-limit set (IFLIST|all) <0–64> off
debug system hardware led mode <0–100>
debug system hardware relay mode <0–100>
debug system info
debug system meminfo
debug trunk
debug vlan (all|trace|debug)
disable
dot1x initialize interface IFNAME
dot1x reauthenticate interface IFNAME
end
exit
list
mac access-group dump <1-1536>

mac access-group show
no debug cfm
no debug dot1x all
no debug dot1x errors
no debug dot1x events
no debug dot1x packets
no debug dot1x registry
no debug dot1x state-machine
no debug erps <0–31>
no debug gmrp
no debug gvrp (all|rcv|tx|gvrp_event|vlan_event)
no debug ip arp inspection
no debug ip dhcp (all|event)
no debug ip dhcp snooping
no debug ip dhcp snooping packet
no debug ip igmp
no debug ip igmp snooping (all|group|management|router|timer)
no debug l2 mac (all|trace|debug)
no debug lacp (all|event|fsm|misc|packet)
no debug lldp
no debug mirror
no debug proto
no debug qos
no debug rate-limit
no debug redundant-ring <0–31>
no debug snmp
no debug spanning-tree (all|bpdu|config|events|general|root|sync|tc)
no debug sw-rate-limit ioctl_dump
no debug sw-rate-limit pkt_dump
no debug system hardware led mode
no debug trunk
no debug vlan (all|trace|debug)
no pager
pager
ping A.B.C.D
ping WORD
ping X:X::X:X
quit
read ip dhcp snooping
reboot
reload default-config file
reload default-ssh file

reload default-ssl file
show acceptable frame type [IFNAME]
show arp access-list [ARP_ACL_NAME]
show auth method list
show auth radius
show auth tacacs+
show cfm database
show cfm domain [NAME]
show clock
show clock summer-time
show clock timezone
show debugging dot1x
show debugging gvrp
show debugging ip dhcp
show debugging ip igmp
show debugging ip igmp snooping
show debugging lacp
show debugging snmp
show debugging spanning-tree
show dot1q-tunnel
show dot1x
show dot1x all
show dot1x authentic-method
show dot1x info
show dot1x interface IFNAME
show dot1x radius
show dot1x statistics interface IFNAME
show dot1x username
show dot1x username mapping
show erps [0–31]
show erps instance
show ethernet-ip
show event-log
show garp timer [IFNAME]
show gmrp
show gvrp configuration [IFNAME]
show gvrp portstate IFNAME VID
show hardware led
show hardware mac
show ingress filtering [IFNAME]
show interface [IFNAME]
show interface vlan [VLANID]

show ip access-group [INTERFACE]
show ip access-list
show ip access-list (<1–99>|<100–199>|<1300–1999>|<2000–2699>|WORD)
show ip arp inspection interface [IFNAME]
show ip arp inspection statistics interface [IFNAME]
show ip arp inspection statistics vlan [VLANID]
show ip arp inspection statistics-checking
show ip arp inspection vlan [VLANID]
show ip dhcp relay
show ip dhcp server
show ip dhcp server statistics
show ip dhcp snooping
show ip dhcp snooping binding
show ip dhcp snooping database write-delay
show ip forwarding
show ip igmp
show ip igmp group
show ip igmp interface IFNAME
show ip igmp query-interval
show ip igmp query-max-response-time
show ip igmp snooping
show ip igmp snooping multicast (dynamic|user|all) [VLANLIST]
show ip igmp snooping multicast count
show ip igmp snooping vlan (VLANLIST|all)
show ip igmp timers
show ip igmp version
show ip route
show ip route A.B.C.D
show ip route A.B.C.D/M
show ip route supernets-only
show ip verify source checking period
show ip verify source interface [IFNAME]
show ipv6 neighbour
show ipv6 route
show l2_interface [IFNAME]
show lacp counters [GROUPID]
show lacp group [1–8]
show lacp internal [1–8]
show lacp neighbor [1–8]
show lacp port-setting [IFNAME]
show lacp system-id
show lacp system-priority

