NETGEAR[®]

GS108T/GS110TP スマートスイッチ ^{ソフトウェア管理マニュアル}

350 East Plumeria Drive San Jose, CA 95134 USA

November 2015 202-10603-03 v2.(英文参照ドキュメント)

NETGEAR製品をお選びいただきありがとうございます。

NETGEAR製品のインストール、設定、または仕様に関するご質問や問題については、下記のNETGEARカス タマーサポートまでご連絡ください。

無償保証を受けるためには、本製品をご購入後30日以内にユーザー登録が必要になります。ユーザー登録 方法につきましては、別紙[ユーザー登録のお知らせ]をご確認ください。

NETGEARカスタマーサポート

電話:フリーコール 0120-921-080

(携帯・PHSなど、フリーコールが使用できない場合:03-6670-3465)

受付時間:平日9:00-20:00、土日祝 10:00-18:00(年中無休)

E-mail:support@netgear.jp

テクニカルサポートの最新情報は、NETGEARのウェブサイトをご参照ください。

http://www.netgear.jp/support/

商標

NETGEAR、NETGEAR ロゴは米国およびその他の国における NETGEAR, Inc.の商標または登録商標です。

その他のブランドおよび製品名は、それぞれの所有者の商標または登録商標です。 記載内容は、予告なしに変更されることがあります。

© 2015 NETGEAR, Inc. All rights reserved.

適合性

本製品をお使いになる前に、適合性の情報をお読みください。 各種規格との適合に関する情報は、ネットギアのウェブサイト(<u>http://www.netgear.com/about/regulatory/</u>)をご覧ください(英語)。

目次

1.	はじめに	7
	本書の構成	
	GS108T/GS110TP ギガビットスマートスイッチを使う	8
	スイッチ管理インターフェース	8
	スイッチをネットワークに接続する	8
	DHCP サーバーがあるネットワークでスイッチを発見する	
	DHCP サーバーがないネットワークでスイッチを発見する	
	固定 IP アドレスを設定する	11
	管理システムのネットワーク設定を構成する	
	管理システムのネットワーク設定を変更する	
	スイッナの固定 IP アトレスを設定する:	13
	Web アクセス	
	Smart Control Center ユーティリティ	
	ネットワークユーティリティ	15
	設定のアッブロードとダウンロード(Configuration Upload and Download)	
	ファームワェアアッフクレート	
	ダスク官理	20
	ユーザーインターフェースを理解する	
	Web インターフェースを使う	21
	SNMP を使う	24
2.	システム設定	
2.	システム設定	
2.	システム設定 <i>Management(マネージメント)</i> システム情報(System Information)	
2.	システム設定 <i>Management(マネージメント)</i> システム情報(System Information) IP 設定(IP Configuration)	26
2.	システム設定 <i>Management(マネージメント)</i> システム情報(System Information). IP 設定(IP Configuration). IPv6 設定(IPv6 Configuration).	26
2.	システム設定 <i>Management(マネージメント)</i> システム情報(System Information) IP 設定(IP Configuration) IPv6 設定(IPv6 Configuration) IPv6 近隣情報(IPv6 Network Neighbor)	26 27 27 28 30 31
2.	システム設定 Management(マネージメント) システム情報(System Information). IP 設定(IP Configuration). IPv6 設定(IPv6 Configuration). IPv6 近隣情報(IPv6 Network Neighbor). 時間(Time).	26 27 27 28 30 31 32 27
2.	システム設定 Management(マネージメント) システム情報(System Information) IP 設定(IP Configuration) IPv6 設定(IPv6 Configuration) IPv6 近隣情報(IPv6 Network Neighbor) 時間(Time) Denial of Service(DoS) DNS	26 27 27 28 30 31 32 37 40
2.	システム設定 Management(マネージメント) システム情報(System Information). IP 設定(IP Configuration). IPv6 設定(IPv6 Configuration). IPv6 近隣情報(IPv6 Network Neighbor). 時間(Time). Denial of Service(DoS). DNS. グリーンイーサネット設定(Green Ethernet Configuration).	26 27 27 28 30 31 32 37 40 42
2.	システム設定 Management(マネージメント)システム情報(System Information)	26 27 27 28 30 31 31 32 37 40 42 42
2.	システム設定 Management(マネージメント) システム情報(System Information) IP 設定(IP Configuration) IPv6 設定(IPv6 Configuration) IPv6 近隣情報(IPv6 Network Neighbor) 時間(Time) Denial of Service(DoS) DNS グリーンイーサネット設定(Green Ethernet Configuration) PoE (GS110TP のみ) PoE 設定(PoE Configuration)	26 27 27 28 30 31 31 32 37 40 42 42 43
2.	システム設定 Management(マネージメント) システム情報(System Information) IP 設定(IP Configuration) IP 改定(IP Configuration) IP v6 設定(IPv6 Configuration) IPv6 近隣情報(IPv6 Network Neighbor)	26 27 27 28 30 31 31 32 37 40 40 42 42 43 44
2.	システム設定Management(マネージメント)システム情報(System Information)IP 設定(IP Configuration)IP 改定(IPv6 Configuration)IPv6 設定(IPv6 Configuration)IPv6 近隣情報(IPv6 Network Neighbor)時間(Time)Denial of Service (DoS)DNSグリーンイーサネット設定(Green Ethernet Configuration)PoE (GS110TP のみ)PoE 設定(PoE Configuration)PoE ポート設定(PoE Port Configuration)タイマーグローバル設定(Timer Global Configuration)	26 27 27 28 30 31 31 32 37 40 42 42 42 43 44 44
2.	システム設定Management(マネージメント)システム情報(System Information)IP 設定(IP Configuration)IP 改定(IP v6 Configuration)IPv6 設定(IPv6 Configuration)IPv6 近隣情報(IPv6 Network Neighbor)時間(Time)Denial of Service (DoS)DNSグリーンイーサネット設定(Green Ethernet Configuration)PoE (GS110TP のみ)PoE 設定(PoE Configuration)PoE ポート設定(PoE Port Configuration)タイマーグローバル設定(Timer Global Configuration)タイマースケジュール設定(Timer Schedule Configuration)	26 27 27 28 30 31 32 37 40 42 42 42 43 44 44 46
2.	システム設定 Management(マネージメント)	26 27 27 28 30 31 31 32 37 40 42 42 42 43 44 44 46 46 46
2.	システム設定 Management(マネージメント)	26 27 27 28 30 31 32 37 40 42 42 42 43 44 44 46 46 46 47
2.	システム設定 Management(マネージメント)	26 27 27 28 30 31 31 32 37 40 42 42 42 43 44 44 46 46 46 46 47 48 50
2.	システム設定 Management(マネージメント)	26 27 27 28 30 31 32 37 40 42 42 43 44 44 46 46 46 46 47 48 50 50
2.	システム設定 Management(マネージメント)	26 27 27 28 30 31 32 37 40 42 42 42 43 44 44 46 46 46 46 46 46 47 48 50 51
2.	システム設定 Management(マネージメント)	26 27 27 28 30 31 31 32 37 40 42 42 43 43 44 44 46 46 46 46 46 46 47 48 50 51 51 52 53
2.	システム設定 Management(マネージメント) システム情報(System Information) IP 設定(IP Configuration) IP 設定(IP Configuration) IPv6 設定(IPv6 Configuration) IPv6 近隣情報(IPv6 Network Neighbor) 時間 (Time) Denial of Service (DoS) DNS グリーンイーサネット設定(Green Ethernet Configuration) PoE (GS110TP のみ) PoE 設定(PoE Configuration) PoE 就定(PoE Configuration) タイマーグローバル設定(Timer Global Configuration) タイマースケジュール設定(Timer Schedule Configuration) タイマースケジョン 1/バージョン 2 トラップフラグ (Trap Flags) SNMP バージョン 1/バージョン 2 トラップフラグ (Trap Flags) SNMP 3 ユーザー設定 (SNMP v3 User Configuration) LLDP LLDP 設定 (LLDP Configuration) LLDP 教士(LLDP Port Settings)	26 27 27 28 30 31 32 37 40 42 42 43 44 44 46 46 46 46 46 46 46 50 51 51 52 53 53 54

LLDP-MED Port Settings	
ローカル情報(Local Information)	57
隣接情報(Neighbors Information)	
サービス-DHCP フィルタ(Services - DHCP Filtering)	62
DHCP フィルタ設定 (DHCP Filtering Configuration)	63
インターフェース設定(Interface Configuration)	
3. スイッチング設定	
$\#$ - b/P_{orto}	66
デート設定(Port Configuration)	66 66
フローコントロール(Flow Control)	
リンクアグリゲーショングループ(Link Aggregation Groups)	
LAG 設定(LAG Configuration)	
LAG メンバーシップ(LAG Membership)	
LACP 設定(LACP Configuration)	71
LACP ポート設定(LACP Port Configuration)	71
VLAN	
VLAN 設定(VLAN Configuration)	72
VLAN メンバーシップ設定(VLAN Membership Configuration)	74
ポート VLAN 設定(Port VLAN ID Configuration)	75
ボイス VLAN(Voice VLAN)	
ボイス VLAN プロパティ(Voice VLAN Properties)	76
ボイス VLAN ボート設定 (Voice VLAN Port Setting)	
ホイス VLAN OUI(Voice VLAN OUI)	
オート VoIP(Auto-VoIP)	
スパニングツリープロトコル(Spanning Tree Protocol)	
STP スイッチ設定(STP Switch Configuration)	80
CST 設定(CST Configuration)	
CST ボート設定(CST Port Configuration)	
CSI ホートスナーダス(CSI Port Status)	85
Kapid STP	
MST 設定 (MST Configuration) MST ポート設定 (MST Port Configuration)	
STP 統計(STP Statistics)	89
マルナイヤスト(Multicast) ナートビデナ設定(Auto-Video Configuration)	
リートビリリ設定(Auto-Video Configuration)	
IGMP スヌーピングクエリア (IGMP Snooping Querier)	
フ+ワーディングデータベース (Forwarding Database)	100
リオリン リオンシア シベ ス(Norwarding Database)	101
ダイナミックアドレス設定(Dynamic Address Configuration)	
スタティック MAC アドレス (Static MAC Address)	
4. QoS 設定	
CoS(Class of Service)	106
基本 CoS 設定(Basic CoS Configuration)	
CoS インターフェース設定(CoS Interface Configuration)	
インターフェースキュー設定(Interface Queue Configuration)	
802.1p からキューへのマッピング(802.1p to Queue Mapping)	
DSCP からキューへのマッピング(DSCP to Queue Mapping)	

DiffServ(ディ	ィフサーブ、Differentiated Services)	
DiffServ 5	定義 (Defining DiffServ)	
DiffServ 🖥	設定(Diffserv Configuration)	
クラス設定	定(Class Configuration)	
IPv6 クラン	ス設定(IPv6 Class Configuration)	
ポリシー言	設定(Policy Configuration)	
サービス	設定(Service Configuration)	
サービス約	統計(Service Statistics)	
5. デバイス	セキュリティ管理	
管理セキュリ	リティ設定(Management Security Settings)	
パスワー	ド変更(Change Password)	
RADIUS	設定(RADIUS Configuration)	
TACACS-	+設定(Configuring TACACS+)	
認証リスト	ト設定(Authentication List Configuration)	
管理アクセン	ス設定(Configuring Management Access)	
HTTP 設筑	定(HTTP Configuration)	
HTTPS 詔	设定(Secure HTTP Configuration)	
証明書ダ	ウンロード(Certificate Download)	
アクセスフ	プロファイル設定(Access Profile Configuration)	
アクセスノ	ルール設定(Access Rule Configuration)	
ポート認証((Port Authentication)	
802.1X 設	定(802.1X Configuration)	
ポート認言	$\mathbb{I}(Port \; Authentication)$	
ポートサマ	マリー(Port Summary)	
トラフィック制	制御(Traffic Control)	
MAC フィル	ルター設定(MAC Filter Configuration)	
MAC フィル	ルターサマリー(MAC Filter Summary)	
ストームコ	コントロール(Storm Control)	
ポートセキ	キュリティ設定(Port Security Configuration)	147
ポートセキ	キュリティインターフェース設定(Port Security Interface Configuration)	147
セキュリテ	Fィ MAC アドレス(Security MAC Address)	
プロテクト	ポート(Protected Ports Membership)	
ACL を設定	する(Configuring Access Control Lists)	
ACL ウィ ^ー	ザード(ACL Wizard)	
MAC ACL		
MAC ルー	ール(MAC Rules)	
MAC バイ	インディング設定(MAC Binding Configuration)	
MAC バイ	′ンディングテーブル (MAC Binding Table)	
IP ACL		
IP ルール	(IP Rules)	
IP 拡張ル	ノール (IP Extended Rule)	
IP バイン・ IP バイン・	ディング設定(IP Binding Configuration) ディングテーブル(IP Binding Table)	
ェハイン		
6. システム	監視	
ポート(Ports	s)	
スイッチ紛	稅訂(Switch Statistics)	
ホート統言	計(Port Statistics)	
ホート詳約	幽稅計 (Port Detailed Statistics)	
EAP 統計	(EAP Statistics)	
システムログ	ゲ(System Logs)	

メモリーログ(Memory Logs)	
フラッシュログ設定(FLASH Log Configuration)	
サーバーログ設定(Server Log Configuration)	
トラップログ(Trap Logs)	
イベントログ(Event Logs)	
ポートミラーリング(Port Mirroring)	
マルチポートミラーリング(Multiple Port Mirroring)	
7. システムメインテナンス	
リセット(Reset)	
再起動(Device Reboot)	
ファクトリーデフォルト(Factory Default)	
スイッチからのファイルアップロード(Upload File From Switch)	
スイッチへのファイルダウンロード(Download File To Switch)	
TFTP ファイルダウンロード(TFTP File Download)	
HTTP ファイルダウンロード(HTTP File Download)	
ファイル 管理(File Management)	
デュアルイメージ設定(Dual Image Configuration)	
デュアルイメージ状態(Dual Image Status)	
トラブルシュート(Troubleshooting)	
Ping	
Ping IPv6	
トレースルート(Traceroute)	
A.ハードウェア仕様とデフォルト設定	195
GS108T/ GS110TP ギガビットスマートスイッチ仕様	
GS108T 仕様	
GS108T/GS110TP スイッチパフォーマンス	
B.設定サンプル	
VLAN(Virtual Local Area Networks)	
VLAN サンプル設定(VLAN Example Configuration)	
ACL(Access Control Lists)	
MAC ACL サンプル設定(MAC ACL Example Configuration)	
スタンダード IP ACL サンプル設定(Standard IP ACL Example Configuration)	

1.はじめに

NETGEAR[®]GS108T/GS110TP ソフトウェア管理マニュアルは GS108T/GS110TP ギガビットスマー トスイッチを Web ベースのグラフィックユーザーインターフェース(GUI)を使って設定・操作する方法 を記述していますこのマニュアルはソフトウェアを設定する手順について記述し、その手順利用可 能なオプションについて説明しています。

本書の構成

GS108T/GS110TP スマートスイッチソフトウェア管理マニュアルには以下の章が含まれています。

- 1.はじめに
- 2.システム設定
- 3.スイッチング設定
- 4.QoS 設定
- 5.デバイスセキュリティ管理
- 6.システム監視
- 7.システムメインテナンス
- Appendix A.ハードウェア仕様とデフォルト設定

GS108T/GS110TP ギガビットスマートスイッチを使う

この章ではネットギア GS108T/GS110TP スマートスイッチを使うための概要とユーザーインターフ ェースへのアクセス方法を示します。また、Smart Control Center ユーティリティの使い方も示しま す。この章は以下の節を含みます。

- スイッチ管理インターフェース
- スイッチをネットワークに接続する
- DHCP サーバーがあるネットワークでスイッチを発見する
- DHCP サーバーがないネットワークでスイッチを発見する
- 管理システムのネットワーク設定を構成する
- Web アクセス
- Smart Control Center ユーティリティ
- ユーザーインターフェースを理解する
- インターフェース命名規則

スイッチ管理インターフェース

NETGEAR スマートスイッチ GS108T と GS110TP にはスイッチ機能を管理、モニターするための Web サーバーと管理ソフトウェアが実装されています。GS108T と GS110TP は管理ソフトウェアを 使わなければシンプルなスイッチとして動作します。しかし、管理ソフトウェアを使って、スイッチの 効率と全体のネットワークパフォーマンスを高める拡張機能を設定することができます。

Web ベースの管理機能によって、高価で複雑な SNMP ソフトウェアを使うかわりに標準的な Web ブラウザでスイッチをリモートからモニター、設定、制御することができます。Web ブラウザでスイッ チのパフォーマンスをモニターし、設定をネットワークに最適化することができます。Web ベースの 管理インターフェースを使って、VLAN、QoS、ACL のようなすべてのスイッチの機能を設定するこ とができます。

NETGEAR は Smart Control Center utility を提供します。このプログラムはウィンドウズで動作し、 お使いのネットワークセグメント(ブロードキャストドメイン)でスイッチを発見する機能を提供します。 はじめてスイッチの電源を入れるときに、Smart Control Center を使ってスイッチを発見し、DHCP サーバーが割り当てたスイッチの IP アドレス情報を確認したり、ネットワークに DHCP サーバーが ない場合に、Smart Control Center でスイッチを発見し、固定 IP アドレスを割り当てたりします。

NETGEAR のスイッチの発見に加えて、Smart Control Center は、パスワード管理、ファームウェ アアップグレード、設定ファイルのバックアップなどの機能を提供します。詳しくは、Smart Control Center ユーティリティをご覧ください。

スイッチをネットワークに接続する

Web ブラウザや SNMP を使ってスイッチをリモート管理するためには、スイッチをネットワークに接続し、ネットワーク設定(IP アドレス、サブネットマスク、デフォルトゲートウェイ)を設定する必要があります。スイッチのデフォルト設定は、IP アドレスが 192.168.0.239、サブネットマスクが255.255.255.0 です。

以下の3つの方法のうちの1つを使ってスイッチのデフォルトネットワーク設定を変更します。

- DHCP を使う-スイッチの DHCP クライアント機能はデフォルトで有効になっています。スイ ッチを DHCP サーバーと同じネットワークに接続すると、スイッチは自動的に IP アドレスを 取得します。Smart Control Center を使ってスイッチに割り当てられたネットワーク情報を 確認することができます。くわしくは、詳しくは DHCP サーバーがあるネットワークでスイッチ を発見するをご覧ください。
- Smart Control Center を使って固定設定をする-DHCP サーバーのないネットワークにスイ ッチを接続する場合は、Smart Control Center を使って固定 IP アドレス、サブネットマス ク、デフォルトゲートウェイを設定することができます。くわしくは、DHCP サーバーがないネ ットワークでスイッチを発見するをご覧ください。
- ローカルホストから接続して固定設定をする-Smart Control Center を使わずに固定アドレス設定をするには、192.168.0.0/24のネットワークのホスト(管理システム)からスイッチに接続し、スイッチのWeb管理インターフェースを使って設定を変更できます。くわしくは、管理システムのネットワーク設定を構成するをご覧ください。

DHCP サーバーがあるネットワークでスイッチを発見する

この章では、DHCP サーバーがあるネットワークでスイッチを設定する方法について記します。ス イッチの DHCP クライアントはデフォルトで有効になっています。スイッチをネットワークに接続する と、DHCP サーバーは自動的にスイッチに IP アドレスを割り当てます。Smart Control Center を使 ってスイッチに自動的に割り当てられた IP アドレスを確認することができます。

DHCP サーバーがあるネットワークにスイッチをインストールするには、以下の手順を行ってください。

- 1. DHCP サーバーのあるネットワークにスイッチを接続する。
- 2. スイッチに AC アダプターを接続して電源を入れます。GS108T,の場合は、ポート1を PoE スイッチの給電ポートに接続して電源を入れることもできます。
- 3. Windows コンピュータに Smart Control Center をインストールします。
- 4. Smart Control Center を起動します。
- 5. Discover ボタンを クリックしてスイッチを検索します。下の図 1 のような画面が表示されます。

Product	MAC Address	IP Address	System	Location	DHCP	Subnet Mask	Gateway	Firm W
G\$108Tv2	00:24:b2:5c:96:49	10.131.12.174			Enabled	255.255.255.0	10.131.12.1	10.26.1.3
	11 ma					4		
	DHCP Refr	esh Rel	boot Device	Web Browser /	Access	Configure Device	Change	Password

図 1. Smart Switch Discovery

6. 表示されている DHCP サーバーから割り当てられた IP アドレスをメモします。Web ブラウ ザを使ってスイッチに直接接続するにはこの IP アドレスが必要です。(Smart Control Center を使わない場合)

Networ	Mainter	nance Ta	asks I	Help	
evice List					
evice List Product	MAC Address	IP Address	System	Location	DHCP

7. スイッチが表示されている行をクリックして選択し、Web Browser Access ボタンをクリックします。下図のような Smart Control Center の Login 画面が表示されます。

NETGEAR'		GS108T
Connect with Innovation"		8 Port Gigabit Smart Switch
Login Help		
Sec.		
	: Login	0
	Password ••••••	
	LO	GIN

Web ブラウザを使ってスイッチを管理します。デフォルトのパスワードは password です。このページからスイッチの管理へと進みます。

DHCP サーバーがないネットワークでスイッチを発見する

この章では Smart Control Center を使って DHCP サーバーのないネットワークでスイッチを設定 する方法を記します。お使いのネットワークに DHCP サーバーがない場合、スイッチに固定 IP アド レスを設定する必要があります。DHCP サーバーがあるネットワークでも、固定 IP アドレスを設定 することが可能です。

固定 IP アドレスを設定する

- 1. ネットワークにスイッチを接続します。
- 2. スイッチに AC アダプターを接続して電源を入れます。GS108T,の場合は、ポート1を PoE スイッチの給電ポートに接続して電源を入れることもできます。
- 3. Windows コンピュータに Smart Control Center をインストールします。
- 4. Smart Control Center を起動します。
- 5. Discover ボタンを クリックして GS108T または GS110TP を検索します。Smart Control Center はレイヤー2 Discovery パケットをブロードキャストドメインにブロードキャストして、 スイッチを発見します。図1のような画面が表示されます。
- 6. スイッチを選択し、Configure Device ボタンをクリックします。下の図のように画面の下の方 に追加の情報を表示します。

Networ	k Mainten	ance Ta	sks	Help				QUI
)evice List								
Product	MAC Address	IP Address	System	Loca	tion DHCP	Subnet Mask	Gateway	Firm W
G\$110TP	00:24:b2:5c:96:49	10.131.12.174			Enable	255.255.255.0	10.131.12.1	10.26.1.3
	DHCP Ref	resh Re	boot Device	Web B	rowser Access	Configure Device	e Change	Password
		DH	CP I	P Address	10.131.12.174	Subnet Mask	255.255.25	5.0
AC: 00:24:b	2:5c:96:49	• Ena	abled (iateway	10.131.12.1	System Name	e	
		🔵 Dis	abled L	ocation		Current Pass	word	

- 7. Disabled ラジオボタンを選択し、DHCP クライアント機能を無効にします。
- 8. 固定 IP アドレス(IP Address)、ゲートウェイ IP アドレス(Gateway)、サブネットマスク(Subnet Mask)、パスワード(Current Password)を入力し、Apply ボタンをクリックします。

メモ: Smart Control Center を使ってスイッチ設定を変更するときは毎回パスワードを入力する必要があります。デフォルトのパスワードは password です。

パソコンとスイッチが同じサブネット上にあることを確認してください。次に使うときのためにメモしてください。

管理システムのネットワーク設定を構成する

Smart Control Center を使わずにスイッチのネットワーク情報を設定するには、PC やラップトップ コンピュータのような管理システムからスイッチに直接接続します。管理システムの IP アドレスは スイッチのデフォルト IP アドレスと同じサブネットにある必要があります。多くのネットワークでは、 管理システムの IP アドレスをスイッチのデフォルト IP アドレス(192.168.0.239)と同じサブネットに変 更することになります。

Windows で動作する管理システムの IP アドレスを変更するには、図にあるように、ローカルエリア コネクションの TCP/IPv4 プロパティを開きます。これらの設定を変更するには Windows の管理者 権限が必要です。

インターネット プロトコル バージョン 4 (TCP/I	Pv4)のプロパティ <u>? ×</u>
全般	
ネットワークでこの機能がサポートされている場 きます。サポートされていない場合は、ネットワー てください。	合は、IP 設定を自動的に取得することがで -り管理者に適切な IP 設定を問い合わせ
○ IP アドレスを自動的に取得する(O)	
──● 次の IP アドレスを使う(S):	
IP アドレス(I):	192 . 168 . 0 . 200
サブネット マスク(U):	255 . 255 . 255 . 0
デフォルト ゲートウェイ(D):	192 . 168 . 0 . 1
○ DNS サーバーのアドレスを自動的に取得	导する(B)
● 次の DNS サーバーのアドレスを使う(E):	
優先 DNS サーバー(P):	
代替 DNS サーバー(A):	· · ·
▶ 終了時に設定を検証する(L)	
	OK ++>1211

⚠ 警告!

管理システムの IP アドレスを変更すると、他のネットワークへの接続が失われ ます。設定を変更する前に、現在のネットワークアドレス設定をメモしておいてく ださい。

管理システムのネットワーク設定を変更する

- 1. お使いの PC で Windows の TCP/IP プロパティを開きます。
- 2. 管理システムの IP アドレスを 192.168.0.200 のような 192.168.0.0 ネットワーク中のアドレス に設定します。IP アドレスは同じサブネットの中のスイッチと同じアドレスは使えません
- 3. OK をクリックします。

スイッチの固定 IP アドレスを設定する:

- 1. 管理システムのイーサネットポートと GS108T または GS110TP のイーサネットポートのど れかをイーサネットケーブルで接続します。
- 2. PC の Web ブラウザを開き、Web ブラウザのアドレスバーにスイッチの IP アドレスを入力 し、管理インターフェースに接続します。
- 3. スイッチのネットワーク設定をお使いのネットワークに合わせて変更します。
- 4. スイッチのネットワーク設定を変更後、管理システムのネットワーク設定を以前の設定に戻します。

Web アクセス

GS108T および GS110TP の管理インターフェースにアクセスするには、以下の方法のうちーつを

お使いください。:

• Smart Control Center を使い、スイッチを選択して Web Browser Access ボタンをクリックする。

Device List					Cur	rent Network Ad	apter 192.168.	1.9
Product	MAC Address	IP Address	System	Location	DHCP	Subnet Mask	Gateway	Firm W
G\$110TP	e4:f4:c6:e4:bb:38	192.168.1.28			Enabled	255.255.255.0	192.168.1.1	5.4.2.1
	DHCP Ref	resh R	eboot Device	Web Browser	Access	Configure Device	e Change	Password

• Web ブラウザでアドレスフィールドにスイッチの IP アドレスを入力する。

Web アクセスが可能かどうか確認するために、GS108T または GS110TP の IP アドレスに対して PING 応答があるかどうか試してみてください。Smart Control Center を使ってスイッチの IP アドレ スとサブネットマスクを設定した場合は、Web ブラウザのアドレスバーに設定したスイッチの IP アド レスを入力してください。スイッチのデフォルト IP アドレスを変更していないならば、192.168.0.239 を入力してください。

Smart Control Center の Web Browser Access ボタンをクリックするか、Web ブラウザのアドレス バーにスイッチの IP アドレスを入力してスイッチに直接接続すると、次の図のようなログイン画面 が表示されます。

NETGEAR'		GS108T
Connect with Innovation		8 Port Gigabit Smart Switch
Login Help		
	:: Login ()	
	Password	
Convright @ 1996-2009 Netgear @		

図 2. ログイン画面

Smart Control Center ユーティリティ

スイッチの発見、ネットワークアドレス設定に加えて、Smart Control Center は以下のような機能を 持っています。

- ネットワークユーティリティ
- 設定のアップロードとダウンロード
- ファームウェアアップグレード
- タスク管理

ネットワークユーティリティ

Network タブで以下のことができます。

- DHCP 更新(DHCP Refresh)-DHCP サーバーからの IP アドレスの解放および再取得。
- デバイスの再起動(Reboot Device)-選択したデバイスの再起動。
- Web ブラウザアクセス(Web Browser Access) 一選択したデバイスの管理インターフェースへの Web ブラウザでの接続。
- デバイスの設定(Configure Device)—IP アドレス、DHCP クライアントモード、システム名、ロケーションを含むスイッチのネットワーク情報の変更。
- パスワードの変更(Change Password)ーデバイスの新しいパスワードの設定。

Device List								
Product	MAC Address	IP Address	System	Location	DHCP	Subnet Mask	Gateway	Firm W
G\$110TP	e4:f4:c6:e4:bb:38	192.168.1.28			Enabled	255.255.255.0	192.168.1.1	5.4.2.19
	DHCP Ref	fresh	Reboot Device	Web Browser A	ccess	Configure Devic	e Change	Password

デバイスの設定(Configuring the Device)

以下の手順でスイッチの情報を変更します

- 1. スイッチを選択します。
- 2. Configure Device ボタンをクリックします。画面に追加情報が表示されます。

MAC: 00:24:b2:5c:96:49	DHEP Enabled Disabled 	IP Address Gateway Location	10.131.12.166	Subnet Mask System Name Current Password	255.255.255.0
Define the basic configuration.					Cancel Apply

- 固定 IP アドレス、デフォルトゲートウェイ、サブネットマスクを設定、あるいは変更するには、DHCP クライアント機能を無効(disabled)にし、新しい情報を入力します。システム名ロケーションを設定することもできます。
- Current Password 欄にパスワードを入力します。有効なスイッチのパスワードを入力しないと、変更を適用することはできません。スイッチのデフォルトパスワードは password です。
- 5. Apply ボタンをクリックしてネットワーク情報の変更を適用します。

パスワードの変更(Change Password)

- 1. スイッチを選択します。
- 2. Change Password ボタンをクリックします。画面に追加情報が表示されます。

MAC: 00:24:b2:5c:96:49	Current Password:	New Password:
Change the selected device password.		Cancel Apply

- 3. Current Password 欄にスイッチのパスワードを入力します。スイッチのデフォルトパスワードは password です。
- **4.** 新しいパスワードを New Password 欄と Confirm Password 欄に入力します。パスワードは 英数字で最大 20 文字です。
- 5. Apply ボタンをクリックして新しいパスワードに変更します。

設定のアップロードとダウンロード(Configuration Upload and Download)

スイッチを変更すると、設定情報はスイッチ中のファイルに保存されます。設定ファイルをスイッチ から管理システムにアップロードすることによって設定をバックアップすることができます。保存さ れた設定ファイルを管理システムからスイッチにダウンロードすることもできます。スイッチにダウ ンロードされた設定ファイルは実行中の設定に上書きされます。

設定のアップロードとダウンロードは変更を行う前に現在のスイッチの設定のコピーを保存(設定 のアップロード)しておきたいときに役に立ちます。設定が気に入らない場合、保存しておいた設定 ファイルをダウンロードして、設定を復元することができます。

現在のスイッチの設定を保存する

1. Maintenance タブをクリックして、設定を保存したいスイッチを選択します。

	Product	MAC Address	IP Address	System	Location	DHCP	Subnet Mask	Gateway	Firm W
-	GS110TP	e4:f4:c6:e4:bb:38	192.168.1.28			Enabled	255.255.255.0	192.168.1.1	5.4.2.19
T									

- 2. Upload Configuration ボタンをクリックします。
- 8. 設定ファイルを保存したいフォルダーを選択し、フォルダーの選択ボタンを押します。

Image: Section	SmartControlCenter			
Network Mail Select 1 folder to store the configuration file. Quit Configuration 1 Fire ・ 3/7391・ドキュント・Test ・ 20 Test0/kk# 1.3 Device Maintenance ※ お気に入り ● 第一日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日	NETGEAR * Connect with Innovation*			
Configuration Firm 1.9 Device Maintenance	Network Mai	Select a folder to store the configuration (アンド・アンド・Test	on file. 区 又 任 Testの検索	п
Product MAC Add Fmm W CS110TP e5nfacCer ライラリ 検索条件に一致する項目はありません。 5.4.2.18 ビアオーショー ビアオーショーシー ションピューシー ションピューシー ションピューシー シロクシャ ビアオーシー シロクシャ シロシック シロシック シロクシャ シロシック シロシック シロシック シロシック シロクショー シロクショー ア シロシック シロシック シロクショー シロクショー Test フォルダー ア ワタンパク画 マンパンター マンパンター ア シロシック Upload Configuration Download Configuration Download Configuration	Configuration Firm Device Maintenance	整理 ▼ 新しいフォルダー	≣ ▼	
フォルダー: Test フォルダーの選択 キャンセル Upload Configuration Download Configuration	Product MAC Add	★ お気に入り ライブラリ ドキュメント ビクチャ ビクチャ ビナオ シュージック シュージック シュージック シュージック ショージック ショー	▲ 名前 × 良 裕前 × 良 検索条件に一致する項目はありません。 ▼ 4 ▶	
		フォルダー: Test	フォルダーの選択 キャンセル	
Upload the selected device configuration to the PC.	Upload the selected device conf	iguration to the PC.	Cancel Apply	

3. スイッチのパスワードを入力して Apply ボタンをクリックします。

設定ファイルは管理システムのコンピュータに*.cfgというようなファイル名でアップロードされます。テキストエディタで設定ファイルを開いて中身を見ることができます。

保存した以前の設定を復元する:

- 1. Maintenance タブをクリックして設定を復元したいスイッチを選択します
- 2. Download Configuration ボタンをクリックします。

- 3. 設定ファイルの選択ウィンドウが表示され、スイッチにダウンロードしたい設定ファイルを選択します。
- 4. **開く**ボタンをクリックします。
- 5. スイッチのパスワードを入力し、Apply ボタンをクリックしダウンロードを開始します。

日時を決めて設定ファイルをダウンロードすることもできます。ダウンロード時間を遅らせるには、 Run Now? チェックをはずし、ダウンロードを行う日時を記入します。

maru	ControlGen	ter							
N Conn	ETGE								
N	letwork	Maintenan	ice Tasl	ks Adapt	er Hel	p			QUIT
	Configur	ation Firmware				Cur	rent Network Ac	lapter 192.168.	1.9
Dev	vice Mainte	nance							
	Product	MAC Address	IP Address	System	Location	DHCP	Subnet Mask	Gateway	Firm W
1	GS110TP	e4:f4:c6:e4:bb:38	192.168.1.28			Enabled	255.255.255.0	192.168.1.1	5.4.2.19
						Uplo	ad Configuration	Download Co	nfiguration
								Date 9/26/201	15 📰
MAC	:e4:f4:c6:e	4:bb:38	C	urrent Password:	******		Run Now?	Time	
C:∖U	sers \ Kashir	nura\Dropbox\Work\	Temp\dev_e4f4c6	e4bb38.cfg				1:33	pm 💌
ownl	oad a config	uration to the selecte	d device.					Cancel	Apply
opyr	ight @ 2009	-2013 Netgear ®							

メモ: Tasks タブをクリックして設定のダウンロード状況を確認することができます。

Network	Maintenan	ce Ta	sks	Adapter Help	QUIT
					Current Network Adapter 192.168.1.9
Task Management		Fro	m 09/19	/2015 To :	10/17/2015
MAC Address	System	Date	Time	Task Name	Task Status
e4:f4:c6:e4:bb:38		09/26/2015	1:21 pm	upload configuration	File transfer internal error.
e4:f4:c6:e4:bb:38		09/26/2015	1:22 pm	upload configuration	Successfully completed.
e4:f4:c6:e4:bb:38		09/26/2015	1:23 pm	upload configuration	Successfully completed.

