



HIRSCHMANN

A **BELDEN** BRAND

Anwender-Handbuch

Konfiguration

Industrial Ethernet Firewall

EAGLE One

Die Nennung von geschützten Warenzeichen in diesem Handbuch berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften.

© 2013 Hirschmann Automation and Control GmbH

Handbücher sowie Software sind urheberrechtlich geschützt. Alle Rechte bleiben vorbehalten. Das Kopieren, Vervielfältigen, Übersetzen, Umsetzen in irgendein elektronisches Medium oder maschinell lesbare Form im Ganzen oder in Teilen ist nicht gestattet. Eine Ausnahme gilt für die Anfertigungen einer Sicherungskopie der Software für den eigenen Gebrauch zu Sicherungszwecken. Bei Geräten mit eingebetteter Software gilt die Endnutzer-Lizenzvereinbarung auf der mitgelieferten CD/DVD.

Die beschriebenen Leistungsmerkmale sind nur dann verbindlich, wenn sie bei Vertragsschluss ausdrücklich vereinbart wurden. Diese Druckschrift wurde von Hirschmann Automation and Control GmbH nach bestem Wissen erstellt. Hirschmann behält sich das Recht vor, den Inhalt dieser Druckschrift ohne Ankündigung zu ändern. Hirschmann gibt keine Garantie oder Gewährleistung hinsichtlich der Richtigkeit oder Genauigkeit der Angaben in dieser Druckschrift.

Hirschmann haftet in keinem Fall für irgendwelche Schäden, die in irgendeinem Zusammenhang mit der Nutzung der Netzkomponenten oder ihrer Betriebssoftware entstehen. Im Übrigen verweisen wir auf die im Lizenzvertrag genannten Nutzungsbedingungen.

Die jeweils neueste Version dieses Handbuches finden Sie im Internet auf den Hirschmann-Produktseiten (www.hirschmann.com).

Gedruckt in Deutschland
Hirschmann Automation and Control GmbH
Stuttgarter Str. 45-51
72654 Neckartenzlingen
Deutschland
Tel.: +49 1805 141538

Inhalt

Über dieses Handbuch	7
Legende	9
1 Einleitung	11
1.1 Sicherheitskonzept	12
1.2 Typische Anwendungen	13
1.3 Anwendung konfigurieren	18
1.3.1 Konfigurationsschritte im Transparent-Modus	19
1.3.2 Konfigurationsschritte im Router-Modus	20
1.3.3 Konfigurationsschritte im PPPoE-Modus	21
2 Zugang zu den Benutzeroberflächen	23
2.1 System-Monitor	24
2.2 Command Line Interface	26
2.3 Grafische Benutzeroberfläche	29
2.3.1 Öffnen der grafischen Benutzeroberfläche über den internen Port	29
2.3.2 Öffnen der grafischen Benutzeroberfläche über den externen Port	32
3 IP-Parameter eingeben	35
3.1 Grundlagen IP-Parameter	37
3.1.1 IP-Adresse (Version 4)	37
3.1.2 Private IP-Adressen	38
3.1.3 Netzmaske	39
3.1.4 Classless Inter-Domain Routing	42
3.2 IP-Parameter über das CLI eingeben	44
3.2.1 IP-Parameter im Transparent-Modus	46
3.2.2 IP-Parameter im Router-Modus	47
3.2.3 Verbindungsparameter im PPPoE-Modus	50
3.3 IP-Parameter per HiDiscovery eingeben	53
3.4 System-Konfiguration vom ACA laden	55
3.5 System-Konfiguration via DHCP	57

3.6	IP-Konfiguration via grafische Benutzeroberfläche	61
3.6.1	IP-Konfiguration im Transparent-Modus	61
3.6.2	IP-Konfiguration im Router-Modus	63
3.6.3	IP-Konfiguration im PPPoE-Modus	65
3.7	Defekte Geräte ersetzen	67
4	Grundeinstellungen	69
4.1	Konfigurationen bearbeiten und verwalten	70
4.1.1	Aktivieren einer Konfiguration	71
4.1.2	Konfiguration speichern	73
4.1.3	Zurücksetzen der Konfiguration in den Lieferzustand	74
4.1.4	Laden der aktiven Konfiguration	75
4.1.5	Kopieren von Konfigurationsdateien	76
4.1.6	Anzeigen einer Konfigurationsdatei	78
4.1.7	Löschen einer Konfigurationsdatei	79
4.1.8	SFTP-Zugriff auf Geräte-Dateien	79
4.1.9	Konfigurationsänderung widerrufen	80
4.2	Neueste Software laden	82
4.2.1	Prüfen der installierten Software-Release	82
4.2.2	Software laden	83
4.2.3	Software vom ACA laden	84
4.2.4	Software über Datei-Auswahl laden	85
4.3	Ports konfigurieren	87
4.4	Die Systemzeit im Netz synchronisieren	89
4.4.1	Uhrzeit einstellen	89
4.4.2	SNTP	91
4.4.3	NTP	95
5	Unterstützung beim Schutz vor unberechtigtem Zugriff	97
5.1	Zugriff via grafische Benutzeroberfläche	99
5.1.1	Beschreibung Zugriff via grafische Benutzeroberfläche	100
5.1.2	Zugriff via grafische Benutzeroberfläche konfigurieren	101
5.2	CLI-Zugriff	107
5.2.1	Beschreibung CLI-Zugriff	107
5.2.2	CLI-Zugriff konfigurieren	108
5.3	Netzmanagement-Zugriff	113
5.4	HiDiscovery-Zugriff aus-/einschalten	114
5.4.1	Beschreibung HiDiscovery-Protokoll	114

5.4.2	HiDiscovery-Funktion aus-/einschalten	115
5.5	Externe Authentifizierung	116
5.5.1	Beschreibung der externen Authentifizierung	116
5.5.2	Anwendungsbeispiel für die externe Authentifizierung	116
6	Datenverkehr kontrollieren	121
6.1	Paketfilter	122
6.1.1	Beschreibung der Paketfilter-Funktion	122
6.1.2	Anwendungsbeispiel für Paketfilter	126
6.1.3	Anwendungsbeispiel für den Firewall-Lern-Modus (FLM)	134
6.2	NAT – Network Address Translation	143
6.2.1	IP-Masquerading	144
6.2.2	1:1-NAT	145
6.2.3	Port-Weiterleitung	148
6.2.4	NAT-Anwendungsbeispiele	149
6.3	Benutzer-Firewall	155
6.3.1	Beschreibung der Benutzer-Firewall-Funktion	155
6.3.2	Anwendungsbeispiel für die Benutzer-Firewall-Funktion	157
6.4	Unterstützung beim Schutz vor Denial of Service (DoS)	160
6.5	VPN – Virtuelles privates Netz	161
6.5.1	IPsec – Internet Protocol Security	162
6.5.2	IKE – Internet Key Exchange	163
6.5.3	Anwendungsbeispiele	165
7	Redundanz einrichten	191
7.1	Transparent-Redundanz	192
7.1.1	Beschreibung der Transparent-Redundanz-Funktion	192
7.1.2	Anwendungsbeispiel für die Transparent-Redundanz	193
7.2	Router-Redundanz	197
7.2.1	Beschreibung der Router-Redundanz-Funktion	197
7.2.2	Anwendungsbeispiel für die Router-Redundanz	199
8	Funktionsdiagnose	203
8.1	Erreichbarkeits-Test (Ping)	204
8.2	Alarmmeldungen versenden	205

8.2.1	Auflistung der SNMP-Traps	206
8.2.2	SNMP-Traps beim Booten	206
8.2.3	Trapeinstellung	207
8.3	Gerätestatus überwachen	208
8.3.1	Gerätestatus konfigurieren	209
8.3.2	Gerätestatus anzeigen	210
8.4	Out-of-band-Signalisierung	211
8.4.1	Meldekontakt steuern	212
8.4.2	Funktionsüberwachung mit Meldekontakt	213
8.4.3	Gerätestatus mit Meldekontakt überwachen	215
8.5	Port-Zustandsanzeige	216
8.6	Netzlast und Ereigniszähler auf Portebene	217
8.6.1	Netzlast	217
8.6.2	Port-Statistiken	218
8.7	Topologie-Erkennung	220
8.7.1	Beschreibung Topologie-Erkennung	220
8.7.2	Anzeige der Topologie-Erkennung	222
8.8	Konfigurations-Check	224
8.9	Berichte	225
A	Konfigurationsumgebung einrichten	227
A.1	DHCP-Server einrichten	228
A.2	Zugriff mittels SSH	234
B	Allgemeine Informationen	237
B.1	Verwendete Abkürzungen	238
B.2	Management Information BASE (MIB)	240
B.3	Technische Daten	243
B.4	Wartung	244
B.4.1	Service-Shell	244
C	Leserkritik	245
D	Stichwortverzeichnis	247
E	Weitere Unterstützung	251

Über dieses Handbuch

Das Dokument „Anwender-Handbuch Konfiguration“ enthält die Informationen, die Sie zur Inbetriebnahme des Gerätes benötigen. Es leitet Sie Schritt für Schritt von der ersten Inbetriebnahme bis zu den grundlegenden Einstellungen für einen Ihrer Umgebung angepassten Betrieb.

In der Praxis hat sich folgende thematische Reihenfolge bewährt:

- ▶ Wahl des Betriebsmodus in Abhängigkeit des Einsatzgebietes,
 - Transparent - Bridging
 - Router - unterschiedliche Subnetze
 - PPPoE - Internetzugang über DSL
- ▶ Konfiguration des gewählten Betriebsmodus´,
- ▶ Firewall-Regeln erstellen / VPN einrichten.

Das Dokument „Anwender-Handbuch Installation“ enthält eine Gerätebeschreibung, Sicherheitshinweise, Anzeigebeschreibung und weitere Informationen, die Sie zur Installation des Gerätes benötigen, bevor Sie mit der Konfiguration des Gerätes beginnen.

Das Dokument „Referenz-Handbuch Command Line Interface“ enthält detaillierte Information zur Bedienung der einzelnen Funktionen des Gerätes über das Command Line Interface.

Das Dokument „Referenz-Handbuch Grafische Benutzeroberfläche (GUI)“ enthält detaillierte Information zur Bedienung der einzelnen Funktionen des Gerätes über die grafische Benutzeroberfläche.

Die Netzmanagement-Software Industrial HiVision bietet Ihnen weitere Möglichkeiten zur komfortablen Konfiguration und Überwachung:

- ▶ Gleichzeitige Konfiguration mehrerer Geräte
- ▶ Grafische Benutzeroberfläche mit Netz-Layout
- ▶ Autotopologie-Erkennung
- ▶ Ereignislogbuch
- ▶ Ereignisbehandlung
- ▶ Client/Server-Struktur
- ▶ Browser-Interface
- ▶ ActiveX-Control für SCADA-Integration
- ▶ SNMP/OPC-Gateway.

Legende

Die in diesem Handbuch verwendeten Auszeichnungen haben folgende Bedeutungen:

	Aufzählung
	Arbeitsschritt
	Zwischenüberschrift
Link	Querverweis mit Verknüpfung
Anmerkung:	Eine Anmerkung betont eine wichtige Tatsache oder lenkt Ihre Aufmerksamkeit auf eine Abhängigkeit.
<code>Courier</code>	ASCII-Darstellung in der grafischen Benutzeroberfläche
	Ausführung in der grafischen Benutzeroberfläche
	Ausführung im Command Line Interface

Verwendete Symbole:

	WLAN-Access-Point
	Router mit Firewall
	Switch mit Firewall
	Router
	Switch

Legende



Bridge



Hub



Beliebiger Computer



Konfigurations-Computer



Server



SPS -
Speicherprogrammier-
bare Steuerung



I/O -
Roboter

1 Einleitung

Maschinen und Produktionseinheiten wie Druckmaschinen oder Roboterstraßen erfordern heute die Übertragung von Produktionsinformationen in Echtzeit. Dies erfordert eine direkte Zugriffsmöglichkeit auf die Maschine aus der Office-Ebene heraus und setzt die Produktionsanlage der potentiellen Gefahr einer bewussten oder unbewussten Manipulation aus.

Die Hirschmann Industrial Ethernet Firewall EAGLE One unterstützt Sie überall dort bei der Schaffung von Sicherheit, wo Prozess- und Fertigungsdaten in bereichsübergreifende Datenerfassungssysteme einfließen oder Systeme abgeglichen werden. Die Segmentierung einzelner Produktionszellen und die Unterstützung bei der Sicherung von Fernwartungszugängen helfen Ihnen dabei, Manipulationen zu verhindern, für die nötige Datensicherheit zu sorgen und einen reibungslosen Betrieb der Anlage zu gewährleisten.

Die Zeiten, in denen Ethernet über die Büro-Anwendung hinaus, verstärkt auch auf Maschinenebene zum Einsatz kommt, erhöhen die Anforderungen an die Sicherheit:

- ▶ Unterstützung beim Schutz sensibler Teilbereiche der Produktion,
- ▶ langfristige Integration von Office IT- und Industrial IT-Netzen als übergreifende Lösung.

Darüber hinaus bietet Ihnen die Hirschmann Industrial Ethernet Firewall EAGLE One drei Zugänge für die Fernwartung:

- ▶ Modem-Zugang mit Firewall-Regeln,
- ▶ Internet-Zugang mit Firewall-Regeln,
- ▶ Zugang über ein virtuelles privates Netz (VPN).

Zur Erhöhung der Verfügbarkeit bietet Ihnen die Hirschmann Industrial Ethernet Firewall EAGLE One zwei Redundanzmechanismen:

- ▶ virtuelle Router-Redundanz,
- ▶ Layer-2-Redundanz für die redundante Ring-/Netzkopplung.

1.1 Sicherheitskonzept

Eine Firewall unterstützt die Sicherheit eines abgeschlossenen internen Netzes. Auf die Sicherheit haben mehrere Hauptfaktoren Einfluss:

- ▶ Zugänge innerhalb des internen Netzes
Oftmals wird die potentielle Gefahr innerhalb eines internen Netzes unterschätzt. Meist gelangen bösartige Programme unbeabsichtigt in das interne Netz, beispielsweise durch eigene Mitarbeiter oder Dienstleister, die ihre eigenen Rechner mit dem internen Netz verbinden. Auch USB-Sticks oder andere Speichermedien können bösartige Programme enthalten.
- ▶ Zugänge zur Firewall
Ergreifen Sie Maßnahmen, die Sie beim Schutz des Zugangs zur Verwaltung der Firewall unterstützen. Denn wer Zugang zur Firewall hat, bestimmt, welche Daten die Firewall passieren können und welche nicht.
- ▶ Einstellungen der Firewall
Eine Firewall unterstützt Sie beim Schutz Ihres internen Netzes vor unerlaubtem Datenverkehr über die Trennlinie internes/externes Netz hinweg. Welche Daten diese Trennlinie überwinden dürfen, legen Sie mit Hilfe der Firewall-Regeln fest.
- ▶ Schutzmaßnahmen gegen Viren
Eine effektive Maßnahme, die Sie beim Schutz Ihres Netzwerks vor Viren unterstützt, ist die Hilfe bei der Vermeidung von Kommunikation zu unsicheren Geräten. Diese Art des Virenschutzes ist effektiv, da die aufwändige Prüfung des Inhaltes von Datenpaketen entfällt. Ein weiterer Vorteil dieser Methode ist, dass Sie genau bestimmen, wer mit wem kommunizieren darf.

1.2 Typische Anwendungen

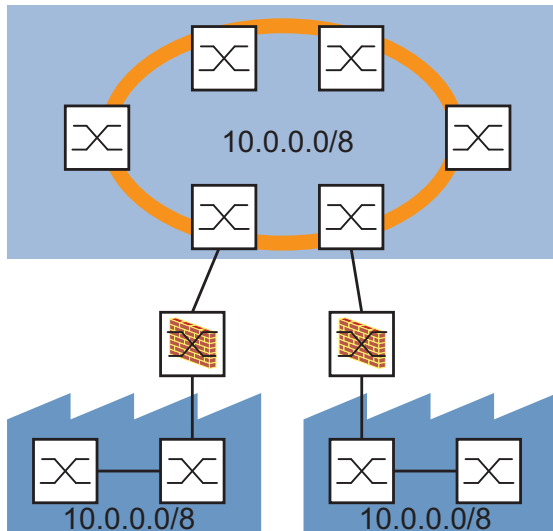
Die EAGLE One-Geräte finden ihren Einsatz überall dort, wo sicherheits-sensible Netzzellen eine Verbindung vom internen Netz ins externe Netz benötigen. Die EAGLE One-Geräte sind das Verbindungsglied zwischen dem internen Netz und dem externen Netz, aus dem unberechtigte Zugriffe möglich sind. In dieser Funktion als Verbindungsglied unterstützen Sie die EAGLE One-Geräte beim Schutz der sicherheitssensiblen Zelle vor unerwünschtem Datenverkehr auf der Verbindung zum externen Netz.

Typische Anwendungen sind:

- ▶ Unterstützung beim Schutz einzelner Produktionszellen in einem flachen Firmennetz.
- ▶ Unterstützung beim Schutz einzelner Produktionszellen in einem gerouteten Firmennetz.
- ▶ Identische Produktionszellen an ein Firmennetz koppeln.
- ▶ Eine Produktionszelle über ein öffentliches Netz mit dem Büronetz verbinden.
- ▶ Unterstützung beim Bereitstellen eines geschützten Service-Zugangs.
- ▶ Maschinen-Gleichteil-Abtrennung

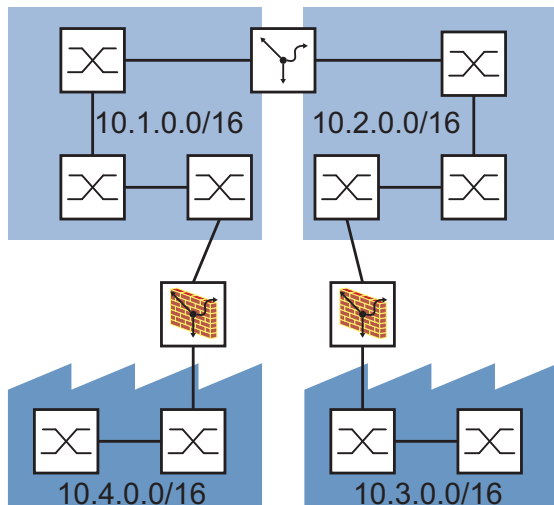
■ Unterstützung beim Schutz einzelner Produktionszellen in einem flachen Firmennetz

Einzelne Produktionszellen tauschen mit Geräten im Firmennetz Informationen aus. Firmennetz und Produktionszellen befinden sich im gleichen Layer-2-Netz. Der EAGLE One arbeitet wie ein Switch mit integrierter Firewall.



■ Unterstützung beim Schutz einzelner Produktionszellen in einem gerouteten Firmennetz.

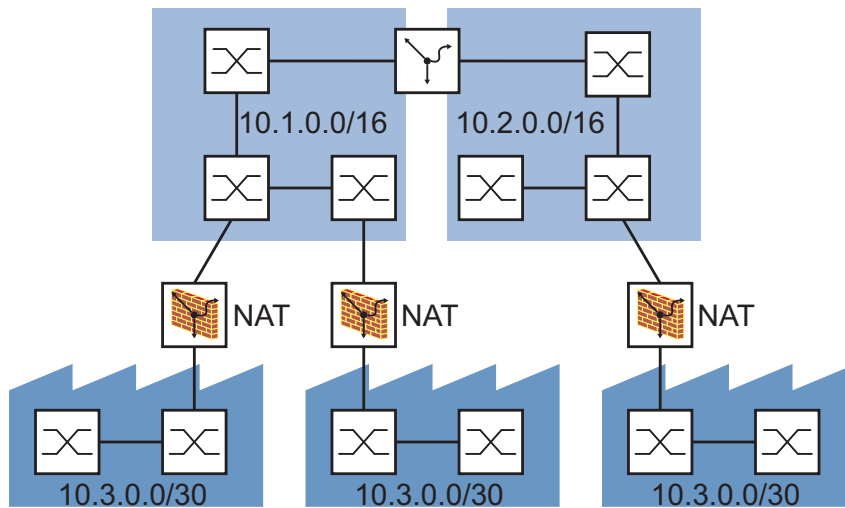
Einzelne Produktionszellen tauschen mit Geräten im Firmennetz Informationen aus. Firmennetz und Produktionszellen befinden sich in unterschiedlichen Subnetzen. Der EAGLE One arbeitet wie ein Router mit integrierter Firewall.



■ Identische Produktionszellen an ein Firmennetz koppeln

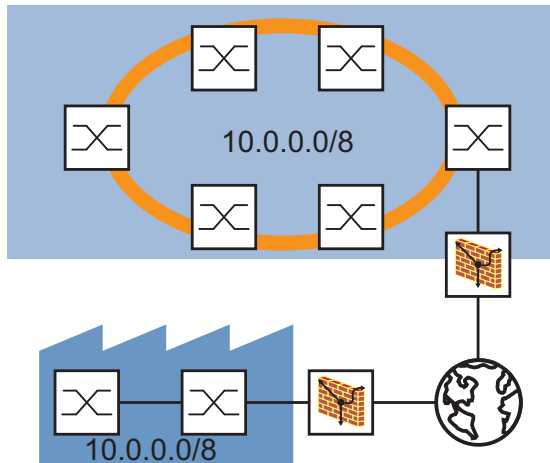
Einzelne identisch aufgebaute Produktionszellen tauschen mit Geräten im Firmennetz Informationen aus. Firmennetz und Produktionszellen befinden sich in unterschiedlichen Subnetzen. Der EAGLE One arbeitet wie ein Router mit integrierter Firewall.

Die NAT-Funktion ermöglicht den identisch aufgebauten Produktionszellen mit dem Firmennetz zu kommunizieren, obwohl die Geräte in den unterschiedlichen Produktionszellen die gleichen IP-Adressen haben.



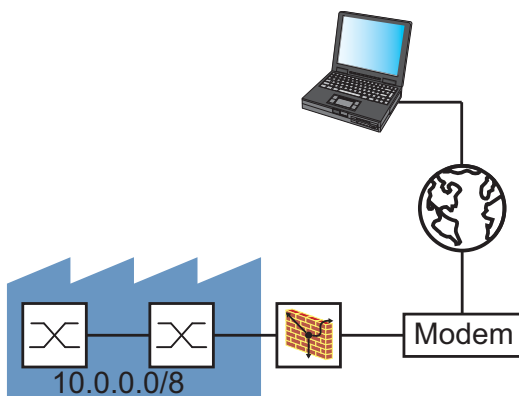
■ Eine Produktionszelle über ein öffentliches Netz mit dem Büronetz verbinden

Eine Produktionszelle tauscht mit Geräten im Firmennetz Informationen aus über das öffentliche Internet. Ein virtueller Informationstunnel (virtual private network, VPN) durch das öffentliche Internet hilft beim Schutz der Kommunikation.



■ Unterstützung beim Bereitstellen eines geschützten Service-Zugangs.

Ein Service-Techniker tauscht mit Geräten in der Produktionszelle Informationen aus über das öffentliche Internet. Ein virtueller Informationstunnel (virtual private network, VPN) durch das öffentliche Internet hilft beim Schutz der Kommunikation.



1.3 Anwendung konfigurieren

Die Industrial Ethernet Firewall kennt 3 Betriebsmodi:

- Transparent-Modus
- Router-Modus
- PPPoE-Modus

Ihre Wahl des Betriebsmodus hängt von Ihrem Anwendungsfall ab. Die Tabelle unten hilft Ihnen bei der Auswahl des Betriebsmodus.

Anwendung	Charakteristik	Betriebsmodus
Unterstützung beim Schutz einzelner Produktionszellen in einem flachen Firmennetz	Vermittlung auf Ebene 2 des ISO/OSI-Schichtenmodells. Die IP-Adressbereiche vor und hinter der Firewall befinden sich im gleichen Subnetz.	Transparent
Unterstützung beim Schutz einzelner Produktionszellen in einem gerouteten Firmennetz	Vermittlung auf Ebene 3 des ISO/OSI-Schichtenmodells. Die IP-Adressbereiche vor und hinter der Firewall befinden sich in unterschiedlichen Subnetzen.	Router
Identische Produktionszellen an ein Firmennetz koppeln	Vermittlung auf Ebene 3 des ISO/OSI-Schichtenmodells. Die IP-Adressbereiche vor und hinter der Firewall befinden sich in unterschiedlichen Subnetzen. Abbilden von IP-Adressen auf einen anderen IP-Adressbereich mit Hilfe der NAT-Funktion.	Router
Eine Produktionszelle über ein öffentliches Netz mit dem Büronetz verbinden	Vermittlung auf Ebene 3 des ISO/OSI-Schichtenmodells. Die IP-Adressbereiche vor und hinter der Firewall befinden sich in unterschiedlichen Subnetzen. Datentransfer in einem geschützten Tunnel durch das öffentliche Internet (VPN).	Router
Unterstützung beim Bereitstellen eines geschützten Service-Zugangs	Service-Zugang über das öffentliche Telefonnetz.	PPPoE

Tab. 1: Auswahl des Betriebsmodus

Abhängig von Ihrer Wahl des Betriebsmodus erfordert die weitere Konfiguration der Industrial Ethernet Firewall ein unterschiedliches Vorgehen.

1.3.1 Konfigurationsschritte im Transparent-Modus

Im Lieferzustand befindet sich die Industrial Ethernet Firewall im Transparent-Modus.

Die Voreinstellungen bieten Ihnen die Möglichkeit, die Industrial Ethernet Firewall sofort in Betrieb zu nehmen. Im Lieferzustand hilft Ihnen die Industrial Ethernet Firewall dabei, den Aufbau einer Kommunikationsverbindung zu verhindern, die von außen initiiert wird. Interne Geräte können eine Kommunikations-Verbindung nach außen aufbauen.

Die folgende Vorgehensweise unterstützt Sie bei der Kontrolle des Zugangs zur Industrial Ethernet Firewall und beim Vornehmen weiterer Einstellungen:

- ☐ Verbindung zur Firewall aufnehmen ([siehe auf Seite 23 „Zugang zu den Benutzeroberflächen“](#))
- ☐ Den Transparent-Betriebsmodus wählen ([siehe auf Seite 46 „IP-Parameter im Transparent-Modus“](#))
- ☐ IP-Parameter für das Gerät eingeben ([siehe auf Seite 46 „IP-Parameter im Transparent-Modus“](#))
- ☐ Maßnahmen ergreifen, welche dabei helfen, die Industrial Ethernet Firewall vor unberechtigtem Zugriff zu schützen ([siehe auf Seite 97 „Unterstützung beim Schutz vor unberechtigtem Zugriff“](#))
- ☐ Regeln für erlaubten und unerlaubten Datenverkehr erstellen ([siehe auf Seite 121 „Datenverkehr kontrollieren“](#))

1.3.2 Konfigurationsschritte im Router-Modus

Im Lieferzustand befindet sich die Industrial Ethernet Firewall im Transparent-Modus.

Die folgende Vorgehensweise unterstützt Sie bei der Kontrolle des Zugangs zur Industrial Ethernet Firewall und beim Vornehmen weiterer Einstellungen:

- ☐ Verbindung zur Firewall aufnehmen ([siehe auf Seite 23 „Zugang zu den Benutzeroberflächen“](#))
- ☐ Den Router-Betriebsmodus wählen ([siehe auf Seite 47 „IP-Parameter im Router-Modus“](#))
- ☐ IP-Parameter für den internen Port eingeben ([siehe auf Seite 47 „Internes Interface“](#))
- ☐ IP-Parameter für den externen Port eingeben ([siehe auf Seite 49 „Externes Interface“](#))
- ☐ Maßnahmen ergreifen, welche dabei helfen, die Industrial Ethernet Firewall vor unberechtigtem Zugriff zu schützen ([siehe auf Seite 97 „Unterstützung beim Schutz vor unberechtigtem Zugriff“](#))
- ☐ Regeln für erlaubten und unerlaubten Datenverkehr erstellen ([siehe auf Seite 121 „Datenverkehr kontrollieren“](#))
- ☐ NAT-Einstellungen vornehmen ([siehe auf Seite 143 „NAT – Network Address Translation“](#))
- ☐ VPN-Verbindung einrichten ([siehe auf Seite 161 „VPN – Virtuelles privates Netz“](#))

1.3.3 Konfigurationsschritte im PPPoE-Modus

Im Lieferzustand befindet sich die Industrial Ethernet Firewall im Transparent-Modus.

Die folgende Vorgehensweise unterstützt Sie bei der Kontrolle des Zugangs zur Industrial Ethernet Firewall und beim Vornehmen weiterer Einstellungen:

- ☐ Verbindung zur Firewall aufnehmen (siehe auf Seite 23 „Zugang zu den Benutzeroberflächen“)
- ☐ Den PPPoE-Betriebsmodus wählen (siehe auf Seite 50 „Verbindungsparameter im PPPoE-Modus“)
- ☐ IP-Parameter für den internen Port eingeben (siehe auf Seite 50 „Internes Interface“)
- ☐ Verbindungsparameter für den externen Port eingeben (siehe auf Seite 51 „Externes Interface“)
- ☐ Automatisches Trennen der PPPoE-Verbindung ein- oder ausschalten (siehe Seite 49 „Externes Interface“)
- ☐ Maßnahmen ergreifen, welche dabei helfen, die Industrial Ethernet Firewall vor unberechtigtem Zugriff zu schützen (siehe auf Seite 97 „Unterstützung beim Schutz vor unberechtigtem Zugriff“)
- ☐ Regeln für erlaubten und unerlaubten Datenverkehr erstellen (siehe auf Seite 121 „Datenverkehr kontrollieren“)
- ☐ NAT-Einstellungen vornehmen (siehe auf Seite 143 „NAT – Network Address Translation“)
- ☐ VPN-Verbindung einrichten (siehe auf Seite 161 „VPN – Virtuelles privates Netz“)

2 Zugang zu den Benutzeroberflächen

Das Gerät bietet Ihnen 3 Benutzeroberflächen, die Sie über unterschiedliche Schnittstellen erreichen:

- ▶ System-Monitor über die V.24-Schnittstelle (out-of-band),
- ▶ Command Line Interface (CLI)
 - über den V.24-Anschluss (out-of-band)
 - über SSH (in-band)
- ▶ Grafische Benutzeroberfläche (GUI) über Ethernet (SNMPv3, in-band).

2.1 System-Monitor

Der System-Monitor ermöglicht

- ▶ die Auswahl der zu ladenden Software,
- ▶ die Durchführung eines Updates der Software,
- ▶ Starten der ausgewählten Software,
- ▶ Beenden des System-Monitors,
- ▶ Löschen der gespeicherten Konfiguration und
- ▶ Anzeige der Bootcode-Information.

■ System-Monitor starten

- ☐ Verbinden Sie mit Hilfe des Terminalkabels (siehe Zubehör)
 - die RJ11-Buchse „V.24“ mit
 - einem Terminal oder einem „COM“-Port eines PCs mit Terminal-emulation nach VT100(physikalische Anbindung siehe Anwender-Handbuch „Installation“).

Speed	9.600 Baud
Data	8 bit
Parity	none
Stoppbit	1 bit
Handshake	off

Tab. 2: Übertragungsparameter

- ☐ Starten Sie das Terminalprogramm auf dem PC und stellen Sie eine Verbindung mit dem Gerät her.

Beim Booten des Gerätes erscheint auf dem Terminal die Meldung „Press <1> to enter System Monitor 1“.

```
< EAGLE One (Boot) Release: 05.3.00 Build: 2013-10-15 08:08 HW: 1.00 >
Press <1> to enter System Monitor 1 ...
1
```

Abb. 1: *Bildschirmansicht beim Bootvorgang*

- ☐ Drücken Sie innerhalb von einer Sekunde die „1“-Taste, um den System-Monitor 1 zu starten.

```
System Monitor 1

(Selected OS: ONE-05.3.00 (2013-10-15 08:08))

1  Select Boot Operating System
2  Update Operating System
3  Start Selected Operating System
4  End (reset and reboot)
5  Erase main configuration file
6  Show Bootcode information

sysMon1>
```

Abb. 2: *Bildschirmansicht System-Monitor 1*

- ☐ Wählen Sie durch Eingabe der Zahl den gewünschten Menüpunkt aus.
- ☐ Um ein Untermenü zu verlassen und zum Hauptmenü des System-Monitor 1 zurückzukehren, drücken Sie <ESC>.

2.2 Command Line Interface

Das Command Line Interface bietet Ihnen die Möglichkeit, die Funktionen des Gerätes über eine lokale oder eine Fernverbindung zu bedienen. IT-Spezialisten finden im Command Line Interface die gewohnte Umgebung zur Konfiguration von IT-Geräten.

Eine detaillierte Beschreibung des Command Line Interface finden Sie im Referenz-Handbuch „Command Line Interface“.

Zugang zum Command Line Interface haben Sie über

- ▶ den V.24-Port (out-of-band),
 - ▶ SSH (in-band).
- Im Lieferzustand
- erlaubt die Firewall-Einstellung den SSH-Zugang über den Port INTERN.
 - hilft die Firewall-Einstellung dabei, den SSH-Zugang über den Port EXTERN zu verhindern.

Anmerkung: Zur Erleichterung der Eingabe bietet Ihnen das CLI die Möglichkeit, Schlüsselwörter abzukürzen. Tippen Sie den Beginn eines Schlüsselwortes ein. Wenn die eingegebenen Buchstaben ein Schlüsselwort kennzeichnen, ergänzt das CLI mit dem Betätigen der Tabulator- oder Leertaste das Schlüsselwort.

Anmerkung: Das Gerät bietet Ihnen die Möglichkeit, die V.24-Schnittstelle als Modem-Schnittstelle oder als Terminal-/CLI-Schnittstelle zu konfigurieren.

Um im Modem-Betrieb dennoch zumindest eingeschränkt auf die CLI-Schnittstelle zuzugreifen, schließen Sie Ihr Terminal (Einstellung am Terminal: 9.600 Baud) an die V.24-Schnittstelle an.

Drücken Sie eine beliebige Taste Ihrer Terminal-Tastatur, bis Ihnen der Login-Bildschirm den CLI-Modus signalisiert.

■ Öffnen des Command Line Interfaces

- ☐ Verbinden Sie das Gerät über V.24 mit einem Terminal oder einem „COM“-Port eines PCs mit Terminalemulation nach VT100 und drücken Sie eine Taste ([siehe auf Seite 24 „System-Monitor starten“](#)) oder rufen Sie das Command Line Interface über SSH auf. Auf dem Bildschirm erscheint ein Fenster für die Eingabe des Benutzernamens. Bis zu fünf Benutzer können auf das Command Line Interface zugreifen.

Copyright (c) 2007-2013 Hirschmann Automation and Control GmbH

All rights reserved

EAGLEONE Release ONE-05.3.0.00

(Build date 2013-09-09 09:09)

System Name: EAGLEONE-000000
Netw. Mode : transparent
Mgmt-IP : a.b.c.d
Base-MAC : 00:11:22:33:44:55
System Time: TUE SEP 17 10:10:10 2013

(Hirschmann EAGLE One)
User:

Abb. 3: Einloggen in das Command Line Interface Programm

- ☐ Geben Sie einen Benutzernamen ein. Im Lieferzustand ist der Benutzername **admin**. Drücken Sie die Eingabetaste.
- ☐ Geben Sie das Passwort ein. Im Lieferzustand ist das Passwort **private**. Drücken Sie die Eingabetaste.
Das Gerät bietet Ihnen die Möglichkeit, den Benutzernamen und das Passwort später im Command Line Interface zu ändern.
Beachten Sie die Schreibweise in Groß-/Kleinbuchstaben.

Das Gerät zeigt den Start-Bildschirm des CLI an.

NOTE: Enter '?' for Command Help. Command help displays all options that are valid for the particular mode.
For the syntax of a particular command form, please consult the documentation.

(Hirschmann EAGLE One) >

Abb. 4: CLI-Bildschirm nach dem Einloggen

2.3 Grafische Benutzeroberfläche

Die grafische Benutzeroberfläche (GUI) bietet Ihnen die Möglichkeit, die Einstellungen des Gerätes von einem Computer im Netz aus komfortabel festzulegen und zu überwachen.

Sie erreichen die grafische Benutzeroberfläche (GUI) mit folgenden Programmen:

- ▶ HiView
- ▶ Web-Browser

Im Lieferzustand

- erlaubt die Firewall-Einstellung den Web-Zugang über das interne Interface
- hilft die Firewall-Einstellung aus Sicherheitsgründen dabei, den Web-Zugang über das externe Interface zu verhindern.

2.3.1 Öffnen der grafischen Benutzeroberfläche über den internen Port

Voraussetzung für das Starten der grafischen Benutzeroberfläche ist, dass die IP-Parameter im Gerät konfiguriert sind. „[IP-Parameter eingeben](#)“ auf [Seite 35](#)

■ HiView

HiView ist eine alleinstehende (stand-alone) Anwendung. HiView bietet Ihnen damit die Möglichkeit, frei von weiteren Anwendungen, wie z. B. einem Browser, die grafische Benutzeroberfläche von Hirschmann Ethernet-Geräten mit Management zu bedienen.

Die Portabilität von HiView bietet Ihnen die Möglichkeit, HiView auf einem portablen Speichermedium zu speichern und auf anderen Computern in Ihrem Datennetz zu starten.

Eine detaillierte Beschreibung der GUI-Applikation HiView finden Sie im „Anwender-Handbuch HiView“.

■ Web-Browser

Alternativ haben Sie die Möglichkeit, die grafische Benutzeroberfläche im Web-Browser zu öffnen, z. B. im Mozilla Firefox ab Version 3.5 oder im Microsoft Internet Explorer ab Version 6. Installieren Sie hierzu auch die Java-Laufzeitumgebung (JRE) in der zuletzt freigegebenen Version. Installationspakete für Ihr Betriebssystem finden Sie unter <http://java.com>.

Grafische Benutzeroberfläche im Web-Browser starten:

- Voraussetzung ist, dass Java in den Sicherheitseinstellungen Ihres Web-Browsers aktiviert ist.
- ☐ Starten Sie Ihren Web-Browser.
- ☐ Schreiben Sie die IP-Adresse des Gerätes in das Adressfeld des Web-Browsers. Verwenden Sie die folgende Form: `https://
xxx.xxx.xxx.xxx`

Der Web-Browser stellt die Verbindung zum Gerät her und zeigt das Login-Fenster.

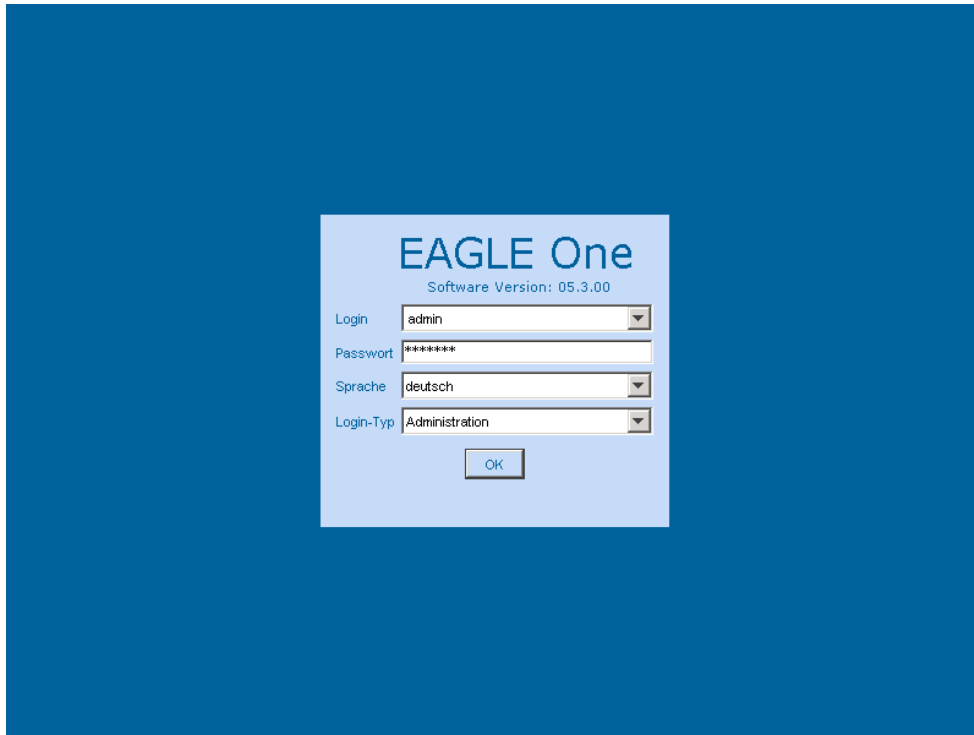


Abb. 5: Login-Fenster

- ☐ Wählen Sie die gewünschte Sprache aus.
- ☐ Wählen Sie im Ausklappmenü `Login`
 - `user`, um mit Leserecht oder
 - `admin`, um mit Schreib- und Leserecht auf das Gerät zuzugreifen.
- ☐ Im Kennwort-Feld ist das Passwort "public", mit dem Sie über Lese-rechte verfügen, vorgegeben. Wollen Sie mit Schreibrechten auf das Gerät zugreifen, dann markieren Sie den Inhalt des Passwortfeldes und überschreiben ihn mit dem Passwort "private" (Lieferzustand).
- ☐ Wählen Sie im Ausklappmenü `Login-Typ`
 - Administration, wenn Sie das Gerät verwalten wollen oder
 - Benutzer-Firewall, wenn Sie sich für die Benutzer-Firewall-Funk-tion anmelden wollen (Voraussetzung: der im Ausklappmenü `Login` gewählte Benutzer ist in der Benutzer-Firewall bereits angelegt).
- ☐ Klicken Sie „OK“.

Der Bildschirm zeigt die grafische Benutzeroberfläche des Gerätes.

Anmerkung: Änderungen, die Sie an den Dialogen vornehmen, übernimmt das Gerät in seinen flüchtigen Speicher, wenn Sie auf „Schreiben“ klicken. Klicken Sie auf „Laden“, um die Anzeige zu aktualisieren.

The screenshot displays the graphical user interface (GUI) for the Hirschmann EAGLE One device. The interface is divided into several sections:

- Gerätestatus (Device Status):** Located at the top, it features a red bar indicating an alarm. The alarm start time is 02.09.08 15:39, and the alarm reason is Netzteil 1 (Power Supply 1).
- Systemdaten (System Data):** This section contains fields for device information:
 - Name: EAGLE-000000
 - Standort: Hirschmann EAGLE
 - Ansprechpartner: Hirschmann Automation and Control GmbH
 - Grundmodul: EAGLE 20 TX/TX H/V.1.12
 - Spannungsversorgung P1/P2: defekt / vorhanden
 - Temperatur (°C): A range from 0 to 70, with a current value of 49.
 - Betriebszeit: 0 Tag(e), 9:15:52
- Gerätedarstellung (Device Representation):** On the right, there is a graphical representation of the device hardware, showing components like the power supply, status LEDs, and various ports (USB, RS-485, V.24).
- Buttons:** At the bottom, there are buttons for "Schreiben" (Write), "Laden" (Load), and "Hilfe" (Help).
- Footer:** The bottom left corner indicates "Aktualisierung in 90 s" (Update in 90 s).

Abb. 6: Grafische Benutzeroberfläche des Gerätes

2.3.2 Öffnen der grafischen Benutzeroberfläche über den externen Port

Im Lieferzustand hilft die Firewall-Einstellung aus Sicherheitsgründen dabei, den Web-Zugang über den externen Port zu verhindern. Sie können Zugang zu dem Gerät über den externen Port erlangen, wenn Sie für Ihren PC eine Regel für den Web-Zugriff und den SNMP-Zugriff anlegen und aktivieren. Öffnen Sie hierzu zuerst die grafische Benutzeroberfläche über den internen Port ([siehe auf Seite 29 „Öffnen der grafischen Benutzeroberfläche über den](#)

internen Port“). Nach dem Anlegen der Zugriffsregeln am externen Port können Sie die grafische Benutzeroberfläche über den externen Port analog wie über den internen Port öffnen.

- ☐ Legen Sie im Menü `Sicherheit:Web-Zugriff` einen neuen Eintrag mit der IP-Adresse Ihres PC als Quelladresse an. Wählen Sie „akzeptieren“ in der Spalte „Aktion“ und aktivieren Sie den Tabelleneintrag.
- ☐ Legen Sie im Menü `Sicherheit:SNMP-Zugriff` einen neuen Eintrag mit der IP-Adresse Ihres PC als Quelladresse an. Wählen Sie „akzeptieren“ in der Spalte „Aktion“ und aktivieren Sie den Tabelleneintrag.
- ☐ Verfahren Sie analog wie beim Öffnen des internen Ports.

3 IP-Parameter eingeben

■ **Wahl des Betriebsmodus**

Die Einträge zu den IP-Parametern hängen vom gewählten Betriebsmodus ab.

- Im Transparent-Modus ist die lokale IP-Adresse auch die IP-Adresse des Managements der Industrial Ethernet Firewall.
- Im Router-/PPPoE-Modus ist die IP-Adresse des internen Interfaces auch die IP-Adresse des Managements der Industrial Ethernet Firewall. Abhängig von den Einstellungen der Firewall können Sie das Management auch über die IP-Adresse des externen Interfaces erreichen.

☐ Entscheiden Sie sich für einen Betriebsmodus, der Ihren Anforderungen genügt.

Im Lieferzustand ist der Transparent-Modus aktiv.

■ **Möglichkeiten zur Eingabe der IP-Parameter für das Management der Industrial Ethernet Firewall**

Geben Sie bei der Erstinstallation des Gerätes die IP-Parameter ein, damit Sie für die weitere Konfiguration auf das Management des Gerätes zugreifen können.

Das Gerät bietet bei der Erstinstallation 5 Möglichkeiten zur Eingabe der lokalen IP-Parameter im Transparent-Modus bzw. der IP-Parameter des internen Interfaces im Router-/PPPoE-Modus:

- ▶ Eingabe mit Hilfe des Command Line Interfaces (CLI).
Diese sogenannte „out-of-band“-Methode wählen Sie, wenn
 - ▶ Sie Ihr Gerät außerhalb seiner Betriebsumgebung vorkonfigurieren
 - ▶ Sie keinen Netzzugang („in-band“) zum Gerät haben
(siehe Seite 44 „IP-Parameter über das CLI eingeben“).
- ▶ Eingabe mit Hilfe des HiDiscovery-Protokolls.
Diese sogenannte „in-band“-Methode wählen Sie, wenn das Gerät bereits im Netz installiert ist oder Sie sonst eine Ethernet-Verbindung zwischen Ihrem PC und dem Gerät haben
(siehe Seite 53 „IP-Parameter per HiDiscovery eingeben“).

- ▶ Konfiguration mit Hilfe des AutoConfiguration Adapter (ACA).
Diese Methode wählen Sie, wenn Sie ein Gerät durch ein Gerät des gleichen Typs austauschen und zuvor die Konfiguration auf einem ACA gespeichert haben ([siehe Seite 55 „System-Konfiguration vom ACA laden“](#)).
- ▶ Konfiguration über DHCP.
Diese sogenannte „in-band“-Methode wählen Sie, wenn Sie das bereits installierte Gerät mittels DHCP konfigurieren wollen. Hierzu benötigen Sie einen DHCP-Server. Der DHCP-Server ordnet dem Gerät anhand seiner MAC-Adresse oder seines Systemnamens die IP-Parameter zu ([siehe Seite 57 „System-Konfiguration via DHCP“](#)).
- ▶ Konfiguration über die grafische Benutzeroberfläche.
Verfügt das Gerät bereits über eine IP-Adresse und ist über das Netz erreichbar, dann bietet Ihnen die grafische Benutzeroberfläche eine weitere Möglichkeit, die IP-Parameter zu konfigurieren.

3.1 Grundlagen IP-Parameter

3.1.1 IP-Adresse (Version 4)

Die IP-Adressen bestehen aus vier Bytes. Die vier Bytes werden durch einen Punkt getrennt, dezimal dargestellt.

Seit 1992 sind im RFC 1340 fünf Klassen von IP-Adressen definiert.

Class	Netzadresse	Hostadresse	Adressbereich
A	1 Byte	3 Bytes	1.0.0.0 bis 126.255.255.255
B	2 Bytes	2 Bytes	128.0.0.0 bis 191.255.255.255
C	3 Bytes	1 Byte	192.0.0.0 bis 223.255.255.255
D			224.0.0.0 bis 239.255.255.255
E			240.0.0.0 bis 255.255.255.255

Tab. 3: Klassen der IP-Adressen

Die Netzadresse stellt den festen Teil der IP-Adresse dar. Das weltweit oberste Organ für die Vergabe von Netzadressen ist die IANA (Internet Assigned Numbers Authority). Wenn Sie einen IP-Adressblock benötigen, dann kontaktieren Sie Ihren Internet-Service-Provider. Internet-Service-Provider wenden sich an ihre lokale übergeordnete Organisation:

- ▶ APNIC (Asia Pacific Network Information Centre) - Asia/Pacific Region
- ▶ ARIN (American Registry for Internet Numbers) - Americas and Sub-Saharan Africa
- ▶ LACNIC (Regional Latin-American and Caribbean IP Address Registry) – Latin America and some Caribbean Islands
- ▶ RIPE NCC (Réseaux IP Européens) - Europe and Surrounding Regions

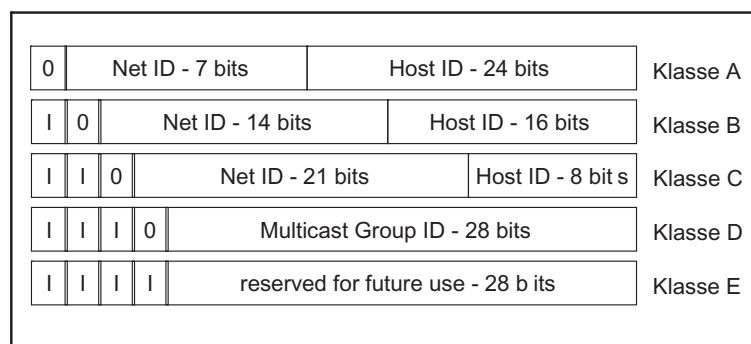


Abb. 7: Bitdarstellung der IP-Adresse

Die IP-Adressen, deren erstes Bit eine Null ist, das heißt die erste Dezimalzahl kleiner als 128 ist, gehören der Klasse A an.