show lldp
show lldp neighbors
show lldp statistics
show mac access-group [INTERFACE]
show mac access-list [WORD]
show mac-address-table
show mac-address-table aging-time
show mac-address-table dynamic
show mac-address-table dynamic address MACADDR
show mac-address-table dynamic interface IFNAME
show mac-address-table dynamic vlan VLANID
show mac-address-table multicast
show mac-address-table multicast MACADDR vlan VLANID
show mac-address-table multicast filtering
show mac-address-table security
show mac-address-table static
show mac-address-table static address MACADDR
show mac-address-table static interface IFNAME
show mac-address-table static vlan VLANID
show memory
show mirror
show modbus
show nameserver
show ntp associations
show port-security interface [IFNAME]
show process
show process backup
show ptp
show qos cos-map
show qos dscp-map
show qos port-priority
show qos queue-sched
show qos trust-mode
show rate-limit egress [IFNAME]
show rate-limit ingress [IFNAME]
show redundant-ring [0-31]
show relay 1
show relay 1 status
show rmon statistics [IFNAME]
show running-config
show service
show sfp

show sfp ddm
show smtp-server
show smtp-server authentication
show smtp-server email-alert
show smtp-server receipt
show smtp-server server
show snmp-server community
show snmp-server contact
show snmp-server host
show snmp-server info
show snmp-server location
show snmp-server name
show snmp-server trap
show snmp-server user
show spanning-tree active
show spanning-tree interface IFNAME
show spanning-tree mst
show spanning-tree mst <0–15>
show spanning-tree mst <0–15> interface IFNAME
show spanning-tree mst configuration
show spanning-tree mst interface IFNAME
show spanning-tree mst root
show spanning-tree summary
show startup-config
show storm-control [IFNAME]
show tftp
show trunk group [1–8]
show trunk load-balance group [1–8]
show users
show version
show vlan
show vlan (static|dynamic) [VLANID]
show vlan VLANID
show vlan dot1q-tunnel mapping
show vlan management
show vlan name VLANAME
show vlan private-vlan
show vlan private-vlan port-list
show vlan private-vlan type
show warning-event
telnet WORD
telnet WORD PORT

traceroute WORD
write
write file
write ip dhcp snooping
write memory
write terminal

6.3. *Global Configuration*-Modus

Weitere Informationen zum Zugriff auf den *Global Configuration*-Modus finden Sie unter *Global Configuration-Modus* auf Seite 232.

ICRL-M(config)# list
access-list test
arp access-list WORD
auth order <1–3>
auth radius server A.B.C.D key RADIUS_KEY [PORT]
auth tacacs+ (primary|secondary) server A.B.C.D <1–65535>
auth tacacs+ (primary|secondary) server secretkey KEY
auth tacacs+ authen_type (ascii|pap|chap)
auth tacacs+ timeout <1–60>)
cfm create domain string NMAE md-level <0–7>
cfm delete domain NAME
cfm domain NAME add association string NAME vlan <1–4094>
cfm domain NAME association NAME port IFNAME (add|delete) remote-mep <1–8191>
cfm domain NAME association NAME port IFNAME add end-point down <1–8191>
cfm domain NAME association NAME port IFNAME delete end-point down
cfm domain NAME association NAME transmit-interval (1000|10000|60000|600000)
cfm domain NAME delete association NAME
cfm group <0–255> rmep <1–8191>
clock set TIME MONTH DAY YEAR
clock summer-time (enable|disable)
clock summer-time <1–5> <0–6> <1–12> START_TIME <1–5> <0–6> <1–12> END_TIME
clock timezone (01|02|03|04|05|06|07|08|09|10|11|12|13|14|15|16|17|18|19|20|21|22|23|24|25|26|27|28|29|30|31|32|33|34|35|36|37|38|39|40|41|42|43|44|45|46|47|48|49|50|51|52|53|54|55|56|57|58|59|60|61|62|63|64|65|66|67|68|69|70|71|72|73|74)
default dot1x system-auth-control
default gvrp configuration
default ip igmp snooping
dot1x authentic-method (radius|local)
dot1x radius secondary-server-ip A.B.C.D key RADIUS_KEY [PORT] [PORT]
dot1x radius server-ip A.B.C.D key RADIUS_KEY [PORT] [PORT]

