HIRSCHMANN
A BELDEN BRAND

ICS Security Handbuch für Hirschmann Switches

Be certain.
Belden.

Verfügbarkeit, Integrität und Vertraulichkeit
Switch-Familie
Classic Switch Software

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.

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).

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

Inhalt

1 Motivation und Ziele 5

1.1 Motivation 6

1.2 Zielsetzung 7

1.3 Anwendungsbereiche 8

1.4 Weitere Informationen 9

2 Beschreibung des Produktes 11

3 Rahmenbedingungen 13

3.1 Systembereitstellungsprozess 15
- 3.1.1 Anforderungsanalyse 16
- 3.1.2 Architektur 17
- 3.1.3 Implementierung 17
- 3.1.4 Test 17
- 3.1.5 Betrieb und Wartung 18
- 3.1.6 Außerdienststellung 18

3.2 Physikalische Rahmenbedingungen 19

3.3 Personelle Anforderungen 20

3.4 Patch-Management 21

3.5 (Security) Incident Handling 22

3.6 Schutz vor Malware 23

3.7 Benutzer und Rechtemanagement 24

3.8 Anforderungen an die Dokumentation 25

4 Sichere Konfiguration 27

4.1 Inbetriebnahme 28
- 4.1.1 Bedrohungen 28
- 4.1.2 Security Quick Check „Inbetriebnahme“ 28
- 4.1.3 Maßnahmen 29

4.2 Trennung von Netzen 38
- 4.2.1 Bedrohungen 38
- 4.2.2 Security Quick Check „Trennung von Netzen“ 39
- 4.2.3 Maßnahmen 40

4.3 Administrativer Zugriff 56
4.3.1 Bedrohungen 56
4.3.2 Security Quick Check „Administrationszugriff“ 57
4.3.3 Maßnahmen 58

4.4 Überwachung 71
4.4.1 Bedrohungen 71
4.4.2 Security Quick Check „Überwachung“ 72
4.4.3 Maßnahmen 73

4.5 Service Level Management (Netz Qualität) 95
4.5.1 Bedrohungen 95
4.5.2 Security Quick Check „Service Level Management“ 96
4.5.3 Maßnahmen 97

4.6 Updates 113
4.6.1 Bedrohungen 113
4.6.2 Security Quick Check 114
4.6.3 Maßnahmen 114

4.7 Außerbetriebnahme 117
4.7.1 Bedrohungen 117
4.7.2 Security Quick Check 117
4.7.3 Maßnahmen 118

4.8 Störung 119
4.8.1 Bedrohungen 119
4.8.2 Security Quick Check „Störung“ 120
4.8.3 Maßnahmen 120

A Referenzen 123

B Leserkritik 124

C Weitere Unterstützung 127

1 Motivation und Ziele

Dieses Dokument basiert auf einer Vorlage, die von TÜV SÜD Rail im Auftrag von Hirschmann für Hirschmann-Geräte erstellt wurde.

1.1 Motivation

Der Switch dient in der industriellen Automation und Leittechnik der Vernetzung von Leittechnik, Anlagen und Büro-IT. Diese Kommunikation wird mehr und mehr durch unsere Kunden gefordert, denn eine durchgängige Kommunikation beschleunigt die Produktion, senkt die Kosten und kann durch eine enge Verknüpfung die Geschäftsprozesse unserer Kunden unterstützen.

Cyber Attacken wie Stuxnet haben aber gezeigt, dass Anlagen der industriellen Automation und Leittechnik angreifbar sind und manipuliert werden können. Insbesondere kann die Vernetzung von industriellen Umgebungen mit der Büro IT zu Angriffen auf die Leittechnik verwendet werden. Sichern Sie deshalb diese Vernetzung und Kommunikation ab. Hierzu kann der Switch in besonderer Weise dienen.

Unabdingbar hierfür ist aber, dass die Sicherheitsanforderungen ermittelt werden, eine sichere Konzeption erstellt wird und in diese das Produkt mit einer sicheren Konfiguration des Produktes integriert wird.

1.2 Zielsetzung

Sichere Netze aufzubauen, ohne dabei durch den Hersteller der Netzprodukte unterstützt zu werden, ist kaum möglich. Dieses Handbuch ist Teil der Anstrengungen, die Hirschmann Automation and Control GmbH unternimmt, die Sicherheit seiner Produkte zu verbessern und den Planern und Anwender bei der sicheren Konfiguration und Nutzung der Produkte zu unterstützen.

Allerdings gibt es keine universal passende Konfiguration, die in allen Situationen als sicher zu betrachten ist. Das vorliegende IT-Sicherheitshandbuch hilft dem Planer und Betreiber der für dieses Dokument relevanten Switche bei folgenden Aktionen:

- ☐ ausreichende und angemessene Sicherheitsanforderungen ermitteln,
- ☐ eine möglichst sichere Konfiguration implementieren,
- ☐ eine Integration in das Monitoring realisieren und das möglichst sichere Betreiben.

1.3 Anwendungsbereiche

Der Switch unterstützt Sie durch vielfältige Kommunikationsmöglichkeiten und ermöglicht reibungslosen Datenaustausch. Dies erstreckt sich über eine große Bandbreite an Brachen wie etwa den Energiesektor, in Automatisierungsbereichen oder im Bahnbereich.

Was die Bereiche eint, ist das Ziel, Endgeräte zu vernetzen. Wobei sich 2 Einsatzszenarien unterscheiden lassen. Der erste Fall ist eine Integration in ein Gesamtsystem, wie etwa in einem Umspannwerk. Der zweite Fall ist ein geschlossenes System wie es ein Anlagenbauer in sein System integriert und anschließend an den Kunden liefert. Dort wird die Anlage und somit auch der Switch in ein Gesamtsystem eingebunden.

In beiden Fällen trägt die Sicherheit des Switches zur Sicherheit des Gesamtsystems bei.

1.4 Weitere Informationen

Über neue erschienene Software-Versionen mit deren Release-Notes informiert ein Software Update Newsletter, zu dem Sie sich gesondert anmelden können.

Wenn Sie mögliche Schwachstellen oder Security-Probleme in Produkten von Hirschmann Automation and Control GmbH gefunden haben, melden Sie diese über die Belden-Security-Web-Seite oder direkt per E-Mail:
https://www.belden.com/security
BEL-SM-PSIRT@belden.com

Die Seite enthält Folgendes:

- “Advisories”
  Berichte über Security-Schwachstellen in unseren Produkten, die aktuell nicht behoben sind.
- “Bulletins”
  Berichte über Security-Schwachstellen in unseren Produkten, die behoben sind.
- “Report Security Vulnerabilities”
  Ein Online-Formular, um Schwachstellen zu melden.

Die Seite enthält ebenso eine Beschreibung, wie Hirschmann Automation and Control GmbH gemeldete Schwachstellen bearbeitet.

2 Beschreibung des Produktes

Die Hirschmann™ Software bietet eine Reihe von Funktionen, die normalerweise in Backbone-Systemen von Unternehmensnetzen verwendet werden. Hierzu zählen umfassende Management-, Diagnose- und Filterfunktionen, verschiedene Redundanzverfahren, Sicherheitsmechanismen und Echtzeitanwendungen. Die in den managed Switch-Reihen MACH, MICE, Rail und OCTOPUS verwendete Software optimiert die Bandbreite, die Konfigurationsfunktionen sowie Service-Funktionen. Bei Version 9 unserer Classic Software genügt zur Konfiguration des gesamten Rings die Konfiguration eines Switches. Zudem lassen sich Konfigurationen auch offline, also ohne aktive Verbindung zum Switch, erstellen.

Switching	
Layer 2 Basic (L2B)	Geeignet für RSB20, OCTOPUS. Der kostengünstige Einstieg in managed Switch-Funktionalität einschließlich Statistiken, Filter und Redundanztechnologien. Die Alternative zu unmanaged Switches.
Layer 2 Enhanced (L2E)	Geeignet für RS20/RS30/RS40, MS20/MS30. Basic-Ebene plus vielfältige Management-, Filter- und Diagnosefunktionen Ebenfalls unterstützt werden schnelle Redundanzverfahren, industrielle Profile sowie Sicherheitsfunktionen. Ideal für standardmäßige Industrieanwendungen.
Layer 2 Professional (L2P)	Geeignet für RS20/RS30/RS40, MS20/MS30, OCTOPUS, PowerMICE, RSR20/RSR30, MACH100, MACH1000, MACH4000. Erweiterte Software plus erweiterte Diagnose- und Filtereigenschaften, Sicherheitsfunktionen und Redundanzverfahren. Ein Softwarepaket für Applikationen, bei denen großer Wert auf kompromisslose Sicherheit der Produktionsanlage und maximale Verfügbarkeit gelegt wird.

Routing	
Layer 3 Enhanced (L3E)	Geeignet für PowerMICE, MACH4000. Layer 2 Professional-Software plus zusätzliche Sicherheit, statisches Routing, Router- und Verbindungsredundanz. Die Layer 3-Software ist für kleinere Datennetze und Anwendungen mit erhöhten Sicherheitsanforderungen gedacht.
Layer 3 Professional (L3P)	Geeignet für PowerMICE, MACH1040, MACH4000. Layer 3 Enhanced plus eine Vielzahl von dynamischen Routing-Protokollen, schneller Routerredundanz und verbesserter Verbindungsredundanz.

3 Rahmenbedingungen

Dieses Dokument bezieht sich bei den Software-Varianten L2E, L2P, L3E und L3P auf die Software 7.1.05.

Die zugrundelegende Software-Version für die Variante L2B ist die Version 05.3.02.

Die in diesem Dokument beschriebenen Funktionen sind relevant für spätere Software-Versionen.
Die meisten in diesem Dokument beschriebenen Funktionen sind relevant für frühere Software-Versionen

Die Produktvarianten EtherNet/IP und PROFINET haben industrieprotokoll-spezifische Voreinstellungen. Deshalb gilt dieses IT-Sicherheitshandbuch nicht für Produktvarianten, die im Produktcode EtherNet/IP oder PROFINET enthalten. Wenn Sie den Inhalt des IT-Sicherheitshandbuchs auf diese Switche anwenden, verlieren diese Switche ihre industrieprotokollspezifischen Einstellungen.

Für die Maßnahmen im Kapitel „Sichere Konfiguration” auf Seite 27 werden folgende Dokumente für die Konfiguration herangezogen:

Titel	Kürzel	Version
Referenz Handbuch Command Line Interface Industrial ETHERNET Switch RSB20, OCTOPUS OS20/OS24 Managed	CLI L2B	Release 5.3 05/2012
Referenz-Handbuch Web-based Interface Industrial ETHERNET Switch RSB20, OCTOPUS OS20/OS24 Managed	GUI L2B	Release 5.3 05/2012
Referenz-Handbuch Command Line Interface Industrial ETHERNET (Gigabit) Switch RS20/RS30/RS40, RSB20, MS20/MS30, OCTOPUS	CLI L2E	Release 7.1 12/2011
Referenz-Handbuch GUI Graphical User Interface Industrial Ethernet (Gigabit-)Switch RS20/RS30/RS40, MS20/MS30, OCTOPUS	GUI L2E	Release 7.1 12/2011
Referenz-Handbuch Command Line Interface Industrial Ethernet (Gigabit-)Switch RS20/RS30/RS40, MS20/MS30, OCTOPUS, PowerMICE, RSR20/RSR30, MACH 100, MACH 1000, MACH 4000	CLI L2P	Release 7.1 12/2011

Titel	Kürzel	Version
Referenz-Handbuch GUI Graphical User Interface Industrial Ethernet (Gigabit-)Switch RS20/RS30/RS40, MS20/MS30, OCTOPUS, Power-MICE,RSR20/RSR30, MACH 100, MACH 1000, MACH 4000	GUI L2P	Release 7.1 12/2011
Referenz-Handbuch Command Line Interface Industrial Ethernet (Gigabit-)Switch PowerMICE, MACH 1040, MACH 4000	CLI L3E	Release 7.1 12/2011
Referenz-Handbuch Command Line Interface Industrial Ethernet (Gigabit-)Switch PowerMICE, MACH 1040, MACH 4000	CLI L3P	Release 7.1 12/2011
Referenz-Handbuch GUI Graphical User Interface Industrial Ethernet (Gigabit-)Switch PowerMICE, MACH 1040, MACH 4000	GUI L3E	Release 7.1 12/2011
Referenz-Handbuch GUI Graphical User Interface Industrial Ethernet (Gigabit-)Switch PowerMICE, MACH 1040, MACH 4000	GUI L3P	Release 7.1 12/2011
Anwender-Handbuch Grundkonfiguration	AHG L2P/ L3E	Release 7.1 12/2011
Grundkonfiguration Industrial Ethernet (Gigabit-)Switch PowerMICE, MACH 1040, MACH 4000	Basic L3P	Release 7.1 12/2011

3.1 Systembereitstellungsprozess

Betreiber von einer IT-Infrastruktur im industriellen Umfeld (im Folgenden kurz System genannt) sollten über einen Systembereitstellungsprozess (im Folgenden SBP abgekürzt) verfügen. Durch den er das System mit allen Security Anforderungen einführt, verändert und wartet. Der SBP setzt sich aus folgenden wesentlichen Phasen zusammen:

- ☐ Anforderungsanalyse
- ☐ Architektur
- ☐ Implementierung
- ☐ Test
- ☐ Betrieb und Wartung
- ☐ Außerbetriebnahme

Der Betreiber eines Systems dokumentiert den SBP mit seinen wesentlichen Phasen und Aktivitäten. Er integriert die zu beachtenden Security Aspekte. Er beschreibt die Verantwortlichkeiten (Rollen und Rechte), die dafür sorgen, dass der SBP den definierten Qualitäts- und Security Anforderungen entspricht; Beispiel: ein geeignetes Qualitätsmanagement, das auch Security adressiert.

Der Betreiber auditiert den SBP regelmäßig, führt Verbesserungen durch und verfolgt die Umsetzung der Verbesserungen. Zudem gewährleistet er, dass ausschließlich qualifiziertes Personal zur Durchführung des SBP eingesetzt wird.

Ein sogenanntes Asset (oder Configuration) Management muss etabliert sein, damit das System mit all seinen Komponenten, Softwareständen erfasst werden kann. Das Asset Management ist Basis für ein Freigabe- (Release-) und Änderungs- (Change-) Management und damit Grundlage für die Qualitätssicherung jeglicher Änderung des Systems.

3.1.1 Anforderungsanalyse

Führen Sie für das System eine ganzheitliche Bedrohungsanalyse durch, die sowohl Prozesse als auch die eingesetzten Techniken berücksichtigt.

Ausgehend vom Anwendungsfall (wie zum Beispiel Installation, Administration, Monitoring etc.) identifizieren Sie gemäß den Security Zielen zunächst alle wesentlichen Bedrohungsszenarien, die zu Risiken führen können. Berücksichtigen Sie in der Beschreibung der Anwendungsfälle auch Annahmen, die Sie über die Umgebung des Systems bzgl. der Anwendungsfälle getroffen haben. Leiten Sie gemäß den identifizierten Bedrohungsszenarien und Risiken Security Voraussetzungen und Security-Maßnahmen für das System ab (dokumentiert in einer Security-Anforderungs-Spezifikation). Achten Sie darauf, dass die aus den Security-Voraussetzungen abgeleiteten Security-Maßnahmen alle Security Voraussetzungen lückenlos abdecken.

Die Security-Anforderungs-Spezifikation ist nach einem 4-Augen-Prinzip einem Review zu unterziehen. Sie dient auch als Grundlage für die Ableitung der Tests für die Security-Maßnahmen für das System.

In Kapitel „Sichere Konfiguration” auf Seite 27 finden Sie Beispiele solcher Anwendungsfälle inklusive Bedrohungen und den Maßnahmen, die Sie für den sicheren Betrieb des Switches treffen sollen.

3.1.2 Architektur

Ein Architektur Dokument beschreibt das System mit allen seinen Komponenten und Security-Maßnahmen. Insbesondere stellt es die Schnittstellen zwischen den einzelnen Komponenten dar. Eine Defense-in-Depth-Strategie verfolgt aufeinanderfolgende Security-Maßnahmen, sodass, wenn ein Angreifer eine Hürde genommen hat, er vor der nächsten Hürde steht. Wenn ein Angreifer eine Security-Maßnahme überwunden hat, bleibt die Security des Gesamtsystems erhalten. Beschreiben Sie das Zusammenwirken der einzelnen Security-Maßnahmen.

Zeichnen Sie ein vollständiges Bild der Security des gesamten Systems, das auch die Defense-in-Depth-Strategie erkennen lässt.

Ein Beispiel einer Defense-in-Depth-Strategie für den industriellen Einsatz finden Sie im Artikel [1] (siehe Referenzen im Anhang).

3.1.3 Implementierung

Die Implementierung der Security-Maßnahmen wird im Allgemeinen durch Projekte realisiert. Verfolgen Sie die Umsetzung der Maßnahmen daher nach einem Projektplan. Dokumentieren Sie die Umsetzung der Security-Maßnahmen.

3.1.4 Test

Weisen Sie die Wirksamkeit und Korrektheit der umgesetzten Maßnahmen durch Tests und Audits nach. Führen Sie nach einem Testplan hierzu Security-Tests und -Audits durch. Werden Lücken entdeckt, schlagen Sie Verbesserungsmaßnahmen vor, dokumentieren Sie diese, setzen Sie diese um und nachverfolgen Sie diese.

3.1.5 Betrieb und Wartung

Identifizieren Sie in der Bedrohungsanalyse auch Risiken, die sich aus Betrieb und Wartung ergeben, zum Beispiel Risiken bei ungenügend abgesicherter Fernwartung. Führen Sie insbesondere jede Änderung am System nach einem dokumentierten Änderungsverwaltungsprozess durch, der Änderungen nach einem 4-Augen-Prinzip autorisiert. Dokumentieren Sie Änderungen am System. Definieren Sie einen Security-Incident-Prozess, mit dem Sie auf Security-Vorfälle angemessen, gemäß der Kritikalität des Incidents (Vorfalls), reagieren können.

3.1.6 Außerdienststellung

Beachten Sie bei der Außerbetriebnahme eines Systems oder von Teilen des Systems ebenfalls Security-Aspekte. Löschen Sie z.B. sensitive Daten von Speichern, sodass Sie eine Wiederherstellung der Daten mit vertretbarem Aufwand ausschließen können oder zerstören Sie die Datenträger entsprechend. Bilden Sie die Außerbetriebnahme auch im Change-Management-Prozess ab, um unerwünschte Effekte auf andere Systeme auszuschließen oder zu berücksichtigen.

3.2 Physikalische Rahmenbedingungen

Achten Sie darauf, dass der physikalische Schutz des Gerätes bzw. der Anlage den Anforderungen aus der zugrunde liegenden Risikoanalyse genügen. Dieser kann sich je nach Umgebung und Bedrohungslage stark unterscheiden.

3.3 Personelle Anforderungen

IT-Sicherheit ist kein Zustand, der ausschließlich mit einem Produkt alleine hergestellt werden kann. Es ist zusätzlich auch Know-how und Erfahrung des Planers und Betreibers notwendig. Hirschmann unterstützt Sie dabei durch verschiedene Schulungsangebote und Zertifizierungsmöglichkeiten.

Sie finden das aktuelle Schulungsangebot unter:

http://www.beldensolutions.com/de/Service/Competence-Center/Training/index.phtml

3.4 Patch-Management

Zum Erhalten der Security im Betrieb ist es wichtig rechtzeitig Kenntnis vom Hersteller zur Installation empfohlene Patches und Releases zu erlangen, diese zu prüfen und ggf. einzuspielen. Führen Sie eine Risikobewertung durch, die sowohl das Risiko für das Einspielen als auch für das Nicht-Einspielen des Patches oder Releases betrachtet. Spielen Sie Sicherheitspatches grundsätzlich ein, es sei denn, gravierende Gründe sprechen dagegen.