Ist das erste Bit einer IP-Adresse eine Eins und das zweite Bit eine Null, das heißt die erste Dezimalzahl liegt im Bereich von 128 bis 191, dann gehört die IP-Adresse der Klasse B an.

Sind die ersten beiden Bits einer IP-Adresse eine Eins, das heißt die erste Dezimalzahl ist größer als 191, dann handelt es sich um eine IP-Adresse der Klasse C.

Die Vergabe der Hostadresse (host id) obliegt dem Netzbetreiber. Er allein ist für die Einmaligkeit der IP-Adressen, die er vergibt, verantwortlich.

3.1.2 Private IP-Adressen

Falls der Ihnen zugewiesene IP-Adressraum nicht ausreichend groß für Ihre Anforderungen ist, oder auch aus anderen Gründen, können Sie sich der IP-Adressen des privaten IP-Adressbereichs bedienen. Die IANA hat in RFC 1918) drei private IP-Adressbereiche festgelegt. Jeder der drei Bereiche befindet sich in einer anderen Klasse.

Internet-Router blockieren Datenpakete mit privaten IP-Adressen. Somit sind die privaten Adressen ausschließlich zur Verwendung in internen Netzen gedacht. Das Network Address Translation Protocol ([siehe auf Seite 143 „NAT – Network Address Translation“](#)) bietet Ihnen die Möglichkeit, Geräte mit privater IP-Adresse eines internen Netzes mit Geräten anderer Netze kommunizieren zu lassen.

IP-Adressbereich	CIDR-Notation	Netzklasse
10.0.0.0 - 10.255.255.255	10.0.0.0/8	A
172.16.0.0 - 172.31.255.255	172.16.0.0/12	B
192.168.0.0 - 192.168.255.255	192.168.0.0/16	C

Tab. 4: *Private Adressbereiche*

3.1.3 Netzmaske

Router und Gateways unterteilen große Netze in Subnetze. Die Netzmaske ordnet die IP-Adressen der einzelnen Geräte einem bestimmten Subnetz zu.

Die Einteilung in Subnetze mit Hilfe der Netzmaske geschieht analog zu der Einteilung in die Klassen A bis C der Netzadresse (net id).

Die Bits der Hostadresse (host id), die die Maske darstellen sollen, werden auf Eins gesetzt. Die restlichen Bits der Hostadresse in der Netzmaske werden auf Null gesetzt (vgl. folgende Beispiele).

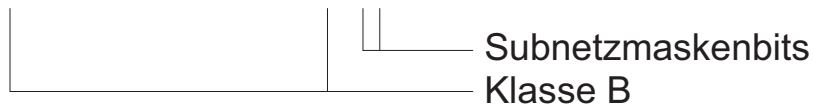
Beispiel für eine Netzmaske:

Dezimale Darstellung

255.255.192.0

Binäre Darstellung

11111111.11111111.11000000.00000000

 Subnetzmaskenbits
Klasse B

Beispiel für IP-Adressen mit Subnetzzuordnung nach der Netzmaske aus dem obigen Beispiel:

Dezimale Darstellung

129.218.65.17

 128 < 129 191 > Klasse B

Binäre Darstellung

10000001.11011010.01000001.00010001

 Subnetz 1
Netzadresse

Dezimale Darstellung

129.218.129.17

 128 < 129 191 > Klasse B

Binäre Darstellung

10000001.11011010.10000001.00010001

 Subnetz 2

■ Beispiel für die Anwendung der Netzmaske

In einem großen Netz ist es möglich, dass Gateways oder Router den Management-Agenten von ihrer Managementstation trennen. Wie erfolgt in einem solchen Fall die Adressierung?

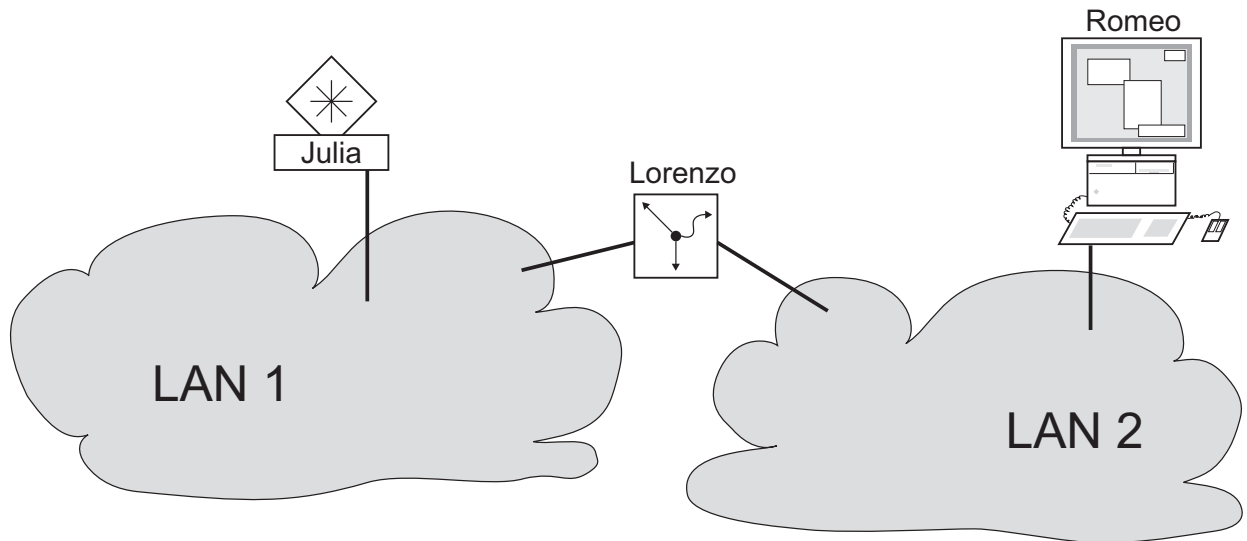


Abb. 8: Management-Agent durch Router von der Managementstation getrennt

Die Managementstation „Romeo“ möchte Daten an den Management-Agenten „Julia“ schicken. Romeo kennt die IP-Adresse von Julia und weiß, dass der Router „Lorenzo“ den Weg zu Julia kennt.

Also packt Romeo seine Botschaft in einen Umschlag und schreibt als Zieladresse die IP-Adresse von Julia und als Quelladresse seine eigene IP-Adresse darauf.

Diesen Umschlag steckt Romeo in einen weiteren Umschlag mit der MAC-Adresse von Lorenzo als Zieladresse und seiner eigenen MAC-Adresse als Quelladresse. Dieser Vorgang ist vergleichbar mit dem Übergang von der Ebene 3 zur Ebene 2 des ISO/OSI-Basis-Referenzmodells.

Nun steckt Romeo das gesamte Datenpaket in den Briefkasten, vergleichbar mit dem Übergang von der Ebene 2 zur Ebene 1, dem Senden des Datenpaketes in das Ethernet.

Lorenzo erhält den Brief, entfernt den äußeren Umschlag und erkennt auf dem inneren Umschlag, dass der Brief für Julia bestimmt ist. Er steckt den inneren Umschlag in einen neuen äußeren Umschlag, schaut in seiner Adressliste, der ARP-Tabelle, nach der MAC-Adresse von Julia und schreibt diese auf den äußeren Umschlag als Zieladresse und seine eigene MAC-Adresse als Quelladresse. Das gesamte Datenpaket steckt er anschließend in den Briefkasten.

Julia empfängt den Brief, entfernt den äußeren Umschlag. Übrig bleibt der innere Umschlag mit Romeos IP-Adresse. Das Öffnen des inneren Umschlages und lesen der Botschaft entspricht einer Übergabe an höhere Protokollschichten des ISO/OSI-Schichtenmodells.

Julia möchte eine Antwort an Romeo zurücksenden. Sie steckt ihre Antwort in einen Umschlag mit der IP-Adresse von Romeo als Zieladresse und ihrer eigenen IP-Adresse als Quelladresse. Doch wohin soll Sie die Antwort schicken? Die MAC-Adresse von Romeo hat sie ja nicht erhalten.

Die MAC-Adresse von Romeo blieb beim Wechseln des äußeren Umschlags bei Lorenzo zurück.

Julia findet in der MIB unter der Variablen `hmNetGatewayIPAddr` Lorenzo als Vermittler zu Romeo. So steckt sie den Umschlag mit den IP-Adressen in einen weiteren Umschlag mit der MAC-Zieladresse von Lorenzo.

Nun findet der Brief den gleichen Weg über Lorenzo zu Romeo, so wie der Brief von Romeo zu Julia fand.

3.1.4 Classless Inter-Domain Routing

Die Klasse C mit maximal 254 Adressen war zu klein und die Klasse B mit maximal 65.534 Adressen war für die meisten Anwender zu groß. Hieraus resultierte eine nicht effektive Nutzung der zur Verfügung stehenden Klasse B-Adressen.

Die Klasse D enthält reservierte Multicast-Adressen. Die Klasse E ist für experimentelle Zwecke reserviert. Ein Gateway, das nicht an diesen Experimenten teilnimmt, ignoriert Datagramme mit diesen Zieladressen. Seit 1993 bietet die RFC 1519 mit Classless Inter-Domain Routing (CIDR) eine Lösung. Das CIDR überwindet diese Klassenschranken und unterstützt klassenlose IP-Adressbereiche.

Mit CIDR geben Sie die Anzahl der Bits an, die den IP-Adressbereich kennzeichnen. Hierzu stellen Sie den IP-Adressbereich in binärer Form dar und zählen die Maskenbits zur Bezeichnung der Netzmaske. Die Netzmaske gibt die Anzahl der Bits an, welche für die IP-Adressen in einem gegebenen Adressbereich, dem Netz-Teil identisch sind. Beispiel:

IP-Adresse dezimal	Netzmaske dezimal	IP-Adresse binär
149.218.112.1	255.255.255.128	10010101 11011010 01110000 00000001
149.218.112.127		10010101 11011010 01110000 01111111
		———— 25 Maskenbits ————

CIDR-Schreibweise: 149.218.112.0/25

———— Maskenbits

Die Zusammenfassung mehrerer Klasse C-Adressbereiche heißt „Supernetting“. Auf diese Weise lassen sich Klasse-B-Adressbereiche sehr fein untergliedern.

3.2 IP-Parameter über das CLI eingeben

Sollten Sie weder über DHCP, HiDiscovery Protokoll noch über den Auto-Configuration Adapter (ACA) das System konfigurieren, dann nehmen Sie die Konfiguration über die V.24-Schnittstelle mit Hilfe des CLI vor.

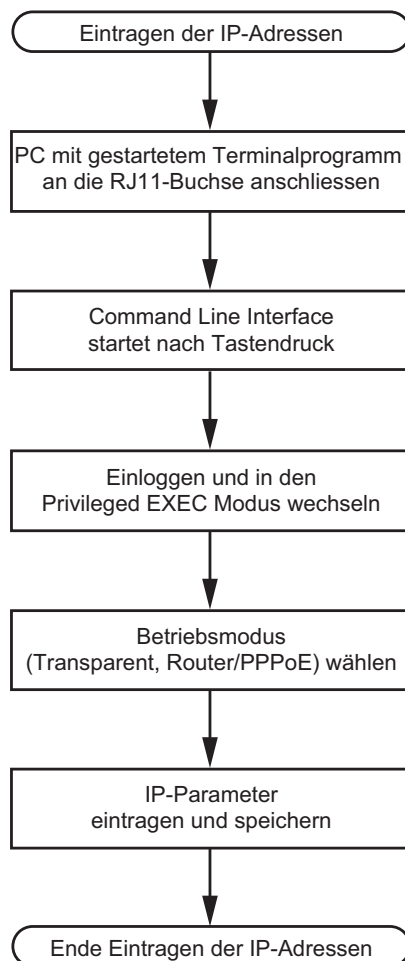


Abb. 9: Ablaufdiagramm Eintragen der IP-Adressen

Anmerkung: Sollten Sie in der Nähe des Installationsortes kein Terminal oder keinen PC mit Terminalemulation zur Verfügung haben, können Sie das Gerät an ihrem Arbeitsplatz konfigurieren und danach an seinen endgültigen Installationsort bringen.

- ☐ Stellen Sie eine Verbindung mit dem Gerät her ([siehe auf Seite 27 „Öffnen des Command Line Interfaces“](#)).

Der Start-Bildschirm erscheint.

NOTE: Enter '?' for Command Help. Command help displays all options that are valid for the particular mode.
For the syntax of a particular command form, please consult the documentation.

(Hirschmann EAGLE One) >

3.2.1 IP-Parameter im Transparent-Modus

- ☐ Stellen Sie den Transparent-Modus ein (Lieferzustand: Transparent-Modus).
- ☐ Falls DHCP eingeschaltet ist, schalten Sie DHCP aus (Lieferzustand: DHCP ist ausgeschaltet).
- ☐ Geben Sie die IP-Parameter ein.
 - ▶ Lokale IP-Adresse
Im Lieferzustand besitzt das Gerät die lokale IP-Adresse 192.168.1.1.
 - ▶ Netzmaske
Haben Sie Ihr Netz in Subnetze aufgeteilt und identifizieren Sie diese mit einer Netzmaske, dann geben Sie an dieser Stelle die Netzmaske ein.
Im Lieferzustand ist die Netzmaske 255.255.255.0 eingetragen.
 - ▶ IP-Adresse des Gateways
Diese Eingabe ist notwendig, wenn sich das Gerät und die Managementstation bzw. der DHCP-Server in unterschiedlichen Subnetzen befinden ([siehe Seite 41 „Beispiel für die Anwendung der Netzmaske“](#)).
Tragen Sie die IP-Adresse des Gateways ein, das das lokale Subnetz mit dem der Managementstation verbindet.
Im Lieferzustand ist die IP-Adresse 0.0.0.0 eingetragen.
- ☐ Speichern Sie die eingegebene Konfiguration.

```
enable
network mode transparent

network transparent proto
none
network transparent
ip-address 172.16.1.100
network transparent netmask
255.255.255.0
network transparent gateway
172.16.1.1
copy config running-config nv
```

Wechsel in den Privileged-EXEC-Modus.

Den Transparent-Modus auswählen (Lieferzustand: Transparent-Modus).

DHCP ausschalten.

Dem Gerät im Transparent-Modus die IP-Adresse 172.16.1.100 zuweisen.

Dem Gerät im Transparent-Modus die Netzmaske 255.255.255.0 zuweisen.

Dem Gerät im Transparent-Modus die Gateway-Adresse 172.16.1.1 zuweisen.

Die aktuelle Konfiguration in den nichtflüchtigen Speicher sichern.

Nach Eingabe der IP-Parameter können Sie das Gerät über die grafische Benutzeroberfläche (siehe Referenz-Handbuch „GUI“) komfortabel konfigurieren.

3.2.2 IP-Parameter im Router-Modus

■ Internes Interface

- ☐ Stellen Sie den Router-Modus ein (Lieferzustand: Transparent-Modus).
- ☐ Falls DHCP eingeschaltet ist, schalten Sie DHCP aus (Lieferzustand: DHCP ist ausgeschaltet).
- ☐ Geben Sie die IP-Parameter ein.
 - ▶ Interne IP-Adresse
Im Lieferzustand besitzt das Gerät im Router-Modus die lokale IP-Adresse 192.168.1.3.
 - ▶ Netzmaske
Haben Sie Ihr Netz in Subnetze aufgeteilt und identifizieren Sie diese mit einer Netzmaske, dann geben Sie an dieser Stelle die Netzmaske ein.
Im Lieferzustand ist die Netzmaske 255.255.255.0 eingetragen.
- ☐ Speichern Sie die eingegebene Konfiguration mit
`copy config running-config nv` oder
`save`.

<code>enable</code>	Wechsel in den Privileged-EXEC-Modus.
<code>network mode router</code>	Den Router-Modus auswählen (Lieferzustand: Transparent-Modus).
<code>network router proto int none</code>	DHCP auf dem internen Router-Interface ausschalten.
<code>network router param int ip-address 172.17.1.100</code>	Dem internen Router-Interface die IP-Adresse 172.17.1.100 zuweisen.
<code>network router param int netmask 255.255.255.0</code>	Dem internen Router-Interface die Netzmaske 255.255.255.0 zuweisen.
<code>copy config running-config nv</code>	Die aktuelle Konfiguration in den nichtflüchtigen Speicher sichern.

Nach Eingabe der IP-Parameter können Sie das Gerät über die grafische Benutzeroberfläche (siehe Referenz-Handbuch „GUI“) komfortabel konfigurieren.

■ Externes Interface

- ☐ Falls DHCP eingeschaltet ist, schalten Sie DHCP aus (Lieferzustand: DHCP ist ausgeschaltet).
- ☐ Geben Sie die IP-Parameter ein.
 - ▶ Externe IP-Adresse
Im Lieferzustand besitzt das Gerät die lokale IP-Adresse 10.0.0.10.
 - ▶ Netzmaske
Haben Sie Ihr Netz in Subnetze aufgeteilt und identifizieren Sie diese mit einer Netzmaske, dann geben Sie an dieser Stelle die Netzmaske ein.
Im Lieferzustand ist die Netzmaske 255.255.255.0 eingetragen.
 - ▶ IP-Adresse des Gateways
Diese Eingabe ist notwendig, wenn sich das Gerät und die Managementstation bzw. der DHCP-Server in unterschiedlichen Subnetzen befinden ([siehe Seite 41 „Beispiel für die Anwendung der Netzmaske“](#)).
Tragen Sie die IP-Adresse des Gateways ein, das das lokale Subnetz mit dem der Managementstation verbindet.
Im Lieferzustand ist die IP-Adresse 0.0.0.0 eingetragen.
- ☐ Speichern Sie die eingegebene Konfiguration mit `copy config running-config nv` oder `save`.

```
enable
network router proto ext
none
network router param ext
ip-address 10.0.1.100
network router param ext
netmask 255.255.240.0
network router gateway
10.0.1.1
```

```
copy config running-config nv
```

Wechsel in den Privileged-EXEC-Modus.

DHCP auf dem externen Router-Interface ausschalten.

Dem externen Router-Interface die IP-Adresse 10.0.1.100 zuweisen.

Dem externen Router-Interface die Netzmaske 255.255.240.0 zuweisen.

Dem Gerät die Gateway-Adresse 10.0.1.1 zuweisen. Das Gateway muss im Netz eines der Router-Interfaces liegen.

Die aktuelle Konfiguration in den nichtflüchtigen Speicher sichern.

3.2.3 Verbindungsparameter im PPPoE-Modus

■ Internes Interface

- ☐ Stellen Sie den PPPoE-Modus ein (Lieferzustand: Transparent-Modus).
- ☐ Falls DHCP eingeschaltet ist, schalten Sie DHCP aus (Lieferzustand: DHCP ist ausgeschaltet).
- ☐ Geben Sie die IP-Parameter ein.
 - ▶ **Interne IP-Adresse**
Im Lieferzustand besitzt das Gerät im Router-Modus die lokale IP-Adresse 192.168.1.3.
 - ▶ **Netzmaske**
Haben Sie Ihr Netz in Subnetze aufgeteilt und identifizieren Sie diese mit einer Netzmaske, dann geben Sie an dieser Stelle die Netzmaske ein.
Im Lieferzustand ist die Netzmaske 255.255.255.0 eingetragen.
- ☐ Speichern Sie die eingegebene Konfiguration mit
`copy config running-config nv` oder
`save`.

<code>enable</code>	Wechsel in den Privileged-EXEC-Modus.
<code>network mode pppoe</code>	Den PPPoE-Modus auswählen (Lieferzustand: Transparent-Modus).
<code>network router proto int none</code>	DHCP ausschalten (Lieferzustand: ausgeschaltet).
<code>network router param int ip-address 172.17.1.100</code>	Dem internen Interface die IP-Adresse 172.17.1.100 zuweisen.
<code>network router param int netmask 255.255.255.0</code>	Dem Gerät im Transparent-Modus die Netzmaske 255.255.255.0 zuweisen.
<code>copy config running-config nv</code>	Die aktuelle Konfiguration in den nichtflüchtigen Speicher sichern.

Nach Eingabe der IP-Parameter können Sie das Gerät über die grafische Benutzeroberfläche (siehe Referenz-Handbuch „GUI“) komfortabel konfigurieren.

■ Externes Interface

- ☐ Geben Sie die Verbindungsparameter ein, die Sie von Ihrem Anbieter für die Verbindung (Provider) erhalten haben.

- ▶ Benutzernamen

- ▶ Kennwort

- ▶ MTU (Maximum Transmission Unit).

Die MTU gibt die maximale Paketgröße an, die diese Verbindung übertragen kann. Stehen größere Datenpakete zur Übertragung an, dann fragmentiert die Firewall das größere Datenpaket in mehrere kleine Datenpakete.

- ☐ Speichern Sie die eingegebene Konfiguration mit

`copy config running-config nv` oder
`save`.

<code>enable</code>	Wechsel in den Privileged-EXEC-Modus.
<code>network pppoe username Peter</code>	Den Benutzernamen „Peter“ eingeben.
<code>network pppoe password Holidays</code>	Das Passwort „Holidays“ eingeben.
<code>network pppoe mtu-size 1492</code>	Die maximale Paketgröße mit 1492 eingeben.
<code>copy config running-config nv</code>	Die aktuelle Konfiguration in den nichtflüchtigen Speicher sichern.

Anmerkung: Sie können die Einstellung der maximalen Paketgröße in der Regel überspringen. Stellen Sie die maximale Paketgröße ein, wenn Sie wissen, dass ihr Internet-Service-Provider einen anderen Wert verwendet.

Das externe Interface erhält über PPPoE seine IP-Adresse vom Anbieter für die Verbindung (Provider).

Das EAGLE One-Gerät bietet Ihnen die Möglichkeit, die PPPoE-Verbindung täglich automatisch zu trennen. Um diese Funktion zu aktivieren, gehen Sie wie folgt vor:

```
enable
```

Wechsel in den Privileged-EXEC-Modus.

```
network pppoe disconnect  
admin-state enable
```

Eingeben, dass das Gerät die PPPoE-Verbindung täglich um die angegebene Uhrzeit automatisch trennt.

```
network pppoe disconnect hour  
2
```

Eingeben der Uhrzeit (Stunde), zu der das Gerät die PPPoE-Verbindung täglich automatisch trennt. Wertebereich: 0 bis 23.

```
copy config running-config nv
```

Die aktuelle Konfiguration in den nichtflüchtigen Speicher sichern.

3.3 IP-Parameter per HiDiscovery eingeben

Das HiDiscovery-Protokoll ermöglicht Ihnen, dem Gerät über das Ethernet IP-Parameter zuzuweisen.

Weitere Parameter können Sie mit der grafischen Benutzeroberfläche (siehe Referenz-Handbuch „GUI“ (Graphical User Interface / Web-based Interface)) komfortabel konfigurieren.

Im Lieferzustand ist die HiDiscovery-Funktion des Gerätes

- ▶ am internen Port eingeschaltet,
- ▶ am externen Port ausgeschaltet.

Anmerkung: Das Gerät bietet Ihnen ausschließlich im und für den Transparent-Modus die Konfiguration mit HiDiscovery an. Der Transparent-Modus ist im Lieferzustand eingeschaltet.

Installieren Sie die HiDiscovery-Software auf Ihrem PC. Sie finden die Software auf der CD, die Sie mit dem Gerät erhalten haben.

- ☐ Zur Installation starten Sie das Installationsprogramm auf der CD.
- ☐ Starten Sie das Programm HiDiscovery.

Beim Start von HiDiscovery untersucht HiDiscovery automatisch das Netz nach Geräten, die das HiDiscovery-Protokoll unterstützen.

HiDiscovery benutzt das erste gefundene Netz-Interface des PCs. Sollte Ihr Rechner über mehrere Netzwerkkarten verfügen, können Sie das gewünschte in der Werkzeugeiste von HiDiscovery auswählen.

HiDiscovery zeigt für jedes Gerät, das auf das HiDiscovery-Protokoll reagiert, eine Zeile an.

Anmerkung: Mit dem Eintragen der IP-Adresse übernimmt das Gerät die lokalen Konfigurationseinstellungen ([siehe auf Seite 70 „Konfigurationen bearbeiten und verwalten“](#)).

Anmerkung: Schalten Sie aus Sicherheitsgründen in der grafischen Benutzeroberfläche die HiDiscovery-Funktion des Gerätes aus, nachdem Sie dem Gerät die IP-Parameter zugewiesen haben ([siehe auf Seite 61 „IP-Konfiguration via grafische Benutzeroberfläche“](#)).

Anmerkung: Speichern Sie die Einstellungen, damit Sie die Eingaben nach einem Neustart noch verfügbar haben ([siehe auf Seite 70 „Konfigurationen bearbeiten und verwalten“](#)).

HiDiscovery ermöglicht das Identifizieren der angezeigten Geräte.

- ☐ Wählen Sie eine Gerätezeile aus.
- ☐ Klicken Sie auf das „Signal“-Symbol in der Werkzeugleiste, um das Blinken der LEDs des ausgewählten Gerätes einzuschalten. Ein weiteres Klicken auf das Symbol schaltet das Blinken aus.
- ☐ Mit einem Doppelklick auf eine Zeile öffnen Sie ein Fenster, in dem Sie den Gerätenamen und die IP-Parameter eintragen können.

3.4 System-Konfiguration vom ACA laden

Der AutoConfiguration Adapter (ACA) ist ein Gerät

- ▶ zum Speichern der Konfigurationsdaten eines Gerätes und
- ▶ zum Speichern der Geräte-Software.

Der ACA ermöglicht bei einem betriebsunfähigen Gerät, eine denkbar einfache Konfigurationsdatenübernahme durch ein Ersatzgerät des gleichen Typs.

Beim Starten des Gerätes prüft das Gerät das Vorhandensein eines ACAs. Ist ein ACA mit gültigem Passwort und gültiger Software vorhanden, dann lädt das Gerät die Konfigurationsdaten aus dem ACA.

Das Passwort ist gültig, wenn

- ▶ das Passwort im Gerät mit dem Passwort im ACA übereinstimmt oder
- ▶ das voreingestellte Passwort im Gerät eingegeben ist.

Um die Konfigurationsdaten im ACA zu speichern ([siehe auf Seite 73 „Konfiguration speichern“](#)).

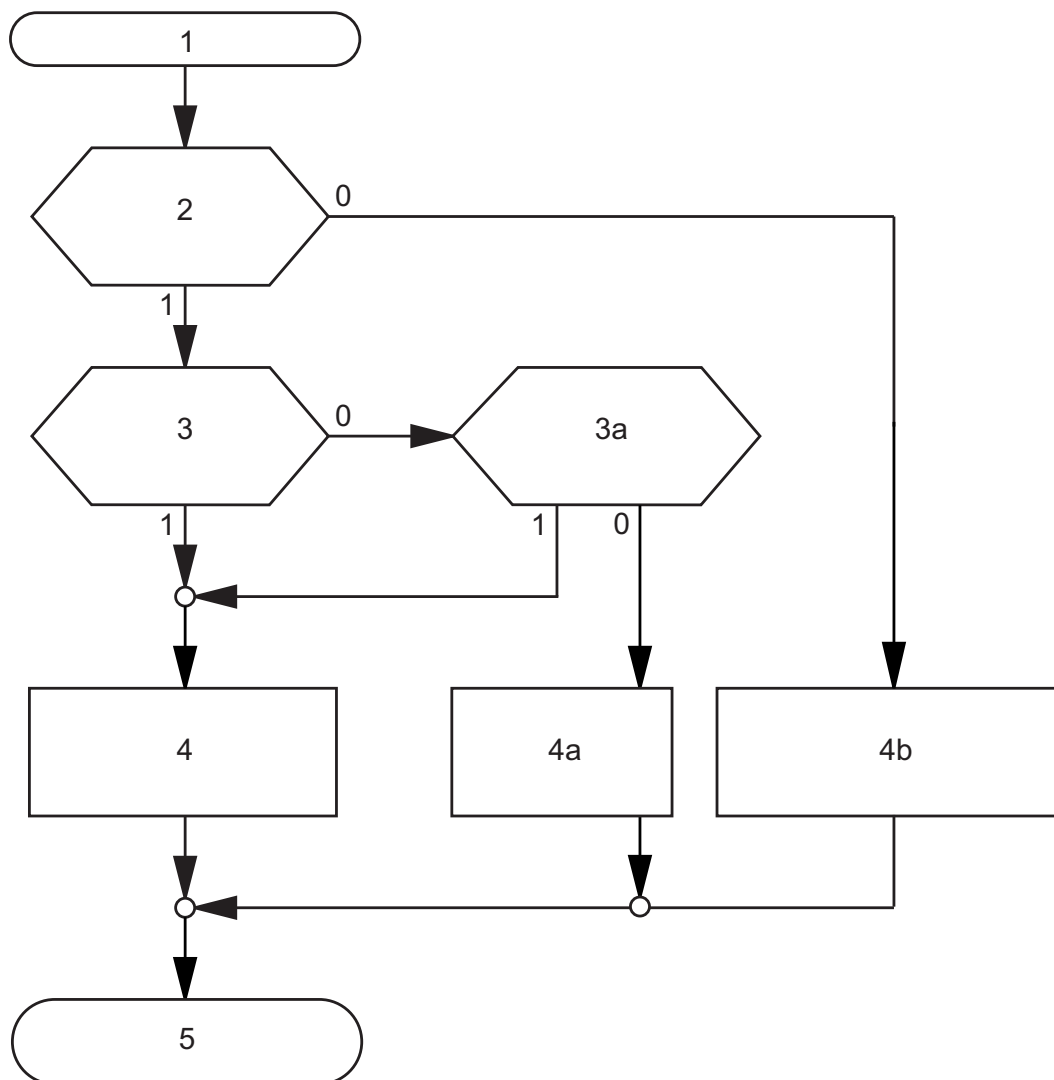


Abb. 10: Ablaufdiagramm Konfigurationsdaten vom ACA laden

1 – Gerät starten

2 – ACA vorhanden?

3 – Passwort im Gerät und ACA identisch?

3a – Voreingestelltes Passwort im Gerät?

4 – Konfiguration vom ACA laden, ACA-LED blinkt 2 × pro Periode grün

4a – Konfiguration aus lokalem Speicher laden, ACA-LED leuchtet grün

4b – Konfiguration aus lokalem Speicher laden, ACA-LED aus

5 – Konfigurationsdaten geladen

3.5 System-Konfiguration via DHCP

Bei der Inbetriebnahme mit Hilfe von DHCP (Dynamic Host Configuration Protocol) erhält ein Gerät gemäß dem Ablaufdiagramm seine IP-Adresse. DHCP bietet die Konfiguration des Gerätes (DHCP-Client) über einen Namen an.

Dieser Name heißt bei DHCP nach RFC 2131 "Client Identifier".

Das Gerät verwendet den in der System-Gruppe der MIB II unter sysName eingetragenen Namen als Client Identifier. Die Eingabe dieses Systemnamens können Sie direkt vornehmen über SNMP, das Management der grafischen Benutzeroberfläche (siehe System-Dialog) oder das Command Line Interface.

Bei der Inbetriebnahme erhält ein Gerät gemäß dem Ablaufdiagramm "DHCP-Prozess" ([siehe Abb. 11](#)) seine IP-Parameter.

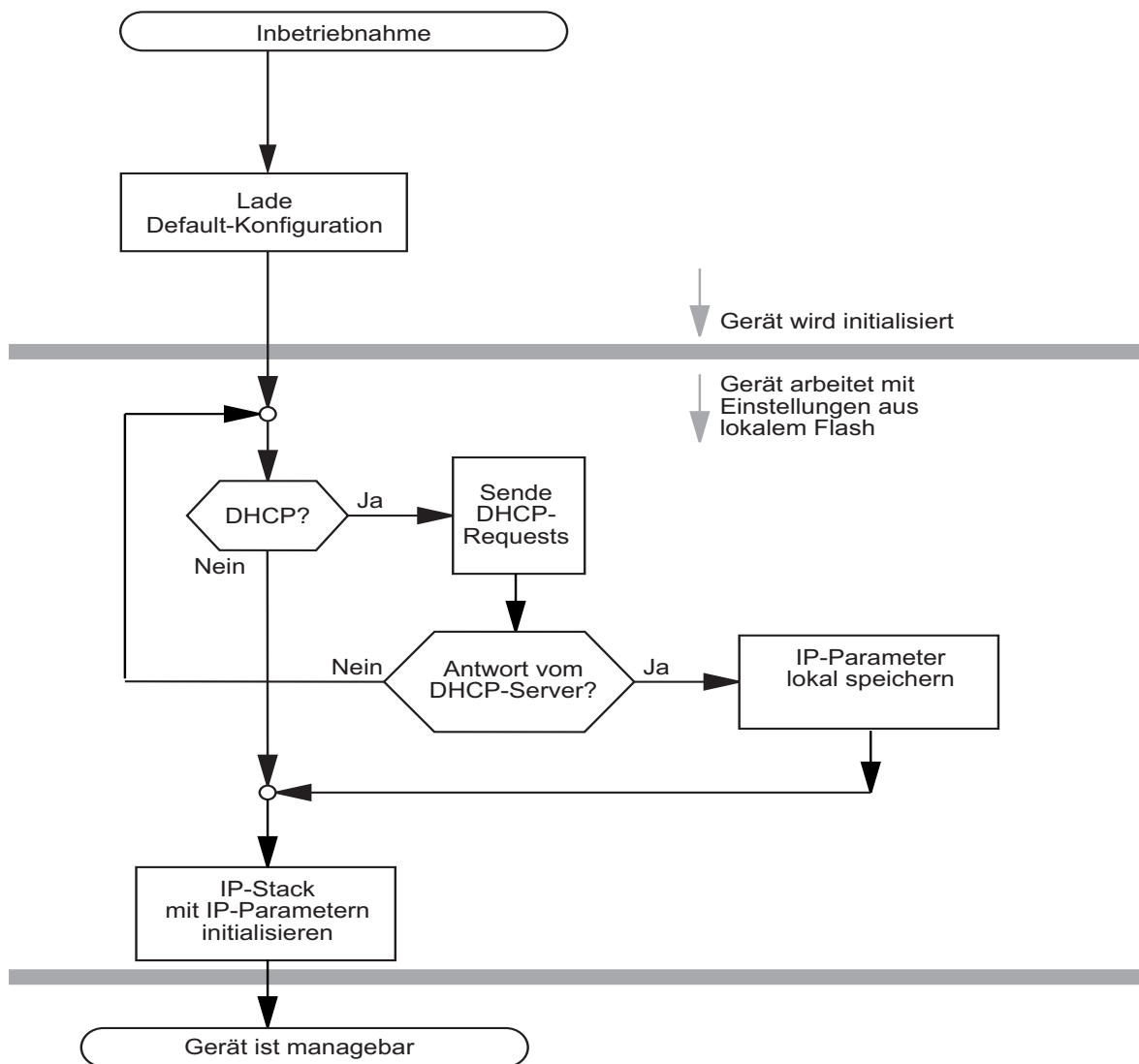


Abb. 11: Ablaufdiagramm DHCP-Prozess

Das Gerät übermittelt seinen Systemnamen dem DHCP-Server. Der DHCP-Server kann dann alternativ zur MAC-Adresse anhand des Systemnamens eine IP-Adresse vergeben.

Das Gerät übernimmt diese Daten als Konfigurationsparameter ([siehe auf Seite 61 „IP-Konfiguration via grafische Benutzeroberfläche“](#)).

Wurde eine IP-Adresse von einem DHCP-Server zugeteilt, wird diese lokal gespeichert.

Option	Bedeutung
1	Subnet Mask
2	Time Offset
3	Router
4	Time server
12	Host Name
61	Client Identifier

Tab. 5: *DHCP-Optionen, die das Gerät anfordert*

Der DHCP-Server stellt die Konfigurationsparameter ("lease") für eine bestimmte Zeitspanne zur Verfügung.

Um dies zu umgehen, bieten DHCP-Server die explizite Konfigurationsmöglichkeit, einem bestimmten Client anhand einer eindeutigen Hardware-ID dieselbe IP-Adresse zuzuordnen (sogenannte statische Adressvergabe).

Im Lieferzustand ist DHCP inaktiv.

Wenn DHCP aktiviert wird, versucht das Gerät, eine IP-Adresse von einem DHCP-Server zu bekommen. Findet es nach einem Neustart keinen DHCP-Server, dann hat es keine IP-Adresse.

Zum Aktivieren/Deaktivieren von DHCP ([siehe auf Seite 61 „IP-Konfiguration via grafische Benutzeroberfläche“](#)).

Anmerkung: Achten Sie bei der Anwendung des Netzmanagements Industrial HiVision darauf, dass DHCP jedem Gerät die original IP-Adresse zuweist.

Im Anhang finden Sie ein Beispiel zur Konfiguration eines BOOTP/DHCP-Servers ([siehe auf Seite 228 „DHCP-Server einrichten“](#)).

Beispiel für eine DHCP-Konfigurationsdatei:

```
# /etc/dhcpd.conf for DHCP Daemon
#
subnet 10.1.112.0 netmask 255.255.240.0 {
option subnet-mask 255.255.240.0;
option routers 10.1.112.96;
}
#
# Host berta requests IP configuration
# with her MAC address
#
host berta {
hardware ethernet 00:80:63:08:65:42;
fixed-address 10.1.112.82;
}
#
# Host hugo requests IP configuration
# with his client identifier.
#
host hugo {
#
option dhcp-client-identifier "hugo";
option dhcp-client-identifier 00:68:75:67:6f;
fixed-address 10.1.112.83;
server-name "10.1.112.11";
filename "/agent/config.dat";
}
```

Zeilen mit vorangestelltem #-Zeichen sind Kommentarzeilen.

Die Zeilen vor den einzeln aufgeführten Geräten bezeichnen Einstellungen, welche für die folgenden Geräte gelten.

Die Zeile fixed-address weist dem Gerät eine feste IP-Adresse zu.

Weitere Informationen entnehmen Sie Ihren DHCP-Server-Handbuch.

3.6 IP-Konfiguration via grafische Benutzeroberfläche

Mit dem Dialog `Grundeinstellungen:Netz` legen Sie fest, aus welcher Quelle das Gerät seine IP-Parameter nach dem Start erhält, weisen IP-Parameter zu, definieren die Handhabung von VLANs und konfigurieren den HiDiscovery-Zugriff.

- ☐ Wählen Sie die Betriebsart ([siehe auf Seite 18 „Anwendung konfigurieren“](#)).

3.6.1 IP-Konfiguration im Transparent-Modus

- ☐ Geben Sie im Rahmen „Protokoll“ ein, woher das Gerät seine IP-Parameter bezieht:
 - ▶ Kreuzen Sie „DHCP“ an, wenn die Konfiguration durch einen DHCP-Server auf der Basis der MAC-Adresse oder des Namens des Gerätes ([siehe Seite 57 „System-Konfiguration via DHCP“](#)) erfolgen soll.
 - ▶ Ist „DHCP“ nicht angekreuzt, verwendet das Gerät die Netzparameter aus seinem lokalen Speicher.
- ☐ Wählen Sie „VLAN-Tag verwenden“, wenn das Gerät das VLAN-Tag der empfangenen Datenpakete auswerten soll. Bei aktiver Funktion können Sie ausschließlich aus dem in „Management VLAN-ID“ (siehe unten) eingetragenen VLAN das Management des Gerätes erreichen.
- ☐ Die Zeile „Management VLAN ID“ bietet Ihnen die Möglichkeit, dem Interface für das Management des Gerätes ein VLAN zuzuweisen „VLAN-Tag verwenden“ (siehe oben).

■ IP-Parameter eingeben

- ☐ Geben Sie im Feld „IP-Adresse“ die IP-Adresse des Gerätes ein.
- ☐ Geben Sie im Feld „Gateway IP-Adresse“ die IP-Adresse des Gateways ein, an welches das Gerät Datenpakete weiterleiten soll, deren Zieladresse außerhalb des eigenen Subnetzes liegen.
- ☐ Geben Sie im Feld „Netzmaske“ die Netzmaske ein.

■ IP-Parameter über DHCP beziehen

- ☐ Den für das DHCP-Protokoll relevanten Namen geben Sie im System-Dialog der grafischen Benutzeroberfläche in der Zeile "Name" ein.

■ HiDiscovery-Protokoll konfigurieren

- ☐ Das HiDiscovery-Protokoll ermöglicht Ihnen, dem Gerät an Hand seiner MAC-Adresse eine IP-Adresse zuzuweisen. Aktivieren Sie das HiDiscovery-Protokoll, wenn Sie von Ihrem PC aus mit der mitgelieferten HiDiscovery-Software dem Gerät eine IP-Adresse übertragen wollen (Lieferzustand: aktiv).

■ IP-Konfiguration speichern

Speichern Sie die Einstellungen, damit Sie die Eingaben nach einem Neustart noch verfügbar haben ([siehe Seite 70 „Konfigurationen bearbeiten und verwalten“](#)).

3.6.2 IP-Konfiguration im Router-Modus

Im Router-Modus benötigt das Gerät die Eingabe der IP-Parameter am internen und am externen Interface.

- ☐ Geben Sie im Rahmen „Protokoll“ ein, woher das Gerät seine IP-Parameter bezieht:
 - ▶ Kreuzen Sie „DHCP“ an, wenn die Konfiguration durch einen DHCP-Server auf der Basis der MAC-Adresse oder des Namens des Gerätes ([siehe Seite 57 „System-Konfiguration via DHCP“](#)) erfolgen soll.
 - ▶ Ist „DHCP“ nicht angekreuzt, verwendet das Gerät die Netzparameter aus seinem lokalen Speicher.
- ☐ Wählen Sie „VLAN-Tag verwenden“, wenn das Gerät das VLAN-Tag der empfangenen Datenpakete auswerten soll. Bei aktiver Funktion verwirft das Gerät jene empfangenen Datenpakete, deren VLAN-Tag eine andere VLAN-ID enthält, als die in diesem Dialog eingetragene VLAN-ID. Datenpakete ohne VLAN-Tag werden ebenfalls verworfen. Die NAT-Funktionen sind dabei außer Kraft gesetzt.
- ☐ Das Feld „VLAN ID“ bietet Ihnen die Möglichkeit, dem Interface ein VLAN zuzuweisen.
Anmerkung: Das Gerät verwendet die Eingabe in diesem Feld ausschließlich dann, wenn „VLAN-Tag verwenden“ angekreuzt ist.

■ IP-Parameter eingeben

- ☐ Geben Sie im Feld „IP-Adresse“ die IP-Adresse des Gerätes ein.
- ☐ Geben Sie im Feld „Netzmaske“ die Netzmaske ein.
- ☐ Geben Sie im Feld „Gateway IP-Adresse“ die IP-Adresse des Gateways ein, an welches das Gerät Datenpakete weiterleiten soll, deren Zieladresse außerhalb des eigenen Subnetzes liegen.
- ☐ Wenn Sie einem Interface mehr als eine IP-Adresse zuweisen wollen, dann können Sie mit „Erzeugen“ weitere IP-Parameter in die Tabelle unten eintragen.
Sie benötigen mehrere IP-Adressen an einem Interface, wenn Sie große flache Netze mit unterschiedlichen Subnetzen an einem Port anschließen.

■ IP-Parameter über DHCP beziehen

- ☐ Den für das DHCP-Protokoll relevanten Namen geben Sie im System-Dialog der grafischen Benutzeroberfläche in der Zeile „Name“ ein.

■ IP-Konfiguration speichern

Speichern Sie die Einstellungen, damit Sie die Eingaben nach einem Neustart noch verfügbar haben ([siehe Seite 70 „Konfigurationen bearbeiten und verwalten“](#)).

3.6.3 IP-Konfiguration im PPPoE-Modus

Im PPOE-Modus benötigt das Gerät die Eingabe der IP-Parameter am internen Interface. Die IP-Parameter für das externe Interface bezieht das Gerät vom Anbieter für die Verbindung (Provider).

- ☐ Geben Sie im Rahmen „Protokoll“ ein, woher das Gerät seine IP-Parameter bezieht:
 - ▶ Kreuzen Sie „DHCP“ an, wenn die Konfiguration durch einen DHCP-Server auf der Basis der MAC-Adresse oder des Namens des Gerätes ([siehe Seite 57 „System-Konfiguration via DHCP“](#)) erfolgen soll.
 - ▶ Ist „DHCP“ nicht angekreuzt, verwendet das Gerät die Netzparameter aus seinem lokalen Speicher.
- ☐ Wählen Sie „VLAN-Tag verwenden“, wenn das Gerät das VLAN-Tag der empfangenen Datenpakete auswerten soll. Bei aktiver Funktion verwirft das Gerät jene empfangenen Datenpakete, deren VLAN-Tag eine andere VLAN-ID enthält, als die in diesem Dialog eingetragene VLAN-ID. Datenpakete ohne VLAN-Tag werden ebenfalls verworfen. Die NAT-Funktionen sind dabei außer Kraft gesetzt.
- ☐ Das Feld „VLAN ID“ bietet Ihnen die Möglichkeit, dem Interface ein VLAN zuzuweisen.
Anmerkung: Das Gerät verwendet die Eingabe in diesem Feld ausschließlich dann, wenn „VLAN-Tag verwenden“ angekreuzt ist.

■ IP-Parameter eingeben

- ☐ Geben Sie im Feld „IP-Adresse“ die IP-Adresse des Gerätes ein.
- ☐ Geben Sie im Feld „Netzmaske“ die Netzmaske ein.
- ☐ Geben Sie im Feld „Gateway IP-Adresse“ die IP-Adresse des Gateways ein, an welches das Gerät Datenpakete weiterleiten soll, deren Zieladresse außerhalb des eigenen Subnetzes liegen.
- ☐ Wenn Sie einem Interface mehr als eine IP-Adresse zuweisen wollen, dann können Sie mit „Erzeugen“ weitere IP-Parameter in die Tabelle unten eintragen.
Sie benötigen mehrere IP-Adressen an einem Interface, wenn Sie große flache Netze mit unterschiedlichen Subnetzen an einem Port anschließen.

■ IP-Parameter über DHCP beziehen

- ☐ Den für das DHCP-Protokoll relevanten Namen geben Sie im System-Dialog der grafischen Benutzeroberfläche in der Zeile „Name“ ein.

■ PPPoE-Verbindungsparameter eingeben

- ☐ Geben Sie die Verbindungsparameter ein, die Sie von Ihrem Anbieter für die Verbindung (Provider) erhalten haben.
 - ▶ Benutzernamen
 - ▶ Kennwort
 - ▶ MTU (Maximum Transmission Unit).
Die MTU gibt die maximale Paketgröße an, die diese Verbindung übertragen kann. Stehen größere Datenpakete zur Übertragung an, dann fragmentiert die Firewall das größere Datenpaket in mehrere kleine Datenpakete.

■ IP-Konfiguration speichern

Speichern Sie die Einstellungen, damit Sie die Eingaben nach einem Neustart noch verfügbar haben ([siehe Seite 70 „Konfigurationen bearbeiten und verwalten“](#)).

3.7 Defekte Geräte ersetzen

Das Gerät bietet eine Plug-and-Play-Lösung zum Austauschen eines defekten Gerätes durch ein Gerät des gleichen Typs (Faulty Device Replacement):

- Konfiguration des neuen Gerätes mit Hilfe eines AutoConfiguration Adapters ([siehe auf Seite 55 „System-Konfiguration vom ACA laden“](#)).

Das neue Gerät erhält beim Starten die gleichen Konfigurationsdaten, die das defekte Gerät hatte.

4 Grundeinstellungen

Zu den Grundeinstellungen des Gerätes gehören:

- ▶ das Bearbeiten und Verwalten von Konfigurationen (Geräte-einstellungen).
- ▶ das Laden der neuesten Software des Gerätes
- ▶ die Konfiguration der Ports des Gerätes
- ▶ die Synchronisation der Systemzeit im Netz

4.1 Konfigurationen bearbeiten und verwalten

Bei einem Neustart lädt das Gerät seine Konfigurationen (Einstellungen) von seinem nicht-flüchtigen Speicher, sofern Sie nicht DHCP aktiviert haben und kein ACA am Gerät angeschlossen ist.