dot1x system-auth-control
dot1x username WORD passwd WORD vlan <1–4094>
end
erps <0–31>
erps instance (enable|disable)
erps instance <0–15> vlan VLANMAP
ethernet-ip run
exit
gmrp mode (enable|disable)
gmrp mode (enable|disable) IFNAME
gvrp mode (enable|disable)
gvrp mode (enable|disable) IFNAME
gvrp registration (normal|fixed|forbidden) IFNAME
hostname .DWORD
interface IFNAME
interface vlan VLAN-ID
ip access-list extended (<100–199>|<2000–2699>)
ip access-list extended WORD
ip access-list standard (<1–99>|<1300–1999>)
ip access-list standard WORD
ip arp inspection filter ARP_ACL_NAME vlan VLANID
ip arp inspection gw-ip A.B.C.D vlan VLANID
ip arp inspection gw-ip verify vlan VLANID
ip arp inspection statistics-checking <1–60>
ip arp inspection vlan VLANID
ip dhcp snooping
ip dhcp snooping binding MACADDR vlan VLANID A.B.C.D interface IFNAME
ip dhcp snooping database write-delay <0–86400>
ip dhcp snooping verify mac-address
ip dhcp snooping vlan <1–4094>
ip forwarding
ip igmp snooping
ip igmp snooping immediate-leave
ip igmp snooping immediate-leave vlan (VLANLIST|all)
ip igmp snooping last-member-query-interval TIMEVALUE
ip igmp snooping last-member-query-interval TIMEVALUE vlan (VLANLIST|all)
ip igmp snooping source-only-learning vlan (VLANLIST|all)
ip igmp snooping vlan (VLANLIST|all)
ip route A.B.C.D A.B.C.D (A.B.C.D|INTERFACE)
ip route A.B.C.D/M (A.B.C.D|INTERFACE)
ip source binding MACADDR vlan VLANID A.B.C.D interface IFNAME
ip verify source checking period <1–60>

ipv6 route X:X::X:X/M (X:X::X:X|INTERFACE)
lacp group <1–8> IFLIST
lacp system-priority <1–65535>
list
lldp holdtime <10–255>
lldp run
lldp timer <5–254>
log stdout
log syslog local
log syslog remote A.B.C.D
mac access-list extended NAME
mac-address-table aging-time TIMEVALUE
mac-address-table multicast MACADDR vlan VLANID interface IFLIST
mac-address-table multicast filtering vlan (VLANLIST|all)
mac-address-table security MACADDR vlan VLANID interface IFNAME
mac-address-table static MACADDR vlan VLANID interface IFNAME
mirror (enable|disable)
mirror destination IFNAME
mirror source IFLIST (rx|tx|both)
modbus (enable|disable)
modbus idle-timeout <500–3000>
modbus master <1–20>
modbus port <1–65535>
nameserver A.B.C.D
no arp access-list WORD
no auth radius server A.B.C.D
no auth tacacs+ (primary|secondary) server
no cfm domain NAME association NAME transmit-interval
no clock set
no clock summer-time
no clock timezone
no dot1x authentic-method
no dot1x radius secondary-server-ip
no dot1x system-auth-control
no dot1x username WORD
no erps instance <0–15>
no ethernet-ip run
no hostname [HOSTNAME]
no interface IFNAME
no interface vlan VLAN-ID
no ip access-list extended (<100–199>|<2000–2699>|WORD)
no ip access-list standard (<1–99>|<1300–1999>|WORD)