3.5 (Security) Incident Handling

Um die IT-Sicherheit im laufenden Betrieb aufrecht zu erhalten, konzipieren Sie die Behandlung von Störungen insbesondere von Security-Incidents (Security-Incident-Handling) und üben Sie die Behandlung von Störungen ein. Um Schäden zu vermeiden bzw. zu begrenzen, sollte die Behandlung der Security Incidents zeitnah und effizient ablaufen. Die möglichen Schäden bei einem Security Incident können dabei sowohl die Vertraulichkeit oder Integrität von Daten als auch die Verfügbarkeit betreffen.

3.6 Schutz vor Malware

Regeln Sie Kompetenzen und Verantwortlichkeiten klar zum Schutz der industriellen Umgebung in Bezug auf Malware (Schadsoftware). Sie benötigen einen Prozess, der präventive Maßnahmen, reaktive Maßnahmen und deren Verantwortlichen benennt. Entwickeln Sie ein Konzept für den Schutz vor Malware, das sowohl technische als auch organisatorische Regelungen vorgibt.

3.7 Benutzer und Rechtemanagement

Ein Benutzer und Rechtemanagement organisiert Rollen und die dazugehörigen Rechte, die Sie laut Tätigkeitsbeschreibung in der vorgesehenen Umgebung benötigen. Darunter fällt neben der Rollen-Erstellung die Zuordnung von Personen zu den Rollen über den gesamten Lebenszyklus.

Typische Aufgaben, die Sie beachten, sind das Erstellen, Verändern, Monitoren und der Entzug von Rechten. Diese Aufgaben sind in einem Prozess abzubilden, der die Identifikation von Personen und Entities regelt und die Zuweisung von Rechten autorisiert.

3.8 Anforderungen an die Dokumentation

Halten Sie sicherheitsrelevante Informationen fest. Organisieren Sie die Lenkung dieser Dokumente. Diese Dokumente dienen im Falle eines Security-Ereignisses als Nachweis für die Einhaltung der Security-Prozesse.

4 Sichere Konfiguration

4.1 Inbetriebnahme

4.1.1 Bedrohungen

Im Auslieferungszustand ist Ihr Gerät für einen einfachen Start vorbereitet. Für einen sicheren Betrieb des Switches sind darüber hinaus weitere Konfigurationseinstellungen notwendig. Durch den Anwendungsfall Installation ergeben sich folgende Bedrohungen:

- ☐ Manipulation der Konfiguration
- ☐ Auslesen der Konfiguration
- ☐ Beeinträchtigung der Verfügbarkeit

4.1.2 Security Quick Check „Inbetriebnahme“

Benötigen Sie?	Wenn notwendig	Wenn nicht notwendig
DHCP	Einschalten von DHCP (Client)	Ausschalten von DHCP (Client)
BOOTP	Einschalten von BOOTP	Ausschalten von BOOTP
PROFINET	Einschalten von PROFINET	Ausschalten von PROFINET
EtherNet/IP	Einschalten von EtherNet/IP	Ausschalten von EtherNet/IP
LLDP	Einschalten von LLDP	Ausschalten von LLDP
AutoConfiguration Adapter (ACA)	ACA beim booten nicht überspringen	ACA beim booten überspringen
Grundprinzip		
Die Maßnahmen folgen dem Minimalprinzip, um die Systemlast des Switches und dessen Angriffsfläche zu reduzieren. Schalten Sie nicht benötigte Dienste generell ab.		

Benötigen Sie?	Wenn notwendig	Wenn nicht notwendig
Allgemeine Maßnahmen		
Lesender Zugriff für HiDiscovery Änderung der Default-Zugänge Deaktivierung Passwort-Sync		

4.1.3 Maßnahmen

Einschalten von DHCP (Client)

Der Switch kann über einen DHCP Server dynamisch IP Informationen, als auch einen TFTP Server für Konfigurationen erhalten. Ein Angreifer kann diesen Service missbrauchen.

Für eine höhere Verfügbarkeit wählen Sie für Infrastrukturkomponenten eine statische IP-Konfiguration. Dynamische IP-Konfigurationen erfordern das Vorhandensein von Protokollen, die für Angreifer ein Ziel darstellen.

Aktion	Default Wert	Empfohlener Wert	Vorhanden		Weitere Information
DHCP Client aktivieren	An	Aktivieren Sie DHCP ausschließlich, wenn Sie eine dynamische Adressvergabe für Ihre Infrastrukturkomponenten benötigen	L2B	Ja	GUI L2B Netz CLI L2B network protocol
			L2E	Ja	GUI L2E Netz CLI L2E network protocol
			L2P	Ja	GUI L2P Netz CLI L2P network protocol
			L3E	Ja	GUI L3E Netz CLI L3E network protocol
			L3P	Ja	GUI L3P Netz CLI L3P network protocol

Einschalten von BOOTP

Der Switch kann über einen BOOTP-Server dynamisch IP Informationen, als auch einen TFTP Server für Konfigurationen erhalten. Ein Angreifer kann diesen Service missbrauchen.

Für eine höhere Verfügbarkeit wählen Sie für Infrastrukturkomponenten eine statische IP-Konfiguration. Dynamische IP-Konfigurationen erfordern das Vorhandensein von Protokollen, die für Angreifer ein Ziel darstellen.

Aktion	Default Wert	Empfohlener Wert	Vorhanden		Weitere Information
BOOTP aktivieren	Aus	Aktivieren Sie BOOTP ausschließlich, wenn Sie eine dynamische Adressvergabe für Ihre Infrastrukturkomponenten benötigen	L2B	Ja	GUI L2B Netz CLI L2B network protocol
			L2E	Ja	GUI L2E Netz CLI L2E network protocol
			L2P	Ja	GUI L2P Netz CLI L2P network protocol
			L3E	Ja	GUI L3E Netz CLI L3E network protocol
			L3P	Ja	GUI L3P Netz CLI L3P network protocol

Einschalten von PROFINET

Über PROFINET ist es möglich bestimmte Eigenschaften des Switches auszulesen und zu ändern. Schalten Sie diese Option ausschließlich ein, wenn Sie PROFINET benötigen.

Aktion	Default Wert	Empfohlener Wert	Vorhanden		Weitere Information
PROFINET aktivieren	Aus	Schalten Sie PROFINET ein, falls das Protokoll zum Einsatz kommen soll	L2B	Nein	
			L2E	Ja	GUI L2E PROFINET IO CLI L2E profinetio
			L2P	Ja	GUI L2P PROFINET IO CLI L2P profinetio
			L3E	Ja	GUI L3E PROFINET IO CLI L3E profinetio
			L3P	Ja	GUI L3P PROFINET IO CLI L3P profinetio

Einschalten von EtherNet/IP

Über EtherNet/IP ist es möglich bestimmte Eigenschaften des Switches auszulesen und zu ändern. Schalten Sie diese Option ausschließlich ein, wenn Sie EtherNet/IP benötigen.

Aktion	Default Wert	Empfohlener Wert	Vorhanden		Weitere Information
EtherNet/IP aktivieren	Aus	Schalten Sie EtherNet/IP ein, falls das Protokoll zum Einsatz kommen soll	L2B	Nein	
			L2E	Ja	GUI L2E EtherNet/IP CLI L2E ethernet-ip
			L2P	Ja	GUI L2P EtherNet/IP CLI L2P ethernet-ip
			L3E	Ja	GUI L3E EtherNet/IP CLI L3E ethernet-ip
			L3P	Ja	GUI L3P EtherNet/IP CLI L3P ethernet-ip

Einschalten von LLDP

Über das Link Layer Discovery Protocol sendet der Switch regelmäßig Informationen über sich in das Netz. Diese Informationen können für die Fehlersuche eine wichtige Hilfe darstellen. Allerdings liefern diese Informationen auch einem Angreifer wertvolle Hinweise und sollten daher ausschließlich wenn unbedingt notwendig genutzt werden.

LLDP-Med ist eine Erweiterung von LLDP. Es ist primär für Voice over IP Anwendungen gedacht und sollte wenn möglich immer ausgeschaltet bleiben.

Aktion	Default Wert	Empfohlener Wert	Vorhanden		Weitere Information
LLDP aktivieren	Ein	LLDP gibt Informationen über Ihren Switch preis. Ausschließlich im Bedarfsfall benutzen.	L2B	Ja	GUI L2B Topologie-Erkennung CLI L2B lldp
			L2E	Ja	GUI L2E Topologie-Erkennung CLI L2E lldp
			L2P	Ja	GUI L2P Topologie-Erkennung CLI L2P lldp
			L3E	Ja	GUI L3E Topologie-Erkennung CLI L3E lldp
			L3P	Ja	GUI L3P Topologie-Erkennung CLI L3P lldp

ACA beim booten nicht überspringen

Das Gerät kann die Konfiguration während des Bootvorganges vom ACA laden. Kommt in Ihrer Umgebung der ACA zum Einsatz, dann behandeln Sie diesen Vorgang mit dem CLI-Befehl (siehe Tabelle unten).

Aktion	Default Wert	Empfohlener Wert	Vorhanden		Weitere Information
ACA nicht überspringen	Aus	Kommt der ACA zum Einsatz, kann hiermit das Gerät die Konfiguration beim Booten laden.	L2B	Nein	
			L2E	Ja	CLI L2E skip-aca-on-boot
			L2P	Ja	CLI L2P skip-aca-on-boot
			L3E	Ja	CLI L3E skip-aca-on-boot
			L3P	Ja	CLI L3P skip-aca-on-boot

Ausschalten von DHCP (Client)

Anmerkung: Der Switch kann über einen DHCP-Server dynamisch IP-Informationen, als auch einen TFTP Server für Konfigurationen erhalten. Die DHCP-Server-Antwort wiederum kann einen Pfad auf eine Remote-Konfiguration enthalten. Dann lädt der Switch beim Booten die Konfiguration über TFTP.

Ein Angreifer kann diesen Service missbrauchen.

Für eine höhere Verfügbarkeit wählen Sie für Infrastrukturkomponenten eine statische IP-Konfiguration. Dynamische IP-Konfigurationen erfordern das Vorhandensein von Protokollen, die für Angreifer ein Ziel darstellen.

Aktion	Default Wert	Empfohlener Wert	Vorhanden		Weitere Information
DHCP-Client deaktivieren	An	Aus	L2B	Ja	GUI L2B Netz CLI L2B network protocol
			L2E	Ja	GUI L2E Netz CLI L2E network protocol
			L2P	Ja	GUI L2P Netz CLI L2P network protocol
			L3E	Ja	GUI L3E Netz CLI L3E network protocol
			L3P	Ja	GUI L3P Netz CLI L3P network protocol

Ausschalten von BOOTP

Anmerkung: Der Switch kann über einen BOOTP-Server dynamisch IP-Informationen, als auch einen TFTP Server für Konfigurationen erhalten. Die BOOTP-Server-Antwort wiederum kann einen Pfad auf eine Remote-Konfiguration enthalten. Dann lädt der Switch beim Booten die Konfiguration über TFTP.

Ein Angreifer kann diesen Service missbrauchen.

Für eine höhere Verfügbarkeit wählen Sie für Infrastrukturkomponenten eine statische IP-Konfiguration. Dynamische IP-Konfigurationen erfordern das Vorhandensein von Protokollen, die für Angreifer ein Ziel darstellen.

Aktion	Default Wert	Empfohlener Wert	Vorhanden		Weitere Information
BOOTP deaktivieren	Aus	Aus	L2B	Ja	GUI L2B Netz CLI L2B network protocol
			L2E	Ja	GUI L2E Netz CLI L2E network protocol
			L2P	Ja	GUI L2P Netz CLI L2P network protocol
			L3E	Ja	GUI L3E Netz CLI L3E network protocol
			L3P	Ja	GUI L3P Netz CLI L3P network protocol

Ausschalten von PROFINET

Über PROFINET ist es möglich bestimmte Eigenschaften des Switches auszulesen und zu ändern. Schalten Sie diese Option ausschließlich ein, wenn Sie PROFINET benötigen.

Aktion	Default Wert	Empfohlener Wert	Vorhanden		Weitere Information
PROFINET deaktivieren	Aus	Aus	L2B	Nein	
			L2E	Ja	GUI L2E PROFINET IO CLI L2E profinetio
			L2P	Ja	GUI L2P PROFINET IO CLI L2P profinetio
			L3E	Ja	GUI L3E PROFINET IO CLI L3E profinetio
			L3P	Ja	GUI L3P PROFINET IO CLI L3P profinetio

Ausschalten von EtherNet/IP

Über EtherNet/IP ist es möglich bestimmte Eigenschaften des Switches auszulesen und zu ändern. Schalten Sie diese Option ausschließlich ein, wenn Sie EtherNet/IP benötigen.

Aktion	Default Wert	Empfohlener Wert	Vorhanden		Weitere Information
EtherNet/IP deaktivieren	aus	aus	L2B	Nein	
			L2E	Ja	GUI L2E EtherNet/IP CLI L2E ethernet-ip
			L2P	Ja	GUI L2P EtherNet/IP CLI L2P ethernet-ip
			L3E	Ja	GUI L3E EtherNet/IP CLI L3E ethernet-ip
			L3P	Ja	GUI L3P EtherNet/IP CLI L3P ethernet-ip

Ausschalten von LLDP

Über das Link Layer Discovery Protocol (LLDP) sendet der Switch regelmäßig Informationen über sich in das Netz. Diese Informationen können für die Fehlersuche eine wichtige Hilfe darstellen. Allerdings liefern diese Informationen auch einem Angreifer wertvolle Hinweise.

Aktion	Default Wert	Empfohlener Wert	Vorhanden		Weitere Information
LLDP deaktivieren	Ein	Aus	L2B	Ja	GUI L2B Topologie-Erkennung CLI L2B lldp
			L2E	Ja	GUI L2E Topologie-Erkennung CLI L2E lldp
			L2P	Ja	GUI L2P Topologie-Erkennung CLI L2P lldp
			L3E	Ja	GUI L3E Topologie-Erkennung CLI L3E lldp
			L3P	Ja	GUI L3P Topologie-Erkennung CLI L3P lldp

Aktion	Default Wert	Empfohlener Wert	Vorhanden		Weitere Information
LLDP-MED deaktivieren	Ein	Aus	L2B	Nein	
			L2E	Nein	
			L2P	Ja	GUI L2P LLDP-MED CLI L2P lldp med
			L3E	Ja	GUI L3E LLDP-MED CLI L3E lldp med
			L3P	Ja	GUI L3P LLDP-MED CLI L3P lldp med

Anmerkung: PROFINET benötigt LLDP für den Betrieb.

ACA beim booten überspringen

Wenn Sie keinen ACA einsetzen, können Sie hiermit den Bootvorgang beschleunigen und das unberechtigte Laden einer Konfiguration beim Starten erschweren.

Aktion	Default Wert	Empfohlener Wert	Vorhanden		Weitere Information
ACA überspringen	Aus	ein	L2B	Nein	
			L2E	Ja	CLI L2E skip-aca-on-boot
			L2P	Ja	CLI L2P skip-aca-on-boot
			L3E	Ja	CLI L3E skip-aca-on-boot
			L3P	Ja	CLI L3P skip-aca-on-boot

Lesender Zugriff für HiDiscovery

HiDiscovery gibt Informationen über ein Gerät preis (Lesemodus) oder erlaubt auch die Änderung von Konfigurationsparametern wie etwa der IP-Adresse (Lese/Schreibmodus). Ein Angreifer hat die Möglichkeit, Informationen über ein Gerät zu sammeln oder auch Datenverkehr umzuleiten, indem er das Default Gateway auf ein System unter seiner Kontrolle umleitet. Die Empfehlung lautet deshalb, HiDiscovery im produktiven Umfeld ausschließlich lesenden Zugriff zu erlauben.

Aktion	Default Wert	Empfohlener Wert	Vorhanden		Weitere Information
HiDiscovery Lesezugriff	An (lesend und schreibend)	Aus (lesend)	L2B	Ja	GUI L2B Netz CLI L2B network protocol
			L2E	Ja	GUI L2E Netz CLI L2E network protocol
			L2P	Ja	GUI L2P Netz CLI L2P network protocol
			L3E	Ja	GUI L3E Netz CLI L3E network protocol
			L3P	Ja	GUI L3P Netz CLI L3P network protocol

Änderung der Default-Zugänge

Eine der 1. Maßnahmen, die ein Angreifer unternimmt, wenn er Zugriff auf ein fremdes System erlangen möchte, ist der Login-Versuch mit Standard-Zugangsdaten. Ändern Sie deshalb die Zugangsdaten bei der Installation.

Anmerkung: Das Ändern des Passworts im CLI ändert ausschließlich das SNMP v1/v2 Passwort. Bei Änderung des Benutzer-Passworts im CLI werden im Gegensatz dazu das Benutzer-Passwort und die SNMP v1/v2 Passwörter geändert. Soll für Benutzer und SNMP v1/v2 jeweils ein eigenes Passwort verwendet werden, deaktivieren Sie die Funktion „Passwort-Sync“.
Siehe „Deaktivierung Passwort-Sync” auf Seite 37.

Aktion	Default Wert	Empfohlener Wert	Vorhanden		Weitere Information
Passwort setzen	User: admin=private user= public	Sicheres Passwort mit 16 Zeichen	L2B	Ja	GUI L2B Passwort / SNMP v3-Zugriff CLI L2B users passwd
			L2E	Ja	GUI L2E Passwort / SNMP v3-Zugriff CLI L2E users passwd
			L2P	Ja	GUI L2P Passwort / SNMP v3-Zugriff CLI L2P users passwd
			L3E	Ja	GUI L3E Passwort / SNMP v3-Zugriff CLI L3E users passwd
			L3P	Ja	GUI L3P Passwort / SNMP v3-Zugriff CLI L3P users passwd

Anmerkung: Durch die Standardeinstellungen wird das Benutzerpasswort mit der SNMP v1/v2 Community abgeglichen.

Deaktivierung Passwort-Sync

Damit für unterschiedliche Benutzer und SNMP-Zugriffsberechtigungen unterschiedliche Passwörter vergeben werden können, deaktivieren Sie die Funktion Passwort-Sync.

Aktion	Default Wert	Empfohlener Wert	Vorhanden		Weitere Information
Passwort Sync ausschalten	An	Aus	L2B	Ja	GUI L2B Passwort / SNMP v3-Zugriff CLI L2B users passwd
			L2E	Ja	GUI L2E Passwort / SNMP v3-Zugriff CLI L2E users passwd
			L2P	Ja	GUI L2P Passwort / SNMP v3-Zugriff CLI L2P users passwd
			L3E	Ja	GUI L3E Passwort / SNMP v3-Zugriff CLI L3E users passwd
			L3P	Ja	GUI L3P Passwort / SNMP v3-Zugriff CLI L3P users passwd

4.2 Trennung von Netzen

4.2.1 Bedrohungen

Trennung von Netzen oder Netzsegmenten ist ein wesentlicher Aspekt von Netzsicherheit. Damit können zum Beispiel verschiedene Vertraulichkeitsklassen abgebildet werden. Für eine sichere Netztrennung bestehende folgende Bedrohungen:

- ☐ Port Fehlkonfiguration
- ☐ VLAN Fehlkonfiguration
- ☐ ACL Fehlkonfiguration
- ☐ Überwindung von VLAN Grenzen
- ☐ ARP-Flooding
- ☐ Vortäuschen einer Identität

Beim Einsatz der Layer-3 Software (Routing) entstehen zusätzlich weitere Bedrohungen:

- ☐ Manipulation VRRP/HiVRRP Protokoll
- ☐ Manipulation Routing durch gefälschte Router Discovery Pakete
- ☐ Manipulation Routing durch gefälschte RIPv1 oder RIPv2 Pakete
- ☐ Manipulation der Routing-Wege durch Proxy-ARP Pakete
- ☐ Gefahr der Fehlkonfiguration durch mehrere IP-Subnetze auf dem gleichen Subnetz (Multinetting)
- ☐ Preisgabe der Netzinfrastruktur durch Router Discovery Pakete

Alle genannten Bedrohungen zielen darauf ab, die Trennung der Netze oder Netzsegmente untereinander zu überwinden oder die Kommunikationswege zwischen Netzsegmenten (Layer-2 und Layer-3) zu manipulieren.

