LINKSYS®

Ein Unternehmen der Cisco Systems, Inc.

8-Port 10/100/1000 Gigabit Switch

VERKABELT

with WebView

Benutzerhandbuch

Modellnr. **SRW2008/SRW2008P/SRW2008MP (EU)**

CISCO SYSTEMS

Urheberrechte und Marken

Verwendung dieses Benutzerhandbuchs

Dieses Benutzerhandbuch wurde so gestaltet, dass der Netzwerkbetrieb mit dem Router einfacher zu verstehen ist als je zuvor. Achten Sie in diesem Benutzerhandbuch auf die folgenden Elemente:

Dieses Häkchen kennzeichnet wichtige Hinweise, die bei der Verwendung des Switches beachtet werden sollten.

Dieses Ausrufezeichen kennzeichnet Sicherheits- oder Warnhinweise, die beachtet werden sollten, damit Ihr Eigentum oder der Switch nicht beschädigt werden.

Dieses Fragezeichen erinnert Sie an einen Vorgang, den Sie während der Verwendung des Switches möglicherweise durchführen müssen.

Zusätzlich zu diesen Symbolen werden Definitionen für technische Begriffe folgendermaßen angegeben:

Begriff: *Definition.*

Des Weiteren enthält jede Abbildung (Diagramm, Screenshot oder andere Bilder) eine Nummer und eine Beschreibung:

Abbildung 0-1: Beispiel einer Bildbeschreibung

Nummern und Beschreibungen finden Sie auch im Abschnitt „Liste der Abbildungen“.

Inhaltsverzeichnis

Kapitel 1: Einleitung 1
- Willkommen 1
- Inhalt des Benutzerhandbuchs 3

Kapitel 2: Aufbau des Switches 4
- Übersicht 4
- SRW2008 – Vorderseite 4
- SRW2008P, SRW2008MP – Vorderseite 6
- Rückseite 7

Kapitel 3: Anschließen des Switches 8
- Übersicht 8
- Vor Installation des Switches... 9
- Platzierungsoptionen 9
- Anschließen des Switches 12

Kapitel 4: Verwenden der Konsolenschnittselle für die Konfiguration 13
- Übersicht 13
- Konfigurieren der HyperTerminal-Anwendung 13
- Herstellen einer Verbindung mit dem Switch über eine Telnet-Sitzung 14
- Konfigurieren des Switches über die Konsolenschnittstelle 15

Kapitel 5: Verwenden des webbasierten Dienstprogramms für die Konfiguration 27
- Übersicht 27
- Zugreifen auf das webbasierte Dienstprogramm 27
- Registerkarte „Setup“ – Summary 28
- Registerkarte „Setup“ – Network Settings 29
- Registerkarte „Setup“ – Time 30
- Registerkarte „Port Management“ – Port Settings 31
- Registerkarte „Port Management“ – Link Aggregation 34
- Registerkarte „Port Management“ – LACP 35
- Registerkarte „Port Management“ – PoE Power Settings 36
- Registerkarte „VLAN Management“ – Create VLAN 36
- Registerkarte „VLAN Management“ – Port Settings 37
- Registerkarte „VLAN Management“ – Ports to VLAN 38

Registerkarte „VLAN Management“ – VLAN to Ports 39
Registerkarte „VLAN Management“ – GVRP 40
Registerkarte „Statistics“ – RMON Statistics 40
Registerkarte „Statistics“ – RMON History 42
Registerkarte „Statistics“ – RMON Alarm 44
Registerkarte „Statistics“ – RMON Events 45
Registerkarte „Statistics“ – Port Utilization 46
Registerkarte „Statistics“ – 802.1x Statistics 47
Registerkarte „Statistics“ – GVRP Statistics 47
Registerkarte „ACL“ – IP Based ACL 48
Registerkarte „ACL“ – MAC Based ACL 51
Registerkarte „Security“ – ACL Binding 52
Registerkarte „Security“ – RADIUS 52
Registerkarte „Security“ – TACACS+ 53
Registerkarte „Security“ – 802.1x Settings 54
Registerkarte „Security“ – Port Security 55
Registerkarte „Security“ – Multiple Hosts 57
Registerkarte „Security“ – Storm Control 57
QoS 58
Registerkarte „QoS“ – CoS Settings 59
Registerkarte „QoS“ – Queue Settings 59
Registerkarte „QoS“ – DSCP Settings 60
Registerkarte „QoS“ – Bandwidth 60
Registerkarte „QoS“ – Basic Mode 61
Registerkarte „QoS“ – Advanced Mode 61
Spanning Tree 64
Registerkarte „Spanning Tree“ – STP Status 64
Registerkarte „Spanning Tree“ – Global STP 65
Registerkarte „Spanning Tree“ – STP Port Settings 66
Registerkarte „Spanning Tree“ – RSTP Port Settings 67
Registerkarte „Spanning Tree“ – MSTP Properties 69
Registerkarte „Spanning Tree“ – MSTP Instance Settings 69
Registerkarte „Spanning Tree“ – MSTP Interface Settings 70
Registerkarte „Multicast“ – IGMP Snooping 72
Registerkarte „Multicast“ – Bridge Multicast 73
Registerkarte „Multicast“ – Bridge Multicast Forward All 74

Registerkarte „SNMP“ – Global Parameters 74
Registerkarte „SNMP“ – Views 75
Registerkarte „SNMP“ – Group Profile 76
Registerkarte „SNMP“ – Group Membership 77
Registerkarte „SNMP“ – Communities 78
Registerkarte „SNMP“ – Notification Filter 79
Registerkarte „SNMP“ – Notification Recipient 80
Registerkarte „Admin“ – User Authentication 81
Registerkarte „Admin“ – Jumbo Frames 82
Registerkarte „Admin“ – Static Address 82
Registerkarte „Admin“ – Dynamic Address 83
Registerkarte „Admin“ – Logging 84
Registerkarte „Admin“ – Port Mirroring 85
Registerkarte „Admin“ – Cable Test 85
Registerkarte „Admin“ – Save Configuration 86
Registerkarte „Admin“ – Firmware Upgrade 87
Registerkarte „Admin“ – Reboot 87
Registerkarte „Admin“ – Factory Defaults 88
Registerkarte „Admin“ – Server Logs 88
Registerkarte „Admin“ – Memory Logs 89
Registerkarte „Admin“ – Flash Logs 89
Anhang A: Info zu Gigabit Ethernet und Glasfaserkabeln 90
Gigabit Ethernet 90
Glasfaserkabel 90
Anhang B: Windows-Hilfe 91
Anhang C: Downloads mithilfe von Xmodem 92
Schritte im im Startmenü 92
Anhang D: Glossar 94
Anhang E: Technische Daten 102
SRW2008 102
SRW2008MP 106
SRW2008P 110
Anhang F: Gewährleistungsinformationen 114
Anhang G: Rechtliche Hinweise 116
Anhang H: Kontaktinformationen 123

Liste der Abbildungen

Abbildung 2-1: Vorderseite des SRW2008 4
Abbildung 2-2: Vorderseite des SRW2008P 6
Abbildung 2-3: Rückseite des SRW2008P 7
Abbildung 3-1: Typische Netzwerkkonfiguration für den SRW2008P 8
Abbildung 3-2: Befestigen der Halterungen am Switch 10
Abbildung 3-3: Montieren des Switches im Gestell 10
Abbildung 3-4: Ordnungsgemäße Ausrichtung des Geräts bei Wandmontage (waagerecht) 11
Abbildung 3-5: Falsche Ausrichtung bei der Wandmontage des Geräts (senkrecht) 11
Abbildung 3-6: Vorlage für Wandmontage 11
Abbildung 4-1: Auffinden von HyperTerminal 13
Abbildung 4-2: Anschließen Beschreibung 13
Abbildung 4-3: Verbinden mit 13
Abbildung 4-4: COM1-Eigenschaften 14
Abbildung 4-5: Telnet-Anmeldebildschirm 14
Abbildung 4-6: Switch Main Menu (Switch-Hauptmenü) 15
Abbildung 4-7: Menü „System Configuration“ (Menü „Systemkonfiguration“) 16
Abbildung 4-8: Menü „System Information Menu“ (Menü „Systeminformationen“) 17
Abbildung 4-9: Versions (Versionen) 17
Abbildung 4-10: General System Information 17
Abbildung 4-11: Menü „Management Settings“ 18
Abbildung 4-12: Serial Port Configuration 18
Abbildung 4-13: Telnet Configuration (Telnet-Konfiguration) 18
Abbildung 4-14: SSH Configuration (SSH-Konfiguration) 19
Abbildung 4-15: SSH Server Configuration (SSH-Serverkonfiguration) 19

Abbildung 4-16: SSH Status (SSH-Status) 19
Abbildung 4-17: SSH Crypto Key Generation (SSH-Kryptographieschlüsselerzeugung) 20
Abbildung 4-18: SSH Keys Fingerprints (SSH-Schlüssel-Fingerprints) 20
Abbildung 4-19: Username & Password Settings (Benutzernamen- und Kennworteinstellungen) 21
Abbildung 4-20: Security Settings (Sicherheitseinstellungen) 21
Abbildung 4-21: SSL Certificate Generation (SSL-Zertifikaterzeugung) 21
Abbildung 4-22: SSL Certificate (SSL-Zertifikat) 22
Abbildung 4-23: IP Configuration 22
Abbildung 4-24: IP Address Configuration (IP-Adresskonfiguration) 23
Abbildung 4-25: HTTP 23
Abbildung 4-26: HTTPS Configuration (HTTPS-Konfiguration) 23
Abbildung 4-27: Network Configuration (Netzwerkkonfiguration) 24
Abbildung 4-28: Ping-Test 24
Abbildung 4-29: TraceRoute-Test 24
Abbildung 4-30: File Management (Dateiverwaltung) 25
Abbildung 4-31: Restore System Default Settings (Systemstandardeinstellungen wiederherstellen) 25
Abbildung 4-32: Reboot System (System neu starten) 25
Abbildung 4-33: Port Status (Anschlussstatus) 26
Abbildung 4-34: Port Configuration (Anschlusskonfiguration) 26
Abbildung 5-1: Anmeldebildschirm 27
Abbildung 5-2: Setup – Summary (Zusammenfassung) 28
Abbildung 5-3: Setup – Network Settings (Netzwerkeinstellungen) 29
Abbildung 5-4: Setup – Time (Zeit) 30
Abbildung 5-5: Port Management (Anschlussverwaltung) – Port Settings (Anschlusseinstellungen) 31
Abbildung 5-6: Port Settings (Anschlusseinstellungen) – Port Configuration Detail (Details der Anschlusskonfiguration) 32

Abbildung 5-7: Port Management (Anschlussverwaltung) – Link Aggregation 34
Abbildung 5-8: Link Aggregation – Link Aggregation Detail
(Details der Link Aggregation) 34
Abbildung 5-9: Port Management (Anschlussverwaltung) – LACP 35
Abbildung 5-10: Port Management (Anschlussverwaltung) – PoE 36
Abbildung 5-11: VLAN Management (VLAN-Verwaltung) –
Create VLAN (VLAN erstellen) 36
Abbildung 5-12: VLAN Management (VLAN-Verwaltung) –
Port Settings (Anschlusseinstellungen) 37
Abbildung 5-13: VLAN Management (VLAN-Verwaltung) –
Ports to VLAN (Anschlüsse an VLAN) 38
Abbildung 5-14: VLAN Management (VLAN-Verwaltung) –
VLAN to Ports (VLAN an Anschlüsse) 39
Abbildung 5-15: VLAN to Ports (VLAN an Anschlüsse) –
Join VLAN (VLAN beitreten) 39
Abbildung 5-16: VLAN Management (VLAN-Verwaltung) – GVRP 40
Abbildung 5-17: Statistics (Statistik) – RMON Statistics (RMON-Statistik) 41
Abbildung 5-18: Statistics (Statistik) – RMON History (RMON-Verlauf) 42
Abbildung 5-19: RMON History-Tabelle (RMON-Verlauf) 43
Abbildung 5-20: Statistics (Statistik) – RMON Alarm (RMON-Alarmmeldung) 44
Abbildung 5-21: Statistics (Statistik) – RMON Events (RMON-Ereignisse) 45
Abbildung 5-22: RMON Events (RMON-Ereignisse) –
Events Log (Ereignisprotokoll) 46
Abbildung 5-23: Statistics (Statistik) – Port Utilization (Anschlussauslastung) 46
Abbildung 5-24: Statistics (Statistik) – 802.1x Statistics (802.1x-Statistik) 47
Abbildung 5-25: Statistics (Statistik) – GVRP Statistics (GVRP-Statistik) 47
Abbildung 5-26: ACL (Zugriffssteuerungsliste) – IP Based ACL
(IP-basierte Zugriffssteuerungsliste) 49
Abbildung 5-27: ACL (Zugriffssteuerungsliste) – MAC Based ACL
(MAC-basierte Zugriffssteuerungsliste) 51

Abbildung 5-28: Security (Sicherheit) – ACL Binding
(Bindung an Zugriffssteuerungsliste) 52
Abbildung 5-29: Security (Sicherheit) – RADIUS (RADIUS) 52
Abbildung 5-30: Security (Sicherheit) – TACACS+ 53
Abbildung 5-31: Security (Sicherheit) – 802.1x Settings
(802.1x-Einstellungen) 54
Abbildung 5-32: 802.1x Settings (802.1x-Einstellungen) –
Setting Timer (Zeitlimit einstellen) 55
Abbildung 5-33: Security (Sicherheit) – Port Security (Anschlusssicherheit) 55
Abbildung 5-34: Security (Sicherheit) – Multiple Hosts (Mehrere Hosts) 57
Abbildung 5-35: Security (Sicherheit) – Storm Control 57
Abbildung 5-36: QoS (Dienstgüte) – CoS Settings
(Einstellungen der Dienstklasse) 59
Abbildung 5-37: QoS (Dienstgüte) – Queue Settings
(Warteschlangeneinstellungen) 59
Abbildung 5-38: QoS (Dienstgüte) – DSCP Settings (DSCP-Einstellungen) 60
Abbildung 5-39: QoS (Dienstgüte) – Bandwidth (Bandbreite) 60
Abbildung 5-40: QoS (Dienstgüte) – Basic Mode (Grundmodus) 61
Abbildung 5-41: QoS (Dienstgüte) – Advanced Mode (Erweiterter Modus) 61
Abbildung 5-42: Advanced Mode (Erweiterter Modus) –
Out of Profile DSCP (Profilunabhängiger DSCP) 62
Abbildung 5-43: Advanced Mode (Erweiterter Modus) –
Policy Name (Richtlinienname) 62
Abbildung 5-44: Advanced Mode (Erweiterter Modus) –
New Class Map (Neue Klassenzuordnung) 62
Abbildung 5-45: Advanced Mode (Erweiterter Modus) –
New Aggregate Policer (Neuer aggregierter Überwacher) 63
Abbildung 5-46: Spanning Tree – STP Status (STP-Status) 64
Abbildung 5-47: Spanning Tree – Global STP (Globales STP) 65

Abbildung 5-48: Spanning Tree – STP Port Settings (STP-Anschlusseinstellungen) 66
Abbildung 5-49: Spanning Tree – RSTP Port Settings (RSTP-Anschlusseinstellungen) 67
Abbildung 5-50: Spanning Tree – MSTP Properties (MSTP-Eigenschaften) 69
Abbildung 5-51: Spanning Tree – MSTP Instance Settings (MSTP-Instanzeinstellungen) 69
Abbildung 5-52: Spanning Tree – MSTP Interface Settings (MSTP-Schnittstelleneinstellungen) 70
Abbildung 5-53: Multicast – IGMP Snooping 72
Abbildung 5-54: Multicast – Bridge Multicast (Bridge Multicast) 73
Abbildung 5-55: Multicast – Bridge Multicast Forward All (Bridge Multicast, alle weiterleiten) 74
Abbildung 5-56: SNMP – Global Parameters (Globale Parameter) 74
Abbildung 5-57: SNMP – Views (Ansichten) 75
Abbildung 5-58: SNMP – Group Profile (Gruppenprofil) 76
Abbildung 5-59: SNMP – Group Membership (Gruppenmitgliedschaft) 77
Abbildung 5-60: SNMP – Communities 78
Abbildung 5-61: SNMP – Notification Filter (Benachrichtigungsfilter) 79
Abbildung 5-62: Notification Recipient (Benachrichtigungsempfänger) 80
Abbildung 5-63: Admin – User Authentication (Benutzerauthentifizierung) 81
Abbildung 5-64: Jumbo Frames (Großrahmen) 82
Abbildung 5-65: Admin – Static Address (Statische Adresse) 82
Abbildung 5-66: Admin – Dynamic Address (Dynamische Adresse) 83
Abbildung 5-67: Admin – Logging (Protokollierung) 84
Abbildung 5-68: Admin – Port Mirroring (Anschlussspiegelung) 85
Abbildung 5-69: Admin – Cable Test (Kabeltest) 85
Abbildung 5-70: Admin – Save Configuration (Konfiguration speichern) 86
Abbildung 5-71: Admin – Firmware Upgrade (Firmwareaktualisierung) 87
Abbildung 5-72: Admin – Reboot (Neustart) 87

Abbildung 5-73: Admin – Factory Defaults (Werkseinstellungen) 88
Abbildung 5-74: Admin – Server Logs (Serverprotokolle) 88
Abbildung 5-75: Admin – Memory Logs (Speicherprotokolle) 89
Abbildung 5-76: Admin – Flash Logs (Flashprotokolle) 89
Abbildung C-1: Startmenü 92
Abbildung C-2: Meldung zu autom. Hochfahren des Switches 92
Abbildung C-3: Send File (Datei senden) 93
Abbildung C-4: Download 93

Kapitel 1: Einleitung

Willkommen

In diesem Handbuch werden fünf Produktmodelle beschrieben.

- **SRW2008** – 8-Port 10/100/1000 Ethernet Switch with WebView.
  Verfügt über acht 10/100/1000 RJ-45-Anschlüsse und 2 freigegebene MiniGBIC-Anschlüsse.

- **SRW2008MP** – 8-Port 10/100/1000 Ethernet Switch with WebView and
  Maximum POE (Power Over Ethernet)
  Verfügt über acht 10/100/1000 RJ-45-Anschlüsse und 2 freigegebene MiniGBIC-Anschlüsse.

- **SRW2008P** – 8-Port 10/100/1000 Ethernet Switch with WebView and POE (Power over Ethernet)
  Verfügt über acht 10/100/1000 RJ-45-Anschlüsse und 2 freigegebene MiniGBIC-Anschlüsse.

Steht eine Funktion für alle Modelle zur Verfügung, wird in diesem Handbuch für die Modellnummer SRW2008*x* angegeben. Wird eine bestimmte Modellnummer erwähnt, steht die Funktion ausschließlich für dieses Modell zur Verfügung.

Der Linksys WebView Managed Switch ermöglicht eine sichere Erweiterung des Netzwerks. Die Konfiguration des Switches wird mit SSL (Secure Socket Layer) für Webzugriff gesichert. Die Benutzersteuerung wird mit 802.1x-Sicherheit gesichert, wobei der RADIUS-Authentifizierungsmechanismus verwendet wird. Die Benutzersteuerung kann auch mithilfe MAC-basierter Filterung verwaltet werden.

Dank umfassender QoS-Funktionen ist die Lösung ideal für Echtzeitanwendungen wie Sprach- und Videoaufnahmen. Die Layer 4-Prioritätswarteschlangen erleichtern in Verbindung mit den Planungsmethoden „Weighted Round Robin“ und „Strict Priority“ die effiziente gleichzeitige Verwaltung von Echtzeit- und Datenverkehr, wodurch den QoS-Anforderungen entsprochen werden kann. Einzelnen Benutzern oder Anwendungen kann mithilfe verschiedener Class of Service-Optionen Priorität vor anderen Benutzern bzw. Anwendungen gewährt werden – nach Anschluss, Layer 2-Priorität (802.1p) und Layer 3-Priorität (TOS oder DSCP). Intelligent Broadcast und Multicast Storm Control verringern die Auswirkungen dieser Datenverkehrstypen auf regulären Datenverkehr. IGMP Snooping überträgt hohe Bandbreiten beanspruchenden Videodatenverkehr ausschließlich an die Anfordernden und vermeidet dadurch eine „Überflutung“ der anderen Benutzer. Eingehender Datenverkehr kann kontrolliert und ausgehender Datenverkehr bearbeitet werden, wodurch die Steuerung des Netzwerkzugriffs und des Datenverkehrsflusses ermöglicht wird.

Die Geräte bieten Funktionen zur Erweiterung der Switches. Link Aggregation ermöglicht die Einrichtung mehrerer Bündelungen mit hoher Bandbreite zwischen Switches. Dies sorgt für eine höhere Zuverlässigkeit des Systems, da dieses auch bei Ausfall einer der Leitungen betriebsbereit bleibt. Mithilfe von Spanning Tree (STP),

Fast Spanning Tree und Rapid Spanning Tree (RSTP) wird ein Netz aus Switches erstellt, das die Verfügbarkeit des Systems erhöht.

Die umfangreichen Verwaltungsfunktionen der WebView-Switches beinhalten SNMP-, RMON-, Telnet- und HTTP-Verwaltungsoptionen. Mithilfe dieser Optionen können die Geräte im Netzwerk flexibel integriert und verwaltet werden.

Die Modelle SRW2008P und SRW2008MP unterstützen automatisches Load Sensing – Die Schaltung zur Regelung der Stromversorgung erkennt automatisch Power over Ethernet auf dem Access Point, bevor die Stromversorgung hergestellt wird. Die Stromversorgung für Ethernet wird für feste 10/100/1000 Base-T/TX-Anschlüsse begrenzt. Der SRW2008MP erreicht auf acht Anschlüssen gleichzeitig eine maximale Ausgangsleistung pro PoE-Anschluss von bis zu 15,4 W, wohingegen der SRW2008P die maximale Ausgangsleistung gleichzeitig auf vier Anschlüssen oder die halbe Leistung auf acht Anschlüssen bereitstellt.

Inhalt des Benutzerhandbuchs

In diesem Benutzerhandbuch werden die zur Einrichtung und Verwendung des Switches erforderlichen Schritte beschrieben.

- Kapitel 1: Einleitung
  In diesem Kapitel werden die Anwendungen des Switches und der Inhalt des Benutzerhandbuchs beschrieben.

- Kapitel 2: Aufbau des Switches
  In diesem Kapitel werden die physischen Eigenschaften des Switches beschrieben.

- Kapitel 3: Anschließen des Switches
  In diesem Kapitel wird das Aufstellen und Anschließen des Switches erläutert.

- Kapitel 4: Verwenden der Konsolenschnittselle für die Konfiguration
  In diesem Kapitel erhalten Sie Informationen zur Verwendung der Konsolenschnittstelle bei der Konfiguration des Switches.

- Kapitel 5: Verwenden des webbasierten Dienstprogramms für die Konfiguration
  In diesem Kapitel wird die Konfiguration des Switches mithilfe des webbasierten Dienstprogramms beschrieben.

- Anhang A: Info zu Gigabit Ethernet und Glasfaserkabeln
  In diesem Anhang finden Sie allgemeine Beschreibungen von Gigabit-Ethernet- und Glasfaserkabeln.

- Anhang B: Windows-Hilfe
  In diesem Anhang wird die Verwendung der Windows-Hilfe für Anweisungen zum Netzwerkbetrieb beschrieben – z. B. das Einrichten eines TCP/IP-Protokolls.

- Anhang C: Downloads mithilfe von Xmodem
  In diesem Anhang erhalten Sie Informationen zum Herunterladen von Software auf den Switch mithilfe von Xmodem.

- Anhang D: Glossar
  Hier finden Sie ein kurzes Glossar mit häufig im Netzwerkbereich verwendeter Terminologie.

- Anhang E: Technische Daten
  Hier finden Sie die technischen Daten des Switches.

- Anhang F: Gewährleistungsinformationen
  Hier finden Sie die Gewährleistungsinformationen des Switches.

- Anhang G: Rechtliche Hinweise
  Hier finden Sie die rechtlichen Hinweise zum Switch.

- Anhang H: Kontaktinformationen
  Hier erhalten Sie die Kontaktinformationen für verschiedene Ansprechpartner bei Linksys, einschließlich des technischen Supports.

Kapitel 2: Aufbau des Switches

Übersicht

Die Switches unterscheiden sich hinsichtlich Anzahl und Arten von LEDs und Anschlüssen. Die Vorderseite der einzelnen Switches wird auf einer der folgenden Seiten angezeigt. Die Rückseite ist bei allen fünf Modellen identisch.

SRW2008 – Vorderseite

Die LEDs des Switches befinden sich auf der Vorderseite des Routers.

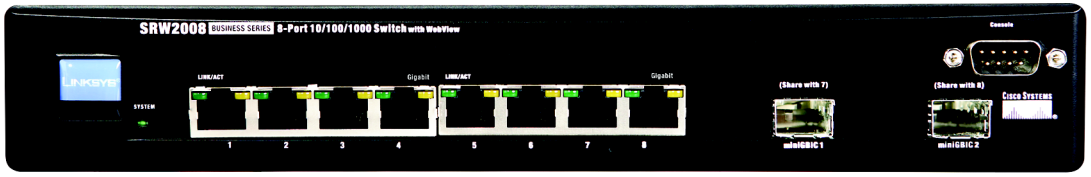


Abbildung 2-1: Vorderseite des SRW2008

LEDs

System — Grün. Die **SYSTEM**-LED leuchtet auf, wenn der Switch eingeschaltet wird.

Link/Act — Grün. Die **LINK/ACT**-LED leuchtet auf und zeigt eine funktionierende Netzwerkverbindung mit einem angeschlossenen Gerät über den entsprechenden Anschluss (1 bis 8) an. Die LED leuchtet auf, wenn der Switch Daten über diesen Anschluss sendet oder empfängt.

Gigabit — Orange. Die **Gigabit**-LED leuchtet auf, wenn auf dem entsprechenden Anschluss (1 bis 8) eine 1000 MBit/s-Verbindung besteht.

Anschlüsse

1-8 Der Switch verfügt über acht Ethernet-Netzwerkanschlüsse mit Auto-Sensing. Für die Anschlüsse werden RJ-45-Stecker verwendet. Die Fast Ethernet-Anschlüsse unterstützen Geschwindigkeiten von 10 MBit/s, 100 MBit/s oder 1000 MBit/s. Die Anschlüsse können im Halb- und Vollduplexmodus betrieben werden. Die Auto-Sensing-Technologie ermöglicht jedem Anschluss das automatische Erkennen der Geschwindigkeit des angeschlossenen Geräts (10 MBit/s, 100 MBit/s oder 1000 MBit/s) und die entsprechende Anpassung von Geschwindigkeit und Duplex.

Konsole Am Konsolenanschluss kann ein serielles Kabel mit dem seriellen Anschluss eines PCs verbunden werden, um mit dem HyperTerminal-Programm des PCs eine Konfiguration vorzunehmen. Weitere Informationen erhalten Sie in *Kapitel 4: Verwenden der Konsolenschnittstelle für die Konfiguration*.

MiniGBIC 1/2 Der Mini-GBIC (Gigabit Interface Converter)-Anschluss ist ein Verbindungspunkt für ein Mini-GBIC-Erweiterungsmodul. Damit kann ein Switch per Glasfaserkabel mit einem anderen Switch verbunden werden. Über den MiniGBIC-Anschluss werden mit Geschwindigkeiten von bis zu 1000 MBit/s Verbindungen mit Segmenten eines Hochgeschwindigkeitsnetzwerks oder einzelnen Arbeitsstationen hergestellt.

Verwenden Sie die MGBT1-, MGBSX1- oder MGBLH1-Mini-GBIC-Module von Linksys mit dem Switch. Für das MGBSX1- und das MGBLH1-Modul wird ein Glasfaserkabel mit LC-Steckern und für das MGBT1-Modul ein Ethernet-Kabel der Kategorie 5e mit einem RJ-45-Stecker benötigt.

SRW2008P, SRW2008MP – Vorderseite

Die LEDs des Switches befinden sich auf der Vorderseite des Routers.

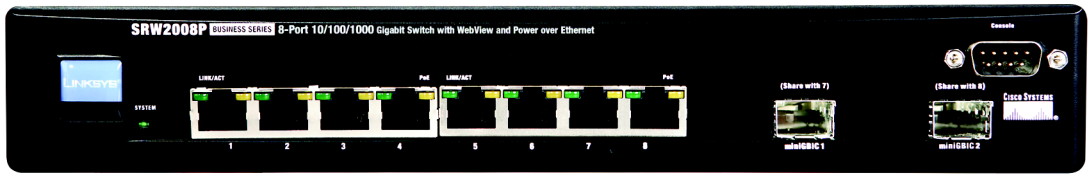


Abbildung 2-2: Vorderseite des SRW2008P

LEDs

System Grün. Die **SYSTEM**-LED leuchtet auf, wenn der Switch eingeschaltet wird.

Link/Act Grün. Die **LINK/ACT**-LED leuchtet auf und zeigt eine funktionierende Netzwerkverbindung mit einem angeschlossenen Gerät über den entsprechenden Anschluss (1 bis 8) an. Die LED leuchtet auf, wenn der Switch Daten über diesen Anschluss sendet oder empfängt.

PoE Orange. Die **PoE**-LED leuchtet auf, wenn ein Gerät unter Verwendung von Power over Ethernet am entsprechenden Anschluss (1 bis 8) angeschlossen ist.

HINWEIS: Der SRW2008P unterstützt bis zu vier Anschlüsse mit 15,4 W oder bis zu acht Anschlüsse mit 7,5 W.
Der SRW2008MP unterstützt bis zu acht Anschlüsse mit 15,4 W.

Anschlüsse

1-8 Der Switch verfügt über acht Ethernet-Netzwerkanschlüsse mit Auto-Sensing. Für die Anschlüsse werden RJ-45-Stecker verwendet. Die Fast Ethernet-Anschlüsse unterstützen Geschwindigkeiten von 10 MBit/s oder 100 MBit/s. Die Anschlüsse können im Halb- und Vollduplexmodus betrieben werden. Die Auto-Sensing-Technologie ermöglicht jedem Anschluss das automatische Erkennen der Geschwindigkeit des angeschlossenen Geräts (10 MBit/s oder 100 MBit/s) und die entsprechende Anpassung von Geschwindigkeit und Duplex.

MiniGBIC1/2 Der Mini-GBIC (Gigabit Interface Converter)-Anschluss ist ein Verbindungspunkt für ein Mini-GBIC-Erweiterungsmodul. Damit kann ein Switch per Glasfaser mit einem anderen Switch verbunden werden. Über den MiniGBIC-Anschluss werden mit Geschwindigkeiten von bis zu 1000 MBit/s Verbindungen mit Segmenten eines Hochgeschwindigkeitsnetzwerks oder einzelnen Arbeitsstationen hergestellt.

Verwenden Sie die MGBT1-, MGBSX1- oder MGBLH1-Mini-GBIC-Module von Linksys mit dem Switch. Für das MGBSX1- und das MGBLH1-Modul wird ein Glasfaserkabel mit LC-Steckern und für das MGBT1-Modul ein Ethernet-Kabel der Kategorie 5e mit einem RJ-45-Stecker benötigt.

Konsole Am Konsolenanschluss kann ein serielles Kabel mit dem seriellen Anschluss eines PCs verbunden werden, um mit dem HyperTerminal-Programm des PCs eine Konfiguration vorzunehmen. Weitere Informationen erhalten Sie in *Kapitel 4: Verwenden der Konsolenschnittstelle für die Konfiguration*.

Rückseite

Der Stromanschluss befindet sich auf der Rückseite des Switches.

Abbildung 2-3: Rückseite des SRW2008P

Power Am **Stromanschluss** wird das mitgelieferte Stromkabel angeschlossen.

HINWEIS: Wenn der Switch zurückgesetzt werden soll, ziehen Sie das Netzkabel an der Rückseite des Geräts heraus. Warten Sie einen Moment, und stecken Sie das Kabel anschließend wieder ein.

Kapitel 3: Anschließen des Switches

Übersicht

In diesem Kapitel wird das Anschließen von Netzwerkgeräten an den Switch erläutert. Nachfolgend sehen Sie die Darstellung einer typischen Netzwerkkonfiguration.

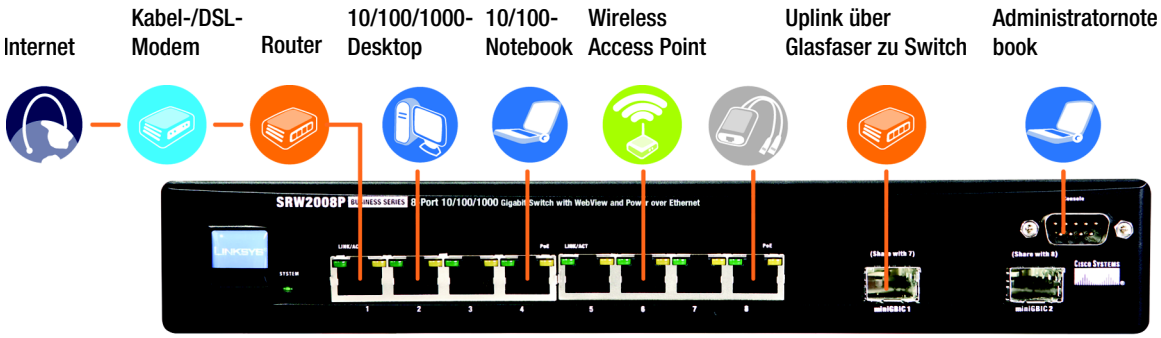


Abbildung 3-1: Typische Netzwerkkonfiguration für den SRW2008P

Stellen Sie beim Anschließen Ihrer Netzwerkgeräte sicher, dass bei der Verkabelung der maximal zulässige Abstand zwischen den Geräten nicht überschritten wird (siehe folgende Tabelle):

Tabelle 1: Zulässiger Abstand (max.)

Von	Zu	Maximaler Abstand
Switch	Switch oder Hub*	100 Meter
Hub	Hub	5 Meter
Switch oder Hub	Computer	100 Meter

*Bei einem Hub handelt es sich um jeden beliebigen Typ eines 100 MBit/s-Hubs, einschließlich regulärer Hubs und stapelbarer Hubs. Zwischen zwei miteinander verbundenen 10 MBit/s-Hubs darf der Abstand maximal 100 Meter betragen.

Vor Installation des Switches...

Beachten Sie bei der Wahl des Standorts für den Switch Folgendes:

- Stellen Sie sicher, dass der Switch frei zugänglich ist und die Kabel problemlos angebracht werden können.
- Verlegen Sie Kabel nicht in Bereichen, an denen elektrische Störungen auftreten und nicht in der Nähe von Stromleitungen und fluoreszierenden Beleuchtungsvorrichtungen.
- Setzen Sie den Switch nicht Nässe oder Feuchtigkeit aus.
- Für eine ausreichende Kühlung des Switches ist ein Mindestabstand von 50 mm zu einem anderen Gegenstand erforderlich.
- Stellen Sie nicht mehr als vier freistehende Switches übereinander auf.

Platzierungsoptionen

Vor dem Anschluss von Kabeln an den Switch muss dieser zuerst aufgestellt werden. Stellen Sie den Switch auf seine vier Gummifüßchen, wenn Sie ihn auf einem Schreibtisch aufstellen möchten, oder montieren Sie den Switch in einem standardmäßigen 19 Zoll breiten und 1U hohen Gestell.

Aufstellen auf Schreibtisch

1. Bringen Sie die Gummifüße an die ausgesparten Bereiche unten am Switch an.
2. Stellen Sie den Switch auf einem Schreibtisch in der Nähe einer Wechselstromquelle auf.
3. Sorgen Sie für eine ausreichende Belüftung des Switches, und beachten Sie die in den technischen Daten genannten Einschränkungen hinsichtlich der Umgebung.
4. Fahren Sie mit dem Abschnitt „Anschließen des Switches“ fort.

Gestellmontage

Beachten Sie bei der Montage des Switches in einem beliebigen standardmäßigen 19 Zoll breiten und 1U hohen Gestell folgende Anweisungen:

1. Stellen Sie den Switch auf einer festen und flachen Oberfläche mit der Vorderseite nach vorne auf.
2. Befestigen Sie mit den im Lieferumfang enthaltenen Schrauben eine Gestellhalterung an einer Seite des Switches. Befestigen Sie anschließend die andere Halterung an der gegenüberliegenden Seite des Geräts.
3. Die Halterungen müssen ordnungsgemäß am Switch befestigt sein.
4. Verwenden Sie zur sicheren Fixierung der Klammern am Gestell die entsprechenden Schrauben (nicht im Lieferumfang enthalten).
5. Fahren Sie mit dem Abschnitt „Anschließen des Switches“ fort.

WICHTIG: Verwenden Sie die zusammen mit den Montagehalterungen gelieferten Schrauben. Durch ungeeignete Schrauben könnte der Switch beschädigt werden und die Garantie erlöschen.

Abbildung 3-2: Befestigen der Halterungen am Switch

Abbildung 3-3: Montieren des Switches im Gestell

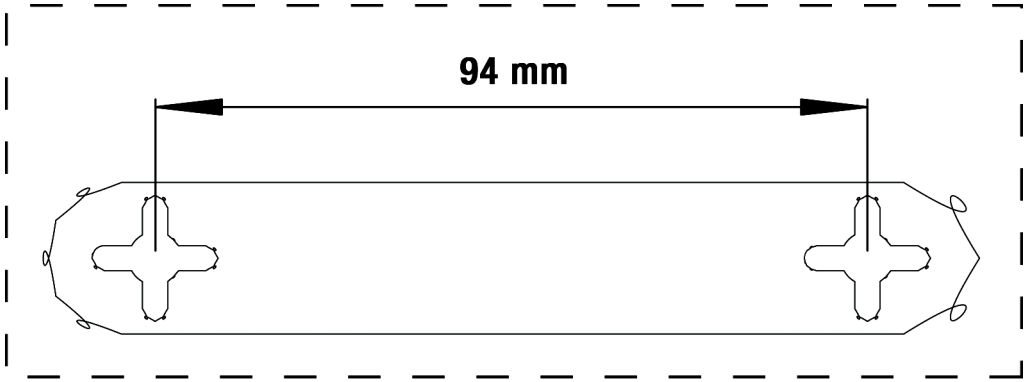
Wandmontage

Bei einer Wandmontage des Switches sollte der Switch waagerecht angebracht werden. Die Vorderseite sollte entweder nach oben oder unten zeigen (siehe Abbildung 3-4). Das Gerät sollte nicht senkrecht montiert werden (siehe Abbildung 3-5).

Zur Montage des Switches werden zwei geeignete Schrauben benötigt.

1. Suchen Sie eine Stelle aus, an der Sie den Switch montieren möchten. Die Wand muss glatt, flach, trocken und stabil sein, und der Standort des Routers muss in Reichweite der Steckdose liegen.
2. Bohren Sie zwei Löcher in die Wand. Bohren Sie die Löscher in einem Abstand von 94 mm. Die Vorlage kann über diese Seite ausgedruckt werden.
3. Fixieren Sie in jedem Loch eine Schraube, und lassen Sie 3 mm des Schraubenkopfs aus dem Loch herausstehen.
4. Bringen Sie den Switch so an, dass sich die Öffnungen für die Wandmontage auf gleicher Höhe mit den zwei Schrauben befinden.
5. Halten Sie die Öffnungen für die Wandmontage über die Schrauben, und schieben Sie den Switch nach unten, bis die Schrauben genau in die Öffnungen für die Wandmontage passen.

Herzlichen Glückwunsch! Die Wandmontage des Switches ist abgeschlossen.



Drucken Sie diese Seite mit einer Größe von 100 % aus, schneiden Sie entlang der gepunkteten Linie, und halten Sie das Blatt gegen die Wand, um die Löcher exakt im erforderlichen Abstand zu bohren.

Abbildung 3-6: Vorlage für Wandmontage

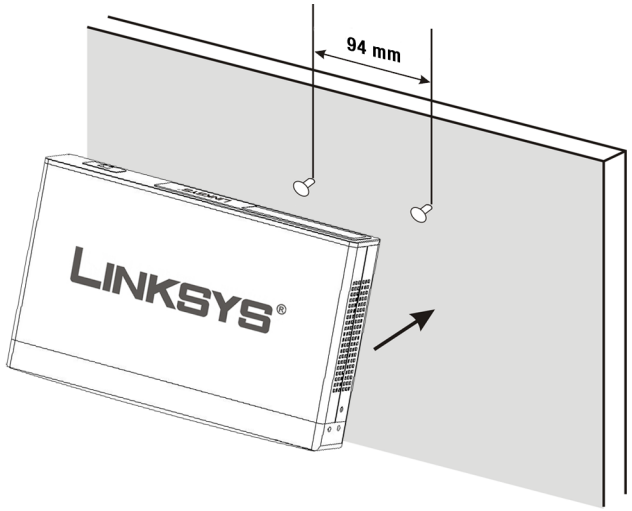


Abbildung 3-4: Ordnungsgemäße Ausrichtung des Geräts bei Wandmontage (waagerecht)

WICHTIG: Montieren Sie den Switch bei einer Wandmontage waagerecht. Montieren Sie den Switch nicht senkrecht.

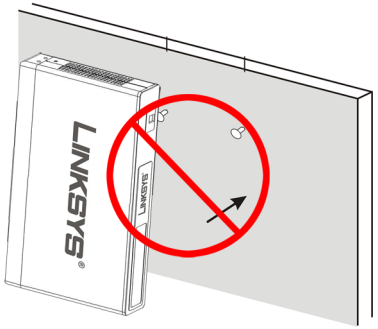


Abbildung 3-5: Falsche Ausrichtung bei der Wandmontage des Geräts (senkrecht)

Anschließen des Switches

Führen Sie zum Anschließen von Netzwerkgeräten an den Switch folgende Anweisungen aus:

1. Stellen Sie sicher, dass alle Geräte, die an den Switch angeschlossen werden, ausgeschaltet sind.
2. Schließen Sie bei 10/100 MBit/s-Geräten ein Ethernet-Netzwerkkabel an einen der nummerierten Anschlüsse am Switch an. Verbinden Sie bei 1000 MBit/s-Geräten ein Ethernet-Netzwerkkabel der Kategorie 5e mit einem der nummerierten Anschlüsse am Switch.
3. Verbinden Sie das andere Ende des Kabels mit einem PC oder einem anderen Netzwerkgerät.
4. Wiederholen Sie zum Anschließen zusätzlicher Geräte die Schritte 2 und 3.
5. Verbinden Sie bei Verwendung eines Mini-GBIC-Anschlusses das Mini-GBIC-Modul mit dem Mini-GBIC-Anschluss. Genaue Anweisungen finden Sie in der Moduldokumentation.
6. Möchten Sie den Switch mithilfe der Konsolenschnittstelle des Switches konfigurieren, verbinden Sie das im Lieferumfang enthaltene serielle Kabel mit dem Konsolenanschluss des Switches, und ziehen Sie die Halteschrauben fest. Verbinden Sie das andere Ende des Kabels mit dem seriellen Anschluss des PCs. (Auf diesem PC muss die VT100-Terminalemulationssoftware (z. B. HyperTerminal) installiert sein.)
7. Schließen Sie das im Lieferumfang enthaltene Netzkabel an den Stromanschluss des Switches an, und stecken Sie das andere Ende in eine Steckdose.
8. Schalten Sie die an diesen Switch angeschlossenen Netzwerkgeräte an. Am Switch leuchtet die jeweilige Link/Act-LED eines aktiven Anschlusses auf. Verfügt ein Anschluss über eine aktive Gigabit-Verbindung, leuchtet auch die entsprechende Gigabit-LED auf.

Informationen zum Konfigurieren des Switches über die Konsolenbenutzeroberfläche erhalten Sie in *Kapitel 4: Verwenden der Konsolenschnittstelle für die Konfiguration*.

Informationen zum Konfigurieren des Switches über das webbasierte Dienstprogramm erhalten Sie in *Kapitel 5: Verwenden des webbasierten Dienstprogramms für die Konfiguration*.

WICHTIG: Verwenden Sie das zusammen mit dem Switch gelieferte Netzkabel. Ein anderes Netzkabel könnte den Switch beschädigen.

HINWEIS: Wenn der Switch zurückgesetzt werden soll, ziehen Sie das Netzkabel an der Rückseite des Geräts heraus. Warten Sie einen Moment, und stecken Sie das Kabel anschließend wieder ein.

Kapitel 4: Verwenden der Konsolenschnittselle für die Konfiguration

Übersicht

Der Switch verfügt über eine menügesteuerte Konsolenschnittstelle für die grundlegende Konfiguration des Switches und die Netzwerkverwaltung. Der Switch kann mithilfe der Befehlszeilenschnittstelle über die Konsolenschnittstelle oder über eine Telnet-Verbindung konfiguriert werden. In diesem Kapitel wird die Konfiguration der Konsolenschnittstelle erläutert. Die Konfiguration kann auch mithilfe des Webdienstprogramms durchgeführt werden (siehe nächstes Kapitel).

Konfigurieren der HyperTerminal-Anwendung

Vor Verwendung der Konsolenschnittstelle muss die HyperTerminal-Anwendung auf dem PC konfiguriert werden.

1. Klicken Sie auf die Schaltfläche **Start**. Wählen Sie **Programme** und anschließend **Zubehör** aus. Wählen Sie die Option **Kommunikation** aus. Wählen Sie in diesem Menü die Option **HyperTerminal** aus.

2. Geben Sie auf dem Bildschirm *Beschreibung der Verbindung* einen Namen für die Verbindung ein. Im vorliegenden Beispiel lautet der Name der Verbindung SRW2008. Wählen Sie ein Symbol für die Anwendung aus. Klicken Sie anschließend auf **OK**.

3. Wählen Sie auf dem Bildschirm *Verbinden mit* einen Anschluss für die Kommunikation mit dem Switch aus: **COM1**, **COM2** oder **TCP/IP**.

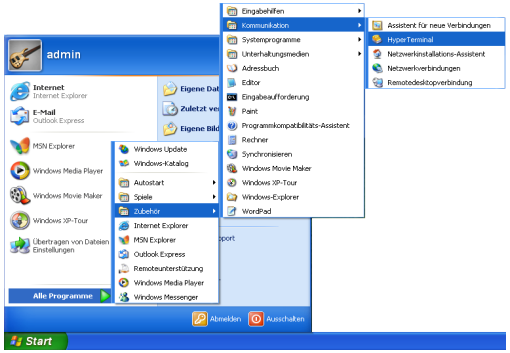


Abbildung 4-1: Auffinden von HyperTerminal

Abbildung 4-2: Anschließen Beschreibung

Abbildung 4-3: Verbinden mit

4. Legen Sie für den seriellen Anschluss folgende Einstellungen fest:

   Bits pro Sekunde: **38400**

   Datenbits: **8**

   Parität: **Keine**

   Stoppbits: **1**

   Datenflusssteuerung: **Keine**

   Klicken Sie anschließend auf **OK**.