no ip arp inspection filter vlan VLANID
no ip arp inspection gw-ip verify vlan VLANID
no ip arp inspection statistics-checking
no ip arp inspection vlan VLANID
no ip dhcp snooping
no ip dhcp snooping binding MACADDR vlan VLANID A.B.C.D interface IFNAME
no ip dhcp snooping binding table
no ip dhcp snooping verify mac-address
no ip dhcp snooping vlan <1–4094>
no ip forwarding
no ip igmp snooping
no ip igmp snooping immediate-leave
no ip igmp snooping immediate-leave vlan (VLANLIST|all)
no ip igmp snooping last-member-query-interval
no ip igmp snooping last-member-query-interval vlan (VLANLIST|all)
no ip igmp snooping source-only-learning vlan (VLANLIST|all)
no ip igmp snooping vlan (VLANLIST|all)
no ip route A.B.C.D A.B.C.D (A.B.C.D|INTERFACE)
no ip route A.B.C.D A.B.C.D (A.B.C.D|INTERFACE) <1–255>
no ip route A.B.C.D/M (A.B.C.D|INTERFACE)
no ip source binding MACADDR vlan VLANID A.B.C.D interface IFNAME
no ipv6 route X:X::X:X/M (X:X::X:X|INTERFACE)
no lacp group <1–8>
no lacp system-priority
no lldp run
no log stdout
no log syslog local
no log syslog remote
no mac access-list extended NAME
no mac-address-table aging-time
no mac-address-table multicast MACADDR vlan VLANID
no mac-address-table multicast MACADDR vlan VLANID interface IFLIST
no mac-address-table multicast filtering vlan (VLANLIST|all)
no mac-address-table security MACADDR vlan VLANID interface IFNAME
no mac-address-table static MACADDR vlan VLANID interface IFNAME
no mirror destination
no mirror source IFLIST (rx|tx|both)
no nameserver A.B.C.D
no ntp peer (primary|secondary)
no ptp run
no qos cos-map
no qos dscp-map

no qos queue-sched
no relay 1
no relay 1 dry
no relay 1 ping
no relay 1 ping reset
no relay 1 port
no relay 1 power
no relay 1 ring
no relay <1–2> di
no smtp-server authentication
no smtp-server authentication username password
no smtp-server enable email-alert
no smtp-server receipt <1–4>
no smtp-server server
no snmp-server community WORD (ro|rw)
no snmp-server community trap
no snmp-server contact
no snmp-server enable trap
no snmp-server host A.B.C.D [VERSION]
no snmp-server location
no snmp-server name
no snmp-server user WORD v3
no spanning-tree bridge-times
no spanning-tree forward-time
no spanning-tree hello-time
no spanning-tree max-age
no spanning-tree mst MSTMAP priority
no spanning-tree mst configuration
no spanning-tree mst forward-time
no spanning-tree mst hello-time
no spanning-tree mst max-age
no spanning-tree mst max-hops
no spanning-tree priority
no spanning-tree transmission-limit
no trunk group <1–8>
no trunk load-balance group <1–8>
no username NAME
no vlan [VLANID]
no warning-event (coldstart|warmstart)
no warning-event (linkdown|linkup) [IFLIST]
no warning-event authentication
no warning-event dai-statistics-changed