4.2.2 Security Quick Check „Trennung von Netzen“

Diese Tabelle gibt Ihnen eine Hilfestellung, welche Maßnahmen in Ihrer Einsatzumgebung im Zusammenhang mit der Trennung von Netzen aus Sicherheitsgründen auf dem Switch idealerweise umgesetzt werden sollten.

Benötigen Sie?	Wenn notwendig	Wenn nicht notwendig
VLANs	Keine Nutzung von VLAN 1 Keine Nutzung von VLAN 0 GVRP ausschalten Ports nicht in mehr als einem VLAN Eindeutige Zuordnung der Switch Ports zu VLANs Keine Verwendung von Port-Mirroring Keine Verwendung von DHCP-Relay	GVRP ausschalten
Routing zwischen Subnetzen notwendig?	Routing einschalten Proxy-ARP ausschalten	Routing ausschalten
Dynamisches Routing-Protokoll RIP notwendig?	RIPv2 mit Authentifizierung nutzen	Ausschließlich statische Routen nutzen Ggf.Nutzung von OSPF ausschließlich mit verschlüsselter Authentifizierung
Dynamisches Routing-Protokoll OSPF notwendig?	Nutzung von OSPF ausschließlich mit verschlüsselter Authentifizierung Ggf.Nutzung von OSPF virtual links ausschließlich mit Authentifizierung	Ausschließlich statische Routen nutzen Ggf.RIPv2 mit Authentifizierung nutzen
Unterschiedliche Sicherheitszonen an den angeschlossenen Netzen vorhanden?	Verwendung von IP Access Control Lists (ACLs)	
Dynamische Multicast-Registrierung mit GMRP	Aktivierung Generic Multicast Registration Protocol (GMRP)	Deaktivierung Generic Multicast Registration Protocol (GMRP)
Grundprinzip		
Schalten Sie Dienste, und Funktionen, die Sie nicht benötigen aus		
Zusätzliche Maßnahmen		
Treffen Sie zur Erhöhung der Security alle Maßnahmen aus dem Abschnitt „Administrationszugriff“, da ein Angreifer mit einem solchen Zugriff alle hier beschrieben Maßnahmen außer Kraft setzen kann.		

4.2.3 Maßnahmen

Keine Nutzung von VLAN 1

Nutzen Sie das VLAN 1 ausschließlich für das HIPER-Ring Protokoll und Ringkopplung. Diese Maßnahme erschwert die Manipulation der Ringprotokolle. Nehmen Sie daher folgende Einstellungen vor:

Aktion	Default Wert	Empfohlener Wert	Vorhanden		Weitere Information
Admin-Interface auf anders VLAN verlagern	1	Im Bereich 2-4042	L2B	Nein	
			L2E	Ja	GUI L2E VLAN CLI L2E network mgmt_vlan
			L2P	Ja	GUI L2P VLAN CLI L2P network mgmt_vlan
			L3E	Ja	GUI L3E VLAN CLI L3E network mgmt_vlan
			L3P	Ja	GUI L3PE VLAN CLI L3P network mgmt_vlan
Zeitserver-Konfiguration auf anderes VLAN umstellen	1	Gleiches VLAN wie für Admin-Interface	L2B	Nein	
			L2E	Ja	GUI L2E SNTP-Konfiguration CLI L2E sntp anycast vlan
			L2P	Ja	GUI L2P SNTP-Konfiguration CLI L2P sntp anycast vlan
			L3E	Ja	GUI L3E SNTP-Konfiguration CLI L3E sntp anycast vlan
			L3P	Ja	GUI L3P SNTP-Konfiguration CLI L3P sntp anycast vlan
Alle Switch-Ports von VLAN1 in anderes VLAN umstellen	1	Im Bereich 2-4042	L2B	Nein	
			L2E	Ja	GUI L2E VLAN Statisch CLI L2E vlan port pvid all
			L2P	Ja	GUI L2P VLAN Statisch CLI L2P vlan port pvid all
			L3E	Ja	GUI L3E VLAN Statisch CLI L3E vlan port pvid all
			L3P	Ja	GUI L3P VLAN Statisch CLI L3P vlan port pvid all

Anmerkung: Für die Ports, über die das HIPER-Ring Protokoll läuft und für Ports für Ring-/Netzkopplungen muss der Port auf VLAN 1 verbleiben, da sonst Funktionsprobleme auftreten.

Anmerkung: Wenn Sie das VLAN für das Management-Interface ändern, dann kann dies Ihre Verbindung zum Switch unterbrechen. Tragen Sie Sorge dafür, dass Sie auch mit der neuen Konfiguration den Switch administrieren können.

Anmerkung: Die VLANs 4043-4095 werden für port-basiertes Routing intern im Switch genutzt, um intern die Trennung der maximal möglichen 52 physikalischen Ports im Switch umzusetzen und dürfen daher nicht durch den Anwender benutzt werden. Bei port-basiertem Routing ist das Ingress Filtering aktiv. Daher verwirft der Switch Pakete mit VLAN-Tags.

Keine Nutzung von VLAN 0

Das VLAN 0 nimmt im Switch eine weitere Sonderrolle ein und ist daher zu betrachten.

Anmerkung: Bei der Nutzung von PROFINET und GOOSE können sich Einschränkungen ergeben.

Aktion	Default Wert	Empfohlener Wert	Vorhanden		Weitere Information
VLAN0 Transparent-Modus deaktivieren	Aus	Aus	L2B	Nein	
			L2E	Ja	GUI L2E VLAN Global CLI L2E vlan0-transparent-mode
			L2P	Ja	GUI L2P VLAN Global CLI L2P vlan0-transparent-mode
			L3E	Ja	GUI L3E VLAN Global CLI L3E vlan0-transparent-mode
			L3P	Ja	GUI L3P VLAN Global CLI L3P vlan0-transparent-mode

GVRP ausschalten

GVRP (GARP VLAN Registration Protocol) erlaubt einem anderen Gerät, in einem Switch ein VLAN anzulegen bzw. einen Port in einem VLAN zu registrieren. Für die Netztrennung zwischen VLANs stellt der Switch eine Sicherheitskomponente dar. Damit kein anderes Gerät die VLAN-Konfiguration verändern kann, schalten Sie GVRP aus.

Aktion	Default Wert	Empfohlener Wert	Vorhanden		Weitere Information
VLAN participation konfigurieren	auto	include oder exclude	L2B	Nein	
			L2E	Ja	GUI L2E VLAN Port CLI L2E vlan participation
			L2P	Ja	GUI L2P VLAN Port CLI L2P vlan participation
			L3E	Ja	GUI L3E VLAN Port CLI L3E vlan participation
			L3P	Ja	GUI L3P VLAN Port CLI L3P vlan participation

Anmerkung: Wenn GVRP trotzdem genutzt werden soll, deaktivieren Sie GVRP auf allen nicht vertrauenswürdigen Ports.

Ports nicht in mehr als einem VLAN

Der Switch bietet Ihnen die Möglichkeit, einem Port mehrere VLANs zuzuordnen. Das hebt eine Trennung zwischen den VLANs teilweise auf. Daher ordnen Sie jedem Switch-Port (User-Port) genau einem VLAN zu (Einstellung U = untagged oder T = tagged).

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
Zuordnung zu genau einem VLAN	- : kein Mitglied aber GVRP erlaubt	Bei Benutzung entweder U oder T	L2B	Nein	
			L2E	Ja	GUI L2E VLAN Port CLI L2E vlan
			L2P	Ja	GUI L2P VLAN Port CLI L2P vlan
			L3E	Ja	GUI L3E VLAN Port CLI L3E vlan
			L3P	Ja	GUI L3P VLAN Port CLI L3P vlan

Eindeutige Zuordnung der Switch Ports zu VLANs

Die Trennung der VLANs untereinander hängt wesentlich von der Einstellung der Ports (- = kein Mitglied, T = tagged, U = untagged und F = forbidden) ab. Generell sollte als Grundeinstellung für jeden Port in jedem VLAN F = forbidden sein. D. h. beim Anlegen eines neuen VLANs sollte jeder Port in diesem VLAN zunächst auf F (kein Mitglied und GVRP verboten) eingestellt und ausschließlich bei Bedarf genau einem VLAN zugeordnet werden.

Konfigurieren Sie den Switch so, dass beim Empfang eines Pakets ohne VLAN Tag an einem Port dieses Paket im Switch nicht einem anderen VLAN zugeordnet wird.

Aktion	Default Wert	Empfohlener Wert	Vorhanden		Weitere Information
Switch Port per Default auf F stellen	- : kein Mitglied aber GVRP erlaubt	Wenn GVRP deaktiviert ist, reicht - = kein Mitglied, ansonsten F = forbidden als Default-Einstellung, Zuordnung dann zu einem VLAN nach Bedarf	L2B	Nein	
			L2E	Ja	GUI L2E VLAN Statisch CLI L2E vlan participation
			L2P	Ja	GUI L2P VLAN Statisch CLI L2P vlan participation
			L3E	Ja	GUI L3E VLAN Statisch CLI L3E vlan participation
			L3P	ja	GUI L3P VLAN Statisch CLI L3P vlan participation
Untagged Frames VLAN zuordnen	1	Gleiches VLAN, wie für diesen Port aktiviert wurde	L2B	Nein	
			L2E	Ja	GUI L2E VLAN Statisch CLI L2E vlan tagging
			L2P	Ja	GUI L2P VLAN Statisch CLI L2P vlan tagging
			L3E	Ja	GUI L3E VLAN Statisch CLI L3E vlan tagging
			L3P	Ja	GUI L3P VLAN Statisch CLI L3P vlan tagging

Aktion	Default Wert	Empfohlener Wert	Vorhanden		Weitere Information
tagged Frames ausschließlich an T-Port erlauben	admitAll	Bei Ports die mit T=tagged konfiguriert sind: admitOnlyVlanTagged	L2B	Nein	
			L2E	Ja	GUI L2E VLAN Port CLI L2E vlan acceptframe
			L2P	Ja	GUI L2P VLAN Port CLI L2P vlan acceptframe
			L3E	Ja	GUI L3E VLAN Port CLI L3E vlan acceptframe
			L3P	Ja	GUI L3P VLAN Port CLI L3P vlan acceptframe
VLAN Tags auswerten (Ingress Filtering)	aus	ein	L2B	Nein	
			L2E	Ja	GUI L2E VLAN Port CLI L2E vlan ingressfilter
			L2P	Ja	GUI L2P VLAN Port CLI L2P vlan ingressfilter
			L3E	Ja	GUI L3E VLAN Port CLI L3E vlan ingressfilter
			L3P	Ja	GUI L3P VLAN Port CLI L3P vlan ingressfilter

Anmerkung: Die Protokolle IGMP (ab L2E) und GMRP (ab L2P) arbeiten ohne VLAN Tags. IGMP Anfragen werden auf allen Ports geflutet, unabhängig von dessen VLAN-Zuordnung.

Anmerkung: Wenn portbasiertes Routing aktiviert wurde, ist auch Ingress-Filtering aktiviert.

Eigene Spanning-Tree-Instanz je VLAN

Durch manipulierte Spanning-Tree-Pakete kann die Netzstruktur beeinflusst werden. Zudem kann nicht ausgeschlossen werden, dass bestimmte Spanning-Tree-Pakete (BPDUs) über Switch und VLAN-Grenzen hinweg transportiert werden und somit Wege für ein fortgeschrittenes Angriffsszenario öffnet.

Die Nutzung einer eigenen Spanning-Tree-Instanz je VLAN schafft hier eine bessere Trennung.

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
MSTP konfigurieren	Aus	An	L2B	Nein	
			L2E	Nein	
			L2P	Ja	GUI L2P MSTP (Multiple Spanning Tree) CLI L2P spanning-tree mst
			L3E	Nein	GUI L3E MSTP (Multiple Spanning Tree) CLI L3E spanning-tree mst
			L3P	Ja	GUI L3P MSTP (Multiple Spanning Tree) CLI L3P spanning-tree mst

Keine Verwendung von Port-Mirroring

Durch das Spiegeln des Netzverkehrs von einem oder mehreren Ports auf einen Ziel-Port (Port-Mirroring) kann Verkehr aus anderen Netzsegmenten mitgelesen werden. Dies kann die Vertraulichkeit dieses Netzsegments gefährden.

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
Kein Port-Mirroring	Aus	Aus	L2B	Ja	GUI L2B Port Mirroring CLI L2B monitor session
			L2E	Ja	GUI L2E Port Mirroring CLI L2E monitor session
			L2P	Ja	GUI L2P Port Mirroring CLI L2P monitor session
			L3E	Ja	GUI L3E Port Mirroring CLI L3E monitor session
			L3P	Ja	GUI L3P Port Mirroring CLI L3P monitor session

Keine Verwendung von DHCP-Relay

Die DHCP Relay Funktion bietet die Möglichkeit, einem Switch an einem bestimmten Switch-Port über die DHCP Option 82 eine definierte IP Adresse zuzuweisen. Diese Funktion kann dazu genutzt werden, einem Gerät an einem bestimmten Switch-Port immer die gleiche IP-Adresse zuzuordnen und Sie das Gerät damit besser verwalten können. Wenn Sie diese Funktion nicht nutzen, schalten Sie diese Option aus.

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
Keine DHCP Server-IP-Adressen konfigurieren	0.0.0.0 (disabled) für alle 4 möglichen Servereinträge	0.0.0.0 (disabled) für alle 4 möglichen Servereinträge	L2B	Ja	GUI L2B DHCP-Relay-Agent CLI L2B dhcp-relay
			L2E	Ja	GUI L2E DHCP-Relay-Agent CLI L2E dhcp-relay
			L2P	Ja	GUI L2P DHCP-Relay-Agent CLI L2P dhcp-relay
			L3E	Ja	GUI L3E DHCP-Relay-Agent CLI L3E dhcp-relay
			L3P	Ja	GUI L3P DHCP-Relay-Agent CLI L3P dhcp-relay

Routing einschalten

Wenn der Switch als Router arbeiten soll, schalten Sie das Routing ein.

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
Routing global einschalten	Aus	Ein	L2B	Nein	
			L2E	Nein	
			L2P	Nein	
			L3E	Ja	GUI L3E Routing Global CLI L3E Routing Commands
			L3P	Ja	GUI L3P Routing Global CLI L3P Routing Commands

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
Routing auf notwendigen Ports einschalten	Aus	Ein	L2B	Nein	
			L2E	Nein	
			L2P	Nein	
			L3E	Ja	GUI L3E Router-Interfaces konfigurieren CLI L3E routing
			L3P	Ja	GUI L3P Router-Interfaces konfigurieren CLI L3P routing

Routing ausschalten

Falls der Switch kein Routing zwischen Layer-3 Subnetzen durchführen soll, schalten Sie die Routing-Funktion komplett aus.

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
Routing global ausschalten	Aus	Aus (default)	L2B	Nein	
			L2E	Nein	
			L2P	Nein	
			L3E	Ja	GUI L3E Routing Global CLI L3E Routing Commands
			L3P	Ja	GUI L3P Routing Global CLI L3P Routing Commands

Proxy-ARP ausschalten

Die Proxy-ARP-Funktion erlaubt Endgeräten über das, als Router arbeitende, Gerät zu kommunizieren, ohne dass sie die notwendigen Routing-Einträge besitzen. Allerdings gelingt so z.B. unberechtigt angeschlossenen Geräten die Kommunikation über den Router hinweg in alle Subnetze, die der Router kennt. Deaktivieren Sie daher Proxy-ARP.

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
Proxy-ARP auf jedem Port ausschalten	Aus	Aus (default)	L2B	Nein	
			L2E	Nein	
			L2P	Nein	
			L3E	Ja	GUI L3E Router-Interfaces konfigurieren CLI L3E ip proxy-arp
			L3P	Ja	GUI L3P Router-Interfaces konfigurieren CLI L3P ip proxy-arp

Net-Directed Broadcasts ausschalten

Net-Directed Broadcasts bieten die Möglichkeit, Broadcasts über den Router hinweg in andere Subnetze zu senden. Dieses Verhalten kann für Angriffe auf die Verfügbarkeit (Denial of Service DoS) verwendet werden. Deaktivieren Sie daher diese Funktion. Im RFC 2644 „Changing the Default for Directed Broadcasts in Routers“ ist definiert, dass das voreingestellte Verhalten von Routern so sein sollte, dass Directed Broadcasts als Default nicht weitergeleitet werden.

Anmerkung: All Net-DirectedBroadcasts (255.255.255.255) werden verworfen.

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
Net- Directed Broadcasts ausschalten	Aus	Aus (default)	L2B	Nein	
			L2E	Nein	
			L2P	Nein	
			L3E	Ja	GUI L3E Router-Interfaces konfigurieren CLI L3E ip netdirbcast
			L3P	Ja	GUI L3P Router-Interfaces konfigurieren CLI L3P ip netdirbcast

ARP gezieltes Lernen aktivieren

In der Grundeinstellung lernt der Router alle MAC-Adressen, die er an seinen Ports sieht und behält diese Adressen für 1.200 Sekunden (= 20 Minuten) im Speicher, bevor er sie wieder bei sich löscht. Durch den Versand gefälschter Pakete mit ungültigen oder nicht vorhandenen MAC-Adressen kann die Tabelle am Router überlaufen und so die Verfügbarkeit oder Integrität (Man in the Middle Angriff) beeinträchtigt werden. Daher sollte der Router ausschließlich MAC-Adressen in seine Tabelle aufnehmen, die er explizit angefragt hat.

Anmerkung: Wird diese Option aktiviert, dauert das 1. Paket einer Verbindung wegen des dann notwendigen ARP-Requests etwas länger.

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
ARP gezieltes Lernen aktivieren	Aus	Ein	L2B	Nein	
			L2E	Nein	
			L2P	Nein	
			L3E	Ja	GUI L3E ARP-Parameter einstellen CLI L3E arp selective-learning
			L3P	Ja	GUI L3P ARP-Parameter einstellen CLI L3P arp selective-learning

Bekannte Einschränkungen:

Der 1. Verbindungsaufbau eines Geräts über den Router könnte geringfügig länger dauern.

Router Discovery deaktivieren

Router-Advertisement kann für eine Reihe von Angriffen auf die IT-Sicherheit verwendet werden. Dabei ist die Problemstelle nicht der Router selbst, sondern die Endgeräte, die auf solche Advertisement-Pakete reagieren und die Pakete dann an (vorgegaukelte) Router schicken. Diese können dann den Verkehr mitlesen oder verfälschen und an den richtigen Router weiterleiten oder den Verkehr verwerfen (Denial of Service).

Daher sollte generell auf ICMP-Router-Advertisement (Router und Endgeräte) verzichtet werden.

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
Router discovery deaktivieren	Aus	Aus	L2B	Nein	
			L2E	Nein	
			L2P	Nein	
			L3E	Ja	GUI L3E Konfiguration Router-Discovery CLI L3E ip irdp
			L3P	Ja	GUI L3P Konfiguration Router-Discovery CLI L3P ip irdp

RIPv2 mit Authentifizierung nutzen

Wenn ein Anwendungsfall die Nutzung eines dynamischen Routing-Protokolls erfordert, nutzen Sie ausschließlich RIP v2 mit MD5-Authentifizierung. Damit können Sie verhindern, dass ein Angreifer ohne Authentifizierung die Routingwege manipuliert durch gefälschte RIP v1-Pakete oder RIP v2-Pakete. Folgen könnten mitlesen, verfälschen oder unterdrücken von Netzverkehr sein.