ファームウェアアップグレード

GS108T/GS110TP スマートスイッチのアプリケーションソフトウェアはアップグレード可能です。ア ップグレード手順とそれのために必要な装置をこの章に記します。ファームウェアアップグレードフ ァイルをダウンロードあるいは入手してコンピュータに保存しておいてください。ここでの手順はコン ピュータからスイッチへ TFTP プロトコルを使って転送を行います。

メモ: Web 管理インターフェースで TFTP ダウンロードまたは HTTP ダウンロード機能を 使ってアップグレードをすることもできます。

ファームウェアをアップグレードする:

- 1. Maintenance タブをクリックし、 その下の Firmware リンクをクリックします。
- 2. アップグレードするスイッチを選択し、Download Firmware ボタンをクリックします。
- 3. 表示された Select new firmware ウィンドウで、スイッチにダウンロードするファームウェア ファイルを選択します。
- 4. 開くボタンをクリックします。

🗑 Smar	rtControlCen	ter							
N	ETGE	AR*	Так	Helt					
	C		ICe Task	is Their	,				(2011)
-	Contryure	acioni i Firmware							
De	vice Mainte	nance		5 M 10 M 1	10 20			testes.	
	Product	MAC Address	IP Address	System	Location	DHCP	Subnet Mask	Gateway	FirmW
1	G\$108Tv2	00:24:b2:5c:96:49	10.131.12.69			Enabled	255.255.255.0	10.131.12.1	9.6.15.10
	G\$724Tv3	00:00:00:01:15:ff	10.131.12.162			Enabled	255.255.255.0	10.131.12.1	5.0.2.5
	FS728TP	30:46:9a:ff:fc:05	10.131.12.67			Enabled	255.255.255.0	10.131.12.1	5.0.2.1
	FS728TPv2	30:46:9a:ff:fb:ff	10.131.12.164			Enabled	255.255.255.0	10.131.12.1	N/A
MA C:\ Dow	C: 00:24:b2:5 Documents a mload firmwa	c:96:49 nd Settings\Administ re to the selected dev	Downly Prir Sec rator\Desktop\G\$1 rice.	oad to primary o mary Storage condary Storage .08T3v0m3.stk	r secondary story ✓ Run this	age? FW after dow	nload	Cancel	Apply Apply
C:\ Dow	Documents a mload firmwa	nd Settings\Administ re to the selected dev 2010 Netgear @	rator\Desktop\GS1 vice.	08T3v0m3.stk				Cancel	Apply

デフォルトでは、ファームウェアはプライマリーの保存エリアにダウンロードされ、ダウンロード 終了後の再起動後にアクティブなファームウェアとなります。ファームウェアをバックアップとし てダウンロードするには、Secondary Storage オプションを選択してください。ダウンロードした ファームウェアが即アクティブになるのを防ぐためには、Run this FW after download の選択を 外してください。

メモ: NETGEAR は冗長化のためにプライマリーとセカンダリーの両方に同じファームウ

ェアをダウンロードすることを推奨します。

- 5. Apply ボタンをクリックします。
- ファームウェアダウンロードを実行するためにスイッチのパスワードを入力します。
 日時を決めてファームウェアのダウンロードとインストールをすることもできます。アップグレード時間を遅らせるには、Run Now? チェックをはずし、アップグレードを行う日時を記入します。
- 7. Apply ボタンをクリックしてファームウェアをスイッチにダウンロードし、新しいファームウェア にアップグレードします。
- 8. ダウンロードとアップグレードが完了後、スイッチは自動的に再起動します。

メモ: Tasks タブをクリックしてファームウェアアップグレードの状態を確認することができます。

警告!

ファームウェアアップグレード実行中に管理システムおよびスイッチの電源を切らないでください。

タスク管理

Tasks タブから、実行済み、実行中、および今後実行する予定の設定のダウンロードおよびファームウェアアップグレードの情報を見ることができます。選択したタスクの削除および予定の変更をすることもできます。次の図は Tasks ページの表示例です。

Network	Maintena	nce	Tasks Help	
Fask Management	2		From 11/06/2009	To 12/04/2009
MAC Address	Date	Time	Task Name	Task Status
00:24:b2:5c:96:49	11/13/2009	10:04 pm	upload configuration	TFTP is in progress
00:24:b2:5c:96:49	11/13/2009	10:29 pm	download configuration	Successfully completed
00:24:b2:5c:96:49	11/13/2009	10:50 pm	upload configuration	TFTP is in progress
00:24:b2:5c:96:49	11/20/2009	1:00 am	download configuration	Command is on schedule
00:24:b2:5c:96:49	11/30/2009	2:00 am	upgrade firmware	Command is on schedule
				Delete Task Reschedule

Tasks ページのコマンドボタンは以下の通りです。

- Delete Task(タスクの削除)ーリストから実行済みあるいは予定されているタスクを削除する。
- Reschedule(スケジュール変更)ー実行予定のファームウェアアップグレードや設定のダウン ロードの実行日時を変更する。
- Select Range(期間選択)-実行済みおよび実行予定のタスクから指定した期間のタスクを 選択する。

ユーザーインターフェースを理解する

スイッチソフトウェアは以下の方法のうちの一つを使ってシステムの設定と監視をする包括的な管理機能を含んでいます。

- Web ユーザーインターフェース
- Simple Network Management Protocol (SNMP)

標準に基づいたそれぞれの方法によって、スイッチソフトウェアの構成要素を設定および監視ができます。お使いになる方法はお使いのネットワークの大きさと要件、およびお使いになる方の好み によります。

GS108T/GS110TP スマートスイッチソフトウェア管理マニュアルは Web ベースインターフェースを使って システムの管理と監視をする方法を記しています。

Web インターフェースを使う

Web ブラウザを使ってスイッチにアクセスするには、ブラウザは以下のソフトウェア要素を満たす 必要があります。

- HTML version 4.0, またはそれ以上
- HTTP version 1.1, またはそれ以上
- Java Runtime Environment 1.6 またはそれ以上

Web インターフェースにログインする

- 1. Web ブラウザを開き、アドレスバーにスイッチの IP アドレスを入力します。
- 2. スイッチのデフォルトパスワードは password です。ログイン画面のパスワード欄にパスワードを入力します。パスワードは大文字と小文字を区別します。
- 3. システム認証の後、システム情報(System Information)ページが表示されます。
- 9. 図 3 はスマートスイッチ Web インターフェース画面です。

デーションタブ フィー	チャーリンク	ヘル	ノプタブ	ログアウトボタン
NETGEAR Connerwith Innovation System Switching Management Device View SN	QoS Security /	Monitoring Maintenance	Help	GS110TP 3 Port Gigabit PoE Smart Switch with 2 Fiber SPP LOCOUT
System Information IP Configuration Time	System Information System Information	i		•
 > Denial of Service > DNS > Green Ethernet Configuration 	System Name System Location System Contact Serial Number System Object ID Date & Time System Up Time Base MAC Address	1.3.6.1.4.1.4526.100.4.19 Jan 01 1970 22:04:40 0 days 22 hours 4 mins 40 secs 00:24:82:E3:02:57		
	Versions			0
	Model Name GS110TP	Boot Version	Software Vers	sion
	<	Ш		 >
Copyright © 1996-2009 Netgear ®			REF	RESH CANCEL APPLY

ページメニュー 設定状況とオプション

図 3. 管理ページ画面

ナビゲーションタブ、フィーチャーリンクとページメニュー

Web インターフェースの上部のナビゲーションタブによって様々なスイッチ機能にすぐにアクセスすることができます。タブはいつでもアクセス可能で、設定項目によらず場所も一定です。

タブを選択すると、タブのすぐ下にタブに関連する機能がリンクとして表示されます。青いバーの中 のフィーチャーリンクは選択したナビゲーションタブに連動して変わります。

各機能の設定ページはページの左側のページメニュー中のリンクとして利用可能です。いくつかのメニューの項目はさらに展開されて複数の設定ページを表示します。複数の設定ページを含む メニューの項目をクリックすると、項目は下向き矢印が先頭に表示され、下に展開された追加のペ ージが表示されます。

System Information
IP Configuration
IPv6 Network Configuration
> IPv6 Network Neighbor
* Time
» SNTP Global Configuration
» SNTP Server Configuration
Denial of Service
> DNS
Green Ethernet

図 4. メニュー構造

設定とモニターオプション

フィーチャーリンクの真下とページメニューの右側には設定情報あるいは選択したページの状態 が表示されます。設定オプションを含むページでは、情報を入力し、ドロップダウンメニューからオ プションを選択することができます。

それぞれのページは表示された情報と設定オプションの説明をする HTML ベースのヘルプへのア クセスボタンがあります。各ページにはコマンドボタンもあります。

ボタン	機能
Add(追加)	Add ボタンをクリックして入力した情報を追加する。
Apply(適用)	Apply ボタンを押して更新した情報をスイッチに送ります。変更は即時に有効になります。
Cancel(キャンセル)	Cancel ボタンを押して画面の設定をキャンセルし、画面上の情報を最新のスイッチの値に 戻します。
Delete(削除)	Delete ボタンを押して選択した項目を削除します。
Refresh(更新)	Refresh ボタンを押してデバイスの最新の情報を表示させます。
Logout(ログアウト)	Logout ボタンを押してセッションを終了します。

以下の表に Web インターフェースのページで使われるコマンドを示します。

デバイスビュー(Device View)

デバイスビュー(Device View)はスイッチのポートを表示する Java[®] applet です。このグラフィックは 設定とモニターオプションへのもうーつのアクセス方法を提供します。グラフィックはスイッチのポ ートの情報、現在の設定および状態、テーブル情報、機能要素も提供します。

デバイスビュー(Device View)は System > Device View で表示されます。

ポートの色はポートがアクティブかどうかを示します。緑色の時はポートが有効、赤の時はポート でエラーが発生しているか、リンクが無効になっています。

以下の図は GS108T のデバイスビューです。



以下の図は GS110TP のデバイスビューです。



ポートをクリックすると、ポートの統計や設定のオプションを表示します。メニューオプションをクリッ

クして設定やモニターオプションのページにアクセスできます。

IETGE	AR'				GS108 8 Port Gigabit Smart Switc
System	Switching QoS Security	Monitoring	Maintenance	Help	LOGOUT
Management	Device View SNMP LLDP Service:				
Devic	View				
	- Kaka Manada - Caraliak	2			
NETGE	A R 100M 10M Mila-ACT	ProSa	FE GS108T		
-					
Prosent Barbard	Port Configuration	7	8 Pottory Defaulte		
	Port Summary Statistics				
	Spanning Tree Port Configuration/Stat	JS			
	VLAN Port Configuration				
	Auto-VoIP Port Configuration				
	ISMI Shooping				
	Port Security Interface Configuration				
	Port Security Interface Configuration Port Security Static				

ポート以外の部分をクリックすると、以下の図のようなメインメニューが表示されます。このメニュー は、ページ上部のナビゲーションタブのメニューと同じものです

I E T G E	AR'					GS108
Inder with Inflore	11011					8 Port Gigabit Smart Swi
System	Switching	QoS Securit	y Monitoring	Maintenance	Help	LOGOL
Management	Device View	SNMP LLDP Serv	ices	U		
Devic	e View					
NETGE	AR	Baths1000M On-Link	PROSA	FE GS108T		
		الد فالد فالد د	e alle alle a			
Present	System			•		
	Switching	► Ports ►	6 7	8 Defoults		
	QoS	LAG LAG				
	Security	VLAN +	Basic + VLAN C	onfiguration		
	Monitoring	Auto-VoIP	Advanced + K			
	Maintenance	Voice VLAN				
	Help	STP >				
		Multicast 🕨				
		Address Table >				

ヘルプページ

各ページにはスイッチを設定し管理する際に役に立つオンラインヘルプへのリンク

の
があります。

SNMP を使う

スイッチソフトウェアは SNMP エージェントが生成するトラップを管理する SNMP グループとユーザ 一の設定をサポートしています。

スイッチは標準的な機能のためのスタンダード public MIB と追加のスイッチ機能をサポートする private MIB の両方を使います。すべての private MIB は"-"の文字から始まります。メインのイン ターフェース設定オブジェクトは private MIB である-SWITCHING-MIB に含まれます。いくつかの インターフェース設定は public MIB である IF-MIB に含まれます。

SNMP はデフォルトで有効です。System > Management > System Information Web ページはログ イン成功後に表示され、スイッチをアクセスするための SNMP マネージャーを設定するために必要 な情報を表示します。

どのユーザーも SNMPv3 プロトコルでスイッチにアクセスすることは出来ますが、スイッチはただ 一つのユーザー"admin"のみをサポートし、一つのプロファイルのみが作成され変更可能です。

Web インターフェースを使って SNMPv3 admin プロファイルの認証およ び暗号化を設定する。

1. System > SNMP > SNMPv3 > User Configuration を選択して User Configuration ページを 表示します。

> SNMP ¥1/¥2 * SNMP ¥3	User Configuration				
 User Configuration 	User Configuration				
Configuration	SNMP v3 Access Mode	Read/Write			
	Authentication Protocol	C None	⊙ MD5 € SHA		
	Encryption Protocol	O None	O DES		
	Encryption Key	•••••	*		

- 2. 認証を有効にするために、MD5 または SHA の Authentication Protocol オプションを選択します。
- **3.** 暗号化を有効にするために、Encryption Protocol の DES オプションを選択します。次に英数の 8 文字以上の暗号化コードを Encryption Key 欄に入力します。
- 4. Apply ボタンをクリックします。

SNMPv1 または SNMPv2 の設定情報にアクセスするには、System > SNMP > SNMPv1/v2 を選択します。

インターフェース命名規則

スイッチは物理および論理インターフェースをサポートします。インターフェースはインターフェース のタイプとインターフェース番号で区別されます。物理ポートはギガビットインターフェースであり、 前面パネルで番号付けられています。論理インターフェースはソフトウェアで設定します。以下の 表では、スイッチで利用可能なすべてのインターフェースの命名規則を示します。

インターフェース	説明	例
物理	物理ポートはギガビットインターフェースであり、1か ら順番に番号が付いています。	g1, g2, g3
LAG(Link Aggregation Group)	LAG インターフェースは論理インターフェースで ブリッジング機能にのみ使われます。	I1, I2, I3 LAG1, LAG2
CPU 管理インターフェース (CPU Management Interface)	これはスイッチ内部のインターフェースでスイッチ の基本 MAC アドレスを管理します。このインターフ ェースは設定不可で、常に MAC アドレステーブル に表示されます。	c1

2.システム設定

System(システム)タブの機能を使ってスイッチの環境との関係を定義します。System タブは以下の機能へのリンクを含んでいます。

- Management(マネージメント)
- PoE (GS110TP のみ)
- SNMP
- LLDP

Management(マネージメント)

この章ではスイッチの状態をどのように表示し、マネージメントインターフェースの IP アドレス、シ ステムクロック設定、DNS 情報のようなスイッチの基本情報を記述するかを記します。 Management リンクから、以下のページにアクセスできます。

- システム情報(System Information)
- IP 設定(IP Configuration)
- IPv6 設定(IPv6 Configuration)
- IPv6 近隣情報(IPv6 Network Neighbor)
- 時間(Time)
- Denial of Service(DoS)
- DNS
- グリーンイーサネット設定(Green Ethernet Configuration)

システム情報(System Information)

ログイン成功後、システム情報(System Information)ページが表示されます。このページでデバイ スの一般情報を設定、表示します。

システム情報(System Information)ページを表示するには、System > Management > System Information をクリックします。以下のような画面が表示されます。

NETGEAR [.]					GS108T
Connect with Innovation™				8 Poi	rt Gigabit Smart Switch
System Switching	QoS Security	Monitoring	Maintenance	Help	LOGOUT
Management Device View St	NMP LLDP Services			СС СС	
System Information In Configuration	System Informat	tion			^
> Time	System Informati	on			1
 > Denial of Service > DNS > Green Ethernet Configuration 	System Name System Location System Contact Serial Number System Object ID Date & Time System Up Time Base MAC Address	1.3.6.1.4 Jan 03 1 2 days 6 00:24:82	.1.4526.100.4.18 970 06:07:44 hours 7 mins 44 secs 1:5C:96:49		E
	Versions	Reat Va		Software Version	•
	GS108Tv2	5.0.3.2	rsion	10.28.11.23	
	[4]		101		
	(*)			REFRESH	CANCEL APPLY

システム情報を設定する

1. System > Management > System Information を選択してシステム情報(System

Information)ページを開きます。

- 2. 以下の項目を記入します。
 - システム名(System Name):スイッチを識別するための名前を入力します。最大 31 文 字までの英数字が使えます。デフォルトは(空白)です。
 - システムロケーション(System Location): スイッチの設置場所を入力します。最大 31 文 字までの英数字が使えます。デフォルトは(空白)です。
 - システムコンタクト(System Contact):スイッチの担当者を入力します。最大 31 文字ま での英数字が使えます。デフォルトは(空白)です。
- 3. Apply ボタンをクリックします。

入力したシステムパラメーターが適用され、デバイスが更新されます。

以下の表にシステムページに表示される情報を示します。

項目	説明
Serial Number	スイッチのシリアル番号
System Object ID	スイッチのエンタープライズ MIB のベースオブジェクト ID
Date & Time	現在の日時
System Up Time	再起動時からの稼働時間
Base MAC Address	システムの MAC アドレス
Model Name	スイッチのモデル名
Boot Version	スイッチのブートコードバージョン
Software Version	スイッチのソフトウェアバージョン

IP 設定(IP Configuration)

IP 設定ページを使い、スイッチ前面のどのポートからでもスイッチとのインバンド通信をするため に使われる論理インターフェースである管理インターフェースのネットワーク情報を設定します。ス イッチのネットワークインターフェースに関連する設定パラメータは前面パネルのポート設定に影 響はありません。

NETGEAR' Connect with Innovation			GS 11 OTP 8 Port Gigabit PoE Smart Switch with 2 Fiber SFP
System Switching	QoS Security Monito	oring Maintenance Help	LOGOUT
Management Device View PoE	SNMP LLDP Services		
System Information	IP Configuration		·
* IP Configuration * Time	IP Configuration	۲	
 Denial of Service DNS Green Ethernet Configuration 	 Dynamic IP Address (DHCP) Dynamic IP Address (BOOTP) Static IP Address 		
	IP Address	10.27.65.165	
	Subnet Mask Default Gateway	255.255.254.0	
			Ξ.
	Management VLAN	•	
	Management VLAN ID 1	(1-4093)	
	[]		()
			CANCEL APPLY

管理インターフェースのネットワーク情報を設定する

- 1. System > Management > IP Configuration を選択して IP Configuration ページを表示しま す。
- 2. スイッチの管理インターフェースのネットワーク情報を設定するために適当なラジオボタンを 選択します。
 - Dynamic IP Address (DHCP): DHCP サーバーからスイッチの IP アドレスを割り当てます。
 - Dynamic IP Address (BOOTP): BootP からスイッチの IP アドレスを割り当てます。
 - Static IP Address: IP アドレス、サブネットマスク、デフォルトゲートウェイを固定で設定 します。情報を記入します。
- 3. Static IP Address オプションを選択した場合、以下の情報を入力します。
 - IP Address: ネットワークインターフェースの IP アドレス。デフォルトの IP アドレスは 192.168.0.239 です。
 - Subnet Mask: インターフェースのサブネットマスク。デフォルト値は 255.255.255.0 です。
 - Default Gateway: IP インターフェースのデフォルトゲートウェイ。デフォルト値は 192.168.0.254 です。
- 4. 管理 VLAN の VLAN ID を記入します。

管理 VLAN は同じ VLAN に属するポートに接続されているワークステーションがスイッチに 接続する IP コネクションをするために使われます。指定されない場合は、有効な管理 VLAN ID はどのポートから IP 接続可能な1 (デフォルト)です。

管理 VLAN に異なる値を設定した場合は、管理 VLAN に所属するポート経由でのみ IP 接続が可能になります。また、管理 VLAN に接続されるポートの PVID(ポート VLAN ID)は管理 VLAN の ID と同じでなければいけません。

管理 VLAN の必要条件は以下の通り。

- 有効な管理 VLAN は一つだけです。
- 新しい管理 VLAN が設定されると、既存の管理 VLAN での接続性は失われます。
- 管理端末は新しい管理 VLAN のポートに接続する必要があります。

メモ: 管理 VLAN が必ず有効になるようにしてください。最低一つのポートの PVID を管理 VLAN ID に合わせてください。

- 5. ネットワーク接続設定を変更した場合は、Apply ボタンをクリックして変更をシステムに適用 します。
- 6. キャンセルする場合は Cancel ボタンをクリックします。

IPv6 設定(IPv6 Configuration)

IPv6 設定ページを使い、スイッチ前面のどのポートからでもスイッチとのインバンド通信をするために使われる論理インターフェースである管理インターフェースのネットワーク情報を設定します。 スイッチのネットワークインターフェースに関連する設定パラメータは前面パネルのポート設定に 影響はありません。



IPv6 ネットワーク情報を設定する。

- 1. System > Management > IPv6 Network Configuration を選択して IPv6 Network Configuration ページを表示します。
- 2. Admin Mode: 有効(Enable)、無効(Disable)を選択します。
- 3. IPv6 Address Auto Configuration Mode:このモードを有効(Enable)にすると、IPv6 アドレス を IPv6 NDP(Neighbor Discovery Protocol)およびルーターアドバータイズメントメッセージの 使用で取得します。
- 4. Current Network Configuration Protocol:DHCPv6 を有効(Enable)にすると,DHCPv6 クライ

アントがスイッチで有効になります。

- 5. IPv6 Gateway:IPv6 ネットワークのデフォルトゲートウェイアドレスを入力します。
- 6. IPv6 Prefix/Prefix Length:スタティック IPv6 プレフィクスを設定します。フォーマットはグロー バルアドレスフォーマットです。
 - EUI64: EUI(Extended Universal Identifier)フラグを有効にするには True を選択します。
 - Add ボタンをクリックします。
 - IPv6 Prefix/Prefix Length を削除するには、削除する項目のチェックボックスを選択し、 Delete ボタンをクリックします。
- 7. 設定を変更後、Apply ボタンをクリックします。
- 8. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。

IPv6 近隣情報(IPv6 Network Neighbor)

IPv6 Network Neighbor ページを使い、IPv6 の近隣情報を確認することができます。

NETGEAR [*] Connect with Innovation ^{**}					8	(Port Gigabit P	OS 110TP oE Smart Switch with 2 Fiber SFP
System Switching	QoS S	ecurity M	onitori	ng Mai	ntenance	Help	LOGOUT
Management Device View	PoE SNMP	LLDP Services	;				
> System Information	IPv6 Netw	ork Interfac	e Nei	ghbor Tab	ole		~
> IP Configuration > IPv6 Network Configuration	: IPv6 Netv	vork Interface	Neighb	or Table		(?)	
 IPv6 Network Neighbor Time 	IPv6 Address	MAC Address	isRtr	Neighbor State	Last Up	dated	
> Denial of Service							
Green Ethernet							
							~
	<						>
						CLEAR	REFRESH
Copyright © 1996-2015 NETGEAR	8						

IPv6 近隣情報を確認する。

System > Management > IPv6 Network Neighbor を選択して IPv6 Network Neighbor Interface Table ページを表示します。

以下に IPv6 Network Neighbor Interface Table 欄に表示される情報の説明を示します。

項目	説明
IPv6 Address	近隣ノードの IPv6 アドレス。
MAC Address	インターフェースの MAC アドレス

IsRtr	近隣ノードがルーターの場合は True、ルーターでない場合は False。			
Neighbor State	 近隣キャッシュエントリー(Neighbor Cache Entry)の状態。 Reach:近隣ノードに到達可能。 Stale:近隣ノードが到達可能か不明になった。 Delay:近隣ノードからの応答が遅れている。 Probe:近隣ノードの到達可能性確認中。 Unknown:不明。 			
Last Updated	近隣ノードが最後に確認されてからの時間。			

時間(Time)

スイッチソフトウェアは SNTP(Simple Network Time Protocol)をサポートしています。手動でシス テム時間を設定することも出来ます。

SNTP は 1/1000 秒単位での正確なネットワーク機器の時間同期を実現します。時間同期はネット ワークの SNTP サーバーによって実行されます。スイッチソフトウェアは SNTP クライアントとして のみ動作し、他のシステムに時間を提供することはできません。

時間基準はストラタム(Stratum)で表されます。ストラタムは参照クロックの精度を定義します。スト ラタムが高い(0 が最高)と、クロックの精度も高くなります。ストラタム 1 かそれ以上の時間を受信 するデバイスはストラタム 2 のデバイスとなります。

以下にストラタムの例を示します。

- Stratum 0: GPS システムのようなリアルタイムクロックがクロックソースとして使われています。
- Stratum 1:ストラタム 0 のタイムソースに直接接続されているサーバーです。ストラタム 1 のタイムサーバーは主要なネットワーク時間基準を提供しています。
- Stratum 2: タイムソースをストラタム 1 サーバーからネットワーク経由で受信しています。
 例えば、ストラタム 2 サーバーはストラタム 1 サーバーからネットワーク経由で NTP を使って時間を受信しています。

SNTP サーバーから受信した情報は時間の精度レベルとサーバーのタイプに基づいて評価されます。

SNTP の時間定義は以下の時間レベルによって評価され、定義されます。

- T1: クライアントが要求メッセージを送信した時間。
- T2: サーバーが要求メッセージを受信した時間。
- T3: サーバーが応答メッセージを送信した時間。
- T4: クライアントが応答メッセージを受信した時間。

IP アドレスがわかっているサーバーにユニキャストでポーリングする方法が使われます。同期の ためにはデバイスに設定された SNTP サーバーのみにポーリングが行われます。サーバー時間 を決定するために T1~T4 が使われます。これがデバイスの時間を同期させる一番の確実な方法 です。この方法では、SNMP サーバー設定ページで設定された SNTP サーバーからの情報のみ が使われます。

デバイスは自発的に要求、あるいは定期的にポーリング要求をして得られた情報を使って同期情 報を取得します。

時間設定(Time Configuration)

時間設定(Time Configuration)ページで日付と時間の設定を確認、調整します。

NETGEAR'			GS108T
Connect with Innovation "			8 Port Gigabit Smart Switch
System Switching	QoS Security Mo	nitoring Maintenance Help	LOGOUT
Management Device View SN	MP LLDP Services		
	T 0 C 1		
System Information	Time Configuration		
* Time	Time Configuration	3	
SNTP Global Configuration	Clock Source	Local OSNTP	
» SNTP Server Configuration	Date	00/00/0000 (DD/MM/YYYY)	
> Denial of Service	Time	08:28:21 (HH:MM:SS)	
Green Ethernet Configuration	Time Zone	UTC 00:00 🛩	
	SNTP Global Status	0	
	Version	4	
	Supported Mode	Unicast	
	Last Update Time	Jan 01 00:00:00 1970	
	Last Attempt Time	Jan 01 00:00:00 1970	
	Last Attempt Status	Other	
	Server IP Address		
	Address Type	Unknown	
	Server Stratum	0 - Unspecified	
	Reference Clock Id		
	Server Mode	Reserved	
	Unicast Server Max Entries	3	
	Unicast Server Current Entries	c	
			~
	(III	>
			REFRESH CANCEL APPLY

スイッチの時間をクロックソースとして使う

- 1. System > Management > Time > SNTP Global Configuration を選択して Time Configuration ページを表示します。
- 2. Clock Source: Local を選択します。
- 3. Date: DD/MM/YYYY 形式で年月日を記入します。
- 4. Time: HH:MM:SS 形式で時間を記入します。

メモ:日付と時間を入力しない場合は、スイッチが使っている時間設定を使うことになります。

Clock Source(時間基準)を Local に設定すると、Time Zone(タイムゾーン)欄はグレー(無効)になります。

5. Applyをクリックして設定をスイッチに適用します。すぐに設定変更がされます。

SNTP で時間を設定する

1. From the Clock Source field, select SNTP.

Clock Source(時間基準)を SNTP に設定すると、Date と Time 欄はグレー(無効)になります。スイッチは日付と時間をネットワークから受信します。

- **2.** スイッチ設置場所に合わせて協定世界時(UTC)との時間差を Time Zone に 設定します。 日本国内は UTC+09:00 です。
- 3. Applyをクリックして設定をスイッチに適用します。すぐに設定変更がされます。
- **4.** SNTP Server Configuration ページで SNTP サーバー設定をします。
- 5. Refresh ボタンをクリックしてスイッチの最新時間情報を表示させます。
- 6. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。

Time Configuration ページの SNTP Global Status はスイッチの SNTP クライアント情報を示します。

* SNTP Global Status	(3
Version	4	
Supported Mode	Unicast	
Last Update Time	Sep 27 13:02:50 2015	
Last Attempt Time	Sep 27 13:02:50 2015	
Last Attempt Status	Success	
Server IP Address	133.243.238.163	
Address Type	IPv4	
Server Stratum	1 - Primary Reference	
Reference Clock Id	NTP Ref: NICT	
Server Mode	Server	
Unicast Server Max Entries	3	
Unicast Server Current Entries	1	

以下の表は SNTP Global Status の項目について記します。

項目	説明
Version	クライアントのサポートする SNTP バージョン。
Supported Mode	クライアントのサポートする SNTP バージョン。複数のモードがサポ ートされる場合もあります。
Last Update Time	SNTP クライアントの最新のシステムクロック更新時間。
Last Attempt Time	最新の SNTP 要求メッセージの送信あるいは応答メッセージの受 信時間。

Field Description	
-------------------	--

Last Attempt Status	最新の SNTP 要求メッセージの送信あるいは応答メッセージの受 信状態。サーバーから応答メッセージがない場合は Other が表示 されます。すべての動作モードで以下の値が使われます。 • Other: 以下のどれにも当てはまらない場合。 • Success: SNTP が正常に動作し、システムクロックが正常 に更新されました。 • Request Timed Out: SNTP サーバーからの応答メッセージ がタイムアウトしました。 • Bad Date Encoded: SNTP サーバーから受信した情報が
Server IP Address	有効なサーバーからのメッセージを受信したサーバーの IP アドレ ス。サーバーからメッセージを受信していない場合は空白。
Address Type	SNTP サーバーのアドレスタイプ。
Server Stratum	SNTP サーバーのストラタム。
Reference Clock Id	参照クロック ID.
Server Mode	SNTP サーバーのモード。
Unicast Sever Max Entries	クライアントのユニキャスト SNTP 要求の最大再送可能数。
Unicast Server Current Entries	クライアントに設定している SNTP サーバー数。

Refresh ボタンをクリックしてページの表示情報を最新に更新します。

SNTP サーバー設定(SNTP Server Configuration)

SNTP Server Configuration ページで SNTP(Simple Network Time Protocol)サーバー設定を確認、変更します。