no warning-event dhcp-snooping
no warning-event di
no warning-event di 1
no warning-event fault-relay
no warning-event fault-relay 1
no warning-event ipsg-statistics-changed
no warning-event port-security [IFLIST]
no warning-event power <1–2>
no warning-event ring
no warning-event sfp
no warning-event time-sync
no write-config (daemon|integrated)
ntp peer (enable|disable)
ntp peer (primary|secondary) IPADDRESS
ptp announce-interval (0|1|2|3|4)
ptp announce-receipt-timeout <2–10>
ptp delay-mechanism (E2E|PTP)
ptp domain-number <0–3>
ptp min-pdelay-req-interval INTERVAL
ptp priority1 <0–255>
ptp priority2 <0–255>
ptp run
ptp run preferred-clock
ptp run slave
ptp sync-interval INTERVAL
qos cos-map PRIORITY QUEUE
qos dscp-map DSCP PRIORITY
qos queue-sched drr <0–2032> <0–2032> <0–2032> <0–2032> <0–2032> <0–2032> <0–2032> <0–2032>
qos queue-sched rr
qos queue-sched sp
qos queue-sched wrr <1–10> <1–10> <1–10> <1–10> <1–10> <1–10> <1–10> <1–10>
qos trust-mode (cos|dscp)
redundant-ring <0–31>
relay 1 di 1 (high|low)
relay 1 dry <0–65535> <0–65535>
relay 1 ping WORD
relay 1 ping WORD reset <1–65535> <0–65535>
relay 1 port PORTLIST
relay 1 power <1–2>
relay 1 power any
relay 1 ring
router dhcp

service http (enable|disable)
service https (enable|disable)
service netvision (enable|disable)
service telnet (enable|disable)
sfp ddm (enable|disable) all
sfp eject all
sfp scan all
smtp-server authentication
smtp-server authentication username WORD password WORD
smtp-server enable email-alert
smtp-server receipt <1–4> EMAIL
smtp-server server A.B.C.D ACCOUNT
snmp-server community WORD (ro|rw)
snmp-server community trap WORD
snmp-server contact .DWORD
snmp-server delay <0–1000000>
snmp-server enable trap
snmp-server host A.B.C.D
snmp-server host A.B.C.D version (1|2) [COMMUNITY]
snmp-server location .DWORD
snmp-server name .DWORD
snmp-server user WORD v3 auth (md5|sha) WORD
snmp-server user WORD v3 noauth
snmp-server user WORD v3 priv (md5|sha) WORD des WORD
spanning-tree (enable|disable)
spanning-tree bridge-times <4–30> <6–40> <1–10>
spanning-tree forward-time <4–30>
spanning-tree hello-time <1–10>
spanning-tree max-age <6–40>
spanning-tree mode (stp|rst)
spanning-tree mode mst
spanning-tree mst MSTMAP priority <0–61440>
spanning-tree mst configuration
spanning-tree mst forward-time <4–30>
spanning-tree mst hello-time <1–10>
spanning-tree mst max-age <6–40>
spanning-tree mst max-hops <1–40>
spanning-tree mst sync vlan <1–4094>
spanning-tree pathcost method (long|short)
spanning-tree priority <0–61440>
spanning-tree transmission-limit <1–10>
tftp disable

tftp enable
trunk group <1–8> IFLIST
trunk load-balance group <1–8> (src-mac|dst-mac|src-dst-mac|src-ip|dst-ip|src-dst-ip)
username NAME passwd plaintext PASSWD privilege PRIV
vlan <1–4094>
warning-event (coldstart|warmstart)
warning-event (linkdown|linkup) [IFLIST]
warning-event authentication
warning-event dai-statistics-changed
warning-event dhcp-snooping
warning-event di
warning-event di 1
warning-event fault-relay
warning-event fault-relay 1
warning-event ipsg-statistics-changed
warning-event port-security [IFLIST]
warning-event power <1-2>
warning-event ring
warning-event sfp
warning-event time-sync
write-config (daemon|integrated)