Bekannte Einschränkung:

Die Verwendung von RIPv2 kann einige Angriffe über das Routing-Protokoll erschweren, bietet aber eine weitere Schutzebene.

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
RIP aktivieren	Aus	Ein	L2B	Nein	
			L2E	Nein	
			L2P	Nein	
			L3E	Ja	GUI L3E RIP CLI L3E ip rip
			L3P	Ja	GUI L3P RIP CLI L3P ip rip
RIP Sendeversion einstellen	ripVersion2	ripVersion2 (default)	L2B	Nein	
			L2E	Nein	
			L2P	Nein	
			L3E	Ja	GUI L3E RIP CLI L3E ip rip send version
			L3P	Ja	GUI L3P RIP CLI L3P ip rip send version
Authentifizierung einstellen	noAuthentication	md5	L2B	Nein	
			L2E	Nein	
			L2P	Nein	
			L3E	Ja	GUI L3E RIP CLI L3E ip rip authentication
			L3P	Ja	GUI L3PE RIP CLI L3P ip rip authentication

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
Schlüssel eingeben	<leer>	Sicheres Passwort mit 16 Zeichen	L2B	Nein	
			L2E	Nein	
			L2P	Nein	
			L3E	Ja	GUI L3E RIP CLI L3E ip rip authentication
			L3P	Ja	GUI L3P RIP CLI L3P ip rip authentication
Schlüssel-ID festlegen	0	Gemeinsame ID wie die anderen Router, mit denen dieser Router kommuniziert	L2B	Nein	
			L2E	Nein	
			L2P	Nein	
			L3E	Ja	GUI L3E RIP CLI L3E ip rip authentication
			L3P	Ja	GUI L3P RIP CLI L3P ip rip authentication

Ausschließlich statische Routen nutzen

Falls die Anwendung kein dynamisches Routing-Protokoll erfordert, nutzen Sie ausschließlich statische Routen. Um mögliche Angriffe über Routing-Protokolle zu verhindern, deaktivieren Sie alle Funktionen dieser Protokolle.

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
RIP ausschalten	Aus	Aus (default)	L2B	Nein	
			L2E	Nein	
			L2P	Nein	
			L3E	Ja	GUI L3E RIP CLI L3E ip rip
			L3P	Ja	GUI L3P RIP CLI L3P ip rip

Nutzung von OSPF ausschließlich mit verschlüsselter Authentifizierung

Bei der Verwendung von OSPF als Routing-Protkoll sollten sich die Router gegenseitig authentifizieren. Dies erschwert einem Angreifer, Routing-Informationen im Netz durch selbst eingeschleuste oder gefälschte Routing-Pakete zu verändern.

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
OSPF Authentifizierung aktivieren	none	encrypt	L2B	Nein	
			L2E	Nein	
			L2P	Nein	
			L3E	Nein	
			L3P	Ja	CLI L3P ip ospf authentication

Nutzung von OSPF virtual links ausschließlich mit Authentifizierung

Sollen für OSPF Routing virtual Links verwendet werden, sollten diese authentifiziert werden, um die Manipulation der Routing-Informationen im Netz zu erschweren.

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
Für OSPF virtual Links Authentifizierung einschalten	Aus	Aus (default)	L2B	Nein	
			L2E	Nein	
			L2P	Nein	
			L3E	Nein	
			L3P	Ja	CLI L3P area virtual-link

Verwendung von IP Access Control Lists (ACLs)

Bei der Kopplung verschiedener Layer-3 Netze über einen Switch mit Layer-3 Software (L3E oder L3P) konfigurieren Sie zur Absicherung gegen unberechtigte Zugriffe zwischen den Netzen auf den Switch Access Control Lists (ACLs). Damit kann der Verkehr anhand von IP-Adressen, IP-Protokollen oder Portnummern eingeschränkt werden.

Damit ist ohne eine spezielle Firewall bereits eine Grundabsicherung möglich.

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
Verwendung von IP ACLs	Aus	Aus (default)	L2B	Nein	
			L2E	Nein	
			L2P	Nein	
			L3E	Ja	CLI L3E QoS IP ACL
			L3P	Ja	CLI L3P Qos IP ACL

Aktivierung Generic Multicast Registration Protocol (GMRP)

Das GMRP Protokoll bietet einem Client die Möglichkeit, sich selbst in eine Multicast-Gruppe auf Layer-2 einzutragen. Schalten Sie dieses Protokoll ausschließlich ein, wenn Sie es wirklich benötigen.

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
Deaktivierung von GMRP	Aus	Ein	L2B	Nein	
			L2E	Nein	
			L2P	Ja	GUI Switching GMRP CLI set gmrp adminmode
			L3E	Ja	GUI Switching GMRP CLI set gmrp adminmode
			L3P	Ja	GUI Switching GMRP CLI set gmrp adminmode

Deaktivierung Generic Multicast Registration Protocol (GMRP)

Das GMRP Protokoll bietet einem Client die Möglichkeit, sich selbst in eine Multicast-Gruppe auf Layer-2 einzutragen. Deaktivieren Sie dieses Protokoll, wenn Sie es nicht unbedingt benötigen.

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
Deaktivierung von GMRP	Aus	Aus (default)	L2B	Nein	
			L2E	Nein	
			L2P	Ja	GUI Switching GMRP CLI no set gmrp admin-mode
			L3E	Ja	GUI Switching GMRP CLI no set gmrp admin-mode
			L3P	Ja	GUI Switching GMRP CLI no set gmrp admin-mode

4.3 Administrativer Zugriff

4.3.1 Bedrohungen

Über den gesamten Lebenszyklus eines Switches ist ein schreibender Zugriff auf den Switch notwendig.

Daraus ergeben sich folgende Bedrohungen:
- ☐ Identitätsdiebstahl
- ☐ Ausweitung der Rechte
- ☐ Manipulation der Konfiguration
- ☐ Konfigurationsfehler

Sie können Bedrohungen mit folgenden Konfigurationspunkten entgegenwirken:

Beachten Sie die Vertraulichkeit und Integrität des Administrationszugriffs. Setzen Sie gesicherte Verbindungen für die Administration ein. Die Switching Plattform bietet je nach Software Version folgende Möglichkeiten, welche die Sicherheit erhöhen:
- ☐ SNMP v3
- ☐ SSH

Der Administrationszugriff über telnet und SNMP v1/v2 bietet keinen Schutz bezüglich Vertraulichkeit und Integrität. Die genannten Protokolle sind als unsicher eingestuft, da Informationen im Klartext übertragen werden und das Abhören und Manipulieren nicht verhindert werden kann.

Der Switch bietet auch die Möglichkeit der Konfiguration über die Webschnittstelle. Dabei wird eine Java Anwendung geladen und die eigentliche Kommunikation erfolgt über SNMP v3 – einschließlich der Anmeldung. Diese Anwendung wird über HTTP ausgeliefert. Hat ein Angreifer Zugriff zum Netz kann er die Login Seite fälschen und Zugangsdaten abgreifen.

Der nachfolgende Abschnitt „Security Quick Check „Administrationszugriff“" auf Seite 57 dient dazu, ausschließlich Dienste auszuwählen, die benötigt werden. Dies verringert die Last und verkleinert die Angriffsfläche. Verwenden Sie für die Übermittlung von Anmeldungsdaten und Konfigurationsparametern ausschließlich verschlüsselte Verbindungen.

4.3.2 Security Quick Check „Administrationszugriff“

Diese Tabelle gibt Ihnen eine Hilfestellung, welche Maßnahmen Sie in Ihrer Einsatzumgebung im Zusammenhang mit Administrationszugriffen auf den Switch idealerweise umsetzen sollen.

Benötigen Sie?	Wenn notwendig	Wenn nicht notwendig
GUI	Konfiguration von SNMP v3 Schreibzugriff	Abschalten von HTTP und HTTPS
CLI Remote	Einschalten von SSH	Abschalten von SSH
	Abschalten von Telnet	Abschalten von Telnet
CLI Seriell	Zeitüberschreitung serielles CLI	Zeitüberschreitung serielles CLI
Zentrales Management	Konfiguration von SNMP v3 Schreibzugriff	Abschalten von SNMP v1/2
	Abschalten von SNMP v1/2	Siehe auchEinschränkung SNMP-Lesezugriff auf bestimmte IP-Adressen
Grundprinzip		

Tab. 1: Security Quick Check „Administrationszugriff“

Benötigen Sie?	Wenn notwendig	Wenn nicht notwendig
Die Maßnahmen folgen dem Minimalprinzip, um die Systemlast des Switches und dessen Angriffsfläche zu reduzieren. Schalten Sie nicht benötigte Dienste generell ab.		
Allgemeine Maßnahmen		
Unabhängig von der Art des Administrationszugriffs treffen Sie folgende Maßnahmen zur Erhöhung der Security: ☐ Einschränkung der Administration auf IP-Adressbereiche ☐ Konfiguration der zentralen Benutzerverwaltung mittels RADIUS ☐ M3.14 Sperren eines Benutzers		

Tab. 1: Security Quick Check „Administrationszugriff“

4.3.3 Maßnahmen

Konfiguration von SNMP v3 Schreibzugriff

Ziehen Sie SNMP v3 den Versionen 1 und 2 vor, da die Version 1 und 2 Passwörter, die der Authentifizierung dienen, im Klartext übertragen. Gleiches gilt für den Austausch der Daten.

Als Verschlüsselungsverfahren kommt DES (Data Encryption Standard) zum Einsatz. SHA1 (Secure Hash Algorithm) Hashes dienen dem Integritätsschutz.

Anmerkung: DES gilt als schwaches Verschlüsselungsverfahren. Ändern Sie deshalb regelmäßig in kurzen Abständen die Schlüssel.

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
Benutzer anlegen	-	Verwenden Sie eindeutige Benutzer	L2B	Ja	CLI L2B users name
			L2E	Ja	CLI L2E users name
			L2P	Ja	CLI L2P users name
			L3E	Ja	CLI L3E users name
			L3P	Ja	CLI L3P users name

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
Schreibrechte für Benutzer festlegen	-	Readwrite	L2B	Ja	CLI L2B users access
			L2E	Ja	CLI L2E users access
			L2P	Ja	CLI L2P users access
			L3E	Ja	CLI L3E users access
			L3P	Ja	CLI L3P users access
Passwort setzen	-	Sicheres Passwort mit 16 Zeichen	L2B	Ja	CLI L2B users passwd
			L2E	Ja	CLI L2E users passwd
			L2P	Ja	CLI L2P users passwd
			L3E	Ja	CLI L3E users passwd
			L3P	Ja	CLI L3P users passwd
SNMP v3 Zugriff erteilen	-	Readwrite	L2B	Ja	CLI L2B users SNMP v3 accessmode
			L2E	Ja	CLI L2E users SNMP v3 accessmode
			L2P	Ja	CLI L2P users SNMP v3 accessmode
			L3E	Ja	CLI L3E users SNMP v3 accessmode
			L3P	Ja	CLI L3P users 3 access-mode
SNMP v3 Authentifizierung	-	SHA	L2B	Ja	CLI L2B users SNMP v3 authentication
			L2E	Ja	CLI L2E users SNMP v3 authentication
			L2P	Ja	CLI L2P users SNMP v3 authentication
			L3E	Ja	CLI L3E users SNMP v3 authentication
			L3P	Ja	CLI L3P users SNMP v3 authentication
SNMP v3 Verschlüsselung	-	DES Schlüssel mit einer Länge von 16 Zeichen	L2B	Nein	
			L2E	Nein	
			L2P	Ja	CLI L2P users SNMP v3 encryption
			L3E	Ja	CLI L3E users SNMP v3 encryption
			L3P	Ja	CLI L3P users SNMP v3 encryption

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
SNMP v3 Verschlüsselung erzwingen	aus	An	L2B	Nein	
			L2E	Nein	
			L2P	Ja	CLI L2P users SNMP v3 encryption
			L3E	Ja	CLI L3E users SNMP v3 encryption
			L3P	Ja	CLI L3P users SNMP v3 encryption

Anmerkung: Kann keine Verschlüsselung aktiviert werden, werden alle Nachrichten im Klartext übertragen.

Einschalten von SSH

SSH bietet Integrität und Vertraulichkeit. Telnet dagegen kann dies nicht gewährleisten, da sowohl die Anmeldung, also auch die eigentliche Kommunikation im Klartext übermittelt wird.

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
SSH-Key übertragen	-	Ausschließlich in vertrauenswürdigen Netzen benutzen	L2B	Nein	
			L2E	Nein	
			L2P	Ja	Defekte Geräte ersetzen
			L3E	Ja	
			L3P	Ja	Basic L3P SSH-Zugriff vorbereiten
SSH-Server anschalten	An	An	L2B	Nein	
			L2E	Nein	
			L2P	Ja	GUI L2P Beschreibung SSH-Zugriff CLI L2P network mgmt-access modify
			L3E	Ja	GUI L3E Beschreibung SSH-Zugriff CLI L3E network mgmt-access modify
			L3P	Ja	GUI L3P Beschreibung SSH-Zugriff CLI L3P network mgmt-access modify

Zeitüberschreitung serielles CLI

Verbessern Sie den Zugangschutz zum CLI durch ein Passwort. Wird das CLI nicht benutzt, wird der Benutzer automatisch ausgeloggt. Dies schützt vor unberechtigtem Zugriff.

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
Zeitüberschreitung einstellen	5 (Minuten)	5 (Minuten)	L2B	Ja	CLI L2B serial timeout
			L2E	Ja	CLI L2E serial timeout
			L2P	Ja	CLI L2P serial timeout
			L3E	Ja	CLI L3E serial timeout
			L3P	Ja	CLI L3P serial timeout

Abschalten von HTTP und HTTPS

Bekannte Einschränkungen:

HTTP und HTTPS können ausschließlich gemeinsam deaktiviert werden.

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
http- und HTTPS-Server abschalten	An	Wird kein Webzugriff benötigt HTTP und HTTPS abschalten	L2B	Ja	GUI L2B Web-Zugriff CLI L2B ip http server
			L2E	Ja	GUI L2E Telnet-/Web-Zugriff CLI L2E ip http server
			L2P	Ja	GUI L2P Telnet-/Web-/SSH-Zugriff CLI L2P ip http server
			L3E	Ja	GUI L3E Telnet-/Web-/SSH-Zugriff CLI L3E ip http server
			L3P	Ja	GUI L3P Telnet-/Web-/SSH-Zugriff CLI L3P ip http server

Abschalten von SNMP v1/2

Bei SNMP v1/v2 dient die Community als Passwort und wird unverschlüsselt übertragen. Sollten Sie keinen externen Zugriff benötigen, schalten Sie SNMP v1/2 ab oder beschränken Sie SNMP v1/2 zumindest auf einen lesenden Zugriff.

Aktion	Default Wert	Empfohlener Wert	Vorhanden		Weitere Information
SNMP v1/2 Server abschalten	An	Aus	L2B	Nein	
			L2E	Ja	GUI L2E SNMP v1/v2-Zugriffs-Einstellungen CLI L2E snmp-access version
			L2P	Ja	GUI L2P SNMP v1/v2-Zugriffs-Einstellungen CLI L2P snmp-access version
			L3E	Ja	GUI L3E SNMP v1/v2-Zugriffs-Einstellungen CLI L3E snmp-access version
			L3P	Ja	GUI L3P SNMP v1/v2-Zugriffs-Einstellungen CLI L3P snmp-access version

Abschalten von Telnet

Telnet überträgt die Daten unverschlüsselt über das Netz und sollte daher nicht benutzt werden.

Bekannte Einschränkung:

Wenn der Telnet-Dienst deaktiviert wurde, funktioniert das Command Line Interface (CLI) in der Web-Oberfläche nicht mehr.

Aktion	Default Wert	Empfohlener Wert	Vorhanden		Weitere Information
telnet-Server abschalten	An	Aus	L2B	Nein	
			L2E	Ja	GUI L2E Telnet-/Web-Zugriff CLI L2E telnet
			L2P	Ja	GUI L2P Telnet-/Web-/SSH-Zugriff CLI L2P telnet
			L3E	Ja	GUI L3E Telnet-/Web-/SSH-Zugriff CLI L3E telnet
			L3P	Ja	GUI L3P Telnet-/Web-/SSH-Zugriff CLI L3P telnet

Anmerkung: Ruft ein Benutzer den Telnet-Dienst über die Webschnittstelle mit HTTP oder HTTPS auf, so werden die Zugangsdaten trotzdem im Klartext übertragen.

Abschalten von SSH

Aktion	Default Wert	Empfohlener Wert	Vorhanden		Weitere Information
SSH-Server abschalten	Aus	wird kein Remote Zugriff auf die Konsole benötigt abschalten	L2B	Nein	
			L2E	Nein	
			L2P	Ja	GUI L2P Telnet-/Web-/SSH-Zugriff CLI L2P network mgmt-access modify
			L3E	Ja	GUI L3E Telnet-/Web-/SSH-Zugriff CLI L3E network mgmt-access modify
			L3P	Ja	GUI L3P Telnet-/Web-/SSH-Zugriff CLI L3P network mgmt-access modify

Anlegen eines lesenden Zugangs

Vermeiden Sie aus folgenden Gründen grundsätzlich die Verwendung des Standardbenutzers „user“:

- ☐ Der Benutzername ist öffentlich bekannt und vereinfacht somit deutlich einen Angriff durch Erraten des Passworts.
- ☐ Aktionen auf dem Switch können keinem Benutzer zugeordnet werden (Nachvollziehbarkeit von Konfigurationsänderungen)

Legen Sie daher für jeden Mitarbeiter einen eigenen Account an.

Aktion	Default Wert	Empfohlener Wert	Vorhanden		Weitere Information
Benutzer anlegen	-	Verwenden Sie eindeutige Benutzer	L2B	Nein	
			L2E	Nein	GUI L2E Passwort / SNMP v3-Zugriff CLI L2E users name
			L2P	Ja	GUI L2P Passwort / SNMP v3-Zugriff CLI L2P users name
			L3E	Ja	GUI L3E Passwort / SNMP v3-Zugriff CLI L3E users name
			L3P	Ja	GUI L3P Passwort / SNMP v3-Zugriff CLI L3P users name

Aktion	Default Wert	Empfohlener Wert	Vorhanden		Weitere Information
Schreibrechte für Benutzer festlegen	-	Readonly	L2B	Nein	
			L2E	Nein	GUI L2E Passwort / SNMP v3-Zugriff CLI L2E users access
			L2P	Ja	GUI L2P Passwort / SNMP v3-Zugriff CLI L2P users access
			L3E	Ja	GUI L3E Passwort / SNMP v3-Zugriff CLI L3E users access
			L3P	Ja	GUI L3P Passwort / SNMP v3-Zugriff CLI L3P users access
Passwort setzen	-	Sicheres Passwort mit 16 Zeichen	L2B	Nein	
			L2E	Ja	GUI L2E Passwort / SNMP v3-Zugriff CLI L2E users passwd
			L2P	Ja	GUI L2P Passwort / SNMP v3-Zugriff CLI L2P users passwd
			L3E	Ja	GUI L3E Passwort / SNMP v3-Zugriff CLI L3E users passwd
			L3P	Ja	GUI L3P Passwort / SNMP v3-Zugriff CLI L3P users passwd

Anlegen eines schreibenden Zugangs

Aktion	Default Wert	Empfohlener Wert	Vorhanden		Weitere Information
Benutzer anlegen	-	Verwenden Sie eindeutige Benutzer	L2B	Ja	GUI L2B Passwort / SNMP v3-Zugriff CLI L2B users name
			L2E	Ja	GUI L2E Passwort / SNMP v3-Zugriff CLI L2E users name
			L2P	Ja	GUI L2P Passwort / SNMP v3-Zugriff CLI L2P users name
			L3E	Ja	GUI L3E Passwort / SNMP v3-Zugriff CLI L3E users name
			L3P	Ja	GUI L3P Passwort / SNMP v3-Zugriff CLI L3P users name
Schreibrechte für Benutzer festlegen	-	readwrite	L2B	Ja	GUI L2B Passwort / SNMP v3-Zugriff CLI L2B users access
			L2E	Ja	GUI L2E Passwort / SNMP v3-Zugriff CLI L2E users access
			L2P	Ja	GUI L2P Passwort / SNMP v3-Zugriff CLI L2P users access
			L3E	Ja	GUI L3E Passwort / SNMP v3-Zugriff CLI L3E users access
			L3P	Ja	GUI L3P Passwort / SNMP v3-Zugriff CLI L3P users access
Passwort setzen	-	Sicheres Passwort mit 16 Zeichen	L2B	Ja	GUI L2B Passwort / SNMP v3-ZugriffCLI L2B users passwd
			L2E	Ja	GUI L2E Passwort / SNMP v3-Zugriff CLI L2E users passwd
			L2P	Ja	GUI L2P Passwort / SNMP v3-Zugriff CLI L2P users passwd
			L3E	Ja	GUI L3E Passwort / SNMP v3-Zugriff CLI L3E users passwd
			L3P	Ja	GUI L3P Passwort / SNMP v3-Zugriff CLI L3P users passwd

Einschränkung der Administration auf IP-Adressbereiche

Beschränken Sie die Administration des Switches nicht nur bezüglich der Dienste, sondern auch der Netze aus denen zugegriffen werden kann.

