



. . . c o n n e c t i n g y o u r b u s i n e s s

LANCOM GS-2124

LANCOM GS-2124

© 2009 LANCOM Systems GmbH, Wuersele (Germany). Alle Rechte vorbehalten.

Alle Angaben in dieser Dokumentation sind nach sorgfältiger Prüfung zusammengestellt worden, gelten jedoch nicht als Zusicherung von Produkteigenschaften. LANCOM Systems haftet ausschließlich in dem Umfang, der in den Verkaufs- und Lieferbedingungen festgelegt ist.

Weitergabe und Vervielfältigung der zu diesem Produkt gehörenden Dokumentation und Software und die Verwendung ihres Inhalts sind nur mit schriftlicher Erlaubnis von LANCOM Systems gestattet. Änderungen, die dem technischen Fortschritt dienen, bleiben vorbehalten.

Windows®, Windows Vista™, Windows NT® und Microsoft® sind eingetragene Marken von Microsoft, Corp.

Das LANCOM Systems-Logo, LCOS und die Bezeichnung LANCOM sind eingetragene Marken der LANCOM Systems GmbH. Alle übrigen verwendeten Namen und Bezeichnungen können Marken oder eingetragene Marken ihrer jeweiligen Eigentümer sein.

LANCOM Systems behält sich vor, die genannten Daten ohne Ankündigung zu ändern und übernimmt keine Gewähr für technische Ungenauigkeiten und/oder Auslassungen.

Produkte von LANCOM Systems enthalten Software, die vom „OpenSSL Project“ für die Verwendung im „OpenSSL Toolkit“ entwickelt wurde (<http://www.openssl.org/>).

Produkte von LANCOM Systems enthalten kryptographische Software, die von Eric Young (ey@cryptsoft.com) geschrieben wurde.

Produkte von LANCOM Systems enthalten Software, die von der NetBSD Foundation, Inc. und ihren Mitarbeitern entwickelt wurde.

Produkte von LANCOM Systems enthalten das LZMA SDK, das von Igor Pavlov entwickelt wurde.

LANCOM Systems GmbH

Adenauerstr. 20/B2

52146 Wuersele

Deutschland

www.lancom.de

Wuersele, April 2009

Ein Wort vorab

Vielen Dank für Ihr Vertrauen!

Die LANCOM Switches sind optimal geeignet für kleine und mittelgroße, aber anspruchsvolle Netzwerke im Business-Umfeld.

Der LANCOM GS-2124 mit seinen 20 Fast-Ethernet und seinen vier Combo Ports (TP/SFP) lässt sich perfekt in LANCOMs Advanced Routing und Forwarding integrieren und unterstützt bis zu 256 aktive VLANs. Er führt eine Bandbreitenkontrolle durch und priorisiert nach vorher festgelegten Kriterien den Datenverkehr (z. B. Voice-Daten oder den bestimmter Ports).

Die LANCOM Switches lassen sich bequem über die übersichtliche WEBconfig administrieren und werden von den LANCOM Management Tools (LANconfig und LANmonitor) unterstützt.

An der Erstellung dieser Dokumentation ...

... haben mehrere Mitarbeiter/innen aus verschiedenen Teilen des Unternehmens mitgewirkt, um Ihnen die bestmögliche Unterstützung bei der Nutzung Ihres LANCOM-Produktes anzubieten.

Sollten Sie einen Fehler finden oder einfach nur Kritik oder Anregung zu dieser Dokumentation äußern wollen, senden Sie bitte eine E-Mail direkt an:

info@lancom.de



Sollten Sie zu den in diesem Handbuch besprochenen Themen noch Fragen haben oder zusätzliche Hilfe benötigen, steht Ihnen unser Internet-Server www.lancom.de rund um die Uhr zur Verfügung. Hier finden Sie im Bereich 'Support' viele Antworten auf „häufig gestellte Fragen ('FAQs')“. Darüber hinaus bietet Ihnen die Wissensdatenbank einen großen Pool an Informationen. Aktuelle Treiber, Firmware, Tools und Dokumentation stehen für Sie jederzeit zum Download bereit. Außerdem steht Ihnen der LANCOM-Support zur Verfügung. Telefonnummern und Kontaktadressen des LANCOM-Supports finden Sie in einem separaten Beileger oder auf der LANCOM Systems-Homepage.

Hinweis-Symbole

Sehr wichtiger Hinweis, dessen Nichtbeachtung zu Schäden führen kann.



Wichtiger Hinweis, der beachtet werden sollte.



Zusätzliche Informationen, deren Beachtung hilfreich sein kann aber nicht erforderlich ist.

Inhalt

1 Einleitung	9
1.1 Funktionsübersicht	9
1.2 Das kann Ihr LANCOM Switch	11
2 Installation	13
2.1 Lieferumfang	13
2.2 Systemvoraussetzungen	13
2.3 Statusanzeigen und Schnittstellen	14
2.3.1 Anschlüsse, LEDs und Taster beim LANCOM GS-2124	14
2.3.2 Anschlüsse auf der Rückseite beim LANCOM GS-2124	15
2.4 Montage und Anschluss des LANCOM Switches	15
2.5 Installation der Software	16
2.5.1 Software-Setup starten	17
2.5.2 Welche Software installieren?	17
3 LANCOM Switch konfigurieren und überwachen	18
3.1 Konfigurationsmöglichkeiten	18
3.1.1 WEBconfig starten	18
3.1.2 Command Line Interface über Netzwerk starten	20
3.1.3 Command Line Interface über serielle Verbindung starten	21
3.2 Welche Konfiguration verwendet das Gerät?	21
3.3 Save/Restore	23
3.3.1 Factory Defaults	24
3.3.2 Save Start	24
3.3.3 Save User	25
3.3.4 Restore User	25
3.4 Export/ Import Configuration File	26
3.5 LANCOM Switch mit LANmonitor überwachen	26
3.5.1 Status der Ethernet-Ports	27

4 Anleitung zum webbasierten Management	29
4.1 Übersicht über das webbasierte Management	30
4.2 System: Basic Config	32
4.2.1 System Information	32
4.2.2 Account	34
4.2.3 Time	35
4.2.4 IP Configuration	37
4.2.5 Loop Detection	40
4.2.6 Management Policy	41
4.2.7 System Log	43
4.2.8 Virtual Stack	44
4.3 System: Port	46
4.3.1 Configuration	46
4.3.2 Status	48
4.3.3 Simple Counter	52
4.3.4 Detail Counter	53
4.4 Security: MAC	56
4.4.1 Mac Address Table	56
4.4.2 Static Filter	58
4.4.3 Static Forward	59
4.4.4 MAC Alias	60
4.4.5 MAC Table	61
4.5 Security: VLAN	62
4.5.1 VLAN Mode	62
4.5.2 Tag-based Group	63
4.5.3 Port-based Group	65
4.5.4 Ports	66
4.5.5 Port Isolation	68
4.5.6 Management VLAN	68
4.6 Security: ACL (Access-Control-List)	68
4.6.1 Ports	69
4.6.2 Rate Limiters	71
4.6.3 Access Control List	71
4.6.4 Wizard	85
4.7 Security: IP MAC Binding	87
4.8 Security: DHCP Snooping	89
4.8.1 DHCP Snooping State	89
4.8.2 DHCP Snooping Entry	90

4.8.3	DHCP Snooping Client	92
4.9	Security: 802.1x Konfiguration	93
4.9.1	Server	98
4.9.2	Port Configuration	99
4.9.3	Status	102
4.9.4	Statistics	103
4.10	Security: Mirroring	104
4.11	Configuration: GVRP	105
4.11.1	Config	106
4.11.2	Counter	109
4.11.3	Group	111
4.12	Configuration: QoS (Quality of Service)	112
4.12.1	Ports	113
4.12.2	Qos Control List	114
4.12.3	Rate Limiters	117
4.12.4	Storm Control	118
4.12.5	Wizard	119
4.13	Configuration: Trunk	121
4.13.1	Port	124
4.13.2	Aggregator View	126
4.13.3	Hash Method	127
4.13.4	LACP System Configuration	127
4.14	Configuration: STP	128
4.14.1	Status	128
4.14.2	Konfiguration	130
4.14.3	Port	132
4.15	Configuration: MSTP	135
4.15.1	State	135
4.15.2	Region Config	135
4.15.3	Instance View	136
4.16	Configuration: Multicast	142
4.16.1	IGMP Mode	143
4.16.2	Proxy	143
4.16.3	Snooping	144
4.16.4	IGMP Group Membership	145
4.17	Management: Alarm	146
4.17.1	Events	146
4.17.2	Email	147

4.18	Management: Diagnostics	148
4.18.1	Diag	148
4.18.2	Ping	149
4.19	Management: Maintenance	149
4.19.1	Reset device	149
4.19.2	Firmware Upgrade	150
4.20	Management: SNMP	150
4.21	Logout	153
5	Operation of CLI Management (englisch)	154
5.1	CLI Management	154
5.1.1	Login	154
5.2	Commands of CLI	155
5.2.1	Global Commands of CLI	155
5.2.2	4-2-2. Local Commands of CLI	161
6	Anhang	273
6.1	Leistungs- und Kenndaten	273
6.2	Anschlussbelegung	274
6.2.1	LAN-Schnittstelle 10/100Base-TX	274
6.3	CE-Konformitätserklärungen	274

1 Einleitung

Bei den LANCOM Switches von Typ LANCOM GS-2124 handelt es sich um gemanagte Layer-2-Switches mit 20 Gigabit-Ports (für Twisted-Pair-Kabel – TP) sowie vier Gigabit-Dual-Media-Ports (für TP- oder Glasfaserkabel), die den IEEE 802.3-Spezifikationen für Gigabit, Fast Ethernet und Ethernet entsprechen.

Die LANCOM Switches können mit einer direkten Verbindung über den seriellen Port (RS-232) oder über eine LAN-Verbindung mit Telnet oder WEBconfig konfiguriert werden. Ein SNMP-Management nach SNMPv2 ist durch die integrierten MIBs ebenfalls möglich.

Mit einem effizienten Netzwerk-Management ermöglichen die LANCOM Switches Anwendungen mit hohem Bandbreitebedarf. Die Geräte unterstützen moderne Funktionen wie QoS (Quality of Service), Rapid Spanning Tree, VLAN, Port Trunking, Bandbreitenbeschränkung, portbasierte Sicherheitseinstellungen, SNMP/RMON und IGMP Snooping. Sie sind damit optimal geeignet für kleine und mittelgroße, aber anspruchsvolle Netzwerke im Business-Umfeld.

Die 10/100/1000 MBit/s-TP-Ports entsprechen den Standards IEEE 802.3u/x/z (Gigabit und Fast Ethernet).

Die 1000 MBit/s-SFP-Ports entsprechen den Standards IEEE 802.3z und 1000Base-SX/LX. Der Glasfaser-Port ist mit der Wavelength Division Multiplexing (WDM) Technologie ausgerüstet, welche die gleichzeitige Full-Duplex-Übertragung in beide Richtungen über eine Faser erlaubt.

1.1 Funktionsübersicht

■ QoS:

Unterstützt Quality of Service nach dem IEEE 802.1P-Standard. Dabei werden zwei prioritätsgesteuerte Warteschlangen nach einem gewichteten Round Robin-Verfahren verwendet (Weighted Round Robin – WRR). Die Klassifizierung der Pakete kann über VLAN-Tags oder portgebunden eingerichtet werden.

■ Spanning Tree:

Unterstützt die Standards IEEE 802.1D und IEEE 802.1w (RSTP: Rapid Spanning Tree Protocol) .

- VLAN:
Unterstützt portbasiertes VLAN und VLAN-Tagging nach IEEE802.1Q mit bis zu 256 aktiven VLANs und VLAN-IDs von 1 bis 4094.
- Port Trunking:
Unterstützt statisches Port-Trunking und dynamisches Port-Trunking nach IEEE 802.3ad LACP.
- Bandbreitenbeschränkung:
Unterstützt die Bandbreitenbeschränkung für eingehende und ausgehende Verbindungen.
- Portbasierte Sicherheitseinstellungen:
Unterstützt das Erlauben oder Verboten der Datenverarbeitung auf einem Port in Abhängigkeit von der MAC-Adresse.
- SNMP/RMON:
SNMP-Agent und RMON MIB. Das Gerät arbeitet als SNMP-Client und übermittelt auf Anfrage des SNMP-Managers Informationen über den aktuellen Zustand. Ausserdem versendet der SNMP-Agent bei Bedarf aktiv TRAP-Nachrichten.
RMON steht als Abkürzung für Remote Network Monitoring und ist ein zweig der SNMP MIB.
Das Gerät unterstützt MIB-2 (RFC 1213), Bridge MIB (RFC 1493), RMON MIB (RFC 1757)-Statistiken der Gruppen 1,2,3,9, Bridge MIB (RFC 1493), Ethernet MIB (RFC 1643) usw.
- IGMP Snooping:
Unterstützt IGMP-Version 2 (RFC 2236). Das Internet Group Management Protocol dient zum Aufbau von Multicast-Gruppen, in denen die Multicast-Pakete ausschließlich an die jeweiligen Gruppenmitglieder übermittelt werden. Mit Hilfe von IGMP wird die benötigte Bandbreite durch unnötige Daten reduziert.

1.2 Das kann Ihr LANCOM Switch

LANCOM GS-2124	
Hardware	
20 10/100/1000 MBit/s Gigabit TP-Ports mit Auto-MDIX-Funktion	✓
4 Gigabit Dual Media Ports (TP/SFP)	✓
Hot-Plugging für SFP-Module	✓
256KB Paket-Zwischenspeicher und 128KB Verwaltungsspeicher	✓
Maximale Paketlänge von 1536 Bytes	✓
Full-Duplex Datenflusssteuerung (IEEE802.3x)	✓
LEDs zur Zustandsanzeige	
System: Power	✓
TP Port 1-24: LINK/ACT, SPD	✓
SFP-Ports 21,22,23,24: LINK/ACT, SPD, SFP	✓
Management	
Klare Darstellung der Port-Zustände und einfache Konfiguration der Ports	✓
Port-spezifische Traffic-Überwachung	✓
Port-Mirror-Funktion	✓
Unterstützung statischer Trunk-Gruppen	✓
VLAN nach 802.1Q mit 256 Einträgen	✓
Unterdrückung der DHCP-Broadcasts zur Entlastung des Netzwerks	✓
Versand von Trap-Nachrichten, wenn definierte Ereignisse stattfinden	✓
Default-Konfiguration, mit der die aktuelle Konfiguration über Telnet oder WEBconfig überschrieben werden kann	✓
Fünf Typen von QoS: MAC-Priorität, 802.1p-Priorität, IP TOS-Priorität, und DiffServ DSCP-Priorität.	✓
WEBconfig und CLI-Management über Telnet o.ä.	✓
Rapid Spanning Tree (802.1w RSTP)	✓

	LANCOM GS-2124
Portbasierte Sicherheitseinstellungen im VLAN nach 802.1x	✓
SNMP-Zugang abschaltbar zum Schutz vor unberechtigten SNMP-Zugriffen	✓
Bandbreitenregelung für ein- und ausgehende Verbindungen	✓
Versand von Trap-Nachrichten über E-Mail und SMS	✓
Diagnose-Funktionen zur Unterstützung des Administrators	✓
Externer Loopback-Test zur Prüfung der Port-Funktion	✓
HTTP für Firmware-Upgrades, System-Logs sowie den Import bzw. Export von Konfigurationen	✓
Remote Boot über WEBconfig, CLI und SNMP	✓
Zeitsynchronisation mit NTP-Servern und Sommerzeitumschaltung	✓
120 Einträge in der Log-Tabelle im Hauptspeicher zur Anzeige über Konsole	✓
Optionen	
LANCOM SFP Glasfaser Transceiver: Art.-Nr. 61556 LANCOM SFP-SX-LC1 Art.-Nr. 61557 LANCOM SFP-LX-LC1	✓

2 Installation

Dieses Kapitel hilft Ihnen, möglichst schnell Hard- und Software zu installieren. Zunächst überprüfen Sie Lieferumfang und Systemvoraussetzungen. Sind alle Voraussetzungen erfüllt, gelingen Anschluss und Inbetriebnahme schnell und ohne Mühe.

2.1 Lieferumfang

Bitte prüfen Sie den Inhalt der Verpackung auf Vollständigkeit, bevor Sie mit der Installation beginnen. Neben dem LANCOM Switch sollte der Karton folgendes Zubehör für Sie bereithalten:

	LANCOM GS-2124
Netz Kabel zum Anschluss an die Stromversorgung	✓
19"-Montagewinkel (2 Stück) und Befestigungsmaterial	✓
Serielles Konfigurationskabel	✓
LANCOM-CD	✓
Gedruckte Dokumentation	✓

Falls etwas fehlen sollte, wenden Sie sich bitte umgehend an Ihren Händler oder an die Kontaktadresse, die auf dem Lieferschein zu Ihrem Gerät angegeben ist.

2.2 Systemvoraussetzungen

Rechner, die mit einem LANCOM in Verbindung treten möchten, müssen mindestens die folgenden Voraussetzungen erfüllen:

- Betriebssystem mit TCP/IP-Unterstützung, z.B. Windows Vista™, Windows XP, Windows Millennium Edition (Me), Windows 2000, Windows 98, Linux, BSD Unix, Apple Mac OS, OS/2.
- Zugang zum LAN über das TCP/IP-Protokoll.
- Browser für die webbasierte Konfiguration.

i Die LANtools benötigen zudem ein Windows-Betriebssystem. Für den Zugriff auf WEBconfig ist ein Web-Browser unter einem beliebigen Betriebssystem erforderlich.

2.3 Statusanzeigen und Schnittstellen

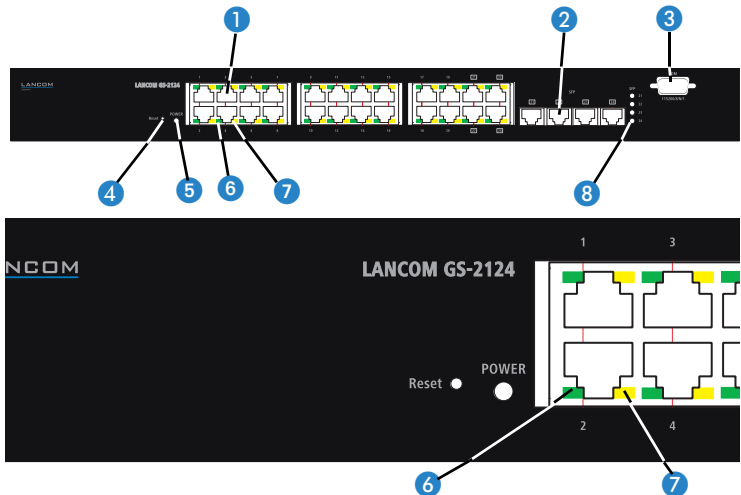
Bedeutung der LEDs

In den folgenden Abschnitten wird das Verhalten der LEDs beschrieben.

! Bitte beachten Sie, dass der LANmonitor über die Anzeige der LEDs hinaus weitere wichtige Informationen über den Status der LANCOM Switches anzeigt '→ LANCOM Switch mit LANmonitor überwachen'.

2.3.1 Anschlüsse, LEDs und Taster beim LANCOM GS-2124

Auf der Vorderseite des Geräts befinden sich Anschlüsse für verschiedene Kabeltypen, Leuchtdioden (LEDs), die Informationen über den Status des Geräts geben, sowie ein Taster.



1 TP-Anschlüsse Anschlüsse für Twisted-pair Kabel.

2 SFP-Anschlüsse Anschlüsse für Small-form-factor-pluggable (SFP) Kabel.

- | | | |
|---|---------------------------------|---|
| 3 | Serieller Anschluss | Anschluss für serielles Konfigurations-Kabel. |
| 4 | Reset | Taster zum Neustarten des Systems. |
| 5 | POWER-LED | Dauerhaft grün, wenn die Spannungsversorgung des Gerätes hergestellt ist. |
| 6 | LINK / ACT-LED
Port 1 bis 24 | <ul style="list-style-type: none"> ■ Dauerhaft grün, wenn die Netzwerkverbindung zum angeschlossenen Gerät hergestellt ist. ■ Blinkt, um Traffic auf diesem Port anzuzeigen. ■ Aus, wenn keine Netzwerkverbindung zum angeschlossenen Gerät hergestellt werden kann. |
| 7 | 10/100/1000 Mbps-LED | <ul style="list-style-type: none"> ■ Leuchtet Grün um eine Verbindung mit 1000 Mbps anzuzeigen ■ Leuchtet Orange um eine Verbindung mit 100 Mbps anzuzeigen ■ Aus, um eine Verbindung mit 10 Mbps anzuzeigen |
| 8 | SFP (LINK/ACT)-LED | <ul style="list-style-type: none"> ■ Dauerhaft grün, wenn die Netzwerkverbindung zum angeschlossenen Gerät hergestellt ist. ■ Blinkt, um Traffic an diesem Port anzuzeigen. ■ Aus, wenn keine Netzwerkverbindung zum angeschlossenen Gerät hergestellt werden kann. |

2.3.2 Anschlüsse auf der Rückseite beim LANCOM GS-2124

Auf der Rückseite des Geräts befinden sich folgende Anschlüsse.




LANCOM GS-2124

- 1 Anschluss für Kaltgerätekabel zur Stromversorgung.


2.4 Montage und Anschluss des LANCOM Switches


Die Installation des LANCOM Switches erfolgt in folgenden Schritten:

- 1 **Montage** – montieren Sie das Gerät in einem freien 19"-Einschub in einem entsprechenden Serverschrank. Bringen Sie ggf. die GummifüÙe auf der Unterseite des Gerätes an, um Kratzer auf den Oberflächen anderer Geräte zu vermeiden.

 Achten Sie auf eine ausreichende Belüftung des Gerätes, um Schäden durch übermäßige Wärmeentwicklung zu vermeiden.

② **LAN-Anschluss** – schließen Sie die Netzwerkgeräte über ein geeignetes Twisted-Pair-Kabel (TP-Kabel) an die Ports des LANCOM Switches an. Die Anschlüsse erkennen die mögliche Übertragungsgeschwindigkeit und die Pin-Belegung automatisch (Autosensing).

 Verwenden Sie nur normgerechte TP-Kabel der Kategorie CAT 5 oder besser mit einer maximalen Länge von 100 m, um eine einwandfreie Datenübertragung zu gewährleisten. Crossover-Kabel mit gekreuzten Kontakten können aufgrund der Autosensing-Funktion ebenfalls verwendet werden.

 Zur Nutzung der Glasfaseranschlüsse sind zusätzliche Module erforderlich, die Sie als Zubehör erwerben können.


③ **Konfiguration über serielle Schnittstelle** – Um den LANCOM Switches direkt konfigurieren zu können, schließen Sie das mitgelieferte serielle Konfigurationskabel an den COM-Anschluss des Gerätes an. Verbinden Sie das andere Ende dieses Kabels mit einem freien COM-Port (RS 232) an einem PC. Hinweise zur Konfiguration über die serielle Schnittstelle und die notwendigen Parameter in einem Terminal-Programm finden Sie unter → 'Command Line Interface über serielle Verbindung starten' im folgenden Kapitel.

④ **Mit Spannung versorgen und einschalten** – versorgen Sie das Gerät über das Kaltgerätekabel mit Spannung.

⑤ **Betriebsbereit?** – Nach einem kurzen Selbsttest des Geräts leuchtet die Power-LED permanent. Grün leuchtende LAN-LINK-LEDs zeigen an, an welchen LAN-Anschlüssen funktionierende Verbindungen hergestellt sind.

2.5 Installation der Software

Der folgende Abschnitt beschreibt die Installation der mitgelieferten Systemsoftware LANtools, die unter Windows läuft.

 Sollten Sie Ihren LANCOM Switch ausschließlich mit PCs verwenden, die unter anderen Betriebssystemen als Windows laufen, können Sie diesen Abschnitt überspringen.

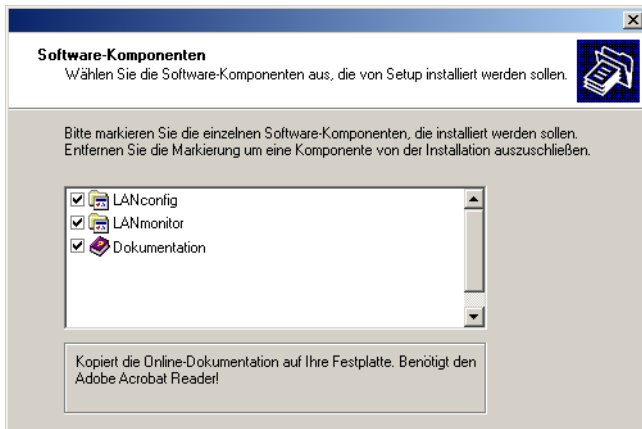
2.5.1 Software-Setup starten

Legen Sie die Produkt-CD in Ihr Laufwerk ein. Daraufhin startet das Setup-Programm automatisch.



Sollte das Setup nicht automatisch starten, so rufen Sie die Datei AUTORUN.EXE aus dem Hauptverzeichnis der LANCOM-CD auf.

Klicken Sie im Setup auf **Software installieren**. Es erscheint folgendes Auswahlmenü auf dem Bildschirm:



2.5.2 Welche Software installieren?

- **LANconfig** ist das Windows-Konfigurationsprogramm für alle LANCOM-Geräte. Mit LANconfig können Sie alle LANCOM-Geräte im Netzwerk suchen. Für einen LANCOM Switch können Sie damit die webbasierte Konfiguration starten.
- Mit **LANmonitor** überwachen Sie auf einem Windows-Rechner alle LANCOM-Geräte. Für einen LANCOM Switch können Sie damit alle wichtigen Statusinformationen wie z.B. den Link-Status oder den PoE-Zustand der Ports einsehen.
- Mit **Dokumentation** kopieren Sie die Dokumentationsdateien auf Ihren PC.

Wählen Sie die gewünschten Software-Optionen aus und bestätigen Sie mit **Weiter**. Die Software wird automatisch installiert.

3 LANCOM Switch konfigurieren und überwachen

3.1 Konfigurationsmöglichkeiten

Zur Konfiguration des Geräts stehen zwei unterschiedliche Wege zur Auswahl:

- Grafische Benutzeroberfläche über einen Browser (WEBconfig): diese Konfigurationsmöglichkeit können Sie nur über eine Netzwerkverbindung nutzen, wenn Sie das Gerät von Ihrem Rechner aus über die IP-Adresse erreichen können.

Hinweise zur Konfiguration über WEBconfig finden Sie im Kapitel "Web-basierte Konfiguration".

- Textorientierte Konfiguration über eine Konsole (Command Line Interface – CLI): diese Konfigurationsmöglichkeit können Sie über Telnet, Hyperterminal o.ä. sowohl über eine Netzwerkverbindung als auch über eine Direktverbindung über die serielle Konfigurationsschnittstelle (RS-232) nutzen.

Hinweise zur Konfiguration über CLI finden Sie im Kapitel "Command Line Interface".

3.1.1 WEBconfig starten

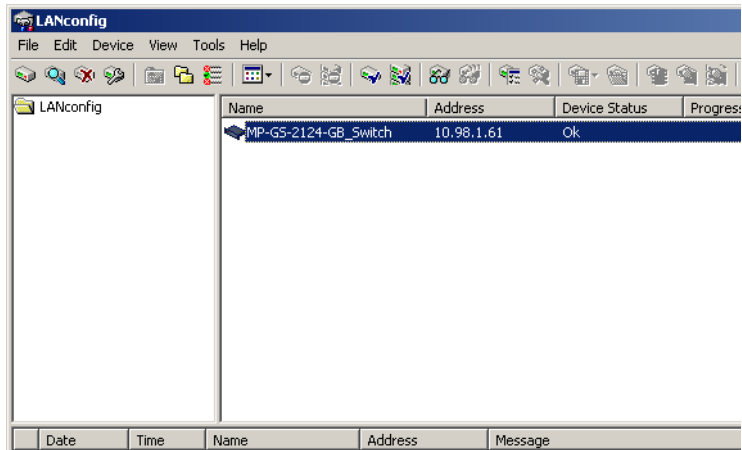
Sie können die Konfiguration über einen Browser auf zwei Wegen starten:

- Wenn Ihnen die IP-Adresse des Gerätes bekannt ist, geben Sie einfach die IP-Adresse in die Adresszeile des Browsers ein. Die bei Auslieferung gültigen Zugangsdaten lauten: Username „admin“, Password „admin“.



■ Kapitel 3: LANCOM Switch konfigurieren und überwachen

- Wenn Ihnen die IP-Adresse des Gerätes nicht bekannt ist, können Sie mit Hilfe von LANconfig danach suchen. Starten Sie dazu LANconfig über **Start ▶ Programs ▶ LANCOM ▶ LANconfig**.



LANconfig sucht automatisch nach erreichbaren Geräten in Ihrem Netzwerk. Neben anderen evtl. vorhandenen LANCOM-Geräten wird dabei auch ein LANCOM Switch gefunden und in der Liste angezeigt. Mit einem

Doppelklick auf diesen Eintrag starten Sie automatisch einen Browser zur entsprechenden IP-Adresse.

Welche IP-Adresse hat mein LANCOM Switch?

Die aktuelle IP-Adresse des LANCOM Switches nach dem Einschalten hängt von der Konstellation des Netzwerks ab.

Netzwerk mit DHCP-Server – Der LANCOM Switch ist bei Auslieferung auf den Auto-DHCP-Modus eingestellt, er sucht also nach einem DHCP-Server, der ihm eine IP-Adresse, die Subnetzmaske und die Adresse des Gateways zuweisen kann. Die zugewiesene IP-Adresse kann dann über entsprechende Tools oder den DHCP-Server ermittelt werden. Handelt es sich beim DHCP-Server z.B. um ein LANCOM-Gerät, so kann die IP-Adresse des LANCOM Switches in der DHCP-Tabelle nachgesehen werden. Der LANCOM Switch kann in diesem Fall von jedem Rechner aus dem Netzwerk erreicht werden, der ebenfalls seine IP-Adresse vom DHCP-Server bezieht.

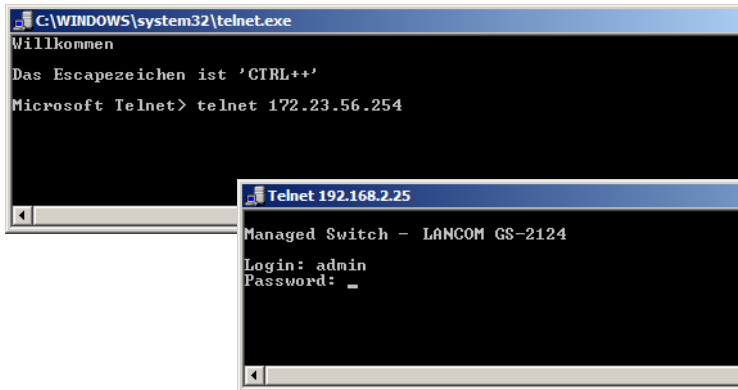
Netzwerk ohne DHCP-Server – Falls im Netzwerk kein DHCP-Server vorhanden ist, so verwendet der LANCOM Switch automatisch die Adresse "172.23.56.250".

Der LANCOM Switch kann in diesem Fall von jedem Rechner aus dem Netzwerk erreicht werden, der auf eine IP-Adresse aus dem Adressbereich "172.23.56.x" eingestellt ist.

3.1.2 Command Line Interface über Netzwerk starten

Wenn Ihnen die IP-Adresse des Gerätes bekannt ist (siehe auch vorhergehender Abschnitt) und der LANCOM Switch von Ihrem Rechner aus über das Netzwerk erreichbar ist, können Sie das Command Line Interface über das Netzwerk nutzen.

- 1 Starten Sie dazu z.B. eine Konsole wie Telnet und geben Sie als Ziel die aktuelle IP-Adresse des Gerätes ein.
- 2 Melden Sie sich mit Benutzername und Kennwort an (Default: admin, admin).



3.1.3 Command Line Interface über serielle Verbindung starten

Wenn Ihnen die IP-Adresse des Gerätes nicht bekannt ist, können Sie das Command Line Interface über eine serielle Direktverbindung nutzen.

- 1 Stellen Sie über das serielle Konfigurationskabel eine Verbindung zwischen dem LANCOM Switch und dem Konfigurationsrechner her (→ 'Montage und Anschluss des LANCOM Switch').
- 2 Starten Sie auf dem Konfigurationsrechner ein Terminalprogramm, z. B. Hyperterminal auf einem Windows-System. Verwenden Sie dabei als Verbindungsparameter:
 - Baudrate: 115200
 - Stop Bits: 1
 - Data Bits: 8
 - Parity: N
 - Fluss-Kontrolle: keine
- 3 Melden Sie sich mit Benutzername und Kennwort an (Default: admin, admin).

3.2 Welche Konfiguration verwendet das Gerät?

Der Switch unterstützt vier unterschiedliche Konfigurationen: Die Start-Konfiguration, die aktuell aktive Working-Konfiguration, die Benutzer-Konfiguration und die Default-Konfiguration.

1 Start-Konfiguration

Bei Systemstart übernimmt das Gerät die Parameter aus der Start-Konfiguration und kopiert diese in die Working-Konfiguration. Bei Auslieferung ist diese Start-Konfiguration gleich der Default-Konfiguration.



Um die Start-Konfiguration zu ändern, müssen die geänderten Parameter gezielt als Start-Konfiguration gespeichert werden.

2 Working-Konfiguration:

Dies ist die aktuell im Gerät aktive Konfiguration, sie kann jederzeit verändert werden. Alle Einstellungsänderungen werden in diesen Einstellungssatz gespeichert. Wann immer Sie eine Änderung mit <Apply> (Anwenden) bestätigen, wird diese Änderung in der Working-Konfiguration gespeichert.



Die Änderungen in der Working-Konfiguration werden **nicht** automatisch in die Start-Konfiguration übernommen, sondern müssen gezielt als Start- oder User-Konfiguration gespeichert werden. Falls die Änderungen in der Working-Konfiguration nicht gespeichert werden, wird beim nächsten Systemstart wieder die vorherige Start-Konfiguration verwendet, die Änderungen an der Working-Konfiguration gehen verloren!

3 User-Konfiguration:

Diese Konfiguration ist für spezielle Anforderungen oder zu Backup-Zwecken angelegt. Sie können einen beliebigen Stand der Working-Konfiguration als User-Konfiguration speichern und diesen Zustand später mit der Funktion "Restore User Configuration" (Wiederherstellen der Benutzerkonfiguration) wiederherstellen.



Mit Hilfe der User-Konfiguration kann z. B. über die serielle Konfigurationsschnittstelle und das Command Line Interface eine funktionsfähige, gesicherte Konfiguration wieder als Start-Konfiguration geladen werden, wenn die aktuelle Start-Konfiguration fehlerhaft ist und das Gerät über das Netzwerk nicht mehr erreichbar ist.

4 Default-Konfiguration:

Dies ist die Werkseinstellung, sie kann nicht verändert werden. In der Web-Oberfläche werden folgende Möglichkeiten angeboten, den Switch auf diesen Einstellungssatz zurückzusetzen.

- Mit der Funktion "Restore Default Configuration including default IP Adress" (Auf Werkseinstellungen inklusive Default-IP-Adresse zurücksetzen) setzen Sie den Switch wieder in den Auslieferungszustand zurück (inklusive des Administrator-Kennworts und der Auto-DHCP-Einstellung).
- Die Funktion "Restore Default Configuration without changing current IP address" erlaubt es ihnen den Switch auf Werkseinstellungen zurückzusetzen, ohne dessen IP-Adresse zu verändern. Der Switch wird auch weiterhin über die von Ihnen zuletzt eingestellte IP-Adresse erreichbar sein.
- Über die serielle Konfigurationsschnittstelle können Sie das Gerät auch ohne Kenntnis des aktuellen Administrator-Kennworts auf den Auslieferungszustand zurücksetzen. Stellen Sie dazu eine serielle Verbindung zu dem Gerät her wie unter → 'Command Line Interface über serielle Verbindung starten' beschrieben. Drücken Sie im Terminalprogramm vor der Eingabe des Benutzernamens Strg+Z und verwenden Sie „RESET“ als Benutzernamen und die MAC-Adresse des geräts (ohne Leerzeichen) als Kennwort.



Mit dieser Aktion wird der Reset-Prozess gestartet, dabei werden alle Einstellungen auf den Auslieferungszustand zurückgesetzt, inklusive des Administrator-Kennworts und der Auto-DHCP-Einstellung.

3.3 Save/Restore

Der Switch unterstützt drei Kopien der Konfiguration für Konfigurations-Management: Die Default-Konfiguration, Aktive-Konfiguration, und die Benutzer-Konfiguration. Sie alle werden im Folgenden beschrieben.

■ Default Configuration:

Diese Konfiguration ist werksseitig festgelegt und lässt sich nicht verändern. Im Web-UI gibt es zwei Möglichkeiten die Default-Konfiguration des Switches wiederherzustellen. Zum einem "Restore Default Configuration including default IP address", bei der neben der Default-Konfiguration auch die Default-IP-Adresse wiederhergestellt wird. Die zweite Option ist "Restore Default Configuration without changing current IP

address“, bei der nur die Konfiguration auf den Werkzustand versetzt wird, die IP-Adresse jedoch nicht geändert wird.

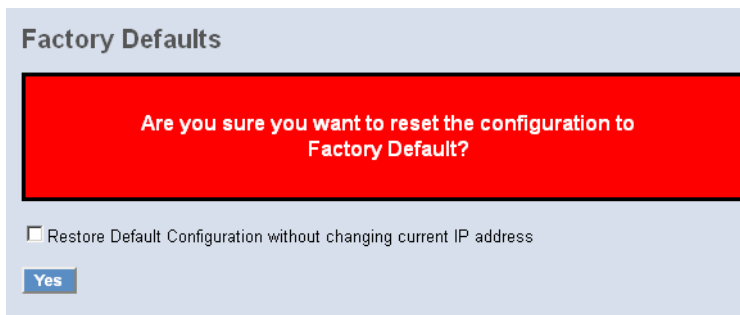
- Working Configuration:

Dies ist die aktuell aktive Konfiguration, sie lässt sich jederzeit verändern. Alle Konfigurationen werden in diese Konfigurations-Datei gespeichert. Wann immer Sie in einem Dialog <Apply> klicken, wird diese Konfiguration aktualisiert.

- User Configuration:

Dies ist die Konfigurations-Datei für Backup-Zwecke, sie lässt sich immer aus der aktuellen Konfiguration aktualisieren. Sie lässt sich durch “Restore User Configuration” wiederherstellen.

3.3.1 Factory Defaults



Factory Defaults

Are you sure you want to reset the configuration to Factory Default?

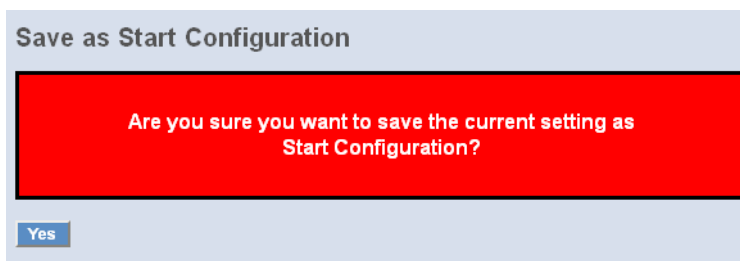
Restore Default Configuration without changing current IP address

Yes

- Restore Default Configuration (includes default IP address)

Dieses Feature kann die werksseitigen Einstellungen wiederherstellen und damit die Start-Konfiguration ersetzen. Die IP-Adresse des Switches wird auch auf 192.168.1.1 zurückgesetzt.

3.3.2 Save Start



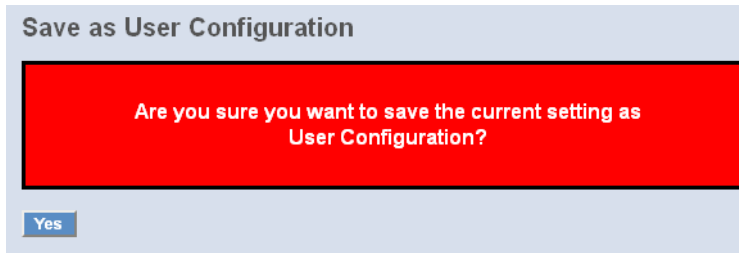
Save as Start Configuration

Are you sure you want to save the current setting as Start Configuration?

Yes

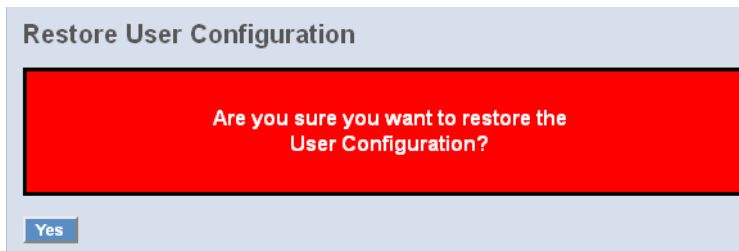
- **Save As Start Configuration**
Speichert die aktuelle Konfiguration als die Start-Konfiguration in den Flash-Speicher.

3.3.3 Save User



- **Save As User Configuration**
Speichert die aktuelle Konfiguration als die Benutzer-Konfiguration in den Flash-Speicher.

3.3.4 Restore User



- **Restore User Configuration**
Hier können Sie die letzte als funktionierend bekannte Benutzer-Konfiguration aus dem Flash-Speicher wiederherstellen und damit die Start-Konfiguration aktualisieren. Nach dem Wiederherstellen der Konfiguration wird die Start-Konfiguration aktualisiert und die Änderungen werden nach einem Reboot wirksam.

3.4 Export/ Import Configuration File

The screenshot shows a configuration panel with three sections:

- Export Configuration File:** A dropdown menu set to 'Current' and an 'Export' button.
- Import Start Configuration File:** A text input field with a 'Durchsuchen...' button and an 'Import' button.
- Import User Configuration File:** A text input field with a 'Durchsuchen...' button and an 'Import' button.

- Config File

Hier können Sie die Start- und Benutzerkonfiguration per TFTP als Backup sichern oder laden.
- Parameter:
 - Export File Path:

Export Start: Exportiert die aktuelle Start-Konfiguration aus dem Flash-Speicher

Export User-Conf: Exportiert die Benutzer-Konfiguration aus dem Flash-Speicher.
 - Import File Path:

Import Start: Importiert eine Start-Konfiguration in den Flash-Speicher.

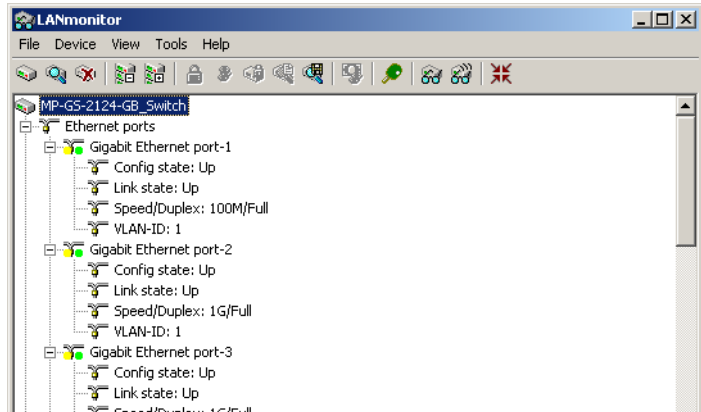
Import User-Conf: Importiert eine Benutzer-Konfiguration in den Flash-Speicher.

3.5 LANCOM Switch mit LANmonitor überwachen

Der Zustand des Gerätes und der einzelnen Ports kann über die LEDs an der Vorderseite beobachtet werden. Mit dem LANmonitor kann diese Überwachung sehr komfortabel von jedem Arbeitsplatz aus geschehen – ohne direkte Sichtverbindung zu den LEDs. Neben den Statusinformationen der LEDs können mit dem LANmonitor noch weitere wichtige Zustandsinformationen über die Ports abgefragt werden.

3.5.1 Status der Ethernet-Ports

Der LANmonitor zeigt für alle Ethernet-Ports des Gerätes den aktuellen Status an. Dabei wird sowohl der vom Administrator konfigurierte Status angezeigt (Config-Status) als auch der tatsächliche Verbindungs-Status des Ports (Link-Status). Dazu wird jeder Port mit zwei farbigen Punkten im LANmonitor dargestellt:



- Der linke Punkt zeigt den Config-Status:
 - grau: der Port ist in der Konfiguration deaktiviert
 - gelb: der Port ist in der Konfiguration aktiviert
- Der rechte Punkt zeigt den Link-Status:
 - grau: an den Port ist kein aktives Netzwerkgerät angeschlossen
 - grün: an den Port ist ein Netzwerkgerät angeschlossen und aktiv

Neben dem Status zeigt LANmonitor außerdem die VLAN-ID für jeden Port an und für aktive Ports mit aktiven Netzwerkgeräten die ermittelte Übertragungsgeschwindigkeit.

4 Anleitung zum webbasierten Management

Dieses Kapitel zeigt Ihnen, wie Sie mit Hilfe des webbasierten Managements (WEBconfig) den LANCOM GS-2124 konfigurieren. Auf diese Weise erhalten Sie einen Zugang zu jedem Port und Status des Switches. Ebenso können Sie den MIB-Status, Spanning Tree Status, Prioritätenstatus, den Multicast Traffic und VLAN Status einsehen sowie die unerlaubte Nutzung überwachen.

Die Grundeinstellungen des Switchs sind in der folgenden Tabelle aufgelistet:

LANCOM GS-2124	
IP Adress	172.23.56.250
Subnet Mask	255.255.255.0
Default Gateway	172.23.56.254
Default DNS-Server	172.23.56.254
Username	admin
Password	admin

Wenn Sie die erste Konfiguration des Switchs mit Hilfe des Command Line Interfaces durchgeführt und dabei die IP-Adresse geändert haben, können Sie die entsprechende IP-Adresse eingeben, z.B. <http://192.168.1.1>. Sie sehen den folgenden Bildschirm, in dem Sie Ihren Benutzernamen und Ihr Passwort zur Authentifizierung eingeben müssen. Wenn Sie sich das erste Mal einloggen, geben Sie sowohl als Benutzername wie auch als Passwort "admin" ein und schließen die Anmeldung ab, indem Sie auf <Login> klicken.


In den Switch können sich gleichzeitig maximal drei Benutzer einloggen. Das Gerät erlaubt jedoch jeweils nur einem Administrator, das System zu konfigurieren. Wenn gleichzeitig mehrere Administratoren eingeloggt sind, erlaubt der Switch demjenigen Administrator das System zu konfigurieren, der sich als erster eingeloggt hat. Die anderen Benutzer können in diesem Fall, auch wenn sie Administratorrechte besitzen, das System nur überwachen.


Zur Darstellung des WEBconfig empfehlen wir mindestens Microsoft Internet Explorer 6.0, Netscape V7.1 oder FireFox V1.00 und eine Bildschirmauflösung von 1024x768.



4.1 Übersicht über das webbasierte Management

Nach dem Einloggen sehen Sie auf dem Bildschirm die Systeminformationen, wie "Model Name", "System Description", "Location", "Contact", "Device Name", "System Up Time", "Current Time", "BIOS Version", "Firmware Version", "Hardware-Mechanical Version", "Serial Number", "Host IP Address", "Host MAC Address", "Device Port", "RAM Size" and "Flash Size". Sie erhalten auch Informationen über die Software Version, die MAC Adresse, die Seriennummer, die Anzahl der Ports usw. .