Während des Betriebs bietet Ihnen das Gerät die Möglichkeit, Konfigurationen (Einstellungen) aus folgenden Quellen zu laden:

- ▶ von seinem nicht-flüchtigen Speicher (Non-Volatile Memory, NVM oder NVRAM),
- ▶ vom AutoConfiguration Adapter. Ist ein ACA am Gerät angeschlossen, dann lädt das Gerät seine Konfiguration vom ACA, falls die auf dem ACA gespeicherte Konfiguration sich von der lokal gespeicherten Konfiguration unterscheidet.

Konfigurationen (Einstellungen) wie z.B. IP-Parameter und Portkonfiguration speichert das Gerät im flüchtigen Arbeitsspeicher. Diese gehen beim Ausschalten oder einem Neustart verloren.

Das Gerät bietet Ihnen die Möglichkeit, Konfigurationen (Einstellungen)

- ▶ zu aktivieren,
- ▶ zu speichern,
- ▶ in den Lieferzustand zu versetzen,
- ▶ vom nicht-flüchtigen Speicher (NVM) zu laden,
- ▶ zu kopieren,
- ▶ anzuzeigen,
- ▶ zu löschen.

Wenn Sie die laufende Konfiguration verändern (z. B. einen Port ausschalten), ändert die grafische Benutzeroberfläche das „Laden/Speichern“-Symbol im Navigationsbaum von einem Diskettensymbol in ein gelbes Dreieck. Nach dem Speichern der Konfiguration zeigt die grafische Benutzeroberfläche das „Laden/Speichern“-Symbol wieder als Diskette an.

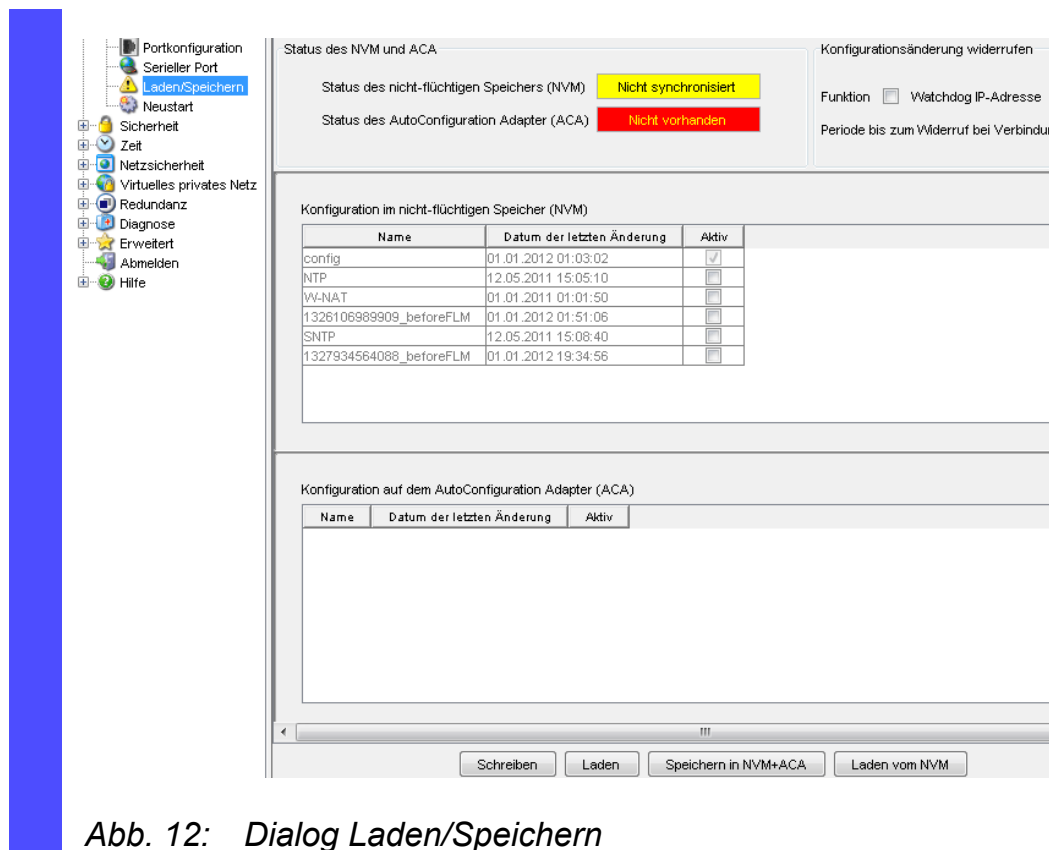


Abb. 12: Dialog Laden/Speichern

4.1.1 Aktivieren einer Konfiguration

Das Gerät bietet Ihnen die Möglichkeit, eine gespeicherte Konfiguration aus der Tabelle „Konfiguration im nicht-flüchtigen Speicher (NVM)“ zu aktivieren.

- ☐ Wählen Sie den Dialog
Grundeinstellungen:Laden/Speichern.

- ☐ Wählen Sie in der NVM-Konfigurationstabelle eine nicht-aktive Konfigurationsdatei aus.
 - ☐ Klicken Sie auf „Aktivieren“.
- In der Spalte „Aktiv“ zeigt Ihnen das Gerät die aktive Konfiguration an. Ist ein ACA mit der gleichen Konfigurationsdatei angeschlossen, aktiviert das Gerät die Konfigurationsdatei auf dem ACA und zeigt die Aktivierung in der NVM-Tabelle ausgegraut an.

enable	Wechsel in den Privileged-EXEC-Modus.
show config profiles nv	Anzeige der im NVM gespeicherten Konfigurationen.
copy config nv profile <name> running-config	Das Gerät lädt die Konfigurationsdaten „Name“ aus dem lokalen nicht-flüchtigen Speicher.

Anmerkung: Wenn Sie eine Konfiguration mit dem alternativen CLI-Kommando `profile activate nv <id>` als aktiv markiert haben, wird diese erst wirksam, nachdem Sie das CLI-Kommando `copy config nv running-config` ausführen.

Anmerkung: Wenn Sie eine Konfiguration laden (aktivieren), dann warten Sie mit einem Zugriff auf das Gerät, bis dieses die Konfigurationsdatei geladen und die neuen Konfigurationseinstellungen vorgenommen hat. Abhängig vom Umfang der Konfigurationseinstellungen kann dieser Vorgang mehrere Sekunden dauern. Warten Sie, bis das Gerät in der Spalte „Aktiv“ die neue Konfiguration markiert.

4.1.2 Konfiguration speichern

Das Gerät bietet Ihnen die Möglichkeit, die aktuelle Konfiguration (Einstellung) auf dem Gerät und den ACA

- ▶ in einer neuen Konfigurationsdatei zu speichern,
- ▶ in der aktiven Konfigurationsdatei zu speichern.

■ Konfiguration in einer neuen Konfigurationsdatei speichern

- ☐ Wählen Sie den Dialog
Grundeinstellungen:Laden/Speichern.
- ☐ Klicken Sie auf „Erzeugen“, um ein Fenster für die Eingabe einer neuen Zeile in der Tabelle zu öffnen.
- ☐ Geben Sie im Datei-Fenster in „Konfigurationsname“ einen Namen ein.
- ☐ Klicken Sie auf „OK“.

Das Gerät speichert die Konfiguration in einer neuen Datei im NVM und auf dem ACA.

Anmerkung: Verwenden Sie in Dateinamen keine Leerzeichen. Die maximale Länge beträgt 32 Zeichen.

■ Konfiguration in der aktiven Konfigurationsdatei speichern

Das Gerät bietet Ihnen die Möglichkeit, die aktive Konfiguration durch die aktuelle Konfiguration zu ersetzen.

Beachten Sie, dass Sie beim Speichern der aktuellen Konfiguration in die aktive Konfigurationsdatei diese überschreiben.

- ☐ Wählen Sie den Dialog
Grundeinstellungen:Laden/Speichern.
- ☐ Klicken Sie auf „Speichern in NVM und ACA“, wenn Sie im nicht-flüchtigen Speicher und auf dem ACA die aktive Konfiguration durch die laufende Konfiguration ersetzen wollen.“.

Anmerkung: Wenn Sie die aktive Konfigurationsdatei aus dem lokalen nicht-flüchtigen Speicher laden möchten klicken Sie auf „Laden vom NVM“.

 enable

copy config running-config nv

Wechsel in den Privileged-EXEC-Modus.

Das Gerät speichert die aktuellen Konfigurationsdaten in den lokalen nicht-flüchtigen Speicher und, sofern ein ACA angeschlossen ist, auch in den ACA

4.1.3 Zurücksetzen der Konfiguration in den Lieferzustand

Das Gerät bietet Ihnen die Möglichkeit, die Konfiguration in den Lieferzustand zurückzusetzen.

 ☐ Wählen Sie den Dialog Grundeinstellungen:Neustart.☐ Klicken Sie auf „Lieferzustand wiederherstellen“. enable

clear factory

clear config

Wechsel in den Privileged-EXEC-Modus.

Den Lieferzustand im NVM und ACA herstellen.

Löschen der aktuellen Konfiguration inklusive der IP-Parameter.

Einstellung im System-Monitor:

☐ Wählen Sie 5 „Erase main configuration file“

Dieser Menüpunkt bietet Ihnen die Möglichkeit, die Konfiguration des Gerätes in seinen Lieferzustand zu versetzen.

☐ Drücken sie die Eingabetaste, um die Konfiguration des Lieferzustandes herzustellen.

Anmerkung: Das Gerät löscht die Tabellen, Einstellungen und Dateien auf dem Gerät und auf einem angeschlossenen ACA.

Anmerkung: Das Kommando „clear config“ löscht nicht den Namen der aktuellen Konfiguration. Verwenden Sie das Kommando „save profile“, um die gelöschte Konfiguration unter einem neuen Namen abzuspeichern.

4.1.4 Laden der aktiven Konfiguration

Das Gerät bietet Ihnen die Möglichkeit, die aktive Konfiguration zu laden.

- ☐ Wählen Sie den Dialog

Grundeinstellungen:Laden/Speichern.

- ☐ Klicken Sie auf „Laden vom NVM“, wenn Sie die aktive Konfiguration aus dem nicht-flüchtigen Speicher laden wollen.

enable

Wechsel in den Privileged-EXEC-Modus.

copy config nv running-config

Aktive Konfiguration laden.

4.1.5 Kopieren von Konfigurationsdateien

■ Kopieren von einem PC auf das Gerät

Das Gerät bietet Ihnen die Möglichkeit, eine Konfigurationsdatei von einem PC auf das Gerät zu kopieren.

- ☐ Wählen Sie den Dialog
Grundeinstellungen:Laden/Speichern.
 - ☐ Klicken Sie neben der NVM-Konfigurationstabelle auf „Kopieren vom PC“.
 - ☐ Klicken Sie im Datei-Auswahl-Rahmen auf „...“.
 - ☐ Wählen Sie im Datei-Auswahl-Fenster die Konfigurationsdatei (*.cfg) aus und klicken Sie auf „Speichern“.
 - ☐ Klicken Sie im Datei-Auswahl-Rahmen auf „Kopieren vom PC“.
- Das Ende der Upload-Aktion wird durch eine der folgenden Meldungen angezeigt:
- ▶ Update erfolgreich beendet.
 - ▶ Datei nicht gefunden, Ursache: Dateiname nicht gefunden oder nicht vorhanden.

■ Kopieren von einem PC auf den ACA

Das Gerät bietet Ihnen die Möglichkeit, eine Konfigurationsdatei von einem PC auf den ACA zu kopieren.

- ☐ Wählen Sie den Dialog
Grundeinstellungen:Laden/Speichern.
 - ☐ Klicken Sie neben der ACA-Konfigurationstabelle auf „Kopieren vom PC“.
 - ☐ Klicken Sie im Datei-Auswahl-Rahmen auf „...“.
 - ☐ Wählen Sie im Datei-Auswahl-Fenster die Konfigurationsdatei (*.cfg) aus und klicken Sie auf „Speichern“.
 - ☐ Klicken Sie im Datei-Auswahl-Rahmen auf „Kopieren vom PC“.
- Das Ende der Upload-Aktion wird durch eine der folgenden Meldungen angezeigt:
- ▶ Update erfolgreich beendet.
 - ▶ Datei nicht gefunden, Ursache: Dateiname nicht gefunden oder nicht vorhanden.

Bei einem Neustart übernimmt das Gerät die Konfigurationsdaten des ACA und speichert sie im Flash-Speicher. Enthält der angeschlossene ACA keine gültigen Daten, z.B. wenn er im Lieferzustand ist, dann lädt das Gerät die Daten aus dem Flash-Speicher.

Vor dem Laden der Konfigurationsdaten vom ACA vergleicht das Gerät das Passwort im Gerät mit dem Passwort in den Konfigurationsdaten des ACA .

Das Gerät übernimmt die Konfigurationsdaten, wenn

- ▶ das Admin-Passwort übereinstimmt oder
- ▶ lokal kein Passwort gespeichert ist oder
- ▶ lokal das Passwort im Lieferzustand ist oder
- ▶ lokal keine Konfiguration gespeichert ist.

■ Kopieren vom Gerät oder vom ACA auf einem PC

Das Gerät bietet Ihnen die Möglichkeit, eine Konfigurationsdatei des Gerätes oder des ACA auf einem PC zu speichern.

- ☐ Wählen Sie den Dialog

Grundeinstellungen:Laden/Speichern.

- ☐ Wählen Sie einen Tabelleneintrag

- des Gerätes (Konfiguration im nicht-flüchtigen Speicher (NVM)) oder
 - des ACA (Konfiguration auf dem AutoConfiguration Adapter (ACA))
- aus.

- ☐ Klicken Sie auf „Kopieren zum PC“.

- ☐ Wählen Sie im Datei-Auswahl-Fenster das gewünschte Verzeichnis aus und klicken Sie auf „Speichern“.

■ Kopieren vom ACA auf das Gerät

Das Gerät bietet Ihnen die Möglichkeit, eine Konfigurationsdatei vom ACA auf das Gerät zu speichern.

- ☐ Wählen Sie den Dialog

Grundeinstellungen:Laden/Speichern.

- ☐ Wählen Sie einen Tabelleneintrag des ACA (Konfiguration auf dem AutoConfiguration Adapter (ACA)) aus.

- ☐ Klicken Sie auf „Kopieren nach NVM“.

```
enable
copy config aca profile
<name> nv
```

Wechsel in den Privileged-EXEC-Modus.
Konfiguration „name“ auf das Gerät laden.

4.1.6 Anzeigen einer Konfigurationsdatei

Das Gerät bietet Ihnen die Möglichkeit, auf dem Gerät und auf dem ACA eine Konfigurationsdatei anzuzeigen.

- ☐ Wählen Sie den Dialog
Grundeinstellungen:Laden/Speichern.
- ☐ Wählen Sie einen Tabelleneintrag
 - des Gerätes (Konfiguration im nicht-flüchtigen Speicher (NVM)) oder
 - des ACA (Konfiguration auf dem AutoConfiguration Adapter (ACA))aus.
- ☐ Klicken Sie auf „Anzeigen“.

4.1.7 Löschen einer Konfigurationsdatei

Das Gerät bietet Ihnen die Möglichkeit, auf dem Gerät und auf dem ACA eine nicht-aktive Konfigurationsdatei zu löschen.

- ☐ Wählen Sie den Dialog
Grundeinstellungen:Laden/Speichern.
- ☐ Wählen Sie einen nicht aktiven Tabelleneintrag
 - des Gerätes (Konfiguration im nicht-flüchtigen Speicher (NVM)) oder
 - des ACA (Konfiguration auf dem AutoConfiguration Adapter (ACA))aus.
- ☐ Klicken Sie auf „Löschen“.

<code>enable</code>	Wechsel in den Privileged-EXEC-Modus.
<code>show config profiles nv</code>	Anzeige der im NVM gespeicherten Konfigurationen.
<code>profile delete nv <index></code>	Konfiguration mit dem angegebenen Index im NVM löschen.
<code>show config profiles aca</code>	Anzeige der im ACA gespeicherten Konfigurationen.
<code>profile delete aca <index></code>	Konfiguration mit dem angegebenen Index im ACA löschen.

4.1.8 SFTP-Zugriff auf Geräte-Dateien

Das Gerät bietet Ihnen die Möglichkeit, per SFTP auf Geräte-Dateien wie Konfigurationsdateien oder den ACA zuzugreifen, ein Firmware-Update oder VPN-Zertifikate auf das Gerät zu laden. Verwenden Sie dazu einen SFTP-Client, z. B. WinSCP. Für den SFTP-Zugriff ist der SSH-Zugriff auf das Gerät erforderlich.

Aktivieren Sie dazu den SSH-Zugriff auf das Gerät ([siehe auf Seite 108 „CLI-Zugriff konfigurieren“](#)).

4.1.9 Konfigurationsänderung widerrufen

Das Gerät bietet Ihnen die Möglichkeit, eine Konfigurationsänderung automatisch zu widerrufen, falls das Gerät durch eine Änderung seine Netzverbindung mit der Managementstation verliert, von der aus Sie das Gerät konfigurieren. Ein Beispiel ist das versehentliche Ändern der IP-Adresse des Geräts.

Sie können diese Funktion bei der Fernwartung des Geräts einsetzen.

Ist die Funktion aktiv, prüft das Gerät, ob es regelmäßig von der IP-Adresse der Managementstation aus angesprochen wird. Bleiben diese Anfragen eine bestimmte Zeit lang aus, ersetzt das Gerät seine aktuelle Konfiguration durch die zuletzt gespeicherte.

Diese Funktion ist nützlich für den Administrator, wenn das Gerät weit entfernt oder schwer zugänglich ist.

Lieferzustand: Funktion: aus, Wartezeit: 600 s.

Anmerkung: Schalten Sie die Funktion nach erfolgreicher Speicherung der Konfiguration aus. Das hilft Ihnen zu vermeiden, dass das Gerät die Konfiguration erneut lädt, nachdem Sie das Web-Interface schließen.

- ☐ Wählen Sie den Dialog
Grundeinstellungen:Laden/Speichern.
- ☐ Zum Einschalten der Funktion markieren Sie „Funktion“ im Rahmen „Konfigurationsänderung widerrufen“.
- ☐ Geben Sie die Wartezeit bei „Periode bis zum Widerruf bei Verbindungsunterbrechung“ ein.
- ☐ Um die Änderungen flüchtig zu speichern, klicken Sie „Schreiben“.
- ☐ Klicken Sie auf „Laden“, um im Feld „Watchdog-IP-Adresse“ die IP-Adresse Ihrer Managementstation anzuzeigen.

- ☐ Zum Ausschalten der Funktion entfernen Sie die Markierung bei „Funktion“ im Rahmen „Konfigurationsänderung widerrufen“.
- ☐ Um die Änderungen flüchtig zu speichern, klicken Sie „Schreiben“.
- ☐ Klicken Sie anschließend auf „Laden“. Das Feld „Watchdog-IP-Adresse“ zeigt nun 0.0.0.0 an.

<code>enable</code>	Wechsel in den Privileged-EXEC-Modus.
<code>show config-watchdog</code>	Anzeige der Einstellungen für den automatischen Widerruf einer Konfigurationsänderung bei Verbindungsunterbrechung.
<code>configure</code>	Wechsel in den Konfigurationsmodus.
<code>config-watchdog admin-state enable</code>	Einschalten des automatischen Widerrufs einer Konfigurationsänderung bei Verbindungsunterbrechung.
<code>config-watchdog admin-state disable</code>	Ausschalten des automatischen Widerrufs einer Konfigurationsänderung bei Verbindungsunterbrechung.
<code>config-watchdog timeout 300</code>	Einstellungen des Timeouts für den automatischen Widerruf einer Konfigurationsänderung bei Verbindungsunterbrechung auf 300 s.

4.2 Neueste Software laden

Hirschmann arbeitet ständig an der Leistungssteigerung der Produkte. Deshalb besteht die Möglichkeit, dass Sie auf der Internetseite von Hirschmann (www.hirschmann.com) eine neuere Release der Geräte-Software finden, als die Release, die auf Ihrem Gerät gespeichert ist.

4.2.1 Prüfen der installierten Software-Release

- ☐ Wählen Sie den Dialog `Grundeinstellungen:Software`.
- ☐ Dieser Dialog zeigt Ihnen die Variante, die Release-Nr. und das Datum der im Gerät gespeicherten Software an.
 - ▶ „Gespeicherte Version“: die Software im nichtflüchtigen Speicher
 - ▶ „Laufende Version“: die momentan ausgeführte Software
 - ▶ „Backup-Version“: die Backup-Software im nichtflüchtigen Speicher

```

enable                                Wechsel in den Privileged-EXEC-Modus.
show system info                      Anzeigen der Systeminformation.
System information
-----
System Description..... Hirschmann EAGLE Security Device
System Name..... EAGLEONE-574C67
System Location..... Hirschmann EAGLE
System Contact..... Hirschmann Automation and Control
                        GmbH
System Uptime..... 0 days 5 hours 0 minutes 0 seconds
System Date and Time (local time zone)... THU OCT 15 08:08:08 2013
OS Software Release..... ONE-05.3.00 2013-10-15 08:08
OOS Software Release (ROM).... ONE-05.3.00 2013-10-15 08:08
Software Release (BAK)..... ONE-05.3.00 2013-10-15 09:09
Device Hardware Revision..... 0101
Device Hardware Description... EagleOne-0200T1T1
Serial Number..... 943011301020201679
Network Operation Mode..... Transparent Mode
IP address (management)..... 10.0.1.203
MAC address (management)..... 00:80:63:57:4c:67
Configuration state (running to NV)..... ok
Configuration state (NV to ACA)..... In sync.
Auto Configuration Adapter, Serial Num.. 9432710010101254
Power Supply P1, State..... ok
Power Supply P2, State..... ok
Temperature (°C)..... 47

Alarm..... None

```

4.2.2 Software laden

Das Gerät bietet zwei Möglichkeiten die Software zu laden:

- ▶ vom ACA 21-USB (out-of-band),
- ▶ über ein Datei-Auswahl-Fenster von Ihrem PC.

Anmerkung: Die Konfiguration des Gerätes bleibt nach der Installation der neuen Software erhalten.

4.2.3 Software vom ACA laden

Den ACA 21-USB können Sie wie einen gewöhnlichen USB-Stick an einen USB-Port Ihres PCs anschließen und die Geräte-Software in das Hauptverzeichnis des ACA 21-USB kopieren.

- ☐ Verbinden Sie den ACA 21-USB, auf den Sie die Geräte-Software kopiert haben, mit dem USB-Port des Gerätes.

■ Laden mit dem Systemmonitor

- ☐ Öffnen Sie den System-Monitor ([siehe Seite 24 „System-Monitor starten“](#)).
- ☐ Wählen Sie 2 und drücken Sie die Eingabetaste, um die Software vom ACA 21-USB in den lokalen Speicher des Gerätes zu kopieren.
- ☐ Geben Sie den Dateinamen der Firmware ein und bestätigen Sie die Eingabe durch drücken der Eingabetaste.
- ☐ Starten Sie den Ladevorgang durch drücken der Eingabetaste.
Am Ende des Ladevorgangs fordert Sie der System-Monitor auf, eine beliebige Taste zu drücken, um fortzufahren.
- ☐ Wählen Sie 3, um die neue Software auf dem Geräte zu starten.

Der System-Monitor bietet Ihnen weitere Möglichkeiten, die in Zusammenhang mit der Software auf Ihrem Gerät stehen:

- ▶ Auswahl der zu ladenden Software,
- ▶ Starten der Software,
- ▶ Kaltstart durchführen

■ Laden mit dem Command Line Interface

- ☐ Öffnen Sie das Command Line Interface ([siehe auf Seite 27 „Öffnen des Command Line Interfaces“](#)).

```
enable
copy firmware aca filename
eagleONE.bin nv

Are you sure (Y/N) ? Y
```

Wechsel in den Privileged-EXEC-Modus.

Die Firmware mit dem Dateinamen „eagleONE.bin“ in den nicht-flüchtigen Speicher laden.

Vorgang mit „Y“ bestätigen.

■ Kaltstart durchführen

```
enable
reboot
```

Wechsel in den Privileged-EXEC-Modus.

Kaltstart durchführen.

Im System-Monitor:

Der Menüpunkt „End (reset and reboot)“ des System-Monitors bietet Ihnen die Möglichkeit, die Hardware des Gerätes zurückzusetzen und einen Neustart durchzuführen.

4.2.4 Software über Datei-Auswahl laden

Für ein Software-Update über das Datei-Auswahl-Fenster kopieren Sie die Geräte-Software auf einem Datenträger, den Sie von Ihrem PC aus erreichen.

- ☐ Klicken Sie im Datei-Auswahl-Rahmen auf „...“.
- ☐ Wählen Sie im Datei-Auswahl-Fenster die Geräte-Software (eagleONE.bin) aus und klicken Sie auf „Öffnen“.
- ☐ Klicken Sie auf „HTTPS-Update“, um die Software auf das Gerät zu übertragen.

Das Ende der Update-Aktion wird durch eine der folgenden Meldungen angezeigt:

- ▶ Update erfolgreich beendet.
 - ▶ Update fehlgeschlagen, Ursache: Falsche Datei.
 - ▶ Update fehlgeschlagen, Ursache: Fehler beim Abspeichern.
- ☐ Nach erfolgreichem Laden aktivieren Sie die neue Software:
Wählen Sie den Dialog `Grundeinstellungen: Neustart` und führen Sie einen Kaltstart durch.
Bei einem Kaltstart lädt das Gerät die Software neu aus dem nicht-flüchtigen Speicher, startet neu und führt einen Selbsttest durch.
 - ☐ Klicken Sie in Ihrem Browser auf „Neu laden“, um nach dem Booten des Gerätes wieder auf das Gerät zugreifen zu können.

4.3 Ports konfigurieren

Die Portkonfiguration umfasst:

- ▶ Portnamen eingeben,
- ▶ Port ein-/ausschalten,
- ▶ Betriebsart wählen,
- ▶ Meldung erkannter Verbindungsfehler,

■ Portnamen eingeben

Die Tabellenspalte „Name“ bietet Ihnen die Möglichkeit, dem Port einen beliebigen Namen zu geben.

■ Port ein-/ausschalten

Im Lieferzustand sind die Ports eingeschaltet.

- ☐ Wählen Sie den Dialog

Grundeinstellungen:Portkonfiguration.

- ☐ Wählen Sie in der Spalte „Port an“ die Ports aus, die mit einem anderen Gerät verbunden sind.

■ Betriebsart wählen

Im Lieferzustand befinden sich die Ports im Betriebsmodus „Automatische Konfiguration“.

Anmerkung: Die aktive automatische Konfiguration hat Vorrang vor der manuellen Konfiguration.

- ☐ Wählen Sie den Dialog

Grundeinstellungen:Portkonfiguration.

- ☐ Falls das an diesem Port angeschlossene Gerät eine feste Einstellung voraussetzt
 - wählen Sie in der Spalte „Manuelle Konfiguration“ die Betriebsart (Übertragungsgeschwindigkeit, Duplexbetrieb) und
 - deaktivieren Sie in der Spalte „Automatische Konfiguration“ den Port.

■ **Erkannte Kommunikationsunterbrechung melden**

Im Lieferzustand zeigt das Gerät einen ermittelten Verbindungsfehler über den Meldekontakt und die LED-Anzeige an. Das Gerät erlaubt Ihnen, diese Anzeige zu unterdrücken. Auf diese Weise vermeiden Sie z. B., ein ausgeschaltetes Gerät fälschlicherweise als unterbrochene Verbindung zu interpretieren.

- ☐ Wählen Sie den Dialog
Grundeinstellungen:Portkonfiguration.
- ☐ Selektieren Sie in der Spalte „Verbindungsfehler weitermelden“ die Ports aus, bei denen Sie eine Verbindungsüberwachung wünschen.

4.4 Die Systemzeit im Netz synchronisieren

Das Gerät bietet Ihnen die Möglichkeit, die Zeit in Ihrem Netz zu synchronisieren.

Was Echtzeit wirklich bedeutet, hängt von den Zeitanforderungen der Anwendung ab.

Mit Hilfe von NTP kann das Gerät die Zeit genauer bestimmen als mit SNTP. Somit kann es als NTP-Server auch eine genauere Uhrzeit anbieten.

Anwendungsgebiete sind beispielsweise:

- ▶ Logbucheinträge
- ▶ Produktionsdaten mit Zeitstempel versehen
- ▶ Prozesssteuerung

4.4.1 Uhrzeit einstellen

Steht Ihnen keine Referenzuhr zur Verfügung, dann haben Sie die Möglichkeit, die Systemzeit vom PC zu übernehmen. Das Gerät setzt bei einem Neustart die Zeit zurück.

Anmerkung: Passen Sie in Zeitzonen mit Sommer-/Winterzeit den lokalen Offset bei der Zeiteinstellung an, falls erforderlich.

Der SNTP-Client kann die SNTP-Server-IP-Adressen und den lokalen Offset auch von einem DHCP-Server beziehen.

Der NTP-Client bezieht seine NTP-Server-IP-Adressen ausschließlich aus der Konfiguration, die Sie einstellen.

- ☐ Wählen Sie den Dialog `Zeit:Grundeinstellungen`.

Dieser Dialog bietet Ihnen die Möglichkeit, zeitbezogene Einstellungen vorzunehmen.

- ▶ Die „Systemzeit (UTC)“ zeigt die Uhrzeit bezogen auf die koordinierte Weltzeitskala UTC (Universal Time Coordinated) an. Die Anzeige ist weltweit gleich. Lokale Zeitverschiebungen bleiben unberücksichtigt.
Mögliche Quellen der Systemzeit (UTC) sind: `local`, `sntp` und `ntp`, siehe „Quelle der Zeit“.
- ▶ Die „Systemzeit“ berechnet das Gerät aus der „Systemzeit (UTC)“ und dem „lokalen Offset“ (der lokalen Zeitdifferenz zur UTC).
„Systemzeit“ = „Systemzeit (UTC)“ + „Lokaler Offset“.
- ▶ „Quelle der Zeit“ zeigt den Ursprung der Systemzeit (UTC) an. Das Gerät wählt automatisch die verfügbare Quelle mit der höchsten Genauigkeit.
Mögliche Quellen sind: `local`, `sntp` und `ntp`.
 - Die Quelle ist zunächst `local`. Dies ist die Systemuhr des Gerätes.
 - Haben Sie den SNTP-Client aktiviert und empfängt das Gerät ein gültiges SNTP-Paket, setzt es seine Zeit-Quelle auf `sntp`.
 - Haben Sie den NTP-Client aktiviert und hat sich dieser synchronisiert, setzt es seine Zeit-Quelle auf `ntp`.
- ☐ Mit „Setze Zeit vom PC“ übernimmt das Gerät die Zeit des PCs als Systemzeit und berechnet mit der lokalen Zeitdifferenz die IEEE 1588 / SNTP-Zeit.
„IEEE 1588 / SNTP-Zeit“ = „Systemzeit“ - „Lokaler Offset“
- ☐ Lokaler Offset dient zur Anzeige/Eingabe der Zeitdifferenz zwischen der lokalen Zeit und der „Systemzeit (UTC)“.

Mit „Setze Offset vom PC“ ermittelt das Gerät die Zeitzone auf Ihrem PC und berechnet daraus die lokale Zeitdifferenz.

<code>enable</code>	Wechsel in den Privileged-EXEC-Modus.
<code>configure</code>	Wechsel in den Konfigurationsmodus.
<code>sntp time <YYYY-MM-DD HH:MM:SS></code>	Einstellen der Systemzeit des Gerätes.
<code>sntp client offset <-1000 to 1000></code>	Eingeben der Zeitdifferenz zwischen der lokalen Zeit und der „SNTP-Zeit“.

4.4.2 SNTP

■ Beschreibung SNTP

Das Simple Network Time Protocol (SNTP) bietet Ihnen die Möglichkeit, die Systemzeit in Ihrem Netz zu synchronisieren.

Das Gerät unterstützt die SNTP-Client- und die SNTP-Server-Funktion.

Der SNTP-Server stellt die UTC (Universal Time Coordinated) zur Verfügung. Die UTC ist die auf die koordinierte Weltzeitmessung bezogene Uhrzeit. Die Anzeige ist weltweit gleich. Lokale Zeitverschiebungen bleiben unberücksichtigt.

SNTP verwendet dasselbe Paketformat wie NTP, daher kann ein SNTP-Client seine Zeit sowohl von einem SNTP-Server als auch von einem NTP-Server beziehen.

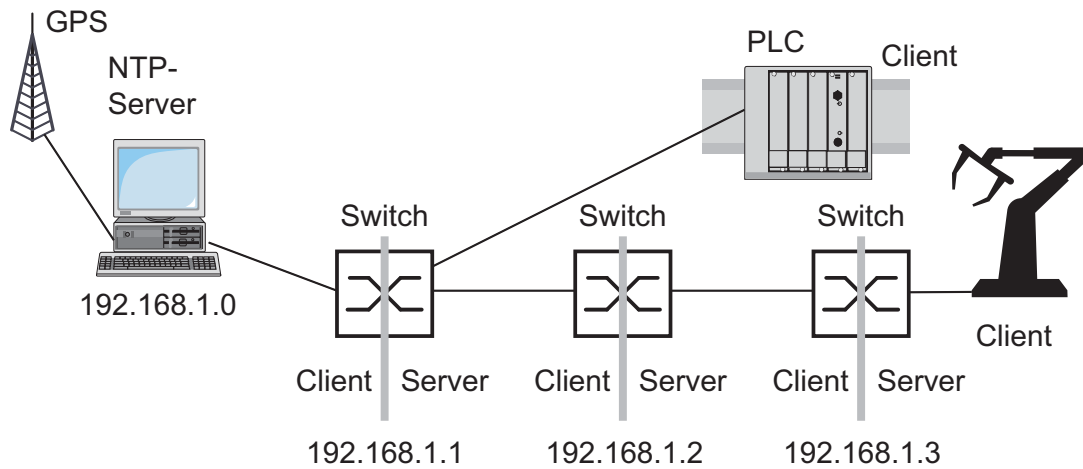


Abb. 13: SNTP-Kaskade

■ Vorbereitung der SNTP-Konfiguration

- ☐ Zeichnen Sie einen Netzplan mit den am SNTP beteiligten Geräten, um einen Überblick über die Weitergabe der Uhrzeit zu erhalten. Beachten Sie bei der Planung, dass die Genauigkeit der Uhrzeit von der Signallaufzeit abhängig ist.

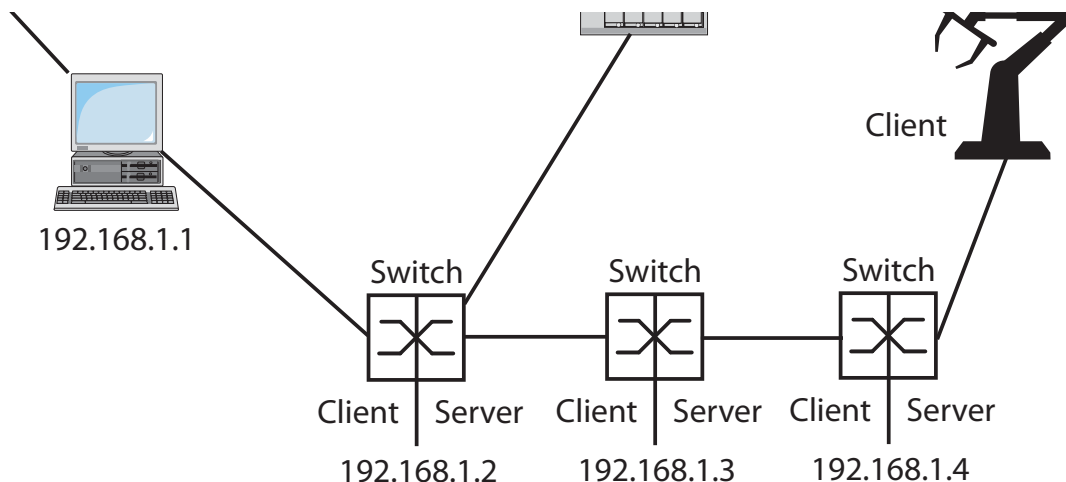


Abb. 14: Beispiel SNTP-Kaskade

- ☐ Schalten Sie die SNTP-Funktion auf den Geräten ein, deren Zeit Sie mittels SNTP einstellen wollen. Der SNTP-Server des Geräts antwortet auf Unicast-Anfragen, sobald er eingeschaltet ist.
- ☐ Wenn Sie keine Referenzuhr zur Verfügung haben, dann bestimmen Sie ein Gerät als Referenzuhr und stellen Sie dessen Systemzeit möglichst genau ein.

Anmerkung: Für eine genaue Systemzeitverteilung mit kaskadierten SNTP-Servern und -Clients verwenden Sie im Signalpfad zwischen SNTP-Servern und SNTP-Clients ausschließlich Netzkomponenten (Router, Switches, Hubs), die SNTP-Pakete mit möglichst kleiner Verzögerung weiterleiten.

■ Konfiguration SNTP

- ☐ Wählen Sie den Dialog `Zeit:SNTP`.

▶ Funktion

- ☐ In diesem Rahmen schalten Sie die SNTP-Funktion global ein/aus.

Anmerkung: Wenn Sie SNTP einschalten, während NTP auf dem Gerät schon aktiv ist, meldet das Gerät einen erkannten Fehler. Um SNTP einzuschalten, deaktivieren Sie zuerst NTP. Im Lieferzustand ist NTP ausgeschaltet.

▶ SNTP-Status

- ☐ Die „Statusmeldung“ zeigt Zustände des SNTP-Clients als eine oder mehrere Textmeldungen an, z.B. `Server 1 antwortet nicht`.

▶ Konfiguration SNTP-Client

- ☐ In „Externe Server-Adresse“ geben Sie die IP-Adresse des SNTP- Servers ein, von dem das Gerät zyklisch die Systemzeit anfordert.
- ☐ In „Redundante Server-Adresse“ geben Sie die IP-Adresse eines weiteren SNTP-Servers ein. Von diesem fordert das Gerät die Systemzeit an, wenn es 1 Sekunde nach einer Anforderung an die „Externe Server-Adresse“ keine Antwort von dieser erhält.

Anmerkung: Wenn Sie von einer externen/redundanten Server-Adresse die Systemzeit beziehen, dann akzeptieren Sie keine SNTP-Broadcast-Pakete (siehe unten). Das hilft Ihnen sicherzustellen, dass das Gerät die Zeit des eingetragenen Servers verwendet.

- ☐ In „Server-Anforderungsintervall“ geben Sie den Zeitabstand ein, in dem das Gerät SNTP-Pakete anfordert (gültige Werte: 1 s bis 3.600 s, Lieferzustand: 30 s).
- ☐ Mit „SNTP-Broadcasts akzeptieren“ übernimmt das Gerät die Systemzeit aus SNTP-Broadcast-/Multicast-Paketen, die es empfängt.

▶ Konfiguration SNTP-Server

- ☐ In „Anycast-Zieladresse“ geben Sie die IP-Adresse an, an die der SNTP-Server des Gerätes seine SNTP-Pakete schickt (siehe Tab. 6).
- ☐ In „Anycast-Sendeintervall“ geben Sie den Zeitabstand an, in dem das Gerät SNTP-Pakete verschickt (gültige Werte: 1 s bis 3.600 s, Lieferzustand: 120 s).
- ☐ Mit „Server deaktivieren bei lokaler Zeitquelle“ schaltet das Gerät die SNTP-Server-Funktion aus, wenn die Quelle der Zeit `local` ist (siehe Dialog `Zeit:Grundeinstellungen`).

IP-Zieladresse	SNTP-Paket versenden an
0.0.0.0	Niemand
Unicast-Adresse (0.0.0.1 - 223.255.255.254)	Unicast-Adresse
Multicast-Adresse (224.0.0.0 - 239.255.255.254), insbesondere 224.0.1.1 (NTP-Adresse)	Multicast-Adresse
255.255.255.255	Broadcast-Adresse

Tab. 6: Zieladressklassen für SNTP- und NTP-Pakete

Gerät	192.168.1.1	192.168.1.2	192.168.1.3
Funktion	an	an	an
Server Zieladresse	0.0.0.0	0.0.0.0	0.0.0.0
Server VLAN-ID	1	1	1
Sendeintervall	120	120	120
Client Externe Server Adresse	192.168.1.0	192.168.1.1	192.168.1.2
Anforderungsintervall	30	30	30
Broadcasts akzeptieren	nein	nein	nein

Tab. 7: Einstellungen für das Beispiel (siehe Abb. 14)

4.4.3 NTP

Das Network Time Protocol (NTP) bietet Ihnen die Möglichkeit, die Systemzeit in Ihrem Netz zu synchronisieren. Das Gerät unterstützt die NTP-Client- und die NTP-Server-Funktion.

Das Gerät kann mit Hilfe von NTP die Zeit genauer bestimmen als mit SNTP. Somit kann es als NTP-Server auch eine genauere Uhrzeit anbieten.

Das Paketformat von NTP und SNTP ist identisch.

Der NTP-Client verwendet im Gegensatz zum SNTP-Client mehrere NTP-Server und einen aufwändigeren Algorithmus zur Synchronisation. Damit kann er die Zeit genauer bestimmen. Die Synchronisation des NTP-Clients kann daher länger dauern als bei einem SNTP-Client.

Verwenden Sie NTP ausschließlich dann, wenn Sie eine höhere Genauigkeit benötigen.

Der NTP-Server stellt die UTC (Universal Time Coordinated) zur Verfügung. Die UTC ist die auf die koordinierte Weltzeitmessung bezogene Uhrzeit. Die Anzeige ist weltweit gleich. Lokale Zeitverschiebungen bleiben unberücksichtigt.

Der NTP-Client bezieht die UTC von einem oder mehreren externen NTP-Servern.

Anmerkung: Für eine möglichst genaue Systemzeitverteilung verwenden Sie für einen NTP-Client mehrere NTP-Server.

Anmerkung: Wenn Sie NTP einschalten (einen anderen Wert als `off` einstellen), während SNTP auf dem Gerät schon aktiv ist, meldet das Gerät einen erkannten Fehler.

Um NTP einzuschalten, deaktivieren Sie zuerst SNTP.

Im Lieferzustand ist SNTP ausgeschaltet.

5 Unterstützung beim Schutz vor unberechtigtem Zugriff

Das Gerät bietet folgende Funktionen zur Unterstützung gegen unberechtigte Zugriffe:

- ▶ Passwort-geschützter Web-Zugriff
- ▶ Passwort-geschützter CLI-Zugriff
- ▶ Passwort-geschützter Netzmanagement-Zugriff
- ▶ HiDiscovery-Funktion
- ▶ Benutzer-Authentifizierung

Anmerkung: Ändern Sie aus Sicherheitsgründen das Passwort des Lieferzustandes. Das hilft Ihnen, einen Zugriff auf das Gerät mit diesem Passwort zu verhindern. Ist das Passwort im Lieferzustand, dann zeigt das Gerät in allen Dialogen in der Kopfzeile „Standardpassword“ an.

Anmerkung: Wählen Sie Ihr Passwort so, dass Sie es sich merken können.

Wenn Sie Ihr Passwort erstellen, verzichten Sie auf

- ▶ kurze Wörter und Zeichenfolgen,
- ▶ Wörter und Zeichenfolgen, die einen Sinn ergeben (z.B. Namen, Jahreszahlen, Geburtstage),
- ▶ Zitate,
- ▶ Aneinanderreihungen einfacher Wörter.

Wenn Sie Ihr Passwort erstellen, benutzen Sie

- ▶ lange Wörter und Zeichenfolgen,
- ▶ Wörter und Zeichenfolgen, die scheinbar keinen Sinn ergeben (z.B. Anfangsbuchstaben der Wörter eines Satzes),
- ▶ seltene Wörter,
- ▶ Phantasiewörter,

- ▶ Kombinationen aus Buchstaben, Ziffern und Sonderzeichen. (Beachten Sie bei der Wahl von Sonderzeichen, dass diese möglicherweise auf ausländischen Tastaturen nicht zur Verfügung stehen.),
- ▶ Änderung und Verfälschung der Schreibweise (z.B. „plAuer FOGel“ statt „Blauer Vogel“).

Anmerkung: Im Lieferzustand ist der SNMPv1- und der SNMPv2-Zugriff ausgeschaltet. Da SNMPv1 und SNMPv2 die Daten unverschlüsselt übertragen, stellt die Verwendung von SNMPv1 und SNMPv2 ein potentiell Sicherheitsrisiko dar. Lassen Sie den SNMPv1- oder SNMPv2-Zugriff ausschließlich dann zu, wenn Sie eine Anwendung, die dies erfordert, einsetzen wollen.

Anmerkung: Im Lieferzustand erlaubt das Gerät den SSH-, SNMPv3- und HTTPS-Zugang.

Anmerkung: Im Lieferzustand erlaubt die Firewall am internen Port den ausgehenden IP-Verkehr sowie den Management-Zugriff (SNMP, HTTPS und SSH) auf das Gerät. Wenn Sie den Management-Zugriff deaktivieren möchten, haben Sie folgende Möglichkeiten:

- ▶ Definieren Sie explizite `drop`-Regeln für den Management-Zugriff.
- ▶ Ändern Sie die entsprechenden Firewall-Regeln für den ausgehenden IP-Verkehr.

5.1 Zugriff via grafische Benutzeroberfläche

Auf die grafische Benutzeroberfläche greifen Sie mit dem Hypertext Transfer Protocol Secure (HTTPS) zu.

HTTPS beinhaltet eine Authentifizierung und eine Verschlüsselung der zu übertragenden Daten. Basis für beides ist ein Zertifikat.

Im Lieferzustand bietet das Gerät ein Hirschmann-Zertifikat. Beim Starten der grafischen Benutzeroberfläche über den Browser wird Sie Ihr Browser, abhängig von dessen Voreinstellungen, fragen, ob Sie dem Zertifikat vertrauen.

Im Dialog `Sicherheit:Web-Zugriff` können Sie ein anderes Zertifikat von Ihrem PC auf das Gerät laden.

Anmerkung: Das Gerät akzeptiert HTTPS-Server-Zertifikate mit einer Schlüssellänge zwischen 512 und 2048 Bits (RSA-Schlüssel im PEM-Format mit nicht-verschlüsseltem privatem Schlüssel).

Vom Server unterstützte Verschlüsselungs-Algorithmen:

- ▶ SSLv3: AES128-SHA
- ▶ TLSv1: AES256-SHA AES128-SHA DES-CBC3-SHA

5.1.1 Beschreibung Zugriff via grafische Benutzeroberfläche

Das Gerät unterstützt Sie beim Schutz des Zugriffs auf die grafische Benutzeroberfläche auf mehrere Arten:

- ▶ Passwort
- ▶ Wahl des SNMP-Ports
Für den Zugriff auf die grafische Benutzeroberfläche benutzt Ihr Browser eine Java-Anwendung, die er vom Gerät herunterlädt. Diese Java-Anwendung kommuniziert über SNMPv3 mit dem Gerät.
Standardmäßig benutzen Anwendungen den Port 161 für eine SNMP-Verbindung.
Das Gerät bietet Ihnen die Möglichkeit, einen anderen Port zu verwenden
- ▶ Alternativ bietet Ihnen das Gerät die Möglichkeit, die SNMP-Zugriffe der grafischen Benutzeroberfläche auf das Gerät durch HTTPS zu tunneln. Damit sind ausschließlich HTTPS-Verbindungen zum Gerät notwendig. Im Lieferzustand ist die Funktion SNMP über HTTPS (Tunnel) inaktiv.
- ▶ Aktivieren/Deaktivieren
- ▶ Wahl des HTTPS-Ports
Für den Zugriff auf die grafische Benutzeroberfläche baut Ihr Browser eine HTTPS-Verbindung zum Gerät auf. Standardmäßig benutzen Anwendungen den Port 443 für eine HTTPS-Verbindung.
Das Gerät bietet Ihnen die Möglichkeit, einen anderen Port zu verwenden
- ▶ Einschränken der für den Zugriff erlaubten IP-Adressen pro Port
Im Lieferzustand können Sie mit jeder IP-Adresse über den internen Port auf das Gerät zugreifen. Das Gerät bietet Ihnen die Möglichkeit, pro Port festzulegen, von welcher IP-Adresse das Gerät einen Zugriff erlaubt oder ablehnt.
- ▶ Automatisches Abmelden nach Inaktivität.

5.1.2 Zugriff via grafische Benutzeroberfläche konfigurieren

Zur Unterstützung beim Zugriffsschutz nutzen Sie die Möglichkeiten, die Ihnen das Gerät bietet.

Die Abbildung zeigt ein typisches Beispiel für den Zugriff auf den internen Port der Firewall.

Die folgende Tabelle enthält beispielhaft die Parameter für das anschließende Konfigurationsbeispiel.

Parameter	Wert
Lesepasswort	Heinrich5
Schreib/Lesepasswort	Ludwig14
SNMP-Port	9223
SNMP-Quelladresse interner Port	10.0.1.17/24
Web-Server aktiv	ja
HTTPS-Port	9027
HTTPS-Quelladresse interner Port	10.0.1.17/24

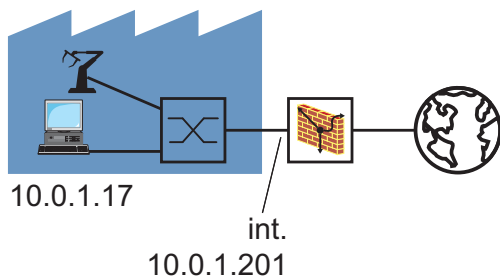


Abb. 15: Zugriff via grafische Benutzeroberfläche Anwendungsbeispiel

☐ Geben Sie neue Passwörter ein.