Aktion	Default Wert	Empfohlener Wert	Vorhanden		Weitere Information
restricted management access (RMA) einschalten	-	An	L2B	Nein	
			L2E	Ja	L2E Eingeschränkter Management-Zugriff CLI L2E network mgmt-access operation
			L2P	Ja	L2P Eingeschränkter Management-Zugriff CLI L2P network mgmt-access operation
			L3E	Ja	L3E Eingeschränkter Management-Zugriff CLI L3E network mgmt-access operation
			L3P	Ja	L3P Eingeschränkter Management-Zugriff CLI L3P network mgmt-access operation
RMA hinzufügen	-	bis zu 16 RMAs können angelegt werden	L2B	Nein	
			L2E	Ja	L2E Eingeschränkter Management-Zugriff CLI L2E network mgmt-access add
			L2P	Ja	L2P Eingeschränkter Management-Zugriff CLI L2P network mgmt-access add
			L3E	Ja	L3E Eingeschränkter Management-Zugriff CLI L3E network mgmt-access add
			L3P	Ja	L3P Eingeschränkter Management-Zugriff CLI L3P network mgmt-access add

Aktion	Default Wert	Empfohlener Wert	Vorhanden		Weitere Information
(RMA) konfigurieren	-	Erfordert die Anwendung ein Protokoll laut „Security Quick Check“ nicht, deaktivieren Sie es global. Erfordert die Anwendung ein Protokoll, dann aktivieren Sie es für das Management Netz	L2B	Nein	
			L2E	Ja	L2E Eingeschränkter Management-Zugriff CLI L2E network mgmt-access modify
			L2P	Ja	L2P Eingeschränkter Management-Zugriff CLI L2P network mgmt-access modify
			L3E	Ja	L3E Eingeschränkter Management-Zugriff CLI L3E network mgmt-access modify
			L3P	Ja	L3P Eingeschränkter Management-Zugriff CLI L3P network mgmt-access modify

Konfiguration der zentralen Benutzerverwaltung mittels RADIUS

Die lokale Verwaltung von Benutzern und deren Passwörtern auf dem Switchen stößt bei größeren Netzen an Grenzen, wenn es darum geht, Passwörter zu ändern, neue Benutzer anzulegen oder Benutzer zu löschen.

Daher ist eine zentrale Benutzerverwaltung auf RADIUS-Servern angeraten.

Bekannte Einschränkungen:

Falls die RADIUS-Server nicht mehr erreichbar sind, ist kein Login auf dem Switch mit einem „RADIUS“-Benutzer mehr möglich. Hier sollte dieses Szenario mit berücksichtigt werden. Es ist immer empfehlenswert, einen Notzugangsbenutzer direkt auf dem Switch anzulegen, dessen Passwort sicher zu verwahren und im Notfall mit diesem Benutzer auf den Switch zuzugreifen. Danach ist dieses Passwort zu ändern.

Aktion	Default Wert	Empfohlener Wert	Vorhanden		Weitere Information
Radius Server konfigurieren	radius server host {auth | acct} <ipaddr> [<port>]	“auth” konfiguriert einen Authentifizierungsserver	L2B	Nein	
			L2E	Nein	
			L2P	Ja	GUI L2P RADIUS-Server-Einstellungen für IEEE 802.1X CLI L2P radius server host
			L3E	Ja	GUI L3E RADIUS-Server-Einstellungen für IEEE 802.1X CLI L3E radius server host
			L3P	Ja	GUI L3P RADIUS-Server-Einstellungen für IEEE 802.1X CLI L3P radius server host

Aktion	Default Wert	Empfohlener Wert	Vorhanden		Weitere Information
Shared secret konfigurieren	-	Vergeben Sie ein Shared secret mit 20 Zeichen	L2B	Nein	
			L2E	Nein	
			L2P	Ja	GUI L2P RADIUS-Server-Einstellungen für IEEE 802.1X CLI L2P radius server key
			L3E	Ja	GUI L3E RADIUS-Server-Einstellungen für IEEE 802.1X CLI L3E radius server key
			L3P	Ja	GUI L3P RADIUS-Server-Einstellungen für IEEE 802.1X CLI L3P radius server key
Authentifizierungsliste für RADIUS anlegen	authentication login <list-name> [method1 [method2 [method3]]]	Method muss „radius“ sein	L2B	Nein	
			L2E	Nein	
			L2P	Ja	GUI L2P IEEE 802.1X-Port-Authentifizierung CLI L2P authentication login
			L3E	Ja	GUI L3E IEEE 802.1X-Port-Authentifizierung CLI L3E authentication login
			L3P	Ja	GUI L3P IEEE 802.1X-Port-Authentifizierung CLI L3P authentication login
Benutzer Anlagen und RADIUS Authentifizierung zuordnen	keiner	users login <user> <list-name>	L2B	Nein	
			L2E	Nein	
			L2P	Ja	CLI L2P users login
			L3E	Ja	CLI L3E users login
			L3P	Ja	CLI L3P users login

4.4 Überwachung

4.4.1 Bedrohungen

Für die Nachvollziehbarkeit von durchgeführten Aktionen sowie die Sicherstellung des fehlerfreien Zustandes des Switches ist eine Überwachung notwendig. Kommt mehr als ein Switch zum Einsatz, ist eine zentrale Überwachung empfehlenswert. Dokumentieren Sie nachvollziehbar Konfigurationsänderungen durch geeignetes Logging. Daraus ergeben sich folgende Bedrohungen:

- ☐ Verlust der Verfügbarkeit, Vertraulichkeit und Integrität durch
- ☐ Konfigurationsfehler
- ☐ Manipulation der Konfiguration
- ☐ Hard- und Software-Fehler

Die Informationen, die ein Switch an die zentrale Überwachungssoftware schickt, können je nach Konfiguration gezielt unterdrückt, geändert oder abgehört werden. Dadurch kann die Vertraulichkeit und Integrität verletzt werden.

4.4.2 Security Quick Check „Überwachung“

Kontrollfrage	Wenn notwendig	Wenn nicht notwendig
Ist die Verfügbarkeit des Netzes wichtig?	Aktivierung von SNMP v1/v2-Lesezugriff	Deaktivierung von SNMP v1/v2
	Aktivierung von SNMP v3-Lesezugriff	Deaktivierung von SNMP v1/v2
	Vergabe sichererer SNMP-Passwörter (Communities)	
	Einschränkung SNMP-Lesezugriff auf bestimmte IP-Adressen	Versand von SNMP Traps
	Versand von SNMP Traps	
	Vergabe sichererer SNMP-Passwörter (Communities)	
	Alarm bei speziellen Fehlern konfigurieren	
	Aktivierung Port-Monitor	
Bestehen (rechtliche) Vorgaben, um Veränderungen an der Konfiguration zu protokollieren?	Zentrale Protokollierung SNMP-Write Zugriffe per Syslog Aktivierung PTP Zeitsynchronisation SNTP-Broadcasts nicht akzeptieren	Deaktivierung zentrale Protokollierung SNMP-Write Zugriffe per Syslog (Default-Einstellung)
Soll ein Sicherheitsvorfall aufgeklärt werden können?	M4.8 oder 4.12 (Zeitsynchronisation) Zentrale Protokollierung per Syslog	Das ist keine Option für sicherheitsrelevante Anwendungen, falls kein Syslog-Server zur Verfügung steht Deaktivierung Syslog
Steht eine SNTP Zeitquelle im Netz zur Verfügung?	Aktivierung und Konfiguration SNTP Client Deaktivierung SNTP Client Deaktivierung PTP Zeitsynchronisation	Deaktivierung PTP Zeitsynchronisation
Steht eine PTP-Zeitquelle im Netz zur Verfügung?	Deaktivierung SNTP Client Ausschalten SNTP-Server Aktivierung PTP Zeitsynchronisation	Aktivierung und Konfiguration SNTP Client Ausschalten SNTP-Server SNTP-Broadcasts nicht akzeptieren
Geräteüberwachung mit Meldekontakt geplant?	Gerätestatus mit Meldekontakt überwachen	
Ist eine Umgebung vorhanden, mit der der Gerätezustand über PROFINET überwacht werden kann?	PROFINET einschalten	PROFINET ausschalten (siehe auch Ausschalten von PROFINET)
Wird VRRP oder HiVRRP eingesetzt?	Versand von SNMP-Traps bei Nutzung von VRRP/HiVRRP	

Tab. 2: Security Quick Check „Überwachung“

Kontrollfrage	Wenn notwendig	Wenn nicht notwendig
Grundprinzipien		
Zentrale Überwachung/ zentrales Monitoring Nachvollziehbarkeit von Änderungen der Konfiguration Gemeinsame Zeit auf allen Systemen Zentrales Logging		
Generell zu treffende Maßnahmen		
☐ Konfiguration Switch-Name ☐ Konfiguration System-Prompt ☐ Konfiguration Switch-Standort und -ansprechpartner		

Tab. 2: Security Quick Check „Überwachung“ (Forts.)

Bekannte Einschränkungen:

- ☐ Die Logdaten können derzeit ausschließlich unverschlüsselt und per UDP Protokoll (möglicher Paketverlust und Gefahr von gefälschten Log-Daten) übertragen werden.
- ☐ Syslog verwendet als Quell-Port den Port 514. Dies erschwert die Stateful Inspection des Verkehrs auf einer Firewall.
- ☐ SNMP v3 (verschlüsselt) ist derzeit ausschließlich in der Professional Software-Variante verfügbar.

4.4.3 Maßnahmen

Sie können den Bedrohungen mit folgenden Konfigurationspunkten entgegenwirken:

Aktivierung von SNMP v1/v2-Lesezugriff

Durch Aktivierung des SNMP v1/v2 Lesezugriffs erhält Netzmanagement-Software ohne SNMP v3 Unterstützung die Möglichkeit, neben der Erreichbarkeit des Switches mittels Ping auch systeminterne Werte, wie z. B. Temperatur oder Status der Netzteile auszulesen.

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
SNMP v1/v2 Lesezugriff aktivieren	SNMP v1 ein SNMP v2 ein	SNMP v1 ein SNMP v2 ein	L2B	Ja	GUI L2B SNMP v1/v2-Zugriffs-Einstellungen CLI L2B snmp-access version
			L2E	Ja	GUI L2E SNMP v1/v2-Zugriffs-Einstellungen CLI L2E snmp-access version
			L2P	Ja	GUI L2P SNMP v1/v2-Zugriffs-Einstellungen CLI L2P snmp-access version
			L3E	Ja	GUI L3E SNMP v1/v2-Zugriffs-Einstellungen CLI L3E snmp-access version
			L3P	Ja	GUI L3P SNMP v1/v2-Zugriffs-Einstellungen CLI L3P snmp-access version

Aktivierung von SNMP v3-Lesezugriff

Durch Aktivierung des SNMP v3 Lesezugriffs erhält eine Netzmanagement-Software die Möglichkeit, neben der Erreichbarkeit des Switches mittels Ping auch systeminterne Werte, wie z. B. Temperatur oder Status der Netzteile auszulesen. SNMP v3 ist im Gegensatz zu den Versionen 1 und 2 verschlüsselt und daher zu bevorzugen.

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
SNMP v3 Lesezugriff aktivieren	Ein	Ein	L2B	Ja	GUI L2B Passwort / SNMP v3-Zugriff CLI L2B users SNMP v3 accessmode
			L2E	Ja	GUI L2E Passwort / SNMP v3-Zugriff CLI L2E users SNMP v3 accessmode
			L2P	Ja	GUI L2P Passwort / SNMP v3-Zugriff CLI L2P users SNMP v3 accessmode
			L3E	Ja	GUI L3E Passwort / SNMP v3-Zugriff CLI L3E users SNMP v3 accessmode
			L3P	Ja	GUI L3P Passwort / SNMP v3-Zugriff CLI L3P users SNMP v3 accessmode

Vergabe sichererer SNMP-Passwörter (Communities)

Für das Auslesen und das Schreiben von Werten mit SNMP v1 und v2 wird als Authentifizierung ein so genannter Community-String (eine Art Passwort) verwendet. Die voreingestellten Werte sind allgemein bekannte Standardwerte und daher in keiner Weise als sicher anzusehen. Ändern Sie diese Werte.

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
Vergabe sichererer SNMP-Passwörter	„public“ und „private“	Community-String mit einer Länge von 16 Zeichen	L2B	Ja	GUI L2B SNMP v1/v2-Zugriffs-Einstellungen CLI L2B snmp-server community
			L2E	Ja	GUI L2E SNMP v1/v2-Zugriffs-Einstellungen CLI L2E snmp-server community
			L2P	Ja	GUI L2P SNMP v1/v2-Zugriffs-Einstellungen CLI L2P snmp-server community
			L3E	Ja	GUI L3E SNMP v1/v2-Zugriffs-Einstellungen CLI L3E snmp-server community
			L3P	Ja	GUI L3P SNMP v1/v2-Zugriffs-Einstellungen CLI L3P snmp-server community

Einschränkung SNMP-Lesezugriff auf bestimmte IP-Adressen

Der Zugriff mit SNMP erlaubt neben der Reglementierung mit dem Community-String auch die Reglementierung des Zugriffs auf eine IP-Adresse oder auf IP-Adressbereiche.

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
Einschränkung SNMP-Zugriff auf bestimmte IP-Adressen	0.0.0.0/0.0.0.0 (Zugriff von jeder Adresse aus erlaubt)	Adresse des Netzmanagements	L2B	Ja	GUI L2B SNMP v1/v2-Zugriffs-Einstellungen CLI L2B snmp-server community ipaddr
			L2E	Ja	GUI L2E SNMP v1/v2-Zugriffs-Einstellungen CLI L2E snmp-server community ipaddr
			L2P	Ja	GUI L2P SNMP v1/v2-Zugriffs-Einstellungen CLI L2P snmp-server community ipaddr
			L3E	Ja	GUI L3E SNMP v1/v2-Zugriffs-Einstellungen CLI L3E snmp-server community ipaddr
			L3P	Ja	GUI L3P SNMP v1/v2-Zugriffs-Einstellungen CLI L3P snmp-server community ipaddr

Deaktivierung von SNMP v1/v2

SNMP v1 und v2 erlauben keine verschlüsselte Datenübertragung. Zudem können Werte über den Switch und die daran angeschlossenen Geräte ausgelesen werden, die für die Vorbereitung oder Durchführung von Angriffen genutzt werden können.

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
Deaktivierung von SNMP v1/v2	v1und v2 aktiv	v1 und v2 aus	L2B	Ja	GUI L2B SNMP v1/v2-Zugriffs-Einstellungen CLI L2B snmp-access version
			L2E	Ja	GUI L2E SNMP v1/v2-Zugriffs-Einstellungen CLI L2E snmp-access version
			L2P	Ja	GUI L2P SNMP v1/v2-Zugriffs-Einstellungen CLI L2P snmp-access version
			L3E	Ja	GUI L3E SNMP v1/v2-Zugriffs-Einstellungen CLI L3E snmp-access version
			L3P	Ja	GUI L3P SNMP v1/v2-Zugriffs-Einstellungen CLI L3P snmp-access version

Versand von SNMP Traps

Neben dem Auslesen von Zustandsinformationen per SNMP-Lesezugriff bieten die Switche die Möglichkeit, Meldungen über Fehlerzustände per SNMP Traps (Benachrichtigen) an ein Netzmanagementsystem zu senden. Aktivieren Sie diese Funktion.

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
Versand von SNMP-Traps	Kein Trap-Ziel konfiguriert	Aktivierung aller vorhandenen Trap-Auslöser (z. B. Authentifizierung, Link Up/Down)	L2B	Ja	GUI L2B Alarme (Traps) CLI L2B snmp-server enable traps
			L2E	Ja	GUI L2E Alarme (Traps) CLI L2E snmp-server enable traps
			L2P	Ja	GUI L2P Alarme (Traps) CLI L2P snmp-server enable traps
			L3E	Ja	GUI L3E Alarme (Traps) CLI L3E snmp-server enable traps
			L3P	Ja	GUI L3P Alarme (Traps) CLI L3P snmp-server enable traps

Versand von SNMP Traps deaktivieren

Neben dem Auslesen von Zustandsinformationen per SNMP-Lesezugriff bieten die Switche die Möglichkeit, Meldungen über Fehlerzustände per SNMP-Traps (Benachrichtigen) an ein Netzmanagementsystem zu senden. Wenn kein Netzmanagement-System (zum Beispiel Industrial HiVision) im Einsatz ist, deaktivieren Sie diese Funktion, um keine unnötigen Informationen im Netz preis zu geben.

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
Versand von SNMP-Traps	Kein Trap-Ziel konfiguriert	Deaktivierung aller vorhandenen Trap-Auslöser (z. B. Authentifizierung, Link Up/Down)	L2B	Ja	GUI L2B Alarme (Traps) CLI L2B snmp-server enable traps
			L2E	Ja	GUI L2E Alarme (Traps) CLI L2E snmp-server enable traps
			L2P	Ja	GUI L2P Alarme (Traps) CLI L2P snmp-server enable traps
			L3E	Ja	GUI L3E Alarme (Traps) CLI L3E snmp-server enable traps
			L3P	Ja	GUI L3P Alarme (Traps) CLI L3P snmp-server enable traps

Aktivierung und Konfiguration SNTP Client

Bei allen SNMP-Traps und Logeinträgen spielt der Zeitpunkt der Meldung eine große Rolle. Besonders bei der Aufklärung eines Sicherheitsvorfalls hilft die exakte und identische Zeit auf allen Geräten. Synchronisieren Sie daher die Uhr des Switches dauerhaft mit einer zentralen Zeitquelle. Wenn ein 2. Zeit-Server verfügbar ist, dann konfigurieren Sie auch diesen.

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
Konfiguration SNTP-Client	Aus	Ein, mindestens ein SNTP-Server konfiguriert und getestet	L2B	Ja	GUI L2B SNTP-Konfiguration CLI L2B sntp client
			L2E	Ja	GUI L2E SNTP-Konfiguration CLI L2E sntp client
			L2P	Ja	GUI L2P SNTP-Konfiguration CLI L2P sntp client
			L3E	Ja	GUI L3E SNTP-Konfiguration CLI L3E sntp client
			L3P	Ja	GUI L3P SNTP-Konfiguration CLI L3P sntp client

Deaktivierung SNTP Client

Sollte keine Zeitquelle im Netz vorhanden sein, deaktivieren Sie den SNTP-Dienst. Deaktivieren Sie gleichermaßen den SNTP-Client bei der Nutzung von PTP.