Auto Logout 3

GS-2124

System

Security

Configuration

Management

Logout

Basic Config

Port

System Information

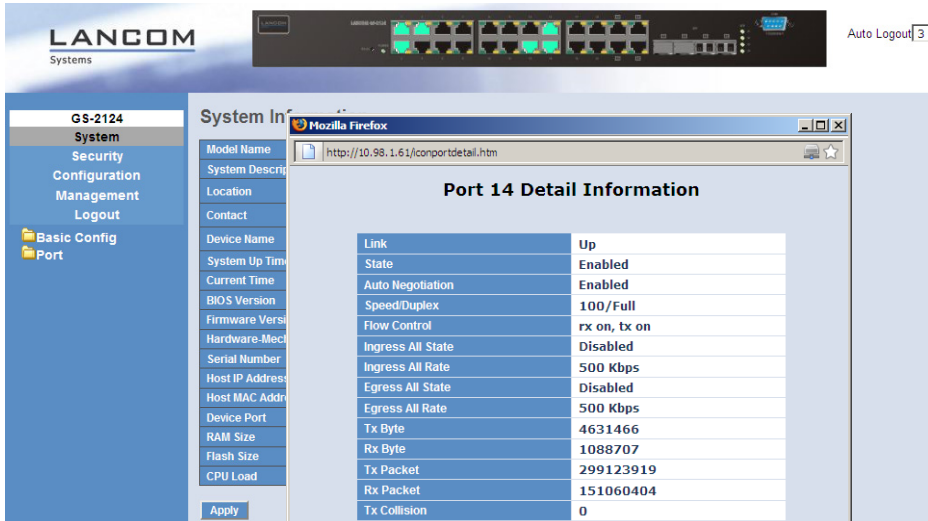
Model Name	LANCOM GS-2124
System Description	24 Gigabit Port L2 Managed Switch
Location	Home_MPLum
Contact	mp@lancom.de
Device Name	MP-GS-2124-GB_Switch
System Up Time	2 Days 17 Hours 11 Mins 30 Secs
Current Time	Fri Apr 17 15:57:05 2009
BIOS Version	V1.04
Firmware Version	v1.31
Hardware-Mechanical Version	V1.01-V1.01
Serial Number	032109000004
Host IP Address	10.98.1.61
Host MAC Address	00-40-c7-5c-00-73
Device Port	UART * 1, TP * 20, Dual-Media Port(RJ45-SFP) * 4
RAM Size	512 M
Flash Size	128 M
CPU Load	14%

Apply

Informationen zum Seiten-Aufbau

Oben auf der Seite sehen Sie die Vorderseite des Switchs. Die verlinkten Ports leuchten grün, im Gegensatz dazu leuchten die unverlinkten Ports nicht.

Mit einem Klick auf die einzelnen Ports in der Grafik öffnen Sie ein Fenster mit Detail-Informationen (gegebenenfalls Pop-Up-Blocker ausschalten).



The screenshot displays the LANCOM GS-2124 web management interface. At the top, there is a header with the LANCOM logo and a photo of the switch. Below the header is a navigation menu on the left with the following items: GS-2124, System, Security, Configuration, Management, Logout, Basic Config, and Port. The main content area shows the 'Port 14 Detail Information' window, which contains the following table:

Link	Up
State	Enabled
Auto Negotiation	Enabled
Speed/Duplex	100/Full
Flow Control	rx on, tx on
Ingress All State	Disabled
Ingress All Rate	500 Kbps
Egress All State	Disabled
Egress All Rate	500 Kbps
Tx Byte	4631466
Rx Byte	1088707
Tx Packet	299123919
Rx Packet	151060404
Tx Collision	0

Das Detailfenster zeigt die grundlegenden Informationen zum Status, zum Traffic und der Bandbreite für den jeweiligen Ein- und Ausgang eines gewählten Ports.

In der Ecke rechts oben befindet sich die Zeit des Auto-Logouts, welcher Sie nach dem Verlassen des Programms vor unberechtigten Nutzern schützt. Wenn Sie die Voreinstellung des Auto-Logouts unverändert lassen, wird sich das System drei Minuten nach der letzten Aktivität automatisch ausloggen. Wenn Sie die Funktion des Auto-Logouts ausschalten, bleiben Sie dauerhaft eingeloggt.

Auf der linken Seite sehen Sie das Hauptmenü. Wenn Sie einen Ordner öffnen, erscheint ein Untermenü. Die Funktionen jedes einzelnen Ordners sind in den entsprechenden Kapiteln erklärt. Wenn Sie eine Funktion anklicken, erfolgt die Ausführung.

4.2 System: Basic Config

4.2.1 System Information

System Information	
Model Name	LANCOM GS-2124
System Description	24 Gigabit Port L2 Managed Switch
Location	Home_MPlum
Contact	imp@lancom.de
Device Name	MP-GS-2124-GB_Switch
System Up Time	5 Days 22 Hours 6 Mins 34 Secs
Current Time	Thu Mar 26 13:21:57 2009
BIOS Version	V1.04
Firmware Version	v1.29
Hardware-Mechanical Version	V1.01-V1.01
Serial Number	032109000004
Host IP Address	10.98.1.61
Host MAC Address	00-40-c7-5c-00-73
Device Port	UART * 1, TP * 20, Dual-Media Port(RJ45-SFP) * 4
RAM Size	512 M
Flash Size	128 M
CPU Load	14%

Apply

- System Information:
Zeigt die grundlegenden Informationen des Systems an.
- Parameter:
 - Model name:
Den Modellnamen entnehmen Sie dieser Anleitung.
 - System description:
Beschreibt das System, in diesem Fall handelt es sich um ein "L2 Plus Managed Switch".
 - Location:
Dies ist der Ort an dem sich der Switch befindet (benutzerdefiniert).
 - Contact:
Hier können Sie den Namen und die Telefonnummer der Kontaktperson eingeben, die Ihnen Hilfestellung leistet. Sie können diese Einstellung über die Benutzeroberfläche oder SNMP konfigurieren.
 - Device name:
Der Name des Switchs (benutzerdefiniert). Die Voreinstellung ist "LANCOM GS-2124".

System up time:

Angabe der Zeit, seit der Switch in Betrieb genommen wurde. (Format: Tag, Stunde, Minute und Sekunde)

 Current time:

Aktuelle Zeitangabe (Format: Tag der Woche, Monat, Tag, Stunden und Minuten, z.B. Thu May 15 12:36:14 2008)

 BIOS version:

Die Version des BIOS in diesem Switch.

 Firmware version:

Die Firmware Version in diesem Switch.

 Hardware-Mechanical version:

Die Version der Hardware und der Mechanik.

 Serial number:

Die Seriennummer wird von der Fabrik vergeben.

 Host IP address:

Die IP-Adresse des Switchs.

 Host MAC address:

Die Ethernet MAC Adresse des Managers von diesem Switch.

 Device Port:

Zeigt alle Typen und Nummern des Switch-Ports.

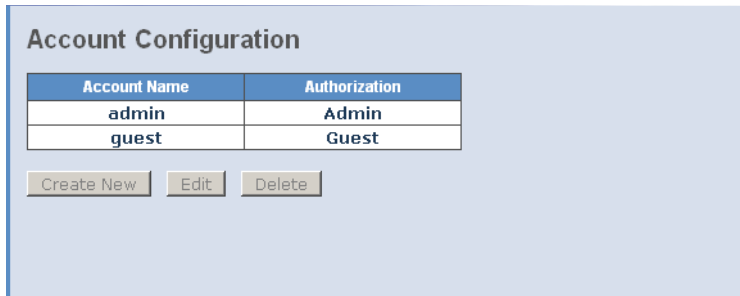
 RAM size:

Die Größe des DRAM in diesem Switch.

 Flash size:

Die Größe des Flash-speicher in diesem Switch.

4.2.2 Account



The screenshot displays the 'Account Configuration' interface. It features a table with two columns: 'Account Name' and 'Authorization'. The table contains two rows: one for 'admin' with 'Admin' authorization, and one for 'guest' with 'Guest' authorization. Below the table are three buttons: 'Create New', 'Edit', and 'Delete'.

Account Name	Authorization
admin	Admin
guest	Guest

Buttons: Create New, Edit, Delete

Mit dieser Funktion kann der Administrator den Benutzernamen und das Passwort erstellen, verändern oder löschen. Der Administrator kann die Passwörter anderer Gastbenutzer verändern ohne das Passwort zu bestätigen. Gastbenutzer können nur ihr eigenes Passwort verändern. Bitte denken Sie daran, dass Sie die jeweilige Identität (Gast/ Administrator) in dem Feld "authorization" eingeben, bevor Sie den Benutzernamen und das Passwort erstellen. Es kann nur ein Administrator angemeldet werden. Dieser kann nicht gelöscht werden. Zusätzlich können jedoch vier Accounts für Gastbenutzer erstellt werden.

- Die Voreinstellung für den Benutzer-Account ist:
Username/ Benutzername: admin
Password/ Passwort: admin

4.2.3 Time

System Time Setting	
Current Time Thu Mar 26 13:24:35 2009	
<input checked="" type="radio"/> Manual	Year <input type="text" value="2009"/> (2000~2036) Month <input type="text" value="3"/> (1~12) Day <input type="text" value="26"/> (1~31) Hour <input type="text" value="13"/> (0~23) Minute <input type="text" value="24"/> (0~59) Second <input type="text" value="35"/> (0~59)
<input checked="" type="radio"/> NTP	<input type="radio"/> 209.81.9.7(USA) <input type="radio"/> 137.189.8.174(HK) <input type="radio"/> 133.100.9.2(JP) <input type="radio"/> 131.188.3.222(Germany) <input checked="" type="radio"/> 10.98.1.33 Time Zone <input type="text" value="GMT+1:00"/>
Daylight Saving	<input type="text" value="2"/>
Daylight Saving Start	Mth <input type="text" value="3"/> Day <input type="text" value="28"/> Hour <input type="text" value="1"/>
Daylight Saving End	Mth <input type="text" value="10"/> Day <input type="text" value="28"/> Hour <input type="text" value="2"/>
<input type="button" value="Apply"/>	

Der Switch bietet den manuellen und den automatischen Weg zum Einstellen der Zeit mit NTP an. Die manuelle Einstellung ist unkompliziert, denn Sie tragen einfach Jahr, Monat, Tag, Stunde, Minute und Sekunde mit einem gültigen Wert ein. Wenn Sie einen ungültigen Wert eintragen, z.B. 61 Minuten, wird der Switch die Eingabe auf die Zahl 59 korrigieren.

NTP ist ein Protokoll, das die Uhren des Switch Zeitsystems synchronisiert. Bei NTP handelt es sich um einen Internet Entwurf, der in der dritten Version in das Protokoll eingebunden wurde und standardmäßig in RFC 1305 formalisiert wird. Der Switch besitzt vier eingebaute NTP Server IP-Adressen im Internet und eine benutzerdefinierte NTP Server IP-Adresse. Die Zeitzone ist Greenwich mean time und wird dargestellt in der Form GMT+/- xx hours.

■ Time

Stellen Sie das System manuell ein oder synchronisieren Sie die Zeitangaben mit Hilfe eines Zeit-Servers. Sie können außerdem verschiedene Zeitzonen einstellen.

■ Parameter

Current Time:

Zeigt die aktuelle Zeit des Systems an.

Manuelle Einstellung:

Mit dieser Funktion können Sie die Zeit manuell einstellen. Füllen Sie die Felder mit gültigen Werten für Jahr, Monat, Tag, Stunde, Minute und Sekunde und klicken Sie anschließend auf "apply". Mögliche Werte für die Parameter Jahr, Monat, Tag, Stunde, Minute und Sekunde sind entspre-

chend ≥ 2000 , 1-12, 1-31, 0-23, 0-59 und 0-59. Wenn Sie einen falschen Wert eingeben und "apply" drücken, wird das System die Zeiteinstellung nicht annehmen.

Default: Jahr = 2000, Monat = 1, Tag = 1, Stunde = 0, Minute = 0, Sekunde = 0

NTP:

NTP ist ein Network Time Protocol und wird dazu benutzt um die Greenwich mean time zu synchronisieren. Wenn Sie den NTP-Modus gebrauchen, wählen Sie einen eingebauten NPT Time Server oder stellen Sie manuell einen benutzerdefinierten NTP Server ein. Bestimmen Sie eine Zeitzone. Der Switch wird die Zeit synchronisieren nachdem Sie "apply" drücken. Auch wenn der Switch die Zeit automatisch synchronisiert, kann NTP die Zeit ohne die Bearbeitung des Benutzers nicht regelmäßig updaten .

Die Zeitzone ist eine offset Zeit von GMT. Bestimmen Sie zuerst die Zeitzone und führen Sie dann die Synchronisation mit Hilfe des NTP aus. Der Switch wird NTP updaten. Der Switch unterstützt konfigurierbare Zeitzone von -12 bis +13 in Schritten von einer Stunde.

Default Zeitzone: Germany +1 Stunde

Einstellung der Sommerzeit:

Für einige Länder wird die Sommerzeit übernommen. Diese Einstellung gleicht die Zeitverschiebung an oder ändert die Zeit, gemäß des Start- und Enddatums. Stellen Sie die Sommerzeit z.B. auf eine Stunde ein. Wenn das eingegebene Startdatum um eine Minute überschritten wird, so wird die Zeit des Systems eine Stunde zurückgesetzt. Wenn das Enddatum überschritten wird, wird ebenfalls so verfahren.

Die Einstellung der Sommerzeit kann -5 bis +5 Stunden betragen, in Schritten von je einer Stunde. Wenn die Zeitverschiebung von der Winter zur Sommerzeit (und umgekehrt) nicht übernommen werden muss/soll, geben Sie in das Feld eine Null ein (oder deaktivieren Sie die Sommerzeiteinstellung). Sie müssen in diesem Fall kein Start- und Enddatum angeben. Wenn Sie eine Zeitverschiebung für die Sommerzeit angeben, müssen Sie für die Aktivierung auch ein Start- und Enddatum angeben.

Default für die Einstellung der Sommerzeit: 0.

Die folgenden Parameter sind konfigurierbar für die Sommerzeiteinstellung:

- Day Light Saving Start / Start der Sommerzeit:
Gibt an, wann die Sommerzeit beginnt.
- Mth /Monat:
Eingabe 1 ~ 12; Default: 1
- Day /Tag:
Eingabe 1 ~ 31; Default: 1
- Hour/ Stunde:
Auswahl 0 ~ 23; Default: 0
- Day Light Saving End/ Ende der Sommerzeit :
Gibt an, wann die Sommerzeit endet.
- Mth/ Monat:
Eingabe 1 ~ 12; Default: 1
- Day/ Tag:
Eingabe 1 ~ 31; Default: 1
- Hour/ Stunde:
Eingabe 0 ~ 23; Default: 0

4.2.4 IP Configuration

IP Configuration

DHCP Setting	<input checked="" type="checkbox"/> Enable
IP Address	<input type="text" value="10.98.1.61"/>
Current IP Address	10.98.1.61
Subnet Mask	<input type="text" value="255.255.255.0"/>
Default Gateway	<input type="text" value="10.98.1.33"/>
Current Gateway	10.98.1.33
DNS Server	<input type="text" value="Auto"/> <input type="text" value="10.98.1.33"/>

Die IP Konfiguration ist eine der wichtigsten Systemeinstellungen des Switchs, denn hiermit kann der Netzwerkmanager die Einstellungen einsehen und bearbeiten. Sie können beim Switch manuelle IP-Adressen oder automatischen IP-Adressen mit Hilfe des DHCP Server einstellen. Wenn Sie die IP-Adresse ändern, müssen Sie den Switch neu booten und können anschließend die neue IP-Adresse für das webbasierte Management und CLI nutzen.

■ IP Configuration

Bestimmt die IP Adresse, die Subnetzmaske, Gateway und DNS (domain name system) des Switchs.

■ Parameter:

□ DHCP Einstellung:

DHCP ist die Abkürzung für Dynamic Host Configuration Protocol. Der Switch bekommt mit Hilfe des DHCP-Client automatisch eine IP-Adresse, wenn Sie die Funktion auf "enable" stellen. Bei dieser Einstellung übermittelt der Switch die Anfrage an den, sich im Netzwerk befindenden, DHCP Server, um eine IP-Adresse zu erhalten. Wenn der DHCP Server ausgeschaltet oder nicht vorhanden ist, wird der Switch so lange weiter anfragen (und dies auch anzeigen) bis der DHCP Server angeschlossen bzw. angeschaltet ist. Sie benötigen zuerst die IP-Adresse vom DHCP Server um weitere booting Prozesse ausführen zu können. Wenn Sie die Einstellung "disable" wählen, müssen Sie die IP-Adresse manuell eingeben. Weitere Details zum Thema IP-Adresse und DHCP finden Sie in Kapitel 2.1.5 "Einstellung der IP-Adresse".

Default: Disable

□ IP-Adresse:

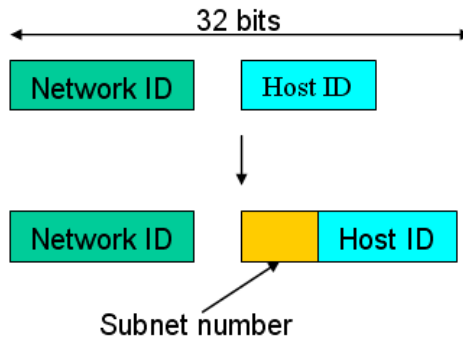
Wenn Sie die DHCP Funktion auf "disable" einstellen, können Sie die IP-Adresse konfigurieren und neue Werte eintragen. Klicken Sie zum Updaten "apply". Wenn DHCP gesperrt ist, lautet der Default "172.23.56.252" (LANCOM GS-2124). Wenn DHCP freigegeben ist, wird diese Angabe vom DHCP Server bestimmt und lässt sich nicht mehr vom Benutzer einstellen.

□ Subnetzmaske:

Die Subnetzmaske teilt die IP-Adresse des Geräts in einen Netzwerkteil und einen Geräteteil auf. Der Netzwerkteil bezeichnet das Netzwerk, in dem sich der Rechner befindet. Nur Rechner in einem gemeinsamen Netzwerk können direkt miteinander kommunizieren. Alle Geräte in anderen Netzwerken können nur über Router erreicht werden. Der Geräteteil bezeichnet dann das einzelne Gerät innerhalb des Netzwerks. Die Geräteadresse muss innerhalb eines Netzwerks eindeutig sein.

Weitere Informationen zu diesem Thema finden Sie in Kapitel "Bestimmung der IP Adresse".

Default: 255.255.255.0



□ Default gateway:

Stellen Sie eine IP-Adresse für ein Gateway ein, um mit Datenpaketen umzugehen, die die Kriterien eines Pfades nicht erfüllen. Wenn ein Datenpaket die Kriterien eines voreingestellten Pfades nicht erfüllt, muss es auf einem Default-Pfad an einen Router weitergeleitet werden. Das bedeutet, dass jedes Paket mit einer undefinierten IP-Adresse automatisch an diese Default-Einheit gesendet wird.

Default: 172.23.56.254

□ DNS (Domain Name System):

Die Übersetzung/Übermittlung der IP-Adresse und der Namensadresse erfolgt mit dem DNS Server. Der Switch unterstützt die DNS Funktion um die Adresse zum DNS Server zu senden und die zugehörige IP Adresse für den Internetzugang zu bekommen.

Es gibt zwei Wege die IP Adresse des DNS festzulegen. Die eine Möglichkeit ist der "fixed mode" und bestimmt die IP Adresse manuell. Die andere ist im "dynamic mode" welche dem DHCP Server zugewiesen ist, wenn DHCP aktiviert/freigegeben ist. Das DNS hilft Ihnen, den "mnemonic adress name" in Erinnerung zu behalten. Der default ist keine Zuteilung einer DNS Adresse.

Default: 172.23.56.254

4.2.5 Loop Detection

Loop Detection

Detection Port

Port No																							
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Locked Port

Port No																							
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Die Loop Detection wird benutzt um den Datenverkehr zu erfassen. Wenn der Switch Datenpaketen mit der selben MAC-Adresse, wie die des Ports empfängt (Looping-Detection-Datenpakete), zeigt die Loop-Detection diese Aktivität an. Der Port ist gesperrt, wenn er die Loop-Detection-Datenpakete empfangen hat. Wenn Sie den Port wieder entsperren wollen, müssen Sie den Looping-Pfad finden und ausschalten. Wählen Sie dann den gesperrten Port aus und klicken Sie auf "resume" um ihn wieder zu aktivieren.

- Loop Detection
 - Zeigt an, ob die Loop-Detection aktiv ist.
- Parameter:
 - Port No:
 - Zeigt die Portnummer an, diese liegt zwischen 1 - 24.
 - Detection Port - Enable:
 - Wenn die Portnummer ausgewählt ist und die Loop-Detection eingeschaltet ist, kann der Port Loops erfassen. Wenn der Port Loops erfasst, wird er gesperrt. (Wenn keine Loops auftreten, bleibt der Port ungesperrt.)
 - Locked Port - Resume:
 - Wenn die Portnummer ausgewählt ist, die Loop-Detection eingeschaltet ist und der Port Loops erfasst, wird er gesperrt. Wenn Resume gewählt wird, wird der gesperrte Port wieder entsperrt. (Wenn Resume nicht gewählt wird, bleibt der Port gesperrt.)

4.2.6 Management Policy

Management Policy List

Add **Delete**

Mit diesen Einstellungen kann der verantwortliche Manager das genaue Setup erstellen, um den Switch zu kontrollieren und die Anzahl der Benutzer zu bestimmen.

Die folgenden Regeln stehen Ihnen zum Management des Switchs zur Verfügung:

- 1 Wenn keine Liste existiert, werden alle Verbindungen akzeptiert.

Accept

- 2 Wenn es nur "accept lists" gibt, werden alle Verbindungen abgelehnt, außer diejenigen innerhalb des akzeptierten Bereichs.

Accept **Deny** **Accept** **Deny** **Accept**

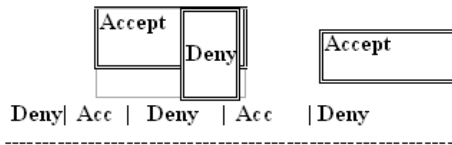
- 3 Wenn es nur "deny lists" gibt, werden alle Verbindungen akzeptiert, außer die Verbindungen innerhalb des abgelehnten Bereichs.

Deny **Accept** **Deny** **Accept** **Deny**

- 4 Wenn es sowohl "accept and deny lists" gibt, werden alle Verbindungen abgelehnt, außer die Verbindungen innerhalb des akzeptierten Bereichs.

+ **Accept** **Deny** **Deny** **Deny** **Accept** **□**

- 5 Wenn es sowohl "accept and deny lists" gibt, werden alle Verbindungen abgelehnt, außer die Verbindungen innerhalb des akzeptierten Bereichs, die nicht gleichzeitig im abgelehnten Bereich sind.



■ Management Security Configuration

Der Switch bietet verschiedene Sicherheitseinstellungen. Mit dieser Funktion kann der Manager den Modus der verbundenen Benutzer kontrollieren. Je nach Modus können Benutzer in zwei Klassen eingeteilt werden: Diejenigen, die Zugang zum Switch haben (accept) und diejenigen, die keinen Zugang zum Switch haben (deny). Einige Einschränkungen können für die Benutzer, die Zugang zum Switch haben, gemacht werden. Zum Beispiel können Sie entscheiden, welcher VLAN VID vom Switch akzeptiert oder abgelehnt wird. Auch der IP-Bereich der Benutzer, der Port für die Verbindung oder die Verbindung zum Switch über http, telnet oder SNMP kann akzeptiert oder abgelehnt werden.

■ Parameter:

- Name:
Der Name sollte maximal acht Stellen haben und kann sich aus jedem beliebigen Buchstaben des Alphabets (A-Z, a-z) sowie aus Zahlen (0-9) zusammensetzen.
- VID:
Der Switch unterstützt zwei Optionen um VLAN VID zu bestimmen, "any" und "custom". Default ist "any". Wenn Sie "custom" auswählen, können Sie eine VID Nummer eingeben. Der zugelassene Bereich der Nummer ist 1 ~ 4094 .
- IP Range:
Der Switch unterstützt zwei Optionen um den IP Range zu bestimmen, "any" und "custom". Default ist "any". Wenn Sie "custom" wählen, können Sie einen IP Bereich zuweisen. Der zugelassene Bereich ist 0.0.0.0~255.255.255.255 .
- Incoming Port:

Der Switch unterstützt zwei Optionen um den Port zu bestimmen, "any" und "custom". Default ist "any". Wenn Sie "custom" wählen, können Sie die Ports bestimmen, mit denen in der Konfiguration Management Sicherheit gearbeitet werden soll.

□ Access Type:

Der Switch unterstützt zwei Optionen um den Access Type zu bestimmen, "any" und "custom". Default ist "any". Wenn Sie "custom" wählen, können Sie den Zugriff unter den drei Optionen "http", "telnet" und "SNMP" auswählen.

□ Action:

Der Switch unterstützt zwei Optionen um die gültige Aktivität zu bestimmen, "deny" und "accept". Default ist "deny". Wenn Sie "accept" wählen, haben Sie die Autorität den Switch zu managen. Wenn Sie die Einstellung "deny" wählen, werden Sie aufgefordert den Switch mit dem von Ihnen gewählten "Access Type" zu managen.

□ Edit/Create:

Neue Einstellungen bezüglich der Sicherheit können übernommen werden, wenn die oben genannten Parameter eingestellt wurden und Sie auf "edit/create" klicken. Natürlich können Sie die Einträge auch verändern, indem Sie die jeweilige Schaltfläche betätigen.

□ Delete:

Löscht die bestehenden Einstellung der Sicherheitstabelle.

4.2.7 System Log

Der Sytem Log gibt Ihnen Informationen über System Logs, inklusive der Information darüber, wann das Gerät gebootet wurde, wie die Ports arbeiten, ob Benutzer eingeloggt sind, Sessions ablaufen und andere Systeminformationen.

■ Kapitel 4: Anleitung zum webbasierten Management

System Log

No	Time	Desc
1	Thu Mar 26 13:21:53 2009	Login [guest]
2	Thu Mar 26 13:04:00 2009	Login [guest]
3	Thu Mar 26 10:49:05 2009	Login [guest]
4	Thu Mar 26 10:43:52 2009	Login [guest]
5	Thu Mar 26 10:33:07 2009	Login [guest]
6	Thu Mar 26 10:29:28 2009	Login [guest]
7	Wed Mar 25 16:02:45 2009	Login [guest]
8	Wed Mar 25 15:57:59 2009	Login [guest]
9	Wed Mar 25 15:40:33 2009	Login [guest]
10	Wed Mar 25 15:06:22 2009	Login [guest]
11	Wed Mar 25 14:47:17 2009	Login [guest]
12	Wed Mar 25 14:34:55 2009	Login [guest]

■ System Log:

Die Trap-Log-Angabe zeigt die Log-Einträge der "SNMP Private Trap events", "SNMP Public Traps" und die Benutzer-Logs die im System auftreten. In der Reporttabelle befinden sich drei Felder mit der Nummer, dem Zeitpunkt und dem Ereignis des Trap-Protokolls.

■ Parameter:

- No.:
Zeigt die Ordnungszahl des Traps an.
- Time:
Zeigt die Zeit des Traps an.
- Desc:
Zeigt eine Beschreibung der Events im System Log.
- Clear:
Löscht die Log Daten.

4.2.8 Virtual Stack

Virtual Stack Configuration

State	Disable ▾
Role	Slave ▾
Group ID	LANCOM

Virtual Stack Management (VSM) ist die Funktion für das Gruppenmanagement. Mit der Konfiguration dieser Funktion, werden mehrere Switches in demselben LAN automatisch als Gruppe betrachtet. Ein Switch in der Gruppe wird als Master angesehen, die anderen werden so genannte "slave devices" (Folgergeräte).

VSM bietet eine einfache Management Funktion. Es ist nicht notwendig, dass Sie sich die Adresse von allen Geräten merken, denn der Manager kann das Netzwerk mit der Adresse des Masterswitchs konfigurieren. Anstelle von SNMP oder Telnet UI, ist VSM auch verfügbar in WEBconfig. Wenn Sie die Einstellung zum Masterswitch vornehmen, werden oben auf dem WEBconfig zwei Buttons für die Gruppeneinstellungen erscheinen. Wenn Sie diese Buttons anklicken, können Sie sich direkt in die Gruppeneinstellungen des WEBconfig einloggen.

Die Schaltfläche ganz links ist für das Mastergerät bestimmt. Wenn Sie auf die Schaltfläche klicken, verändert sich die Hintergrundfarbe, damit wird angezeigt, dass das Gerät von Ihnen gemanagt wird.

Hinweis: Die Gruppierung wird vorübergehend entfernt, wenn Sie sich mit Hilfe der Konsole einloggen.

Die Einstellung der Gruppe wird angezeigt als "station address" (die letzte Nummer der IP-Adresse) mit dem "device name" der Schaltfläche (z.B. 196_LANCOM GS-2124). Wenn keine entsprechende Einstellung existiert, wird "----" angezeigt.

Wenn die Gruppeneinstellung vorgenommen wurde, können Sie das System nicht mehr durch Telnet, Console oder Web konfigurieren, sondern nur noch mit Hilfe des Mastergerätes.

Es können bis zu 16 Geräte für VSM zusammengeschaltet werden, jedoch kann es in jeder Gruppe nur einen Master geben. Für die Masterredundanz können Sie mehr als zwei Master bestimmen. Der Master mit dem kleineren MAC-Wert ist der primäre Master. Jedes dieser 16 Geräte kann das Mastergerät werden und die Geräte können gegenseitig ein Backup machen.

■ Parameter:

State:

Diese Einstellung wird für die Aktivierung oder Deaktivierung des VSM gebraucht. Default ist aktiv.

Role:

Gibt die Rolle des Switchs im Virtual Stack an. Es werden zwei Typen angeboten, master oder slave (Folgergerät). Default ist master.

■ Kapitel 4: Anleitung zum webbasierten Management

□ Group ID:

Dies ist der Gruppen-Identifizierer (group identifier (GID)) des VSM. Gültig sind alle Buchstaben von A-Z, a-z, Zahlen von 0-9, die Zeichen "-" und "_". Die maximale Länge beträgt 15 Stellen.

4.3 System: Port

Dieser Zweig der Konfiguration beinhaltet die Bereiche Port Konfiguration, Port Status, Simple Counter und Detail Counter.

4.3.1 Configuration

Port Configuration						
Port	Media	Speed	Flow Control	Maximum Frame	Excessive Collision Mode	Description
1	TP	Auto	<input checked="" type="checkbox"/>	9600	Discard	Uplink zum LANCOM 1823
2	TP	Auto	<input checked="" type="checkbox"/>	9600	Discard	zum Server 10.98.1.43
3	TP	Auto	<input checked="" type="checkbox"/>	9600	Discard	Uplink GB PoE Switch > 10.98.
4	TP	Auto	<input checked="" type="checkbox"/>	9600	Discard	
5	TP	Auto	<input checked="" type="checkbox"/>	9600	Discard	
6	TP	Auto	<input checked="" type="checkbox"/>	9600	Discard	
7	TP	Auto	<input checked="" type="checkbox"/>	9600	Discard	
8	TP	Auto	<input checked="" type="checkbox"/>	9600	Discard	
9	TP	Auto	<input checked="" type="checkbox"/>	9600	Discard	
10	TP	Auto	<input checked="" type="checkbox"/>	9600	Discard	
11	TP	Auto	<input checked="" type="checkbox"/>	9600	Discard	
12	TP	Auto	<input checked="" type="checkbox"/>	9600	Discard	
13	TP	Auto	<input checked="" type="checkbox"/>	9600	Discard	
14	TP	Auto	<input checked="" type="checkbox"/>	9600	Discard	dLAN Schlafzimmer 10.98.1.46
15	TP	Auto	<input checked="" type="checkbox"/>	9600	Discard	oAP310 10.98.1.38
16	TP	Auto	<input checked="" type="checkbox"/>	9600	Discard	dm600 10.98.1.47
17	TP	Auto	<input checked="" type="checkbox"/>	9600	Discard	
18	TP	Auto	<input checked="" type="checkbox"/>	9600	Discard	
19	TP	Auto	<input checked="" type="checkbox"/>	9600	Discard	
20	TP	Auto	<input checked="" type="checkbox"/>	9600	Discard	
21	TP	Auto	<input checked="" type="checkbox"/>	9600	Discard	
	SFP	Auto				
22	TP	Auto	<input checked="" type="checkbox"/>	9600	Discard	
	SFP	Auto				
23	TP	Auto	<input checked="" type="checkbox"/>	9600	Discard	
	SFP	Auto				
24	TP	Auto	<input checked="" type="checkbox"/>	9600	Discard	
	SFP	Auto				

Apply

In der Port-Konfiguration können Sie Einstellungen für jeden Port vornehmen. Die folgenden Einstellungen können von Ihnen vorgenommen werden.

■ Port Konfiguration

Hier können Sie den Operations-Modus für jeden Port festlegen.

■ Parameter:

□ Speed/Duplex:

Hier können Sie die Geschwindigkeit und Duplex-Methode des Ports festlegen. Bei der Geschwindigkeit können Sie zwischen 10, 100 und 1000 MBit/s Baud-Rate für Fast-Ethernet an den Ports 1-24 wählen. Wenn an die SFP-Ports 21, 22, 23 und/oder 24 ein Glasfaserkabel angeschlossen ist, wird die Geschwindigkeit automatisch auf 1000 MBit/s festgelegt. Mit einem Twisted-Pair-Kabel können Sie die Geschwindigkeit an diesen Ports zwischen 10/100/1000 MBit/s wählen. Beim Duplex-Modus haben Sie die Wahl zwischen "half duplex" (Semiduplex) und "full duplex" (Vollduplex).

Die folgende Tabelle fasste alle Konfigurationsoptionen zusammen.

Media type	NWay	Speed	Duplex
100M TP	ON/OFF	10/100M	Full/Half
1000M TP	ON/OFF	10/100/1000M	Full for all, Half for 10/100
1000M Fiber	ON/OFF	1000M	Full

Im automatischen Verhandlungs-Modus (Auto-Negotiation) ist kein Default-Wert gesetzt. Im erzwungenen Modus (Forced Mode) bestimmt Ihre Einstellung den Default-Wert.

□ Flow Control:

Bei der Flusskontrolle (Flow Control) können Sie zwischen dem symmetrischen und dem asymmetrischen Modus wählen. Im symmetrischen Modus können beide Partner ein "PAUSE"-Paket senden, wenn sie überlastet sind. Im asymmetrischen Modus wird ein Gerät, das nur empfängt, die "PAUSE"-Pakete anderer Geräte beachten, aber selber keine versenden. Dies bezeichnet man als unidirektionale Flusskontrolle. Default: Symmetric (Symmetrisch).

□ Maximum Frame:

Hier können Sie den Wert für die maximale Länge der Datenpakete im Bereich von 1518 bis 9600 Bytes einstellen.

□ Excessive Collision Mode:

Für das Verhalten bei einer aussergewöhnlich hohen Anzahl von Datenkollisionen können zwei Varianten gewählt werden:

Discard: Mit der Einstellung "Discard" werden Datenpakete bei aussergewöhnlich häufigen Kollisionen verworfen. Dieses Verhalten entspricht dem Standard IEEE 802.3 bei Halb-Duplex-Verbindungen.

mode determines whether the MAC drop frames after an excessive collision has occurred. If set, a frame is dropped after excessive collisions. This is IEEE Std 802.3 half-duplex flow control operation.

Restart: Mit der Einstellung "Restart" werden Datenpakete bei aussergewöhnlich häufigen Kollisionen nicht verworfen, sondern erneut gesendet. Dieses Verhalten stellt eine Verletzung des Standards IEEE 802.3 bei Halb-Duplex-Verbindungen dar, ist aber in manchen Anwendungen nützlich.

4.3.2 Status

Port Status

Port	Link	Speed	Flow Control		Description	Media
			Rx	Tx		
1	up	100fdx	√	√	Uplink zum LANCOM 1823	TP
2	up	1Gfdx	√	√	zum Server 10.98.1.43	TP
3	up	1Gfdx	X	X	Uplink GB PoE Switch > 10.98.1.62	TP
4	down	down	X	X		TP
5	down	down	X	X		TP
6	down	down	X	X		TP
7	down	down	X	X		TP
8	down	down	X	X		TP
9	down	down	X	X		TP
10	down	down	X	X		TP
11	down	down	X	X		TP
12	down	down	X	X		TP
13	down	down	X	X		TP
14	up	100fdx	√	√	dLAN Schlafzimmer 10.98.1.46	TP
15	up	100fdx	√	√	OAP310 10.98.1.38	TP
16	up	100fdx	X	X	dm600 10.98.1.47	TP
17	down	down	X	X		TP
18	down	down	X	X		TP
19	down	down	X	X		TP
20	down	down	X	X		TP
21	down	down	X	X		TP
22	down	down	X	X		TP
23	down	down	X	X		TP
24	down	down	X	X		TP

Im Port-Status werden Informationen über den Status aller Ports gesammelt und angezeigt. Die Einträge können nach Port-Nummer, Medium, Link-Sta-

tus, Port-Status, Status der Auto-Negotiation, Geschwindigkeit/Duplex, PX-Pause und TX-Pause sortiert werden. Für die Ports 21, 22, 23 und 24 wird eine zusätzliche Information über den Medien-Typ angezeigt.

■ Port-Status

Zeigt den aktuellen Status aller Ports im Switch. Die Anzeige wird alle 5 Sekunden aktualisiert, so dass geänderte Zustände der Ports schnell angezeigt werden.

■ Parameter

□ Port No:

Die Nummer des Ports von 1 bis 24.

□ Media:

Der an den Ports angeschlossene Medien-Typ. Die Ports 21, 22, 23 und 24 sind optionale Module, die sowohl Glasfaser-Kabel als auch UTP-Kabel für Gigabit Ethernet (1000Mbit/s) oder 10/100Mbit/s Fast Ethernet unterstützen. Die Ports können unterschiedliche Medien verwalten. Für einen Glasfaser-Port können umfangreiche Informationen über den Anschlusstyp, die Entfernung usw. angezeigt werden.

□ Link:

Zeigt an, ob der Port aktiv ist oder nicht. Wenn der Port mit einem aktiven Netzwerkgerät verbunden ist, zeigt der Link "Up", sonst "Down". Dieser Zustand bezieht sich auf beide Seiten der Verbindung.

Kein Default-Wert.

□ State:

Zeigt an, ob die Datenübertragung für den Port aktiviert oder deaktiviert ist. Wenn die Datenübertragung aktiviert ist, können über diesen Port Daten empfangen und versendet werden. Wenn die Datenübertragung deaktiviert ist, können über den Port keine Daten übertragen werden. Der Port-Status wird vom Anwender eingestellt.

Default: aktiviert.

□ Auto Nego.:

Zeigt den Aushandlungsmodus für die Ethernet-Verbindung. Wenn die Auto-Negotiation (automatische Aushandlung) aktiviert ist, werden die Verbindungsgeschwindigkeit und die Duplexfähigkeit zwischen dem Switch und dem angeschlossenen Netzwerkgerät automatisch ausgehandelt. Dabei wird die beste Verbindungsmöglichkeit gewählt. Wenn die Auto-Negotiation deaktiviert ist, müssen

die beiden Geräte auf die gleichen Werte für Geschwindigkeit und Duplex-Modus eingestellt werden, sonst geht der Port in den Zustand "Down".

Default: Aktiviert

□ Speed / Duplex:

Zeigt die Verbindungsgeschwindigkeit und den Duplex-Status des Ports. Für TP-Kabel werden die Geschwindigkeiten 10, 100 oder 1000 MBit/s unterstützt, Full- und Half-Duplex sind möglich. Für ein 1 GBit-Glasfaserkabel wird nur 1000 MBit/s unterstützt.

Der Status der Geschwindigkeit und des Duplex-Modus hängt von den Einstellungen für die automatische Verhandlung und den Vorgaben des Benutzers ab.

Default: Keiner. Hängt von den Ergebnissen der automatischen Aushandlung ab.

□ Rx Pause:

Das Verfahren beim Annehmen von PAUSE-Frames. Wenn diese Option aktiviert ist, beachtet der Port die PAUSE-Frames, anderenfalls ignoriert er sie.

Default: Keiner

□ Tx Pause:

Das Verfahren beim Versenden von PAUSE-Frames. Wenn diese Option aktiviert ist, versendet der Port die PAUSE-Frames, anderenfalls versendet er keine solchen Frames.

Default: Keiner

■ **Detail-Information für SFP-Ports:**

□ Connector Type:

Zeigt den Typ des verbundenen Kabels an, z.B. UTP, SC, ST oder LC.

□ Fiber Type:

Gibt den Modus des optischen Kabels an, also z.B. Multi-Mode, Single-Mode.

□ Tx Central Wavelength:

Gibt die zentrale Wellenlänge des Glasfaserkabels an, z.B. 850 nm, 1310 nm, 1550 nm etc.

- Baud Rate:
Zeigt die maximal unterstützte Baud-Rate des Glasfasermoduls an.
Zum Beispiel 10M, 100M, 1G etc.
- Vendor OUI:
Hier können Sie den Hersteller-OUI-Code ablesen, der von der IEEE verliehen wird.
- Vendor Name:
Hier können Sie den Hersteller-Namen des Modul-Herstellers ablesen.
- Vendor P/N:
Zeigt an, wie der Modul-Hersteller das Modul bezeichnet.
- Vendor Rev (Revision):
Zeigt die Revisions-Nummer des Moduls.
- Vendor SN (Serial Number):
Hier können Sie die Seriennummer des Moduls ablesen. Sie wird vom Modul-Hersteller festgelegt.
- Date Code:
Zeigt das Herstellungs-Datum des Moduls.
- Temperature:
Hier finden Sie die aktuelle Temperatur des Moduls.
- Vcc:
Zeigt die Gleichstrom-Spannung an, die am Modul anliegt.
- Mon1(Bias) mA:
Zeigt die Vorspannung des Moduls.
- Mon2(TX PWR):
Zeigt den Übertragungsstrom des Moduls.
- Mon3(RX PWR):
Zeigt die Empfangsleistung des Moduls.

4.3.3 Simple Counter

Port Statistics Overview									Auto-refresh <input type="checkbox"/>	Refresh	Clear
Port #	Packets		Bytes		Errors		Drops				
	Receive	Transmit	Receive	Transmit	Receive	Transmit	Receive	Transmit			
1	16267179	12099516	15155825112	2931467884	246	0	246	0			
2	5104210	7415085	2260606921	7864373317	0	0	0	0			
3	477554	1551601	69489750	905182762	0	0	0	0			
4	0	0	0	0	0	0	0	0			
5	0	0	0	0	0	0	0	0			
6	0	0	0	0	0	0	0	0			
7	0	0	0	0	0	0	0	0			
8	0	0	0	0	0	0	0	0			
9	0	0	0	0	0	0	0	0			
10	0	0	0	0	0	0	0	0			
11	3713014	5420036	1083072850	6486441238	0	0	4	0			
12	0	0	0	0	0	0	0	0			
13	0	0	0	0	0	0	0	0			
14	8087339	2746758	1031732803	350401436	0	0	0	0			
15	1601531	2843855	461282165	1437049234	1	0	1	0			
16	1580029	2708987	130597568	314423594	0	0	0	0			
17	0	0	0	0	0	0	0	0			
18	0	0	0	0	0	0	0	0			
19	0	0	0	0	0	0	0	0			
20	0	0	0	0	0	0	0	0			
21	0	0	0	0	0	0	0	0			
22	0	0	0	0	0	0	0	0			
23	0	0	0	0	0	0	0	0			
24	0	0	0	0	0	0	0	0			

Der einfache Zähler (Simple Counter) zeichnet alle Pakete, die die Ports durchlaufen auf, sowohl fehlerfreie als auch fehlerhafte.

In der Abbildung sehen Sie wie alle Zähler für einen Port gleichzeitig angezeigt werden können. Dabei kann jedes Datenfeld mit einem 20-Digit langen Datenstring gefüllt sein. Wenn der Zähler ein bestimmtes Maximum überschreitet, wird er wieder zurückgesetzt und beginnt das Zählen von Neuem. Sie können das Interval (zwischen 3 und 10 Sekunden) festlegen, indem die Daten aktualisiert werden. Default-Einstellung ist 3 Sekunden.

■ Simple Counter

Zeigt Ihnen eine Zusammenfassung des Datenverkehrs für einen Port an. Es werden die Zähler für Tx-Byte, Rx-Byte, Tx-Pakete, Rx-Pakete, Tx-Kollisionen und Rx-Fehler-Pakete dargestellt.

■ Parameters:

- Tx Byte:
Insgesamt gesendete Bytes.
- Rx Byte:
Insgesamt empfangene Bytes.

- Tx Packet:
Die Anzahl der versandten Pakete.
- Rx Packet:
Die Anzahl der empfangenen Pakete.
- Tx Collision:
Anzahl der beim Senden festgestellten Datenpaket-Kollisionen.
- Rx Error Packet:
Anzahl der empfangenen fehlerhaften Pakete.

4.3.4 Detail Counter

Detailed Port Statistics Port 1			
		Port 1	Auto-refresh <input type="checkbox"/>
		<input type="button" value="Refresh"/>	<input type="button" value="Clear"/>
Receive Total		Transmit Total	
Rx Packets	16267917	Tx Packets	12099967
Rx Octets	15155894011	Tx Octets	2931533718
Rx Unicast	15213715	Tx Unicast	12000803
Rx Multicast	103894	Tx Multicast	60387
Rx Broadcast	950062	Tx Broadcast	38777
Rx Pause	0	Tx Pause	60077
Receive Size Counters		Transmit Size Counters	
Rx 64 Bytes	1060600	Tx 64 Bytes	5793400
Rx 65-127 Bytes	3064194	Tx 65-127 Bytes	4229639
Rx 128-255 Bytes	1634836	Tx 128-255 Bytes	256611
Rx 256-511 Bytes	242656	Tx 256-511 Bytes	111882
Rx 512-1023 Bytes	372356	Tx 512-1023 Bytes	296771
Rx 1024-1526 Bytes	9673262	Tx 1024-1526 Bytes	1409464
Rx 1527-Bytes	5	Tx 1527-Bytes	0
Receive Error Counters		Transmit Error Counters	
Rx Drops	246	Tx Drops	0
Rx CRC/Alignment	246	Tx Late/Exc. Coll.	0
Rx Undersize	0		
Rx Oversize	0		
Rx Fragments	0		
Rx Jabber	0		

Der Detail-Zähler (Detail Counter) zeichnet allen Datenverkehr für einen Port auf. Auch hier wird die gesamte Menge der Datenpakete angezeigt, unabhängig ob sie fehlerfrei waren oder nicht.

Wie Sie in der Abbildung sehen können, wird hier stets nur ein Port gleichzeitig angezeigt. Um den angezeigten Port zu wechseln, klicken Sie in der "Select"-Dropdown-Liste auf einen anderen Port.