NETGEAR Connect with Innovation							GS110 8 Port Gigabit PoE Smart Sw with 2 Fiber	TP /itch SFP
System Switching	QoS	Security	Monito	ring Ma	intenance	Help	LOGOU	л
Management Device View Po	E SNMP	LLDP	Services					
 System Information IP Configuration 	SNTP Se	erver Co	onfiguratio	on				^
* Time	SNTP S	Server Co						
 SNTP Global Configuration SNTP Server Configuration 	Serv Type	er Ado	lress	Port (1-65535)	Priority (1-3)	Version (1-4)		
Denial of Service DNC	IPV4			123	1	4		
Green Ethernet Configuration	_							
	SNTP S	Server St	atus		III			
	Address	Last Update Time	Last Attempt Time	Last Attempt Status	Requests	Failed Requests		
								~
	<] [:	>
					RE	FRESH ADD	DELETE CANCEL APPLY	

新しい SNTP サーバーを設定する

- 1. SNTP サーバーの情報を欄に入力します。
 - Server Type: SNTP サーバーのアドレスタイプを入力します。IP アドレス(IPv4) または ホスト名 (DNS)です。
 - Address: SNTP サーバーの IP アドレスまたはホスト名を入力します。
 - Port: SNTP サーバーが使うポート番号を指定します。有効な値は 1-65535 です。デフ オルト値は 123 です。
 - Priority: SNTP リクエストが送信されるサーバーの優先度を指定します。1-3 の値で1 が最優先です。デフォルトは1です。
 - Version: プロトコルのバージョン(1-4)を指定します。 デフォルトは 4 です。
- 2. Add.をクリックして SNTP サーバー設定を追加します。
- 3. 上の手順を繰り返して SNTP サーバー情報を追加します。SNTP サーバーは最大3つまで 設定可能です。
- 4. SNTP サーバー設定を削除するには、サーバー設定の先頭のチェックボックスをチェックして、Delete ボタンをクリックします。入力が削除され、スイッチ情報は更新されます。
- 5. 既存の SNTP サーバー設定を更新するには、サーバー設定の先頭のチェックボックスをチェックして新しい値を入力し、Apply.ボタンをクリックします。すぐに設定変更がされます。
- 6. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。
SNTP Server Status の表はスイッチに設定された SNTP サーバーの状態を示します。

:: SNTP Server Status (?)					
Address	Last Update Time	Last Attempt Time	Last Attempt Status	Requests	Failed Requests
133.243.238.163	Sep 27 14:12:13 2015	Sep 27 14:12:13 2015	Success	92	0

SNTP Server Status の表の項目については以下の通り。

項目	説明
Address	すべての SNTP サーバーアドレスを表示します。サーバー設定がない場合は "No SNTP server exists"と点滅表示されます。
Last Update Time	SNTP クライアントの最新のシステムクロック更新時間。
Last Attempt Time	最新の SNTP 要求メッセージの送信あるいは応答メッセージの受 信時間。
Last Attempt Status	 最新の SNTP 要求メッセージの送信あるいは応答メッセージの受信状態。サーバーから応答メッセージがない場合は Other が表示されます。すべての動作モードで以下の値が使われます。 Other: 以下のどれにも当てはまらない場合。 Success: SNTP が正常に動作し、システムクロックが正常に更新されました。 Request Timed Out: SNTP サーバーからの応答メッセージがタイムアウトしました。 Bad Date Encoded: SNTP サーバーから受信した情報が無効。
Requests	スイッチが再起動してからの SNTP 要求メッセージの数。
Failed Requests	スイッチが再起動してからの失敗した SNTP 要求メッセージの数。

Refresh ボタンをクリックしてページの表示情報を最新に更新します。

Denial of Service (DoS)

Denial of Service (DoS) ページで DoS 設定をします。スイッチソフトウェアは特定の DoS 攻撃のタ イプを分類しブロックする機能をサポートしています。スイッチを設定して 6 つのタイプの DoS 攻撃 を監視、ブロックすることができます。

- SIP=DIP: 送信元 IP アドレス =あて先 IP アドレス。
- First Fragment: TCP ヘッダーサイズが指定された値より小さい。

- TCP Fragment: IP フラグメントオフセット = 1。
- TCP Flag: TCP Flag SYN set and Source Port < 1024 or TCP Control Flags = 0 and TCP Sequence Number = 0 or TCP Flags FIN, URG, and PSH set and TCP Sequence Number = 0 or TCP Flags SYN and FIN set.
- L4 Port: 送信元 TCP/UDP ポート =あて先 TCP/UDP ポート。
- ICMP: ICMP Ping パケットの最大長を制限。

自動 DoS 設定(Auto-DoS Configuration)

Auto-DoS Configuration ページでは、スイッチで利用可能な機能のうちで L4 ポート攻撃以外のすべてを有効にすることができます。前項でスイッチがサポートしている DoS 攻撃のタイプについて記しています。

NETGEAR'				GS108T 8 Port Gigabit Smart Switch
System Switching	QoS Security	Monitoring Maintenance	Help	LOGOUT
Management Device View St	NMP LLDP Services			
 System Information IP Configuration 	Auto-DoS Config	juration	(7)	j.
Ornial of Service Auto-DoS Configuration Dos Configuration DoS Configuration ONS Green Ethernet Configuration	Auto-DoS Mode	④ Disable ○ Enable		
	<	//III		(>)
				CANCEL APPLY

Auto-DoS 機能を設定する。

- 1. System > Management > Denial of Service > Auto-DoS Configuration を選択して Auto-DoS Configuration ページを表示します。
- 2. Auto-DoS Mode のラジオボタンを選択します。
 - **Disable**: Auto-DoS を無効にする。(デフォルト)
 - Enable: Auto-DoS を有効にする。
- 3. Apply.ボタンをクリックして変更した設定をスイッチに適用します。すぐに設定変更がされます。
- 4. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。

DoS 設定(DoS Configuration)

DoS Configuration ページによりスイッチで監視、ブロックしたい DoS 攻撃のタイプを選択します。

NETGEAR Connect with Innovation"			GS110TP 8 Port Gigabit PoE Smart Switch with 2 Fiber SFP
System Switching	QoS Security Monitoring	Maintenance Help	LOGOUT
Management Device View PoE	SNMP LLDP Services		
 System Information IP Configuration 	Denial of Service Configuration	on	
 Time SNTP Global Configuration SNTP Server Configuration Denial of Service Auto-Dos Configuration Dos Configuration Dos S Green Ethernet Configuration 	Denial of Service Configuration Denial of Service SIP=DIP Denial of Service First Fragment Denial of Service Min TCP Hdr Size Denial of Service TCP Fragment Denial of Service TCP Flag Denial of Service L4 Port Denial of Service ICMP Denial of Service Max ICMP Size	 Disable C Enable Disable Enable Disable Enable (0 to 255) Disable Enable <li< th=""><th>1</th></li<>	1
	<]		
Copyright © 1996-2010 Netgear ®			CANCEL

DoS 設定をする。

- System > Management > Denial of Service > DoS Configuration をクリックして DoS Configuration ページを表示します。
- 2. 監視およびブロックをしたい DoS 攻撃のタイプを選択し、必要な値を記入します。
 - Denial of Service SIP=DIP. ラジオボタンを選択して機能の有効、無効を選択します。送 信元 IP アドレスと宛先 IP アドレスが一致するパケットを廃棄します。デフォルトは無効 です。
 - Denial of Service First Fragment. ラジオボタンを選択して機能の有効、無効を選択します。TCP ヘッダーが Denial of Service Min TCP Hdr Size に設定された長さよりも短い パケットを廃棄します。デフォルトは無効です。
 - Denial of Service Min TCP Hdr Size. Denial of Service First Fragment.が有効のときに この値より TCP ヘッダーが短いパケットを廃棄します。デフォルト値は 20 バイトです。
 - Denial of Service TCP Fragment. ラジオボタンを選択して機能の有効、無効を選択します。IP fragment offset 値が1のパケットを廃棄します。デフォルトは無効です。
 - Denial of Service TCP Flag. ラジオボタンを選択して機能の有効、無効を選択します。 以下の条件を満たすパケットを廃棄します。TCP flag SYN set and TCP source port less than 1024 or TCP control flags set to 0 and TCP sequence number set to 0 or TCP flags FIN, URG, and PSH set and TCP sequence number set to 0 or both TCP flags SYN and FIN set. デフォルトは無効です。
 - Denial of Service L4 Port. ラジオボタンを選択して機能の有効、無効を選択します。
 TCP/UDP 送信元ポートが TCP/UDP 宛先ポートに等しいパケットを廃棄します。 デフォルトは無効です。
 - Denial of Service ICMP. ラジオボタンを選択して機能の有効、無効を選択します。
 Denial of Service Max ICMP Size に設定された ICMP パケットサイズよりも多きい

ICMP パケットを廃棄します。デフォルトは無効です。

- Denial of Service Max ICMP Size. Denial of Service ICMP.が有効のときに、この値より も大きい ICMP パケットが廃棄されます。0-1023の間で設定でき、デフォルトは 512 バ イトです。
- 3. Apply.ボタンをクリックして変更した DoS 設定をスイッチに適用します。
- 4. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。

DNS

スイッチの DNS クライアント機能の設定をすることができます。

DNS 設定(DNS Configuration)

DNS Configuration ページで DNS サーバー設定をします。

NETGEAR'				GS108T
Connect with Innovation "				8 Port Gigabit Smart Switch
System Switching	QoS Security Monit	toring Maintenance	Help	LOGOUT
Management Device View St	NMP LLDP Services			
 System Information IP Configuration 	DNS Configuration			~
 Time Denial of Service DNS DNS Configuration Host Configuration 	DNS Configuration DNS Status DNS Default Name (0 to 255 characters)	O Disable 💿 Enable	3	_
Green Ethernet Configuration	: DNS Server Configuration		۲	=
	ID	DNS Server		
	<)	IIII		×
			ADD	DELETE CANCEL APPLY
Copyright © 1996-2009 Netgear ®				

DNS 設定をする

- 1. System > Management > DNS > DNS Configuration を選択して DNS Configuration ページ を表示します。
- 2. DNS Status でスイッチの DNS クライアント機能を有効にします。
 - Enable: 有効にしてスイッチが DNS サーバーに DNS クエリを送信して DNS ドメインネームを解決します。
 - Disable: 無効にしてスイッチが DNS クエリを送信しないようにします。
- システムがルックアップを実行する際に DNS default domain name がドメイン名として提供 されます。(test が入力されたとき、デフォルトドメイン名が netgear.com である場合、test は test.netgear.com となります。).
- 4. スイッチが DNS クエリを送信する DNS サーバーの IPv4アドレスを DNS Server Address に入力して Add. ボタンをクリックします。作成した順番に使われます。
- 5. リストから DNS サーバーを削除するには、削除したいサーバーのチェックボックスをクリックして Delete. ボタンをクリックします。

- 6. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。
- 7. Apply.ボタンをクリックして変更した設定をスイッチに適用します。すぐに設定変更がされます。

ホスト設定(Host Configuration)

このページを使ってホスト名と IP アドレスのマニュアルマッピングをしたり、ダイナミックな DNS マッピングの確認をします。

NETGEAR Connect with Innovation		GS110TP 8 Port Gigabit POE Smart Switch with 2 Fiber SFP
System Switching QoS Security Monitorin	g Maintenance Help	LOGOUT
Management Device View PoE SNMP LLDP Services		
 > System Information > IP Configuration > Time > Denial of Service > DNS > DNS Configuration > Host Configuration > Host Configuration > Green Ethernet Configuration Host Total Elapsed 	() IP Address Type IP Address	
<		
Convright @ 1996-2010 Netgear @	CLEAR REFRESH ADD	DELETE CANCEL APPLY

DNS テーブルに固定設定を追加する。

- 1. System > Management > DNS > Host Configuration をクリックして Host Configuration ページを表示します。
- 2. Host Name: 追加したいホスト名を Host Name 欄に記入します。最大 158 文字です。
- 3. IP Address:ホスト名に関連付けたい IP アドレス(IPv4)を記入します。
- 4. Add ボタンをクリックします。下のリストに入力したものが表示されます。
- 5. テーブルから削除するには、削除したいもののチェックボックスをクリックして Delete.ボタン をクリックします。
- 6. ホスト名や IP アドレスを変更したい場合は、チェックボックスをクリックして情報を変更して から Apply ボタンをクリックします。
- 7. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。

Dynamic Host Configuration table はスイッチが学習したホスト名とIP アドレスの関係を表示します。以下に Dynamic Host Configuration の表の項目の説明を記します。

項目	説明
Host	ホスト名
Total	テーブルに追加されてからの総時間。

Elapsed	最新のテーブル更新がされてからの時間。
Туре	追加された情報のタイプ。
Addresses	IP アドレス。

Refresh ボタンをクリックして最新のテーブル情報に更新します。

Clear ボタンをクリックしてダイナミックなホスト情報を削除します。学習した情報が表示されます。

グリーンイーサネット設定(Green Ethernet Configuration)

このページでグリーンイーサネット設定をします。この機能で電源消費を削減できます。

GS108	8 Port G					AR'	NETGE
1060	Help	Maintenance	Monitoring	Security	QoS	Switching	System
	n ar			LLDP Services	SNMP L	Device View	Management
			configuration	en Ethernet C	Gree	rmation	System Info
(onfiguration	reen Ethernet Co	Gr	tion	IP Configura Time
	Enable	🔿 Disable		t Cable Mode	Short	rvice	Denial of Se
					in	net Configuratio	Green Ether
					<		
CANCEL APPLY							
CANCEL						6-2009 Netgear @	apyright @ 199

グリーンイーサネット(Green Ethernet)を設定する。

- 1. System > Management > Green Ethernet Configuration を選択して Green Ethernet Configuration ページを表示します。
- 2. Short Cable Mode を設定する。
 - Enable:スイッチは接続されたケーブルでケーブルテストを行い、ケーブル長が 10m 未満の場合はポートを低消費電力モード(微小電力)にします。
 - Disable:ケーブル長によらず全ポート最大電力で動作します。
- 3. Apply.ボタンをクリックして変更した設定をスイッチに適用します。すぐに設定変更がされます。

PoE (GS110TP のみ)

GS110TP のポート1~8(g1-g8)は IEEE802.3af 対応です。各ポートは 15.4W までの電力を PoE 受電機器(PD)に給電可能です。合計の給電容量(パワーバジェット)は 46W です。ポートの優先 度、タイマー、PD への電力制限等の設定をすることによって GS110TP のパワーバジェットを有効 に使うことができます。

システム(System)タブの下の PoE リンクからポート g1-g8 のポートの PoE の状態を確認したり設定することができます。

PoE リンクから以下のページにアクセスできます。

- PoE 設定(PoE Configuration)
- PoE ポート設定(PoE Port Configuration)
- タイマーグローバル設定(Timer Global Configuration)
- タイマースケジュール設定(Timer Schedule Configuration)

PoE 設定(PoE Configuration)

スイッチの PoE 電力状況を PoE Configuration ページで確認し、SNMP トラップ設定をすることもできます。

メモ: System > PoE > Advanced > PoE Configuration. をクリックしても PoE Configuration ペ ージを表示できます。

nect with Innovation			8 Port Gigabit PoE Smart Switch with 2 Fiber SFP
System S	witching QoS	Security Monitoring Maintenance	Help
Management C	Device View PoE SNMP	LLDP Services	
Basic	PoE Configuration	1	^
	PoE Configuration	۲	
Advanced	Power Status Nominal Power Threshold Power Consumed Power Traps	On 46 Watt 39 Watt 0.0 Watt ④ Disable ○ Enable	E
	<	10	

PoE トラップ設定をする。

- 1. System > PoE > Basic > PoE Configuration を選択して PoE Configuration ページを表示 します。
- 2. Traps のラジオボタンを選択します。
- 3. Apply ボタンをクリックして新しい設定を適用します。
- 4. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。
- 5. Refresh ボタンをクリックして最新の情報に更新します。

PoE Configuration 欄は以下の情報を表示します。

項目	説明
Power Status	PoE 機能が有効か無効かを示します。

Nominal Power	スイッチが供給できる定格電力の総量。
Threshold Power	スイッチが供給できる電力残量。
Consumed Power	現在供給している総電力量。

PoE ポート設定(PoE Port Configuration)

PoE Port Configuration ページでポート単位の PoE 設定をします。

EIGEAR ect with Innovation *											8	8 Port Gigabi	t PoE Smart with 2 Fib
System Switch	ing	QoS	Secur	ity Mor	itoring Maintenance	Help	o						LOG
anagement Device \	/iew	PoE	SNMP LLDI	Services									
asic	Pol	- Port	t Configura	tion									
ivanced			coonigure										
PoE Configuration		PoE Po	ort Configura	tion									()
	POI	RTS									GO TO INTE	RFACE	GO
Timer Global Configuration Timer Schodule		Port	Admin Mode	Priority Level	Detection Mode	Class	Timer Schedule	Output Voltage (Volt)	Output Current (mA)	Output Power (Watt)	Power Limit Type	Power Limit (mWatt)	Status
Configuration			~	~	×		~				~		
		g1	Enable	Low	802.3af 2point Only	0	None	0	0	0.000	Class	15400	Searching
		g2	Enable	Low	802.3af 2point Only	0	None	0	0	0.000	Class	15400	Searching
		g3	Enable	Low	802.3af 2point Only	0	None	0	0	0.000	Class	15400	Searching
		g4	Enable	Low	802.3af 2point Only	0	None	0	0	0.000	Class	15400	Searching
		g5	Enable	Low	802.3af 2point Only	0	None	0	0	0.000	Class	15400	Searching
		g6	Enable	Low	802.3af 2point Only	0	None	0	0	0.000	Class	15400	Searching
		g7	Enable	Low	802.3af 2point Only	0	None	0	0	0.000	Class	15400	Searching
		g8	Enable	Low	802.3af 2point Only	0	None	0	0	0.000	Class	15400	Searching
	POI	RTS									GO TO INTE	RFACE	60
											-		
											CAN	ICEL REFRE	SH APPI

PoE ポート設定をする

- 1. System > PoE > Advanced > PoE Port Configuration をクリックして PoE Port Configuration ページを表示します。
- 2. 設定をするポートのチェックボックスをクリックして、以下の各項目の設定をします。
 - Admin Mode: ポートへの給電を有効、無効に設定します。
 - Priority Level: 給電総量がスイッチの給電可能量を超えたときのポートの優先度を指定します。スイッチは接続されたデバイスすべてに給電できるとは限りません。優先度にしたがってデバイスに給電されます。同じ優先度の場合は、ポート番号の若い方が優先されます。
 - Detection Mode: ポートに接続されたデバイスの検知モード。以下のモードの中の一 つを選択します。
 - Legacy Only:レガシーPD のみを検出する場合に選択します。
 - 802.3af 2point Only:2 ポイント検出モードのみで検出する場合に選択します。
 - 802.3af 4point Only:4 ポイント検出モードのみで検出する場合に選択します。これ がデフォルト設定です。
 - 802.3af 2point and Legacy: 2 ポイント検出とレガシー検出を使う場合に選択しま

す。

- 802.3af 4point and Legacy: 4 ポイント検出とレガシー検出を使う場合に選択します。
- Class:. ポートに接続されている受電機器のクラスを確認できますクラスは受電機器が スイッチから受電している電力の範囲で決まります。クラスの定義は以下の通りです。
 - 0:0.44-12.95W
 - 1:0.44-3.83W
 - **2:**3.84–6.48W
 - **3**:6.49–12.95W
 - 4:予約済
- Timer Schedule. ポートに給電するタイマー設定できます。デフォルトのタイマー設定は ありません。タイマー設定をするには、Timer Global Configuration ページで設定しま す。
- Output Voltage:出力電力。単位はボルト(V)。
- Output Current: 出力電流。単位はミリアンペア(mA)。
- Output Power: デバイスに供給されている電力。単位はワット(W)。
- Power Limit Type:以下の中から電力制限のタイプを選択します。
 - Class:検出したクラス値をもとに制限するときに選択します。この選択をすると、
 Power Limit 欄に設定した値は無視されます。
 - User: Power Limit 欄に制限値を設定するときに選択します。
- Power Limit:ポートから提供できる最大電力を指定します。
- Status:ポートでの PD 検出状態を表示します。
 - Disabled: 給電していません。
 - DeliveringPower:給電中。
 - Fault:故障。
 - Test:テストモード。
 - OtherFault:その他の障害。
 - Searching: 検出中。
- 3. Apply ボタンをクリックして新しい設定を適用します。
- 4. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。
- 5. Refresh ボタンをクリックして最新の情報に更新します。

タイマーグローバル設定(Timer Global Configuration)

Timer Global Configuration ページでタイマー設定を作成、削除およびこの機能の管理状態を制御 します。タイマーはポートへ給電する時間を制御します。以下の手順でポートにタイマー設定を追 加します。

- 1. Timer Global Configuration でタイマー設定を作成します。
- 2. Timer Schedule Configuration ページでタイマーの設定をします。
- 3. PoE Port Configuration ページでポートにタイマーを割り当てます。

メモ:ポートにタイマー設定を割り当てるためにはタイマー機能を有効にする必要があります。

Onnect with Innovation	R'						GS110T 8 Port Gigabit PoE Smart Swit with 2 Fiber St
System Sv	vitching	QoS	Security	Monitoring	Maintenance	Help	LOGOUT
Management De	vice View 📋	PoE SNM	NP LLDP S	ervices		4.2. 36 -	
Basic	Timer G	Global Co	nfiguration				
 Advanced » PoE 	Timer	Schedule			(2)		
Configuration	Admin Mo	de	💿 Disal	ole 🔿 Enable			
Configuration	Timor	Cabadula	Name				
	Tin	ner Schedu	ile Name	ID			
» Timer Schedule Configuration							
	<				IIII		
						ADD	DELETE CANCEL APPLY
opyright @ 1996-201	In Netgear ®					382	

グローバルタイマー設定をする

- 1. System > PoE > Advanced > Timer Global Configuration を選択して Timer Global Configuration ページを表示します。
- 2. タイマーを追加するには、Timer Schedule Name 欄にタイマーの名前を記入し、Add ボタン をクリックします。
- **3.** タイマーを削除するには、削除するタイマーのチェックボックスを選択し、Delete ボタンをクリックします。
- 4. タイマーを有効あるいは無効にするには、Admin Mode のラジオボタンを選択し、Apply ボタ ンをクリックします。
- 5. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。

タイマースケジュール設定(Timer Schedule Configuration)

Timer Schedule Configuration ページでポートへの電源供給を止める時間を設定します。例えば、 毎晩、毎週末、一年のうちある一週間電源を止めることができます。

NETGEAI Connect with Innovation	R'		GS110TP 8 Port Gigabit PoE Smart Switch with 2 Fiber SFP
System Sw	itching QoS	Security Monitoring Maintenance Help	LOGOUT
Management Dev	rice View PoE SNMP	LLDP Services	
> Basic	Timer Schedule		
* Advanced * PoE	Timer Schedule S	election	0
Configuration	Timer Schedule Name		
* POE Port Configuration	Timer Schedule C	onfiguration	1
 Timer Global Configuration 	Shutdown Time Start	00:00 (hh:mm)	
 Timer Schedule Configuration 	Date Start	00:00 (hh:mm)	
	Date Stop	No End Date Date	
	Recurrence Pattern Daily Mode	Daily W Every Day(s)	
		- weekbay	
			,
[<]		
			CANCEL APPLY
Convright @ 1996-201	0 Netgear ®		

タイマースケジュールを設定する。

- 1. System > PoE > Advanced > Timer Schedule Configuration を選択して Timer Schedule Configuration ページを表示します。
- **2.** Timer Global Configuration ページで作成したスケジュール名を Timer ScheduleSelection で選択します。
- 3. Shutdown Time Start に電源を切る時間を記入します。時間の範囲は 00:00 から 23:59 で す。
- 4. Shutdown Time End に電源を入れる時間を記入します。時間の範囲は 00:00 から 23:59 で す。
- 5. 電源を切ることを開始する日を Date Start のカレンダーアイコンをクリックして指定します。
- 必要なら、このスケジュールを終了する日を、カレンダーアイコンをクリックして指定します。
 この場合には End Date のラジオボタンを選択します。
- 7. 必要なら、Recurrence Pattern および Daily Mode 欄を使います。
- 8. Apply ボタンをクリックして設定を保存します。
- 9. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。

SNMP

System タブの下の SNMP リンクで SNMP バージョン 1、2、3 の設定ができます。 SNMP リンクから、以下のページにアクセスできます。

- SNMP バージョン 1/バージョン 2
- トラップフラグ (Trap Flags)

• SNMPv3 ユーザー設定(SNMP v3 User Configuration)

SNMP バージョン 1/バージョン 2

SNMPV1/V2 メニューで、SNMP コミュニティ情報やトラップ、トラップフラグの設定ができます。

コミュニティ設定(Community Configuration)

デフォルトで2つの SNMP コミュニティがあります。

- Private:読み書き可能(Read/Write)、有効(Enable)
- Public:読み取りのみ(Read Only)、有効(Enable)

これらはよく知られたコミュニティです。このページでデフォルトの変更やコミュニティの追加をします。こ のページで定義できるコミュニティは SNMPv1 および SNMPv2c のみでアクセス可能です。読み書き可 能(Read/Write)のコミュニティのみが SNMP で変更可能です。

SNMPv1 または SNMPv2c を使っている場合は、このページを使います。

NETGE Connect with Innovation	AR'					8	GS108T Port Gigabit Smart Switch
System	Switching	g QoS	Security Mc	nitoring Mainte	nance H	elp	LOGOUT
Management	Device Vie	w SNMP LL	DP Services			98 ¹	
• SNMP V1/V2 • Community Configuration	Com	nmunity Confi ommunity Confi	iguration guration			0	
» Trap Configuration		Management Station IP	Management Station IP Mask	Community String	Access Mode	Status	
» Trap Flags			0.0.0.0		ReadOnly 💌	Disable 🛩	1
- SHIF VS		0.0.0.0	0.0.0	public	ReadOnly	Enable	
		0.0.0.0	0.0.0	private	ReadWrite	Enable	
	<						>
						ADD DEI	LETE CANCEL APPLY
Copyright © 1996-	-2009 Netg	ear ®					

SNMP コミュニティを設定する

- 1. System > SNMP > SNMP V1/V2 > Community Configuration を選択して Community Configuration ページを表示します。
- 2. 新しい SNMP コミュニティを追加するには、以下の項目を設定して、Add ボタンをクリックします。
- Management Station IP:管理端末の IP アドレスを指定します。Management Station IP Mask も同時に設定します。このマスクはこのコミュニティを使ってスイッチにアクセスする SNMP クライアントとアドレスの範囲を指定します。SNMP クライアントがこのアドレスを使っ てスイッチにアクセスします。Management Station IP と Management Station IP Mask のど ちらも 0.0.0 の場合、どの IP アドレスからもアクセス可能です。それ以外の場合は、クライ アントの IP アドレスとマスクの AND と管理端末とマスクの AND を比較し、同じアドレスの 場合にアクセス可能とします。たとえば、Management Station IP と Management Station IP Mask が 192.168.1.0/255.255.255.0 であった場合、192.168.1.0~192.168.1.255 の IP アドレ スのクライアントがアクセス可能です。1台のみからアクセス可能にしたい場合は、 Management Station IP Mask を 255.255.255.255 に設定し、Management Station IP のアド

レスを使ってアクセスします。

- **4. Management Station IP Mask**: 管理端末の IP アドレスに合わせてサブネットマスクを設定 します。
- 5. Community String: コミュニティ名を設定します。大文字小文字を区別し最長 16 文字までで す。
- 6. Access Mode:このコミュニティのアクセスレベルをメニューから Read/Write または Read Only に設定します。
- 7. Status:このコミュニティの状態をドロップダウンメニューの Enable(有効)と Disable(無効)から選択します。コミュニティ名に重複があると有効化できません。
- 8. コミュニティ設定を変更するには、コミュニティのチェックボックスを選択後、必要な部分を変 更し、Apply ボタンをクリックします。設定変更は即時に有効になります。
- 9. コミュニティを削除するには、コミュニティのチェックボックスを選択後、Delete ボタンをクリックします。
- 10. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。

トラップ設定(Trap Configuration)

このページではトラップ(Trap)の送信先を設定します。

NETGEAR Connect with Innovation					GS110TP 8 Port Gigabit PoE Smart Switch with 2 Fiber SFP
System Switching	QoS Security	Monitoring	Maintenance	Help	LOGOUT
Management Device View	/ PoE SNMP LLDP	Services			
× SNMP V1/V2 Trap	Configuration				
Community Configuration	rap Configuration				0
Trap Configuration	Recipients IP	Version C	Community String	Status	
» Trap Flags		SNMPv1		Disable 💌	
Sin VS					
					×
<				_	
				ADD	DELETE CANCEL APPLY
Copyright © 1996-2010 Netge	ar ®				

SNMP トラップ(SNMP trap)設定をする

- 1. System > SNMP > SNMP V1/V2 > Trap Configuration.を選択して設定画面を表示します。
- 2. SNMP トラップを受信するホストを追加するには、Trap Configuration に以下の項目を設定 して Add ボタンをクリックします。
 - Recipients IP.このスイッチからの SNMP トラップを受信するアドレスをx.x.x.x 形式 で指定します。
 - Version. SNMPトラップで使用する SNMP のバージョンをメニューから選択します。
 - SNMP v1: SNMPv1 を使用します。

- SNMP v2: SNMPv2c を使用します。
- Community String. SNMP トラップ用のコミュニティストリングを指定します。大文字 小文字を区別し最長 16 文字までです。
- Status.トラップの有効・無効をメニューから選択します。
- Enable:トラップの送信を有効にします。
- Disable: トラップの送信を無効にします。
- 2. トラップ設定を変更するには、コミュニティのチェックボックスを選択後、必要な部分を変更 し、Apply ボタンをクリックします。設定変更は即時に有効になります。
- 3. トラップ設定を削除するには、トラップ設定のチェックボックスを選択後、Delete ボタンをクリ ックします。
- 4. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。

トラップフラグ(Trap Flags)

システムが生成する SNMP トラップ情報を設定することができます。

Trap Flags ページでスイッチが SNMP マネージャーに送信するトラップを有効・無効にすることが できます。スイッチがトラップを送信する条件に一致したとき、トラップメッセージが有効になってい る SNMP トラップ宛先に送信され、トラップログ(trap log)に記録されます。

NETGEAR Connect with Innovation					8 Port Gi	GS110TP igabit PoE Smart Switch with 2 Fiber SFP
System Swite	hing QoS S	ecurity A	Aonitoring	Maintenance	Help	LOGOUT
Management Device	View PoE SNMP	LLDP Service	s			
* SNMP V1/V2	Trap Flags					
Configuration	Trap Flags			0		
» Trap Configuration	Authentication	C Disabl	e 🖲 Enable			
> Trap Flags > SNMP V3	Link Up/Down	C Disabl	e 🖲 Enable			
	Spanning Tree	C Disabl	e 🖲 Enable			
	MAC Learn/Ageout	C Disabl	e 🖲 Enable			
	POE	Oisabl	e 🔿 Enable			
						CANCEL APPLY
Convright @ 1996-2015 M	ETCEAD @					

トラップフラグ(Trap Flag)を設定する。

- 1. System > SNMP > SNMP V1/V2 > Trap Flags を選択して Trap Flags ページを表示しま す。それぞれのトラップについて有効・無効を設定します。
 - Authentication:認証エラーのトラップの送信を設定します。デフォルトは有効(Enable)です。
 - Link Up/Down:リンクのアップダウントラップの送信を設定します。デフォルトは有効 (Enable)です。

- Spanning Tree:スパニングツリーのトラップの送信を設定します。デフォルトは有効 (Enable)です。
- MAC Learn/Ageout: MAC アドレスの学習およびエージアウトの際のトラップ送信を設定します。デフォルトは有効(Enable)です。
- POE:PoE のトラップの送信を設定します。デフォルトは無効(Disable)です。
- 2. 設定変更後、Apply ボタンをクリックします。設定変更は即時に有効になります。
- 3. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。

SNMPv3 ユーザー設定(SNMP v3 User Configuration)

ここでは SNMPv3 の設定をします。

NETGE	AR'				GS108T
					8 Port Gigabit Smart Switch
System	Switching QoS	Security Monitoring	Maintenance	Help	LOGOUT
Management	Device View SNMP LLDI	P Services	ië State state stat		
SNMP V1/V2	User Configuration	10			
 SNPP V3 User Configuration 	User Configuration		0		
and the second	SNMP v3 Access Mode	Read/Write			
	Authentication Protocol	None ○ MD5 ○ SH SH	4		
	Encryption Protocol	None ○ DES DES			
	Encryption Key				
	<		Ш		>
					CANCEL APPLY
opyright © 1996	5-2009 Netgear 🕲				

SNMPv3 Access Mode は変更不可の情報でユーザーアカウントの権限を示します。admin アカウントは常に読み書き可能(Read/Write)でありその他のアカウントは読み取り専用(Read Only)です。