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
Deaktivierung SNTP-Client	Aus	Aus (siehe Textbeschreibung oben)	L2B	Ja	GUI L2B SNTP-Konfiguration CLI L2B sntp operation
			L2E	Ja	GUI L2E SNTP-Konfiguration CLI L2E sntp operation
			L2P	Ja	GUI L2P SNTP-Konfiguration CLI L2P sntp operation
			L3E	Ja	GUI L3E SNTP-Konfiguration CLI L3E sntp operation
			L3P	Ja	GUI L3P SNTP-Konfiguration CLI L3P sntp operation

Ausschalten SNTP-Server

Jeder unnötig laufende Dienst auf dem Switch bietet eine Angriffsfläche. Deaktivieren Sie deshalb auch den SNTP-Serverdienst, wenn Sie den Switch nicht als SNTP-Server betreiben.

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
Konfiguration SNTP-Server	Ein (wenn SNTP aktiviert wurde)	aus	L2B	Ja	GUI L2B SNTP-Konfiguration CLI L2B sntp operation
			L2E	Ja	GUI L2E SNTP-Konfiguration CLI L2E sntp operation
			L2P	Ja	GUI L2P SNTP-Konfiguration CLI L2P sntp operation
			L3E	Ja	GUI L3E SNTP-Konfiguration CLI L3E sntp operation
			L3P	Ja	GUI L3P SNTP-Konfiguration CLI L3P sntp operation

SNTP-Broadcasts nicht akzeptieren

SNTP-Broadcasts können von beliebigen Geräten innerhalb des gleichen Subnetzes versendet werden. Das erlaubt die Manipulation der lokalen Uhrzeit im Switch. Zudem ist der Switch bei aktiviertem Empfang von SNTP-Broadcasts mit einem weiteren Dienst im Netz ansprechbar. Deaktivieren Sie deshalb den Empfang von SNTP Broadcasts.

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
SNTP Broadcasts nicht akzeptieren	Akzeptieren	Nicht akzeptieren	L2B	Ja	GUI L2B SNTP-Konfiguration CLI L2B sntp client accept-broadcast
			L2E	Ja	GUI L2E SNTP-Konfiguration CLI L2E sntp client accept-broadcast
			L2P	Ja	GUI L2P SNTP-Konfiguration CLI L2P sntp client accept-broadcast
			L3E	Ja	GUI L3E SNTP-Konfiguration CLI L3E sntp client accept-broadcast
			L3P	Ja	GUI L3P SNTP-Konfiguration CLI L3P sntp client accept-broadcast

Aktivierung PTP Zeitsynchronisation

Bei SNMP-Traps und Logeinträgen spielt der Zeitpunkt der Meldung eine große Rolle. Besonderes bei der Aufklärung eines Sicherheitsvorfalls hilft die exakte und identische Zeit auf allen Geräten. Synchronisieren Sie daher die Uhr des Switches dauerhaft mit einer zentralen Zeitquelle. Als Alternative zu SNTP steht mit PTP eine präzisere Variante zur Verfügung. Benutzen Sie die neuere Version 2 von PTP.

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
Einschalten PTP	Aus	Ein	L2B	Ja	GUI L2B PTP (IEEE 1588) CLI L2B lldp tlv ptp
			L2E	Ja	GUI L2E PTP (IEEE 1588) CLI L2E lldp tlv ptp
			L2P	Ja	GUI L2P PTP (IEEE 1588) CLI L2P lldp tlv ptp
			L3E	Ja	GUI L3E PTP (IEEE 1588) CLI L3E lldp tlv ptp
			L3P	Ja	GUI L3P PTP (IEEE 1588) CLI L3P lldp tlv ptp

Deaktivierung PTP Zeitsynchronisation

Wenn keine Zeit per PTP im Netz zur Verfügung steht oder die Zeit mit SNTP auf dem Switch synchronisiert wird, deaktivieren Sie PTP.

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
Ausschalten PTP	Aus	Aus (siehe Text oben)	L2B	Ja	GUI L2B PTP (IEEE 1588) CLI L2B lldp tlv ptp
			L2E	Ja	GUI L2E PTP (IEEE 1588) CLI L2E lldp tlv ptp
			L2P	Ja	GUI L2P PTP (IEEE 1588) CLI L2P lldp tlv ptp
			L3E	Ja	GUI L3E PTP (IEEE 1588) CLI L3E lldp tlv ptp
			L3P	Ja	GUI L3P PTP (IEEE 1588) CLI L3P lldp tlv ptp

Bekannte Einschränkungen:

- ☐ Derzeit steht keine Möglichkeit zur Verfügung, bei der Zeitsynchronisation die Kommunikationspartner zu authentifizieren (wie es z. B. bei NTPv3 mit MD5 Prüfsummen möglich wäre).

Zentrale Protokollierung per Syslog

Die zentrale Speicherung von Logmeldungen erlaubt eine schnellere Aufklärung von Sicherheitsvorfällen und eine schnellere Fehlersuche bei Betriebsstörungen. Zudem erschwert die Speicherung der Logdaten auf einem anderen System Manipulationsversuche der Logdaten.

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
Versand von Logeinträgen über Syslog einschalten	Aus	An	L2B	Nein	
			L2E	Ja	GUI L2E Syslog CLI L2E logging host
			L2P	Ja	GUI L2P Syslog CLI L2P logging host
			L3E	Ja	GUI L3E Syslog CLI L3E logging host
			L3P	Ja	GUI L3P Syslog CLI L3P logging host
Versand von Logeinträgen über Syslog zu mindestens einem Server einrichten und aktivieren	Kein Server definiert	Mindestens ein syslog Server, der als „aktiv“ konfiguriert ist	L2B	Nein	
			L2E	Ja	GUI L2E Syslog CLI L2E logging host
			L2P	Ja	GUI L2P Syslog CLI L2P logging host
			L3E	Ja	GUI L3E Syslog CLI L3E logging host
			L3P	Ja	GUI L3P Syslog CLI L3P logging host
Versand von Logeinträgen über Syslog mit „informational“ und höher	Debug	Informational	L2B	Nein	
			L2E	Ja	GUI L2E Syslog CLI L2E logging host
			L2P	Ja	GUI L2P Syslog CLI L2P logging host
			L3E	Ja	GUI L3E Syslog CLI L3E logging host
			L3P	Ja	GUI L3P Syslog CLI L3P logging host

Deaktivierung Syslog

Falls kein Syslog-Server zu Verfügung steht, schalten Sie den Versand von Logeinträgen über Syslog aus.

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
Syslog	Aus	Aus	L2B	Nein	
			L2E	Ja	GUI L2E Syslog CLI L2E logging host remove
			L2P	Ja	GUI L2P Syslog CLI L2P logging host remove
			L3E	Ja	GUI L3E Syslog CLI L3E logging snmp-requests set operation
			L3P	Ja	GUI L3P Syslog CLI L3P logging snmp-requests set operation

Zentrale Protokollierung SNMP-Write Zugriffe per Syslog

Um Änderungen oder Manipulationen an der Konfiguration des Switches nachvollziehen zu können, protokollieren Sie die SNMP-Schreibzugriffe und senden Sie die Logeinträge an den zentralen Syslog-Server.

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
SNMP Write Requests loggen	Aus	Ein, Schweregrad „informational“	L2B	Nein	
			L2E	Ja	GUI L2E Syslog CLI L2E logging snmp-requests set operation
			L2P	Ja	GUI L2P Syslog CLI L2P logging snmp-requests set operation
			L3E	Ja	GUI L3E Syslog CLI L3E logging snmp-requests set operation
			L3P	Ja	GUI L3P Syslog CLI L3P logging snmp-requests set operation

Deaktivierung zentrale Protokollierung SNMP-Write Zugriffe per Syslog

Wenn kein Syslog-Server vorhanden ist, deaktivieren Sie die Protokollierung von SNMP-Write-Zugriffen per Syslog.

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
SNMP Write Requests loggen	Aus	Aus	L2B	Nein	
			L2E	Ja	GUI L2E Syslog CLI L2E logging snmp-requests set operation
			L2P	Ja	GUI L2P Syslog CLI L2P logging snmp-requests set operation
			L3E	Ja	GUI L3E Syslog CLI L3E logging snmp-requests set operation
			L3P	Ja	GUI L3P Syslog CLI L3P logging snmp-requests set operation

Konfiguration Switch-Name

Um bei einer Installation mit mehr als einem Switch die Switche einfach unterscheiden zu können, geben Sie dem Switch einen Namen. Dies erleichtert auch die Identifikation des Switches in einem Netzmanagementsystem, das diesen Wert per SNMP auslesen kann.

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
Switchname konfigurieren	<Produkt>-<Teil der MAC-Adresse>	<Name>	L2B	Ja	GUI L2B System CLI L2B snmp-server sysname
			L2E	Ja	GUI L2E System CLI L2E snmp-server sysname
			L2P	Ja	GUI L2P System CLI L2P snmp-server sysname
			L3E	Ja	GUI L3E System CLI L3E snmp-server sysname
			L3P	Ja	GUI L3P System CLI L3P snmp-server sysname

Konfiguration System-Prompt

Um bei einer Installation mit mehr als einem Switch die Switche einfach unterscheiden zu können, vergeben Sie ein Systemprompt, den das CLI anzeigt. Das hilft, Fehlkonfigurationen zu vermeiden.

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
System-prompt konfigurieren	(Hirschmann Railswitch)	<Name>	L2B	Ja	CLI L2B set prompt
			L2E	Ja	CLI L2E set prompt
			L2P	Ja	CLI L2P set prompt
			L3E	Ja	CLI L3E set prompt
			L3P	Ja	CLI L3P set prompt

Konfiguration Switch-Standort und -ansprechpartner

Um bei einer Installation mit mehr als einem Switch den Standort und zuständigen Ansprechpartner schneller ermitteln zu können, hinterlegen Sie diese im Switch. Dies erleichtert die Identifikation des Switches in einem Netzmanagementsystem, das diese Werte per SNMP ausgelesen kann.

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
Standort konfigurieren	Hirschmann Railswitch	<Standortbezeichnung>	L2B	Ja	GUI L2B System CLI L2B snmp-server location
			L2E	Ja	GUI L2E System CLI L2E snmp-server location
			L2P	Ja	GUI L2P System CLI L2P snmp-server location
			L3E	Ja	GUI L3E System CLI L3E snmp-server location
			L3P	Ja	GUI L3P System CLI L3P snmp-server location

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
Ansprechpartner konfigurieren	Hirschmann Automation and Control GmbH	<Ansprechpartner>	L2B	Ja	GUI L2B System CLI L2B snmp-server contact
			L2E	Ja	GUI L2E System CLI L2E snmp-server contact
			L2P	Ja	GUI L2P System CLI L2P snmp-server contact
			L3E	Ja	GUI L3E System CLI L3E snmp-server contact
			L3P	Ja	GUI L3P System CLI L3P snmp-server contact

Alarm bei hoher Netzlast konfigurieren

Um bei einer Netzlast, die einen bestimmten Schwellwert übersteigt, alarmiert zu werden, schalten Sie diese Alarmierung je Port ein. Der obere Grenzwert ist dabei von der Installationsumgebung des Switches abhängig. Ermitteln Sie deshalb den oberen Grenzwert vor Ort.

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
Alarm bei hoher Netzlast (Oberer Grenzwert)	0,00%	<je nach Netzumgebung>, Alarm aktivieren	L2B	Ja	GUI L2B Auslastung (Netzlast)
			L2E	Ja	GUI L2E Auslastung (Netzlast)
			L2P	Ja	GUI L2P Auslastung (Netzlast)
			L3E	Ja	GUI L3E Auslastung (Netzlast)
			L3P	Ja	GUI L3P Auslastung (Netzlast)

Alarm bei speziellen Fehlern konfigurieren

Der Switch bietet die Möglichkeit, bestimmte Fehlerzustände per SNMP Trap zu melden. Nutzen Sie diese Option, um Fehlerzustände zeitnah erkennen zu können.

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
Trap bei Statuswechsel erzeugen	Aus	Ein	L2B	Ja	GUI L2B Trapeinstellung CLI L2B snmp trap link-status
			L2E	Ja	GUI L2E Trapeinstellung CLI L2E snmp trap link-status
			L2P	Ja	GUI L2P Trapeinstellung CLI L2P snmp trap link-status
			L3E	Ja	GUI L3E Trapeinstellung CLI L3E snmp trap link-status
			L3P	Ja	GUI L3P Trapeinstellung CLI L3P snmp trap link-status
Überwachung	Netzteil 1 überwachen Netzteil 2 überwachen Temperatur ignorieren Modul entfernen ignorieren ACA entfernen ignorieren ACA nicht synchron ignorieren Verbindungsfehler ignorieren Ring-Redundanz ignorieren	Netzteil 1 überwachen Netzteil 2 überwachen (wenn angeschlossen) Temperatur überwachen ACA entfernen (je nach Einsatzfall) ACA nicht synchron (je nach Einsatzfall, nicht L2B) Verbindungsfehler überwachen Ring-Redundanz überwachen (wenn genutzt, nicht L2B) Ring-/Netzkopplung überwachen (wenn genutzt, nicht L2B)	L2B	Ja	GUI L2B Gerätestatus CLI L2B device-status monitor
			L2E	Ja	GUI L2E Gerätestatus CLI L2E device-status monitor
			L2P	Ja	GUI L2P Gerätestatus CLI L2P device-status monitor
			L3E	Ja	GUI L3E Gerätestatus CLI L3E device-status monitor
			L3P	Ja	GUI L3P Gerätestatus CLI L3P device-status monitor

Gerätestatus mit Meldekontakt überwachen

Der Switch bietet die Möglichkeit, bestimmte Fehlerzustände über den Meldekontakt zu signalisieren. Nutzen Sie diese Option, um Fehlerzustände zeitnah erkennen zu können.

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
Modus Meldekontakt	Meldekontakt 1: Gerätestatus Meldekontakt 2: Manuelle Einstellung (Kontakt geschlossen)	Funktionsüberwachung	L2B	Ja	GUI L2B Meldekontakt CLI L2B signal-contact
			L2E	Ja	GUI L2E Meldekontakt CLI L2E signal-contact
			L2P	Ja	GUI L2P Meldekontakt CLI L2P signal-contact
			L3E	Ja	GUI L3E Meldekontakt CLI L3E signal-contact
			L3P	Ja	GUI L3P Meldekontakt CLI L3P signal-contact
Trap bei Statuswechsel erzeugen	Aus	Aus (bereits bei M4.21 nicht konfiguriert)	L2B	Ja	GUI L2B Trapeinstellung CLI L2B snmp trap link-status
			L2E	Ja	GUI L2E Trapeinstellung CLI L2E snmp trap link-status
			L2P	Ja	GUI L2P Trapeinstellung CLI L2P snmp trap link-status
			L3E	Ja	GUI L3E Trapeinstellung CLI L3E snmp trap link-status
			L3P	Ja	GUI L3P Trapeinstellung CLI L3P snmp trap link-status

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
Überwachung	Netzteil 1 überwachen Netzteil 2 überwachen Temperatur ignorieren Modul entfernen ignorieren ACA entfernen ignorieren ACA nicht synchron ignorieren Verbindungsfehler ignorieren Ring-Redundanz ignorieren	Netzteil 1 überwachen Netzteil 2 überwachen (wenn angeschlossen) Temperatur überwachen (nicht L2B) ACA entfernen (je nach Einsatzfall) ACA nicht synchron (je nach Einsatzfall, nicht L2B) Verbindungsfehler überwachen Ring-Redundanz überwachen (wenn genutzt, nicht L2B) Ring-/Netzkopplung überwachen (wenn genutzt, nicht L2B)	L2B	Ja	GUI L2B Gerätestatus CLI L2B device-status monitor
			L2E	Ja	GUI L2E Gerätestatus CLI L2E device-status monitor
			L2P	Ja	GUI L2P Gerätestatus CLI L2P device-status monitor
			L3E	Ja	GUI L3E Gerätestatus CLI L3E device-status monitor
			L3P	Ja	GUI L3P Gerätestatus CLI L3P device-status monitor

PROFINET einschalten

Wenn in der Netzumgebung eine Überwachung von PROFINET-Komponenten möglich ist, aktivieren Sie PROFINET auf dem Switch und importieren Sie die GSDML-Datei in die Projektierungsumgebung der PROFINET-Umgebung.

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
PROFINET einschalten	Aus	Ein	L2B	Nein	
			L2E	Ja	GUI L2E PROFINET IO CLI L2E PROFINET IO
			L2P	Ja	GUI L2P PROFINET IO CLI L2P PROFINET IO
			L3E	Ja	GUI L3E PROFINET IO CLI L3E PROFINET IO
			L3P	Ja	GUI L3P PROFINET IO CLI L3P PROFINET IO

PROFINET ausschalten

Falls keine Überwachung des Switches über PROFINET möglich ist, deaktivieren Sie das PROFINET Protokoll auf dem Switch (Vor-Einstellung).

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
PROFINET ausschalten	Aus	Aus	L2B	Nein	
			L2E	Ja	GUI L2E PROFINET IO CLI L2E PROFINET IO
			L2P	Ja	GUI L2P PROFINET IO CLI L2P PROFINET IO
			L3E	Ja	GUI L3E PROFINET IO CLI L3E PROFINET IO
			L3P	Ja	GUI L3P PROFINET IO CLI L3P PROFINET IO

Aktivierung Port-Monitor

Die Port-Monitor Funktionen können Link-Änderungen und CRC-Fehler erkennen und melden. Dadurch können Sie das An- und Abstecken von Geräten erkennen. Auch fehlerhafte Verbindungen (z. B. defektes Kabel) können Sie so erkennen.