Dabei kann jedes Datenfeld mit einem 20-Digit langen Datenstring gefüllt sein. Wenn der Zähler ein bestimmtes Maximum überschreitet, wird er wieder zurückgesetzt und beginnt von neuem das Zählen. Sie können das Intervall (zwischen 3 und 10 Sekunden) festlegen, indem die Daten aktualisiert werden. Default-Einstellung ist 3 Sekunden.

■ Detail Counter

Zeigt Ihnen detaillierte Zähler-Informationen für jeden Port an. Es kann stets nur ein Port gleichzeitig dargestellt werden.

■ Parameter

- Rx Packets:
Die Anzahl der empfangenen Pakete.
- Rx Octets:
Insgesamt empfangene Bytes.
- Rx Errors:
Anzahl der empfangenen fehlerhaften Pakete.
- Rx Unicast Packets:
Die Anzahl der empfangenen Unicast-Pakete.
- Rx Broadcast Packets:
Zeigt Ihnen die Anzahl der empfangenen Broadcast-Pakete.
- Rx Multicast Packets:
Die Anzahl der empfangenen Multicast-Pakete.
- Rx Pause Packets:
Gibt Ihnen die Anzahl der empfangenen "PAUSE"-Pakete an.
- Tx Collisions:
Anzahl der beim Senden festgestellten Datenpaket-Kollisionen.
- Tx Single Collision: Anzahl der gesendeten Pakete, die genau eine Kollision hatten.
- Tx Multiple Collision:
Anzahl der gesendeten Pakete, die mehr als eine Kollision hatten.
- Tx Drop Packets:
Anzahl der wegen zu vieler Kollisionen, späten Kollisionen oder wegen des Alters des Pakets verworfenen Pakete.
- Tx Deferred Transmit:
Anzahl der wegen Überlastung des Mediums beim Senden verzögerten Pakete.
- Tx Late Collision:
Anzahl der späten Kollisionen. Dabei ist eine Kollision nach der ersten 512-Bit-Anzahl des Sendens aufgetreten.

- Tx Excessive Collision:
Anzahl der Pakete/Frames, die nicht gesendet wurden, weil bereits 16 Versuche des Sendens gescheitert sind.
- Packets 64 Octets:
Anzahl der empfangenen 64-Byte Frames/Pakete.
- Packets 65-127 Octets:
Anzahl der empfangenen 65- bis 127-Byte Frames/Pakete.
- Packets 128-255 Octets:
Anzahl der empfangenen 128- bis 255-ByteFrames.
- Packets 256-511 Octets:
Anzahl der 256- bis 511-Byte-Frames, die empfangen wurden.
- Packets 512-1023 Octets:
Anzahl der empfangenen 512- bis 1023-Byte-Frames.
- Packets 1024- 1522 Octets:
Anzahl der empfangenen 1024- bis 1522-Byte-Frames.
- Tx Packets:
Insgesamt versandte Pakete.
- TX Octets: Insgesamt versandte Datenmenge in Bytes.
- Tx Unicast Packets:
Die Anzahl der versandten Unicast-Pakete.
- Tx Broadcast Packets:
Gibt Ihnen die Anzahl der versandten Broadcast-Pakete an.
- Tx Multicast Packets:
Die Anzahl der versandten Multicast-Pakete.
- Tx Pause Packets:
Hier sehen Sie, wieviele "PAUSE"-Pakete von diesem Port gesendet wurden.
- Rx FCS Errors:
Anzahl der fehlerhaften FCS-Pakete.
- Rx Alignment Errors:
Anzahl der Pakete mit einem Alignment-Fehler.

- Rx Fragments:
Anzahl der kurzen Frames (unter 64 Bytes) mit einem ungültigen CRC (Cyclic Redundancy Check).
- Rx Jabbers:
Anzahl der langen Frames (wie im tomax_length Register angegeben) mit einem gescheiterten CRC.
- Rx Drop Packets:
Wegen Fehlen eines ausreichenden Empfangs-Buffers verworfene Frames.
- Rx Undersize Packets:
Anzahl der kurzen Frames (unter 64 Bytes) mit bestandenen CRC.
- Rx Oversize Packets:
Anzahl der großen Frames (nach dem Wert im max_length Register) mit gültigen CRC.

4.4 Security: MAC

Die MAC-Tabellen-Konfiguration beinhaltet viele Funktionen, z.B. die MAC-Tabellen-Information, MAC-Tabellen-Wartung, Static Forward, Static Filter und MAC-Alias, die nicht zu einem bestimmten Funktionstypen zugeordnet werden können. Alle Funktionen werden im Folgenden beschrieben.

4.4.1 Mac Address Table

MAC Address Table Configuration

Aging Configuration

Age time	<input type="text" value="300"/>	seconds.
Disable automatic aging	<input type="checkbox"/>	

MAC Table Learning

	Port Members																							
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Auto	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒
Disable	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒
Secure	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒

■ MAC Address Table Information

Diese Funktion ermöglicht es Ihnen das Verhalten der MAC-Tabelle einzustellen. Eine inaktive MAC-Adresse, welche die Age-out-Time der MAC-Adresse übersteigt wird aus der MAC-Tabelle gelöscht. Der Bereich der Age-out-Time liegt zwischen 10 - 1.000.000 Sekunden. Diese Einstellung hat keine Auswirkungen auf statische MAC-Adressen.

Zusätzlich kann das Lernlimit der MAC-Maintenance die Anzahl der MACs begrenzen, die jeder Port lernen kann.

■ Parameter:

□ Aging Time:

Löscht eine für diese Zeit inaktive MAC-Adresse aus der MAC-Tabelle. Dies hat keine Auswirkungen auf die statische MAC-Adresse. Der Bereich der Aging-Time der MAC-Adresse liegt zwischen 10 - 1.000.000 Sekunden. Die Default Aging-Time beträgt 300 Sekunden.

□ Disable automatic aging:

Stoppt den Aging-Timer der MAC-Tabelle. Gelernte MAC-Adressen werden dann nicht länger automatisch altern. Stop the MAC table aging timer, the learned MAC address will not age out automatically

□ Auto:

Aktiviert für diesen Port den dynamischen Lern-Mechanismus.

□ Disable:

Schaltet den dynamischen Lern-Mechanismus für diesen Port aus. Der Port wird nur noch statische MAC-Adressen verwenden.

□ Secure:

Schaltet den dynamischen Lern-Mechanismus für diesen Port aus und übergibt die dynamisch gelernten Adressen an die CPU.

□ Save:

Sichert die MAC-Tabellen-Konfiguration.

□ Reset:

Setzt die MAC-Tabellen-Konfiguration zurück.

4.4.2 Static Filter

Static Filter

MAC	VID	Alias
<input type="text"/> - <input type="text"/> - <input type="text"/> - <input type="text"/> - <input type="text"/> - <input type="text"/>	<input type="text"/>	<input type="text"/>

Apply

No	MAC	VID	Alias

Delete

■ Static Filter

Mit Hilfe des Statischen Filters können Sie das Weiterleiten von Paketen verhindern, wenn die MAC-Adresse des Pakets in der Liste eingetragen ist. Sie können diese Tabelle leicht verwalten, indem Sie MAC-Adresse, VID (VLAN ID) und Alias-Felder eingeben. Um einen Eintrag aus der Liste zu löschen, klicken Sie auf die Schaltfläche <Delete>.

■ Parameter:

- MAC:
Die MAC-Adresse ist eine sechs Byte lange Hardware-Adresse, die gewöhnlich hexadezimal geschrieben und mit Bindestrichen getrennt wird, z.B. 00 - 40 - C7 - D6 - 00 - 02
- VID:
VLAN Identifier. Wird nur verwendet, wenn tagged VLAN aktiviert ist. Der gültige Bereich ist 1 -4094.
- Alias:
Ein von Ihnen gewählter MAC-Alias.

4.4.3 Static Forward

Static Forward

MAC						Port No	VID	Alias
-	-	-	-	-	-			

Apply

No	MAC	Port	VID	Alias
----	-----	------	-----	-------

Delete

■ Static Forward

Statisches Weiterleiten erlaubt es eine MAC-Adresse einem spezifischen Port zuzuordnen. Die Liste der Statischen Weiterleitungen muss manuell erstellt werden, indem man die MAC-Adresse und deren Alias in die Liste einträgt.

Wenn eine MAC-Adresse einem spezifischen Port zugeordnet wurde, wird aller Datenverkehr zu dieser MAC-Adresse an diesen Port weitergeleitet.

Um eine MAC-Adresse in die Liste aufzunehmen, müssen Sie lediglich 4 Parameter eintragen: MAC-Adresse, zugehöriger Port, VID und Alias. Mit Hilfe des <Delete> Buttons können Sie bestehende Einträge auch wieder löschen.

■ Parameter:

- MAC:
Die MAC-Adresse ist eine sechs Byte lange Hardware-Adresse, die gewöhnlich hexadezimal geschrieben und mit Bindestrichen getrennt wird, z.B. 00 - 40 - C7 - D6 - 00 - 02
- Port No:
Die Nummer des Ports. Dieser Wert muss zwischen 1 ~24 liegen.
- VID:
VLAN Identifier. Wird nur verwendet, wenn tagged VLAN aktiviert ist. Der gültige Bereich ist 1 -4094.

- Alias:
Ein von Ihnen gewählter MAC-Alias.

4.4.4 MAC Alias

MAC Alias

	MAC	Alias
-	-	-

Apply

No	MAC	Alias

Delete

- **MAC Alias**
Mit der MAC-Alias-Funktion können Sie der MAC-Adresse einen Namen zuteilen. Damit können Sie z.B. einen unerlaubten Vorgang einer MAC-Adresse einem Benutzer zuzuordnen. Zu Beginn werden alle Paare bestehender Alias-Namen und MAC-Adressen angezeigt.
Es gibt drei MAC-Alias-Funktionen in dieser Tabelle, MAC Alias Add, MAC Alias Edit und MAC Alias Delete. Drücken Sie den Button <Create/Edit> um einen neuen Alias-Namen zu einer bestimmte MAC-Adresse hinzuzufügen oder um einen bestehenden Eintrag zu verändern oder drücken Sie <Delete> um ihn zu löschen. Sie können einen Alias-Namen mit den Buchstaben A-Z, a-z und den Zahlen 0-9 erstellen, mit einer maximalen Länge von 15 Stellen.
- **Parameter:**
 - **MAC Address:**
Die MAC-Adresse ist eine sechs Byte lange Hardware-Adresse, die gewöhnlich hexadezimal geschrieben und mit Bindestrichen getrennt wird, z.B. 00 - 40 - C7 - D6 - 00 - 02
 - **Alias:**
Ein von Ihnen gewählter MAC-Alias.

Note: Falls zu viele MAC-Adressen gelernt wurden, empfehlen wir die MAC-Adresse und zugehöriger Alias direkt einzugeben.

4.4.5 MAC Table

MAC Table Information

Port	<input checked="" type="checkbox"/> 01 <input checked="" type="checkbox"/> 02 <input checked="" type="checkbox"/> 03 <input checked="" type="checkbox"/> 04 <input checked="" type="checkbox"/> 05 <input checked="" type="checkbox"/> 06 <input checked="" type="checkbox"/> 07 <input checked="" type="checkbox"/> 08 <input checked="" type="checkbox"/> 09 <input checked="" type="checkbox"/> 10 <input checked="" type="checkbox"/> 11 <input checked="" type="checkbox"/> 12 <input checked="" type="checkbox"/> 13 <input checked="" type="checkbox"/> 14 <input checked="" type="checkbox"/> 15 <input checked="" type="checkbox"/> 16 <input checked="" type="checkbox"/> 17 <input checked="" type="checkbox"/> 18 <input checked="" type="checkbox"/> 19 <input checked="" type="checkbox"/> 20 <input checked="" type="checkbox"/> 21 <input checked="" type="checkbox"/> 22 <input checked="" type="checkbox"/> 23 <input checked="" type="checkbox"/> 24 <input checked="" type="checkbox"/> Select/Unselect All
Search	MAC: <input type="text"/> ?? - <input type="text"/> ?? - <input type="text"/> ?? - <input type="text"/> ?? - <input type="text"/> ?? VID: <input type="text"/> ?

Alias	MAC Address	Port	VID

■ Dynamic MAC Table

Zeigt den statischen oder dynamischen MAC-Leineintrag und den Status des ausgewählten Ports.

■ Parameter:

- Type:
Zeigt an, ob dynamische oder statische MAC-Adressen verwendet werden.
- VLAN:
VLAN Identifier. Wird nur verwendet, wenn tagged VLAN aktiviert ist. Der gültige Bereich ist 1 -4094.
- MAC address:
Zeigt Ihnen die MAC-Adresse des gesuchten Eintrags in der MAC-Liste an.
- Port:
Der Port an dem die gesuchte MAC-Adresse erreichbar ist.
- Refresh:
Aktualisiert die MAC-Tabelle.
- Clear:
Setzt die aktuelle Auswahl wieder zurück..
- Previous Page:
Wechselt auf die vorherige Seite.

- Next Page:
Wechselt auf die nächste Seite.

4.5 Security: VLAN

Der Switch unterstützt sowohl Tag-basierte VLAN (802.1g) als auch Port-basierte VLAN. Es können bis zu 256 aktive VLANs mit den VLAN-IDs (Identitäten) 1 bis 4094 erstellt werden. Mit den VLAN-Einstellungen können Sie Ihr Netzwerk in kleinere, leichter überschaubare Teil-Netzwerke einteilen. Sie können durch eine optimale Einstellung neben einem Gewinn an Performance- und Sicherheit auch die Notwendigkeit des Netzwerk-Managements reduzieren.

4.5.1 VLAN Mode



The screenshot shows a web-based configuration interface for VLAN Mode. At the top, the title 'VLAN Mode' is displayed. Below the title, there is a dropdown menu labeled 'VLAN Mode' with 'Tag-based' selected. Below the dropdown menu, there is an 'Apply' button.

- VLAN Mode Setting

Die WLAN.Modus-Funktion beinhaltet fünf Betriebs-Modi: Port-basiert, Tag-basiert, Metro-Modus, Double-Tag und Disable. Sie können einen davon wählen, indem Sie ihn aus dem Dropdownmenü wählen und anschließend auf <Apply> klicken. Ihre Änderungen werden sofort übernommen und angewandt.
- Parameter:
 - VLAN Mode:

Tag-based:

Ein Tag-basiertes VLAN identifiziert seine Mitglieder an deren VID. Sollten zusätzlich noch ein- und ausgehende Filter-Listen angelegt worden sein, werden diese Filter auch zusätzlich angewendet um festzustellen, ob ein Paket weitergeleitet wird. Der Switch unterstützt den 802.1q-Standard.

Jedes von Ihnen erstellte Tag-basierte VLAN muss einen VLAN-Namen und eine VLAN-ID zugewiesen bekommen. Die ID muss

zwischen 1 und 4094 liegen. Sie können insgesamt 256 VLAN-Gruppen erstellen.

Port-based:

Port-basiertes VLAN legt die Mitglieder über den Port fest. Alle Pakete von oder zu einem Mitglieder-Port werden akzeptiert. Bestehende Filterregeln werden nicht angewandt. Einziges Kriterium für eine Weiterleitung eines Pakets ist die physikalische Verbindung zu einem der Mitglieder-Ports. So kann innerhalb eines Port-basierten VLAN aus den Ports 1,2,3 und 4 nur einer dieser Ports mit den anderen Mitglieder-Ports kommunizieren, der Port 5 etwa wäre von der Interaktion ausgeschlossen. Jedes Port-basierte VLAN muss von Ihnen mit einem Namen versehen werden. Dieser Switch unterstützt maximal 24 Port-basierte VLANs.

4.5.2 Tag-based Group

Tag-Based VLAN Memberships Configuration																					
IGMP-A: IGMP Aware P-VLAN: Private VLAN GVRP-P: GVRP Propagation																					
VLAN Name					Port Members																
Del	VID	IGMP-A	P-VLAN	GVRP-P	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
				Default	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
	1	Disable	Disable	Disable																	

■ Tag-based Group Configuration

Hier finden Sie Informationen zu bereits bestehenden Tag-basierten VLANs. An dieser Stelle können Sie auch Tag-basierte VLAN komfortabel erstellen, bearbeiten oder löschen.

■ Parameter:

VLAN Name:

Ein Administrator kann dem VLAN hier einen Namen zuweisen. Beachten Sie dabei, dass der Name nur aus den Buchstaben A-Z (Klein- und Großbuchstaben) den Ziffern 0-9, sowie den Trennzeichen "-" und "_" bestehen darf. Der Name darf maximal 15 Zeichen lang sein.

- VLAN ID:
Die sogenannte VLAN-ID(Identität). Jedes Tag-basierte VLAN hat eine einzigartige VID. Diese Option erscheint nur im Tag- oder Doppel-Tag-basierten Modus.
- IGMP Proxy:
Ein IGMP Proxy erlaubt es dem Switch IGMP-Host-Nachrichten an Stelle von anderen Hosts, die mit Standard-IGMP-Interfaces gefunden wurden, zu versenden. Dieser Parameter lässt sich für jedes VLAN individuell festlegen. Ist für ein VLAN IGMP deaktiviert, wird der Switch keine IGMP-Nachrichten zwischen den Mitgliedern austauschen. Ist die Funktion dagegen aktiviert, erlaubt der Switch den Austausch und leitet die IGMP-Proxy-Router Port-Konfiguration an die Mitglieder weiter, was es Ihnen erlaubt die Pfadkosten zum Proxy zu senken. Dieser alternative Pfad wird damit zum Upstream-Interface.
- Member Port:
Hier können Sie die Mitglieder eines neu geschaffenen VLANs festlegen. Dabei beschreibt "Enable" das ein Port Mitglied des entsprechenden VLANs ist. Durch das Abhaken der Checkbox neben einem Port setzen sie den Wert für diesen Port auf "Enable" und machen ihn zu einem Mitglied des VLANs.
- Add new VLAN:
Geben Sie dem neuen Tag-basierten VLAN einen Namen, eine VID und wählen sie dann durch Abhaken der Checkboxes neben den Ports die Mitglieder. Konfigurieren Sie anschließend die SYM-VLAN-Funktion. Durch ein Klicken auf die Schaltfläche <Apply> treten ihre Änderungen in Effekt.
- Delete Group:
Durch das Klicken des <Delete>-Buttons können Sie das ausgewählte Tag-basierte VLAN löschen.

Note: Wenn Sie PVLANS (Private VLANs) nutzen möchten, finden Sie mehr Informationen im "Port Isolations"-Kapitel.

4.5.3 Port-based Group

VLAN Name		Port Members																			
Delete	Group	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
	Default	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
	1																				

■ Port-based Group Configuration

Hier finden Sie Informationen zu den bereits bestehenden Port-basierten VLANs sowie die Möglichkeit komfortabel neue VLANs zu erstellen und bestehende zu bearbeiten oder zu löschen.

■ Parameter

VLAN Name:

Hier können Sie dem VLAN einen Namen zuweisen. Beachten Sie dabei, dass der Name nur aus den Buchstaben A-Z (Klein- und Großbuchstaben) den Ziffern 0-9, sowie den Trennzeichen "-" und "_". Der Name darf maximal 15 Zeichen lang sein.

Member Port:

Hier können Sie die Mitglieder eines neu geschaffenen VLANs festlegen. "Enable" beschreibt, dass ein Port Mitglied des entsprechenden VLANs ist. Durch das Abhaken der Checkbox neben einem Port setzen Sie den Wert für diesen Port auf "Enable" und machen ihn zu einem Mitglied des VLANs.

Add Group:

Geben Sie dem neuen Port-basierten VLAN einen Namen und eine VID und wählen Sie dann durch Anhaken der Checkboxen neben den Ports die Mitglieder.

Delete Group:

Klicken Sie auf die Schaltfläche <Delete>, um den gewählten Eintrag aus der Liste zu entfernen.

4.5.4 Ports

VLAN Port Configuration

Tag Identifier:

Port #	VLAN Aware	Ingress Filtering	Frame Type	PVID	Role	Untag VID	Double Tag
1	<input type="checkbox"/>	<input type="checkbox"/>	All	1	Access	0	Disable
2	<input type="checkbox"/>	<input type="checkbox"/>	All	1	Access	0	Disable
3	<input type="checkbox"/>	<input type="checkbox"/>	All	1	Access	0	Disable
4	<input type="checkbox"/>	<input type="checkbox"/>	All	1	Access	0	Disable
5	<input type="checkbox"/>	<input type="checkbox"/>	All	1	Access	0	Disable
6	<input type="checkbox"/>	<input type="checkbox"/>	All	1	Access	0	Disable
7	<input type="checkbox"/>	<input type="checkbox"/>	All	1	Access	0	Disable
8	<input type="checkbox"/>	<input type="checkbox"/>	All	1	Access	0	Disable
9	<input type="checkbox"/>	<input type="checkbox"/>	All	1	Access	0	Disable
10	<input type="checkbox"/>	<input type="checkbox"/>	All	1	Access	0	Disable
11	<input type="checkbox"/>	<input type="checkbox"/>	All	1	Access	0	Disable
12	<input type="checkbox"/>	<input type="checkbox"/>	All	1	Access	0	Disable
13	<input type="checkbox"/>	<input type="checkbox"/>	All	1	Access	0	Disable
14	<input type="checkbox"/>	<input type="checkbox"/>	All	1	Access	0	Disable
15	<input type="checkbox"/>	<input type="checkbox"/>	All	1	Access	0	Disable
16	<input type="checkbox"/>	<input type="checkbox"/>	All	1	Access	0	Disable
17	<input type="checkbox"/>	<input type="checkbox"/>	All	1	Access	0	Disable
18	<input type="checkbox"/>	<input type="checkbox"/>	All	1	Access	0	Disable
19	<input type="checkbox"/>	<input type="checkbox"/>	All	1	Access	0	Disable
20	<input type="checkbox"/>	<input type="checkbox"/>	All	1	Access	0	Disable
21	<input type="checkbox"/>	<input type="checkbox"/>	All	1	Access	0	Disable
22	<input type="checkbox"/>	<input type="checkbox"/>	All	1	Access	0	Disable
23	<input type="checkbox"/>	<input type="checkbox"/>	All	1	Access	0	Disable
24	<input type="checkbox"/>	<input type="checkbox"/>	All	1	Access	0	Disable

■ VLAN Port Configuration

Sie können eine VID zwischen 1 und 4094 für jeden Port festlegen. Darüber hinaus können Sie für jeden Port individuell Eingangsfiler festlegen. Es gibt zwei Eingangsfiler-Regeln die sich durch den Switch anwenden lassen: Der Eingangsfiler 1 bedeutet, dass nur Pakete mit zu diesem Port passenden VID weitergeleitet werden. Der Switch wird nur Pakete an den Port weiterleiten, deren VID mit der konfigurierten VID des Ports übereinstimmt. Der zweite Filter lässt den Switch jedes Paket ignorieren, dass gar kein Tag aufweist. Sie können für die einzelnen Ports auch verschiedene Rolle auswählen: Acces, Trunk oder Hybrid.

■ Parameter:

- Port 1-24:

Nummer des Ports, auf den die Regel angewandt wird.

- VLAN Aware:
Wählen Sie hier, ob auf diesem Port die IEEE 802.1Q-Technologie angewandt wird.
- Ingress Filtering:
Wählen Sie hier, ob auf diesem Port Eingangsfiler Anwendung finden sollen.
- Frame Type:
All: Es werden alle Pakete weitergeleitet, sowohl getaggete als auch ungetaggte.
Tagged: Es werden nur getaggte Pakete weitergeleitet, nicht getaggte Pakete werden verworfen.
- PVID:
Kann einen Wert zwischen 1 und 4094 annehmen. Bevor Sie einem Port eine PVID zuweisen, müssen Sie ein Tag-basiertes VLAN mit derselben Bezeichnung anlegen. Sollte zum Beispiel ein Port x ein ungetaggttes Paket erhalten, wird der Switch diesem Paket die PVID von Port x zuweisen und es dann als getaggttes Paket weiterleiten.
- Role:
Hier können Sie den Ausgangsfiler für diesen Port festlegen. Sie haben die Wahl zwischen den Rollen Access, Trunk und Hybrid. In der Trunk-Rolle müsse alle abgehenden Pakete ein VLAN-Tag haben. Wählen Sie die Access-Rolle, werden alle abgehenden Pakete ohne VLAN-Tag verschickt. Hat ein Paket zwei Tags, wird nur eines entfernt und das Paket wird mit einem der beiden Tags verschickt. Die Hybrid-Rolle ähnelt der Trunk-Rolle, mit dem Unterschied, dass es bestimmte Pakete ohne Tag verschickt. Sie können dieses Tag individuell für jeden Port festlegen. Der Port wird allen Paketen mit diesem Tag dieses entfernen, aber ansonsten nur getaggte Pakete versenden.
- Untag VID:
Zulässige Werte sind 1 bis 4094. Dieses Feld wird nur dann angewandt, wenn die Rolle des Ports auf "Hybrid" gesetzt ist.

4.5.5 Port Isolation

Port Isolation Configuration

Port Number																							
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Wenn Sie PVLANS (Private VLANs) am Switch nutzen möchten, gehen Sie wie folgt vor:

- 1 Erstellen Sie ein VLAN als primäres VLAN und setzen Sie die VLAN ID auf 2. Aktivieren Sie bei der Erstellung den Private VLAN Service.
- 2 Weisen Sie dem VLAN neue Port-Mitglieder zu.
- 3 Diese Mitglieder müssen nun der Port-Isolation zugeordnet werden.
- 4 Durch ein Klicken auf den Button <Save> beenden Sie den PVLAN-Konfigurationsprozess.

4.5.6 Management VLAN

Management VLAN

VLAN ID

- Management VLAN
Sie können ein VLAN spezifisch Wartungs- und Managementzwecken zuordnen.
- Parameter:
 - VID:
Specific Management VLAN ID.

4.6 Security: ACL (Access-Control-List)

Die ACL (Access-Control-List) des LANCOM GS-2124 ist die meistgenutzte Funktion im IOS (Internetwork Operating System) und kontrolliert den Zugriff. Die ACL wird zum Einen für die Datenfilterung benutzt und zum Anderen um

bestimmte Teile des Datenverkehrs zu analysieren, weiterzuleiten oder zu beeinflussen.

Die ACLs sind unterteilt in EtherTypes, IPv4, ARP-Protokoll, MAC, VLAN Parameters usw. Im Folgenden wird auf die Standardlisten und die erweiterten Listen für TCP/IP eingegangen. Wenn Sie ACEs (Access Control Entry) für den Zugriff definieren, können Sie eine Richtlinie (Richtliniennummer 1-8) für jeden Port bestimmen. Dieser Umstand erleichtert es zu entscheiden, mit welcher ACL-Richtlinie Sie arbeiten werden.

4.6.1 Ports

ACL Ports Configuration

Port #	Policy ID	Action	Rate Limiter ID	Port Copy	Counter
1	1	Permit	Disabled	Disabled	16154955
2	1	Permit	Disabled	Disabled	5086192
3	1	Permit	Disabled	Disabled	472983
4	1	Permit	Disabled	Disabled	0
5	1	Permit	Disabled	Disabled	0
6	1	Permit	Disabled	Disabled	0
7	1	Permit	Disabled	Disabled	0
8	1	Permit	Disabled	Disabled	0
9	1	Permit	Disabled	Disabled	0
10	1	Permit	Disabled	Disabled	0
11	1	Permit	Disabled	Disabled	3699263
12	1	Permit	Disabled	Disabled	0
13	1	Permit	Disabled	Disabled	0
14	1	Permit	Disabled	Disabled	1723284
15	1	Permit	Disabled	Disabled	1598931
16	1	Permit	Disabled	Disabled	1566794
17	1	Permit	Disabled	Disabled	0
18	1	Permit	Disabled	Disabled	0
19	1	Permit	Disabled	Disabled	0
20	1	Permit	Disabled	Disabled	0
21	1	Permit	Disabled	Disabled	0
22	1	Permit	Disabled	Disabled	0
23	1	Permit	Disabled	Disabled	0
24	1	Permit	Disabled	Disabled	0

Apply

■ ACL Port Configuration

Die ACL-Einstellung des Switchs unterstützt bis zu 128 ACEs (Access-Control-Einträge) und verwendet diese gemeinsamen 128 ACEs für die Zugangsbestimmung. Sie können einen ACE erstellen und diesen jedem Port mit "any" hinzufügen. Sie können diesen ACE aber auch einer Richtlinie oder einem Port hinzufügen. Es gibt acht Richtlinien und jedem Port kann eine Richtlinie zugewiesen werden. Zusätzlich müssen Sie entscheiden, welche Aktionen ("permit", "deny", "rate limitation" und "port

copy“) mit den folgenden Paketen ausgeführt werden sollen: IPv4, Ether-Type, ARP Protocol, MAC Parameters und VLAN Parameters.

- Pakete ablehnen oder akzeptieren "deny" / "permit"
- Rate Limiter: Einheit: Pakete pro Sekunde (pps)
- Port Copy: 1 - 24

■ Parameter:

- Port #:
 - Portnummer 1-24
- Policy ID:
 - Richtlinien ID-Bereich: 1-8
- Action:
 - Erlaubt die Weiterleitung der eingetroffenen ACL-Pakete oder lehnt sie ab.
- Rate Limiter ID:
 - Disabled: Schaltet die Rate-Limitation ab.
 - Rate Limiter ID-Bereich: 1-16. Bestimmen Sie eine Rate-Limiter-ID für diesen Port. Die eingetroffenen ACL-Pakete werden durch die Rate-Limiter-ID-Konfiguration begrenzt.
- Port Copy:
 - Disabled: Die Funktion ist ausgeschaltet und somit werden die eingetroffenen ACL-Pakete nicht auf einen bestimmten Port kopiert.
 - Port number: 1-24. Die Funktion ist eingeschaltet und die ACL-Pakete werden auf den gewählten Port kopiert.
 - Counter: Der Zähler eines Ports wird von seinem ursprünglichen Wert Null um eins ansteigen, wenn er ein ACL-Paket empfängt.

4.6.2 Rate Limiters

ACL Rate Limiter Configuration

Rate Limiter ID	Rate (pps)
1	1K
2	16K
3	512
4	1
5	1
6	1
7	1
8	1
9	1
10	1
11	1
12	1
13	1
14	1
15	1
16	1

Apply

■ ACL Rate Limiter Configuration

Es gibt 16 Rate-Limiter-IDs. Sie können jedem Port eine Limiter-ID zuweisen. Die Rate-Limit-Konfigurationseinheit ist Paket pro Sekunde (pps).

■ Parameter:

- Rate Limiter ID:

ID-Bereich: 1-16

- Rate (pps):

1 / 2 / 4 / 8 / 16 / 32 / 64 / 128 / 256 / 512 / 1K / 2K / 4K / 8K / 16K / 32K / 64K / 128K / 256K / 512K / 1024K

4.6.3 Access Control List

Access Control List Configuration Auto-refresh **Refresh** **Clear**

Ingress Port	Frame Type	Action	Rate Limiter	Port Copy	Counters
Any	ARP	Deny	1	Disabled	142
Any	ARP	Permit	1	Disabled	40903
Any	ARP	Permit	3	Disabled	0
Any	ARP	Permit	1	Disabled	0
Any	ARP	Permit	Any	Disabled	107469
Any	undefined	Deny	Any	Disabled	0
Any	EType	Deny	Any	Disabled	0
Any	IPv4/DHCP Client (Out)	Permit	Any	Disabled	411
Any	IPv4/DHCP Server (Out)	Permit	Any	Disabled	34255
Any	IPv4/Other	Permit	Any	Disabled	26374
Any	IPv4 DIP:0.0.0.0	Permit	Any	Disabled	18
Any	undefined	Permit	Any	Disabled	0
Any	EType	Permit	Any	Disabled	0

+

■ ACL Rate Limiter Configuration

Die ACL-Einstellung des Switchs unterstützt bis zu 128 ACEs (Access-Control-Einträge) und verwendet diese gemeinsamen 128 ACEs für die Zugangsbestimmung. Sie können einen ACE erstellen und diesen jedem Port mit "any" hinzufügen. Sie können diesen ACE aber auch einer Richtlinie oder einem Port hinzufügen. Es gibt acht Richtlinien und jedem Port kann eine Richtlinie zugewiesen werden. Zusätzlich müssen Sie entscheiden, welche Aktionen ("permit", "deny", "rate limitation" und "port copy") mit den folgenden Paketen ausgeführt werden sollen: IPv4, Ether-Type, ARP Protocol, MAC Parameters und VLAN Parameters.

■ Parameter description:

□ Ingress Port:

Konfigurierbarer Bereich: Any / Policy 1-8 / Port 1-24

Any: Fügt diese ACE-Regel jeder Port-Zugangsbestimmung hinzu.
Policy 1-8: Fügt diese ACE-Regel bestimmten Richtlinien hinzu.

Port 1-24: Fügt diese ACE-Regel bestimmten Port-Zugangsbestimmungen hinzu.

■ Parameter:

□ Frame Type:

Range: Any / Ethernet Type / ARP / IPv4

Any: Beinhaltet alle Typen von Datenpaketen.

Ethernet Type: Beinhaltet alle Ethernet-Pakete.

ARP: Beinhaltet alle ARP-Protokoll-Pakete. I

IPv4: Beinhaltet alle IPv4-Protokoll-Pakete.

■ ACE Configuration

Die ACL-Einstellung des Switchs unterstützt bis zu 128 ACEs (Access-Control-Einträge) und verwendet diese gemeinsamen 128 ACEs für die Zugangsbestimmung. Sie können einen ACE erstellen und diesen jedem Port mit "any" hinzufügen. Sie können diesen ACE aber auch einer Richtlinie oder einem Port hinzufügen. Es gibt acht Richtlinien und jedem Port kann eine Richtlinie zugewiesen werden. Zusätzlich müssen Sie entscheiden, welche Aktionen ("permit", "deny", "rate limitation" und "port copy") mit den folgenden Paketen ausgeführt werden sollen: IPv4, Ether-Type, ARP Protocol, MAC Parameters und VLAN Parameters.

- Parameter:
 - Ingress Port:
 - Range: Any / Policy 1-8 / Port 1-24
 - Any: Fügt diese ACE-Regel jeder Port-Zugangsbestimmung hinzu.
 - Policy 1-8: Fügt diese ACE-Regel bestimmten Richtlinien hinzu.
 - Port 1-24: Fügt diese ACE-Regel bestimmten Port-Zugangsbestimmungen hinzu.
 - IP Protocol Filter:
 - Range: Any / Ethernet Type / ARP / IPv4
 - Any: Beinhaltet alle Typen von Datenpaketen.
 - Ethernet Type: Beinhaltet alle Ethernet-Pakete.
 - ARP: Beinhaltet alle ARP-Protokoll-Pakete. |
 - IPv4: Beinhaltet alle IPv4-Protokoll-Pakete.
 - MAC Parameters: (When Frame Type = Any)
 - DMAC Filter: Bereich: Any / MC / BC / UC
 - Any: Beinhaltet alle MAC-Zieladressen.
 - MC: Beinhaltet alle Multicast-MAC-Adressen.
 - BC: Beinhaltet alle Broadcast-MAC-Adressen.
 - UC: Beinhaltet alle Unicast-MAC-Adressen.
 - MAC Parameters: (When Frame Type = Ethernet Type)
 - SMAC Filter:
 - Range: Any / Specific
 - Any: Beinhaltet alle MAC-Quelladressen.
 - Specific: Entspricht dem SMAC-Wert einer spezifizierte MAC-Quelladresse.
 - DMAC Filter:
 - Any: Beinhaltet alle MAC-Zieladressen.
 - MC: Beinhaltet alle Multicast-MAC-Adressen.
 - BC: Beinhaltet alle Broadcast-MAC-Adressen.
 - UC: Beinhaltet alle Unicast-MAC-Adressen.
 - Specific: Entspricht dem DMAC-Wert einer spezifizierte MAC-Zieladresse.

- MAC Parameters: (When Frame Type = ARP)
 - SMAC Filter:
 - Range: Any / Specific
 - Any: Beinhaltet alle MAC-Quelladressen.
 - Specific: Entspricht dem SMAC-Wert einer spezifizierte MAC-Quelladresse.
 - DMAC Filter:
 - Range: Any / MC / BC / UC
 - Any: Beinhaltet alle MAC-Zieladressen.
 - MC: Beinhaltet alle Multicast-MAC-Adressen.
 - BC: Beinhaltet alle Broadcast-MAC-Adressen.
 - UC: Beinhaltet alle Unicast-MAC-Adressen.
- MAC Parameters: (When Frame Type = IPv4)
 - DMAC Filter:
 - Range: Any / MC / BC / UC
 - Any: Beinhaltet alle MAC-Zieladressen.
 - MC: Beinhaltet alle Multicast-MAC-Adressen.
 - BC: Beinhaltet alle Broadcast-MAC-Adressen.
 - UC: Beinhaltet alle Unicast-MAC-Adressen.
- Ether Type Parameters: (When Frame Type = Ethernet Type)
 - EtherType Filter:
 - Range: Any / Specific
 - Any: Beinhaltet alle Ethernet-Pakete.
 - Specific: Entspricht einem bestimmtem Wert eines Ethernet-Typs.
 - Ethernet Type Value:
 - The Ethernet Type Range: 0x600-0xFFFF

□ ARP Parameters: (When Frame Type = ARP)

ARP/RARP:

Range: Any / ARP / RARP / Other

Any: Beinhaltet alle ARP/RARP-Protokoll-Datenpakete.

ARP: Beinhaltet alle ARP-Protokoll-Datenpakete.

RARP: Beinhaltet alle RARP-Datenpakete.

Other: Beinhaltet andere Typen von Datenpaketen, außer ARP/RARP-Protokoll.

Request/Reply:

Range: Any / Request / Reply

Any: Beinhaltet alle ARP/RARP-Anfragen und -Antworten.

Request: Beinhaltet alle ARP/RARP-Anfrage-Datenpakete.

Reply: Beinhaltet alle ARP/RARP-Antwort-Datenpakete.

Sender IP Filter:

Range: Any / Host / Network

Any: Beinhaltet alle Sender-IP-Adressen.

Host: Beinhaltet nur eine bestimmte Sender-Host-IP-Adresse.

Network: Ein bestimmtes IP-Subnetz-Segment der Sender-IP-Maske.

Sender IP Address: Default: 192.168.1.1

Sender IP Mask: Default: 255.255.255.0

Target IP Filter:

Range: Any / Host / Network

Any: Beinhaltet alle IP-Zieladressen.

Host: Beinhaltet nur eine bestimmte IP-Host-Zieladresse.

Network: Ein bestimmtes IP-Subnetz-Segment der IP-Ziel-Maske.

Target IP Address: Default: 192.168.1.254

Target IP Mask: Default: 255.255.255.0

ARP SMAC Match:

Range: Any / 0 / 1

Any: Beides, d.h. 0 und 1

0: Die Zugangs-ARP-Datenpakete, bei denen die MAC-Quelle nicht mit der SMAC-Adresse in den MAC-Einstellungen übereinstimmt.

1: Die Zugangs-ARP-Datenpakete, bei denen die MAC-Quelle mit der SMAC-Adresse in den MAC-Einstellungen übereinstimmt.

RARP DMAC Match:

Range: Any / 0 / 1

Any: Beides, d.h. 0 und 1

0: Die Zugangs-RARP-Datenpakete, bei denen die MAC-Zieladresse nicht mit der DMAC-Adresse in den MAC-Einstellungen übereinstimmt.

1: Die Zugangs-RARP-Datenpakete, bei denen die MAC-Zieladresse mit der SMAC-Adresse in den MAC-Einstellungen übereinstimmt.

IP/Ethernet Length:

Range: Any / 0 / 1

Any: Beides, d.h. 0 und 1

0: Die Zugangs-ARP/PARP-Datenpakete, bei denen die Größe der Hardware (0x6) oder des Protokolls (0x4) nicht mit den angegebenen Werten (0x6 bzw. 0x4) übereinstimmt.

1: Die Zugangs-ARP/PARP-Datenpakete, bei denen die Größe der Hardware (0x6) oder des Protokolls (0x4) mit den angegebenen Werten (0x6 bzw. 0x4) übereinstimmt.

IP:

Range: Any / 0 / 1

Any: Beides, d.h. 0 und 1

0: Die Zugangs-ARP/PARP-Datenpakete, bei denen der Protokolltyp nicht 0x800 ist.

1: Die Zugangs-ARP/PARP-Datenpakete, bei denen der Protokolltyp 0x800 ist.

Ethernet:

Range: Any / 0 / 1

Any: Beides, d.h. 0 und 1

0: Die Zugangs-ARP/PARP-Datenpakete, bei denen der Hardwaretyp nicht 0x100 ist.

1: Die Zugangs-ARP/PARP-Datenpakete, bei denen der Hardwaretyp 0x100 ist.

- IP Parameters: (When Frame Type = IPv4 and IP Protocol Filter = Any)
IPTTL: (Time To Live)

Gibt an wie viele Router ein Datagramm durchlaufen können. Jeder Router verringert seinen Wert um eins bis er Null erreicht und das Datagramm verworfen wird. Das verhindert, dass fehlgeleitete Datagramme im Internet verbleiben.

Range: Any / Non-zero / Zero

Any: Beinhaltet alle Bedingungen für IPTTL.

Non-Zero: Beinhaltet IPTTL ist nicht gleich Null.

Zero: Beinhaltet IPTTL ist gleich Null.

- IP Fragment: (IP Fragmentation Flag)

Kontrolliert die Fragmentierung des Pakets und das Identifikationsfeld. Die Flags geben an, ob das Fragment unterteilt werden kann, ob es unterteilt ist und ob das aktuelle Fragment die Endversion des Pakets ist.

Range: Any / Yes / No

Any: Beinhaltet alle IP Fragment-Klassen.

Yes: Das Zugangsdatenpaket ist ein ein Fragmentpaket.

No: Das Zugangspaket ist kein Fragmentpaket.

- IP Option:

Eine Liste optionaler Spezifizierungen für die Sicherheitsbeschränkungen, Erfassung der Route und Quell-Routing. Nicht jedes Datagramm bietet ein Optionsfeld an.

Range: Any / Yes / No

Any: Beinhaltet alle IP-Optionen.

Yes: Das Zugangsdatenpaket ist durch die IP-Optionen festgelegt.

No: Das Zugangsdatenpaket ist nicht durch die IP-Optionen festgelegt.

SIP Filter: (SIP Source IP Address)

Range: Any / Host / Network

Any: Beinhaltet alle IP-Quell-Adressen.

Host: Beinhaltet nur eine bestimmte IP-Host-Quell-Adressen.

Network: Beinhaltet ein bestimmtes IP-Subnetz-Segment der IP-Quellmaske.

SIP Address: Default: 192.168.1.1

SIP Mask: Default: 255.255.255.0

DIP Filter: (DIP Destination IP Address)

Range: Any / Host / Network

Any: Beinhaltet alle IP-Zieladressen.

Host: Beinhaltet nur eine bestimmte IP-Host-Zieladresse.

Network: Beinhaltet ein bestimmtes IP-Subnetz-Segment der IP-Zielmaske.

DIP Address: Default: 192.168.1.254

DIP Mask: Default: 255.255.255.0

□ IP Parameters: (Frame Type = IPv4 and IP Protocol Filter = ICMP)

ICMP Type Filter:

Range: Any / Specific

Any: Beinhaltet alle Typen von ICMP-Werten.

Specific: Entspricht der Einstellung des ICMP-Wertes für die Zugangsbestimmung.

ICMP Type Value: Range: 0-255

ICMP Code Filter:

Range: Any / Specific

Any: Beinhaltet alle ICMP-Code-Werte.

Specific: Entspricht der Einstellung des ICMP-Code-Wertes für die Zugangsbestimmung.

ICMP Code Value: Range: 0-255

- IP Parameters: (Frame Type = IPv4 and IP Protocol Filter = UDP)

Source Port Filter:

Range: Any / Specific / Range

Any: Beinhaltet alle UDP-Quell-Ports.

Specific: Entspricht der Quell-Port-Nummer für die Zugangsbestimmung.

Range: Entspricht der Einstellung des Quell-Ports-Bereichs für die Zugangsbestimmung.

Source Port No.: Range: 0-65535

Source Port Range.: Range: 0-65535

Dest. Port Filter:

Range: Any / Specific / Range

Any: Beinhaltet alle UDP-Zielports.

Specific: Entspricht der Ziel-Port-Nummer für die Zugangsbestimmung.

Range: Entspricht der Einstellung des Ziel-Port-Bereichs für die Zugangsbestimmung.

Dest. Port No.: (Destination Port Number)

Range: 0-65535

Dest. Port Range.: (Destination Port Range)

Range: 0-65535

- IP Parameters: (Frame Type = IPv4 and IP Protocol Filter = TCP)

Source Port Filter:

Range: Any / Specific / Range

Any: Beinhaltet alle TCP- Quell-Ports.

Specific: Entspricht der Quell-Port-Nummer für die Zugangsbestimmung.

Range: Entspricht der Einstellung des Quell-Ports-Bereichs für die Zugangsbestimmung.

Source Port No.: Range: 0-65535

Source Port Range.: Range: 0-65535

Dest. Port Filter:

Range: Any / Specific / Range

Any: Beinhaltet alle TCP-Ziel-Ports.

Specific: Entspricht der Ziel-Port-Nummer für die Zugangsbestimmung.

Range: Entspricht der Einstellung des Ziel-Port-Bereichs für die Zugangsbestimmung.

Dest. Port No.: Range: 0-65535

Dest. Port Range.: Range: 0-65535

TCP FIN:

TCP Control Bit FIN: Keine weiteren Daten vom Sender.

Range: Any / 0 / 1

Any: Beinhaltet alle TCP FIN-Fälle.

0: Das TCP Kontroll-Bit FIN ist 0.

1: Das TCP Kontroll-Bit FIN ist 1.

TCP SYN:

TCP Control Bit SYN: Synchronisiert die Sequenznummern.

Range: Any / 0 / 1

Any: Beinhaltet alle TCP SYN-Fälle.

0: Das TCP Kontroll-Bit SYN ist 0.

1: Das TCP Kontroll-Bit SYN ist 1.

TCP RST:

TCP Control Bit RST: Stellt die Verbindung wieder her.

Range: Any / 0 / 1

Any: Beinhaltet alle TCP RST-Fälle.

0: Das TCP Kontroll-Bit RST ist 0.

1: Das TCP Kontroll-Bit RST ist 1.

TCP PSH:

TCP Control Bit PSH: Betrifft die Push-Funktion.

Range: Any / 0 / 1

Any: Beinhaltet alle TCP PSH-Fälle.

0: Das TCP Kontroll-Bit PSH ist 0.

1: Das TCP Kontroll-Bit PSH ist 1.

TCP ACK:

TCP Control Bit ACK: Betrifft die (Empfangs-)Bestätigung.

Range: Any / 0 / 1

Any: Beinhaltet alle TCP ACK-Fälle.

0: Das TCP Kontroll-Bit ACK ist 0.

1: Das TCP Kontroll-Bit ACK ist 1.

TCP URG:

TCP Control Bit URG: Betrifft das Urgent-Pointer-Feld.

Range: Any / 0 / 1

Any: Beinhaltet alle TCP URG-Fälle.

0: Das TCP Kontroll-Bit URG ist 0.

1: Das TCP Kontroll-Bit URG ist 1.

IP Protocol Value:

Der IP-Protokoll-Wert kann im Ende des TCP-Headers im Optionsfeld stehen. Er hat stets ein vielfaches von 8 Bit als Länge.