SNMPv3 設定をする。

- System > SNMP > SNMP V1/V2 > Community Configuration を選択して Community Configuration ページを表示します。 以下の項目について設定をします。
- 2. Authentication Protocol: SNMPv3 の認証プロトコルを選択します。選択肢は、None, MD5, または SHA です。
 - None: SNMP データにアクセスできません。
 - MD5 or SHA: SNMPv3 認証パスワードとしてスイッチのユーザーログインパスワードが 使われます。パスワードは 8 文字です。
- 3. Encryption Protocol: SNMPv3 パケットの暗号化方式を選択します。
 - None:暗号化を行わない。
 - **DES**:.DES を使用する。

- 4. Encryption Key: DES の際に暗号化キーを入力する。最大 15 文字です。(0 も含む)
- 5. 設定後、Apply ボタンをクリックします。設定は即時に有効になります。
- 6. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。

LLDP

IEEE 802.1AB で定義されている Link Layer Discovery Protocol (LLDP)で、LAN に接続された機器が能力および物理構成を通知することができます。この情報を使ってシステム接続構成や LAN の誤った構成を知ることができます。

LDPリンクから以下のページにアクセスできます。

- LLDP 設定(LLDP Configuration)
- LLDP ポート設定(LLDP Port Settings)
- LLDP-MED ネットワークポリシー(LLDP-MED Network Policy)
- LLDP-MED Port Settings
- ローカル情報(Local Information)

LLDP は一方向のプロトコルで、要求・応答というような通信はありません。情報はこの機能を送信 する機能を実装している機器から送信(advertise)され、受信機能を実装している機器によって受 信・処理されます。送信・受信の機能はポート単位に設定できます。デフォルト設定では、送信・受 信共に無効になっています。

Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED) は以下の点で LLDP 機能を拡張したものです。

- VLAN、レイヤー2の優先度、DiffServ 設定のようなLANのポリシーの自動検出し、プラグ アンドプレイネットワークを可能にする。
- ロケーションデータベースを作成し、デバイスの位置検出を行う。
- PoE(Power over Ethernet)機器の電源管理の拡張および自動化。
- ネットワーク管理者がネットワーク機器の追跡や機器特性(製造元、ソフトウェアバージョン、ハードウェアバージョン、機器シリアル番号)を確認するようなインベントリー管理。

LLDP 設定(LLDP Configuration)

LLDP Configuration ページで LLDP および LLDP-MED 設定をします。

NETGEA Connect with Innovation	R'			GS110TP 8 Port Gigabit PoE Smart Switch with 2 Fiber SFP
System St	witching QoS Secu	rity Monitoring Maintenance	Help	
Management De	evice View PoE SNMP LLD	P Services		
* Basic	LLDP Configuration			^
Configuration	LLDP Properties	۲		
> Advanced	TLV Advertised Interval Hold Multiplier Reinitializing Delay Transmit Delay	30 (5 to 32768 secs) 4 (2 to 10 secs) 2 (1 to 10 secs) 5 (5 to 3600 secs) 3		1
	Fast Start Duration	3 (1 to 10 Times)		
	<]			×
				REFRESH CANCEL APPLY

グローバル LLDP(Global LLDP)設定をする

- System > LLDP > Basic > LLDP Configuration を選択して LLDP Configuration ページを 表示します。
 System > LLDP > Advanced > LLDP Configuration を指定して LLDP Configuration ページを開くこともできます。
- 2. 以下の項目の設定をします。
 - TLV Advertised Interval: フレームの送信間隔を指定します。デフォルトは 30 秒です。
 設定可能な値は 1-32768(秒)です。
 - Hold Multiplier: 送信情報の有効期間を決める送信間隔の倍数。デフォルトは4です。
 設定範囲は 2-10 です。係数。
 - Reinitializing Delay: LLDP がポートで再初期化するまでの時間。デフォルトは2秒です。設定範囲は1-10秒です。
 - Transmit Delay:設定が変更してから情報を送信するまでの時間。デフォルトは 5 秒で す。設定範囲は 5-3600 秒です。
- LLDP-MED properties の Fast Start Duration は、LLDP-MED 対応機器を検出し、LLDP ーMED ファストスタート(Fast Start)メカニズムが起動された際に LLDP パケットを 1 秒間隔 で連続送信する数を設定します。デフォルトは 3 です。設定範囲は 1-10 です。
- 4. Apply ボタンをクリックして設定をスイッチに適用します。設定は即時に有効になります。
- 5. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。
- 6. Refresh ボタンをクリックして画面を最新の情報に更新します。

LLDP ポート設定(LLDP Port Settings)

LLDP Port Settings ページでインターフェースに LLDP 設定をします。

System	Switching	0.05	Security	Monitoring	Mainten	Hele	LOGO
Management	Device View	V SNMP	LLDP Service	ces	Mannene	ince incip	
Basic	LLD	P Port Se	ttings				
Advanced		DP Port Se	ttinas			(2)	
Configuration				GO TO		GO	
 LLDP Port Settings LLDP-MED 		Interface	Admin Status	Management IP Address	Notification	Optional TLVs	
Network Policy			~	×	~	N	
 LLDP-MED Port Settings 		g1	Disabled	Stop Advertise	Disable	Disable	
> Local		g2	Disabled	Stop Advertise	Disable	Disable	
Information Neighbors		g3	Disabled	Stop Advertise	Disable	Disable	
Information		g4	Disabled	Stop Advertise	Disable	Disable	
		g5	Disabled	Stop Advertise	Disable	Disable	
		g6	Disabled	Stop Advertise	Disable	Disable	
		g7	Disabled	Stop Advertise	Disable	Disable	
		g8	Disabled	Stop Advertise	Disable	Disable	
				GO TO		GO	

LLDP ポート設定をする。

- 1. System > LLDP > Advanced > LLDP Port Settings を選択して LLDP Port Settings ページ を表示します。
- 2. 以下の LLDP ポート設定を変更します。
 - Interface: LLDP 設定を変更するポートを選択します。
 - Admin Status: LLDP パケットの送信・受信の設定をします。
 - Tx Only::指定したポートで LLDP パケットの送信のみをします。
 - Rx Only:指定したポートで LLDP パケットの受信のみをします。
 - Tx and Rx::指定したポートで LLDP パケットの送受信をします。
 - Disabled 指定したポートで LLDP パケットの送受信をしません。
 - Management IP Address: LLDP パケットに管理 IP アドレスとしてスイッチの IP アドレス を含むかどうかを設定します。選択肢は以下となります。
 - Stop Advertise: 指定したポートで管理 IP アドレスを送信しません。
 - Auto Advertise:指定したポートでスイッチの IP アドレスを管理 IP アドレスとして送信します。
 - Notification: 有効(Enabled)に設定された場合は、LLDP で変更を検知した場合にトラッ

プを送信します。デフォルト設定は無効(Disabled)です。

- Optional TLV(s):オプションの type-length value (TLV)の送信を有効・無効に設定します。TLV 情報はシステム名(system name)、システム情報(system description),システム能力(system capabilities), ポート情報(port description)です。
- 3. Apply ボタンをクリックして設定をスイッチに適用します。設定は即時に有効になります。
- 4. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。

LLDP-MED ネットワークポリシー(LLDP-MED Network Policy)

このページでは指定されたポートから送信された LLDP-MED ネットワークポリシー(LLPD-MED network policy) TLV の情報を表示します。

NETGEA	R'							GS110TI 8 Port Gigabit PoE Smart Swite with 2 Fiber SF
System Sw	vitching Q	Securit	у	Monitorin	g Ma	intenance	Help	LOGOUT
Management De	vice View PoE	SNMP LLDP	Servie	ces				
 Basic Advanced LLDP Configuration 	LLDP-MED	Network Policy	icy /			۲		
 » LLDP Port Settings » LLDP-MED 	:: Network P	olicies Informa	tion			(2)		
 » LLDP-MED Port Settings » Local Information 	Network Policy Number	Application	VLAN ID	VLAN Type	User Priority	DSCP		
» Neighbors Information	<							!</td
								REFRESH

System > LLDP > Advanced > LLDP-MED Network Policy を選択して LLDP-MED Network Policy ペー ジを表示します。

Interface メニューで、情報を表示するポートを選択します。以下の表に表示される情報の説明を示します。

項目	説明
Network Policy Number	ポリシー番号を表示します。

Application	 以下のメディアアプリケーションタイプを表示します。 Unknown(不明) Voice(音声) Guest Voice(ゲスト音声) Guest Voice Signaling(ゲスト音声シグナリング) Softphone Voice(ソフトフォン音声) Video Conferencing(ビデオ会議) Streaming Video(ストリーミングビデオ) Video Signaling(ビデオシグナリング) ポートは複数のアプリケーションタイプを受信できます。ネットワークポリシーTLV(network policy TLV)がポートから
	送信されたときのみ表示されます。
VLAN ID	ポリシーに関連付けられた VLAN ID。
VLAN Type	ポリシーに関連付けられた VLAN がタグ付きかタグ無しか を表示します。
User Priority	ポリシーに関連付けられた優先度。
DSCP	ポリシーに関連付けられた DSCP。

Refresh ボタンをクリックしてスイッチの最新の情報に更新します。

LLDP-MED Port Settings

インターフェースの LLDP-MED モードを有効に	し、設定をします。
----------------------------	-----------

					or on algabit offart of
System Sw	vitching QoS Se	curity Monitoring	Maintenance	Help	LOGO
Management Dev	vice View SNMP LLDP	Services			
Basic	LLDP-MED Port Setti	ngs			
Advanced » LLDP	LLDP-MED Port Setting	js	۲		
Configuration » LLDP Port	Port LLDP-MED Status	g1 M			
Settings » LLDP-MED	Notification	Disable			
LLDP-MED Port	Transmit Optional TLVs	Disable			
Settings • Local					
Neighbors					
Information	<1		in .		1
	N				

ポートに LLDP-MED 設定(LLDP-MED Settings)をする

- 1. System > LLDP > Advanced > LLDP-MED Port Settings を選択して、LLDP-MED Settings ページを表示します。
- 2. Port:設定するポートを選択します。
- 3. LLDP-MED Status: LLDP-MED の有効・無効を選択します。

- Notification: デバイスが接続されたり切断されたときにトポロジーチェンジ通知を送信する かどうかを指定します。
- 5. Transmit Optional TLVs:LLDP パケットにオプションの TLV 値を送信するかどうかを指定 します。有効(Enabled)の場合、以下の TLV 値が送信されます。
 - MED Capabilities
 - Network Policy
 - Location Identification
 - Extended Power via MDI: PSE
 - Extended Power via MDI: PD
 - Inventory
- 6. Apply ボタンをクリックして設定をスイッチに適用します。設定は即時に有効になり、設定は 保存されます。
- 7. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。

ローカル情報(Local Information)

LLDP Local Information ページでポートが送信する LLDP 情報を表示します。

NETGEA Connect with Innovation	R.					GS110TP 8 Port Gigabit PoE Smart Switch with 2 Fiber SFP
System Sw	ritching	QoS Security	Monitoring	Maintenance	Help	LOGOUT
Management Dev	vice View	PoE SNMP LLDP	Services			3
> Basic	Local II	nformation				
* Advanced	Devic	e Information				(7)
Configuration	No local in	nterfaces are enabled to t	transmit LLDP <mark>d</mark> ata.			
 » LLDP Port Settings 						
» LLDP-MED	· Port I	Information				0
Network Policy	Interfac	e Port ID Subtype	Port ID	Port Description	Advertisement	
Settings	<u>a1</u>	MAC Address	00:24:B2:E3:02:59		Disable	
» Local	<u>92</u>	MAC Address	00:24:B2:E3:02:59		Disable	
Information	<u>a3</u>	MAC Address	00:24:B2:E3:02:59		Disable	
» Neighbors	<u>q4</u>	MAC Address	00:24:B2:E3:02:59		Disable	
Information	<u>q5</u>	MAC Address	00:24:B2:E3:02:59		Disable	
	<u>q6</u>	MAC Address	00:24:B2:E3:02:59		Disable	
	<u>a7</u>	MAC Address	00:24:B2:E3:02:59		Disable	
	<u>q8</u>	MAC Address	00:24:B2:E3:02:59		Disable	
	99	MAC Address	00:24:B2:E3:02:59		Disable	
	<u>q10</u>	MAC Address	00:24:B2:E3:02:59		Disable	
						×
	<					>
						REFRESH
Copyright © 1996-201	0 Netgear ®					

Local Information ページで表示される各ポート情報の説明は以下の通りです。

項目	説明
Interface	インターフェース番号
Port ID Subtype	Port ID 欄に表示される情報のタイプ。
Port ID	ポートの物理アドレス。

Port Description	ユーザーが定義したポート情報。
Advertisement	ポートの情報送信の状態。

LLDP > Local Information.を選択して、LLDP Local Information ページを表示します。 Refresh ボタンをクリックしてスイッチの最新の情報に更新します。

Port Information の表の Interface 部分のポート番号をクリックして追加の情報を表示します。

選択したポートの情報がポップアップウィンドウ内に表示されます。

Managed Ad	dress					(?)	
		IDv4					
Address		10.13	1,12,183				
Interface SubTyp	e	ifInde	×				
Interface Numbe	r	13					
MAC/PHY D	etails					(?)	
Auto-Negotiation	Supported	True				-	
Auto-Negotiation	Enabled	True					
Auto-Negotiation	Advertised	other	other				
Operational MAU Type		Unknown					
MED Details						?	
Capabilities Supp	orted	Capal	bilities.Network				
Current Capabilities		Capal	bilities,Network				
Device Class		Netwo	rk				
Network Po	licies					0	
Application Type	VLAN ID		VLAN Type	User Priority	DSCP		

選択されたポートの詳細情報の説明は以下の表のとおりです。

項目	説明
Managed Address	
Address SubType	管理インターフェースが使っているアドレスのタイプ。たとえ ば IPv4 アドレス。
Address	管理用に使われるアドレス。
Interface SubType	ポートのタイプ。
Interface Number	ポートの番号。
MAC/PHY Details	
Auto-Negotiation Supported	ポートでオートネゴシエーションをサポートしているか否か。 値は True または False。
Auto-Negotiation Enabled	ポートでオートネゴシエーションをサポートしているか否か。 値は True(有効)または False(無効)。
Auto Negotiation Advertised Capabilities	ポートのオートネゴシエーションでサポートしているモード。

GS108T/GS110TP スマートスイッチソフトウェア管理マニュアル

Operational MAU Type	MAU(Medium Attachment Unit)のタイプ。

項目	説明
MED Details	
Capabilities Supported	ポートで有効になっている MED 能力。
Current Capabilities	ポートが送信している TLV の値。
Device Class	ネットワークに接続される機器であることを示します。
Network Policies	
Application Type	ポリシーに関連付けられたアプリケーションタイプ。
VLAN ID	ポリシーに関連付けられた VLAN ID。
VLAN Type	VLAN のタイプ。 Tagged または untagged。
User Priority	ポリシーに関連付けられた優先度。
DSCP	ポリシーに関連付けられた DSCP.

隣接情報(Neighbors Information)

Neighbors Information ページで特定のポートが受信した LLDP 情報を表示します。

NETGE	AR'							GS10	08
onnect with Innovation	n							8 Port Gigabit Smart S	Swite
System	Switching	QoS	Security	Monitoring	Maintenar	ice	Help	[100	GOUT
Management	Device View	SNMP LI	DP Services						
Basic	Neighbo	ors Inform	nation						
* Advanced * LLDP	Neigh	bors Inform	nation					0	
Configuration > LLDP Port	MSAP	Local	Chassis ID Subtype	Chassis TD	Port ID Subtype	Port	System		
Settings			Cabrype		Caseype				
» LLDP-MED Network Policy	e								
» LLDP-MED Port	t								
Settings » Local									
Information									
Information	-								
	<								
								REFR	ESH
111 0 1000									

System > LLDP > Advanced > Neighbors Information.を選択して Neighbors Information ページを表示します。

項目	説明
MSAP Entry	リモートデバイスの Media Service Access Point (MSAP)エン トリー番号を表示します。
Local Port	LLDP 情報を受信したポート。

Chassis ID Subtype	リモートデバイスの Chassis ID のタイプ。
Chassis ID	リモートスイッチの Chassis ID。
Port ID Subtype	リモートデバイスの Port ID のタイプ。
Port ID	リモートデバイスの Port ID。
System Name	リモートデバイスのシステム名。

Refresh ボタンをクリックしてスイッチの最新の情報に更新します。

Neighbors Information の表の MSAP Entry 部分をクリックして追加の情報を表示します。 選択したポートの情報がポップアップウィンドウ内に表示されます。

Port Detai	ls				(?)	MED Details	5			0	
Local Port		g3				Capabilities Supp	Capabilities Supported Capabilities, Network Policy, In		olicy, Invent	ory	
MSAP Entry 13				Current Capabilit	ties Capal	olities,Network F	olicy, Invent	tory			
						Device class	N/A	ik connectivity			
						PoE Power Source	N/A				
Basic Deta	ils				(2)	PoE Power Prior	ity N/A				
Chassis ID Sub	Type	MACA	ddrass			PoE Power Value	e N/A				
Chassis ID Sub	Type	00:14	:6C:34:5E:4E			Hardware Revisi	on 0×0				
Port ID SubTyp	e	MAC A	ddress			Firmware Revisi	on 1.5				
Port ID		00:14	16C:34:5F:51			Software Revisio	on 9.9.0.	9.9.0.9			
Port Descriptio	n					Serial Number	15D3	15D35B4U00224			
System Name						Model Name	FSM7:	352S			
System Descrip	ption	FSM73	52S 48+4 L3 Sta	ckable Switch		Asset ID					
System Capabi	lities	bridge	, router								
						Location In	formation			1	
Managed A	Address				0	Civic	N/A				
Address			Interface	Interface		Coordinates	N/A				
SubType	Address		SubType	Number		ECS ELIN	N/A				
Þ						Unknown	N/A				
МАС/РНУ	Details				(7)	* Network Po	licies			(
Auto-Negotiati	on Supported	True				Application	VLAN ID	VLAN Type	User	DSCP	
Auto-Negotiati	on Enabled	True				туре			Priority		
Auto-Negotiati	on Advertised										
Capabilities											
Operational MA	U Type	Unkno	nwn			LLDP Unkn	own TLVs			(

Field	Description
Port Details	
Local Port	LLDP 情報を受信したローカルポート情報。
MSAP Entry	リモートデバイスの Media Service Access Point (MSAP)エ ントリー番号。
Basic Details	
Chassis ID Subtype	リモートデバイスの Chassis ID のタイプ。
Chassis ID	リモートデバイスの Chassis ID。
Port ID Subtype	リモートデバイスの Port ID のタイプ。

Port ID	リモートデバイスの Port ID。
Port Description	リモートデバイスのポート情報。
System Name	リモートデバイスのシステム名。
System Description	リモートデバイスのシステム情報。
System Capabilities	リモートデバイスのシステム能力。
Managed Addresses	
Address SubType	リモートデバイスの管理アドレスのタイプ。
Address	リモートデバイスの管理アドレス。
Interface SubType	リモートデバイスのインターフェースのタイプ。
Interface Number	リモートデバイスのインターフェース番号。
MAC/PHY Details	
Auto-Negotiation Supported	リモートデバイスのポートでオートネゴシエーションをサポー
	トしているか否か。 値は True または False。
Auto-Negotiation Enabled	リモートデバイスのポートでオートネゴシエーションをサポー
	トしているか否か。値は True(有効)または False(無効)。
Auto Negotiation Advertised	リモートデバイスのポートのオートネゴシエーションでサポー
Capabilities	トしているモード。
Operational MAU Type	リモートデバイスの MAU(Medium Attachment Unit)のタイ ー

Field	Description
MED Details	
Capabilities Supported	MED TLV で受信されたデバイスの能力。
Current Capabilities	MED TLV で受信されたデバイスの能力。
Device Class	LLDP-MED エンドポイントのクラス。
	● Endpoint Class 1 標準エンドポイントクラス、基本 LLDP サービスを提供。
	 Endpoint Class 2 メディアエンドポイントクラス Class 1 の 機能に加えてメディアストリーミングを提供。
	 Endpoint Class 3 コミュニケーションデバイスクラス、 Class 1,2 の機能に加えて、緊急通報、レイヤ 2 スイッチサポ ート、デバイス情報管理機能を提供。
PoE Device Type	PoE デバイスタイプ。
PoE Power Source	PoE ポートの電源供給元。
PoE Power Priority	PoE ポートの優先度。
PoE Power Value	PoE ポートの電力値。
Hardware Revision	リモートデバイスのハードウェアバージョン。

Firmware Revision	リモートデバイスのファームウェアバージョン。
Software Revision	リモートデバイスのソフトウェアバージョン。
Serial Number	リモートデバイスから送信されたシリアル番号。
Model Name	リモートデバイスから送信されたモデル名。
Asset ID	リモートデバイスの Asset ID。
Location Information	
Civic	リモートデバイスからロケーション TLV で送信された住所。
Coordinates	リモートデバイスからロケーション TLV で送信された経度、緯 度、高度。
ECS ELIN	リモートデバイスからロケーション TLV で送信された
	Emergency Call Service (ECS) Emergency Location
	Identification Number (ELIN)。 長さは 10-25。
Unknown	不明な位置情報。

Field	Description
Network Policies	
Application Type	ポリシーに関連付けられたリモートデバイスのアプリケー ションタイプ。
VLAN ID	ポリシーに関連付けられたリモートデバイスの VLAN ID。
VLAN Type	リモートデバイスの VLAN のタイプ。Tagged または
User Priority	ポリシーに関連付けられたリモートデバイスの優先度。
DSCP	ポリシーに関連付けられたリモートデバイスの DSCP.
LLDP Unknown TLVs	
Туре	不明の TLV タイプ。
Value	不明の TLV 値。

サービス-DHCP フィルタ(Services - DHCP Filtering)

DHCP フィルタは非公式の DHCP サーバーからのセキュリティ攻撃に対する対策として有効です。 非公式な DHCP サーバーがクライアントからの DHCP リクエストに応答し、ゲートウェイの IP アド レスとしてを非公式な DHCP サーバーの IP アドレスをクライアントに通知すると、他のネットワーク へのトラフィックをすべてサーバーに送信し、パスワードの覗き見や中間者攻撃を仕掛けたりしま す。DHCP フィルタ機能で、各ポートを信頼できる(trusted)ポートまたは信頼できない(untrusted)ポ ートとして設定することができます。正しい DHCP サーバーの接続されたポートは trusted ポートと して設定します。Trusted ポートで受信された DHCP 応答は転送されます。他のポートは untrusted とします。Untrusted ポートでは DHCP(または BootP)応答は廃棄されます。

Servicesリンクから以下のページにアクセスできます。

- DHCP フィルタ設定(DHCP Filtering Configuration)
- インターフェース設定(Interface Configuration)

DHCP フィルタ設定(DHCP Filtering Configuration)

DHCP Filtering Configuration ページで DHCP フィルタ機能を有効にします。

NETGEA Connect with Innovation**	R'					GS110TP 8 Port Gigabit PoE Smart Switch with 2 Fiber SFP
System Sv	vitching QoS	Security Mon	nitoring	Maintenance	Help	LOGOUT
Management De	vice View PoE SNMP	LLDP Services				
~ DHCP Filtering	Configuration					
 Configuration Interface 	Configuration			0		
Configuration	Admin Mode	💿 Disable 🔘 Er	nable			
	<					
						CANCEL APPLY
Copyright © 1996-20	10 Netgear ®					

グローバル DHCP フィルタ設定をする。

- 1. System > Services > DHCP Filtering > Configuration を選択して DHCP Filter Configuration ページを表示します。
- 2. Admin Mode: DHCP フィルタを Enable(有効)または Disable(無効)にするかを選択します。
- 3. Apply ボタンをクリックして設定をスイッチに適用します。設定は即時に有効になり、設定は 保存されます。
- 4. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。

インターフェース設定(Interface Configuration)

DHCP Filtering Interface Configuration ページで各ポートの Trusted、Untrusted 設定をします。

System Sv	witching	QoS Sec	curity Monitoring Maintenance Help	LOGO
Management De	vice View	SNMP LLDP	Services	
WCD Eilkening	Intert	ace Configuration	on	
Configuration	Inte	rface Configuration	0	
	PORTS	LAGS All	GO TO INTERFACE GO	
A second s		Interface	Trust Mode	
		g1	Disabled	
		g2	Disabled	
		g3	Disabled	
		g4	Disabled	
		g5	Disabled	
		g6	Disabled	
		g7	Disabled	
		g8	Disabled	
	PORTS	LAGS All	GO TO INTERFACE GO	
	<]][

GS108T/GS110TP スマートスイッチソフトウェア管理マニュアル

Trusted ポートで受信された DHCP 応答は転送されます。Untrusted ポートで受信された DHCP (または BootP)レスポンスは廃棄されます。

インターフェースに DHCP フィルタ(DHCP filtering)を設定する

- 1. System > Services > DHCP Filtering > Interface Configuration を選択して Interface Configuration を表示します。
- 2. PORTS をクリックして、ポートで DHCP フィルタを設定します。
- 3. LAGS をクリックして、Link Aggregation Group (LAG)で DHCP フィルタを設定します。
- **4.** ALL をクリックして、ポートと Link Aggregation Group (LAG)の両方で DHCP フィルタを設定 します。
- 5. 設定をしたいポートまたは LAG の横のチェックボックスをクリックして選択をします。複数の 選択も可能です。
- 6. モードを選択します。
 - Enable:(Trusted)DHCP 応答が転送されます。
 - Disable:(Unstusted): DHCP (または BootP)応答が廃棄されます。
- 7. Apply ボタンをクリックして設定をスイッチに適用します。設定は即時に有効になり、設定は 保存されます。
- 8. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。

3.スイッチング設定

Switching タブでレイヤー2機能を設定します。Switching タブは次の機能のリンクを含みます。

- ポート(Ports)
- リンクアグリゲーショングループ(Link Aggregation Groups)
- VLAN
- ボイス VLAN (Voice VLAN)
- ・ オート VoIP(Auto-VoIP)
- スパニングツリープロトコル(Spanning Tree Protocol)
- マルチキャスト(Multicast)
- フォワーディングデータベース(Forwarding Database)

ポート(Ports)

ポート(Ports)タブでスイッチの物理ポート情報を見ることができます。ポート(Ports)リンクから以下のページにアクセスできます。

- ポート設定(Port Configuration)
- フローコントロール(Flow Control)

ポート設定(Port Configuration)

ポート設定(Port Con	ifiguration)ページでス	イッチの物理インター	-フェースを設定します。
----------------	-------------------	------------	--------------

Po	t Coi	nfiguration												
	© Port Configuration 0													
PO	RTS LAGS All COTO INTERFACE CO										GO			
	Port	Description	Port Type	Admin Mode	Port Speed	Sleep Mode	Short Cable Mode	Physical Status	Link Status	Link Trap	Maximum Frame Size (1518 To 9216)	MAC Address	PortList Bit Offset	ifindex
				Enable 💙	Auto 💌	Enable 🔽	Enable 💌			Enable 💌				
	g1			Enable	Auto	Disable	Disable	100 Mbps Full Duplex	Link Up	Enable	1518	00:24:B2:5C:96:4B	1	1
	g2			Enable	Auto	Disable	Disable		Link Down	Enable	1518	00:24:82:5C:96:4B	2	2
	g3			Enable	Auto	Disable	Disable		Link Down	Enable	1518	00:24:82:5C:96:4B	3	3
	g4			Enable	Auto	Disable	Disable		Link Down	Enable	1518	00:24:82:5C:96:4B	4	4
	g5			Enable	Auto	Disable	Disable		Link Down	Enable	1518	00:24:B2:5C:96:4B	5	5
	g6			Enable	Auto	Disable	Disable		Link Down	Enable	1518	00:24:82:5C:96:4B	6	6
	g7			Enable	Auto	Disable	Disable		Link Down	Enable	1518	00:24:B2:5C:96:4B	7	7
	g8			Enable	Auto	Disable	Disable		Link Down	Enable	1518	00:24:B2:5C:96:4B	8	8
PO	TS	LAGS	A	II.								GO TO INTERF	ACE	GO

ポート設定をする。

- 1. Switching > Ports > Port Configuration を選択して Port Configuration ページを表示します。
- 2. PORTS をクリックして、物理ポート設定をします。
- 3. LAGS をクリックして、Link Aggregation Group (LAG)設定をします。
- 4. ALL をクリックして、物理ポートと Link Aggregation Group (LAG)の両方の設定をします。
- 5. 設定をしたいポートまたは LAG の横のチェックボックスをクリックして選択をします。複数の選択も 可能です。
 - Description:ポートの説明を記入します。最大 64 文字です。
 - Port Type: 通常は空白です。その他の場合は以下の情報が表示されます。
 - MON:ポートはモニターポートです。
 - LAG:ポートはリンクアグリゲーショントランクの一部であることを示します。
 - Admin Mode:メニューからポートの管理状態を選択します。
 - Enable:ポートは利用可能です。(デフォルト)
 - Disable:ポートはダウン状態で利用不可能です。
 - Port Speed:ポートの速度とデュプレックスモード。Autoの場合は、速度とデュプレックスモードはオートネゴシエーションで設定されます。ポートの最大能力(全二重、1000Mbps)がアドバタイズされます。それ以外の場合は、デュプレックスモードと速度を選択します。デフォルトはAutoです。
 - Sleep Mode:ポートのグリーンイーサネットモードを選択します。
 - Enable:ポートリンクがダウンの場合、ポートは自動的に短時間にダウンし、定期的にリンク

パルスをちぇっくします。リンク先にデバイスがいない場合、スリープモードに入り電力消費 を抑えます。

- Disable:ポートにデバイスが接続されていないときでも電力が供給されます。
- Short Cable Mode: グリーンイーサネットモードのショートケーブルモードを有効にします。
 - Enable:ポートが 1Gbps 速度でリンクアップした際に、ケーブルテストを実行し、ケーブル長が 10m 未満と判断した場合に、低電カモード(定格電力)で動作します。
 - Disable:ショートケーブルモードは無効です。
- Physical Status::ポートの速度とデュプレックスモードを表示します。
- Link Status:リンク状態(Up/Down)を示します。
- Link Trap:リンク状態が変化したときにトラップを送信します。デフォルトは Enable(有効)です。
 - Enable:リンク状態が変化したときにトラップを送信します。
 - Disable:リンク状態が変化してもトラップを送信しません。
- Maximum Frame Size: イーサネットの最大フレームサイズ (Maximum Frame Size)を設定します。フレームサイズはイーサネットヘッダー、CRC およびペイロードを含み、範囲は 1518-9216 バイトです。デフォルト値は 1518 バイトです。
- MAC Address:ポートの物理アドレスを表示します。
- PortList Bit Offset: PortList MIB オブジェクトタイプが SNMP 管理で使用される場合、ポートに 対するビットオフセット値を表示します。
- **ifIndex**.:ポートの ifIndex 値。
- 6. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。
- 7. Apply ボタンをクリックして設定をスイッチに適用します。

フローコントロール(Flow Control)

IEEE 802.3x フローコントロールによって、ポートの負荷が高くなった際に、ポートを一時停止(ポーズ)することにより短時間パケットを廃棄します。この結果、優先度が高いトラフィックやネットワークを制御するトラフィックも失うことになります。When IEEE 802.3x フローコントロールが有効な環境では、処理能力の低いスイッチは能力の高いスイッチにパケットの送出を抑えるように要求します。能力の低いスイッチのバッファーオーバーフローを防ぐために、パケットの送出が一時的に停止されます。

NETGEAR Connect with Innovation*		GS110TP 8 Port Gigabit POE Smart Switch with 2 Fiber SFP
System Swite	hing QoS Security Monitoring Maintenance He	
Ports LAG VLAN	Voice VLAN Auto-VoIP STP Multicast Address Table	
• Port Configuration	Flow Control	
Flow Control	Flow Control	۲
	Global Flow Control (IEEE 802.3x) Mode	
	[] [
		CANCEL
Convright @ 1996-2010	Jataaar ®	

フローコントロール設定をする。

- 1. Switching > Ports, > Flow Control を選択して Flow Control ページを表示します。
- 2. Global Flow Control (IEEE 802.3x) Mode 欄でスイッチとしての IEEE 802.3x フローコントロールの設 定をします。
 - Enable:フローコントロールを有効にします。スイッチのバッファーが一杯になるとポーズフレームを送信します。
 - Disable フローコントロールを無効にします。スイッチのバッファーが一杯になってもポーズフレ ームを送信しません。
- 3. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。
- 4. Apply ボタンをクリックして設定をスイッチに適用します。

リンクアグリゲーショングループ(Link Aggregation Groups)

リンクアグリゲーショングループ(LAG)、(ポートチャネルとも呼ばれます)によって、複数の全二重 のイーサネットリンクを一つの論理リンクに多重することができます。ネットワークデバイスは LAG を一つのリンクであるように扱い、障害に対する冗長性を増加させ、負荷分散を可能とします。 LAG を作成した後に、LAG VLAN メンバーシップを割り当てます。デフォルトで LAG は管理 VLAN のメンバーになります。

LAG インターフェースはスタティックまたはダイナミックのどちらかが可能です。LAG のメンバーの プロトコルは同じである必要があります。スタティックポートチャネル(LAG)インターフェースは対向 のスイッチがメンバーポートを多重しなくてもかまいません。