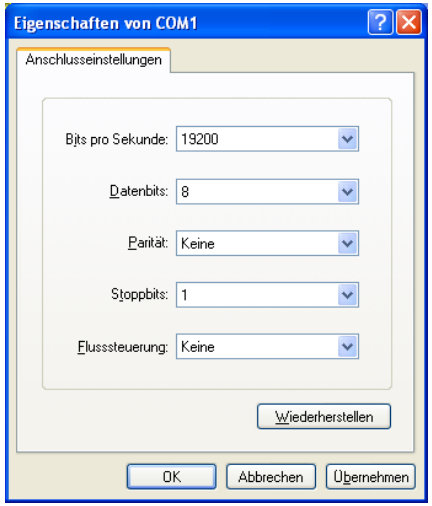


Abbildung 4-4: COM1-Eigenschaften

Herstellen einer Verbindung mit dem Switch über eine Telnet-Sitzung

Öffnen Sie einen Befehlszeileneditor, und geben Sie **telnet 192.168.1.254** ein. Drücken Sie anschließend die **EINGABETASTE**.

Der Anmeldebildschirm wird angezeigt. Klicken Sie beim ersten Öffnen der Befehlszeilenschnittstelle auf **Edit**, und drücken Sie die EINGABETASTE. Geben Sie ins Feld *User Name* den Benutzernamen **admin** ein. Lassen Sie das Feld *Password* leer.

Drücken Sie die **Esc**-Taste, um zum Anmeldebildschirm zurückzukehren. Navigieren Sie mit der rechten Pfeiltaste zu **Execute**, und drücken Sie zum Öffnen der Befehlszeilenschnittstelle die **EINGABETASTE**.

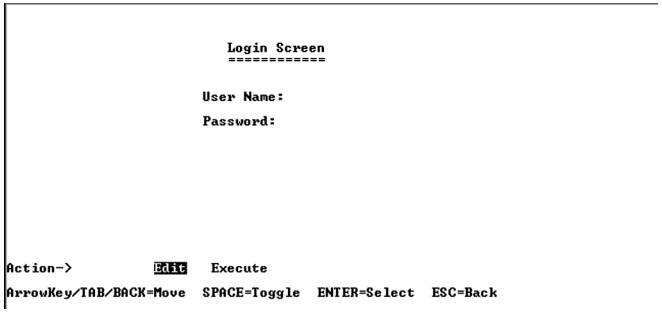


Abbildung 4-5: Telnet-Anmeldebildschirm

Konfigurieren des Switches über die Konsolenschnittstelle

Die Konsolenbildschirme bestehen aus mehreren Menüs. Jedes Menü beinhaltet mehrere Optionen, die senkrecht aufgeführt sind. Eine Menüoption wird durch Markieren ausgewählt; durch Drücken der **EINGABETASTE** wird die markierte Option aktiviert.

Navigieren Sie durch die Menüs und Aktionen der Konsolenschnittstelle, indem Sie die NACH-OBEN- bzw. die NACH-UNTEN-TASTE und die NACH-LINKS- bzw. die NACH-RECHTS-TASTE verwenden. Drücken Sie zum Auswählen einer Menüoption die EINGABETASTE und ESC, um zur vorigen Auswahl zurückzukehren. Menüoptionen und beliebige eingegebene oder vorhandene Werte werden markiert. Unten auf dem Bildschirm werden die verfügbaren Aktionen aufgeführt.

Switch Main Menu (Switch-Hauptmenü)

Auf dem Bildschirm für das Hauptmenü des Systems werden folgende Optionen angezeigt:

1. System Configuration Information Menu
2. Port Status (Anschlussstatus)
3. Port Configuration (Anschlusskonfiguration)
4. Help
0. Logout

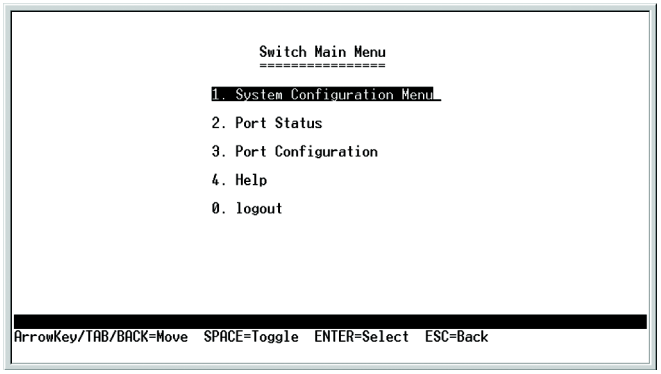


Abbildung 4-6: Switch Main Menu (Switch-Hauptmenü)

Menü „System Configuration“ (Menü „Systemkonfiguration“)

Auf dem Bildschirm *System Configuration Menu* sind folgende Optionen verfügbar:

1. System Information
2. Management Settings
3. User & Password Settings
4. Security Settings (Sicherheitseinstellungen)
5. IP Configuration
6. File Management (Dateiverwaltung)
7. Restore System Default Settings (Systemstandardeinstellungen wiederherstellen)
8. Reboot System (System neu starten)
0. Back to main menu

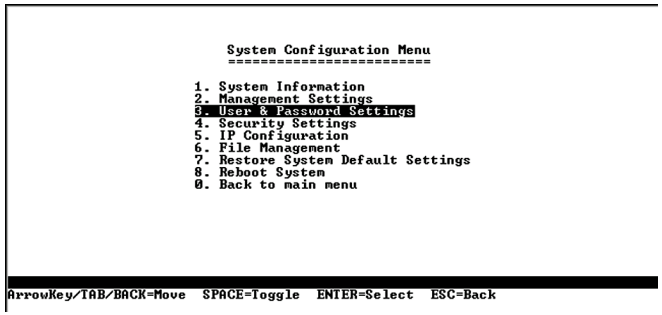


Abbildung 4-7: Menü „System Configuration“ (Menü „Systemkonfiguration“)

System Information

Auf diesem Bildschirm können die Firmwareversionen und allgemeine Systeminformationen des Switches überprüft werden.

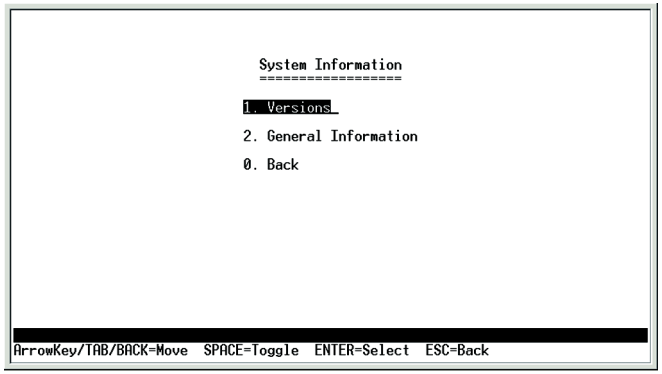


Abbildung 4-8: Menü „System Information Menu“ (Menü „Systeminformationen“)

Versions (Versionen)

Auf dem Bildschirm *Versions* werden die Start-, Software- und Hardwarefirmwareversionen angezeigt.

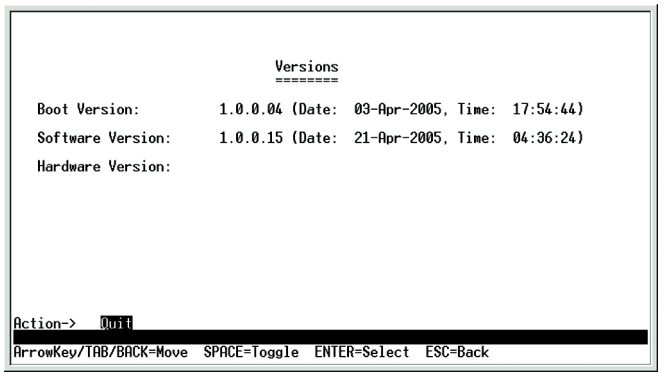


Abbildung 4-9: Versions (Versionen)

General System Information

Auf dem Bildschirm *General System Information* werden Beschreibung, Systembetriebszeit, System-MAC-Adresse, Systemkontakt, Systemname und Systemstandort des Switches angezeigt.

Wählen Sie **Edit** aus, und drücken Sie die **EINGABETASTE**, um Änderungen vorzunehmen. Drücken Sie anschließend **ESC**, um zum Menü *Action* zurückzukehren. Wählen Sie **Save** aus, und drücken Sie zum Speichern der Änderungen auf die **EINGABETASTE**. Wählen Sie zum Schließen des Bildschirms **Quit** aus, und drücken Sie die **EINGABETASTE**.

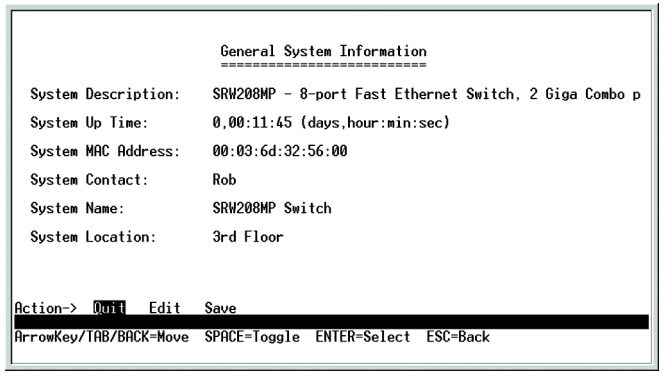


Abbildung 4-10: General System Information

Management Settings

Auf dem Bildschirm *Management Settings* können Sitzungen für serielle Anschlüsse, Telnet-Sitzungen oder Secure Telnet (SSH) konfiguriert werden.

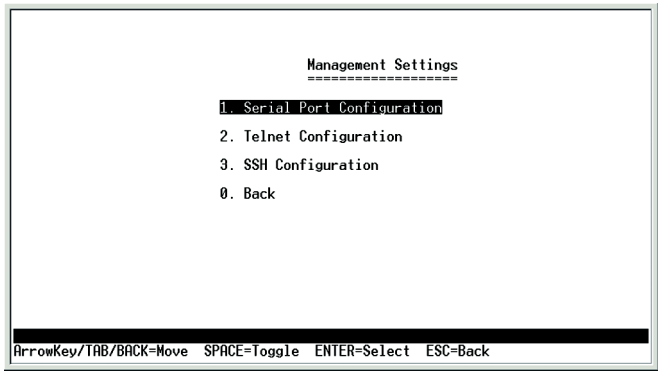


Abbildung 4-11: Menü „Management Settings“

Serial Port Configuration

Die Baudrate des Switches wird auf dem Bildschirm *Serial Port Configuration* angezeigt.

Wählen Sie **Edit** aus, und drücken Sie die **EINGABETASTE**, um Änderungen vorzunehmen. Legen Sie die gewünschte Geschwindigkeit fest, und drücken Sie nach Vornehmen der Änderungen **ESC**, um zum Menü *Action* zurückzukehren. Wählen Sie **Save** aus, und drücken Sie zum Speichern der Änderungen auf die **EINGABETASTE**. Wählen Sie zum Schließen des Bildschirms **Quit** aus, und drücken Sie die **EINGABETASTE**.

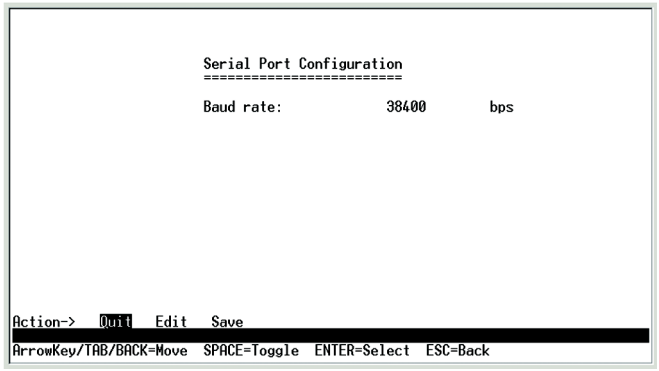


Abbildung 4-12: Serial Port Configuration

Telnet Configuration (Telnet-Konfiguration)

Auf dem Bildschirm *Telnet Configuration* wird das Zeitlimit angezeigt. Der Wert wird in Sekunden angegeben. Möchten Sie für die Telnet-Sitzung kein Zeitlimit festlegen, geben Sie 0 Sekunden ein.

Wählen Sie **Edit** aus, und drücken Sie die **EINGABETASTE**, um Änderungen vorzunehmen. Drücken Sie anschließend **ESC**, um zum Menü *Action* zurückzukehren. Wählen Sie **Save** aus, und drücken Sie zum Speichern der Änderungen auf die **EINGABETASTE**. Wählen Sie zum Schließen des Bildschirms **Quit** aus, und drücken Sie die **EINGABETASTE**.

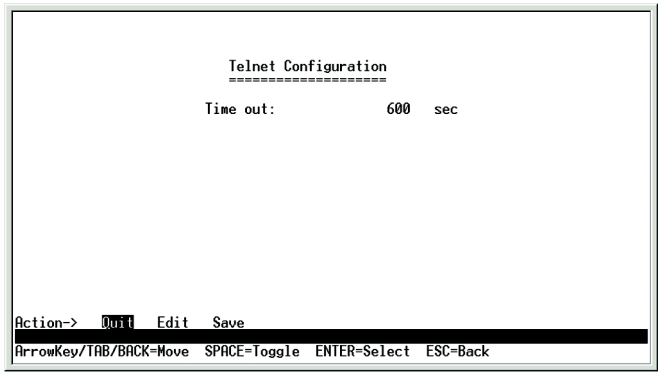


Abbildung 4-13: Telnet Configuration (Telnet-Konfiguration)

SSH Configuration (SSH-Konfiguration)

Auf dem Bildschirm werden Optionen für SSH-Serverkonfiguration, SSH-Serverstatus, SSH-Kryptographieschlüsselerzeugung und SSH-Schlüssel-Fingerprint angezeigt.

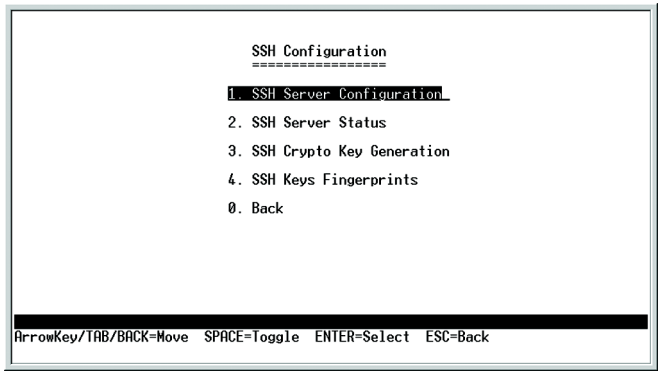


Abbildung 4-14: SSH Configuration (SSH-Konfiguration)

SSH Server Configuration (SSH-Serverkonfiguration)

Der SSH-Server kann auf dem Bildschirm *SSH Server Configuration* aktiviert oder deaktiviert werden. Navigieren Sie dazu zur Option für SSH-Server, und aktivieren bzw. deaktivieren Sie die Option durch Drücken der **LEERTASTE**. Der SSH-Serveranschluss kann durch Eingeben des Werts geändert werden.

Wählen Sie **Edit** aus, und drücken Sie die **EINGABETASTE**, um Änderungen vorzunehmen. Drücken Sie anschließend **ESC**, um zum Menü *Action* zurückzukehren. Wählen Sie **Save** aus, und drücken Sie zum Speichern der Änderungen auf die **EINGABETASTE**. Wählen Sie zum Schließen des Bildschirms **Quit** aus, und drücken Sie die **EINGABETASTE**.

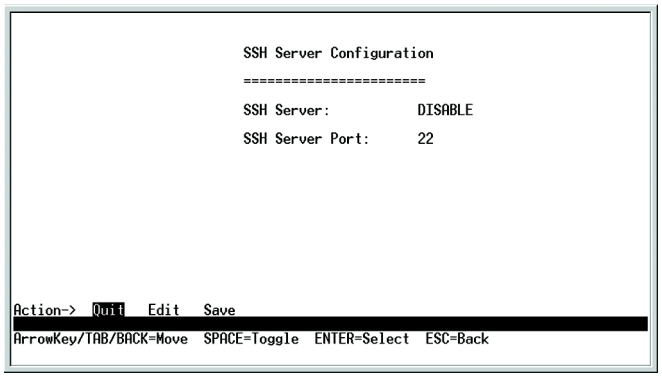


Abbildung 4-15: SSH Server Configuration (SSH-Serverkonfiguration)

SSH Status (SSH-Status)

Auf dem Bildschirm *SSH Status* werden der Status des SSH-Servers (aktiviert bzw. deaktiviert), der RSA- und DSA-Schlüsselstatus sowie alle geöffneten SSH-Sitzungen angezeigt.

Wählen Sie zum Aktualisieren des Bildschirms ggf. **Refresh** aus. Wählen Sie zum Schließen des Bildschirms **Quit** aus, und drücken Sie die **EINGABETASTE**.

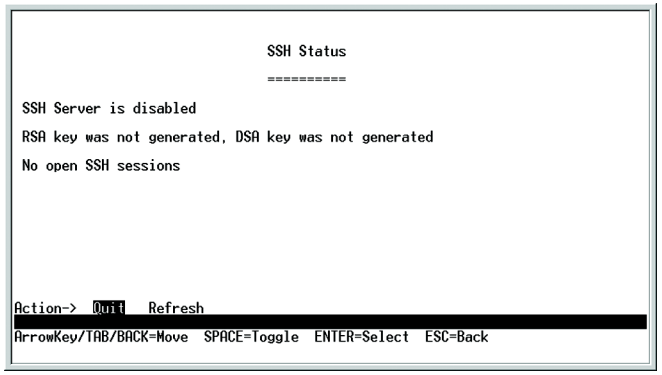


Abbildung 4-16: SSH Status (SSH-Status)

SSH Crypto Key Generation (SSH-Kryptographieschlüsselerzeugung)

Auf dem Bildschirm *SSH Crypto Key Generation* kann für den Algorithmus des öffentlichen SSH-Schlüssels zwischen RSA und DSA gewechselt werden. Verwenden Sie dazu die **LEERTASTE**. Die Länge des öffentlichen SSH-Schlüssels kann nicht geändert werden.

Wählen Sie **Edit** aus, und drücken Sie die **EINGABETASTE**, um Änderungen vorzunehmen. Drücken Sie anschließend **ESC**, um zum Menü *Action* zurückzukehren. Wählen Sie **Save** aus, und drücken Sie zum Speichern der Änderungen auf die **EINGABETASTE**. Wählen Sie zum Schließen des Bildschirms **Quit** aus, und drücken Sie die **EINGABETASTE**.

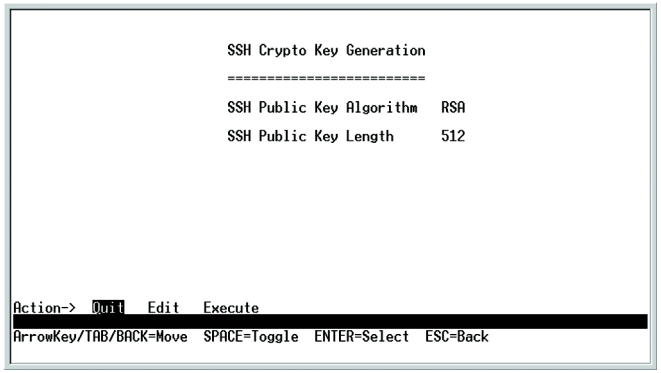


Abbildung 4-17: SSH Crypto Key Generation (SSH-Kryptographieschlüsselerzeugung)

SSH Keys Fingerprints (SSH-Schlüssel-Fingerprints)

Auf dem Bildschirm *SSH Keys Fingerprints* werden die RSA- und DSA-Schlüssel nach eventueller Erzeugung angezeigt.

Wählen Sie zum Aktualisieren des Bildschirms ggf. **Refresh** aus. Wählen Sie zum Schließen des Bildschirms **Quit** aus, und drücken Sie die **EINGABETASTE**.

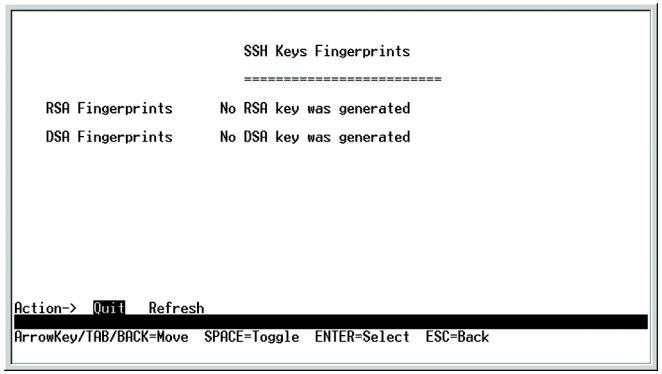


Abbildung 4-18: SSH Keys Fingerprints (SSH-Schlüssel-Fingerprints)

Username & Password Settings (Benutzernamen- und Kennworteinstellungen)

Auf diesem Bildschirm können die Benutzernamen und Kennwörter der Benutzer, die auf den Switch zugreifen, verwaltet werden.

Wählen Sie **Edit** aus, und drücken Sie die **EINGABETASTE**, um Änderungen vorzunehmen. Drücken Sie anschließend **ESC**, um zum Menü *Action* zurückzukehren. Wählen Sie **Save** aus, und drücken Sie zum Speichern der Änderungen auf die **EINGABETASTE**. Wählen Sie zum Schließen des Bildschirms **Quit** aus, und drücken Sie die **EINGABETASTE**.

HINWEIS: Auf dem Bildschirm für Benutzernamen- und Kennworteinstellungen können auch Kennwörter für andere Benutzer festgelegt werden.

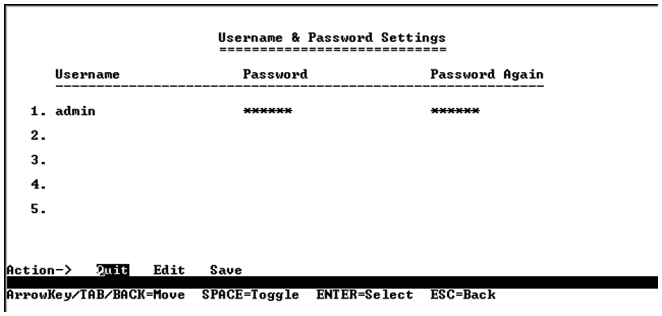


Abbildung 4-19: Username & Password Settings (Benutzernamen- und Kennworteinstellungen)

Security Settings (Sicherheitseinstellungen)

Auf dem Bildschirm für die Sicherheitseinstellungen können die Sicherheitseinstellungen des Switches konfiguriert sowie erzeugt und angezeigt werden.

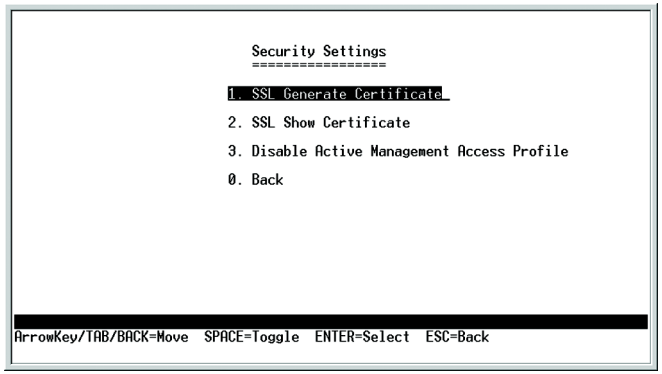


Abbildung 4-20: Security Settings (Sicherheitseinstellungen)

SSL Certificate Generation (SSL-Zertifikaterzeugung)

Geben Sie auf dem Bildschirm für die Zertifikaterzeugung ein mit dem Gerät erzeugtes Zertifikat an.

Folgende Felder sind verfügbar:

Public Key Length – Angabe der SSL-RSA-Schlüssellänge. (Bereich: 512-2048)

Organization Name – Angabe des Namens der Organisation. (Bereich: 1-64)

Locality or City Name – Angabe des Standorts oder der Stadt. (Bereich: 1-64)

State or Province Name – Angabe des Staats oder der Region. (Bereich: 1-64)

Country Name – Angabe des Ländernamens. (Bereich: 2-2)

Validity Term – Angabe des Zeitraums (in Tagen), in dem die Zertifizierung gültig ist. (Bereich: 30-3650)

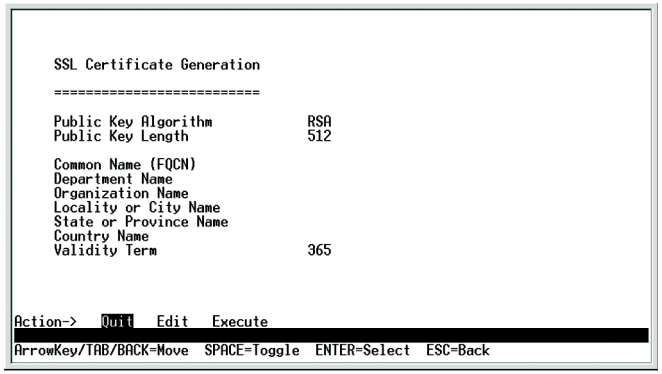


Abbildung 4-21: SSL Certificate Generation (SSL-Zertifikaterzeugung)

Show Certificate

Zeigen Sie auf dem Bildschirm für das Anzeigen von Zertifikaten das interne Zertifikat an.

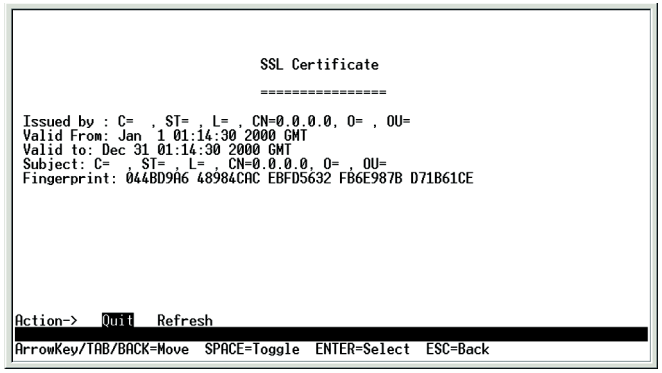


Abbildung 4-22: SSL Certificate (SSL-Zertifikat)

Disable Active Management Profile

Bei Auswählen dieser Option werden Sie dazu aufgefordert, das Deaktivieren des Active Management-Profils zu bestätigen.

IP Configuration

Auf dem Bildschirm *IP Configuration* sind folgende Optionen verfügbar: **IP Address Settings**, **HTTP Configuration**, **HTTPS Configuration** und **Network Configuration**.

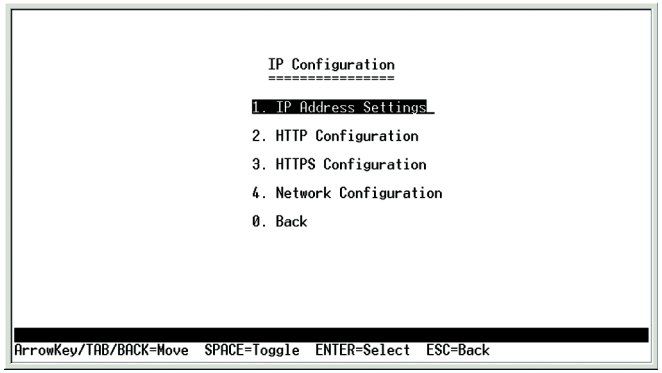


Abbildung 4-23: IP Configuration

IP Address Configuration (IP-Adresskonfiguration)

Hier werden die IP-Daten für den Switch angezeigt.

IP Address. Die IP-Adresse des angezeigten Switches. (Die Standard-IP-Adresse lautet **192.168.1.254**.) Stellen Sie sicher, dass die eingegebene Adresse korrekt ist und nicht in Konflikt mit einem anderen Gerät im Netzwerk steht.

Subnet Mask. Die Subnetzmaske des Switches wird angezeigt.

Default Gateway. Die IP-Adresse des Netzwerk-Standardgateways wird angezeigt.

Management VLAN. Die VLAN-ID-Nummer wird angezeigt.

DHCP client. Der Status des DHCP-Client wird angezeigt. Soll der Switch als DHCP-Client fungieren, wählen Sie **ENABLE** aus. Möchten Sie dem Switch eine statische IP-Adresse zuweisen, geben Sie die IP-Einstellungen ein, und wählen Sie **DISABLE** aus.

Wählen Sie **Edit** aus, um Änderungen vorzunehmen. Drücken Sie anschließend **ESC**, um zum Menü *Action* zurückzukehren, und wählen Sie zum Speichern der Änderungen **Save** aus.

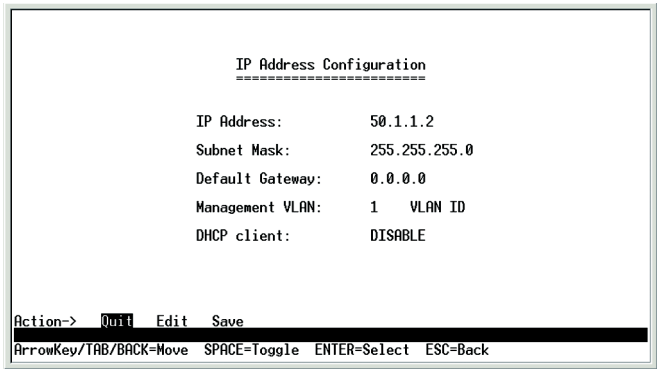


Abbildung 4-24: IP Address Configuration (IP-Adresskonfiguration)

HTTP

Auf dem Bildschirm *HTTP* werden Status und Anschlussnummer des HTTP-Servers angezeigt.

Wählen Sie **Edit** aus, und drücken Sie die **EINGABETASTE**, um Änderungen vorzunehmen. Drücken Sie anschließend **ESC**, um zum Menü *Action* zurückzukehren. Wählen Sie **Save** aus, und drücken Sie zum Speichern der Änderungen auf die **EINGABETASTE**. Wählen Sie zum Schließen des Bildschirms **Quit** aus, und drücken Sie die **EINGABETASTE**.

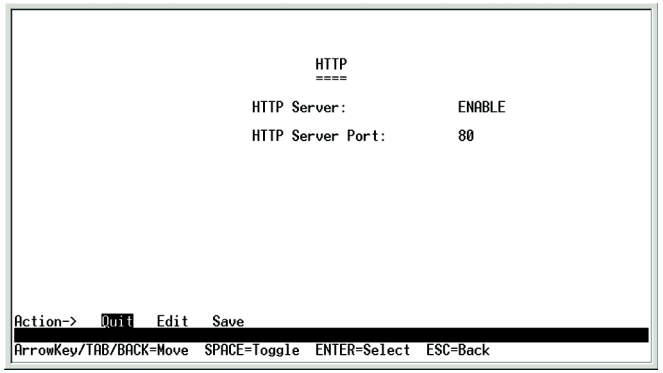


Abbildung 4-25: HTTP

HTTPS Configuration (HTTPS-Konfiguration)

Konfigurieren Sie auf dem Bildschirm *HTTPS Configuration* HTTPS-Einstellungen. Sie können den HTTPS-Server aktivieren oder deaktivieren und den Anschluss, an dem eine Sitzung aktiviert ist, konfigurieren.

Wählen Sie **Edit** aus, und drücken Sie die **EINGABETASTE**, um Änderungen vorzunehmen. Drücken Sie anschließend **ESC**, um zum Menü *Action* zurückzukehren. Wählen Sie **Save** aus, und drücken Sie zum Speichern der Änderungen auf die **EINGABETASTE**. Wählen Sie zum Schließen des Bildschirms **Quit** aus, und drücken Sie die **EINGABETASTE**.

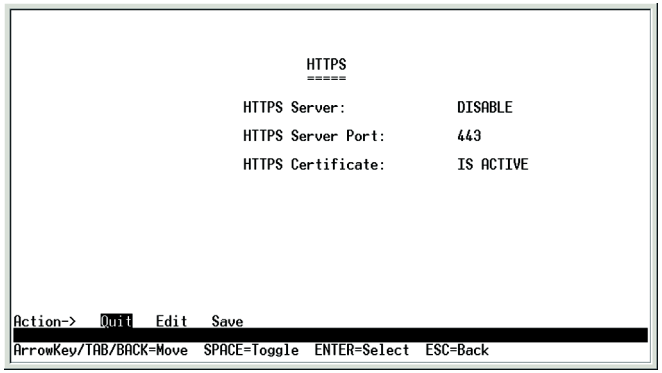


Abbildung 4-26: HTTPS Configuration (HTTPS-Konfiguration)

Network Configuration (Netzwerkkonfiguration)

Auf dem Bildschirm *Network Configuration* kann zwischen zwei Tests gewählt werden: Ping und TraceRoute.

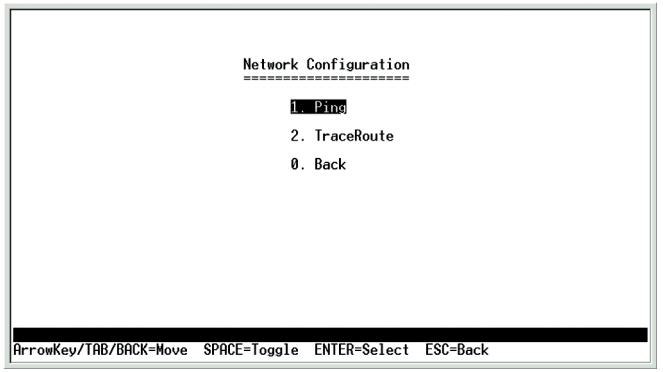


Abbildung 4-27: Network Configuration (Netzwerkkonfiguration)

Ping

Auf dem Bildschirm *Ping* wird die IP-Adresse des Standorts, zu dem Sie Kontakt aufnehmen möchten, angezeigt.

Wählen Sie zum Ändern der IP-Adresse **Edit** und anschließend zum Starten des Ping-Tests **Execute** aus.

Nach dem Ping-Test werden auf dem Bildschirm *Ping* IP-Adresse und Status sowie die Statistik des Ping-Tests angezeigt.

Wählen Sie **Edit** aus, und drücken Sie die **EINGABETASTE**, um Änderungen vorzunehmen. Drücken Sie anschließend **ESC**, um zum Menü *Action* zurückzukehren. Wählen Sie **Save** aus, und drücken Sie zum Speichern der Änderungen auf die **EINGABETASTE**. Wählen Sie zum Schließen des Bildschirms **Quit** aus, und drücken Sie die **EINGABETASTE**.

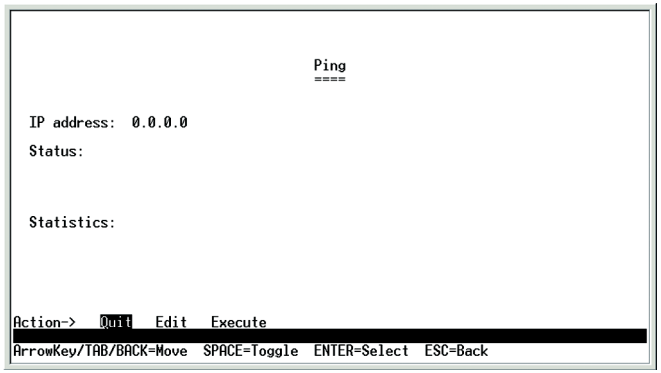


Abbildung 4-28: Ping-Test

TraceRoute

Auf dem Bildschirm *TraceRoute* wird die IP-Adresse der Adresse, deren Route verfolgt werden soll, angezeigt.

Wählen Sie zum Ändern der IP-Adresse **Edit** und anschließend zum Starten des Traceroute-Tests **Execute** aus.

Nach dem Traceroute-Test werden auf dem Bildschirm *TraceRoute* IP-Adresse und Status sowie die Statistik des Traceroute-Tests angezeigt.

Wählen Sie **Edit** aus, und drücken Sie die **EINGABETASTE**, um Änderungen vorzunehmen. Drücken Sie anschließend **ESC**, um zum Menü *Action* zurückzukehren. Wählen Sie **Save** aus, und drücken Sie zum Speichern der Änderungen auf die **EINGABETASTE**. Wählen Sie zum Schließen des Bildschirms **Quit** aus, und drücken Sie die **EINGABETASTE**.

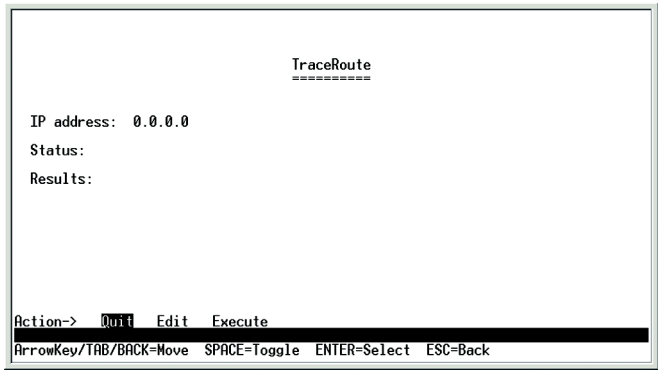


Abbildung 4-29: TraceRoute-Test

File Management (Dateiverwaltung)

Über den Bildschirm *File Management* können mithilfe eines TFTP-Servers Dateien herauf- oder heruntergeladen werden (z. B. Startkonfigurations-, Start- oder Bilddateien).

Wählen Sie zum Ändern der Einstellungen **Edit** aus. Drücken Sie anschließend **ESC**, um zum Menü *Action* zurückzukehren, und wählen Sie zum Hoch- bzw. Herunterladen der gewünschten Datei **Execute** aus.

Führen Sie beim Herunterladen eines neuen Startbilds folgende Schritte aus:

1. Laden Sie den neuen Startcode herunter. SETZEN SIE NICHT DAS GERÄT ZURÜCK!

2. Laden Sie das neue Softwarebild herunter.

3. Setzen Sie nun das Gerät zurück.

HINWEIS: Stellen Sie beim Herunterladen einer Konfigurationsdatei sicher, dass diese gültig ist. Stellen Sie nach Bearbeitung der Datei sicher, dass nur gültige Einträge konfiguriert wurden.

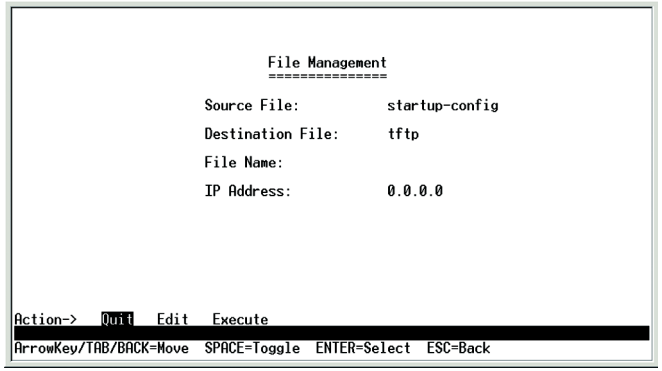


Abbildung 4-30: File Management (Dateiverwaltung)

Restore System Default Settings (Systemstandardeinstellungen wiederherstellen)

Wählen Sie zum Zurücksetzen des Switches auf die Herstellerstandards **Restore System Default Settings** aus, und drücken Sie die **EINGABETASTE**. Sie werden gefragt, ob Sie den Vorgang fortsetzen möchten. Drücken Sie zum Zurücksetzen der Standardeinstellungen des Switches die **Y**-Taste bzw. zum Abbrechen des Vorgangs die **N**-Taste.

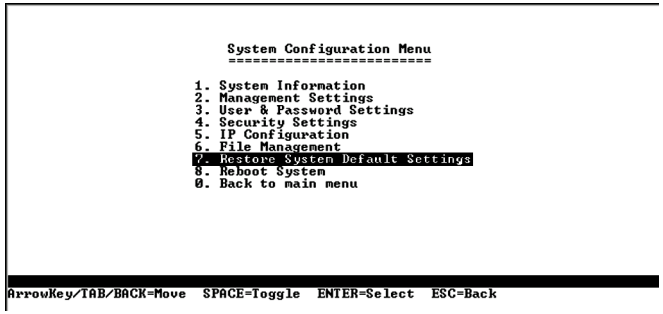


Abbildung 4-31: Restore System Default Settings (Systemstandardeinstellungen wiederherstellen)

Reboot System (System neu starten)

Wählen Sie **Reboot System** aus, und drücken Sie die **EINGABETASTE**, um den Switch ggf. neu zu starten. Sie werden gefragt, ob Sie den Vorgang fortsetzen möchten. Drücken Sie zum Neustarten des Switches die **Y**-Taste bzw. zum Abbrechen des Vorgangs die **N**-Taste. Nach dem Neustart des Switches wird der Bildschirm *Switch Main Menu* angezeigt.

Back to main menu

Wählen Sie **Back to main menu** aus, und drücken Sie die **EINGABETASTE**, um zum Bildschirm *Switch Main Menu* zurückzukehren.

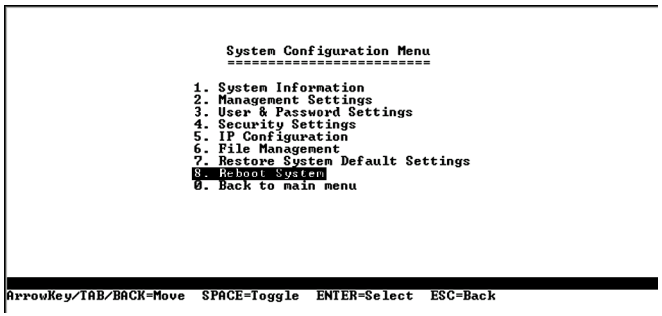


Abbildung 4-32: Reboot System (System neu starten)

Port Status (Anschlussstatus)

Wählen Sie auf dem Bildschirm *Switch Main Menu* die Option **Port Status** aus, und drücken Sie die **EINGABETASTE**, wenn Sie die Statusinformationen für die Switchanschlüsse anzeigen möchten.

Auf dem Bildschirm *Port Status* werden die Anschlussnummern, deren Status, der Verbindungsstatus, die Geschwindigkeit und der Duplexmodus sowie der Status der Datenflusssteuerung (dies ist der Datenfluss der Paketübertragungen) angezeigt.

Anschlusseinstellungen müssen ggf. auf dem Bildschirm *Port Configuration* vorgenommen werden.

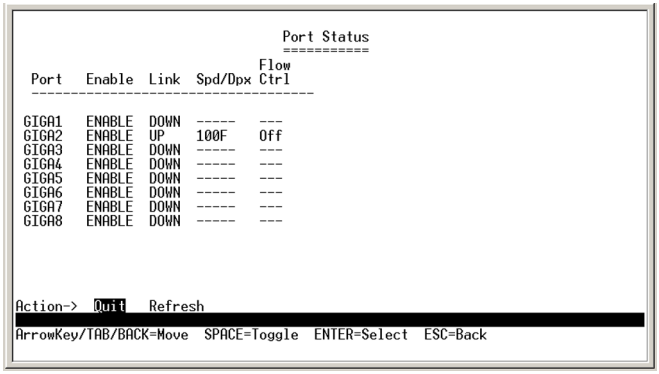


Abbildung 4-33: Port Status (Anschlussstatus)

Port Configuration (Anschlusskonfiguration)

Wählen Sie auf dem Bildschirm *Switch Main Menu* die Option **Port Configuration** aus, und drücken Sie die **EINGABETASTE**, um die Switchanschlüsse zu konfigurieren.

Auf dem Bildschirm *Port Configuration* werden die Anschlussnummern, deren Status, der Status der automatischen Aushandlung, die Geschwindigkeit und der Duplexmodus sowie der Status der Datenflusssteuerung (dies ist der Datenfluss der Paketübertragungen) angezeigt.

Wählen Sie **Edit** aus, und drücken Sie die **EINGABETASTE**, um Änderungen vorzunehmen. Drücken Sie anschließend **ESC**, um zum Menü *Action* zurückzukehren. Wählen Sie **Save** aus, und drücken Sie zum Speichern der Änderungen auf die **EINGABETASTE**. Wählen Sie zum Schließen des Bildschirms **Quit** aus, und drücken Sie die **EINGABETASTE**.

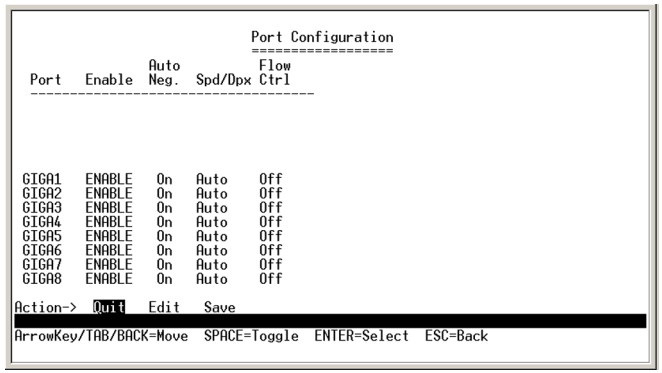


Abbildung 4-34: Port Configuration (Anschlusskonfiguration)

Help

Wählen Sie **Help** aus, und drücken Sie zum Anzeigen der Hilfeinformationen die **EINGABETASTE**. Auf diesem Bildschirm wird das Navigieren durch die verschiedenen Bildschirme der Konsolenschnittstelle erläutert.

Kapitel 5: Verwenden des webbasierten Dienstprogramms für die Konfiguration

Übersicht

In diesem Kapitel werden die Funktionen des webbasierten Dienstprogramms beschrieben. Alle in diesem Kapitel gezeigten Funktionen sind, falls nicht anders angegeben, in allen Fast Ethernet-Switches enthalten. Zusätzliche Funktionen für bestimmte Switches sind entsprechend gekennzeichnet.

Zugreifen auf das webbasierte Dienstprogramm

HINWEIS: Das webbasierte Dienstprogramm ist für die Anzeige mit einer Bildschirmauflösung von 1024 x 768 optimiert. Es wird ferner die Verwendung von Internet Explorer Version 5.5 oder höher empfohlen.

Öffnen Sie den Webbrowser, und geben Sie im Feld *Address* die IP-Adresse **192.168.1.254** ein. Drücken Sie anschließend die **EINGABETASTE**. Der Anmeldebildschirm wird angezeigt.

HINWEIS: Die Standard-IP-Adresse des Geräts lautet 192.168.1.254. Geben Sie die richtige Adresse ein, falls Sie diese Adresse geändert haben. Das Gerät muss sich in demselben Subnetz wie die Verwaltungsstation befinden, die zum Konfigurieren des Geräts verwendet wird.

Wenn Sie das webbasierte Dienstprogramm zum ersten Mal öffnen, geben Sie in das Feld *User Name* den Namen **admin** ein und lassen das Feld *Password* leer. Klicken Sie auf die Schaltfläche **OK**. Das Kennwort können Sie später im Bildschirm *System Password* angeben.

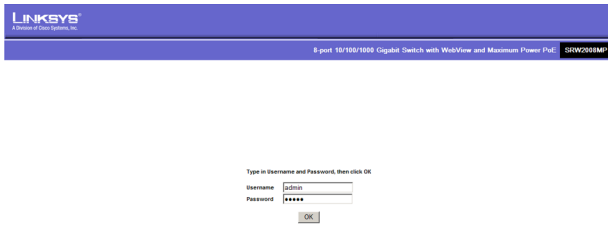


Abbildung 5-1: Anmeldebildschirm

Zuerst wird der Bildschirm *Setup Summary* angezeigt. Das webbasierte Dienstprogramm verfügt über zwölf Hauptregisterkarten: **Setup**, **Port Management**, **VLAN Management**, **Statistics**, **ACL**, **Security**, **QoS** (Quality of Service), **Spanning Tree**, **Multicast**, **SNMP**, **Admin** und **Logout**. Klicken Sie auf eine der Hauptregisterkarten, um weitere Registerkarten anzuzeigen.