Momentan definierte Optionen schließen ein (die Art wird oktal dargestellt):

0 - Ende des Option-Feld

1 - No-Operation

Range: Any / 0 / 1

Any: Schließt alle IP-Protokoll-Werte ein

0: Der Wert des IP-Protokolls-Feld ist 0

1: Der Wert des IP-Protokolls-Feld ist 1

- IP Parameters: (Frame Type = IPv4 and IP Protocol Filter = Other)

IP Protocol Value: Default: 255

IP TTL: (Time To Live ~ Zeit zu Leben)

Legt fest wie viele Router ein Datapaket passieren kann, bevor es verworfen wird. Jeder Routing-Schritt verringert diesen Wert um 1 solange, bis der Wert 0 erreicht und das Paket verworfen wird. Dies stellt sicher, dass kein fehlgeleitetes Paket unbegrenzt lange im Netzwerk verschickt wird.

Range: Any / Non-zero / Zero

Any: Beinhaltet alle Bedingungen für IP TTL.

Non-Zero: Alle Werte für IP TTL die nicht Null sind.

Zero: Die IP TTL ist genau Null.

- IP Fragment: (IP Fragmentation Flag)

Dieses Feld dient gemeinsam mit dem Identification-Feld der Kontrolle von Datenfragmentation. Die Schalter zeigen an, ob ein

Datenpaket möglicherweise fragmentiert wurde, ob es fragmentiert ist, und ob es das letzte Datenpaket ist.

Range: Any / Yes / No

Any: Beinhaltet alle möglichen Fragmentations-Zustände

Yes: Das eingehende Paket ist fragmentiert.

No: Das eingehende Paket ist nicht fragmentiert.

IP Option:

Enthält eine Liste optionaler Spezifikationen für Sicherheitsbeschränkungen, Routen-Aufzeichnungen und Quellen-Routing. Nicht jedes Datenpaket spezifiziert das Options-Feld.

Range: Any / Yes / No

Any: Beinhaltet alle möglichen Werte für das Feld IP-Option

Yes: Das eingehende Paket spezifiziert das IP-Options-Feld

No: Das eingehende Paket spezifiziert das IP-Options-Feld nicht

SIP Filter: (SIP Source IP Address)

Range: Any / Host / Network

Any: Beinhaltet alle Quellen-IP-Adressen

Host: Nur eine, spezifische Quell-IP-Adresse

Network: Ein spezifisches Sub-Netzwerk im Bereich der Quell-IP-Maske.

SIP Address: Default: 192.168.1.1

SIP Mask: Default: 255.255.255.0

DIP Filter: (DIP Destination IP Address)

Range: Any / Host / Network

Any: Beinhaltet alle möglichen Ziel-IP-Adressen.

Host: Nur eine, spezifische Ziel-IP-Adresse

Network: Ein spezifisches Sub-Netzwerk hinter der Ziel-IP-Maske

DIP Address: Default: 192.168.1.254

DIP Mask: Default: 255.255.255.0

□ VLAN Parameters:

VLAN ID Filter:

Range: Any / Specific

Any: Beinhaltet alle VLAN IDs

Specific: Je nach folgender VLAN ID und Tag-Prioritäts-Einstellungen für Eingangs-Klassifikation.

VLAN ID:

Range: 1-4094

Tag Priority:

Range: Any / 0-7

Any: Beinhaltet alle Tag-Prioritäten

0-7: Die Tag-Priorität ist ein Wert zwischen 0 - 7 .

Action Parameters:

Wenn das eingehende Paket die obigen ACL-Eingangs-Klassifikations-Regeln bestanden hat, stehen Ihnen die folgenden Aktionen zur Auswahl:

Action:

Range: Permit / Deny

Permit: Gestattet dem Paket, dass die Eingangs-Klassifikations-Regeln bestanden hat, die Weiterleitung auf andere Ports an dem Switch.

Deny: Verwirft die Pakete, die die Eingangs-Klassifikations-Regeln bestanden haben.

Rate Limiter:

Range: Disabled / 1-16

Disable: Schaltet das Raten-Limit aus.

1-16: Wendet ein Raten-Limit entsprechend des gewählten Werts auf das Paket an, dass die Eingangs-Klassifikation bestanden hat.

Port Copy:

Range: Disabled / 1-24

Disable: Schaltet die Port-Kopier-Funktion aus.

1-24: Die Pakete, die die Eingangs-Klassifikation bestanden

haben, werden auf den ausgewählten Port kopiert.

4.6.4 Wizard

Welcome to the ACL Configuration Wizard!

Please select an action:

- Set up Policy Rules**
Set up the default policy rules for Client ports, Server ports, Network ports, and Guest ports.
- Set up Port Policies**
Group ports into several types according to different ACL policies.
- Set up Typical Network Application Rules**
Set up the specific ACL for different typical network application access control.

To continue, click Next.

Next >

■ Wizard

Die Wizard-Funktion hilft Ihnen anhand von vier typische Anwendungsszenarien leicht und effizient ACL für ihre Anwendung zu konfigurieren.

■ Parameter:

- Please select an Action:
Einrichten einer Regeln-Richtlinie / Einrichten einer Port-Richtlinie / Einrichten einer typischen Netzwerk-Anwendungs-Regel / Einrichten einer Quell-MAC und Quell-IP-Bindung
Next: Klicken Sie auf <Next> um mit der aktuellen Auswahl fortzufahren und automatisch zum nächsten Schritt zu gehen.
- Cancel:
Bricht die aktuelle Konfiguration ab und kehrt zur Hauptseite des Wizards zurück.
- Back:
Klicken Sie auf <Back> um einen Schritt zurück zu gehen.
- Wizard Again:
Mit einem Klick auf die Schaltfläche <Wizard Again> kehren Sie auf die Hauptseite des Wizards zurück.
- Finish:
Mit einem Klick auf <Finish> beendet Sie die Sammlung der relevanten Werte durch die Wizard-Konfiguration. Mit einem weiteren Klick auf

<Apply> übernimmt der Switch die neuen Parameter an den relevanten Stellen.

- Parameter:
 - Common Server:
DHCP / DNS / FTP / HTTP / IMAP / NFS / POP3 / SAMBA / SMTP / TELNET / TFTP
 - Instant Messaging:
Google Talk / MSN Messenger / Yahoo Messenger
 - User Definition:
Ethernet Type / UDP Port / TCP Port
 - Others:
TCP Port / ICMP / Multicast IP Stream / NetBIOS / Ping Request / Ping Reply / SNMP / SNMP Traps
 - Ingress Port:
Any / Policy1-8 / Port1-24
 - Action:
Permit / Deny
 - Rate Limiter ID:
Disabled / 1-16
- Parameter:
 - Port #:
1-24
 - Binding Enabled:
Die ACL-Funktion des Switches wird zur Unterstützung der IP/MAC-Binding-Funktion benutzt. Es können maximal 128 Einträge angewendet werden.
 - Source MAC Address:
xx-xx-xx-xx-xx-xx (zum Beispiel: 00-40-c7-00-00-01)
 - Source IP Address:
xxx.xxx.xxx.xxx (zum Beispiel: 192.168.1.100)

4.7 Security: IP MAC Binding

Der IP Netzwerk-Layer benutzt eine Vier-Byte-Adresse. Der Ethernet-Link-Layer benutzt eine Sechs-Byte-MAC-Adresse. Wenn diese beiden Adresstypen miteinander verbunden werden, ist eine Datenübermittlung zwischen diesen beiden Layern möglich. Die grundlegendste Absicht von IP-MAC-Binding ist es, nur autorisierten Nutzern den Zugriff zum Switch zu erlauben. Diese autorisierten Nutzer haben mit der IP-MAC-Adresse und der Portnummer (mit dem vorkonfigurierten Datenspeicher) Zugriff zum Switch-Port. Wenn ein unbefugter Nutzer auf einen Port mit IP-MAC-Binding zugreifen will, blockt ihn das System und verwirft seine Pakete.

IP MAC Binding Configuration

State:

Trust Port: 1. 2. 3. 4. 5. 6. 7. 8. 9. 10. 11. 12. 13. 14. 15. 16. 17. 18. 19. 20. 21. 22. 23. 24.

MAC	IP	Port No	VID
<input type="text" value="-"/> - <input type="text" value="-"/> - <input type="text" value="-"/> - <input type="text" value="-"/> - <input type="text" value="-"/> - <input type="text" value="-"/>	<input type="text" value=""/>	<input type="text" value="1"/>	<input type="text" value=""/>

No	MAC	IP	Port	VID
----	-----	----	------	-----

■ IP MAC Binding Configuration

Der Switch besitzt eine IP-MAC-Binding-Tabelle für Clients und eine für Server. In der Clients-Tabelle können maximal 512 Einträge gemacht werden. In der Server-Tabelle können maximal 64 Einträge gemacht werden. Die Bestimmung der autorisierten Nutzer kann manuell erfolgen. Diese Funktion ist global, das bedeutet, dass ein Nutzer diese Funktion für alle Ports im Switch ein- und ausschalten kann.

■ Parameters:

- State:
 - “Disabled” oder “Enabled”

- Time Interval:
Bereich: 10 / 20 / 30. Das Zeitintervall betrifft das ARP-Echo, dieses wird der Switch gemäß des Server-Tabelleneintrags senden.
- Server/Client:
Der Switch besitzt eine IP-MAC-Binding-Tabelle für Clients und eine für Server. In der Clients-Tabelle können maximal 512 Einträge gemacht werden. In der Server-Tabelle können maximal 64 Einträge gemacht werden.
- MAC:
Sechs-Byte-MAC-Adresse: xx-xx-xx-xx-xx-xx (Zum Beispiel: 00-40-c7-00-00-01)
- IP:
Vier-Byte-IP-Adresse: xxx.xxx.xxx.xxx (Zum Beispiel: 192.168.1.100)
- Port No:
Portnummer 1-24
- VID:
VLAN ID 1-4094
- Add:
Geben Sie MAC, IP, Port und VID ein und klicken Sie auf "add" um einen neuen Eintrag in der IP-MAC-Binding-Tabelle zu machen.
- Delete:
Wählen Sie einen Eintrag in der Tabelle aus und klicken Sie auf "delete" um diesen Eintrag zu löschen.

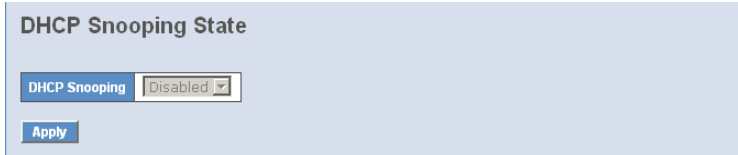
IP MAC Binding Dynamic Entry

No	MAC	IP	Port	VID

Delete

4.8 Security: DHCP Snooping

4.8.1 DHCP Snooping State



DHCP Snooping State

DHCP Snooping Disabled

Apply

■ DHCP Snooping State

Die durch DHCP den Clients an unsicheren Ports zugewiesenen Adressen lassen sich durch dynamic bindings, die mit DHCP-Snooping registriert wurden, genau kontrollieren. DHCP-Snooping erlaubt es einem Switch das Netzwerk vor Rogue-DHCP-Servern oder anderen Geräten, die Port-relevante Informationen an den DHCP-Server senden, zu schützen. Diese Informationen erleichtern das Auflösen einer IP-Adresse zu einem physikalischen Port.

■ Parameter:

DHCP Snooping state:

Dieser Parameter deaktiviert oder aktiviert DHCP Snooping auf dem Switch. Der Default ist Disabled (deaktiviert).

Note: Denken Sie daran <Apply> zu klicken, um die Einstellung zu übernehmen.

4.8.2 DHCP Snooping Entry

DHCP Snooping Entry

VID	Trust Port 1	Trust Port 2	Server IP	Option 82	Action

VID	<input type="text"/>	Trust Port 1	Disable ▾	Trust Port 2	Disable ▾
Server IP	<input type="text"/>	Option 82	Disable ▾	Action	Keep ▾

Default Entry

VID	0	Trust Port 1	Disable ▾	Trust Port 2	Disable ▾
Server IP	0.0.0.0	Option 82	Disable ▾	Action	Keep ▾

■ DHCP Snooping Entry

Mit einem DHCP-Snooping-Eintrag können sie einen vertrauenswürdigen DHCP-Server und zwei vertrauenswürdige Ports zu den für DHCP-Snooping verfügbaren Einträgen hinzufügen. Diese Informationen erleichtern es Ihnen einer IP-Adresse einen physikalischen Port zuzuweisen. Sie können hier über das Aktivieren oder Deaktivieren der DHCP-Option 82 entscheiden.

■ Parameter:

- VID:

Falls DHCP-Snooping aktiviert wurde und in diesem speziellen VLAN angewendet wird, wird der Switch DHCP-packet-filtering an allen nicht vertrauenswürdigen Ports innerhalb dieses VLANs verwenden. Dieser Schalter aktiviert DHCP-snooping für diese VLAN-ID.
- Trust Port 1:

Wenn DHCP-Snooping global aktiviert wurden, und auch für das VLAN verwendet wird, das das DHCP-Paket empfangen hat, werden alle DHCP-Pakete an den vertrauenswürdigen Port weitergeleitet. Hier können Sie diesen Port auswählen. Zulässig ist jeder Port von 0 bis 24. Dabei beschreibt 0, dass dieses Feature deaktiviert wurde.

- Trust port 2:
Hier können Sie einen zweiten vertrauenswürdigen Port einstellen. Alle Ports zwischen 0 und 24 sind zulässig, dabei meint der Port 0, dass dieses Feature deaktiviert wurde.
- Trust VID:
Hier können Sie eine vertrauenswürdige VLAN-ID eingeben. Zulässig sind alle VIDs zwischen 1 und 4094.
- Server IP:
Hier tragen Sie einen vertrauenswürdigen DHCP-Server und seine IP-Adresse für das DHCP-Snooping ein.
- Option 82:
Aktiviert oder Deaktiviert die DHCP-Option 82 am Switch. Per Default deaktiviert (disable).
- Action:
Konfiguriert den Umgang mit einem DHCP-Request-Paket das empfangen wurde. Mögliche Werte: Keep / Drop / Replace
Note: Die folgenden Filter-Regeln werden angewendet:
 - Falls DHCP-Snooping deaktiviert ist, werden alle DHCP-Pakete weitergeleitet.
 - Falls DHCP-Snooping aktiviert ist und auch für das VLAN verwendet wird, indem das DHCP-Paket empfangen wurde, werden alle DHCP-Pakete an einen vertrauenswürdigen Port weitergeleitet.
 - Falls DHCP-Snooping aktiviert ist und auch für das VLAN verwendet wird, indem das DHCP-Paket empfangen wurde, der Port, von dem das DHCP-Paket stammt aber nicht vertrauenswürdige ist, wird wie folgt fortgefahren:
 - Wenn das DHCP-Paket eine Antwort des DHCP-Servers ist, wird es verworfen.
 - Stammt das DHCP-Paket von einem Client, etwa eine DISCOVER-, REQUEST-, INFORM-, DECLINE- oder RELEASE-Nachricht, wird es weitergeleitet, wenn MAC-Verifikation deaktiviert ist. Sollte MAC-Verifikation aktiviert sein, wird die Nachricht nur dann wei-

tergeleitet, wenn die Hardwareadresse des Clients im DHCP-Paket mit der Quell-MAC-Adresse im Ethernet-Header übereinstimmt.

Lässt sich das DHCP-Paket nicht einem erkennbaren Typ zuweisen, wird es verworfen.

Wenn ein DHCP-Paket von einem Client alle Filter-Kriterien erfüllt, wird es nur an vertrauenswürdige Ports innerhalb desselben VLANs weitergeleitet.

Wird an einem vertrauenswürdigen Port ein DHCP-Paket von einem Server empfangen, wird es sowohl an vertrauenswürdige wie an nicht-vertrauenswürdige Ports im selbem VLAN weitergeleitet.

4.8.3 DHCP Snooping Client

DHCP Snooping Client				
MAC	VID	Port	IP	Lease

■ DHCP Snooping Client

Zeigt die DHCP-Snooping Clients.

■ Parameter:

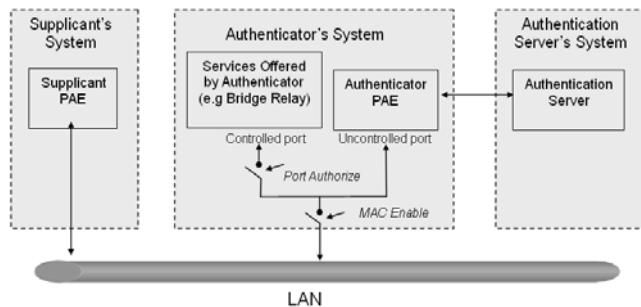
- MAC:
Zeigt die MAC-Adresse des DHCP-Snooping Clients.
- VID:
Zeigt die VLAN ID des DHCP-Snooping Clients.
- Port:
Zeigt den Port des DHCP-Snooping Clients.
- IP:
Zeigt die IP-Adresse des DHCP-Snooping Clients.

- Lease:
Zeigt die Lease-Zeit des DHCP-Snooping Clients an.

4.9 Security: 802.1x Konfiguration

Die 802.1x Port-basierte Netzwerkzugangs-Verwaltung ist eine Methode bestimmte Benutzer auf bestimmte Netzwerkressourcen zu beschränken, indem man ihre Benutzerinformation authentifiziert. Dadurch ist der Netzwerkzugang durch einen 802.1x-fähigen Port ohne Authentifizierung ausgeschlossen. Sollte ein Benutzer das Netzwerk durch einen solchen Port betreten wollen, muss er zunächst seinen Accountnamen eingeben und dann auf die Authentifizierungsbestätigung warten bevor er über den 802.1x-fähigen Port Pakete senden oder schicken kann.

Damit Geräte und Endstationen Netzwerkressourcen unter 802.1x-Kontrolle nutzen können, müssen sie eine Authentifizierungs-Anfrage für diese kontrollierten Ports an den Authenticator senden. Der Authenticator reicht diese Anfrage dann an den Authentifizierungs-Server weiter, der sie bearbeitet und verifiziert und dann die Nutzung der Ports gestattet oder ablehnt.



Nach dem IEEE802.1x-Standard sind drei Komponenten implementiert: Der Authenticator, Supplicant und der Authentifizierungs-Server.

- **Supplicant:**
Diese Entität wird dafür, benutzt auf Anfrage des Authenticators dessen PAE (Port Access Entity) die Authentifizierungs-Informationen zu kommunizieren.
- **Authenticator:**
Eine Entität für die Kontrolle sowohl authentifizierter, als auch nicht-authentifizierter Ports. Sie authentifiziert die Supplicant-Entität je nach-

dem wie der Austausch der Authentifizierungs-Nachricht zwischen ihr und dem Supplicant-PAE abgelaufen ist. Sie können eine Zeit festlegen nach der der Authenticator eine Re-Authentifizierung des Supplicant verlangt. Während der Re-Authentifizierung bleibt der Port (bis zum eventuellen Scheitern des Authentifizierungs-Vorgangs) in einem authentifizierten Zustand.

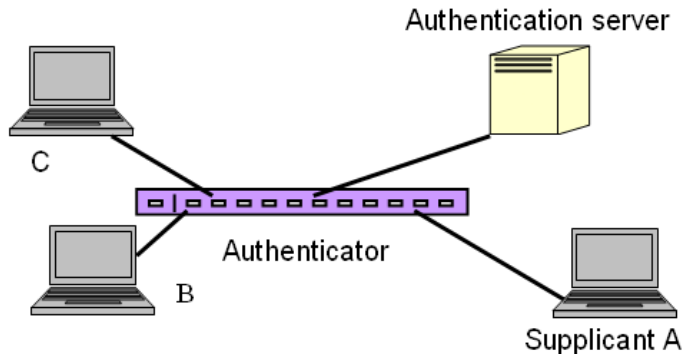
Einen als Authenticator fungierenden Port können Sie sich als zwei logische Ports vorstellen, einen kontrollierten und einen unkontrollierten. Der kontrollierte Port kann nur dann Pakete passieren lassen, wenn der PAE des Authenticators dies gestattet; Während der unkontrollierte Port alle Pakete mit einer PAE-Gruppen-MAC-Adresse mit dem Wert 01-80-c2-00-00-03 zu jeder Zeit passieren lassen wird.

■ Authentication server:

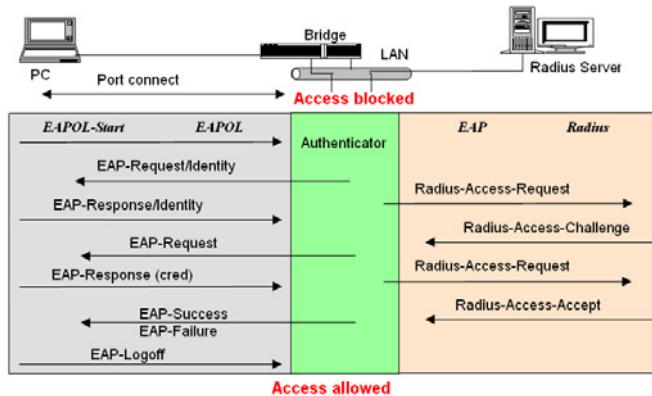
Dieses Gerät leistet den Authentifizierungs-Service durch EAP für den Authenticator. Dabei nutzt es Authentifizierungs-Zertifikate, die vom Supplicant geliefert wurden, um dessen Zugangsberechtigung zum Netzwerk festzustellen.

Wenn die Supplicant-PAE eine Authentifizierungs-Anfrage an die Authenticator-PAE richtet, wird diese den Supplicant um das Senden der Authentifizierungs-Nachricht bitten. Diese Nachricht sendet der Authenticator dann an den RADIUS-Server weiter um die Informationen zu verifizieren. Der RADIUS-Server wird dann die Anfrage gestatten oder abweisen und entsprechend antworten.

Während des Authentifizierungs-Prozesses werden die Nachrichtenpakete zwischen Supplicant und Authenticator durch das Extensible-Authentication-Protocol-over-LAN (EAPOL) eingekapselt. Auch die Kommunikation zwischen Authenticator und Authentifizierungs-Server nutzt das EAPOL. Vor einer erfolgreichen Authentifizierung kann der Supplicant den Authenticator nur für den Authentifizierungs-Nachrichtenaustausch erreichen, oder auf das Netzwerk über den unkontrollierten Port zugreifen.



Die Abbildung zeigt eine typische Konfiguration: Ein einzelner Supplicant, ein Authenticator und ein Authentifizierungs-Server. B und C sind im internen Netzwerk, D ist ein Authentifizierungs-Server, auf dem RADIUS ausgeführt wird. Der zentrale Switch fungiert als Authenticator, zu dem PC A verbunden ist. A ist ein Computer ausserhalb des kontrollierten Ports und führt eine Supplicant-PAE aus. Angenommen, PC A möchte Zugriff auf die Ressourcen auf den Geräten B und C, dann muss er zunächst eine Authentifizierungs-Nachricht mit dem Authenticator durch ein EAPOL-Paket austauschen. Der Authenticator wird dann die Authentifizierungs-Zertifikate dem Authentifizierungs-Server vorlegen. Sollte dieser der Authentifizierung zustimmen, sendet er diese Information dem Authenticator, der dann dem PC A den Zugang auf die Geräte B und C durch den Switch gestattet. Sollte es zwei direkt miteinander verbundene Switches geben, hat der Verbindungs-Port zwischen den beiden möglicherweise sowohl die Rolle eines Supplicants, als auch eines Authenticators, da der Verkehr hier bidirektional ist.



Die Abbildung zeigt den Ablauf einer 802.1x Authentifizierung. Die Login-Schritte basieren auf 802.1x Port-Zugangs-Kontrollmanagement. Auf der linken Seite kommt das EAPOL-, auf der rechten das EAP-Protokoll zum Einsatz.

- 1 Zu Beginn des Prozesses ist der Supplicant A nicht authentifiziert und auch der Port am Switch, der als Authenticator fungiert, ist im nicht autorisierten Zustand. Der Zugang ist also in diesem Schritt noch blockiert.
- 2 Sowohl Authenticator als auch Supplicant können einen Nachrichtenaustausch initiieren. Wenn der Supplicant den Austausch beginnt, sendet er eine EAPOL-Start-Nachricht an den Authenticator, auf die dieser sofort mit einem EAP-Request/Identity-(EAP-Identitätsanfrage) Paket antworten wird.
- 3 Der Authenticator sendet regelmässig EAP-Request/Identity-Pakete an den Supplicant um eine Re-Authentifizierung der Identität anzufragen.
- 4 Sollte der Authenticator den Austausch nicht durch das Senden des EAP-Request/Identity-Pakets beginnen, wird der Supplicant durch das Senden des EAPOL-Pakets den Prozess starten.
- 5 Als nächstes wird der Supplicant ein EAP-Response/Identity-(EAP-Identitätsantwort) Paket als Antwort an den Authenticator schicken. Der Authenticator wird dann die Benutzer-ID in den RADIUS-Access-Request-(RADIUS-Zugang)Befehl einbetten und diesen an den Authentifizierungs-Server senden um so die Identität des Benutzers zu bestätigen.

- 6 Nach dem Empfangen des RADIUS-Access-Request-Befehls wird der Authentifizierungs-Server ein RADIUS-Access-Challenge-(RADIUS-Identitätsanforderung) Paket an den Supplicant senden, indem er ihn auffordert sein Benutzerpasswort durch die Authenticator-PAE einzugeben.
- 7 Der Supplicant wird sein Benutzerpasswort in die Zertifikatsinformationen konvertieren (z.B. im MDF- oder OPT-Format) und antwortet diese Zertifikationsinformationen sowie den spezifischen Authentifizierungsalgorithmus als EAP-Response-Paket an den Authentifizierungs-Server durch die Authenticator-PAE. Durch den Wert des entsprechenden Feldes der Nachricht-PDU weiß der Authentifizierungs-Server, welchen Algorithmus er anwenden muss um die Zertifikatsinformation zu verifizieren, z.B. EAP-MD5 (Message Digest 5), EAP-OTP (One Time Password) oder einen anderen Algorithmus.
- 8 Wenn Benutzer-ID und Passwort korrekt eingegeben wurden, wird der Authentifizierungs-Server ein RADIUS-Access-Accept-(RADIUS-Zugangsbestätigung) Befehl an den Authenticator senden. Sollten die Benutzereingaben nicht korrekt sein wird er entsprechend ein RADIUS-Access-Reject-(RADIUS-Zugangsverweigerung) Paket senden.
- 9 Der Authenticator wird ein EAP-Success-(EAP-Erfolg) Paket an den Supplicant senden, wenn es ein RADIUS-Access-Accept-Paket vom Authentifizierungs-Server erhält. Gleichzeitig wechselt der Port unter 802.1x-Kontrolle des Supplicants in den autorisierten Zustand. Der Supplicant und andere Geräte an diesem Port können nun auf das Netzwerk zugreifen. Sollte der Authenticator dagegen ein RADIUS-Access-Reject-Paket erhalten, wird dem Supplicant ein EAP-Failure-(EAP-Scheitern) Befehl weitergegeben. Dies bedeutet, dass die Authentifizierung fehlgeschlagen ist und der entsprechende Port im unauthorisierten Zustand bleibt, d.h. der Supplicant und andere an diesen Port angeschlossene Geräte haben keinen Zugriff auf das Netzwerk.
- 10 Der Supplicant kann eine EAP-Logoff-Nachricht an den Server senden. Dies löst ein Wechseln des entsprechenden Ports in den unauthorisierten Zustand aus.

MultiHost 802.1X ist die einzige Authentifizierungsmethode, die der Switch unterstützt. Diese Methode gestattet es nur korrekt authentifizierten Geräten, die über einen solchen Port verbunden sind, auf das Netzwerk zuzugreifen.

Die Port-basierte 802.1X Netzwerkzugangs-Kontrollfunktion des Switches unterstützt ausschließlich Basis-MultiHost-Modus. Dieser kann zwischen der MAC-Adresse und der VID eines Gerätes unterscheiden. Die folgende Gegenüberstellung zeigt zusammenfassend die Kombination von Authentifizierungs- und Portstatus im Vergleich zum Portmodus-Status, den sie im 802.1x Port-Modus einstellen können, und dem Portkontrolle-Status, den Sie in den Port-Einstellungen setzen können. Dabei bedeutet Zugangsberechtigung, dass der jeweilige MAC-Zugang autorisiert wurde.

Port Mode	Port Control	Authentication	Port Status
Disable	Don't Care	Don't Care	Port Uncontrolled
Multihost	Auto	Successful	Port Authorized
Multihost	Auto	Failure	Port Unauthorized
Multihost	ForceUnauthorized	Don't Care	Port Unauthorized
Multihost	ForceAuthorized	Don't Care	Port Authorized

4.9.1 Server

802.1X Server Configuration

Authentication Server	
Server IP Address 1	<input type="text" value="192.168.1.1"/>
UDP Port	<input type="text" value="1812"/>
Server IP Address 2	<input type="text" value="192.168.1.1"/>
UDP Port	<input type="text" value="1812"/>
Secret Key	<input type="text" value="Radius"/>
Accounting Server	
Server IP Address 1	<input type="text" value="192.168.1.1"/>
UDP Port	<input type="text" value="1813"/>
Server IP Address 2	<input type="text" value="192.168.1.1"/>
UDP Port	<input type="text" value="1813"/>
Secret Key	<input type="text" value="Radius"/>

- 802.1X Server Configuration
Konfiguriert die globalen Parameter für RADIUS-Authentifizierung in 802.1X-gesicherten Umgebungen.

■ Parameter:

□ Authentication Server

Server IP Server:

IP-Adresse des Authentifizierungs-Servers.

Default: 192.168.1.1

UDP Port:

Default-Port ist 1812.

Secret Key:

Zeigt den geheimen Schlüssel zwischen Authentifizierungs-Server und dem Authenticator. Besteht aus einer Kette von 1-31 Zeichen. Diese Kette kann Groß- und Kleinschreibung, sowie die Zahlen 0-9 beinhalten. Es darf kein Leerzeichen zwischen den Zeichen stehen.

Default: Radius

4.9.2 Port Configuration

802.1X Port Configuration

Port	Port 1
Mode	Disabled
Port Control	Auto
reAuthMax	2 (1-10)
txPeriod	30 (1-65535 sec)
quietPeriod	60 (0-65535 sec)
reAuthEnabled	ON
reAuthPeriod	120 (1-65535 sec)
maxReq	2 (1-10)
suppTimeout	30 (1-255 sec)
serverTimeout	30 (1-255 sec)

Save

■ 802.1X Port Configuration

Konfiguriert die 802.1X-Parameter für jeden Port individuell. Die folgenden Parameter können eingestellt werden:

Parameter:

- Port:
Wählen Sie hier den Port aus, für den Sie die die zugehörigen 802.1X-Parameter konfigurieren möchten. Diese Parameter sind Port control, reAuthMax, txPeriod, Quiet Period, reAuthEnabled, reAuthPeriod, max. Request, suppTimeout, serverTimeout und Controlled direction.
- Mode:
Range: Disable / Normal / Advanced / Clientless
Disable: Schaltet IEEE 802.1X für diesen Port aus.
Normal: Alle Clients an diesem Port werden authentifiziert, wenn sich ein Client nach 802.1X erfolgreich angemeldet hat.
Advanced: Jeder der Clients an diesem Port muss sich eigenständig nach 802.1X authentifizieren.
Clientless: Die Clients brauchen keine 802.1X-Unterstützung, dass heißt ein Client-PC (zum Beispiel WINDOWS XP) muss die 802.1X-Unterstützung nicht aktiviert haben um sich unter 802.1X anzumelden. In diesem Fall muss der Netzwerk-Administrator den RADIUS-Server mit dem MAC-Adresse jedes Clients für die RADIUS-Account-ID und Passwort konfigurieren.
- Port Control:
Konfiguriert den Operationsmodus des Authentifizierung. Es stehen drei Modi zur Verfügung: supported, ForceUnauthorized, ForceAuthorized, Auto.
ForceUnauthorized: Der Controlled-Port wird gezwungen im unauthorisierten Zustand zu bleiben.
ForceAuthorized: Der Controlled-Port wird gezwungen im authorisierten Zustand zu bleiben.
Auto: Der Zustand des Controlled-Ports hängt vom Ausgang des Authentifizierungs-Vorgang zwischen Authentifizierungs-Server und Supplicant ab.
Default: Auto
- reAuthMax(1-10):
Konfiguriert die Anzahl an Authentifizierungs-Versuchen die erlaubt sind, bevor der Port in den unauthentifizierten Zustand versetzt wird.
Default: 2

- txPeriod(1-65.535 s):
Konfiguriert die erlaubte Zeitspanne zum Senden des EAPOL PDU zwischen Authenticator und Supplicant.
Default: 30
- Quiet Period(0-65.535 s):
Konfiguriert die Zeitspanne, während der nicht versucht wird auf den Supplicant zuzugreifen.
Default: 60 Sekunden
- reAuthEnabled:
Schaltet reguläre Authentifizierung an diesem Port ein.
Default: ON
- reAuthPeriod(1-65.535 s):
Eine Zeitspanne in Sekunden, die nicht 0 sein darf, zwischen den periodischen Re-Authentifizierungen des Supplicant.
Default: 3.600
- max. Request(1-10):
Das Maximum des erneuten Sendens des EAP Request vom Authenticator an den Supplicant bevor er die Authentifizierungs-Sitzung beendet. Mögliche Werte: 1-10.
Default: 2
- suppTimeout(1-65535 s):
Konfiguriert die Timeout-Bedingung für den Austausch zwischen Authenticator und Supplicant in Sekunden. Mögliche Werte. 1 - 65.535.
Default: 30 Sekunden
- serverTimeout(1-65.535 s):
Konfiguriert die Timeout-Bedingung für den Austausch zwischen Authentifizierungs-Server und Authenticator in Sekunden. Mögliche Werte. 1 -65.535.
Default: 30 Sekunden

4.9.3 Status

802.1X Status

Port	Mode	Status
1	Disable	-
2	Disable	-
3	Disable	-
4	Disable	-
5	Disable	-
6	Disable	-
7	Disable	-
8	Disable	-
9	Disable	-
10	Disable	-
11	Disable	-
12	Disable	-
13	Disable	-
14	Disable	-
15	Disable	-
16	Disable	-
17	Disable	-
18	Disable	-
19	Disable	-
20	Disable	-
21	Disable	-
22	Disable	-
23	Disable	-
24	Disable	-

- **802.1X Status**
Zeigt für jeden Port den aktuellen IEEE 802.1X Modus und Zustand an.
- **Parameter:**
 - Port:**
Port number: 1-24
 - Mode:**
Zeigt den Operations-Modus dieses Ports an. Es gibt vier Modi. Disable, Normal, Advance und Clientless
 - Status:**
Zeigt den den 802.1X-Sicherheits-Zustand dieses Ports an: Autorisiert oder Un-Autorisiert

4.9.4 Statistics

802.1X Port Statistics Port 1	
Port 1 Auto-refresh Refresh Clear	
Authenticator Counters	
authEntersConnecting	0
authEapLogoffsWhileConnecting	0
authEntersAuthenticating	0
authAuthSuccessesWhileAuthenticating	0
authAuthTimeoutsWhileAuthenticating	0
authAuthFailWhileAuthenticating	0
authAuthEapStartsWhileAuthenticating	0
authAuthEapLogoffWhileAuthenticating	0
authAuthReauthsWhileAuthenticated	0
authAuthEapStartsWhileAuthenticated	0
authAuthEapLogoffWhileAuthenticated	0
Backend Authenticator Counters	
backendResponses	0
backendAccessChallenges	0
backendOtherRequestsToSupplicant	0
backendAuthSuccesses	0
backendAuthFails	0
802.1X MIB Counters	
dot1xAuthEapolFramesRx	0
dot1xAuthEapolFramesTx	0
dot1xAuthEapolStartFramesRx	0
dot1xAuthEapolLogoffFramesRx	0
dot1xAuthEapolRespIdFramesRx	0
dot1xAuthEapolRespFramesRx	0
dot1xAuthEapolReqIdFramesTx	0
dot1xAuthEapolReqFramesTx	0
dot1xAuthInvalidEapolFramesRx	0
dot1xAuthEapLengthErrorFramesRx	0
dot1xAuthLastEapolFrameVersion	0
dot1xAuthLastEapolFrameSource	00-00-00-00-00-00

■ 802.1X Port Statistics Port1

Zeigt die relevanten Statistiken für IEEE 802.1X Authentifizierung an.

■ Parameter:

- Port:
Port Number: 1-24
- Auto - refresh:
Aktualisiert die Zähler im Web-UI automatisch.
- Refresh:
Durch ein Klicken auf <Refresh> werden die Zähler im Web-UI manuell aktualisiert.
- Clear:
Ein Klicken auf <Clear> setzt alle Authentifizierungs-Zähler im Web-UI zurück.

4.10 Security: Mirroring

Mirror Configuration

Port to mirror to:

Port #	Source Enable	Destination Enable
1	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>	<input type="checkbox"/>
5	<input type="checkbox"/>	<input type="checkbox"/>
6	<input type="checkbox"/>	<input type="checkbox"/>
7	<input type="checkbox"/>	<input type="checkbox"/>
8	<input type="checkbox"/>	<input type="checkbox"/>
9	<input type="checkbox"/>	<input type="checkbox"/>
10	<input type="checkbox"/>	<input type="checkbox"/>
11	<input type="checkbox"/>	<input type="checkbox"/>
12	<input type="checkbox"/>	<input type="checkbox"/>
13	<input type="checkbox"/>	<input type="checkbox"/>
14	<input type="checkbox"/>	<input type="checkbox"/>
15	<input type="checkbox"/>	<input type="checkbox"/>
16	<input type="checkbox"/>	<input type="checkbox"/>
17	<input type="checkbox"/>	<input type="checkbox"/>
18	<input type="checkbox"/>	<input type="checkbox"/>
19	<input type="checkbox"/>	<input type="checkbox"/>
20	<input type="checkbox"/>	<input type="checkbox"/>
21	<input type="checkbox"/>	<input type="checkbox"/>
22	<input type="checkbox"/>	<input type="checkbox"/>
23	<input type="checkbox"/>	<input type="checkbox"/>
24	<input type="checkbox"/>	<input type="checkbox"/>

■ Mirror Konfiguration

Die Mirror Konfiguration (Spiegelkonfiguration) dient dazu den Datenverkehr im Netzwerk zu überwachen. Wenn zum Beispiel Port A der überwachende Port ist und Port B der zu überwachende Port ist, dann wird der Datenverkehr, der bei Port B eintrifft, auf Port A kopiert und überwacht.

Hinweis: Wenn Sie die Spiegelkonfiguration bearbeiten, sollten Sie keinen Port gleichzeitig zu einem "Sniffer-Port" und einem "aggregated port" machen, da dies zu Problemen führen kann.

■ Parameter:

- Port to mirror to:
Range: Disabled / Port 1-24
Bestimmen Sie den Überwachungsport.

- Port #:
Range: 1-24
Bestimmen Sie die zu überwachenden Ports.
- Source Enable:
"Source enable" bedeutet, dass der eingehende Datenverkehr des überwachten Ports auf den Überwachungsport kopiert wird.
- Destination Enable:
"Destination enable" bedeutet, dass der ausgehende Datenverkehr des überwachten Ports auf den Überwachungsport kopiert wird.

4.11 Configuration: GVRP

GVRP (Generic VLAN Registration Protocol) ist eine auf dem Generic-Attribute-Registration-Protocol (GARP) basierende Anwendung, die hauptsächlich dafür benutzt wird, die Gruppenmitgliedschaft der VLANs automatisch und dynamisch zu warten. Die GVRP bringt die Möglichkeit mit, den VLAN-Registrierungsservice durch eine GARP-Anwendung auszuführen. Dabei greift sie auf die GARP-Information-Declaration (GID) zurück um die mit der Attribute-Datenbank verknüpften Ports zu erhalten, sowie auf die GARP-Information-Propagation (GIP) um mit Switches und Endstationen zu kommunizieren. Mit GID und GIP erhalten Maschinen im GVRP-Zustand die Inhalte der Dynamic-VLAN-Registration für jedes VLAN und verbreiten diese Informationen zu anderen GVRP-fähigen Geräten. Dadurch werden deren Wissensdatenbanken, sowie die Sets der mit gerade aktiven Mitgliedern verknüpften VLANs und die jeweiligen Ports, durch die diese Mitglieder zu erreichen sind, aufgesetzt und aktuell gehalten.

In den GVRP Einstellungen sind drei Funktionen unterstützt, die im Folgenden erklärt werden: GRVP-Config, GRVP-Counter und GVRP-Group.

4.11.1 Config

GVRP Configuration

GVRP State:

Port	Join Time	Leave Time	LeaveAll Time	Default Applicant Mode	Default Registrar Mode	Restricted Mode
1	20	60	1000	Normal	Normal	Disabled
2	20	60	1000	Normal	Normal	Disabled
3	20	60	1000	Normal	Normal	Disabled
4	20	60	1000	Normal	Normal	Disabled
5	20	60	1000	Normal	Normal	Disabled
6	20	60	1000	Normal	Normal	Disabled
7	20	60	1000	Normal	Normal	Disabled
8	20	60	1000	Normal	Normal	Disabled
9	20	60	1000	Normal	Normal	Disabled
10	20	60	1000	Normal	Normal	Disabled
11	20	60	1000	Normal	Normal	Disabled
12	20	60	1000	Normal	Normal	Disabled
13	20	60	1000	Normal	Normal	Disabled
14	20	60	1000	Normal	Normal	Disabled
15	20	60	1000	Normal	Normal	Disabled
16	20	60	1000	Normal	Normal	Disabled
17	20	60	1000	Normal	Normal	Disabled
18	20	60	1000	Normal	Normal	Disabled
19	20	60	1000	Normal	Normal	Disabled
20	20	60	1000	Normal	Normal	Disabled
21	20	60	1000	Normal	Normal	Disabled
22	20	60	1000	Normal	Normal	Disabled
23	20	60	1000	Normal	Normal	Disabled
24	20	60	1000	Normal	Normal	Disabled

■ GVRP Config

Die GVRP-Konfiguration wird benutzt um den GVRP-Operationsmodus jedes Portes einzustellen. Hierfür müssen Sie sieben Parameter einstellen, die im Folgenden beschrieben werden.

■ Parameter:

GVRP State Setting:

Hier können Sie den GVRP-Zustand auf einfache Art und Weise ein- bzw. ausschalten. Sie können die Liste mit der Maus oder mit dem "Nach-Unten-Pfeil" nach unten scrollen um dann zwischen "Enable" oder "Disable" entscheiden. Danach können Sie mit dem "Apply"-Button die Änderung übernehmen, die dann sofort aktiv wird.

- Join Time:
Hier können Sie die Join-Time in Hundertstelsekunden festlegen. Möglicher Einstellungsrahmen: 20-100 Hundertstelsekunden, Default 20 Hundertstelsekunden.
- Leave Time:
Die Leave-Time lässt sich im Rahmen von 60-300 Hundertstelsekunden einstellen. Die Default-Einstellung ist auf 60 Hundertstelsekunden eingestellt.
- Leave All Time:
Nach einer Zeitspanne wird angekündigt, dass alle Geräte die angemeldet sind, abgemeldet werden. Falls dennoch ein Gerät neu angemeldet wird, wird die Anmeldung im Switch gespeichert. Lässt sich im Bereich von 1.000-5.000 Zeiteinheiten einstellen, die Default-Einstellung ist auf 1.000 Zeiteinheiten festgelegt.
- Default Applicant Mode:
Dieser Modus beschreibt den Typus des Teilnehmers. Sie können zwischen zwei Modi wählen: Normal und Non-Participant.

Normal:
In diesem Modus nimmt der Switch in vollen Umfang am GARP-Protokoll-Austausch teil. Dies ist die Default-Einstellung.

Non-Participant:
Der Switch wird keine GARP-Nachrichten beantworten und auch selber keine senden. Er wird nur Nachrichten empfangen und auf GVRP-BPDU (Bridge Protocol Data Unit) reagieren.

Default Registrar Mode:

Es gibt drei Modi für den Registrar, zwischen denen Sie wählen können: Normal registrar, Fixed Registrar und Forbidden Registrar.

Normal:

Der Registrar antwortet normal auf eingehende GARP-Nachrichten. Dies ist die Default-Einstellung.

Fixed:

Der Registrar ignoriert alle GARP-Nachrichten und alle Mitglieder verbleiben im registrierten (IN) Zustand.

Forbidden:

Der Registrar ignoriert alle GARP-Nachrichten und alle Mitglieder bleiben im unregistrierten (EMPTY) Zustand.

 Restricted Mode:

Hier können Sie das Erstellen von dynamischen VLANs beschränken. Es gibt zwei Einstellungen, zwischen denen Sie wählen können: Enabled und Disabled.

Disabled:

Sollte der Switch eine GVRP-PDU (Protocol Data Unit) empfangen, wird er ein dynamisches VLAN erstellen. Dies ist die Default-Einstellung.

Enabled:

Der Switch wird kein dynamisches VLAN erstellen, wenn er eine GVRP-PDU empfängt. Sollte die dynamische GVRP-PDU zu einem existierenden statischen VLAN passen, wird der Switch diesen Port VLAN Gruppenmitgliedern hinzufügen.

4.11.2 Counter

GVRP Counter

Select Port

Counter Name	Received	Transmitted
Total GVRP Packets	0	0
Invalid GVRP Packets	0	
LeaveAll message	0	0
JoinEmpty message	0	0
JoinIn message	0	0
LeaveEmpty message	0	0
Empty message	0	

■ GVRP Counter

Alle GVRP-Zähler sind grundsätzlich in empfangene (received) und gesendete (transmitted) GARP-Pakete aufgeteilt, damit Sie die GVRP-Vorgänge überwachen können.

■ Parameter:

□ Received:

Total GVRP Packets:

Insgesamt empfangene GVRP-BPDUs der GVRP-Anwendung.

Invalid GVRP Packets:

Anzahl der ungültigen GARP-BPDUs, die die GVRP-Anwendung erhalten hat.

LeaveAll Message Packets:

Anzahl der GARP-BPDUs mit der "LeaveAll"-Nachricht, die die GARP-Anwendung empfangen hat.

JoinEmpty Message Packets:

Anzahl der GARP-BPDUs mit der "JoinEmpty"-Nachricht, die die GARP-Anwendung empfangen hat.

JoinIn Message Packets:

Anzahl der GARP-BPDUs mit der "JoinIn"-Nachricht, die die GARP-Anwendung empfangen hat.

LeaveEmpty Message Packets:

Anzahl der GARP-BPDUs mit der "LeaveEmpty"-Nachricht, die die GARP-Anwendung empfangen hat.

Empty Message Packets:

Anzahl der leeren GARP-BPDUs, die die GARP-Anwendung empfangen hat.