スタティック LAG の場合、LAG PDU の送受信はしません。GS108T および GS110TP は最大4つの LAG をサポートしています。

LAGリンクから以下のページにアクセスできます。

- LAG 設定(LAG Configuration)
- LAG メンバーシップ(LAG Membership)
- LACP 設定(LACP Configuration)
- LACP ポート設定(LACP Port Configuration)

LAG 設定(LAG Configuration)

LAG 設定ページを使って、複数の全二重イーサネットリンクを束ねて、ポートチャネルとも言われ るリンクアグリゲーショングループ(LAG)を作ることができます。 スイッチは LAG を一つのリンクの ように扱います。

NETGEAR										o Dest Oissehil	GS108T
System Switch	hing	QoS	Security Monito	ring	Maintenanc	e Help				8 Port Gigabit	
Ports LAG VLAN	i Void	e VLAN Auto-V	oIP STP Multicast	Address	Table						
* Basic * LAG Configuration	LAG Configuration LAG Configuration ()										
» LAG Membership > Advanced		Lag Name	Description	Lag ID	Link Trap	Admin Mode	STP Mode	LAG Type	Active Ports	LAG state	
		LAG1		1	Disable	Enable	✓ Disable	Static		Link Down	-
		LAG2 LAG3		2	Disable Disable	Enable Enable	Disable Disable	Static Static		Link Down Link Down	=
		LAG4		4	Disable	Enable	Disable	Static		Link Down	
											~
										CANCE	L APPLY
Copyright © 1996-2009	Netgea	ar ®									

LAG 設定をする。

- 1. Switching > LAG > Basic > LAG Configuration を選択して LAG Configuration ページを表示します。
- 2. 設定をする LAG のチェックボックスを選択します。複数を選択して共通項目の設定をすることもできます。
- 3. 以下の項目を確認および設定をします。
 - LAG Name: LAG の名前を記入します。 長さは英数 15 文字までです。
 - Description: LAG の説明を記入します。長さは英数 64 文字までです。
 - LAG ID: LAG に割り当てられた番号を表示します。この欄は読み取りのみです。
 - Link Trap:リンクステータス変更時にトラップの送信の有無を指定します。デフォルトは無効 (Disable)です。
 - Admin Mode: Enable または Disable をメニューから選択します。LAG が無効の場合は、トラフィックは送受信されず、LAG PDU は廃棄されますが、LAG を構成するリンク構成は保持されます。デフォルトは有効です。
 - STP Mode:LAG の STP モードを設定します。
 - LAG Type:スタティック(Static)または LACP を選択します。Static の場合は、LAG PDU を送受 信しません。デフォルトはスタティック(Static)です。
 - Active Ports:アクティブなポートのリストを表示します。一つのLAGは最大4ポートを割り当てることができます。
 - LAG State:アップ(Up)またはダウン(Down)を示します。
- 4. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。
- 5. Apply ボタンをクリックして設定をスイッチに適用します。すぐに設定変更がされます。

LAG メンバーシップ(LAG Membership)

LAG メンバーシップ(LAG Membership)ページを使って LAG を構成します。

NETGEAR Connect with Innovation	•			GS110TP 8 Port Gigabit PoE Smart Switch with 2 Fiber SFP
System Swit	ching QoS	Security Monitoring	Maintenance Help	LOGOUT
Ports LAG VLAN	N Voice VLAN Auto	-VoIP STP Multicast Address T	Table	10
* Basic	LAG Membersh	ip		^
» LAG Configuration	Membership		Ć	D
» LAG Membership	LAG ID	Lag 1 💌	CURRENT MEMBERS	
Advanced	LAG Name	LAG1		
	*			
	<			
				CANCEL
Copyright © 1996-2010	Netgear ®			

LAG を作成する。:

- 1. Switching > LAG > Basic > LAG Membership を選択して LAG Membership ページを表示します。
- 2. LAG ID: 設定する LAG を選択します。
- 3. LAG Name: LAG の名前を記入します。 英数 15 文字までです。
- 4. オレンジのバーを選択してポートを表示します。
- 5. LAG にするポートの下のボックスをクリックして選択します。以下の図はポート 7 と 8 を LAG にする 例です。

: Mei	mbersl	nip								
LAG ID				Lag 1 💌					CURRENT MEMBERS	
LAG Name				LAG1						
•										
Port	1	2	3	4	5	6	7	8	9	10
							X	X		

- 6. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。
- 7. Apply ボタンをクリックして設定をスイッチに適用します。すぐに設定変更がされます。
- 8. LAG を構成するポートを表示するには Current Members ボタンをクリックします。

LACP 設定(LACP Configuration)

NETGEAR Connect with Innovation"							GS108T 8 Port Gigabit Smart Switch
System Switch	ing QoS	Security	Monitoring	Maintenance	Help		LOGOUT
Ports LAG VLAN	Voice VLAN A	uto-VolP STP	Multicast Addr	ess Table			
> Basic	LACP Confi	guration					
 Advanced » LAG Configuration 	LACP Confi	guration	•				
 » LAG Membership » LACP Configuration 	LACP System Priority 32768 (0 to 65535)						
» LACP Port Configuration							
	. 1						
	•						
							CANCEL APPLY

LACP を設定する。

- 1. Switching > LAG > Advanced > LACP Configuration を選択して. LACP Configuration ページを表示 します。
- 2. LACP System Priority:リンクアグリゲーションのプライオリティを指定します。小さな値が高いプライ オリティになります。値の範囲は 0-65535 です。デフォルトは 32768 です。
- 3. Refresh ボタンをクリックしてスイッチの最新情報を表示させます。
- 4. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。
- 5. Apply ボタンをクリックして設定をスイッチに適用します。すぐに設定変更がされます。

LACP ポート設定(LACP Port Configuration)

NETGEAR Connect with Innovation"	5.			GS110TP 8 Port Gigabit PoE Smart Switch with 2 Fiber SFP
System Swi	itching QoS	Security Mo	onitoring Maintenance Help	LOGOUT
Ports LAG VLA	N Voice VLAN	Auto-VoIP STP Mult	icast 🕴 Address Table	
> Basic	LACP Port Pri	ority		^
* Advanced * LAG	LACP Port Pri	iority	0	
Configuration » LAG Membership		GO TO INTER	RFACE GO	
» LACP	Interface	LACP Priority	Timeout	
Configuration				
Configuration	g1	N/A	N/A	
	g2	N/A	N/A	
	g3	N/A	N/A	
	g+	N/A	N/A	
	g6	N/A	N/A	
	g7	N/A	N/A	
	g8	N/A	N/A	
	g9	N/A	N/A	
	g10	N/A	N/A	
ſ	<		110	×
Convright @ 1996-2010	Netgear @			CANCEL

LACP ポートプライオリティを設定する。

- 1. Switching > LAG > Advanced > LACP Port Configuration を選択して. LACP Port Configuration ペ ージを表示します。
- 2. 設定するポートのチェックボックスを選択します。複数のポートを選択して共通の設定をすることもで きます。

メモ:LAGを構成していないポートを選択することはできません。

- 3. LACP Priority:ポート間でパケットの送信値の範囲は 0-255 です。デフォルト値は 128 です。
- 4. Timeout:受信した LACP メッセージを無効にするまでの時間を指定します。Long と Short のタイム アウトを指定します。
 - Long:Long タイムアウト値を使用します。
 - Short: Short タイムアウト値を使用します。
- 5. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。
- 6. Apply ボタンをクリックして設定をスイッチに適用します。すぐに設定変更がされます。

VLAN

レイヤー2 スイッチに VLAN 機能を追加すると、ブリッジングとルーティングの利点の一部を得るこ とができます。 VLAN スイッチはブリッジのように、レイヤー2 ヘッダに基づき高速にデータを転送 し、ルーターのように、管理、セキュリティ、マルチキャストトラフィックの管理に優れたネットワーク の論理的な分割をすることができます。

デフォルトでスイッチのポートは同じブロードキャストドメインに属します。 VLAN は同じスイッチ上 方ポートを電気的に別のブロードキャストドメインに分割し、ブロードキャストパケットがスイッチ上 のすべてのポートに送信されることを防ぎます。 VLAN を使うと、ユーザーを論理的にグループ化 できます。

各 VLAN はパケットのレイヤー2 ヘッダー中の IEEE802.1Q タグの中に設定される VLAN ID を持ちます。端末はタグまたはタグの VLAN 部分を省略し、パケットを最初に受信するスイッチのポートが受信を拒否するか、デフォルト VLAN ID のタグを挿入します。複数の VLAN を扱えるポートもあるが、デフォルト VLAN ID は一つだけです。

VLAN リンクから以下のページにアクセスすることができます。

- VLAN 設定(VLAN Configuration)
- VLAN メンバーシップ設定(VLAN Membership Configuration)
- ポート VLAN 設定(Port VLAN ID Configuration)

VLAN 設定(VLAN Configuration)

VLAN 設定 (VLAN Configuration)ページを使って VLAN メンバーシップテーブル (VLAN membership table)に含まれる VLAN グループを設定します。GS108T と GS110TP は最大 64 の VLAN を扱うことができます。3 つの VLAN はデフォルトで作成されます。
- VLAN 1: すべてのポートがメンバーのデフォルト VLAN。
- VLAN 2: 音声トラフィック用。
- VLAN 3: 自動ビデオトラフィック用。

NETGEAR	r		GS108T
Connect with Innovation**			8 Port Gigabit Smart Switch
System Swi	tching QoS	Security Monitoring	Maintenance Help
Ports LAG VLA	N Voice VLAN A	uto-VoIP STP Multicast Ad	dress Table
* Basic	VLAN Config	uration	
 VLAN Configuration 	VLAN Config	juration	0
Advanced	VLAN ID	VLAN Name	VLAN Type
			Static M
	1	Default	Default
	2	Voice VLAN	Default
	3	Auto-Video	Default
	Reset		0
	Reset Configurat	ion	
			ADD DELETE CANCEL APPLY
Copyright © 1996-200	9 Netgear ®		

VLAN を設定する。

- 1. Switching > VLAN > Basic > VLAN Configuration を選択して. VLAN Configuration ページを表示します。
- VLAN を追加するには、VLAN ID、VLAN 名 (VLAN Name)、VLAN タイプ (VLAN Type)を設定し、 Add ボタンをクリックします。
 - VLAN ID:新しい VLAN ID を入力します。VLAN ID の範囲は 1-4093 です。
 - VLAN Name: VLAN 名を記入できます。英数字の 32 文字までです。空白でも構いません。デフ オルトは空白です。VLAN ID 1 の VLAN 名は常に Default です。
 - VLAN Type: VLAN のタイプを指定します。タイプは Static のみが設定可能です。デフォルトの3 つの VLAN の VLAN Type は Default で変更不可です。
- 3. VLAN を削除するには、削除する VLAN のチェックボックスを選択し、Delete ボタンをクリックしま す。デフォルトの 3 つの VLAN を削除することはできません。
- 4. VLAN の設定を変更するには、変更をする VLAN のチェックボックスを選択し、Apply ボタンをクリックします。すぐに設定変更がされます。
- 5. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。
- 6. VLAN 設定をリセットするには、Reset Configuration チェックボックスを選択し、ポップアップメッセージウィンドウの OK ボタンをクリックします。

VLAN メンバーシップ設定(VLAN Membership Configuration)

VLAN Membership Configuration ページで VLAN ポートメンバーシップを設定します

NETGEA Connect with Innovation"	R'														GS110TP 8 Port Gigabit PoE Smart Switch with 2 Fiber SFP
System S	witching	Q	oS	Sec	curity		Monito	oring	N	ainte	nance	He	lp		
Ports LAG V	LAN Void	e VLAN	Aut	o-VolP	STI	P M	ulticast	Ad	dress Ta	ble					
Basic Advanced VI AN	VLAN	Mem	bers	hip lip										(2)	·
Configuration	VLAN	(D		1	~			Grou	p Opera	tion		Untag All	~		
* VLAN Membershin	VLAN	Name		De	efault			UNT	AGGED	ORT M	EMBERS				
» Port PVID	VLAN	Гуре		De	efault			TA	GGED P	ORT ME	MBERS				=
Connguration	Port	1	2	3	4	5	6	7	8	9	10				
	• L	AG													
	<														×
															CANCEL APPLY
Copyright © 1996-20	010 Netgear	®													

VLAN メンバーシップを設定する。

- 1. Switching > VLAN > Advanced > VLAN Membership を選択して VLAN Membership Configuration ページを表示します。
- 2. ポートを設定したい VLAN ID を選択します。
- 3. VLAN Type 欄の下のオレンジ色のバーをクリックして、スイッチの物理ポートを表示します。
- 4. 下のオレンジ色のバーをクリックしてスイッチの LAG を表示します。
- 5. VLAN に追加したいポートまたは LAG をクリックして選択します。それぞれのインターフェースをタグ 付き(T)またはタグ無し(U)として追加できます。
 - Tagged:このポートから送信されるフレームはポートの VLAN ID のタグ付きで送信されます。
 - Untagged:このポートから送信されるフレームはタグ無しで送信されます。ポートは一つの VLANのみに属します。デフォルトでは、すべてのポートは VLAN 1 のタグ無しポートになってい ます。

以下の図で、ポートg6,g7,およびg8がVLAN2のタグ付きポートに設定されています。

VLA	N Mer	nbers	hip										- (
VLAN	D		2	×			Group	o Opera	tion		Untag All	~	
VLAN	Name		Vo	oice VL	AN		UNT	AGGED	PORT MI	EMBERS			
VLAN	Гуре		De	efault			TA	GGED P	ORT ME	MBERS			
Port		2	3	4	5	6	7	8	0	10			
· on			, in the second s			Т	T	т	-	10			

- 6. Group Operations 欄を使って、すべてのポートと LAG の設定をすることができます。
 - Untag All: すべてのポートをタグ無しにします。
 - Tag AI: すべてのポートをタグ付きにします。

- Remove All: すべてのポートを選択した VLAN から削除します。
- 7. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。
- 8. Apply ボタンをクリックして設定をスイッチに適用します。すぐに設定変更がされます。

ポート VLAN 設定(Port VLAN ID Configuration)

ポート PVID 設定 (Port PVID Configuration)ページでポート VLAN ID (PVID) をインターフェースに 割り当てます。

- すべてのポートは設定済みの PVID を持つ必要があります。
- 指定されない場合はデフォルト VLAN の PVID が使われます。
- ポートのデフォルト PVID を変更するには、ポートをメンバーとして持つ VLAN を作成する必要があります。
- Port VLAN ID (PVID) Configuration ページを使ってポートに VLAN を作成します。

ystem Sw	ritching Qo	S Sec	urity Monit	oring N	laintenance Help	LOGO
rts LAG VU	N Voice VLAN	Auto-VolP	STP Multicas	t Address To	ble	
sic	Port PVID	Configu	ration			
lvanced						
/LAN	PVID Cont	iguration			()	
/LAN	PORTS LAG	5 All	GO TO I	NTERFACE	GO	
Aembership Port PVID	Interfac	e (1 to 4093)	Acceptable Frame Types	Ingress Filtering	Port Priority (0 to 7)	
omguration			×	~		
	g 1	1	Admit All	Disable	0	
	g 2	1	Admit All	Disable	0	
	g 3	1	Admit All	Disable	0	
	g 4	1	Admit All	Disable	0	
	g5	1	Admit All	Disable	0	
	□ g6	1	Admit All	Disable	0	
	g7	1	Admit All	Disable	0	
	2 g8	1	Admit All	Disable	0	
	PORTS LAG	5 All	GO TO I	NTERFACE	GO	
	(*)					

PVID 情報を設定する。To configure PVID information:

- 1. Switching > VLAN > Advanced > Port PVID Configuration を選択して Port PVID Configuration ペ ージを表示します。
- 2. PORTS をクリックして物理ポートの PVID 設定をします。
- 3. LAGS をクリックして LAG の PVID 設定をします。
- 4. ALL をクリックして物理ポートと LAG の PVID 設定をします。
- 5. 設定するインターフェースのチェックボックスを選択します。複数のインターフェースを選択して共通 部分の設定をすることもできます。先頭のチェックボックスをクリックするとすべてのインターフェース を選択できます。
- 6. PVID:ポートの PVID を指定します。

- Acceptable Frame Types:ポートが受信したフレームをどう処理するか指定します。どちらの設定でも、VLAN タグ付きフレームは IEEE802. 1Q 標準に従って転送されます。デフォルト設定は Admit All です。
 - VLAN Only: VLAN タグ付きフレームのみを受信します。
 - Admit All: VLAN タグのついていないフレームはポート VLAN ID が割り当てられます。
- 8. Ingress Filtering:タグ付きフレームの処理方法を指定します。
 - Enable:ポートの VLAN ID と異なる VLAN のフレームを廃棄します。タグ無しのフレームはポート VLAN ID と同じ VLAN ID となります。
 - Disable: すべてのフレームは IEEE802.1Q 標準に従って転送されます。デフォルト設定は: Disable です。
- 9. Port Priority (0 to 7): 受信したタグ無しフレームに対して割り当てられる 802.1p 優先度を指定しま す。0-7 の範囲です。
- 10. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。
- 11. Apply ボタンをクリックして設定をスイッチに適用します。すぐに設定変更がされます。

ボイス VLAN(Voice VLAN)

IP 電話機からのトラフィックを運ぶポートのボイス VLAN 設定をします。ボイス VLAN 機能は IP 電話機の音声品質をデータトラフィックによって劣化することを防ぎます。

Voice VLAN リンクから以下のページにアクセスできます。

- ボイス VLAN プロパティ(Voice VLAN Properties)
- ボイス VLAN ポート設定(Voice VLAN Port Setting)
- ・ ボイス VLAN OUI(Voice VLAN OUI)

ボイス VLAN プロパティ(Voice VLAN Properties)

NETGEAR [*] Connect with Innovation ^{**}	GS110TP 8 Port Gigabit PoE Smart Switch with 2 Fiber SFP
System Switching QoS Security Monitoring Maintenance	Нејр
Ports LAG VLAN Voice VLAN Auto-VoIP STP Multicast Address Table	
(<)	CANCEL APPLY

ボイス VLAN を設定する。

1. Switching > Voice VLAN > Basic > Properties を選択して Voice VLAN Properties ページを表示し

ます。

- 2. Voice VLAN Status: スイッチでボイス VLAN を使うかどうか設定します。使用する場合は Enable を 選択します。IP 電話機からのトラフィックを扱わない場合は Disable を選択します。
- 3. Voice VLAN ID:ボイストラフィックを運ぶ VLAN ID を指定します。VLAN は設定済みである必要が あります。
- 4. Class of Service: Remark CoS が有効(Enable)である場合に、ボイス VLAN として受信したパケット に割り当てる CoS 値を指定します。
- 5. Remark CoS:受信したパケットの CoS 値を割り当てるときに有効(Enable)にします。
- 6. Voice VLAN Aging Time: 受信した IP 電話機からのパケットの OUI の有効期間を指定します。1 分から 30 日の範囲で指定します。
- 7. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。
- 8. Apply ボタンをクリックして設定をスイッチに適用します。すぐに設定変更がされます。

ボイス VLAN ポート設定(Voice VLAN Port Setting)

Onnect with Innovati	A K				8 Port Gigabit Smart Swi
System	Switching	QoS Se	curity Monitorin	Maintenance Help	LOGOL
Ports LAG	VLAN Voice V	/LAN Auto-Voli	P STP Multicast	Address Table	
Basic	Port S	etting			
dvanced	Port	Setting		(2)	
Port Setting		betting	CO TO INTE	REACE	
OUI	Select	Interface	Voice VI AN Mode	Membership	
			Enable 💙		
		g1	Disable	Not Active	
		g2	Disable	Not Active	
		g3	Disable	Not Active	
		g4	Disable	Not Active	
		g5	Disable	Not Active	
		g6	Disable	Not Active	
		g7	Disable	Not Active	
		ga			
			GOTOINTE		
	<][:

ボイス VLAN ポート設定をする。

- 1. Switching > Voice VLAN > Advanced > Port Setting を選択して Voice VLAN Port Setting ページ を表示します。
- 2. 設定するポートのチェックボックスを選択します。複数のポートを選択して共通の設定をすることもで きます。先頭のチェックボックスをクリックするとすべてのポートを選択できます。
- 3. Voice VLAN Mode:ポートでボイス VLAN を有効(Enable)にするか選択します。
- 4. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。
- 5. Apply ボタンをクリックして設定をスイッチに適用します。すぐに設定変更がされます。

メモ:Membership 欄はポートのボイス VLAN 状態が有効(Active)かどうかを示します。

ボイス VLAN OUI(Voice VLAN OUI)

スイッチは以下の IP 電話機メーカーの OUI 設定がされています。

- 00:01:E3: SIEMENS
- 00:03:6B: CISCO1
- 00:12:43: CISCO2
- 00:0F:E2: H3C
- 00:60:B9: NITSUKO
- 00:D0:1E: PINTEL
- 00:E0:75: VERILINK
- 00:E0:BB: 3COM
- 00:04:0D: AVAYA1
- 00:1B:4F: AVAYA2

新しい OUI の設定や OUI の記述を変更することができます。

NETGE	A R'				GS108T
Connect with Innovati	on."				8 Port Gigabit Smart Switch
System	Switching	QoS Security	Monitoring	Maintenance H	lelp (LOGOUT)
Ports LAG	VLAN Voice	VLAN Auto-VolP ST	P Multicast Add	ress Table	
Basic	OUI				<u>^</u>
* Advanced » Properties	OUI			۲	
» Port Setting	Select	Telephony OUI(s)	Description		
* <u>OUI</u>					
		00:01:E3	SIEMENS		
		00:03:6B	CISCO1		
		00:12:43	CISCO2		
		00:0F:E2	НЗС		
		00:60:89	NITSUKO		
		00:D0:1E	PINTEL		
		00:E0:75	VER ILINK		
		00:E0:BB	3COM		
		00:04:0D	AVAYA1		
		00:1B:4F	AVAYA2		
	<			illi	
				ADD	DELETE CANCEL APPLY RESTORE DEFAULTS
Copyright © 199	6-2009 Netgear	8			

OUI 設定をする。

- 1. Switching > Voice VLAN > Advanced > OUI.を選択して Voice VLAN OUI ページを表示します。
- 2. Telephony OUI(s):OUI 値を設定します。OUI プレフィクスと説明を記入し、Add ボタンをクリックしま す。OUI プレフィクスの形式は、AA:BB:CC とします。
- 3. リスト中の OUI プレフィクスを削除するには、削除する OUI のチェックボックスを選択し、Delete ボタ ンをクリックします。
- 4. OUI 設定を変更するには、変更する OUI のチェックボックスを選択し、変更をします。変更後、Apply ボタンをクリックします。
- 5. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。

6. Restore Defaults ボタンをクリックして初期設定に戻します。

オート VoIP(Auto-VoIP)

オート VoIP(Auto-VoIP)は、この機能が有効なポートで、遅延に敏感な音声トラフィックに自動的に データトラフィックよりも高い優先度を与えます。オート VoIP(Auto-VoIP)は、以下の VoIP プロトコ ルを運ぶパケットをチェックします。

- SIP(Session Initiation Protocol)
- • H.323
- SCCP(Signaling Connection Control Part)
- MGCP(Media Gateway Control Protocol)

オート VoIP が有効にされたポートで受信した VoIP フレームは CoS 値が 3 に設定されます。

NETGE Connect with Innovati	AR'					6 Port Gigabit PoE Smart Switch with 2 Fiber SFP
System	Switching	QoS S	ecurity Monitoring	Maintenance	Help	LOGOUT
Ports LAG	VLAN Voice	VLAN Auto-Vo	STP Multicast A	ddress Table		
v Auto-VoIP	Auto-V	OIP Configu	ration			^
	Auto	-VoIP Configura	ation	(7)		
			GO TO INTERFA			
		Interface	Auto-VoIP Mode	Traffic Class		
		g1	Enable	3		
		g2	Enable	3		
		g3	Enable	3		=
		94	Enable	3		
		06	Enable	3		
		g7	Enable	3		
		g8	Enable	3		
		g9	Enable	3		
		g10	Enable	3		
			GO TO INTERFA	CE GO		
	<			III		
						CANCEL
Copyright © 1996	-2010 Netgear @	0				

オート VoIP 設定をする。

- 1. Switching > Auto-VoIP を選択して Auto-VoIP ページを表示します。
- 2. 設定するポートのチェックボックスを選択します。複数のポートを選択して共通の設定をすることもで きます。先頭のチェックボックスをクリックするとすべてのポートを選択できます。
- 3. Auto-VoIP Mode:選択したポートでオート VoIP を有効(Enable)にします。
- 4. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。
- 5. Apply ボタンをクリックして設定をスイッチに適用します。すぐに設定変更がされます。

スパニングツリープロトコル(Spanning Tree Protocol)

スパニングツリープロトコル(STP)はブリッジの配置に対してツリートポロジーを提供します。STP

はまたネットワークの端末間に唯一の経路を提供し、ループを排除します。スパニングツリーには Common STP、Multiple STP、Rapid STP があります。

古典的な STP はループを防止および排除し、端末間の一つの経路を提供します。

MST(Multiple Spanning Tree Protocol)は VLAN トラフィックを異なるインターフェースに効率的に 流すために複数の STP をサポートします。各スパニングツリーは IEEE802.1w の RSTP(Rapid Spanning Tree)のように動作します。RSTP と伝統的な STP(IEEE802.1D)の違いは、全二重の接続 性を設定および認識する能力、およびエンド端末に接続されているポートを高速に Forwarding 状 態に変移させ、トポロジーチェンジ通知を抑えることです。これらの機能は"ポイントトゥポイント (point to point)"と"エッジポート(edge port)"と呼ばれます。MSTP は RSTP と STP と互換があり ます。MSTP は STP と RSTP ブリッジと適切に動作します。MSTP ブリッジは RSTP あるいは STP ブリッジと全く同じように設定することができます。

メモ:2つのブリッジが混在する場合、動作するバージョンは 802.1s であるべきであり、設定、名前、digest key, revision level は一致するべきです。

STPリンクから以下の機能にアクセスできます。

- STP スイッチ設定(STP Switch Configuration)
- CST 設定(CST Configuration)
- CST ポート設定(CST Port Configuration)
- CST ポートステータス (CST Port Status)
- Rapid STP
- MST 設定(MST Configuration)
- MST ポート設定(MST Port Configuration)
- STP 統計(STP Statistics)

STP スイッチ設定(STP Switch Configuration)

STP Configuration ページでスイッチの STP を有効にする事ができます。

And with Innovation" System Switching Ports LAG VLAN Voice tasic STP C Configuration STP Ope Configur Configur BPDU Fil	QoS Security VIAN Auto-VolP STF configuration bal Settings g Tree State ration Mode ration Name ration Revision Level ration Digest Key soding	Monitoring Maintenance Help Multicost Address Toble Olisable Enable STP RSTP MSTP 00-24-B2-5C-96-49 0 (0 to 65535) Drar61727570283ct4483821d8ab26d	8 Port Gigabit Smart Sw
System Switching Ports LAG VIAN Voice Lasic STP C Configuration Xdvanced Spannin STP Ope Configur Configur BPDU Fi	QoS Security VIAN Auto-VolP STF configuration bal Settings g Tree State ration Mode ration Name ration Revision Level ration Digest Key coding	Monitoring Maintenance Help Multicat Address Toble Olisable Enable STP RSTP MSTP 00-24-B2-5C-96-49 0 (0 to 65535) Drar36127550283ctd483821d8ab26d	000)
Avers LAG VLAN Voice static STP Configuration Advanced Spannin STP Ope Configu Configu BPDU Fl	VIAN Auto-VolP ST Onfiguration bal Settings g Tree State ration Mode ration Name ration Revision Level ration Revision Revision Level ration Revision Revision Level ration Revision Rev	Multicost Address Toble • Disable • STP • Oc-24-B2-5C-96-49 • O to 65535) Oxar36127(50283ctd483821d8ab26d	
asic STP Configuration dvanced Spannin STP Ope Configur Configur BPDU FI	Configuration bal Settings g Tree State ration Mode ration Name ration Revision Level ration Digest Key sodian	Oisable Enable STP MSTP MSTP 00-24-B2-5C-96-49 0	
STP Configuration dvanced Spannin Configur Configur BPDU FI	pal Settings g Tree State eration Mode ration Name ration Devision Level ration Digest Key coding	Disable Enable STP RSTP MSTP 00-24-B2-5C-96-49 0 to 65535) 0xar36127(50283cd4883821d8ab26d	
Configuration dvanced Spannin STP Ope Configur Configur BPDU FI	oal Settings g Tree State eration Mode ration Name ration Revision Level ration Digest Key ooding	Disable Enable STP RSTP MSTP 00-24-B2-5C-96-49 0 to 65535) 0xar36127(50283rd4)83821d8ab26d	
dvanced Spannin STP Ope Configu Configu BPDU FI	g Tree State eration Mode ration Name ration Revision Level ration Digest Key ordina	Disable Disable STP RSTP MSTP 00-24-B2-5C-96-49 (0 to 65535) 0xar36127(50283cd4883821d8ab26d	
	ocumy	All 💌 💿 Disable 🔘 Enable	
STP	Status	٥	
Bridge I Time Sir Topolog Topolog Designa	dentifier ice Topology Change y Change Count y Change ted Root	80:00:00:24:b2:5c:96:49 0 day 13 hr 1 min 14 sec 0 False 80:00:00:24:b2:5c:96:49	
Root Pa Root Po Max Aos	th Cost rt = (secs)	0	
Forward Hold Tin	Delay (secs) ne (secs)	15 6	
CST Reg CST Pat	ional Root h Cost	80:00:00:24:b2:5c:96:49 0	
<		m][

スイッチの STP 設定をする。

- 1. Switching > STP > Basic > STP Configuration を選択して STP Configuration ページを表示します。
- 2. Spanning Tree State:スイッチでスパニングツリーを有効(Enable)にします。
- 3. STP Operation Mode: STP のモードを選択します。
 - **STP:** (Spanning Tree Protocol): IEEE 802.1D
 - **RSTP:** (Rapid Spanning Tree Protocol): IEEE 802.1w
 - MSTP: (Multiple Spanning Tree Protocol): IEEE 802.1s
- 4. 設定名 (Configuration Name) と更新レベルを指定します。
 - Configuration Name: 設定に名前をつけます。 英数32文字までです。
 - Configuration Revision Level: 更新レベルとして数字を入力します。範囲は 0-65535 です。
- 5. BPDU Flooding:STP が無効の際に、BPDU Flooding をすべてのポートかポート単位に有効にする か指定します。この機能が有効(Enable)にされると、受信した BPDU パケットは他のポートにフラッ ディングされます。
- 6. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。
- 7. Apply ボタンをクリックして設定をスイッチに適用します。すぐに設定変更がされます。
- 以下の表に STP Status 欄に表示される情報の説明を示します。

項目	説明
Bridge Identifier	CST(Common Spanning Tree)のブリッジ ID。 ブリッジプライオ リティとブリッジのベース MAC アドレスからなります。
Time Since Topology Change	CST(Common Spanning Tree)のトポロジーチェンジが発生し てからの時間(秒)

Topology Change Count	CST(Common Spanning Tree)でのトポロジーチェンジの回 数。
Topology Change	トポロジーチェンジが進行中(True)かどうかを示します。
Designated Root	ルートブリッジのブリッジ ID。ブリッジのブリッジプライオリティ とMAC アドレスからなります。
Root Path Cost	CST のルートブリッジへのパスコスト。
Root Port	CST のルートヘアクセスするポート。
Max Age (secs)	最大エージタイム(秒)
Forward Delay (secs)	フォワードディレイ(秒)
Hold Time (secs)	Configuration BPDUs を送信する最小間隔(秒).
CST Regional Root	CST Regional Root のブリッジ ID。
CST Path Cost	CST の Regional Root へのパスコスト。

Refresh ボタンをクリックしてスイッチの最新情報を表示させます。

CST 設定(CST Configuration)

Spanning Tree CST Configuration ページで CST(Common Spanning Tree)と IST(Internal Spanning Tree)を設定します。

NETGEAR	5.					B Port Gigabit PoE Smart Sw with 2 Fiber
System Swi	itching	QoS Security	Monito	oring Mainte	nance Help	LOGOU
Ports LAG VLA	N Voice VL	AN Auto-VolP S1	iP Multicast	Address Table		
Basic	CST Con	figuration				
Advanced » STP	· CST Co	nfiguration			0	
Configuration	Bridge Prio	rity	32768	(0 to 61440)		
	Bridge Max	Age (secs)	20	(6 to 40)		
» CST Port	Bridge Helle	Time (secs)	2			
Configuration	Bridge Forv	vard Delay (secs)	15	(4 to 30)		
» CST Port Status	Spanning T	ree Maximum Hops	20	(1 to 127)		
» RSTP » MST						
Configuration	. MSTP S	Status			(1)	
» MST Port	MST ID	VID	FI	D		
Configuration	CST	123	1	23		
· on otdisites						
	<					
						REFRESH CANCEL APPLY