6.4. *Port Interface Configuration*-Modus

Weitere Informationen zum Zugriff auf den *Port Interface Configuration*-Modus finden Sie unter *Port Interface Configuration-Modus* auf Seite 240.

```
ICRL-M(config)# interface gi1
ICRL-M(config-if)# list
 acceptable frame type (all|vlantaggedonly)
 description .LINE
 dot1x admin-control-direction (both|in)
 dot1x default
 dot1x guest-vlan <1–4094>
 dot1x host-mode (single-host|multi-host)
 dot1x mab
 dot1x max-req <1–10>
 dot1x port-control (auto|force-authorized|force-unauthorized)
 dot1x reauthentication
 dot1x timeout (reauth-period|quiet-period|tx-period|supp-timeout|server-timeout) TIMEVALUE
 duplex (half|full)
 end
 ethertype [0x0800–0xFFFF]
 exit
 flowcontrol (off|on)
 garp join-timer <10–10000>
 garp leave-timer <30–30000>
 garp leaveall-timer <150–150000>
 ingress filtering (enable|disable)
 ip access-group (<1–199> |<1300–2699>|WORD) in
 ip arp inspection limit none
 ip arp inspection limit rate <0–65>
 ip arp inspection trust
 ip dhcp snooping trust
 ip verify source port-security (ip|ip-mac)
 lacp port-priority <1–65535>
 lacp timeout (long|short)
 list
 loopback
 mac access-group NAME in
 media-type sfp speed (100|1000)
 mtu <64–9216>
 no description
 no dot1x admin-control-direction
 no dot1x guest-vlan
```

no dot1x host-mode
no dot1x mab
no dot1x max-req
no dot1x port-control
no dot1x reauthentication
no dot1x timeout (reauth-period|quiet-period|tx-period|supp-timeout|server-timeout)
no duplex
no garp join-timer
no garp leave-timer
no garp leaveall-timer
no ip access-group
no ip arp inspection limit
no ip arp inspection trust
no ip dhcp snooping trust
no ip verify source port-security
no lacp port-priority
no lacp timeout
no loopback
no mac access-group
no mtu
no qos priority
no rate-limit egress bandwidth
no rate-limit ingress bandwidth
no shutdown
no spanning-tree bpdufilter
no spanning-tree bpduguard
no spanning-tree cost
no spanning-tree edge-port
no spanning-tree link-type
no spanning-tree mst MSTMAP cost
no spanning-tree mst MSTMAP port-priority
no spanning-tree port-priority
no spanning-tree stp-state
no storm-control (broadcast|dlf|multicast)
no switchport access vlan VLANID
no switchport block
no switchport dot1q-tunnel mode access
no switchport dot1q-tunnel mode uplink
no switchport mode private-vlan host
no switchport mode private-vlan promiscuous
no switchport mode svl
no switchport port-security

no switchport port-security auto-learn
no switchport port-security shutdown-time
no switchport port-security sticky
no switchport private-vlan host-association
no switchport trunk native vlan
no switchport vlan mapping VID dot1q-tunnel OUTERVID
qos priority DEFAULT-PRIORITY
quit
rate-limit egress bandwidth <64–1000000>
rate-limit ingress bandwidth <64–1000000>
sfp ddm (enable|disable)
sfp eject
sfp scan
shutdown
spanning-tree bpdufilter
spanning-tree bpduguard
spanning-tree cost <1–200000000>
spanning-tree edge-port
spanning-tree link-type (auto|point-to-point|shared)
spanning-tree mst MSTMAP cost <1–200000000>
spanning-tree mst MSTMAP port-priority <0–240>
spanning-tree port-priority <0–240>
spanning-tree stp-state (enable|disable)
speed (10|100|1000|auto)
storm-control (broadcast|dlf|multicast) <2–262142>
switchport access vlan VLANID
switchport access vlan add VLANLIST
switchport access vlan remove VLANLIST
switchport block (multicast|unicast|both)
switchport dot1q-tunnel mode access
switchport dot1q-tunnel mode uplink
switchport mode private-vlan host
switchport mode private-vlan promiscuous
switchport mode svl VLANID
switchport port-security
switchport port-security auto-learn <0–10>
switchport port-security shutdown-time <0–86400>
switchport port-security sticky
switchport private-vlan host-association <2–4094> <2–4094>
switchport private-vlan mapping <2–4094> add VLANLIST
switchport private-vlan mapping <2–4094> remove VLANLIST
switchport trunk allowed vlan add VLANLIST

switchport trunk allowed vlan remove VLANLIST
switchport trunk native vlan VLANID
switchport vlan mapping VID dot1q-tunnel OUTERVID