- Transmitted:
 - Total GVRP Packets:
 - Insgesamt gesendete GARP-BPDUs der GVRP-Anwendung.
 - Invalid GVRP Packets:
 - Anzahl der ungültigen GARP-BPDUs, die die GVRP-Anwendung gesendet hat.
 - LeaveAll Message Packets:
 - Anzahl der GARP-BPDUs mit der "LeaveAll"-Nachricht, die die GVRP-Anwendung gesendet hat.
 - JoinEmpty Message Packets:
 - Anzahl der GARP-BPDUs mit der "JoinEmpty"-Nachricht, die die GVRP-Anwendung gesendet hat.
 - JoinIn Message Packets:
 - Anzahl der GARP-BPDUs mit der "JoinIn"-Nachricht, die die GVRP-Anwendung gesendet hat.
 - LeaveEmpty Message Packets:
 - Anzahl der GARP-BPDUs mit der "LeaveEmpty"-Nachricht, die die GVRP-Anwendung gesendet hat.
 - Empty Message Packets:
 - Anzahl der von der GVRP-Anwendung empfangenen leeren GARP-BPDUs.

4.11.3 Group

GVRP VLAN Group Information	
VID	Member Port
Edit Administrative Control	

- GVRP Group VLAN Information
Zeigt die dynamischen Gruppenmitglieder und deren Informationen.

- Parameter
 - VID:
VLAN-Identifizier. Wenn eine GVRP-Gruppe ein dynamisches VLAN erstellt, so wird jeder dynamischen VLAN-Gruppe ein VID zwischen 1 und 4.094 zugewiesen.
 - Member Port:
Die Mitglieder derselben dynamischen VLAN-Gruppe.
 - Edit Administrative Control:
Hier können Sie beim Erstellen einer GVRP-Gruppe den "Applicant Mode" und den "Registrar Mode" mittels der Administrative-Control-Function ändern.

4.12 Configuration: QoS (Quality of Service)

Der Switch unterstützt vier QoS-Warteschlangen mit strikten und gewichteten fair queuing scheduling pro Port. Es stehen 24 QoS-Control-Lists (QCL) zur programmierbaren QoS-Klassifizierung mittels IEEE 802.1p, Ethertype, VID, IPv4/IPv6 DSCP und UDP/TCP-Ports and -Portbereichen zur Verfügung.

Damit besteht hohe Flexibilität in der Zuweisung von eingehenden Datenpaketen zu einer QoS-Klasse. Während der QoS-Klassifikation wird nach Informationen in bis zu Layer 4, inklusive IPv4 und IPv6 DSCP, IPv4 TCP/UDP-Ports und Benutzerpriorität von getaggten Datenpaketen gesucht. Dieser QoS-Klassifizierungs-Mechanismus wird durch eine QoS-Control-List (QCL) implementiert. Die einem Datenpaket zugewiesene QoS-Klasse wird im Gerät verwendet um Queuing, Scheduling und Aufstauungs-Kontrolle für ein Paket je nachdem, was in der zugehörigen Klasse definiert wurde, zu leisten.

Der Switch unterstützt erweiterte Speicher-Kontroll-Mechanismen um exzellente Performance für alle QoS-Klassen in allen Traffic-Szenarios, inklusive Jumbo-Paketen, zu leisten.

4.12.1 Ports

Port QoS Configuration

Number of Classes

Port	Default Class	QCL	User Priority	Queuing Mode	Queue Weighted (Low:Normal:Medium:High)			
1	Low	1	0	Strict Priority	1	2	4	8
2	Low	1	0	Strict Priority	1	2	4	8
3	Low	1	0	Strict Priority	1	2	4	8
4	Low	1	0	Strict Priority	1	2	4	8
5	Low	1	0	Strict Priority	1	2	4	8
6	Low	1	0	Strict Priority	1	2	4	8
7	Low	1	0	Strict Priority	1	2	4	8
8	Low	1	0	Strict Priority	1	2	4	8
9	Low	1	0	Strict Priority	1	2	4	8
10	Low	1	0	Strict Priority	1	2	4	8
11	Low	1	0	Strict Priority	1	2	4	8
12	Low	1	0	Strict Priority	1	2	4	8
13	Low	1	0	Strict Priority	1	2	4	8
14	Low	1	0	Strict Priority	1	2	4	8
15	Low	1	0	Strict Priority	1	2	4	8
16	Low	1	0	Strict Priority	1	2	4	8
17	Low	1	0	Strict Priority	1	2	4	8
18	Low	1	0	Strict Priority	1	2	4	8
19	Low	1	0	Strict Priority	1	2	4	8
20	Low	1	0	Strict Priority	1	2	4	8
21	Low	1	0	Strict Priority	1	2	4	8
22	Low	1	0	Strict Priority	1	2	4	8
23	Low	1	0	Strict Priority	1	2	4	8
24	Low	1	0	Strict Priority	1	2	4	8

Apply

■ Port QoS Configuration

Konfiguriert das QoS-Verhalten für jeden Port. Jeder Port hat dabei vier QoS-Warteschlangen mit entweder strict priority oder weighted fair Queuing-Scheduling. Es stehen 24 QoS-Control-Lists (QCL) zur vorausgehenden programmierten QoS-Klassifizierung mittels IEEE 802.1p, Ether-type, VID, IPv4/IPv6 DSCP und UDP/TCP-Ports and -Portbereichen zur Verfügung.

■ Parameter:

- Number of Classes: 1 / 2 / 4

- Port:
Sie können hier den Port (1~24) sowie dessen Priority-Class für die Per-PortPriority-Funktion wählen.
- Default Class:
Sie können hier zwischen hoher und niedriger Priorität für jeden Port wählen.
Low / Normal / Medium / High
- QCL:
Wählen Sie hier aus welche QCL-Regel 1~24 dieser Port anwendet. Jeder Port muss eine der QCL-Regeln für seine QoS-Verhalten anwenden.
- User priority:
Der Benutzer-Prioritäts-Wert 0~7 (3 Bits) wird als Index für die acht QoS-Klassen-Werte für VLAN-basiertes oder Prioritäts-getaggte Pakete verwendet.
- Queuing Mode:
Wählen Sie zwischen zwei Warteschlangen-Methoden: Strict Priority und Weighted Fair. Per Default ist strict priority eingestellt. Nach der Auswahl müssen Sie <Apply> klicken um die Einstellung zu übernehmen.
- Queue Weighted:
Pro Port gibt es vier Warteschlangen und vier Klassen gewichteter Zahlen (1 / 2 / 4 / 8) für jede Warteschlange. Sie können hier die gewichtete Nummer auswählen, wenn die Scheduling-Methode auf "Weighted Fair" gesetzt wurde.

4.12.2 Qos Control List

QoS Control List Configuration

QCE Type	Type Value	Traffic Class
----------	------------	---------------

- Qos Control List Configuration
Jeder Port hat vier QoS-Warteschlangen mit entweder strict priority oder weighted fair Queuing-Scheduling. Es stehen 24 QoS-Control-Lists (QCL)

zur programmierbaren QoS-Klassifizierung mittels IEEE 802.1p, Ethertype, VID, IPv4/IPv6 DSCP und UDP/TCP-Ports and -Portbereichen zur Verfügung.

QCE Configuration: Eine QCL besteht aus 12 QoS-Control-Entries (QCEs) die vom Kopf der Liste bis zum Ende nach einer Übereinstimmung durchsucht werden. Der erste passende QCE bestimmt die QoS-Klassifizierung des Pakets. Die Reihenfolge der QCE ist daher von entscheidender Bedeutung für das Resultat des QoS-Klassifizierungs-Algorithmus. Wird kein passender QCE gefunden, wird die Default-QoS-Klasse in der QoS-Port-Konfiguration verwendet.

- Parameter:
 - QCL#:
 - QCL number : 1~24
 - QCE Type:
 - Ethernet Type / VLAN ID / UDP/TCP Port / DSCP / ToS / Tag Priority
 - Ethernet Type Value:
 - Mögliche Werte sind 0x600~0xFFFF. Die meisten bekannten Protokolle haben bereits EtherType-Feld-Werte festgelegt. Die üblichsten Werte im EtherType-Feld und dazugehörigen Protokolle sind:

Ethertype (Hexadecimal)	Protocol
0x0800	IP, Internet Protocol
0x0801	X.75 Internet
0x0802	NBS Internet
0x0803	ECMA Internet
0x0804	Chaosnet
0x0805	X.25 Level 3
0x0806	ARP, Address Resolution Protocol.
0x0808	Frame Relay ARP [RFC1701]
0x6559	Raw Frame Relay [RFC1701]
0x8035	DRARP, Dynamic RARP. RARP, Reverse Address Resolution Protocol.
0x8037	Novell Netware IPX
0x809B	EtherTalk (AppleTalk over Ethernet)

Ethertype (Hexadecimal)	Protocol
0x80D5	IBM SNA Services over Ethernet
0x 80F3	AARP, AppleTalk Address Resolution Protocol.
0x8100	IEEE Std 802.1Q - Customer VLAN Tag Type.
0x8137	IPX, Internet Packet Exchange.
0x 814C	SNMP, Simple Network Management Protocol.
0x86DD	IPv6, Internet Protocol version 6.
0x880B	PPP, Point-to-Point Protocol.
0x 880C	GSMP, General Switch Management Protocol.
0x8847	MPLS, Multi-Protocol Label Switching (unicast).
0x8848	MPLS, Multi-Protocol Label Switching (multicast).
0x8863	PPPoE, PPP Over Ethernet (Discovery Stage).
0x8864	PPPoE, PPP Over Ethernet (PPP Session Stage).
0x88BB	LWAPP, Light Weight Access Point Protocol.
0x88CC	LLDP, Link Layer Discovery Protocol.
0x8E88	EAPOL, EAP over LAN.
0x9000	Loopback (Configuration Test Protocol)
0xFFFF	reserved.

- VLAN ID:
Mögliche VIDs: 1~4094
- UDP/TCP Port:
Wählt einen UDP/TCP nach Bereich oder spezifisch aus:
 UDP/TCP Port Range:
 Legen Sie hier einen Port-Bereich fest. Mögliche Port-Bereiche:
 0~65.535
 Unter der folgenden URL finden Sie Informationen zur Belegung
 von Port-Bereichen:
<http://www.iana.org/assignments/port-numbers>
 UDP/TCP Port No.:
 Legen Sie hier einen spezifischen Port fest. Mögliche Werte:
 0~65535

- DSCP Value:
Mögliche DSCP-Werte: 0~63
- Traffic Class:
Low / Normal / Medium / High

4.12.3 Rate Limiters

DE

Rate Limit Configuration

Port #	Ingress Enabled	Ingress Rate	Ingress Unit	Egress Enabled	Egress Rate	Egress Unit
1	<input type="checkbox"/>	500	kpbs	<input type="checkbox"/>	500	kpbs
2	<input type="checkbox"/>	500	kpbs	<input type="checkbox"/>	500	kpbs
3	<input type="checkbox"/>	500	kpbs	<input type="checkbox"/>	500	kpbs
4	<input type="checkbox"/>	500	kpbs	<input type="checkbox"/>	500	kpbs
5	<input type="checkbox"/>	500	kpbs	<input type="checkbox"/>	500	kpbs
6	<input type="checkbox"/>	500	kpbs	<input type="checkbox"/>	500	kpbs
7	<input type="checkbox"/>	500	kpbs	<input type="checkbox"/>	500	kpbs
8	<input type="checkbox"/>	500	kpbs	<input type="checkbox"/>	500	kpbs
9	<input type="checkbox"/>	500	kpbs	<input type="checkbox"/>	500	kpbs
10	<input type="checkbox"/>	500	kpbs	<input type="checkbox"/>	500	kpbs
11	<input type="checkbox"/>	500	kpbs	<input type="checkbox"/>	500	kpbs
12	<input type="checkbox"/>	500	kpbs	<input type="checkbox"/>	500	kpbs
13	<input type="checkbox"/>	500	kpbs	<input type="checkbox"/>	500	kpbs
14	<input type="checkbox"/>	500	kpbs	<input type="checkbox"/>	500	kpbs
15	<input type="checkbox"/>	500	kpbs	<input type="checkbox"/>	500	kpbs
16	<input type="checkbox"/>	500	kpbs	<input type="checkbox"/>	500	kpbs
17	<input type="checkbox"/>	500	kpbs	<input type="checkbox"/>	500	kpbs
18	<input type="checkbox"/>	500	kpbs	<input type="checkbox"/>	500	kpbs
19	<input type="checkbox"/>	500	kpbs	<input type="checkbox"/>	500	kpbs
20	<input type="checkbox"/>	500	kpbs	<input type="checkbox"/>	500	kpbs
21	<input type="checkbox"/>	500	kpbs	<input type="checkbox"/>	500	kpbs
22	<input type="checkbox"/>	500	kpbs	<input type="checkbox"/>	500	kpbs
23	<input type="checkbox"/>	500	kpbs	<input type="checkbox"/>	500	kpbs
24	<input type="checkbox"/>	500	kpbs	<input type="checkbox"/>	500	kpbs

Apply

■ Rate Limit Configuration

In jedem Port ist ein Eingangs-Policer und ein Ausgangs-Shaper integriert, mit deren Hilfe sich die Bandbreite von empfangenen und gesendeten Datenpaketen limitieren lässt. Der Eingangs-Policer und Ausgangs-Shaper wird pro Port von der Rate-Limit-Konfiguration geregelt.

■ Parameter:

- Port #:
Port number.

- **Policer Enabled:**
Verwendet den Policer um die eingehende Bandbreite nach der Policer-Rate zu begrenzen.
- **Policer Rate:**
Mögliche Policer-Raten-Werte:
500 Kbps ~ 1000000 Kbps
1 Mbps ~ 1000 Mbps
- **Policer Unit:**
Hier können Sie zwischen den zwei Einheiten de Eingangs-Policer-Rate wählen: kbps / Mbps
- **Shaper Enabled:**
Verwendet den Shaper um die ausgehende Bandbreite nach der Shaper-Rate zu begrenzen.
- **Shaper Rate:**
Mögliche Shaper-Raten-Werte:
500 Kbps ~ 1000000 Kbps
1 Mbps ~ 1000 Mbps
- **Shaper Unit:**
Hier können Sie zwischen den zwei Einheiten de Ausgangs-Shaper-Rate wählen: kbps / Mbps

4.12.4 Storm Control

Storm Control Configuration

Frame Type	Status	Rate (pps)
Flooded unicast	<input type="checkbox"/>	1
Multicast	<input type="checkbox"/>	1
Broadcast	<input type="checkbox"/>	1

Apply

- **Storm Control Configuration**
Der Switch unterstützt Storm-Control über den Eingangs-Policer um Flooded Unicast-, Multicast- und Broadcast-Pakete zu limitieren und so einem Storm-Ereignis vorzubeugen.

- Parameter:
 - Frame Type:
Es lassen sich drei Storm-Paket-Arten kontrollieren: Flooded unicast / Multicast / Broadcast
 - Status:
Enable/Disable Selection: Ein Häkchen in der Box bedeutet das Feature ist eingeschaltet, eine freie Box bedeutet es ist ausgeschaltet
 - Rate(pps):
Wählen Sie aus der folgenden Raten-Liste. Die Werte sind in Paket pro Sekunde (pps) angegeben.
1 / 2 / 4 / 8 / 16 / 32 / 64 / 128 / 256 / 512 / 1K / 2K / 4K / 8K / 16K / 32K / 64K / 128K / 256K / 512K / 1024K

4.12.5 Wizard

Welcome to the QCL Configuration Wizard!

Please select an action:

- Set up Port Policies**
Group ports into several types according to different QCL policies.
- Set up Typical Network Application Rules**
Set up the specific QCL for different typical network application quality control.
- Set up TOS Precedence Mapping**
Set up the traffic class mapping to the precedence part of TOS (3 bits) when receiving IPv4/IPv6 packets.
- Set up VLAN Tag Priority Mapping**
Set up the traffic class mapping to the user priority value (3 bits) when receiving VLAN tagged packets.

To continue, click Next.

Next >

- Wizard
Der QCL-Konfigurations-Wizard zielt darauf ab, Ihnen das Einstellen der QCL-Regeln zur QoS-Konfiguration zu erleichtern. Der Wizard stellt Ihnen übliche Netzwerk-Applikationen der Regeln zur Verfügung, die Sie dann komfortabel einsetzen können.

- Parameter:
 - Please select an Action:
Wählen Sie eine der folgenden Aktionen und klicken Sie dann auf <Next> um die QCL-Konfiguration abzuschliessen:
Set up Port Policies
Set up Typical Network Application Rules
Set up TOS Precedence Mapping
Set up VLAN Tag Priority Mapping
 - Next:
Geht zum nächsten Schritt.
 - Cancel:
Bricht die aktuelle Konfiguration ab und geht zum letzten Schritt zurück.
 - Back:
Zurück zum vorherigen Schritt.
 - QCL ID:
QoS Control List (QCL): 1~24
 - Port Member:
Port Member: 1~24
 - Wizard Again:
Klicken Sie auf <Wizard Again> um zum QCL-Konfigurations-Wizard zurückzukehren.
 - Finish:
Durch ein Klicken auf <Finish> werden die Parameter entsprechend des Wizards gesammelt und auf der Oberfläche angezeigt. Durch ein Klicken auf <Apply> bestätigen Sie geänderte Parameter.
 - Audio and Video:
QuickTime 4 Server / MSN Messenger Phone / Yahoo Messenger Phone / Napster / Real Audio
 - Games:
Blizzard Battlenet (Diablo2 and StarCraft) / Fighter Ace II / Quake2 / Quake3 / MSN Game Zone

- User Definition:
 - Ethernet Type / VLAN ID / UDP/TCP Port / DSCP
 - Ethernet Type Value: Type Bereich: 0x600~0xFFFF
 - VLAN ID: VLAN ID Bereich: 1~4094
 - UDP/TCP Port: Zwei Modi: Range / Specific
 - UDP/TCP Port Range: Port-Bereich: 0~65535
 - UDP/TCP Port No.: Port-Bereich: 0~65535
 - DSCP Value: DSCP-Werte-Bereich: 0~63
- QCL ID:
 - QCL ID Bereich: 1~24
- Traffic Class:
 - Es gibt vier verfügbare Klassen: Low / Normal / Medium / High
- QCL #:
 - QoS Control List (QCL): 1~24
- QCL ID:
 - QoS Control List (QCL): 1~24
- TOS Precedence 0~7 Class:
 - Low / Normal / Medium / High
- QCL ID:
 - QoS Control List (QCL): 1~24
- Tag Priority 0~7 Class:
 - Low / Normal / Medium / High

4.13 Configuration: Trunk

In den Port-Trunking-Einstellungen können Sie entscheiden, wie bei Link-Bündelung verfahren werden soll. Sie können mehr als einen Port mit derselben Geschwindigkeit, Full-Duplex und derselben MAC-Adresse als einen logischen Port zusammenfassen, dem dann die gebündelte Bandbreite dieser Ports zur Verfügung steht. Damit können Sie mit ihrer bestehenden Ethernet-Infrastruktur höhere Bandbreiten verwirklichen. Beispielsweise erreichen Sie durch das Zusammenfassen von drei Ports zu einem logischen Port die dreifache Bandbreite.

Der Switch unterstützt zwei Methoden des Port-Trunking:

1 LACP:

Ports mit dem "Link Aggregation Control Protocol" nach IEEE 802.3ad (LACP, Link-Bündelungs-Kontroll-Protokoll) als Port-Trunking-Methode können eine eindeutige "LACP-GroupID" (Zwischen 1 und 3) (LACP-Gruppen-Identität) festlegen um einen logischen Port zu bilden. Der Vorteil dieser Methode ist, dass ein Port sich mit dem Gegenport abstimmt bevor er ein aktives Mitglied (auch Aggregator genannt) einer Trunk-Gruppe, also eines logischen Ports wird. Das LACP ist daher die sicherere Trunking-Methode.

Port-Trunking wird in folgenden Fällen nicht funktionieren:

- Link-Bündelung über mehrere Switches
- Bündelung mit nicht IEEE 802.3-MAC-kompatiblen Links
- Operieren im Half-Duplex Modus
- Das Bündeln von Ports mit verschiedenen Datenraten

2 Static Trunk:

Wenn Sie für Ports die Static-Trunk-Methode (Statische Trunks) wählen, müssen Sie ihnen eine bestimmte "Static-GroupID" (Ebenfalls 1-3, die Statische-Gruppen-Identität kann dieselbe sein, wie die einer LACP-Gruppe) zuweisen. Der Vorteil dieser Methode ist, dass ein Port sofort als aktives Mitglied eines logischen Ports funktioniert, ohne sich vorher mit der Gegenseite abstimmen zu müssen. Dies ist gleichzeitig allerdings auch ein Nachteil, da die jeweiligen gegenüberliegenden Ports eventuell nicht als logischer Port konfiguriert sind. Deshalb sollten Sie in diesem Fall auf beiden Seiten Static-Trunk als Methode wählen. Beachten Sie bitte auch, dass Links mit niedriger Geschwindigkeit bei dieser Methode nicht aktive Mitglieder eines logischen Ports werden, wenn man sie mit Links höherer Geschwindigkeit bündelt.

Der Switch erlaubt es, bis zu drei Static-Trunk- und LACP-Gruppen in der Management-Ansicht festzulegen. Es können jedoch nur drei logische Ports gleichzeitig aktiv sein. Eine LACP-Gruppe mit mehr als einem aktiven Mitglied wird als aktiver logischer Port verstanden, während eine LACP-Gruppe mit nur einem aktiven Mitglied nicht als solcher unterstützt wird. Jede Statische Trunk-Gruppe ist automatisch ein aktiver logischer Port.

Jede Trunk-Gruppe unterstützt maximal zwölf aktive Mitglieder. Bitte beachten Sie, dass einige Entscheidungen automatisch vom System getroffen werden, während sie Einstellungen der Trunk-Ports vornehmen. Trunk-Einstellungsregeln finden Sie im Folgenden:

- ① Zwölf Ports benutzen bereits die Static-Trunk-Gruppen-ID 1, der 13. Port, der die selbe Static-Trunk-Gruppen-ID benutzen will, wird automatisch die None-Trunking-Methode benutzen und die Gruppen-ID wird 0 sein. Das bedeutet, dass der Port sich nicht mit den anderen Ports verbindet.
- ② Wenn 14 Ports die LACP-Trunk-Gruppen-ID 1 benutzen, können sich höchstens 12 Ports verbinden und in einen betriebsbereiten Zustand übergehen.
- ③ Ein Port, der die None-Trunking-Methode oder Gruppen-ID 0 benutzt, wird automatisch die None-Trunking-Methode oder Gruppen-ID 0 benutzen.

4.13.1 Port

Trunk Port Setting/Status

Port	Trunk Port Setting			Trunk Port Status	
	Method	Group	Active LACP	Aggr	Status
1	None	0	Active	1	Ready
2	None	0	Active	2	Ready
3	None	0	Active	3	Ready
4	None	0	Active	4	---
5	None	0	Active	5	---
6	None	0	Active	6	---
7	None	0	Active	7	---
8	None	0	Active	8	---
9	None	0	Active	9	---
10	None	0	Active	10	---
11	None	0	Active	11	---
12	None	0	Active	12	---
13	None	0	Active	13	---
14	None	0	Active	14	Ready
15	None	0	Active	15	Ready
16	None	0	Active	16	Ready
17	None	0	Active	17	---
18	None	0	Active	18	---
19	None	0	Active	19	---
20	None	0	Active	20	---
21	None	0	Active	21	---
22	None	0	Active	22	---
23	None	0	Active	23	---
24	None	0	Active	24	---

Apply/Refresh

- Trunk Port Setting/Status
Hier können Sie die Zugehörigkeit zu einer Trunk-Gruppe für jeden Port einsehen und konfigurieren.
- Parameter:
 - Port:
Portnummer: 1-24

- Method: Legen Sie hier die Methode fest, die der Port nutzen soll um mit anderen Ports gebündelt zu werden.
 - None: Der Port wird sich nicht mit anderen Ports bündeln.
 - LACP: Das LACP wird benutzt um den Port mit anderen Ports zu einem logischen Port zu bündeln.
 - Static: Der Port wird Static-Trunk als Methode verwenden um sich mit anderen Ports, die ebenfalls Static-Trunk nutzen, zu bündeln.
- Group:
 - Alle Ports, die dieselbe Methode verwenden, müssen einer eindeutigen Gruppen-Identität (zwischen 1 und 8) zugeordnet werden, wenn sie als logischer Port gebündelt werden,
- Active LACP:
 - Dieses Feld wird nur dann angezeigt, wenn die Trunking-Methode für diesen Port LACP ist.
 - Active:
 - Ein aktiver LACP Port wird mit dem Senden einer LACPDU(LACP-Paket) an sein Gegenüber beginnen, sobald die LACP Entität die Kontrolle über diesen Port übernommen hat.
 - Passive:
 - Ein passiver LACP Port wird nicht von sich aus eine LACPDU senden, bevor er nicht ein solches Paket von seinem Gegenüber erhalten hat.
- Aggtr:
 - Aggtr ist eine Abkürzung für "Aggregator". Jeder Port ist auch ein Aggregator, und seine Aggregator-ID ist dieselbe wie seine Port-Nummer. Einen Aggregator können wir als Repräsentant seiner Trunking-Gruppe betrachten. Alle Ports mit derselben Gruppen-Identität und Trunk-Methode lassen sich zu einem bestimmten Aggregator-Port zusammen bündeln. Der Aggregator-Port ist normalerweise der Port mit der niedrigsten Port-Nummer innerhalb der Trunk-Gruppe.
- Status:
 - Dieses Feld zeigt Ihnen den Trunk-Status eines Ports an, der an der Port-Bündelung teilnimmt. Ports, die nicht an der Port-Bündelung teilnehmen, erscheinen als "not ready"(Nicht bereit).

4.13.2 Aggregator View

DE

Aggregator View

Aggregator	Method	Member Ports	Ready Ports
1	None	1	1
2	None	2	2
3	None	3	3
4	None	4	
5	None	5	
6	None	6	
7	None	7	
8	None	8	
9	None	9	
10	None	10	
11	None	11	
12	None	12	
13	None	13	
14	None	14	14
15	None	15	15
16	None	16	16
17	None	17	
18	None	18	
19	None	19	
20	None	20	
21	None	21	
22	None	22	
23	None	23	
24	None	24	

Refresh
LACP Detail

■ Aggregator View

Zeigt Ihnen die aktuellen Trunk-Informationen aus Sicht eines Aggregators an.

■ Parameter:

Aggregator:

Hier finden Sie die Aggregator-ID (1-26) für jeden Port, die mit der generellen Port-Nummer bzw. -ID übereinstimmt, da jeder Port potentiell ein Aggregator ist.

Method:

Zeigt Ihnen die Methode an, die ein Port verwendet um sich mit anderen Ports zu bündeln.

- Member Ports:
Alle Port-Mitglieder eines Aggregators werden Ihnen hier angezeigt.
- Ready Ports:
Nur die aktiven Mitglieder eines Aggregators werden angezeigt.

4.13.3 Hash Method

Aggregation Mode Configuration

Hash Code Contributors	
Source MAC Address	<input checked="" type="checkbox"/>
Destination MAC Address	<input type="checkbox"/>
IP Address	<input checked="" type="checkbox"/>
TCP/UDP Port Number	<input checked="" type="checkbox"/>

4.13.4 LACP System Configuration

LACP System Priority

System Priority	32768 (1~65535)
-----------------	-----------------

- LACP System Configuration

In den LACP-System-Einstellungen können Sie den Prioritätsteil der LACP-System-ID festlegen. Das LACP wird nur Ports zusammenbündeln, deren Partner sich ebenfalls auf nur einem System befinden. Jedes System, das das LACP unterstützt bekommt dazu eine eindeutige, globale System-ID zugewiesen. Diese System-ID besteht aus einem 64-Bit Feld, das wiederum aus einer 48-Bit MAC-Adresse und einem 16-Bit Prioritätswert besteht.
- Parameter
 - System Priority:
Die Systempriorität lässt sich von Ihnen zwischen 1 und 65.535 festlegen. Die Default-Einstellung ist 32.768.

4.14 Configuration: STP

Das Spanning Tree Protocol (STP) ist eine standardisierte Methode (IEEE 802.1D) um Schleifen in geschwichten Netzwerken zu vermeiden. Wenn STP aktiv ist, sollten Sie sicherstellen, dass zu einem Zeitpunkt nur eine Verbindung zwischen zwei Knotenpunkten des Netzwerks aktiviert ist. Sie können das Spanning Tree Protocol mit Hilfe des Web-Managements aktivieren und dort auch weiterführende Einstellungen vornehmen. Es wird empfohlen, dass Sie STP in allen Switches aktivieren, um sicher zu sein, dass es immer nur eine aktive Verbindung im Netzwerk gibt.

4.14.1 Status

STP Status	
STP State	Disabled
Bridge ID	00:40:C7:5C:00:73
Bridge Priority	32768
Designated Root	00:40:C7:5C:00:73
Designated Priority	32768
Root Port	0
Root Path Cost	0
Current Max. Age(sec)	20
Current Forward Delay(sec)	15
Hello Time(sec)	2
STP Topology Change Count	0
Time Since Last Topology Change(sec)	0

■ STP Status

Im Spanning Tree Status können Sie 12 Parameter einsehen, um den aktuellen Stand des STP zu erfahren. Im Folgenden werden die Eigenschaften der 12 Parameter beschrieben.

■ Parameter:

- STP State:
Zeigt den aktuellen STP Stand "enable" oder "disable". Default ist "enable".
- Bridge ID:
Zeigt die Bridge-ID des Switches, welche auch die MAC-Adresse ist.
- Bridge Priority:
Zeigt die aktuelle Einstellung der Bridge-Priority. Default ist 32.768.

- Designated Root:
Zeigt die ID der Root-Bridge dieses Netzwerksegments. Wenn dieser Switch eine Root-Bridge ist, wird der Designated-Root die Bridge-ID des Switchs anzeigen.
- Designated Priority:
Zeigt die aktuelle Root-Bridge-Priority.
- Root Port:
Zeigt die Root-Port-Number mit den niedrigsten Verbindungskosten für Verbindungen zur Root-Bridge an.
- Root Path Cost:
Zeigt die Verbindungskosten zwischen dem Root-Port und dem vorgesehenen Port der Root-Bridge.
- Current Max. Age:
Aktuelle Angabe der maximum age time (maximale Lebensdauer) der Root-Bridge. Maximum age time wird benutzt, wenn die STP Topologie verändert werden soll. Wenn eine Bridge eine Nachricht zur Betriebsbereitschaft (Hello-Message) von der Root-Bridge nicht empfängt bis die maximum age time auf 0 heruntergezählt hat, wird die Root-Bridge als nicht funktionstüchtig angesehen. Die Bridge sendet dann eine Topology Change Notification (TCN) BPDU an alle anderen Bridges.

Alle Bridges im LAN können neu entscheiden und sich merken wer die Root-Bridge ist. Die maximum age time wird von der Root-Bridge in Sekunden bestimmt. Default ist 20 Sekunden.
- Current Forward Delay:
Zeigt die aktuelle Forward-Delay-Time der Root-Bridge (Verzögerung beim Senden einer Nachricht). Der Wert der Forward-Delay-Time wird beim Rooten bestimmt. Die Forward-Delay-Time ist die Zeit die verstreicht vom Listening-State bis zum Learning-State oder vom Learning-State zum Forwarding-State eines Bridge-Ports.
- Hello Time:
Zeigt die aktuelle Hello-time der Root-Bridge. Die Hello-time ist ein Zeitintervall, welches von der Root-Bridge bestimmt wird. Es wird dazu benutzt, um über einen bestimmten Zeitraum alle anderen Bridges aufzufordern, jede Hello-Time-Sekunde Hello-Message zu der Bridge mit dem zugewiesenen Designated-Port zu senden.

- STP Topology Change Count:
STP Topology Change Count gibt die Zeit in Sekunden an, die vom Beginn des Spanning Tree Topology Change bis zum Ende der STP Konvergenz benötigt wird. Wenn der STP-Wechsel einmal umgewandelt ist, wird der Topologiewechsel auf 0 zurück gestellt. Die dafür auf dem Bildschirm angegebene Zeit wird exakt oder fast exakt wiedergegeben .
- Time Since Last Topology Change:
Time Since Last Topology Change gibt die akkumulierte Zeit in Sekunden an, die seit dem letzten STP Topologiewechsel vergangen ist. Wenn ein Topologiewechsel ausgelöst wird, stellt sich der Zähler zurück auf 0. Er fängt erneut an zu zählen, wenn eine STP Topology Change abgeschlossen ist.

4.14.2 Konfiguration

STP Configuration

Spanning Tree Protocol	Disable ▾
Bridge Priority (0-61440)	32768 ▾
Hello Time (1-10 sec)	2
Max. Age (6-40 sec)	20
Forward Delay (4-30 sec)	15
Force Version	RSTP ▾

Note: $2 * (\text{Forward Delay} - 1) \geq \text{Max Age}$
 $\text{Max Age} \geq 2 * (\text{Hello Time} + 1)$

Apply

Note: You will lose connection with this device for a while if you enable STP.

Das Spanning Tree Protocol (STP), beinhaltet RSTP. In der Spanning Tree Konfiguration gibt es sechs Parameter, die Sie konfigurieren können. Im Folgenden werden die Eigenschaften der Parameter beschrieben.

- STP Configuration
Sie können die folgenden Spanning Tree Parameter auf "enable" oder "disable" einstellen um die STP Funktion zu kontrollieren. Wählen Sie den RSTP/STP Modus und beeinflussen Sie den STP Status der Maschine um BPDU zu senden. Default setting des Spanning Tree Protocol ist "disable".

■ Parameter:

- Spanning Tree Protocol:
802.1W Rapid STP Funktion kann auf "enable" oder "disable" eingestellt werden. Default ist "disable".
- Bridge Priority:
Je niedriger der hier eingestellte Wert ist, desto höhere Priorität hat die Bridge. Normalerweise ist die Bridge mit der höchsten Priorität die Root-Bridge. Wenn Sie den LANCOM Switch als Root-Bridge benutzen wollen, können Sie ihren Wert niedriger wählen, als den Wert der Bridge im LAN. Gültige Werte liegen zwischen 0 ~ 61.440. Default ist 32.768.
- Hello Time:
Hello-Time wird benutzt, um die Zeit, für das Senden von einem normalen BPDU, von bestimmten Ports über Bridges zu begrenzen. Die Hello-Time entscheidet, wie lange eine Bridge eine Nachricht zu einer anderen Bridge schicken sollte und darüber, ob sie funktionstüchtig ist. Wenn zum Beispiel der LANCOM Switch die Root-Bridge des LANs ist, werden alle anderen Bridges wie vom Switch zugewiesen die Hello-time benutzen um miteinander zu kommunizieren. Die gültigen Werte liegen zwischen 1 ~ 10 in Sekunden. Default ist 2 Sekunden.
- Max. Age:
Wenn der LANCOM Switch die Root-Bridge ist, wird das ganze LAN die Einstellung des maximum age time des Switches übernehmen. Wenn eine Bridge eine BPDU von der Root-Bridge erhält und die age time dieser Nachricht das Maximum der Root-Bridge übersteigt, wird die Bridge die Root-Bridge als nicht funktionstüchtig ansehen und eine Topology Change Notification (TCN) BPDU an alle anderen Bridges senden. Alle anderen Bridges im LAN können sowohl bestimmen, als auch sich merken, wer die Root-Bridge ist. Der gültige Wert für das maximum age liegt zwischen 6 ~ 40 Sekunden. Default ist 20 Sekunden.
- Forward Delay:
Sie können die Forward-Delay-Time der Root-Bridge einstellen. Diese Einstellungsmöglichkeit gibt es nur bei der Root-Bridge. Die Forward-Delay-Time ist die Zeit, die ein Bridge-Port benötigt, um vom Listening-State in den Learning-State oder vom Learning-State in den Forwarding-State zu gelangen. Die Forward-Delay-Time besteht aus zwei

Phasen, die erste Phase ist der Übergang vom Listening-State zum Learning-State und die zweite Phase ist vom Learning-State zum Forwarding-State. Es wird angenommen, dass die Forward-Delay-Time pro Phase 15 Sekunden und somit insgesamt 30 Sekunden beträgt. Dies steht im Zusammenhang mit der STP-Convergent-Time. Gültige Werte liegen zwischen 4 ~ 30 Sekunden. Default ist 15 Sekunden.

□ Force Version:

Für den STP Algorithmus werden Ihnen zwei Optionen angeboten, RSTP und STP. Wenn Sie STP wählen, wird RSTP nachrangig angesehen. Der Switch unterstützt RSTP (802.1w), welches rückwärts kompatibel mit STP (802.1d) ist.

4.14.3 Port

STP Port Configuration						
Port No	Port Status	Path Cost Status	Configured Path Cost	Priority	Admin Port Type	Admin Point To Point
1	FORWARDING	2000000	0	128	Normal	Auto
2	FORWARDING	2000000	0	128	Normal	Auto
3	FORWARDING	2000000	0	128	Normal	Auto
4	FORWARDING	2000000	0	128	Normal	Auto
5	FORWARDING	2000000	0	128	Normal	Auto
6	FORWARDING	2000000	0	128	Normal	Auto
7	FORWARDING	2000000	0	128	Normal	Auto
8	FORWARDING	2000000	0	128	Normal	Auto
9	FORWARDING	2000000	0	128	Normal	Auto
10	FORWARDING	2000000	0	128	Normal	Auto
11	FORWARDING	2000000	0	128	Normal	Auto
12	FORWARDING	2000000	0	128	Normal	Auto
13	FORWARDING	2000000	0	128	Normal	Auto
14	FORWARDING	2000000	0	128	Normal	Auto
15	FORWARDING	2000000	0	128	Normal	Auto
16	FORWARDING	2000000	0	128	Normal	Auto
17	FORWARDING	2000000	0	128	Normal	Auto
18	FORWARDING	2000000	0	128	Normal	Auto
19	FORWARDING	2000000	0	128	Normal	Auto
20	FORWARDING	2000000	0	128	Normal	Auto
21	FORWARDING	2000000	0	128	Normal	Auto
22	FORWARDING	2000000	0	128	Normal	Auto
23	FORWARDING	2000000	0	128	Normal	Auto
24	FORWARDING	2000000	0	128	Normal	Auto

Edit MCheck

■ STP Port Setting

Zur Einstellung des STP-Ports stehen Ihnen verschiedene Parameter zur Verfügung. Sie können jeden Port aktivieren oder deaktivieren, indem Sie den Port-Status bestimmen. Sie können ebenfalls die Verbindungskosten und die Priorität der einzelnen Ports einstellen, indem Sie den jeweiligen Wert eintragen und Admin-Edge-Port oder Admin-Point-to-Point einstellen.

■ Parameter:

□ Port Status:

Gibt den aktuellen Status des Ports an. Es gibt nach der 802.1w Spezifikation drei mögliche Zustände.

“Discarding State” bedeutet, dass dieser Port weder Pakete schicken noch erlerntes Wissen einbringen kann.

Beachten Sie: Drei andere Status (“disable state”, “blocking state” und “listening state”) werden nach der 802.1d Spezifikation alle durch den “discarding state” vertreten.

“Learning state” bedeutet, dass der Port sein gelerntes Wissen einbringen, aber keine Pakete versenden kann.

“Forwarding state” bedeutet, dass der Port sowohl sein erlerntes Wissen einbringen, als auch Pakete verschicken kann.

□ Path Cost Status:

Dies ist der Wert der Verbindung vom Port zur Root-Bridge. Der STP Algorithmus bestimmt die beste Verbindung zur Root-Bridge, indem er die Summe der Verbindungskosten von allen Ports für diese Verbindung berechnet. So ist wahrscheinlicher, dass ein Port mit geringeren Verbindungskosten Root-Port wird.

□ Configured Path Cost:

Der Bereich geht von 0 - 200.000.000. Wenn die Verbindungskosten auf Null eingestellt sind, wird das STP den empfohlenen Wert aus der Auto-Verhandlung des entsprechenden Links bekommen und diesen Wert im Path Cost Status anzeigen. Wenn dies nicht der Fall ist, wird der Wert angezeigt, den der Administrator im Configured-Path-Cost und Path-Cost-Status eingegeben hat.

Der empfohlene Wert für 802.1w RSTP liegt zwischen 1 - 200.000.000.

10 Mbps : 2.000.000

100 Mbps : 200.000

1 Gbps : 20.000

Default : 0

□ Priority:

In diesem Fall ist die Priorität des Ports gemeint. Die Priorität und die Nummer des Ports ergeben zusammen die ID des Ports. Port-IDs wer-

den oft verglichen, um zu bestimmen welcher Port einer Bridge Root-Port wird. Der Bereich umfasst 0 - 240. Default ist 128.

□ Admin Edge Port:

Wenn Sie die Einstellung "yes" wählen, wird der Port ein Edge-Port. Ein Edge-Port ist ein Port, der mit einem Gerät verbunden ist, dass das STP oder RSTP nicht beherrscht. Normalerweise ist das verbundene Gerät dann eine Endpunkt. Edge-Ports gelangen sofort in einen Forwarding-State und überspringen den Listening- und Learning-State, weil der Edge-Port keine Bridging-Loops im Netzwerk erstellen kann. Dies beschleunigt die Konvergenz. Wenn der Link des Edge-Ports umschaltet, wird die STP-Topologie nicht verändert. Im Gegensatz zu einem Designated-Port oder einem Root-Port, schaltet der Edge-Port auf einen normalen Spanning-Tree-Port um, sobald er ein BPDU empfängt. Default ist "no".

□ Admin Point To Point:

Aus der Sicht des RSTP ist ein Port ein Point-to-Point-Link, wenn er im vollduplexen Modus ist und ein Shared-Link, wenn er im halbduplexen Modus ist. Schnelle RSTP-Konvergenz kann nur in Point-to-Point-Links und in Edge-Ports stattfinden. Da der Port schnell in einen Forwarding-State gelangt, kann die Konvergenz beschleunigt werden.

Es gibt drei Parameter "auto" "true" und "false", die dazu benutzt werden den Typ des Point-to-Point-Links zu bestimmen. Wenn Sie diesen Parameter auf "auto" einstellen, befindet sich RSTP im duplexen Modus. In den heutzutage geschwichten Netzwerken laufen die meisten Links im vollduplexen Modus. Manchmal kann das Ergebnis auch halbduplex sein. In diesem Fall wird der Port nicht in den Forwarding-State umschalten. Wenn Sie die Einstellung "true" wählen, wird der Port von RSTP als Point-to-Point-Link angesehen und bedingungslos in den Forwarding-State gebracht. Wenn Sie "false" wählen, wird die Umwandlung zum Forwarding-State nicht vorkommen. Default ist "auto".

□ M Check

Der Migration-Check zwingt den Port ein RSTP BPDU anstelle eines nachrangigen STP BPDU bei der nächsten Übertragung zu senden. Der Vorteil dieses Vorgangs ist, dass der Port schnell wieder zum RSTP-Port wird. Klicken Sie <M Check> um ein RSTP BPDU von dem, von Ihnen ausgewählten, Port zu senden.

4.15 Configuration: MSTP

Die Anwendung von MSTP geschieht nach IEEE 802.1Q 2005 Klausel 13, Multiple-Spanning-Tree-Protokoll. MSTP ermöglicht Datenpaketen, die zu verschiedenen VLANs gehören, verschiedenen Pfaden zu folgen, jeder basierend auf einem eigenen Multiple Spanning Tree Instance (MSTI), mit MST Bereichen und /oder MST-Bridges. Die richtige Konfiguration von MSTP in einer 802.1Q VLAN Umgebung versichert eine schleifenfreie Datenübertragung für eine Gruppe VLANs in einem MSTI. Mit Hilfe dieses Features werden auch redundante Pfade und Load Balancing in VLAN Umgebungen erreicht. Eine Spanning-Tree-Instanz CIST (Common and Internal Spanning Tree) gibt es immer, es können bis zu 64 weitere Spanning-Trees bereitgestellt werden.

4.15.1 State

MSTP State

Multiple Spanning Tree Protocol	Disable ▾
Force Version	MSTP ▾

Apply

■ MSTP State

Der MSTP Status ist "enable" oder "disable". Sie können hier auch eine Version des Spanning-Tree-Protokolls auswählen, mit dem MSTP arbeiten soll.

■ Parameter:

- Multiple Spanning Tree Protocol:
"disabled" oder "enabled"
- Force Version:
STP / RSTP / MSTP

4.15.2 Region Config

MSTP Region Config

Region Name (0-32 characters)	mstpRegion1
Revision Level (0-65535)	0

Apply

■ MSTP Region Config

Hier können Sie die grundsätzliche Identifikation einer MSTP-Bridge konfigurieren. Bridges in einem gemeinsamen Bereich müssen den selben Bereichsnamen und das selbe Revisions-Level haben.

■ Parameter:

 Region Name:

0-32 Zeichen. (Ein variabler Text verschlüsselt in einem festgelegten Feld mit 32 Achtbitzeichen nach der RFC 2271 Definition von SnmpAdminString.)

 Revision Level:

0-65.535

4.15.3 Instance View

Instance ID	Corresponding Vlan
0	1-4094

■ MSTP Instance Config

Hier sehen Sie die Tabelle mit den MST Instanzen, die Informationen (Zugehörigkeit eines MST zum VLAN) aller Spanning-Tree-Instanzen in dem ausgewählten MST-Bereich enthält, zu dem die Bridge gehört. Mit dieser Tabelle können Sie MSTP-Konfigurationsdateien hinzufügen und den MSTP-Status abfragen.

■ Parameter description:

 Instance ID:

Jede Spanning-Tree-Instanz muss eine eigene ID zwischen 0-4095 haben. Instanz 0 (CIST) gibt es immer und kann nicht gelöscht wer-

den. Zusätzliche Spanning-Tree-Instanzen (MSTIs) können hinzugefügt oder gelöscht werden. Mindestens ein VLAN muss für ein MSTI bereitgestellt sein, um den Bedarf für das MSTI anzugeben.

- Corresponding VLANs:

0-4095.

Multiple VLANS können zu einem MSTI gehören. Allen VLANS die nicht automatisch bereitgestellt sind, wird automatisch die Instanz 0 (CIST) zugeteilt.

- Edit MSTI / VLAN:

Siehe Abbildung. Hier können Sie ein MSTI hinzufügen und seine VLAN-Mitglieder angeben oder die VLAN-Mitglieder für ein bestimmtes MSTI verändern.

- Del MSTI:

Hier können Sie ein MSTI löschen.

- Del All MSTI:

Hier können Sie alle bestehenden MSTIs auf einmal löschen.

- Instance Configuration:

Hier können Sie die Parameter für die Spanning-Tree-Instanzen einstellen.

- Port Config:

Hier können Sie die Parameter für den Spanning-Tree-Port für jeden Port einstellen.

- Instance Status:

Siehe Abbildung. Hier sehen Sie den Status-Report einer bestimmten Spanning-Tree-Instanz.

- Port Status:

Hier sehen Sie den Status-Report von allen Ports bezüglich einer bestimmten Spanning-Tree-Instanz.