☐ Wählen Sie den Dialog `Sicherheit:Passwort`.

- ☐ Wählen Sie „Lese Passwort ändern (user)“, um das Lese Passwort einzugeben.
- ☐ Geben Sie das neue Lese Passwort in der Zeile „Neues Passwort“ ein und wiederholen Sie die Eingabe in der Zeile „Bitte nochmals eingeben“.
- ☐ Wählen Sie „Schreib-/Lese Passwort ändern (admin)“, um das Schreib-/Lese Passwort einzugeben.
- ☐ Geben Sie das Schreib-/Lese Passwort ein und wiederholen Sie die Eingabe.

Anmerkung: Wenn Sie kein Passwort mit der Berechtigung „schreiben/lesen“ kennen, haben Sie keine Möglichkeit, auf das Gerät schreibend zuzugreifen.

Anmerkung: Aus Sicherheitsgründen zeigt der Dialog die Passwörter in Form von Sternen an. Notieren Sie sich jede Änderung. Ohne gültiges Passwort können Sie nicht auf das Gerät zugreifen.

Anmerkung: Verwenden Sie bei SNMP Version 3 für das Passwort 5 bis 32 Zeichen, da viele Anwendungen keine kürzeren Passwörter akzeptieren.

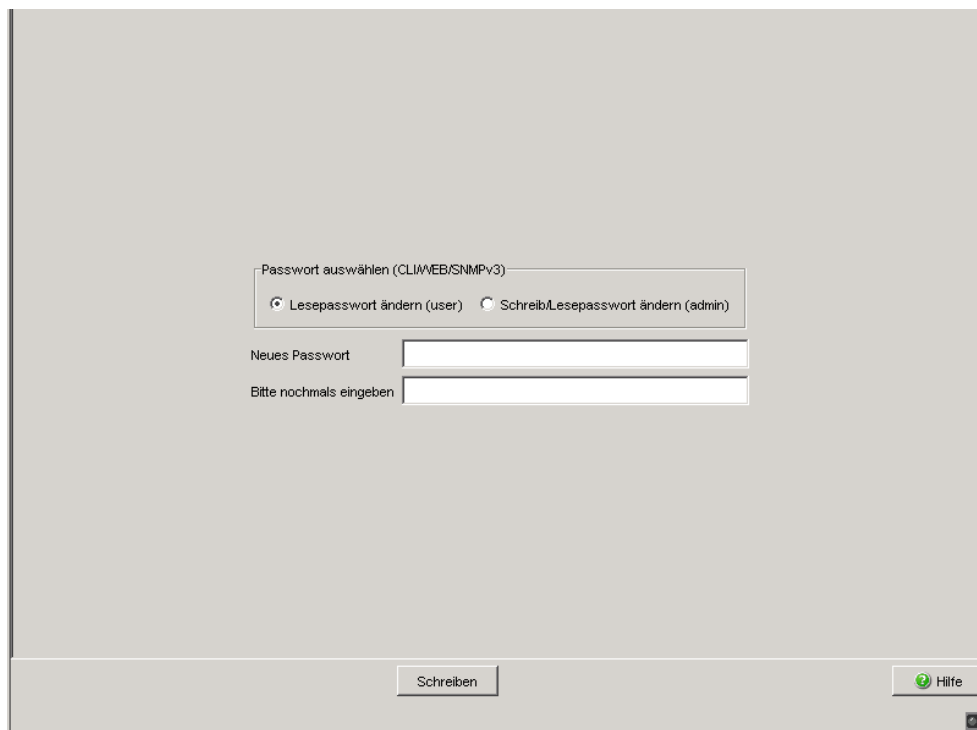


Abb. 16: Dialog Passwort

- ☐ Um die Änderungen flüchtig zu speichern, klicken Sie „Schreiben“.

- ☐ Konfigurieren Sie den SNMP-Zugriff.

- ☐ Wählen Sie den Dialog `Sicherheit:SNMP-Zugriff`.

- ☐ Ändern Sie den SNMP-Port auf z.B. 9223.

Einschränken der IP-Adressen, die über SNMP zugreifen dürfen:

- ☐ Klicken Sie auf „Eintrag erzeugen“.

- ☐ Wählen Sie in der Zelle „Port“ des neuen Eintrags in der Tabelle
int.

- ☐ Doppelklicken Sie in die Zelle „Quelladresse (CIDR) und geben Sie
die Quelladresse ein, z.B. 10.0.1.17.

Wenn dies der einzige aktive Eintrag in dieser Tabelle ist, dann kann
ausschließlich der PC mit dieser IP-Adresse über dieses Protokoll
zugreifen.

- ☐ Klicken Sie in das Feld „Aktiv“ dieses Eintrags, um den Eintrag zu
aktivieren.

- ☐ Um die Änderungen flüchtig zu speichern, klicken Sie „Schreiben“.

Konfiguration

SNMP-Port

SNMP über HTTPS (Tunnel) Konfiguration ☐ An ☒ Aus

Index	Port	Quelladresse (CIDR)	Aktion	Log	Beschreibung	Aktiv	Fehler
-------	------	---------------------	--------	-----	--------------	-------	--------

Schreiben Laden Erzeugen Löschen ↑ ↓ Hilfe

Abb. 17: Dialog SNMP-Zugriff

☐ Konfigurieren Sie den Web-Zugriff.

☐ Wählen Sie den Dialog `Sicherheit:Web-Zugriff`.

☐ Ändern Sie den HTTPS-Port auf z.B. 9027.

Einschränken der IP-Adressen, die über HTTPS zugreifen dürfen:

☐ Klicken Sie auf „Eintrag erzeugen“.

☐ Wählen Sie in der Zelle „Port“ des neuen Eintrags in der Tabelle
int.

☐ Doppelklicken Sie in die Zelle „Quelladresse (CIDR) und geben Sie
die Quelladresse ein, z.B. 10.0.1.17.

Wenn dies der einzige aktive Eintrag in dieser Tabelle ist, dann kann
ausschließlich der PC mit dieser IP-Adresse über dieses Protokoll
zugreifen.

☐ Klicken Sie in das Feld „Aktiv“ dieses Eintrags, um den Eintrag zu
aktivieren.

☐ Um die Änderungen flüchtig zu speichern, klicken Sie „Schreiben“.

Index	Port	Quelladresse (CIDR)	Aktion	Log	Beschreibung	Aktiv	Fehler
1	ext	any	accept	disable		☒	

Abb. 18: Dialog Web-Zugriff

☐ Konfigurieren Sie das automatische Abmelden.

- ☐ Wählen Sie den Dialog *Abmelden*.
- ☐ Klicken Sie im Rahmen „Grafische Benutzeroberfläche“ in der Zeile „Automatisch“ auf „An“.
- ☐ Geben Sie in der Zeile „Nach [min]“ die Anzahl von Minuten ein, nach welcher das Gerät die HTTPS-Verbindung automatisch bei Inaktivität beendet.
- ☐ Um die Änderungen flüchtig zu speichern, klicken Sie „Schreiben“.

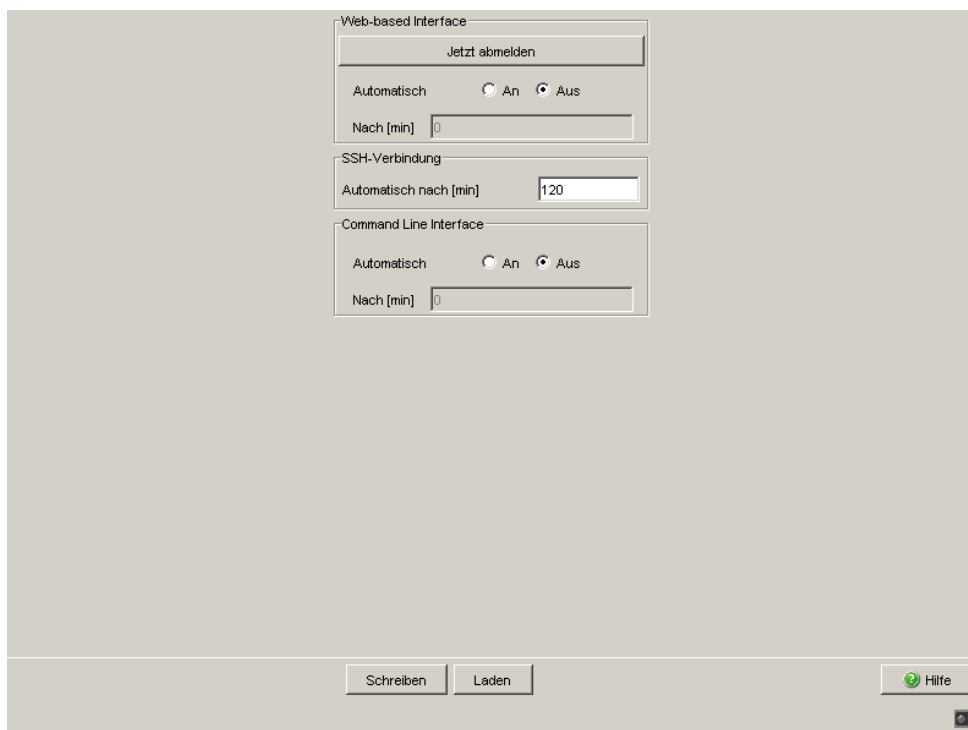


Abb. 19: Dialog Abmelden

☐ Speichern Sie die Einstellungen in den nicht-flüchtigen Speicher.

- 
- ☐ Öffnen Sie hierzu den Dialog Grundeinstellungen:Laden/Speichern.
 - ☐ Klicken Sie auf „Speichern in NVM + ACA“, um die Daten nicht-flüchtig zu speichern.

5.2 CLI-Zugriff

Für den Zugriff auf das Command Line Interface (CLI) benötigen Sie eine direkte Verbindung von Ihrem PC zum Seriellen Port oder eine Secure Shell (SSH)-Verbindung zu Ihrem Gerät ([siehe auf Seite 234 „Zugriff mittels SSH“](#)).

5.2.1 Beschreibung CLI-Zugriff

Das Gerät hilft Ihnen beim Schutz des Zugriffs auf das CLI auf mehrere Arten:

- ▶ Passwort
- ▶ Aktivieren/Deaktivieren
Nach dem Abschalten des SSH-Servers hilft das Gerät beim Verhindern eines erneuten Zugriffs über eine neue SSH-Verbindung. Eine bestehende SSH-Verbindung bleibt erhalten.
- ▶ Wahl des SSH-Ports
Standardmäßig benutzen Anwendungen den Port 22 für eine SSH-Verbindung.
Das Gerät bietet Ihnen die Möglichkeit, einen anderen Port zu verwenden
- ▶ Einschränken der für den Zugriff erlaubten IP-Adressen pro Port
Im Lieferzustand können Sie mit jeder IP-Adresse über den internen Port auf das Gerät zugreifen. Das Gerät bietet Ihnen die Möglichkeit, pro Port festzulegen, von welcher IP-Adresse das Gerät einen Zugriff erlaubt oder ablehnt.
- ▶ Automatisches Abmelden nach Inaktivität.

5.2.2 CLI-Zugriff konfigurieren

Zur Unterstützung beim Zugriffsschutz nutzen Sie die Möglichkeiten, die Ihnen das Gerät bietet.

Die Abbildung zeigt ein typisches Beispiel für den Zugriff auf den internen Port der Firewall.

Die folgende Tabelle enthält beispielhaft die Parameter für das anschließende Konfigurationsbeispiel.

Parameter	Wert
Lesepasswort	Heinrich5
Schreib/Lesepasswort	Ludwig14
SSH-Zugriff aktiv	ja
SSH-Port	9234
SSH-Quelladresse interner Port	10.0.1.17/24

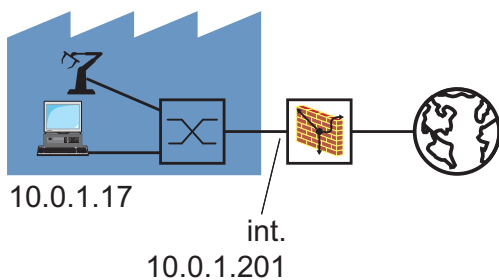


Abb. 20: Command Line Interface-Zugriff Anwendungsbeispiel

☐ Geben Sie neue Passwörter ein.

- ☐ Wählen Sie den Dialog `Sicherheit:Passwort`.
- ☐ Wählen Sie „Lesepasswort ändern (user)“, um das Lesepasswort einzugeben.
- ☐ Geben Sie das neue Lesepasswort in der Zeile „Neues Passwort“ ein und wiederholen Sie die Eingabe in der Zeile „Bitte nochmals eingeben“.

- ☐ Wählen Sie „Schreib-/Lese Passwort ändern (admin)“, um das Schreib-/Lese Passwort einzugeben.
- ☐ Geben Sie das Schreib-/Lese Passwort ein und wiederholen Sie die Eingabe.

Anmerkung: Wenn Sie kein Passwort mit der Berechtigung „schreiben/lesen“ kennen, haben Sie keine Möglichkeit, auf das Gerät schreibend zuzugreifen.

Anmerkung: Aus Sicherheitsgründen zeigt der Dialog die Passwörter in Form von Sternen an. Notieren Sie sich jede Änderung. Ohne gültiges Passwort können Sie nicht auf das Gerät zugreifen.

Anmerkung: Verwenden Sie bei SNMP Version 3 für das Passwort 5 bis 32 Zeichen, da viele Anwendungen keine kürzeren Passwörter akzeptieren.

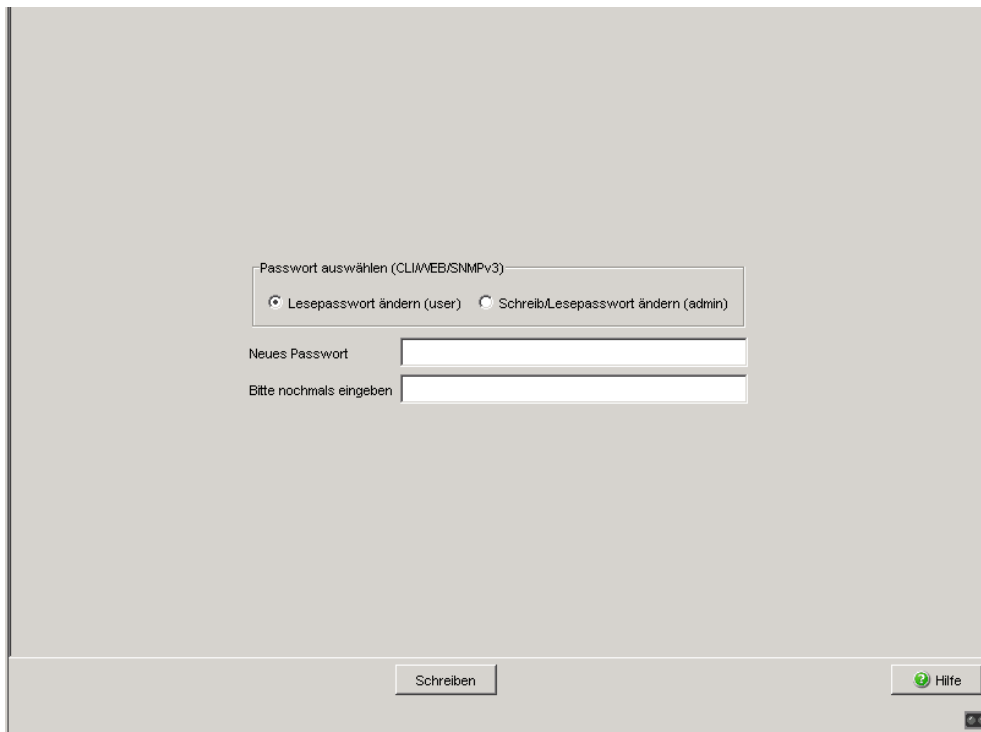


Abb. 21: Dialog Passwort

- ☐ Um die Änderungen flüchtig zu speichern, klicken Sie „Schreiben“.

☐ Konfigurieren Sie den SSH-Zugriff.

☐ Wählen Sie den Dialog `Sicherheit:SSH-Zugriff`.

☐ Ändern Sie den SSH-Port auf z.B. 9243.

Einschränken der IP-Adressen, die über SSH zugreifen dürfen:

☐ Klicken Sie auf „Eintrag erzeugen“.

☐ Wählen Sie in der Zelle „Port“ des neuen Eintrags in der Tabelle
int.

☐ Doppelklicken Sie in die Zelle „Quelladresse (CIDR) und geben Sie
die Quelladresse ein, z.B. 10.0.1.17.

Wenn dies der einzige aktive Eintrag in dieser Tabelle ist, dann kann
ausschließlich der PC mit dieser IP-Adresse über dieses Protokoll
zugreifen.

☐ Klicken Sie in das Feld „Aktiv“ dieses Eintrags, um den Eintrag zu
aktivieren.

☐ Um die Änderungen flüchtig zu speichern, klicken Sie „Schreiben“.

Anmerkung: Das Gerät bietet Ihnen die Möglichkeit, per SFTP auf
Geräte-Dateien wie Konfigurationsdateien oder den ACA zuzugreifen,
ein Firmware-Update oder VPN-Zertifikate auf das Gerät zu laden.
Verwenden Sie dazu einen SFTP-Client, z. B. WinSCP. Für den SFTP-
Zugriff ist der SSH-Zugriff auf das Gerät erforderlich.

Index	Port	Quelladresse (CIDR)	Aktion	Log	Beschreibung	Aktiv	Fehler
1	ext	any	accept	disable		☒	

Abb. 22: Dialog SSH-Zugriff

☐ Konfigurieren Sie das automatische Abmelden.

- ☐ Wählen Sie den Dialog `Abmelden`.
- ☐ Geben Sie im Rahmen „SSH-Verbindung“ in der Zeile „Automatisch nach [min]“ die Anzahl von Minuten ein, nach welcher das Gerät die SSH-Verbindung automatisch bei Inaktivität beendet.
- ☐ Klicken Sie im Rahmen „Command Line Interface“ in der Zeile „Automatisch“ auf „An“.
- ☐ Geben Sie in der Zeile „Nach [min]“ die Anzahl von Minuten ein, nach welcher das Gerät die HTTPS-Verbindung automatisch bei Inaktivität beendet.
- ☐ Um die Änderungen flüchtig zu speichern, klicken Sie „Schreiben“.

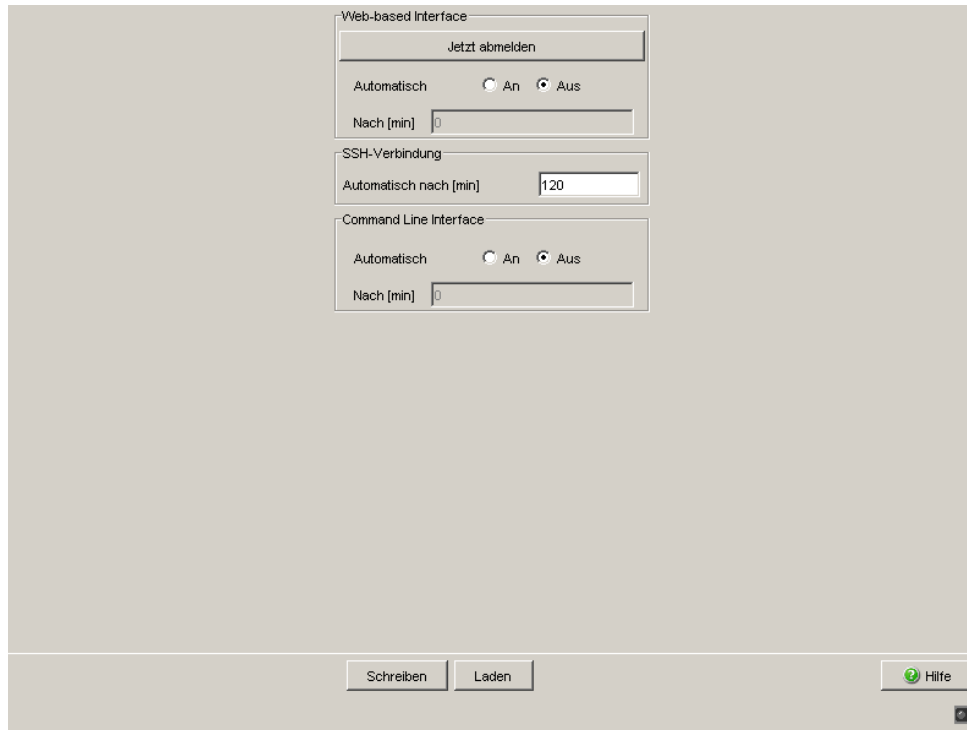


Abb. 23: Dialog Abmelden

☐ Speichern Sie die Einstellungen in den nicht-flüchtigen Speicher.

- ☐ Öffnen Sie hierzu den Dialog Grundeinstellungen:Laden/Speichern.
- ☐ Klicken Sie auf „Speichern in NVM + ACA“, um die Daten nicht-flüchtig zu speichern.

5.3 Netzmanagement-Zugriff

Eine Netzmanagement-Station kommuniziert über das Simple Network Management Protocol (SNMP) mit dem Gerät.

Jedes SNMP-Paket enthält die IP-Adresse des sendenden Rechners und das Passwort, mit welchem der Absender des Pakets auf die MIB des Gerätes zugreifen will.

Das Gerät empfängt das SNMP-Paket, prüft die IP-Adresse des sendenden Rechners und vergleicht das Passwort mit seinen internen Einträgen. Liegt das Passwort mit dem entsprechenden Zugriffsrecht vor und ist die IP-Adresse des sendenden Rechners als berechtigt eingetragen, dann gewährt das Gerät den Zugriff.

Im Lieferzustand ist das Gerät über das Passwort „public“ (nur lesen) und „private“ (lesen und schreiben) von jedem Rechner aus zugänglich.

Um Sie beim Schutz Ihres Gerätes vor unerwünschten Eingriffen zu unterstützen:

- ☐ Definieren Sie zuerst ein neues Passwort, unter welchem Sie mit allen Rechten von Ihrem Rechner aus zugreifen können.
- ☐ Behandeln Sie dieses Passwort vertraulich. Denn jeder, der das Passwort kennt, kann mit der IP-Adresse ihres Rechners auf die MIB des Gerätes zugreifen.
- ☐ Prüfen Sie, mit welcher SNMP-Version Ihre Netzmanagement-Software kommuniziert.
Falls notwendig, aktivieren Sie SNMPv1 oder SNMPv2.
- ☐ Tragen Sie die SNMP-Zugriffsregeln ein.

5.4 HiDiscovery-Zugriff aus-/ einschalten

5.4.1 Beschreibung HiDiscovery-Protokoll

Das HiDiscovery-Protokoll ermöglicht Ihnen, dem Gerät im Transparent-Modus anhand seiner MAC-Adresse eine IP-Adresse zuzuweisen ([siehe auf Seite 53 „IP-Parameter per HiDiscovery eingeben“](#)). HiDiscovery ist ein Layer 2-Protokoll.

Anmerkung: Schränken Sie aus Sicherheitsgründen die HiDiscovery-Funktion des Gerätes ein oder schalten Sie sie aus, nachdem Sie dem Gerät die IP-Parameter zugewiesen haben.

5.4.2 HiDiscovery-Funktion aus-/einschalten

- ☐ Wählen Sie den Dialog `Grundeinstellungen:Netz:Transparent-Modus`.
- ☐ Im Rahmen „HiDiscovery Protokoll“ schalten Sie die HiDiscovery-Funktion aus oder beschränken Sie den Zugriff auf „read-only“.

`enable`

Wechsel in den Privileged-EXEC-Modus.

`network protocol hidiscovery
off`

HiDiscovery-Funktion ausschalten.

`network protocol hidiscovery
read-only`

HiDiscovery-Funktion mit dem Zugriffsrecht
„lesen“ einschalten

`network protocol hidiscovery
read-write`

HiDiscovery-Funktion mit dem Zugriffsrecht
„lesen und schreiben“ einschalten

5.5 Externe Authentifizierung

5.5.1 Beschreibung der externen Authentifizierung

„Externe Authentifizierung“ des Gerätes bietet Ihnen die Möglichkeit, zur Authentifizierung eines Benutzers Benutzer-Firewall-Konten mit zugehörigen Passwörtern anzulegen. Für jedes Konto können Sie durch die Wahl einer Authentifizierungsliste drei Authentifizierungsmethoden festlegen, die das Gerät bei einem Zugriff über diesen Kontonamen nacheinander anwendet. Das Gerät bietet die Authentifizierung mit Hilfe seiner Benutzerdatenbank (lokal) oder über einen RADIUS-Server.

Legen Sie Konten (Benutzer) für die Anwendung der Benutzer-Firewall-Funktion an ([siehe auf Seite 155 „Benutzer-Firewall“](#)).

5.5.2 Anwendungsbeispiel für die externe Authentifizierung

Ein typischer Fall ist ein Servicetechniker, der sich im Anmeldefenster der grafischen Benutzeroberfläche unter dem Login-Typ „Benutzerfirewall“ auf der Firewall anmelden möchte. Nach erfolgreicher Anmeldung erhält er über die Benutzer-Firewall-Funktion ([siehe Seite 155](#)) einen zeitlich begrenzten, durch ergänzende Regeln definierten Zugriff auf das interne und externe Netz, um z.B. ein Software-Update für die Wartung eines Roboters von einem Server herunterzuladen.

Parameter für das Anwendungsbeispiel für die Benutzer-Firewall-Funktion ([siehe Seite 155](#)):

Parameter	Wert
Kontoname	Service
Authentifizierungsliste	userFirewallLoginDefaultList

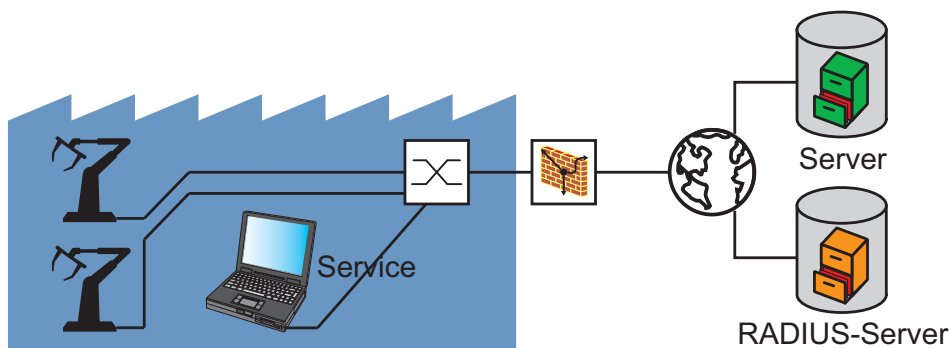


Abb. 24: Externe Authentifizierung Anwendungsbeispiel

Ablauf der Authentifizierung:

- ▶ Der Benutzer meldet sich auf dem Gerät im Anmeldefenster der grafischen Benutzeroberfläche unter dem Login-Typ „Benutzerfirewall“ mit Benutzernamen und Passwort an.
- ▶ Das Gerät prüft, ob für diesen Benutzer mit diesem Passwort ein Eintrag unter `Externe Authentifizierung:Benutzer-Firewall` Konten vorhanden ist.
- ▶ Ist ein Eintrag vorhanden und ist dieser aktiv, dann wendet das Gerät die Authentifizierungsmethoden entsprechend der Authentifizierungsliste dieses Eintrags an.
Ist kein Eintrag vorhanden, und ist in „Authentifizierungsliste für unbekannte Benutzer“ eine Authentifizierungsliste eingetragen, wendet das

Gerät die Authentifizierungsmethoden entsprechend der Authentifizierungsliste dieses Eintrags an.

Ist kein Eintrag vorhanden, und ist in „Authentifizierungsliste für unbekannte Benutzer“ keine Authentifizierungsliste eingetragen, lehnt das Gerät die Authentifizierung ab.

- ▶ Führt eine der Authentifizierungsmethoden der Authentifizierungsliste zur Authentifizierung, ist der Benutzer angemeldet und kann damit die Benutzer-Firewall-Funktion verwenden.

- ☐ Konfigurieren Sie das Benutzer-Firewall-Konto.

- ☐ Wählen Sie den Dialog `Sicherheit:Externe Authentifizierung:Benutzer-Firewall Konten`.
- ☐ Klicken Sie auf „Eintrag erzeugen“.
Hierdurch öffnen Sie einen Dialog zur Eingabe des Namens für dieses Benutzer-Firewall-Konto.
- ☐ Geben Sie den Namen für dieses Konto ein, z.B. `Service`.
- ☐ Klicken Sie auf „OK“.
Hierdurch fügen Sie der Tabelle einen neuen Eintrag hinzu.
- ☐ Doppelklicken Sie in die Zelle „Passwort für lokale Authentifizierung“ dieses Eintrags und geben Sie das Passwort ein.
- ☐ Klicken Sie in das Feld „Aktiv“ dieses Eintrags, um den Eintrag zu aktivieren.
- ☐ Um die Änderungen flüchtig zu speichern, klicken Sie „Schreiben“.

- ☐ Speichern Sie die Einstellungen in den nicht-flüchtigen Speicher.

- ☐ Öffnen Sie hierzu den Dialog `Grundeinstellungen:Laden/Speichern`.
- ☐ Klicken Sie auf „Speichern in NVM + ACA“, um die Daten nicht-flüchtig zu speichern.

Die Authentifizierungslisten enthalten im Lieferumfang die Liste „userFirewallDefaultList“. Das Beispiel ist so gewählt, dass Sie die Parameter dieser Liste beibehalten können.

6 Datenverkehr kontrollieren

Dieses Kapitel beschreibt die Hauptaufgabe einer Firewall. Eine Firewall überprüft die zur Weiterleitung bestimmten Daten nach vorgegebenen Regeln. Daten, die den Regeln entsprechen, leitet eine Firewall weiter oder blockiert sie. Daten, auf die keine Regel zutrifft, blockiert eine Firewall.

Zur Kontrolle des Datenverkehrs bietet der EAGLE One folgende Funktionen:

- ▶ Paketinhaltsbezogene Daten-Verkehrskontrolle (Paketfilter)
- ▶ NAT - Network Address Translation
- ▶ Benutzerbezogene Daten-Verkehrskontrolle (Benutzer-Firewall)
- ▶ Kontrolle der Dienstanforderungen (Denial of Service, DoS)
- ▶ VPN - Virtuelles Privates Netz

Die Firewall beobachtet und überwacht den Datenverkehr. Aus den Ergebnissen der Beobachtung und Überwachung zusammen mit den Regeln für die Netzsicherheit erstellt die Firewall sogenannte Zustandstabellen. Nach diesen Zustandstabellen entscheidet die Firewall, ob sie die Daten vermittelt, verwirft oder zurückweist.

6.1 Paketfilter

6.1.1 Beschreibung der Paketfilter-Funktion

Bei der paketinhaltsbezogenen Datenverkehrskontrolle überprüft die Firewall den Inhalt der zu vermittelnden Datenpakete. Hierbei bietet die Firewall verschiedene Paket-Gruppen zur Definition der Überprüfungs-kriterien an:

- ▶ **Eingehende IP-Pakete**
Diese Gruppe bietet Ihnen die Möglichkeit, am externen Port eingehende IP-Pakete nach ihren IP-Adressierungsinformationen und Protokoll-information zu filtern.
- ▶ **Ausgehende IP-Pakete**
Diese Gruppe bietet Ihnen die Möglichkeit, am internen Port eingehende IP-Pakete nach ihren IP-Adressierungsinformationen und Protokoll-information zu filtern.
- ▶ **Eingehende MAC-Pakete**
Diese Gruppe bietet Ihnen die Möglichkeit, am externen Port eingehende MAC-Pakete nach ihren MAC-Adressierungsinformationen zu filtern.
Im Router-Modus vermittelt die Firewall ausschließlich IP-Pakete.
- ▶ **Ausgehende MAC-Pakete**
Diese Gruppe bietet Ihnen die Möglichkeit, am internen Port eingehende MAC-Pakete nach ihren MAC-Adressierungsinformationen zu filtern.
Im Router-Modus vermittelt die Firewall ausschließlich IP-Pakete.
- ▶ **Eingehende PPP-Pakete**
Diese Gruppe bietet Ihnen die Möglichkeit, am externen Port eingehende PPP-Pakete nach ihren IP-Adressierungsinformationen zu filtern.

Sie können Filterregeln definieren, bei deren Zutreffen die Firewall die Pakete entweder

- verwirft,
- zurückweist oder
- vermittelt.

Aktion	Bedeutung
verwerfen (drop)	Datenpaket löschen
zurückweisen (reject)	Datenpaket löschen und den Absender informieren
vermitteln (accept)	Datenpaket entsprechend der Adressinformationen weiterleiten.

Tab. 8: *Behandlung gefilterter Datenpakete*

Die Firewall überprüft jedes Datenpaket beginnend mit der ersten Regel. Die erste Regel, die zutrifft, bestimmt, wie die Firewall das Datenpaket behandelt.

Die letzte Regel „alles verwerfen“ unterstützt Sie beim Schutz vor unerwünschten Datenpaketen.

Anmerkung: Wenn Sie Paketfilter-Einträge hinzufügen, die Verkehr verbieten, oder bestehende ändern, um Verkehr zu verbieten, beachten Sie, dass in der Zustandstabelle noch Einträge vorhanden sein können, die den Verkehr bis zum Ablauf des Eintrags dennoch erlauben. Wenn Sie einen Paketfilter-Eintrag löschen, löscht das Gerät die gesamte Zustandstabelle.

■ Adressvorlagen

Adressvorlagen bieten Ihnen die Möglichkeit, IP-Paketfilter-Einträge einfacher und schneller zu erstellen und zu ändern.

Wenn Sie in mehreren Regeln die selben IP-Adressbereiche als Quell- oder Zieladresse verwenden, haben Sie die Möglichkeit, diese Adressen als eine Adressvorlage zu definieren. Eine Adressvorlage besteht aus 1 oder mehreren Adress-Einträgen mit dem selben Namen. Eine einzelne Adresse können Sie optional mit der Adressmaske /32 angeben. Sie können die einzelnen Adressen der Adressvorlage getrennt aktivieren oder deaktivieren.

In Ihren Paketfilter-Einträgen verwenden Sie eine Adressvorlage in Form einer Variablen. Eine Variable kennzeichnen Sie, indem Sie ihrem Namen ein Dollar-Zeichen („\$“) voranstellen. Sie haben die Möglichkeit, für Quell- und Zieladressen Variablen zu verwenden.

Das Gerät erzeugt aus einem Paketfilter-Eintrag mit Variablen automatisch die passenden Paketfilter-Einträge. Wenn Sie die Adressvorlage für eine Variable ändern, passt das Gerät automatisch die erzeugten Paketfilter-Einträge an.

Beispielsweise können Sie für die Adressen in Ihrem internen Netz eine Adressvorlage erstellen und diese als Variable in Ihren Paketfilter-Einträgen verwenden. Wenn Sie Ihrem internen Netz ein weiteres Gerät hinzufügen, das die selben Paketfilter bekommen soll wie die bisherigen Geräte, können Sie die entsprechenden Paketfilter-Einträge durch das Ändern einer einzigen Adressvorlage zu aktualisieren.

Anmerkung: Die Anzahl durch Variablen erzeugten Paketfilter-Einträge ist zusammen mit der Anzahl der anderen Paketfilter-Einträge auf 1.024 begrenzt.

Im Lieferzustand sind keine Adressvorlagen definiert.

■ Firewall-Lern-Modus (FLM)

Der Firewall-Lern-Modus ist ein innovativer Einrichtungsassistent. Er unterstützt sie bei der Analyse des Verkehrs und der Erstellung passender Regeln zum Erlauben von erwünschtem Verkehr.

Der Assistent für den Firewall-Lern-Modus bietet Ihnen die Möglichkeit:

- ▶ auf einfache Weise automatisch den Verkehr zu ermitteln, den Ihre vorhandenen Regeln noch nicht erlauben (eigentlicher Lern-Modus),
- ▶ diesen Verkehr nach verschiedenen Kriterien zu analysieren,
- ▶ aus dem erwünschten Verkehr automatisch neue Regelvorschläge zu erstellen,
- ▶ diese Regeln bei Bedarf zu modifizieren und deren Verkehrsabdeckung automatisch zu visualisieren, und
- ▶ die neuen Regeln auf die gewünschte Abdeckung zu testen.

Anmerkung: Der Assistent für den Firewall-Lern-Modus erfordert dennoch Fachkenntnisse über Datennetze, da der Bediener für die erstellten Regeln verantwortlich ist.

Der FLM bezieht sich ausschließlich auf Pakete, die das Gerät (die Firewall) durchqueren möchten. Pakete, die an das Gerät selbst gerichtet sind und solche, die das Gerät selbst erzeugt, sind davon ausgenommen.

Führen Sie zur FLM-unterstützten Regel-Erstellung folgende Schritte aus:

- ☐ Setzen Sie die Firewall an der vorgesehenen Stelle in Ihr Netz ein.
- ☐ Aktivieren Sie den FLM-Assistenten an den gewünschten Interfaces der Firewall (typischerweise an beiden Interface).
- ☐ Starten Sie den eigentlichen Lern-Modus.
- ☐ Betreiben Sie die Geräte in Ihrem Netz eine Zeitlang, so dass die Firewall den erwünschten Verkehr lernt.
- ☐ Stoppen Sie den Lern-Modus.
- ☐ Lassen Sie sich den gelernten Verkehr auf dem ausgewählten Interface anzeigen:
 - ▶ Hat die Firewall zu wenig Verkehr gelernt, setzen Sie den Lern-Modus fort, um mehr Verkehr zu lernen.
 - ▶ Hat die Firewall genügend Verkehr gelernt, inspizieren Sie die erfassten Daten.
- ☐ Wählen Sie erwünschte Einträge aus den erfassten Daten aus und fügen Sie sie dem temporären Regelsatz hinzu.
- ☐ Modifizieren Sie gegebenenfalls die hinzugefügten Regeln.
- ☐ Ignorieren Sie unerwünschte Einträge in den erfassten Daten, d. h., legen Sie dafür keine Regeln an. Die Firewall sperrt so nach dem Beenden des Lern- und Test-Modus diesen Verkehr.
- ☐ Geben Sie die gewünschten Regeln zum Test frei.
- ☐ Starten Sie den Testmodus:
 - ▶ Arbeiten die Geräte in Ihrem Netz wie gewünscht, schreiben Sie die temporären Regeln in Ihre Regelbasis.
 - ▶ Arbeiten die Geräte in Ihrem Netz anders als gewünscht, modifizieren Sie die zum Test freigegebenen Regeln. Alternativ starten Sie den Lern-Modus erneut, um mehr Verkehr zu lernen.
- ☐ Beenden Sie den Assistenten für den Firewall-Lern-Modus.
- ☐ Speichern Sie die Regeln in der Konfiguration.

6.1.2 Anwendungsbeispiel für Paketfilter

Die Abbildung zeigt einen typischen Anwendungsfall:

Ein Fertigungssteuerer möchte die Daten von einem Produktionsroboter abfragen. Der Produktionsroboter steht in einer Fertigungszelle, die mit Hilfe einer Firewall vom Firmennetz getrennt ist. Die Firewall soll dabei helfen, den Datenverkehr zwischen der Fertigungszelle und dem restlichen Firmennetz zu unterbinden. Einzig der Datenverkehr zwischen dem Roboter und dem PC des Fertigungssteuerers darf frei fließen.

Bekannt sind:

Parameter	Roboter	Firewall	PC
IP-Adresse interner Port		10.0.1.201	
IP-Adresse externer Port		10.0.2.1	
IP-Adresse	10.0.1.5		10.0.2.17
Gateway	10.0.1.201		10.0.2.1

Voraussetzungen für die weitere Konfiguration:

- ▶ Die Firewall ist im Router-Modus.
- ▶ Die IP-Parameter der Firewall-Router-Interface sind konfiguriert.
- ▶ Die Geräte im internen Netz haben als Gateway die IP-Adresse des internen Interfaces (Port 1) der Firewall.
- ▶ Gateway und IP-Adresse des PCs und des Roboters sind konfiguriert.

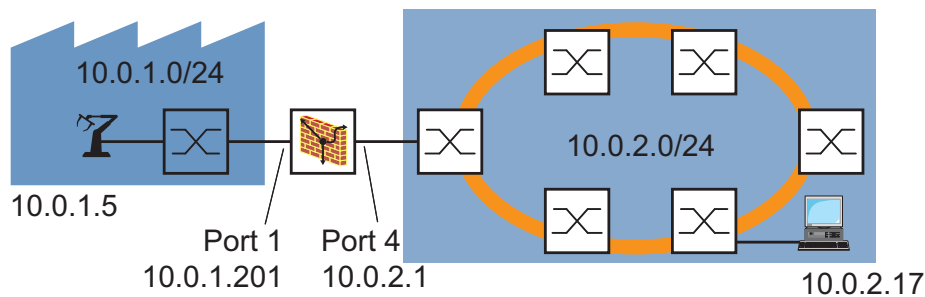


Abb. 25: Paketfilter Anwendungsbeispiel

☐ Geben Sie die Filterdaten für eingehende IP-Pakete ein.

☐ Wählen Sie den Dialog

Netzwerk: Paketfilter: Eingehende IP-Pakete.

Im Lieferzustand besitzt der EAGLE One bereits einen unsichtbaren Eintrag, der dabei hilft, den Datenverkehr vom externen in das interne Netz zu unterbinden.

☐ Klicken Sie auf „Eintrag erzeugen“.

Hierdurch fügen Sie der Tabelle einen neuen Eintrag hinzu.

☐ Tragen Sie die Filterdaten ein für „freier Zugang für PC“:

„Beschreibung“: freier Zugang für PC

„Quelladresse (CIDR)“: 10.0.2.17/32

„Quellport“: any

„Zieladresse (CIDR)“: 10.0.1.5/32

„Zielpport“: any

„Protokoll“: any

„Aktion“: accept

„Log“: disable

☐ Klicken Sie in das Feld „Aktiv“ dieses Eintrags, um den Eintrag zu aktivieren.

☐ Um die Änderungen flüchtig zu speichern, klicken Sie „Schreiben“.

Das Gerät bietet Ihnen die Möglichkeit, eingehende IP-Pakete selektiv auf bestimmte ICMP-Traffic-Kriterien zu prüfen. Um diese Funktion für einen bestehenden oder einen neuen Paketfilter zu aktivieren, gehen Sie wie folgt vor:

- ☐ Wählen Sie den Dialog
`Netzsicherheit:Paketfilter:Eingehende IP-Pakete`.
- ☐ Fügen Sie nach Ihrem Bedarf der Tabelle einen neuen Eintrag hinzu und tragen Sie die Filterdaten ein wie in der vorhergehenden Tabelle beschrieben (siehe Kapitel „[Anwendungsbeispiel für Paketfilter](#)“).
- ☐ Wählen Sie im Auswahlfeld „Protokoll“ den Eintrag `icmp` aus.
- ☐ Geben Sie im Eingabefeld „Quellport“ den ICMP-Typ und -Code ein:
`type 3 code 1` hat die Bedeutung:
 - Destination Unreachable (ICMP-Typ 3)
 - Host Unreachable (ICMP-Code 1)Die Werte hinter `type` und `code` sind 1- bis 3-stellige Dezimalwerte. Die Angabe des ICMP-Code ist optional. Mögliche Werte für ICMP-Typ und -Code entnehmen Sie der Tabelle „ICMP-Typen und -Codes“ im Referenz-Handbuch „Graphische Benutzeroberfläche (GUI) Industrial Ethernet Firewall EAGLE 20“.
- ☐ Klicken Sie auf „Schreiben“, um den Eintrag in der Konfiguration flüchtig zu speichern.

- ☐ Geben Sie die Filterdaten für ausgehende IP-Pakete ein.

- ☐ Wählen Sie den Dialog
`Netzsicherheit:Paketfilter:Ausgehende IP-Pakete`.
Im Lieferzustand besitzt der EAGLE One bereits einen Eintrag, der den Datenverkehr vom internen in das externe Netz erlaubt.
- ☐ Markieren Sie den Eintrag.

- ☐ Tragen Sie die Filterdaten ein für „alles verwerfen“:
 - „Beschreibung“: alles verwerfen
 - „Quelladresse (CIDR)“: any
 - „Quellport“: any
 - „Zieladresse (CIDR)“: any
 - „Zielport“: any
 - „Protokoll“: any
 - „Aktion“: drop
 - „Log“: disable
- ☐ Klicken Sie in das Feld „Aktiv“ dieses Eintrags, um den Eintrag zu aktivieren.
- ☐ Markieren Sie den Eintrag.
 - Klicken Sie auf „↑“.
 - Wiederholen Sie den Vorgang, bis der Eintrag die erste Zeile der Tabelle darstellt.
- ☐ Klicken Sie auf „Eintrag erzeugen“.
 - Hierdurch fügen Sie der Tabelle einen neuen Eintrag hinzu.
- ☐ Markieren Sie den Eintrag.
- ☐ Tragen Sie die Filterdaten ein für „freier Zugang für Roboter“:
 - „Beschreibung“: freier Zugang für Roboter
 - „Quelladresse (CIDR)“: 10.0.1.5/32
 - „Quellport“: any
 - „Zieladresse (CIDR)“: 10.0.2.17/32
 - „Zielport“: any
 - „Protokoll“: any
 - „Action“: accept
 - „Log“: disable
- ☐ Klicken Sie in das Feld „Aktiv“ dieses Eintrags, um den Eintrag zu aktivieren.
- ☐ Markieren Sie den Eintrag.
 - Klicken Sie auf „↑“.
 - Wiederholen Sie den Vorgang, bis der Eintrag die erste Zeile der Tabelle darstellt.
- ☐ Um die Änderungen flüchtig zu speichern, klicken Sie „Schreiben“.

- ☐ Speichern Sie die Einstellungen in den nicht-flüchtigen Speicher.

- 
- ☐ Öffnen Sie hierzu den Dialog Grundeinstellungen:Laden/Speichern.
 - ☐ Klicken Sie auf „Speichern in NVM + ACA“, um die Daten nicht-flüchtig zu speichern.

■ Anwendungsbeispiel für Adressvorlagen

Ein Fertigungssteuerer möchte die Daten eines zweiten Produktionsroboters abfragen. Da noch weitere Roboter hinzukommen werden, entschließt er sich, die Adressen der Roboter in einer Adressvorlage anzulegen und die Vorlage als Variable in den bestehenden Paketfilter-Einträgen zu verwenden.

Bekannt sind:

Parameter	Roboter 1	Roboter 2	Firewall	PC
IP-Adresse interner Port			10.0.1.201	
IP-Adresse externer Port			10.0.2.1	
IP-Adresse	10.0.1.5	10.0.1.6		10.0.2.17
Gateway	10.0.1.201	10.0.1.201		10.0.2.1

Voraussetzungen für die weitere Konfiguration:

- Das vorige „Anwendungsbeispiel für Paketfilter“ ist bereits konfiguriert.

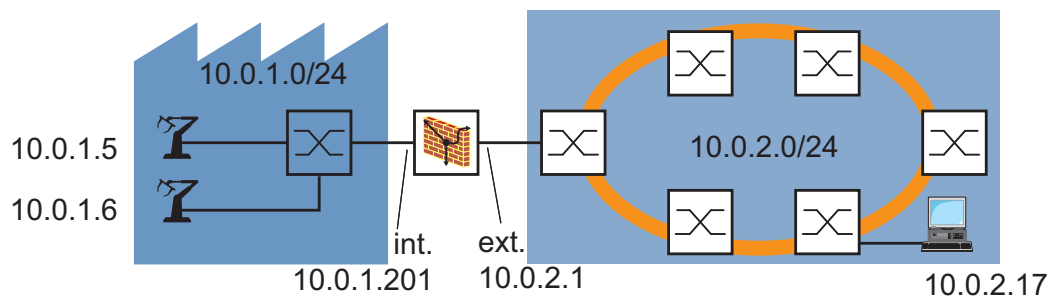


Abb. 26: Paketfilter mit Adressvorlage, Anwendungsbeispiel

- ☐ Erstellen Sie die Adressvorlage für die Roboter in der Fertigungszelle.

- ☐ Wählen Sie den Dialog

Netzsicherheit:Paketfilter:Adressvorlagen.

- ☐ Klicken Sie auf „Eintrag erzeugen“.

- ☐ Tragen Sie die 1. Adresse der Adressvorlage in den Dialog ein. Eine einzelne Adresse können Sie optional mit der Adressmaske /32 angeben:

„Listen-Name“: robo_zelle_1

„IP-Adresse (CIDR)“: 10.0.1.5/32

- ☐ Klicken Sie auf „OK“, um den Eintrag in der Adressvorlagen-Tabelle zu erzeugen.