HINWEIS: Die LEDs, die im webbasierten Dienstprogramm angezeigt werden, sind nicht mit den LEDs sind nicht mit den LEDs an der Vorderseite des Switch identisch. Die LEDs an der Vorderseite des Gehäuses zeigen andere Statusinformationen an, die in *Kapitel 2: Aufbau des Switch*.

Die LEDs im Bildschirm **Setup Summary** zeigen Statusinformationen zu den entsprechenden Anschlüssen an. Eine grüne LED zeigt eine Verbindung an, und eine graue LED steht für keine Verbindung. Eine orangefarbene LED zeigt an, dass der Anschluss vom Administrator geschlossen wurde. Wenn Sie auf die LED eines Anschlusses klicken, wird die Statistik für den jeweiligen Anschluss angezeigt.

HINWEIS: Nachdem Sie mithilfe des webbasierten Dienstprogramms Werte konfiguriert haben, müssen Sie ggf. die Seite aktualisieren, um die aktualisierte Konfiguration sehen zu können.

Registerkarte „Setup“ – Summary

Der Bildschirm *Summary* enthält Geräte- und Systeminformationen zum Switch.

Abbildung 5-2: Setup – Summary (Zusammenfassung)

Device Information

Host Name: Zeigt den Namen des Switch an, falls auf der Registerkarte **Setup - Network Settings ein Name eingegeben wurde.**

IP Address. Zeigt die IP-Adresse des Switch an (Konfiguration über die Registerkarte **Setup - Network Settings**).

Subnet Mask. Zeigt die Subnetzmaske des Switch an (Konfiguration über die Registerkarte **Setup - Network Settings**).

DNS Servers. Zeigt die DNS-Server an (Konfiguration über die Registerkarte **Setup - Network Settings**).

Default Gateway. Zeigt den Standard-Gateway an (Konfiguration über die Registerkarte **Setup - Network Settings**).

Address Mode. Zeigt an, ob der Switch mit einer statischen oder dynamischen IP-Adresse konfiguriert wurde (Konfiguration über die Registerkarte **Setup - Network Settings**).

Base MAC Address. Dies ist die MAC-Adresse des Switch.

System Information

Serial Number. Zeigt die Seriennummer des Produkts an.

Model Name. Zeigt die Modellnummer und den Namen des Switch an.

Hardware Version. Zeigt die Versionsnummer der Hardware des Switch an.

Boot Version. Zeigt die Systemstartversion an, die auf dem Gerät momentan ausgeführt wird.

Firmware Version. Zeigt die Firmwareversionsnummer (Software) an.

System Name. Zeigt den Systemnamen an (Konfiguration über die Registerkarte Setup – Network Settings).

System Contact. Zeigt die Kontaktperson für den Switch an (Konfiguration über die Registerkarte **Setup - Network Settings**).

System Up Time. Zeigt die Zeit an, die seit dem letzten Zurücksetzen des Switch verstrichen ist.

Current Time. Zeigt die Systemzeit an (Konfiguration über die Registerkarte **Setup - Time**).

PoE Information

HINWEIS: *PoE Information* wird nur auf dem Bildschirm **Summary** des SRW2008P und SRW2008MP angezeigt.

Maximum Available Power. Zeigt die maximale Stromleistung an, die das Gerät liefern kann.

System Operation Status. Zeigt an, ob die PoE-Funktion aktiviert oder deaktiviert ist.

Main Power Consumption. Zeigt den aktuellen Stromverbrauch an.

Registerkarte „Setup“ - Network Settings

Im Bildschirm *Network Settings* können Sie Schnittstellen DHCP- oder statische IP-Einstellungen zuweisen und außerdem Standard-Gateways zuweisen.

Identification

System Name. In diesem Feld können Sie einen Systemnamen zuweisen.

System Location. In diesem Feld geben Sie eine Beschreibung ein, wo sich der Switch befindet, z. B. Dritter Stock.

System Contact. Geben Sie in dieses Feld die für die Administration zuständige Kontaktperson ein.

System Object ID. Zeigt die Systemobjekt-ID an.

Base MAC Address. Dies ist die MAC-Adresse des Switch.

IP Configuration

Management VLAN. In diesem Dropdownmenü können Sie das VLAN für die Verwaltung auswählen.

IP Address Mode. In diesem Dropdownmenü können Sie die Konfiguration einer statischen oder dynamischen IP-Adresse auswählen.

Host Name: Geben Sie hier den DHCP-Hostnamen ein.

IP Address. Wenn Sie eine statische IP-Adresse verwenden, geben Sie die IP-Adresse hier ein.

Subnet Mask. Geben Sie die Subnetzmaske der momentan konfigurierten IP-Adresse ein.

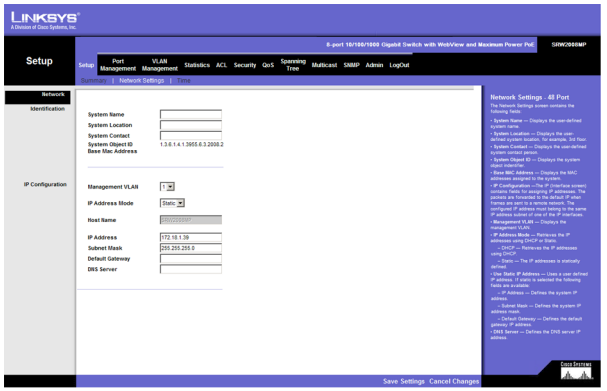


Abbildung 5-3: Setup – Network Settings (Netzwerkeinstellungen)

Default Gateway. Geben Sie die IP-Adresse für den Standard-Gateway ein.

DNS Server. Geben Sie die Informationen zum primären DNS-Server ein.

Klicken Sie zum Speichern der Änderungen auf **Save Settings** oder auf **Cancel Changes**, um die Informationen zu verwerfen.

Registerkarte „Setup“ – Time

Im Bildschirm *Time* können Sie die Zeiteinstellungen für den Switch konfigurieren.

Set Time

Use System Time. Wenn Sie diese Option aktivieren, wird die lokale Hardwareuhr verwendet.

Use SNTP Time. Wenn Sie diese Option aktivieren, wird die Uhrzeit über einen SNTP-Server (Simple Network Time Protocol) synchronisiert.

Local Time

Hours. Hier geben Sie die Stunde an.

Minutes. Hier geben Sie die Minuten an.

Seconds. Hier geben Sie die Sekunden an.

Month. Hier geben Sie den Monat an.

Day. Hier geben Sie den Tag an.

Year. Hier geben Sie das Jahr an.

Time Zone. Hier geben Sie die Abweichung zwischen Greenwich Mean Time (GMT) und Ortszeit an.

Daylight Saving

Daylight Saving. Wählen Sie **Daylight Saving**, um diese Funktion für den Switch zu aktivieren. Wenn für den Switch die Sommerzeit der USA verwendet werden soll, wählen Sie **USA**. Wenn für den Switch die Sommerzeit der EU verwendet werden soll, wählen Sie **European**. Wenn Sie für die Sommerzeit andere Einstellungen verwenden möchten, wählen Sie **Custom** und füllen die Felder *From* und *To* aus.

Time Set Offset (1-1440). Geben Sie für andere Länder als die USA und der EU die Stunden an, die für die Sommerzeit verwendet werden. Die Standardeinstellung beträgt **60** Minuten.

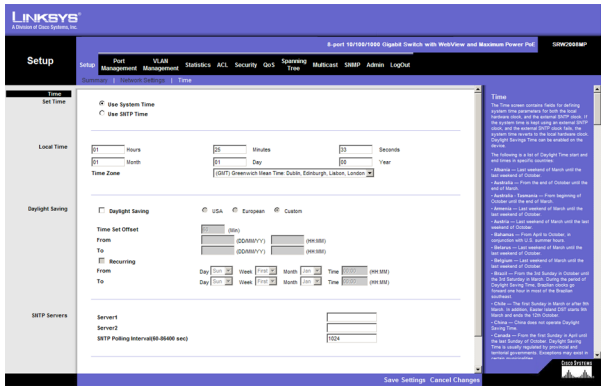


Abbildung 5-4: Setup – Time (Zeit)

From. Wenn Sie für die Einstellung *Daylight Saving* die Option **Other** gewählt haben, geben Sie das Datum und die Uhrzeit ein, an dem bzw. zu der die Sommerzeit beginnt.

To. Wenn Sie für die Einstellung *Daylight Saving* die Option **Other** gewählt haben, geben Sie das Datum und die Uhrzeit ein, an dem bzw. zu der die Sommerzeit endet.

Recurring. Wenn Sie für die Einstellung *Daylight Saving* die Option **Other** gewählt haben und die Sommerzeit jedes Jahr über dieselben Start- und Enddaten verfügt, können Sie **Recurring** wählen.

From. Wenn Sie **Recurring** gewählt haben, geben Sie das Datum und die Uhrzeit ein, an dem bzw. zu der die Sommerzeit beginnt.

To. Wenn Sie **Recurring** gewählt haben, geben Sie das Datum und die Uhrzeit ein, an dem bzw. zu der die Sommerzeit endet.

SNTP Servers

Server1. Geben Sie hier den primären SNTP-Server ein.

Server2. Geben Sie hier einen sekundären SNTP-Server ein.

SNTP Polling Interval (60-86400). Der hier definierte Wert bestimmt den Zeitraum (in Sekunden), bevor der Switch den SNTP-Server abfragt. Der Standardwert lautet 1024 Sekunden (ca. alle 17 Minuten).

Klicken Sie zum Speichern der Änderungen auf **Save Settings** oder auf **Cancel Changes**, um die Informationen zu verwerfen.

Registerkarte „Port Management“ – Port Settings

Im Bildschirm *Port Management - Port Settings* werden die Einstellungen der einzelnen Anschlüsse des Switch angezeigt.

Port. Die Nummer des Anschlusses. Um ein SFP-Modul zu verwenden, klicken Sie für den entsprechenden Anschluss (G1, G2) auf die Schaltfläche **Detail**.

Description. Zeigt eine kurze Beschreibung des Anschlusses an (Zugriff durch Klicken auf die Schaltfläche **Detail**).

Administrative Status. Sie können den Anschluss offline schalten, indem Sie die Option **Down** wählen. Wenn **Up** ausgewählt ist, ist der normale Zugriff auf den Anschluss möglich.

Link Status. **Up** zeigt an, dass ein Anschluss über eine aktive Verbindung verfügt. **Down** zeigt an, dass keine aktive Verbindung besteht oder dass der Anschluss von einem Administrator offline geschaltet wurde.

Speed. Zeigt die Verbindungsgeschwindigkeit des Anschlusses an. Sie können die Geschwindigkeit nur konfigurieren, wenn die automatische Aushandlung für den Anschluss deaktiviert ist.

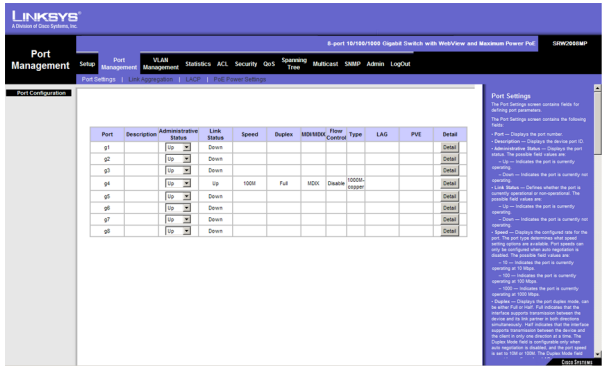


Abbildung 5-5: Port Management (Anschlussverwaltung) – Port Settings (Anschlusseinstellungen)

Duplex. Der Duplexmodus des Anschlusses, also Vollduplex (die Übertragung erfolgt in beide Richtungen gleichzeitig) oder Halbduplex (die Übertragung erfolgt nur jeweils in eine Richtung). Sie können diesen Modus nur konfigurieren, wenn die automatische Aushandlung deaktiviert und die Anschlussgeschwindigkeit auf 10 Mbit/s oder 100 Mbit/s gesetzt ist. Die Konfiguration über Link Aggregation Groups (LAGs) ist nicht möglich.

MDI/MIDX. Der MDI/MDIX-Status des Anschlusses. Die Einstellung **MDI** wird verwendet, wenn der Anschluss über eine Verbindung zu einer Endstation verfügt. Die Einstellung **MDIX** wird verwendet, wenn der Anschluss über eine Verbindung zu einem Hub oder einem anderen Switch verfügt.

Flow Control. Dies ist der Datenflusssteuerungsstatus des Anschlusses. Er ist aktiv, wenn der Anschluss den Vollduplexmodus verwendet.

Type. Zeigt den Anschlusstyp an.

LAG. Zeigt an, ob der Anschluss einer LAG angehört.

PVE. Wenn es sich bei einem Anschluss um einen PVE-Anschluss (Private VLAN Edge) handelt, umgeht dieser die Weiterleitungsdatenbank und leitet den gesamten Unicast-, Multicast- und Broadcastdatenverkehr an einen Uplink weiter. Bei Uplinks kann es sich um Anschlüsse oder LAGs handeln.

Detail. Verwenden Sie die Schaltfläche **Detail**, um den Bildschirm **Port Configuration Detail** zu öffnen.

Bildschirm **Port Configuration Detail**

Port. Die Nummer des Anschlusses.

Description. Zeigt eine kurze Beschreibung des Anschlusses an (Zugriff durch Klicken auf die Schaltfläche **Detail**).

Port Type. Dies ist der Anschlusstyp.

Admin Status. Sie können den Anschluss offline schalten, indem Sie die Option **Down** wählen. Wenn **Up** ausgewählt ist, ist der normale Zugriff auf den Anschluss möglich.

Current Port Status. Zeigt den aktuellen Status des Anschlusses an.

Reactivate Suspended Port. Wenn Sie einen deaktivierten Anschluss wieder aktivieren möchten, aktivieren Sie das Kontrollkästchen.

Operational Status. Zeigt an, ob der Anschluss aktiv ist.

Admin Speed. Hier ändern Sie die Geschwindigkeit des Anschlusses.

Current Port Speed. Zeigt die aktuelle Geschwindigkeit des Anschlusses an.

Admin Duplex. Hier ändern Sie den Duplexmodus.

Current Duplex Mode. Dies ist der Duplexmodus des Anschlusses.

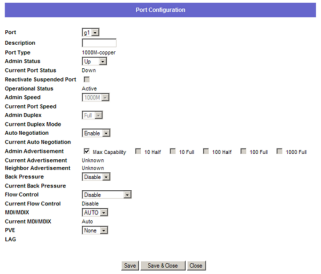


Abbildung 5-6: Port Settings (Anschlusseinstellungen) – Port Configuration Detail (Details der Anschlusskonfiguration)

Auto Negotiation. Hier aktivieren bzw. deaktivieren Sie für den Anschluss die automatische Aushandlung. Wenn Sie ein SFP-Modul verwenden, muss die automatische Aushandlung für den jeweiligen Anschluss auf Disable gesetzt sein.

Current Auto Negotiation. Dies ist die aktuelle Einstellung der automatischen Aushandlung eines Anschlusses.

Admin Advertisement. Gibt die Leistungsdaten des Anschlusses an. Sie können mehrere Optionen auswählen oder Max Capability verwenden, um alle Optionen auszuwählen. Die verfügbaren Optionen lauten:

- **Max Capability**. Zeigt an, dass die Anschlussgeschwindigkeiten und Duplexmoduseinstellungen akzeptiert werden können.
- **10 Half**. Zeigt an, dass der Anschluss 10 Mbit/s und den Halbduplexmodus verwendet.
- **10 Full**. Zeigt an, dass der Anschluss 10 Mbit/s und den Vollduplexmodus verwendet.
- **100 Half**. Zeigt an, dass der Anschluss 100 Mbit/s und den Halbduplexmodus verwendet.
- **100 Full**. Zeigt an, dass der Anschluss 100 Mbit/s und den Vollduplexmodus verwendet.
- **1000**. Zeigt an, dass der Anschluss 1000 Mbit/s und den Vollduplexmodus verwendet.

Current Advertisement. Der Anschluss kündigt seinem Nachbaranschluss seine Funktionen an, um den Aushandlungsprozess zu starten. In diesem Feld werden die aktuellen Ankündigungseinstellungen angezeigt.

Neighbor Advertisement. Der Nachbaranschluss (der Anschluss, an den die ausgewählte Schnittstelle angeschlossen ist) kündigt seine Funktionen dem Anschluss an, um den Aushandlungsprozess zu starten. In diesem Feld werden die aktuellen Einstellungen des Nachbaranschlusses angezeigt.

Back Pressure. Sie können die Funktion Back Pressure des ausgewählten Anschlusses aktivieren oder deaktivieren.

Current Back Pressure. Zeigt an, ob die Funktion Back Pressure für den momentan ausgewählten Anschluss aktiviert oder deaktiviert ist.

Flow Control. Sie können die Funktion Flow Control des ausgewählten Anschlusses aktivieren oder deaktivieren.

Current Flow Control. Zeigt an, ob die Funktion Flow Control für den momentan ausgewählten Anschluss aktiviert oder deaktiviert ist.

MDI/MDIX. Wählen Sie die Einstellung **Auto**, wenn der Anschluss den Kabeltyp automatisch erkennen soll. Wählen Sie **MDI**, wenn der Anschluss über eine Verbindung zu einer Endstation verfügt. Wählen Sie **MDIX**, wenn der Anschluss über eine Verbindung zu einem Hub oder einem anderen Switch verfügt.

Current MDI/MDIX. Der aktuelle MDI/MDIX-Status des Anschlusses.

PVE. Wenn es sich bei einem Anschluss um einen PVE-Anschluss (Private VLAN Edge) handelt, umgeht dieser die Weiterleitungsdatenbank und leitet den gesamten Unicast-, Multicast- und Broadcastdatenverkehr an einen Uplink weiter.

HINWEIS: Alle Anschlüsse einer PVE-Gruppe sollten derselben VLAN-Gruppe angehören.

Klicken Sie zum Speichern der Änderungen auf **Save Settings**.

Registerkarte „Port Management“ – Link Aggregation

LAG. Zeigt an, ob der Anschluss einer LAG angehört.

Description. Beschreibung der jeweiligen LAG.

Admin Status. Der Administrationsstatus der LAG. Up zeigt an, dass die LAG verfügbar ist. **Down** zeigt an, dass der Administrator den Anschluss offline geschaltet hat. Achten Sie beim Ändern der Option darauf, dass Sie auf die Option **Save Settings** klicken.

Type. Zeigt den LAG-Typ an.

Link Status. Zeigt den Linkstatus an.

Speed. Zeigt die Verbindungsgeschwindigkeit an.

Duplex. Zeigt den Duplexmodus der Verbindung an.

Flow Control. Zeigt den Datenflusssteuerungsstatus der LAG an. Er ist aktiv, wenn der Anschluss den Vollduplexmodus verwendet.

LAG Mode. Zeigt den LAG-Status **On**, **Off** oder **Not Present** an.

Detail (Schaltfläche). Verwenden Sie die Schaltfläche **Detail**, um den Bildschirm **Link Aggregation Detail** zu öffnen.

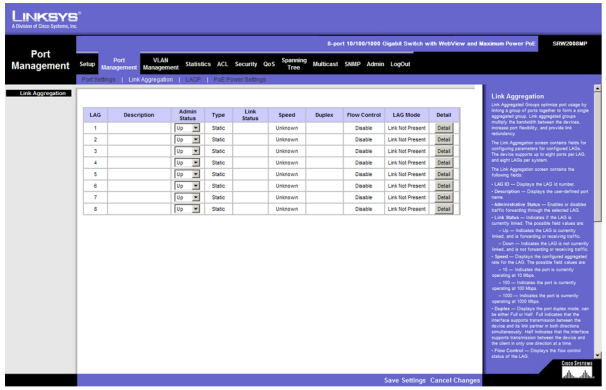


Abbildung 5-7: Port Management (Anschlussverwaltung) – Link Aggregation

Bildschirm Link Aggregation Detail

LAG Configuration

LAG. Die Nummer der ausgewählten LAG.

Description. Hier können Sie zu Referenzzwecken eine allgemeine Beschreibung eingeben.

LACP. Zeigt an, ob sich die LAG im LACP-Modus (Link Aggregation Control Protocol) befindet.

LAG Type. Die Anschlusstypen der LAG.

Administrative Status. Aktiviert bzw. deaktiviert die Datenverkehrweiterleitung über die gewählte LAG.

Current Status. Zeigt an, ob die LAG momentan in Betrieb ist.

Reactivate Suspended LAG. Aktiviert eine LAG wieder, wenn die LAG aufgrund einer Anschlusssperre oder eines Vorgangs der Zugriffssteuerungsliste deaktiviert wurde.

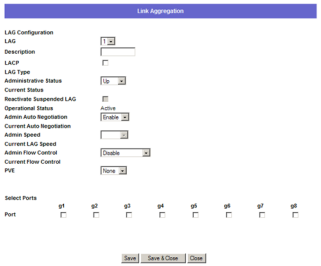


Abbildung 5-8: Link Aggregation – Link Aggregation Detail (Details der Link Aggregation)

Admin Auto Negotiation. Aktiviert bzw. deaktiviert die automatische Aushandlung für die LAG. Die automatische Aushandlung ist ein Protokoll zwischen zwei Linkpartnern, mit dem eine LAG ihrem Partner Übertragungsrate, Duplexmodus und Datenflusssteuerungsfähigkeiten übermittelt (die Standardeinstellung der Datenflusssteuerung ist deaktiviert).

Current Auto Negotiation. Die aktuelle Einstellung für die automatische Aushandlung.

Admin Speed. Die konfigurierte Geschwindigkeit, mit der die LAG betrieben wird.

Current LAG Speed. Die aktuelle Geschwindigkeit, mit der die LAG betrieben wird.

Admin Flow Control. Aktiviert bzw. deaktiviert die Datenflusssteuerung oder aktiviert die automatische Aushandlung der Datenflusssteuerung für die LAG.

Current Flow Control. Die vom Benutzer verwendete Einstellung für die Datenflusssteuerung.

PVE. Zeigt die PVE-Gruppe an, für die die LAG konfiguriert ist.

Select Ports

Ports. Zeigt die Anschlüsse an, die Mitglieder der gewählten LAG sind.

Registerkarte „Port Management“ – LACP

Sie können Aggregatanschlüsse zu Link Aggregation-Anschlussgruppen verknüpfen. Jede Gruppe umfasst Anschlüsse mit identischer Geschwindigkeit, die auf den Vollduplexbetrieb gesetzt sind.

Sie können aggregierte Links manuell einrichten oder automatisch einrichten lassen, indem Sie für die relevanten Links das Link Aggregation Control Protocol (LACP) aktivieren. Sie können Aggregatanschlüsse zu Link Aggregation-Anschlussgruppen verknüpfen. Jede Gruppe umfasst Anschlüsse mit identischer Geschwindigkeit. Der Bildschirm LACP enthält Felder zum Konfigurieren von LACP-LAGs.

LACP System Priority. Zeigt den globalen LACP-Prioritätswert an. Der mögliche Bereich ist 1 bis 65.535. Der Standardwert ist 1.

Port. Definiert die Anschlussnummer, der Werte für Zeitraum und Priorität zugewiesen werden.

LACP Port Priority. Definiert die LACP-Priorität für den Anschluss. Der Feldbereich beträgt 1 bis 65.535.

LACP Timeout. Der administrative LACP-Zeitraum (Timeout). Sie können einen kurzen oder einen langen Wert für den Zeitraum wählen. Die Standardeinstellung ist Long.

Admin Key. Ein Kanal wird nur zwischen Anschlüssen eingerichtet, die über denselben Verwaltungsschlüssel verfügen. Dies gilt nur für Anschlüsse, die in demselben Switch angeordnet sind.

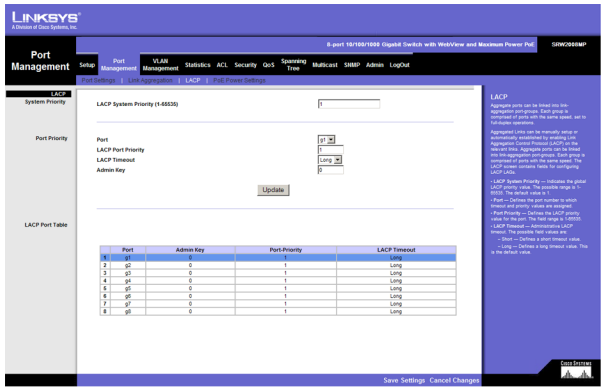


Abbildung 5-9: Port Management (Anschlussverwaltung) – LACP

Registerkarte „Port Management“ – PoE Power Settings

HINWEIS: Auf der Seite Modify PoE werden die momentan konfigurierten PoE-Anschlüsse angezeigt. Diese Option ist nur für die Geräte SRW2008P und SRW2008MP verfügbar.

Port. Zeigt die Nummer des gewählten Anschlusses an.

Admin Status. Zeigt an, ob PoE für den Anschluss aktiviert oder deaktiviert ist.

Priority. Zeigt die PoE-Prioritätseinstellung des Anschlusses an. Folgende Werte sind möglich: Critical, High und Low. Die Standardeinstellung lautet Low.

Power Allocation (milliwatts). Zeigt die Ist-Stromleistung an, die das Gerät liefern kann.

Mode. Zeigt an, ob der Anschluss für die Verwendung von PoE aktiviert ist.

Power Consumption (milliwatts). Zeigt die Strommenge an, die vom Gerät verbraucht wird.

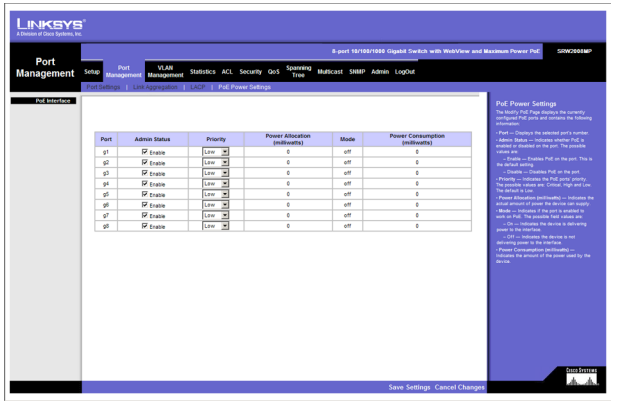


Abbildung 5-10: Port Management (Anschlussverwaltung) – PoE

Registerkarte „VLAN Management“ – Create VLAN

Auf dem Bildschirm Create VLAN werden Informationen und globale Parameter zum Konfigurieren von und Arbeiten mit VLANs angezeigt.

Single VLAN

VLAN ID (2-4094). Zeigt die ID-Nummer des zu konfigurierenden VLAN an. Sie können bis zu 256 VLANs erstellen. Sie verwenden dieses Feld, um VLANs einzeln hinzuzufügen. Um die definierte VLAN-ID-Nummer hinzuzufügen, klicken Sie auf die Schaltfläche **Add**.

VLAN Name. Zeigt den benutzerdefinierten VLAN-Namen an.

VLAN Range

VLAN Range. Zeigt einen Bereich mit VLANs an, die konfiguriert werden. Um den definierten Bereich der VLAN-ID-Nummer hinzuzufügen, klicken Sie auf die Schaltfläche **Add Range**.

VLAN Table

Unter VLAN Table wird eine Liste aller konfigurierten VLANs angezeigt. Hier werden die VLAN-ID, der VLAN-Name und der VLAN-Status angezeigt. Klicken Sie zum Entfernen eines VLAN auf die Schaltfläche **Remove**.

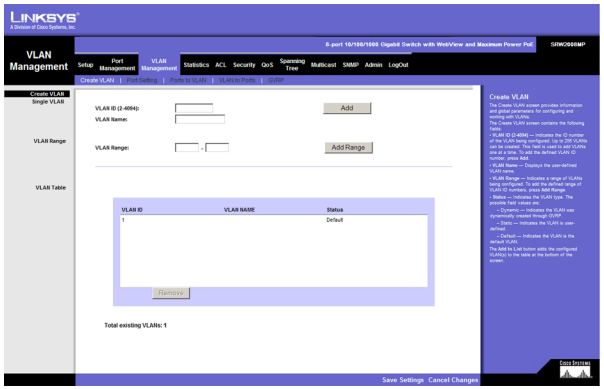


Abbildung 5-11: VLAN Management (VLAN-Verwaltung) – Create VLAN (VLAN erstellen)

HINWEIS: VLANs, die mithilfe von GVRP dynamisch erstellt werden, wird der VLAN-Name Undefined zugewiesen.

Registerkarte „VLAN Management“ – Port Settings

Die VLAN-Anschlusseinstellungen enthalten Parameter zum Verwalten von Anschlüssen, die Teil eines VLAN sind. Die Standard-VLAN-ID (PVID) des Anschlusses wird auf dem Bildschirm Port Settings für das VLAN konfiguriert. Alle nicht getaggten Pakete, die beim Gerät ankommen, werden von der PVID des Anschlusses getaggt.

Port. Die Anschlussnummer, die im VLAN enthalten ist.

Mode. Zeigt den Anschlussmodus an. Folgende Werte sind möglich:

- **General.** Der Anschluss gehört VLANs an, und jedes VLAN ist als „getaggt“ oder „nicht getaggt“ benutzerdefiniert (802.1Q-Vollmodus).
- **Access.** Der Anschluss gehört zu einem einzelnen nicht getaggten VLAN. Wenn sich ein Anschluss im Modus Access befindet, können die für den Anschluss akzeptierten Pakettypen nicht bezeichnet werden. Außerdem ist es nicht möglich, die Eingangsfilterung für einen Zugangsanschluss zu aktivieren oder zu deaktivieren.
- **Trunk.** Der Anschluss gehört VLANs an, bei denen alle Anschlüsse getaggt sind (außer bei einem optionalen systemeigenen Einzel-VLAN).

Acceptable Frame Type. Der am Anschluss akzeptierte Pakettyp. Folgende Werte sind möglich:

- **Admit Tag Only.** Zeigt an, dass am Anschluss nur getaggte Pakete akzeptiert werden.
- **Admit All.** Zeigt an, dass am Anschluss sowohl getaggte als auch nicht getaggte Pakete akzeptiert werden.

PVID. Weist nicht getaggten Paketen eine VLAN-ID zu. Die möglichen Werte sind 2 bis 4.094. VLAN 4095 ist standardmäßig und gemäß der Vorgehensweise in der Branche als VLAN für Ablehnungen definiert. Pakete, die für dieses VLAN klassifiziert sind, werden verworfen.

Ingress Filtering. Aktiviert bzw. deaktiviert die Eingangsfilterung für den Anschluss. Bei der Eingangsfilterung werden Pakete verworfen, die keinen Eingangsanschluss enthalten.

LAG. Zeigt die LAG an, für die das VLAN definiert ist.

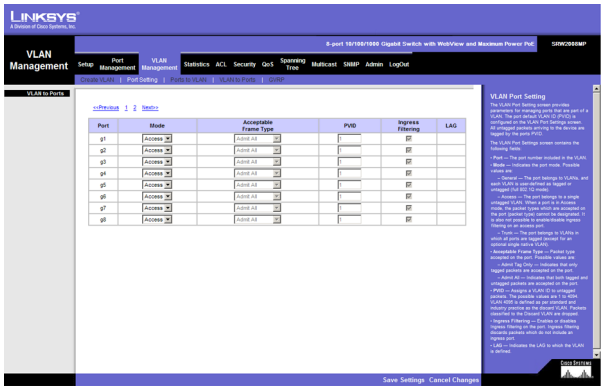


Abbildung 5-12: VLAN Management (VLAN-Verwaltung) – Port Settings (Anschlusseinstellungen)

Registerkarte „VLAN Management“ – Ports to VLAN

Der Bildschirm Ports to VLAN enthält Felder zum Konfigurieren von Anschlüssen für ein VLAN. Die Standard-VLAN-ID (PVID) des Anschlusses wird auf dem Bildschirm Create VLAN konfiguriert. Alle nicht getaggten Pakete, die beim Gerät ankommen, werden von der PVID des Anschlusses getaggt.

Der Bildschirm Ports to VLAN enthält eine Anschlusstabelle mit VLAN-Parametern für die einzelnen Anschlüsse. Sie weisen den Anschlüssen die VLAN-Mitgliedschaft zu, indem Sie die bereitgestellten Konfigurationsoptionen auswählen und konfigurieren.

VLAN. Die VLAN-Nummer.

Access. Zeigt an, dass der Anschluss einem einzelnen nicht getaggten VLAN angehört. Wenn sich ein Anschluss im Modus Access befindet, können die für den Anschluss akzeptierten Pakettypen nicht bezeichnet werden. Die Eingangsfilterung kann für einen Zugangsanschluss nicht aktiviert bzw. deaktiviert werden.

Trunk. Zeigt an, dass der Anschluss VLANs angehört, bei denen alle Anschlüsse getaggt sind, mit Ausnahme eines Anschlusses, der nicht getaggt sein muss.

General. Zeigt an, dass der Anschluss VLANs angehört und jedes VLAN als „getaggt“ oder „nicht getaggt“ benutzerdefiniert ist (802.1Q-Vollmodus).

Tagged. Definiert die Schnittstelle als getaggtes Mitglied eines VLAN. Alle von der Schnittstelle weitergeleiteten Pakete sind getaggt. Die Pakete enthalten VLAN-Informationen.

Untagged. Die von der Schnittstelle weitergeleiteten Pakete sind nicht getaggt.

Forbidden. Verbotene Anschlüsse sind nicht im VLAN enthalten.

Exclude. Schließt die Schnittstelle aus dem VLAN aus. Sie können die Schnittstelle dem VLAN jedoch per GVRP hinzufügen.

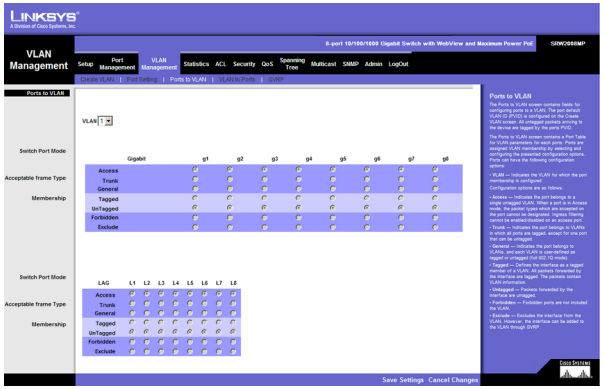


Abbildung 5-13: VLAN Management (VLAN-Verwaltung) – Ports to VLAN (Anschlüsse an VLAN)

Registerkarte „VLAN Management“ – VLAN to Ports

Der Bildschirm VLAN to Ports enthält Felder zum Konfigurieren von VLANs für einen Anschluss.

Interface. Zeigt die Schnittstellennummer an.

Mode. Zeigt den Modus Port to VLAN an. Folgende Feldwerte sind möglich:

- **General.** Zeigt an, dass der Anschluss VLANs angehört und jedes VLAN als „getaggt“ oder „nicht getaggt“ benutzerdefiniert ist (802.1Q-Vollmodus).
- **Access.** Zeigt an, dass der Anschluss einem einzelnen nicht getaggten VLAN angehört. Wenn sich ein Anschluss im Modus Access befindet, können die für den Anschluss akzeptierten Pakettypen nicht bezeichnet werden.
  Die Eingangsfilterung kann für einen Zugangsanschluss nicht aktiviert bzw. deaktiviert werden.
- **Trunk.** Zeigt an, dass der Anschluss VLANs angehört, bei denen alle Anschlüsse getaggt sind, mit Ausnahme eines Anschlusses, der nicht getaggt sein muss.

Join VLAN. Definiert die VLANs, mit denen die Schnittstelle verbunden ist.

VLANs. Zeigt das PVID-Tag an.

LAG. Zeigt an, ob der Anschluss Mitglied einer LAG ist. Wenn er Mitglied einer LAG ist, kann er nicht für ein VLAN konfiguriert werden. Die LAG, der er angehört, kann jedoch für ein VLAN konfiguriert werden.

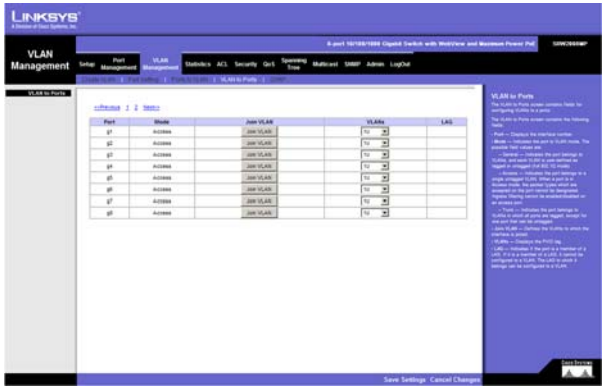


Abbildung 5-14: VLAN Management (VLAN-Verwaltung) – VLAN to Ports (VLAN an Anschlüsse)

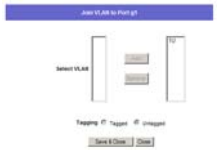


Abbildung 5-15: VLAN to Ports (VLAN an Anschlüsse) – Join VLAN (VLAN beitreten)

Registerkarte „VLAN Management“ – GVRP

Das GARP VLAN Registration Protocol (GVRP) wird speziell für die automatische Verteilung der Informationen zur VLAN-Mitgliedschaft zwischen VLAN-fähigen Verbindungen bereitgestellt. Mithilfe von GVRP können VLAN-fähige Verbindungen automatisch die Zuordnung von VLANs zu Verbindungsanschlüssen lernen, ohne dass jede Verbindung einzeln konfiguriert und die VLAN-Mitgliedschaft registriert werden muss.

Die LAG-Informationen des globalen Systems zeigen dieselben Feldinformationen wie die Anschlüsse an, stellen jedoch die LAG-GVRP-Informationen dar.

Der Bildschirm GVRP ist in zwei Bereiche unterteilt: GVRP und GVRP Table. Die Felddefinitionen sind für beide Bereiche identisch.

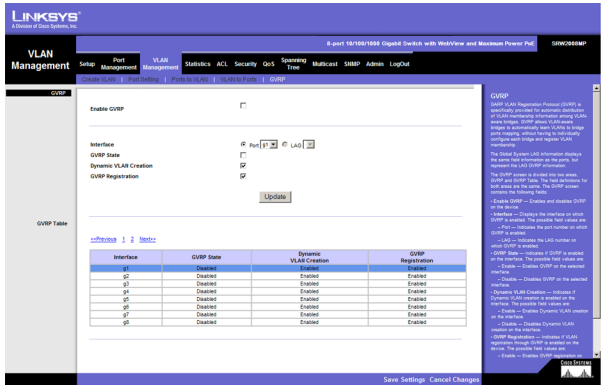


Abbildung 5-16: VLAN Management (VLAN-Verwaltung) – GVRP

Enable GVRP. Aktiviert bzw. deaktiviert GVRP auf dem Gerät.

Interface. Zeigt die Schnittstelle an, auf der GVRP aktiviert ist. Folgende Feldwerte sind möglich:

- **Port.** Zeigt die Nummer des Anschlusses an, für den GVRP aktiviert ist.
- **LAG.** Zeigt die die Nummer der LAG an, für die GVRP aktiviert ist.

GVRP State. Wenn das Kontrollkästchen aktiviert ist, ist GVRP für die Schnittstelle aktiviert.

Dynamic VLAN Creation. Wenn das Kontrollkästchen aktiviert ist, ist die dynamische VLAN-Erstellung für die Schnittstelle aktiviert.

GVRP Registration. Wenn das Kontrollkästchen aktiviert ist, ist die VLAN-Registrierung per GVRP für das Gerät aktiviert.

Mit der Schaltfläche **Update** fügen Sie die konfigurierte GVRP-Einstellung der Tabelle unten auf dem Bildschirm hinzu.

Registerkarte „Statistics“ – RMON Statistics

Der Bildschirm RMON Statistics enthält Felder zum Anzeigen der Informationen zur Verwendung des Geräts und zu Fehler, die im Gerät aufgetreten sind.

Interface. Zeigt das Gerät an, für das die Statistik angezeigt wird. Folgende Feldwerte sind möglich:

- **Port.** Definiert den entsprechenden Anschluss, für den die RMON-Statistik angezeigt wird.
- **LAG.** Definiert die entsprechende LAG, für die die RMON-Statistik angezeigt wird.

Refresh Rate. Definiert den Zeitraum bis zur Aktualisierung der Schnittstellenstatistik. Folgende Feldwerte sind möglich:

- **No Refresh.** Zeigt an, dass die RMON-Statistik nicht aktualisiert wird.
- **15 Sec.** Zeigt an, dass die RMON-Statistik alle 15 Sekunden aktualisiert wird.
- **30 Sec.** Zeigt an, dass die RMON-Statistik alle 30 Sekunden aktualisiert wird.
- **60 Sec.** Zeigt an, dass die RMON-Statistik alle 60 Sekunden aktualisiert wird.

Drop Events. Zeigt die Anzahl der verworfenen Ereignisse an, die für die Schnittstelle seit der letzten Aktualisierung des Geräts angefallen sind.

Received Bytes (Octets). Zeigt die Anzahl der Oktetts an, die die Schnittstelle seit der letzten Aktualisierung des Geräts empfangen hat. Diese Zahl beinhaltet fehlerhafte Pakete und FCS-Oktetts, jedoch keine Rahmenbits.

Received Packets. Zeigt die Anzahl an Paketen an, die von der Schnittstelle seit der letzten Aktualisierung des Geräts empfangen wurden. Dazu gehören fehlerhafte Pakete, Multicast- und Broadcastpakete.

Broadcast Packets Received. Zeigt die Anzahl der fehlerfreien Broadcastpakete an, die die Schnittstelle seit der letzten Aktualisierung des Geräts empfangen hat. Diese Zahl enthält keine Multicastpakete.

Multicast Packets Received. Zeigt die Anzahl der fehlerfreien Multicastpakete an, die die Schnittstelle seit der letzten Aktualisierung des Geräts empfangen hat.

CRC & Align Errors. Zeigt die Anzahl der CRC- und Align-Fehler an, die für die Schnittstelle seit der letzten Aktualisierung des Geräts angefallen sind.

Undersize Packets. Zeigt die Anzahl der Pakete mit zu geringer Größe (weniger als 64 Oktetts) an, die die Schnittstelle seit der letzten Aktualisierung des Geräts empfangen hat.

Oversize Packets. Zeigt die Anzahl der Pakete mit zu hoher Größe (mehr als 1.518 Oktetts) an, die die Schnittstelle seit der letzten Aktualisierung des Geräts empfangen hat.

Fragments. Zeigt die Anzahl der Fragmente (Pakete mit weniger als 64 Oktetts, einschließlich Rahmenbits, jedoch ohne FCS-Oktetts) an, die die Schnittstelle seit der letzten Aktualisierung des Geräts empfangen hat.

Jabbers. Zeigt die gesamte Anzahl der empfangenen Pakete an, deren Länge mehr als 1.518 Oktetts betrug. Diese Zahl enthält keine Rahmenbits, dafür jedoch FCS-Oktetts, die entweder über eine fehlerhafte Frame Check Sequence (FCS) mit einer integrierten Anzahl an Oktetts (FCS-Fehler) oder über eine fehlerhafte FCS mit einem nicht integrierten Oktett (Align-Fehler) verfügen. Der Feldbereich zum Erkennen von so genannten „Jabbers“ beträgt zwischen 20 ms und 150 ms.

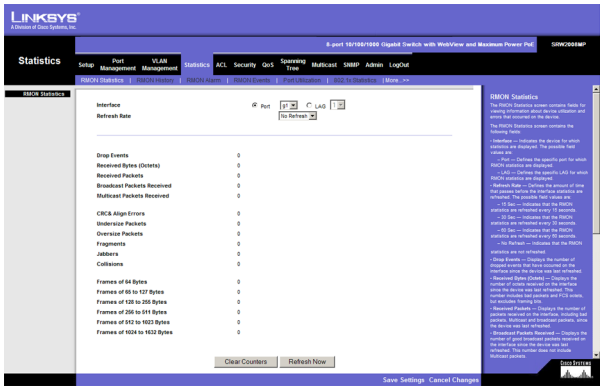


Abbildung 5-17: Statistics (Statistik) – RMON Statistics (RMON-Statistik)

Collisions. Zeigt die Anzahl der Kollisionen an, die die Schnittstelle seit der letzten Aktualisierung des Geräts empfangen hat.

Frames of xx Bytes. Zeigt die Anzahl der xx-Byte-Rahmen an, die die Schnittstelle seit der letzten Aktualisierung des Geräts empfangen hat.

Clear Counters (Schaltfläche). Mit dieser Option setzen Sie alle statistischen Zählungen zurück.

Refresh Now (Schaltfläche). Verwenden Sie diese Option zum Aktualisieren der Statistik.

Registerkarte „Statistics“ – RMON History

Der Bildschirm RMON History enthält Informationen zu Datenbeispielen der Anschlüsse. Die Beispiele können z. B. Schnittstellendefinitionen oder Abfragezeiträume enthalten.

Der Bildschirm RMON History Control ist in die Bereich RMON History und Log Table unterteilt.

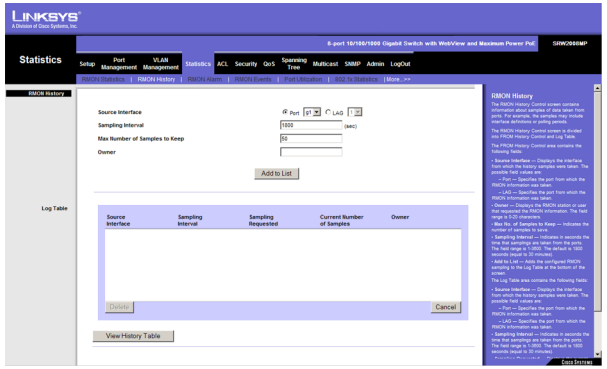


Abbildung 5-18: Statistics (Statistik) – RMON History (RMON-Verlauf)

Source Interface. Zeigt die Schnittstelle an, von der die Verlaufsbeispiele stammen. Folgende Feldwerte sind möglich:

- **Port.** Zeigt den Anschluss an, von dem die RMON-Informationen stammen.
- **LAG.** Zeigt den Anschluss an, von dem die RMON-Informationen stammen.

Sampling Interval. Zeigt den Zeitraum (in Sekunden) an, nach dem Beispieldaten der Anschlüsse aufgezeichnet werden. Der Feldbereich ist 1 bis 3.600. Die Standardeinstellung lautet 1.800 Sekunden (entspricht 30 Minuten).

Max No. of Samples to Keep. Zeigt die Anzahl der zu speichernden Beispiele an.

Owner. Zeigt die RMON-Station bzw. den -Benutzer an, die bzw. der die RMON-Informationen angefordert hat. Der Feldbereich beträgt 0 bis 20 Zeichen.