- VLAN Mapping:

VID STRING

- VID STRING Example:

2.5-7.100-200.301.303.1000-1500 (Valid VID Range:1-4094)

- Priority:
Gibt die Priorität der CIST-Verbindung an.
0 / 4096 / 8192 / 12288 / 16384 / 20480 / 24576 / 28672 / 32768 / 36864 / 40960 / 45056 / 49152 / 53248 / 57344 / 61440
- MAX. Age:
6-40 Sekunden. Es gilt die selbe Definition, wie im RSTP-Protokoll.
- Forward Delay:
4-30 Sekunden. Es gilt die selbe Definition, wie im RSTP-Protokoll.
- MAX. Hops:
6-40 Sekunden. Hierbei handelt es sich um einen neuen Parameter für das Multiple-Spanning-Tree-Protokoll. Es wird bei internen Spanning-Tree-Instanzen benutzt. "CIST Remaining Hops" oder "MSTI Remaining Hops" in der Spanning-Tree-Protokoll-Nachricht, nehmen um eins ab, wenn die Nachricht an die Nachbar-Bridge gegeben wird. Wenn die "Remaining Hops" in einer Nachricht Null sind, wird die Nachricht (BPDU) als invalide angesehen. "Max Hops" wird dazu verwendet um den ursprünglichen Wert der "Remaining Hops" für die Root-Bridge des Bereiches (CIST-Regional-Root oder MSTI-Regional-Root) zu spezifizieren.
- Port:
1-24
- Path Cost:
1 - 200,000,000.
Es gilt die selbe Definition wie in der RSTP Spezifizierung. In MSTP kann dieser Parameter jedoch zu den jeweiligen Ports von CIST und MSTI hinzugefügt werden.
- Priority:
0 / 16 / 32 / 48 / 64 / 80 / 96 / 112 / 128 / 144 / 160 / 176 / 192 / 208 / 224 / 240
Es gilt die selbe Definition wie in der RSTP Spezifizierung. In MSTP kann dieser Parameter jedoch zu den jeweiligen Ports von CIST und MSTI hinzugefügt werden.
- Hello Time:
1 / 2. Im Gegensatz zu RSTP kann die Hello Time für jeden einzelnen Port eines CIST eingestellt werden.

- Admin Edge:
Yes / No. Es gilt die selbe Definition wie in der RSTP Spezifizierung für CIST-Ports.
- Admin P2P:
Auto / True / False. Es gilt die selbe Definition wie in der RSTP Spezifizierung für CIST Ports.
- Restricted Role:
Yes / No. Wenn die Einstellung "Yes" ist, kann der Port nicht als Root-Port ausgewählt werden, auch wenn er den besten Spanning-Tree-Priority-Vector hat. Dieser Port wird als Ersatz-Port ausgewählt, nachdem der Root-Port bestimmt wurde. Die Voreinstellung dieses Ports ist "No". Wenn diese Einstellung gewählt ist, kann es zu einer Schwächung der Spanning-Tree-Verbindungsfähigkeit kommen. Diese Einstellung wird von einem Netzwerkadministrator vorgenommen, um zu verhindern, dass externe Bridges (über die der Administrator keine volle Kontrolle hat) die aktive Spanning-Tree-Topologie beeinflussen.
- Restricted TCN:
Yes / No. Wenn "Yes" eingestellt ist, leitet der Port empfangene Topologie-Änderungsmeldungen bzw. Topologie-Änderungen nicht an andere Ports weiter. Bei der Voreinstellung "No" kann es zu einem temporären Verlust der Verbindung kommen, nachdem es Änderungen in einer aktiven Spanning-Tree-Topologie gab, als Ergebnis einer dauerhaften, nicht korrekt gelernten Lokalisierung der Station. Diese Einstellung wird von einem Netzwerkadministrator vorgenommen, um zu verhindern, dass externe Bridges (über die der Administrator keine volle Kontrolle hat) in internen Bereichen Address-Flushing verursachen. Es kann auch der Fall sein, dass der Status der MAC-Operation für die zugehörigen LANs häufig wechselt.
- Mcheck:
Es gilt die selbe Definition wie in der RSTP Spezifizierung für CIST-Ports.
- MSTP State:
Die Einstellung des MSTP-Protokolls kann "enable" oder "disable" sein.
- Force Version:
Zeigt die aktuelle Version des konfigurierten Spanning-Tree-Protokolls.

- Bridge Max Age:
Zeigt die Einstellung des "Max Age" der Bridge.
- Bridge Forward Delay:
Zeigt die Einstellung der Sendeverzögerung der Bridge.
- Bridge Max Hops:
Zeigt die Einstellung der "Max Hops" der Bridge.
- Instance Priority:
Gibt die Priorität des Spanning-Trees für einer bestimmten Tree-Instanz an (CIST oder MSTI)
- Bridge Mac Address:
MAC-Adresse der Bridge.
- CIST ROOT PRIORITY:
Priorität des Spanning-Trees der CIST-Root-Bridge.
- CIST ROOT MAC:
Die MAC-Adresse der CIST-Root-Bridge.
- CIST EXTERNAL ROOT PATH COST:
Root-Pfadkosten aus Sicht des MST Bereiches der Bridge.
- CIST ROOT PORT ID:
Die Port-ID des Bridge-Root-Ports. In MSTP kann der Peer-Port eines Root-Port in dem selben oder in einem anderen MSTP-Bereich liegen. Ist letzteres der Fall, ist der Eigentümer des Root-Ports die CIST-Regional-Root-Bridge.
- CIST REGIONAL ROOT PRIORITY:
Zeigt die Priorität des Spanning-Tree der CIST-Regional-Root-Bridge an. Die CIST-Regional-Root-Bridge ist von der CIST-Root-Bridge zu unterscheiden. Eine Ausnahme ist vorhanden, wenn eine Bridge zu einem MST Bereich gehört und gleichzeitig die Root-Bridge des CST (Common Spanning Tree) ist. Ein MST Bereich im CST kann als gewöhnliche RSTP-Bridge angesehen werden. Das IST (Internal Spanning Tree) und MSTIs sind für andere Bridges außerhalb dieses Bereiches sichtbar.
- CIST REGIONAL ROOT MAC:
Die Mac-Adresse der CIST-Regional-Root-Bridge.

- CIST INTERNAL ROOT PATH COST:
Root-Pfadkosten aus Sicht der Bridges im IST.
- CIST CURRENT MAX AGE: Zeigt das aktuelle maximale Alter der CIST-Root-Bridge an.
- CIST CURRENT FORWARD DELAY:
Zeigt die aktuelle Sendeverzögerung der CIST-Root-Bridge an.
- TIME SINCE LAST TOPOLOGY CHANGE (SECS):
Gibt die Zeit in Sekunden an, die seit der letzten empfangenen Änderungsmeldung bzw. Änderung der Topologie vergangen ist. Wenn eine neue Änderung vorgenommen wird, setzt sich der Zähler zurück auf Null.
- TOPOLOGY CHANGE COUNT(SECS):
Gibt die Zeit in Sekunden für eine Spanning-Tree-Instanz an, die seit Beginn der Topologie-Änderung bis zum Ende der STP-Konvergenz vergangen ist. Wenn keine Änderung der Topologie vollzogen wird und keine Ankündigung für eine Topologieänderung empfangen wird, stellt sich der Zähler zurück auf Null.
- Port No:
1-24
- Status:
Für den Forwarding-Status gilt die selbe Definition wie in der RSTP Spezifikation. Mögliche Werte sind "Forwarding", "Learning", und "Discarding".
- Status:
Gibt die Rolle eines Ports in der Spanning-Tree-Topologie an. Mögliche Werte sind: "dsbl" (disable port), "alt" (alternate port), "bkup" (backup port), "ROOT" (root port), "DSGN" (designated port), "MSTR" (master port). Die letzten drei Werte sind mögliche Rollen für einen Port der in den Forwarding-Status übergeht.
- Path Cost:
Zeigt aktuelle Port-Pfadkosten für jeden Port in einem bestimmten Spanning-Tree-Instanz.
- Priority:
Zeigt die Port Priorität für jeden Port in einer bestimmten Spanning-Tree-Instanz.

- Hello:
Gibt die Hello-Time jedes Ports in der folgenden Form an: Aktuelle Hello Time/ Hello Time Einstellung.
- Oper. Edge:
Gibt an, ob ein Port (in der Realität) ein Edge-Port ist oder nicht.
- Oper. P2P:
Gibt an, ob ein Port (in der Realität) ein Point-to-Point-Port ist oder nicht.
- Restricted Role:
Hier gilt die selbe Definition wie in "Port Config".
- Restricted Tcn:
Hier gilt die selbe Definition wie in "Port Config".

4.16 Configuration: Multicast

Die Funktion IGMP Snooping dient zur Organisation von Multicast-Gruppen. IGMP Snooping sendet die Multicast-Pakete zu den Ports der VLAN-Gruppe. Durch IP-Multicast-Pakete im Netzwerk wird die Bandbreite nicht unnötig belastet. Das liegt daran, dass ein Switch, der kein IGMP oder IGMP-Snooping unterstützt, Multicast- und Broadcast-Pakete nicht unterscheiden kann. Ohne IGMP Snooping unterscheidet sich das Senden von Multicast-Paketen daher nicht vom Senden von Broadcast-Paketen.

Ein Switch unterstützt IGMP Snooping mit den folgenden Funktionen: Anfragen, Anmelden und Verlassen. Ein Paket-Typ, der zwischen einem IP-Multicast-Router bzw. einem Switch und einem IP-Multicast-Host ausgetauscht wird, kann die Informationen des Multicast-Table updaten, wenn ein Mitglied (Port) zu einer IP-Multicast-Zieladresse hinzukommt oder sie verlässt. Wenn der Switch ein IP-Multicast-Paket bekommt, kann er es mit dieser Funktion an die Mitglieder senden, die vorher in eine bestimmte IP-Multicast-Gruppe eingetreten sind. IGMP Snooping verwirft die Pakete, wenn der Benutzer Multicast-Pakete zu einer Multicast-Gruppe schickt, die nicht im Vorfeld erstellt wurde.

4.16.1 IGMP Mode



Wählen Sie hier die Betriebsart für die Verwendung von IGMP für Multicast.

■ Parameter

IGMP Mode

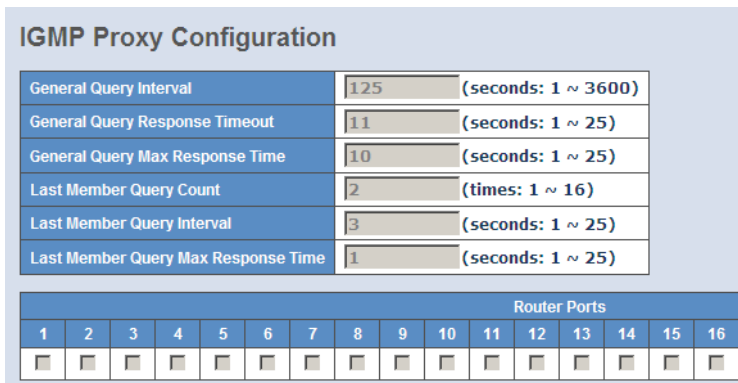
Disable: Deaktiviert die Verwendung von IGMP für Multicast.

Proxy: Aktiviert den IGMP-Proxy für die Verarbeitung der Multicast-Pakete.

Snooping: Aktiviert die IGMP-Snooping-Funktion für den Switch.

4.16.2 Proxy

Der IGMP Proxy kann IGMP-Nachrichten anstelle der Hosts beantworten, die an einem IGMP-Port angeschlossen sind. Schalten Sie den IGMP Proxy ein für einen Switch, der an einen Router näher an der Wurzel des Netzwerks angeschlossen ist. Der Router sollte dazu auch IGMP unterstützen.



IGMP Proxy Configuration	
General Query Interval	125 (seconds: 1 ~ 3600)
General Query Response Timeout	11 (seconds: 1 ~ 25)
General Query Max Response Time	10 (seconds: 1 ~ 25)
Last Member Query Count	2 (times: 1 ~ 16)
Last Member Query Interval	3 (seconds: 1 ~ 25)
Last Member Query Max Response Time	1 (seconds: 1 ~ 25)

Router Ports															
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

■ Parameter

General Query Interval:

Interval, in dem der IGMP Proxy Anfragen an die Hosts sendet (1 bis 3600 Sekunden).

- General Query Response Timeout :
Timeout für die Antworten auf die IGMP-Anfragen (1 bis 25 Sekunden).
- General Query Max Response Time :
Maximale Antwortzeit für allgemeine IGMP-Nachrichten (1 bis 25 Sekunden)
- Last Member Query Count :
Frequenz für die Anfragen an spezielle Mitglieder (1 bis 16 Sekunden)
- Last Member Query Interval :
Interval für die Anfragen an spezielle Mitglieder (1 bis 25 Sekunden)
- Last Member Query Max Response Time :
Maximale Antwortzeit für die Anfragen an spezielle Mitglieder (1 bis 25 Sekunden)
- Update Interval of Router Port :
Interval für die Updates auf den Router Ports (1 bis 3600 Sekunden)
- Router Ports:
Auswahl der Interfaces, die mit einem IGMP Router verbunden sind.
- Apply:
Sichern der Konfiguration.

4.16.3 Snooping

IGMP snooping Configuration

Host Time Out (seconds: 1 ~ 65535)

Fast Leave															
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Router Ports															
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Aktivieren Sie hier die Ports, auf denen IGMP Snooping aktiv sein soll.

- Parameter
 - Fast Leave: Diese Ports überwacht der Switch auf IGMP Nachrichten, mit denen die Hosts das Verlassen von Multicast-Gruppen melden.
 - Router Ports: Diese Ports überwacht der Switch auf IGMP Nachrichten von Routern.

4.16.4 IGMP Group Membership

Hier können Sie die aktuellen IGMP-Mitgliedschaften zu Multicastgruppen einsehen.

IGMP Group Membership			Port Members															
Index	Group Address	VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
			<div style="display: flex; justify-content: space-between; width: 100%;"> Previous Page Next Page Refresh </div>															

- Parameter
 - IGMP Group Membership:
Zeigt die aktuellen Mitgliedschaften der Ports an.
 - Previous Page:
Wechselt zur vorherigen Seite der Anzeige.
 - Next Page:
Wechselt zur nächsten Seite der Anzeige.
 - Refresh:
Aktualisiert die Anzeige.

4.17 Management: Alarm

4.17.1 Events

Trap Events Configuration

Email Select/Unselect All

Trap Select/Unselect All

Event	Email	Trap
Cold Start	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Warm Start	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Link Down	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Link Up	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Authentication Failure	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Login	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Logout	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Module Inserted	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Module Removed	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Dual Media Swapped	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Looping Detected	<input checked="" type="checkbox"/>	<input type="checkbox"/>
STP Disabled	<input checked="" type="checkbox"/>	<input type="checkbox"/>
STP Enabled	<input checked="" type="checkbox"/>	<input type="checkbox"/>

■ Events Konfiguration

Die Trap-Event-Konfiguration wird benutzt um den Switch zu veranlassen Trap-Informationen zu senden, wenn bestimmte Trap-Events auftreten. Sie haben die Möglichkeit zu definieren wie mit 22 verschiedenen Trap-Events umgegangen wird. Die Trap-Informationen über eine aufgetretene Trap können über drei verschiedene Wege an Sie gesendet werden: Per E-Mail, per Handy-SMS und als Trap an den SNMP-Manager. Die Nachricht wird entsprechend Ihrer Auswahl gesendet.

■ Parameter:

- Trap:
 - Cold Start, Warm Start, Link Down, Link Up, Authentication Failure (Authentifizierung gescheitert), User login (Benutzer angemeldet), User logout (Benutzer abgemeldet).
- STP:
 - STP Topology Changed (STP-Topologie geändert), STP Disabled (STP Ausgeschaltet), STP Enabled (STP Einschaltet).

- LACP:
LACP Disabled (LACP Ausgeschaltet), LACP Enabled (LACP Eingeschaltet), LACP Member Added (LACP Mitglied hinzugefügt), LACP Port Failure (LACP Port-Fehler).
- GVRP:
GVRP Disabled (GVRP Ausgeschaltet), GVRP Enabled (GVRP Eingeschaltet).
- VLAN:
Port-based VLAN Enabled (Port-basiertes VLAN aktiviert), Tag-based VLAN Enabled (auf Tags basierendes VLAN aktiviert).
- Module Swap:
Module Inserted (Modul eingesetzt), Module Removed (Modul entfernt), Dual Media Swapped (Dual Media Port getauscht).

4.17.2 Email

Alarm Configuration

Mail Server	<input type="text" value="10.1.1.1"/>
User Name	<input type="text"/>
Password	<input type="password" value="*****"/>
Sender	<input type="text"/>
Email Adress 1	<input type="text" value="mp@lancom.de"/>
Email Adress 2	<input type="text"/>
Email Adress 3	<input type="text"/>
Email Adress 4	<input type="text"/>
Email Adress 5	<input type="text"/>
Email Adress 6	<input type="text"/>

■ E-Mail/ SMS Konfiguration

In der Alarmkonfiguration können Sie festlegen, welche Personen über eine aufgetretene Trap per E-Mail, SMS oder beides informiert werden sollen. Sie können maximal 6 E-Mail-Adressen, sowie 6 Handy-Nummern angeben. Die 22 Trap-Events werden an den SNMP Manager gesendet, sollte eine Trap auftreten. Nach dem Auswählen der Trap-Events können Sie die gewünschten E-Mail-Adressen und Handy-Nummern eintragen. Klicken Sie anschließend <Apply>(Bestätigen) und die neuen Einstellungen werden in wenigen Sekunden übernommen.

Hinweis: SMS können eventuell nicht in ihrem Handysystem funktionieren.

■ Parameter:

E-Mail:

Mail Server: Die IP-Adresse des Servers, der ihre E-Mail überträgt.

Username: Ihr Benutzername auf dem Mail-Server.

Password: Ihr Passwort auf dem Mail-Server.

E-Mail Address 1 – 6: E-Mail-Adressen, die die Alarm-Nachricht erhalten sollen.

SMS:

SMS Server: Die IP-Adresse des Servers, der ihre SMS sendet.

Username: Ihr Benutzername bei Ihrem Internet-Service-Provider.

Password: Ihr Benutzerpasswort bei Ihrem Internet-Service-Provider.

Mobile Phone 1-6: Die Handy-Nummern, die die Alarm-Nachricht erhalten sollen.

4.18 Management: Diagnostics

Dieses Kapitel beschreibt die Funktionen zur Selbstdiagnose. Jede von ihnen wird im Folgenden der Reihe nach beschrieben.

4.18.1 Diag

Diagnostics

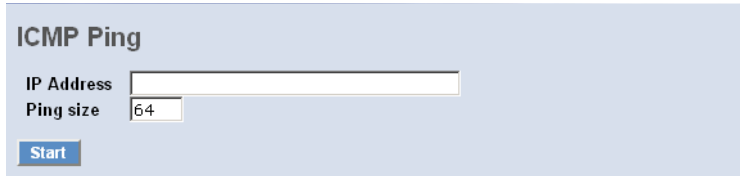
UART Test	OK
DRAM Test	OK
Flash Test	OK

Run

■ Diagnostics

Sie finden hier eine Reihe von grundsätzlichen Systemdiagnose-Werkzeugen. Die EEPROM-, UART-, DRAM- und Flash-Tests sollen Ihnen bei der Entscheidung helfen, ob ein System reparaturbedürftig ist oder nicht.

4.18.2 Ping



ICMP Ping

IP Address

Ping size

Start

■ Ping Test

Mit dem Ping-Test können Sie durch das ICMP-Protokoll feststellen ob ein Zielgerät aktiv ist oder nicht. Geben Sie einfach eine Ihnen bekannte IP-Adresse ein und klicken Sie den <Ping>-Button. Anschließend wird Ihnen das Resultat des Tests zeigen ob das Zielgerät erreichbar ist.

■ Parameter

- IP Address:
Eine IP-Adresse der Version IPv4, also z.B. 192.168.1.1.
- Default Gateway:
Die IP-Adresse des Default-Gateway.

4.19 Management: Maintenance

Dieses Kapitel beschreibt wie Sie das Gerät resetten können, wie Sie eine neue Firmware einspielen und welche Schlüssel-Parameter die System-Wartung verändern.

4.19.1 Reset device



Warm Restart

Are you sure you want to perform a Warm Restart?

Yes

Es gibt verschiedene Wege, das Gerät zurückzusetzen: Das Einschalten des Geräts, den Hardware-Reset und den Software-Reset. Sie können den RESET-Knopf an der Front-Blende drücken um den Switch zu resetten. Nach dem Upgraden der Software, dem Verändern der IP-Konfiguration oder dem Wech-

sel des VLAN-Modus muss der Switch neu gestartet werden um die neue Konfiguration umzusetzen. Im Folgenden wird der Software-Reset zum Rebooten aus dem Haupt-Menü beschrieben.

4.19.2 Firmware Upgrade

DE

The screenshot shows a web interface titled 'Firmware Upgrade'. Below the title is a search bar with the text 'Durchsuchen...' and a blue button labeled 'Upgrade'.

Diese Funktion hilft Ihnen ein Upgrade der Software durchzuführen, um eine Funktion zu reparieren oder zu verbessern. Der Switch stellt einen TFTP-Kliente zur Verfügung, um ein Upgrade der Software durchzuführen. Sie können dies mit Hilfe des Ethernet bewerkstelligen.

■ Software upload

Klicken Sie auf <Browse> um eine GS-Firmware auf dem PC zu wählen. Mit einem Klick auf <Upload> bestätigen sie das Einspielen der neuen Firmware. Die neue Firmware wird in den Switch hochgeladen werden und dann in den Flash-Speicher geschrieben. Sie müssen anschließend den Switch neu starten, um die neue Firmware aktiv werden zu lassen.

4.20 Management: SNMP

The screenshot shows a web interface titled 'SNMP Configuration'. At the top, there are radio buttons for 'Enable' (selected) and 'Disable'. Below this is a table for configuring SNMP traps and communities. The table has columns for 'Trap Host IP Address', 'Trap Host Port', 'Community', and 'Community'. The 'Community' column has a dropdown menu set to 'Disable'.

SNMP	<input checked="" type="radio"/> Enable <input type="radio"/> Disable			
Get Community	public			
Set Community	private	162	Community	Disable
Trap Host 1 IP Address	0.0.0.0	162	Community	public
Trap Host 2 IP Address	0.0.0.0	162	Community	public
Trap Host 3 IP Address	0.0.0.0	162	Community	public
Trap Host 4 IP Address	0.0.0.0	162	Community	public
Trap Host 5 IP Address	0.0.0.0	162	Community	public
Trap Host 6 IP Address	0.0.0.0	162	Community	public

At the bottom of the interface is an 'Apply' button.

Jedes Network-Management-System (NMS), das das Simple-Network-Management-Protocol (SNMP) beherrscht, kann die mit SNMP-Agenten ausgerüsteten Geräte, unter der Voraussetzung, dass auf den Geräten die Management-Information-Base (MIB) korrekt installiert ist, kontrollieren. Das

SNMP ist ein Protokoll um den Informationstransfer zwischen SNMP-Manager und SNMP-Agent zu kontrollieren und vermittelt die Object-Identity (OID) der Management-Information-Base (MIB) in der Form einer SMI-Syntax (Structure Management Information). Auf dem Switch läuft ein SNMP-Agent um auf die Anfragen eines SNMP-Managers zu reagieren.

Grundsätzlich bleibt der Agent passiv bis auf das Senden der Trap-Information. Der SNMP-Agent lässt sich auf dem Switch ein- und ausschalten. Wenn Sie den Schalter SNMP auf "Enable" stellen, wird der SNMP-Agent gestartet. Alle unterstützten MIB-OIDs, inklusive RNOM-MIB, sind dann für einen SNMP-Manager verfügbar. Wenn der Schalter auf "Disable" gestellt ist, wird der SNMP-Agent deaktiviert und der bzw. die damit verbundene Community-Name, Trap-Host, IP-Adresse sowie alle MIB-Zähler in Zukunft ignoriert.

■ SNMP Configuration

Hier können Sie Einstellungen am SNMP, Community-Namen, Trap-Host and Public-Traps sowie an der SNMP-Drossel vornehmen. Ein SNMP-Manager muss sich durch Angeben beider Community-Namen authentifizieren, um Zugriff auf die MIB-Informationen auf dem Zielgerät zu erhalten. Also müssen beide Parteien den selben Community-Namen erhalten. Sobald die Einstellungen vorgenommen sind, klicken Sie auf <Apply> um sie zu aktivieren.

■ Parameter:

SNMP:

Hier können Sie SNMP ein- bzw. ausschalten. In der Default-Einstellung ist SNMP eingeschaltet ("Enable").



Bitte beachten Sie, dass der LANmonitor keine Informationen über den LANCOM Switch anzeigen kann, wenn die SNMP-Unterstützung ausgeschaltet ist.

Get/Set/Trap Community:

Der Community-Name wird als Passwort genutzt um sicher zustellen, dass ein Network-Management-Unit derselben Community wie das Zielgerät angehört. Sollte es einen anderen Community-Namen haben, gehört es einer anderen Gruppe an, und kann deshalb nicht

auf das Zielgerät via SNMP zugreifen. Wenn beide den selben Community-Namen haben, können sie miteinander kommunizieren.

Den Community-Namen können Sie einstellen. Er darf maximal 15 beliebige Zeichen (aber ohne Leerzeichen) betragen und die Groß- und Kleinschreibung muss beachtet werden.

Den Community-Namen müssen Sie für jede Funktion einzeln festlegen. Er lässt sich nicht für mehrere Funktionen verwenden (d.h. der Community-Name für GET lässt sich nicht nochmal für SET vergeben).

Default SNMP function : Enable

Default community name for GET: public

Default community name for SET: private

Default community name for Trap: public

Default Set function : Disable

Default trap host IP address: 0.0.0.0

Default port number :162

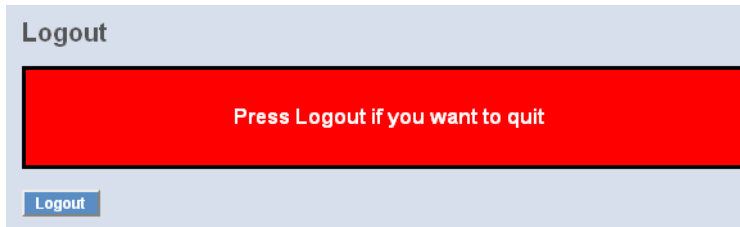
□ Trap:

Der Switch unterstützt bis zu 6 Trap-Hosts. Sie können jedem davon eine eigene IP-Adresse und einen eigenen Community-Namen zuweisen. Um einen Trap-Host aufzusetzen, müssen Sie einen Trap-Manager erstellen, indem Sie eine IP-Adresse als Host einer Trap-Message zuweisen. Der Trap-Host ist eine Network-Management-Unit des SNMP-Managers, welche die Trap-Message eines SNMP-Agenten empfängt. 6 Trap-Hosts können den Verlust einer wichtigen Trap-Message effektiv verhindern.

Für jede Public-Trap unterstützt der Switch die Trap-Events Cold Start, Warm Start, Link Down, Link Up und Authentication Failure Trap. Jedes dieser Events können Sie im Menü Alarm > Events individuell ein- und ausschalten. Wenn sie eingeschaltet sind, wird die jeweilige Trap aktiv eine Nachricht (Trap Message) an den Trap-Host schicken wenn sie auftritt. Sollten alle öffentlichen Traps ausgeschaltet sein, wird keine öffentliche Trap Message gesendet. Die Enterprise-Trap ist als Private-Trap klassifiziert, und ist daher im Kapitel über Trap Alarm Configuration erklärt.

Die Default Einstellung für alle Public-Traps ist "Enable".

4.21 Logout



Sie können sich mit der Logout-Funktion manuell abmelden. Sie können den Switch jedoch auch so einstellen, dass er Sie automatisch abmeldet.

■ Logout

Die Logout-Funktion verhindert, dass unbefugte Benutzer Zugriff auf das System haben. Wenn Sie sich nicht abmelden und den Browser verlassen, meldet der Switch Sie automatisch ab. Neben dem manuellen und impliziten Logout, können Sie den automatischen Logout ein- oder ausschalten. Der <Auto Logout> befindet sich auf der Bildschirmoberfläche rechts oben.

■ Parameter:

Auto Logout:

Wenn die Auto-Logout-Funktion eingeschaltet ist ("ON") und es findet über einen Zeitraum von drei Minuten weder eine Tastenbetätigung, noch eine Bildschirmbewegung statt, wird der Switch Sie automatisch abmelden. Default ist ON.

5 Operation of CLI Management (english)

5.1 CLI Management

Refer to Chapter 2 for basic installation. The following description is the brief of the network connection.

- Locate the correct DB-9 null modem cable with female DB-9 connector. Null modem cable comes with the management switch. Refer to the Appendix B for null modem cable configuration.
- Attach the DB-9 female connector to the male DB-9 serial port connector on the Management board.
- Attach the other end of the DB-9 cable to an ASCII terminal emulator or PC Com-1, 2 port. For example, PC runs Microsoft Windows HyperTerminal utility.
- At "Com Port Properties" Menu, configure the parameters as below: (see the next section)

Baud rate	115200
Stop bits	1
Data bits	8
Parity	N
Flow control	none

5.1.1 Login

The command-line interface (CLI) is a text-based interface. User can access the CLI through either a direct serial connection to the device or a Telnet session. The default values of the managed switch are listed below:

Username: admin

Password: admin

After you login successfully, the prompt will be shown as "#" if you are the first login person and your authorization is administrator; otherwise it may show "\$". See the following two figures. The former means you behave as an administrator and have the access right of the system. As to the latter, it means you behave as a guest and are only allowed to view the system without the permission to do any setting for this switch.

5.2 Commands of CLI

```

Telnet 10.98.1.61
Managed Switch - LANCOM GS-2124
Login: guest
Password: *****
LANCOM GS-2124$ ?
 802.1X          Enter into 802.1X mode
 account        Enter into account mode
 acl            Enter into acl mode
 alarm         Enter into alarm mode
 autologout     Change autologout time
 config-file    Enter into config file mode
 dhcp_snooping Enter into dhcp snooping mode
 diagnostics    Enter into diagnostics mode
 gvrp          Enter into gvrp mode
 ip            Enter into ip mode
 ip_mac_binding Enter into ip mac binding mode
 loop-detection Enter into Loop Detection(LD) mode
 mac           Enter into mac mode
 mirror        Enter into mirror mode
 mstp          Enter into mstp mode
 multicast     Enter into multicast mode
 policy        Enter into Management Policy mode
 port          Enter into port mode
 qos           Enter into qos mode
 snmp          Enter into snmp mode
 stp           Enter into stp mode
 system        Enter into system mode
 time          Enter into time mode
 traplog       Enter into trap log mode
 ..(q to quit)

 trunk          Enter into trunk mode
 vlan           Enter into vlan mode
 vs             Enter into virtual stack mode

```

5.2.1 Global Commands of CLI

■ end

□ Syntax:

end

□ Description:

Back to the top mode.

When you enter this command, your current position would move to the top mode. If you use this command in the top mode, you are still in the position of the top mode.

□ Argument:

None.

□ Possible value:

None.

□ Example:

GS-2124L# alarm

```
GS-2124L(alarm)# events
GS-2124L(alarm-events)# end
GS-2124L#
```

■ **exit**

Syntax:
exit

Description:
Back to the previous mode.

When you enter this command, your current position would move back to the previous mode. If you use this command in the top mode, you are still in the position of the top mode.

Argument:
None.

Possible value:
None.

Example:
GS-2124L# trunk
GS-2124L(trunk)# exit
GS-2124L#

■ **help**

Syntax:
help

Description:
To show available commands.

Some commands are the combination of more than two words. When you enter this command, the CLI would show the complete commands. Besides, the command would help you classify the commands between the local commands and the global ones.

Argument:
None.

Possible value:
None.

Example:

```
GS-2124L# ip
```

```
GS-2124L(ip)# help
```

```
Commands available:
```

```
-----<< Local commands >>-----
```

```
set ip          Set ip,subnet mask and gateway
```

```
set dns        Set dns
```

```
enable dhcp    Enable DHCP, and set dns auto or manual
```

```
disable dhcp   Disable DHCP
```

```
show          Show IP Configuration
```

```
-----<< Global commands >>-----
```

```
exit          Back to the previous mode
```

```
end           Back to the top mode
```

```
help         Show available commands
```

```
history      Show a list of previously run commands
```

```
logout       Logout the system
```

```
save start   Save as start config
```

```
save user    Save as user config
```

```
restore default Restore default config
```

```
restore user Restore user config
```

■ history

□ Syntax:

```
history [#]
```

□ Description:

To show a list of previous commands that you had ever run.

When you enter this command, the CLI would show a list of commands which you had typed before. The CLI supports up to 256 records. If no argument is typed, the CLI would list total records up to 256. If optional argument is given, the CLI would only show the last numbers of records, given by the argument.

□ Argument:

[#]: show last number of history records. (optional)

■ Kapitel 5: Operation of CLI Management (englisch)

- Possible value:

[#]: 1, 2, 3, ..., 256

- Example:

GS-2124L(ip)# history

Command history:

0. trunk
1. exit
2. GS-2124L# trunk
3. GS-2124L(trunk)# exit
4. GS-2124L#
5. ?
6. trunk
7. exit
8. alarm
9. events
10. end
11. ip
12. help
13. ip
14. history

GS-2124L(ip)# history 3

Command history:

13. ip
14. history
15. history 3

GS-2124L(ip)#

■ **logout**

- Syntax:

logout

- Description:

When you enter this command via Telnet connection, you would logout the system and disconnect. If you connect the system through direct serial port with RS-232 cable, you would logout the system and be back to the initial login prompt when you run this command.

Argument:

None.

Possible value:

None.

Example:

GS-2124L# logout

■ restore default

Syntax:

restore default

Description:

When you use this function in CLI, the system will show you the information "Do you want to restore the default IP address?(y/n)". If you choose Y or y, the IP address will restore to default "192.168.1.1". If you choose N or n, the IP address will keep the same one that you had saved before.

If restoring default successfully, the CLI would prompt if reboot immediately or not. If you press Y or y, the system would reboot immediately; otherwise, it would be back to the CLI system. After restoring default configuration, all the changes in the startup configuration would be lost. After rebooting, the entire startup configuration would reset to factory default.

Argument:

None.

Possible value:

None.

Example:

GS-2124L# restore default

Restoring ...

Restore Default Configuration Successfully

Press any key to reboot system.

■ **restore user**

□ Syntax:

restore user

□ Description:

To restore the startup configuration as user defined configuration. If restoring default successfully, the CLI would prompt if reboot immediately or not. If you press Y or y, the system would reboot immediately; others would back to the CLI system. After restoring user-defined configuration, all the changes in the startup configuration would be lost. After rebooting, the entire startup configuration would replace as user defined one.

□ Argument:

None.

□ Possible value:

None.

□ Example:

```
GS-2124L# restore user
```

```
Restoring ...
```

```
Restore User Configuration Successfully
```

```
Press any key to reboot system.
```

■ **save start**

□ Syntax:

save start

□ Description:

To save the current configuration as the start one. When you enter this command, the CLI would save your current configuration into the non-volatile FLASH. If you want the configuration still works after rebooting, save the configuration using the command 'save stat'.

□ Argument:

None.

□ Possible value:

None.

□ Example:

```
GS-2124L# save start
```

Saving start...

Save Successfully

GS-2124L#

■ **save user**

□ Syntax:

save user

□ Description:

To save the current configuration as the user-defined configuration. When you enter this command, the CLI would save your current configuration into the non-volatile FLASH as user-defined configuration.

□ Argument:

None.

□ Possible value:

None.

□ Example:

GS-2124L# save user

Saving user...

Save Successfully

GS-2124L#

5.2.2 4-2-2. Local Commands of CLI

802.1X

■ **set maxReq**

□ Syntax:

set maxReq <port-range> <vlaue>

□ Description:

The maximum number of times that the state machine will retransmit an EAP Request packet to the Supplicant before it times out the authentication session.

□ Argument:

<port range> : syntax 1,5-7, available from 1 to 24

<value>: max-times , range 1-10

■ Kapitel 5: Operation of CLI Management (english)

- Possible value:
 <port range> : 1 to 24
 <value>: 1-10, default is 2

□ Example:
 GS-2124L(802.1X)# set maxReq 2 2

■ set mode

□ Syntax:
 set mode <port-range> <mode>

□ Description:
 To set up the 802.1X authentication mode of each port.

□ Argument:
 <port range> : syntax 1,5-7, available from 1 to 24
 <mode>: set up 802.1X mode
 0:disable the 802.1X function
 1:set 802.1X to Multi-host mode

□ Possible value:
 <port range> : 1 to 24
 <mode>: 0 or 1

□ Example:
 GS-2124L(802.1X)# set mode 2 1
 GS-2124L(802.1X)#

■ set port-control

□ Syntax:
 set port-control <port-range> <unauthorized| authorized| auto>

□ Description:
 To set up 802.1X status of each port.

□ Argument:
 <port range> : syntax 1,5-7, available from 1 to 24
 <authorized> : Set up the status of each port
 0:ForceUnauthorized
 1:ForceAuthorized

2:Auto

□ Possible value:

<port range> : 1 to 24

<authorized> : 0, 1 or 2

□ Example:

GS-2124L(802.1X)# set port-control 2 2

■ set quietPeriod

□ Syntax:

set quietPeriod <port-range> <value>

□ Description:

A timer used by the Authenticator state machine to define periods of time during when it will not attempt to acquire a Supplicant.

□ Argument:

<port range> : syntax 1,5-7, available from 1 to 24

<value> : timer , range 0-65535

□ Possible value:

<port range> : 1 to 24

<value> : 0-65535, default is 60

□ Example:

GS-2124L(802.1X)# set quietPeriod 2 30

■ set reAuthEnabled

□ Syntax:

set reAuthEnabled <port-range> <on | off >

□ Description:

A constant that define whether regular reauthentication will take place on this port.

□ Argument:

<port range> : syntax 1,5-7, available from 1 to 24

<on | off > :

0:OFF Disable reauthentication

1:ON Enable reauthentication

□ Possible value:

<port range> : 1 to 24

< on | off |> : 0 or 1, default is 1

□ Example:

```
GS-2124L(802.1X)# set reAuthEnabled 2 1
```

■ set reAuthMax

□ Syntax:

```
set reAuthMax <port-range> <value>
```

□ Description:

The number of reauthentication attempts that are permitted before the port becomes Unauthorized.

□ Argument:

<port range> : syntax 1,5-7, available from 1 to 24

<value> : max. value , range 1-10

□ Possible value:

<port range> : 1 to 24

<value> : 1-10, default is 2

□ Example:

```
GS-2124L(802.1X)# set reAuthMax 2 2
```

■ set reAuthPeriod

□ Syntax:

```
set reAuthPeriod <port-range> <value>
```

□ Description:

A constant that defines a nonzero number of seconds between periodic reauthentication of the supplicant.

□ Argument:

<port range> : syntax 1,5-7, available from 1 to 24

<value> : timer , range 1-65535

□ Possible value:

<port range> : 1 to 24

<value> : 1-65535, default is 3600

□ Example:

```
GS-2124L(802.1X)# set reAuthPeriod 2 3600
```

■ set serverTimeout

□ Syntax:

set serverTimeout <port-range> <value>

□ Description:

A timer used by the Backend Authentication state machine in order to determine timeout conditions in the exchanges between the Authenticator and the Supplicant or Authentication Server. The initial value of this timer is either suppTimeout or serverTimeout, as determined by the operation of the Backend Authentication state machine.

□ Argument:

<port range> : syntax 1,5-7, available from 1 to 24

<value> : timer , range 1-65535

□ Possible value:

<port range> : 1 to 24

<value> : 1-65535, default is 30

□ Example:

```
GS-2124L(802.1X)# set serverTimeout 2 30
```

■ set auth-server

□ Syntax:

set auth-server <ip-address> <udp-port> <secret-key>

□ Description:

To configure the settings related with 802.1X Radius Server.

□ Argument:

<ip-address> : the IP address of Radius Server

<udp-port> : the service port of Radius Server(Authorization port)

<secret-key> : set up the value of secret-key, and the length of secret-key is

from 1 to 31

□ Possible value:

<udp-port > : 1~65535, default is 1812

□ Example:

```
GS-2124L(802.1X)# set auth-server 192.168.1.115 1812 WinRadius
```

■ **set suppTimeout**

□ Syntax:

set suppTimeout <port-range> <value>

□ Description:

A timer used by the Backend Authentication state machine in order to determine timeout conditions in the exchanges between the Authenticator and the Supplicant or Authentication Server. The initial value of this timer is either suppTimeout or serverTimeout, as determined by the operation of the Backend Authentication state machine.

□ Argument:

<port range> : syntax 1,5-7, available from 1 to 24

<value> : timer , range 1-65535

□ Possible value:

<port range> : 1 to 24

<value> : 1-65535, default is 30

□ Example:

```
GS-2124L(802.1X)# set suppTimeout 2 30
```

■ **set txPeriod**

□ Syntax:

set txPeriod <port-range> <value>

□ Description:

A timer used by the Authenticator PAE state machine to determine when an EAPOL PDU is to be transmitted

□ Argument:

<port range> : syntax 1,5-7, available from 1 to 24

<value> : timer , range 1-65535

□ Possible value:

<port range> : 1 to 24

<value> : 1-65535, default is 30

□ Example:

```
GS-2124L(802.1X)# set txPeriod 2 30
```

■ **show status**

□ Syntax:

show status

- Description:

To display the mode of each port.

- Argument:

None

- Possible value:

None

- Example:

GS-2124L(802.1X)# show status

```
Port   Mode
```

```
=====
```

```
1  Disable
2  Multi-host
3  Disable
4  Disable
5  Disable
6  Disable
```

■ show port-config

- Syntax:

show port-config <port-range>

- Description:

To display the parameter settings of each port.

- Argument:

<port range> : syntax 1,5-7, available from 1 to 24

- Possible value:

<port range> : 1 to 24

- Example:

GS-2124L(802.1X)# show port-config 1, 2

```
port 1) Mode      : Disabled
```

```
port control : Auto
```


■ Kapitel 5: Operation of CLI Management (englisch)

```

reAuthMax    : 2
txPeriod     : 30
Quiet Period : 60
reAuthEnabled : ON
reAuthPeriod : 120
max. Request : 2
suppTimeout  : 30
serverTimeout : 30

```

port 2) Mode : Disabled

port control : Auto

```

reAuthMax    : 2
txPeriod     : 30
Quiet Period : 60
reAuthEnabled : ON
reAuthPeriod : 120
max. Request : 2
suppTimeout  : 30
serverTimeout : 30

```

■ show statistics

□ Syntax:

```
show statistics <#>
```

□ Description:

To display the statistics of each port.

□ Argument:

<#> syntax 1,5-7, available from 1 to 24

□ Possible value:

<#> 1 to 24

:

■ show server

□ Syntax:

show server

□ Description:

Show the Radius server configuration

□ Argument:

None

□ Possible value:

None

□ Example:

GS-2124L(802.1X)# show server

Authentication Server

IP Address: 192.168.1.1

UDP Port : 1812

Secret Key : Radius

Accounting Server

IP Address: 192.168.1.1

UDP Port : 1812

Secret Key : Radius

° account

■ add

□ Syntax:

add <name>

□ Description:

To create a new guest user. When you create a new guest user, you must type in password and confirm password.

□ Argument:

<name> : new account name

□ Possible value:

A string must be at least 5 character.

□ Example:

```
GS-2124L(account)# add aaaaa
```

```
Password:
```

```
Confirm Password:
```

```
GS-2124L(account)#
```

■ del

Syntax:

```
del <name>
```

Description:

To delete an existing account.

Argument:

<name> : existing user account

Possible value:

None.

Example:

```
GS-2124L(account)# del aaaaa
```

```
Account aaaaa deleted
```

■ modify

Syntax:

```
modify <username>
```

Description:

To change the username and password of an existing account.

Argument:

<name> : existing user account

Possible value:

None.

Example:

```
GS-2124L(account)# modify aaaaa
```

```
username/password: the length is from 5 to 15.
```

```
Current username (aaaaa):bbbb
```

```
New password:
```

```
Confirm password:
```

Username changed successfully.

Password changed successfully.

■ show

□ Syntax:

show

□ Description:

To show system account, including account name and identity.

□ Argument:

None.

□ Possible value:

None.

□ Example:

GS-2124L(account)# show

Account Name	Identity

admin	Administrator
guest	guest

° acl

■ ace

□ Syntax:

ace <index>

□ Description:

To display the ace configuration.

□ Argument:

<index> : the access control rule index value

□ Possible value:

None.

□ Example:

GS-2124L(acl)# ace 2

index: 2

rule: switch

vid: any
 tag_prio: any
 dmac: any
 frame type: arp
 arp type: Request/Reply (opcode): any
 source ip: any
 destination ip: any
 ARP flag
 ARP SMAC Match: any
 RARP DMAC Match: any
 IP/Ethernet Length: any
 IP: any
 Ethernet: any
 action: 1
 rate limiter: 0
 copy port: 0

■ **action**

□ Syntax:

action <port> <permit|deny> <rate_limiter> <port copy>

□ Description:

To set the access control per port as packet filter action rule.

□ Argument:

<port> : 1-24

<permit/deny>: permit: 1, deny: 0

<rate_limiter>: 0-16 (0:disable)

<port copy> : 0-24 (0:disable)

□ Possible value:

<port> : 1-24

<permit/deny>: 0-1

<rate_limiter>: 0-16

<port copy> : 0-24

- Example:

```
GS-2124L(ac1)# action 5 0 2 2
```

```
GS-2124L(ac1)# show
```

```
port policy id action rate limiter port copy counter a class map
```

```
.. .. i-i- i- i- ..
5 1 deny 2 2
23 1 permit 0 0 0
24 1 permit 0 0 0
rate limiter rate(pps)
```

```
-----
1 1
2 1
3 1
4 1
5 1
```

```
i-i- i-i-
GS-2124L(ac1)#
```

■ delete

- Syntax:

```
delete <index>
```

- Description:

To delete the ACE (Access Control Entry) configuration on the switch.

- Argument:

<index> : the access control rule index value

- Possible value:

None.

- Example:

```
GS-2124L(ac1)# delete 1
```

```
GS-2124L(ac1)#
```

■ **move**

- Syntax:

move <index1> <index2>

- Description:

To move the ACE (Access Control Entry) configuration between index1 and index2..

- Argument:

None.

- Possible value:

None.

- Example:

FGS-2924(account)# move 1 2

■ **policy**

- Syntax:

policy <policy> <ports>

- Description:

To set acl port policy on switch

- Argument:

<policy> : 1-8

<ports> : 1-24

- Possible value:

<policy> : 1-8

<ports> : 1-24

- Example:

GS-2124L(acl)# policy 3 10

GS-2124L(acl)#

■ **ratelimiter**

- Syntax:

ratelimiter <id> <rate>

- Description:

To set access control rule with rate limiter on switch

□ Argument:

<id> : 1-16

<rate> : 1,2,4,8,16,32,64,128,256,512,1000,2000, 4000,8000,
16000,32000,64000,128000,256000,512000,1024000

□ Possible value:

<id> : 1-16

<rate> : 1,2,4,8,16,32,64,128,256,512,1000,2000, 4000,8000,
16000,32000,64000,128000,256000,512000,1024000

□ Example:

GS-2124L(acl)# ratelimiter 3 16000

GS-2124L(acl)#

■ set

□ Syntax:

set [<index>] [<next index>]

[switch | (port <port>) | (policy <policy>)]

[<vid>] [<tag_prio>] [<dmac_type>]

[(any) |

(etype [<etype>] [<smac>]) |

(arp [<arp type>] [<opcode>]

(any | [<source ip>] [<source ip mask>])

(any | [<destination ip>] [<destination ip mask>])

[<source mac>] [<arp smac match flag>]

[<raro dmac match flag>] [<ip/ethernet length flag>]

[<ip flag>] [<ethernet flag>]) |

(ip [(<source ip> <source ip mask>) | any]

[(<destination ip> <destination ip mask>) | any]

[<ip ttl>] [<ip fragment>] [<ip option>]

[(icmp <icmp type> <icmp code>) |

(udp <source port range> <destination port range>) |

(tcp <source port range> <destination port range>


```

    <tcp fin flag> <tcp syn flag> <tcp rst flag>
    <tcp psh flag> <tcp ack flag> <tcp urg flag> |
    (other <ip protocol value>) |
    (any)]
]
[<action>] [<rate limiter>] [<port copy>]

```

□ Description:

To set access control entry on switch

□ Argument:

□ Possible value:

□ Example:

■ **show**

□ Syntax:

show

□ Description:

To show all access control entry setting on switch

□ Argument:

none

□ Possible value:

none

□ Example:

GS-2124L(acl)# show

```
port policy id action rate limiter port copy counter a class map
```

```
.. .. i-i- i- i- ..
```

```
5 1 deny 2 2
```

```
23 1 permit 0 0 0
```

```
24 1 permit 0 0 0
```

```
rate limiter rate(pps)
```

```

-----
      1      1
      2      1
      3      1
      4      1
      5      1

      i-i-    i-i-
GS-2124L(ac)#

```

° alarm

```
<<email>>
```

■ del mail-address

Syntax:

```
del mail-address <#>
```

Description:

To remove the configuration of E-mail address.