- ☐ Klicken Sie in das Feld „Aktiv“ dieses Eintrags, um den Eintrag zu aktivieren.
 - ☐ Klicken Sie nochmals auf „Eintrag erzeugen“.
 - ☐ Tragen Sie die 2. Adresse der Adressvorlage in den Dialog ein. Verwenden Sie dabei den selben Namen:
„Listen-Name“: robo_zelle_1
„IP-Adresse (CIDR)“: 10.0.1.6/32
 - ☐ Klicken Sie auf „OK“, um den Eintrag in der Adressvorlagen-Tabelle zu erzeugen.
 - ☐ Klicken Sie in das Feld „Aktiv“ dieses Eintrags, um den Eintrag zu aktivieren.
 - ☐ Klicken Sie auf „Schreiben“, um die Einträge in der Konfiguration flüchtig zu speichern.
- ☐ Nehmen Sie die Variable in die Filterdaten für eingehende IP-Pakete auf.

- ☐ Wählen Sie den Dialog
Netzicherheit:Paketfilter:Eingehende IP-Pakete.
- ☐ Wählen Sie den Eintrag „freier Zugang für PC“.
- ☐ Ersetzen Sie die Zieladresse in den Eintrag „freier Zugang für PC“ durch die Variable. Stellen Sie dem Variablennamen ein Dollar-Zeichen („\$“) voran, um die Variable zu kennzeichnen:
„Beschreibung“: freier Zugang für PC
„Quelladresse (CIDR)“: 10.0.2.17/32
„Quellport“: any
„Zieladresse (CIDR)“: \$robo_zelle_1 (statt 10.0.1.5/32)
„Zielpport“: any
„Protokoll“: any
„Aktion“: accept
„Log“: disable
- ☐ Um die Änderungen flüchtig zu speichern, klicken Sie „Schreiben“.

- ☐ Nehmen Sie die Variable in die Filterdaten für ausgehende IP-Pakete auf.

- ☐ Wählen Sie den Dialog
Netzicherheit:Paketfilter:Ausgehende IP-Pakete.
- ☐ Wählen Sie den Eintrag „freier Zugang für Roboter“.

- ☐ Ersetzen Sie die Quelladresse in den Eintrag „freier Zugang für PC“ durch die Variable:
 - „Beschreibung“: freier Zugang für Roboter
 - „Quelladresse (CIDR)“: \$robo_zelle_1 (statt 10.0.1.5/32)
 - „Quellport“: any
 - „Zieladresse (CIDR)“: 10.0.2.17/32
 - „Zielpport“: any
 - „Protokoll“: any
 - „Action“: accept
 - „Log“: disable
- ☐ Um die Änderungen flüchtig zu speichern, klicken Sie „Schreiben“.

☐ Speichern Sie die Einstellungen in den nicht-flüchtigen Speicher.

- ☐ Öffnen Sie hierzu den Dialog Grundeinstellungen:Laden/Speichern.
- ☐ Klicken Sie auf „Speichern in NVM + ACA“, um die Daten nicht-flüchtig zu speichern.

6.1.3 Anwendungsbeispiel für den Firewall-Lern-Modus (FLM)

Die Abbildung zeigt einen typischen Anwendungsfall:

Ein Fertigungssteuerer richtet eine neue Fertigungszelle ein. Eine Firewall soll die Fertigungszelle vom Firmennetz trennen. Sie soll ausschließlich den erwünschten Verkehr vom Konfigurations-Computer im Firmennetz zu den Geräten in der Fertigungszelle erlauben und anderen Verkehr, insbesondere aus dem Transfernetz verwerfen. In der Gegenrichtung von der Fertigungszelle ins Firmennetz soll der Datenverkehr frei fließen.

Zu Beginn möchte der Benutzer von seinem Konfigurations-Computer im Firmennetz auf den Switch in der Fertigungszelle zugreifen und diesen konfigurieren.

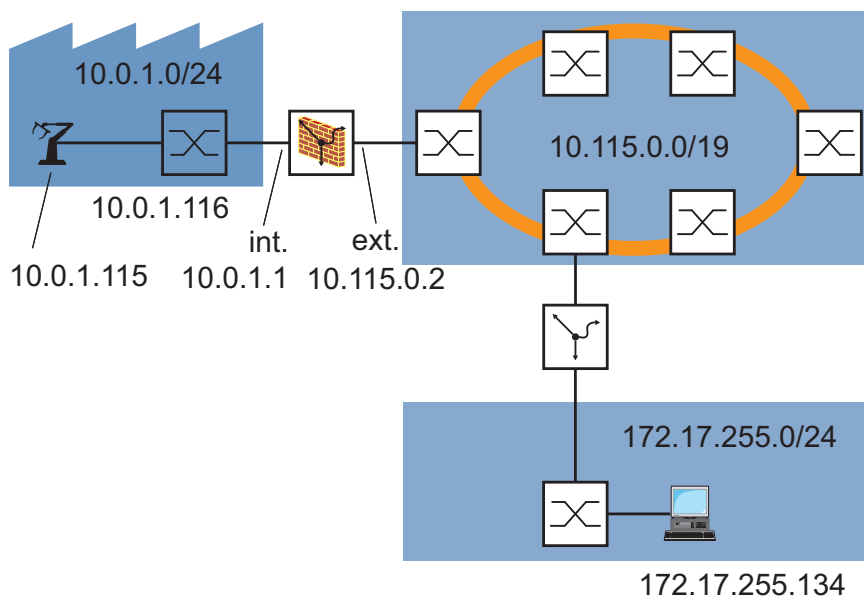


Abb. 27: Firewall-Lern-Modus- (FLM-) Anwendungsbeispiel

Bekannt sind die folgenden IP-Adressen:

Parameter	Roboter	Switch	Firewall	Konfigurations-Computer
IP-Adr. interner Port			10.0.1.1	
IP-Adr. externer Port			10.115.0.2	
IP-Adresse	10.0.1.115	10.0.1.116		172.17.255.134
Default-Gateway	10.0.1.1	10.0.1.1		

Im Lieferzustand

- ▶ erlaubt die Firewall den Verkehr vom internen zum externen Interface. Diese Konfiguration möchte der Benutzer beibehalten.
- ▶ verwirft die Firewall den Verkehr vom externen zum internen Interface. Diese Konfiguration möchte der Benutzer ändern.

Voraussetzungen für die weitere Konfiguration:

- ▶ Die Firewall ist im Router-Modus.
- ▶ Die IP-Parameter der Firewall-Router-Interface sind konfiguriert.
- ▶ Die Paketfilter-Regeln am externen Interface der Firewall sind im Lieferzustand.
- ▶ Die Geräte im internen Netz haben als Gateway die IP-Adresse des internen Interfaces (Port 1) der Firewall.
- ▶ Die IP-Parameter des Konfigurations-Computers und des Routers im Firmennetz sind konfiguriert.

Besonderheiten des Lernmodus:

- ▶ Das Gerät lernt im Lern-Modus ausschließlich den Verkehr, der durch die aktuellen Regeln unabgedeckt ist. Dies ist der Verkehr, für den Sie weder spezifische Verwerfen-Regeln (`drop`, `reject`) noch Akzeptieren-Regeln (`accept`) konfiguriert haben.
- ▶ Das Gerät ignoriert damit während des Lernens den Verkehr, für den Sie bereits explizite Verwerfen- oder Akzeptieren-Regeln konfiguriert haben.
- ▶ Der Assistent für den Firewall-Lern-Modus erstellt ausschließlich Akzeptieren- (`accept`-) Regeln. Die Stateful Firewall erlaubt im Betrieb den Verkehr, den sie mit einer `accept`-Regel erfasst hat, anschließend für diese Kommunikationsbeziehung.

Öffnen des Assistenten für den Firewall-Lern-Modus:

- ☐ Wählen Sie den Dialog
Netzwerk: Paketfilter: Firewall-Lern-Modus.
- ☐ Klicken Sie im Rahmen „Funktion“ auf „An“.
- ☐ Um den Assistenten für den Firewall-Lern-Modus einzuschalten klicken Sie auf „Schreiben“.

Die grafische Benutzeroberfläche weist Sie auf den Eintritt in den Firewall-Lern-Modus hin und fragt Sie, ob Sie die aktuelle Konfiguration des Gerätes speichern möchten.

- ☐ Klicken Sie auf „Ja“.

Die grafische Benutzeroberfläche fordert Sie zur Eingabe eines Dateinamens auf. Der vorgeschlagene Dateiname hat das Format

nnnnnnnnnnnnnnnn beforeFLM.

- ☐ Geben Sie für den Dateinamen `Beispiel01_vor_FLM` ein und klicken Sie „OK“.

Das Gerät speichert die aktuelle Konfiguration unter dem angegebenen Namen im NVM und setzt diese in den Zustand „aktiv“.

Die grafische Benutzeroberfläche Interface aktiviert anschließend die Bedienelemente für den Firewall-Lern-Modus.

Das Lernen starten:

- ☐ Wählen Sie das externe Interface zum Lernen aus.
- ☐ Um den eigentlichen Lernvorgang auf der Firewall zu starten, klicken Sie auf „Starte Lernmodus“.
- ☐ Laden Sie auf Ihrem Konfigurations-Computer in einem anderen Browser-Fenster die grafische Benutzeroberfläche des Switch in der Produktionszelle. Die grafische Benutzeroberfläche greift per http und snmp auf den Switch zu. Dieser Datenverkehr ist von Ihnen erwünscht, um den Switch zu konfigurieren.
- ☐ Wechseln Sie wieder zum Assistenten für den Firewall-Lern-Modus und klicken Sie auf „Laden“.

Das Gerät aktualisiert seine Anzeige im Rahmen „Information“ und zeigt die Anzahl der gelernten IP-Verbindungen an.

- ☐ Um den Lernmodus anzuhalten, klicken Sie auf „Stoppe Lernmodus“.

Die grafische Benutzeroberfläche aktiviert die Karteikarte „Externes Interface“.

Verkehrsdaten inspizieren und mit Hilfe des Assistenten Regeln für erwünschten Verkehr ableiten:

- ☐ Wählen Sie die Karteikarte „Externes Interface“.
- ☐ Sortieren Sie im Rahmen „Erfasste Daten“ die Tabelle aufsteigend nach der Spalte „Quelladresse“.
- ☐ Suchen Sie die 1. Zeile mit der IP-Adresse des Konfigurations-Computers.
- ☐ Suchen Sie ab dieser Zeile die http-Verkehrsdaten zwischen Konfigurations-Computer und Switch (tcp-Port 80). Dies ist die 1. Zeile mit:
 - der Zieladresse des Switch,
 - dem Zielport 80 und
 - dem Protokoll `tcp`.

- ☐ Markieren Sie diese Zeile.

- ☐ Klicken Sie auf „Zum Regelsatz hinzufügen“.

Das Gerät übernimmt die gelernten Daten der selektierten Zeile in eine neue Regel.

Die grafische Benutzeroberfläche markiert im Rahmen „Erfasste Daten“ die Zeile dunkelgrün, die die neue Regel abdeckt.

- ☐ Um die zufälligen Quellports der http-Anfragen zu erlauben, ändern Sie den Quellport der Regel auf `any`.

Die grafische Benutzeroberfläche markiert nun im Rahmen „Erfasste Daten“ die Zeilen dunkelgrün, die die neue Regel abdeckt.

- ☐ Suchen Sie nochmals im Rahmen „Erfasste Daten“ die 1. Zeile mit der IP-Adresse des Konfigurations-Computers.

- ☐ Suchen Sie ab dieser Zeile die snmp-Verkehrsdaten zwischen Konfigurations-Computer und Switch (udp-Port 161). Dies ist die 1. Zeile mit:
 - der Zieladresse des Switch,
 - dem Zielport 161 und
 - dem Protokoll `udp`.

- ☐ Markieren Sie diese Zeile.

- ☐ Klicken Sie auf „Zum Regelsatz hinzufügen“.

Das Gerät übernimmt die gelernten Daten der selektierten Zeile in eine neue Regel.

Die grafische Benutzeroberfläche markiert die Zeile dunkelgrün, die die neue Regel abdeckt.

Die Zeilen, die die vorher erstellte Regel abdeckt, markiert die grafische Benutzeroberfläche hellgrün.

- ☐ Um die zufälligen Quellports der snmp-Anfragen zu erlauben, ändern Sie den Quellport der Regel auf `any`.

Die grafische Benutzeroberfläche markiert nun im Rahmen „Erfasste Daten“ die Zeilen dunkelgrün, die die neue Regel abdeckt.

Sie haben nun aus dem erwünschten Verkehr neue Regeln erstellt, mit deren Hilfe die Firewall diesen Verkehr erlauben wird, nachdem Sie den Assistenten für den Firewall-Lern-Modus beendet haben.

Den anderen gelernten Verkehr soll die Firewall im Betrieb verwerfen. Sie ignorieren daher diesen Verkehr bei der Regel-Erstellung.

Die grafische Benutzeroberfläche stellt im Rahmen „Erfasste Daten“ diese Zeilen unmarkiert (mit weißem Hintergrund) dar.

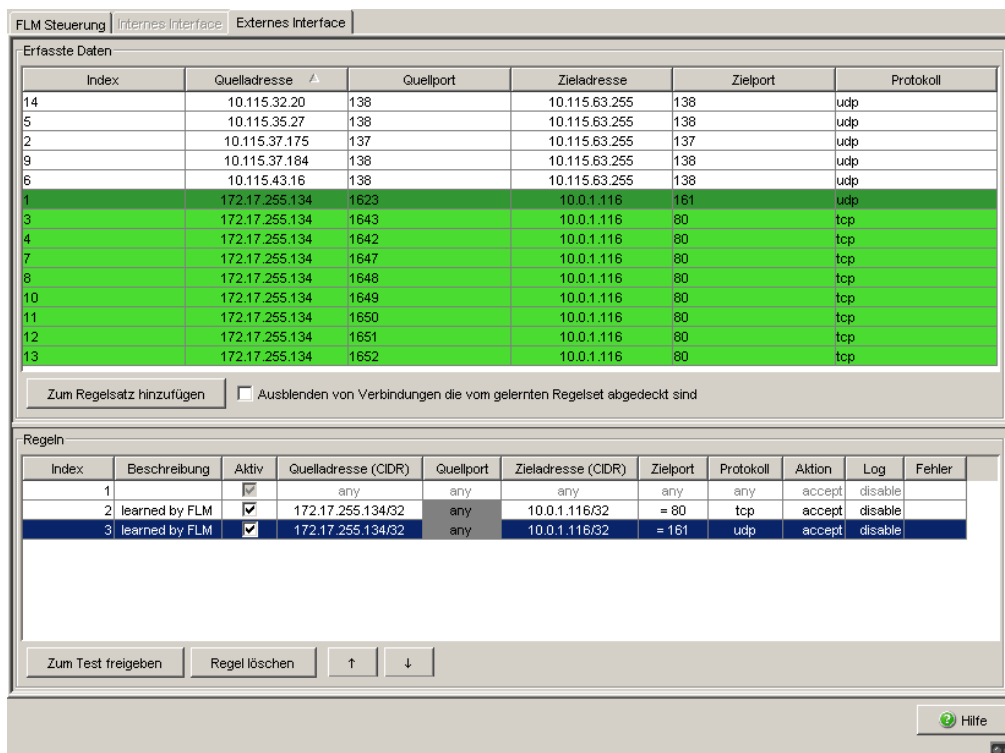


Abb. 28: Dialog Firewall-Lern-Modus, Karteikarte „Externes Interface“

Die neu erstellten Paketfilter-Regeln testen:

- ☐ Klicken Sie auf „Zum Test freigeben“.
- ☐ Wählen Sie die Karteikarte „FLM-Steuerung“.
- ☐ Klicken Sie auf „Starte Testmodus“.

Die grafische Benutzeroberfläche setzt die Anzahl der bisher im Testmodus gelernten „IP-Einträge“ auf 0.

- ☐ Laden Sie nochmals auf Ihrem Konfigurations-Computer in einem anderen Browser-Fenster die grafische Benutzeroberfläche des Switch in der Produktionszelle neu. Greifen Sie zum Test der neuen Paketfilter-Regeln nochmals auf Dialogseiten und HTML-Seiten zu. Damit erzeugen Sie den erwünschten snmp- und http-Verkehr.
- ☐ Wechseln Sie wieder zum Assistenten für den Firewall-Lern-Modus.
- ☐ Klicken Sie auf „Stoppe Testmodus“.

Die grafische Benutzeroberfläche aktualisiert ihre Anzeige und zeigt die Anzahl der IP-Einträge an, die das Gerät im Testmodus neu gelernt hat.

- ☐ Wählen Sie die Karteikarte „Externes Interface“.

Das Gerät hat den http- und snmp-Verkehr, den Sie vorher erlaubt haben, nun beim Lernen ignoriert.

Entdecken Sie in den gelernten Daten weiteren Verkehr, den Sie erlauben möchten, haben Sie die Möglichkeit, aus diesem Verkehr weitere Regeln abzuleiten.

Wiederholen Sie danach den Test.

Den Assistenten für den Firewall-Lern-Modus beenden und die neuen Paketfilter-Regeln speichern:

- ☐ Wählen Sie die Karteikarte „FLM-Steuerung“.
- ☐ Klicken Sie im Rahmen „Funktion“ auf „Aus“.
- ☐ Um den Assistenten für den Firewall-Lern-Modus zu beenden, klicken Sie auf „Schreiben“.

Die grafische Benutzeroberfläche weist Sie auf das Verlassen des Firewall-Lern-Modus hin und fragt Sie, ob Sie die aktuelle Konfiguration des Gerätes speichern oder die vorherige Konfiguration wiederherstellen möchten.

- ☐ Klicken Sie auf „Schreiben“.

Die grafische Benutzeroberfläche fordert Sie zur Eingabe eines Dateinamens auf. Der vorgeschlagene Dateiname hat das Format

`nnnnnnnnnnnnnnnn_afterFLM.`

- ☐ Geben Sie für den Dateinamen `Beispiel01_nach_FLM` ein und klicken Sie „OK“.

Das Gerät speichert die aktuelle Konfiguration mit den neuen Paketfilter-Regeln unter dem angegebenen Namen im NVM und setzt diese in den Zustand „aktiv“.

Die grafische Benutzeroberfläche deaktiviert anschließend die Bedienelemente für den Firewall-Lern-Modus und die Karteikarte „Externes Interface“.

Weitere Möglichkeiten:

Wenn Sie neue Geräte in der Fertigungszelle hinzufügen oder die Geräte in der Fertigungszelle auch von anderen Konfigurations-Computern aus verwalten wollen, haben Sie die Möglichkeit:

- ▶ den Assistenten für den Firewall-Lern-Modus erneut auszuführen und weitere Regeln für neuen, erwünschten Verkehr zu erstellen, z. B. für die Steuerung eines Roboters.
- ▶ bestehende Regeln manuell im Dialog `Eingehende IP-Pakete` zu ändern, z.B.
 - Um die ganze Fertigungszelle als Ziel für erwünschten `http`- und `snmp`-Datenverkehr zuzulassen, ändern Sie die Einträge für „Ziel-adresse (CIDR)“ auf `10.0.1.0/24`.
 - Um von den Konfigurations-Computern im Administrations-Subnetz aus per `http` und `snmp` auf die Fertigungszelle zugreifen zu können, ändern Sie die Einträge für „Quelladresse (CIDR)“ auf `172.17.255.0/24`.
 - Um die Web-Server der Geräte in der Fertigungszelle rasch zu verbergen, ändern Sie bei dem Eintrag mit dem Zielport `80` und dem Protokoll `tcp` die Aktion auf `drop`. Die Firewall erlaubt weiterhin das Management der Geräte per `snmp`.
 - Um zu Testzwecken mittels eines momentan noch unbekannten, proprietären, TCP-basierten Protokolls auf einen Roboter zuzugreifen, ändern Sie den Eintrag für „Zielport“ vorübergehend von `80` auf `any` und stellen Sie die Aktion auf `accept`.

Außerdem haben Sie die Möglichkeit, neue Regeln im Dialog `Eingehende IP-Pakete` manuell hinzuzufügen:

- ▶ für erwünschten Verkehr, z.B. für die Ansteuerung eines Roboters, der ein proprietäres Protokoll mit der Layer 4-Protokoll-Nr. 141 verwendet:
 - Beschreibung: `Roboter, IP/141`
 - aktiv: `an`
 - Quelladresse: `172.17.255.0/24`
 - Quellport: `any`
 - Zieladresse (CIDR): `10.0.1.5/32`
 - Zielport: `any`

- Protokoll: 141
 - Aktion: `accept`
- ggf. auch für unerwünschten Verkehr, z.B. um NetBIOS-Verkehr an die Netz-Broadcast-Adresse des Firmennetzes beim Lernen explizit zu ignorieren:
- Beschreibung: `NetBIOS-Broadcasts verwerfen`
 - aktiv: `an`
 - Quelladresse: `10.115.0.0/19`
 - Quellport: `any`
 - Zieladresse (CIDR): `any`
 - Zielport: `136><140`
 - Protokoll: `any`
 - Aktion: `drop`

Anmerkung: Wenn Sie Verkehr an einem Interface lernen, für das Sie eine aktive `drop`-Regel konfiguriert haben, ignoriert die Firewall beim Lernen den Verkehr, auf den die Regel zutrifft.

Um diesen Verkehr zu lernen und zu inspizieren, deaktivieren Sie vor dem Lernen die `drop`-Regel.

6.2 NAT – Network Address Translation

Das Network Address Translation (NAT)-Protokoll beschreibt ein Verfahren, automatisiert und transparent IP-Adressinformationen in Datenpaketen zu verändern und dennoch die Datenpakete zielgenau zu vermitteln.

NAT kommt zum Einsatz, wenn IP-Adressen eines internen Netzes nicht nach außen sichtbar sein sollen. Die Gründe hierfür können z.B. sein:

- ▶ die Struktur des internen Netzes vor der Außenwelt zu verstecken.
- ▶ das Verstecken privater IP-Adressen ([siehe auf Seite 38 „Private IP-Adressen“](#)).
- ▶ die Mehrfachverwendung von IP-Adressen z.B. durch Bildung identischer Produktionszellen.

Abhängig vom Grund, weshalb Sie NAT einsetzen, bietet Ihnen NAT unterschiedliche Verfahren zur Umsetzung der IP-Adressinformation an.

Eigenschaften	IP-Masquerading	1:1-NAT	Portweiterleitung
Initiierung einer Verbindung von innen	ja	ja	nein
Initiierung einer Verbindung von außen	nein	ja	ja

Tab. 9: Vergleich der einzelnen NAT-Verfahren

6.2.1 IP-Masquerading

IP-Masquerading verwenden Sie, um die interne Netzstruktur nach außen hin zu verstecken, sodass sie hinter einer Maske zu verbergen.

Beim IP-Masquerading ersetzt die Firewall die Quell-IP-Adresse eines Datenpaketes aus dem internen Netz durch die externe IP-Adresse der Firewall. Zur Identifizierung der unterschiedlichen internen IP-Adressen fügt NAT der Adressinformation die logische Portnummer der Verbindung hinzu. Das Hinzufügen der Port-Information gab dem IP-Masquerading auch den Namen „Network Address Port Translation“ (NAPT).

Durch die Umsetzung der IP-Adressen mit Hilfe von Port-Informationen können Geräte aus dem internen Netz heraus Kommunikations-Verbindungen nach außen aufbauen. Da Geräte im externen Netz aber ausschließlich die externe IP-Adresse der Firewall kennen, sind sie nicht in der Lage, eine Kommunikations-Verbindung zu einem Gerät im internen Netz aufzubauen.

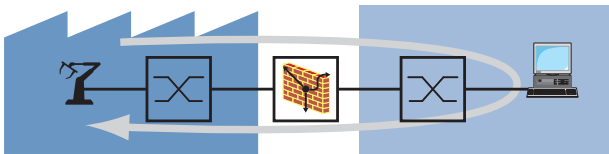


Abb. 29: Aufbau einer Kommunikations-Verbindung bei IP-Masquerading

6.2.2 1:1-NAT

1:1-NAT verwenden Sie, wenn Sie identische Produktionszellen mit gleichen IP-Adressen aufbauen und diese mit dem externen Netz verbinden wollen. Die Firewall ordnet dazu den Geräten im internen Netz eine andere IP-Adresse im externen Netz zu.

Beim 1:1-NAT ersetzt die Firewall die Quell-IP-Adresse eines Datenpaketes aus dem internen Netz durch eine IP-Adresse des externen Netzes.

Durch die 1:1-Umsetzung der IP-Adressen können Geräte aus dem internen Netz heraus Kommunikations-Verbindungen nach außen aufbauen und Geräte im externen Netz Kommunikations-Verbindungen zu einem Gerät im internen Netz aufbauen.

Deshalb wird 1:1-NAT auch bidirektionales NAT genannt.

Sie haben die Möglichkeit, 1:1-NAT mit der Router-Redundanz zu kombinieren. Dabei bilden 2 physikalische Geräte einen virtuellen, hochverfügbaren 1:1-NAT-Router ([siehe auf Seite 197 „Router-Redundanz“](#)).

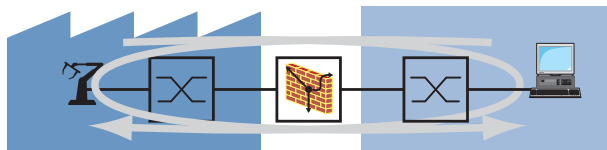


Abb. 30: Aufbau einer Kommunikations-Verbindung bei 1:1-NAT

Anmerkung: 1:1-NAT verändert ausschließlich IP-Adressen im IP-Header der Pakete. Für FTP bietet das Gerät ein Application Layer Gateway.

Anmerkung: Bei 1:1-NAT antwortet die Firewall auf ARP-Anfragen aus dem externen Netz an Adressen, die sie aus dem internen Netz abbildet. Dies gilt auch, wenn im internen Netz kein Gerät mit der IP-Adresse existiert. Vergeben Sie daher im externen Netz an Geräte ausschließlich IP-Adressen, die außerhalb des Bereichs liegen, den 1:1-NAT vom internen in das externe Netz abbildet.

■ Inverses 1:1-NAT

Inverses 1:1-NAT verwenden Sie , wenn die Geräte im internen Netz mit den Geräten im externen Netz so kommunizieren sollen, als wären die Geräte des externen Netzes im internen Netz. Die Firewall ordnet dazu den Geräten im externen Netz eine andere IP-Adresse des internen Netzes zu.

Bei inversem 1:1-NAT ersetzt die Firewall die Ziel-IP-Adresse eines Datenpaketes aus dem internen Netz durch eine IP-Adresse des externen Netzes.

Erstellen Sie dazu für die Geräte im externen Netz einen inversen 1:1-NAT-Eintrag.

Anmerkung: Bei inversem 1:1-NAT antwortet die Firewall auf ARP-Anfragen aus dem internen Netz an Adressen, die sie aus dem externen Netz abbildet. Dies gilt auch, wenn im externen Netz kein Gerät mit der IP-Adresse existiert. Vergeben Sie daher im internen Netz an Geräte ausschließlich IP-Adressen, die außerhalb des Bereichs liegen, den der inverse 1:1-NAT-Eintrag vom externen in das interne Netz abbildet.

■ **Double-NAT**

Double-NAT, auch Twice-NAT genannt, verwenden Sie, wenn die Geräte im internen Netz mit den Geräten im externen Netz so kommunizieren sollen, als wären die Geräte des externen Netzes im internen Netz und umgekehrt.

Die Firewall ordnet dabei

- ▶ den Geräten im internen Netz eine andere IP-Adresse des externen Netzes zu (1:1-NAT-Funktion) und
- ▶ den Geräten im externen Netz eine andere IP-Adresse des internen Netzes zu (inverse 1:1-NAT-Funktion).

Bei Double-NAT ersetzt die Firewall bei einem Datenpaket aus dem internen Netz

- ▶ die Quell-IP-Adresse durch eine IP-Adresse des externen Netzes und
- ▶ die Ziel-IP-Adresse durch eine IP-Adresse des externen Netzes.

Erstellen Sie dazu für die Geräte im internen Netz einen 1:1-NAT-Eintrag und zusätzlich für die Geräte im externen Netz einen inversen 1:1-NAT-Eintrag.

6.2.3 Port-Weiterleitung

Portweiterleitung verwenden Sie, wenn Sie die interne Netzstruktur nach außen hin verstecken wollen, aber den Aufbau einer Kommunikationsverbindung von außen nach innen zulassen wollen.

Bei der Portweiterleitung bauen ein oder mehrere externe Geräte eine Kommunikationsverbindung in das interne Netz auf. Hierbei adressiert ein externes Gerät Datenpakete an einen bestimmten Port mit der externen IP-Adresse der Firewall. Datenpakete mit einer zulässigen Quell-IP-Adresse, die die Firewall an diesem Port empfängt, leitet die Firewall an den Port des in der NAT-Tabelle eingetragenen internen Gerätes weiter. Daher stammt der Name Portweiterleitung. Da in diesem Fall ein dediziertes Ziel adressiert wird, heißt dieses Verfahren auch Destination-NAT.

Durch die Umsetzung der IP-Adressen und der Port-Information an Hand der eingehenden Portadressierung können Geräte aus dem externen Netz Kommunikations-Verbindungen nach innen aufbauen.

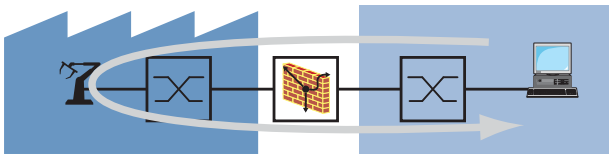


Abb. 31: Aufbau einer Kommunikations-Verbindung bei Portweiterleitung

Eine typische Anwendung im industriellen Bereich ist der Port 5631 zur Fernwartung eines PCs in einer Produktionszelle.

6.2.4 NAT-Anwendungsbeispiele

■ Eine Produktionszelle über 1:1-NAT mit dem Firmennetz verbinden

Sie haben mehrere identische Produktionszellen und möchten diese mit Ihrem Firmennetz verbinden. Da selbst die verwendeten IP-Adressen in den Produktionszellen identisch sind, übersetzen Sie die IP-Adressen mit Hilfe der 1:1-NAT-Funktion.

Bekannt sind:

Parameter	IP-Parameter Firewall 1	IP-Parameter Firewall 2
Internes Netz (Produktionszelle)	10.0.1.193/28	10.0.2.1/28
Externes Netz (Firmennetz)	10.0.1.193/28	10.0.2.17/28

Voraussetzungen für die weitere Konfiguration:

- ▶ Die Firewall ist im Router-Modus.
- ▶ Die IP-Parameter der Router-Interfaces sind konfiguriert.
- ▶ Gateway und IP-Adresse der Geräte in den Produktionszellen sind konfiguriert.
- ▶ Die Geräte in den Produktionszellen verwenden als Gateway die IP-Adresse des internen Interface (Port 1) der Firewall.

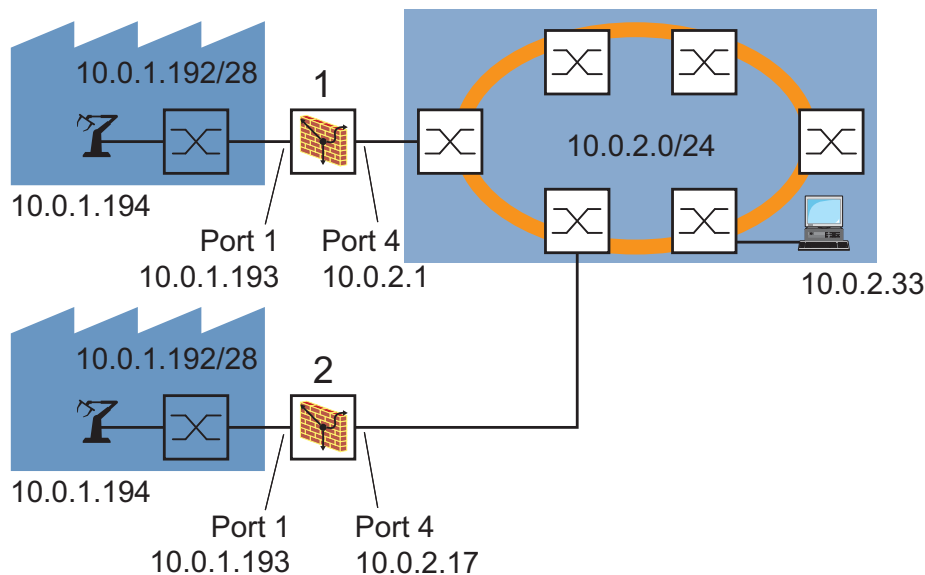


Abb. 32: Eine von mehreren identischen Produktionszellen über 1:1-NAT mit dem Firmennetz verbinden

- ☐ Konfigurieren Sie zunächst die Firewall 1.
Geben Sie die Parameter für die Übersetzung der IP-Adressen ein.
- ☐ Wählen Sie den Dialog `Netzwerk: NAT: 1:1-NAT`.
- ☐ Klicken Sie auf „Eintrag erzeugen“.
Hierdurch fügen Sie der Tabelle einen neuen Eintrag hinzu.
- ☐ Tragen Sie die Parameter für die Übersetzung der IP-Adressen ein:
„Beschreibung“: Produktionshalle 1
„Internes Netz“: 10.0.1.193
„Externes Netz“: 10.0.2.1
„Netzmaske“: 28
- ☐ Klicken Sie in das Feld „Aktiv“ dieses Eintrags, um den Eintrag zu aktivieren.
- ☐ Um die Änderungen flüchtig zu speichern, klicken Sie „Schreiben“.
- ☐ Speichern Sie die Einstellungen in den nicht-flüchtigen Speicher.
- ☐ Öffnen Sie hierzu den Dialog `Grundeinstellungen: Laden/Speichern`.
- ☐ Klicken Sie auf „Speichern in NVM + ACA“, um die Daten nicht-flüchtig zu speichern.

- ☐ Konfigurieren Sie die Firewall 2 auf die gleiche Weise.
Verwenden Sie die Werte für die Firewall 2 aus der Tabelle auf der vorhergehenden Seite.

■ 2 Geräte über Double-NAT verbinden

Sie möchten zu Testzwecken eine Workstation in Ihrem Firmennetz mit einem Roboter in einer Produktionszelle verbinden. Da der Testaufbau erfordert, dass sich beide Geräte logisch im selben Netz befinden, übersetzen Sie die IP-Adressen mit Hilfe der Double-NAT-Funktion.

Bekannt sind:

Parameter	Roboter	Workstation
IP-Adresse im Produktionsnetz (intern)	10.0.1.194	10.0.1.195 ^a
IP-Adresse im Firmennetz (extern)	10.0.2.194 ^a	10.0.2.195

Tab. 10: IP-Adressen der Testgeräte

a: Diese IP-Adresse wird durch NAT erzeugt

Voraussetzungen für die weitere Konfiguration:

- ▶ Die Firewall ist im Router-Modus.
- ▶ Die IP-Parameter der Router-Interfaces sind konfiguriert.
- ▶ Die IP-Adressen der Geräte sind konfiguriert.

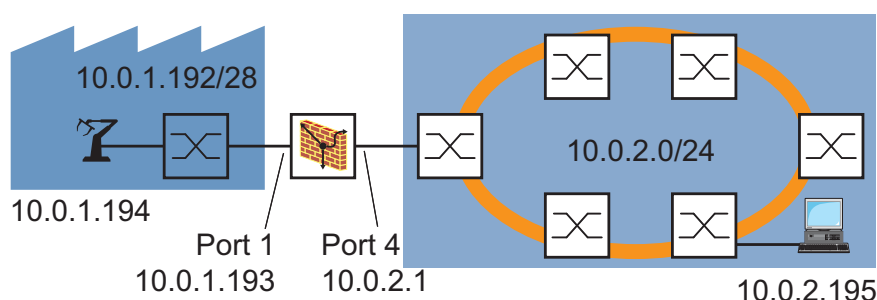


Abb. 33: 2 Geräte über Double-NAT verbinden

- ☐ Geben Sie die Parameter für die Übersetzung der IP-Adressen ein.

- ☐ Wählen Sie den Dialog
Netzicherheit:NAT:1:1-NAT.

- ☐ Klicken Sie auf „Eintrag erzeugen“.
Hierdurch fügen Sie der Tabelle einen neuen Eintrag hinzu.
- ☐ Tragen Sie die Parameter für die Übersetzung der IP-Adresse des Roboters ein:
„Beschreibung“: Roboter Produktionshalle (Test)
„Internes Netz“: 10.0.1.194
„Externes Netz“: 10.0.2.194
„Netzmaske“: 32
- ☐ Klicken Sie in das Feld „Output“ (Double-NAT) dieses Eintrags, um Double-NAT für den Eintrag zu aktivieren.
- ☐ Klicken Sie in das Feld „Aktiv“ dieses Eintrags, um den Eintrag zu aktivieren.
- ☐ Klicken Sie auf „Eintrag erzeugen“.
Hierdurch fügen Sie der Tabelle einen neuen Eintrag hinzu.
- ☐ Tragen Sie die Parameter für die Übersetzung der IP-Adresse der Workstation ein:
„Beschreibung“: Workstation Firmennetz (Test)
„Internes Netz“: 10.0.1.195
„Externes Netz“: 10.0.2.195
„Netzmaske“: 32
- ☐ Klicken Sie in das Feld „Output“ (Double-NAT) dieses Eintrags, um Double-NAT für den Eintrag zu aktivieren.
- ☐ Klicken Sie in das Feld „Invertiert“ dieses Eintrags, um den Eintrag als invertierten 1:1-NAT-Eintrag zu markieren.
- ☐ Klicken Sie in das Feld „Aktiv“ dieses Eintrags, um den Eintrag zu aktivieren.
- ☐ Klicken Sie auf „Schreiben“, um die Einträge in der Konfiguration flüchtig zu speichern.

☐ Speichern Sie die Einstellungen in den nicht-flüchtigen Speicher.

- ☐ Öffnen Sie hierzu den Dialog Grundeinstellungen:Laden/Speichern.
- ☐ Klicken Sie auf „Speichern in NVM + ACA“, um die Daten nicht-flüchtig zu speichern.

■ Einen Switch in einer Produktionszelle von einem PC außerhalb der Produktionszelle verwalten (Port-Weiterleitung)

Sie haben eine Produktionszelle mit eigenen IP-Adressen, die im Firmennetz nicht sichtbar sein sollen über eine Firewall mit Ihrem Firmennetz verbunden. Damit ein Administrator im Firmennetz einen Switch innerhalb der Produktionszelle verwalten kann, konfigurieren Sie die Portweiterleitungs-Funktion.

Bekannt sind:

Parameter	Switch	Firewall	PC
IP-Adresse interner Port		10.0.1.201	
IP-Adresse externer Port		10.0.2.1	
IP-Adresse	10.0.1.193		10.0.2.17
Gateway	10.0.1.201		10.0.2.1

Voraussetzungen für die weitere Konfiguration:

- ▶ Die Firewall ist im Router-Modus.
- ▶ Die IP-Parameter der Router-Interfaces sind konfiguriert.
- ▶ Gateway und IP-Adresse der Geräte in den Produktionszellen sind konfiguriert.
- ▶ Die Geräte in den Produktionszellen verwenden als Gateway die IP-Adresse des internen Interface (Port 1) der Firewall.

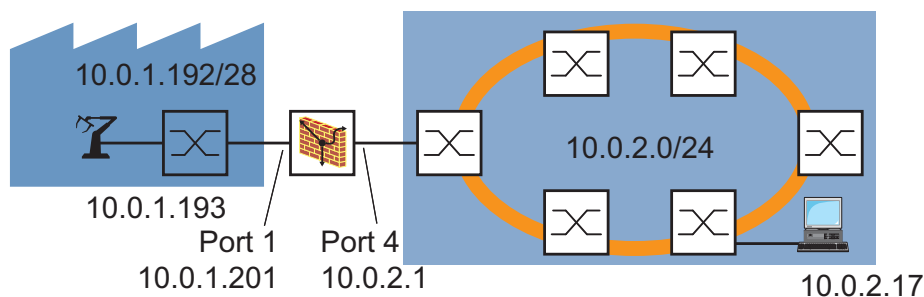


Abb. 34: Einen Switch innerhalb der Produktionszelle von außerhalb verwalten

- ☐ Konfigurieren Sie die Firewall.
Geben Sie die Parameter für die Übersetzung der IP-Adressen ein.

- ☐ Wählen Sie den Dialog
Netzicherheit:NAT:Portweiterleitung.
- ☐ Klicken Sie auf „Eintrag erzeugen“.
Hierdurch fügen Sie der Tabelle einen neuen Eintrag hinzu.

- ☐ Tragen Sie die Parameter für die http-Übertragung ein:
 - „Quelladresse (CIDR)“: 10.0.1.17/24
 - „Quellport“: any
 - „Eingangsadresse“: 10.0.2.1
 - „Eingangsport“: 8080
 - Portnummern, die höher sind als 1024 können Sie frei vergeben.
 - „Weiterleitungsadresse“: 10.0.1.193
 - „Weiterleitungsport“: http, Web-Server des Switch.
 - „Protokoll“: tcp.
- ☐ Klicken Sie in das Feld „Aktiv“ dieses Eintrags, um den Eintrag zu aktivieren.
- ☐ Klicken Sie auf „Eintrag erzeugen“.
Hierdurch fügen Sie der Tabelle einen neuen Eintrag hinzu.
- ☐ Tragen Sie die Parameter für die SNMP-Übertragung ein:
 - „Quelladresse (CIDR)“: 10.0.1.17/24
 - „Quellport“: any
 - „Eingangsadresse“: 10.0.2.1
 - „Eingangsport“: 8081
 - Portnummern, die höher sind als 1024 können Sie frei vergeben.
 - „Weiterleitungsadresse“: 10.0.1.193
 - „Weiterleitungsport“: snmp, für die Kommunikation des Applets mit der Web-Seite des Switch.
 - „Protokoll“: udp.
- ☐ Klicken Sie in das Feld „Aktiv“ dieses Eintrags, um den Eintrag zu aktivieren.
- ☐ Klicken Sie auf „Schreiben“, um die Einträge in der Konfiguration flüchtig zu speichern.

☐ Speichern Sie die Einstellungen in den nicht-flüchtigen Speicher.

- ☐ Öffnen Sie hierzu den Dialog Grundeinstellungen:Laden/Speichern.
- ☐ Klicken Sie auf „Speichern in NVM + ACA“, um die Daten nicht-flüchtig zu speichern.

6.3 Benutzer-Firewall

6.3.1 Beschreibung der Benutzer-Firewall-Funktion

Bei der benutzerbezogenen Datenverkehrskontrolle überprüft die Firewall die Daten eines von Ihnen zuvor definierten Benutzers ([siehe auf Seite 116 „Beschreibung der externen Authentifizierung“](#)). Die Firewall bietet Ihnen die Möglichkeit, mehrere Benutzer zu definieren. Für jeden definierten Benutzer können Sie unterschiedliche Regeln erstellen, nach denen die Firewall Datenpakete des definierten Benutzers behandelt.

Nachdem sich ein Benutzer auf der Webseite der Firewall für die Benutzer-Firewall angemeldet hat ([siehe Abb. 5](#)), prüft die Firewall die Datenpakete dieses Benutzers nach den für ihn definierten Regeln.

Trifft keine dieser Regeln zu, dann überprüft die Firewall diese Datenpakete nach den Regeln der allgemeinen Paketfilter ([siehe auf Seite 122 „Paketfilter“](#)).

Index	Regelgruppe	Referenz	Interface	Quellnetz	Quellport	Zielnetz	Zielport	Protokoll	Aktion	Log
1	Special Traffic	-1	egress	any	any	any	any	any	accept	disable
2	Rate-Limits (DoS)	-1	internal	any	any	any	any	tcp-syn	drop	enable
3	Rate-Limits (DoS)	-1	external	any	any	any	any	tcp-syn	drop	enable
4	Rate-Limits (DoS)	-1	internal	any	any	any	any	icmp-echo	drop	enable
5	Rate-Limits (DoS)	-1	external	any	any	any	any	icmp-echo	drop	enable
6	Special Traffic	-1	loopback	any	any	any	any	any	accept	disable
7	Special Traffic	-1	error	any	any	any	any	any	accept	disable
8	Miscellaneous	1	internal	any	any	me	= 53	udp	accept	disable
9	HTTPS Access	0	internal	any	any	me	= 443	tcp	accept	disable
10	HTTPS Access	0	any	any	any	me	= 443	tcp	drop	disable
11	SSH Access	0	internal	any	any	me	= ssh	tcp	accept	disable
12	SSH Access	0	any	any	any	me	= ssh	tcp	drop	disable
13	SNMP Access	0	internal	any	any	me	= 161	udp	accept	disable
14	SNMP Access	0	any	any	any	me	= 161	udp	drop	disable
15	PPP Packet Filter	0	ppp (serial)	any	any	any	any	any	drop	disable
16	Packet Filter IP Outgoing	1	internal	any	any	any	any	any	accept	disable
17	Packet Filter IP Outgoing	0	internal	any	any	any	any	any	drop	disable
18	Packet Filter IP Incoming	0	external	any	any	any	any	any	drop	disable
19	Default Rules	-1	any	any	any	any	any	any	drop	disable

Abb. 35: IP-Firewall-Liste

Die Benutzer-Firewall-Funktion setzen Sie ein, wenn Sie bestimmten Benutzern zeitlich begrenzt einen durch Regeln erweiterten Zugriff auf das interne oder externe Netz gewähren wollen.

6.3.2 Anwendungsbeispiel für die Benutzer-Firewall-Funktion

Die Abbildung zeigt einen typischen Anwendungsfall:

Ein Service-Techniker möchte ein Software-Update für die Wartung eines Roboters von einem Server herunterladen.

Bekannt sind:

Parameter	Firewall	Service-PC	Server
IP-Adresse interner Port	10.0.1.201		
Externer Port	PPPoE		
IP-Adresse		10.0.1.51	10.149.1.51
Gateway		10.0.1.201	

Voraussetzungen für die weitere Konfiguration:

- ▶ Die Firewall ist im Router-Modus.
- ▶ Die IP-Parameter der Firewall-Router-Interface sind konfiguriert.
- ▶ Die Geräte im internen Netz haben als Gateway die IP-Adresse des internen Interfaces (Port 1) der Firewall.
- ▶ Gateway und IP-Adresse des PCs sind konfiguriert.
- ▶ Die Paketfilter sind entsprechend des Beispiels ([siehe auf Seite 126 „Anwendungsbeispiel für Paketfilter“](#)) konfiguriert.
- ▶ Die externe Authentifizierung für den „Service“ ist konfiguriert ([siehe auf Seite 116 „Anwendungsbeispiel für die externe Authentifizierung“](#)).

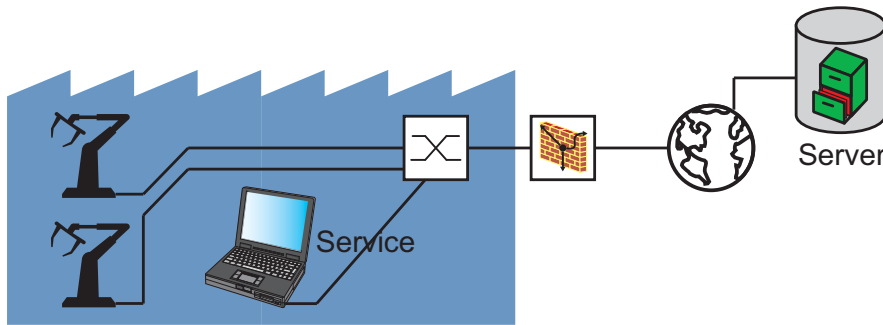


Abb. 36: Benutzer-Firewall Anwendungsbeispiel

☐ Erstellen Sie einen Benutzer-Firewall-Eintrag.

- ☐ Wählen Sie den Dialog
Netzwerk:Benutzer-Firewall-Einträge.
- ☐ Klicken Sie auf „Eintrag erzeugen“.
Hierdurch fügen Sie der Tabelle einen neuen Eintrag hinzu.
- ☐ Markieren Sie den Eintrag.
Klicken Sie auf „Bearbeiten“.
- ☐ Wählen Sie die Karteikarte Grundeinstellungen.
- ☐ Geben Sie die Daten ein:
 - ▶ „Name“, Service-Benutzer
Das ist der Name für diesen Benutzer-Firewall-Eintrag.
 - ▶ „Zeitgrenze“, 7200
Maximale Zugriffsdauer in Sekunden.
 - ▶ „Zeitgrenzentyp“, static
Mit der Anmeldung des Benutzers beginnt das Dekrementieren der Zeitgrenze.
 - ▶ „Quelladresse“, 10.0.1.51
Das ist die IP-Adresse des Service-PCs.
 - ▶ „Beschreibung“, Öffnen des Zugangs zur Fertigungszelle für den Service-Einsatz.
- ☐ Wählen Sie die Karteikarte Konten.
- ☐ Klicken Sie auf „Eintrag erzeugen“.
Ein Dialog bietet Ihnen die Möglichkeit, ein bestehendes Konto auszuwählen, z.B. Service (siehe auf Seite 116 „Anwendungsbeispiel für die externe Authentifizierung“).
Wählen Sie ein Konto aus.
Klicken Sie auf „OK“.