Mit der Schaltfläche **Add to List** fügen Sie die konfigurierten RMON-Beispieldaten der Log Table unten auf dem Bildschirm hinzu.

Log Table

Sampling Requested. Zeigt die Anzahl der zu speichernden Beispiele an. Der Feldbereich ist 1 bis 65.535. Der Standardwert ist 50.

Current Number of Samples. Zeigt die aktuelle Anzahl der aufgezeichneten Beispieldaten an.

Schaltfläche **View History**. Durch Klicken auf diese Schaltfläche wird der Bildschirm RMON History geöffnet.

RMON History

Der Bildschirm RMON History enthält statistische Netzwerkbeispieldaten für die einzelnen Schnittstellen. Jeder Tabelleneintrag umfasst alle Zählerwerte, die für ein einzelnes Beispiel erfasst wurden.

History Entry No. Zeigt die Nummer des Eintrags in der Verlaufstabelle an.

Owner. Zeigt die RMON-Station bzw. den -Benutzer an, die bzw. der die RMON-Informationen angefordert hat. Der Feldbereich beträgt 0 bis 20 Zeichen.

Sample No. Zeigt die Nummer des Beispiels an, von dem die Statistik stammt.

Drop Events. Zeigt die Anzahl der verworfenen Ereignisse an, die für die Schnittstelle seit der letzten Aktualisierung des Geräts angefallen sind.

Received Bytes (Octets). Zeigt die Anzahl der Oktetts an, die die Schnittstelle seit der letzten Aktualisierung des Geräts empfangen hat. Diese Zahl beinhaltet fehlerhafte Pakete und FCS-Oktetts, jedoch keine Rahmenbits.

Received Packets. Zeigt die Anzahl an Paketen an, die von der Schnittstelle seit der letzten Aktualisierung des Geräts empfangen wurden. Dazu gehören fehlerhafte Pakete, Multicast- und Broadcastpakete.

Broadcast Packets. Zeigt die Anzahl der fehlerfreien Broadcastpakete an, die die Schnittstelle seit der letzten Aktualisierung des Geräts empfangen hat. Diese Zahl enthält keine Multicastpakete.

Multicast Packets. Zeigt die Anzahl der fehlerfreien Multicastpakete an, die die Schnittstelle seit der letzten Aktualisierung des Geräts empfangen hat.

CRC & Align Errors. Zeigt die Anzahl der CRC- und Align-Fehler an, die für die Schnittstelle seit der letzten Aktualisierung des Geräts angefallen sind.

Undersize Packets. Zeigt die Anzahl der Pakete mit zu geringer Größe (weniger als 64 Oktetts) an, die die Schnittstelle seit der letzten Aktualisierung des Geräts empfangen hat.

Oversize Packets. Zeigt die Anzahl der Pakete mit zu hoher Größe (mehr als 1.518 Oktetts) an, die die Schnittstelle seit der letzten Aktualisierung des Geräts empfangen hat.

Fragments. Zeigt die Anzahl der Fragmente (Pakete mit weniger als 64 Oktetts, einschließlich Rahmenbits, jedoch ohne FCS-Oktetts) an, die die Schnittstelle seit der letzten Aktualisierung des Geräts empfangen hat.

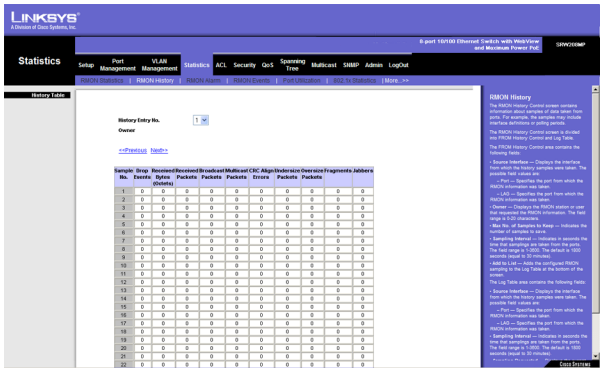


Abbildung 5-19: RMON History-Tabelle (RMON-Verlauf)

Jabbers. Zeigt die gesamte Anzahl der empfangenen Pakete an, deren Länge mehr als 1.518 Oktetts betrug. Diese Zahl enthält keine Rahmenbits, dafür jedoch FCS-Oktetts, die entweder über eine fehlerhafte Frame Check Sequence (FCS) mit einer integrierten Anzahl an Oktetts (FCS-Fehler) oder über eine fehlerhafte FCS mit einem nicht integrierten Oktett (Align-Fehler) verfügen. Der Feldbereich zum Erkennen von so genannten „Jabbers“ beträgt zwischen 20 ms und 150 ms.

Collisions. Zeigt die Anzahl der Kollisionen an, die die Schnittstelle seit der letzten Aktualisierung des Geräts empfangen hat.

Utilization. Zeigt den Prozentsatz der verwendeten Schnittstelle an.

Registerkarte „Statistics“ – RMON Alarm

Der Bildschirm RMON Alarm enthält Felder zum Festlegen von Netzwerkalarmmeldungen. Netzwerkalarmmeldungen treten auf, wenn ein Netzwerkproblem oder -ereignis erkannt wird. Steigende und fallende Schwellenwerte lösen Ereignisse aus.

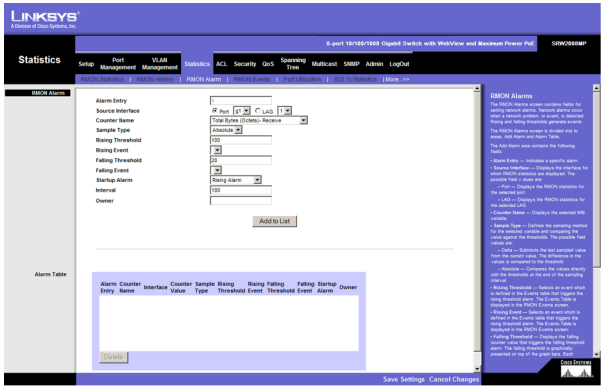


Abbildung 5-20: Statistics (Statistik) – RMON Alarm (RMON-Alarmmeldung)

Alarm Entry. Zeigt eine bestimmte Alarmmeldung an.

Source Interface. Zeigt die Schnittstelle an, für die die RMON-Statistik angezeigt wird. Folgende Feldwerte sind möglich:

- **Port.** Zeigt die RMON-Statistik für den ausgewählten Anschluss an.
- **LAG.** Zeigt die RMON-Statistik für die ausgewählte LAG an.

Counter Name. Zeigt die gewählte MIB-Variable an.

Sample Type. Definiert das Verfahren zur Erfassung der ausgewählten Variable und für den Vergleich des Werts mit den Schwellenwerten. Folgende Feldwerte sind möglich:

- **Absolute.** Vergleicht die Werte direkt mit den Schwellenwerten am Ende des Erfassungsintervalls.
- **Delta.** Subtrahiert den zuletzt erfassten Wert vom aktuellen Wert. Die Differenz der Werte wird mit dem Schwellenwert verglichen.

Rising Threshold. Zeigt den steigenden Zählerwert an, der die Alarmmeldung für den steigenden Schwellenwert auslöst. Der steigende Schwellenwert wird oberhalb der Balken angezeigt. Jeder überwachten Variablen wird eine Farbe zugewiesen.

Rising Event. Zeigt den Mechanismus für die Anzeige der Alarmmeldungen an. Folgende Feldwerte sind möglich:

- **LOG.** Zeigt an, dass für das Gerät bzw. im Verwaltungssystem kein Speichermechanismus vorhanden ist. Wenn Sie das Gerät nicht zurücksetzen, bleibt der Eintrag in der Log Table bestehen.

- **TRAP.** Zeigt an, dass eine SNMP-Trap erzeugt und über den Trap-Mechanismus gesendet wird. Sie können die Trap auch speichern, indem Sie den Trap-Mechanismus verwenden.
- **Both.** Zeigt an, dass sowohl der Log- als auch der Trap-Mechanismus zum Berichten von Alarmmeldungen verwendet wird.

Falling Threshold. Zeigt den fallenden Zählerwert an, der die Alarmmeldung für den fallenden Schwellenwert auslöst. Der fallende Schwellenwert wird oberhalb der Balken grafisch dargestellt. Jeder überwachten Variablen wird eine Farbe zugewiesen.

Falling Event. Zeigt den Mechanismus für die Anzeige der Alarmmeldungen an. Folgende Feldwerte sind möglich:

- **LOG.** Zeigt an, dass für das Gerät bzw. im Verwaltungssystem kein Speichermechanismus vorhanden ist. Wenn Sie das Gerät nicht zurücksetzen, bleibt der Eintrag in der Log Table bestehen.
- **TRAP.** Zeigt an, dass eine SNMP-Trap erzeugt und über den Trap-Mechanismus gesendet wird. Sie können die Trap auch speichern, indem Sie den Trap-Mechanismus verwenden.
- **Both**. Zeigt an, dass sowohl der Log- als auch der Trap-Mechanismus zum Berichten von Alarmmeldungen verwendet wird.

Startup Alarm. Zeigt das auslösende Element an, das die Erzeugung der Alarmmeldung aktiviert. Ein Anstieg ist als der Übergang von einem niedrigen Schwellenwert zu einem hohen Schwellenwert durch den Schwellenwert definiert.

Interval. Definiert den Intervallzeitraum der Alarmmeldung in Sekunden.

Owner. Zeigt das Gerät bzw. den Benutzer an, das bzw. der die Alarmmeldung definiert hat.

Mit der Schaltfläche **Add to List** fügen Sie den Eintrag der Tabelle mit den RMON-Alarmmeldungen hinzu.

Der Bereich mit der Tabelle mit den Alarmmeldungen enthält das folgende zusätzliche Feld:

Counter Value. Zeigt den aktuellen Zählerwert für die jeweilige Alarmmeldung an.

Registerkarte „Statistics“ – RMON Events

Der Bildschirm RMON Events enthält Felder zum Definieren von RMON-Ereignissen.

Add Event

Event Entry. Zeigt das Ereignis an.

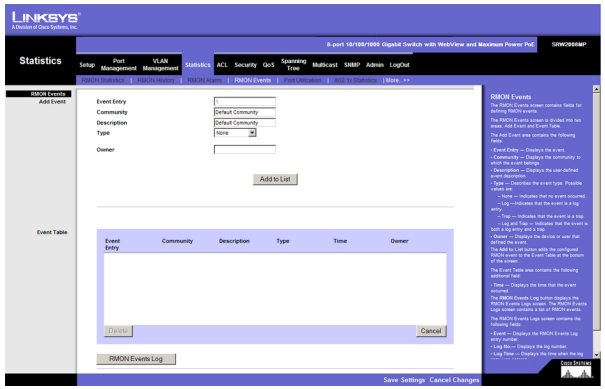


Abbildung 5-21: Statistics (Statistik) – RMON Events (RMON-Ereignisse)

Community. Zeigt die Community an, der das Ereignis angehört.

Description. Zeigt die benutzerdefinierte Ereignisbeschreibung an.

Type. Beschreibt den Ereignistyp. Folgende Werte sind möglich:

- **None.** Zeigt an, dass kein Ereignis eingetreten ist.
- **Log.** Zeigt an, dass es sich bei dem Ereignis um einen Protokolleintrag handelt.
- **Trap.** Zeigt an, dass es sich bei dem Ereignis um eine Trap handelt.
- **Log and Trap**. Zeigt an, dass es sich bei dem Ereignis sowohl um einen Protokolleintrag als auch um eine Trap handelt.

Owner. Zeigt das Gerät bzw. den Benutzer an, das bzw. der das Ereignis definiert hat.

Mit der Schaltfläche **Add to List** fügen Sie das konfigurierte RMON-Ereignis der Event Table unten auf dem Bildschirm hinzu.

Der Bereich Event Table enthält das folgende zusätzliche Feld:

Time. Zeigt den Zeitpunkt an, zu dem das Ereignis eingetreten ist.

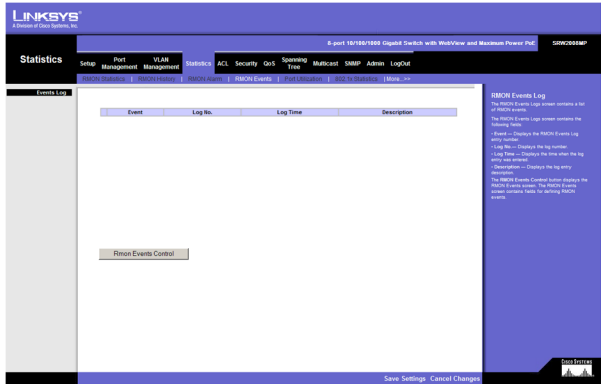


Abbildung 5-22: RMON Events (RMON-Ereignisse) – Events Log (Ereignisprotokoll)

Registerkarte „Statistics“ – Port Utilization

Auf dem Bildschirm **Port Utilization** wird die Menge an Ressourcen angezeigt, die die einzelnen Schnittstellen momentan nutzen. Grün angezeigte Anschlüsse funktionieren normal, während rot angezeigte Anschlüsse momentan eine übermäßige Menge an Netzwerkverkehr übertragen.

Refresh Rate. Zeigt den Zeitraum bis zur Aktualisierung der Statistik zur Anschlussauslastung an. Folgende Feldwerte sind möglich:

- **No Refresh.** Zeigt an, dass die Statistik nicht aktualisiert wird.
- **15 Sec.** Zeigt an, dass die Statistik alle 15 Sekunden aktualisiert wird.
- **30 Sec.** Zeigt an, dass die Statistik alle 30 Sekunden aktualisiert wird.
- **60 Sec.** Zeigt an, dass die Statistik alle 60 Sekunden aktualisiert wird.

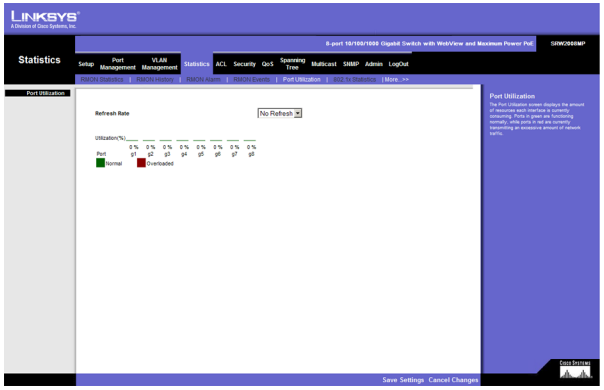


Abbildung 5-23: Statistics (Statistik) – Port Utilization (Anschlussauslastung)

Registerkarte „Statistics“ – 802.1x Statistics

Der Bildschirm 802.1X Statistics enthält Informationen zu EAP-Paketen, die an einem bestimmten Anschluss empfangen werden.

Port. Zeigt den Anschluss an, von dem die statistischen Daten abgefragt werden.

Refresh Rate. Zeigt den Zeitraum bis zur Aktualisierung der EAP-Statistik an. Folgende Feldwerte sind möglich:

- **No Refresh.** Zeigt an, dass die EAP-Statistik nicht aktualisiert wird.
- **15 Sec.** Zeigt an, dass die EAP-Statistik alle 15 Sekunden aktualisiert wird.
- **30 Sec.** Zeigt an, dass die EAP-Statistik alle 30 Sekunden aktualisiert wird.
- **60 Sec.** Zeigt an, dass die EAP-Statistik alle 60 Sekunden aktualisiert wird.

Name. Zeigt die gemessenen 802.1x-Statistikdaten an.

Description. Beschreibt die gemessenen 802.1x-Statistikdaten.

Packet. Zeigt die Paketmenge an, die für die jeweilige 802.1x-Statistik gemessen wurde.

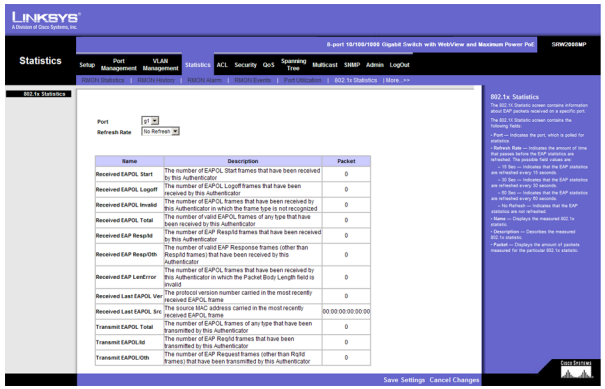


Abbildung 5-24: Statistics (Statistik) – 802.1x Statistics (802.1x-Statistik)

Registerkarte „Statistics“ – GVRP Statistics

Der Bildschirm GVRP Statistics enthält die Gerätestatistik für GVRP.

Der Bildschirm GVRP Statistics ist in zwei Bereiche unterteilt: GVRP Statistics Table und GVRP Error Statistics Table. Die folgenden Felder gelten für beide Tabellen:

Interface. Zeigt den Schnittstellentyp an, für den die Statistik angezeigt wird.

- **Port.** Zeigt an, dass die Anschlussstatistik angezeigt wird.
- **LAG.** Zeigt an, dass die LAG-Statistik angezeigt wird.

Refresh Rate. Zeigt den Zeitraum bis zur Aktualisierung der GVRP-Statistik an. Folgende Feldwerte sind möglich:

- **No Refresh.** Zeigt an, dass die GVRP-Statistik nicht aktualisiert wird.
- **15 Sec.** Zeigt an, dass die GVRP-Statistik alle 15 Sekunden aktualisiert wird.

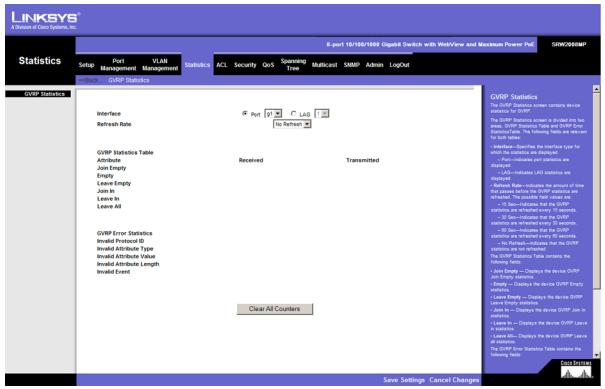


Abbildung 5-25: Statistics (Statistik) – GVRP Statistics (GVRP-Statistik)

- **30 Sec.** Zeigt an, dass die GVRP-Statistik alle 30 Sekunden aktualisiert wird.
- **60 Sec.** Zeigt an, dass die GVRP-Statistik alle 60 Sekunden aktualisiert wird.

Die GVRP Statistics Table enthält die folgenden Felder:

Join Empty. Zeigt die Statistik GVRP Join Empty für das Gerät an.

Empty. Zeigt die Statistik GVRP Empty für das Gerät an.

Leave Empty. Zeigt die Statistik GVRP Leave Empty für das Gerät an.

Join In. Zeigt die Statistik GVRP Join In für das Gerät an.

Leave In. Zeigt die Statistik GVRP Leave In für das Gerät an.

Leave All. Zeigt die Statistik GVRP Leave All für das Gerät an.

Die GVRP Error Statistics Table enthält die folgenden Felder:

Invalid Protocol ID. Zeigt die Statistik GVRP Invalid Protocol ID für das Gerät an.

Invalid Attribute Type. Zeigt die Statistik GVRP Invalid Attribute ID für das Gerät an.

Invalid Attribute Value. Zeigt die Statistik GVRP Invalid Attribute Value für das Gerät an.

Invalid Attribute Length. Zeigt die Statistik GVRP Invalid Attribute Length für das Gerät an.

Invalid Events. Zeigt die Statistik GVRP Invalid Events für das Gerät an.

Mit der Schaltfläche **Clear All Counters** setzen Sie alle Tabellen zurück.

Registerkarte „ACL“ – IP Based ACL

Der Bildschirm IP Based ACL enthält Informationen zum Definieren von IP-basierten Zugriffssteuerungslisten (Access Control Lists, ACLs).

ACL Name. Zeigt die benutzerdefinierten IP-basierten Zugriffssteuerungslisten an.

New ACL Name. Definiert eine neue benutzerdefinierte IP-basierte Zugriffssteuerungsliste.

Delete ACL. Löscht die ausgewählte Zugriffssteuerungsliste.

Action. Zeigt die Aktion an, die dem Paket zugewiesen ist, das mit der Zugriffssteuerungsliste übereinstimmt. Pakete werden weitergeleitet oder verworfen. Außerdem kann der Anschluss geschlossen, eine Trap an den Netzwerkadministrator gesendet oder eine Paketrate als Einschränkung der Weiterleitung zugewiesen werden. Es sind folgende Optionen verfügbar:

- **Permit.** Leitet Pakete weiter, die die Kriterien der Zugriffssteuerungsliste erfüllen.
- **Deny.** Verwirft Pakete, die die Kriterien der Zugriffssteuerungsliste erfüllen.
- **Shutdown.** Verwirft Pakete, die die Kriterien der Zugriffssteuerungsliste erfüllen, und deaktiviert den Anschluss, an den das Paket adressiert war. Sie können Anschlüsse auf dem Bildschirm Port Management wieder aktivieren.

Protocol. Erstellt basierend auf einem bestimmten Protokoll ein ACE (Access Control Event), also ein Zugriffssteuerungsereignis.

- **Select from List.** Trifft eine Auswahl aus einer Protokollliste, auf der das ACE basieren kann. Folgende Feldwerte sind möglich:
  - **Any.** Ordnet das Protokoll einem beliebigen anderen Protokoll zu.
  - **EIGRP.** Zeigt an, dass zum Klassifizieren der Netzwerkflüsse das Enhanced Interior Gateway Routing Protocol (EIGRP) verwendet wird.
  - **ICMP.** Zeigt an, dass zum Klassifizieren der Netzwerkflüsse das Internet Control Message Protocol (ICMP) verwendet wird.
  - **IGMP.** Zeigt an, dass zum Klassifizieren der Netzwerkflüsse das Internet Group Management Protocol (IGMP) verwendet wird.
  - **TCP.** Zeigt an, dass zum Klassifizieren der Netzwerkflüsse das Transmission Control Protocol verwendet wird.
  - **OSPF.** Ordnet das Paket dem Open Shortest Path First-Protokoll (OSPF) zu.
  - **UDP.** Zeigt an, dass zum Klassifizieren der Netzwerkflüsse das User Datagram Protocol verwendet wird.
- **Protocol ID To Match.** Fügt dem Zugriffssteuerungsereignis benutzerdefinierte Protokolle hinzu, denen Pakete zugeordnet sind. Jedes Protokoll verfügt über eine bestimmte eindeutige Protokollnummer. Der zulässige Feldbereich beträgt 0 bis 255.

TCP Flags. Filtert Pakete nach TCP-Flag. Gefilterte Pakete werden entweder weitergeleitet oder verworfen. Das Filtern von Paketen nach TCP-Flags verbessert die Paketsteuerung, was zu einer erhöhten Netzwerksicherheit führt. Sie können folgende Werte zuweisen:

- **Set.** Aktiviert das Filtern von Paketen anhand von ausgewählten Flags.

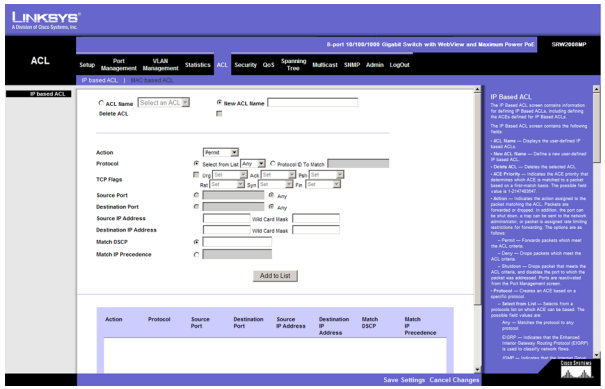


Abbildung 5-26: ACL (Zugriffssteuerungsliste) – IP Based ACL (IP-basierte Zugriffssteuerungsliste)

- **Unset.** Deaktiviert das Filtern von Paketen anhand von ausgewählten Flags.
- **Don't care.** Zeigt an, dass sich ausgewählte Pakete nicht auf den Prozess der Paketfilterung auswirken.

Sie können folgende TCP-Flags auswählen:

Urg. Zeigt an, dass ein Paket dringend ist.

Ack. Zeigt an, dass ein Paket bestätigt wurde.

Psh. Zeigt an, dass auf ein Paket ein Push-Vorgang angewendet wurde.

Rst. Zeigt an, dass die Verbindung verworfen wurde.

Syn. Zeigt an, dass das Starten einer Sitzung angefordert wird.

Fin. Zeigt an, dass das Schließen einer Sitzung angefordert wird.

Source Port. Definiert den TCP/UDP-Quellanschluss, dem das Zugriffssteuerungsereignis zugeordnet ist. Das Feld ist nur aktiv, wenn Sie im Dropdownmenü Select from den Eintrag 800/6-TCP oder 800/17-UDP auswählen. Der zulässige Feldbereich beträgt 0 bis 65.535.

Destination Port. Definiert den TCP/UDP-Zielanschluss. Das Feld ist nur aktiv, wenn Sie im Dropdownmenü Select from den Eintrag 800/6-TCP oder 800/17-UDP auswählen. Der zulässige Feldbereich beträgt 0 bis 65.535.

Source IP Address. Ordnet die IP-Adresse des Quellanschlusses, an die Pakete adressiert sind, dem Zugriffssteuerungsereignis zu.

Wildcard Mask. Definiert die Platzhaltermaske der Quell-IP-Adresse. Platzhaltermasken legen fest, welche Bits verwendet und welche Bits ignoriert werden. Die Platzhaltermaske 255.255.255.255 zeigt an, dass kein Bit wichtig ist. Die Platzhaltermaske 0.0.0.0 zeigt an, dass alle Bits wichtig sind. Wenn die Quell-IP-Adresse z. B. 149.36.184.198 und die Platzhaltermaske 255.36.184.00 lautet, werden die ersten acht Bits der IP-Adresse ignoriert und die letzten acht Bits verwendet.

Dest. IP Address. Ordnet die IP-Adresse des Zielanschlusses, an die Pakete adressiert sind, dem Zugriffssteuerungsereignis zu.

Wildcard Mask. Definiert die Platzhaltermaske der Ziel-IP-Adresse.

Match DSCP. Ordnet den DSCP-Wert eines Pakets dem Zugriffssteuerungsereignis zu. Es wird entweder der DSCP-Wert oder der IP-Vorrangigkeitswert verwendet, um den Zugriffssteuerungslisten Pakete zuzuordnen. Der zulässige Feldbereich beträgt 0 bis 63.

Match IP Precedence. Ordnet den IP-Vorrangigkeitswert eines Pakets dem Zugriffssteuerungsereignis zu. Es wird entweder der DSCP-Wert oder der IP-Vorrangigkeitswert verwendet, um den Zugriffssteuerungslisten Pakete zuzuordnen. Der zulässige Feldbereich beträgt 0 bis 7.

Mit der Schaltfläche **Add to List** fügen Sie die konfigurierten IP-basierten Zugriffssteuerungslisten der IP Based ACL Table unten auf dem Bildschirm hinzu.

Registerkarte „ACL“ – MAC Based ACL

Auf dem Bildschirm **MAC Based ACL** können Sie eine MAC-basierte Zugriffssteuerungsliste definieren. Sie können Zugriffssteuerungsereignisse (ACEs) nur hinzufügen, wenn die Zugriffssteuerungsliste (ACL) keiner Schnittstelle fest zugeordnet ist.

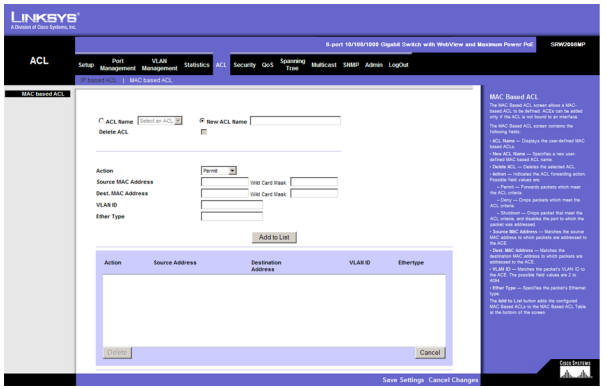


Abbildung 5-27: ACL (Zugriffssteuerungsliste) – MAC Based ACL (MAC-basierte Zugriffssteuerungsliste)

ACL Name. Zeigt die benutzerdefinierten MAC-basierten Zugriffssteuerungslisten an.

New ACL Name. Legt einen neuen benutzerdefinierten MAC-basierten Zugriffssteuerungslisten-Namen fest.

Delete ACL. Löscht die ausgewählte Zugriffssteuerungsliste.

Action. Zeigt die Weiterleitungsaktion der Zugriffssteuerungsliste an. Folgende Feldwerte sind möglich:

- **Permit.** Leitet Pakete weiter, die die Kriterien der Zugriffssteuerungsliste erfüllen.
- **Deny.** Verwirft Pakete, die die Kriterien der Zugriffssteuerungsliste erfüllen.
- **Shutdown.** Verwirft Pakete, die die Kriterien der Zugriffssteuerungsliste erfüllen, und deaktiviert den Anschluss, an den das Paket adressiert war.

Source MAC Address. Ordnet die Quell-MAC-Adresse, an die Pakete adressiert sind, dem Zugriffssteuerungsereignis zu.

Wildcard Mask. Definiert die Platzhaltermaske der Quell-IP-Adresse. Platzhaltermasken legen fest, welche Bits verwendet und welche Bits ignoriert werden. Die Platzhaltermaske 255.255.255.255 zeigt an, dass kein Bit wichtig ist. Die Platzhaltermaske 0.0.0.0 zeigt an, dass alle Bits wichtig sind. Wenn die Quell-IP-Adresse z. B. 149.36.184.198 und die Platzhaltermaske 255.36.184.00 lautet, werden die ersten acht Bits der IP-Adresse ignoriert und die letzten acht Bits verwendet.

Dest. MAC Address. Ordnet die Ziel-MAC-Adresse, an die Pakete adressiert sind, dem Zugriffssteuerungsereignis zu.

Wildcard Mask. Definiert die Platzhaltermaske der Ziel-IP-Adresse.

VLAN ID. Ordnet die VLAN-ID eines Pakets dem Zugriffssteuerungsereignis zu. Zulässige Feldwerte sind 2 bis 4.094:

Ether Type. Gibt den Ethernet-Typ eines Pakets an.

Mit der Schaltfläche **Add to List** fügen Sie die konfigurierten MAC-basierten Zugriffssteuerungslisten der MAC Based ACL Table unten auf dem Bildschirm hinzu.

Registerkarte „Security“ – ACL Binding

Wenn eine Zugriffssteuerungsliste einer Schnittstelle fest zugeordnet ist, werden alle definierten Regeln des Zugriffssteuerungsereignisses auf die ausgewählte Schnittstelle angewendet. Immer wenn eine Zugriffssteuerungsliste für einen Anschluss, eine LAG oder ein VLAN zugewiesen wird, werden Flüsse von dieser Eingangsschnittstelle, die nicht mit der Zugriffssteuerungsliste übereinstimmen, der Standardregel zugeordnet. Die Standardregel bewirkt, dass nicht übereinstimmende Pakete verworfen werden.

Interface. Zeigt die Schnittstelle an, der die Zugriffssteuerungsliste fest zugeordnet ist.

ACL Name. Zeigt die Zugriffssteuerungsliste an, die der Schnittstelle fest zugeordnet ist.

Mit der Schaltfläche **Add to List** fügen Sie die Konfiguration für die Bindung der Zugriffssteuerungsliste der ACL Binding Table unten auf dem Bildschirm hinzu.

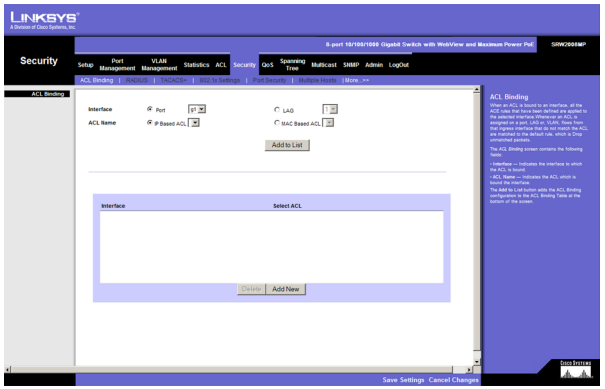


Abbildung 5-28: Security (Sicherheit) – ACL Binding (Bindung an Zugriffssteuerungsliste)

Registerkarte „Security“ – RADIUS

RADIUS-Server (Remote Authorization Dial-In User Service) geben Netzwerken zusätzliche Sicherheit. RADIUS-Server bieten ein zentrales Authentifizierungsverfahren für den Webzugriff.

IP Address. Die IP-Adresse des Authentifizierungsservers.

Priority. Die Priorität des Servers. Mögliche Werte sind 0 bis 65.535, wobei 1 der höchste Wert ist. Die Priorität des RADIUS-Servers wird verwendet, um die Abfragereihenfolge der Server zu konfigurieren.

Authentication Port. Identifiziert den Authentifizierungsanschluss. Der Authentifizierungsanschluss wird zum Überprüfen der RADIUS-Serverauthentifizierung verwendet. Die Standardeinstellung des authentifizierten Anschlusses lautet 1.812.

Number of Retries. Definiert die Anzahl an übertragenen Anforderungen, die an einen RADIUS-Server gesendet werden können, bevor ein Fehler auftritt. Mögliche Feldwerte sind 1 bis 10. Die Standardeinstellung ist 3.

Timeout for Reply. Definiert den Zeitraum in Sekunden, wie lange das Gerät auf eine Antwort des RADIUS-Servers wartet, bevor erneut versucht wird, die Abfrage durchzuführen, bzw. zum nächsten Server gewechselt wird. Mögliche Feldwerte sind 1 bis 30. Die Standardeinstellung ist 3.

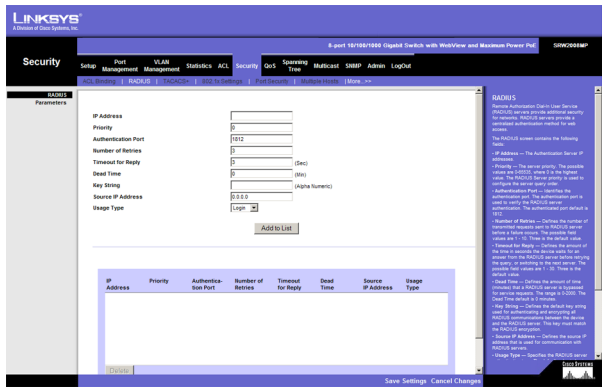


Abbildung 5-29: Security (Sicherheit) – RADIUS (RADIUS)

Dead Time. Definiert den Zeitraum (in Minuten), für den ein RADIUS-Server bei Dienstanforderungen umgangen wird. Der Bereich ist 0 bis 2.000. Die Standardeinstellung beträgt 0 Minuten.

Key String. Definiert die standardmäßige Schlüsselzeichenfolge, die für das Authentifizieren und Verschlüsseln der gesamten RADIUS-Kommunikation zwischen dem Gerät und dem RADIUS-Server verwendet wird. Dieser Schlüssel muss der RADIUS-Verschlüsselung entsprechen.

Source IP Address. Definiert die Quell-IP-Adresse, die für die Kommunikation mit RADIUS-Servern verwendet wird.

Usage Type. Legt den Authentifizierungstyp für den RADIUS-Server fest. Der Standardwert lautet Login. Folgende Feldwerte sind möglich:

- **Login.** Zeigt an, dass der RADIUS-Server zum Authentifizieren von Benutzernamen und Kennwörtern verwendet wird.
- **802.1X.** Zeigt an, dass der RADIUS-Server für die 802.1X-Authentifizierung verwendet wird.
- **All.** Zeigt an, dass der RADIUS-Server zum Authentifizieren von Benutzernamen und Kennwörtern und zum Authentifizieren von 802.1X-Anschlüssen verwendet wird.

Mit der Schaltfläche **Add to List** fügen Sie die RADIUS-Konfiguration der RADIUS Table unten auf dem Bildschirm hinzu.

Registerkarte „Security“ – TACACS+

Das Gerät bietet TACACS+-Clientunterstützung (Terminal Access Controller Access Control System). TACACS+ ermöglicht eine zentrale Sicherheitsfunktion zum Überprüfen der Benutzer, die auf das Gerät zugreifen. Mithilfe von TACACS+ wird ein zentrales Benutzerverwaltungssystem bereitgestellt, während gleichzeitig die Konsistenz mit RADIUS und anderen Authentifizierungsprozessen gewahrt bleibt. Das TACACS+-Protokoll stellt die Netzwerkintegrität sicher, indem ein verschlüsselter Protokollaustausch zwischen dem Gerät und dem TACACS+-Server erfolgt.

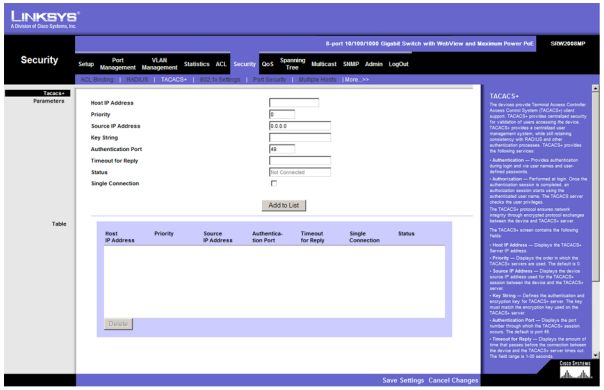


Abbildung 5-30: Security (Sicherheit) – TACACS+

Host IP Address. Zeigt die IP-Adresse des TACACS+-Servers an.

Priority. Zeigt die Reihenfolge an, in der die TACACS+-Server verwendet werden. Standardmäßig ist *0* eingestellt.

Source IP Address. Zeigt die Quell-IP-Adresse des Geräts an, die für die TACACS+-Sitzung zwischen dem Gerät und dem TACACS+-Server verwendet wird.

Key String. Definiert den Authentifizierungs- und Verschlüsselungsschlüssel für TACACS+-Server. Dieser Schlüssel muss dem Verschlüsselungsschlüssel entsprechen, der auf dem TACACS+-Server verwendet wird.

Authentication Port. Zeigt die Nummer des Anschlusses an, über den die TACACS+-Sitzung ausgeführt wird. Standardmäßig wird der Anschluss 49 verwendet.

Timeout for Reply. Zeigt den Zeitraum an, der verstreicht, bevor für die Verbindung zwischen dem Gerät und dem TACACS+-Server die Zeitüberschreitung erreicht ist. Der Feldbereich beträgt 1 bis 30 Sekunden.

Status. Zeigt den Verbindungsstatus zwischen dem Gerät und dem TACACS+-Server an. Folgende Feldwerte sind möglich:

- Connected. Zwischen dem Gerät und dem TACACS+-Server besteht eine Verbindung.
- Not Connected. Zwischen dem Gerät und dem TACACS+-Server besteht keine Verbindung.

Single Connection. Wenn diese Option aktiviert ist, wird zwischen dem Gerät und dem TACACS+-Server eine einzelne offene Verbindung verwendet.

Mit der Schaltfläche **Add to List** fügen Sie die TACACS+-Konfiguration der TACACS+ Table unten auf dem Bildschirm hinzu.

Registerkarte „Security“ – 802.1x Settings

Die anschlussbasierte Authentifizierung aktiviert Benutzer des Authentifizierungssystems Anschluss für Anschluss über einen externen Server. Nur authentifizierte und genehmigte Systembenutzer können Daten übertragen und empfangen. Anschlüsse werden mithilfe des Extensible Authentication Protocol (EAP) über den RADIUS-Server authentifiziert.

Enable 802.1x. Aktivieren Sie das Kontrollkästchen, um die 802.1x-Authentifizierung zu aktivieren.

Port. Zeigt den Namen des Anschlusses an.

Status Port Control. Gibt den Autorisierungsstatus des Anschlusses an. Folgende Feldwerte sind möglich:

- **Force-Authorized.** Der Status des überwachten Anschlusses wird auf Force-Authorized (Datenverkehr weiterleiten) gesetzt.
- **Force-Unauthorized.** Der überwachte Anschlussstatus wird auf Force-Unauthorized (Datenverkehr verwerfen) gesetzt.

Enable Periodic Reauthentication. Lässt die sofortige Neuauthentifizierung des Anschlusses zu.

Mit der Schaltfläche **Setting Timer** öffnen Sie den Bildschirm Setting Timer, auf dem Sie die Anschlüsse für die 802.1x-Funktionen konfigurieren können.

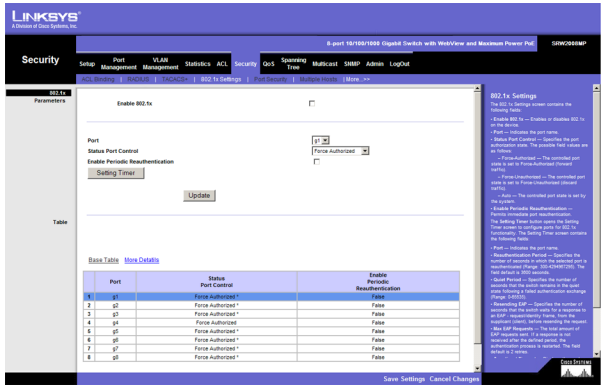


Abbildung 5-31: Security (Sicherheit) – 802.1x Settings (802.1x-Einstellungen)

Bildschirm Setting Timer

Port. Zeigt den Namen des Anschlusses an.

Reauthentication Period. Gibt den Zeitraum in Sekunden an, in dem die erneute Authentifizierung des ausgewählten Anschlusses erfolgt (Bereich: 300-4294967295). Standardmäßig ist das Feld auf 3600 Sekunden eingestellt.

Quiet Period. Gibt den Zeitraum in Sekunden an, in dem der Switch nach einem fehlgeschlagenen Authentifizierungsaustausch im Ruhezustand verbleibt (Bereich: 0-65535).

Resending EAP. Gibt den Zeitraum in Sekunden an, wie lange der Switch auf eine Antwort des anfordernden Computers (Clients) auf einen „EAP – Anforderung/Identität-Rahmen“ wartet, bevor die Anforderung erneut gesendet wird.

Max EAP Requests. Die gesamte Anzahl der gesendeten EAP-Anforderungen. Wird innerhalb des definierten Zeitraums keine Antwort empfangen, wird der Authentifizierungsprozess neu gestartet. Standardmäßig werden zwei Versuche durchgeführt.

Supplicant Timeout. Zeigt den Zeitraum in Sekunden an, der verstreicht, bevor EAP-Anforderungen erneut an den anfordernden Computer gesendet werden (Bereich: 1-65535). Standardmäßig ist das Feld auf 30 Sekunden eingestellt.

Server Timeout. Gibt den Zeitraum in Sekunden an, die verstreichen, bevor der Switch eine Anforderung erneut an den Authentifizierungsserver sendet (Bereich: 1-65535). Standardmäßig ist das Feld auf 30 Sekunden eingestellt.

Abbildung 5-32: 802.1x Settings (802.1x-Einstellungen) – Setting Timer (Zeitlimit einstellen)

Registerkarte „Security“ – Port Security

Sie können die Netzwerksicherheit erhöhen, indem Sie den Zugriff auf einen Anschluss nur auf Benutzer mit bestimmten MAC-Adressen beschränken. MAC-Adressen können dynamisch gelernt oder statisch konfiguriert werden. Die Sicherheitsfunktion für gesperrte Anschlüsse überwacht sowohl empfangene als auch „gelernte“ Pakete, die an bestimmten Anschlüssen empfangen werden. Der Zugriff auf den gesperrten Anschluss ist auf Benutzer mit bestimmten MAC-Adressen beschränkt. Diese Adressen werden für den Anschluss entweder manuell definiert oder am Anschluss bis zu dem Punkt „gelernt“, an dem der Anschluss gesperrt wird. Wenn ein Paket an einem gesperrten Anschluss empfangen wird und die Quell-MAC-Adresse diesem Anschluss nicht fest zugeordnet ist (sie wurde entweder an einem anderen Anschluss gelernt oder ist dem System nicht bekannt), wird der Schutzmechanismus aufgerufen. Der Mechanismus verfügt über verschiedene Optionen. Nicht autorisierte Pakete, die an einem gesperrten Anschluss ankommen, werden auf eine der folgenden Arten behandelt:

- Weiterleiten
- Verwerfen ohne Trap
- Verwerfen mit Trap
- Bewirken, dass der Anschluss geschlossen wird

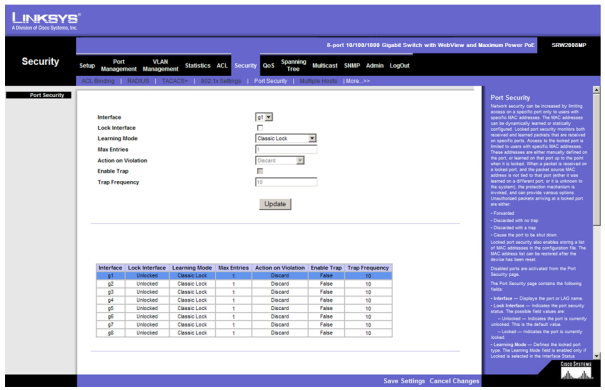


Abbildung 5-33: Security (Sicherheit) – Port Security (Anschlusssicherheit)

Die Sicherheitsfunktion zum Sperren von Anschlüssen ermöglicht auch das Speichern einer Liste von MAC-Adressen in der Konfigurationsdatei. Die Liste mit den MAC-Adressen kann wiederhergestellt werden, nachdem das Gerät zurückgesetzt wurde.

Sie können deaktivierte Anschlüsse auf der Seite Port Security aktivieren.

Interface. Zeigt den Namen des Anschlusses oder der LAG an.

Lock Interface. Wenn Sie diese Option aktivieren, wird die angegebene Schnittstelle gesperrt.

Learning Mode. Definiert den Typ des gesperrten Anschlusses. Das Feld Learning Mode ist nur aktiviert, wenn im Feld Interface Status die Option Locked gewählt ist. Folgende Feldwerte sind möglich:

- **Classic Lock.** Sperrt den Anschluss mithilfe des klassischen Sperrmechanismus. Der Anschluss wird sofort gesperrt, und zwar unabhängig von der Anzahl an Adressen, die bereits gelernt wurden.
- **Limited Dynamic Lock.** Sperrt den Anschluss, indem die aktuellen dynamischen MAC-Adressen, die dem Anschluss zugeordnet sind, gelöscht werden. Der Anschluss führt das Lernen bis zur maximalen Anzahl von Adressen durch, die für den Anschluss zulässig sind. Sowohl das Neulernen als auch das Altern von MAC-Adressen ist aktiviert.

Um den Learning Mode zu ändern, müssen Sie die Option Lock Interface auf Unlocked setzen. Nachdem Sie den Modus geändert haben, können Sie für Lock Interface wieder eine andere Einstellung wählen.

Max Entries. Gibt die Anzahl an MAC-Adressen an, die auf dem Anschluss gelernt werden können. Das Feld Max Entries ist nur aktiviert, wenn im Feld Interface Status die Option Locked aktiviert ist. Zusätzlich wird der Modus Limited Dynamic Lock aktiviert. Standardmäßig ist *1* eingestellt.