Argument:

<#>: email address number, range: 1 to 6

Possible value:

<#>: 1 to 6

Example:

```
GS-2124L(alarm-email)# del mail-address 2
```

■ del server-user

Syntax:

```
del server-user
```

Description:

To remove the configuration of server, user account and password.

Argument:

None.

Possible value:

None.

- Example:

```
GS-2124L(alarm-email)# del server-user
```

■ set mail-address

- Syntax:

```
set mail-address <#> <mail address>
```

- Description:

To set up the email address.

- Argument:

<#>:email address number, range: 1 to 6

<mail address>:email address

- Possible value:

<#>: 1 to 6

- Example:

```
GS-2124L(alarm-email)# set mail-address 1 abc@mail.abc.com
```

■ set server

- Syntax:

```
set server <ip>
```

- Description:

To set up the IP address of the email server.

- Argument:

<ip>:email server ip address or domain name

- Possible value:

None.

- Example:

```
GS-2124L(alarm-email)# set server 192.168.1.6
```

■ set user

- Syntax:

```
set user <username>
```

- Description:

To set up the account and password of the email server.

- Argument:

<username>: email server account and password

- Possible value:

None.

- Example:

GS-2124L (alarm-email)# set user admin

■ show

- Syntax:

show

- Description:

To display the configuration of e-mail.

- Argument:

None.

- Possible value:

None.

- Example:

GS-2124L(alarm-email)# show

Mail Server : 192.168.1.6

Username : admin

Password : *****

Email Address 1: abc@mail.abc.com

Email Address 2:

Email Address 3:

Email Address 4:

Email Address 5:

Email Address 6:

<<events>>

■ del all

- Syntax:

del all <range>

- Description:

To disable email, sms and trap of events.

- Argument:

<range>:del the range of events, syntax 1,5-7

□ Possible value:

<range>: 1~24

□ Example:

GS-2124L(alarm-events)# del all 1-3

■ del email

□ Syntax:

del email <range>

□ Description:

To disable the email of the events.

□ Argument:

<range>:del the range of email, syntax 1,5-7

□ Possible value:

<range>: 1~24

□ Example:

GS-2124L(alarm-events)# del email 1-3

■ del trap

□ Syntax:

del trap <range>

□ Description:

To disable the trap of the events.

□ Argument:

<range>:del the range of trap, syntax 1,5-7

□ Possible value:

<range>: 1~24

□ Example:

GS-2124L(alarm-events)# del trap 1-3

■ set all

□ Syntax:

set all <range>

□ Description:

To enable email, sms and trap of events.

- Argument:
<range>: set the range of events, syntax 1,5-7

- Possible value:
<range>: 1~24

- Example:
GS-2124L(alarm-events)# set all 1-3

■ set email

- Syntax:
set email <range>

- Description:
To enable the email of the events.

- Argument:
<range>: set the range of email, syntax 1,5-7

- Possible value:
<range>: 1~24

- Example:
GS-2124L(alarm-events)# set email 1-3

■ set trap

- Syntax:
set trap <range>

- Description:
To enable the trap of the events.

- Argument:
<range>: set the range of trap, syntax 1,5-7

- Possible value:
<range>: 1~24

- Example:
GS-2124L(alarm-events)# set trap 1-3

■ show

- Syntax:
show

- Description:

To display the configuration of alarm event.

□ Argument:

None.

□ Possible value:

None.

□ Example:

GS-2124L(alarm-events)# show

Events	Email SMS Trap

1 Cold Start	v
2 Warm Start	v
3 Link Down	v
4 Link Up	v
5 Authentication Failure	v
6 Login	
7 Logout	
8 Module Inserted	
9 Module Removed	
10 Dual Media Swapped	
11 Looping Detected	
12 STP Disabled	
13 STP Enabled	
14 STP Topology Changed	
15 LACP Disabled	
16 LACP Enabled	
17 LACP Member Added	
18 LACP Aggregates Port Failure	
19 GVRP Disabled	
20 GVRP Enabled	
21 VLAN Disabled	

- 22 Port-based Vlan Enabled
- 23 Tag-based Vlan Enabled
- 24 IP MAC Binding Enabled
- 25 IP MAC Binding Disabled
- 26 IP MAC Binding Client Authenticate error
- 27 IP MAC Binding Server Authenticate error

■ show (alarm)

- Syntax:

show

- Description:

The Show for alarm here is used to display the configuration of Events, or E-mail.

- Argument:

None.

- Possible value:

None.

- Example:

GS-2124L(alarm)# show events

GS-2124L(alarm)# show email

° autologout

autologout

- Syntax:

autologout <time>

- Description:

To set up the timer of autologout.

- Argument:

<time>: range 1 to 3600 seconds, 0 for autologout off, current setting is 180 seconds.

- Possible value:

<time>: 0,1-3600

- Example:


```
GS-2124L# autologout 3600
Set autologout time to 3600 seconds
```

° config-file

■ export

- Syntax:

```
export <current | user> < ip address>
```

- Description:

[To run the](#) export function.

- Argument:

< Usage> set up current or user

< ip address> the TFTP server ip address

- Possible value:

none

- Example:

```
GS-2124L(config-file)# export current 192.168.1.63
```

Export successful_.

■ import

- Syntax:

```
import <current | user> < ip address>
```

- Description:

To run the [im](#)port start function.

- Argument:

None

- Possible value:

None

- Example:

```
GS-2124L(config-file)# import current 192.168.1.63
```

Import successful_.

° firmware

■ Upgrade

- Syntax:

upgrade <ip_address> <file_path>

□ Description:

To set up the image file that will be upgraded.

□ Argument:

< ip address> : TFTP server ip address

<filepath>: upgrade file path

□ Possible value:

< ip address> : TFTP server ip address

<filepath>: upgrade file path

□ Example:

```
GS-2124L(firmware)# upgrade 192.168.2.4 fgs2924R_GS-2124L_v2.03.img
```

° gvrp

■ set state

□ Syntax:

set state < 0 | 1>

□ Description:

To disable/ enable the gvrp function.

□ Argument:

0 : disable the gvrp function

1 : enable the gvrp function

□ Possible value:

0 : disable the gvrp function

1 : enable the gvrp function

□ Example:

```
GS-2124L(gvrp)# set state 1
```

■ group applicant

□ Syntax:

group applicant <vid> <port> < 0 | 1>

□ Description:

To enter any of gvrp group for changing gvrp group setting. You can change the applicant or registrar mode of existing gvrp group per port.

■ Kapitel 5: Operation of CLI Management (englisch)

- Argument:

<vid>: enter which gvrp group you had created, using value is vid.
Available range: 1 to 4094

<port>: 1 to 24

< 0 | 1 > :

- Possible value:

<vid>: 1~4094

<port>: 1 to 24

- Example:

```
GS-2124L(gvrp)# group applicant 2 5 0
```

GVRP group information

Current Dynamic Group Number: 1

VID	Member	Port
2	5	

2 5

■ set applicant

- Syntax:

```
set applicant <port> < 0 | 1 >
```

- Description:

To set default applicant mode for each port.

- Argument:

<port>: port range, syntax 1,5-7, available from 1 to 24

<0>: set applicant as normal mode

<1>: set applicant as non-participant mode

- Possible value:

<port>: 1 to 24

< 0 | 1 >: normal or non-participant

- Example:

```
GS-2124L(gvrp)# set applicant 1-10 non-participant
```

■ set registrar

- Syntax:

```
set registrar <port> < 0 | 1 | 2 >
```

□ Description:

To set default registrar mode for each port.

□ Argument:

<port>: port range, syntax 1,5-7, available from 1 to 24

<0>: set registrar as normal mode

<1>: set registrar as fixed mode

<2>: set registrar as forbidden mode

□ Possible value:

<range>: 1 to 24

< 0 | 1 | 2>: normal or fixed or forbidden

□ Example:

```
GS-2124L(gvrp)# set registrar 1-5 fixed
```

■ **set restricted**

□ Syntax:

```
set restricted <port> <0 | 1 | 2>
```

□ Description:

To set the restricted mode for each port.

□ Argument:

<port>: port range, syntax 1,5-7, available from 1 to 24

<0>: set restricted normal

<1>: set restricted fixed

<2>: set restricted forbidden

□ Possible value:

<port>: 1 to 24

< 0 | 1 | 2>: normal, fixed or forbidden

□ Example:

```
GS-2124L(gvrp)# set restricted 1-10 1
```

```
GS-2124L(gvrp)# show config
```

```
GVRP state: Enable
```

```
Port Join Time Leave Time LeaveAll Time Applicant Registrar Restricted
```

```

-----
-
1  20  60  1000  Normal  Normal  Enable
2  20  60  1000  Normal  Normal  Enable
3  20  60  1000  Normal  Normal  Enable
4  20  60  1000  Normal  Normal  Enable
5  20  60  1000  Normal  Normal  Enable
6  20  60  1000  Normal  Normal  Enable
7  20  60  1000  Normal  Normal  Enable
8  20  60  1000  Normal  Normal  Enable
9  20  60  1000  Normal  Normal  Enable
10 20  60  1000  Normal  Normal  Enable
      :
      :
      :
22 20  60  1000  Normal  Normal  Disable
23 20  60  1000  Normal  Normal  Disable
24 20  60  1000  Normal  Normal  Disable

```

■ **set timer**

□ Syntax:

```
set timer <port> <JoinTime> <leaveTime> <leaveAllTime>
```

□ Description:

To set gvrp join time, leave time, and leaveall time for each port.

□ Argument:

<port> : port range, syntax 1,5-7, available from 1 to 24

<JoinTime>: join timer, available from 20 to 100

<LeaveTime>: leave timer, available from 60 to 300

<LeaveAllTime>: leaveall timer, available from 1000 to 5000

Leave Time must equal double Join Time at least.

□ Possible value:

<port> : 1 to 24

<JoinTime>: 20 to 100
 <LeaveTime>: 60 to 300
 <LeaveAllTime>: 1000 to 5000

□ Example:

```
GS-2124L(gvrp)# set timer 2-8 25 80 2000
```

■ show

□ Syntax:

```
show
```

□ Description:

To display the gvrp configuration.

□ Argument:

None

□ Possible value:

None

□ Example:

```
GS-2124L(gvrp)# show
```

```
GVRP state: Enable
```

```
Port Join Time Leave Time LeaveAll Time Applicant Registrar Restricted
```

```
-----
```

```

1  20   60   1000  Normal   Normal   Disable
2  25   80   2000  Normal   Normal   Disable
3  25   80   2000  Normal   Normal   Disable
4  25   80   2000  Normal   Normal   Disable
5  25   80   2000  Normal   Normal   Disable
6  25   80   2000  Normal   Normal   Disable
7  25   80   2000  Normal   Normal   Disable
8  25   80   2000  Normal   Normal   Disable
   :
   :
23 20   60   1000  Normal   Normal   Disable
```

24 20 60 1000 Normal Normal Disable

■ counter

□ Syntax:

counter <port>

□ Description:

To display the counter number of the port.

□ Argument:

<port>: port number

□ Possible value:

<port>: available from 1 to 24

□ Example:

GS-2124L(gvrp)# counter 2

Received

Total GVRP Packets : 0

Invalid GVRP Packets : 0

LeaveAll message : 0

JoinEmpty message : 0

JoinIn message : 0

LeaveEmpty message : 0

Empty message : 0

Transmitted

Total GVRP Packets : 0

Invalid GVRP Packets : 0

LeaveAll message : 0

JoinEmpty message : 0

JoinIn message : 0

LeaveEmpty message : 0

Empty message : 0

■ group grpinfo

□ Syntax:

group grpinfo <vid>

- Description:

To show the gvrp group.

- Argument:

<vid>: To set the vlan id from 1 to 4094

- Possible value:

<vid>: 1 to 4094

- Example:

```
GS-2124L(gvrp)# group grpinfo 2
```

```
GVRP group information
```

```
VID Member Port
```

° hostname

■ hostname

- Syntax:

```
hostname <name>
```

- Description:

To set up the hostname of the switch.

- Argument:

<name>: hostname, max. 40 characters.

- Possible value:

<name>: hostname, max. 40 characters.

- Example:

```
GS-2124L# hostname Company
```

```
Company#
```

° igmp

■ set drp

- Syntax:

```
set drp <port >
```

- Description:

Set router ports to disable.

- Argument:

<port >: syntax 1,5-7, available from 1 to 24

□ Possible value:

<port >: 1 to 24

□ Example:

GS-2124L(igmp)# set drp 1-10

■ set erp

□ Syntax:

set erp <port>

□ Description:

Set router ports to enable

□ Argument:

<port>: syntax 1,5-7, available from 1 to 24

□ Possible value:

<port>: 1 to 24

□ Example:

GS-2124L(igmp)# set erp 1

■ set flood

□ Syntax:

set flood <state>

□ Description:

To set up disable / enable unregister ipmc flooding.

□ Argument:

<state>: 0:disable, 1:enable

□ Possible value:

<state>: 0,or 1

□ Example:

GS-2124L(igmp)# set flood 1

■ show gm

□ Syntax:

show gm

□ Description:

To display group membership.

- Argument:

None.

- Possible value:

None.

- Example:

GS-2124L(igmp)# show gm

■ show igmpp

- Syntax:

show igmpp

- Description:

To display igmp proxy setting

- Argument:

None.

- Possible value:

None.

- Example:

GS-2124L(igmp)# show igmpp

° IP

■ disable dhcp

- Syntax:

disable dhcp

- Description:

To disable the DHCP function of the system.

- Argument:

None

- Possible value:

None

- Example:

GS-2124L(ip)# disable dhcp



■ enable dhcp

- Syntax:

enable dhcp <manual|auto>

□ Description:

To enable the system DHCP function and set DNS server via manual or auto mode.

□ Argument:

<manual|auto> : set dhcp by using manual or auto mode.

□ Possible value:

<manual|auto> : manual or auto

□ Example:

GS-2124L(ip)# enable dhcp manual

■ set dns

□ Syntax:

set dns <ip>

□ Description:

To set the IP address of DNS server.

□ Argument:

<ip> : dns ip address

□ Possible value:

168.95.1.1

□ Example:

GS-2124L (ip)# set dns 168.95.1.1

■ set ip

□ Syntax:

set ip <ip> <mask> <gateway>

□ Description:

To set the system IP address, subnet mask and gateway.

□ Argument:

<ip> : ip address

<mask> : subnet mask

<gateway> : default gateway

□ Possible value:

<ip> : 192.168.1.2 or others

<mask> : 255.255.255.0 or others

<gateway> : 192.168.1.253 or others

□ Example:

```
GS-2124L(ip)# set ip 192.168.1.2 255.255.255.0 192.168.1.253
```

■ show

□ Syntax:

show

□ Description:

To display the system's DHCP function state, IP address, subnet mask, default gateway, DNS mode, DNS server IP address and current IP address.

□ Argument:

None

□ Possible value:

None

□ Example:

```
GS-2124L(ip)# show
```

```
DHCP          : Disable
```

```
IP Address    : 192.168.2.237
```

```
Current IP Address : 192.168.2.237
```

```
Subnet mask   : 255.255.255.0
```

```
Gateway       : 192.168.2.252
```

```
DNS Setting   : Manual
```

```
DNS Server    : 168.95.1.1
```

° ip_mac_binding

■ set entry

□ Syntax:

```
set entry < 0 | 1> < mac> < ip> < port no> < vid>
```

□ Description:

To set ip mac binding entry

■ Kapitel 5: Operation of CLI Management (english)

□ Argument:

< 0 | 1 > : 0 : Client , 1: Server

<mac> : mac address

< ip > : ip address

< port > : syntax 1,5-7, available from 1 to 24

< vid > : vlan id, 1 to 4094

□ Possible value:

< 0 | 1 > : 0 : Client , 1: Server

<mac> : format: 00-02-03-04-05-06

< ip > : ip address

< port > : 1 to 24

< vid > : 1 to 4094

□ Example:

```
GS-2124L(ip_mac_binding)# set entry 1 00-11-2f-de-7b-a9 192.168.2.2
1 1
```

■ delete ip

□ Syntax:

```
delete ip < 0 | 1 > <ip>
```

□ Description:

Delete ip mac binding entry by ip.

□ Argument:

<0 | 1> : 0 : client, 1: server

<ip> : ip address

□ Possible value:

None

□ Example:

```
GS-2124L(ip_mac_binding)# delete ip 1 192.168.2.2
```

■ set state

□ Syntax:

```
show
```

□ Description:

To display the mac alias entry.

□ Argument:

None

□ Possible value:

None

□ Example:

```
GS-2124L(mac-table-alias)# show
```

MAC Alias List

MAC Address	Alias
-------------	-------

1) 00-02-03-04-05-06 aaa

2) 00-33-03-04-05-06 ccc

3) 00-44-33-44-55-44 www

° loop-detection

■ disable

□ Syntax:

disable <#>

□ Description:

To disable switch ports the loop detection function.

□ Argument:

<#> : set up the range of the ports to search for, syntax 1,5-7, available form 1 to 24

□ Possible value:

<#> :1 to 24

□ Example:

```
GS-2124L(loop-detection)# disable 1-24
```

```
GS-2124L(loop-detection)# show
```

Detection Port	Locked Port
----------------	-------------

Port Status	Port Status
-------------	-------------

1 Disable	1 Normal
-----------	----------

2 Disable	2 Normal
-----------	----------

3	Disable	3	Normal
4	Disable	4	Normal
5	Disable	5	Normal
6	Disable	6	Normal
7	Disable	7	Normal
8	Disable	8	Normal

i-i-i-

■ **enable**

□ Syntax:

enable <#>

□ Description:

To enable switch ports the loop detection function.

□ Argument:

<#> : set up the range of the ports to search for, syntax 1,5-7, available form 1 to 24

□ Possible value:

<#> :1 to 24

□ Example:

GS-2124L(loop-detection)# enable 1-24

GS-2124L(loop-detection)# show

Detection Port	Locked Port
Port Status	Port Status

```
-----
```

1	Enable	1	Normal
2	Enable	2	Normal
3	Enable	3	Normal
4	Enable	4	Normal
5	Enable	5	Normal
6	Enable	6	Normal
7	Enable	7	Normal
8	Enable	8	Normal

```
i-i-i-i-
```

■ Resume

□ Syntax:

```
resume <#>
```

□ Description:

To resume locked ports on switch.

□ Argument:

<#> : set up the range of the ports to search for, syntax 1,5-7, available form 1 to 24

□ Possible value:

<#> :1 to 24

□ Example:

```
GS-2124L (loop-detection)# resume 1-24
```

```
GS-2124L (loop-detection)# show
```

Detection Port	Locked Port
Port Status	Port Status

```
-----
```

1 Enable	1 Normal
2 Enable	2 Normal
3 Enable	3 Normal
4 Enable	4 Normal
5 Enable	5 Normal
6 Enable	6 Normal
7 Enable	7 Normal
8 Enable	8 Normal

```
i-i-i-i-
```

■ Resume

□ Syntax:

```
resume <#>
```

□ Description:

To resume locked ports on switch.

■ Kapitel 5: Operation of CLI Management (englisch)

- Argument:

<#> : set up the range of the ports to search for, syntax 1,5-7, available form 1 to 24

- Possible value:

<#> :1 to 24

- Example:

```
GS-2124L (loop-detection)# resume 1-24
```

```
GS-2124L (loop-detection)# show
```

Detection Port	Locked Port
Port Status	Port Status

1 Enable	1 Normal
2 Enable	2 Normal
3 Enable	3 Normal
4 Enable	4 Normal
5 Enable	5 Normal
6 Enable	6 Normal
7 Enable	7 Normal
8 Enable	8 Normal

i-i-i-i-

■ show

- Syntax:

show

- Description:

To display loop detection configure.

- Argument:

None

- Possible value:

None

- Example:

```
GS-2124L (loop-detection)# show
```

Detection Port	Locked Port
Port Status	Port Status

```
-----
  1 Enable    1 Normal
  2 Enable    2 Normal
  3 Enable    3 Normal
  4 Enable    4 Normal
  5 Enable    5 Normal
  6 Enable    6 Normal
  7 Enable    7 Normal
  8 Enable    8 Normal
```

```
i-i-i-i-
```

° Mac

■ <<alias>>

■ del

□ Syntax:

```
del <mac>
```

□ Description:

To del mac alias entry.

□ Argument:

```
<mac> : set up the MAC format: xx-xx-xx-xx-xx-xx
```

□ Possible value:

```
<mac> : set up the MAC format: xx-xx-xx-xx-xx-xx
```

□ Example:

```
GS-2124L(mac-alias)# set 23-56-r5-55-3f-03 test3
```

```
GS-2124L(mac-alias)# show
```

```
MAC Alias
```

No	MAC	Alias
----	-----	-------

```
=====
  1 23-56-00-55-3F-03 test3
```

■ Kapitel 5: Operation of CLI Management (englisch)

```
2 23-56-00-55-EF-03 test13
```

```
3 23-56-00-55-EF-33 test1
```

```
GS-2124L(mac-alias)# del 23-56-00-55-3F-03
```

```
GS-2124L(mac-alias)# show
```

```
MAC Alias
```

```
No      MAC      Alias
```

```
=====
```

```
1 23-56-00-55-EF-03 test13
```

```
2 23-56-00-55-EF-33 test1
```

■ set

Syntax:

```
set <mac> <alias>
```

Description:

To set mac alias entry.

Argument:

<mac> : mac address, xx-xx-xx-xx-xx-xx

<alias> : mac alias name, max 15 characters

Possible value:

<mac> : set up the MAC format: xx-xx-xx-xx-xx-xx

<alias> : mac alias name, max 15 characters

Example:

```
GS-2124L(mac-alias)# set 23-56-r5-55-3f-03 test3
```

```
GS-2124L(mac-alias)# show
```

```
MAC Alias
```

```
No      MAC      Alias
```

```
=====
```

```
1 23-56-00-55-3F-03 test3
```

```
2 23-56-00-55-EF-03 test13
```

```
3 23-56-00-55-EF-33 test1
```

■ show

Syntax:

show

□ Description:

To display mac alias entry.

□ Argument:

None

□ Possible value:

none

□ Example:

GS-2124L(mac-alias)# show

MAC Alias

No	MAC	Alias
1	23-56-00-55-3F-03	test3
2	23-56-00-55-EF-03	test13
3	23-56-00-55-EF-33	test1

=====

1 23-56-00-55-3F-03 test3

2 23-56-00-55-EF-03 test13

3 23-56-00-55-EF-33 test1

■ <<mac-table>>

■ flush

□ Syntax:

flush

□ Description:

To del dynamic mac entry.

□ Argument:

none

□ Possible value:

none

□ Example:

GS-2124L(mac-mac-table)# flush

GS-2124L(mac-mac-table)# show

No	Type	VLAN	MAC	Port Members
----	------	------	-----	--------------

■ Kapitel 5: Operation of CLI Management (englisch)

```

          1      Static          1      FF-FF-FF-FF-FF-FF
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,1
          8,19,20,21,22,23,24,

```

■ show

- Syntax:

show

- Description:

To show all mac table informaion.

- Argument:

none

- Possible value:

none

- Example:

GS-2124L(mac-mac-table)# show

```

No  Type  VLAN      MAC          Port Members
-----

```

```

          1      Static          1      FF-FF-FF-FF-FF-FF
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,1
          8,19,20,21,22,23,24,

```

■ <<maintenance>>

■ set age-time

- Syntax:

set age-time <#>

- Description:

To set mac table age out time of dynamic learning mac.

- Argument:

<#>: age-timer in seconds, 0, 10 1000000. The value zero disables aging

- Possible value:

<#>: 0, 10 to 1000000.

- Example:

GS-2124L(mac-table-maintain)# set age-time 300

```
GS-2124L(mac-maintenance)# show
E api_ai 26/vtss_
Aging Configuration:   Enter into sta
Age time: 300mode
MAC Table Learning
Port  Learning Mode-<< Global commands >
2    Auto
3    Auto
4    Auto
5    Auto
6    Auto
7    Auto
8    Auto
9    Auto
10   Auto
11   Auto
12   Auto
13   Auto
14   Auto
15   Auto
16   Auto
17   Auto
18   Auto
19   Auto
20   Auto
21   Auto
22   Auto
23   Auto
24   Auto
```

■ **set learning**

□ Syntax:

```
set learning <range> <auto|disable|secure>
```

□ Description:

To set mac table learning.

□ Argument:

<range syntax> : 1,5-7, available from 1 to 24

<auto >: auto learning

<disable >: disable learning

<secure >: learn frames are discarded

□ Possible value:

<range syntax> : 1,5-7, available from 1 to 24

<auto >: auto learning

<disable >: disable learning

<secure >: learn frames are discarded.

□ Example:

```
GS-2124L(mac-table-maintain)# set learning 1-24 auto
```

```
GS-2124L(mac-maintenance)# show
```

```
E api_ai 26/vtss_
```

```
Aging Configuration:   Enter into sta
```

```
Age time: 300mode
```

```
MAC Table Learning
```

```
Port  Learning Mode-<< Global commands >
```

```
2    Auto
```

```
3    Auto
```

```
4    Auto
```

```
5    Auto
```

```
6    Auto
```

```
7    Auto
```

```
8    Auto
```

```
9    Auto
```

10 Auto
11 Auto
12 Auto
13 Auto
14 Auto
15 Auto
16 Auto
17 Auto
18 Auto
19 Auto
20 Auto
21 Auto
22 Auto
23 Auto
24 Auto

■ **show**

□ Syntax:

show

□ Description:

To display mac table maintenance

□ Argument:

Noneq

□ Possible value:

None

□ Example:

GS-2124L(mac-maintenance)# show

1 Static

Aging Configuration:FF 1,2,3,4,5,6,7,8,9

Age time: 3004,15,16,17,1

MAC Table Learning

Port Learning Mode

2 Auto
3 Auto
4 Auto
5 Auto
6 Auto
7 Auto
8 Auto
9 Auto
10 Auto
11 Auto
12 Auto
13 Auto
14 Auto
15 Auto
16 Auto
17 Auto
18 Auto
19 Auto
20 Auto
21 Auto
22 Auto
23 Auto
24 Auto

■ <<static-mac>>

■ add

□ Syntax:

add <mac> <port> <vid> [alias]

□ Description:

To add the static mac entry.

□ Argument:

<mac> : mac address, format: 00-02-03-04-05-06

<port> : 0-24. The value "0" means this entry is filtering entry
 <vid> : vlan id. 0, 1-4094. VID must be zero if vlan mode is not tag-based
 [alias] : mac alias name, max. 15 characters

□ Possible value:

<mac> : mac address

<port> : 0-24

<vid> : 0, 1-4094

[alias] : mac alias name

□ Example:

```
GS-2124L(mac-static-mac)# add 00-02-03-04-05-06 3 0 aaa
```

```
GS-2124L(mac-static-mac)#
```



■ del

□ Syntax:

```
del <mac> <vid>
```

□ Description:

To del the static mac entry.

□ Argument:

<mac> : mac address, format: 00-02-03-04-05-06

<vid> : vlan id. 0, 1-4094. VID must be zero if vlan mode is not tag-based

□ Possible value:

<mac> : mac address

<vid> : 0, 1-4094

□ Example:

```
GS-2124L(mac-static-mac)# del 00-02-03-04-05-06 0
```

```
GS-2124L(mac-static-mac)#
```

■ show filter

□ Syntax:

```
show filter
```

□ Description:

To display the static filtering mac entry.

■ Kapitel 5: Operation of CLI Management (englisch)

- Argument:

None

- Possible value:

None

- Example:

```
GS-2124L(mac-static-mac)# show filter
```

```
Static Filtering Etnry: (Total 1 item(s))
```

```
1) mac: 00-33-03-04-05-06, vid: -, alias: ccc
```

```
GS-2124L(mac-static-mac)#
```

■ show forward

- Syntax:

```
show forward
```

- Description:

To display the static forwarding mac entry.

- Argument:

None

- Possible value:

None

- Example:

```
GS-2124L(mac-static-mac)# show forward
```

```
Static Forwarding Etnry: (Total 1 item(s))
```

```
1) mac: 00-02-03-04-05-06, port: 3, vid: -, alias: aaa
```

```
GS-2124L(mac-static-mac)#
```

° mirror

■ set mirror

- Syntax:

```
set mirror < #>
```

- Description:

To set mirror port and enable/disable mirror function

- Argument:

<#>: port, available from 1 to 24 and 0.

1 to 24: available port number

0: disable mirror function

□ Possible value:

<#>: 1 to 24

□ Example:

```
GS-2124L(mirror)# set mirror 2
```

■ set monitor-destination

□ Syntax:

```
set monitor-destination <range>
```

□ Description:

To set monitor destination port. The packets sent by this port will be copied to the monitoring port.

□ Argument:

<range>: the port that is chosen for monitored port of the mirror function, syntax 1,5-7, available from 1 to 24

□ Possible value:

<range>: 1 to 24

□ Example:

```
GS-2124L(mirror)# set monitor-destination 2-15
```

```
GS-2124L(mirror)# show
```

```

2           V
3           V
4           V
5           V
6           V
7           V
8           V
9           V
10          V
11          V
12          V

```

■ Kapitel 5: Operation of CLI Management (english)

13	V
14	V
15	V
16	
17	
18	

■ set monitor-source

□ Syntax:

set monitor-source <range>

□ Description:

To set up the monitoring port of the mirror function. User can observe the packets that the monitored port received via this port.

□ Argument:

<range>: the monitoring port that is chosen for the mirror function. Only one port is allowed to configure, available from 1 to 24

□ Possible value:

<range>:1 to 24

□ Example:

```
GS-2124L(mirror)# set monitor-source 18
```

```
GS-2124L(mirror)# show
```

```
Port to mirror to: 1
```

Port	Source Enable	Destination Enable
2		V
3		V
4		V
5		V
6		V
7		V
8		V
9		V

10 V
 11 V
 12 V
 13 V
 14 V
 15 V

16

17

18 V

19

20

21

22

23

24

GS-2124L(mirror)#

■ **show**

□ Syntax:

show

□ Description:

To display the setting status of mirror configuration.

□ Argument:

None

□ Possible value:

None

□ Example:

GS-2124L(mirror)# show

Port to mirror to: 1

Port	Source Enable	Destination Enable
------	---------------	--------------------

2		V
---	--	---

3		V
---	--	---

 ■ Kapitel 5: Operation of CLI Management (englisch)

DE

4	V
5	V
6	V
7	V
8	V
9	V
10	V
11	V
12	V
13	V
14	V
15	V
16	
17	
18	V
19	
20	
21	
22	
23	
24	
GS-2124L(mirror)#	

° mstp

■ disable

□ Syntax:

disable

□ Description:

To disable mstp function.

□ Argument:

None

- Possible value:

None

- Example:

GS-2124L (mstp)# disable

■ enable

- Syntax:

enable

- Description:

To enable mstp function.

- Argument:

None

- Possible value:

None

- Example:

GS-2124L (mstp)# enable

■ migrate-check

- Syntax:

migrate-check <port-range>

- Description:

To force the port to transmit RST BPDUs.

- Argument:

Usage: migrate-check <port range>

- port range syntax: 1,5-7, available from 1 to 24

- Possible value:

Usage: migrate-check <port range>

- port range syntax: 1,5-7, available from 1 to 24

- Example:

GS-2124L (mstp)# migrate-check 1-2

■ set config

- Syntax:

set config <Max Age><Forward Delay><Max Hops>

- Description:

To set max age,forward delay,max hops.

□ Argument:

<Max Age> : available from 6 to 40. Recommended value is 20

<Forward Delay(sec)> : available from 4 to 30. Recommended value is 15

<Max Hops> : available from 6 to 40. Recommended value is 20

□ Possible value:

<Max Age> : available from 6 to 40. Recommended value is 20

<Forward Delay(sec)> : available from 4 to 30. Recommended value is 15

<Max Hops> : available from 6 to 40. Recommended value is 20

□ Example:

```
GS-2124L(mstp)# set config 20 15 20
```

```
GS-2124L(mstp)#
```

■ set msti-vlan

□ Syntax:

```
set msti-vlan <instance-id><vid-string>
```

□ Description:

To map Vlan ID(s) to an MSTI

□ Argument:

<instance-id> : MSTI id available from 1 to 4095

□ <vid-string> : syntax example: 2.5-7.100-200

□ Possible value:

<instance-id> : available from 1 to 4094

□ Example:

```
GS-2124L(mstp)# set msti-vlan 2 2.5
```

msti 2 had been successfully created and(or)

vlan(s) have been added to map to this msti.

```
GS-2124L(mstp)#
```

■ set p-cost

□ Syntax:

```
set p-cost <instance_id> <port range> <path cost>
```

□ Description:

To set port path cost per instance

- Argument:
- <port range> syntax: 1,5-7, available from 1 to 24
<path cost> : 0, 1-200000000. The value zero means auto status
- Possible value:
<port range> : available from 1 to 24
<path cost> : The value zero means auto status, 0-2000000000
- Example:
GS-2124L(mstp)# set p-cost 2 8-10 0
GS-2124L(mstp)#

■ set p-edge

- Syntax:
set p-edge <port range> <admin edge>
- Description:
To set per port admin edge
- Argument:
- <port range> syntax: 1,5-7, available from 1 to 24
<admin edge> : 0->non-edge port,1->edge ports
- Possible value:
- <port range> syntax: 1,5-7, available from 1 to 24
<admin edge> : 0->non-edge port,1->edge ports
- Example:
GS-2124L(mstp)# set p-edge 10-12 0
GS-2124L(mstp)#

■ set p-hello

- Syntax:
set p-hello <port range> <hello time>
- Description:
To set per port hello time
- Argument:
- <port range> : syntax: 1,5-7, available from 1 to 24
<hello time> : only 1~2 are valid values
- Possible value:

□ <port range> : syntax: 1,5-7, available from 1 to 24
 <hello time> : only 1~2 are valid values

□ Example:

```
GS-2124L(mstp)# set p-hello 5-10 1
```

```
GS-2124L(mstp)#
```

■ set p-p2p

□ Syntax:

```
set p-p2p <port range> <admin p2p>
```

□ Description:

To set per port admin p2p

□ Argument:

□ <port range> syntax: 1,5-7, available from 1 to 24
 <admin p2p> : Admin point to point, <auto|true|false>

□ Possible value:

□ <port range> syntax: 1,5-7, available from 1 to 24
 <admin p2p> : Admin point to point, <auto|true|false>

□ Example:

```
GS-2124L(mstp)# set p-p2p 8-10 auto
```

```
GS-2124L(mstp)#
```

■ set priority

□ Syntax:

```
set priority <instance-id><Instance Priority>
```

□ Description:

To set instance priority

□ Argument:

<instance-id> : 0->CIST; 1-4095->MSTI

<Instance Priority> : must be a multiple of 4096,available from 0 to 61440

□ Possible value:

<instance-id> : 0->CIST; 1-4095->MSTI

<Instance Priority> : 0 to 61440

□ Example:

```
GS-2124L(mstp)# set priority 0 4096
GS-2124L(mstp)# enable
MSTP started
GS-2124L(mstp)# show instance 0
mstp status : enabled
force version : 3
instance id: 0
bridge max age : 20
bridge forward delay : 15
bridge max hops : 20
instance priority : 4096
bridge mac : 00:40:c7:5e:00:09
CIST ROOT PRIORITY : 4096
CIST ROOT MAC : 00:40:c7:5e:00:09
CIST EXTERNAL ROOT PATH COST : 0
CIST ROOT PORT ID : 0
CIST REGIONAL ROOT PRIORITY : 4096
CIST REGIONAL ROOT MAC : 00:40:c7:5e:00:09
CIST INTERNAL ROOT PATH COST : 0
CIST CURRENT MAX AGE : 20
CIST CURRENT FORWARD DELAY : 15
TIME SINCE LAST TOPOLOGY CHANGE(SECS) : 2
TOPOLOGY CHANGE COUNT(SECS) : 0
GS-2124L(mstp)#
```

■ set r-role

- Syntax:
set r-role <port range> <restricted role>
- Description:
To set per port restricted role
- Argument:

■ Kapitel 5: Operation of CLI Management (englisch)

□ <port range> syntax: 1,5-7, available from 1 to 24

<restricted role> : 0->>false,1->True

□ Possible value:

<port range> : 1 to 24

<restricted role> : 0->>false,1->True

□ Example:

```
GS-2124L(mstp)# set r-role 8-12 1
```

```
GS-2124L(mstp)# set r-role 13-16 0
```

```
GS-2124L(mstp)# show ports 0
```

```
=====
==Operational== ==Restricted==
PortPortStatus Role PathCost Pri Hello Edge- Port P2P Role Tcn
=====
1 FORWARDING DSGN 200000 128 2/2 V V
2 DISCARDING dsbl 2000000 128 2/2 V
3 DISCARDING dsbl 2000000 128 2/2 V
4 DISCARDING dsbl 2000000 128 2/2 V
5 FORWARDING DSGN 200000 128 2/2 V V
6 DISCARDING dsbl 2000000 128 2/2 V
7 FORWARDING DSGN 20000 128 2/2 V V
8 DISCARDING dsbl 2000000 128 2/2 V V
9 DISCARDING dsbl 2000000 128 2/2 V V
10 DISCARDING dsbl 2000000 128 2/2 V V
11 DISCARDING dsbl 2000000 128 2/2 V V
12 DISCARDING dsbl 2000000 128 2/2 V V
13 DISCARDING dsbl 2000000 128 2/2 V
14 DISCARDING dsbl 2000000 128 2/2 V
15 DISCARDING dsbl 2000000 128 2/2 V
16 DISCARDING dsbl 2000000 128 2/2 V
17 DISCARDING dsbl 2000000 128 2/2 V
```

```

18 DISCARDING dsbl 2000000 128 2/2 V
19 DISCARDING dsbl 2000000 128 2/2 V
20 DISCARDING dsbl 2000000 128 2/2 V
21 DISCARDING dsbl 2000000 128 2/2 V
22 DISCARDING dsbl 2000000 128 2/2 V
23 DISCARDING dsbl 2000000 128 2/2 V
24 DISCARDING dsbl 2000000 128 2/2 V
GS-2124L(mstp)#

```

■ set r-tcn

□ Syntax:

```
set r-tcn <port range> <restricted tcn>
```

□ Description:

To set per port restricted tcn

□ Argument:

□ <port range> syntax: 1,5-7, available from 1 to 24

<restricted tcn> : 0->>false,1->True

□ Possible value:

<port range> : 1 to 24

<restricted tcn> : 0->>false,1->True

□ Example:

```
GS-2124L(mstp)# set r-tcn 9-10 1
```

```
GS-2124L(mstp)# set r-tcn 14-20 1
```

```
GS-2124L(mstp)# show pconf 0
```

```

Port Path Cost Priority Hello Edge-Port P2P Role Tcn
system      Enter in

```

```

=====
=====... (q to quit)
=====

```

```

2    0 128 2 true auto false false
3    0 128 2 true auto false true
4    0 128 2 true auto false true
5    0 128 2 true auto false false

```

6	0	128	2	true	auto	false	false
7	0	128	2	true	auto	false	false
8	0	128	2	true	auto	true	false
9	0	128	2	true	auto	true	true
10	0	128	2	true	auto	true	true
11	0	128	2	true	auto	true	false
12	0	128	2	true	auto	true	false
13	0	128	2	true	auto	false	false
14	0	128	2	true	auto	false	true
15	0	128	2	true	auto	false	true
16	0	128	2	true	auto	false	true
17	0	128	2	true	auto	true	true
18	0	128	2	true	auto	true	true
19	0	128	2	true	auto	true	true
20	0	128	2	true	auto	true	true
21	0	128	2	true	auto	true	false
22	0	128	2	true	auto	true	false
23	0	128	2	true	auto	true	false
24	0	128	2	true	auto	true	false

GS-2124L(mstp)#

■ **set region-name**

□ Syntax:

set region-name <string>

□ Description:

To set mstp region name(0~32 bytes)

□ Argument:

<string> :a null region name

□ Possible value:

<string> :1-32

□ Example:

GS-2124L(mstp)# set region-name test2

```
GS-2124L(mstp)# show region-info
```

```
Name : test2
```

```
Revision : 0
```

```
Instances : 0
```

```
GS-2124L(mstp)#
```

■ **set revision-level**

- Syntax:

```
set rev <revision-level>
```

- Description:

```
To set mstp revision-level(0~65535)
```

- Argument:

```
<revision-level> :0~65535
```

- Possible value:

```
<revision-level> :0~65535
```

- Example:

```
GS-2124L(mstp)# set revision-level 30000
```

```
GS-2124L(mstp)# show region-info
```

```
Name : test2
```

```
Revision : 30000
```

```
Instances : 0
```

```
GS-2124L(mstp)#
```

■ **set version**

- Syntax:

```
set version <stp|rstp|mstp>
```

- Description:

```
To set force-version
```

- Argument:

```
<revision-level> :0~65535
```

- Possible value:

```
<revision-level> :0~65535
```

- Example:


```
GS-2924(mstp)# set version mstp
```

■ **show instance**

□ Syntax:

```
show instance <instance-id>
```

□ Description:

To show instance status

□ Argument:

```
<instance-id> :0->CIST;1-4095->MSTI
```

□ Possible value:

```
<instance-id> :0->CIST;1-4095->MSTI
```

□ Example:

```
GS-2124L(mstp)# show instance 0
```

```
mstp status : enabled
```

```
force version : 2
```

```
instance id: 0
```

```
bridge max age : 20
```

```
bridge forward delay : 15
```

```
bridge max hops : 20
```

```
instance priority : 4096
```

```
bridge mac : 00:40:c7:5e:00:09
```

```
CIST ROOT PRIORITY : 4096
```

```
CIST ROOT MAC : 00:40:c7:5e:00:09
```

```
CIST EXTERNAL ROOT PATH COST : 0
```

```
CIST ROOT PORT ID : 0
```

```
CIST REGIONAL ROOT PRIORITY : 4096
```

```
CIST REGIONAL ROOT MAC : 00:40:c7:5e:00:09
```

```
CIST INTERNAL ROOT PATH COST : 0
```

```
CIST CURRENT MAX AGE : 20
```

```
CIST CURRENT FORWARD DELAY : 15
```

```
TIME SINCE LAST TOPOLOGY CHANGE(SECS) : 2569
```

```
TOPOLOGY CHANGE COUNT(SECS) : 0
```

```
GS-2124L(mstp)#
```

■ show pconf

□ Syntax:

```
show pconf <instance-id>
```

□ Description:

To show port configuration

□ Argument:

instance-id:0->CIST;1-4095->MSTI

□ Possible value:

<instance-id> :0->CIST;1-4095->MSTI

□ Example:

```
GS-2124L(mstp)# show pconf 0
```

```
set r-role      Se
2      0 128 2   true auto false false
3      0 128 2   true auto false true
4      0 128 2   true auto false true
5      0 128 2   true auto false false
6      0 128 2   true auto false false
7      0 128 2   true auto false false
8      0 128 2   true auto true false
9      0 128 2   true auto true true
10     0 128 2   true auto true true
11     0 128 2   true auto true false
12     0 128 2   true auto true false
13     0 128 2   true auto false false
14     0 128 2   true auto false true
15     0 128 2   true auto false true
16     0 128 2   true auto false true
17     0 128 2   true auto true true
18     0 128 2   true auto true true
19     0 128 2   true auto true true
```

■ Kapitel 5: Operation of CLI Management (englisch)

```

20    0 128 2 true auto true true
21    0 128 2 true auto true false
22    0 128 2 true auto true false
23    0 128 2 true auto true false
24    0 128 2 true auto true false

```

GS-2124L(mstp)#

■ show ports

□ Syntax:

show ports <instance-id>

□ Description:

To show port status

□ Argument:

instance-id:0->CIST;1-4095->MSTI

□ Possible value:

<instance-id> :0->CIST;1-4095->MSTI

□ Example:

GS-2124L(mstp)# show ports 0

■ show region-info

□ Syntax:

show region-info

□ Description:

To show region config

□ Argument:

none

□ Possible value:

none

□ Example:

GS-2124L(mstp)# show region-info

Name : test2

Revision : 30000

Instances : 0

GS-2124L(mstp)#

■ show vlan-map

□ Syntax:

show vlan-map <instance-id>

□ Description:

To show vlan mapping of an instance

□ Argument:

<nstance-id> :0->CIST;1-4095->MSTI

□ Possible value:

<instance-id> :0->CIST;1-4095->MSTI

□ Example:

GS-2124L(mstp)# show vlan-map 0

instance 0 has those vlans :

0-4095

GS-2124L(mstp)#

° policy

■ add

□ Syntax:

add [name <value>] [ip <value>] [port <value>] [type <value>] action <value>

□ Description:

To add a new management policy entry.

□ Argument:

Synopsis: add name George ip 192.168.1.1-192.168.1.90 port 2-5,8
type h,s action a

Synopsis: add name Mary ip 192.168.2.1-192.168.2.90 action deny

□ Possible value:

None

□ Example:

GS-2124L(policy)# add name Mary ip 192.168.3.1-192.168.3.4 action deny

GS-2124L(policy)# show

- 1) Name : george IP Range : 192.168.1.1-192.168.1.90
 Action : Accept Access Type : HTTP SNMP
 Port : 2 3 4 5 8
- 2) Name : rule1 IP Range : 192.168.2.1-192.168.2.30
 Action : Deny Access Type : HTTP TELENT SNMP
 Port : 11 12 13 14 15
- 3) Name : Mary IP Range : 192.168.3.1-192.168.3.4
 Action : Deny Access Type : Any
 Port : Any

GS-2124L(policy)#

■ **delete**

- Syntax:

delete <index>

- Description:

To add a new management policy entry.