CST の設定をする。

1. Switching > STP > Advanced> CST Configuration を選択して CST Configuration ページを表示します。

- 2. 以下の情報を設定します。
 - Bridge Priority: STP が動作している時にブリッジやスイッチにはプライオリティが設定されます。BPDU の交換後一番小さなプライオリティのスイッチがルートブリッジになります。 CST(Common Spanning Tree)とIST(Internal Spanning Tree)にプライオリティを設定します。有効な値の範囲は 0-61440 です。ブリッジプライオリティは 4096 の倍数になります。4096 の倍数以外に設定した場合は、その値より小さくかつ近い 4096 の倍数に設定されます。0~4095 の範囲の値を設定すると、0 と設定されます。デフォルト値は 32768 です。
 - Bridge Max Age (secs): CST(Common Spanning Tree)と IST(Internal Spanning Tree)のトポロジ ーチェンジを実行するまで待機するブリッジ最大エージタイム(秒)を設定します。有効な範囲は 6-40(秒)です Specifies the bridge maximum age time for the Common and Internal Spanning Tree (CST)。デフォルト値は 20(秒)です。
 - Bridge Hello Time (secs):. CST(Common Spanning Tree)とIST(Internal Spanning Tree)の Hello Time。デフォルトは 2(秒)です。
 - Bridge Forward Delay (secs): Bridge Forward Delay 時間を設定します。範囲は 4-30(秒)です。
 デフォルトは 15(秒)です。
 - Spanning Tree Maximum Hops: Spanning Tree Maximum Hops を指定します。範囲は 1-127 で す。
- 3. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。
- 4. Apply ボタンをクリックして設定をスイッチに適用します。すぐに設定変更がされます。

以下に CST Configuration ページの MSTP Status 欄に表示される情報の説明を示します。

項目	説明
MST ID	MST インスタンス(CST を含む)と対応する VLAN ID。
VID	VLAN ID と対応する FID (Filter ID)。
FID	FID と対応する VLAN ID。

Refresh ボタンをクリックしてスイッチの最新情報を表示させます。

CST ポート設定(CST Port Configuration)

CST Port Configuration ページで CST(Common Spanning Tree)と IST(Internal Spanning Tree)の ポート設定をします。

vstem Swit	tching	QoS	Securit	Monit	oring Maint	engace	Help			[
	N Vo	ice VLAN	Auto-VolP	STP Multicast	Address Table	cillanco	norp			
	CET	Dort Co	nfiguratio	n						
vanced	COL	FUILCO	ingurado							
TP	P	ort Config	uration							(7)
Configuration	POR	IS LAG	5 All					GO TO INTERFACE		GO
Configuration		Interface	STP Status	Fast Link	Port State	Path Cost	Priority	External Port Path Cost	Port ID	Hello Timer
onfiguration			×	×						
ST Port Status		g1	Disable	Disable	Manual forwarding	0	128	0	32769	2
IST		g2	Disable	Disable	Disabled	0	128	0	32770	2
onfiguration		g3	Disable	Disable	Disabled	0	128	0	32771	2
IST Port		g4	Disable	Disable	Disabled	0	128	0	32772	2
TP Statistics		g5	Disable	Disable	Disabled	0	128	0	32773	2
		g6	Disable	Disable	Disabled	0	128	0	32774	2
		g7	Disable	Disable	Disabled	0	128	0	32775	2
		g8	Disable	Disable	Disabled	0	128	0	32776	2
	POR	TS LAG	5 All				3	GO TO INTERFACE		GO
	<					1				

CST ポート設定をする。

- 1. Switching > STP > Advanced > CST Port Configuration を選択して CST port settings ページを表示します。
- 2. PORTS をクリックして、物理ポートの CST 設定をします。
- 3. LAGS をクリックして、Link Aggregation Group (LAG)の CST 設定をします。
- 4. ALL をクリックして、物理ポートと Link Aggregation Group (LAG)の両方の CST 設定をします。
- 5. 設定をしたいポートまたは LAG の横のチェックボックスをクリックして選択をします。複数の選択も 可能です。
- 6. 選択したポートまたは LAG の CST 設定をします。
 - STP Status:ポートまたは LAG で STP を有効(Enable)にするか設定します。
 - Fast Link: CST でエッジポート(Edge Port)かどうかを指定します。デフォルトは Disable です。
 - Port State:ポートの状態を示します。読み取りのみです
 - Path Cost:パスコストを設定します。有効な範囲は 1-200000000 です。
 - Priority:ポートプライオリティを設定します。16の倍数である必要があり、それ以外の場合はそれ以下の最大の16の倍数に設定されます。
 - External Port Path Cost:範囲は 1-200000000 です。
 - Port ID:.CST 内でのポート ID を示します。ポートプライオリティとポートのインターフェース番号からなります。
 - Hello Timer: 値は固定で2(秒)です。
- 7. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。
- 8. Apply ボタンをクリックして設定をスイッチに適用します。すぐに設定変更がされます。

9. Refresh ボタンをクリックしてスイッチの最新情報を表示させます。

CST ポートステータス(CST Port Status)

CST Port Status ページでポートの CST(Common Spanning Tree)と IST(Internal Spanning Tree) 状態を表示します。

Switching > STP > Advanced >CST Port Status を選択して CST Port Status ページを表示します。

sets LAG VLAN Vo	ice VLAN Auto-1	VoIP ST	Monitoring M Multicost Address Tob	aintenance Ne	Help							(190		
asic	CST Port	CST Port Status												
dvanced STP Confinuation	CST Por	CST Port Status 0												
CST Configuration	PORTS	LAGS	All											
CST Port Configuration CS1 Port Status	Interface	Port Role	Designated Root	Designated Cost	Designated Bridge	Designated Port	Topology Change Acknowledge	Edge Port	Point- to-Point MAC	CST Regional Root	CST Path Cost	Port Forwarding State		
RSTP #ST Configuration	g1	Disabled	801001001241b21e3102157	0	80:00:00:24:b2:e3:02:57	0	False	False	True	801001001241b21e3102157	0	Manual forwardin		
4ST Port	g2	Disabled	80:00:00:24:b2:e3:02:57	0	80:00:00:24:b2:e3:02:57	0	False	False	False	80:00:00:24:b2:e3:02:57	0	Disabled		
Configuration	03	Disabled	80:00:00:24:52:e3:02:57	0	801001001241b21e3102157	0	False	False	Falze	801001001241521e3102157	0	Disabled		
TP Statistics	94	Disabled	80:00:00:24:b2:e3:02:57	0	80:00:00:24:b2:e3:02:57	0	False	False	False	80:00:00:24:b2:e3:02:57	ō	Disabled		
	0.5	Disabled	80100100124162143102157	0	80:00:00:24:52:e3:02:57	0	False	False	False	801001001241b2re3102157	ô	Disabled		
	96	Disabled	80:00:00:24:52:63:02:57	0	80:00:00:24:52:63:02:57	0	False	False	False	80:00:00:24:b2:e3:02:57	0	Disabled		
	97	Disabled	80:00:00:24:b2:e3:02:57	0	80:00:00:24:b2:e3:02:57	0	False	False	False	80:00:00:24:b2:e3:02:57	0	Disabled		
	98	Disabled	80100100124192143102157	0	80:00:00:24:52:43:02:57	0	False	False	False	801001001241b21e3102157	0	Disabled		
	g.9	Disabled	801001001241b21e3102157	0	80:00:00:24:b2:e3:02:57	0	False	False	False	\$01001001241b21e3102157	0	Disabled		
	g10	Disabled	80100100124:521e3102:57	0	801001001241b21e3102157	0	False	False	Falze	801001001241b21e3102157	0	Disabled		
	PORTS	LACS	All											

以下に CST Port Status 欄に表示される情報の説明を示します。

Refresh ボタンをクリックしてスイッチの最新情報を表示します。

項目	説明
Interface	スイッチのインターフェース番号。
Port Role	ポートロール。以下のうちの一つ。Root Port, Designated Port, Alternate Port, Backup Port, Master Port, Disabled Port.
Designated Root	ルートブリッジ ID。
Designated Cost	STP トポロジーに参加しているポートのコスト。
Designated Bridge	ルートポートに接続されているブリッジのブリッジ ID。
Designated Port	ルートポートのポート ID。
Topology Change Acknowledge	次に送信される BPDU が topology change acknowledgement flag が設定されているかどうか。 True ま たは False 。
Edge Port	エッジポートに設定されているかどうか。Enabled または Disabled.
Point-to-point MAC	ポイント-ポイント接続かどうか。True はたは False。
CST Regional Root	CST のルートブリッジ ID。

CST Path Cost	CST のパスコスト。
Port Forwarding State	ポートのフォワーディング状態。

Rapid STP

Rapid STP ページで RSTP のポート状態を表示します。

Switching > STP > Advanced > RSTP.を選択して Rapid STP ページを表示します。

Basic	Rapid STP					
» STP	Rapid STP					0
Configuration * CST	PORTS LAGS	All				
Configuration	Interface	Role	Mode	Fast Link	Status Manual facuarding	
» CST Port	g1	Disabled	METD	False	Disabled	
» CST Port Status	03	Disabled	MSTP	False	Disabled	
	g4	Disabled	MSTP	False	Disabled	
» MST Configuration	g5	Disabled	MSTP	False	Disabled	
» MST Port	g6	Disabled	MSTP	False	Disabled	
Configuration	g7	Disabled	MSTP	False	Disabled	
» STP Statistics	g8	Disabled	MSTP	False	Disabled	
	PORTS LAGS	All				

以下に Rapid STP 欄に表示される情報の説明を示します。

項目	説明
Interface	スイッチのポートまたは LAG 番号。
Role	ポートロール。Root Port, Designated Port, Alternate Port, Backup Port, Master Port または Disabled Port.
Mode	STP のモード。STP, RSTP または MSTP.
Fast Link	エッジポート設定。
Status	インターフェースのフォワーディング状態。

Refresh ボタンをクリックしてスイッチの最新情報を表示させます。

MST 設定(MST Configuration)

MST Configuration ページでスイッチの MST(Multiple Spanning Tree) 設定をします。

NETGEAR	9 5									8 Port Gigal	GS110T bit PoE Smart Swi with 2 Fiber S
System Swit	ching Qo	S Secu	rity	Monitoring) Mai	ntenance	Help	Ì			LOGOU
Ports LAG VLAN	Voice VLAN	Auto-VoIP	STP	Multicast /	Address Table						
Basic	MST Config	juration									
* Advanced * STP Configuration	BST Conf	iguration								(?)	
 > CST Configuration > CST Port Configuration > CST Port Status 	MST ID	Priority	Vlan Id	Bridge Identifier	Time Since Topology Change	Topology Change Count	Topology Change	Designated Root	Root Path Cost	Root Port	
» RSTP» MST Configuration											
 MST Port Configuration STD Statistics 											
# STP Statistics											
	<					Ш					
								ADD	DEI	FTF CAN	NCEL APPLY

MST を設定する。

- 1. Switching > STP > Advanced > MST Configuration を選択して MST Configuration ページを表示し ます。
- 2. MST を追加するには、以下の情報を設定して Add ボタンをクリックします。
 - MST ID: MST ID を 1-4094 の範囲で記入します。
 - Priority: MST のブリッジプライオリティを設定します。BPDU の交換後一番小さなプライオリティ のスイッチがルートブリッジになります。ブリッジプライオリティは 4096 の倍数になります。4096 の倍数以外に設定した場合は、その値より小さくかつ近い 4096 の倍数に設定されます。0~ 4095 の範囲の値を設定すると、0と設定されます。デフォルト値は 32768 です。有効な値の範 囲は 0-61440 です。
 - VLAN ID: MST と関連付ける VLAN ID を選択します。
- 3. MST を削除するには、削除する MST のチェックボックスを選択し、Delete ボタンをクリックします。
- 4. MST 設定を変更するには、変更する MST のチェックボックスを選択し、変更をします。変更後、 Apply ボタンをクリックします。
- 5. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。

項目	説明
Bridge Identifier	MST のブリッジ ID。
Time Since Topology Change	前回の MST トポロジーチェンジからの時間。
Topology Change Count	MST のトポロジーチェンジの回数。
Topology Change	トポロジーチェンジが実行中かどうかを示します。 True または False.
Designated Root	MST のルートブリッジ ID.
Root Path Cost	MST のルートパスコスト。

以下に MST Configuration 欄に表示される情報の説明を示します。

```
Root Port
```

ルートブリッジへのポート。

MST ポート設定(MST Port Configuration)

MST Port Configuration ページでポートの MST 設定をします。

10.5	Status										
Sele	Select MST 12 💌										
	MST Port Co	onfiguratio	n				_				
POF	LAGS	5 All									
	Interface	Port Priority	Port Path Cost	Auto Calculated Port Path Cost	Port ID	Port Up Time Since Counters Last Cleared	Port Mode				
]							
	g1	128	200000	Enable	32769	0 day 0 hr 0 min 12 sec	Enabled				
	g2	128	0	Enable	32770	0 day 0 hr 0 min 13 sec	Enabled				
	g3	128	0	Enable	32771	0 day 0 hr 0 min 13 sec	Disabled				
	g4	128	0	Enable	32772	0 day 0 hr 0 min 13 sec	Disabled				

					0				
				do to Inteki Ace	00				
Port Forwarding State		Designated Root	Designated Cost	Designated Bridge	Designated Port				
Forwarding	Master	80:0c:02:18:12:aa:bb:cc	0	80:0c:02:18:12:aa:bb:cc	32769				
Disabled	Disabled	80:0c:02:18:12:aa:bb:cc	0	80:0c:02:18:12:aa:bb:cc	0				
Disabled	Disabled	80:0c:02:18:12:aa:bb:cc	0	80:0c:02:18:12:aa:bb:cc	0				
Disabled	Disabled	80:0c:02:18:12:aa:bb:cc	0	80:0c:02:18:12:aa:bb:cc	0				

メモ:スイッチで MST が設定されていない場合は、"No MSTs Available"というメッセージ (下図参照)が表示され他には何も表示されません。

Status		0
	No MSTs Available	

MST ポート設定をする。

- 1. Switching > STP > Advanced > MST Port Configuration を選択して MST Port Configuration ペー ジを表示します。
- 2. PORTS をクリックして、物理ポートの MST 設定をします。
- 3. LAGS をクリックして、Link Aggregation Group (LAG)の MST 設定をします。
- 4. ALL をクリックして、物理ポートと Link Aggregation Group (LAG)の両方の MST 設定をします。
- 5. 設定をしたいポートまたは LAG の横のチェックボックスをクリックして選択をします。複数の選択も 可能です。
- 6. 選択したポートまたは LAG の MST 設定をします。

- Port Priority: MST のポートプライオリティを設定します。ポートプライオリティは 16 の倍数になります。16 の倍数以外に設定した場合は、その値より小さくかつ近い 16 の倍数に設定されます。0~15 の範囲の値を設定すると、0と設定されます。有効な値の範囲は 0-240 です。デフォルトは 128 です。
- Port Path Cost:ポートパスコストを設定します。値の範囲は 1-200000000 です。
- 6. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。
- 7. Apply ボタンをクリックして設定をスイッチに適用します。すぐに設定変更がされます。

以下に MST Port Configuration 欄に表示される読み取りのみの情報の説明を示します。

Field	Description
Auto-calculated Port Path Cost	パスコストの自動計算。
Port ID	MST のポート ID。
Port Up Time Since Counters Last Cleared	カウンターが初期化されてからの時間。
Port Mode	STP モードの 有効(Enable)または 無効(Disable)。
Port Forwarding State	ポートの STP 状態。 • Disabled • Blocking • Listening • Learning • Forwarding
Port Role	MST のポートロール。 Root Port, Designated Port, Alternate Port, Backup Port, Master Port, または Disabled Port.
Designated Root	MST のルートブリッジ ID。
Designated Cost	STP トポロジーに参加しているポートのコスト。
Designated Bridge	ルートポートに接続されているブリッジのブリッジ ID。
Designated Port	ルートポートのポート ID。

Refresh ボタンをクリックしてスイッチの最新情報を表示させます。

STP 統計(STP Statistics)

STP Statistics ページで各ポートが送受信したタイプ毎の BPDU の数を確認することができます。 Switching > STP > Advanced > STP Statistics を選択して STP statistics ページを表示します。

sic	STP Statis	tics					
Vanced STP Configuration	STP Stati	istics					
CST Configuration	PORTS	LAGS All					
CST Port Configuration	Interface	STP BPDUs Received	STP BPDUs Transmitted	RSTP BPDUs Received	RSTP BPDUs Transmitted	MSTP BPDUs Received	MSTP BPDUs Transmitted
CST Port Status	g1	0	0	0	0	0	0
IST Configuration	g2	0	0	0	0	0	0
ST Port	g3	0	0	0	0	0	0
onfiguration	g4	0	0	0	0	0	0
	g 5	0	0	0	0	0	0
	g6	0	0	0	0	0	0
	g7	0	0	0	0	0	0
	g8	0	0	0	0	0	0

以下に STP Statistics 欄に表示される情報の説明を示します。

Field	Description
Interface	インターフェース番号。
STP BPDUs Received	ポートで受信された STP BPDU 数。
STP BPDUs Transmitted	ポートで送信された STP BPDU 数。
RSTP BPDUs Received	ポートで受信された RSTP BPDU 数。
RSTP BPDUs Transmitted	ポートで送信された RSTP BPDU 数。
MSTP BPDUs Received	ポートで受信された MSTP BPDU 数。
MSTP BPDUs Transmitted	ポートで送信された MSTP BPDU 数。

Refresh ボタンをクリックしてスイッチの最新情報を表示させます。

マルチキャスト(Multicast)

マルチキャスト IP トラフィックはホストグループ向けのトラフィックです。ホストグループはクラス D の IP アドレス(224.0.0.0-239.255.255.255.255)を使います。

マルチキャストリンクから以下のページにアクセスできます。

- オートビデオ設定(Auto-Video Configuration)
- IGMP スヌーピング (IGMP Snooping)
- IGMP スヌーピングクエリア (IGMP Snooping Querier)

オートビデオ設定(Auto-Video Configuration)

オートビデオ機能はスイッチが監視ビデオカメラのようなデバイスやアプリケーションをサポートしているなら、IGMP スヌーピングクエリア設定を単純にします。

NETGEAR Connect with Innovation	r .				GS 110TP 8 Port Gigabit PoE Smart Switch with 2 Fiber SFP
System Swi	itching QoS	Security Monitoring	Maintenance	Help	LOGOUT
Ports LAG VLA	N Voice VLAN Auto-	VoIP STP Multicast Add	ress Table		
v Auto-Video	Auto-Video Config	uration			
IGMP Snooping IGMP Snooping	Auto-Video Configu	ration	(?)		
Querier	Auto-Video Status Auto-Video VLAN	 Disable Enable 			
					3
	γ.				∼
	•]				
					REFRESH

オートビデオ機能を設定する。

- 1. Switching > Multicast > Auto-Video を選択して Auto-Video Configuration ページを表示します。
- 2. オートビデオ機能を有効、無効にします。
 - Enable: IGMP スヌーピングクエリアは自動的にオートビデオ VLAN のデフォルト VLAN ID に設 定されます。
 - Disable: IGMP スヌーピング設定をする必要があります。
- 3. Apply ボタンをクリックして設定をスイッチに適用します。すぐに設定変更がされます。
- 4. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。

IGMP スヌーピング(IGMP Snooping)

IGMP(Internet Group Management Protocol)スヌーピングはスイッチがマルチキャストトラフィックを インテリジェントに転送します。マルチキャスト IPトラフィックはホストグループ向けのトラフィックで す。ホストグループはクラス D の IP アドレス(224.0.0.0-239.255.255.255.255)を使います。IGMP ク エリーとレポートメッセージに基づき、スイッチはマルチキャストを要求しているポートのみにトラフ ィックを転送します。これによってスイッチがトラフィックを全ポートにブロードキャストすることを防 止し、ネットワークパフォーマンスに影響を与えることを防ぎます。

伝統的なイーサネットは多くの機器を一つの共有ネットワークに接続することを避けるために異なるネットワークセグメントに分割していました。ブリッジやスイッチがそれらのセグメントをつなげています。ブロードキャストやマルチキャストの宛先アドレスを持ったパケットを受信すると、スイッチは IEEE MAC ブリッジ標準にもとづきパケットのコピーをそのポート以外のネットワークへ転送します。その結果、ネットワークに接続されているすべてのノードがパケットをアクセスする事ができます。

この手法はすべての接続されたノードに転送するブロードキャストパケットの場合はうまく機能します。マルチキャストパケットの場合は、特にパケットが少数のノードに送られる場合にネットワークの有効利用度は低くなります。パケットはパケットを必要とするノードが存在しないネットワークセ

グメントにもフラッドされます。マルチキャストパケットがシェアードメディアにフラッドされている間、 データを送信できなくなります。LAN セグメントが共有(シェア)されていない場合、例えば全二重 のリンクでは帯域の浪費問題はより悪くなります。

スイッチが IGMP パケットをスヌープ(のぞき見)することを許すのは、この問題を解決する良い方 法です。スイッチは IGMP パケットの情報を使って、どのセグメントがパケットを受信すべきかを判 断します。

IGMP スヌーピング設定(IGMP Snooping Configuration)

IGMP Snooping Configuration ページでマルチキャストを転送するリストを作成するために使われる IGMP スヌーピング設定をします。

NETGEA Connect with Innovation	R'							8 F	GS108T Port Gigabit Smart Switch
System Sw	vitching	QoS	Security	Monitoring	Maintenar	nce	Help		LOGOUT
Ports LAG VL	AN Voice	VLAN Au	to-VoIP STP	Multicast Addre	iss Table				
> Auto-Video	IGMP S	nooping	Configuratio	on					<u> </u>
» IGMP Snooping	IGMP	Snooping (Configuration					(?)	
Configuration	IGMP Sno	oping Status			Oisable	OEna	able		
Interface	Validate I	GMP IP head	der		O Disable	● Ena	able		
Configuration	Block Unk	nown Multica	ast Address		Oisable	O Ena	able		
 » IGMP Snooping Table » MFDB Table 	IGMP	Statistics						(?)	
» MFDB Statistics	Multicast (Control Fram	ne Count		o				=
» IGMP Snooping VLAN	Interface	s Enabled fo	r IGMP Snooping		None				
Configuration	Data Fran	nes Forward	ed by the CPU		0				
> IGMP Snooping									
Querier	: VLAN	Ids Enable	d for IGMP Sn	ooping				(?)	
	· VLAN	Ids Enable	d for IGMP Sn	ooping Querier				(?)	
1	<]				Ш				×
									CANCEL APPLY
Copyright © 1996-201	0 Netgear ®								

IGMP スヌーピングを設定する。

- 1. Switching > Multicast > IGMP Snooping > IGMP Snooping Configuration を選択して IGMP Snooping Configuration ページを表示します。
- 2. IGMP Snooping Status: スイッチで IGMP スヌーピングを有効にする。
 - Enable: IGMP スヌーピングを有効にし、スイッチはすべての IGMP パケットをスヌープしてパケットを送信するグループアドレスの存在するネットワークを決定します。
 - Disable: スイッチは IGMP パケットをスヌープしません。
- 3. Validate IGMP IP Header: IGMP IP ヘッダーの検査を設定します。
 - Enable: スイッチは IGMP IP ヘッダーの.Router Alert option, ToS, TTL 情報のチェックをします。
 - Disable:スイッチは IGMP IP ヘッダーの.Router Alert option, ToS, TTL 情報のチェックをしません。
- 4. Block Unknown Multicast Address:未知のマルチキャストアドレスをブロックします。

項目	設定
Multicast Control Frame Count	処理したマルチキャスト制御フレームの数。
Interfaces Enabled for IGMP Snooping	IGMP スヌーピングが有効なインターフェースのリ スト。
Data Frames Forwarded by the CPU	転送されたデータフレームの数。
VLAN Ids Enabled For IGMP Snooping	IGMP スヌーピングが有効にされた VLAN ID。
VLAN Ids Enabled For IGMP Snooping Querier	IGMP スヌーピングクエリアが有効にされた VLAN ID。

• Enable:未知のマルチキャストアドレスが宛先のパケットを廃棄します。

- Disable: 未知のマルチキャストアドレスが宛先のパケットを転送します。
- 5. Apply ボタンをクリックして設定をスイッチに適用します。すぐに設定変更がされます。
- 6. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。

以下に IGMP Statistics 欄そその下の欄に表示される情報の説明を示します。

IGMP スヌーピングインターフェース設定をする。

IGMP Snooping Interface Configuration ページでインターフェースの IGMP スヌーピング設定をします。

Sw	vitchi	ng Qo	S Secur	ity Ma	onitoring	Maintena	nce Help	[10]
orts LAG VL	AN	Voice VLAN	Auto-VolP	STP Mult	icast Addre	ss Table		
uto Vidoo	IG	AP Snoon	ng Interfa	ce Config	uration			
MP Snooping	101	in Shoop	ing interna	cc comig				
IGMP Snooping		GMP Snoop	ing Interface	e Configurat	ion		(3)	
GMP Snooping	POI	RTS LAG	S All		GO TO		GO	
Interface Configuration IGMP Snooping		Interface	Admin Mode	Host Timeout	Max Response Time	MRouter Timeout	Fast Leave Admin Mode	
MFDB Table			M					
MFDB Statistics		g1	Disable	260	10	0	Disable	
GMP Snooping		g2	Disable	260	10	0	Disable	
Configuration		g3	Disable	260	10	0	Disable	
MP Snooping		g4	Disable	260	10	0	Disable	
Jerier		g5	Disable	260	10	0	Disable	
		g6	Disable	260	10	0	Disable	
		g7	Disable	260	10	0	Disable	
		g8	Disable	260	10	0	Disable	
		g9	Disable	260	10	0	Disable	
		g10	Disable	260	10	0	Disable	
	POP	TS LAG	s All		GO TO	INTERFACE	GO	
r	•1							

IGMP スヌーピングインターフェース設定をする。

1. Switching > Multicast > IGMP Snooping > IGMP Snooping Interface Configuration を選択して

IGMP Snooping Interface Configuration ページを表示します。PORTS

- 2. PORTS をクリックして、物理ポートの IGMP スヌーピング設定をします。
- 3. LAGS をクリックして、Link Aggregation Group (LAG)の IGMP スヌーピング設定をします。
- **4.** ALL をクリックして、物理ポートと Link Aggregation Group (LAG)の両方の IGMP スヌーピング設定 をします。
- 5. 設定をしたいポートまたは LAG の横のチェックボックスをクリックして選択をします。複数の選択も 可能です。
- 6. 選択したポートまたは LAG の IGMP スヌーピング設定をします。
 - Admin Mode:インターフェースで IGMP スヌーピングを有効 (Enable) にします。デフォルトは無効 (Disable)です。
 - Host Timeout: IGMP スヌーピングのグループメンバーシップのインターバル。有効な値は 2-3600(秒)。デフォルトは 260(秒)。
 - Max Response Time:スイッチがクエリを送信することを待つ最大時間。1 以上 Host Timeout 値 未満。デフォルトは 10(秒)。
 - MRouter Timeout: ルーターのメッセージ受信の待ち時間。有効な値は 2-3600(秒)。デフォルトは 0(秒)。0 はタイムアウトしない設定です。
 - Fast Leave Admin Mode: Fast Leave モードを有効(Enable)にします。デフォルトは無効 (Disable)です。
- 7. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。
- 8. Apply ボタンをクリックして設定をスイッチに適用します。すぐに設定変更がされます。

IGMP スヌーピングテーブル (IGMP Snooping Table)

IGMP Snooping Table ページで IGMP スヌーピングのために作成されたマルチキャスト転送データ ベースのエントリーを見ることができます。

Switching > Multicast > IGMP Snooping > IGMP Snooping Table を選択して IGMP Snooping Table ペー ジを表示します。

NETGEA	R'							GS108T	1
Connect with Innovation"							8 Port Gigat	it Smart Switch	I
System S	witching	QoS S	ecurity	Monitoring	Maintenan	e He	lp	LOGOUT	
Ports LAG V	LAN Voice V	'LAN Auto-Vo	IP STP	Multicost Addr	ess Table				
> Auto-Video	IGMP Sn	ooping Tal	ole					F	^
* IGMP Snooping * IGMP	IGMP S	nooping Tabl	e		()				
Snooping Configuration	Search by M	AC Address			60				
» IGMP	MAC Address	VLAN ID	Туре	Description	Interface				
Interface									
Configuration * TGMP									
Snooping									111
Table * MEDB Table									
» MFDB									
Statistics									
» IGMP									
VLAN									
Configuration									
IGMP Snooping								L	
Querier									~
	<			Ш)	
							CLEAR REFR	CANCEL	
Copyright @ 1000.0	009 Notoone	2							

以下に IGMP Snooping Table 欄に表示される情報の説明を示します。

項目	説明
MAC Address	スイッチが転送あるいはフィルタしたマルチキャスト MAC アドレス。コロン(:)で 2 桁ごとに区切られた 12 桁の 16 進数で表されます。(例: 01:00:5e:45:67:89)
VLAN ID	スイッチが転送あるいはフィルタした情報を持つ VLAN ID。
Туре	タイプ。スタティック(Static)あるいはダイナミック(Dynamic)。
Description	マルチキャストテーブル入力の説明。以下のどれか。 Management Configured, Network Configured, Network Assisted。
Interface	転送(Fwd)されるインターフェースあるいはフィルタ(Flt)されるインターフェー ス。

画面下部のボタンを使って以下の動作をすることができます。

- Clear ボタンをクリックして IGMP 設定をクリアします。
- Refresh ボタンをクリックしてスイッチの最新情報を表示させます。

マルチキャストフォワーディングデータベーステーブル(Multicast Forwarding Database Table)

レイヤー2 マルチキャストフォワーディングデータベース(MFDB)はマルチキャスト MAC アドレスが 宛先のパケットの転送先を判断するために使われます。マルチキャストの転送先を制限すること により、トラフィックが不要なネットワークに転送されることを防ぎます。

パケットがスイッチに到着すると、MAC アドレスと VLAN ID が組み合わされてレイヤー2 マルチキ ャストフォワーディングデータベースで検索がされます。一致がない場合は、パケットはスイッチの 設定によって VLAN 中のすべてのポートにフラッドされるか廃棄されます。一致した場合はそのマ ルチキャストグループメンバーポートのみに転送されます。

MFDB Table ページですべての有効なマルチキャストアドレスのポートを確認することができます。 MAC アドレス単位に表示されます。一つまたは複数のプロトコルがデータに含まれます。

Switching > Multicast > IGMP Snooping > MFDB Table を選択して MFDB Table ページを表示します。

NETGEA	R'						8 Port Gigat	GS110T bit PoE Smart Swit with 2 Fiber S
System S	witching	QoS	Security	Monitoring	Maintenance	Help		LOGOUT
Ports LAG VI	AN Voice	VLAN Auto	-VoIP STP	Multicast Ad	dress Table			
Auto-Video	MFDB	Table						
» IGMP Snooping » IGMP Snooping	MFDE	3 Table					(2)	
Configuration	Search by	MAC Address				GO		
 IGMP Snooping Interface Configuration 	MAC Address	VLAN 5 ID	Component	Type Desc	cription Interface	Forwarding Interfaces		
» IGMP Snooping								
* MEDB Table								
» MFDB Statistics								
» IGMP Snooping								
VLAN								
IGMP Snooping								
Querier								
	<				100			>
								DEEDESH
								REFRESH

Field	Description
MAC Address	マルチキャスト MAC アドレス。MAC アドレスで検索する場合は、コロン(:) で 2 桁ごとに区切られた 12 桁の 16 進数(例: 01:00:5e:45:67:89)を入力 し Go ボタンをクリックします。完全に一致する必要があります。
VLAN ID	MAC アドレスに関連する VLAN ID。
Component	このフォワーディングデータベースに入力された方法。IGMP Snooping または Static Filtering。
Туре	タイプ。スタティック(Static)あるいはダイナミック(Dynamic)。
Description	マルチキャストテーブル入力の説明。以下のどれか。Management Configured, Network Configured, Network Assisted。
Interface	転送(Fwd)されるインターフェースあるいはフィルタ(Flt)されるインターフ ェース。
Forwarding Interfaces	転送先インターフェース。

以下に MFDB Table 欄に表示される情報の説明を示します。

Refresh ボタンをクリックしてスイッチの最新情報を表示させます。

MFDB 統計(MFDB Statistics)

MFDB Statistics ページで MFDB テーブルの統計情報を確認できます。

Switching > Multicast > IGMP Snooping > MFDB Statistics を選択して FDB Statistics ページを表示し



ます。

以下に MFDB Statistics 欄に表示される情報の説明を示します。

GS108T/GS110TP スマートスイッチソフトウェア管理マニュアル

Field	Description
Max MFDB Table Entries	テーブルの最大容量。
Most MFDB Entries Since Last Reset	スイッチのリセット後のテーブルの最大値。
Current Entries	現在のテーブル使用量。

Refresh ボタンをクリックしてスイッチの最新情報を表示させます。

IGMP スヌーピング VLAN 設定(IGMP Snooping VLAN Configuration)