- ☐ Wählen Sie die Karteikarte `Regeln`.
- ☐ Klicken Sie auf „Eintrag erzeugen“.
Hierdurch fügen Sie der Tabelle einen neuen Eintrag hinzu.
- ☐ Markieren Sie den Eintrag.
Klicken Sie auf „Bearbeiten“.
- ☐ Geben Sie die Daten ein:
 - ▶ „Quellport“, `any`
Da der Quellport, über den der Browser des Notebooks kommuniziert, normalerweise kein fester Port ist, ist die Einstellung `any` notwendig.
 - ▶ „Zielnetz“, `10.149.1.51/32`
IP-Adresse des Servers, auf welchem die Software für den Roboter liegt.
 - ▶ „Zielport“, `http`
Mit der Einstellung `http` kann der Service-Techniker über seinen Browser die Software herunterladen.
 - ▶ „Beschreibung“, `Software-Download`
Sinnhafte Beschreibung der Regel.
 - ▶ „Protokoll“, `tcp`.
 - ▶ „Log“, wenn Sie die Zugriffe protokollieren wollen, dann wählen Sie diese Funktion an.
- ☐ Um die Änderungen flüchtig zu speichern, klicken Sie „Schreiben“.
- ☐ Klicken Sie auf „Zurück“.
Hierdurch gelangen Sie zurück in die Karteikarte `Regeln`.
- ☐ Klicken Sie in das Feld „Aktiv“ dieses Eintrags, um den Eintrag zu aktivieren.
- ☐ Klicken Sie auf „Zurück“.
Hierdurch gelangen Sie zurück in die Tabellenansicht.
- ☐ Klicken Sie in das Feld „Aktiv“ dieses Eintrags, um den Eintrag zu aktivieren.
- ☐ Um die Änderungen flüchtig zu speichern, klicken Sie „Schreiben“.

- ☐ Speichern Sie die Einstellungen in den nicht-flüchtigen Speicher.

- ☐ Öffnen Sie hierzu den Dialog `Grundeinstellungen:Laden/Speichern`.
- ☐ Klicken Sie auf „Speichern in NVM + ACA“, um die Daten nicht-flüchtig zu speichern.

6.4 Unterstützung beim Schutz vor Denial of Service (DoS)

Diese Funktion unterstützt Sie beim Schutz Ihres Netzes und Ihres Servers vor einem unerlaubten Zugriff durch eine Überflutung mit TCP-Verbindungen, Ping-Paketen und ARP-Paketen.

Anmerkung: Passen Sie die in den Voreinstellungen festgelegten Werte den tatsächlich benötigten TCP-Verbindungen, Ping-Paketen und ARP-Paketen in Ihrem Netz an. Das Gerät bietet Ihnen außerdem die Möglichkeit, bei Überschreitung einer Grenze einen Log-Eintrag zu erzeugen. Dies können Sie für jede Grenze gesondert einstellen.

6.5 VPN – Virtuelles privates Netz

Ein virtuelles privates Netz (VPN) bezeichnet einen Teil eines öffentlichen Netzes, das jemand für seine privaten Zwecke nutzt.

Das besondere an einem VPN ist, wie der Name „privat“ schon ausdrückt, die Abgeschlossenheit gegenüber dem öffentlichen Netz. Unterschiedliche Mechanismen unterstützen den Schutz der Daten des virtuellen privaten Netzes vor Lauschangriffen, Datenverfälschung und sonstigen Angriffen fremder Teilnehmer.

Im industriellen Umfeld dient ein VPN z.B. dazu, zwei Werksteile über das öffentliche Internet miteinander zu verbinden.

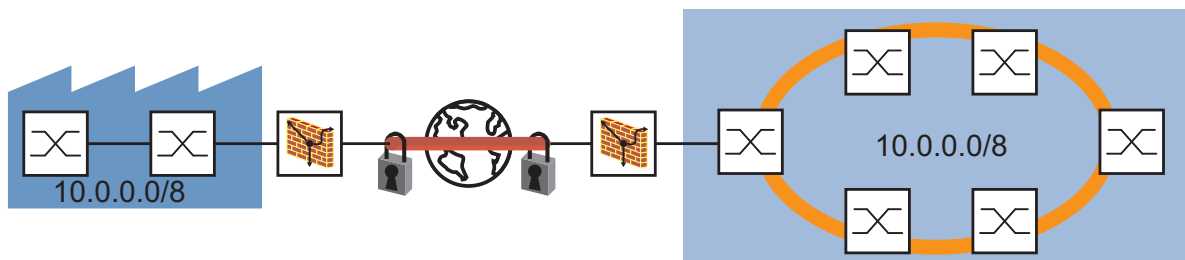


Abb. 37: VPN zum Verbinden zweier Werksteile

6.5.1 IPsec – Internet Protocol Security

IPsec (Internet Protocol Security) ist das am häufigsten eingesetzte VPN-Protokoll. IPsec regelt das Einrichten einer VPN-Verbindung und die Maßnahmen zur sicheren Datenübertragung im virtuellen privaten Netz. Zur sicheren Datenübertragung in einem VPN gehören:

- ▶ **Integritätsschutz**
Der Integritätsschutz hilft Ihnen sicherzustellen, dass die übertragenen Daten echt sind, d.h. von einem vertrauenswürdigen Absender stammen (authentisch sind) und der Inhalt unverfälscht beim Empfänger ankommt.
- ▶ **Verschlüsselung**
Die Verschlüsselung hilft Ihnen sicherzustellen, dass kein Unbefugter Einsicht in die Daten erlangt.
Verschlüsselungsverfahren kodieren die zu übertragenden Daten mit einem Code (Schlüssel), der ausschließlich den befugten Kommunikationsteilnehmern zur Verfügung steht.
- ▶ **Verkehrsflussvertraulichkeit**
Die Verkehrsflussvertraulichkeit hilft Ihnen sicherzustellen, dass kein Unbefugter Kenntnis über den wahren Empfänger und Absender eines Datenpaketes erhält.
Dies erreicht IPsec im Tunnelmodus durch die Verschlüsselung des kompletten IP-Paketes.

Zur Aushandlung der anzuwendenden Sicherheitsparameter zwischen den beiden Endpunkten einer VPN-Verbindung bietet IPsec zwei Modi (Transportmodus und Tunnelmodus):

- ▶ **Transportmodus:**
Im Transportmodus authentifizieren sich zwei Endgeräte gegenseitig und richten dann die zur Signierung und Verschlüsselung erforderlichen Parameter ein. Da die Kommunikation zwischen zwei definierten Endgeräten stattfindet, bleiben Empfänger- und Absender-Adresse sichtbar.
- ▶ **Tunnelmodus:**
Im Tunnelmodus authentifizieren sich zwei Router/Gateways gegenseitig und richten dann die zur Signierung und Verschlüsselung erforderlichen Parameter ein.
Die VPN-Verbindung hat zwar mit den beiden Routern/Gateways zwei adressierbare Endpunkte, aber die Kommunikation findet zwischen den Teilnehmern der an den Routern/Gateways angeschlossenen Netzen statt. Dies erlaubt die Verschlüsselung der zu übertragenden Kommunikationsdaten inklusive der Empfänger- und Absender-Adresse. Zur Adressierung zu den Endpunkten der VPN-Verbindung dienen die

Adressen der Router/Gateways.

Der Tunnelmodus bietet sich auch für die VPN-Verbindung zwischen einem Endgerät und einem Router/Gateway an. So bleiben die Adressdaten innerhalb des am Router/Gateway angeschlossenen Netzes verborgen.

6.5.2 IKE – Internet Key Exchange

IPsec benutzt das Internet Key Exchange Protokoll zur Authentisierung, zum Schlüsselaustausch und zur Vereinbarung weiterer Parameter für die Sicherheitsbeziehung einer VPN-Verbindung.

■ Authentisierung

Nutzen Sie die Authentisierung als Bestandteil der Sicherheitsbeziehung. Bei der Authentisierung legen sich die Verbindungspartner gegenseitig sozusagen Ihre Ausweise vor.

Dieser Ausweis kann aus

- ▶ einem sogenannten Pre-Shared-Key, einer zuvor über einen anderen Kommunikationsweg ausgetauschten Zeichenfolge, bestehen.
- ▶ einem digitalen Zertifikat, das eine Zertifizierungsstelle (Certification Authority, CA) vergeben hat, bestehen.

Zertifikate nach dem X.509-Standard enthalten z.B.

- Angaben zur Zertifizierungsstelle selbst,
- Gültigkeitsdauer des Zertifikates,
- zur erlaubten Anwendung,
- die Identität desjenigen, dem das Zertifikat zugeordnet ist (X.500 DN),

- der zu dieser Identität gehörige öffentliche Schlüssel,
 - digitale Signatur zur Beglaubigung der Verbindung zwischen dieser Identität und diesem zugehörigen öffentlichen Schlüssel.
- Größere Firmen und Behörden verfügen meist über eine eigene Zertifizierungsstelle. Zertifikate können Sie auch bei der Firma Hirschmann Automation and Control GmbH erwerben.
- Eine gebräuchliche Dateinamenserweiterung für ein Zertifikat nach dem PKCS#12-Standard ist „.p12“.
- Die in einer PKCS#12-Datei enthaltenen Informationen können Ihnen auch getrennt in einzelnen Dateien mit der Dateinamenserweiterung „.pem“ vorliegen.

■ Verschlüsselung

Um den Schutz der Daten zu unterstützen, bedient sich IKE verschiedener kryptografischer Algorithmen zur Verschlüsselung der Daten. Die Endpunkte der VPN-Verbindung benötigen die Schlüssel zur Codierung und Decodierung der Daten.

In einem ersten Schritt zum Aufbau der IKE-Sicherheitsbeziehung zwischen den Endpunkten der VPN-Verbindung

- ▶ einigen sich diese auf einen kryptografischen Algorithmus, der später die Schlüssel für die Codierung und Decodierung der IKE-Protokoll-Nachrichten verwendet.
- ▶ legen diese die Zeiträume fest, in denen die Schlüsselwechsel stattfinden und
- ▶ kommunizieren diese die Endpunkte, an denen die Codierung und Decodierung erfolgt. Die Endpunkte definiert zuvor der Administrator in den Einstellungen der Endpunkte der VPN-Verbindung.

Im zweiten Schritt vereinbaren die Endpunkte der VPN-Verbindung die Schlüssel zur Codierung und Decodierung der Daten.

6.5.3 Anwendungsbeispiele

Die folgenden Beispiele berücksichtigen die Besonderheiten von häufig vorkommenden Anwendungsfällen.

■ Zwei Subnetze miteinander verbinden

In einem großen Firmennetz seien die Subnetze über ein Transfernetz miteinander verbunden. Zwei dieser Subnetze, z.B. die Fertigungssteuerung und die Produktionshalle, sind über ein VPN zu verbinden. Da die internen IP-Adressen versteckt bleiben sollen, ist das VPN im Tunnelmodus zu betreiben.

Bekannt sind:

Parameter	Firewall Nummer 1	Firewall Nummer 2
IP-Adresse interner Port	10.0.1.201	10.0.3.201
IP-Adresse externer Port	10.0.2.1	10.0.2.2
Pre-Shared-Key	123456abcdef	123456abcdef
IKE - Modus, Starten als	Initiator	Responder
IP-Parameter der zu verbindenden Netze	10.0.1.0/24	10.0.3.0/24

Voraussetzungen für die weitere Konfiguration:

- ▶ Beide Firewalls sind im Router-Modus.
- ▶ Die IP-Parameter der Firewall-Router-Interface sind konfiguriert.
- ▶ Die Geräte im internen Netz haben als Gateway die IP-Adresse des internen Interfaces (Port 1) der Firewall.

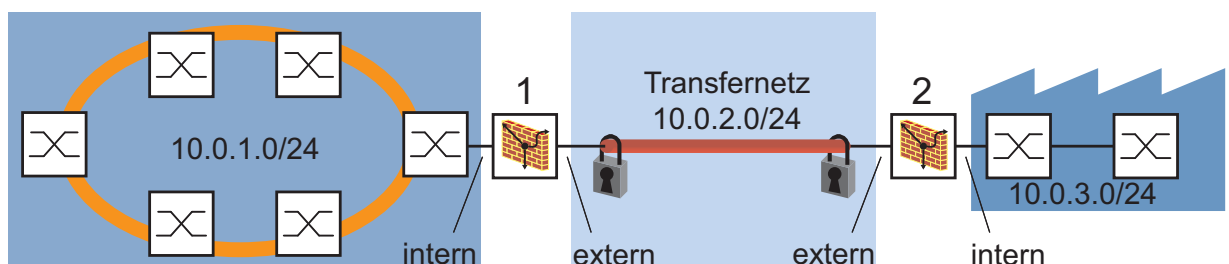


Abb. 38: Zwei Subnetze über ein Transfernetz miteinander verbinden

- ☐ Legen Sie eine neue VPN-Verbindung an.

- ☐ Wählen Sie den Dialog
Virtuelles privates Netz:Verbindungen.
- ☐ Klicken Sie auf „Eintrag erzeugen“.
Der Dialog zum Bearbeiten der Einträge bietet Ihnen in der Karteikarte Grundeinstellungen die Möglichkeit, dieser Verbindung einen beliebigen Namen zu geben.
- ☐ Geben Sie der Verbindung einen Namen, z.B.
„Fertigungssteuerung-Produktionshalle 1“.

Die Firewall bietet Ihnen die Möglichkeit, eine Verbindung ferngesteuert zu aktivieren/deaktivieren. Im Kommando zum ferngesteuerten Aktivieren/Deaktivieren geben Sie den Namen der Verbindung als Parameter ein. Das Kommando lautet:

```
https://vpn-user:passwort@host/nph-vpn.cgi?name=verbindung&cmd=(up|down)
```

Beispiel:

```
https://vpn:helen25miller@10.0.2.1/nph-vpn.cgi?name=Fertigungssteuerung-Produktionshalle&cmd=up
```

Abhängig von Ihrem Browser können Sie alternativ die Syntax ohne vpn-user:passwort@ wählen und den VPN-User mit dem Passwort im Dialog eingeben.

- ☐ Geben Sie die Authentisierungsparameter ein.

- ☐ Wählen Sie die Karteikarte Authentisierung.
- ☐ Geben Sie im Rahmen Schlüsselinformation ein:
 - ▶ „Methode“ psk
 - ▶ „Pre-Shared-Key“, z.B. 123456abcdef
- ☐ Geben Sie im Rahmen Identitäten ein:
 - ▶ „Lokaler Typ“ ipaddr
Hiermit legen Sie fest, dass der Eintrag in „Lokale ID“ eine IP-Adresse ist.
 - ▶ „Lokale ID“, z.B. 10.0.2.1 Wert zur Identifikation (im Rahmen der Authentisierung) auf der gegenüberliegenden Seite
 - ▶ „Entfernter Typ“ ipaddr
Hiermit legen Sie fest, dass die entfernte IP-Adresse ein Teil der Identifikation ist.
 - ▶ „Entfernte ID“, z.B. 10.0.2.2

- ☐ Geben Sie die IKE-Schlüsselaustauschparameter ein.

- ☐ Wählen Sie die Karteikarte **IKE - Schlüssel-Austausch**.
 - ☐ Geben Sie im Rahmen **Modus** ein:
 - ▶ „Protokoll“ **auto**
Hiermit wählt die Firewall die Protokollversion in Abhängigkeit der VPN-Gegenstelle automatisch aus.
 - ▶ „Starten als“, **initiator**
Hiermit initiiert diese Firewall die VPN-Verbindung zur Gegenstelle.
 - ▶ „DPD-Zeitbegrenzung“, **120**
Hiermit beendet die Firewall die VPN-Verbindung, wenn sie innerhalb von 120 Sekunden kein Lebenszeichen von der Gegenstelle erhält.
 - ▶ „Lebenszeit“, **28800**
Nach dem Ablauf dieser Lebenszeit handeln die beiden beteiligten Firewalls neue Schlüssel für die IKE-Sicherheitsbeziehung (IKE-SA) aus. Die Lebenszeit dient dem periodischen Schlüsselwechsel für die IKE-SA.
 - ▶ „Kompatibilitätsmodus“, **Aus**
 - ☐ Geben Sie im Rahmen **Algorithmen** ein, welche Verschlüsselungs-Verfahren Sie für die verschiedenen Anwendungen wünschen:
 - ▶ „Schlüsselvereinbarung“ **modp1024**
 - ▶ „Hash“, z.B. **md5**
 - ▶ „Integrität“ **hmacsha1**
 - ▶ „Verschlüsselung“ **aes128**
 - ☐ Geben Sie im Rahmen **Endpunkte (Peers)** ein:
 - ▶ „Lokale IP-Adresse“ **10.0.2.1**
 - ▶ „Entfernte IP-Adresse“ **10.0.2.2**
- Im vorliegenden Beispiel bilden die externen Ports der beiden Firewalls die Endpunkte der VPN-Verbindung.

- ☐ Geben Sie die IPsec-Datenaustauschparameter ein.

- ☐ Wählen Sie die Karteikarte **IPsec - Daten-Austausch**.
- ☐ Geben Sie im Rahmen **Modus** ein:
 - ▶ „Betriebsart (Encapsulation)“ **tunnel**
Hiermit verschlüsselt die Firewall das gesamte Datenpaket inklusive der IP-Adressen der Kommunikationspartner.
 - ▶ „NAT-T erzwingen“ **nein**.
 - ▶ „Lebenszeit“ **3600**.
- ☐ Geben Sie im Rahmen **Algorithmen** ein:
 - ▶ „Schlüssel-Vereinbarung“ **modp1024**
 - ▶ „Integrität“ **hmacsha1**
 - ▶ „Verschlüsselung“ **aes128**
- ☐ Geben Sie die Parameter für die IP-Netze, deren Daten über die VPN-Verbindung übertragen werden sollen, ein.

- ☐ Wählen Sie die Karteikarte **IP-Netze**.
- ☐ Klicken Sie auf **Eintrag erzeugen**.

- ☐ Nach einem Doppelklick in eine Zelle des Eintrags können Sie die Zelle bearbeiten:
 - ▶ „Quelladresse (CIDR)“ 10.0.1.0/24
 - ▶ „Quellport“ any
 - ▶ „Zieladresse“ 10.0.3.0/24
 - ▶ „Zielport“ any
 - ▶ „Protokoll“ any
 - ▶ „Beschreibung“ freier Datenverkehr zwischen den beiden Netzen Fertigungssteuerung und Produktionshalle
 - ▶ „Aktiv“ ein
- ☐ Um die Änderungen flüchtig zu speichern, klicken Sie „Schreiben“.

☐ Aktivieren Sie die Verbindung.

- ☐ Klicken Sie auf „Zurück“, um zu der Verbindungsübersicht zurück zu gelangen.
- ☐ Wählen Sie im Eintrag der Verbindung `Aktiv`, um die Verbindung zu aktivieren.
- ☐ Um die Änderungen flüchtig zu speichern, klicken Sie „Schreiben“.

☐ Speichern Sie die Einstellungen in den nicht-flüchtigen Speicher.

- ☐ Öffnen Sie hierzu den Dialog `Grundeinstellungen:Laden/Speichern`.
- ☐ Klicken Sie auf „Speichern in NVM + ACA“, um die Daten nicht-flüchtig zu speichern.

☐ Führen Sie exakt die gleichen Einstellungen auf beiden Firewalls aus. Tauschen Sie lediglich an der zweiten Firewall in den Einstellungen für die Authentisierung, den IKE-Schlüssel-Austausch und die IP-Netze die IP-Adressen für die Endpunkte bzw. Netze.

■ Mehrere Subnetze über ein gemeinsames Netz miteinander verbinden (Hub-and-Spoke-Architektur)

Eine neu gegründete Abteilung in der 2. Produktionshalle führt Servicearbeiten nicht nur lokal, sondern auch für die 1. Produktionshalle durch. Dabei greifen Geräte über die bestehende VPN-Verbindung auch auf das 1. Produktionsnetz zu. Zur Realisierung wählt der Administrator die Architektur „Hub and Spoke“, da sich diese einfach einrichten lässt und keine zusätzliche Hardware erfordert.

Die Firewall 1 in der Fertigungssteuerung übernimmt dabei die Funktion des Zentralknotens („Hub“). Die VPN-Verbindungen übernehmen die Funktion der „Speichen“ („Spokes“).

Arbeitet die Firewall als Hub, sendet sie die gerouteten Pakete am selben Interface wieder aus, an dem sie sie empfangen hat. Das heißt auch „Hub-and-Spoke-Routing“.

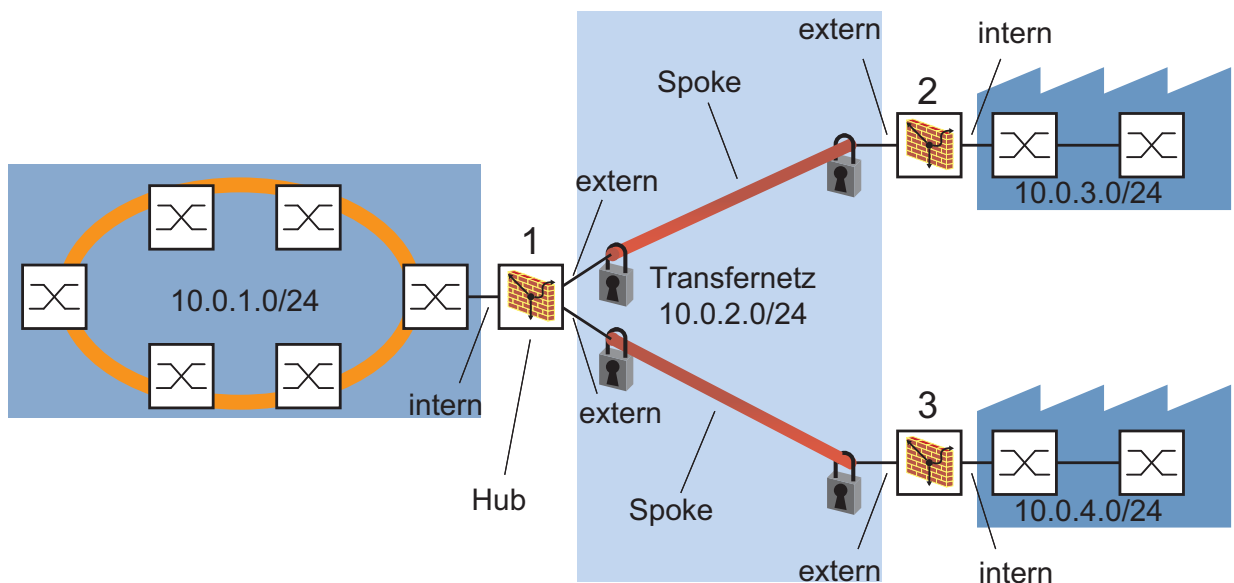


Abb. 39: Mehrere Subnetze über ein gemeinsames Netz miteinander verbinden (Hub-and-Spoke-Routing)

Bekannt sind:

Parameter	Firewall 1	Firewall 2	Firewall 3
IP-Adresse interner Port	10.0.1.201	10.0.3.201	10.0.4.201
IP-Adresse externer Port	10.0.2.1	10.0.2.2	10.0.2.3
Pre-Shared-Key	456789defghi	456789defghi	456789defghi
IKE - Modus, Starten als	Initiator	Responder	Responder
IP-Parameter der zu verbindenden Netze	10.0.1.0/24	10.0.3.0/24	10.0.4.0/24

Tab. 11: Interface-Einstellungen für „Hub-and-Spoke“ auf den beteiligten Firewalls

Für das Routing der Firewall 1 stellen Sie die IP-Netze für jede VPN-Verbindung im Dialog `VPN:Verbindungen` und dort in der Karteikarte `IP-Netze` nach der folgenden Tabelle ein:

VPN-Name	Index	Quelladresse (CIDR)	Zieladresse (CIDR)	Beschreibung
Fertigungssteuerung-Produktionshalle 1	1	10.0.1.0/24	10.0.3.0/24	FW 1 zu FW 2
	2	10.0.4.0/24	10.0.3.0/24	FW 3 zu FW 2
Fertigungssteuerung-Produktionshalle 2	1	10.0.1.0/24	10.0.4.0/24	FW 1 zu FW 3
	2	10.0.3.0/24	10.0.4.0/24	FW 2 zu FW 3

Tab. 12: VPN-Routing-Einstellungen für „Hub-and-Spoke“ auf der Hub-Firewall

Anmerkung: Die Zeilen mit dem Index 1 ermöglichen die Kommunikation des Subnetzes der Fertigungssteuerung (10.0.1.0/24) direkt mit Subnetzen der Produktionshallen 1 und 2 (10.0.3.0/24 bzw. 10.0.4.0/24).

Für das Routing der Firewalls 2 und 3 stellen Sie die IP-Netze für die VPN-Verbindungen im Dialog `VPN:Verbindungen` und dort in der Karteikarte `IP-Netze` nach der folgenden Tabelle ein:

Firewall-Nr.	Index	Quelladresse (CIDR)	Zieladresse (CIDR)	Beschreibung
2	1	10.0.3.0/24	10.0.1.0/24	FW 2 zu FW 1
2	2	10.0.3.0/24	10.0.4.0/24	FW 2 zu FW 3
3	1	10.0.4.0/24	10.0.1.0/24	FW 3 zu FW 1
3	2	10.0.4.0/24	10.0.3.0/24	FW 3 zu FW 2

Tab. 13: VPN-Routing-Einstellungen für „Hub and Spoke“ auf den Spoke-Firewalls

Voraussetzungen für die weitere Konfiguration:

- ▶ Die VPN-Parameter sind auf den 3 Geräten konfiguriert.
- ▶ Die IP-Parameter der Firewall-Router-Interface sind konfiguriert.

- ▶ Die Geräte im internen Netz haben als Gateway die IP-Adresse des internen Interfaces (Port 1) der jeweiligen Firewall.
- ▶ Die Firewalls haben die Software-Version 4.4 oder höher.

☐ Legen Sie auf der Firewall 1 das Routing für die Firewall 2 an.

☐ Wählen Sie den Dialog

`Virtuelles privates Netz:Verbindungen`.

☐ Wählen Sie die Verbindung mit dem Namen „Fertigungssteuerung-Produktionshalle 1“ aus und klicken Sie auf „Bearbeiten“.

☐ Wählen Sie die Karteikarte „IP-Netze“. Das Gerät zeigt eine leere Tabelle an.

☐ Klicken Sie auf „Eintrag erzeugen“, um eine neue Zeile zu erzeugen.

☐ Geben Sie in der 1. Zeile ein:

▶ „Quelladresse (CIDR)“, 10.0.1.0/24

▶ „Zieladresse (CIDR)“, 10.0.3.0/24

▶ „Beschreibung“, FW 1 zu FW 2

☐ Klicken Sie auf „Eintrag erzeugen“, um eine neue Zeile zu erzeugen.

☐ Geben Sie in der 2. Zeile ein:

▶ „Quelladresse (CIDR)“, 10.0.4.0/24

▶ „Zieladresse (CIDR)“, 10.0.3.0/24

▶ „Beschreibung“, FW 3 zu FW 2

☐ Klicken Sie auf „Schreiben“, um die Daten flüchtig zu speichern.

☐ Klicken Sie auf „Zurück“, um zum Dialog `Virtuelles privates Netz:Verbindungen` zurückzukehren.

☐ Legen Sie auf der Firewall 1 das Routing für die Firewall 3 an.

☐ Wählen Sie die Verbindung mit dem Namen „Fertigungssteuerung-Produktionshalle 2“ aus und klicken Sie auf „Bearbeiten“.

☐ Wählen Sie die Karteikarte „IP-Netze“. Das Gerät zeigt eine leere Tabelle an.

☐ Klicken Sie auf „Eintrag erzeugen“, um eine neue Zeile zu erzeugen.

☐ Geben Sie in der 1. Zeile ein:

▶ „Quelladresse (CIDR)“, 10.0.1.0/24

▶ „Zieladresse (CIDR)“, 10.0.4.0/24

▶ „Beschreibung“, FW 1 zu FW 3

☐ Klicken Sie auf „Eintrag erzeugen“, um eine neue Zeile zu erzeugen.

☐ Geben Sie in der 2. Zeile ein:

▶ „Quelladresse (CIDR)“, 10.0.3.0/24

▶ „Zieladresse (CIDR)“, 10.0.4.0/24

▶ „Beschreibung“, FW 2 zu FW 3

☐ Klicken Sie auf „Schreiben“, um die Daten flüchtig zu speichern.

- ☐ Klicken Sie auf „Zurück“, um zum Dialog `Virtuelles privates Netz:Verbindungen` zurückzukehren.

- ☐ Speichern Sie Ihre Einstellungen.

- ☐ Klicken Sie auf „Schreiben“, um die Daten flüchtig zu speichern.
- ☐ Öffnen Sie hierzu den Dialog `Grundeinstellungen:Laden/Speichern`.
- ☐ Klicken Sie auf „Speichern in NVM + ACA“, um die Daten nicht-flüchtig zu speichern.

- ☐ Legen Sie das Routing auf der Firewall 2 an.

- ☐ Wählen Sie den Dialog `Virtuelles privates Netz:Verbindungen`.
- ☐ Wählen Sie die Verbindung mit dem Namen „Fertigungssteuerungs-Produktionshalle 1“ aus und klicken Sie auf „Bearbeiten“.
- ☐ Wählen Sie die Karteikarte „IP-Netze“. Das Gerät zeigt eine leere Tabelle an.
- ☐ Klicken Sie auf „Eintrag erzeugen“, um eine neue Zeile zu erzeugen.
- ☐ Geben Sie in der 1. Zeile ein:
 - ▶ „Quelladresse (CIDR)“, 10.0.3.0/24
 - ▶ „Zieladresse (CIDR)“, 10.0.1.0/24
 - ▶ „Beschreibung“, FW 2 zu FW 1
- ☐ Klicken Sie auf „Eintrag erzeugen“, um eine neue Zeile zu erzeugen.
- ☐ Geben Sie in der 2. Zeile ein:
 - ▶ „Quelladresse (CIDR)“, 10.0.3.0/24
 - ▶ „Zieladresse (CIDR)“, 10.0.4.0/24
 - ▶ „Beschreibung“, FW 2 zu FW 3
- ☐ Klicken Sie auf „Schreiben“, um die Routing- und Mapping-Daten flüchtig zu speichern.
- ☐ Klicken Sie auf „Zurück“, um zum Dialog `Virtuelles privates Netz:Verbindungen` zurückzukehren.
- ☐ Klicken Sie auf „Schreiben“, um die Daten flüchtig zu speichern.
- ☐ Öffnen Sie hierzu den Dialog `Grundeinstellungen:Laden/Speichern`.
- ☐ Klicken Sie auf „Speichern in NVM + ACA“, um die Daten nicht-flüchtig zu speichern.

- ☐ Legen Sie das Routing auf der Firewall 3 an.

- ☐ Wählen Sie den Dialog
Virtuelles privates Netz:Verbindungen.
- ☐ Wählen Sie die Verbindung mit dem Namen „Fertigungssteuerung-Produktionshalle 2“ aus und klicken Sie auf „Bearbeiten“.
- ☐ Wählen Sie die Karteikarte „IP-Netze“. Das Gerät zeigt eine leere Tabelle an.
- ☐ Klicken Sie auf „Eintrag erzeugen“, um eine neue Zeile zu erzeugen.
- ☐ Geben Sie in der 1. Zeile ein:
 - ▶ „Quelladresse (CIDR)“, 10.0.4.0/24
 - ▶ „Zieladresse (CIDR)“, 10.0.1.0/24
 - ▶ „Beschreibung“, FW 3 zu FW 1
- ☐ Klicken Sie auf „Eintrag erzeugen“, um eine neue Zeile zu erzeugen.
- ☐ Geben Sie in der 2. Zeile ein:
 - ▶ „Quelladresse (CIDR)“, 10.0.4.0/24
 - ▶ „Zieladresse (CIDR)“, 10.0.3.0/24
 - ▶ „Beschreibung“, FW 3 zu FW 2
- ☐ Klicken Sie auf „Schreiben“, um die Routing- und Mapping-Daten flüchtig zu speichern.
- ☐ Klicken Sie auf „Zurück“, um zum Dialog Virtuelles privates Netz:Verbindungen zurückzukehren.
- ☐ Klicken Sie auf „Schreiben“, um die Daten flüchtig zu speichern.
- ☐ Öffnen Sie hierzu den Dialog Grundeinstellungen:Laden/Speichern.
- ☐ Klicken Sie auf „Speichern in NVM + ACA“, um die Daten nicht-flüchtig zu speichern.

■ Hirschmann-Adress-Mapping

Das Hirschmann-Adress-Mapping ermöglicht Ihnen den Aufbau von beliebig vielen Netzen mit identischen IP-Adressbereichen, die per VPN mit einem gemeinsamen Netz verbunden sind und von dem gemeinsamen Netz aus eindeutig unterscheidbar sind. Die Vorteile sind:

- ▶ Die identischen Adressbereiche der einzelnen Netze vereinfachen die Portierung der Konfiguration.
- ▶ Die Unterscheidbarkeit von dem gemeinsamen Netz aus ermöglicht die eindeutige Administration.

Das Hirschmann-Adress-Mapping können Sie z.B. einsetzen, um mehrere Produktionszellen zentral zu administrieren.

Die Firewall bietet mit dem Hirschmann-Adress-Mapping die Möglichkeit, bei der VPN-Anbindung die internen IP-Adressen durch extern gültige und eindeutige IP-Adressen zu ersetzen. Das Hirschmann-Adress-Mapping arbeitet wie ein in die VPN-Verbindung integrierter 1:1-NAT-Router. Ausgehende Datenpakete aus einem definierbaren Adress-Bereich versieht die Firewall dabei mit einer neuen Absende-Adresse - die Firewall mappt somit die interne Absende-Adresse auf eine extern gültige. Eingehende Datenpakete an diese gemappten Adressen versieht die Firewall automatisch mit der intern gültigen Ziel-Adresse. Diese Zuordnung ist umkehrbar eindeutig.

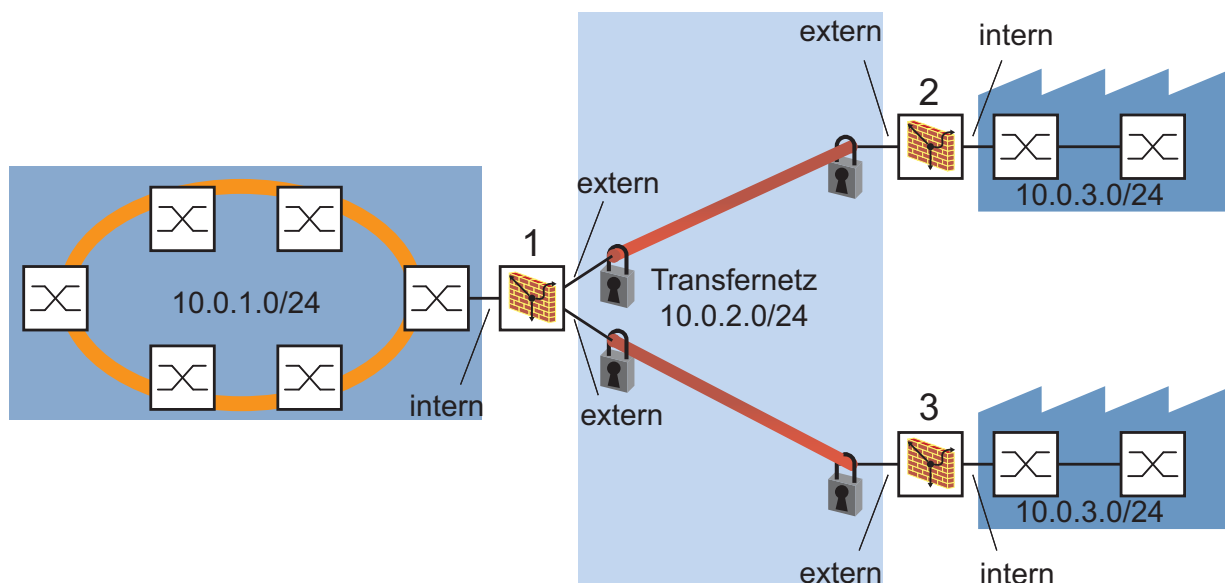


Abb. 40: Mehrere identische Subnetze von einem gemeinsamen Netz aus adressieren (Hirschmann-Adress-Mapping)

Bekannt sind:

Parameter	Firewall 1	Firewall 2	Firewall 3
IP-Adresse interner Port	10.0.1.201	10.0.3.201	10.0.3.201
IP-Adresse externer Port	10.0.2.1	10.0.2.2	10.0.2.3
Pre-Shared-Key	456789defghi	456789defghi	456789defghi
IKE - Modus, Starten als	Initiator	Responder	Responder
IP-Parameter der zu verbindenden Netze	10.0.1.0/24	10.0.3.0/24	10.0.3.0/24
Gemappte IP-Parameter der Netze	-	10.0.4.0/24	10.0.5.0/24

Tab. 14: Interface-Einstellungen für Hirschmann-Adress-Mapping auf den beteiligten Firewalls

Für das Routing der Firewall 1 stellen Sie die IP-Netze für jede VPN-Verbindung im Dialog **VPN:Verbindungen** und dort in der Karteikarte **IP-Netze** nach der folgenden Tabelle ein:

VPN-Name	Index	Quelladresse (CIDR)	Zieladresse (CIDR)	Beschreibung
Fertigungssteuerung-Produktionshalle 1	1	10.0.1.0/24	10.0.4.0/24	FW 1 zu FW 2
Fertigungssteuerung-Produktionshalle 2	1	10.0.1.0/24	10.0.5.0/24	FW 1 zu FW 3

Tab. 15: VPN-Routing-Einstellungen für Hirschmann-Adress-Mapping auf der Firewall der Fertigungssteuerung

Für das Adress-Mapping der Firewalls 2 und 3 stellen Sie die IP-Netze im Dialog **VPN:Verbindungen** und dort in der Karteikarte **IP-Netze** nach der folgenden Tabelle ein:

Firewall	Index	Quelladresse (CIDR)	Zieladresse (CIDR)	Gemappte Quelladresse (CIDR)	Beschreibung
2	1	10.0.3.0/24	10.0.1.0/24	10.0.4.0/24	FW 2 nach FW 1
3	1	10.0.3.0/24	10.0.1.0/24	10.0.5.0/24	FW 3 nach FW 1

Tab. 16: VPN-Routing-Einstellungen für Hirschmann-Adress-Mapping auf den Firewalls der Produktionsnetze

Anmerkung: In der Spalte „Mapping-Zieladresse (CIDR)“ ist kein Eintrag erforderlich.

Voraussetzungen für die weitere Konfiguration:

- ▶ Die VPN-Parameter sind auf den 3 Geräten konfiguriert.
- ▶ Die IP-Parameter der Firewall-Router-Interface sind konfiguriert.
- ▶ Die Geräte im internen Netz haben als Gateway die IP-Adresse des internen Interfaces (Port 1) der jeweiligen Firewall.

☐ Legen Sie auf der Firewall 1 das Routing für die Firewall 2 an.

☐ Wählen Sie den Dialog

`Virtuelles privates Netz:Verbindungen`.

☐ Wählen Sie die Verbindung mit dem Namen „Fertigungssteuerung-Produktionshalle 1“ aus und klicken Sie auf „Bearbeiten“.

☐ Wählen Sie die Karteikarte „IP-Netze“. Das Gerät zeigt eine leere Tabelle an.

☐ Klicken Sie auf „Eintrag erzeugen“, um eine neue Zeile zu erzeugen.

☐ Geben Sie in der 1. Zeile ein:

- ▶ „Quelladresse (CIDR)“, `10.0.1.0/24`
- ▶ „Zieladresse (CIDR)“, `10.0.4.0/24` (gemapptes Netz)
- ▶ „Beschreibung“, FW 1 zu FW 2

☐ Klicken Sie auf „Schreiben“, um die Daten flüchtig zu speichern.

☐ Klicken Sie auf „Zurück“, um zum Dialog `Virtuelles privates Netz:Verbindungen` zurückzukehren.

☐ Legen Sie auf der Firewall 1 das Routing für die Firewall 3 an.

☐ Wählen Sie die Verbindung mit dem Namen „Fertigungssteuerung-Produktionshalle 2“ aus und klicken Sie auf „Bearbeiten“.

☐ Wählen Sie die Karteikarte „IP-Netze“. Das Gerät zeigt eine leere Tabelle an.

☐ Klicken Sie auf „Eintrag erzeugen“, um eine neue Zeile zu erzeugen.

☐ Geben Sie in der 1. Zeile ein:

- ▶ „Quelladresse (CIDR)“, `10.0.1.0/24`
- ▶ „Zieladresse (CIDR)“, `10.0.5.0/24` (gemapptes Netz)
- ▶ „Beschreibung“, FW 1 zu FW 3

☐ Klicken Sie auf „Schreiben“, um die Daten flüchtig zu speichern.

☐ Klicken Sie auf „Zurück“, um zum Dialog `Virtuelles privates Netz:Verbindungen` zurückzukehren.

☐ Speichern Sie Ihre Einstellungen.

☐ Klicken Sie auf „Schreiben“, um die Daten flüchtig zu speichern.

- ☐ Öffnen Sie hierzu den Dialog `Grundeinstellungen:Laden/Speichern`.
- ☐ Klicken Sie auf „Speichern in NVM + ACA“, um die Daten nichtflüchtig zu speichern.
- ☐ Legen Sie das Adress-Mapping für die Firewall 2 an.
- ☐ Wählen Sie den Dialog `Virtuelles privates Netz:Verbindungen`.
- ☐ Wählen Sie die Verbindung mit dem Namen „Fertigungssteuerungs-Produktionshalle 1“ aus und klicken Sie auf „Bearbeiten“.
- ☐ Wählen Sie die Karteikarte „IP-Netze“. Das Gerät zeigt eine leere Tabelle an.
- ☐ Klicken Sie auf „Eintrag erzeugen“, um eine neue Zeile zu erzeugen.
- ☐ Geben Sie in der 2. Zeile ein:
 - ▶ „Quelladresse (CIDR)“, 10.0.3.0/24
 - ▶ „Zieladresse (CIDR)“, 10.0.1.0/24
 - ▶ „Mapping-Quelladresse (CIDR)“, 10.0.4.0/24
 - ▶ „Beschreibung“, FW 2 zu FW 1
- ☐ Klicken Sie auf „Schreiben“, um die Daten flüchtig zu speichern.
- ☐ Klicken Sie auf „Zurück“, um zum Dialog `Virtuelles privates Netz:Verbindungen` zurückzukehren.
- ☐ Klicken Sie auf „Schreiben“, um die Daten flüchtig zu speichern.
- ☐ Öffnen Sie hierzu den Dialog `Grundeinstellungen:Laden/Speichern`.
- ☐ Klicken Sie auf „Speichern in NVM + ACA“, um die Daten nichtflüchtig zu speichern.
- ☐ Legen Sie das Routing für die Firewall 3 an.
- ☐ Wählen Sie den Dialog `Virtuelles privates Netz:Verbindungen`.
- ☐ Wählen Sie die Verbindung mit dem Namen „Fertigungssteuerungs-Produktionshalle 2“ aus und klicken Sie auf „Bearbeiten“.
- ☐ Wählen Sie die Karteikarte „IP-Netze“. Das Gerät zeigt eine leere Tabelle an.
- ☐ Klicken Sie auf „Eintrag erzeugen“, um eine neue Zeile zu erzeugen.
- ☐ Geben Sie in der 2. Zeile ein:
 - ▶ „Quelladresse (CIDR)“, 10.0.3.0/24
 - ▶ „Zieladresse (CIDR)“, 10.0.1.0/24
 - ▶ „Mapping-Quelladresse (CIDR)“, 10.0.5.0/24
 - ▶ „Beschreibung“, FW 3 zu FW 1

- ☐ Klicken Sie auf „Schreiben“, um die Daten flüchtig zu speichern.
- ☐ Klicken Sie auf „Zurück“, um zum Dialog `Virtuelles privates Netz:Verbindungen` zurückzukehren.
- ☐ Klicken Sie auf „Schreiben“, um die Daten flüchtig zu speichern.
- ☐ Öffnen Sie hierzu den Dialog `Grundeinstellungen:Laden/Speichern`.
- ☐ Klicken Sie auf „Speichern in NVM + ACA“, um die Daten nicht-flüchtig zu speichern.

■ Einen PC mit einem Subnetz verbinden

Der Produktionsleiter möchte von zu Hause Einblick in die aktuellen Produktionsdaten haben. Zu diesem Zweck baut er eine VPN-Verbindung über einen DSL-Anschluss auf. Da sein DSL-Anschluss keine feste IP-Adresse hat, benutzt er DynDNS zur Ermittlung seiner IP-Adresse. Erhöhte Sicherheitsanforderungen legen die Verwendung von X.509-Schlüssel-Informationen nahe.

Parameter	Firewall Nummer 5	Firewall Nummer 6
IP-Adresse interner Port	10.0.1.202	10.0.3.202
IP-Adresse externer Port	10.149.112.92	DynDNS
Schlüssel-Information	PKCS#12-Datei	PKCS#12-Datei
IKE - Modus, Starten als	Initiator	Responder
IP-Parameter der zu verbindenden Netze	10.0.1.0/24	10.0.5.25/32

Voraussetzungen für die weitere Konfiguration:

- ▶ Beide Firewalls sind im PPPoE-Modus.
- ▶ Die Anmeldedaten für den DSL-Anbieter sind konfiguriert.
- ▶ Die IP-Parameter des internen Interfaces sind konfiguriert.
- ▶ Die Geräte im internen Netz haben als Gateway die IP-Adresse des internen Interfaces (Port 1) der Firewall.
- ▶ Sie verfügen über einen Account bei www.DynDNS.org.
- ▶ Die PKS#12-Dateien/Maschinenzertifikate mit den Schlüsselinformationen liegen von der gleichen Zertifizierungsstelle vor.



Abb. 41: Einen PC über ein öffentliches Netz mit einem Subnetz verbinden

- ☐ Konfigurieren Sie den DynDNS-Client auf dem EAGLE One Nr. 6. Zur Konfiguration des DynDNS benötigen Sie:
 - den Namen des DynDNS-Servers.
Bei DynDNS.org lautet der Hostname des HTTP-Servers für den DynDNS-Dienst „members.dyndns.org“.
 - den „Username“, von der Anmeldung bei DynDNS.org, z.B. „hugo“

- das „Password“, von der Anmeldung bei DynDNS.org
z.B. „oguh“
- den bei DynDNS.org registrierten „Hostname“, von der Anmeldung
bei DynDNS.org, z.B. „gerhardsFW.dyndns.org“

☐ Wählen Sie den Dialog

Erweitert:DNS:DynDNS.

☐ Aktivieren Sie „Registrieren“, damit der EAGLE One Nr. 6 dem DynDNS-Server seine aktuelle IP-Adresse mitteilt, sobald sich diese verändert.

☐ Geben Sie den Name des DynDNS-Server ein:

member.dyndns.org.

☐ Geben Sie in „Login“ Ihren DynDNS-Usernamen ein: hugo.

☐ Geben Sie in „Passwort“ Ihr DynDNS-Passwort ein: oguh.

☐ Geben Sie in „Hostname“ Ihren DynDNS-Hostnamen ein:

gerhardsFW.dyndns.org.

☐ Konfigurieren Sie den DNS-Server auf dem EAGLE One Nr. 5.

Zur Konfiguration des DynDNS benötigen Sie:

- den Namen des DynDNS-Servers.
Bei DynDNS.org lautet der Hostname des HTTP-Servers für den DynDNS-Dienst „members.dyndns.org“.
- den „Username“, von der Anmeldung bei DynDNS.org,
z.B. „hugo“
- das „Password“, von der Anmeldung bei DynDNS.org
z.B. „oguh“
- den bei DynDNS.org registrierten „Hostname“, von der Anmeldung
bei DynDNS.org, z.B. „gerhardsFW.dyndns.org“

☐ Wählen Sie den Dialog

Erweitert:DNS:DynDNS.

☐ Aktivieren Sie „Registrieren“, damit der EAGLE One Nr. 5 dem DynDNS-Server seine aktuelle IP-Adresse mitteilt, sobald sich diese verändert.

☐ Geben Sie den Name des DynDNS-Server ein:

member.dyndns.org.

☐ Geben Sie in „Login“ Ihren DynDNS-Usernamen ein: hugo.

☐ Geben Sie in „Passwort“ Ihr DynDNS-Passwort ein: oguh.

☐ Geben Sie in „Hostname“ Ihren DynDNS-Hostnamen ein:

gerhardsFW.dyndns.org.

- ☐ Legen Sie auf dem EAGLE One Nr. 5 eine neue VPN-Verbindung zum EAGLE One Nr.6 an.

- ☐ Wählen Sie den Dialog `Virtuelles privates Netz:Verbindungen`.
- ☐ Klicken Sie auf „Eintrag erzeugen“.
Der Dialog zum Bearbeiten der Einträge bietet Ihnen in der Karteikarte `Grundeinstellungen` die Möglichkeit, dieser Verbindung einen beliebigen Namen zu geben.
- ☐ Geben Sie der Verbindung einen Namen, z.B. „Home - Produktionshalle Nummer 3“.

- ☐ Geben Sie die Authentisierungsparameter ein.