Action on Violation. Zeigt die Aktion an, die auf Pakete angewendet wird, die an einem gesperrten Anschluss ankommen. Folgende Feldwerte sind möglich:

- **Discard.** Verwirft Pakete aus nicht gelernten Quellen. Dies ist die Standardeinstellung.
- **Forward Normal.** Leitet Pakete von einer unbekannten Quelle weiter, ohne die MAC-Adresse zu lernen.
- **Discard Disable.** Verwirft Pakete von allen nicht gelernten Quellen und schließt den Anschluss. Der Anschluss bleibt geschlossen, bis er wieder aktiviert oder bis das Gerät zurückgesetzt wird.

Enable Trap. Aktiviert Traps, wenn ein Paket an einem gesperrten Anschluss empfangen wird.

Trap Frequency. Der Zeitraum zwischen Traps (in Sekunden). Der Standardwert beträgt 10 Sekunden.

Registerkarte „Security“ – Multiple Hosts

Auf dem Bildschirm **Multiple Hosts** können Netzwerkverwalter erweiterte anschlussbasierte Authentifizierungseinstellungen für bestimmte Anschlüsse und VLANs konfigurieren.

Port. Zeigt die Nummer des Anschlusses an, für den die erweiterte anschlussbasierte Authentifizierung aktiviert ist.

Enable Multiple Hosts. Wenn diese Option aktiviert ist, zeigt dies an, dass mehrere Hosts aktiviert sind. Mehrere Hosts müssen aktiviert werden, um entweder den Eingangsfilter zu deaktivieren oder um für den ausgewählten Anschluss die Sicherheitsfunktion zum Sperren von Anschlüssen zu verwenden.

Action on Violation. Definiert die anzuwendende Aktion für Pakete, die im Einzelhostmodus von einem Host eingehen, bei dessen MAC-Adresse es sich nicht um die MAC-Adresse des anfordernden Computers handelt. Folgende Feldwerte sind möglich:

- **Discard.** Verwirft die Pakete. Dies ist die Standardeinstellung.
- **Forward.** Leitet das Paket weiter.
- **Discard Disable.** Verwirft die Pakete und schließt den Anschluss. Der Anschluss bleibt geschlossen, bis er wieder aktiviert oder bis das Gerät zurückgesetzt wird.

Enable Traps. Wenn diese Option aktiviert ist, zeigt dies an, dass Traps für mehrere Hosts aktiviert sind.

Trap Frequency. Definiert den Zeitraum, nach dem Traps jeweils an den Host gesendet werden. Sie können das Feld **Trap Frequency** (1 bis 1.000.000) nur definieren, wenn die Funktion zur Verwendung mehrerer Hosts deaktiviert ist. Standardmäßig ist 10 Sekunden eingestellt.

Status. Zeigt den Status des Hosts an. Wenn ein Sternchen (*) angezeigt wird, ist der Anschluss entweder nicht verknüpft oder nicht aktiv. Folgende Feldwerte sind möglich:

Number of Violations. Zeigt die Anzahl der Pakete an, die an der Schnittstelle im Einzelhostmodus von einem Host eingegangen sind, bei dessen MAC-Adresse es sich nicht um die MAC-Adresse des anfordernden Computers handelt.

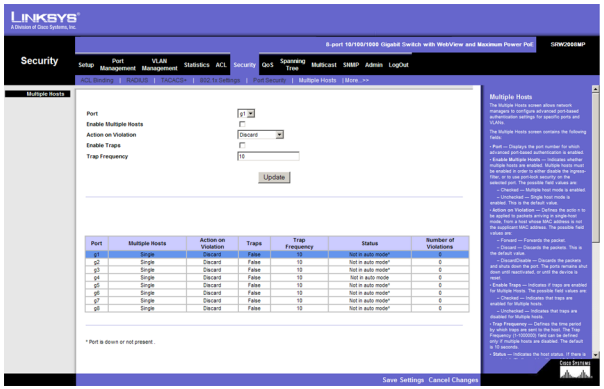


Abbildung 5-34: Security (Sicherheit) – Multiple Hosts (Mehrere Hosts)

Registerkarte „Security“ – Storm Control

Port. Zeigt die Nummer des Anschlusses an, für den die Storm Control aktiviert ist.

Broadcast Control. Zeigt an, ob Broadcastpakettypen auf der jeweiligen Schnittstelle weitergeleitet werden.

Mode. Gibt den Broadcastmodus an, der für das Gerät momentan aktiviert ist. Folgende Feldwerte sind möglich:

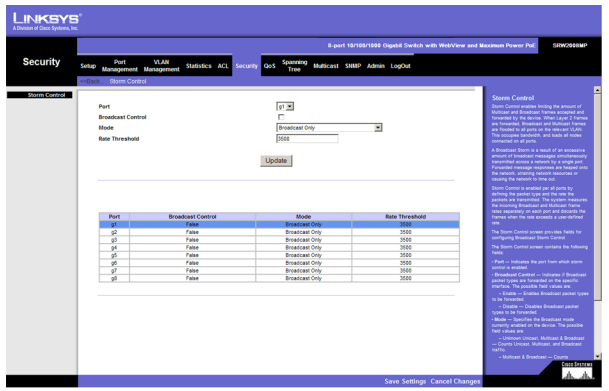


Abbildung 5-35: Security (Sicherheit) – Storm Control

- **Unknown Unicast, Multicast & Broadcast**. Zählt den Unicast-, Multicast- und Broadcastdatenverkehr.
- **Multicast & Broadcast**. Zählt den Broadcast- und Multicastdatenverkehr zusammen.
- **Broadcast Only**. Zählt nur den Broadcastdatenverkehr.

Rate Threshold. Die maximale Geschwindigkeit (Pakete pro Sekunde), mit der unbekannte Pakete weitergeleitet werden. Der Standardwert beträgt 3500, und der Wertebereich ist 70 bis 100.000.

QoS

Netzwerkverkehr lässt sich in der Regel nicht vorhersagen, und die einzig mögliche Basissicherheit ist die bestmögliche Datenverkehrsbereitstellung. Um diese Herausforderung zu meistern, wird im gesamten Netzwerk die so genannte Quality of Service (QoS) angewendet. Auf diese Weise wird sichergestellt, dass der Netzwerkverkehr anhand bestimmter Kriterien mit Prioritäten versehen wird und dass einige Arten von Datenverkehr bevorzugt behandelt werden. Die Verwendung von QoS für ein Netzwerk optimiert die Netzwerkleistung und umfasst zwei grundlegende Vorgehensweisen:

Das Klassifizieren von eingehendem Verkehr in Behandlungsklassen. Dies erfolgt anhand von Attributen, z. B.:

- Eingangsschnittstelle
- Paketinhalt
- Kombination dieser Attribute

Das Bereitstellen verschiedener Mechanismen zum Bestimmen der Zuordnung von Netzwerkressourcen zu verschiedenen Behandlungsklassen, z. B.:

- Zuweisung von Netzwerkverkehr zu einer bestimmten Hardwarewarteschlange
- Zuweisung von internen Ressourcen
- Verkehrsformung (Traffic Shaping)

Die Begriffe Class of Service (CoS) und QoS werden im folgenden Kontext verwendet:

CoS stellt verschiedene Layer 2-Datenverkehrdienste bereit. CoS bezieht sich auf die Klassifizierung von Verkehr-zu-Verkehr-Klassen, die als aggregierte Einheit ohne individuelle Einstellungen pro Fluss behandelt werden. Normalerweise steht CoS in Beziehung zum 802.1p-Dienst, der Flüsse gemäß deren Layer 2-Priorität klassifiziert, wie im VLAN-Header festgelegt.

QoS bezieht sich auf Layer 2-Verkehr und höher. QoS behandelt Einstellungen pro Fluss, auch innerhalb einer einzelnen Datenverkehrsklasse.

Registerkarte „QoS“ – CoS Settings

Der Bildschirm **CoS Settings** enthält Felder zum Aktivieren bzw. Deaktivieren der Dienstklasse (CoS). Außerdem können Sie den Modus **Trust** auswählen. Der Modus **Trust** verwendet vordefinierte Felder im Paket, um die Einstellungen der Ausgangswarteschlange zu bestimmen.

Der Bildschirm **CoS Settings** ist in zwei Bereiche unterteilt: **CoS Settings** und **CoS to Queue**.

CoS Mode. Zeigt an, ob die Dienstgüte für die Schnittstelle aktiviert ist. Folgende Werte sind möglich:

- **Disable.** Deaktiviert die Dienstgüte für die Schnittstelle.
- **Basic.** Aktiviert die Dienstgüte für die Schnittstelle.
- **Advanced.** Aktiviert den erweiterten Modus der Dienstgüte für die Schnittstelle.

Class of Service. Gibt die Tag-Werte für die Dienstklassenpriorität an, wobei 0 der niedrigste und 7 der höchste Wert ist.

Queue. Definiert die Warteschlange zur Datenverkehrsweiterleitung, der die Dienstklassenpriorität zugeordnet ist. Es werden vier Warteschlangen für Datenverkehrsprioritäten unterstützt.

Mit der Schaltfläche **Restore Defaults** können Sie die Werkseinstellung des Geräts für die Zuordnung der Dienstklassenwerte zu einer Weiterleitungswarteschlange wiederherstellen.

CoS Default

Interface. Schnittstelle, für die die Dienstklassenkonfiguration gilt.

Default CoS. Bestimmt den Standardwert der Dienstklasse für eingehende Pakete, für die kein VLAN-Tag definiert ist. Die möglichen Feldwerte lauten 0 bis 7. Die Standarddienstklasse ist 0.

Restore Defaults. Stellt die Werkseinstellung des Geräts für die Zuordnung der Dienstklassenwerte zu einer Weiterleitungswarteschlange wieder her.

LAG. LAG, für die die Dienstklassenkonfiguration gilt.

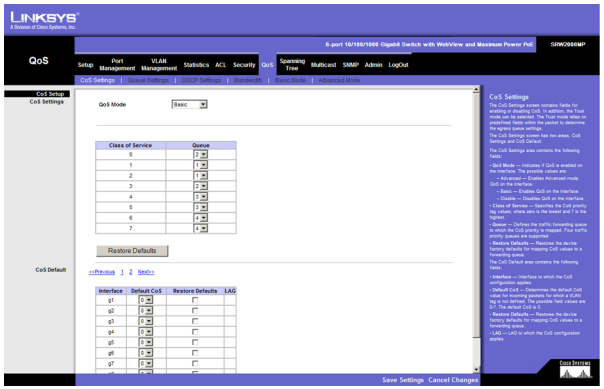


Abbildung 5-36: QoS (Dienstgüte) – CoS Settings (Einstellungen der Dienstklasse)

Registerkarte „QoS“ – Queue Settings

Der Bildschirm **Queue Settings** enthält Felder, mit denen Sie die Weiterleitungstypen der Dienstgütenwarteschlange definieren können.

Strict Priority. Zeigt an, dass die Verkehrsplanung für die ausgewählte Warteschlange strikt auf der Warteschlangenpriorität basiert.

WRR. Zeigt an, dass die Verkehrsplanung für die ausgewählte Warteschlange strikt auf WRR basiert.

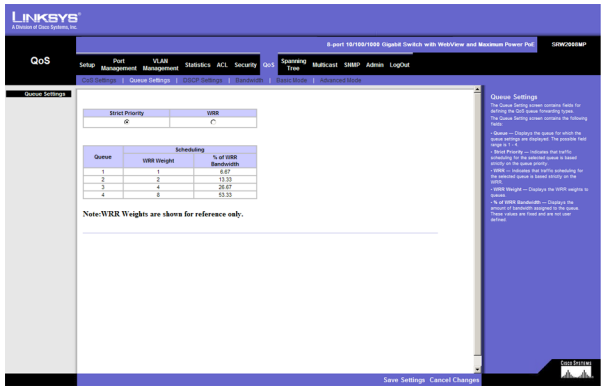


Abbildung 5-37: QoS (Dienstgüte) – Queue Settings (Warteschlangeneinstellungen)

Queue. Gibt die Warteschlange an, für die die Warteschlangeneinstellungen angezeigt werden. Der zulässige Feldbereich beträgt 1 bis 4.

WRR Weight. Zeigt die WRR-Gewichtungen für Warteschlangen an.

% of WRR Bandwidth. Zeigt die Menge an Bandbreite an, die der Warteschlange zugewiesen ist. Diese Werte stehen fest und sind nicht vom Benutzer definiert.

Registerkarte „QoS“ – DSCP Settings

Auf dem Bildschirm **DSCP Settings** können Sie DSCP-Werte bestimmten Warteschlangen zuordnen.

Der Bildschirm **DSCP Settings** enthält die folgenden Felder:

DSCP. Zeigt den DSCP-Wert (Differentiated Services Code Point) im eingehenden Paket an.

Queue. Ordnet den DSCP-Wert der ausgewählten Warteschlange zu.

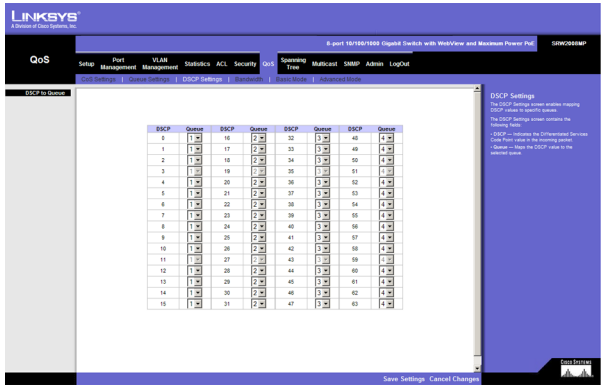


Abbildung 5-38: QoS (Dienstgüte) – DSCP Settings (DSCP-Einstellungen)

Registerkarte „QoS“ – Bandwidth

Auf dem Bildschirm **Bandwidth** können Netzwerkverwalter die Bandbreiteneinstellungen für eine angegebene Ausgangsschnittstelle definieren. Das Ändern der Warteschlangenplanung wirkt sich global auf die Warteschlangeneinstellungen aus. Der Bildschirm **Bandwidth** wird nicht mit dem Modus **Service** verwendet, da Bandbreiteneinstellungen auf Diensten basieren.

Die Warteschlangenbearbeitung kann pro Warteschlange und/oder pro Schnittstelle erfolgen. Die Bearbeitung (Shaping) wird mithilfe des niedrigeren angegebenen Werts bestimmt. Sie wählen den Typ der Warteschlangenbearbeitung auf dem Bildschirm **Bandwidth** aus.

Interface. Gibt die Schnittstelle an, für die die Informationen zur Warteschlangenbearbeitung angezeigt werden. Folgende Feldwerte sind möglich:

- **Port.** Gibt den Anschluss an, für den die Bandbreiteneinstellungen angezeigt werden.
- **LAG.** Gibt die LAG an, für die die Bandbreiteneinstellungen angezeigt werden.

Ingress Rate Limit Status. Zeigt an, ob für die Schnittstelle die Ratenbeschränkung definiert ist.

Rate Limit (62-1000000 Kbps). Definiert die Menge an Bandbreite, die der Schnittstelle zugewiesen ist. Zulässige Feldwerte sind 62 bis 1.000.000 KBit/s.

Egress Shaping Rate on Selected Port. Zeigt an, ob für die Schnittstelle die Ratenbeschränkung aktiviert ist.

Committed Information Rate (CIR). Definiert CIR als Typ für die Warteschlangenbearbeitung. Zulässige Feldwerte sind 64 bis 1.000.000 KBit/s.

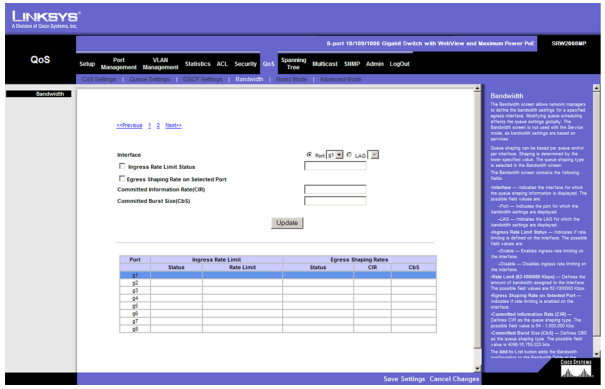


Abbildung 5-39: QoS (Dienstgüte) – Bandwidth (Bandbreite)

Committed Burst Size (CBS). Definiert CBS als Typ für die Warteschlangenbearbeitung. Zulässige Feldwerte sind 4.096 bis 16.769.020 Bit.

Mit der Schaltfläche **Add to List** fügen Sie die Bandbreitenkonfiguration der **Bandwidth Table** unten auf dem Bildschirm hinzu.

Registerkarte „QoS“ – Basic Mode

Der Bildschirm **Basic Mode** enthält die folgenden Felder:

Trust Mode. Zeigt den Modus **Trust** an. Wenn das CoS-Tag und das DSCP-Tag eines Pakets verschiedenen Warteschlangen zugeordnet sind, bestimmt der Modus **Trust** die Warteschlange, der das Paket zugewiesen wird. Folgende Werte sind möglich:

- **CoS.** Setzt den Modus **Trust** für das Gerät auf **CoS**. Die CoS-Zuordnung bestimmt die Paketwarteschlange.
- **DSCP.** Setzt den Modus **Trust** für das Gerät auf **DSCP**. Die DSCP-Zuordnung bestimmt die Paketwarteschlange.

Abbildung 5-40: QoS (Dienstgüte) – Basic Mode (Grundmodus)

Registerkarte „QoS“ – Advanced Mode

Der erweiterte Dienstgütemodus (Advanced QoS) bietet Regeln zum Angeben der Flussklassifizierung und zum Zuweisen von Regelaktionen, die sich auf die Bandbreitenverwaltung beziehen. Die Regeln basieren auf den Zugriffssteuerungslisten (siehe Registerkarte **Access Control**).

MAC-Zugriffssteuerungslisten und IP-Zugriffssteuerungslisten können in komplexeren Strukturen gruppiert werden, die als Richtlinien bezeichnet werden. Richtlinien können auf eine Schnittstelle angewendet werden. Zugriffssteuerungslisten in Richtlinien werden in der Reihenfolge angewendet, in der sie in der Richtlinie enthalten sind. Sie können eine Richtlinie nur einem Anschluss zuordnen.

Im erweiterten Dienstgütemodus können Sie Zugriffssteuerungslisten direkt auf eine Schnittstelle anwenden, indem Sie die Option **Security – ACL Binding** verwenden. Sie können eine Richtlinie und eine Zugriffssteuerungsliste jedoch nicht gleichzeitig auf eine Schnittstelle anwenden.

Nachdem Sie einer bestimmten Warteschlange Pakete zugewiesen haben, können Sie z. B. die folgenden Dienste anwenden: Konfigurieren von Ausgabewarteschlangen für das Planungsschema oder Konfigurieren der Ausgabebearbeitung für Burst Size, CIR oder CBS pro Schnittstelle oder pro Warteschlange.

Out of Profile DSCP Assignments. Mit dieser Schaltfläche öffnen Sie den Bildschirm **Out of Profile DSCP**.

Abbildung 5-41: QoS (Dienstgüte) – Advanced Mode (Erweiterter Modus)

Bildschirm **Out of Profile DSCP**

DSCP In. Zeigt den Wert für **DSCP In** an.

DSCP Out. Zeigt den aktuellen Wert für **DSCP Out** an. Sie können im Dropdownmenü einen neuen Wert auswählen.

Mit der Schaltfläche **Policy Settings** öffnen Sie den Bildschirm **Policy Name**.

Bildschirm **Policy Name**

Policy Name. Definiert einen neuen Richtliniennamen.

Add to List. Mit der Schaltfläche **Add to List** fügen Sie die Richtlinie der Tabelle mit den Richtliniennamen hinzu.

Select Policy. Hier können Sie eine vorhandene Richtlinie anhand ihres Namens auswählen. Die Richtlinie kann Folgendes umfassen:

- Class Map (Klassenzuordnung)
- Action (Aktion)
- Policer (Überwacher)

New Policy Name. Definiert einen neuen Richtliniennamen.

Class Map. Hier können Sie eine vorhandene Klassenzuordnung anhand ihres Namens auswählen.

New Class Map. Mit der Schaltfläche **New Class Map** öffnen Sie den Bildschirm **New Class Map**.

Bildschirm **New Class Map**

Class Map Name. Definiert einen neuen Namen für eine Klassenzuordnung.

Preferred ACL. Zeigt an, ob Pakete zuerst anhand einer IP-basierten Zugriffssteuerungsliste oder einer MAC-basierten Zugriffssteuerungsliste abgestimmt werden. Folgende Feldwerte sind möglich:

- **IP Based ACLs.** Ordnet Pakete zuerst IP-basierten Zugriffssteuerungslisten und dann MAC-basierten Zugriffssteuerungslisten zu.
- **MAC Based ACLs.** Ordnet Pakete zuerst MAC-basierten Zugriffssteuerungslisten und dann IP-basierten Zugriffssteuerungslisten zu.

IP ACL. Ordnet Pakete zuerst IP-basierten Zugriffssteuerungslisten und dann MAC-basierten Zugriffssteuerungslisten zu.

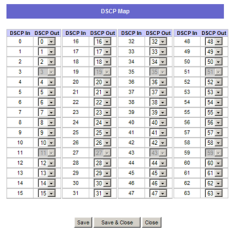


Abbildung 5-42: Advanced Mode (Erweiterter Modus) – Out of Profile DSCP (Profilunabhängiger DSCP)

Abbildung 5-43: Advanced Mode (Erweiterter Modus) – Policy Name (Richtlinienname)

Abbildung 5-44: Advanced Mode (Erweiterter Modus) – New Class Map (Neue Klassenzuordnung)

Match. Kriterien, die zum Zuordnen von IP-Adressen und/oder MAC-Adressen zur Adresse einer Zugriffssteuerungsliste verwendet werden. Folgende Feldwerte sind möglich:

- **And.** Sowohl die MAC-basierte als auch die IP-basierte Zugriffssteuerungsliste muss mit einem Paket übereinstimmen.
- **Or.** Entweder die MAC-basierte oder die IP-basierte Zugriffssteuerungsliste muss mit einem Paket übereinstimmen.

MAC ACL. Ordnet Pakete zuerst MAC-basierten Zugriffssteuerungslisten und dann IP-basierten Zugriffssteuerungslisten zu.

Police. Aktiviert Überwachungsfunktionen.

Type. Der Überwachungstyp für die Klasse. Folgende Werte sind möglich:

Aggregate Policer. Konfiguriert die Klasse für die Verwendung eines konfigurierten aggregierten Überwachers, den Sie aus dem Dropdownmenü auswählen. Ein aggregierter Überwacher wird definiert, wenn der Überwacher von mehreren Klassen gemeinsam genutzt wird. Datenverkehr von zwei verschiedenen Anschlüssen kann zu Überwachungszwecken konfiguriert werden. Ein aggregierter Überwacher kann in einer Richtlinienzuordnung auf mehrere Klassen angewendet werden, aber er kann nicht über verschiedene Richtlinienzuordnungen hinweg verwendet werden.

Single. Konfiguriert die Klasse für die Verwendung von manuell konfigurierten Informationsraten und Überschreitungsaktionen.

Aggregate Policer. Benutzerdefinierte aggregierte Überwacher.

Aggregate Policer Settings. Mit der Schaltfläche **Aggregate Policer** öffnen Sie den Bildschirm **New Aggregate Policer**.

Bildschirm **New Aggregate Policer**

Aggregate Policer Name. Geben Sie in dieses Feld einen Namen ein.

Ingress Committed Information Rate (CIR). Definiert CIR in Bit pro Sekunde. Dieses Feld ist nur relevant, wenn der Wert **Police** auf **Single** gesetzt ist.

Ingress Committed Burst Size (CBS). Definiert CBS in Byte pro Sekunde. Dieses Feld ist nur relevant, wenn der Wert **Police** auf **Single** gesetzt ist.

Exceed Action. Aktion, die eingehenden Paketen zugewiesen wird, die die CIR überschreiten. Dieses Feld ist nur relevant, wenn der Wert **Police** auf **Single** gesetzt ist. Folgende Werte sind möglich:

- **Drop.** Verwirft Pakete, die den definierten CIR-Wert überschreiten.
- **Remark DSCP.** Kommentiert die DSCP-Werte von Paketen, die den definierten CIR-Wert überschreiten.
- **None.** Leitet Pakete weiter, die den definierten CIR-Wert überschreiten.

Abbildung 5-45: Advanced Mode (Erweiterter Modus) – New Aggregate Policer (Neuer aggregierter Überwacher)

Spanning Tree

Das Spanning Tree Protocol (STP) verfügt über eine Strukturtopografie für eine beliebige Anordnung von Bridges. STP stellt außerdem einen Pfad zwischen Endstationen in einem Netzwerk her und entfernt dadurch Schleifen.

Schleifen entstehen, wenn zwischen Hosts wechselnde Routen vorhanden sind. In einem erweiterten Netzwerk können Schleifen dazu führen, dass Bridges Datenverkehr unendlich lange weiterleiten, so dass die Menge des Datenverkehrs erhöht und die Effizienz des Netzwerks reduziert wird.

Das Gerät unterstützt die folgenden Spanning Tree-Versionen:

- **Classic STP.** Stellt einen einzelnen Pfad zwischen Endstationen bereit und vermeidet und beseitigt auf diese Weise Schleifen.
- **Rapid STP.** Erkennt und verwendet Netzwerktopologien, die eine schnellere Spanning Tree-Konvergenz ermöglichen, ohne dass Weiterleitungsschleifen erstellt werden müssen.
- **Multiple STP.** Bietet umfassende Konnektivität für Pakete, die einem beliebigen VLAN zugeordnet sind. **Multiple STP** basiert auf dem RSTP. Außerdem werden bei dieser Option Pakete übertragen, die über verschiedene MST-Regionen unterschiedlichen VLANs zugewiesen sind. MST-Regionen fungieren als Einzel-Bridge.

Registerkarte „Spanning Tree“ – STP Status

Auf dem Bildschirm **STP Status** wird der STP-Status des Geräts beschrieben.

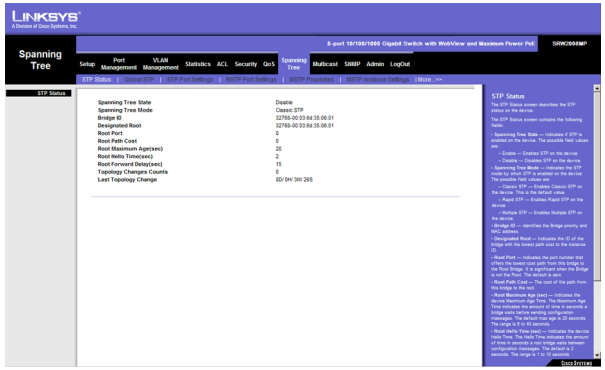


Abbildung 5-46: Spanning Tree – STP Status (STP-Status)

Spanning Tree State. Zeigt an, ob STP für das Gerät aktiviert ist.

Spanning Tree Mode. Zeigt den STP-Modus an, über den STP auf dem Gerät aktiviert ist.

Bridge ID. Gibt die Bridge-Priorität und die MAC-Adresse an.

Designated Root. Zeigt für die Instanz-ID die ID der Bridge mit den niedrigsten Pfadkosten an.

Root Port. Zeigt die Nummer des Anschlusses an, der den kostengünstigsten Pfad von dieser Bridge zur Root Bridge bietet. Dies ist wichtig, wenn es sich bei der Bridge nicht um das Root-Element handelt. Der Standardwert lautet 0.

Root Path Cost. Die Kosten des Pfads von dieser Bridge zum Root-Element.

Root Maximum Age (sec). Zeigt die **Maximum Age Time** des Geräts an. Die **Maximum Age Time** zeigt den Zeitraum in Sekunden an, wie lange eine Bridge wartet, bevor sie Konfigurationsmeldungen sendet.
Der Standardwert ist 20 Sekunden. Der Bereich beträgt 6 bis 40 Sekunden.

Root Hello Time (sec). Zeigt die **Hello Time** des Geräts an. Die **Hello Time** zeigt den Zeitraum in Sekunden an, wie lange eine Root Bridge zwischen Konfigurationsmeldungen abwartet. Standardmäßig ist 2 Sekunden eingestellt. Der Bereich beträgt 1 bis 10 Sekunden.

Root Forward delay (sec). Zeigt die Weiterleitungsverzögerung des Geräts an. Als **Forward Delay Time** wird der Zeitraum in Sekunden angezeigt, wie lange eine Bridge vor dem Weiterleiten von Paketen im Hör- und Lernzustand verbleibt. Standardmäßig ist 15 Sekunden eingestellt. Der Bereich beträgt 4 bis 30 Sekunden.

Topology Changes Counts. Zeigt die Gesamtmenge an STP-Statusänderungen an, die eingetreten sind.

Last Topology Change. Zeigt den Zeitraum an, der verstrichen ist, seitdem die Bridge initialisiert oder zurückgesetzt und die letzte topografische Änderung vorgenommen wurde. Der Zeitraum wird im Format „Tag Stunde Minute Sekunde“ angezeigt, z. B. „2 Tage 5 Stunden 10 Minuten und 4 Sekunden“.

Registerkarte „Spanning Tree“ – Global STP

Der Bildschirm **Global STP** enthält Parameter zum Aktivieren von STP auf dem Gerät.

Global Setting

Spanning Tree State. Zeigt an, ob STP für das Gerät aktiviert ist.

STP Operation Mode. Zeigt den STP-Modus an, über den STP auf dem Gerät aktiviert ist. Folgende Feldwerte sind möglich:

- **Classic STP.** Aktiviert **Classic STP** auf dem Gerät. Dies ist die Standardeinstellung.
- **Rapid STP.** Aktiviert **Rapid STP** auf dem Gerät.
- **Multiple STP.** Aktiviert **Multiple STP** auf dem Gerät.

BPDU Handling. Bestimmt, wie BPDU-Pakete verwaltet werden, wenn STP für den Anschluss bzw. das Gerät deaktiviert ist. BPDUs werden verwendet, um Spanning Tree-Informationen zu übertragen. Folgende Feldwerte sind möglich:

- **Filtering.** Filtert BPDU-Pakete, wenn Spanning Tree für eine Schnittstelle deaktiviert ist. Dies ist die Standardeinstellung.
- **Flooding.** Führt für BPDU-Pakete eine Überflutung durch, wenn Spanning Tree für eine Schnittstelle deaktiviert ist.

Path Cost Default Values. Gibt die Methode an, die zum Zuweisen von Standardpfadkosten zu STP-Anschlüssen verwendet wird. Folgende Feldwerte sind möglich:

- **Short.** Gibt für Anschlusspfadkosten den Bereich 1 bis 65.535 an. Dies ist die Standardeinstellung.

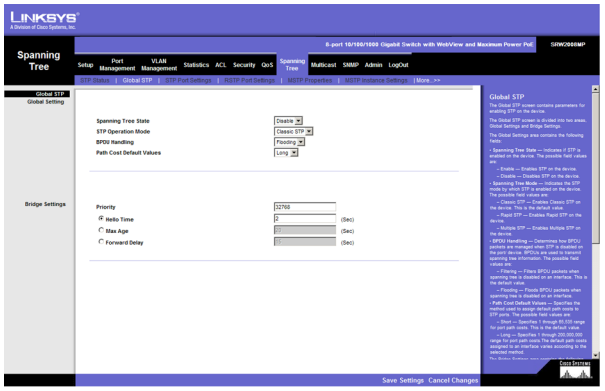


Abbildung 5-47: Spanning Tree – Global STP (Globales STP)

- **Long.** Gibt für Anschlusspfadkosten den Bereich 1 bis 200.000.000 an. Die Standardpfadkosten, die einer Schnittstelle zugewiesen sind, variieren je nach gewählter Methode.

Bridge Settings

Priority. Gibt den Wert der Bridge-Priorität an. Wenn Switches oder Bridges das STP ausführen, wird jeweils eine Priorität zugewiesen. Nach dem Austauschen von BPDUs wird das Gerät mit dem niedrigsten Prioritätswert zur Root Bridge. Der Standardwert ist 32.768. Der Wert für die Anschlusspriorität wird in Schritten von 4.096 vergeben, z. B. 4.096, 8.192, 12.288 usw. Der zulässige Bereich lautet 0 bis 65.535.

Hello Time. Gibt die **Hello Time** des Geräts an. Die **Hello Time** zeigt den Zeitraum in Sekunden an, wie lange eine Root Bridge zwischen Konfigurationsmeldungen abwartet. Standardmäßig ist 2 Sekunden eingestellt. Der Bereich beträgt 1 bis 10 Sekunden.

Max Age. Gibt die **Maximum Age Time** des Geräts an. Die **Maximum Age Time** zeigt den Zeitraum in Sekunden an, wie lange eine Bridge wartet, bevor sie Konfigurationsmeldungen sendet. Der Standardwert ist 20 Sekunden. Der Bereich beträgt 6 bis 40 Sekunden.

Forward Delay. Gibt die Weiterleitungsverzögerung des Geräts an. Als **Forward Delay Time** wird der Zeitraum in Sekunden angezeigt, wie lange eine Bridge vor dem Weiterleiten von Paketen im Hör- und Lernzustand verbleibt. Standardmäßig ist 15 Sekunden eingestellt. Der Bereich beträgt 4 bis 30 Sekunden.

Registerkarte „Spanning Tree“ – STP Port Settings

Netzwerkadministratoren können den Bildschirm **STP Interface Settings** verwenden, um bestimmten Schnittstellen STP-Einstellungen zuzuweisen.

Die Seite **STP Interface Settings** enthält die folgenden Felder:

Interface. Zeigt den Anschluss oder die LAG an, für den bzw. die STP aktiviert ist.

STP. Zeigt an, ob STP für den Anschluss aktiviert ist.

Port Fast. Zeigt an, ob die schnelle Verbindung (Fast Link) für den Anschluss aktiviert ist. Wenn für einen Anschluss der Modus **Fast Link** aktiviert ist, wird die Option **Port State** automatisch in den Status **Forwarding** versetzt, wenn die Anschlussverbindung aktiv ist. Mithilfe von **Fast Link** wird die Konvergenz des STP-Protokolls optimiert. Die STP-Konvergenz kann in großen Netzwerken 30 bis 60 Sekunden in Anspruch nehmen.

Port State. Zeigt den aktuellen STP-Status eines Anschlusses an. Wenn die Option aktiviert ist, bestimmt der Anschlussstatus, welche Weiterleitungsaktion für Datenverkehr ausgeführt wird. Folgende Anschlussstatuseinstellungen sind möglich:

- **Disabled.** Zeigt an, dass STP für den Anschluss momentan deaktiviert ist. Der Anschluss leitet Datenverkehr weiter, während er MAC-Adressen „lernt“.

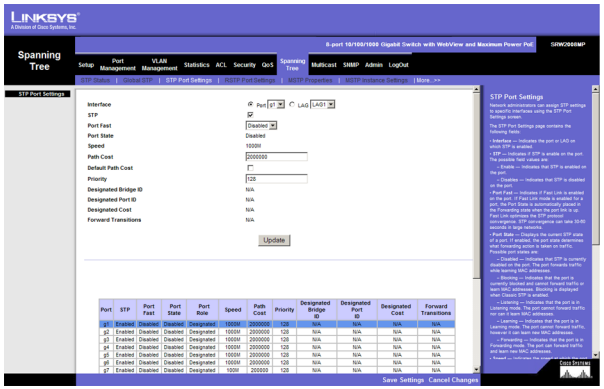


Abbildung 5-48: Spanning Tree – STP Port Settings (STP-Anschlusseinstellungen)

- **Blocking.** Zeigt an, dass der Anschluss momentan blockiert ist und keinen Datenverkehr weiterleiten bzw. keine MAC-Adressen lernen kann. **Blocking** wird angezeigt, wenn **Classic STP** aktiviert ist.
- **Listening.** Zeigt an, dass der Anschluss sich im Modus **Listening** befindet. Der Anschluss kann weder Datenverkehr weiterleiten noch MAC-Adressen lernen.
- **Learning.** Zeigt an, dass der Anschluss sich im Modus **Learning** befindet. Der Anschluss kann keinen Datenverkehr weiterleiten, jedoch neue MAC-Adressen lernen.
- **Forwarding.** Zeigt an, dass der Anschluss sich im Modus **Forwarding** befindet. Der Anschluss kann Datenverkehr weiterleiten und neue MAC-Adressen lernen.

Speed. Zeigt die Geschwindigkeit an, mit der der Anschluss betrieben wird.

Path Cost. Zeigt den Beitrag des Anschlusses zu den Stammpfadkosten (Root Path Cost) an. Die Pfadkosten werden auf einen höheren oder niedrigeren Wert gesetzt und zum Weiterleiten von Datenverkehr verwendet, wenn die Route eines Pfads geändert wird.

Default Path Cost. Wenn diese Option aktiviert ist, werden die Standardpfadkosten implementiert.

Priority. Der Prioritätswert des Anschlusses. Der Prioritätswert beeinflusst die Anschlussauswahl, wenn eine Bridge über zwei Anschlüsse verfügt, die per Schleife verbunden sind. Der Prioritätswert kann zwischen 0 und 240 liegen und wird in 16er-Schritten angegeben.

Designated Bridge ID. Zeigt die Bridge-Priorität und die MAC-Adresse der jeweiligen Bridge an.

Designated Port ID. Zeigt die Priorität und Schnittstelle für den ausgewählten Anschluss an.

Designated Cost. Zeigt die Kosten des Anschlusses an, der der STP-Topologie angehört. Anschlüsse mit niedrigeren Kosten werden weniger häufig gesperrt, wenn STP Schleifen erkennt.

Forward Transitions. Zeigt an, wie häufig der Anschluss aus dem Status **Blocking** in den Status **Forwarding** übergegangen ist.

Registerkarte „Spanning Tree“ – RSTP Port Settings

Der klassische Spanning Tree verhindert in einer allgemeinen Netzwerktopologie Layer 2-Weiterleistungsschleifen, aber die Konvergenz kann zwischen 30 und 60 Sekunden in Anspruch nehmen. Dieser Zeitraum kann dazu führen, dass die Erkennung möglicher Schleifen und die Verbreitung von Topologiestatusänderungen verzögert wird. Das Rapid Spanning Tree Protocol (RSTP) erkennt und verwendet Netzwerktopologien, die eine schnellere STP-Konvergenz ohne die Entstehung von Weiterleitungsschleifen ermöglichen.

Interface. Zeigt den Anschluss oder die LAG an, für den bzw. die **Rapid STP** aktiviert ist.

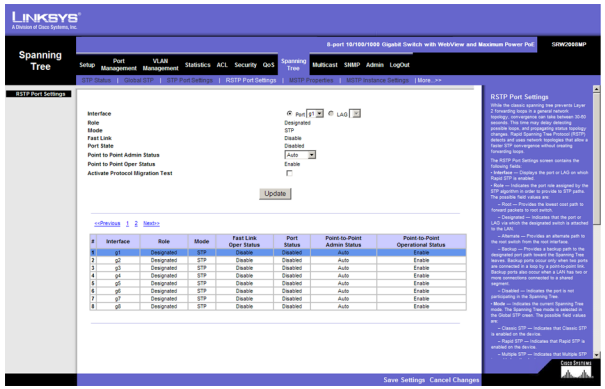


Abbildung 5-49: Spanning Tree – RSTP Port Settings (RSTP-Anschlusseinstellungen)

Role. Zeigt die Anschlussfunktion an, die vom STP-Algorithmus zugewiesen wird, um STP-Pfade bereitzustellen. Folgende Feldwerte sind möglich:

- **Root.** Stellt den Pfad mit den niedrigsten Kosten zum Weiterleiten von Paketen an den Root Switch bereit.
- **Designated.** Zeigt den Anschluss bzw. die LAG an, über den bzw. die der jeweilige Switch an das LAN angeschlossen ist.
- **Alternate.** Stellt für den Root Switch einen alternativen Pfad von der Root-Schnittstelle bereit.
- **Backup.** Stellt auf dem Weg zu den Spanning Tree-Verästelungen für den jeweiligen Anschlusspfad einen Sicherungspfad bereit. Sicherungsanschlüsse werden nur verwendet, wenn zwei Anschlüsse in einer Schleife mithilfe einer Punkt-zu-Punkt-Verbindung verbunden sind. Sie werden außerdem verwendet, wenn in einem LAN zwei oder mehr Verbindungen zu einem gemeinsam genutzten Segment verbunden sind.
- **Disabled.** Zeigt an, dass der Anschluss nicht Teil des Spanning Tree ist.

Mode. Zeigt den aktuellen Modus des Spanning Tree an. Sie können den Modus des Spanning Tree auf dem Bildschirm **Global STP** auswählen. Folgende Feldwerte sind möglich:

- **Classic STP.** Zeigt an, dass für das Gerät **Classic STP** aktiviert ist.
- **Rapid STP.** Zeigt an, dass für das Gerät **Rapid STP** aktiviert ist.
- **Multiple STP.** Zeigt an, dass für das Gerät **Multiple STP** aktiviert ist.

Fast Link. Zeigt an, ob für den Anschluss bzw. die LAG die Option **Fast Link** aktiviert ist. Wenn **Fast Link** für einen Anschluss aktiviert ist, wird der Anschluss automatisch in den Weiterleitungsstatus versetzt.

Port State. Zeigt an, ob RSTP für die Schnittstelle aktiviert ist.

Point-to-Point Admin Status. Zeigt an, ob eine Punkt-zu-Punkt-Verbindung eingerichtet ist oder ob es zulässig ist, dass das Gerät eine Punkt-zu-Punkt-Verbindung einrichtet. Folgende Feldwerte sind möglich:

- **Auto.** Das Gerät richtet automatisch Punkt-zu-Punkt-Verbindungen ein.
- **Enabled.** Ermöglicht es dem Gerät, eine Punkt-zu-Punkt-Verbindung einzurichten. Zum Einrichten der Kommunikation über eine Punkt-zu-Punkt-Verbindung sendet die PPP-Ausgangseinheit zuerst LCP-Pakete (Link Control Protocol), um die Datenverbindung zu konfigurieren und zu testen. Nach Einrichten einer Verbindung und Aushandeln optionaler Vorgehensweisen, die für das LCP erforderlich sind, sendet die PPP-Ausgangseinheit NCP-Pakete (Network Control Protocol), um mindestens ein Netzwerk-Layerprotokoll auszuwählen und zu konfigurieren. Nachdem die einzelnen Netzwerk-Layerprotokolle konfiguriert wurden, können Pakete der einzelnen Netzwerk-Layerprotokolle über die Verbindung gesendet werden. Die Verbindung bleibt für die Kommunikation konfiguriert, bis explizite LCP- oder NCP-Pakete die Verbindung schließen oder bis ein externes Ereignis eintritt. Hierbei handelt es sich um den eigentlichen Verbindungstyp des Switchanschlusses. Dieser kann sich vom administrativen Status unterscheiden.

- **Disabled.** Deaktiviert die Punkt-zu-Punkt-Verbindung.

Point-to-Point Oper Status. Zeigt den Punkt-zu-Punkt-Betriebsstatus an.

Um einen Migrationstest durchzuführen, klicken Sie neben dem Feld **Activate Protocol Migration Test** auf **Activate**. Beim Test werden LCP-Pakete (Link Control Protocol) gesendet, um zu prüfen, ob eine Datenverbindung aktiviert ist.

Registerkarte „Spanning Tree“ – MSTP Properties

MSTP ermöglicht verschiedene Lastausgleichverfahren. Wenn für eine STP-Instanz z. B. der Anschluss A gesperrt ist, wird der Anschluss in einer anderen STP-Instanz in den Status **Forwarding** versetzt. Der Bildschirm **MSTP Properties** enthält Informationen zum Definieren von globalen MSTP-Einstellungen, z. B. Regionsnamen, MSTP-Versionen und maximale Anzahl an Sprüngen.

Der Bildschirm **MSTP Properties** enthält die folgenden Felder:

Region Name. Stellt einen benutzerdefinierten STP-Regionsnamen bereit.

Revision. Definiert eine nicht signierte 16-Bit-Nummer, die die Version der aktuellen MST-Konfiguration angibt. Die Versionsnummer wird als Teil der MST-Konfiguration benötigt. Der zulässige Feldbereich beträgt 0 bis 65.535.

Max Hops. Zeigt die Gesamtzahl der Sprünge an, die in einer bestimmten Region auftreten, bevor die BPDU verworfen wird. Nachdem die BPDU verworfen wurde, erfolgt die Alterung der Anschlussinformationen. Der zulässige Feldbereich beträgt 1 bis 40. Der Standardwert für das Feld lautet 20 Sprünge.

IST Master. Zeigt die Spanning Tree-Masterinstanz an. Der IST-Master ist das Root-Element der angegebenen Instanz.

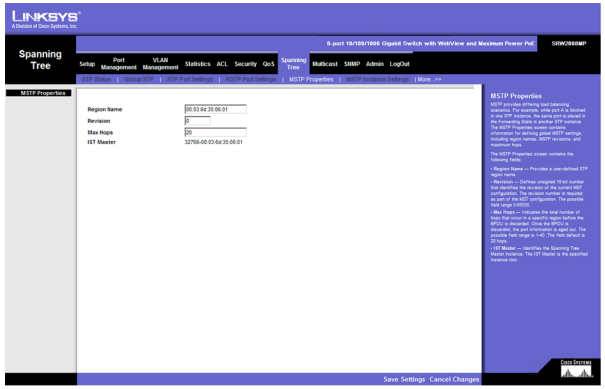


Abbildung 5-50: Spanning Tree – MSTP Properties (MSTP-Eigenschaften)

Registerkarte „Spanning Tree“ – MSTP Instance Settings

Beim MSTP-Betrieb werden VLANs STP-Instanzen zugeordnet. Pakete, die verschiedenen VLANs zugewiesen sind, werden in Multiple Spanning Trees-Regionen (MST Regions) auf verschiedenen Pfaden übertragen. Bei Regionen handelt es sich um eine oder mehrere Multiple Spanning Tree-Bridges, über die Rahmen übertragen werden können. Bei der MST-Konfiguration wird die MST-Region definiert, der das Gerät angehört. Eine Konfiguration umfasst den Namen, die Version und die Region, der das Gerät angehört.

Netzwerkadministratoren können die Einstellungen der MSTP-Instanzen definieren, indem sie den Bildschirm **MSTP Instance Settings** verwenden.

Instance ID. Definiert die VLAN-Gruppe, der die Schnittstelle zugewiesen ist.

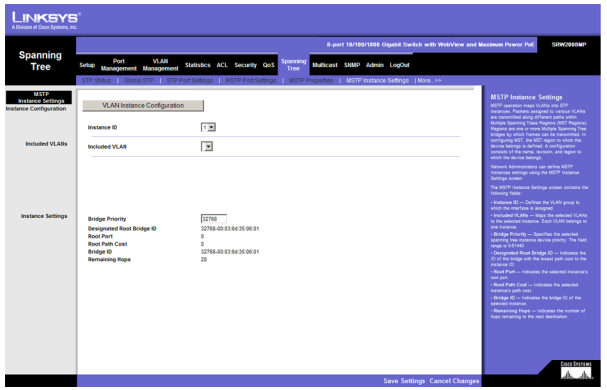


Abbildung 5-51: Spanning Tree – MSTP Instance Settings (MSTP-Instanzeinstellungen)

Included VLAN. Ordnet das ausgewählte VLAN der ausgewählten Instanz zu. Jedes VLAN gehört zu einer Instanz.