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
Port-Monitor Global einschalten	Aus	Ein	L2B	Nein	
			L2E	Nein	
			L2P	Ja	GUI L2P Port-Monitor CLI L2P port-monitor (Global Config)
			L3E	Ja	GUI L3E Port-Monitor CLI L3E port-monitor (Global Config)
			L3P	Ja	GUI L3P Port-Monitor CLI L3P port-monitor (Global Config)

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
Port-Monitor für jeden Port einschalten	Aus	Ein	L2B	Nein	
			L2E	Nein	
			L2P	Ja	GUI L2P Port-Monitor CLI L2P port-monitor (Global Config)
			L3E	Ja	GUI L3E Port-Monitor CLI L3E port-monitor (Global Config)
			L3P	Ja	GUI L3P Port-Monitor CLI L3P port-monitor (Global Config)
Erkennung Linkänderung für jeden Port einschalten	Aus	Ein	L2B	Nein	
			L2E	Nein	
			L2P	Ja	GUI L2P Port-Monitor CLI L2P port-monitor condition link-flap (Global Config)
			L3E	Ja	GUI L3E Port-Monitor CLI L3E port-monitor condition link-flap (Global Config)
			L3P	Ja	GUI L3P Port-Monitor CLI L3P port-monitor condition link-flap (Global Config)
Erkennung CRC-/Fragmentfehler für jeden Port einschalten	Aus	Ein	L2B	Nein	
			L2E	Nein	
			L2P	Ja	GUI L2P Port-Monitor CLI L2P port-monitor condition crc-fragment (Global Config)
			L3E	Ja	GUI L3E Port-Monitor CLI L3E port-monitor condition crc-fragment (Global Config)
			L3P	Ja	GUI L3P Port-Monitor CLI L3P port-monitor condition crc-fragment (Global Config)

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
Aktion: Trap senden für jeden Port einschalten	Port deaktivieren	Trap senden	L2B	Nein	
			L2E	Nein	
			L2P	Ja	GUI L2P Port-Monitor CLI L2P port-monitor action
			L3E	Ja	GUI L3E Port-Monitor CLI L3E port-monitor action
			L3P	Ja	GUI L3P Port-Monitor CLI L3P port-monitor action

Versand von SNMP-Traps bei Nutzung von VRRP/HiVRRP

Wenn Sie Router-Redundanz mit VRRP oder HiVRRP verwenden, lassen Sie sich vom Switch wichtige Zustandsänderungen mittels SNMP-Trap signalisieren:

- ☐ Wenn der Router Master wird
- ☐ Wenn der Router VRRP-Pakete mit falscher Authentifizierung empfängt

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
VRRP Master Trap senden	Aus	Ein	L2B	Nein	
			L2E	Nein	
			L2P	Nein	
			L3E	Ja	GUI L3E VRRP/HiVRRP CLI L3E vrrp trap
			L3P	Ja	GUI L3P VRRP/HiVRRP CLI L3P vrrp trap
VRRP Authentifizierungstrap senden	Aus	Ein	L2B	Nein	
			L2E	Nein	
			L2P	Nein	
			L3E	Ja	GUI L3E VRRP/HiVRRP CLI L3E vrrp trap
			L3P	Ja	GUI L3P VRRP/HiVRRP CLI L3P vrrp trap

4.5 Service Level Management (Netz Qualität)

4.5.1 Bedrohungen

Ein wesentliches Schutzziel von IT-Sicherheit ist die Verfügbarkeit. In industriellen Umgebungen geht die Netzverfügbarkeit über die reine Erreichbarkeit von Systemen hinaus. Folgende Aspekte spielen je nach Anwendung eine Rolle:

- ☐ Quality of service (QoS)
- ☐ Integrität des Netzes
- ☐ Hochverfügbarkeit (Ringstruktur, vermaschte Struktur)

Für den Switch und damit das Netz ergeben sich dabei folgende Bedrohungen:

- ☐ Verbindungsverlust durch Ausfall des Switches
- ☐ Verbindungsverlust durch Kabeldefekt
- ☐ Verbindungsverlust durch Überlast
- ☐ Verbindungsverlust durch Angriff auf die Redundanzmechanismen
- ☐ Latenzen durch Überlast
- ☐ Jitter durch Überlast
- ☐ Beeinträchtigung der Verfügbarkeit durch Anschluss von nicht gewünschten Geräten

4.5.2 Security Quick Check „Service Level Management“

Benötigen Sie?	Wenn notwendig	Wenn nicht notwendig
Eine hohe Netzverfügbarkeit	Aufbau des Netzes in Ringstruktur Aktivierung HIPER-Ring Protokoll Aktivierung MRP Aktivierung beschleunigter Ring-Konfiguration Deaktivierung Spanning Tree Protokoll	
Hohe Netzverfügbarkeit und Netztrennung mittels VLAN	Priorisierung Switch-Management-Pakete Konfiguration des Trust-Modus	
Sind verschiedene Prioritätsklassen für den Netzverkehr notwendig?	Konfiguration der Prioritätsklassen je Port Konfiguration Mapping der VLAN-Prioritätsklassen zu Traffic Class Konfiguration Mapping IP DSCP zu Traffic Class	
Kann der unberechtigte Anschluss von Geräten an das Netz den Service Level des Netzes beeinträchtigen?	Konfiguration MAC-basierter Portsicherheit Konfiguration IP-basierter Portsicherheit Konfiguration 802.1x Portsicherheit	
Kann Überlastung des Netzes zu Problemen führen?	Schwellwert für oberen Grenzwert der Netzlast setzen und per SNMP Trap alarmieren Konfiguration Lastbegrenzer	
Wird der Switch als Router in einer Umgebung mit hohen Ansprüchen an die Verfügbarkeit eingesetzt?	Redundanten Router einsetzen	
Grundprinzip		
Die Maßnahmen folgen dem Minimalprinzip, um die Systemlast des Switches und dessen Angriffsfläche zu reduzieren. Schalten Sie nicht benötigte Dienste generell ab.		
Allgemeine Maßnahmen		
RAM Selbsttest aktivieren Kaltstart bei undefiniertem Software-Verhalten aktivieren		

Tab. 3: Security Quick Check „Service Level Management“

4.5.3 Maßnahmen

Bekannte Einschränkungen:
☐ Je nach Switchmodell sind 4 oder 8 Traffic Classes möglich

Aufbau des Netzes in Ringstruktur

Die Ringstruktur bietet mit seinen Redundanzprotokollen eine höhere Ausfallsicherheit für hochverfügbare Netze. Bauen Sie deshalb das Netz als Ring auf.

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
Aufbau des Netzes in Ringstruktur	Keiner	Keiner	L2B	Ja	GUI L2B Ring-Redundanz CLI L2B HIPER-Ring
			L2E	Ja	GUI L2E Ring-Redundanz CLI L2E HIPER-Ring
			L2P	Ja	GUI L2P Ring-Redundanz CLI L2P HIPER-Ring
			L3E	Ja	GUI L3E Ring-Redundanz CLI L3E HIPER-Ring
			L3P	Ja	GUI L3P Ring-Redundanz CLI L3P HIPER-Ring

Aktivierung HIPER-Ring Protokoll

Das HIPER-Ring Protokoll unterstützt die Hochverfügbarkeit in ringförmig aufgebauten Netzen. Es bietet zudem definierte Umschaltzeiten und umfangreiche Protokollierungs- und Alarmierungsmöglichkeiten beim Ausfall einer Teilstrecke. HIPER-Ring ist ein von Hirschmann entwickeltes Protokoll, das sich in vielen Jahren in der Praxis bestens bewährt hat.

Anmerkung: Es kann entweder HIPER-Ring oder MRP verwendet werden.

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
Aktivierung HIPER-Ring Protokoll	Ein	Ein	L2B	Ja	GUI L2B HIPER-Ring konfigurieren CLI L2B hiper-ring
			L2E	Ja	GUI L2E HIPER-Ring konfigurieren CLI L2E hiper-ring
			L2P	Ja	GUI L2P HIPER-Ring konfigurieren CLI L2P hiper-ring
			L3E	Ja	GUI L3E HIPER-Ring konfigurieren CLI L3E hiper-ring
			L3P	Ja	GUI L3P HIPER-Ring konfigurieren CLI L3P hiper-ring

Aktivierung MRP

Das MRP Protokoll bietet ebenfalls die für den Betrieb von hochverfügbaren Netzen in Ringform notwendige Funktionen ähnlich wie HIPER-Ring. Allerdings ist MRP ein offenes und standardisiertes Protokoll, das mit den Produkten anderer Hersteller interoperabel ist. Zudem bietet es bei einer Ringstörung garantierte Umschaltzeiten unter Einhaltung der spezifizierten Rahmenbedingungen. Außerdem kann das VLAN für das Ringprotokoll frei definiert werden.

Anmerkung: Es kann entweder HIPER-Ring oder MRP verwendet werden.

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
Aktivierung MRP	Aus	Ein	L2B	Ja	GUI L2B MRP-Ring konfigurieren CLI L2B mrp current-domain
			L2E	Ja	GUI L2E MRP-Ring konfigurieren CLI L2E mrp current-domain
			L2P	Ja	GUI L2E MRP-Ring konfigurieren CLI L2E mrp current-domain
			L3E	Ja	GUI L3E MRP-Ring konfigurieren CLI L3E mrp current-domain
			L3P	Ja	GUI L3P MRP-Ring konfigurieren CLI L3P mrp current-domain

Aktivierung beschleunigter Ring-Konfiguration

Bei einem Ausfall einer Teilstrecke innerhalb eines ringförmig aufgebauten Netzes bietet diese Option eine schnellere Wiederherstellung der Datenübertragung im Ring.

Nutzen Sie, wenn möglich, beschleunigte Ringkonfiguration. Ausnahmen können aber sehr große Ringe, viel Verkehr im Ring oder eine hohe Paketverlustrate sein.

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
Aktivierung beschleunigter Ring-Konfiguration	standard	aktiviert	L2B	Ja	GUI L2B HIPER-Ring konfigurieren CLI L2B hiper-ring recovery-delay
			L2E	Ja	GUI L2E HIPER-Ring konfigurieren CLI L2E hiper-ring recovery-delay
			L2P	Ja	GUI L2P HIPER-Ring konfigurieren CLI L2P hiper-ring recovery-delay
			L3E	Ja	GUI L3E HIPER-Ring konfigurieren CLI L3E hiper-ring recovery-delay
			L3P	Ja	GUI L3P HIPER-Ring konfigurieren CLI L3P hiper-ring recovery-delay

Deaktivierung Spanning Tree Protokoll

Wenn das Netz komplett in Ringstruktur aufgebaut ist und die Bildung von Schleifen (Loops) im Netz ausgeschlossen werden kann, sollte das Spanning Tree Protokoll deaktiviert werden. Ansonsten führt jede Änderung des Zustands an einem Switch-Port zur Neukonfiguration des Spanning Trees im Netz und verhindert für mehrere Sekunden bis zu wenigen Minuten den Netzverkehr.

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
Deaktivierung Spanning Tree Protokoll	Aus	Aus	L2B	Ja	GUI L2B Global CLI L2B spanning-tree
			L2E	Ja	GUI L2E Global CLI L2E spanning-tree
			L2P	Ja	GUI L2P Global CLI L2P spanning-tree
			L3E	Ja	GUI L3E Global CLI L3E spanning-tree
			L3P	Ja	GUI L3P Global CLI L3P spanning-tree

Priorisierung Switch-Management-Pakete

Die Switche bieten die Möglichkeit, Management-Pakete für die Konfiguration und Überwachung der Switche zu priorisieren. Somit kann bei hoher Netzlast der Management-Verkehr zuverlässiger übertragen werden. Gerade bei Fehlersituationen ist der Zugriff auf die Switche für eine Eingrenzung der Ursache und Fehlerbehebung sehr wichtig. Aktivieren Sie daher diese Option.

Die Priorisierung wirkt für HTTP, HTTPS, Telnet und weiteren IP-Verkehr an die Management-IP-Adresse des Switches.

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
Priorisierung der Switch-Management-Pakete	0	7	L2B	Ja	GUI L2B Global CLI L2B network priority
			L2E	Ja	GUI L2E Global CLI L2E network priority
			L2P	Ja	GUI L2P Global CLI L2P network priority
			L3E	Ja	GUI L3E Global CLI L3E network priority
			L3P	Ja	GUI L3P Global CLI L3P network priority

Konfiguration des Trust-Modus

Der Trust-Modus legt fest, ob und wie der Switch QoS Tags in empfangenen Paketen auswertet und die Pakete entsprechend priorisiert.

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
Konfiguration des Trust-Modus	trustDot1p	Bei Verwendung von VLAN auf diesem Port: „trustDot1p“, sonst „trustDscp“	L2B	Ja	GUI L2B Global CLI L2B classofservice trust
			L2E	Ja	GUI L2E Global CLI L2E classofservice trust
			L2P	Ja	GUI L2P Global CLI L2P classofservice trust
			L3E	Ja	GUI L3E Global CLI L3E classofservice trust
			L3P	Ja	GUI L3P Portkonfiguration CLI L3P classofservice trust

Konfiguration der Prioritätsklassen je Port

Pakete die mit den Modi „trustDot1p“ oder „trustDscp“ nicht priorisiert werden können oder Pakete, die im „untrusted“ Modus empfangen werden, werden anhand der konfigurierten Priorität des Switch-Ports priorisiert. Konfigurieren Sie deshalb auf den Switch-Ports die Prioritäten (als Rückfallebene).

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
Port-Priorität	0	Je nach Anwendung zwischen 0 und 7	L2B	Ja	GUI L2B Port-Priorität eingeben CLI L2B vlan port priority all
			L2E	Ja	GUI L2E Port-Priorität eingeben CLI L2E vlan port priority all
			L2P	Ja	GUI L2P Port-Priorität eingeben CLI L2P vlan port priority all
			L3E	Ja	GUI L3E Port-Priorität eingeben CLI L3E vlan port priority all
			L3P	Ja	GUI L3P Port-Priorität eingeben CLI L3P vlan port priority all

Konfiguration Mapping der VLAN-Prioritätsklassen zu Traffic Class

Die folgende Switche unterstützen 4 Traffic Class-Einteilungen:

RS20/30/40; MS20/30; Octopus; MACH102; RSR; MACH1020/1030; RSB

Im VLAN nach 802.1d werden jedoch acht Prioritäten unterstützt. Mappen Sie deshalb die VLAN-Prioritäten auf die interne Traffic Class. Die Voreinstellungen sind in der Regel ausreichend. Überprüfen Sie im konkreten Anwendungsfall die Voreinstellungen und passen Sie sie gegebenenfalls an.

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
802.1q zu Traffic Class Mapping	0 1 2 3 4 5 6 7	1 (default) 0 (default) 0 (default) 1 (default) 2 (default) 2 (default) 3 (default) 3 (default)	L2B	Ja	GUI L2B 802.1D/p-Mapping CLI L2B classofservice dot1p-mapping
			L2E	Ja	GUI L2E 802.1D/p-Mapping CLI L2E classofservice dot1p-mapping
			L2P	Ja	GUI L2P 802.1D/p-Mapping CLI L2P classofservice dot1p-mapping
			L3E	Ja	GUI L3E 802.1D/p-Mapping CLI L3E classofservice dot1p-mapping
			L3P	Ja	GUI L3P 802.1D/p-Mapping CLI L3P classofservice dot1p-mapping

Konfiguration Mapping IP DSCP zu Traffic Class

Die Switche unterstützen in den meisten Versionen 4 Traffic Class-Einteilungen. Ausnahme: In den Softwareversionen L3E und L3P unterstützen die Switche 8 Traffic Classes. IP DSCP unterstützt aber 63 DSCP-Werte. Mappen Sie deshalb die DSCP-Werte auf die internen Traffic Classes. Die Voreinstellungen sind in der Regel ausreichend. Überprüfen Sie im konkreten Anwendungsfall die Voreinstellungen und passen Sie sie gegebenenfalls an.

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
DSCP zu Traffic Class Mapping	Siehe CLI Dokumentation	Default-Werte	L2B	Ja	GUI L2B IP-DSCP-Mapping CLI L2B classofservice ip-dscp-mapping
			L2E	Ja	GUI L2E IP-DSCP-Mapping CLI L2E classofservice ip-dscp-mapping
			L2P	Ja	GUI L2P IP-DSCP-Mapping CLI L2P classofservice ip-dscp-mapping

Konfiguration MAC-basierter Portsicherheit

Um den Anschluss unerwünschter Geräte am Netz zu verhindern, bieten die Switche die Möglichkeit, bestimmte Geräte anhand deren MAC-Adressen je Port zuzulassen. Für Umgebungen, in denen die physikalische Zugangskontrolle zu einem Switch-Port nicht ausreichend ist, kann damit die Sicherheit verbessert werden.

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
Konfiguration MAC-basierte Portsicherheit	Keine MAC-Adressen definiert	MAC-Adressen, die an dem Switch-Port zugelassen werden sollen	L2B	Nein	
			L2E	Ja	GUI L2E Portsicherheit CLI L2E port-sec allowed-mac
			L2P	Ja	GUI L2P Portsicherheit CLI L2P port-sec allowed-mac
			L3E	Ja	GUI L3E Portsicherheit CLI L3E port-sec allowed-mac
			L3P	Ja	GUI L3P Portsicherheit CLI L3P port-sec allowed-mac

Mögliche negative Auswirkungen:

Verfügbarkeit: Bei einem Tausch von angeschlossenen Geräten (z. B. in einem Service-Fall) ändert sich die MAC-Adresse und das Gerät bekommt keine Netzverbindung, solange nicht auch der Switch-Port umkonfiguriert wurde.

Bekannte Einschränkungen:

Die MAC-Adresse lässt sich bei vielen Systemen manuell umstellen und dadurch der Schutz überwinden. Es können per CLI maximal 10 Adressen am Stück konfiguriert werden. Insgesamt sind 50 Adressen per einzelnen Add/Delete-Kommandos möglich.

Konfiguration IP-basierter Portsicherheit

Um den Anschluss unerwünschter Geräte am Netz zu verhindern, bieten die Switche die Möglichkeit, bestimmte Geräte anhand deren IP-Adressen je Port zuzulassen.

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
Konfiguration IP-basierte Portsicherheit	Keine IP-Adressen definiert	IP-Adressen, die an dem Switch-Port zugelassen werden sollen	L2B	Nein	
			L2E	Ja	GUI L2E Portsicherheit CLI L2E port-sec allowed-ip
			L2P	Ja	GUI L2P Portsicherheit CLI L2P port-sec allowed-ip
			L3E	Ja	GUI L3E Portsicherheit CLI L3E port-sec allowed-ip
			L3P	Ja	GUI L3P Portsicherheit CLI L3P port-sec allowed-ip

Bekannte Einschränkungen:

Die Filterung nach IP-Adressen bietet in den meisten Fällen geringen Schutz. Es können maximal 10 IP-Adressen pro Port konfiguriert werden.

Konfiguration 802.1x Portsicherheit

Um den Anschluss unerwünschter Geräte am Netz zu verhindern, bieten die Switche auch die Möglichkeit, die Anmeldung zentral über einen oder 2 RADIUS-Server zu steuern. Dabei werden zugelassene MAC-Adressen und bei Bedarf auch die Zuordnung zu bestimmten VLANs zentral konfiguriert.

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
Konfiguration 802.1x Portsicherheit	Siehe CLI Dokumentation	Default-Werte	L2B	Nein	
			L2E	Nein	
			L2P	Ja	GUI L2P IEEE 802.1X-Port-Authentifizierung CLI L2P dot1x port-control
			L3E	Ja	GUI L3E IEEE 802.1X-Port-Authentifizierung CLI L3E dot1x port-control
			L3P	Ja	GUI L3P IEEE 802.1X-Port-Authentifizierung CLI L3P dot1x port-control

Mögliche negative Auswirkungen:

Verfügbarkeit: Beim Ausfall aller RADIUS-Server bzw. der Netzverbindung dorthin kann sich kein Gerät mehr am Netz anmelden.

Schwellwert für oberen Grenzwert der Netzlast setzen und per SNMP Trap alarmieren

Um eine Überlastsituation zu erkennen, bietet der Switch die Möglichkeit, bei Überschreitung eines Schwellwerts der Netzlast je Port einen Alarm zu versenden. Aktivieren Sie diese Funktion, um eine Überlastsituation zeitnah zu erkennen.

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
Schwellwert Netzlast und Alarm konfigurieren	0,00 % und ausgeschaltet für jedes Interface	Lastwerte je nach Einsatzsituation, Alarmierung ein	L2B	Ja	GUI L2B Auslastung (Netzlast)
			L2E	Ja	GUI L2E Auslastung (Netzlast)
			L2P	Ja	GUI L2P Auslastung (Netzlast)
			L3E	Ja	GUI L3E Auslastung (Netzlast)
			L3P	Ja	GUI L3P Auslastung (Netzlast)

Konfiguration Lastbegrenzer

Die Funktion des Lastbegrenzers erlaubt, eingehende oder ausgehende Pakete (Broadcasts, Multicast, Unicast von noch nicht gelernten MAC-Adressen) auf eine bestimmte Bandbreite (Kbit/s) oder auf Pakete zu filtern (ist abhängig vom eingesetzten Produkt). Dies verbessert den Schutz sowohl des Switches als auch der dahinter liegenden Geräte vor Überlast.

Benutzen Sie den Lastbegrenzer ausschließlich, wenn die Auswirkungen auf das Netz abschätzbar sind und Sie die Risiken eines Einsatzes dieser Funktion abschätzen und akzeptieren können.