- ☐ Wählen Sie die Karteikarte `Authentisierung`.
- ☐ Geben Sie im Rahmen `Schlüsselinformation` ein:
 - ▶ „Methode“ `x509rsa`
- ☐ Geben Sie im Rahmen `Identitäten` ein:
 - ▶ „Lokaler Typ“ `asn1dn`
Hiermit legen Sie fest, dass sich die lokale Firewall mit dem „Distinguished Name“ aus dem Zertifikat selbst identifiziert.
 - ▶ „Entfernter Typ“ `asn1dn`
Hiermit legen Sie fest, dass sich die entfernte Firewall mit dem „Distinguished Name“ aus dem Zertifikat selbst identifiziert.

- ☐ Geben Sie die Zertifikatsparameter ein.

- ☐ Wählen Sie die Karteikarte `Zertifikate`.
- ☐ Klicken Sie auf „PKCS#12-Datei vom PC laden“.
Der Dialog „Kopieren vom PC“ bietet Ihnen die Möglichkeit,
 - die PKCS#12-Datei auszuwählen,
 - das zum Zertifikat gehörige Passwort einzugeben und
 - mit einem Klick auf „Kopieren vom PC“ die PKCS#12-Datei auf die Firewall zu laden.Nach dem Laden der PKCS#12-Datei können Sie im Dialog die einzelnen Zertifikatsanteile sehen.

- ☐ Geben Sie die IKE-Schlüsselaustauschparameter ein.

- ☐ Wählen Sie die Karteikarte `IKE - Schlüssel-Austausch`.
- ☐ Geben Sie im Rahmen `Modus` ein:
 - ▶ „Protokoll“ `auto`
Hiermit wählt die Firewall die Protokollversion in Abhängigkeit der VPN-Gegenstelle automatisch aus.
 - ▶ „Starten als“, `initiator`
Hiermit initiiert diese Firewall die VPN-Verbindung zur Gegenstelle.
 - ▶ „DPD-Zeitbegrenzung“, `120`
Hiermit beendet die Firewall die VPN-Verbindung, wenn sie innerhalb von 120 Sekunden kein Lebenszeichen von der Gegenstelle erhält.
 - ▶ „Lebenszeit“, `28800`
Nach dem Ablauf dieser Lebenszeit handeln die beiden beteiligten Firewalls neue Schlüssel für die IKE-Sicherheitsbeziehung (IKE-SA) aus. Die Lebenszeit dient dem periodischen Schlüsselwechsel für die IKE-SA.
 - ▶ „Kompatibilitätsmodus“, `Aus`
- ☐ Geben Sie im Rahmen `Algorithmen` ein, welche Verschlüsselungs-Verfahren Sie für die verschiedenen Anwendungen wünschen:
 - ▶ „Schlüsselvereinbarung“ `modp1024`
 - ▶ „Hash“, z.B. `md5`
 - ▶ „Integrität“ `hmacsha1`
 - ▶ „Verschlüsselung“ `aes128`
- ☐ Geben Sie im Rahmen `Endpunkte (Peers)` ein:
 - ▶ „Lokale IP-Adresse“ `10.149.112.92`
 - ▶ „Entfernte IP-Adresse“ `gerhardsFW.dyndns.org`

Im vorliegenden Beispiel bilden die externen Ports der beiden Firewalls die Endpunkte der VPN-Verbindung. Während die lokale IP-Adresse bekannt ist, unterliegt die entfernte IP-Adresse Änderungen durch den DSL-Provider. In diesem Fall ermittelt die Firewall die entfernte IP-Adresse mittels DynDNS.

- ☐ Geben Sie die Parameter für die IP-Netze, deren Daten über die VPN-Verbindung übertragen werden sollen, ein.

- ☐ Wählen Sie die Karteikarte `IP-Netze`.
- ☐ Klicken Sie auf `Eintrag erzeugen`.
- ☐ Nach einem Doppelklick in eine Zelle des Eintrags können Sie die Zelle bearbeiten:
 - ▶ „Quelladresse (CIDR)“ `10.0.1.0/24`
 - ▶ „Quellport“ `any`
 - ▶ „Zieladresse“ `gerhardsFW.dyndns.org`
 - ▶ „Zielport“ `any`
 - ▶ „Protokoll“ `any`
 - ▶ „Beschreibung“ `freier Datenverkehr zwischen Home und Produktionshalle`
 - ▶ „Aktiv“ `ein`
- ☐ Um die Änderungen flüchtig zu speichern, klicken Sie `„Schreiben“`.

☐ Speichern Sie die Einstellungen in den nicht-flüchtigen Speicher.

☐ Öffnen Sie hierzu den Dialog Grundeinstellungen:Laden/Speichern.

☐ Klicken Sie auf „Speichern in NVM + ACA“, um die Daten nicht-flüchtig zu speichern.

☐ Führen Sie exakt die gleichen Einstellungen auf beiden Firewalls aus. Tauschen Sie lediglich an der zweiten Firewall in den Einstellungen für die Authentisierung, den IKE-Schlüssel-Austausch und die IP-Netze die IP-Adressen für die Endpunkte bzw. Netze.

■ Einen LANCOM Advanced VPN-Client mit einem privaten Netz verbinden

In diesem Fall möchte ein Produktionsleiter von einem beliebigen Standort innerhalb der Firma über eine VPN-Verbindung auf seine Produktionsdaten zugreifen. Hierzu benutzt er ein Notebook mit installierter LANCOM-Client-Software. So kann er die VPN-Verbindung direkt zwischen seinem Notebook und dem EAGLE One aufbauen.

Parameter	Firewall	LANCOM-Client
IP-Adresse interner Port	10.0.1.201	
IP-Adresse externer Port	10.0.2.1	
Pre-Shared-Key	123456abcdef	123456abcdef
IKE - Modus, Starten als	Responder	Initiator
IP-Parameter der zu verbindenden Netze	10.0.1.0/24	10.0.2.92/32

Voraussetzungen für die weitere Konfiguration:

- ▶ Die Firewall ist im Router-Modus.
- ▶ Die IP-Parameter der Firewall-Router-Interface sind konfiguriert.
- ▶ Die Geräte im internen Netz haben als Gateway die IP-Adresse des internen Interfaces (Port 1) der Firewall.

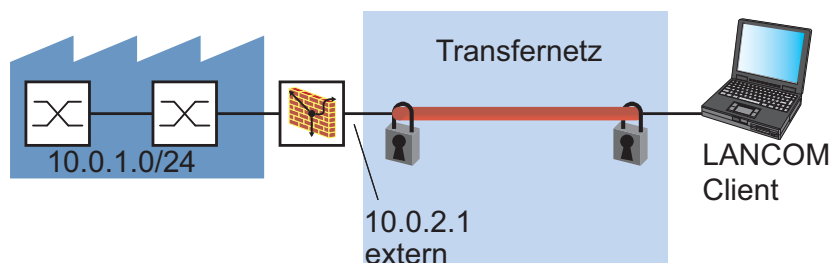


Abb. 42: Einen LANCOM-Client über ein öffentliches Netz mit einem privaten Netz verbinden

Einstellungen am EAGLE One:

- ☐ Legen Sie eine neue VPN-Verbindung an.

- ☐ Wählen Sie den Dialog

Virtuelles privates Netz:Verbindungen.

- ☐ Klicken Sie auf „Eintrag erzeugen“.

Der Dialog zum Bearbeiten der Einträge bietet Ihnen in der Karteikarte Grundeinstellungen die Möglichkeit, dieser Verbindung einen beliebigen Namen zu geben.

- ☐ Geben Sie der Verbindung einen Namen, z.B. „FertigungsLeitung-Produktionshalle“.

- ☐ Geben Sie die Authentisierungsparameter ein.

- ☐ Wählen Sie die Karteikarte Authentisierung.

- ☐ Geben Sie im Rahmen Schlüsselinformation ein:

- ▶ „Methode“ `psk`
- ▶ „Pre-Shared-Key“, z.B. `123456abcdef`

- ☐ Geben Sie im Rahmen Identitäten ein:

- ▶ „Lokaler Typ“ `default`
- ▶ „Entfernter Typ“ `fqdn`
Hiermit legen Sie fest, dass die entfernte Schlüssel-Identifikation ein Teil der Identifikation ist.
- ▶ „Entfernte ID“, z.B. `www.beldensolutions.com`

- ☐ Geben Sie die IKE-Schlüsselaustauschparameter ein.

- ☐ Wählen Sie die Karteikarte IKE – Schlüssel-Austausch.

- ☐ Geben Sie im Rahmen Modus ein:

- ▶ „Protokoll“ `auto`
Hiermit wählt die Firewall die Protokollversion in Abhängigkeit der VPN-Gegenstelle automatisch aus.
- ▶ „Starten als“, `responder`
Hiermit antwortet diese Firewall auf die Anfrage zum VPN-Verbindungsaufbau der Gegenstelle.
- ▶ „DPD-Zeitbegrenzung“, `120`
Hiermit beendet die Firewall die VPN-Verbindung, wenn sie innerhalb von 120 Sekunden kein Lebenszeichen von der Gegenstelle erhält.
- ▶ „Lebenszeit“, `28800`
Nach dem Ablauf dieser Lebenszeit handeln die beiden beteiligten Firewalls neue Schlüssel für die IKE-Sicherheitsbeziehung (IKE-SA) aus. Die Lebenszeit dient dem periodischen Schlüsselwechsel für die IKE-SA.
- ▶ „Kompatibilitätsmodus“, `Aus`

- ☐ Geben Sie im Rahmen Algorithmen ein, welche Verschlüsselungs-Verfahren Sie für die verschiedenen Anwendungen wünschen:

- ▶ „Schlüsselvereinbarung“ `modp1024`
- ▶ „Hash“, z.B. `md5`
- ▶ „Integrität“ `hmacmd5`
- ▶ „Verschlüsselung“ `aes128`

- ☐ Geben Sie im Rahmen Endpunkte (Peers) ein:

- ▶ „Lokale IP-Adresse“ `10.0.2.1`
- ▶ „Entfernte IP-Adresse“ `10.0.2.92`

Im vorliegenden Beispiel bildet der externen Port der Firewall und das Ethernet-Interface des LANCOM-Clients die Endpunkte der VPN-Verbindung.

☐ Geben Sie die IPsec-Datenaustauschparameter ein.

☐ Wählen Sie die Karteikarte `IPsec - Daten-Austausch`.

☐ Geben Sie im Rahmen `Modus` ein.

- ▶ „Betriebsart (Encapsulation)“ `tunnel`
Hiermit verschlüsselt die Firewall das gesamte Datenpaket inklusive der IP-Adressen der Kommunikationspartner.
- ▶ „NAT-T erzwingen“ `nein`.
- ▶ „Lebenszeit“ `3600`.

☐ Geben Sie im Rahmen `Algorithmen` ein:

- ▶ „Schlüssel-Vereinbarung“ `modp1024`
- ▶ „Integrität“ `hmacmd5`
- ▶ „Verschlüsselung“ `aes128`

☐ Geben Sie die Parameter für die IP-Netze, deren Daten über die VPN-Verbindung übertragen werden sollen, ein.

☐ Wählen Sie die Karteikarte `IP-Netze`.

☐ Klicken Sie auf `Eintrag erzeugen`.

☐ Nach einem Doppelklick in eine Zelle des Eintrags können Sie die Zelle bearbeiten:

- ▶ „Quelladresse (CIDR)“ `10.0.1.0/24`
- ▶ „Quellport“ `any`
- ▶ „Zieladresse“ `10.0.2.92/32`
- ▶ „Zielport“ `any`
- ▶ „Protokoll“ `any`
- ▶ „Beschreibung“ `freier Datenverkehr zwischen Fertigungsleitung und Produktionshalle`
- ▶ „Aktiv“ `ein`

☐ Um die Änderungen flüchtig zu speichern, klicken Sie `„Schreiben“`.

☐ Speichern Sie die Einstellungen in den nicht-flüchtigen Speicher.

☐ Öffnen Sie hierzu den Dialog `Grundeinstellungen:Laden/Speichern`.

☐ Klicken Sie auf `„Speichern in NVM + ACA“`, um die Daten nicht-flüchtig zu speichern.

Einstellungen am Notebook mit dem LANCOM Advanced VPN Client:

Voraussetzung: Die LANCOM Advanced VPN Client Software ist auf dem Notebook installiert.

☐ Starten Sie die LANCOM Client Software auf Ihrem PC.

☐ Erstellen Sie ein neues Profil mit

Konfiguration: Profil-Einstellungen.

☐ Klicken Sie auf „Neuer Eintrag“.

Ein Assistent führt Sie durch die Konfiguration des neuen Profils.

☐ Wählen Sie als Verbindungstyp

„Verbindung zum Firmannetz über IPsec“.

Klicken Sie auf „Weiter“.

☐ Geben Sie einen Namen für das Profil ein.

Klicken Sie auf „Weiter“.

☐ Wählen Sie als Verbindungsmedium „LAN (over IP)“.

Klicken Sie auf „Weiter“.

☐ Geben Sie als Gateway-Adresse die IP-Adresse des externen Interfaces der Firewall, z.B. 10.0.2.1, ein.

Klicken Sie auf „Weiter“.

☐ Wählen Sie als Austausch-Modus „Main-Mode“.

Wählen Sie die PFS-Gruppe „DH-Group 2 (1024 Bit)“.

Klicken Sie auf „Weiter“.

☐ Geben Sie unter „Shared Secret“ den Pre-Shared-Key 123456abcdef ein.

Wiederholen Sie die Eingabe des Pre-Shared-Key.

Wählen Sie den lokalen Identitätstyp „Fully Qualified Domain Name“.

Geben Sie die lokale Identitäts-ID `www.beldensolutions.com` ein.

Klicken Sie auf „Weiter“.

☐ Wählen Sie für die IP-Adressen-Zuweisung die manuelle Vergabe

„Lokale IP-Adresse verwenden“.

Klicken Sie auf „Weiter“.

☐ Für die Auswahl des IP-Netzes zur Kommunikation klicken Sie auf „Neu“.

Geben Sie die IP-Adresse und die Netzmaske des Netzes in der Produktionshalle ein, z.B. 10.0.1.0 und 255.255.255.0.

Klicken Sie auf „OK“.

Klicken Sie auf „Fertigstellen“.

Hiermit beenden Sie den Assistenten zur Konfiguration des Profils.

☐ Markieren Sie das neue Profil und klicken Sie auf „Konfigurieren“.

☐ Klicken Sie im linken Feld auf „IPsec-Einstellungen“.

☐ Geben Sie unter „Richtlinie“ ein:

– „IKE-Richtlinie“: Pre-shared Key.

– „IPsec-Richtlinie“: ESP-AES128-MD5.

- ☐ Klicken Sie auf „Gültigkeit“.
- ☐ Tragen Sie im Rahmen „IPsec-Richtlinie“ unter „Dauer“ 000:01:00:00 ein.
Dieser Wert ist gleich der „Lebenszeit“ bei den EAGLE One-Einstellungen unter „IPsec - Daten-Austausch“.
- ☐ Klicken Sie auf „OK“, um das Eingabe-Fenster zu schließen.
- ☐ Klicken Sie auf „OK“, um die Profil-Einstellung zu beenden.
- ☐ Wählen Sie im LANCOM-Client-Hauptfenster das erstellte Profil aus und klicken Sie auf „Verbinden“, um die VPN-Verbindung zum EAGLE One aufzubauen.
Sollte der LANCOM-Client die Verbindung nicht aufbauen können, dann starten Sie den PC mit dem LANCOM-Client neu.
Klicken Sie nach dem Neustart auf „Verbinden“, um die VPN-Verbindung zum EAGLE One aufzubauen.

■ **VPN-Verbindung automatisch aktivieren und Aktivierung per VPN-LED anzeigen**

Das EAGLE One-Gerät bietet Ihnen die Funktion des Service-Modus. Im Service-Modus aktiviert das Gerät automatisch eine oder mehrere von Ihnen vorkonfigurierte VPN-Verbindungen in Abhängigkeit der ausgewählten Quelle für den Service-Modus:

- ▶ powersupply
Der Service-Modus startet, wenn die redundante Stromversorgung des Gerätes außer Funktion ist oder Sie die redundante Stromversorgung des Gerätes zu diesem Zweck ausschalten.
- ▶ digitalinput-low
Der Service-Modus startet, wenn am digitalen Eingang die Eingangsspannung Low-Pegel (Zustand „0“) anliegt.
- ▶ digitalinput-high
Der Service-Modus startet, wenn am digitalen Eingang die Eingangsspannung High-Pegel (Zustand „1“) anliegt.

- ☐ Legen Sie eine neue VPN-Verbindung an und konfigurieren Sie die Verbindung.

- ☐ Wählen Sie den Dialog
Virtuelles privates Netz:Verbindungen.
- ☐ Klicken Sie auf „Eintrag erzeugen“.
- ☐ Geben Sie im Feld „Name“ einen Namen für die Verbindung ein,
zum Beispiel Instandhaltung_Produktion.

- ☐ Kreuzen Sie das Feld „Service Mode“ an, um den Service-Modus für diese Verbindung zu aktivieren.
 - ☐ Kreuzen Sie das Feld „Aktiv“ an
 - ☐ Wählen Sie im Feld „Exchange Mode“ den Eintrag `mainaggressive`.
 - ☐ Klicken Sie auf „Schreiben“, um den Eintrag in der Konfiguration flüchtig zu speichern.
- ☐ Wiederholen Sie diese Schritte für weitere VPN-Verbindungen.

Das Feld „Status“ zeigt Ihnen den Zustand für jede VPN-Verbindung an. Bei aktiviertem Service-Modus lautet der Eintrag `up`.

Das EAGLE One-Gerät bietet Ihnen die Möglichkeit, die LED „VPN“ zur Anzeige von aktiven VPN-Verbindungen zu verwenden. Um diese Funktion zu aktivieren, gehen Sie wie folgt vor:

- ☐ Wählen Sie den Dialog `Virtuelles privates Netz:Verbindungen`.
- ☐ Kreuzen Sie das Feld „VPN-LED-Statusanzeige“ an.
- ☐ Klicken Sie auf „Schreiben“, um den Eintrag in der Konfiguration flüchtig zu speichern.

Die LED „VPN“ des EAGLE One-Gerätes leuchtet grün, wenn eine oder mehrere VPN-Verbindungen aktiv und im Zustand `up` sind.

7 Redundanz einrichten

Die Redundanzfunktion der Firewall bietet Ihnen die Möglichkeit, die Firewall und ihre Zuleitungen redundant auszuführen.

Ist eine Firewall oder eine Zuleitung zur Firewall außer Funktion, dann übernimmt die andere Firewall mit ihren Zuleitungen die Funktion der ersten Firewall.

Hierzu synchronisieren die beiden Firewalls laufend den Zustand der Stateful Firewall. So bleiben beim Wechsel von einer Firewall zur anderen bestehende Verbindungen erhalten.

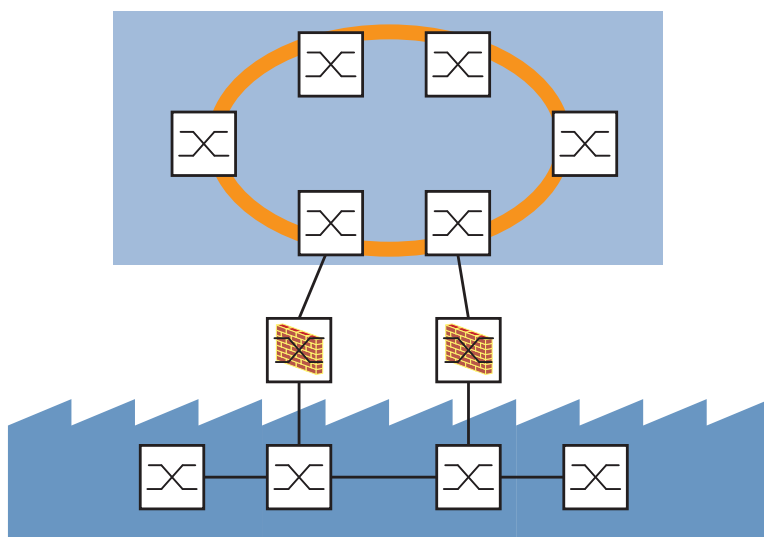


Abb. 43: Redundante Firewall-Verbindung

7.1 Transparent-Redundanz

7.1.1 Beschreibung der Transparent-Redundanz-Funktion

Im Netz-Transparent-Modus bietet Ihnen die Firewall die Möglichkeit, in die Pfade zweier redundant gekoppelter Netze jeweils eine Firewall zu schalten (siehe Anwender-Handbuch Redundanz-Konfiguration Ihres Hirschmann-Gerätes, das die redundante Kopplung unterstützt). Ist die Haupt-Verbindung außer Funktion, übernimmt die Ersatz-Firewall die Aufgaben der Haupt-Firewall.

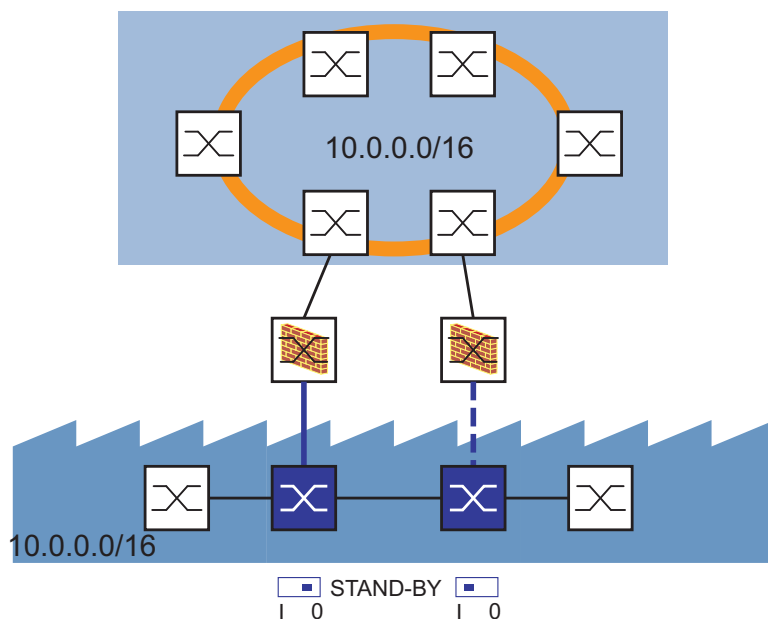


Abb. 44: Transparent-Redundanz

7.1.2 Anwendungsbeispiel für die Transparent-Redundanz

Die Transparent-Redundanz setzen Sie in einem flachen Netz ein.

Eine Fertigungszelle, die ständig aktuelle Produktionsdaten benötigt, haben Sie aus Gründen der Verfügbarkeit über eine redundante Kopplung an das Firmennetz angebunden.

Um die Sicherheit der Produktionszelle zu unterstützen, installieren Sie in jedem Pfad zum Firmennetz eine Firewall.

Bekannt sind:

Parameter	Firewall 1	Firewall 2
Eigene IP-Adresse	10.0.0.201/16	10.0.0.202/16
IP-Adresse des Redundanzpartners	10.0.0.202/16	10.0.0.201/16

Voraussetzungen für die weitere Konfiguration:

- ▶ Die Firewall ist im Transparent-Modus.
- ▶ Die IP-Parameter im Transparent-Modus sind konfiguriert.

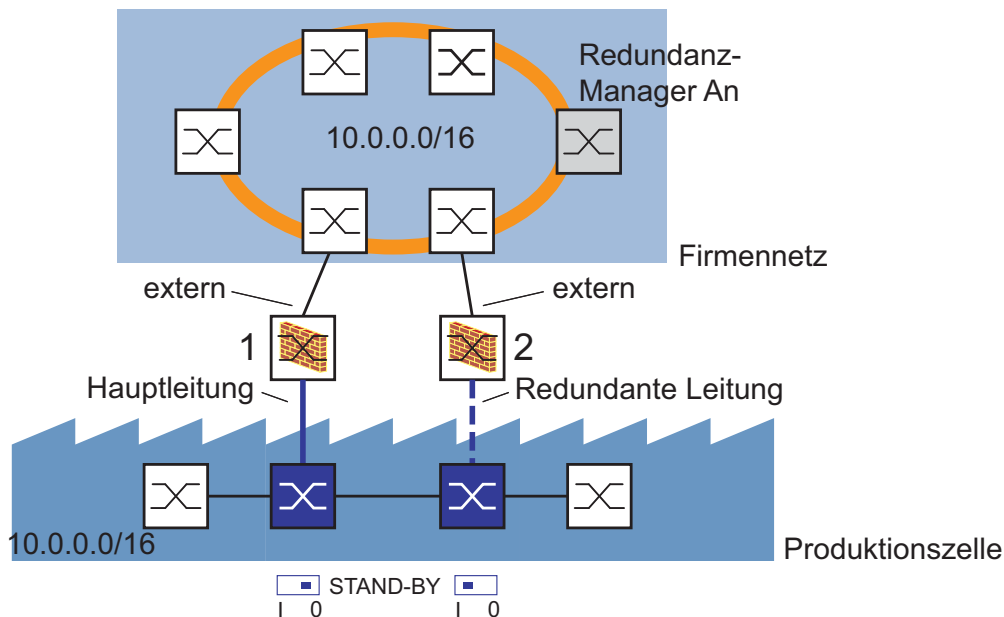


Abb. 45: Transparent-Redundanz Anwendungsbeispiel

- ☐ Konfigurieren Sie zunächst die Firewall Nummer 1.
Geben Sie die Parameter für die Transparent-Redundanz ein und schalten Sie die Funktion an.
- ☐ Wählen Sie den Dialog
Redundanz:Transparent.
- ☐ Klicken Sie im Rahmen „Konfiguration“ in der Zeile „Funktion“ auf An, um die Funktion einzuschalten.
- ☐ Wählen Sie im Rahmen „Transparent-Modus“ den Master- oder Slave-Port: `internal` (Hauptleitung).
- ☐ Geben Sie im Rahmen „Firewall-Zustandstabellen-Synchronisation“ die IP-Adresse des Redundanzpartners ein.
In diesem Fall ist das die IP-Adresse der Firewall Nummer 2:
`10.0.0.202`.
- ☐ Um die Änderungen flüchtig zu speichern, klicken Sie „Schreiben“.

☐ Speichern Sie die Einstellungen in den nicht-flüchtigen Speicher.

☐ Öffnen Sie hierzu den Dialog `Grundeinstellungen:Laden/Speichern`.

☐ Klicken Sie auf „Speichern in NVM + ACA“, um die Daten nicht-flüchtig zu speichern.

☐ Konfigurieren Sie anschließend die Firewall Nummer 2.
Geben Sie die Parameter für die Transparent-Redundanz ein und schalten Sie die Funktion an.

☐ Wählen Sie den Dialog
`Redundanz:Transparent`.

☐ Klicken Sie im Rahmen „Konfiguration“ in der Zeile „Funktion“ auf `An`, um die Funktion einzuschalten.

☐ Wählen Sie im Rahmen „Transparent-Modus“ den Master- oder Slave- Port: `internal` (Redundante Leitung).

☐ Geben Sie im Rahmen „Firewall-Zustandstabellen-Synchronisation“ die IP-Adresse des Redundanzpartners ein.
In diesem Fall ist das die IP-Adresse der Firewall Nummer 1:
`10.0.0.201`.

☐ Um die Änderungen flüchtig zu speichern, klicken Sie „Schreiben“.

☐ Speichern Sie die Einstellungen in den nicht-flüchtigen Speicher.

☐ Öffnen Sie hierzu den Dialog `Grundeinstellungen:Laden/Speichern`.



- ☐ Klicken Sie auf „Speichern in NVM + ACA“, um die Daten nicht-flüchtig zu speichern.

Anmerkung: Die grafische Benutzeroberfläche zeigt Ihnen im Dialogfenster `Redundanz:Transparent` im Anzeigefeld hinter `Kommunikation` den Layer 2-Status Ihrer Redundanzverbindung an:

- ▶ Hinter dem Parameter `Kommunikation` ist das Anzeigefeld `Aktiv` angekreuzt: Die Kommunikation über die Hauptleitung Ihrer Redundanz-Konfiguration aktiv.
- ▶ Hinter dem Parameter `Kommunikation` ist das Anzeigefeld `Inaktiv` angekreuzt: Momentan findet keine Kommunikation über die Hauptleitung Ihrer Redundanz-Konfiguration statt.
- ☐ Prüfen Sie, ob eventuell eine Datenleitung oder Netzkomponente in Ihrer Redundanz-Konfiguration außer Funktion ist. Prüfen Sie den Redundanzstatus über die Switches im Pfad der redundanten Ring-/Netzkopplung, in den Sie die Firewall eingebunden haben (siehe Anwender-Handbuch Redundanz-Konfiguration Ihres Hirschmann-Gerätes, das die redundante Kopplung unterstützt).

7.2 Router-Redundanz

7.2.1 Beschreibung der Router-Redundanz-Funktion

Im Router-Modus bietet Ihnen die Firewall die Möglichkeit, zu einer bestehenden Verbindung zweier Netze über eine Firewall eine redundante Leitung und eine redundante Firewall zu installieren.

Endgeräte bieten in der Regel die Möglichkeit, ein Default-Gateway für die Vermittlung von Datenpaketen in fremde Subnetze einzutragen. An dieser Stelle bezeichnet der Begriff „Gateway“ einen Router, über den das Endgerät in andere Subnetze kommunizieren kann.

Ist dieser Router außer Funktion, kann das Endgerät keine Daten mehr in fremde Subnetze senden.

In diesem Fall hilft die Router-Redundanz-Funktion der Firewall mit der virtuellen IP-Adresse. Diese Funktion bietet eine Gateway-Redundanz. Sie verwendet ein Verfahren, das 2 Router zu einem virtuellen Router zusammenfasst. Endgeräte adressieren den virtuellen Router und die Router-Redundanz-Funktion hilft sicherzustellen, dass ein physikalischer Router, der dem virtuellen Router angehört, die Vermittlung übernimmt.

Die beiden Firewalls tauschen ständig sowohl über das interne als auch über das externe Interface Informationen aus. Somit prüfen sie auch gleichzeitig ihre Erreichbarkeit.

Entdeckt die Firewall, die momentan die virtuelle Router-Rolle hat, eine Leitungs-Unterbrechung an einem ihrer Ports, informiert sie ihre Partner-Firewall, die darauf die virtuelle Router-Rolle übernimmt.

Zusätzlich bietet Ihnen die Firewall zur Überwachung von Leitungen im angeschlossenen Netzwerk die ICMP-Host-Check-Funktion.

Sobald eine Firewall die Verbindung zur anderen Firewall an einem Port verliert, senden beide Firewalls Ping-Anfragen an die in der ICMP-Host-Check-Tabelle eingetragenen IP-Adressen.

Nach der Auswertung der Ping-Antworten entscheiden die beiden Firewalls,

welche Firewall die aktive Vermittlungsfunktion übernimmt.

Das Eintragen von spezifischen IP-Adressen, z.B. von Servern, Routern, Controllern/PLC in die ICMP-Host-Check-Tabelle hilft Ihnen bei der Sicherstellung einer hohen Verfügbarkeit der Verbindung zu diesen Geräten im internen und externen Netz.

Ist die Haupt-Verbindung außer Funktion, übernimmt die redundante Firewall die Aufgaben der Haupt-Firewall.

Sie können die Router-Redundanz mit 1:1-NAT kombinieren. Sie erhalten damit einen hochverfügbaren 1:1-NAT-Router ([siehe auf Seite 145 „1:1-NAT“](#)).

Anmerkung: Bei 1:1-NAT antwortet die Firewall auf ARP-Anfragen aus dem externen Netz an Adressen, die sie aus dem internen Netz abbildet. Dies gilt auch, wenn im internen Netz kein Gerät mit der IP-Adresse existiert. Vergeben Sie daher im externen Netz an Geräte ausschließlich IP-Adressen, die außerhalb des Bereichs liegen, den 1:1-NAT vom internen in das externe Netz abbildet.

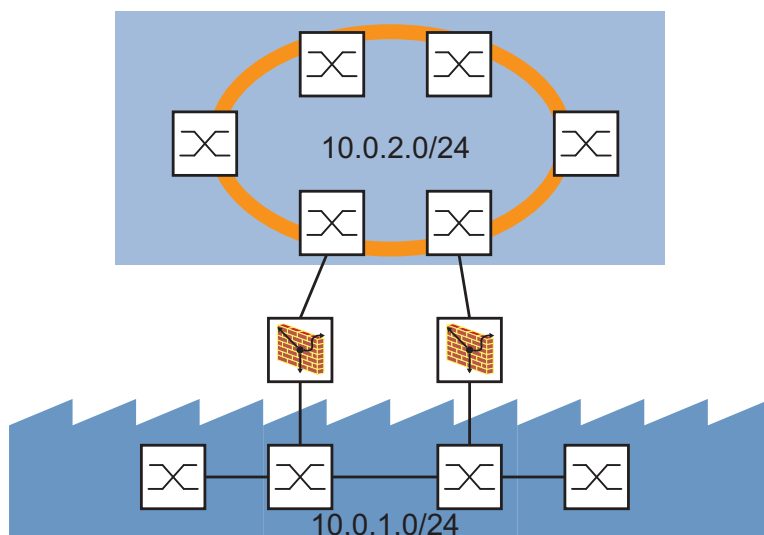


Abb. 46: Router-Redundanz

7.2.2 Anwendungsbeispiel für die Router-Redundanz

Die Router-Redundanz setzen Sie ein, wenn Sie die Firewall im Router-Modus betreiben.

Eine Fertigungszelle, die ständig aktuelle Produktionsdaten benötigt, haben Sie aus Gründen der Verfügbarkeit über eine redundante Leitung mit einer redundanten Firewall an das Firmennetz angebunden.

Bekannt sind:

Parameter	Firewall 1	Firewall 2
Priorität	100	90
Interne IP-Adresse	10.0.1.201/24	10.0.1.202/24
Virtuelle IP-Adresse (VR-IP) des internen Interface	10.0.1.200/24	10.0.1.200/24
Virtuelle Router-Identifikation (VRID) des internen Interface	1	1
IP-Adresse des Redundanzpartners (internes Interface)	10.0.1.202/24	10.0.1.201/24
Externe IP-Adresse	10.0.2.201/24	10.0.2.202/24
Virtuelle IP-Adresse (VR-IP) des externen Interface	10.0.2.200/24	10.0.2.200/24
Virtuelle Router-Identifikation (VRID) des externen Interface	2	2
IP-Adresse des Redundanzpartners (externes Interface)	10.0.2.202/24	10.0.2.201/24

Voraussetzungen für die weitere Konfiguration:

- ▶ Die Firewall ist im Router-Modus.
- ▶ Die IP-Parameter im Router-Modus sind konfiguriert.
- ▶ Die Geräte des internen Netzes (Produktionszelle) haben als Gateway die VR-IP-Adresse des internen Interfaces.
- ▶ Die Geräte des externen Netzes (Firmennetzes) haben als Gateway die VR-IP-Adresse des externen Interfaces.

Anmerkung: Achten Sie bei der Verwendung mehrerer redundanter Router in Ihrem Netz auf die Einmaligkeit der verwendeten VRIDs. Das hilft Ihnen bei der Vermeidung gegenseitiger, störender Einflüsse dieser virtuellen Router-Anwendungen, die VRRP verwenden.

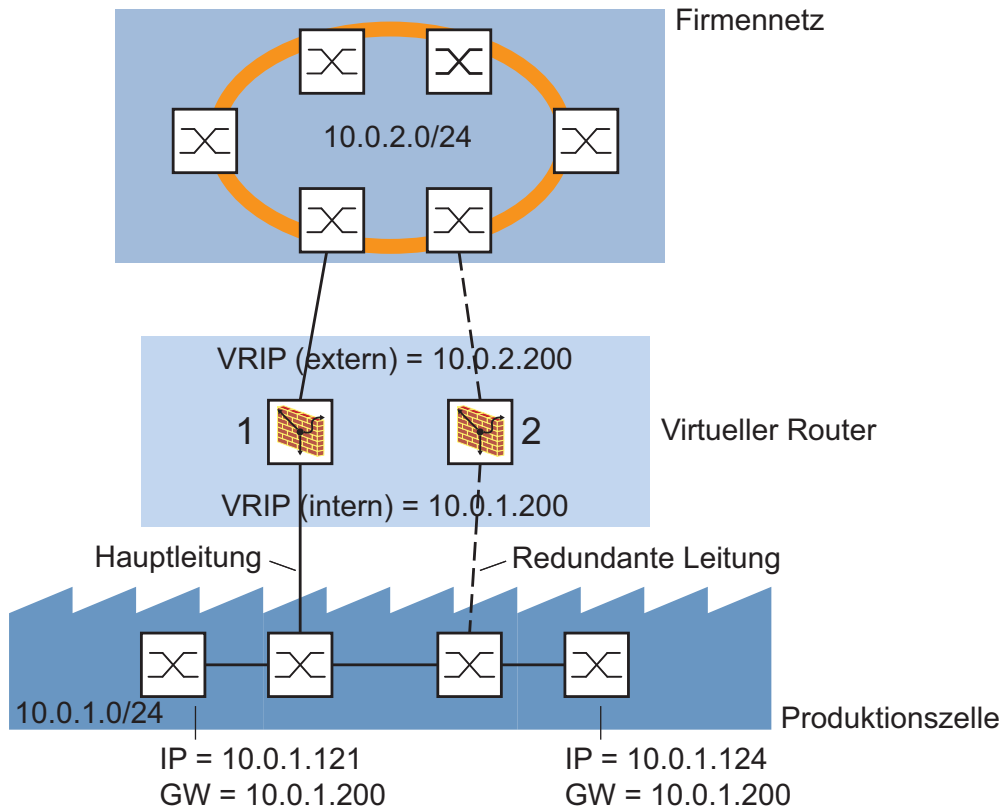


Abb. 47: Router-Redundanz Anwendungsbeispiel

- ☐ Konfigurieren Sie zunächst die Firewall Nummer 1.
Geben Sie die Parameter für die Router-Redundanz ein und schalten Sie die Funktion an.

- ☐ Wählen Sie den Dialog
Redundanz:Router.
- ☐ Wählen Sie die Karteikarte
Grundeinstellungen.

-
- ☐ Klicken Sie im Rahmen „Konfiguration“ in der Zeile „Funktion“ auf An, um die Funktion einzuschalten.
 - ☐ Geben Sie die Parameter gemäß der Tabelle oben ein.
 - ☐ Um die Änderungen flüchtig zu speichern, klicken Sie „Schreiben“.
-
- ☐ Speichern Sie die Einstellungen in den nicht-flüchtigen Speicher.
-
- ☐ Öffnen Sie hierzu den Dialog Grundeinstellungen:Laden/Speichern.
 - ☐ Klicken Sie auf „Speichern in NVM + ACA“, um die Daten nicht-flüchtig zu speichern.
-
- ☐ Konfigurieren Sie anschließend die Firewall Nummer 2.
Geben Sie die Parameter für die Router-Redundanz ein und schalten Sie die Funktion an.
 - ☐ Speichern Sie die Einstellungen in den nicht-flüchtigen Speicher.

8 Funktionsdiagnose

Zur Funktionsdiagnose bietet Ihnen das Gerät folgende Diagnosewerkzeuge an:

- ▶ Erreichbarkeits-Test (Ping)
- ▶ Alarmmeldungen versenden
- ▶ Gerätestatus überwachen
- ▶ Out-of-band-Signalisierung durch Meldekontakt
- ▶ Port-Zustandsanzeige
- ▶ Topologie-Erkennung
- ▶ Konfigurations-Check
- ▶ Berichte
- ▶ MAC-Firewall-Liste
- ▶ IP-Firewall-Liste

8.1 Erreichbarkeits-Test (Ping)

Die Firewall bietet Ihnen die Möglichkeit, die Erreichbarkeit eines beliebigen Netzknotens direkt vom Gerät aus zu testen, auch durch einen VPN-Tunnel hindurch.

Damit erhalten Sie bei erkannten Schwachpunkten im Netz oder bei der Vorbereitung einer Konfiguration rasch eine Aussage über die Erreichbarkeit eines bestimmten Netzknotens (z.B. eines Servers) vom Gerät aus.

Der Erreichbarkeits-Test sendet eine Reihe von ICMP-Echo-Anforderungen aus und prüft, ob die Antworten innerhalb einer Maximalzeit eintreffen. Das Testergebnis können Sie nach einigen Sekunden im selben Dialogfenster ablesen.

Anmerkung: Der Erreichbarkeits-Test setzt voraus, dass der Netzknoten, den Sie testen möchten, ICMP unterstützt und dass vorhandene Firewalls im Pfad ICMP-Echo-Anforderungen und -antworten durchlassen.

Lieferzustand: ausgeschaltet, Quelladresse: 0.0.0.0.

Bei 0.0.0.0 als Quelladresse verwendet die Firewall die IP-Adresse des Interface, an dem die Pings ausgesandt werden. Die Firewall bestimmt das Interface aus der Zieladresse und der Routing-Tabelle.

8.2 Alarmmeldungen versenden

Das Gerät meldet außergewöhnliche Ereignisse, die während des Normalbetriebs auftreten, sofort an die Verwaltungsstation. Dies geschieht über Nachrichten, sogenannte „Traps“, die das Polling-Verfahren umgehen („Polling“: Abfrage der Datenstationen in regelmäßigen Abständen). Traps ermöglichen eine schnelle Reaktion auf außergewöhnliche Ereignisse.

Beispiele für solche Ereignisse sind:

- ▶ Hardware-Reset
- ▶ Änderungen der Konfiguration
- ▶ Segmentierung eines Ports
- ▶ ...

Das Gerät sendet Traps an verschiedene Hosts, um die Übertragungssicherheit für die Nachrichten zu erhöhen. Die nicht quittierte Trap-Nachricht besteht aus einem Paket mit Informationen zu einem außergewöhnlichen Ereignis.

Das Gerät sendet Traps an jene Hosts, die in der Zieltabelle für Traps eingetragen sind. Das Gerät bietet Ihnen die Möglichkeit, die Trap-Zieltabelle mit der Verwaltungsstation über SNMP zu konfigurieren.

8.2.1 Auflistung der SNMP-Traps

Eine Liste aller Traps, die das Gerät verschicken kann, finden Sie im „Referenz-Handbuch Grafische Benutzeroberfläche“.

8.2.2 SNMP-Traps beim Booten

Das Gerät sendet bei jedem Booten die Alarmmeldung „ColdStart“.

8.2.3 Trapeinstellung

- ☐ Öffnen Sie den Dialog `Diagnose:Alarmer (Traps)`.
Dieser Dialog bietet Ihnen die Möglichkeit festzulegen, welche Ereignisse einen Alarm (Trap) auslösen und an wen diese Alarmer gesendet werden sollen.
- ☐ Klicken Sie auf „Eintrag erzeugen“, um einen neuen Tabelleneintrag zu erzeugen
- ☐ In der Spalte „Name“ geben Sie einen Namen für den Empfänger ein, an den die Traps geschickt werden sollen.
- ☐ In der Spalte „IP-Adresse“ geben Sie die IP-Adresse des Empfängers an, an den die Traps geschickt werden sollen.
- ☐ Klicken Sie auf „OK“.
- ☐ In der Spalte „Aktiv“ kreuzen Sie die Einträge an, die beim Versenden von Traps berücksichtigt werden sollen.
- ☐ Im Rahmen „Auswahl“ wählen Sie die Trap-Kategorien aus, von denen Sie Traps versenden wollen.

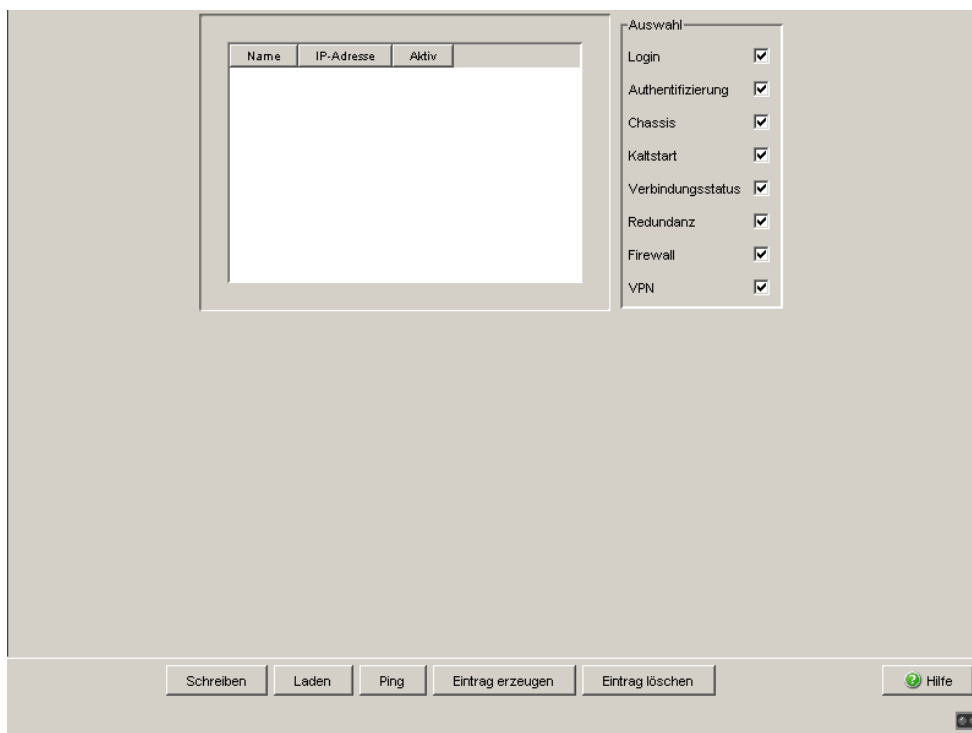


Abb. 48: Dialog Alarmer

8.3 Gerätestatus überwachen

Der Gerätestatus gibt einen Überblick über den Gesamtzustand des Gerätes. Viele Prozessvisualisierungssysteme erfassen den Gerätestatus eines Gerätes, um seinen Zustand grafisch darzustellen.

Das Gerät zeigt seinen aktuellen Status als „Fehler“ oder „Ok“ im Rahmen „Gerätestatus“ an. Das Gerät bestimmt diesen Status aus den einzelnen Überwachungsergebnissen.

Das Gerät bietet Ihnen die Möglichkeit, den Gerätezustand

- ▶ über einen Meldekontakt out-of-band zu signalisieren
(siehe auf Seite 215 „Gerätestatus mit Meldekontakt überwachen“)
- ▶ durch das Versenden eines Traps bei einer Änderung des Gerätezustandes zu signalisieren.
- ▶ in der grafischen Benutzeroberfläche auf der Systemseite zu erkennen und
- ▶ im Command Line Interface abzufragen.

Der Gerätestatus des Gerätes erfasst:

- ▶ einen erkannten Fehler in der Versorgungsspannung, den erkannten Ausfall mindestens einer der zwei Versorgungsspannungen, eine erkannte Störung im Gerät (interne Versorgungsspannung).
- ▶ Über- oder Unterschreiten der eingestellten Temperaturschwelle.
- ▶ das Entfernen des ACA.
- ▶ die unterbrochene Verbindung zu mindestens einem Port. Die Meldung des Linkstatus kann beim Gerät pro Port über das Management maskiert werden (siehe auf Seite 88 „Erkannte Kommunikationsunterbrechung melden“). Im Lieferzustand erfolgt keine Verbindungsüberwachung.

Welche Ereignisse den Gerätestatus bestimmen, hängt von der Einstellung im Management ab.

Anmerkung: Bei nicht redundanter Zuführung der Versorgungsspannung meldet das Gerät das Fehlen einer Versorgungsspannung. Sie können diese Meldung verhindern, indem Sie die Versorgungsspannung über beide Eingänge zuführen oder die Überwachung ausschalten ([siehe auf Seite 215 „Gerätestatus mit Meldekontakt überwachen“](#)).

8.3.1 Gerätestatus konfigurieren

- ☐ Öffnen Sie den Dialog `Diagnose:Gerätestatus`.
- ☐ Wählen Sie im Feld „Überwachung“ die Ereignisse, die Sie überwachen möchten.
- ☐ Zur Temperaturüberwachung stellen Sie zusätzlich die Temperaturschwellen im Dialog `Grundeinstellungen:System` am Ende der Systemdaten ein .

```
enable
configure
device-status monitor all
enable
device-status trap enable
```

Wechsel in den Privileged-EXEC-Modus.

Wechsel in den Konfigurationsmodus.

Bezieht alle möglichen Ereignisse zur Gerätestatusermittlung mit ein.

Aktiviert das Versenden eines Traps, wenn sich der Gerätestatus ändert.

8.3.2 Gerätestatus anzeigen

- ☐ Wählen Sie den Dialog Grundeinstellungen: System .

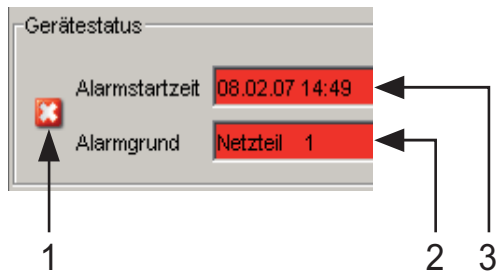


Abb. 49: Gerätestatus- und Alarm-Anzeige
1 - Das Symbol zeigt den Gerätestatus an
2 - Ursache des ältesten, bestehenden Alarms
3 - Beginn des ältesten, bestehenden Alarms

`show device-status`

Zeigt den Gerätestatus und die Einstellung zur Gerätestatusermittlung an.