Bridge Priority. Gibt die ausgewählte Gerätepriorität für die Spanning Tree-Instanz an. Der Feldbereich beträgt 0 bis 61.440.

Designated Root Bridge ID. Zeigt für die Instanz-ID die ID der Bridge mit den niedrigsten Pfadkosten an.

Root Port. Zeigt den Stammanschluss (Root Port) für die ausgewählte Instanz an.

Root Path Cost. Zeigt die Pfadkosten für die ausgewählte Instanz an.

Bridge ID. Zeigt die Bridge-ID für die ausgewählte Instanz an.

Remaining Hops. Zeigt die Anzahl an Sprüngen an, die bis zum nächsten Ziel verbleiben.

Registerkarte „Spanning Tree“ – MSTP Interface Settings

Netzwerkadministratoren können MSTP-Schnittstelleneinstellungen zuweisen, indem sie den Bildschirm **MSTP Interface Settings** verwenden.

Der Bildschirm **MSTP Interface Settings** enthält die folgenden Felder:

Instance ID. Listet die auf dem Gerät konfigurierten MSTP-Instanzen auf. Der zulässige Feldbereich beträgt 0 bis 15.

Interface. Gibt die Schnittstelle an, für die die MSTP-Einstellungen angezeigt werden. Folgende Feldwerte sind möglich:

- **Port.** Gibt den Anschluss an, für den die MSTP-Einstellungen angezeigt werden.
- **LAG.** Gibt die LAG an, für die die MSTP-Einstellungen angezeigt werden.

Port State. Zeigt an, ob der Anschluss für die jeweilige Instanz aktiviert ist.

Type. Zeigt an, ob der Anschluss ein Punkt-zu-Punkt-Anschluss oder ein Anschluss ist, der mit einem Hub verbunden ist. Folgende Feldwerte sind möglich:

- **Boundary Port.** Zeigt an, dass es sich bei dem Anschluss um einen Grenzanschluss handelt.
  Ein Grenzanschluss verbindet MST-Bridges mit einem LAN in einem abseits gelegenen Bereich. Wenn es sich bei dem Anschluss um einen Grenzanschluss handelt, wird auch angezeigt, ob das Gerät am anderen Ende der Verbindung im RSTP- oder im STP-Modus arbeitet.
- **Master Port.** Zeigt an, dass es sich bei dem Anschluss um einen Masteranschluss handelt.
  Ein Masteranschluss stellt die Konnektivität von einer MSTP-Region zum abseits gelegenen CIST-Root bereit.
- **Internal.** Zeigt an, dass es sich bei dem Anschluss um einen internen Anschluss handelt.

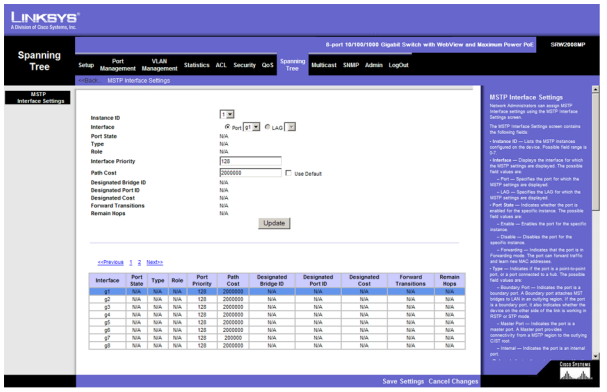


Abbildung 5-52: Spanning Tree – MSTP Interface Settings (MSTP-Schnittstelleneinstellungen)

Role. Zeigt die Anschlussfunktion an, die vom STP-Algorithmus zugewiesen wird, um STP-Pfade bereitzustellen. Folgende Feldwerte sind möglich:

- **Root.** Stellt den Pfad mit den niedrigsten Kosten zum Weiterleiten von Paketen an das Root-Gerät bereit.
- **Designated.** Zeigt den Anschluss bzw. die LAG an, über den bzw. die das jeweilige Gerät an das LAN angeschlossen ist.
- **Alternate.** Stellt für das Root-Gerät einen alternativen Pfad von der Root-Schnittstelle bereit.
- **Backup.** Stellt auf dem Weg zu den Spanning Tree-Verästelungen für den jeweiligen Anschlusspfad einen Sicherungspfad bereit. Sicherungsanschlüsse werden nur verwendet, wenn zwei Anschlüsse in einer Schleife mithilfe einer Punkt-zu-Punkt-Verbindung verbunden sind. Sie werden außerdem verwendet, wenn in einem LAN zwei oder mehr Verbindungen zu einem gemeinsam genutzten Segment verbunden sind.
- **Disabled.** Zeigt an, dass der Anschluss nicht Teil des Spanning Tree ist.

Mode. Zeigt den aktuellen Modus des Spanning Tree an. Sie können den Modus des Spanning Tree auf dem Bildschirm **Global STP** auswählen. Folgende Feldwerte sind möglich:

- **Classic STP.** Zeigt an, dass für das Gerät **Classic STP** aktiviert ist.
- **Rapid STP.** Zeigt an, dass für das Gerät **Rapid STP** aktiviert ist.
- **Multiple STP.** Zeigt an, dass für das Gerät **Multiple STP** aktiviert ist.

Interface Priority. Definiert für die angegebene Instanz die Schnittstellenpriorität. Der Standardwert lautet 128.

Path Cost. Zeigt den Beitrag des Anschlusses zur Spanning Tree-Instanz an. Der Bereich sollte immer 1 bis 200.000.000 betragen.

Designated Bridge ID. Zeigt die ID-Nummer der Bridge an, die die Verbindung bzw. das gemeinsam genutzte LAN mit dem Stammelement (Root) verbindet.

Designated Port ID. Zeigt die ID-Nummer des Anschlusses auf der jeweiligen Bridge an, die die Verbindung bzw. das gemeinsam genutzte LAN mit dem Stammelement (Root) verbindet.

Designated Cost. Zeigt an, dass die Standardpfadkosten anhand der Methode zugewiesen wurden, die Sie auf dem Bildschirm **Spanning Tree Global Settings** ausgewählt haben.

Forward Transitions. Zeigt an, wie häufig der Anschluss aus dem Status **Forwarding** in den Status **Blocking** übergegangen ist.

Remaining Hops. Zeigt die Sprünge an, die bis zum nächsten Ziel verbleiben.

Registerkarte „Multicast“ – IGMP Snooping

Wenn das IGMP Snooping global aktiviert ist, werden alle IGMP-Pakete an die CPU weitergeleitet. Die CPU analysiert die eingehenden Pakete und bestimmt Folgendes:

- Welche Anschlüsse möchten welchen Multicastgruppen angehören?
- Welche Anschlüsse verfügen über Multicastrouter, die IGMP-Abfragen erzeugen?
- Welche Routingprotokolle leiten Pakete und Multicast-Datenverkehr weiter?

Anschlüsse, die einer bestimmten Multicastgruppe angehören möchten, geben einen IGMP-Bericht aus, in dem angegeben ist, dass eine Multicastgruppe Mitglieder aufnimmt. Dies führt zur Erstellung der Multicast-Filterdatenbank.

Enable IGMP Snooping. Zeigt an, ob das IGMP Snooping für das Gerät aktiviert ist. Das IGMP Snooping kann nur aktiviert sein, wenn die Option **Bridge Multicast Filtering** aktiviert ist.

VLAN ID. Gibt die VLAN-ID an.

IGMP Status. Zeigt an, ob das IGMP Snooping für das VLAN aktiviert ist.

Auto Learn. Zeigt an, ob das automatische Lernen für das Gerät aktiviert ist. Wenn die Option **Auto Learn** aktiviert ist, lernt das Gerät automatisch, wo sich andere Multicastgruppen befinden. Aktiviert bzw. deaktiviert das automatische Lernen für das Ethernet-Gerät.

Host Timeout. Zeigt an, wie lange der Host auf den Empfang einer Nachricht wartet, bevor eine Zeitüberschreitung vorliegt. Standardmäßig ist 260 Sekunden eingestellt.

MRouter Timeout. Zeigt an, wie lange der Multicastrouter auf den Empfang einer Nachricht wartet, bevor eine Zeitüberschreitung vorliegt. Der Standardwert beträgt 300 Sekunden.

Leave Timeout. Zeigt an, wie lange der Host wartet, nachdem die Anforderung zum Verlassen der IGMP-Gruppe erfolgt und keine Join-Nachricht von einer anderen Station eingegangen ist, bevor eine Zeitüberschreitung vorliegt. Wenn ein **Leave Timeout** eintritt, weist der Switch das Multicastgerät an, das Senden von Datenverkehr zu stoppen. Beim Wert für **Leave Timeout** handelt es sich entweder um einen benutzerdefinierten Wert oder um einen Wert zum sofortigen Verlassen. Standardmäßig ist 10 Sekunden eingestellt.

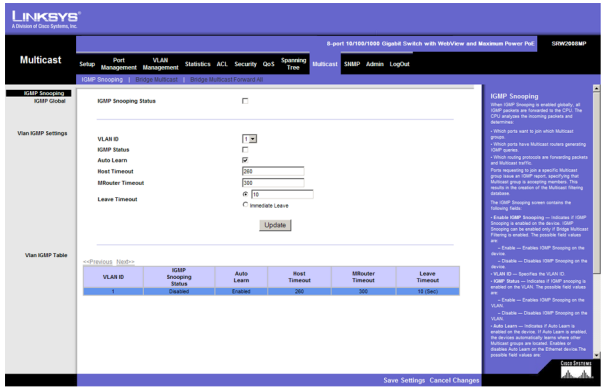


Abbildung 5-53: Multicast – IGMP Snooping

Registerkarte „Multicast“ – Bridge Multicast

Auf dem Bildschirm **Bridge Multicast** werden die Anschlüsse und LAGs angezeigt, die in den Tabellen mit den Anschlüssen und LAGs der Multicastdienst-Gruppe zugeordnet sind. In den Tabellen mit den Anschlüssen und LAGs wird auch jeweils angezeigt, auf welche Weise ein Anschluss bzw. eine LAG Mitglied der Multicastgruppe geworden ist. Sie können Anschlüsse entweder vorhandenen Gruppen oder neuen Multicastdienst-Gruppen hinzufügen. Auf dem Bildschirm **Bridge Multicast** können Sie neue Multicastdienst-Gruppen erstellen. Außerdem werden auf dem Bildschirm **Bridge Multicast** Anschlüsse einer bestimmten Multicastdienst-Adressengruppe zugewiesen.

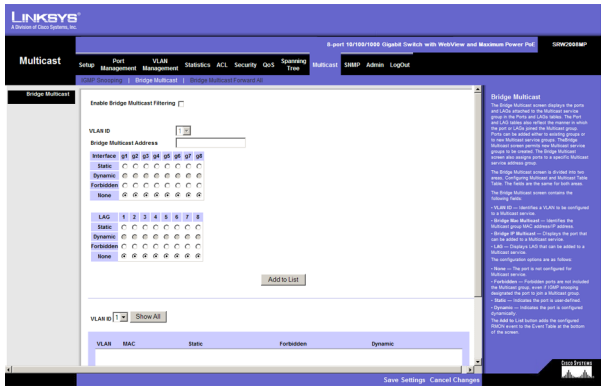


Abbildung 5-54: Multicast – Bridge Multicast (Bridge Multicast)

Der Bildschirm **Bridge Multicast** ist in zwei Bereiche unterteilt: **Configuring Multicast** und **Multicast Table**. Die Felder sind in beiden Bereichen identisch.

VLAN ID. Gibt ein VLAN an, das für einen Multicastdienst konfiguriert werden soll.

Bridge Multicast Address. Gibt die MAC-Adresse bzw. IP-Adresse der Multicastgruppe an.

Bridge IP Multicast. Zeigt den Anschluss an, der einem Multicastdienst hinzugefügt werden kann.

LAG. Zeigt die LAG an, die einem Multicastdienst hinzugefügt werden kann.

Es sind folgende Konfigurationsoptionen verfügbar:

- **Static.** Zeigt an, dass der Anschluss benutzerdefiniert ist.
- **Dynamic.** Zeigt an, dass der Anschluss dynamisch konfiguriert wird.
- **Forbidden.** Verbotene Anschlüsse sind in der Multicastgruppe nicht enthalten. Dies ist auch dann nicht der Fall, wenn der Anschluss per IGMP Snooping angewiesen wurde, Mitglied einer Multicastgruppe zu werden.
- **None.** Der Anschluss ist nicht für den Multicastdienst konfiguriert.

Mit der Schaltfläche **Add to List** fügen Sie das konfigurierte RMON-Ereignis der **Event Table** unten auf dem Bildschirm hinzu.

Registerkarte „Multicast“ – Bridge Multicast Forward All

Der Bildschirm **Bridge Multicast Forward All** enthält Felder zum Zuordnen von Anschlüssen bzw. LAGs zu einem Gerät, das an einen benachbarten Multicastrouter bzw. -switch angeschlossen ist. Wenn das IGMP Snooping aktiviert ist, werden Multicastpakete an den entsprechenden Anschluss bzw. das VLAN weitergeleitet.

Der Bildschirm **Bridge Multicast Forward All** enthält die folgenden Felder:

VLAN ID. Gibt das VLAN an, für das Multicastparameter angezeigt werden.

Es sind folgende Konfigurationsoptionen verfügbar:

- **None.** Der Anschluss ist nicht für den Multicastdienst konfiguriert.
- **Forbidden.** Verbotene Anschlüsse sind in der Multicastgruppe nicht enthalten. Dies ist auch dann nicht der Fall, wenn der Anschluss per IGMP Snooping angewiesen wurde, Mitglied einer Multicastgruppe zu werden.
- **Static.** Zeigt an, dass der Anschluss benutzerdefiniert ist.
- **Dynamic.** Zeigt an, dass der Anschluss dynamisch konfiguriert wird.

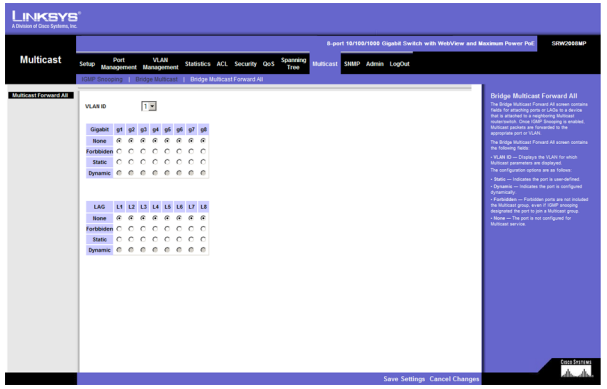


Abbildung 5-55: Multicast – Bridge Multicast Forward All (Bridge Multicast, alle weiterleiten)

Registerkarte „SNMP“ – Global Parameters

Der Bildschirm **Global Parameters** enthält Parameter zum Definieren von SNMP-Benachrichtigungsparametern.

Local Engine ID. Zeigt die Engine-ID des lokalen Geräts an. Der Feldwert ist eine hexadezimale Zeichenfolge. Jedes Byte besteht in hexadezimalen Zeichenfolgen aus zwei hexadezimalen Ziffern. Dabei kann jedes Byte durch einen Punkt oder einen Doppelpunkt abgetrennt werden. Sie müssen die Engine-ID definieren, bevor Sie SNMPv3 aktivieren. Wählen Sie für Standalone-Geräte eine Standard-Engine-ID, die aus Enterprise-Nummer und MAC-Standardadresse besteht. Konfigurieren Sie bei einem stapelbaren System die Engine-ID, und stellen Sie sicher, dass die Engine-ID für die Verwaltungsdomäne eindeutig ist. Auf diese Weise verhindern Sie, dass zwei Geräte eines Netzwerks dieselbe Engine-ID aufweisen.

Use Default. Verwendet die vom Gerät erzeugte Engine-ID. Die Standard-Engine-ID basiert auf der MAC-Adresse des Geräts und ist standardmäßig wie folgt definiert:

- Erste 4 Oktetts — Erstes Bit = 1, und der Rest ist die IANA Enterprise-Nummer.
- Fünftes Oktett — Auf 3 setzen, um die darauffolgende MAC-Adresse anzuzeigen.
- Letzte 6 Oktetts — MAC-Adresse des Geräts.

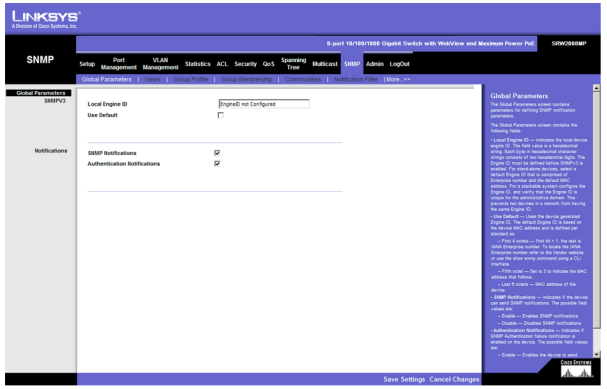


Abbildung 5-56: SNMP – Global Parameters (Globale Parameter)

SNMP Notifications. Zeigt an, ob das Gerät SNMP-Benachrichtigungen senden kann.

Authentication Notifications. Zeigt an, ob für das Gerät die Benachrichtigung beim Fehlschlagen der SNMP-Authentifizierung aktiviert ist.

Registerkarte „SNMP“ – Views

SNMP-Ansichten ermöglichen bzw. sperren den Zugriff auf Gerätefunktionen oder Funktionsaspekte. Sie können z. B. eine Ansicht definieren, die aussagt, dass SNMP-Guppe A schreibgeschützten Zugriff (Read-Only, R/O) auf Multicastgruppen hat, während SNMP-Gruppe B Schreib-/Lesezugriff (Read-Write, R/W) auf Multicastgruppen hat. Der Funktionszugriff wird über den MIB-Namen oder über die MIB-Objekt-ID gewährt.

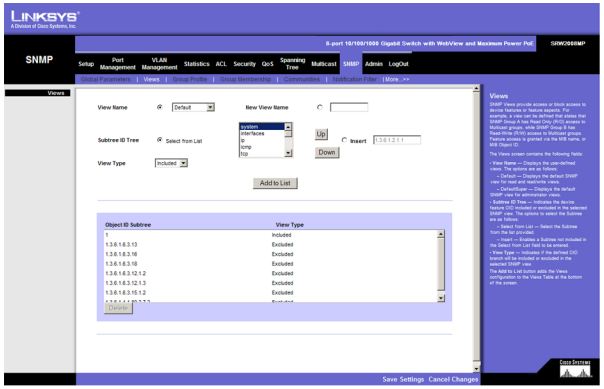


Abbildung 5-57: SNMP – Views (Ansichten)

View Name. Zeigt die benutzerdefinierten Ansichten an. Es sind folgende Optionen verfügbar:

- **Default.** Zeigt die SNMP-Standardansicht für Lese- und Schreib-/Leseansichten an.
- **DefaultSuper.** Zeigt die SNMP-Standardansicht für Administratoransichten an.

Subtree ID Tree. Zeigt die Gerätefunktion-OID an, die in der ausgewählten SNMP-Ansicht enthalten bzw. nicht enthalten sein kann. Zum Auswählen der Unterstruktur sind folgende Optionen verfügbar:

- **Select from List.** Wählen Sie die Unterstruktur aus der angezeigten Liste aus.
- **Insert.** Ermöglicht, dass Sie eine Unterstruktur eingeben, die im Feld **Select from List** nicht enthalten ist.

View Type. Zeigt an, ob die definierte OID-Verzweigung in der ausgewählten SNMP-Ansicht enthalten bzw. nicht enthalten ist.

Mit der Schaltfläche **Add to List** fügen Sie die Ansichtenkonfiguration der **Views Table** unten auf dem Bildschirm hinzu.

Registerkarte „SNMP“ – Group Profile

Der Bildschirm **Group Profile** enthält Informationen zum Erstellen von SNMP-Gruppen und zum Zuweisen von Berechtigungen für die SNMP-Zugriffssteuerung zu SNMP-Gruppen. Mithilfe von Gruppen können Netzwerkverwalter bestimmten Gerätefunktionen bzw. Funktionsaspekten Zugriffsrechte zuweisen.

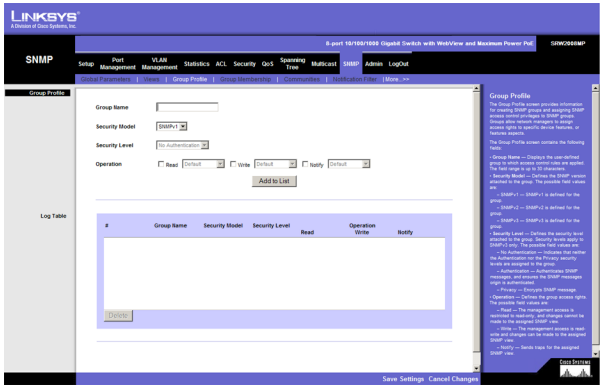


Abbildung 5-58: SNMP – Group Profile (Gruppenprofil)

Group Name. Zeigt die benutzerdefinierte Gruppe an, auf die Regeln für die Zugriffssteuerung angewendet werden. Der Feldbereich umfasst bis zu 30 Zeichen.

Security Model. Definiert die SNMP-Version, die der Gruppe zugeordnet ist. Folgende Feldwerte sind möglich:

- **SNMPv1.** SNMPv1 ist für die Gruppe definiert.
- **SNMPv2.** SNMPv2 ist für die Gruppe definiert.
- **SNMPv3.** SNMPv3 ist für die Gruppe definiert.

Security Level. Definiert die Sicherheitsebene, die der Gruppe zugeordnet ist. Sicherheitsebenen gelten nur für SNMPv3. Folgende Feldwerte sind möglich:

- **No Authentication.** Zeigt an, dass der Gruppe weder Sicherheitsebenen für die Authentifizierung (Authentication) noch für den Datenschutz (Privacy) zugewiesen sind.
- **Authentication.** Authentifiziert SNMP-Nachrichten und stellt sicher, dass der Ursprung von SNMP-Nachrichten authentifiziert wird.
- **Privacy.** Verschlüsselt SNMP-Nachrichten.

Operation. Definiert die Zugriffsrechte der Gruppe. Folgende Feldwerte sind möglich:

- **Read.** Der Verwaltungszugriff ist auf den schreibgeschützten Zugriff beschränkt, und es können keine Änderungen an der zugewiesenen SNMP-Ansicht vorgenommen werden.
- **Write.** Für den Verwaltungszugriff besteht Schreib-/Lesezugriff, und es können Änderungen an der zugewiesenen SNMP-Ansicht vorgenommen werden.
- **Notify.** Sendet für die zugewiesene SNMP-Ansicht Traps.

Registerkarte „SNMP“ – Group Membership

Der Bildschirm **Group Membership** enthält Informationen zum Zuweisen von SNMP-Zugriffssteuerungsberechtigungen zu SNMP-Gruppen.

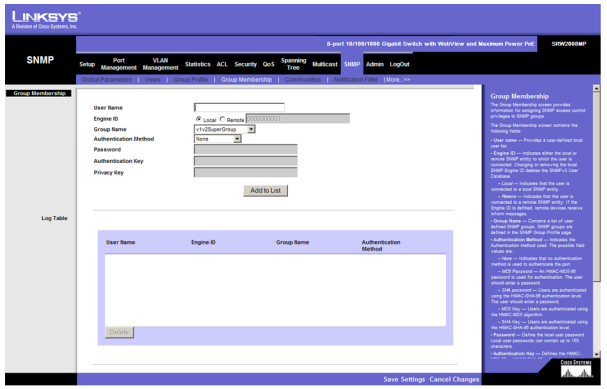


Abbildung 5-59: SNMP – Group Membership (Gruppenmitgliedschaft)

User name. Stellt eine benutzerdefinierte Liste der lokalen Benutzer bereit.

Engine ID. Zeigt entweder die lokale oder die Remote-SNMP-Einheit an, mit der der Benutzer verbunden ist. Wenn Sie die lokale SNMP-Engine-ID ändern oder entfernen, wird die SNMPv3-Benutzerdatenbank gelöscht.

- **Local.** Zeigt an, dass der Benutzer mit einer lokalen SNMP-Einheit verbunden ist.
- **Remote.** Zeigt an, dass der Benutzer mit einer Remote-SNMP-Einheit verbunden ist. Wenn die Engine-ID definiert ist, empfangen Remotegeräte INFORM-Meldungen.

Group Name. Enthält eine Liste mit benutzerdefinierten SNMP-Gruppen. SNMP-Gruppen sind auf der Seite **SNMP Group Profile** definiert.

Authentication Method. Zeigt die verwendete Authentifizierungsmethode an. Folgende Feldwerte sind möglich:

- **None.** Zeigt an, dass keine Authentifizierungsmethode verwendet wird, um den Anschluss zu authentifizieren.
- **MD5 Password.** Zeigt an, dass die Anschlussauthentifizierung per HMAC-MD5-96-Kennwortauthentifizierung erfolgt.
- **SHA Password.** Zeigt an, dass die Anschlussauthentifizierung per HMAC-SHA-96-Kennwortauthentifizierung erfolgt.
- **MD5 Key.** Zeigt an, dass die Anschlussauthentifizierung per HMAC-MD5-Algorithmus erfolgt.
- **SHA Key.** Zeigt an, dass die Anschlussauthentifizierung per HMAC-SHA-96-Authentifizierung erfolgt.

Password. Definiert das lokale Benutzerkennwort. Lokale Benutzerkennwörter können bis zu 159 Zeichen enthalten.

Authentication Key. Definiert die Authentifizierungsebene HMAC-MD5-96 oder HMAC-SHA-96. Die Authentifizierungs- und Datenschutzschlüssel werden eingegeben, um den Authentifizierungsschlüssel zu definieren. Wenn nur die Authentifizierung erforderlich ist, werden 16 Byte definiert. Wenn sowohl der Datenschutz als auch die Authentifizierung erforderlich ist, werden 32 Byte definiert. Jedes Byte besteht in hexadezimalen Zeichenfolgen aus zwei hexadezimalen Ziffern. Dabei kann jedes Byte durch einen Punkt oder einen Doppelpunkt abgetrennt werden.

Privacy Key. Definiert den Datenschutzschlüssel (LSB). Wenn nur die Authentifizierung erforderlich ist, werden 20 Byte definiert. Wenn sowohl der Datenschutz als auch die Authentifizierung erforderlich ist, werden 36 Byte definiert. Jedes Byte besteht in hexadezimalen Zeichenfolgen aus zwei hexadezimalen Ziffern. Dabei kann jedes Byte durch einen Punkt oder einen Doppelpunkt abgetrennt werden.

Mit der Schaltfläche **Add to List** fügen Sie die Konfiguration **Group Membership** der entsprechenden Tabelle unten auf dem Bildschirm hinzu.

Registerkarte „SNMP“ – Communities

Der Bildschirm **Communities** ist in drei Bereiche unterteilt: **Communities**, **Basic Table** und **Advanced Table**.

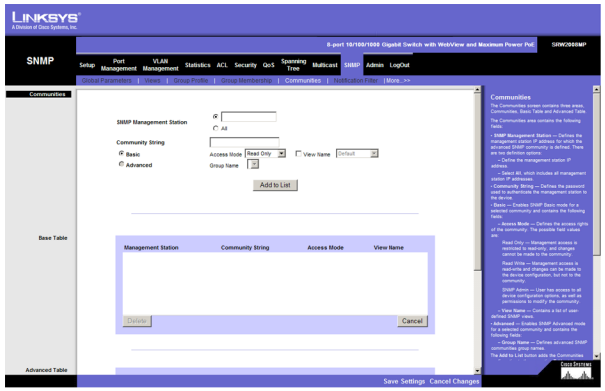


Abbildung 5-60: SNMP – Communities

SNMP Management Station. Definiert die IP-Adresse der Verwaltungsstation, für die die erweiterte SNMP-Community definiert wird. Es sind zwei Definitionsoptionen verfügbar:

- Definieren der IP-Adresse der Verwaltungsstation.
- **All.** Enthält alle IP-Adressen von Verwaltungsstationen.

Community String. Definiert das Kennwort, das zum Authentifizieren der Verwaltungsstation für das Gerät verwendet wird.

Basic. Aktiviert für eine ausgewählte Community den Modus **SNMP Basic** und enthält die folgenden Felder:

Access Mode. Definiert die Zugriffsrechte der Community. Folgende Feldwerte sind möglich:

- **Read Only.** Der Verwaltungszugriff ist auf den schreibgeschützten Zugriff beschränkt, und es können keine Änderungen an der Community vorgenommen werden.
- **Read Write.** Für den Verwaltungszugriff besteht Schreib-/Lesezugriff, und es können Änderungen an der Gerätekonfiguration vorgenommen werden, jedoch nicht an der Community.
- **SNMP Admin.** Benutzer haben Zugriff auf alle Optionen zur Gerätekonfiguration und verfügen über Berechtigungen zum Ändern der Community.

View Name. Enthält eine Liste mit benutzerdefinierten SNMP-Ansichten.

Advanced. Aktiviert für eine ausgewählte Community den Modus **SNMP Advanced** und enthält die folgenden Felder:

Group Name. Definiert Gruppennamen für erweiterte SNMP-Communities.

Mit der Schaltfläche **Add to List** fügen Sie die Communitykonfiguration der entsprechenden Tabelle unten auf dem Bildschirm hinzu.

Base Table

Management Station – Zeigt die IP-Adresse der Verwaltungsstation an, für die die Basis-SNMP-Community definiert wird.

Community String – Zeigt das Kennwort an, das zum Authentifizieren der Verwaltungsstation für das Gerät verwendet wird.

Access Mode — Zeigt die Zugriffsrechte der Community an.

View Name — Zeigt die benutzerdefinierte SNMP-Ansicht an.

Advanced Table

Management Station — Zeigt die IP-Adresse der Verwaltungsstation an, für die die Basis-SNMP-Community definiert wird.

Community String — Zeigt das Kennwort an, das zum Authentifizieren der Verwaltungsstation für das Gerät verwendet wird.

Group Name — Zeigt den Gruppennamen für erweiterte SNMP-Communities an.

Registerkarte „SNMP“ – Notification Filter

Auf dem Bildschirm **Notification Filter** können Sie Traps filtern, die auf OIDs basieren. Jede OID ist mit einer Gerätefunktion bzw. einem Funktionsaspekt verknüpft. Auf dem Bildschirm **Notification Filter** können Netzwerkverwalter außerdem Benachrichtigungen filtern.

Filter Name. Enthält eine Liste mit benutzerdefinierten Benachrichtigungsfiltern.

New Object Identifier Subtree. Zeigt die OID an, für die Benachrichtigungen gesendet oder gesperrt werden. Wenn ein Filter einer OID zugeordnet ist, werden Traps oder INFORM-Meldungen erzeugt und an die Trap-Empfänger gesendet. Sie wählen Objekt-IDs entweder unter **Select from List** oder **Object ID List** aus. Es sind zwei Konfigurationsoptionen verfügbar:

- **Select from List.** Wählen Sie die OID aus der angezeigten Liste aus.
- **Object ID.** Geben Sie eine OID ein, die unter **Select from List** nicht aufgeführt ist.

Filter Type. Zeigt an, ob für die OID INFORM-Meldungen oder Traps an die Trap-Empfänger gesendet werden.

- **Excluded.** Beschränkt das Senden von Traps oder INFORM-Meldungen für OIDs.
- **Included.** Sendet Traps oder INFORM-Meldungen für OIDs.

Mit der Schaltfläche **Add to List** fügen Sie die Konfiguration für den Benachrichtigungsfilter der **Notification Filter Table** unten auf dem Bildschirm hinzu.

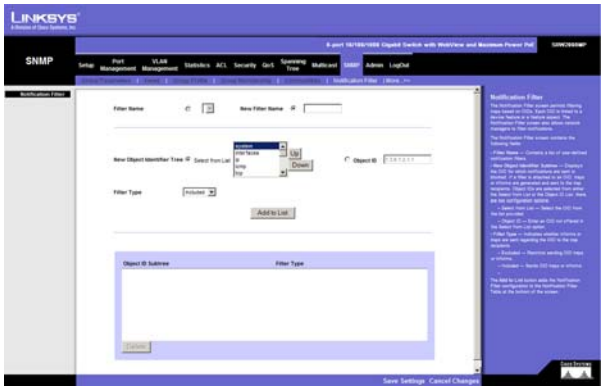


Abbildung 5-61: SNMP – Notification Filter (Benachrichtigungsfilter)

Registerkarte „SNMP“ – Notification Recipient

Der Bildschirm **Notification Recipient** enthält Informationen zum Definieren von Filtern, die bestimmen, ob Traps an bestimmte Benutzer gesendet werden und welcher Trap-Typ dabei verwendet wird. SNMP-Benachrichtigungsfilter stellen die folgenden Dienste bereit:

- Identifizieren von Verwaltungs-Trap-Zielen
- Trap-Filterung
- Auswählen von Trap-Erzeugungsparametern
- Bereitstellen von Zugriffssteuerungsprüfungen

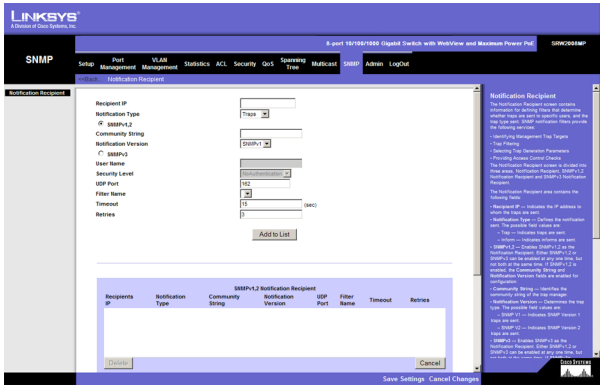


Abbildung 5-62: Notification Recipient (Benachrichtigungsempfänger)

Recipient IP. Zeigt die IP-Adresse an, an die die Traps gesendet werden.

Notification Type. Definiert die gesendete Benachrichtigung. Folgende Feldwerte sind möglich:

- **Traps.** Zeigt an, dass Traps gesendet werden.
- **Informs.** Zeigt an, dass INFORM-Meldungen gesendet werden.

SNMPv1.2. Aktiviert SNMPv1.2 als Benachrichtigungsempfänger. Es kann jeweils entweder SNMPv1.2 oder SNMPv3 aktiviert sein, aber nicht beides gleichzeitig. Wenn SNMPv1.2 aktiviert ist, sind die Felder **Community String** und **Notification Version** für die Konfiguration aktiviert:

- **Community String.** Identifiziert die Communityzeichenfolge des Trap-Managers.
- **Notification Version.** Bestimmt den Trap-Typ. Folgende Feldwerte sind möglich:
  - SNMP V1. Zeigt an, dass Traps der SNMP-Version 1 gesendet werden.
  - SNMP V2. Zeigt an, dass Traps der SNMP-Version 2 gesendet werden.

SNMPv3. Aktiviert SNMPv3 als Benachrichtigungsempfänger. Es kann jeweils entweder SNMPv1.2 oder SNMPv3 aktiviert sein, aber nicht beides gleichzeitig. Wenn SNMPv3 aktiviert ist, sind die Felder **User Name** und **Security Level** für die Konfiguration aktiviert:

User Name. Definiert den Benutzer, an den SNMP-Benachrichtigungen gesendet werden.

Security Level. Definiert die Methode, mit der das Paket authentifiziert wird. Folgende Feldwerte sind möglich:

- **No Authentication.** Zeigt an, dass das Paket weder authentifiziert noch verschlüsselt wurde.

- **Authentication.** Zeigt an, dass das Paket authentifiziert wurde.
- **Privacy.** Zeigt an, dass das Paket sowohl authentifiziert als auch verschlüsselt wurde.

UDP Port. Zeigt den UDP-Anschluss an, der zum Senden von Benachrichtigungen verwendet wird. Standardmäßig ist 162 eingestellt.

Filter Name. Zeigt an, ob der SNMP-Filter eingerichtet wurde, für den der Filter **SNMP Notification** definiert wurde.

Timeout. Zeigt an, wie lange (in Sekunden) das Gerät wartet, bevor es INFORM-Meldungen sendet. Standardmäßig ist 15 Sekunden eingestellt.

Retries. Zeigt an, wie häufig das Gerät eine INFORM-Anforderung erneut sendet. Standardmäßig ist 3 Sekunden eingestellt.

Mit der Schaltfläche **Add to List** fügen Sie die Konfiguration **Notification Recipient** der entsprechenden Tabelle unten auf dem Bildschirm hinzu.

Registerkarte „Admin“ – User Authentication

Der Bildschirm **User Authentication** wird verwendet, um Benutzerkennwörter zu ändern.

Authentication Type. Definiert die Benutzerauthentifizierungsmethoden. Sie können auch Kombinationen der verschiedenen Authentifizierungsmethoden auswählen. Folgende Feldwerte sind möglich:

- **Local.** Authentifiziert Benutzer auf Geräteebene. Das Gerät prüft Benutzername und Kennwort auf die Authentifizierung.
- **RADIUS.** Authentifiziert Benutzer auf dem RADIUS-Server.
- **TACACS+.** Authentifiziert Benutzer auf dem TACACS+-Server.
- **None.** Weist dem Authentifizierungsprofil keine Authentifizierungsmethode zu.

User Name. Zeigt den Benutzernamen an.

Password. Gibt das neue Kennwort an. Das Kennwort wird nicht angezeigt. Bei der Eingabe wird im Feld für jedes Zeichen ein Sternchen (*) angezeigt. (Bereich: 1 bis 159 Zeichen)

Confirm Password. Bestätigt das neue Kennwort. Das Kennwort, das Sie in dieses Feld eingeben, muss genau dem Kennwort entsprechen, das Sie in das Feld **Password** eingegeben haben.

Mit der Schaltfläche **Add to List** fügen Sie die Benutzerkonfiguration der Tabelle des lokalen Benutzers hinzu.

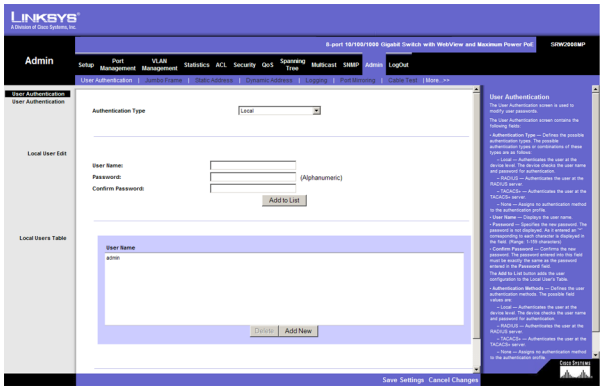


Abbildung 5-63: Admin – User Authentication (Benutzerauthentifizierung)

Registerkarte „Admin“ – Jumbo Frames

Jumbo Frames. Diese Option ermöglicht den Transport identischer Daten in einer geringeren Zahl von Frames. Dadurch werden der Overhead, die Verarbeitungszeit und die Anzahl der Unterbrechungen verringert.

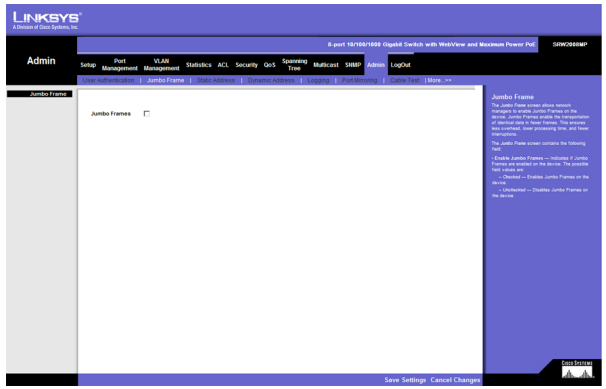


Abbildung 5-64: Jumbo Frames (Großrahmen)

Registerkarte „Admin“ – Static Address

Auf diesem Switch können Sie eine statische Adresse einer bestimmten Schnittstelle zuweisen. Statische Adressen sind an die zugewiesene Schnittstelle gebunden und können nicht verschoben werden. Wenn eine statische Adresse an einer anderen Schnittstelle erkannt wird, wird die Adresse ignoriert und nicht in die Adresstabelle geschrieben.

Interface. Zeigt die Schnittstelle an, auf die sich der Eintrag bezieht:

- **Port.** Die spezifische Anschlussnummer, auf die sich die Parameter der Weiterleitungstabelle beziehen.
- **LAG.** Die spezifische LAG-Nummer, auf die sich die Parameter der Weiterleitungstabelle beziehen.

MAC Address. Zeigt die MAC-Adresse an, auf die sich der Eintrag bezieht.

VLAN ID. Zeigt die VLAN-ID-Nummer an, auf die sich der Eintrag bezieht.

VLAN Name. Zeigt den VLAN-Namen an, auf den sich der Eintrag bezieht.

Status. Zeigt an, wie der Eintrag erstellt wurde. Folgende Feldwerte sind möglich:

- **Permanent.** Die MAC-Adresse ist eine dauerhafte Adresse.
- **Delete on Reset.** Die MAC-Adresse wird gelöscht, wenn das Gerät zurückgesetzt wird.
- **Delete on Timeout.** Die MAC-Adresse wird gelöscht, wenn eine Zeitüberschreitung vorliegt.
- **Secure.** Die MAC-Adresse ist für gesperrte Anschlüsse definiert.

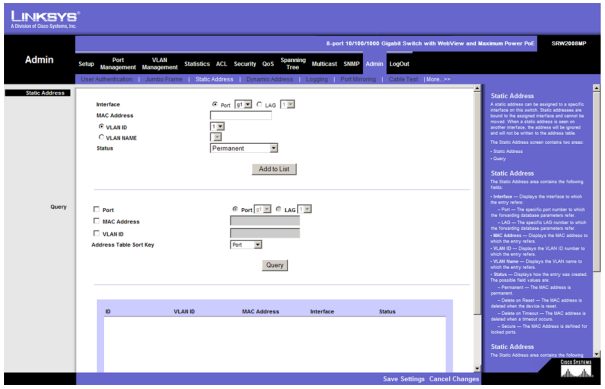


Abbildung 5-65: Admin – Static Address (Statische Adresse)

Query

Port. Gibt die Schnittstelle an, für die die Tabelle abgefragt wird. Es gibt zwei Schnittstellentypen, aus denen Sie wählen können.

- **Port.** Die spezifische Anschlussnummer.
- **LAG.** Die spezifische LAG-Nummer.

MAC Address. Gibt die MAC-Adresse an, für die die Tabelle abgefragt wird.

VLAN ID. Gibt die VLAN-ID an, für die die Tabelle abgefragt wird.

Address Table Sort Key. Gibt die Methode an, anhand der die Tabelle mit den dynamischen MAC-Adressen sortiert wird. Sie können die Adresstabelle nach Adresse, VLAN oder Schnittstelle sortieren.

Registerkarte „Admin“ – Dynamic Address

Die Tabelle mit den dynamischen Adressen enthält die MAC-Adressen, die gelernt wurden, indem beim Eintreffen des Datenverkehrs auf dem Switch die Quelladresse überwacht wurde. Wenn die Zieladresse des eingehenden Datenverkehrs in der Datenbank gefunden wird, werden die für diese Adresse bestimmten Pakete direkt an den zugeordneten Anschluss weitergeleitet. Anderenfalls erfolgt die Überflutung aller Anschlüsse mit dem Datenverkehr.

Der Bildschirm **Dynamic Address** enthält Parameter zum Abfragen von Informationen in der Tabelle mit den dynamischen MAC-Adressen, z. B. den Schnittstellentyp, die MAC-Adressen, VLAN und Tabellenspeicherung. Die Tabelle mit den dynamischen MAC-Adressen enthält Informationen zum Alterungszeitraum, der für eine dynamische MAC-Adresse gilt, bevor sie gelöscht wird. Außerdem enthält sie Parameter zum Abfragen und Anzeigen der Tabelle mit den dynamischen MAC-Adressen. Die Tabelle mit den dynamischen MAC-Adressen enthält auch Adressparameter, mit deren Hilfe Pakete direkt an die Anschlüsse weitergeleitet werden.
Sie können die Tabelle mit den dynamischen Adressen nach Schnittstelle, VLAN und MAC-Adresse sortieren.

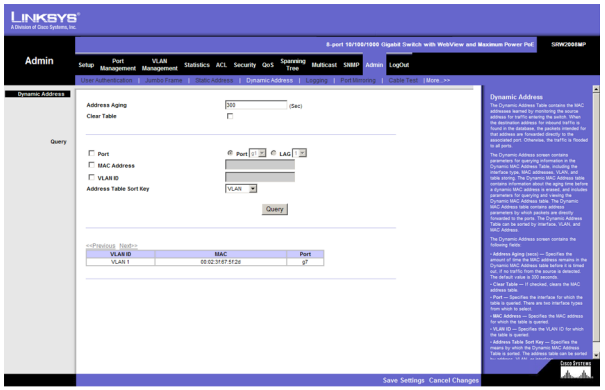


Abbildung 5-66: Admin – Dynamic Address (Dynamische Adresse)

Address Aging. Gibt den Zeitraum (in Sekunden) an, wie lange die MAC-Adresse in der Tabelle mit den dynamischen MAC-Adressen verbleibt, bevor die Zeitüberschreitung erreicht ist. Dies gilt, wenn kein Datenverkehr der Quelle erkannt wird. Der Standardwert beträgt 300 Sekunden.

Clear Table. Wenn Sie diese Option aktivieren, wird die Tabelle mit den MAC-Adressen gelöscht.

Query

Port. Gibt die Schnittstelle an, für die die Tabelle abgefragt wird. Es gibt zwei Schnittstellentypen, aus denen Sie wählen können.

- **Port.** Die spezifische Anschlussnummer.
- **LAG.** Die spezifische LAG-Nummer.

MAC Address. Gibt die MAC-Adresse an, für die die Tabelle abgefragt wird.

VLAN ID. Gibt die VLAN-ID an, für die die Tabelle abgefragt wird.

Address Table Sort Key. Gibt die Methode an, anhand der die Tabelle mit den dynamischen MAC-Adressen sortiert wird. Sie können die Adresstabelle nach Adresse, VLAN oder Schnittstelle sortieren.

Registerkarte „Admin“ – Logging

Die Systemprotokolle ermöglichen das Anzeigen von Geräteereignissen in Echtzeit und das Aufzeichnen der Ereignisse zur späteren Verwendung. Systemprotokolle zeichnen Ereignisse auf und verwalten sie. Außerdem berichten sie über Fehler oder INFORM-Meldungen.