IGMP Snooping VLAN Configuration ページで IGMP スヌーピング VLAN 設定をします。

NETGEAR Connect with Innovation	s .					8	GS110 Port Gigabit PoE Smart S with 2 Fiber)TP witch r SFP
System Swi Ports LAG VLA	itching Q	oS Secu	rity Monitor STP Multicast	ing Maintena Address Table	nce Help		[1060	τυα
> Auto-Video > IGMP Snooping > IGMP Snooping	IGMP Sno	oping VLAN	Configuration				0	^
Configuration » IGMP Snooping Interface Configuration	Vlan ID	Fast Leave Admin Mode	Host Timeout	Maximum Response Time	MRouter Timeout	Query Mode	Query Interval	
 » IGMP Snooping Table » MFDB Table » MFDB Statistics 		Disable 💌				Disable 💌		Ш
* IGMP Snooping VLAN Configuration								
• IGMP Snooping Querier	<]]	>
Copyright © 1996-2010	D Netgear ®					ADD DELET	TE CANCEL APPLY	

IGMP スヌーピング VLAN 設定をする。

- 1. Switching > Multicast > IGMP Snooping > IGMP Snooping VLAN Configuration を選択して IGMP Snooping VLAN Configuration ページを表示します。
- 2. IGMP を設定する VLAN ID を Vlan ID 欄に記入し、以下の設定をし Add ボタンをクリックします。
 - Fast Leave Admin Mode: VLAN で Fast Leave モードを有効(Enable)にします。デフォルトは無効(Disable)です。Fast Leave モードを有効にすると、スイッチは IGMP Leave メッセージを受信すると、すぐにポートをマルチキャストグループのフォワーディングテーブルから削除します。ポートに端末が1台だけ接続されている場合に Fast Leave モードを有効にすべきです。Fast Leave モードは IGMP バージョン2のみがサポートします。
 - Host Timeout:IGMP スヌーピングのグループメンバーシップのインターバル。有効な値は (Maximum Response Time + 1)から 3600(秒)。デフォルトは 260(秒)。
 - Maximum Response Time: スイッチがクエリを送信することを待つ最大時間。1-25(秒)、Host Timeout 値未満。デフォルトは 10(秒)。
 - MRouter Timeout: ルーターのメッセージ受信の待ち時間。有効な値は 2-3600(秒)。デフォルトは 0(秒)。0 はタイムアウトしない設定です。

- Query Mode: IGMP クエリモードの有効・無効。
- Query Interval: クエリのインターバル。有効な値は 1-1800(秒)。 デフォルトは 60(秒)。
- 3. VLAN の IGMP を削除するには、削除する IGMP のチェックボックスを選択し、Delete ボタンをクリックします。
- 4. VLAN の IGMP を変更するには、変更する IGMP のチェックボックスを選択し、変更をします。 変更 後、 Apply ボタンをクリックします。
- 5. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。

IGMP スヌーピングクエリア(IGMP Snooping Querier)

IGMP スヌーピングでは中心のスイッチまたはルーターは定期的に全てのエンド端末にクエリ(問い合わせ)を行い、マルチキャストのメンバーシップを伝えます。この中心が IGMP クエリアです。 IGMP レポートとして知られる IGMP クエリの応答によって、スイッチはマルチキャストグループメン バーシップをポート単位で最新に保つことができます。スイッチが最新の情報を得られない場合 は、スイッチはその端末が存在する場所へのマルチキャストの送信を停止します。

IGMP Snooping Querier リンクから以下のページにアクセスできます。

- IGMP Snooping Querier Configuration on page 51
- IGMP Snooping Querier VLAN Configuration on page 52
- IGMP Snooping Querier VLAN Status on page 53

IGMP スヌーピングクエリア設定(IGMP Snooping Querier Configuration)

このページで IGMP クエリア設定をします。

NETGEA	R'		GS108T
Connect with Innovation			8 Port Gigabit Smart Switch
System Sv	vitching QoS Security	Monitoring Maintenance Help	LOGOUT
Ports LAG VI	AN Voice VLAN Auto-VoIP STP	Multicast Address Table	
 Auto-Video IGMP Snooping IGMP Snooping 	Querier Configuration	۲	<u>^</u>
Querier > Querier Configuration > Querier VLAN Configuration > Querier VLAN	Querier Admin Mode Snooping Querier Address IGMP Version Query Interval(secs) Querier Expiry Interval(secs)	Disable Enable 0.0.0.0 2 (1 to 2) 60 (1 to 1800) 60 (60 to 300)	
Status	[4]	- 101	
			REFRESH CANCEL APPLY
Copyright © 1996-2	009 Netgear ®		

IGMP スヌーピングクエリア設定をする。

- 1. Switching > Multicast > IGMP Snooping Querier > IGMP Snooping > Querier Configuration を選択 して Querier Configuration ページを表示し、以下の項目を設定します
 - Querier Admin Mode: IGMP スヌーピングクエリアを有効(Enable),無効(Disable)にします。
 - Snooping Querier Address: IGMP クエリを送信する IP アドレスを設定します。
 - IGMP Version: IGMP クエリを送信する時に使う IGMP のバージョン。1 または 2。

- Query Interval: IGMP クエリを送信する周期(秒)。範囲は 1-1800(秒)。 デフォルトは 60(秒)。
- Querier Expiry Interval: IGMP クエリの結果情報の有効時間(秒)。範囲は 60-300(秒)。デフォ ルトは 60(秒)。
- 7. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。
- 8. Apply ボタンをクリックして設定をスイッチに適用します。すぐに設定変更がされます。
- 9. Refresh ボタンをクリックしてスイッチの最新情報を表示させます。

IGMP スヌーピングクエリア VLAN 設定(IGMP Snooping Querier VLAN Configuration)

VLAN で IGMP スヌーピングクリエアを使う設定をします。

NETGEA Connect with Innovation [®]	R.		GS110TP 8 Port Gigabit POE Smart Switch with 2 Fiber SFP
System Sw	itching QoS Security	Monitoring Maintenance Help	LOGOUT
Ports LAG VL	AN Voice VLAN Auto-VolP STP	Multicast Address Table	
 Auto-Video IGMP Snooping IGMP Snooping Querier Querier Configuration Querier VLAN Configuration Querier VLAN Status 	Querier VLAN Configuration Querier VLAN Configuration VLAN ID VLAN ID Querier Election Participate Mode Snooping Querier VLAN Address	n New Entry ♥ (1 to 4093) Disable ♥ 0.0.00	
	<]		×
Copyright © 1996-201	0 Netgear ®	R	EFRESH DELETE CANCEL APPLY

VLAN で IGMP スヌーピングクエリア設定をする。

- 1. Switching > Multicast > IGMP Snooping Querier > Querier VLAN Configuration を選択して Querier VLAN Configuration ページを表示します。
- **2.** IGMP スヌーピング用の新しい VLAN ID を作成するには VLAN ID 欄で New Entry を選択し、以下 の情報を設定します。
 - VLAN ID: IGMP スヌーピングを有効にする VLAN ID を入力します。(1-4093)
 - Querier Election Participate Mode :
 - Disabled: VLAN 中でバージョンが同じクエリを発見すると、クエリを停止します。
 - Enabled: クエリアの選抜に参加します。 VLAN 中で IP アドレスが一番小さなものがクエリア になります。
 - Snooping Querier VLAN Address: VLAN 中で使う IGMP スヌーピングクエリアの IP アドレスを指定します。
- 3. Apply ボタンをクリックして設定をスイッチに適用します。すぐに設定変更がされます。
- 4. VLAN の IGMP スヌーピングクエリアを削除するには、削除するクエリア VLAN ID を選択し、Delete

Field	Description
VLAN ID	IGMP スヌーピングクエリアが有効になっている VLAN の VLAN ID。
Operational State	VLAN 中の IGMP スヌーピングクエリアの状態。 • Querier:IGNP スヌーピングクエリアとして動作している。 • Non-Querier:IGNP スヌーピングクエリアとして動作していない。 • Disabled: IGNP スヌーピングクエリアは無効である。
Operational Version	動作中の IGMP スヌーピングクエリアのバージョン。
Last Querier Address	VLAN 中の IGMP スヌーピングクエリアの IP アドレス。
Last Querier Version	スヌープ(のぞき見)したクエリのバージョン。
Operational Max Response Time	クエリの最大の応答時間(秒)

ボタンをクリックします。

- 5. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。
- 6. Refresh ボタンをクリックしてスイッチの最新情報を表示させます。

IGMP スヌーピングクエリア VLAN 状態(IGMP Snooping Querier VLAN Status)

VLAN の IGMP スヌーピングクエリの運用状態とその他の情報を確認することができます。

Switching > Multicast > IGMP Snooping Querier > Querier VLAN Status を選択して Querier VLAN Status ページを表示します。

以下に Querier VLAN Status 欄に表示される情報の説明を示します。

NETGEA	R'					8 Port	Gigabit Smart Swite
System Sv	vitching Q	oS Security	Monitoring	Maintenance	He	alp	LOGOU
Ports LAG VL	AN Voice VLAN	Auto-VolP STP /	Aulticast Address	Toble			
Auto-Video IGMP Snooping IGMP Snooping	Querier VL	AN Status LAN Status				۲	
Querier » Querier Configuration » Querier VLAN	VLAN ID	Operational State	Operational Version	Last Querier Address	Last Querier Version	Operational Max Response Time (secs)	
Configuration » Querier VLAN Status							
	<			IIII			
							REFRESH

Refresh ボタンをクリックしてスイッチの最新情報を表示させます。

フォワーディングデータベース(Forwarding Database)

フォワーディングデータベースは受信したパケットの MAC アドレスのリストを維持します。トランス ペアレントブリッジ機能はフォワーディングデータベースを使って受信したフレームの転送先を決定 します。 Address Table フォルダは以下の機能へのリンクを含んでいます。

- MAC アドレステーブル (MAC Address Table)
- ダイナミックアドレス設定(Dynamic Address Configuration)
- スタティック MAC アドレス (Static MAC Address)

MAC アドレステーブル (MAC Address Table)

MAC アドレステーブルはスイッチが転送およびフィルタするユニキャストアドレス情報を持っていま す。トランスペアレントブリッジ機能はこの情報を使って受信したフレームをどのように伝達するか を決定します。MAC アドレステーブルページの検索(Search)機能を使ってテーブル情報を表示で

System	Switching	QoS Security	Monitoring	Maintenance	Help	LOGO
Ports LAG	VLAN Voice V	LAN Auto-VolP STP	Multicast A	ddress Table		
asic	Address	Table				lo facilita da Electra de Carleiro da Ele
Table	MAC A	ddress Table		0		
dvanced	Search By	VLAN ID		GO		
	Total MAC	Addresses 83				
	VLAN ID	MAC Address	Interface	Status		
	1	00:00:E2:6D:2C:2A	g1	Learned		
	1	00:02:66:88:88:88	g1	Learned		
	1	00:02:BC:00:17:D0	g1	Learned		
	1	00:02:BC:00:70:41	g1	Learned		
	1	00:03:05:01:29:20	g1	Learned		
	1	00:0B:78:66:06:F4	g1	Learned		
	1	00:0C:29:86:B6:CB	g1	Learned		
	1	00:0C:76:05:A1:FB	g1	Learned		
	1	00:0E:7F:60:49:BD	g1	Learned		
	1	00:0F:FE:00:2B:47	g1	Learned		
	1	00:0F:FE:17:82:67	g1	Learned		
	1	00:0F:FE:19:E3:F8	g1	Learned		
	1	00:0F:FE:A4:8A:C5	g1	Learned		
	<					

MAC アドレステーブルを検索する。

- Switching > Address Table > Basic > Address Table を選択して Address Table ページを表示します。
- 2. Search By 欄で MAC Address, VLAN ID, Interface のいずれかを選択します。
 - MAC Address:コロン(:)で2桁ごとに区切られた12桁の16進数を入力し、Goボタンをクリックします。完全に一致する必要があります。
 - VLAN ID:完全に一致する必要があります。VLAN ID を入力して Go ボタンをクリックします。
 - Interface: インターフェース番号(g1,g2,…)を入力し、Goボタンをクリックします。
- 3. Clear ボタンをクリックしてダイナミック MAC アドレスをテーブルからクリアします。
- 4. Refresh ボタンをクリックして MAC アドレスの最新情報を表示させます。
- 5. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。

以下に MAC Address Table 欄に表示される情報の説明を示します。

Field	Description
VLAN ID	MAC アドレスが存在する VLAN の VLAN ID。
MAC Address	スイッチが転送あるいはフィルタしたユニキャスト MAC アドレス。コ ロン(:)で 2 桁ごとに区切られた 12 桁の 16 進数で表されます。(例: 00:0F:89:AB:CD:EF)
Interface	この MAC アドレスが学習されたポート。このポートからこの MAC ア ドレスに到達することができます。
Status	テーブルエントリーの状態。 • Static:スタティック設定。 • Learned:学習したアドレス。 • Management:システム MAC アドレス。c1インターフェースに 存在します。

ダイナミックアドレス設定(Dynamic Address Configuration)

Dynamic Addresses ページで学習した MAC アドレスをフォワーディングデータベースにどのくらい 保持するかを設定できます。スタティック情報は消去されません。



ダイナミックアドレス設定をする。

- 1. Switching > Address Table > Advanced > Dynamic Addresses を選択して Dynamic Addresses ペー ジを表示します。
- 2. Address Aging: IEEE 802.1D-1990 は 300 秒を推奨しています。設定範囲は 10-1000000(秒)です。 デフォルトは 300(秒)です。
- 3. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。
- 4. Apply ボタンをクリックして設定をスイッチに適用します。すぐに設定変更がされます。

スタティック MAC アドレス (Static MAC Address)

Static MAC Address ページでインターフェースのスタティック MAC アドレスを設定、確認できます。

NETGE Connect with Innovation	AR'						GS 110TP 8 Port Gigabit POE Smart Switch with 2 Fiber SFP
System	Switching	QoS	Security	Monitoring	Maintenance	Help	LOGOUT
Ports LAG	VLAN Voice		uto-VolP STP	Multicast Add	ress Table		
 Basic Advanced Dynamic 	Static Stati	MAC Ad	dress dress		0		
Addresses > Address Table > Static MAC Address		an ID	MAC Address		Interface g1		Ħ
	٢						
Copyright © 1996	-2010 Netgear @	B				REFRESH ADD	DELETE CANCEL APPLY

スタティック MAC アドレスを設定する。

- 1. Switching > Address Table Advanced > Static MAC Address を選択して Static MAC Address ページを表示します。
- 2. スタティック MAC アドレスを入力するには、
 - a. Vlan ID:MAC アドレスを設定したい VLAN ID を選択します。
 - **b.** Static MAC Address:MAC アドレスを入力します。
 - c. Interface:インターフェースを選択します。
 - d. Add ボタンをクリックします。
- 3. スタティック MAC アドレスを削除するには、削除するスタティック MAC アドレスを選択し、Delete ボ タンをクリックします。
- 4. スタティック MAC アドレスを変更するには、変更する MAC アドレスのチェックボックスを選択し、変更が終わったら Apply ボタンをクリックして設定をスイッチに適用します。
- 5. Refresh ボタンをクリックして最新情報を表示させます。

6. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。

4.QoS 設定

QoS タブの機能を使ってスイッチの QoS(Quality of Service)設定をします。 QoS タブは以下の機能へのリンクを含んでいます。

- CoS(Class of Service)
- DiffServ(ディフサーブ、Differentiated Services)

典型的なスイッチでは各物理ポートは一つまたは複数のキューを使ってパケットを転送していま す。ポートに複数のキューがある場合は、ユーザーの設定に応じてあるパケットは他のパケットに 比べて優先度を与えられることがあります。パケットがポートから送信されるためにキューされた 時、送信される速度はキューがどのように設定され、ポートの他のキューにどのくらいのトラフィッ クが存在するかに依存します。遅延が必要ならば、スケジューラーがキューに送信許可を与える までパケットはキューに留まります。キューがいっぱいになると、パケットを保存する余地がなくな るので、スイッチはパケットを廃棄します。

QoS は厳密なタイミング条件のあるパケットを、より遅延に寛容なパケットに対して区別することに よって一貫性のある、予測可能なデータ伝達をする手段の一つです。

QoS が可能なネットワークでは、厳密なタイミング条件のあるパケットは特別の扱い(special treatment)を受けます。これを念頭に、ネットワークのすべての要素は QoS 実行可能である必要 があります。一つのノードが QoS 非対応であると、ネットワークの欠陥となり、全体のパケットフロ ーは妥協したものとなります。

CoS(Class of Service)

CoS(Class of Service)キューイング機能はある面においてスイッチのキューイングを直接設定で きることになります。これによって DiffServ のような複雑なものが必要とされていない場合は、ネッ トワークトラフィックの異なるタイプに対する期待される QoS 動作を提供することができます。イン ターフェースに到着するパケットのプライオリティがマッピングテーブルを使ってパケットを適切な送 信 CoS キューに送ることができます。最低帯域保証や送信速度シェーピングのようなキューマッピ ングに影響する CoS キュー特性はキューあるいはポート単位で設定可能です。

ポートで4つのキューがサポートされています。

QoS タブの下の Class of Service リンクから以下のページにアクセスできます。

- 基本 CoS 設定(Basic CoS Configuration)
- CoS インターフェース設定(CoS Interface Configuration)
- インターフェースキュー設定(Interface Queue Configuration)
- 802.1p からキューへのマッピング(802.1p to Queue Mapping)
- DSCP からキューへのマッピング (DSCP to Queue Mapping)

基本 CoS 設定(Basic CoS Configuration)

Trust Mode Configuration ページで、インターフェースで CoSトラストモードを設定します。スイッ チの各ポートはパケットの 802.1p または IP DSCP を信頼するか、パケットのプライオリティ設定を 信頼しない(untrust mode)かを設定することができます。ポートがトラストモードに設定されると、信 頼できる情報に基づきマッピングテーブルを使います。このマッピングテーブルで、パケットの出力 ポートの CoS キューを決定します。もちろん、マッピングテーブルを役立てるためには信頼できる 情報がパケットに存在する必要があり、情報がない場合のデフォルト動作もあります。これらの動 作は、パケットを入力ポートに設定されたデフォルトプライオリティの CoS に向けることを含みま す。

あるいは、ポートがアントラスト(untrusted)に設定されていると、受信したパケットのプライオリティ を信頼せず、代わりにポートデフォルトプライオリティを使います。Untrusted ポートで受信されたす べてのパケットは、入力ポートで設定されたデフォルトプライオリティに従って送信ポートの特定の CoS キューに渡されます。この処理は、IP DSCP 値を信頼する設定のポートに IP ではないパケッ トが受信された時のように、トラステッドマッピングが使えない場合にも使われます。

DETGEA	R'					GS108 8 Port Gigabit Smart Swit
System Sv	witching Qo	S Security	Monitoring	Maintenance	Help	LOGOL
Basic Advanced * CoS	CoS Configur	ation		0		
Configuration » CoS Interface Configuartion » Interface Oueue	 Global Interface 	g1 💙	Global Trust Mode Interface Irust Mode	ed 💌		
Configuration > 802.1p to Queue Mapping > DSCP to Queue Mapping						
Mapping	<]][

グローバル CoS 設定をする。

- 1. QoS > Basic > CoS Configuration を選択して CoS Configuration ページを表示します。
- 2. Global ラジオボタンを選択してすべてのインターフェースに適用するトラストモードを設定します。

あるいは、Interface ラジオボタンを選択してトラストモード設定を個々のインターフェースに設定します。インターフェース設定はグローバル設定よりも優先されます。

- 3. すべてのインターフェース (Global Trust Mode)またはインターフェース(Interface Trust Mode)の どちらかのトラストモードを選択します。この設定でフレームがポートに入力した時の CoS マーキ ングのタイプを決定します。
- 4. Untrusted:受信パケットの CoS 設定を信用しません。
- 5. 802.1p:IEE802.1p で規定されている 8 段階のプライオリティタグは p0-p7 です。QoS 設定は 8 段階のプライオリティをスイッチ内部の1から4の4段階のハードウェアプライオリティキュー(High, Normal, Low, and Lowest)にマッピングします。
- 6. DSCP: DiffServ フィールドの上位6ビットは DSCP(Differentiated Services Code Point)ビットと 呼ばれています。
- 7. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。
- 8. Apply ボタンをクリックして設定をスイッチに適用します。

CoS インターフェース設定(CoS Interface Configuration)

CoS Interface Configuration ページでインターフェースシェーピング速度をすべてのインターフェースまたは個々のインターフェースに設定します。

							with 2 Fiber S
System Swite	hing	QoS	Security	Monitoring	Maintenance	Help	LOGOU
CoS DiffServ							
Basic	Cos	5 Interfac	e Configurat	ion			
Advanced » CoS Configuration		CoS Interfa	ce Configuration	n	(?)		
» CoS Interface	POF	ITS LAGS	All	GO TO INTERFA	CE GO		
Configuration > Interface Queue Configuration > 802.1p to Queue		Interface	Interface Trust Mode	Interface Egress Shaping Rate (16 to 16384)	Interface Ingress Rate Limit (16 to 16384)		
Mapping » DSCP to Queue			Untrusted 💌				
Mapping		g1	802.1p	0	0		
		g2	802.1p	0	0		
		g3	802.1p	0	0		
		g4	802.1p	0	0		
		g 5	802.1p	0	0		
		g6	802.1p	0	0		
		g7	802.1p	0	0		
		g8	802.1p	0	0		
		g 9	802.1p	0	0		
		g10	802.1p	0	0		
	POF	LAGS	All	GO TO INTERFA			

インターフェースに CoS 設定をする。

- 1. QoS > CoS > Advanced > CoS Interface Configuration を選択して CoS Interface Configuration ページを表示します。
- 2. PORTS をクリックして、物理ポートの CoS 設定をします。
- 3. LAGS をクリックして、LAG (Link Aggregation Group)の CoS 設定をします。
- 4. ALL をクリックして、物理ポートとLAG (Link Aggregation Group)の両方の CoS 設定をします。
- 5. 設定をしたいポートまたは LAG の横のチェックボックスをクリックして選択をします。複数の選択 をして共通の設定をすることも可能です。
- 6. Interface Trust Mode: 選択したポートが受信したパケットを信頼するかどうかを指定します。
 - Untrusted: 受信したパケットの CoS 情報を信頼しない。
 - 802.1p:受信したパケットの IEEE802.1p CoS 情報を信頼します。IEE802.1p で規定されている 8 段階のプライオリティ(p0-p7)をスイッチ内部の1から4の4段階のハードウェアプライオリティキュー(High, Normal, Low, and Lowest)にマッピングします。
 - Interface Egress Shaping Rate(16 to 16384):インターフェースに許可された出力方向の最大 帯域を設定します。この設定は送信速度をシェーピングするのに使われます。この値はキュ ー単位の最大帯域設定とは独立です。単位は kbps です。デフォルト値は 0 で無制限を意味 します。
 - Interface Ingress Shaping Rate(16 to 16384): ンターフェースに許可された入力方向の最大 帯域を設定します。単位は kbps です。デフォルト値は 0 で無制限を意味します。
- 7. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。
- 8. Apply ボタンをクリックして設定をスイッチに適用します。

インターフェースキュー設定(Interface Queue Configuration)

Interface Queue Configuration ページでスイッチ出力(Egress)キューを設定することによって特定
のキュー動作を定義することができます。設定可能なパラメータは、キューが利用可能な帯域、輻 輳発生時のキューの深さ、ポートに設定されているすべてのキューのセットでのパケット送信の順 序です。各ポートは CoS キュー関連の設定ができます。

設定方法を簡単にするために、CoSキューパラメータをグローバルおよびポート単位で設定できるようになっています。グローバル設定の変更はすべてのポートに自動的に適用されます。

nect with innovation							8 Port Gig	abit Smart Sw
System S	witch	ing G	οS	Security	Monitoring	Maintenance	Help	LOGO
Basic	Int	erface Qu	ieue Co	onfiguration				
dvanced CoS		Interface Q	ueue Co	nfiguration		1		
Configuration	PO	RTS LAG	s All	G	O TO INTERFACE	GO		
CoS Interface Configuartion		Interface	Queue ID	Minimum Bandwidth (0 to 100)	Scheduler Type	Queue Management Type		
			0 🕶	0	×			
802.1p to		g1	0	0	weighted	taildrop		
Queue		g2	0	0	weighted	taildrop		
DSCP to		g3	0	0	weighted	taildrop		
Queue		g4	0	0	weighted	taildrop		
Mapping		g5	0	0	weighted	taildrop		
		g6	0	0	weighted	taildrop		
		g7	0	0	weighted	taildrop		
		g8	0	0	weighted	taildrop		
	POI	RTS LAG	s All	G	D TO INTERFACE	GO		
	<							

インターフェースに CoS キュー設定をする。

- 1. QoS > CoS > Advanced > Interface Queue Configuration を選択して Interface Queue Configuration ページを表示します。
- 2. PORTS をクリックして、物理ポートの CoS キュー設定をします。
- 3. LAGS をクリックして、LAG (Link Aggregation Group)の CoS キュー設定をします。
- 4. ALL をクリックして、物理ポートとLAG (Link Aggregation Group)の両方の CoS キュー設定をします。
- 設定をしたいポートまたはLAGの横のチェックボックスをクリックして選択をします。複数の選択をして共通の設定をすることも可能です。先頭のチェックボックスをクリックするとすべてのインターフェースを選択できます。
- 6. 以下の項目の設定をします。
 - Queue ID:0-3 のキューを選択します。
 - Minimum Bandwidth:選択したキューの帯域(%)を指定します。範囲は 0-100(%)で 1(%)単位で 指定します。
 - Scheduler Type:キューの処理方法をメニューから選択します。トラフィックタイプに応じて選択します。デフォルトは Weighted です。
 - Weighted: Weighted round robin 方式で処理します。
 - Strict: プライオリティの高いトラフィックが優先的に送信されます。
 - Queue Management Type:キューがいっぱいになった時の処理を示します。キューがいっぱいになった状態で到着したパケットは廃棄されます。
- 7. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させま

す。

8. Apply ボタンをクリックして設定をスイッチに適用します。

802.1p からキューへのマッピング(802.1p to Queue Mapping)

802.1p to Queue Mapping ページで 802.1p プライオリティとキューのマッピングを確認・設定します。

System Sv	vitching	QoS		Security	Moi	nitoring	Mai	ntenance	Help	1000
CoS DiffServ										
Basic	802.1p	to Ou	eue Ma	apping						
Advanced									-	
» CoS	802.1	p Queu	e Config	uration					0	
Configuration	💿 Globa	d .				🔵 In	terface	g1 😽		
» CoS Interrace Configuration										
» Interface	802.1	p to Qu	eue Map	ping					(?)	
Queue	802.1p			-					-	
Configuration	Priority	U	1	2	3	4	2	0	1	
Oueue Manning	Queue	1 💌	0 🕶	0 💌	1 🚩	2 🕶	2 🕶	3 🚩	3 💌	
» DSCP to Queue										
Mapping										
1	<									

802.1p プライオリティをキューにマッピングする

- 1. QoS > CoS > Advanced > 802.1p to Queue Mapping を選択して 802.1p to Queue Mapping ページを表示します。
- 2. Global ラジオボタンを選択してすべてのインターフェースに同じ 802.1p プライオリティから CoS へのマッピングをするか、インターフェース単位にマッピングするかを選択します。

あるいは、Interface ラジオボタンを選択してインターフェース単位に 802.1p プライオリティから CoS へのマッピングを設定します。インターフェース設定はグローバル設定よりも優先されます。

3. 802.1p プライオリティに対して、対応するキューを選択します。

802.1p Priority 行は 8 つの 802.1p プライオリティそれぞれに対してトラフィッククラスが選択でき るようになっています。Queue のプライオリティは 0 が一番低く、3 が最高となります。

トラフィッククラス 0-3 はポートでのハードウェアキューをあらわします。

- 4. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。
- 5. Apply ボタンをクリックして設定をスイッチに適用します。

DSCP からキューへのマッピング(DSCP to Queue Mapping)

DSCP to Queue Mapping ページで DSCP 値に従ってキューへのマッピングを設定します。

		0.0	C							
System 3	owitching	QoS	Security	Moni	toring N	laintenan	ice Help			
Cos Dinserv										
Basic	DSCP to Queue Mapping									
Advanced » CoS	DSCP to Q	ueue Ma	pping					(?)		
Configuration	Class Selector	(CS) PHB		- 10 P						
» CoS Interface	DSCP	Queue	DSCP	Queue	DSCP	Queue	DSCP	Queue		
» Interface	CS 0	1 💙	CS 1	0 🗸	CS 2	0 🗸	CS 3	1 💌		
Queue Configuration	CS 4	2.84	CS 5		CS 6	2 44	CS 7	2.4		
Configuration » 802.1p to	(100000)	2 *	(101000)	2 *	(110000)	3.	(111000)			
Queue	Assured Forw	arding (AF) PHB		Sec. all the second					
» DSCP to	DSCP	Queue	DSCP	Queue	DSCP	Queue	DSCP	Queue		
	(001010)	0	(010010)	0 🛩	(011010)	1 🛩	(100010)	2 💌		
Mapping	AF 12 (001100)	0 🕶	AF 22 (010100)	0~	AF 32 (011100)	1~	AF 42 (100100)	2 🕶		
	AF 13 (001110)	0 💌	AF 23 (010110)	0~	AF 33 (011110)	1	AF 43 (100110)	2 🛩		
	Expedited For	warding (E	F) PHB							
	DSCP				Queue					
	EF (101110)				2 🗙					
	Other DSCP V	alues (Loc	al/Experimenta	l Use)	0.000		0.000			
	1 (000001)	Queue	2 (000010)	Queue	3 (000011)	Queue	4 (000100)	Queue		
	5 (000101)	1 ¥	6 (000110)	1 🗸	7 (000111)	1 🗸	9 (001001)	0~		
	11 (001011)	0 🗸	13 (001101)	0 🗸	15 (001111)	0 🗸	17 (010001)	0 ~		
	19 (010011)	0 🗸	21 (010101)	0 🗸	23 (010111)	0 🗸	25 (011001)	1 🗸		
	27 (011011)	1 🗸	29 (011101)	1 🗸	31 (011111)	1 🗸	33 (100001)	2 🕶		
	35 (100011)	2 🗸	37 (100101)	2 🛩	39 (100111)	2 🕶	41 (101001)	2 🕶		
	42 (101010)	2 🗸	43 (101011)	2 🛩	44 (101100)	2 🛩	45 (101101)	2 💌		
	47 (101111)	2 🗸	49 (110001)	3 🗸	50 (110010)	3 🗸	51 (110011)	3 🕶		
	52 (110100)	3 🗸	53 (110101)	3 🛩	54 (110110)	3 🛩	55 (110111)	3 🛩		
	57 (111001)	3 🗸	58 (111010)	3 🗸	59 (111011)	3 🕶	60 (111100)	3 🕶		
	61 (111101)	3 🕶	62 (111110)	3 🛩	63 (111111)	3 🛩				

DSCP からキューへのマッピング

- 1. QoS > CoS > Advanced > DSCP to Queue Mapping を選択して DSCP to Queue Mapping ページを表示します。
- それぞれの DSCP 値に対してハードウェアキューを設定し関連付けます。トラフィッククラス 0-3 はポートでのハードウェアキューをあらわします。キューのプライオリティは 0 が一番低く、3 が最 高となります。
- 3. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。
- 4. Apply ボタンをクリックして設定をスイッチに適用します。

DiffServ(ディフサーブ、Differentiated Services)

QoS 機能にはトラフィックをストリームに分類してホップごとの振る舞いに合わせて QoS 処理を行う DiffServ(Differentiated Services)サポートも含まれています。

標準的な IP ベースのネットワークはベストエフォートデータ伝送を提供するように設計されていま す。ベストエフォートサービスは保証なしにデータを届けることを意味しています。輻輳時には、パ ケットは遅延したり、散発的に届いたり、廃棄されたりします。Eメール転送、ファイル転送のような 典型的なインターネットアプリケーションにとっては多少のサービス劣化は許容され、多くの場合は 気づくことはありません。逆に、音声やビデオのような時間遅延要件が厳しいアプリケーションに取 っては少しのサービス劣化も許容できません。

DiffServ 定義(Defining DiffServ)

DiffServ を利用するには、DiffServ メニューページで以下の項目を最初に設定する必要があります。

- 1. Class: クラスを作成してクラス基準(criteria)を定義します。
- 2. Policy:ポリシーを作成してクラスにポリシーを関連付け、ポリシーステートメントを定義します。
- 3. Service:ポリシーを受信インターフェースに追加します。

パケットは定義された基準に基づいて分類、処理されます。分類基準はクラスによって定義されま す。処理はポリシーの属性(attribute)で定義されます。ポリシーアトリビュートはクラスごとのイン スタンスベースで定義され、一致が発生した場合にアトリビュートが適用されます。ポリシーは複数 のクラスを持てます。ポリシーが有効なとき、どのクラスがパケットと一致したかによってアクション が実行されます。

パケット処理はパケットのクラスがマッチするかを試すことから始まります。ポリシーの中のクラスの一致が見つかった時点でポリシーが適用されます。

DiffServ メニューページは様々な DiffServ 設定と表示機能へのリンクを含みます。

QoS > DiffServを選択すると以下の機能のリンクへのページを表示します。

- DiffServ 設定(Diffserv Configuration)
- クラス設定(Class Configuration) 9
- IPv6 クラス設定(IPv6 Class Configuration)
- ポリシー設定(Policy Configuration)
- サービス設定(Service Configuration)
- サービス統計(Service Statistics)