8.4 Out-of-band-Signalisierung

Die Meldekontakte dienen der Steuerung externer Geräte und der Funktionsüberwachung des Gerätes und ermöglichen damit eine Ferndiagnose. Über den potentialfreien Meldekontakt (Relaiskontakt, Ruhestromschaltung) meldet das Gerät durch Kontaktunterbrechung:

- ▶ eine erkannte fehlerhafte Versorgungsspannung
den erkannten Ausfall mindestens einer der zwei Versorgungsspannungen,
eine erkannte Störung im Gerät (interne Versorgungsspannung).
- ▶ Über- oder Unterschreiten der eingestellten Temperaturschwelle.
- ▶ das Entfernen des ACA.
- ▶ die unterbrochene Verbindung zu mindestens einem Port. Die Meldung des Linkstatus kann beim Gerät pro Port über das Management maskiert werden ([siehe auf Seite 88 „Erkannte Kommunikationsunterbrechung melden“](#)). Im Lieferzustand erfolgt keine Verbindungsüberwachung.

Welche Ereignisse einen Kontakt schalten, hängt von der Einstellung im Management ab.

Anmerkung: Bei nicht redundanter Zuführung der Versorgungsspannung meldet das Gerät das Fehlen einer Versorgungsspannung. Sie können diese Meldung verhindern, indem Sie die Versorgungsspannung über beide Eingänge zuführen oder die Überwachung ausschalten ([siehe auf Seite 215 „Gerätestatus mit Meldekontakt überwachen“](#)).

8.4.1 Meldekontakt steuern

Dieser Modus dient der Fernsteuerung des Signalkontaktes.

Anwendungsmöglichkeiten:

- ▶ Simulation eines bei einer SPS-Fehlerüberwachung ermittelten Fehlers.
- ▶ Fernbedienen eines Gerätes über SNMP, z. B. Einschalten einer Kamera.

- ☐ Wählen Sie den Dialog `Diagnose:Meldekontakt`.
- ☐ Wählen Sie „Manuelle Einstellung“ im Feld „Modus Meldekontakt“, um den Meldekontakt manuell zu schalten.
- ☐ Wählen Sie „Offen“ im Feld „Manuelle Einstellung“, um den Kontakt zu öffnen.
- ☐ Wählen Sie „Geschlossen“ im Feld „Manuelle Einstellung“, um den Kontakt zu schließen.

enable	Wechsel in den Privileged-EXEC-Modus.
configure	Wechsel in den Konfigurationsmodus.
signal-contact mode manual	Wählt die Betriebsart manuelle Einstellung für den Meldekontakt.
signal-contact state open	Öffnet den Meldekontakt.
signal-contact state closed	Schließt den Meldekontakt.

8.4.2 Funktionsüberwachung mit Meldekontakt

■ Funktionsüberwachung konfigurieren

- ☐ Wählen Sie den Dialog `Diagnose:Meldekontakt`.
- ☐ Wählen Sie „Funktionsüberwachung“ im Feld „Modus Meldekontakt“, um den Kontakt zur Funktionsüberwachung zu nutzen.
- ☐ Wählen Sie im Feld „Funktionsüberwachung“ die Ereignisse, die Sie überwachen möchten.
- ☐ Zur Temperaturüberwachung stellen Sie im Dialog `Grundeinstellungen:System` am Ende der Systemdaten die Temperaturschwellen ein.

```
enable
configure
signal-contact monitor
temperature enable
signal-contact trap enable
```

Wechsel in den Privileged-EXEC-Modus.

Wechsel in den Konfigurationsmodus.

Bezieht die Temperatur zur Funktionsüberwachung mit ein.

Aktiviert das Versenden eines Traps, wenn sich der Zustand der Funktionsüberwachung ändert.

■ Meldekontakt-Anzeige

Das Gerät bietet 3 weitere Möglichkeiten, den Zustand des Meldekontaktes darzustellen:

- ▶ LED-Anzeige am Gerät,
- ▶ Anzeige in der grafischen Benutzeroberfläche,
- ▶ Abfrage im Command Line Interface.

Modus Meldekontakt		
	☒ Funktionsüberwachung	☐ Manuelle Einstellung
	☐ Gerätestatus	
Trapeinstellung		
Trap bei Statuswechsel erzeugen	☐	
Funktionsüberwachung		
Kontakt	☐ Offen (Fehler)	☒ Geschlossen (Ok)
Netzteil 1	☒ Überwachen	☐ Ignorieren
Netzteil 2	☒ Überwachen	☐ Ignorieren
Temperatur	☐ Überwachen	☒ Ignorieren
ACA entfernen	☒ Überwachen	☐ Ignorieren
ACA nicht synchron	☒ Überwachen	☐ Ignorieren
Verbindungsfehler	☒ Überwachen	☐ Ignorieren

Abb. 50: Dialog Meldekontakt

```
show signal-contact
```

Zeigt den Zustand der Funktionsüberwachung und die Einstellung zur Statusermittlung an.

8.4.3 Gerätestatus mit Meldekontakt überwachen

Die Auswahl „Gerätestatus“ bietet Ihnen die Möglichkeit, ähnlich wie bei der Funktionsüberwachung den Gerätestatus ([siehe auf Seite 208 „Gerätestatus überwachen“](#)) über den Meldekontakt zu überwachen.

8.5 Port-Zustandsanzeige

☐ Wählen Sie den Dialog `Grundeinstellungen: System`.

Die Gerätedarstellung zeigt das Gerät. Symbole auf den Ports stellen den Status der einzelnen Ports dar.

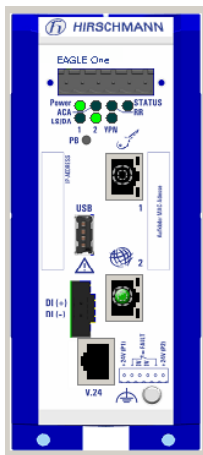


Abb. 51: Gerätedarstellung

Bedeutung der Symbole:

-  Der Port (10, 100 MBit/s) ist freigegeben und die Verbindung ist in Ordnung.
-  Der Port ist vom Management gesperrt und hat eine Verbindung.
-  Der Port ist vom Management gesperrt und hat keine Verbindung.
-  Der Port ist im Autonegotiation-Modus.
-  Der Port ist im HDX-Modus.

8.6 Netzlast und Ereigniszähler auf Portebene

8.6.1 Netzlast

Die Netzlast gibt an, wie viel Prozent der tatsächlich verfügbaren Datenübertragungsrate in Ihrem Netz momentan genutzt werden. Sie können die Netzlast als einfachen Indikator für die Dimensionierung Ihres Netzes verwenden. Ist die durchschnittliche Netzlast über einen langen Zeitraum sehr hoch, sollten Sie das Netz neu dimensionieren und beispielsweise für eine höhere Datenübertragungsrate des Netzes oder Netzlasttrennung sorgen.

Um die Netzlast pro Port anzuzeigen, gehen Sie wie folgt vor:

 ☐ Wählen Sie den Dialog `Diagnose:Ports:Netzlast`.

	<code>enable</code>	Wechsel in den Privileged-EXEC-Modus.
	<code>show interfaces utilization</code>	Zeigt die Netzlast in Prozent für Port 1 (intern) und Port 2 (extern) an.

8.6.2 Port-Statistiken

Die Port-Statistiktabelle versetzt den erfahrenen Netzbetreuer in die Lage, erkannte eventuelle Schwachpunkte im Netz zu identifizieren.

Diese Tabelle zeigt Ihnen die Inhalte verschiedener Ereigniszähler an. Im Menüpunkt Neustart können Sie mit „Warmstart“, „Kaltstart“ oder „Portzähler zurücksetzen“ die Ereigniszähler auf 0 zurücksetzen.

Die Paketzähler summieren die Ereignisse aus Sende- und Empfangsrichtung.

- ☐ Wählen Sie den Dialog `Diagnose:Ports:Statistiken`.
- ☐ Um die Zähler zurückzusetzen, klicken Sie im Dialog Grundeinstellungen:Neustart auf „Portzähler zurücksetzen“.

Port	Empfangene Pakete	Empfangene Unicast Pakete	Empfangene Multicast Pakete	Empfangene Broadcast Pakete	Empfangene Oktets	Empfangsseitig verworfene Pakete	Empfangene fehlerhafte Pakete	Empfangene unbekannte Protokolle
intern (Port 1)	864	844	9	11	1084754	0	0	
extern (Port 2)	1718	1131	24	563	206542	0	0	

Laden
Hilfe

Abb. 52: Anzeige Portstatistiken

```
enable
show interfaces counters
```

Wechsel in den Privileged-EXEC-Modus.
Zeigt die Statistikzähler für Port 1 (intern) und Port 2 (extern) an.

Das Gerät ermittelt mit Hilfe des Address Resolution Protocols (ARP) zur IP-Adresse eines Gerätes die zugehörige MAC-Adresse und speichert diese Zuordnung in der ARP-Tabelle ab.

- ☐ Wählen Sie den Dialog `Diagnose:Ports:ARP`.
- ☐ Um die Zähler zurückzusetzen, klicken Sie im Dialog `Grundeinstellungen:Neustart` auf „ARP-Tabelle zurücksetzen“.

Port	IP-Adresse	MAC-Adresse	Letztes Upd...	Typ	Aktiv
extern (Port 2)	10.115.43.8	08:00:20:3B:15:89	0 Tag(e), 0:02:34	dynamic	☒
extern (Port 2)	10.115.43.12	00:03:BA:12:EA:94	0 Tag(e), 0:05:07	dynamic	☒
intern (Port 1)	10.0.1.112	00:80:63:51:82:80	0 Tag(e), 0:06:28	dynamic	☒
extern (Port 2)	10.115.44.21	00:24:E8:DD:55:AF	0 Tag(e), 0:06:34	dynamic	☒
extern (Port 2)	10.115.32.3	00:00:5E:00:01:05	0 Tag(e), 0:06:48	dynamic	☒

Laden
Hilfe

Abb. 53: Beispiel für ARP-Einträge

```
enable
show network statistics
```

Wechsel in den Privileged-EXEC-Modus.
Zeigt die Netzstatistiken für Port 1 (intern) und Port 2 (extern) an, inklusive der ARP-Einträge.

8.7 Topologie-Erkennung

8.7.1 Beschreibung Topologie-Erkennung

IEEE 802.1AB beschreibt das Link Layer Discovery Protocol (LLDP). Das LLDP ermöglicht dem Anwender eine automatische Topologie-Erkennung seines LANs.

Ein Gerät mit aktivem LLDP

- ▶ verbreitet eigene Verbindungs- und Management-Informationen an die angrenzenden Geräte des gemeinsamen LANs. Diese können dort ausgewertet werden, sofern diese Geräte auch das LLDP aktiviert haben.
- ▶ empfängt Verbindungs- und Management-Informationen von angrenzenden Geräten des gemeinsamen LANs, sofern diese auch das LLDP aktiviert haben.
- ▶ errichtet ein Management-Informationsschema und Objektdefinitionen zum Speichern von Informationen benachbarter Geräte mit aktiviertem LLDP.

Als zentrales Element enthält die Verbindungsinformation die genaue, eindeutige Kennzeichnung eines Verbindungsendpunktes: MSAP (MAC Service Access Point). Diese setzt sich zusammen aus einer netzweit eindeutigen Kennung des Gerätes und einer für dieses Gerät eindeutigen Portkennung.

Inhalt der Verbindungs- und Management-Informationen:

- ▶ Chassis-Kennung (dessen MAC-Adresse)
- ▶ Port-Kennung (dessen Port-MAC-Adresse)
- ▶ Beschreibung des Ports
- ▶ Systemname
- ▶ Systembeschreibung
- ▶ Unterstützte "System Capabilities"

- ▶ Momentan aktivierte "System Capabilities"
- ▶ Interface-ID der Management-Adresse
- ▶ Zustand der Autonegotiation am Port
- ▶ Medium, Halb-/Vollduplexeinstellung und Geschwindigkeits-Einstellung des Ports
- ▶ Information über die VLANs, die im Gerät eingerichtet sind (VLAN-ID und VLAN-Namen; unabhängig davon, ob der Port VLAN-Mitglied ist).

Diese Informationen kann eine Netzmanagementstation von einem Gerät mit aktivem LLDP abrufen. Mit diesen Informationen ist die Netzmanagementstation in der Lage, die Topologie des Netzes darzustellen.

Zum Informationsaustausch benutzt LLDP eine IEEE-MAC-Adresse, die Geräte normalerweise nicht vermitteln. Deshalb verwerfen Geräte ohne LLDP-Unterstützung LLDP-Pakete. So unterbindet ein nicht LLDP-fähiges Gerät zwischen 2 LLDP-fähigen Geräten den LLDP-Informationsaustausch zwischen diesen beiden Geräten. Um dies zu umgehen, versenden und empfangen Hirschmann-Geräte zusätzliche LLDP-Pakete mit der Hirschmann-Multicast-MAC-Adresse 01:80:63:2F:FF:0B. Hirschmann-Geräte mit LLDP-Funktion sind somit in der Lage, LLDP-Informationen auch über nicht LLDP-fähige Geräte hinweg untereinander auszutauschen.

Die Management Information Base (MIB) eines LLDP-fähigen Hirschmann-Gerätes hält die LLDP-Informationen in der lldp-MIB und in der privaten hmLLDP vor.

8.7.2 Anzeige der Topologie-Erkennung

☐ Wählen Sie den Dialog `Diagnose:Topologie-Erkennung`. Dieser Dialog bietet Ihnen die Möglichkeit, die Funktion zur Topologie-Erkennung (LLDP) ein/auszuschalten. Die Topologie-Tabelle zeigt Ihnen die gesammelten Informationen zu Nachbargeräten an. Mit diesen Informationen ist eine Netzmanagement-Station in der Lage, die Struktur Ihres Netzes darzustellen.

Port	Nachbar-Bezeichner	Nachbar IP-Adresse	Nachbar Port Beschreibung	Nachbar Systemname
1.2	00 80 63 a4 cd 00	10.115.0.77	Module: 1 Port: 23 - 1 Gbit	MACH-A4CD00
1.1	00 80 63 1f 10 54	10.0.1.13	Module: 1 Port: 10 - 10/100 Mbit TX	RS-1F1054

Abb. 54: Topologie-Erkennung

Sind an einem Port, z.B. über einen Hub, mehrere Geräte angeschlossen, dann zeigt die Tabelle pro angeschlossenem Gerät eine Zeile an.

Wenn

- ▶ Geräte mit aktiver Topologie-Erkennungs-Funktion und
- ▶ Geräte ohne aktive Topologie-Erkennungs-Funktion an einem Port angeschlossen sind, dann blendet die Topologie-Tabelle die Geräte ohne aktive Topologie-Erkennung aus.

Wenn

- ▶ nur Geräte ohne aktive Topologie-Erkennung an einem Port angeschlossen sind, dann enthält die Tabelle stellvertretend für alle Geräte eine Zeile für diesen Port. Diese Zeile enthält die Anzahl der angeschlossenen Geräte.
IP-Adressen von Geräten, die die Topologie-Tabelle übersichtshalber ausblendet, finden Sie in der Konfigurations-Check-Tabelle, [\(siehe auf Seite 224 „Konfigurations-Check“\)](#).

8.8 Konfigurations-Check

Diese Funktion bietet Ihnen die Möglichkeit, nach der Installation und Konfiguration Ihre Konfiguration zu überprüfen. Zur Überprüfung bezieht der Konfigurations-Check die Konfiguration der Nachbargeräte mit ein.

Mit einem Klick auf eine Zeile finden Sie im unteren Teil des Dialogs Details zum Ergebnis der Prüfung eines Ports.

8.9 Berichte

Folgende Berichte stehen zur Diagnose zur Verfügung:

► Systeminformation.

Die Systeminformation ist eine HTML-Datei, welche die systemrelevanten Daten enthält.

☐ Wählen Sie den Dialog `Diagnose:Bericht`.

☐ Mit einem Klick auf „Systeminformation“ öffnen Sie die HTML-Datei in der grafischen Benutzeroberfläche.

A Konfigurationsumgebung einrichten

A.1 DHCP-Server einrichten

Auf der Produkt-CD, die dem Gerät bei der Lieferung beiliegt, finden Sie die Software für einen DHCP-Server der Firma Softwareentwicklung, IT-Consulting Dr. Herbert Hanewinkel. Sie können die Software bis zu 30 Kalendertage nach dem Datum der ersten Installation testen, um zu entscheiden, ob Sie eine Lizenz erwerben wollen.

- ☐ Zur Installation des DHCP-Servers auf Ihrem PC
legen Sie die Produkt-CD in das CD-Laufwerk Ihres PCs und wählen Sie unter Zusatzsoftware "haneWIN DHCP-Server".
Führen Sie die Installation gemäß des Installationsassistenten durch.
- ☐ Starten Sie das Programm DHCP Server.

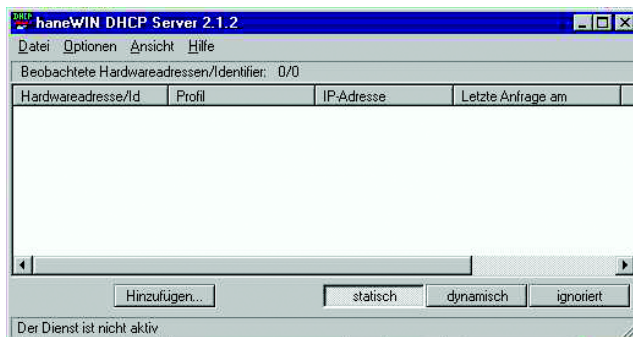


Abb. 55: Startfenster des DHCP-Servers

Anmerkung: Die Installation beinhaltet einen Dienst, der in der Grundkonfiguration automatisch beim Einschalten von Windows gestartet wird. Dieser Dienst ist auch aktiv, wenn das Programm selbst nicht gestartet ist. Der gestartete Dienst beantwortet DHCP-Anfragen.

- ☐ Öffnen Sie das Fenster für die Programmeinstellungen in der Menüleiste: **Optionen:Einstellungen** und wählen Sie die Karteikarte **DHCP**.
- ☐ Nehmen Sie die im Bild dargestellten Einstellungen vor und klicken Sie auf **OK**.

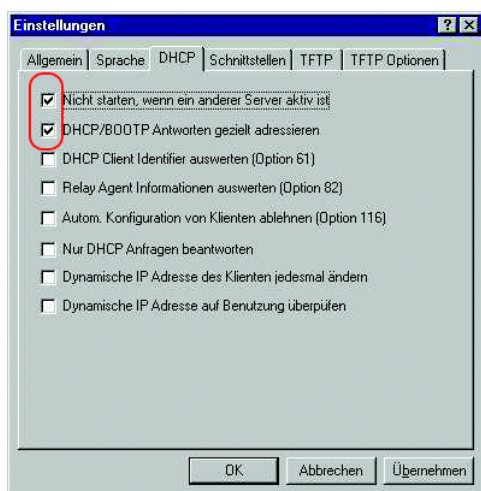


Abb. 56: DHCP-Einstellung

- ☐ Zur Eingabe der Konfigurationsprofile wählen Sie in der Menüleiste `Optionen:Konfigurationsprofile verwalten`.
- ☐ Geben Sie den Namen für das neue Konfigurationsprofil ein und klicken Sie auf `Hinzufügen`.

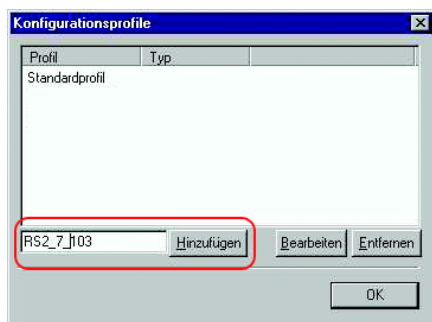


Abb. 57: Konfigurationsprofile hinzufügen

- ☐ Geben Sie die Netzmaske ein und klicken Sie auf Übernehmen.

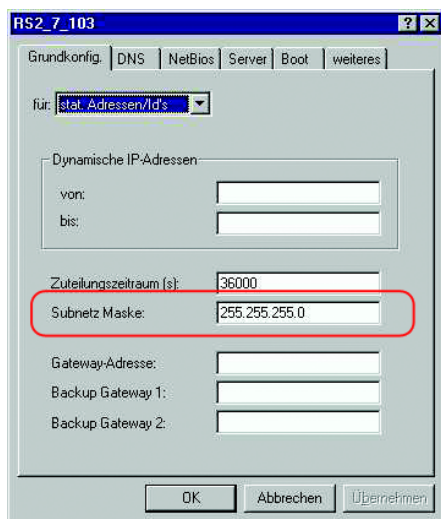


Abb. 58: Netzmaske im Konfigurationsprofil

- ☐ Wählen Sie die Karteikarte `Boot`.
- ☐ Geben Sie die IP-Adresse Ihres tftp-Servers.
- ☐ Geben Sie den Pfad und den Dateinamen für die Konfigurationsdatei ein.
- ☐ Klicken Sie auf `Übernehmen` und danach auf `OK`.

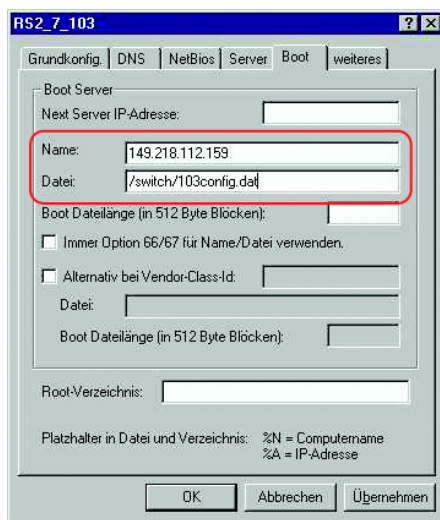


Abb. 59: Konfigurationsdatei auf dem tftp-Server

- ☐ Fügen Sie für jeden Gerätetyp ein Profil hinzu.
Haben Geräte des gleichen Typs unterschiedliche Konfigurationen, dann fügen Sie für jede Konfiguration ein Profil hinzu.
Zum Beenden des Hinzufügens der Konfigurationsprofile klicken Sie auf OK.

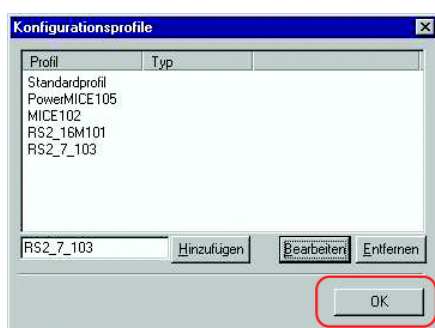


Abb. 60: Konfigurationsprofile verwalten

- ☐ Zur Eingabe der statischen Adressen klicken Sie im Hauptfenster auf Statisch.

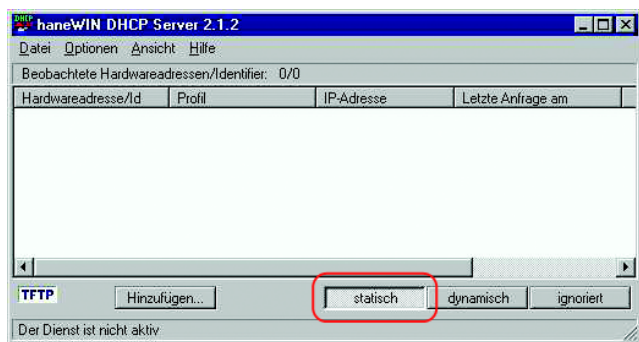


Abb. 61: Statische Adresseingabe

- ☐ Klicken Sie auf Hinzufügen.

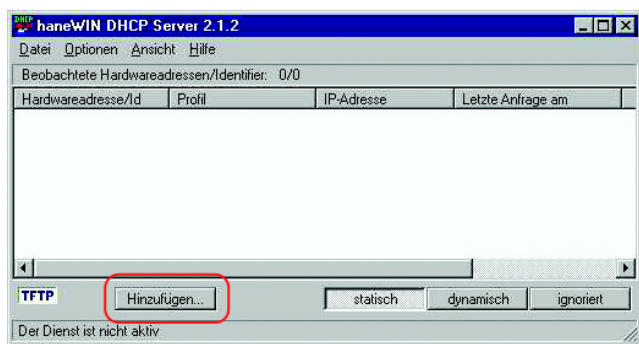
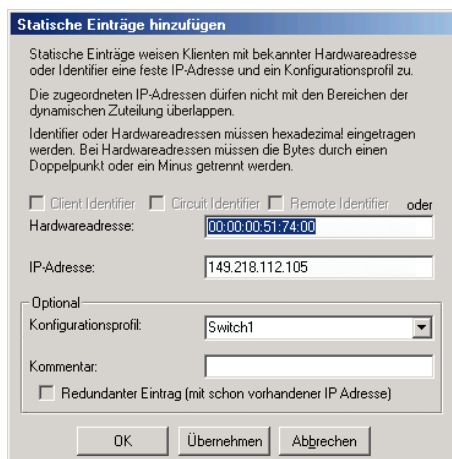


Abb. 62: Statische Adressen hinzufügen

- ☐ Geben Sie die MAC-Adresse des Gerätes ein.
- ☐ Geben Sie die IP-Adresse des Gerätes ein.
- ☐ Wählen Sie das Konfigurationsprofil des Gerätes.
- ☐ Klicken Sie auf Übernehmen und danach auf OK.



Statische Einträge hinzufügen

Statische Einträge weisen Klienten mit bekannter Hardwareadresse oder Identifier eine feste IP-Adresse und ein Konfigurationsprofil zu. Die zugeordneten IP-Adressen dürfen nicht mit den Bereichen der dynamischen Zuteilung überlappen. Identifier oder Hardwareadressen müssen hexadezimal eingetragen werden. Bei Hardwareadressen müssen die Bytes durch einen Doppelpunkt oder ein Minus getrennt werden.

☐ Client Identifier ☐ Circuit Identifier ☐ Remote Identifier oder

Hardwareadresse:

IP-Adresse:

Optional:

Konfigurationsprofil:

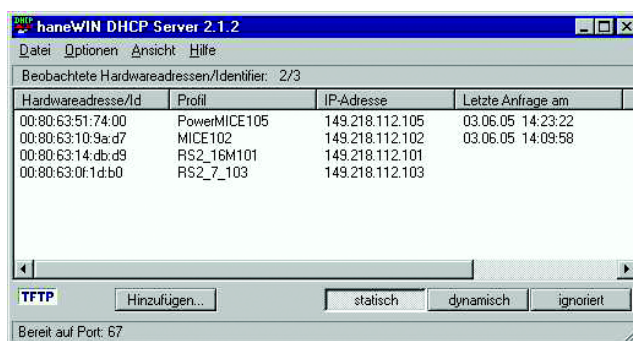
Kommentar:

☐ Redundanter Eintrag (mit schon vorhandener IP Adresse)

OK Übernehmen Abbrechen

Abb. 63: Einträge für statische Adressen

- ☐ Fügen Sie für jedes Gerät, das vom DHCP-Server seine Parameter erhalten soll, einen Eintrag hinzu.



haneWIN DHCP Server 2.1.2

Datei Optionen Ansicht Hilfe

Beobachtete Hardwareadressen/Identifier: 2/3

Hardwareadresse/Id	Profil	IP-Adresse	Letzte Anfrage am
00:80:63:51:74:00	PowerMICE105	149.218.112.105	03.06.05 14:23:22
00:80:63:10:9a:d7	MICE102	149.218.112.102	03.06.05 14:09:58
00:80:63:14:db:d9	RS2_16M101	149.218.112.101	
00:80:63:0f:1d:b0	RS2_7_103	149.218.112.103	

TFTP Hinzufügen... statisch dynamisch ignoriert

Bereit auf Port: 67

Abb. 64: DHCP-Server mit Einträgen

A.2 Zugriff mittels SSH

Eine Möglichkeit mittels SSH auf Ihr Gerät zuzugreifen, bietet das Programm PuTTY. Dieses Programm finden Sie auf der Produkt-CD.

- ☐ Starten Sie das Programm mit einem Doppelklick.
- ☐ Geben Sie die IP-Adresse Ihres Gerätes ein.
- ☐ Wählen Sie „SSH“.
- ☐ Klicken Sie auf „Open“, um die Verbindung zu Ihrem Gerät aufzubauen.
Abhängig vom Gerät und vom Zeitpunkt der Konfiguration von SSH kann der Verbindungsaufbau bis zu einer Minute dauern.

Gegen Ende des Verbindungsaufbaus zeigt PuTTY eine Sicherheitsalarmmeldung und bietet Ihnen die Möglichkeit, den Fingerabdruck des Schlüssels zu überprüfen.



Abb. 65: Sicherheitsabfrage für den Fingerabdruck

- ☐ Überprüfen Sie den Fingerabdruck. Das hilft Ihnen dabei, sich vor unliebsamen Gästen zu schützen.
- ☐ Stimmt der Fingerabdruck mit dem des Geräteschlüssels überein, dann klicken Sie „Ja“.

Anmerkung: Hirschmann liefert das Gerät mit einem eindeutigen, permanent gespeicherten SSH-RSA/DSA-Geräteschlüssel aus. Dieser eindeutige Schlüssel ermöglicht Ihnen die Identifizierung des Geräts beim SSH-Zugriff.

Erfahrenen Netzadministratoren bietet die OpenSSH-Suite eine weitere Möglichkeit, mittels SSH auf Ihr Gerät zuzugreifen. Zum Aufbau der Datenverbindung geben Sie folgenden Befehl ein:

```
ssh admin@10.149.112.53
```

`admin` stellt den Benutzernamen dar.

`10.149.112.53` stellt die IP-Adresse Ihres Gerätes dar.

B Allgemeine Informationen

B.1 Verwendete Abkürzungen

ACA	AutoConfiguration Adapter
ACL	Access Control List
AES	Advanced Encryption Standard
BOOTP	Bootstrap Protocol
CIDR	Classless Inter-Domain Routing
CLI	Command Line Interface
DHCP	Dynamic Host Configuration Protocol)
DES	Data Encryption Standard
DN	Distinguished Name
FDB	Forwarding Database
FQDN	Fully Qualified Domain Name
GARP	General Attribute Registration Protocol
GMRP	GARP Multicast Registration Protocol
HMAC	Hashed Message Authentication Code
http	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
IKE	Internet Key Exchange
IP	Internet Protocol
IPsec	IP Security
LED	Light Emitting Diode
LLDP	Link Layer Discovery Protocol
MAC	Media Access Control
MD5	Message Digest 5
MODP	Modular Exponentiation
NTP	Network Time Protocol
NVM	Non-volatile Memory
PC	Personal Computer
PTP	Precision Time Protocol
QoS	Quality of Service
RFC	Request For Comment
RM	Redundancy Manager
RS	Rail Switch
RSTP	Rapid Spanning Tree Protocol
SA	Security Association
SFP	Small Form-factor Pluggable
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol

SNTP	Simple Network Time Protocol
TCP	Transfer Control Protocol
TFTP	Trivial File Transfer Protocol
TP	Twisted Pair
UDP	User Datagram Protocol
URL	Uniform Resource Locator
UTC	Coordinated Universal Time
VLAN	Virtual Local Area Network

B.2 Management Information BASE (MIB)

Die Management Information Base (MIB) ist als abstrakte Baumstruktur angelegt.

Die Verzweigungspunkte sind die Objektklassen. Die „Blätter“ der MIB tragen die Bezeichnung generische Objektklassen.

Die Instanziierung der generischen Objektklassen, das heißt, die abstrakte Struktur auf die Realität abzubilden, erfolgt z.B. durch die Angabe des Ports oder der Quelladresse (Source Address), soweit dies zur eindeutigen Identifizierung nötig ist.

Diesen Instanzen sind Werte (Integer, TimeTicks, Counter oder Octet String) zugeordnet, die gelesen und teilweise auch verändert werden können. Die Object Description oder der Object-ID (OID) bezeichnet die Objektklasse. Mit dem Subidentifizier (SID) werden sie instanziiert.

Beispiel:

Die generische Objektklasse

`hmPSState` (OID = 1.3.6.1.4.1.248.14.1.2.1.3)

ist die Beschreibung der abstrakten Information „Netzteilstatus“. Es lässt sich daraus noch kein Wert auslesen, es ist ja auch noch nicht bekannt, welches Netzteil gemeint ist.

Durch die Angabe des Subidentifiers (2) wird diese abstrakte Information auf die Wirklichkeit abgebildet, instanziiert, und bezeichnet so den Betriebszustand des Netzteils 2. Diese Instanz bekommt einen Wert zugewiesen, der gelesen werden kann. Damit liefert die Instanz „get

1.3.6.1.4.1.248.14.1.2.1.3.2“ als Antwort „1“, das heißt, das Netzteil ist betriebsbereit.

Einige verwendete Abkürzungen in der MIB:

Comm	Gruppen-Zugriffsrecht
con	Konfiguration
Descr	Beschreibung
Fan	Lüfter
ID	Identifizierer
Lwr	unterer (z. B. Grenzwert)
PS	Spannungsversorgung
Pwr	Stromversorgung
sys	System
UI	Benutzer-Schnittstelle (User Interface)
Upr	oberer (z. B. Grenzwert)
ven	vendor = Hersteller (Hirschmann)

Definition der verwendeten Syntaxbegriffe:

Integer	Ganze Zahl im Bereich von -2^{31} - $2^{31}-1$
IP-Adresse	xxx.xxx.xxx.xxx (xxx = ganze Zahl im Bereich von 0-255)
MAC-Adresse	12-stellige Hexzahl nach ISO/IEC 8802-3
Object Identifier	x.x.x.x... (z. B. 1.3.6.1.1.4.1.248...)
Octet String	ASCII-Zeichen-Kette
PSID	Spannungsversorgungsidentifikation (Nummer des Netzteils)
TimeTicks	Stop-Uhr, verronnene Zeit = Zahlenwert/100 in Sekunden Zahlenwert = ganze Zahl im Bereich von $0-2^{32}-1$
Timeout	Zeitwert in hundertstel Sekunden Zeitwert = ganze Zahl im Bereich von $0-2^{32}-1$
Typfeld	4-stellige Hexzahl nach ISO/IEC 8802-3
Zähler	Ganze Zahl ($0-2^{32}-1$), deren Wert beim Auftreten bestimmter Ereignisse um 1 erhöht wird.

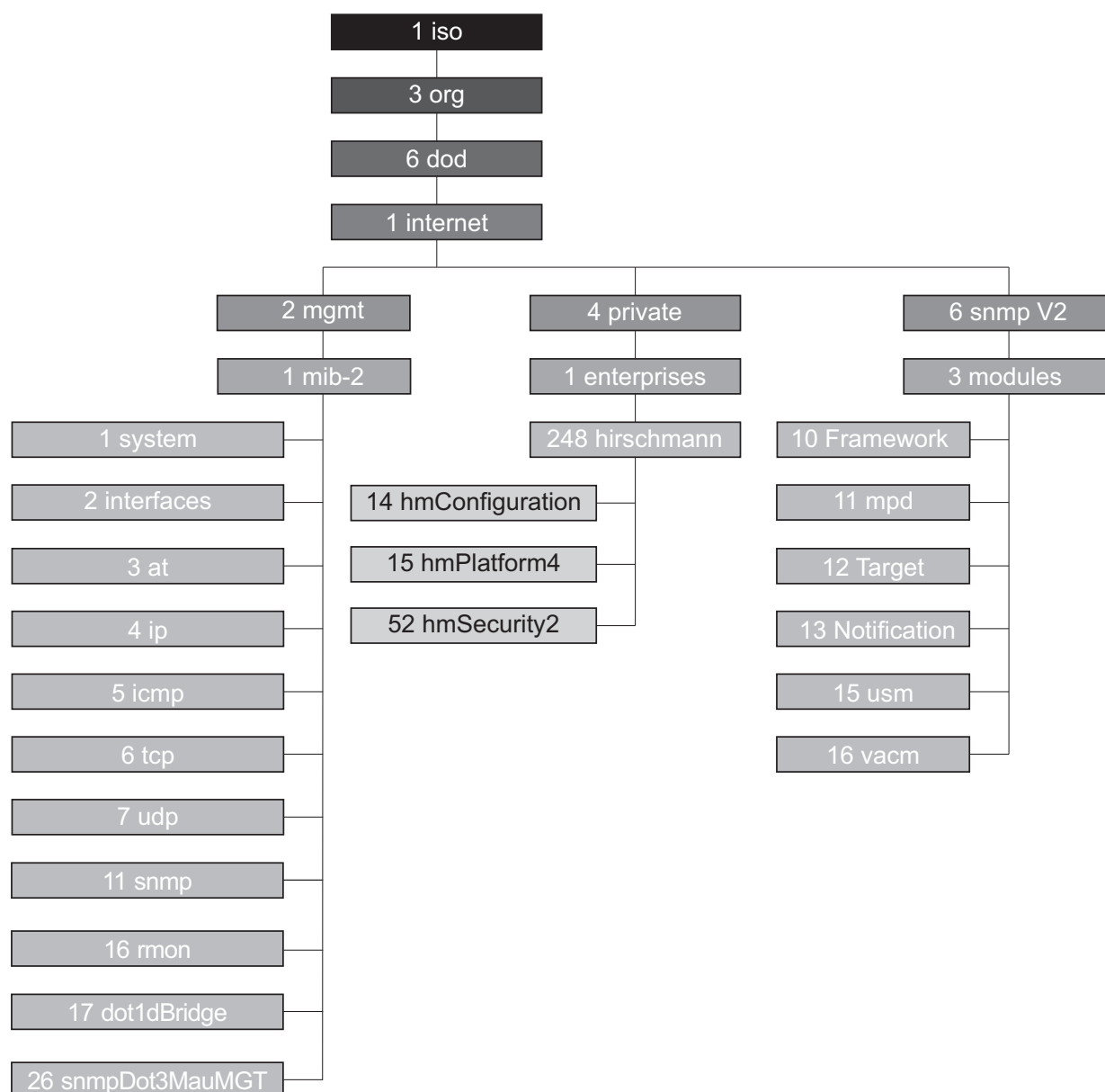


Abb. 66: Baumstruktur der Hirschmann-MIB

Die vollständige Beschreibung der MIB finden Sie auf der CD-ROM, die zum Lieferumfang des Gerätes gehört.

B.3 Technische Daten

Die technischen Daten finden Sie im Dokument „Referenz-Handbuch GUI“.

B.4 Wartung

Hirschmann arbeitet ständig an der Verbesserung und Weiterentwicklung der Software. Prüfen Sie regelmäßig, ob ein neuerer Stand der Software Ihnen weitere Vorteile bietet. Informationen und Downloads von Software finden Sie auf den Produktseiten der Hirschmann-Website.

B.4.1 Service-Shell

Die Service-Shell-Funktion dient der Wartung Ihres funktionsfähigen Gerätes durch einen Servicetechniker. Falls Sie Serviceunterstützung benötigen, bietet diese Funktion dem Servicetechniker die Möglichkeit, von außerhalb auf interne Funktionen Ihres Geräts zuzugreifen.

Anmerkung: Die Service-Shell-Funktion dient ausschließlich Servicezwecken. Sie ermöglicht den Zugriff auf interne Funktionen des Geräts. Führen Sie keinesfalls interne Funktionen ohne die Anweisung eines Servicetechnikers aus. Das Ausführen interner Funktionen wie beispielsweise das Löschen des NVM-Inhalts (permanenter Speicher) führt unter Umständen dazu, dass Ihr Gerät funktionsunfähig wird.

Anmerkung: Das Deaktivieren der Service-Shell-Funktion hat permanente Wirkung.

Um die Service-Shell-Funktion reaktivieren zu lassen, senden Sie das Gerät zurück an den Hersteller.

C Leserkritik

Wie denken Sie über dieses Handbuch? Wir sind stets bemüht, in unseren Handbüchern das betreffende Produkt vollständig zu beschreiben und wichtiges Hintergrundwissen zu vermitteln, damit der Einsatz dieses Produkts problemlos erfolgen kann. Ihre Kommentare und Anregungen unterstützen uns, die Qualität und den Informationsgrad dieser Dokumentation noch zu steigern.

Ihre Beurteilung für dieses Handbuch:

	sehr gut	gut	befriedigend	mäßig	schlecht
Exakte Beschreibung	☐	☐	☐	☐	☐
Lesbarkeit	☐	☐	☐	☐	☐
Verständlichkeit	☐	☐	☐	☐	☐
Beispiele	☐	☐	☐	☐	☐
Aufbau	☐	☐	☐	☐	☐
Vollständigkeit	☐	☐	☐	☐	☐
Grafiken	☐	☐	☐	☐	☐
Zeichnungen	☐	☐	☐	☐	☐
Tabellen	☐	☐	☐	☐	☐

Haben Sie in diesem Handbuch Fehler entdeckt?
Wenn ja, welche auf welcher Seite?

Anregungen, Verbesserungsvorschläge, Ergänzungsvorschläge:

Allgemeine Kommentare:

Absender:

Firma / Abteilung:

Name / Telefonnummer:

Straße:

PLZ / Ort:

E-Mail:

Datum / Unterschrift:

Sehr geehrter Anwender,

Bitte schicken Sie dieses Blatt ausgefüllt zurück

- ▶ als Fax an die Nummer +49 (0)7127 14-1600 oder
- ▶ per Post an

Hirschmann Automation and Control GmbH
Abteilung 01RD-NT
Stuttgarter Str. 45-51
72654 Neckartenzlingen

D Stichwortverzeichnis

1			
1 zu 1-NAT	145	DoS	121, 160
		Double-NAT	147
A		E	
ACA	55, 70, 73, 84	Echtzeit	89
ACA 21-USB	83	Erreichbarkeit	197
Administration (Login-Typ)	31	Erreichbarkeits-Test	204
Adressvorlagen	123	Erstinstallation	35
Alarm	207		
Alarmnachrichten	205	F	
Alleinstehend	29	FAQ	251
Anforderungsintervall (SNTP)	94	Faulty Device Replacement	67
APNIC	37	Ferndiagnose	211
ARIN	37	Firewall-Lern-Modus	124
ARP	42	FLM	124
Authentifizierung	99	Funktionsüberwachung	211
Authentisierung	163		
AutoConfiguration Adapter	55	G	
Automatisches Abmelden	100, 107	Gateway	39, 46, 49, 197
Automatische Konfiguration	87	Generische Objektklassen	240
		Gerätestatus	208, 208
B		Grafische Benutzeroberfläche	23, 29
Benutzerfirewall	121	Grafische Benutzeroberfläche-Zugriff	100
Benutzernamen	27		
Benutzer-Firewall	155, 156	H	
Benutzer-Firewall (Login-Typ)	31	HaneWin	228
Bericht	225	Hardware-Reset	205
Betriebsmodus	35	HDX-Modus	216
Bidirektionales NAT	145	HiDiscovery	53, 114, 115
BOOTP	59, 70	Hirschmann-Adress-Mapping	174
Booten	24	Hostadresse	38
		HTTPS	99, 100
C		Hub and Spoke-Routing	169
CA	163		
CDROM	228	I	
Certification Authority	163	IANA	37, 38
CIDR	42	ICMP-Echo-Anforderung	204
CLI	23	IEEE-MAC-Adress	221
Classless Inter Domain Routing	42	IKE Internet Key Exchange	163
Command Line Interface	23, 26	Industrial HiVision	8, 59
		Instanzierung	240
D		Integrität	162
Datenverkehr	121	Internet Assigned Numbers Authority	37
Default-Gateway	197	Internet Key Exchange Protokoll	163
Denial of Service	121, 160	Internet Protocol Security	162
Destination-NAT	148	Internet Protocol Security (IPsec)	162
DHCP	36, 57, 57, 70	Internet-Router	39
DHCP-Client	57, 57	Internet-Service-Provider	37
DHCP-Server	228	Inverses 1zu1-NAT	146

IPsec	162, 162, 163	OpenSSH-Suite	235, 235
IP-Adresse	37, 37, 46, 47, 49, 50, 58	out-of-band	26
IP-Adressvorlagen	123		
IP-Masquerading	144, 144	P	
IP-Parameter	35	Paketfilter	121, 122, 122
ISO/OSI-Schichtenmodell	42	Paketgröße	51, 66
		Passwort	27, 31, 100, 107
K		Ping	204
Kaltstart	85	Polling	205
Konfiguration	18	Portabel	30
Konfigurationsänderungen	205	Portkonfiguration	87
Konfigurationsdaten	76, 76	Portweiterleitung	148, 148
Konfigurations-Check	224	Port ein-/ausschalten	87
		PPPoE-Modus	21, 35, 50, 65
L		Pre-Shared-Key	163
LACNIC	37	Private IP-Adresse	38, 38
Lern-Modus	124		
Leserecht	31	R	
Lieferzustand	74, 113	Reboot	85
LLDP	222	Redundanz	191, 191, 197
Login-Fenster	31	Referenzuhr	89, 93
Login-Typ	31	Relaiskontakt	211
		Release	82
M		Reset	85
MAC-Zieladresse	42	RIPE NCC	37
Management VLAN-ID	61	Router	39
Maximum Transmission Unit	51, 66	Router-Modus	20, 35, 63, 197
Meldekontakt	88, 211	Router-Redundanz	197, 197
Modus	87	Ruhestromschaltung	211
MTU	51, 66		
message URL http		S	
//www.dyndns.com/services/dns/dyndns/	179	Schreibrecht	31
		Schulungsangebote	251
N		Segmentierung	205
NAPT	144	Service-Provider	37
NAT	121, 143, 143	Setze Zeit vom PC	90
Nachricht	205	SFTP-Zugriff	79, 110
Network Address Port Translation	144	Sicherheitskonzept	12
Network Address Translation	121, 143, 143	Signallaufzeit	93
Network Address Translation Protocol	39	SNMP	29, 113, 205
Netzadresse	37	SNMPv3	100
Netzmanagement	59	SNMP-Port	100, 107
Netzmanagementstation	222	SNTP	94
Netzmaske	39, 46, 47, 49, 50, 51, 66	SNTP-Broadcasts akzeptieren	94
Neustart	85	Software-Release	82
Nicht-flüchtiger Speicher	71	SSH	23, 26, 26
NTP	95	Stand-alone	29
NTP-Client	95	Stateful Firewall	191
NTP-Server	95	Subidentifizier	240
		Subnetz	46, 47, 49, 50
O		Symbol	9
Object Description	240	Systemname	57, 57
Object-ID	240	Systemzeit	93
Objektklassen	240	Systemzeit (Bezug von einem SNTP-Server)	

System-Monitor 94
23, 24

T

Technische Fragen 251
Templates (IP-Adressen) 123
Topologie 222
Transparent-Modus 19, 35, 46, 61
Transparent-Redundanz 192
Trap 205, 207
Trap-Zieltabelle 205
Tunnelmodus 162
Twice-NAT 147

U

Universal Time Coordinated 96
Update 24
USB-Stick 84
UTC 96
Übertragungsparameter 24
Übertragungssicherheit 205

V

Verbindungsfehler 88
Verbindungsüberwachung 208, 211
Verkehrsflussvertraulichkeit 162
Verschlüsselung 99
Vertraulichkeit 162
Virtuelles Privates Netz 121
VLAN ID 61
VLAN-Tag 61
Vorlagen (IP-Adressen) 123
VPN 121, 161
V.24 26, 27
V.24-Anschluss 23
V.24-Schnittstelle 23

X

X.509 rsa 163

Z

Zertifikat 99, 163
Zertifizierungsstelle 163
Zieltabelle 205
Zugriffsrecht 113

E Weitere Unterstützung

■ Technische Fragen

Bei technischen Fragen wenden Sie sich bitte an den Hirschmann-Vertragspartner in Ihrer Nähe oder direkt an Hirschmann.

Die Adressen unserer Vertragspartner finden Sie im Internet unter <http://www.hirschmann.com>

Unser Support steht Ihnen zur Verfügung unter <https://hirschmann-support.belden.eu.com>

Sie erreichen uns

in der Region EMEA unter

- ▶ Tel.: +49 (0)1805 14-1538
- ▶ E-Mail: hac.support@belden.com

in der Region Amerika unter

- ▶ Tel.: +1 (717) 217-2270
- ▶ E-Mail: inet-support.us@belden.com

in der Region Asien-Pazifik unter

- ▶ Tel.: +65 6854 9860
- ▶ E-Mail: inet-ap@belden.com

■ Hirschmann Competence Center

Das Hirschmann Competence Center mit dem kompletten Spektrum innovativer Dienstleistungen hat vor den Wettbewerbern gleich dreifach die Nase vorn:

- ▶ Das Consulting umfasst die gesamte technische Beratung von der Systembewertung über die Netzplanung bis hin zur Projektierung.
- ▶ Das Training bietet Grundlagenvermittlung, Produkteinweisung und Anwenderschulung mit Zertifizierung.
Das aktuelle Schulungsangebot zu Technologie und Produkten finden Sie unter <http://www.hicomcenter.com>
- ▶ Der Support reicht von der Inbetriebnahme über den Bereitschafts-service bis zu Wartungskonzepten.

Mit dem Hirschmann Competence Center entscheiden Sie sich in jedem Fall gegen jeglichen Kompromiss. Das kundenindividuelle Angebot lässt Ihnen die Wahl, welche Komponenten Sie in Anspruch nehmen.

Internet:

<http://www.hicomcenter.com>



HIRSCHMANN

A **BELDEN** BRAND