Ereignismeldungen haben ein eindeutiges Format. Es entspricht dem empfohlenen Meldungsformat der SYSLOG-Protokolle für Fehlermeldungen. SYSLOG-Meldungen und Meldungen des lokalen Geräts wird z. B. ein Code für den Schweregrad zugewiesen. Außerdem enthalten sie einen mnemonischen Meldungscode, der die Quellanwendung angibt, die die Meldung erzeugt hat. Auf diese Weise können Meldungen anhand ihrer Dringlichkeit und Relevanz gefiltert werden. Jeder Meldungsschweregrad bestimmt eine Gruppe von Ereignisprotokollierungsgeräten, die bei einer Ereignisprotokollierung jeweils gesendet wird.

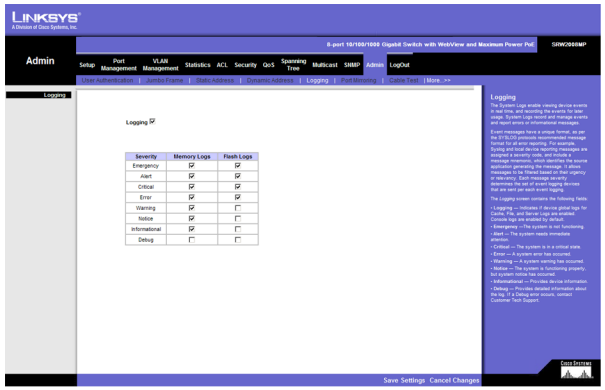


Abbildung 5-67: Admin – Logging (Protokollierung)

Logging. Zeigt an, ob globale Geräteprotokolle für Cache-, Datei- und Serverprotokolle aktiviert sind. Konsolenprotokolle sind standardmäßig aktiviert.

- **Emergency.** Das System ist nicht betriebsbereit.
- **Alert.** Das System muss sofort geprüft werden.
- **Critical.** Das System befindet sich in einem kritischen Zustand.
- **Error.** Ein Systemfehler ist aufgetreten.
- **Warning.** Eine Systemwarnung ist aufgetreten.
- **Notice.** Das System funktioniert reibungslos, aber es wurde ein Systemhinweis ausgegeben.
- **Informational.** Stellt Geräteinformationen bereit.
- **Debug.** Stellt ausführliche Informationen zum Protokoll bereit. Wenden Sie sich an den technischen Support, wenn ein Debugfehler auftritt.

Registerkarte „Admin“ – Port Mirroring

Port Mirroring (Anschlussspiegelung) überwacht und spiegelt Netzwerkdatenverkehr durch Weiterleiten von Kopien eingehender und ausgehender Pakete von einem Anschluss zu einem Überwachungsanschluss. Sie können diese Option als Diagnosetool und/oder Debugfunktion verwenden. **Port Mirroring** aktiviert außerdem das Überwachen der Switchleistung.

Netzwerkadministratoren konfigurieren die Anschlussspiegelung, indem sie einen bestimmten Anschluss auswählen, um alle Pakete zu kopieren, und andere Anschlüsse auswählen, von denen die Pakete kopiert werden.

Source Port. Definiert den Anschluss, auf den Datenverkehr gespiegelt wird.

Type. Zeigt die Anschlussmoduskonfiguration für die Anschlussspiegelung an. Folgende Feldwerte sind möglich:

- **RxOnly.** Definiert die Anschlussspiegelung für empfangende Anschlüsse. Dies ist die Standardeinstellung.
- **TxOnly.** Definiert die Anschlussspiegelung für übertragende Anschlüsse.

Both. Definiert die Anschlussspiegelung für empfangende und übertragende Anschlüsse.

Target Port. Definiert den Anschluss, von dem Datenverkehr gespiegelt wird.

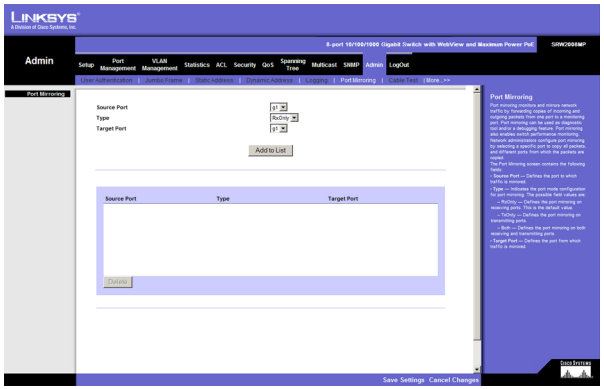


Abbildung 5-68: Admin – Port Mirroring (Anschlussspiegelung)

Registerkarte „Admin“ – Cable Test

Auf dem Bildschirm **Cable Test** werden Ergebnisse von Leistungstests für Kupferkabel angezeigt. Die maximale Kabellänge, die getestet werden kann, beträgt 120 Meter. Die Kabel werden getestet, wenn die Anschlüsse inaktiv sind, mit Ausnahme des Tests der ungefähren Kabellänge.

Port. Dies ist der Anschluss, an den das Kabel angeschlossen ist.

Test Result. Dies ist das Testergebnis. **OK** zeigt an, dass das Kabel den Test bestanden hat. **No Cable** bedeutet, dass an den Anschluss kein Kabel angeschlossen ist. **Open Cable** bedeutet, dass das Kabel nur auf einer Seite angeschlossen ist. **Short Cable** bedeutet, dass im Kabel ein Kurzschluss aufgetreten ist. **Undefined** bedeutet, dass der Test nicht ordnungsgemäß durchgeführt werden konnte.

Cable Fault Distance. Dies ist die Entfernung vom Anschluss, in der der Kabelfehler aufgetreten ist.

Last Update. Dies ist der Zeitpunkt, zu dem der Anschluss das letzte Mal getestet wurde.

Test. Klicken Sie auf die Schaltfläche **Test**, um den Test durchzuführen.

Cable Length. Die ungefähre Länge des Kabels. Der Test der Kabellänge kann nur durchgeführt werden, wenn der Anschluss aktiv ist und mit 1 GBit/s betrieben wird.

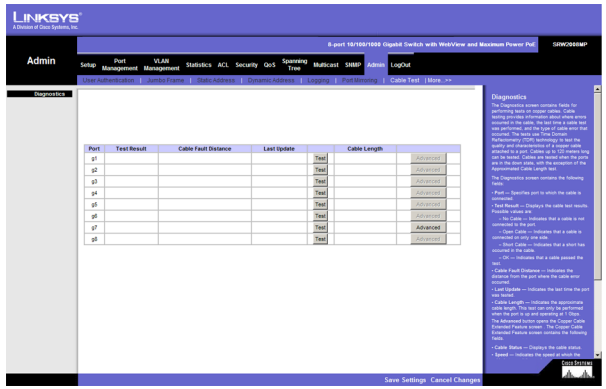


Abbildung 5-69: Admin – Cable Test (Kabeltest)

Registerkarte „Admin“ – Save Configuration

Nach dem Herunterladen einer neuen Bilddatei sollte das Gerät neu gestartet werden. Führen Sie beim Herunterladen eines neuen Startbilds folgende Schritte aus:

1. Laden Sie den neuen Startcode herunter. SETZEN SIE NICHT DAS GERÄT ZURÜCK!
2. Laden Sie das neue Softwarebild herunter.
3. Setzen Sie nun das Gerät zurück.

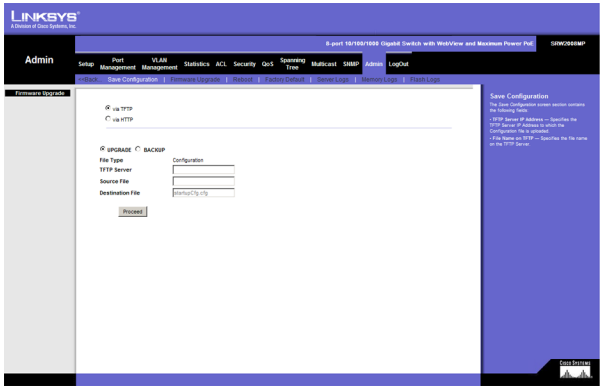


Abbildung 5-70: Admin – Save Configuration (Konfiguration speichern)

Via TFTP

Upgrade. Wählen Sie diese Option, um den Switch über eine Datei zu aktualisieren, die auf einem TFTP-Server gespeichert ist.

- **TFTP Server.** Die IP-Adresse des TFTP-Servers, der die Quelldatei für die Aktualisierung enthält.
- **Source File.** Gibt den Namen der Aktualisierungsdatei auf dem TFTP-Server an.

Backup. Geben Sie die Adresse des TFTP-Servers ein, um die Switchkonfiguration per TFTP zu sichern.

- **TFTP Server.** Gibt die IP-Adresse des TFTP-Servers an, auf dem die Konfigurationsdatei gespeichert wird.
- **Destination File.** Gibt den Namen der Konfigurationsdatei an. Die Standardeinstellung ist **StartupCfg.cfg**.

HINWEIS: Stellen Sie beim Herunterladen einer Konfigurationsdatei sicher, dass diese gültig ist. Stellen Sie nach Bearbeitung der Datei sicher, dass nur gültige Einträge konfiguriert wurden.

Via HTTP

Sie verwenden den Bildschirm **HTTP Firmware Upgrade**, um mithilfe des Webbrowsers Konfigurationsinformationen zu speichern.

Upgrade. Wählen Sie diese Option, um den Switch über eine Datei zu aktualisieren, die auf der lokalen Festplatte gespeichert ist.

- **Source File.** Geben Sie den Namen und Pfad der Datei ein, oder klicken Sie auf **Browse**, um die Aktualisierungsdatei zu suchen.

Backup

- **Proceed.** Sie verwenden die Schaltfläche **Proceed**, um die Konfiguration auf der lokalen Festplatte zu sichern.

Registerkarte „Admin“ – Firmware Upgrade

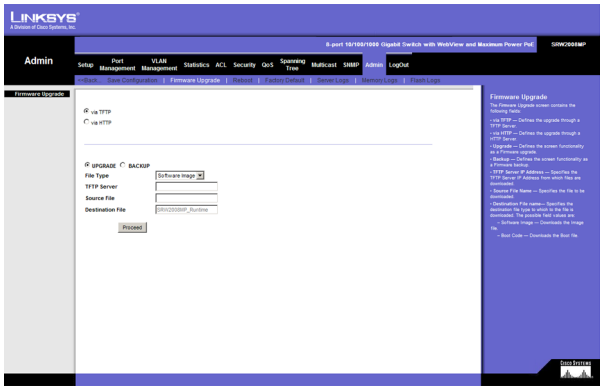


Abbildung 5-71: Admin – Firmware Upgrade (Firmwareaktualisierung)

Der Bildschirm **Firmware Upgrade** enthält die folgenden Felder:

via TFTP. Definiert die Aktualisierung über einen TFTP-Server.

via HTTP. Ermöglicht die Aktualisierung der Firmware mithilfe des Webbrowsers.

Upgrade. Definiert die Bildschirmfunktionen als Firmwareaktualisierung.

Backup. Definiert die Bildschirmfunktionen als Firmwaresicherung.

TFTP Server IP Address. Gibt die IP-Adresse des TFTP-Servers an, von dem Dateien heruntergeladen werden.

Source File Name. Gibt die herunterzuladende Datei an.

Destination File name. Gibt den Typ der Zieldatei an, der beim Herunterladen der Datei verwendet wird. Folgende Feldwerte sind möglich:

Software Image. Lädt die Bilddatei herunter.

Boot Code. Lädt die Startdatei herunter.

Registerkarte „Admin“ – Reboot

Abbildung 5-72: Admin – Reboot (Neustart)

Auf dem Bildschirm **Reboot** setzen Sie das Gerät zurück. Die Gerätekonfiguration wird automatisch gespeichert, bevor das Gerät neu gestartet wird.

Registerkarte „Admin“ – Factory Defaults

Auf dem Bildschirm **Factory Reset** können Netzwerkverwalter das Gerät auf die Werkseinstellungen zurücksetzen, die bei Auslieferung des Switches vorgegeben waren. Wenn Sie die Werkseinstellungen wiederherstellen, wird die Konfigurationsdatei gelöscht.

HINWEIS: Wenn Sie die Werkseinstellungen wiederherstellen, werden alle von Ihnen vorgenommenen Konfigurationseinstellungen gelöscht. Sie können eine Sicherung Ihrer aktuellen Konfigurationseinstellungen auf dem Bildschirm *Admin – Save Configuration* speichern.

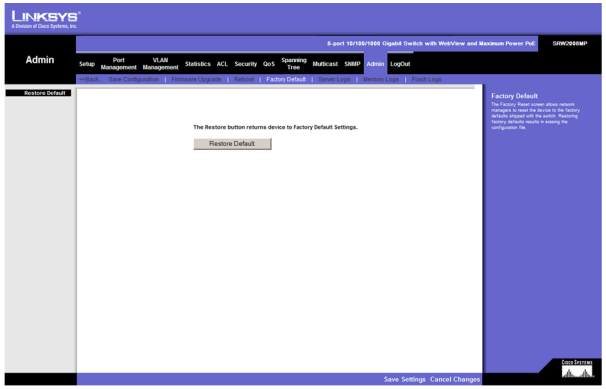


Abbildung 5-73: Admin – Factory Defaults (Werkseinstellungen)

Registerkarte „Admin“ – Server Logs

Der Bildschirm **Server Logs** enthält Informationen zum Anzeigen und Konfigurieren der Remote-Protokollserver. Sie können neue Protokollserver definieren und den Protokollschweregrad angeben, der an die einzelnen Server gesendet wird.

Server. Gibt den Server an, an den Protokolle gesendet werden können.

UDP Port (1 bis 65.535). Definiert den UDP-Anschluss, an den die Serverprotokolle gesendet werden. Der mögliche Bereich ist 1 bis 65.535. Der Standardwert ist 514.

Facility. Definiert eine benutzerdefinierte Anwendung, von der Systemprotokolle an den Remoteserver gesendet werden. Einem einzelnen Server kann dabei nur ein Element zugewiesen sein. Wenn Sie eine zweite Elementebene zuweisen, wird das erste Element außer Kraft gesetzt. Alle Anwendungen, die für ein Gerät definiert sind, verwenden auf einem Server dasselbe Element. Die Standardeinstellung des Felds ist **Local 7**. Mögliche Feldwerte sind **Local 0** bis **Local 7**.

Description. Stellt eine benutzerdefinierte Serverbeschreibung bereit.

Minimum Severity. Zeigt den minimalen Schweregrad an, für den Protokolle an den Server gesendet werden. Wenn Sie z. B. **Notice** auswählen, werden alle Protokolle ab dem Schweregrad **Notice** und höher an den Remoteserver gesendet.

Mit der Schaltfläche **Add to List** fügen Sie die Serverprotokollkonfiguration der **Server Log Table** unten auf dem Bildschirm hinzu.

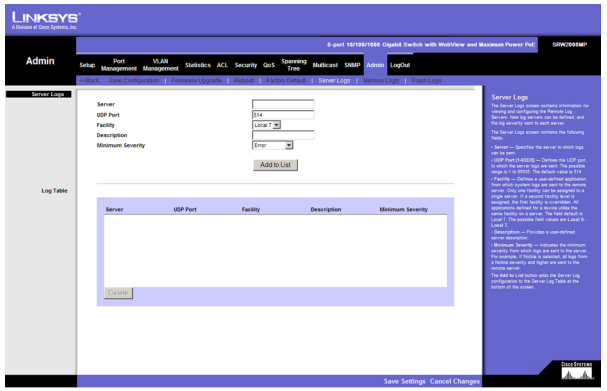


Abbildung 5-74: Admin – Server Logs (Serverprotokolle)

Registerkarte „Admin“ – Memory Logs

Der Bildschirm **Memory Log** enthält alle Systemprotokolle, die im Arbeitspeicher (Cache) gespeichert sind, in chronologischer Reihenfolge.

Log Index. Zeigt die Protokollnummer an.

Log Time. Zeigt den Zeitpunkt an, zu dem das Protokoll erzeugt wurde.

Severity. Zeigt den Schweregrad des Protokolls an.

Description. Zeigt den Text der Protokollmeldung an.

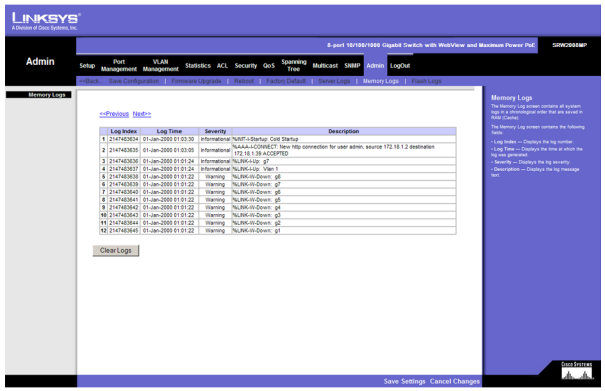


Abbildung 5-75: Admin – Memory Logs (Speicherprotokolle)

Registerkarte „Admin“ – Flash Logs

Der Bildschirm **Flash Log** enthält Informationen zu Protokolleinträgen, die unter FLASH in der Protokolldatei gespeichert wurden, z. B. den Zeitpunkt der Protokollerstellung, den Protokollschweregrad und eine Beschreibung der Protokollmeldung. Das Meldungsprotokoll (Message Log) ist nach dem Neustart verfügbar.

Log Index. Zeigt die Protokollnummer an.

Log Time. Zeigt den Zeitpunkt an, zu dem das Protokoll erzeugt wurde.

Severity. Zeigt den Schweregrad des Protokolls an.

Description. Zeigt den Text der Protokollmeldung an.

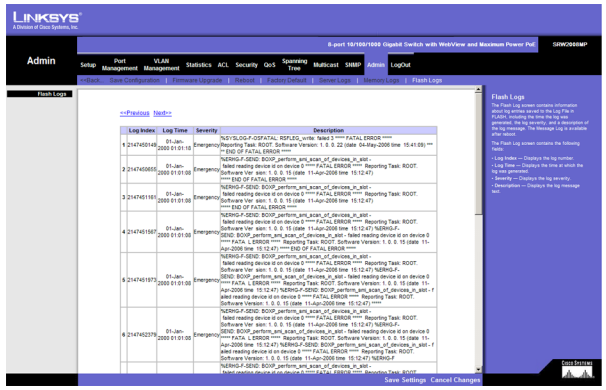


Abbildung 5-76: Admin – Flash Logs (Flashprotokolle)

Anhang A: Info zu Gigabit Ethernet und Glasfaserkabeln

Gigabit Ethernet

Gigabit Ethernet läuft mit einer Geschwindigkeit von 1 GBit/s (Gigabit pro Sekende) und damit zehn mal schneller als 100 MBit/s Fast Ethernet. Dennoch ist nach wie vor vollständige Kompatibilität mit Hardware von 100 MBit/s Fast Ethernet gewährleistet. Benutzer können Gigabit-Ethernet-Hardware entweder mit Glasfaserkabeln oder Kupferkabeln der Kategorie 5e anschließen. Glasfasern sind dabei besser für Netzwerk-Backbones geeignet. Durch die schrittweise Integration des Gigabit-Standards in bestehende Netzwerke erreichen derzeitige Computeranwendungen schnellere Zugriffszeiten für Netzwerkdaten, Hardware und Internetverbindungen.

Glasfaserkabel

Glasfaserkabel bestehen aus flexiblen, optisch effizienten Glasfasern, die mit einer Gummischicht überzogen sind. Glasfasern nutzen zum Senden und Empfangen von Daten Lichtphotonen anstelle von Elektronen. Mit Glasfasern lassen sich pro Sekunde theoretisch Datenmengen im Terabit-Bereich übertragen, doch die derzeit erhältliche Signalhardware kann pro Sekunde nur einige Gigabit verarbeiten.

Glasfaserkabel verfügen über zwei Arten von Hauptsteckern. Das am häufigsten verwendete Glasfaserkabel ist ein Multi-Mode-Glasfaserkabel mit einem 62,5 Mikrometer großen Glasfaserkern. Single-Mode-Glasfaserkabel sind um einiges effizienter als Multi-Mode-Kabel, aufgrund des kleineren optischen Kerns jedoch weitaus teurer. Dieser optische Kern bewahrt die Intensität übertragener Lichtsignale. Für eine Glasfaserverbindung sind zwei Glasfaserkabel erforderlich: eines der Kabel dient der Datenübertragung, das andere dem Datenempfang.

Jedes Glasfaserkabel verfügt über einen Stecker, der in einen Glasfaserkabelanschluss auf einem Netzerkadapter, Hub oder Switch eingesteckt werden kann. In den USA wird für die meisten dieser Kabel ein quadratischer SC-Stecker verwendet, der einrastet, wenn er in einen Anschluss gesteckt oder mit einem anderen Kabel verbunden wird. In Europa findet meist der abgerundete ST-Stecker Verwendung.

Verwenden Sie die MGBT1-, MGBSX1- oder MGBLH1-Mini-GBIC-Module von Linksys mit den Gigabit-Switches von Linksys. Für das MGBSX1- und das MGBLH1-Modul wird ein Glasfaserkabel mit LC-Steckern und für das MGBT1-Modul ein Ethernet-Kabel der Kategorie 5e mit einem RJ-45-Stecker benötigt.

Anhang B: Windows-Hilfe

Microsoft Windows ist für beinahe alle Netzwerkprodukte erforderlich. Windows ist das weltweit am häufigsten eingesetzte Betriebssystem und verfügt standardmäßig über zahlreiche Funktionen zur Vereinfachung des Netzwerkbetriebs. Diese Funktionen sind über die Windows-Hilfe aufrufbar und werden im vorliegenden Anhang beschrieben.

TCP/IP

Ein Computer kann erst bei aktiviertem TCP/IP innerhalb des Netzwerks kommunizieren. Bei TCP/IP handelt es sich um eine Reihe von Anweisungen oder ein Protokoll, die/das alle PCs zur Netzwerkkommunikation befolgen. Dies gilt ebenso für Wireless-Netzwerke. Die PCs können nicht über ein Wireless-Netzwerk kommunizieren, wenn TCP/IP nicht aktiviert ist. Die Windows-Hilfe beinhaltet vollständige Anweisungen zum Aktivieren von TCP/IP.

Freigegebene Ressourcen

Sofern Sie Drucker, Ordner oder Dateien zur gemeinsamen Verwendung über das Netzwerk freigeben möchten, erhalten Sie in der Windows-Hilfe umfassende Anweisungen zur Verwendung von freigegebenen Ressourcen.

Netzwerkumgebung

Andere Computer in Ihrem Netzwerk werden unter Netzwerkumgebung angegeben. Die Windows-Hilfe beinhaltet umfassende Anweisungen zum Hinzufügen von Computern zum Netzwerk.

Anhang C: Downloads mithilfe von Xmodem

Schritte im im Startmenü

Das Startmenü kann beim Hochfahren des Geräts aufgerufen werden. Ein zweites Zeitfenster steht zur Verfügung, um das Startmenü umgehend nach dem POST-Test zu starten. Auf das Menü kann direkt von einem mit dem Konsolenanschluss verbundenen Terminal zugegriffen werden. Die einzelnen Schritte im Startmenü können unter Verwendung des ASCII-Terminals oder des Windows-HyperTerminals ausgeführt werden.

Die Software wird bei Verfügbarkeit einer neuen Version heruntergeladen, um beschädigte Dateien zu ersetzen und die Systemsoftware zu aktualisieren. So laden Sie die Software über das Startmenü herunter:

So rufen Sie das Startmenü auf:

1. Schalten Sie Computer und Switch aus.
2. Verbinden Sie das vom COM-Anschluss am Computer reichende Null-Modem-Kabel mit dem Konsolenanschluss des Switches.
3. Schalten Sie den Computer ein, und starten Sie HyperTerminal. Beachten Sie dabei die Anweisungen in ***Kapitel 4: Verwenden der Konsolenschnittselle für die Konfiguration***, um HyperTerminal für die Herstellung einer Verbindung mit dem Switch zu konfigurieren.
4. Schalten Sie den Switch ein, und warten Sie, bis Sie eine Meldung erhalten, dass das Gerät automatisch hochgefahren wird:

   Autoboot in 2 seconds - press RETURN or Esc. to abort and enter prom.

5. Drücken Sie bei Erscheinen dieser Meldung die **EINGABETASTE**, um das Startmenü zu öffnen.

HINWEIS: Wird innerhalb von 35 Sekunden keine Auswahl getroffen (Standard), tritt eine Zeitüberschreitung ein, und die Verbindung zum Gerät muss zum erneuten Start des Vorgangs getrennt werden.

6. Wählen Sie die Option **[1] Download Software** aus. Daraufhin erscheint die Meldung *Downloading code using XMODEM*, wobei auf dem Bildschirm Zeichen angezeigt werden. Werden diese Schritte auf der nächsten Seite nicht ausgeführt, um die Datei für den Download innerhalb einer bestimmten Frist zu suchen, wird das Gerät zurückgesetzt.

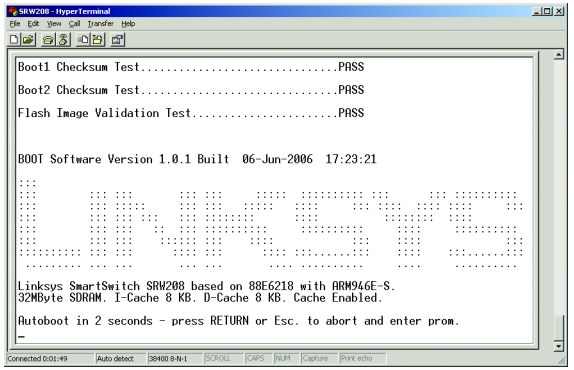


Abbildung C-1: Meldung zu autom. Hochfahren des Switches

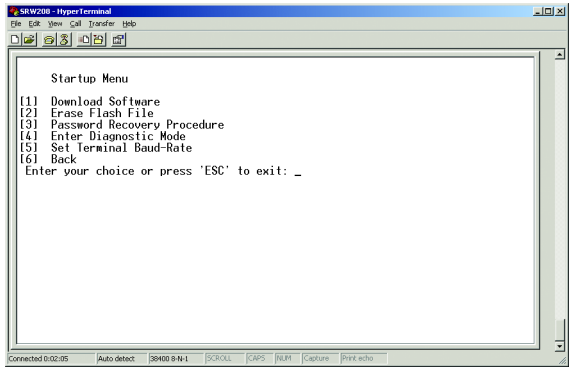


Abbildung C-2: Startmenü

7. Wählen Sie im Dropdownmenü *Transfer* die Option **Send File** aus.

8. Geben Sie im Feld *Filename:* den Pfad der herunterzuladenden Datei ein, oder klicken Sie zum Suchen der Datei auf **Browse**.

   Nur gültige Dateien mit einem „*.ros“- oder „*.rfb“-Suffix, die von Linksys bereitgestellt wurden, können heruntergeladen werden. Das Herunterladen ungültiger Dateien hat nicht vorhersehbare Auswirkungen zur Folge.

   Überprüfen Sie, ob im Feld *Protocol:* das Xmodem-Protokoll ausgewählt ist.

9. Drücken Sie nach dem Herunterladen der Software auf **Send**.

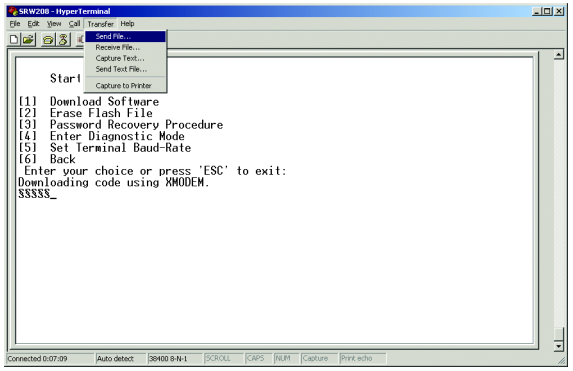


Abbildung C-3: Send File (Datei senden)

Nach dem Herunterladen der Software wird das Gerät automatisch neu hochgefahren.

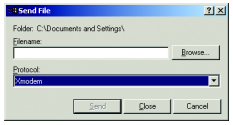


Abbildung C-4: Download

Anhang D: Glossar

Dieses Glossar beinhaltet einige grundlegende Begriffe aus dem Bereich Netzwerke, die Ihnen unter Umständen bei der Verwendung dieses Produkts begegnen. Spezielle Begriffe finden Sie im vollständigen Linksys-Glossar unter http://www.linksys.com/glossary.

Access Point – Ein Gerät, das Computern mit Wireless-Funktionen die Kommunikation mit einem Kabelnetzwerk ermöglicht. Wird auch zum Erweitern des Bereichs eines Wireless-Netzwerks verwendet.

ACE – Filter in Zugriffssteuerungslisten (Access Control Lists, ACL) zur Bestimmung des weiterzuleitenden Netzwerkdatenverkehrs. Ein ACE (Access Control Entry, Zugriffssteuerungseintrag) basiert auf den folgenden Kriterien:

- Protokoll
- Protocol-ID
- Quellanschluss
- Zielanschluss
- Platzhaltermaske
- Quell-IP-Adresse
- Ziel-IP-Adresse

ACL (Access **C**ontrol **L**ist**)** – Access Control Lists (dt.: Zugriffssteuerungslisten) dienen dem Gewähren, Verweigern oder Beschränken des Zugriffs auf Geräte, Funktionen oder Anwendungen.

Anschluss – Die Stelle an einem Computer oder einem Netzwerkgerät, in die Kabel oder Adapter eingesteckt werden.

Automatische Aushandlung – Ermöglicht 10/100 MBit/s oder 10/100/1000 MBit/s Ethernet-Anschlüssen das automatische Einrichten des optimalen Duplexmodus sowie optimaler Datenflusssteuerung und Geschwindigkeit.

Bandbreite – Die Übertragungskapazität eines bestimmten Geräts oder Netzwerks.

Bandbreitenzuweisung – Zeigt die einer bestimmten Anwendung, einem Benutzer und/oder einer Benutzeroberfläche zugewiesene Bandbreite an.

Baud – Zeigt die Anzahl der im Sekundentakt übertragenen Signalelemente an.

Best Effort – Bedeutet, dass Datenverkehr der Warteschlange mit der geringsten Priorität zugewiesen wird und Paketübertragung nicht gewährleistet ist.

Bit – Eine binäre Ziffer.

Bridge – (dt. „Brücke“) Ein Gerät, mit dem zwei Netzwerke miteinander verbunden werden. Eine Bridge ist hardwarespezifisch, jedoch protokollabhängig. Bridges werden auf Layer 1- und Layer 2-Ebenen ausgeführt.

Broadcastdomäne – Geräte, die von einem beliebigen Gerät in einem angegebenen Satz ausgehende Broadcastrahmen empfangen. Router binden Broadcastdomänen, da Router keine Broadcastrahmen weiterleiten.

Broadcaststurm – Tritt auf, wenn eine sehr große Anzahl von Broadcastmeldungen gleichzeitig im gesamten Netzwerk über einen Anschluss übertragen wird. Weitergeleitete Antworten auf Meldungen werden im Netzwerk angehäuft und sorgen für eine Überlastung der Netzwerkressourcen oder eine Zeitüberschreitung des Netzwerks.

Browser – Ein Anwendungsprogramm zur Betrachtung von und Interaktion mit Informationen aus dem World Wide Web.

Bündelung – Link Aggregation. Optimiert die Anschlussverwendung durch Zusammenfassen einer Gruppe von Anschlüssen zur Bildung einer einzelnen Bündelung (zusammengefasste Gruppen).

Burst – Schnellere Paketübertragung im Vergleich zur normalen Übertragungsrate. Bursts sind zeitlich begrenzt und treten nur unter bestimmten Bedingungen auf.

Burstgröße – Bezeichnet die Burstgröße, die Pakete mit einer höheren als der normalen Geschwindigkeit überträgt.

Byte – Eine Dateneinheit, die in der Regel eine Länge von acht Bit aufweist

CBS (**C**ommitted **B**urst **S**ize) – Bezeichnet die maximale Anzahl von Datenbits, die in einem bestimmten Zeitintervall übertragen werden.

CIR (**C**ommitted **I**nformation **R**ate) – Für die Datenrate wird über ein Mindestzeitintervall ein Durchschnittswert ermittelt.

Communities – Eine Gruppe von Benutzern, die identische Systemzugriffsrechte behält.

CoS (**C**lass **o**f **S**ervice) – Das 802.1p-Prioritätsschema. CoS bietet Möglichkeiten zum Kennzeichnen von Paketen mit Prioritätsinformationen. Dem Layer II-Paketkopf wird ein CoS-Wert zwischen 0-7 hinzugefügt, wobei 0 die niedrigste und 7 die höchste Priorität ist.

Datenflusssteuerung – Ermöglicht langsameren Geräten die Kommunikation mit schnelleren Geräten. Dies wird dadurch ermöglicht, dass das schnellere Gerät das Senden von Datenpaketen unterlässt.

DDNS (**D**ynamic **D**omain **N**ame **S**ystem) – Ermöglicht das Hosten einer Website oder eines FTP- oder E-Mail-Servers mit einem festen Domänennamen (z. B. www.xyz.com) und einer dynamischen IP-Adresse.

DHCP (**D**ynamic **H**ost **C**onfiguration **P**rotocol) – Ein Netzwerkprotokoll, mit dem Administratoren Netzwerkcomputern durch befristetes „Vermieten“ einer IP-Adresse an Benutzer temporäre anstelle von ständigen IP-Adressen zuweisen können.

DHCP-Clients – Ein Internethost, der DHCP zum Abrufen von Konfigurationsparametern wie Netzwerkadressen verwendet.

DHCP-Server – Ein Internethost, der DHCP-Clients Konfigurationsparameter zurückgibt.

DNS (**D**omain **N**ame **S**erver) – Die IP-Adresse des Internetdienstanbieter-Servers, mit dem die Namen von Websites in IP-Adressen übersetzt werden.

Domäne – Ein bestimmter Name für ein Computernetzwerk.

Download – Empfang einer über ein Netzwerk übertragenen Datei.

DSCP (**D**iff**S**erve **C**ode **P**oint) bietet eine Methode zum Kennzeichnen von IP-Paketen mit QoS-Prioritätsinformationen.

DSL (**D**igital **S**ubscriber **L**ine) – Eine ständig aktive Breitbandverbindung über herkömmliche Telefonleitungen.

Durchsatz – Die innerhalb eines bestimmten Zeitraums erfolgreich zwischen Knoten übertragene Datenmenge.

Dynamische IP-Adresse – Eine durch einen DHCP-Server zugewiesene temporäre IP-Adresse.

EIGRP (**E**nhanced **I**nterior **G**ateway **R**outing **P**rotocol) – Bietet schnelle Konvergenz und unterstützt Subnetzmasken mit variabler Länge und mehrere Netzwerk-Layerprotokolle.

Ethernet – IEEE-Standardnetzwerkprotokoll, mit dem angegeben wird, wie Daten auf einem gängigen Übertragungsmedium angeordnet und von diesem abgerufen werden.

Firmware – Der Programmierungscode, mit dem ein Netzwerkgerät ausgeführt wird.

FTP (**F**ile **T**ransfer **P**rotocol) – Ein Protokoll zur Übertragung von Dateien über ein TCP/IP-Netzwerk.

GARP (**G**eneral **A**ttributes **R**egistration **P**rotocol) – Registriert Clientstationen in einer Multicastdomäne.

Gateway – Ein Gerät, mit dem Netzwerke mit anderen, nicht kompatiblen Kommunikationsprotokollen verbunden werden.

GBIC (**G**iga**B**it **I**nterface **C**onverter) – Ein Hardwaremodul zum Anschließen von Netzwerkgeräten an glasfaserbasierte Übertragungssysteme. GBIC konvertiert die seriellen elektrischen Signale in serielle optische Signale und umgekehrt.

Gegendruck – Ein mit dem Halbduplexmodus verwendeter Mechanismus, der einem Anschluss ermöglicht, eine Meldung nicht zu empfangen.

Großrahmen – Dienen dem Transport von identischen Daten in einer geringeren Anzahl von Rahmen. Großrahmen senken den Overhead, die Verarbeitungszeit und die Anzahl der Unterbrechungen.

GVRP (**G**ARP **V**LAN **R**egistration **P**rotocol) – Registriert Clientstationen in VLANs.

Halbduplex – Datenübertragung, die über eine Leitung in zwei Richtungen abgewickelt werden kann. Allerdings ist die Übertragung jeweils nur in eine Richtung möglich.

HTTP (**H**yper**T**ext **T**ransport **P**rotocol) – Das zum Herstellen einer Verbindung zu Servern im Internet verwendete Kommunikationsprotokoll.

HTTPS (**H**yper**T**ext **T**ransport **P**rotocol **S**ecure) – Eine Erweiterung des standardmäßigen HTTP-Protokolls zur Erhöhung der Sicherheit durch Verschlüsseln des Datenverkehrs von einer Website. Standardmäßig verwendet dieses Protokoll den TCP-Anschluss 443.

ICMP (Internet **C**ontrol **M**essage **P**rotocol) – Ermöglicht dem Gateway oder dem Zielhost die Kommunikation mit dem Ausgangshost. Beispiel: Melden eines Verarbeitungsfehlers.

IGMP (**I**nternet **G**roup **M**anagement **P**rotocol) – Ermöglicht Hosts die Benachrichtigung des lokalen Switches oder Routers, dass Übertragungen, die einer bestimmten Multicastgruppe zugewiesen sind, empfangen werden sollen.

IP (**I**nternet **P**rotocol) – Ein Protokoll zum Senden von Daten über ein Netzwerk.

IP-Adresse – Die zum Identifizieren eines Computers oder Geräts in einem Netzwerk verwendete Adresse.

IPCONFIG – Ein Dienstprogramm in Windows 2000 und XP zum Anzeigen der IP-Adresse eines bestimmten Netzwerkgeräts.

IPSec (**I**nternet **P**rotocol **Sec**urity) – Ein VPN-Protokoll, mit dem der sichere Austausch von Paketen auf IP-Ebene implementiert wird.

ISP (**I**nternet **S**ervice **P**rovider) – Ein Unternehmen, das den Zugriff auf das Internet bereitstellt.

Kabelmodem – Ein Gerät, das einen Computer mit dem Kabelfernsehen verbindet, welches wiederum eine Verbindung zum Internet herstellt.

Klassenzuordnungen – Ein Teil des Quality of Service-Systems, der aus einer IP-Zugriffssteuerungsliste und/oder einer MAC-Zugriffssteuerungsliste besteht. Klassenzuordnungen werden so konfiguriert, dass sie den Paketkriterien entsprechen, und die werden per „First-Fit“ mit den Paketen abgeglichen.

Kombinationsanschlüsse – Ein einzelner logischer Anschluss mit zwei physischen Verbindungen, einschließlich einer RJ-45- und einer SFP-Verbindung.

LAG (**L**ink **A**ggregated **G**roup) – Fasst Anschlüsse oder VLANs zu einem virtuellen Anschluss oder VLAN zusammen.

LAN – Die ein lokales Netzwerk bildenden Computer und Netzwerkgeräte.

Lautet die Ziel-IP-Adresse 149.36.184.198 und die Platzhaltermaske 255.36.184.00, werden die ersten beiden Abschnitte der IP-Adresse verwendet und die letzten beiden Abschnitte ignoriert.

MAC (**M**edia **A**ccess **C**ontrol)-**Adresse** – Die eindeutige Adresse, die ein Hersteller jedem Netzwerkgerät zuweist.

Maske – Ein Filter, der bestimmte Werte ein- bzw. ausschließt (z. B. Teile einer IP-Adresse).

MBit/s (**M**ega**b**it **P**ro **S**ekunde) – Eine Million Bit pro Sekunde; eine Einheit zur Messung der Datenübertragung.

MD5 (**M**essage **D**igest **5**) – Ein Algorithmus, der einen 128-Bit-Hash erzeugt. MD5 ist eine Variante von MD4 und erhöht die MD4-Sicherheit. MD5 überprüft die Integrität der Kommunikation und authentifiziert den Ursprung der Kommunikation.

MDI (**M**edia **D**ependent **I**nterface) – Ein für Endstationen verwendetes Kabel.

MDIX (**M**edia **D**ependent **I**nterface with Crossover) – Ein für Hubs und Switches verwendetes Kabel.

MIB (**M**anagement **I**nformation **B**ase) – MIBs beinhalten Informationen zu bestimmten Aspekten von Netzwerkkomponenten.

Multicast – Überträgt Kopien eines Einzelpakets an mehrere Anschlüsse.

Netzwerk – Mehrere Computer oder Geräte, die zur Datenfreigabe, -speicherung und/oder -übertragung zwischen Benutzern miteinander verbunden sind.

NMS (**N**etwork **M**anagement **S**system) – Eine Benutzeroberfläche, über die ein System verwaltet werden kann.

OID (**O**bject **Id**entifier) – Wird von SNMP zum Identifizieren von verwalteten Objekten verwendet. In einem SNMP-Manager/-Agent-Netzwerkverwaltungsmodell muss jedes verwaltete Objekt zur Identifizierung über eine OID verfügen.

Paket – Eine über ein Netzwerk gesendete Dateneinheit.

Ping (**P**acket **IN**ternet **G**roper) – Ein Internetdienstprogramm, mit dem bestimmt wird, ob eine bestimmte IP-Adresse online ist.

Platzhaltermaske – Gibt an, welche IP-Adressabschnitte verwendet und welche ignoriert werden. Die Platzhaltermaske 255.255.255.255 zeigt an, dass kein Bit wichtig ist. Die Platzhaltermaske 0.0.0.0 zeigt an, dass alle Bits wichtig sind.

Port Mirroring – (dt: „Anschlussspiegelung“) Überwacht und spiegelt Netzwerkdatenverkehr durch Weiterleiten von Kopien ein- und ausgehender Pakete von einem Anschluss zu einem Überwachungsanschluss.

Power **o**ver **E**thernet (**PoE**) – Eine Technologie zur Übertragung von Daten und Strom über ein Ethernet-Netzwerkkabel.

QoS (**Q**uality **o**f **S**ervice) – Bietet Richtlinien mit Filtersätzen (Regeln). Mit QoS können Netzwerkverwalter entscheiden, wie und welche Art von Netzwerkdatenverkehr gemäß Prioritäten, Anwendungstypen sowie Ausgangs- und Zieladressen weitergeleitet wird.

RADIUS (**R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice) – Ein Protokoll, das zur Steuerung des Netzwerkzugriffs einen Authentifizierungsserver verwendet.

RJ-45 (**R**egistered **J**ack-**45**) – Ein Ethernet-Stecker mit bis zu acht Kontaktstellen.

RMON (Remote Monitoring) – Stellt Netzwerkinformationen bereit, die von einer Arbeitsstation abgerufen werden.

Router – Ein Netzwerkgerät, mit dem mehrere Netzwerke miteinander verbunden werden.

RSTP (**R**apid **S**panning **T**ree **P**rotocol) – Erkennt und verwendet Netzwerktopologien, die eine schnellere Konvergenz der umfassenden Struktur ohne Erstellen von Weiterleitungsschleifen ermöglichen.

Server – Jeder beliebige Computer, dessen Funktion in einem Netzwerk darin besteht, dem Benutzer Zugriff auf Dateien sowie verschiedene Geräte wie Druck- und Kommunikationsgeräte zu verschaffen.

SMTP (**S**imple **M**ail **T**ransfer **P**rotocol) – Das standardmäßige E-Mail-Protokoll im Internet.

SNMP (**S**imple **N**etwork **M**anagement **P**rotocol) – Ein häufig verwendetes Protokoll zur Netzwerküberwachung und -steuerung.

SSH – Secure Shell. Ein Dienstprogramm, das sichere Authentifizierung und Kommunikation bei der Anmeldung an einem anderen Computer über ein Netzwerk verwendet.

SSL (**S**ecure **S**ocket **L**ayer) – Eine Verschlüsselungstechnologie für das Internet, das für sichere Transaktionen, wie die Übertragung von Kreditkartennummern für e-commerce, verwendet wird.

Standardgateway – Ein Gerät, mit dem Internetdatenverkehr von einem LAN weitergeleitet wird.

Starten – Zum Starten eines Geräts und der Ausführungsanweisungen.

Statische IP-Adresse – Eine feste einem Computer oder Gerät zugewiesene Adresse, die mit einem Netzwerk verbunden ist.

STP (**S**panning **T**ree **P**rotocol) – Verhindert Schleifen im Netzwerkdatenverkehr. Das Spanning Tree Protocol (STP) verfügt über eine Strukturtopographie für eine beliebige Anordnung von Bridges. STP stellt einen Pfad zwischen Endstationen in einem Netzwerk her und entfernt dadurch Schleifen.

Subnetz (**Sub**-**net**work) – Subnetze sind Teile eines Netzwerks, die eine gemeinsame Adresskomponente verwenden. In TCP/IP-Netzwerken sind Geräte, die gemeinsam ein Präfix verwenden, Teil desselben Subnetzes. Beispielsweise sind alle Geräte mit dem Präfix 157.100.100.100 Teil desselben Subnetzes.

Subnetzmaske – Ein Adresscode zur Bestimmung der Größe des Netzwerks.

Switch – Ein Switch filtert Pakete zwischen LAN-Segmenten und leitet diese weiter. Switches unterstützen alle Paketprotokolltypen.

TACACS+ (**T**erminal **A**ccess **C**ontroller **A**ccess **C**ontrol **S**ystem **Plus**) – Von Cisco bereitgestellte proprietäre Erweiterung des Terminal Access Controller Access Control System (TACACS). Bietet zusätzliche Unterstützung für Authentifizierung, Autorisierung und Kontoführung.

TCP (**T**ransmission **C**ontrol **P**rotocol) – Ein Netzwerkprotokoll für die Datenübertragung, das eine Bestätigung des Empfängers der gesendeten Daten erfordert.

TCP/IP (**T**ransmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol) – Ein Anweisungssatz, der von PCs zur Kommunikation über ein Netzwerk verwendet wird.

Telnet – Ein Benutzerbefehl- und TCP/IP-Protokoll für den Zugriff auf Remote-PCs.

TFTP (**T**rivial **F**ile **T**ransfer **P**rotocol) – Eine Version des TCP/IP-FTP-Protokolls, die über keine Verzeichnis- oder Kennwortfunktionen verfügt.

TX Rate – Übertragungsrate.

Überwachung – Bestimmt, ob die Datenverkehrsebenen innerhalb eines angegebenen Profils liegen. Mit Überwachungsfunktionen wird die maximale Datenverkehrsrate zum Senden oder Empfangen von Paketen auf einer Benutzeroberfläche verwaltet.

UDP (**U**ser **D**ata **P**rotocol) – Kommunikationsprotokoll, das Pakete überträgt, jedoch nicht deren Zustellung gewährleistet.

Upgrade – Ersetzen einer vorhandenen Software oder Firmware mit einer aktuelleren Version.

Upload – Übertragung einer Datei über ein Netzwerk.

URL (**U**niform **R**esource **L**ocator) – Die Adresse einer Datei im Internet.

Verschlüsselung – Verschlüsseln von in einem Netzwerk übertragenen Daten.

VLAN (**W**ireless **L**ocal **A**rea **N**etwork) – Logische Untergruppen, die ein lokales Netzwerk (LAN) bilden. VLANs werden in der Regel mithilfe von Software und nicht in Form einer Hardwarelösung angelegt.

Vollduplex – Die Fähigkeit eines Netzwerkgeräts zum gleichzeitigen Empfangen und Übertragen von Daten.