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
Eingangspaketty-pen	BC (Broad-casts)	BC (default)	L2B	Nein	
			L2E	Ja	GUI L2E Lastbegren-zer CLI L2E storm-control broadcast
			L2P	Ja	GUI L2P Lastbegren-zer CLI L2P storm-control broadcast
			L3E	Ja	GUI L3E Lastbegren-zer CLI L3E storm-control broadcast
			L3P	Ja	GUI L3P Lastbegren-zer CLI L3P storm-control broadcast
Eingangsbegren-zer	Aus	Ein	L2B	Nein	
			L2E	Ja	GUI L2E Lastbegren-zer CLI L2E storm-control ingress-limiting
			L2P	Ja	GUI L2P Lastbegren-zer CLI L2P storm-control ingress-limiting
			L3E	Ja	GUI L3E Lastbegren-zer CLI L3E storm-control ingress-limiting
			L3P	Ja	GUI L3P Lastbegren-zer CLI L3P storm-control ingress-limiting

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
Eingangsbegrenzerrate je Port	0 (aus)	5% der Portbandbreite	L2B	Nein	
			L2E	Ja	GUI L2E Lastbegrenzer CLI L2E storm-control ingress-limit
			L2P	Ja	GUI L2P Lastbegrenzer CLI L2P storm-control ingress-limit
			L3E	Ja	GUI L3E Lastbegrenzer CLI L3E storm-control ingress-limit
			L3P	Ja	GUI L3P Lastbegrenzer CLI L3P storm-control ingress-limit
Ausgangsbegrenzer BC	Aus	Aus (default)	L2B	Nein	
			L2E	Ja	GUI L2E Lastbegrenzer CLI L2E storm-control broadcast
			L2P	Ja	GUI L2P Lastbegrenzer CLI L2P storm-control broadcast
			L3E	Ja	GUI L3E Lastbegrenzer CLI L3E storm-control broadcast
			L3P	Ja	GUI L3P Lastbegrenzer CLI L3P storm-control broadcast

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
Ausgangssbegrenzerrate BC je Port	0 (aus)	0 (aus, default)	L2B	Nein	
			L2E	Ja	GUI L2E Lastbegrenzer CLI L2E storm-control broadcast (port-related)
			L2P	Ja	GUI L2P Lastbegrenzer CLI L2P storm-control broadcast (port-related)
			L3E	Ja	GUI L3E Lastbegrenzer CLI L3E storm-control broadcast (port-related)
			L3P	Ja	GUI L3P Lastbegrenzer CLI L3P storm-control broadcast (port-related)
Ausgangssbegrenzerrate alle	Aus	Aus (default)	L2B	Nein	
			L2E	Ja	GUI L2E Lastbegrenzer CLI L2E storm-control egress-limiting
			L2P	Ja	GUI L2P Lastbegrenzer CLI L2P storm-control egress-limiting
			L3E	Ja	GUI L3E Lastbegrenzer CLI L3E storm-control egress-limiting
			L3P	Ja	GUI L3P Lastbegrenzer CLI L3P storm-control egress-limiting

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
Ausgangssbe-grenzerrate alle je Port	0 (aus)	0 (aus, default)	L2B	Nein	
			L2E	Ja	GUI L2E Lastbegren-zer CLI L2E storm-control egress-limit
			L2P	Ja	GUI L2P Lastbegren-zer CLI L2P storm-control egress-limit
			L3E	Ja	GUI L3E Lastbegren-zer CLI L3E storm-control egress-limit
			L3P	Ja	GUI L3P Lastbegren-zer CLI L3P storm-control egress-limit

Redundanten Router einsetzen

Bei der Verwendung des Switches als Router in einer Umgebung mit hohen Verfügbarkeitsanforderungen setzen Sie einen weiteren Router für die Erhöhung der Verfügbarkeit im Fall eines Ausfalls (Redundanz) ein. Diese Router kommunizieren mittels VRRP oder HiVRRP Protokoll, um festzustellen, wann der andere Router die Datenvermittlung übernimmt. Durch gefälschte (Hi)VRRP Pakete besteht auch hier die Möglichkeit, die Verfügbarkeit des Netzes zu beeinträchtigen.

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
VRRP/HiVRRP einschalten	Aus	Ein	L2B	Nein	
			L2E	Nein	
			L2P	Nein	
			L3E	Ja	GUI L3E VRRP/HiV-RRP Konfiguration CLI L3E ip vrrp
			L3P	Ja	GUI L3P VRRP/HiV-RRP Konfiguration CLI L3P ip vrrp

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
Authentifizierung auf Interface einschalten (im Wizard)	noAuthentication	simpleTextPassword	L2B	Nein	
			L2E	Nein	
			L2P	Nein	
			L3E	Ja	GUI L3E VRRP/HiVRRP Konfiguration CLI L3E ip vrrp authentication
			L3P	Ja	GUI L3P VRRP/HiVRRP Konfiguration CLI L3P ip vrrp authentication
Schlüssel eingeben (im Wizard)	<leer>	Sicheres Passwort mit 16 Zeichen	L2B	Nein	
			L2E	Nein	
			L2P	Nein	
			L3E	Ja	GUI L3E VRRP/HiVRRP Konfiguration CLI L3E ip vrrp authentication
			L3P	Ja	GUI L3P VRRP/HiVRRP Konfiguration CLI L3P ip vrrp authentication

RAM Selbsttest aktivieren

Der RAM-Selbsttest testet den Arbeitsspeicher des Switches beim Booten auf mögliche Fehler und kann dadurch Fehler im Betrieb verhindern.

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
RAM Test	Ein	Ein	L2B	Ja	GUI L2B Selbsttest CLI L2B selftest
			L2E	Ja	GUI L2E Selbsttest CLI L2E selftest ramtest
			L2P	Ja	GUI L2P Selbsttest CLI L2P selftest ramtest
			L3E	Ja	GUI L3E Selbsttest CLI L3E selftest ramtest
			L3P	Ja	GUI L3P Selbsttest CLI L3P selftest ramtest

Kaltstart bei undefiniertem Software-Verhalten

Falls während des Betriebs in der Software des Switches ein undefiniertes Verhalten auftritt, kann sich der Switch selbst neu starten. Diese Funktion hilft, Fehler und Probleme im Betrieb durch einzelne nicht mehr (korrekt) funktionierende Teilsysteme zu verhindern.

Aktion	Default Wert	Empfohlener Wert	Vorhanden in SW-Version		Weitere Information
Kaltstart bei undefinierten Software-Verhalten	Ein	Ein	L2B	Ja	GUI L2B Selbsttest CLI L2B selftest reboot-on-error
			L2E	Ja	GUI L2E Selbsttest CLI L2E selftest reboot-on-error
			L2P	Ja	GUI L2P Selbsttest CLI L2P selftest reboot-on-error
			L3E	Ja	GUI L3E Selbsttest CLI L3E selftest reboot-on-error
			L3P	Ja	GUI L3P Selbsttest CLI L3P selftest reboot-on-error

4.6 Updates

4.6.1 Bedrohungen

Hirschmann erweitert und verbessert regelmäßig die Software des Switches. Die daraus resultierenden Updates stellt Hirschmann zum Herunterladen von der Produkt-Seite im Internet bereit. Spielen Sie Updates auf den Switch auf.

Daraus ergeben sich folgende Bedrohungen:
- ☐ Einspielen fehlerhafter/ schädlicher Software
- ☐ Unterbrechung des Update Prozesses
- ☐ Missbrauch der Update Funktion

Es kann gezielt ein fehlerhaftes oder bösartiges Update eingespielt werden was die Vertraulichkeit und Integrität und auch die Verfügbarkeit beeinträchtigen kann.

Sie können den Bedrohungen mit folgenden Konfigurationspunkten entgegenwirken:

4.6.2 Security Quick Check

Benötigen Sie?	Wenn notwendig	Wenn nicht notwendig
Sicherheit für Ihre Anwendung	Regelmäßige Prüfung auf sicherheitsrelevante Updates und deren Installation	

Grundprinzip
Es werden täglich neue Sicherheitslücken in den unterschiedlichsten Systemen entdeckt. Schließen Sie bei Sicherheitsrelevanten Systemen sind diese zeitnah. Das kann oft durch die Installation einer neuen Software auf dem Switch erfolgen.
Allgemeine Maßnahmen
☐ Regelmäßige Prüfung auf Updates mit Fehlerbehebungen und deren Installation ☐ Bezug der Updates von einer vertrauenswürdigen Quelle ☐ Updates nicht während des laufenden Betriebs

Tab. 4: Security Quick Check „Updates“

4.6.3 Maßnahmen

Regelmäßige Prüfung auf sicherheitsrelevante Updates und deren Installation

Viele bekannt gewordene Sicherheitslücken können Sie durch ein Update, das die Lücken schließt, beheben. Hierzu beachten Sie Folgendes:

- ☐ Informieren Sie sich regelmäßig bei Hirschmann über bekannt gewordene Sicherheitslücken
- ☐ Sobald eine neue Software die Lücken schließt, spielen Sie die neue Software ein.

Mögliche Informationsquellen finden Sie im Abschnitt 1.4 „Weitere Informationen“.

Regelmäßige Prüfung auf Updates mit Fehlerbehebungen und deren Installation

Neben Sicherheitsproblemen können Sie durch Updates auch funktionale Probleme beheben, auch solche, die u. U. zwar existieren, aber noch nicht auffällig geworden sind.

Hierzu beachten Sie Folgendes:

- ☐ Informieren Sie sich regelmäßig bei Hirschmann über bekannt gewordene Sicherheitslücken
- ☐ Sobald eine neue Software die Lücken schließt, spielen Sie die neue Software ein.

Mögliche Informationsquellen finden Sie im Abschnitt 1.4 „Weitere Informationen“.

Bezug der Updates von einer vertrauenswürdigen Quelle

Beziehen Sie die Software ausschließlich direkt vom Hersteller unter http://www.hirschmann.de/de/Hirschmann/Industrial_Ethernet/Software/Software_Platforms/index.phtml in einem ZIP-Archiv. Das ZIP-Archiv kann über Prüfsummen erkennen, ob die Updates auf dem Übertragungsweg durch Übertragungsfehler beschädigt wurden.

Bekannte Einschränkungen: Die Updates sind nicht digital signiert und somit nicht vor Manipulation auf dem Weg von Hirschmann auf den Switch geschützt.

Das JAR-File (JAVA-Applet) in der Software ist mit SHA-1 Prüfsummen versehen. Zudem ist das JAR-File mit einem Code-Signing Zertifikat von Hirschmann (Digital ID Class 3 Java Object Signing) signiert, das von Verisign ausgestellt wurde.

Wenn die Gültigkeit des Zertifikats abgelaufen ist, erhält der Anwender darüber einen Warnhinweis. Eine Verlängerung des Zertifikats ist nicht möglich. Evtl. können Sie durch ein Update auf eine aktuelle Software-Version des Switches ein neueres Zertifikat einspielen. Informieren Sie sich dazu bei Bedarf über die Release-Notes.

Updates nicht während des laufenden Betriebs

Während des Updates ist der Prozessor des Switches zusätzlich belastet und kann sich ggfs. anders verhalten. Zudem erfordert der Switch nach dem Update einen Neustart . Dies kann, insbesondere bei Nutzung von Spanning Tree, die Netzverfügbarkeit beeinträchtigen.

4.7 Außerbetriebnahme

4.7.1 Bedrohungen

Hat ein Switch das Ende der geplanten Einsatzzeit erreicht, nehmen Sie ihn außer Betrieb.

Daraus ergeben sich folgende Bedrohungen:
☐ Auslesen der Konfiguration nach Außerbetriebnahme
☐ Wiederanschluss durch menschliches Fehlverhalten/ Sabotage
☐ Auslesen von geheimen Schlüsseln (SSL und SSH)

4.7.2 Security Quick Check

Benötigen Sie?	Wenn notwendig	Wenn nicht notwendig
Sicherheit nach der geplanten Lebens-zeit	Regelmäßige Prüfung auf sicherheitsrelevante Updates und deren Installation Zurücksetzen der Konfiguration (clear config) Löschen des Auto-Configuration Adapters (ACA)	
Grundprinzip		
Das Auslesen der Konfiguration kann die Vertraulichkeit beeinträchtigen, da zum Beispiel Passwörter ausgelesen werden können.		

4.7.3 Maßnahmen

Sie können den Bedrohungen mit folgenden Konfigurationspunkten entgegenwirken:

Zurücksetzen der Konfiguration

Wird ein Switch unbeabsichtigt oder fahrlässig an ein Netz angeschlossen, kann die Verfügbarkeit beeinträchtigt werden. Beispiele hierfür sind Spanning Tree Berechnungszeiten oder IP-Adresskonflikte

Aktion	Default Wert	Empfohlener Wert	Vorhanden		Weitere Information
Clear Config	-	Clear config factory	L2B	Ja	GUI L2B Konfiguration laden/speichern CLI L2B clear config factory
			L2E	Ja	GUI L2E Konfiguration laden/speichern CLI L2E clear config factory
			L2P	Ja	GUI L2P Konfiguration laden/speichern CLI L2P clear config factory
			L3E	Ja	GUI L3E Konfiguration laden/speichern CLI L3E clear config factory
			L3P	Ja	GUI L3P Konfiguration laden/speichern CLI L3P clear config factory

Löschen des Auto-Configuration Adapters (ACA)

Das einfache Entfernen der vorhanden Dateien auf dem ACA bietet noch keinen ausreichenden Schutz, mit dem Sie die Wiederherstellung durch Dritte verhindern können. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt für die sichere Löschung von Flash-Speichern wie etwa dem ACA „Bei hohem Schutzbedarf muss der gesamte Speicherbereich mit geeigneter Software dreimal überschrieben werden.“ [2]

Eine Möglichkeit für eine geeignete Software finden Sie auf der Seite des BSI. [3]

4.8 Störung

4.8.1 Bedrohungen

Der erworbene Switch ist ein hochwertiges Produkt bezüglich Hardware und Software. Dennoch kann es auch hier zu Beeinträchtigungen kommen, etwa, wenn ein Gerät außerhalb der empfohlenen Spezifikation betrieben wird.

Daraus ergeben sich folgende Bedrohungen:

- Beeinträchtigung der Verfügbarkeit
- Auslesen der Konfiguration
- Auslesen von geheimen Schlüsseln (SSL und SSH), Passwörtern und SNMP Community Strings

4.8.2 Security Quick Check „Störung“

Benötigen Sie?	Wenn notwendig	Wenn nicht notwendig
Vertraulichkeit in sehr sensiblen Bereichen und Sie tauschen das Gerät aus	Regelmäßige Prüfung auf sicherheitsrelevante Updates und deren Installation. Der Helpdesk kann Ihre Diagnose des Defekts bewerten und den RMA Prozess einleiten. Sollte es sich, wider Erwarten um einen Konfigurationsfehler handeln, spart der Weg über den Helpdesk Zeit im Vergleich zum direkten Einschicken. Da der Speicher Technologie bedingt nicht sicher gelöscht werden kann, wird keine Gewährleistung für die gespeicherten Daten übernommen. Kontakt zum Helpdesk	Kontakt zum Helpdesk

Grundprinzip

Das Auslesen der Konfiguration kann die Vertraulichkeit beeinträchtigen, da zum Beispiel Passwörter ausgelesen werden können. Dies kann in sehr sensiblen Bereichen als nicht akzeptabel eingestuft werden.

4.8.3 Maßnahmen

Kontakt zum Helpdesk

Nehmen Sie Kontakt zum Helpdesk auf, damit Ihr Fall schnellst möglich bearbeitet werden kann. Sie erreichen den Helpdesk über folgendes Portal.

https://hirschmann-support.belden.eu.com

Der Helpdesk kann Ihre Diagnose des Defekts bewerten und den RMA Prozess einleiten. Sollte es sich, wider Erwarten um einen Konfigurationsfehler handeln, spart der Weg über den Helpdesk Zeit im Vergleich zum direkten Einschicken.

Da der Speicher Technologie bedingt nicht sicher gelöscht werden kann, wird keine Gewährleistung für die gespeicherten Daten übernommen.

Physikalisch vernichten

Sollten Sie das Gerät in einem hoch sensiblen Bereich eingesetzt haben, verzichten Sie auf das Einschicken des Gerätes, sondern nehmen Sie selbst die Entsorgung durch physikalische Vernichtung vor.

A Referenzen

[1] Homeland Security (2009) Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies

[2] Bundesamt für Sicherheit in der Informationstechnik (2011) IT-Grundschutz-Katalog - M 2.167 Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Daten

[3] Bundesamt für Sicherheit in der Informationstechnik - So löschen Sie Daten richtig https://www.bsi-fuer-buerger.de/BSIFB/DE/MeinPC/Richtig-Loeschen/richtigloeschen_node.html

B 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	O	O	O	O	O
Lesbarkeit	O	O	O	O	O
Verständlichkeit	O	O	O	O	O
Beispiele	O	O	O	O	O
Aufbau	O	O	O	O	O
Vollständigkeit	O	O	O	O	O
Grafiken	O	O	O	O	O
Zeichnungen	O	O	O	O	O
Tabellen	O	O	O	O	O

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

C 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.

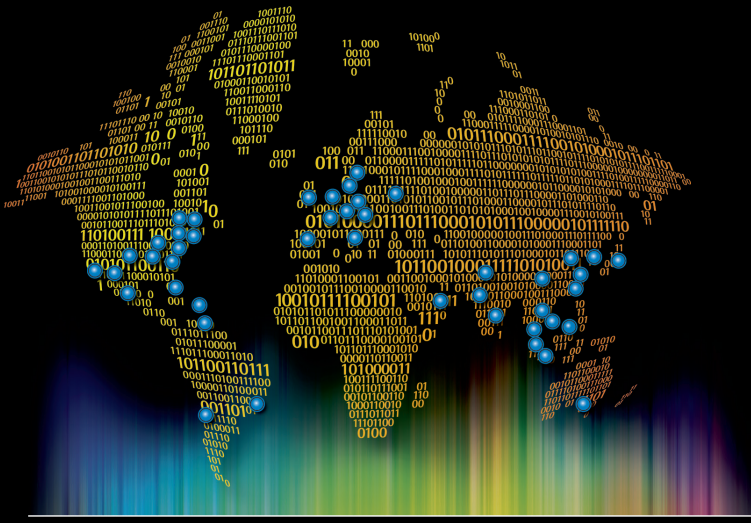
Mit dem Hirschmann Competence Center entscheiden Sie sich in jedem Fall gegen jeglichen Kompromiss. Das kundenindividuelle Angebot lässt Ihnen die Wahl, welche Komponenten Sie in Anspruch nehmen.
Internet:
http://www.hicomcenter.com

HIRSCHMANN
A BELDEN BRAND

www.hirschmann.com

GLOBALE STANDORTE

Mehr Informationen
finden Sie auf
www.beldensolutions.com



Be certain
you stay
in touch.

EUROPA/MITTLERER OSTEN/AFRIKA

Deutschland – Hauptsitz
Tel.: +49-7127-14-0
inet-sales@belden.com

Frankreich
Tel.: +33-1-393-501-00
reseau.france@belden.com

Großbritannien
Tel.: +44 161 4983749
manchester.salesinfo@belden.com

Italien
Tel.: +39-039-5965-250
info.milano@belden.com

Niederlande
Tel.: +31-773-878-555
venlo.salesinfo@belden.com

Russland
Tel.: +7-495-287-1391
info@belden.ru

Spanien
Tel.: +34-91-746-17-30
madrid.salesinfo@belden.com

Schweden
Tel.: +46-40-699-88-60
inet-sales@belden.com

Vereinigte Arabische Emirate
Tel.: +971-4-391-0490
dubai.salesinfo@belden.com

AMERIKA

USA
Tel.: +1-855-400-9071
inetsalesops@belden.com

ASIEN/PAZIFIK

Singapur
Tel.: +65-6879-9800
singapore.sales@belden.com

China
Tel.: +86-21-5445-2353
China.Marketing@belden.com

Kontakt

Gedruckt in Deutschland

ICS-SECURITY-HANDBUCH-FUER-HIRSCHMANN-SWITCHES_INIT_HIR_0915_G_EMEA