6.5. VLAN Interface Configuration-Modus

Weitere Informationen zum Zugriff auf den *VLAN Interface Configuration*-Modus finden Sie unter *VLAN Interface Configuration-Modus* auf Seite 243.

```
ICRL-M(config-if)# interface vlan1
ICRL-M(config-if)# list
  description .LINE
  end
  exit
  ip address A.B.C.D/M
  ip dhcp client
  ip dhcp client renew
  ip igmp
  ip igmp last-member-query-count CNT
  ip igmp last-member-query-interval SECONDS
  ip igmp query-interval SECONDS
  ip igmp query-max-response-time SECONDS
  ip igmp robustness-variable CNT
  ip igmp version (1|2)
  ipv6 accept-ra
  ipv6 address X:X::X:X/M
  list
  no description
  no ip address A.B.C.D/M
  no ip dhcp client
  no ip igmp
  no ipv6 accept-ra
  no ipv6 address X:X::X:X/M
  no shutdown
  quit
  shutdown
```

7. Technischer Support

7.1. Pepperl+Fuchs-SFP-Module

Pepperl+Fuchs bietet eine Vielzahl von SFP-Transceivern. Diese zertifizierten SFP-Transceiver können vom RocketLinx ICRL-M identifiziert und in der Web-Benutzerschnittstelle angezeigt werden. Wir empfehlen die Verwendung von Pepperl+Fuchs-SFPs bei der Konfiguration des RocketLinx ICRL-M.

Anmerkung: *SFP-Transceiver von geringer Qualität können zu schlechter Netzwerk-Performance führen und erfüllen möglicherweise nicht die angegebenen Entfernungs- oder Temperaturwerte.*

7.2. Pepperl+Fuchs Private MIB

Pepperl+Fuchs unterstützt viele Standard-MIBs für Benutzer zur Konfiguration oder Überwachung der Switch-Konfiguration über SNMP. Da einige Befehle jedoch in Standard-MIBs nicht gefunden werden können, stellt Pepperl+Fuchs eine Private-MIB-Datei bereit. Kompilieren Sie die Private-MIB-Datei mit Ihrem SNMP-Tool. Die Private MIB kann von https://www.pepperl-fuchs.com heruntergeladen werden.

Die Private-MIB-Struktur ist identisch mit der Webstruktur. Diese ist einfacher zu verstehen und zu verwenden. Wenn Sie nicht mit Standard-MIBs vertraut sind, können Sie den Switch direkt mit der Private MIB verwalten/überwachen, ohne herausfinden zu müssen, wo sich die OIDs der Befehle befinden.

FACTORY AUTOMATION – SENSING YOUR NEEDS

Worldwide Headquarters
Pepperl+Fuchs GmbH
68307 Mannheim · Germany
Tel. +49 621 776-0
E-mail: info@de.pepperl-fuchs.com

USA Headquarters
Pepperl+Fuchs Inc.
Twinsburg, Ohio 44087 · USA
Tel. +1 330 4253555
E-mail: sales@us.pepperl-fuchs.com

Asia Pacific Headquarters
Pepperl+Fuchs Pte Ltd.
Company Registration No. 199003130E
Singapore 139942
Tel. +65 67799091
E-mail: sales@sg.pepperl-fuchs.com

www.pepperl-fuchs.com

PEPPERL+FUCHS
SENSING YOUR NEEDS

TDOCT-B286_ENG
5/21/20