- Argument:

<index> : a specific or range management policy entry(s)

e.g. delete 2,3,8-12

- Possible value:

<index> : a specific or range management policy entry(s)

- Example:

GS-2124L(policy)# add name rule2 ip 192.168.4.23-192.168.4.33 port 6-8 type s,t

action d

GS-2124L(policy)# show

- 1) Name : rule1 IP Range : 192.168.4.5-192.168.4.22
 Action : Deny Access Type : HTTP TELENT SNMP
 Port : 2 3 4 5
- 2) Name : rule2 IP Range : 192.168.4.23-192.168.4.33
 Action : Deny Access Type : TELENT SNMP
 Port : 6 7 8

```
GS-2124L(policy)# delete 2
```

```
GS-2124L(policy)# show
```

```
1) Name : rule1      IP Range : 192.168.4.5-192.168.4.22
   Action : Deny     Access Type : HTTP TELENT SNMP
   Port : 2 3 4 5
```

```
GS-2124L(policy)#
```

■ show

Syntax:

```
show
```

Description:

To show management policy list.

Argument:

```
none
```

Possible value:

```
none
```

Example:

```
GS-2124L(policy)# show
```

```
1) Name : rule1      IP Range : 192.168.4.5-192.168.4.22
   Action : Deny     Access Type : HTTP TELENT SNMP
   Port : 2 3 4 5
```

```
2) Name : rule2      IP Range : 192.168.4.23-192.168.4.33
   Action : Deny     Access Type : TELENT SNMP
   Port : 6 7 8
```

° port

■ clear counter

Syntax:

```
clear counter
```

Description:

To clear all ports' counter (include simple and detail port counter) information.

Argument:

None

□ Possible value:

None

□ Example:

GS-2124L(port)# clear counter

■ set description

□ Syntax:

set description <port-range> <description>

□ Description:

To set port description

□ Argument:

<port range> syntax : 1,5-7, available from 1 to 24

<description> : set port description, max 47 characters

□ Possible value:

<port range> : 1 to 24

<description> : max 47 characters

□ Example:

GS-2124L(port)# set description 3-8 salesdepartment

GS-2124L(port)# show config

```
Speed/ Flow Maximum ExcessiveSynopsis: add name George ip
192.168.1.1-
```

```
Port Duplex Control Frame Collision Description
```

```
type
```

```
2 Auto Disabled 9600 Discard
3 Auto Disabled 9600 Discard salesdepartment
4 Auto Disabled 9600 Discard salesdepartment
5 Auto Disabled 9600 Discard salesdepartment
6 Auto Disabled 9600 Discard salesdepartment
7 Auto Disabled 9600 Discard salesdepartment
8 Auto Disabled 9600 Discard salesdepartment
9 Auto Disabled 9600 Discard
```

■ **set excessive-collision**

□ Syntax:

```
set excessive-collision <port-range> <discard|restart>
```

□ Description:

To set port description

□ Argument:

<port range> syntax : 1,5-7, available from 1 to 24

□ Possible value:

<port range> : 1 to 24

□ Example:

```
GS-2124L(port)# set excessive-collision 6-10 restart
```

```
GS-2124L(port)# show config
```

```
Speed/ Flow Maximum Excessive
```

```
Port Duplex Control Frame Collision Description a list of previously run
command set priority
```

```
-----
DISCAR
```

```
2 Auto Disabled 9600 Discard
3 Auto Disabled 9600 Discard salesdepartment
4 Auto Disabled 9600 Discard salesdepartment
5 Auto Disabled 9600 Discard salesdepartment
6 Auto Disabled 9600 Restart salesdepartment
7 Auto Disabled 9600 Restart salesdepartment
8 Auto Disabled 9600 Restart salesdepartment
9 Auto Disabled 9600 Restart
10 Auto Disabled 9600 Restart
11 Auto Disabled 9600 Discard
```

■ **set flow-control**

□ Syntax:

```
set flow-control <port-range> <enable|disable>
```

□ Description:

To set per-port flow control

- Argument:

<port-range>: syntax 1,5-7, available from 1 to 24

- Possible value:

<port-range>: 1 ~ 24

- Example:

```
GS-2124L(port)# set flow-control 3-10
```

```
GS-2124L(port)# show config
```

```
1 Auto   Disabled 9600  Discard
2 Auto   Disabled 9600  Discard
3 Auto   Enabled  9600  Discard salesdepartment
4 Auto   Enabled  9600  Discard salesdepartment
5 Auto   Enabled  9600  Discard salesdepartment
6 Auto   Enabled  9600  Restart salesdepartment
7 Auto   Enabled  9600  Restart salesdepartment
8 Auto   Enabled  9600  Restart salesdepartment
9 Auto   Enabled  9600  Restart
10 Auto  Enabled  9600  Restart
11 Auto  Disabled 9600  Discard
12 Auto  Disabled 9600  Discard
```

■ set max-frame

- Syntax:

```
set max-frame <port-range> <value>
```

- Description:

To set per-port maximum frame size

- Argument:

<port range> syntax : 1,5-7, available from 1 to 24

<value> : Allowed value are 1518-9600 bytes.

- Possible value:

<port range> syntax : 1 to 24

<value> : 1518-9600 bytes.

- Example:

```
GS-2124L(port)# set max-frame 3-6 1518
```

```
GS-2124L(port)# show config
```

```
Speed/ Flow Maximum Excessiveommands
2 Auto Disabled 9600 Discard
3 Auto Enabled 1518 Discard salesdepartment
4 Auto Enabled 1518 Discard salesdepartment
5 Auto Enabled 1518 Discard salesdepartment
6 Auto Enabled 1518 Restart salesdepartment
7 Auto Enabled 9600 Restart salesdepartment
8 Auto Enabled 9600 Restart salesdepartment
9 Auto Enabled 9600 Restart
10 Auto Enabled 9600 Restart
11 Auto Disabled 9600 Discard
```

■ set speed



□ Syntax:

```
set speed <port-range>
<disable|auto|1Gfull|100full|100half|10full|10half
```

□ Description:

To set port capability.

□ Argument:

<port-range>:syntax 1,5-7, available from 1 to 24

<port-speed>:

auto: set auto-negotiation mode

10half: set speed/duplex 10M Half

10full: set speed/duplex 10M Full

100half: set speed/duplex 100M Half

100full: set speed/duplex 100M Full

1Gfull: set speed/duplex 1G Full

□ Possible value:

<port-range>: 1 to 24

<port-speed>: auto, 10half, 10full, 100half, 100full, 1Gfull

□ Example:

```
GS-2124L(port)# set speed 3 auto
```

```
GS-2124L(port)# show status
```

```
Speed/
```

```
Port Link Duplex Rx Pause Tx Pause Description
```

```
-----
 1 Up 100M/Full Disabled Disabled
 2 Down Down Disabled Disabled
 3 Up 100M/Full Disabled Disabled
 4 Down Down Disabled Disabled
 5 Down Down Disabled Disabled
 6 Down Down Disabled Disabled
 7 Up 1G/Full Disabled Disabled
 8 Down Down Disabled Disabled
 9 Down Down Disabled Disabled
```

■ show config

□ Syntax:

```
show config
```

□ Description:

To display the each port's configuration information.

□ Argument:

None.

□ Possible value:

None.

□ Example:

```
GS-2124L(port)# show config
```

```
Speed/ Flow Maximum Excessive
```

```
Port Duplex Control Frame Collision Description
```

```
-----
 1 Auto Disabled 9600 Discard
```

```

2 1G/Full Disabled 9600 Discard
3 Auto Disabled 9600 Discard
4 1G/Full Disabled 9600 Discard
5 1G/Full Disabled 9600 Discard
6 Auto Disabled 9600 Discard
7 Auto Disabled 9600 Discard
8 Auto Disabled 9600 Discard
9 Auto Disabled 9600 Discard
10 Auto Disabled 9600 Discard
11 Auto Disabled 9600 Discard
12 Auto Disabled 9600 Discard

```

■ show detail-counter

- Syntax:

```
show detail-counter <port>
```

- Description:

To display the display detail port counter.

- Argument:

<port>: port, available from 1 to 24

- Possible value:

<port>:1 ~ 24

- Example:

```
GS-2124L (port)# show detail-counter 3
```

Rx Multicast	6	Tx Multicast	641
Rx Broadcast	94	Tx Broadcast	5251
Rx Pause	0	Tx Pause	0
Receive Size Counters		Transmit Size Counters	

Rx 64 Bytes	7381	Tx 64 Bytes	4351
Rx 65-127 Bytes	291	Tx 65-127 Bytes	2342
Rx 128-255 Bytes	118	Tx 128-255 Bytes	605
Rx 256-511 Bytes	53	Tx 256-511 Bytes	1081

 ■ Kapitel 5: Operation of CLI Management (englisch)

Rx 512-1023 Bytes	33	Tx 512-1023 Bytes	144
Rx 1024-1526 Bytes	28	Tx 1024-1526 Bytes	11453
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Error Counters		Transmit Error Counters	

Rx Drops	0	Tx Drops	0
Rx CRC/Alignment	0	Tx Late/Exc. Coll.	0
Rx Undersize	0		
Rx Oversize	0		
Rx Fragments	0		
Rx Jabber	0		

 ■ **show sfp**

□ Syntax:

show sfp <port>

□ Description:

To display the SFP module information.

□ Argument:

<port>: SFP port of the switch, available from 1, 24

□ Possible value:

<port>: 1- 24,

□ Example:

GS-2124L(port)# show sfp 11

Port 11 SFP information

 Connector Type : SFP - Unknown or unspecified

Fiber Type : Reserved

Tx Central Wavelength : 0

Baud Rate : 1G

Vendor OUI : 00:00:00

Vendor Name : FIBERXON INC.

Vendor PN : FTM-C012R-LC

```

Vendor Rev      : 10
Vendor SN      : PP220052901281
Date Code     : 051012
Temperature    : none
Vcc           : none
Mon1 (Bias) mA : none
Mon2 (TX PWR) : none
Mon3 (RX PWR) : none
GS-2124L(port)#
Port 23 SFP information

```

```

-----
Connector Type  : SFP - LC
Fiber Type     : Multi-mode (MM)
Tx Central Wavelength : 850
Baud Rate      : 1G
Vendor OUI     : 00:40:c7
Vendor Name    : APAC Opto
Vendor PN      : KM28-C3S-TC-N
Vendor Rev     : 0000
Vendor SN      : 5425010708
Date Code     : 050530
Temperature    : none
Vcc           : none
Mon1 (Bias) mA : none
Mon2 (TX PWR) : none
Mon3 (RX PWR) : none

```

■ **show simple-counter**

- Syntax:
show simple-counter
- Description:

To display the summary counting of each port's traffic.

□ Argument:

None.

□ Possible value:

None.

□ Example:

```
GS-2124L (port)# show simple-counter
```

```
set max-frame      Set per-port maximum frame size
```

```
13  0  0  0  0  0  0  0  0  0
14  0  0  0  0  0  0  0  0  0
15  0  0  0  0  0  0  0  0  0
16  0  0  0  0  0  0  0  0  0
17  0  0  0  0  0  0  0  0  0
18  0  0  0  0  0  0  0  0  0
19  0  0  0  0  0  0  0  0  0
20  0  0  0  0  0  0  0  0  0
21  0  0  0  0  0  0  0  0  0
22  0  0  0  0  0  0  0  0  0
23  0  0  0  0  0  0  0  0  0
24  0  0  0  0  0  0  0  0  0
```

```
GS-2124L(port)#
```

■ **show status**

□ Syntax:

```
show status
```

□ Description:

To display the port's current status.

□ Argument:

None.

□ Possible value:

None.

□ Example:

```

GS-2124L(port)# show status
      Speed/1G/Full  Disable
Port Link Duplex  Rx Pause Tx Pause  Description
 3 Auto   Disabled 9600   Discard
 2 Down Down   Disabled Disabled
 3 Up   100M/Full Disabled Disabled
 4 Down Down   Disabled Disabled
 5 Down Down   Disabled Disabled
 6 Down Down   Disabled Disabled
 7 Up   1G/Full Disabled Disabled
 8 Down Down   Disabled Disabled
 9 Down Down   Disabled Disabled
10 Down Down   Disabled Disabled
11 Up   Null/Half Disabled Disabled
12 Down Down   Disabled Disabled
13 Down Down   Disabled Disabled
14 Down Down   Disabled Disabled
15 Down Down   Disabled Disabled
16 Down Down   Disabled Disabled
17 Down Down   Disabled Disabled
18 Down Down   Disabled Disabled
19 Down Down   Disabled Disabled
20 Down Down   Disabled Disabled
21 Down Down   Disabled Disabled
22 Down Down   Disabled Disabled
23 Down Down   Disabled Disabled
24 Down Down   Disabled Disabled
GS-2124L(port)#

```


° qos

■ <<ports>>



■ set class

- Syntax:

set class <#>

- Description:

To set number of classes.

- Argument:

#: Number of classes, available 1, 2, 4

- Possible value:

<#>: 1,2,4

- Example:

GS-2124L(qos-ports)# set class 2

GS-2124L(qos-ports)#

■ set port

- Syntax:

set port <range> <default class> <qcl> <user priority> <queuing mode>
<low queue weighted> <normal queue weighted> <medium queue
weighted> <high queue we
ighted>

- Description:

To set port information.

- Argument:

<range syntax>: 1,5-7, available from 1 to 24

<default class option>: low | normal | medium | high

<qcl> : available from 1 to 24

<user priority>: available from 0 to 7

<queuing mode>: strict | weighted

<low queue weighted>: 1 / 2 / 4 / 8

<normal queue weighted>: 1 / 2 / 4 / 8

<medium queue weighted> : 1 / 2 / 4 / 8

<high queue weighted>: 1 / 2 / 4 / 8

□ Possible value:

<range syntax>: 1 to 24

<default class option>: low | normal | medium | high

<qcl> : 1 to 24

<user priority>: 0 to 7

<queuing mode>: strict | weighted

<low queue weighted>: 1 / 2 / 4 / 8

<normal queue weighted>: 1 / 2 / 4 / 8

<medium queue weighted> : 1 / 2 / 4 / 8

<high queue weighted>: 1 / 2 / 4 / 8

□ Example:

```
GS-2124L(qos-ports)# set port 2 medium 1 3 weithted 2 2 2 2
```

```
GS-2124L(qos-ports)# show
```

```
 2 Medium    1    3   Weighted Fair  2 / 2 / 2 / 2
 3 Low      1    0   Strict Priority 1 / 2 / 4 / 8
 4 Low      1    0   Strict Priority 1 / 2 / 4 / 8
 5 Low      1    0   Strict Priority 1 / 2 / 4 / 8
 6 Low      1    0   Strict Priority 1 / 2 / 4 / 8
 7 Low      1    0   Strict Priority 1 / 2 / 4 / 8
 8 Low      1    0   Strict Priority 1 / 2 / 4 / 8
 9 Low      1    0   Strict Priority 1 / 2 / 4 / 8
10 Low      1    0   Strict Priority 1 / 2 / 4 / 8
11 Low      1    0   Strict Priority 1 / 2 / 4 / 8
12 Low      1    0   Strict Priority 1 / 2 / 4 / 8
13 Low      1    0   Strict Priority 1 / 2 / 4 / 8
14 Low      1    0   Strict Priority 1 / 2 / 4 / 8
```

```
¡K¡K¡K
```

```
GS-2124L(qos-ports)#
```

■ **show**

□ Syntax:

show

□ Description:

To show port information.

□ Argument:

none

□ Possible value:

none

□ Example:

GS-2124L(qos-ports)# show

Number of Classes:2

2	Medium	1	3	Weighted Fair	2 / 2 / 2 / 2
---	--------	---	---	---------------	---------------

3	Low	1	0	Strict Priority	1 / 2 / 4 / 8
---	-----	---	---	-----------------	---------------

4	Low	1	0	Strict Priority	1 / 2 / 4 / 8
---	-----	---	---	-----------------	---------------

5	Low	1	0	Strict Priority	1 / 2 / 4 / 8
---	-----	---	---	-----------------	---------------

6	Low	1	0	Strict Priority	1 / 2 / 4 / 8
---	-----	---	---	-----------------	---------------

7	Low	1	0	Strict Priority	1 / 2 / 4 / 8
---	-----	---	---	-----------------	---------------

8	Low	1	0	Strict Priority	1 / 2 / 4 / 8
---	-----	---	---	-----------------	---------------

9	Low	1	0	Strict Priority	1 / 2 / 4 / 8
---	-----	---	---	-----------------	---------------

10	Low	1	0	Strict Priority	1 / 2 / 4 / 8
----	-----	---	---	-----------------	---------------

<<qcl>>

■ **set**

□ Syntax:

set <dscp> <tos> <tagpriority> <qce type> <value> <class>

□ Description:

To add the QCE entry in the specific QCL

□ Argument:

<dscp>: dscp field, syntax 1,5-7, available from 0 to 63

<tos> : tos priority , available from 1 to 8

<tagpriority> : tag priority, available from 1 to 8

<qce type> : ethernet

<value> : 0xffff0

<class> : high

□ Possible value:

<dscp>: dscp field, syntax 1,5-7, available from 0 to 63

<tos> : tos priority , available from 1 to 8

<tagpriority> : tag priority, available from 1 to 8

<qce type> : ethernet

<value> : 0xffff0

<class> : high

□ Example:

```
GS-2124L(qos-qcl)# set 2 0 3 ethernet 0xffff0 high
```

```
GS-2124L(qos-qcl)# show 2 1
```

```
QCE Type:      Ethernet Type
```

```
Ethernet Type Value:0xffff0
```

```
Traffic Class:  High
```

```
GS-2124L(qos-qcl)#
```

■ move

□ Syntax:

```
move <qcl> <qce> <new qce>
```

□ Description:

To move up the specific QCE entry in the specific QCL

□ Argument:

<qcl> : the qcl number, available from 1 to 24.

<qce> : the original qce number, available from 1 to 12.

<new qce> : the new qce number, available from 1 to 12.

□ Possible value:

<qcl> : available from 1 to 24.

<qce> : available from 1 to 12.

<new qce> : available from 1 to 12.

□ Example:

```
GS-2124L(qos-qcl)# move 2 1 1
```

■ delete

□ Syntax:

```
delete <qcl> <qce range>
```

□ Description:

To delete the specific QCE entry in the specific QCL.

□ Argument:

<qcl> : the qcl number, available from 1 to 24.

<qce range> : 1,5-7, available from 1 to 12

□ Possible value:

<qcl> : available from 1 to 24.

<qce range> : available from 1 to 12

□ Example:

```
GS-2124L(qos-qcl)# delete 2 1
```

```
<<rate>>
```

■ set

□ Syntax:

```
set <range> <policer enabled> <rate> <unit> <shaper enabled> <rate> <unit>
```

□ Description:

To set rate limit configuration

□ Argument:

<range syntax> : 1,5-7, available from 1 to 24

<policer enabled> : 1 means enable and 0 means disable

<rate>: allowed values are 500kbps-1Gkps

<unit>: 'k' means kbps and 'm' means mbps

<shaper enabled>: 1 means enable and 0 means disable

<rate>: allowed values are 500kbps-1Gkps

<unit>: 'k' means kbps and 'm' means mbps

□ Possible value:

□ range syntax: 1,5-7, available from 1 to 24

policer enabled: 1 means enable and 0 means disable

rate: allowed values are 500kbps-1Gkps

unit: 'k' means kbps and 'm' means mbps

shaper enabled: 1 means enable and 0 means disable

rate: allowed values are 500kbps-1Gkps

unit: 'k' means kbps and 'm' means mbps

□ Example:

```
GS-2124L(qos-rate)# set 2 1 1000 m 1 1000 m
```

```
GS-2124L(qos-rate)# show
```

2	V	1000	Mbps	V	1000	Mbps
3		500	kbps	500	kbps	
4		500	kbps	500	kbps	
5		500	kbps	500	kbps	
6		500	kbps	500	kbps	
7		500	kbps	500	kbps	
8		500	kbps	500	kbps	
9		500	kbps	500	kbps	
10		500	kbps	500	kbps	

■ << storm >>

■ set broadcast

■

□ Syntax:

```
set broadcast <status> <rate>
```

□ Description:

To set broadcast storm control configuration

□ Argument:

<status> : 1 means enable and 0 means disable

<rate> : 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1k, 2k, 4k, 8k, 16k, 32k, 64k, 128k

, 256k, 512k

□ Possible value:

<status> : 1 means enable and 0 means disable

<rate> : 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1k, 2k, 4k, 8k, 16k, 32k, 64k, 128k, 256k, 512k

□ Example:

```
GS-2124L(qos-storm)# set broadcast 1 512
```

```
GS-2124L(qos-storm)# show
```

```
Frame Type   Status   Rate(Packet Per Second)
```

```
-----
Flooded unicast      1
Multicast            1
Broadcast           V   512
```

■ set multicast

□ Syntax:

```
set multicast <status> <rate>
```

□ Description:

To set multicast storm control configuration

□ Argument:

<status> : 1 means enable and 0 means disable

<rate> : 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1k, 2k, 4k, 8k, 16k, 32k, 64k, 128k, 256k, 512k

□ Possible value:

<status> : 1 means enable and 0 means disable

<rate> : 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1k, 2k, 4k, 8k, 16k, 32k, 64k, 128k, 256k, 512k

□ Example:

```
GS-2124L(qos-storm)# set multicast 1 64
```

```
GS-2124L(qos-storm)# show
```

```
Frame Type   Status   Rate(Packet Per Second)
```

```
-----
```

```
Flooded unicast    1
Multicast         V   64
Broadcast         V  512
```

■ set unicast

□ Syntax:

```
set unicast <status> <rate>
```

□ Description:

To set flooded unicast storm control configuration

□ Argument:

<status> : 1 means enable and 0 means disable

<rate> : 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1k, 2k, 4k, 8k, 16k, 32k,
64k, 128k

, 256k, 512k

□ Possible value:

<status> : 1 means enable and 0 means disable

<rate> : 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1k, 2k, 4k, 8k, 16k, 32k,
64k, 128k

, 256k, 512k

□ Example:

```
GS-2124L(qos-storm)# set unicast 1 128
```

```
GS-2124L(qos-storm)# show
```

```
Frame Type   Status   Rate(Packet Per Second)
```

```
-----
```

```
Flooded unicast V    128
```

```
Multicast     V    64
```

```
Broadcast     V   512
```

■ show

□ Syntax:

```
show
```

□ Description:

To show storm control configuration

Argument:

none

Possible value:

none

Example:

GS-2124L(qos-storm)# show

Frame Type	Status	Rate(Packet Per Second)

Flooded unicast	V	128
Multicast	V	64
Broadcast	V	512

° reboot

■ reboot

Syntax:

reboot

Description:

To reboot the system.

Argument:

None.

Possible value:

None.

Example:

GS-2124L# reboot

° snmp

■ <<disable>>

Syntax:

disable set-ability

disable snmp

Description:

The Disable here is used for the de-activation of snmp or set-community.

- Argument:

None.

- Possible value:

None.

- Example:

```
GS-2124L(sntp)# disable snmp
```

```
GS-2124L(sntp)# disable set-ability
```

■ <<enable>>

- Syntax:

```
enable set-ability
```

```
enable snmp
```

- Description:

The Enable here is used for the activation snmp or set-community.

- Argument:

None.

- Possible value:

None.

- Example:

```
GS-2124L(sntp)# enable snmp
```

```
GS-2124L(sntp)# enable set-ability
```

■ <<set>>

- Syntax:

```
set get-community <community>
```

```
set set-community <community>
```

```
set trap <#> <ip> [port] [community]
```

- Description:

The Set here is used for the setup of get-community, set-community, trap host ip, host port and trap-community.

- Argument:

<#>: trap number

<ip>: ip address or domain name

<port>: trap port

<community>:trap community name

□ Possible value:

<#>: 1 to 6

<port>:1~65535

□ Example:

```
GS-2124L(snmp)# set get-community public
```

```
GS-2124L(snmp)# set set-community private
```

```
GS-2124L(snmp)# set trap 1 192.168.1.1 162 public
```

■ show

□ Syntax:

show

□ Description:

The Show here is to display the configuration of SNMP.

□ Argument:

None.

□ Possible value:

None.

□ Example:

```
GS-2124L(snmp)# show
```

```
SNMP      : Enable
```

```
Get Community: public
```

```
Set Community: private [Enable]
```

```
Trap Host 1 IP Address: 192.168.1.1 Port: 162 Community: public
```

```
Trap Host 2 IP Address: 0.0.0.0 Port: 162 Community: public
```

```
Trap Host 3 IP Address: 0.0.0.0 Port: 162 Community: public
```

```
Trap Host 4 IP Address: 0.0.0.0 Port: 162 Community: public
```

```
Trap Host 5 IP Address: 0.0.0.0 Port: 162 Community: public
```

```
Trap Host 6 IP Address: 0.0.0.0 Port: 162 Community: public
```

° stp

■ MCheck

□ Syntax:

MCheck <range>

□ Description:

To force the port to transmit RST BPDUs.

□ Argument:

<range>: syntax 1,5-7, available from 1 to 24

□ Possible value:

<range>: 1 to 24

□ Example:

```
GS-2124L(stp)# Mcheck 1-8
```

```
disable
```

□ Syntax:

```
disable
```

□ Description:

To disable the STP function.

□ Argument:

None.

□ Possible value:

None.

□ Example:

```
GS-2124L(stp)# disable
```

```
enable
```

□ Syntax:

```
enable
```

□ Description:

To enable the STP function.

□ Argument:

None.

□ Possible value:

None.

□ Example:

```
GS-2124L(stp)# enable
```

■ **set config**

□ Syntax:

set config <Bridge Priority> <Hello Time> <Max. Age> <Forward Delay>

□ Description:

To set up the parameters of STP.

□ Argument:

<Bridge Priority>: priority must be a multiple of 4096, available from 0 to 61440.

<Hello Time>: available from 1 to 10.

<Max. Age>: available from 6 to 40.

<Forward Delay>: available from 4 to 30.

Note: $2 * (\text{Forward Delay} - 1) \geq \text{Max Age}$

$\text{Max Age} \geq 2 * (\text{Hello Time} + 1)$

□ Possible value:

<Bridge Priority>: 0 to 61440

<Hello Time>: 1 to 10

<Max. Age>: 6 to 40

<Forward Delay>: 4 to 30

□ Example:

GS-2124L(stp)# set config 61440 2 20 15

■ **set port**

□ Syntax:

set port <range> <path cost> <priority> <edge_port> <admin p2p>

□ Description:

To set up the port information of STP.

□ Argument:

<range>: syntax 1,5-7, available from 1 to 24

<path cost>: 0, 1-20000000. The value zero means auto status

<priority>: priority must be a multiple of 16, available from 0 to 240

<edge_port> : Admin Edge Port, <yes|no>

<admin p2p>: Admin point to point, <auto|true|false>

- Possible value:
 <range>: 1 to 24
 <path cost>: 0, 1-200000000
 <priority>: 0 to 240
 <edge_port>: yes / no
 <admin p2p>: auto / true / false

- Example:
 GS-2124L(stp)# set port 1-16 0 128 yes auto

■ set version

- Syntax:
 set version <stp|rstp>
- Description:
 To set up the version of STP.
- Argument:
 <stp|rstp>:stp / rstp
- Possible value:
 <stp|rstp>:stp / rstp
- Example:
 GS-2124L(stp)# set version rstp_

■ show config

- Syntax:
 show config
- Description:
 To display the configuration of STP.
- Argument:
 None.
- Possible value:
 None.
- Example:
 GS-2124L(stp)# show config
 STP State Configuration :
 Spanning Tree Protocol : Enabled

Bridge Priority (0-61440) : 61440

Hello Time (1-10 sec) : 2

Max. Age (6-40 sec) : 20

Forward Delay (4-30 sec) : 15

Force Version : RSTP

■ show port

□ Syntax:

show port

□ Description:

To display the port information of STP.

□ Argument:

None.

□ Possible value:

None.

□ Example:

GS-2124L# stp

GS-2124L(stp)# show port

Port Port Status Path Cost Priority Admin Edge Port Admin Point To Point

Port	Port	Status	Path	Cost	Priority	Admin	Edge	Port	Admin	Point To Point
1	DISCARDING	2000000	128	No	Auto					
2	DISCARDING	2000000	128	No	Auto					
3	DISCARDING	2000000	128	No	Auto					
4	DISCARDING	2000000	128	No	Auto					
5	DISCARDING	2000000	128	No	Auto					
6	DISCARDING	2000000	128	No	Auto					
7	DISCARDING	2000000	128	No	Auto					
8	DISCARDING	2000000	128	No	Auto					
9	DISCARDING	2000000	128	No	Auto					
10	DISCARDING	2000000	128	No	Auto					
11	DISCARDING	2000000	128	No	Auto					

12	DISCARDING	2000000	128	No	Auto
13	DISCARDING	2000000	128	No	Auto
14	DISCARDING	2000000	128	No	Auto
15	DISCARDING	2000000	128	No	Auto
16	DISCARDING	2000000	128	No	Auto
17	DISCARDING	2000000	128	No	Auto
18	DISCARDING	2000000	128	No	Auto
19	DISCARDING	2000000	128	No	Auto
20	DISCARDING	2000000	128	No	Auto
21	DISCARDING	2000000	128	No	Auto
22	DISCARDING	2000000	128	No	Auto
...(q to quit)					
23	DISCARDING	2000000	128	No	Auto
24	DISCARDING	2000000	128	No	Auto

■ show status

□ Syntax:

show status

□ Description:

To display the status of STP.

□ Argument:

None.

□ Possible value:

None.

□ Example:

GS-2124L(stp)# show status

STP Status :

STP State : Enabled

Bridge ID : 00:40:C7:D8:09:1D

Bridge Priority : 61440

Designated Root : 00:40:C7:D8:09:1D

Designated Priority : 61440


```

Root Port                : 0
Root Path Cost           : 0
Current Max. Age(sec)    : 20
Current Forward Delay(sec) : 15
Hello Time(sec)         : 2
STP Topology Change Count : 0
Time Since Last Topology Change(sec) : 848_

```

° system

■ set contact

□ Syntax:

```
set contact <contact string>
```

□ Description:

To set the contact description of the switch.

□ Argument:

<contact>:string length up to 40 characters.

□ Possible value:

<contact>: A, b, c, d, ... ,z and 1, 2, 3, etc.

□ Example:

```
GS-2124L(system)# set contact Taipei
```

■ set device-name

□ Syntax:

```
set device-name <device-name string>
```

□ Description:

To set the device name description of the switch.

□ Argument:

<device-name>: string length up to 40 characters.

□ Possible value:

<device-name>: A, b, c, d, ... ,z and 1, 2, 3, etc.

□ Example:

```
GS-2124L(system)# set device-name CR-2600
```

■ **set location**

- Syntax:

set location <location string>

- Description:

To set the location description of the switch.

- Argument:

<location>: string length up to 40 characters.

- Possible value:

<location>: A, b, c, d, ... ,z and 1, 2, 3, etc.

- Example:

GS-2124L(system)# set location Taipei

■ **show**

- Syntax:

show

- Description:

To display the basic information of the switch.

- Argument:

None.

- Possible value:

None.

- Example:

GS-2124L(system)# show

Model Name : GS-2124L

System Description : L2 Managed Switch

Location :

Contact :

Device Name : GS-2124L

System Up Time : 0 Days 0 Hours 4 Mins 14 Secs

Current Time : Tue Jan 17 16:28:46 2006

BIOS Version : v1.05

Firmware Version : v2.08

 ■ Kapitel 5: Operation of CLI Management (englisch)

Hardware-Mechanical Version : v1.01-v1.01
 Serial Number : 030C02000003
 Host IP Address : 192.168.1.1
 Host MAC Address : 00-40-c7-e7-00-10
 Device Port : UART * 1, TP * 22, Dual-Media Port(RJ45/SFP) * 2
 RAM Size : 16 M
 Flash Size : 2 M

° traplog

■ clear

Syntax:

clear

Description:

To clear trap log.

Argument:

none

Possible value:

none

Example:

GS-2124L(traplog)# clear

GS-2124L(traplog)# show

No	time	desc

■ show

Syntax:

show

Description:

To display the trap log.

Argument:

None.

Possible value:

None.

□ Example:

```
GS-2124L(tftp)# show
```

```
2 Mon Mar 17 15:18:38 2008gvrp mode> <qce type> .
```

```
    Dual Media Swapped [Port:1][SwapTo:TP]ge hostnamexit/ 4 / 8
```

```
3 Mon Mar 17 15:18:38 2008nto igmp mode, available from
```

```
    Link Up [Port:1]Enter into ip mode
```

```
6 Mon Mar 17 15:18:38 2008
```

```
    Dual Media Swapped [Port:5][SwapTo:TP]
```

```
7 Mon Mar 17 15:18:38 2008
```

```
    Link Up [Port:5]
```

```
8 Mon Mar 17 15:18:48 2008
```

```
    Login [admin]
```

° time

■ set daylightsaving

□ Syntax:

```
set daylightsaving <hr> <MM/DD/HH> <mm/dd/hh>
```

□ Description:

To set up the daylight saving.

□ Argument:

hr : daylight saving hour, range: -5 to +5

MM : daylight saving start Month (01-12)

DD : daylight saving start Day (01-31)

HH : daylight saving start Hour (00-23)

mm : daylight saving end Month (01-12)

dd : daylight saving end Day (01-31)

hh : daylight saving end Hour (00-23)

□ Possible value:

hr : -5 to +5

MM : (01-12)

DD : (01-31)

HH : (00-23)

mm : (01-12)

dd : (01-31)

hh : (00-23)

□ Example:

```
GS-2124L(time)# set daylightsaving 3 10/12/01 11/12/01
```

Save Successfully

■ set manual

□ Syntax:

```
set manual <YYYY/MM/DD> <hh:mm:ss>
```

□ Description:

To set up the current time manually.

□ Argument:

YYYY : Year (2000-2036) MM : Month (01-12)

DD : Day (01-31) hh : Hour (00-23)

mm : Minute (00-59) ss : Second (00-59)

□ Possible value:

YYYY : (2000-2036) MM : (01-12)

DD : (01-31) hh : (00-23)

mm : (00-59) ss : (00-59)

□ Example:

```
GS-2124L(time)# set manual 2004/12/23 16:18:00
```

■ set ntp

□ Syntax:

```
set ntp <ip> <timezone>
```

□ Description:

To set up the current time via NTP server.

□ Argument:

<ip>: ntp server ip address or domain name

<timezone>: time zone (GMT), range: -12 to +13

□ Possible value:

<timezone>: -12,-11...,0,1...,13

□ Example:

```
GS-2124L(time)# set ntp clock.via.net 8
```

Synchronizing...(1)

Synchronization success

■ show

□ Syntax:

```
show
```

□ Description:

To show the time configuration, including "Current Time", "NTP Server", "Timezone", "Daylight Saving", "Daylight Saving Start" and "Daylight Saving End"

□ Argument:

None.

□ Possible value:

None.

□ Example:

```
GS-2124L(time)# show
```

```
Current Time: Thu Thu 14 15:04:03 2005
```

```
NTP Server: 209.81.9.7
```

```
Timezone: GMT+8:00
```

```
Day light Saving: 0 Hours
```

```
Day light Saving Start: Mth: 1 Day: 1 Hour: 0
```

```
Day light Saving End : Mth: 1 Day: 1 Hour: 0
```

```
GS-2124L(time)#
```

° trunk

■ del trunk

□ Syntax:

```
del trunk <port-range>
```

□ Description:

To delete the trunking port.

■ Kapitel 5: Operation of CLI Management (englisch)

- Argument:
<port-range>: port range, syntax 1,5-7, available from 1 to 24
- Possible value:
<port-range>: 1 to 24
- Example:
GS-2124L(trunk)# del trunk 1



■ set priority

- Syntax:
set priority <range>
- Description:
To set up the LACP system priority.
- Argument:
<range>: available from 1 to 65535.
- Possible value:
<range>: 1 to 65535, default: 32768
- Example:
GS-2124L(trunk)# set priority 33333



set trunk

- Syntax:
set trunk <port-range> <method> <group> <active LACP>
- Description:
To set up the status of trunk, including the group number and mode of the trunk as well as LACP mode.
- Argument:
<port-range> : port range, syntax 1,5-7, available from 1 to 24
<method>:
static : adopt the static link aggregation
lacp : adopt the dynamic link aggregation- link aggregation control protocol
<group>: 1-8.
<active LACP>:

active : set the LACP to active mode

passive : set the LACP to passive mode

□ Possible value:

<port-range> : 1 to 24

<method>: static / lacp

<group>: 1-8.

<active LACP>: active /passive

□ Example:

GS-2124L(trunk)# set trunk 1-4 lacp 1 active

■ show aggtr-view

□ Syntax:

show aggtr-view

□ Description:

To display the aggregator list.

□ Argument:

None.

□ Possible value:

None.

□ Example:

GS-2124L(trunk)# show aggtr-view

Aggregator 1) Method: None

Member Ports: 1

Ready Ports: 1

Aggregator 2) Method: LACP

Member Ports: 2

Ready Ports:

: :

■ show lacp-detail

□ Syntax:

show lacp-detail <aggtr>

□ Description:

To display the detailed information of the LACP trunk group.

- Argument:

<aggr>: aggregator, available from 1 to 24

- Possible value:

<aggr>: 1 to 24

- Example:

GS-2124L(trunk)# show lacp-detail 2

Aggregator 2 Information:

Actor		Partner	
System Priority	MAC Address	System Priority	MAC Address
32768	00-40-c7-e8-00-02	32768	00-00-00-00-00-00
Port	Key	Port	Key
2	257	2	0

■ show lacp-priority

- Syntax:

show lacp-priority

- Description:

To display the value of LACP Priority.

- Argument:

None.

- Possible value:

None.

- Example:

GS-2124L(trunk)# show lacp-priority

LACP System Priority : 32768

■ show status

- Syntax:

show status

□ Description:

To display the aggregator status and the settings of each port.

□ Argument:

None.

□ Possible value:

None.

□ Example:

GS-2124L(trunk)# show status

Trunk Port Setting				Trunk Port Status	
port	Method	Group	Active	LACP	Aggtregator Status
1	None	0	Active	1	Ready
2	LACP	1	Active	2	---
3	LACP	1	Active	3	---
4	LACP	1	Active	4	---
5	LACP	1	Active	5	---
6	LACP	1	Active	6	---
7	LACP	1	Active	7	---
:					
19	None	0	Active	19	---
20	None	0	Active	20	---
21	None	0	Active	21	---
22	None	0	Active	22	---
23	None	0	Active	23	---
24	None	0	Active	24	---

° vlan

■ del port-group

□ Syntax:

del port-group <name>

■ Kapitel 5: Operation of CLI Management (englisch)

- Description:
To delete the port-based vlan group.
- Argument:
<name>: which vlan group you want to delete.
- Possible value:
<name>: port-vlan name
- Example:
GS-2124L(vlan)# del port-group VLAN-2

■ del tag-group

- Syntax:
del tag-group <vid>
- Description:
To delete the tag-based vlan group.
- Argument:
<vid>: which vlan group you want to delete, available from 1 to 4094
- Possible value:
<vid>: 1 to 4094
- Example:
GS-2124L(vlan)# del tag-group 2
disable drop-untag
- Syntax:
disable drop-untag <range>
- Description:
Don't drop the untagged frames.
- Argument:
<range> : which port(s) you want to set, syntax 1,5-7, available from 1 to 24
- Possible value:
<range>: 1 to 24
- Example:
GS-2124L(vlan)# disable drop-untag 5-10
disable sym-vlan

- Syntax:

disable sym-vlan <range>

- Description:

To drop frames from the non-member port.

- Argument:

<range>: which port(s) you want to set, syntax 1,5-7, available from 1 to 24

- Possible value:

<range>: 1 to 24

- Example:

```
GS-2124L(vlan)# disable sym-vlan 5-10
enable drop-untag
```

- Syntax:

enable drop-untag <range>

- Description:

To drop the untagged frames.

- Argument:

<range>: which port(s) you want to set, syntax 1,5-7, available from 1 to 24

- Possible value:

<range>: 1 to 24

- Example:

```
GS-2124L(vlan)# enable drop-untag 5-10
enable sym-vlan
```

- Syntax:

enable sym-vlan <range>

- Description:

To drop frames from the non-member port.

- Argument:

<range> : which port(s) you want to set, syntax 1,5-7, available from 1 to 24

- Possible value:

<range>: 1 to 24

□ Example:

```
GS-2124L(vlan)# enable sym-vlan 5-10
```

■ set mode

□ Syntax:

```
set mode <disable|port|tag|metro|double-tag> [up-link]
```

□ Description:

To switch VLAN mode, including disable, port-based, tag-based, metro and double-tag modes.

□ Argument:

<disable>: vlan disable

<tag>: set tag-based vlan

<port>: set port-based vlan

<metro>: set metro mode vlan

<double-tag>: enable Q-in-Q function

<up-link>: syntax 1,5-7, available from 23 to 24, only for metro mode vlan

□ Possible value:

<disable|port|tag|metro|double-tag>: disable,port,tag,metro,double-tag

[up-link]: 23 or 24 or "23,24"

□ Example:

```
GS-2124L(vlan)# set mode port
```

■ set port-group

□ Syntax:

```
set port-group <name> <range>
```

□ Description:

To add or edit a port-based VLAN group.

□ Argument:

<name>: port-vlan name

<range>: syntax 1,5-7, available from 1 to 24

□ Possible value:

<range>: 1 to 24

- Example:

```
GS-2124L(vlan)# set port-group VLAN-1 2-5,6,15-13
```

■ set port-role

- Syntax:

```
set port-role <range> <access|trunk|hybrid> [vid]
```

- Description:

To set egress rule: configure the port roles.

- Argument:

<range> :which port(s) you want to set, syntax 1,5-7, available from 1 to 24

<access>: Do not tag frames

<trunk>: Tag all frames

<hybrid>: Tag all frames except a specific VID

<vid>: untag-vid for hybrid port

- Possible value:

<range>: 1 to 24

<vid>: 1 to 4094

- Example:

```
GS-2124L(vlan)# set port-role 5 hybrid 6
```

■ set pvid

- Syntax:

```
set pvid <range> <pvid>
```

- Description:

To set the pvid of vlan.

- Argument:

<range>: which port(s) you want to set PVID(s), syntax 1,5-7, available from

1 to 24

<pvid>: which PVID(s) you want to set, available from 1 to 4094

- Possible value:

<range>: 1 to 24

<pvid>: 1 to 4094

- Example:

```
GS-2124L(vlan)# set pvid 3,5,6-8 5
```

■ set tag-group

- Syntax:

```
set tag-group <vid> <name> <range> <#>
```

- Description:

To add or edit the tag-based vlan group.

- Argument:

<vid>: vlan ID, range from 1 to 4094

<name>: tag-vlan name

<range>: vlan group members, syntax 1,5-7, available from 1 to 24

<#>: sym/asym vlan setting. 1: symmetric vlan, 0: asymmetric vlan

- Possible value:

<vid>: 1 to 4094

<range>: 1 to 24

<#>: 0 or 1

- Example:

```
GS-2124L(vlan)# set tag-group 2 VLAN-2 2-5,6,15-13 0
```

■ show group

- Syntax:

```
show group
```

- Description:

To display the vlan mode and vlan group.

- Argument:

None.

- Possible value:

None.

- Example:

```
GS-2124L(vlan)# show group
```

Vlan mode is double-tag.

1) Vlan Name : default

Vlan ID : 1

Sym-vlan : Disable

Member : 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

2) Vlan Name : VLAN-2

Vlan ID : 2

Sym-vlan : Disable

Member : 2 3 4 5 6 13 14 15

DE

■ show port

□ Syntax:

show port

□ Description:

To display pvid, ingress/egress rule.

□ Argument:

None.

□ Possible value:

None.

□ Example:

GS-2124L(vlan)# show pvid

Port	PVID	Rule1	Rule2	Port Rule	Untag Vid
1	1	Disable	Disable	Access	-
2	1	Disable	Disable	Access	-
3	5	Disable	Disable	Access	-
4	1	Disable	Disable	Access	-
5	5	Enable	Disable	Hybrid	6
6	5	Enable	Disable	Access	-
7	5	Enable	Disable	Access	-
8	5	Enable	Disable	Access	-
9	1	Enable	Disable	Access	-
10	1	Enable	Disable	Access	-
11	1	Disable	Disable	Access	-

■ Kapitel 5: Operation of CLI Management (englisch)

			:			
				:		
23	1	Disable	Disable	Access	-	
24	1	Disable	Disable	Access	-	

6 Anhang

6.1 Leistungs- und Kenndaten

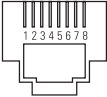
LANCOM GS-2124		
Performance	Switching Technologie	Store and forward mit Latenzzeiten kleiner 5 µs
	Anzahl MAC-Adressen	Unterstützung von maximal 8K MAC-Adressen
	Durchsatz	maximal 48 Gbit/s auf der Backplane
	Virtual Stacking Management (VSM)	Unterstützt Stacking von bis zu 16 Geräten, mehrere Switches können über eine IP-Adresse verwaltet werden
	VLAN	Port-basiertes und IEEE 802.1q tag-basiertes VLAN mit bis zu 4096 VLAN und bis zu 256 aktiven VLANs; Unterstützung von Ingress und Egress Paket-Filtern im Port-basierten VLAN
LAN-Protokolle	Link Aggregation Control Protocol (LACP)	Maximal 12 Gruppen, maximal 16 Mitglieder pro Gruppe, Unterstützt DA, SA und DA+SA MAC basiertes Trunking mit automatischem Fail-over
	Multicasting	Unterstützt IGMP snooping inklusive aktivem und passivem Modus
	GVRP/GARP	802.1q mit GVRP/GARP
	Spanning Tree Protokoll (STP) / Rapid STP / Multiple STP	802.1d/1w/1s
Anschlüsse	Ethernet Ports	20 Ports 10/100/1000 Mbit/s Ethernet, 4 Combo-Ports TP/SFP 10/100/1000 Mbit/s
	Serielle Schnittstelle	Serielle Konfigurationsschnittstelle
Stromversorgung		Internes Netzteil (110–230 V, 50-60 Hz)
Gehäuse		Robustes Metallgehäuse, 19" 1 HE (440 x 44,2 x 209 mm) mit abschraubbaren Montagewinkeln, Netzwerkanschlüsse auf der Frontseite
Normen		CE-konform nach EN 55022, EN 55024, EN 60950
Umgebung/ Temperatur		Temperaturbereich 0–40°C; Luftfeuchtigkeit 5–90%; nicht kondensierend
Zubehör		<ul style="list-style-type: none"> ■ 1000Base-SX SFP-Modul, LANCOM SFP-SX-LC1, Art.-Nr.: 61556 ■ 1000Base-LX SFP-Modul, LANCOM SFP-LX-LC1, Art.-Nr.: 61557
Service		5 Jahre Garantie auf alle Komponenten
Support		Über Hotline und Internet

6.2 Anschlussbelegung

6.2.1 LAN-Schnittstelle 10/100Base-TX

8-polige RJ45-Buchsen, entsprechend ISO 8877, EN 60603-7

DE

Steckverbindung	Pin	Leitung
	1	T+
	2	T-
	3	R+
	4	PoE/G
	5	PoE/G
	6	R-
	7	PoE/-48 V
	8	PoE/-48 V

6.3 CE-Konformitätserklärungen



Hiermit erklärt LANCOM Systems, dass sich die in dieser Dokumentation beschriebenen Geräte in Übereinstimmung mit den grundlegenden Anforderungen und den anderen relevanten Vorschriften der Richtlinie 1999/5/EG befinden.

Die CE-Konformitätserklärungen für Ihr Gerät finden Sie im jeweiligen Produktbereich der LANCOM-Website (www.lancom.de).