WAN (**W**ide **A**rea **N**etwork) – Netzwerke, die einen großen geografischen Bereich abdecken.

Zugriffsmodus – Bezeichnet die Methode, mit der Benutzern Zugriff auf das System gewährt wird.

Zugriffsprofile – Ermöglicht Netzwerkverwaltern das Definieren von Profilen und Regeln für den Zugriff auf das Gerät. Der Zugriff auf Verwaltungsfunktionen kann auf Benutzergruppen beschränkt werden, die nach folgenden Kriterien definiert werden:

- Zugangsschnittstellen.
- Quell-IP-Adresse und/oder Quell-IP-Subnetze.

Anhang E: Technische Daten

SRW2008

Modell	SRW2008
Anschlüsse	8 RJ-45-Stecker für 10BASE-T/100BASE-TX/1000Base-T mit 2 freigegebenen SFP-Anschlüssen auf Anschluss 7 und 8 (Kombinationsanschluss) Konsolenanschluss Auto MDI/MDI-X Automatische Aushandlung/Manuell – Einstellung
Verkabelungstyp	Mindestens UTP CAT 5 für 10BASE-T/100BASE-TX bzw. mindestens UTP CAT 5e für 1000BASE-T
LEDs	Link/Act, Gigabit-Geschwindigkeit, System
Leistung	
Switchkapazität	16 GB nicht blockierend
Weiterleitungsrate	11,9 MPPS Wire-Speed (Weiterleitung der Daten mit Leitungsgeschwindigkeit
Layer 2	
Größe MAC-Tabelle	8K
Anzahl der VLANs	256 aktive VLANs (4096 – Bereich)
VLAN	Anschluss- und tagbasierte 802.1Q-VLANs Verwaltungs-VLAN
HOL Blocking	Verhinderung von Head Of Line Blocking

Management

Webbenutzeroberfl.	Integriert in Webbenutzeroberfläche für einfache browserbasierte Konfiguration (HTTP/HTTPS)
SNMP	SNMP-Version v1, v2c, v3 mit Unterstützung für Traps
SNMP MIBs	RFC1213 MIB-2, RFC2863 Interface MIB, RFC2665 Ether-like MIB, RFC1493 Bridge MIB, RFC2674 Extended Bridge MIB (P-bridge, Q-bridge), RFC2819 RMON MIB (nur Gruppen 1, 2, 3, 9), RFC2737 Entity MIB, RFC 2618 RADIUS Client MIB RFC 1215 Traps
RMON	Der eingebettete Remote-Monitoring (RMON)-Softwareagent unterstützt vier RMON-Gruppen (Verlauf, Statistik, Alarme und Ereignisse) für erweiterte Datenverkehrverwaltung, Überwachung und Analyse.
Firmwareaktualis.	Aktualisierung mit Web-Browser (HTTP) und über TFTP
Port Mirroring	Der Datenverkehr auf einem Anschluss lässt sich zur Analyse mit einer Netzwerk-Analysefunktion oder einem RMON-Probe auf einen anderen Anschluss spiegeln.
Verwaltung, sonstige	Traceroute Secure Socket Layer (SSL) Secure Shell (SSH) RADIUS Port Mirroring TFTP-Aktualisierung SSL-Sicherheit für Webbenutzeroberfläche DHCP-Clienttabelle BootP SNTP Xmodem-Aktualisierung Cable Diagnostics (Kabeldiagnose) PING Telnet-Client (sichere SSH-Unterstützung)

Sicherheit

IEEE 802.1x	802.1x – RADIUS-Authentifizierung. MD5-Verschlüsselung
Zugriffsteuerung	ACLs – Drop- oder Ratenbeschränkung basierend auf: Quell- und Zieladresse – MAC-basiert Quell- und Ziel-IP-Adresse Protokoll TOS/DSCP Anschluss VLAN Ethertype

Verfügbarkeit

Link Aggregation	Link Aggregation mit IEEE 802.3ad LACP Bis zu acht Anschlüsse in max. acht Gruppen
Storm Control	Broadcast, Multicast und Unknown Unicast
Spanning Tree	IEEE 802.1D Spanning Tree, IEEE 802.1w Rapid Spanning Tree, IEEE 802.1s Multiple Spanning Tree
IGMP Snooping	IGMP (v1/v2) Snooping überträgt hohe Bandbreiten beanspruchenden Videodatenverkehr ausschließlich an die Anfordernden. Unterstützung von 256 Multicastgruppen.

QoS

Prioritätsstufen	4 Hardware-Warteschlangen
Planung	Priority Queueing und Weighted Round Robin (WRR)
Class of Service	Anschlussbasiert Auf Basis von 802.1p-VLAN-Priorität Auf Basis von IPv4/v6 IP Precedence/TOS/DSCP

	Auf Basis von TCP/UDP-Anschluss Diffserv Zugriffsteuerungslisten für Klassifizierungen und Anmerkungen
Ratenbeschränkung	Zugangsüberwachung Ausgangsratensteuerung
Standards	802.3 10BASE-T Ethernet, 802.3u 100BASE-TX Fast Ethernet, 802.3ab 1000BASE-T Gigabit Ethernet, 802.3z Gigabit Ethernet, 802.3x-Datenflusssteuerung, 802.3 ad LACP, 802.1d STP, 802.1Q/p VLAN, 802.1w Rapid STP, 802.1s Multiple STP, 802.1x Port Access Authentication
Umgebung	
Abmessungen	279 mm x 44 x 170 mm
Gewicht	1 kg
Stromversorg.	Externer Wechselstromadapter
Zertifizierung	FCC Part15 Class A, CE Class A, UL, cUL, CE mark, CB
Betriebstemp.	0 ºC bis 40 ºC
Aufbewahrungstemp.	-20 ºC bis 70 ºC
Luftfeucht. b. Betrieb	10 % bis 90 %
Luftf. bei Aufbew.	10 % bis 95 %

SRW2008MP

Anschlüsse	8 RJ-45-Stecker für 10BASE-T/100BASE-TX/1000Base-T mit 2 freigegebenen SFP-Anschlüssen auf Anschluss 7 und 8 (Kombinationsanschluss) Konsolenanschluss Auto MDI/MDI-X Automatische Aushandlung/Manuell – Einstellung
Verkabelungstyp	Mindestens UTP CAT 5 für 10BASE-T/100BASE-TX bzw. mindestens UTP CAT 5e für 1000BASE-T
LEDs	Link/Act, PoE, System
POE	802.3af-kompatibel. Bietet ein IEEE-Standardmaximum von 15,4 W auf acht 10/100-Anschlüssen
Leistung	
Switchkapazität	16 GB nicht blockierend
Weiterleitungsrate	11,9 MPPS Wire-Speed (Weiterleitung der Daten mit Leitungsgeschwindigkeit
Layer 2	
Größe MAC-Tabelle	8K
Anzahl der VLANs	256 aktive VLANs (4096 – Bereich)
VLAN	Anschluss- und tagbasierte 802.1Q-VLANs Verwaltungs-VLAN
HOL Blocking	Verhinderung von Head Of Line Blocking
Management	
Webbenutzeroberfl.	Integriert in Webbenutzeroberfläche für einfache browserbasierte Konfiguration (HTTP/HTTPS)

SNMP	SNMP-Version v1, v2c, v3 mit Unterstützung für Traps
SNMP MIBs	RFC1213 MIB-2, RFC2863 Interface MIB, RFC2665 Ether-like MIB, RFC1493 Bridge MIB, RFC2674 Extended Bridge MIB (P-bridge, Q-bridge), RFC2819 RMON MIB (nur Gruppen 1, 2, 3, 9), RFC2737 Entity MIB, RFC 2618 RADIUS Client MIB RFC 1215 Traps
RMON	Der eingebettete Remote-Monitoring (RMON)-Softwareagent unterstützt vier RMON-Gruppen (Verlauf, Statistik, Alarme und Ereignisse) für erweiterte Datenverkehrssteuerung, Überwachung und Analyse.
Firmwareaktualis.	Aktualisierung mit Web-Browser (HTTP) und über TFTP
Port Mirroring	Der Datenverkehr auf einem Anschluss lässt sich zur Analyse mit einer Netzwerk-Analysefunktion oder einem RMON-Probe auf einen anderen Anschluss spiegeln.
Verwaltung, sonstige	Traceroute Secure Socket Layer (SSL) Secure Shell (SSH) RADIUS Port Mirroring TFTP-Aktualisierung SSL-Sicherheit für Webbenutzeroberfläche DHCP-Clienttabelle BootP SNTP Xmodem-Aktualisierung Cable Diagnostics (Kabeldiagnose) PING Telnet-Client (sichere SSH-Unterstützung)

Sicherheit

IEEE 802.1x	802.1x – RADIUS-Authentifizierung. MD5-Verschlüsselung

Zugriffsteuerung	ACLs – Drop- oder Ratenbeschränkung basierend auf: Quell- und Zieladresse – MAC-basiert Quell- und Ziel-IP-Adresse Protokoll TOS/DSCP Anschluss VLAN Ethertype

Verfügbarkeit

Link Aggregation	Link Aggregation mit IEEE 802.3ad LACP Bis zu acht Anschlüsse in max. acht Gruppen
Storm Control	Broadcast, Muticast und Unknown Unicast
Spanning Tree	IEEE 802.1D Spanning Tree, IEEE 802.1w Rapid Spanning Tree, IEEE 802.1s Multiple Spanning Tree
IGMP Snooping	IGMP (v1/v2) Snooping überträgt hohe Bandbreiten beanspruchenden Videodatenverkehr ausschließlich an die Anfordernden. Unterstützung von 256 Multicastgruppen.

QoS

Prioritätsstufen	4 Hardware-Warteschlangen
Planung	Priority Queueing und Weighted Round Robin (WRR)
Class of Service	Anschlussbasiert Auf Basis von 802.1p-VLAN-Priorität Auf Basis von IPv4/v6 IP Precedence/TOS/DSCP Auf Basis von TCP/UDP-Anschluss Diffserv Zugriffsteuerungslisten für Klassifizierungen und Anmerkungen

Ratenbeschränkung	Zugangsüberwachung Ausgangsratensteuerung
Standards	802.3 10BASE-T Ethernet, 802.3u 100BASE-TX Fast Ethernet, 802.3ab 1000BASE-T Gigabit Ethernet, 802.3z Gigabit Ethernet, 802.3x-Datenflusssteuerung, 802.3 ad LACP, 802.3af POE, 802.1d STP, 802.1Q/p VLAN, 802.1w Rapid STP, 802.1s Multiple STP, 802.1x Port Access Authentication

Umgebung

Abmessungen	279 mm x 44 x 170 mm
Gewicht	1,2 kg
Stromversorg.	Externe Wechselstromadapter
Zertifizierungen	FCC Part15 Class A, CE Class A, UL, cUL, CE mark, CB
Betriebstemp.	0 ºC bis 40 ºC
Aufbewahrungstemp.	-20 ºC bis 70 ºC
Luftfeucht. bei Betr.	10 % bis 90 %, nicht kondensierend
Luftf. bei Aufbew.	10 % bis 95 %, nicht kondensierend

SRW2008P

Anschlüsse	8 RJ-45-Stecker für 10BASE-T/100BASE-TX/1000Base-T mit 2 freigegebenen SFP-Anschlüssen auf Anschluss 7 und 8 (Kombinationsanschluss) Konsolenanschluss Auto MDI/MDI-X Automatische Aushandlung/Manuell – Einstellung
Verkabelungstyp	Mindestens UTP CAT 5 für 10BASE-T/100BASE-TX bzw. mindestens UTP CAT 5e für 1000BASE-T
LEDs	Link/Act, PoE, System
POE	802.3af-kompatibel. Bietet ein IEEE-Standardmaximum von 15,4 W auf vier 10/100/1000-Anschlüssen oder von 7,5 W auf acht 10/100/1000-Anschlüssen

Leistung

Switchkapazität	16 GB nicht blockierend
Weiterleitungsrate	11,9 MPPS Wire-Speed (Weiterleitung der Daten mit Leitungsgeschwindigkeit

Layer 2

Größe MAC-Tabelle	8K
Anzahl der VLANs	256 aktive VLANs (4096 – Bereich)
VLAN	Anschluss- und tagbasierte 802.1Q-VLANs Verwaltungs-VLAN
HOL Blocking	Verhinderung von Head Of Line Blocking

Management

Webbenutzeroberfl.	Integriert in Webbenutzeroberfläche für einfache browserbasierte Konfiguration (HTTP/HTTPS)
SNMP	SNMP-Version v1, v2c, v3 mit Unterstützung für Traps
SNMP MIBs	RFC1213 MIB-2, RFC2863 Interface MIB, RFC2665 Ether-like MIB, RFC1493 Bridge MIB, RFC2674 Extended Bridge MIB (P-bridge, Q-bridge), RFC2819 RMON MIB (nur Gruppen 1, 2, 3, 9), RFC2737 Entity MIB, RFC 2618 RADIUS Client MIB RFC 1215 Traps
RMON	Der eingebettete Remote-Monitoring (RMON)-Softwareagent unterstützt vier RMON-Gruppen (Verlauf, Statistik, Alarme und Ereignisse) für erweiterte Datenverkehrssteuerung, Überwachung und Analyse.
Firmwareaktualis.	Aktualisierung mit Web-Browser (HTTP) und über TFTP
Port Mirroring	Der Datenverkehr auf einem Anschluss lässt sich zur Analyse mit einer Netzwerk-Analysefunktion oder einem RMON-Probe auf einen anderen Anschluss spiegeln.
Verwaltung, sonstige	Traceroute Secure Socket Layer (SSL) Secure Shell (SSH) RADIUS Port Mirroring TFTP-Aktualisierung SSL-Sicherheit für Webbenutzeroberfläche DHCP-Clienttabelle BootP SNTP Xmodem-Aktualisierung Cable Diagnostics (Kabeldiagnose) PING Telnet-Client (sichere SSH-Unterstützung)

Sicherheit

IEEE 802.1x	802.1x – RADIUS-Authentifizierung. MD5-Verschlüsselung
Zugriffsteuerung	ACLs – Drop- oder Ratenbeschränkung basierend auf: Quell- und Zieladresse – MAC-basiert Quell- und Ziel-IP-Adresse Protokoll TOS/DSCP Anschluss VLAN Ethertype

Verfügbarkeit

Link Aggregation	Link Aggregation mit IEEE 802.3ad LACP Bis zu acht Anschlüsse in max. acht Gruppen
Storm Control	Broadcast, Muticast und Unknown Unicast
Spanning Tree	IEEE 802.1D Spanning Tree, IEEE 802.1w Rapid Spanning Tree, IEEE 802.1s Multiple Spanning Tree
IGMP Snooping	IGMP (v1/v2) Snooping überträgt hohe Bandbreiten beanspruchenden Videodatenverkehr ausschließlich an die Anfordernden. Unterstützung von 256 Multicastgruppen.

QoS

Prioritätsstufen	4 Hardware-Warteschlangen
Planung	Priority Queueing und Weighted Round Robin (WRR)
Class of Service	Anschlussbasiert Auf Basis von 802.1p-VLAN-Priorität Auf Basis von IPv4/v6 IP Precedence/TOS/DSCP

	Auf Basis von TCP/UDP-Anschluss Diffserv Zugriffsteuerungslisten für Klassifizierungen und Anmerkungen
Ratenbeschränkung	Zugangsüberwachung Ausgangsratensteuerung
Standards	802.3 10BASE-T Ethernet, 802.3u 100BASE-TX Fast Ethernet, 802.3ab 1000BASE-T Gigabit Ethernet, 802.3z Gigabit Ethernet, 802.3x-Datenflusssteuerung, 802.3 ad LACP,802.3af POE, 802.1d STP, 802.1Q/p VLAN, 802.1w Rapid STP, 802.1s Multiple STP, 802.1x Port Access Authentication

Umgebung

Abmessungen	279 mm x 44 x 170 mm
Gewicht	1,2 kg
Stromversorg.	Externe Wechselstromadapter
Zertifizierungen	FCC Part15 Class A, CE Class A, UL, cUL, CE mark, CB
Betriebstemp.	0 ºC bis 40 ºC
Aufbewahrungstemp.	-20 ºC bis 70 ºC
Luftfeucht. bei Betr.	10 % bis 90 %, nicht kondensierend
Luftf. bei Aufbew.	10 % bis 95 %, nicht kondensierend

Anhang F: Gewährleistungsinformationen

Linksys garantiert seinen Kunden, dass bei dem Linksys-Produkt für einen Zeitraum von drei Jahren (die „Gewährleistungsfrist“) bei ordnungsgemäßer Verwendung hinsichtlich Material und Verarbeitungsqualität im Wesentlichen keine Mängel auftreten.

Sie erhalten ein exklusives Recht auf Nachbesserung, dabei steht es Linksys hinsichtlich der Haftungspflicht im Rahmen der Gewährleistung frei, das Produkt in Stand zu setzen oder den Kaufpreis abzüglich Nachlässen zu erstatten. Diese begrenzte Gewährleistung gilt nur für den Erstkäufer.

Weist das Produkt während der Gewährleistungsfrist Mängel auf, wenden Sie sich telefonisch an den technischen Support von Linksys, um ggf. eine vom Lieferanten vergebene Kennnummer für die Warenrücksendung (Return Authorization Number) zu erhalten. HALTEN SIE BEIM ANRUF IHREN KAUFBELEG BEREIT. Falls Sie zur Rückgabe des Produkts aufgefordert werden, markieren Sie außen an der Verpackung deutlich sichtbar die Return Authorization Number, und legen Sie eine Kopie Ihres ursprünglichen Kaufbelegs bei. RÜCKSENDUNGSAUFFORDERUNGEN KÖNNEN OHNE KAUFBELEG NICHT BEARBEITET WERDEN. Sie sind für den Versand defekter Produkte an Linksys verantwortlich. Linksys übernimmt nur die Kosten für den UPS-Versand auf dem Landweg von Linksys zurück zum Kunden. Kunden außerhalb der Vereinigten Staaten und Kanadas müssen sämtliche Versand- und Bearbeitungsgebühren übernehmen.

ALLE KONKLUDENTEN GEWÄHRLEISTUNGEN UND BEDINGUNGEN HINSICHTLICH MARKTGÄNGIGKEIT ODER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK SIND AUF DIE DAUER DER GEWÄHRLEISTUNGSFRIST BESCHRÄNKT. ALLE ANDEREN AUSDRÜCKLICHEN ODER KONKLUDENTEN BEDINGUNGEN UND GEWÄHRLEISTUNGEN, EINSCHLIESSLICH JEGLICHER KONKLUDENTER GEWÄHRLEISTUNGEN HINSICHTLICH NICHTVERLETZUNG, WERDEN ZURÜCKGEWIESEN. Einige Rechtsprechungen gestatten keine Beschränkungen hinsichtlich der Dauer der konkludenten Gewährleistung, sodass die obige Beschränkung für Sie gegebenenfalls keine Gültigkeit besitzt. Diese Gewährleistung verleiht Ihnen bestimmte Rechte, und Sie besitzen abhängig von der jeweiligen Rechtsprechung unter Umständen noch zusätzliche Rechte.

Diese Gewährleistung besitzt keine Gültigkeit, wenn das Produkt (a) geändert wurde, es sei denn von Linksys, (b) nicht den Anweisungen von Linksys entsprechend installiert, betrieben, repariert oder gewartet wurde, oder (c) unverhältnismäßiger physischer oder elektrischer Belastung ausgesetzt war, unsachgemäß verwendet, mangelhaft gewartet oder durch einen Unfall beschädigt wurde. Darüber hinaus übernimmt Linksys aufgrund der fortlaufenden Entwicklung neuer Methoden zum Eindringen in bzw. Angriff auf Netzwerke keine Gewährleistung, dass das Produkt gegen Eindringen oder Angriffe jederzeit geschützt ist.

IN DEM NICHT PER GESETZ UNTERSAGTEN AUSMASS ÜBERNIMMT LINKSYS UNTER KEINEN UMSTÄNDEN DIE HAFTUNG FÜR JEGLICHEN DATENVERLUST, ENTGANGENE EINNAHMEN ODER GEWINNE ODER FÜR SPEZIELLE, INDIREKTE UND BEILÄUFIG ENTSTANDENE SCHÄDEN SOWIE FOLGESCHÄDEN UND LEISTET KEINEN SCHADENERSATZZAHLUNGEN, UNGEACHTET DER HAFTUNGSTHEORIE (EINSCHLIESSLICH FAHRLÄSSIGKEIT), DIE AUFGRUND ODER IN ZUSAMMENHANG MIT DER VERWENDUNG ODER DER NICHTVERWENDBARKEIT (EINSCHLIESSLICH JEGLICHER SOFTWARE) ENTSTANDEN SIND, AUCH WENN LINKSYS ÜBER DIE MÖGLICHKEIT SOLCHER SCHÄDEN UNTERRICHTET WAR. UNTER KEINEN UMSTÄNDEN GEHT DIE HAFTUNG VON LINKSYS ÜBER DIE DEN VON IHNEN BEZAHLTEN BETRAG FÜR DAS PRODUKT HINAUS. Die vorangehenden Beschränkungen gelten auch dann, wenn eine Gewährleistung oder ein Rechtsmittel, das im Rahmen dieser Vereinbarung gewährt wird, ihrem bzw. seinem wesentlichen Zweck nicht gerecht wird. In einigen Rechtsprechungen ist der Ausschluss oder die Beschränkung von beiläufig oder als Folge entstandenen Schäden nicht gestattet, sodass die oben genannte Beschränkung oder der Ausschluss gegebenenfalls für Sie keine Gültigkeit besitzt.

Diese Gewährleistung ist nur in dem Land gültig, in dem das Produkt erworben wurde.

Richten Sie alle Anfragen an folgende Adresse: Linksys, P.O. Box 18558, Irvine, CA 92623, USA.

Anhang G: Rechtliche Hinweise

FCC-Hinweis

Dieses Produkt wurde getestet und entspricht gemäß Teil 15 der FCC-Bestimmungen den Spezifikationen für digitale Geräte der Klasse B. Diese Beschränkungen dienen zum Schutz vor schädlichen Störungen in Wohnumgebungen. Dieses Gerät erzeugt, verwendet und strahlt unter Umständen Hochfrequenzenergie aus und verursacht bei unsachgemäßer Installation und Verwendung möglicherweise Störungen bei Funkübertragungen. Allerdings besteht keine Garantie, dass die Störung nicht bei einer bestimmten Installation auftritt. Verursacht das Gerät Störungen beim Funk- und Fernsehempfang, die beim Ein- und Ausschalten des Geräts auftreten, versuchen Sie die Störung mithilfe einer der folgenden Maßnahmen zu beheben:

- Neuausrichten oder Aufstellen der Empfangsantenne an einem anderen Ort
- Vergrößern des Abstands zwischen den verschiedenen Geräten
- Anschließen des Geräts an eine andere Steckdose als die des Empfängers
- Unterstützung durch einen Händler oder erfahrenen Funk- und Fernsehtechniker

Sicherheitshinweise

Vorsicht: Verwenden Sie zur Verringerung des Brandrisikos nur ein Telekommunikationsnetzkabel, das mindestens No. 26 AWG (amerikanische Norm für Drahtquerschnitte) entspricht.

Bringen Sie dieses Produkt nicht mit Nässe in Berührung (z. B. in einem nassen Keller oder in der Nähe eines Swimmingpools).

Verwenden Sie dieses Produkt nicht während eines Gewitters. In diesem Fall besteht ein geringes Risiko eines Stromschlags.

Industry Canada (Kanada)

Dieses Gerät entspricht der Industry Canada-Bestimmung ICES-003.

Cet appareil est conforme à la norme NMB003 d'Industrie Canada.

IC-Hinweis

Der Betrieb unterliegt den folgenden beiden Bedingungen:

1. Dieses Gerät darf keine Störungen verursachen und

2. Dieses Gerät muss jegliche Störung tolerieren, einschließlich Störungen, die einen unerwünschten Betrieb des Geräts zur Folge haben.

Règlement d'Industry Canada

Le fonctionnement est soumis aux conditions suivantes :

1. Ce périphérique ne doit pas causer d'interférences;

2. Ce périphérique doit accepter toutes les interférences reçues, y compris celles qui risquent d'entraîner un fonctionnement indésirable.

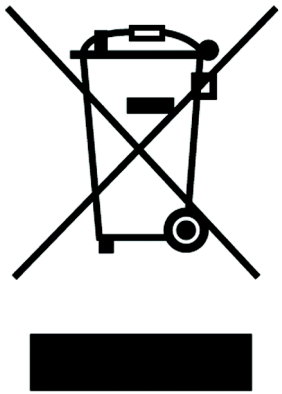
EG-Konformitätserklärung (Europa)

In Übereinstimmung mit der EMC-Richtlinie 89/336/EWG, der Niederspannungsrichtlinie 73/23/EWG und der Ergänzungsrichtlinie 93/68/EWG entspricht dieses Produkt folgenden Standards:

- EN55022 – Emission
- EN55024 – Störfestigkeit
- EN60950 – Sicherheit

Benutzerinformationen für Gebrauchsgüter, die durch die EU-Richtlinie 2002/96/EG zu Elektro- und Elektronikalt-/schrottgeräten (WEEE) abgedeckt sind

Dieses Dokument beinhaltet wichtige Informationen für Benutzer hinsichtlich der ordnungsgemäßen Entsorgung und Wiederaufbereitung von Linksys-Produkten. Verbraucher sind dazu verpflichtet, die in diesem Hinweis genannten Richtlinien bezüglich aller elektronischen Produkte, die folgendes Symbol tragen, einzuhalten:



English

Environmental Information for Customers in the European Union

European Directive 2002/96/EC requires that the equipment bearing this symbol on the product and/or its packaging must not be disposed of with unsorted municipal waste. The symbol indicates that this product should be disposed of separately from regular household waste streams. It is your responsibility to dispose of this and other electric and electronic equipment via designated collection facilities appointed by the government or local authorities. Correct disposal and recycling will help prevent potential negative consequences to the environment and human health. For more detailed information about the disposal of your old equipment, please contact your local authorities, waste disposal service, or the shop where you purchased the product.

Ceština/Czech

Informace o ochraně životního prostředí pro zákazníky v zemích Evropské unie

Evropská směrnice 2002/96/ES zakazuje, aby zařízení označené tímto symbolem na produktu anebo na obalu bylo likvidováno s netříděným komunálním odpadem. Tento symbol udává, že daný produkt musí být likvidován odděleně od běžného komunálního odpadu. Odpovídáte za likvidaci tohoto produktu a dalších elektrických a elektronických zařízení prostřednictvím určených sběrných míst stanovených vládou nebo místními úřady. Správná likvidace a recyklace pomáhá předcházet potenciálním negativním dopadům na životní prostředí a lidské zdraví. Podrobnější informace o likvidaci starého vybavení si laskavě vyžádejte od místních úřadů, podniku zabývajícího se likvidací komunálních odpadů nebo obchodu, kde jste produkt zakoupili.

Dansk/Danish

Miljøinformation for kunder i EU

EU-direktiv 2002/96/EF kræver, at udstyr der bærer dette symbol på produktet og/eller emballagen ikke må bortskaffes som usorteret kommunalt affald. Symbolet betyder, at dette produkt skal bortskaffes adskilt fra det almindelige husholdningsaffald. Det er dit ansvar at bortskaffe dette og andet elektrisk og elektronisk udstyr via bestemte indsamlingssteder udpeget af staten eller de lokale myndigheder. Korrekt bortskaffelse og genvinding vil hjælpe med til at undgå mulige skader for miljøet og menneskers sundhed. Kontakt venligst de lokale myndigheder, renovationstjenesten eller den butik, hvor du har købt produktet, angående mere detaljeret information om bortskaffelse af dit gamle udstyr.

Deutsch/German

Umweltinformation für Kunden innerhalb der Europäischen Union

Die Europäische Richtlinie 2002/96/EC verlangt, dass technische Ausrüstung, die direkt am Gerät und/oder an der Verpackung mit diesem Symbol versehen ist nicht zusammen mit unsortiertem Gemeindeabfall entsorgt werden darf. Das Symbol weist darauf hin, dass das Produkt von regulärem Haushaltmüll getrennt entsorgt werden sollte. Es liegt in Ihrer Verantwortung, dieses Gerät und andere elektrische und elektronische Geräte über die dafür zuständigen und von der Regierung oder örtlichen Behörden dazu bestimmten Sammelstellen zu entsorgen. Ordnungsgemäßes Entsorgen und Recyceln trägt dazu bei, potentielle negative Folgen für Umwelt und die menschliche Gesundheit zu vermeiden. Wenn Sie weitere Informationen zur Entsorgung Ihrer Altgeräte benötigen, wenden Sie sich bitte an die örtlichen Behörden oder städtischen Entsorgungsdienste oder an den Händler, bei dem Sie das Produkt erworben haben.

Eesti/Estonian

Keskkonnaalane informatsioon Euroopa Liidus asuvatele klientidele

Euroopa Liidu direktiivi 2002/96/EÜ nõuete kohaselt on seadmeid, millel on tootel või pakendil käesolev sümbol, keelatud kõrvaldada koos sorteerimata olmejäätmetega. See sümbol näitab, et toode tuleks kõrvaldada eraldi tavalistest olmejäätmevoogudest. Olete kohustatud kõrvaldama käesoleva ja ka muud elektri- ja elektroonikaseadmed riigi või kohalike ametiasutuste poolt ette nähtud kogumispunktide kaudu. Seadmete korrektne kõrvaldamine ja ringlussevõtt aitab vältida võimalikke negatiivseid tagajärgi keskkonnale ning inimeste tervisele. Vanade seadmete kõrvaldamise kohta täpsema informatsiooni saamiseks võtke palun ühendust kohalike ametiasutustega, jäätmekäitlusfirmaga või kauplusega, kust te toote ostsite.

Español/Spanish

Información medioambiental para clientes de la Unión Europea

La Directiva 2002/96/CE de la UE exige que los equipos que lleven este símbolo en el propio aparato y/o en su embalaje no deben eliminarse junto con otros residuos urbanos no seleccionados. El símbolo indica que el producto en cuestión debe separarse de los residuos domésticos convencionales con vistas a su eliminación. Es responsabilidad suya desechar este y cualesquiera otros aparatos eléctricos y electrónicos a través de los puntos de recogida que ponen a su disposición el gobierno y las autoridades locales. Al desechar y reciclar correctamente estos aparatos estará contribuyendo a evitar posibles consecuencias negativas para el medio ambiente y la salud de las personas. Si desea obtener información más detallada sobre la eliminación segura de su aparato usado, consulte a las autoridades locales, al servicio de recogida y eliminación de residuos de su zona o pregunte en la tienda donde adquirió el producto.

Ξλληνικά/Greek

Στοιχεία περιβαλλοντικής προστασίας για πελάτες εντός της Ευρωπαϊκής Ένωσης

Η Κοινοτική Οδηγία 2002/96/EC απαιτεί ότι ο εξοπλισμός ο οποίος φέρει αυτό το σύμβολο στο προϊόν και/ή στη συσκευασία του δεν πρέπει να απορρίπτεται μαζί με τα μικτά κοινοτικά απορρίμματα. Το σύμβολο υποδεικνύει ότι αυτό το προϊόν θα πρέπει να απορρίπτεται ξεχωριστά από τα συνήθη οικιακά απορρίμματα. Είστε υπεύθυνος για την απόρριψη του παρόντος και άλλου ηλεκτρικού και ηλεκτρονικού εξοπλισμού μέσω των καθορισμένων εγκαταστάσεων συγκέντρωσης απορριμμάτων οι οποίες παρέχονται από το κράτος ή τις αρμόδιες τοπικές αρχές. Η σωστή απόρριψη και ανακύκλωση συμβάλλει στην πρόληψη πιθανών αρνητικών συνεπειών για το περιβάλλον και την υγεία. Για περισσότερες πληροφορίες σχετικά με την απόρριψη του παλιού σας εξοπλισμού, παρακαλώ επικοινωνήστε με τις τοπικές αρχές, τις υπηρεσίες απόρριψης ή το κατάστημα από το οποίο αγοράσατε το προϊόν.

Français/French

Informations environnementales pour les clients de l'Union européenne

La directive européenne 2002/96/CE exige que l'équipement sur lequel est apposé ce symbole sur le produit et/ou son emballage ne soit pas jeté avec les autres ordures ménagères. Ce symbole indique que le produit doit être éliminé dans un circuit distinct de celui pour les déchets des ménages. Il est de votre responsabilité de jeter ce matériel ainsi que tout autre matériel électrique ou électronique par les moyens de collecte indiqués par le gouvernement et les pouvoirs publics des collectivités territoriales. L'élimination et le recyclage en bonne et due forme ont pour but de lutter contre l'impact néfaste potentiel de ce type de produits sur l'environnement et la santé publique. Pour plus d'informations sur le mode d'élimination de votre ancien équipement, veuillez prendre contact avec les pouvoirs publics locaux, le service de traitement des déchets, ou l'endroit où vous avez acheté le produit.

Italiano/Italian

Informazioni relative all'ambiente per i clienti residenti nell'Unione Europea

La direttiva europea 2002/96/EC richiede che le apparecchiature contrassegnate con questo simbolo sul prodotto e/o sull'imballaggio non siano smaltite insieme ai rifiuti urbani non differenziati. Il simbolo indica che questo prodotto non deve essere smaltito insieme ai normali rifiuti domestici. È responsabilità del proprietario smaltire sia questi prodotti sia le altre apparecchiature elettriche ed elettroniche mediante le specifiche strutture di raccolta indicate dal governo o dagli enti pubblici locali. Il corretto smaltimento ed il riciclaggio aiuteranno a prevenire conseguenze potenzialmente negative per l'ambiente e per la salute dell'essere umano. Per ricevere informazioni più dettagliate circa lo smaltimento delle vecchie apparecchiature in Vostro possesso, Vi invitiamo a contattare gli enti pubblici di competenza, il servizio di smaltimento rifiuti o il negozio nel quale avete acquistato il prodotto.

Latviešu valoda/Latvian

Ekoloģiska informācija klientiem Eiropas Savienības jurisdikcijā

Direktīvā 2002/96/EK ir prasība, ka aprīkojumu, kam pievienota zīme uz paša izstrādājuma vai uz tā iesaiņojuma, nedrīkst izmest nešķirotā veidā kopā ar komunālajiem atkritumiem (tiem, ko rada vietēji iedzīvotāji un uzņēmumi). Šī zīme nozīmē to, ka šī ierīce ir jāizmet atkritumos tā, lai tā nenonāktu kopā ar parastiem mājsaimniecības atkritumiem. Jūsu pienākums ir šo un citas elektriskas un elektroniskas ierīces izmest atkritumos, izmantojot īpašus atkritumu savākšanas veidus un līdzekļus, ko nodrošina valsts un pašvaldību iestādes. Ja izmešana atkritumos un pārstrāde tiek veikta pareizi, tad mazinās iespējamais kaitējums dabai un cilvēku veselībai. Sīkākas ziņas par novecojuša aprīkojuma izmešanu atkritumos jūs varat saņemt vietējā pašvaldībā, atkritumu savākšanas dienestā, kā arī veikalā, kur iegādājāties šo izstrādājumu.

Lietuvškai/Lithuanian

Aplinkosaugos informacija, skirta Europos Sąjungos vartotojams

Europos direktyva 2002/96/EC numato, kad įrangos, kuri ir (arba) kurios pakuotė yra pažymėta šiuo simboliu, negalima šalinti kartu su nerūšiuotomis komunalinėmis atliekomis. Šis simbolis rodo, kad gaminį reikia šalinti atskirai nuo bendro buitinių atliekų srauto. Jūs privalote užtikrinti, kad ši ir kita elektros ar elektroninė įranga būtų šalinama per tam tikras nacionalinės ar vietinės valdžios nustatytas atliekų rinkimo sistemas. Tinkamai šalinant ir perdirbant atliekas, bus išvengta galimos žalos aplinkai ir žmonių sveikatai. Daugiau informacijos apie jūsų senos įrangos šalinimą gali pateikti vietinės valdžios institucijos, atliekų šalinimo tarnybos arba parduotuvės, kuriose įsigijote tą gaminį.

Malti/Maltese

Informazzjoni Ambjentali għal Klijenti fl-Unjoni Ewropea

Id-Direttiva Ewropea 2002/96/KE titlob li t-tagħmir li jkun fih is-simbolu fuq il-prodott u/jew fuq l-ippakkjar ma jistax jintrema ma' skart muniċipali li ma ġiex isseparat. Is-simbolu jindika li dan il-prodott għandu jintrema separatament minn ma' l-iskart domestiku regolari. Hija responsabbiltà tiegħek li tarmi dan it-tagħmir u kull tagħmir ieħor ta' l-elettriku u elettroniku permezz ta' faċilitajiet ta' ġbir appuntati apposta mill-gvern jew mill-awtoritajiet lokali. Ir-rimi b'mod korrett u r-riċiklaġġ jgħin jipprevjeni konsegwenzi negattivi potenzjali għall-ambjent u għas-saħħa tal-bniedem. Għal aktar informazzjoni dettaljata dwar ir-rimi tat-tagħmir antik tiegħek, jekk jogħġbok ikkuntattja lill-awtoritajiet lokali tiegħek, is-servizzi għar-rimi ta' l-iskart, jew il-ħanut minn fejn xtrajt il-prodott.

Magyar/Hungarian

Környezetvédelmi információ az európai uniós vásárlók számára

A 2002/96/EC számú európai uniós irányelv megkívánja, hogy azokat a termékeket, amelyeken, és/vagy amelyek csomagolásán az alábbi címke megjelenik, tilos a többi szelektálatlan lakossági hulladékkal együtt kidobni. A címke azt jelöli, hogy az adott termék kidobásakor a szokványos háztartási hulladékelszállítási rendszerektől elkülönített eljárást kell alkalmazni. Az Ön felelőssége, hogy ezt, és más elektromos és elektronikus berendezéseit a kormányzati vagy a helyi hatóságok által kijelölt gyűjtőredszereken keresztül számolja fel. A megfelelő hulladékfeldolgozás segít a környezetre és az emberi egészségre potenciálisan ártalmas negatív hatások megelőzésében. Ha elavult berendezéseinek felszámolásához további részletes információra van szüksége, kérjük, lépjen kapcsolatba a helyi hatóságokkal, a hulladékfeldolgozási szolgálattal, vagy azzal üzlettel, ahol a terméket vásárolta.

Nederlands/Dutch

Milieu-informatie voor klanten in de Europese Unie

De Europese Richtlijn 2002/96/EC schrijft voor dat apparatuur die is voorzien van dit symbool op het product of de verpakking, niet mag worden ingezameld met niet-gescheiden huishoudelijk afval. Dit symbool geeft aan dat het product apart moet worden ingezameld. U bent zelf verantwoordelijk voor de vernietiging van deze en andere elektrische en elektronische apparatuur via de daarvoor door de landelijke of plaatselijke overheid aangewezen inzamelingskanalen. De juiste vernietiging en recycling van deze apparatuur voorkomt mogelijke negatieve gevolgen voor het milieu en de gezondheid. Voor meer informatie over het vernietigen van uw oude apparatuur neemt u contact op met de plaatselijke autoriteiten of afvalverwerkingsdienst, of met de winkel waar u het product hebt aangeschaft.

Norsk/Norwegian

Miljøinformasjon for kunder i EU

EU-direktiv 2002/96/EF krever at utstyr med følgende symbol avbildet på produktet og/eller pakningen, ikke må kastes sammen med usortert avfall. Symbolet indikerer at dette produktet skal håndteres atskilt fra ordinær avfallsinnsamling for husholdningsavfall. Det er ditt ansvar å kvitte deg med dette produktet og annet elektrisk og elektronisk avfall via egne innsamlingsordninger slik myndighetene eller kommunene bestemmer. Korrekt avfallshåndtering og gjenvinning vil være med på å forhindre mulige negative konsekvenser for miljø og helse. For nærmere informasjon om håndtering av det kasserte utstyret ditt, kan du ta kontakt med kommunen, en innsamlingsstasjon for avfall eller butikken der du kjøpte produktet.

Polski/Polish

Informacja dla klientów w Unii Europejskiej o przepisach dotyczących ochrony środowiska

Dyrektywa Europejska 2002/96/EC wymaga, aby sprzęt oznaczony symbolem znajdującym się na produkcie i/lub jego opakowaniu nie był wyrzucany razem z innymi niesortowanymi odpadami komunalnymi. Symbol ten wskazuje, że produkt nie powinien być usuwany razem ze zwykłymi odpadami z gospodarstw domowych. Na Państwu spoczywa obowiązek wyrzucania tego i innych urządzeń elektrycznych oraz elektronicznych w punktach odbioru wyznaczonych przez władze krajowe lub lokalne. Pozbywanie się sprzętu we właściwy sposób i jego recykling pomogą zapobiec potencjalnie negatywnym konsekwencjom dla środowiska i zdrowia ludzkiego. W celu uzyskania szczegółowych informacji o usuwaniu starego sprzętu, prosimy zwrócić się do lokalnych władz, służb oczyszczania miasta lub sklepu, w którym produkt został nabyty.

Português/Portuguese

Informação ambiental para clientes da União Europeia

A Directiva Europeia 2002/96/CE exige que o equipamento que exibe este símbolo no produto e/ou na sua embalagem não seja eliminado junto com os resíduos municipais não separados. O símbolo indica que este produto deve ser eliminado separadamente dos resíduos domésticos regulares. É da sua responsabilidade eliminar este e qualquer outro equipamento eléctrico e electrónico através dos instalações de recolha designadas pelas autoridades governamentais ou locais. A eliminação e reciclagem correctas ajudarão a prevenir as consequências negativas para o ambiente e para a saúde humana. Para obter informações mais detalhadas sobre a forma de eliminar o seu equipamento antigo, contacte as autoridades locais, os serviços de eliminação de resíduos ou o estabelecimento comercial onde adquiriu o produto.

Slovenčina/Slovak

Informácie o ochrane životného prostredia pre zákazníkov v Európskej únii

Podľa európskej smernice 2002/96/ES zariadenie s týmto symbolom na produkte a/alebo jeho balení nesmie byť likvidované spolu s netriedeným komunálnym odpadom. Symbol znamená, že produkt by sa mal likvidovať oddelene od bežného odpadu z domácností. Je vašou povinnosťou likvidovať toto i ostatné elektrické a elektronické zariadenia prostredníctvom špecializovaných zberných zariadení určených vládou alebo miestnymi orgánmi. Správna likvidácia a recyklácia pomôže zabrániť prípadným negatívnym dopadom na životné prostredie a zdravie ľudí. Ak máte záujem o podrobnejšie informácie o likvidácii starého zariadenia, obráťte sa, prosím, na miestne orgány, organizácie zaoberajúce sa likvidáciou odpadov alebo obchod, v ktorom ste si produkt zakúpili.

Slovenčina/Slovene

Okoljske informacije za stranke v Evropski uniji

Evropska direktiva 2002/96/EC prepoveduje odlaganje opreme, označene s tem simbolom – na izdelku in/ali na embalaži – med običajne, nerazvrščene odpadke. Ta simbol opozarja, da je treba izdelek odvreči ločeno od preostalih gospodinjskih odpadkov. Vaša odgovornost je, da to in preostalo električno in elektronsko opremo odnesete na posebna zbirališča, ki jih določijo državne ustanove ali lokalna uprava. S pravilnim odlaganjem in recikliranjem boste preprečili morebitne škodljive vplive na okolje in zdravje ljudi. Če želite izvedeti več o odlaganju stare opreme, se obrnite na lokalno upravo, odpad ali trgovino, kjer ste izdelek kupili.

Suomi/Finnish

Ympäristöä koskevia tietoja EU-alueen asiakkaille

EU-direktiivi 2002/96/EY edellyttää, että jos laitteistossa on tämä symboli itse tuotteessa ja/tai sen pakkauksessa, laitteistoa ei saa hävittää lajittelemattoman yhdyskuntajätteen mukana. Symboli merkitsee sitä, että tämä tuote on hävitettävä erillään tavallisesta kotitalousjätteestä. Sinun vastuullasi on hävittää tämä elektroniikkatuote ja muut vastaavat elektroniikkatuotteet viemällä tuote tai tuotteet viranomaisten määräämään keräyspisteeseen. Laitteiston oikea hävittäminen estää mahdolliset kielteiset vaikutukset ympäristöön ja ihmisten terveyteen. Lisätietoja vanhan laitteiston oikeasta hävitystavasta saa paikallisilta viranomaisilta, jätteenhävityspalvelusta tai siitä myymälästä, josta ostit tuotteen.

Svenska/Swedish

Miljöinformation för kunder i Europeiska unionen

Det europeiska direktivet 2002/96/EC kräver att utrustning med denna symbol på produkten och/eller förpackningen inte får kastas med osorterat kommunalt avfall Symbolen visar att denna produkt bör kastas efter att den avskiljts från vanligt hushållsavfall. Det faller på ditt ansvar att kasta denna och annan elektrisk och elektronisk utrustning på fastställda insamlingsplatser utsedda av regeringen eller lokala myndigheter. Korrekt kassering och återvinning skyddar mot eventuella negativa konsekvenser för miljön och personhälsa. För mer detaljerad information om kassering av din gamla utrustning kontaktar du dina lokala myndigheter, avfallshanteringen eller butiken där du köpte produkten.

Weitere Informationen erhalten Sie unter www.linksys.com/international.

Anhang H: Kontaktinformationen

Möchten Sie sich mit Linksys in Verbindung setzen?
Besuchen Sie uns online unter folgender Adresse, um Informationen zu den aktuellen Produkten und Updates zu erhalten:
http://www.linksys.com/international

Sollten bei einem Linksys-Produkt Probleme auftreten, erreichen Sie uns per E-Mail unter folgender Adresse:

In Europa	E-Mail-Adresse
Belgien	support.be@linksys.com
Dänemark	support.dk@linksys.com
Deutschland	support.de@linksys.com
Finnland	support.fi@linksys.com
Frankreich	support.fr@linksys.com
Griechenland	support.gr@linksys.com (nur in englischer Sprache)
Großbritannien	support.uk@linksys.com
Irland	support.ie@linksys.com
Italien	support.it@linksys.com
Niederlande	support.nl@linksys.com
Norwegen	support.no@linksys.com
Österreich	support.at@linksys.com
Polen	support.pl@linksys.com
Portugal	support.pt@linksys.com
Russland	support.ru@linksys.com
Schweden	support.se@linksys.com
Schweiz	support.ch@linksys.com
Spanien	support.es@linksys.com

In Europa	E-Mail-Adresse
Tschechische Republik	support.cz@linksys.com
Türkei	support.tk@linksys.com
Ungarn	support.hu@linksys.com

Außerhalb Europas	E-Mail-Adresse
Asien/Pazifik	asiasupport@linksys.com (nur in englischer Sprache)
Lateinamerika	support.portuguese@linksys.com oder support.spanish@linksys.com
Naher Osten und Afrika	support.mea@linksys.com (nur in englischer Sprache)
Südafrika	support.ze@linksys.com (nur in englischer Sprache)
USA und Kanada	support@linksys.com
VAE	support.ae@linksys.com (nur in englischer Sprache)

Hinweis: In einigen Ländern steht der Support eventuell nur in englischer Sprache zur Verfügung.