DiffServ 設定(Diffserv Configuration)

Diffserv Configuration ページでは、現在のモード設定および DiffServ プライベート MIB の現在および最大行数を確認することができます。

NETGEA	R'		GS110T 8 Port Gigabit PoE Smart Swit with 2 Fiber S
System S	witching QoS	Security Monitoring Maintenance H	elp
CoS DiffServ	DiffServ Configurat	ion	
	DiffServ Configurati	on 💿	
Advanced	DiffServ Admin Mode	🔿 Disable 💿 Enable	
	• .		
	Status	0	
	MIB Table	Current Size / Max Size	
	Class table	0 / 32	
	Class Rule table	0 / 192	
	Policy table	0 / 32	
	Policy Instance table	0 / 320	
	Policy Attributes table	0 / 960	
	Service table	0 / 16	
	<		>
			REFRESH CANCEL APPLY

グローバル DiffServ 設定をする。

- 1. QoS > DiffServ > Advanced > Diffserv Configuration を選択して Diffserv Configuration ページ を表示します。
- 2. DiffServ のモードを選択します。
 - Enable:DiffServ が有効(enable)です。
 - **Disable:** DiffServ が無効(disable)です。
- 3. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。
- 4. Apply ボタンをクリックして設定をスイッチに適用します。

以下に DiffServ Configuratior	ページの Status	。欄に表示される情	報の説明を示します。
----------------------------	-------------	-----------	------------

項目	説明
Class Table	クラステーブルの現在と最大の行数。
Class Rule Table	クラスルールテーブルの現在と最大の行数。
Policy Table	ポリシーテーブルの現在と最大の行数。
Policy Instance Table	ポリシーインスタンステーブルの現在と最大の行数。
Policy Attributes Table	ポリシーアトリビュートテーブルの現在と最大の行数。
Service Table	サービステーブルの現在と最大の行数。

Refresh ボタンをクリックしてスイッチの最新情報を表示させます。

クラス設定(Class Configuration)

Class Configuration ページで DiffServ クラス名の追加、および既存クラスの変更および削除がで きます。DiffServ クラスと関連付けるクライテリアを定義することもできます。パケットを受信した際 にこれらの DiffServ クラスが使われてパケットが優先されます。一つのクラス中で複数のマッチク ライテリアを持つことができます。クラスを作成した後、クラスリンクをクリックしてクラスページを表

示します。

Onnect with Innovation	A R'						6 Port Gigabit PoE Smart Swite with 2 Fiber Sf
System	Switching	QoS	Security	Monitoring	Maintenance	Help	LOGOUT
CoS DiffServ			80				
Basic Advanced	Class Co	onfigurati Configurati	on		(9)		
 Configuration Class Configuration 	Class	s Name		Class Type			
 » Policy Configuration » Service Configuration 							
» Service Statistics							
	<						
					REFRESH	ADD [DELETE CANCEL APPLY

DiffServ クラスを設定する

- 1. QoS > DiffServ > Advanced > Class Configuration を選択して Class Configuration ページを表示します。
- 新しいクラスを作成するには、クラス名を Class Name 欄に記入し、Class Type を指定して Add ボタンをクリックします。
 スイッチのサポートしている Class Type は All のみです。
- 3. 既存のクラス名を変更するには、変更するクラスのチェックボックスを選択し、変更をします。変 更後、Apply ボタンをクリックします。
- 4. クラスを削除するには、削除するクラスのチェックボックスを選択し、Delete ボタンをクリックします。
- 5. Refresh ボタンをクリックしてスイッチの最新情報を表示させます。
- 6. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。

クラスマッチクライテリアを設定する

1. 作成済みのクラス名をクリックします。

NETGEA Connect with Innovation	R'						6 Port Gigabit PoE Smart Sw with 2 Fiber
System S	Switching	QoS	Security	Monitoring	Maintenance	Help	LOGOU
CoS DiffServ			8				
Basic	Class Co	nfigurati	on				
 Advanced » DiffServ 	Class (Configuratio	on		۲		
Configuration » Class	Class	Name		Class Type			
Configuration		ş					
* Policy Configuration				All			
 Service Configuration 							
» Service Statistics							
	1						
	<						
					REFRESH	ADD [DELETE CANCEL APPLY
Copyright © 1996-2	010 Netgear ®						

クラス名はハイパーリンクになっており、以下のような DiffServ Clas Configuration 画面が表 示されます。

System S	witching QoS Secur	ity Monitoring Maintenance Help	LOGO					
COS DINOBIA								
Basic	Class Configuration							
Advanced	3							
 DiffServ Configuration 	Class Information	0						
Class	Class Name	voice						
	Class Type	All						
Policy								
Configuration Service	Diffserv Class Configuration ()							
Configuration	Reference Class	No Reference Class Present						
Service	Class of Service							
Statistics	VLAN	(1 - 4093)						
	Ethernet Type	(0600 - FFFF)						
	Source MAC							
	Source MAC Mask							
	Destination MAC							
	Destination MAC Mask							
	Protocol Type	0 (0 - 255)						
	Source IP Address							
	Source Mask	(0.65535)						
	Destination ID Address							
	Destination Mask							
	Destination L4 Port	♥ 0 (0 - 65535)						
	IP DSCP	0 (0 - 63)						
	IP Precedence	(0 - 7)						
	IP ToS	ToS Bit Value ToS Bit Mask						

- 2. DiffServ クラスに関連付けられたクライテリア(criteria)を定義します。
 - Reference Class:参照クラスを指定します。
 - Class of Service:802.1p CoS 値(0-7)を選択します。
 - VLAN: VLAN ID(1-4093)を指定します。
 - EtherType: イーサタイプを選択します。値で指定したいときは、User Value を選択し、0600-FFFF の範囲で値を記入します。
 - Source MAC:送信元 MAC アドレスを指定します。
 - Source MAC Mask:送信元 MAC アドレスマスクを指定します。FF:FF:FF:FF:FF:FF:FF の場合は 一つの MAC アドレスを指定することになります。
 - Destination MAC: 宛先 MAC アドレスを指定します。
 - Destination MAC Mask: 宛先 MAC アドレスマスクを指定します。FF:FF:FF:FF:FF:FF: の場合 は一つの MAC アドレスを指定することになります。
 - Protocol Type:レイヤー4 プロトコルを指定します。Other を指定してプロトコル番号(0-255) を指定することもできます。
 - Source IP Address:送信元 IP アドレス(A.B.C.D 形式)を指定します。
 - Source Mask: 送信元 IP アドレスマスクを指定します。
 - Source L4 Port:送信元 TCP/UDP ポート番号を指定します。Other を指定してポート番号を 直接設定することもできます。
 - Destination IP Address: 宛先 IP アドレス(A.B.C.D 形式)を指定します。
 - Destination Mask: 宛先 IP アドレスマスクを指定します。

- Destination L4 Port: 宛先 TCP/UDP ポート番号を指定します。Other を指定してポート番号 を直接設定することもできます。
- IP DSCP: パケットの DSCP を指定します。Other を指定して DSCP の値(0-63)を直接指定することもできます。
- IP Precedence:パケットの IP Precedence 値(0-7)を指定します。
- IP ToS: パケットの IP ヘッダーの ToS ビット(16 進 2 桁)を指定します。
- 3. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。
- 4. Apply ボタンをクリックして設定をスイッチに適用します。すぐに設定変更がされます。
- 5. Refresh ボタンをクリックしてスイッチの最新情報を表示させます。

IPv6 クラス設定(IPv6 Class Configuration)

IPv6 クラス設定で IPv6 パケット識別を行って、今までの QoS ACL と DiffServ 機能を拡張すること ができます。イーサネット IPV6 パケットはイーサタイプの値で IPv4と区別ができ、イーサタイプで IPv6 を識別可能です。

NETGEAR Connect with Innovation			8 Port Giga	GS110TP bit PoE Smart Switch with 2 Fiber SFP
System Swite	hing QoS S	ecurity Monitoring	Maintenance Hel	р Сосоот
CoS DiffServ				
> Basic	IPv6 Class Config	uration		~
* Advanced * DiffServ	IPv6 Class Configu	Iration	0	
Configuration	Class Name	Class Type		
» IPv6 Class				
Configuration >> Policy				
Configuration				
 Service Configuration 				
» Service Statistics				
				~
	<			>
		REFRE	SH ADD DELETE CAI	NCEL APPLY
	ETCEAD @			

IPv6 クラスを設定する。

- 1. QoS > DiffServ > Advanced > IPv6 Class Configuration を選択して IPv6 Class Configuration ペ ージを表示します。
- 新しいクラスを作成するには、クラス名を Class Name 欄に記入し、Class Type を指定して Add ボタンをクリックします。
 スイッチのサポートしている Class Type は All のみです。
- 3. 既存のクラス名を変更するには、変更するクラスのチェックボックスを選択し、変更をします。変 更後、Apply ボタンをクリックします。
- 4. クラスを削除するには、削除するクラスのチェックボックスを選択し、Delete ボタンをクリックします。
- 5. Refresh ボタンをクリックしてスイッチの最新情報を表示させます。
- 6. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。

クラスマッチクライテリアを設定する。

1. 作成済みのクラス名をクリックします。

NETGEAR' GS110 Conrect with Innovation" 8 Port Gigabil PdE Smort with 2 Fibb	OTP Switch er SFP
System Switching QoS Security Monitoring Maintenance Help Loca	τυς
CoS DiffServ	
Basic J Basic J Hyd Class Configuration Differv Configuration Configuration Policy Configuration Service Service Statistics I Public Class Configuration I Public Cla	^
	_ ~
REFRESH ADD DELETE CANCEL APPL	
Copyright © 1996-2015 NETGEAR ®	

クラス名はハイパーリンクになっており、以下のような DiffServ Class Configuration 画面が表示されます。

NETGEAR Connect with Innovation	•	B Port Gigabit Po v	E Smart Switch ith 2 Fiber SFP
System Swite CoS DiffServ	hing QoS Security	Monitoring Maintenance Help	LOGOUT
> Basic > Advanced	Class IPv6 Configuration		^
» DiffServ	Class Information		0
Configuration > Class Configuration > IPv6 Class Configuration	Class Name Class Type	IPv6Class1 All	
» Policy	Diffserv Class Configuration		0
Configuration > Service Configuration > Service Statistics	Match Every Reference Class Source IPv6 Prefix/Length Source L4 Port Destination IPv6 Prefix/Length	V V 0 (0 - 65535)	
	Destination L4 Port	V 0 (0 - 65535)	
			~
	<	REFRESH CANCEL	APPLY
Copyright © 1996-2015 N	IETGEAR ®		

- 2. IPv6 クラスに関連付けられたクライテリア(criteria)を定義します。
 - Class Name: 作成したクラス名が表示されます。
 - Class Type:クラスタイプが表示されます。All のみです。
 - Match Every:Any のみが選択可能です。
 - Reference Class:参照クラスを指定します。
 - Source IPv6 Prefix/Length:送信元 IPv6 プレフィクスを設定します。フォーマットはグローバルアドレスフォーマットです。
 - Source L4 Port:送信元 TCP/UDP ポート番号を指定します。Other を指定してポート番号を 直接設定することもできます。

- Destination IPv6 Prefix/Length: 宛先 IPv6 プレフィクスを設定します。フォーマットはグローバルアドレスフォーマットです。
- Destination L4 Port: 宛先 TCP/UDP ポート番号を指定します。Other を指定してポート番号 を直接設定することもできます。
- 3. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。
- 4. Apply ボタンをクリックして設定をスイッチに適用します。すぐに設定変更がされます。
- 5. Refresh ボタンをクリックしてスイッチの最新情報を表示させます。

ポリシー設定(Policy Configuration)

Policy Configuration ページでクラスとポリシーの関連付けをします。ポリシーを作成後、ポリシー リンクをクリックしてポリシークラス設定を行います。

NETGEA Connect with Innovation	R.				8 Port Gig	GS108T abit Smart Switch	
System	Switching QoS	Security	Monitoring	Maintenance	Help	LOGOUT	
CoS DiffServ							
Basic	Policy Configurati	ion					
* Advanced * DiffServ	Policy Configurati	on		۲			
Configuration » Class	Policy Selector		Policy Type	Member Class			
Configuration]			-	
Configuration » Service							
Configuration							
Statistics							
						_	リシーを作成後、
	< <u>.</u>		Ш				
				A	DD DELETE C	ANCEL APPLY	
Copyright © 1996-2	009 Netgear ®						

DiffServ ポリシーを設定する。

- 1. QoS > DiffServ > Advanced > Policy Configuration を選択して Policy Configuration ページを表示します。
- ポリシーを作成するには、Policy Selector 欄にポリシー名を入力し、Member Class 欄でクラスを 選択します。Add ボタンをクリックしてポリシーを作成します。 ポリシータイプ (Policy Type)は In のみであり、受信方向のトラフィックにのみ有効です。この設 定は変更不可です。
- 3. 既存のポリシー名を変更するには、変更するポリシーのチェックボックスを選択し、変更をしま す。変更後、Apply ボタンをクリックします。
- ポリシーを削除するには、削除するポリシーのチェックボックスを選択し、Delete ボタンをクリックします。
- 5. Refresh ボタンをクリックしてスイッチの最新情報を表示させます。
- 6. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。

ポリシーアトリビュートを設定する。

1. ポリシーをクリックして Policy Class Configuration ページを表示します。

NETGEA Connect with Innovation	R.					8 Port G	GS108T igabit Smart Switch
System CoS DiffServ	Switch	ing QoS	Security	Monitoring	Maintena	nce Help	LOGOUT
Basic Advanced DiffServ	Pol	icy Configuration	on		(2)		
Configuration » Class		Policy Selector		Policy Type	Member Class		
× Policy Configuration		newPol		In	voice 💌		E.
» Service Configuration » Service Statistics							
	<						×
Copyright @ 1996-2	009 Ne	toear ®				ADD DELETE	CANCEL APPLY

ポリシー名はハイパーリンクになっており、以下のような Policy Class Configuration 画面が表示されます。

NETGEA Connect with Innovation"	R.					GS110TP 8 Port Gigabit PoE Smart Switch with 2 Fiber SFP
System S	witching QoS	Security	Monitoring	Maintenance	Help	LOGOUT
CoS DiffServ						
> Basic ~ Advanced	Policy Class Con	figuration				0
 » DiffServ Configuration » Class Configuration » IPv6 Class Configuration 	Policy Name Policy Type Member Class Name	[Test In IPv6Class1			
 Policy Configuration 	Policy Attribute					0
 » Service Configuration » Service Statictics 	Assign Queue	l				
	Policy Attribute O	Drop Mark COS Mark IP DSCP		0 💌 af11 💌		
	c	Simple Policy				
		Color Mode		ColorBlind	I	
		Committed Rat	e			
		Committed Bur	st Size			
		Conform Action	1	Violate Action @ Send		
		 Drop Mark CoS Mark IP DS 	0 💌	C Drop Mark Cos	0 💌 SCP af11 💌	
	1					p
					R	EFRESH CANCEL APPLY

- 2. Assign Queue:このクラス・ポリシーで割り当てるキューを選択します。
- 3. Policy Attribute:以下のポリシーアトリビュート(Policy Attribute)を設定します。

- Drop:パケットを廃棄する場合に選択します。
- Mark CoS: 802.1p CoS 値(0-7)を適用したい場合に選択します。CoS を含むタグを持たない パケットに対してはヘッダーが追加されます。
- Mark IP DSCP: DSCP 値を適用したい場合に選択します。
- Simple Policy:トラフィックポリシングを実施したい場合に選択し、以下の設定をします。
- 4. Simple Policy を選択した場合に以下の設定をします。
 - Color Mode: このスイッチでは固定で color blind のみです。
 - Committed Rate: 速度を kbps 単位で指定します。 値の範囲は 1-4294967295 です。
 - Committed Burst Size: バーストサイズを kbyte 単位で指定します。 値の範囲は 1-128 です。
 - Conform Action: Committed Rate および Committed Burst Size に適合した場合にパケット に対するアクションを以下から選択します。
 - Send: (デフォルト)そのまま転送されます。
 - Drop:廃棄されます。
 - Mark CoS: 指定した CoS 値を設定して転送します。
 - Mark IP DSCP: DSCP 値を設定して転送します。
 - Violate Action: Committed Rate および Committed Burst Size に違反した場合にパケットに 対するアクションを以下から選択します。
 - Send: (デフォルト)そのまま転送されます。
 - Drop:廃棄されます。
 - Mark CoS: 指定した CoS 値を設定して転送します。
 - Mark IP DSCP: DSCP 値を設定して転送します。
- 5. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。
- 6. Apply ボタンをクリックして設定をスイッチに適用します。すぐに設定変更がされます。
- 7. Refresh ボタンをクリックしてスイッチの最新情報を表示させます。

サービス設定(Service Configuration)

Service Configuration ページでインターフェースにポリシーを有効にします。

Connect with Innovation							with 2 Fiber S
System	Switchin	ng QoS	Security	Monitorin	g Maintenance	Help	LOGOUT
CoS DiffServ							
Basic	Ser	vice Config	uration				
Advanced		onvice Confi	uration		0		
 DiffServ Configuration 	POR			CO TO INTERFA	CE		
» Class	POR	ENGS		GO TO INTERIA	Operational		
 Policy 		Interface	Policy In	Direction	Status		
Configuration			None 💌				
		g1					
» Service		g2					
Statistics		g3					
		g4	_	_			
		g5					
		g6					
		g/					
		g0 a9					
		g10					
	POR	TS LAGS	All	GO TO INTERFA	CEGO		
	<				ш		>

インターフェースに DiffServ ポリシーを適用する。

- 1. QoS > DiffServ > Advanced > Service Configuration を選択して Service Configuration ページを 表示します。
- 2. PORTS をクリックして、物理ポートの DiffServ ポリシー設定をします。
- 3. LAGS をクリックして、LAG (Link Aggregation Group)の DiffServ ポリシー設定をします。
- **4.** ALL をクリックして、物理ポートと LAG (Link Aggregation Group)の両方の DiffServ ポリシー設定をします。
- 5. 設定をしたいポートまたは LAG の横のチェックボックスをクリックして選択をします。複数の選択 をして共通の設定をすることも可能です。先頭のチェックボックスをクリックするとすべてのインタ ーフェースを選択できます。
- 6. 選択したインターフェースにポリシーを適用するには、Policy In メニューからポリシーを選択して Apply ボタンをクリックします。
- 7. 選択したインターフェースのポリシーを削除するには、Policy In メニューからポリシーNone を選択して Apply ボタンをクリックします。
- 8. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。

サービス統計(Service Statistics)

Service Statistics ページで DiffServ ポリシーを適用したインターフェースのサービスレベルの統計情報を確認することができます。

QoS > DiffServ > Advanced > Service Statistics を選択して Service Statistics メニューを表示します。

IETGEA	R'						GS108
nnect with Innovation						8 Port Gigabi	t Smart Swit
System S	Switching	QoS Security	Monitoring	Maintenan	ce Hel	р	LOGOU
CoS DiffServ	(D) 						
Basic	Service Sta	atistics					
» DiffServ	Service S	tatistics				(?)	
Configuration » Class	Interface	Direction	Policy Name	Operational Status	Discarded Packets	Member Classes	
Configuration » Policy	g3	In	pol_voip	Down	0	voice 💙	
Configuration							
Configuration							
Statistics							
	<						
							REFRESH

以下に DiffServ Configuration ページの Status 欄に表示される情報の説明を示します。

項目	説明
Interface	統計情報を表示するインターフェースを表示します。
Direction	統計を表示するトラフィックの方向を表示します。常に In(受信方向)で す。
Policy Name	インターフェースに適用されているポリシー名を表示します。
Operational Status	インターフェースの動作状態を示します。 Up または Down のどちらかで す。
Discarded Packets	廃棄されたパケット数を表示します。
Member Classes	表示したいクラスを選択します。

Refresh ボタンをクリックしてスイッチの最新情報を表示させます。

5.デバイスセキュリティ管理

Security タブにある機能を使ってポート、ユーザー、およびサーバーセキュリティのセキュリティ管理を設定します。Security タブは以下の機能へのリンクリンクを含みます。

- 管理セキュリティ設定(Management Security Settings)
- 管理アクセス設定(Configuring Management Access)
- ポート認証(Port Authentication)
- トラフィック制御(Traffic Control)
- ACLを設定する(Configuring Access Control Lists)

管理セキュリティ設定(Management Security Settings)

Management Security Settings ページでログインパスワード、RADIUS、TACACS+および認証リストを設定することができます。

Security > Management Security タブで以下の機能にアクセスできます。

- パスワード変更(Change Password)
- RADIUS 設定(RADIUS Configuration)
- TACACS+設定(Configuring TACACS+)
- 認証リスト設定(Authentication List Configuration)

パスワード変更(Change Password)

NETGEAR'					GS108
Connect with Innovation™				8 Port Gigabit	Smart Swite
System Switc	hing QoS Security	Monitoring	Maintenance	Help	LOGOUT
Management Security	Access Port Authentication Traf	fic Control ACL			
• User Configuration	Change Password				
Change Password RADIUS	· Change Password			()	
TACACS+ Authentication List	Old Password	•••••	(1 to 20)	
Addicated to 1 cist	New Password		(1 to 20)	
	Confirm Password Reset Password		(1 to 20)	
	<))
				REFRESH CANCE	L APPLY
onvright @ 1996-2009 N	etaear @				

管理インターフェースのログインパスワードを変更する

- **1.** Security > Management Security > User Configuration > Change Password を選択してパスワード変更ページを表示します。
- 2. Old Password:既存のパスワードを入力します。入力したパスワードは*で表示されます。パス ワードは 20 文字までの英数字で、大文字と小文字が区別されます。
- 3. New Password:新しいパスワードを入力します。
- 4. Confirm Password:新しいパスワードを再度入力します。
- 5. Reset Password:パスワードを初期化したい時にチェックボックスをクリックします。
- 6. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。
- 7. Apply ボタンをクリックして設定をスイッチに適用します。

メモ:パスワードを忘れてしまった場合、全面パネルの Factory Defaults ボタンを 5 秒以上 押してファクトリーデフォルト設定を回復します。Reset ボタンはスイッチを再起動するのみで す。

RADIUS 設定(RADIUS Configuration)

RADIUS サーバーはネットワークに追加のセキュリティを提供します。RADIUS サーバーはユーザ ー単位の認証情報を含むユーザーデータベースを維持します。スイッチはネットワークの使用を認 証する前にユーザー名とパスワードを認証する RADIUS サーバーへ情報を転送します。RADIUS サーバーは以下のものに対する集中型の認証手順を提供します。

- Web アクセス(Web Access)
- 802.1X(Access Control Port)

RADIUS フォルダは以下の機能へのリンクを含みます。

- グローバル設定(Global Configuration)
- RADIUS サーバー設定(RADIUS Server Configuration)
- アカウンティングサーバー設定(Accounting Server Configuration)

グローバル設定(Global Configuration)

RADIUS Configuration ページでネットワーク上の RADIUS サーバーの情報を追加します。

NETGEAR' Connect with Innovation	GS110TP 8 Port Gigabit PoE Smart Switch with 2 Fiber SFP
System Switching QoS Security Monitoring Maintene	ance Help LOGOUT
Management Security Access Port Authentication Traffic Control ACL	
> User Configuration > RADIUS = Global Configuration > Server Configuration > Accounting Server Configuration > Accounting Server Configuration > Accounting Server Configuration > TACACS+ > Authentication List	⑦
<	×
	CANCEL
Copyright © 1996-2010 Netgear ®	

RADIUS サーバー設定がされていない場合は、Current Server IP Address 欄は空白です。スイッ チは最大 3 台までの RADIUS サーバーを設定することができます。複数の RADIUS サーバーが 設定されると、Current Server がプライマリーサーバーとなります。サーバーがプライマリーサーバ ーとして 1 台も設定されていない場合は、Current Server は直近に追加された RADIUS サーバー となります。

グローバル RADIUS サーバー設定をする

- 1. Security > Management Security > RADIUS > Global Configuration を選択して Global Configuration ページを表示します。
- 2. Max Number of Retransmits: RADIUS サーバーへの要求パケットの最大送信回数(1-15)。

Max Number of Retransmits と Timeout Duration を設定する際は最大遅延を考慮する必要があり ます。複数の RADIUS サーバーが設定される場合、最大再送回数に達してから次のサーバーに 移ります。RADIUS サーバーから応答がなくタイムアウトになるまで再送はされません。したがっ て、RADIUS アプリケーションから応答を受信するまでの最大時間はすべてのサーバーへの再送 タイムアウトの合計値と等しくなります。RADUIS 要求がユーザーログインによって発生するなら ば、すべてのユーザーインターフェースは RADIUS アプリケーションが応答を返すまではブロックさ れます。

3. Timeout Duration:要求の再送タイムアウト値(秒)を設定します。(1-30)

Max Number of Retransmits と Timeout Duration を設定する際は最大遅延を考慮する必要があり ます。複数の RADIUS サーバーが設定される場合、最大再送回数に達してから次のサーバーに 移ります。RADIUS サーバーから応答がなくタイムアウトになるまで再送はされません。したがっ て、RADIUS アプリケーションから応答を受信するまでの最大時間はすべてのサーバーへの再送 タイムアウトの合計値と等しくなります。RADUIS 要求がユーザーログインによって発生するなら ば、すべてのユーザーインターフェースは RADIUS アプリケーションが応答を返すまではブロックさ れます。

- **4. Accounting Mode**: RADIUS アカウンティングモードの有効(Enable)、無効(Disable)を選択 します。
- 5. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。
- 6. Apply ボタンをクリックして設定をスイッチに適用します。

RADIUS サーバー設定(RADIUS Server Configuration)

RADIUS Server Configuration ページで RADIUS サーバーの設定をします。

NETGEAR Connect with Innovation												B Port Gigat	GS108 bit Smart Swi	β T tch
System Switching	QoS	Se	curity	Monitoring	Maintena	nce	Help						LOGO	л
Management Security Ac	cess Port Aut	henticatic	n Traffic C	Control ACL										
User Configuration RADIUS Slobal Configuration	Server C	onfigu Configu	ration										۲	^
 Server Configuration Accounting Server Configuration TACACS+ 	Se Se	erver Ad	ldress	Auti 181	nentication 2	Port S	ecret Configu	red Secre	t	Active Secondar	Me y M Di	ssage Autho sable 💌	enticator	
Authentication List	Statisti	cs		20.							20		0	
	Server Address	Round Trip Time	Access Requests	Access Retransmission	Access Accepts	Access Rejects	Access Challenges	Malformed Access Responses	Bad Authenticators	Pending Requests	Timeouts	Unknown Types	Packets Dropped	
									CLEAR COUNTERS	REFRESH	ADD D	ELETE CAN	CEL APPLY	

RADIUS サーバー設定をする

- 1. Security > Management Security, > RADIUS > Server Configuration を選択して Server Configuration ページを表示します。
- 2. RADIUS サーバーを追加するには、以下の項目を設定して、Add ボタンをクリックします。
 - Server Address: RADIUS サーバーの IP アドレスを記入します。
 - Authentication Port: RADIUS サーバー認証に使う UDP ポートを記入します。(0-65535)
 - Secret Configured: RADIUS シークレットを使用するには Yes を選択します。
 - Secret: 共有シークレットを記入します。
 - Active: サーバーが Primary か Secondary かを選択します。
- 7. Message Authenticator: Message Authenticator の有効(Enable)、無効(Disable)を選択します。

- 8. 既存の RADIUS サーバー設定を変更するには、変更する RADIUS サーバーのチェックボックス を選択し、変更をします。変更後、Apply ボタンをクリックします。
- 9. RADIUS サーバーを削除するには、削除する RADIUS サーバーのチェックボックスを選択し、 Delete ボタンをクリックします。
- 10. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。
- 11. Refresh ボタンをクリックしてスイッチの最新情報を表示させます。
- 以下に Server Configuration ページの Statistics 欄に表示される情報の説明を示します。

項目	説明
Server Address	RADIUS サーバーの IP アドレス。
Round Trip Time	RADIUS 認証サーバーへの応答時間(1/100 秒単位) 。
Access Requests	RADIUS 認証要求パケットの送信数。再送回数は含まない。
Access Retransmissions	RADIUS 認証要求パケットの再送数。
Access Accepts	サーバーから受信した RADIUS 認証許可パケット(無効を含む)の数。
Access Rejects	サーバーから受信した RADIUS 認証拒否パケット(無効を含む)の数。
Access Challenges	サーバーから受信した RADIUS 認証チャレンジパケット(無効を含む)の数。
Malformed Access Responses	RADIUS サーバーから受信した不正な形式の RADIUS 認証応答パケット数。 不正な形式のパケットには、無効な長さのパケットが含まれます。無効なオー センティケーター、無効な署名属性を含むパケットおよび不明なタイプのパケッ トは含まれません。
Bad Authenticators	RADIUS サーバーから受信した無効なオーセンティケーターや無効な署名属 性を含む RADIUS 認証応答パケットの数。
Pending Requests	RADIUS サーバーに送信された後に、タイムアウトになっていないか、または 応答を受信していない、RADIUS 認証要求パケット数。
Timeouts	RADIUS サーバーに対する認証タイムアウト数。
Unknown Types	RADIUS サーバーの認証ポートから受信した不明なタイプの RADIUS パケットの数。
Packets Dropped	RADIUS サーバーの認証ポートから受信し、何らかの理由で破棄された RADIUS パケット数。

ページ下部のボタンを使って以下の操作をします。

- Clear Counters ボタンをクリックして値を初期化します。
- Refresh ボタンをクリックしてスイッチの最新情報を表示させます。

アカウンティングサーバー設定(Accounting Server Configuration)

RADIUS Accounting Server Configuration ページでネットワークの RADIUS アカウンティングサー バー設定をします。

System Swite	hing QoS	Security	Monitoring	Maintenance	Help	LOGO
Management Security	Access Port Aut	hentication Traf	fic Control ACL			
User Configuration	Accounting S	Server Config	uration			
RADIUS » Global	Accounting	Server Configur	ation	0		
Configuration	Accounting Serve	er 0.0.0.0				
» Server Configuration	Address	1813		(0 to 65535)		
Accounting Server	Secret Configure	d No	~			
TACACS+	Secret					
Authentication List	Accounting Mode	Disable				
	Accounting	Server Statistic	5	0		
	Accounting Serve	er Address				
	Round Trip Time	(secs) ests				
	Accounting Retra	ansmissions				
	Accounting Resp	onses Inting Responses				
	Bad Authenticat	ors				
	Pending Request	s				
	Unknown Types					
	Packets Dropped	1				
	.1					

RADIUS アカウンティングサーバー設定をする

- 1. Security > Management Security > RADIUS > Accounting Server Configuration を選択して Accounting Server Configuration ページを表示します。
- 2. RADIUS アカウンティングサーバーを追加するには、以下の項目を設定して、Apply ボタンをクリックします。
 - Accounting Server Address: RADIUS アカウンティングサーバーの IP アドレスを記入します。
 - Port: RADIUS アカウンティングサーバー認証に使う UDP ポートを記入します。(0-65535)
 - Secret Configured: RADIUS シークレットを使用するには Yes を選択します。
 - Secret:共有シークレットを記入します。
 - Accounting Mode: RADIUS アカウンティングモードの有効(Enable)、無効(Disable)を選択します。
- 3. RADIUS アカウンティングサーバーを削除するには、削除する RADIUS アカウンティングサーバ ーのチェックボックスを選択し、Delete ボタンをクリックします。
- 4. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。
- 5. Refresh ボタンをクリックしてスイッチの最新情報を表示させます。

Accounting Server Configuration ページの Accounting Server Statistics 欄に表示される情報の説明を示します。

項目	説明
Accounting Server Address	RADIUS アカウンティングサーバーの IP アドレス。
Round Trip Time (secs)	RADIUS アカウンティングサーバーへの応答時間(1/100 秒単位)。

GS108T/GS110TP スマートスイッチソフトウェア管理マニュアル

Accounting Requests	RADIUS アカウンティング要求パケットの送信数。再送回数は含まない。
Accounting Retransmissions	RADIUS アカウンティング要求パケットの再送数。
Accounting Responses	RADIUS アカウンティングパケットのアカウンティングポートでの受信数。
Malformed Accounting Responses	RADIUS サーバーから受信した不正な形式の RADIUS アカウンティング応 答パケット数。不正な形式のパケットには、無効な長さのパケットが含まれ ます。無効なオーセンティケーター、無効な署名属性を含むパケットおよび 不明なタイプのパケットは含まれません。
Bad Authenticators	RADIUS サーバーから受信した無効なオーセンティケーターや無効 な署名属性を含む RADIUS アカウンティング応答パケットの数。
Pending Requests	RADIUS アカウンティングサーバーに送信された後に、タイムアウトに なっていないか、または応答を受信していない、RADIUS アカウンティ
Timeouts	RADIUS アカウンティングサーバーに対する認証タイムアウト数。
Unknown Types	RADIUS アカウンティングサーバーのアカウンティングポートから受信した不 明なタイプの RADIUS パケットの数。
Packets Dropped	RADIUS アカウンティングサーバーのアカウンティングポートから受信し、何 らかの理由で破棄された RADIUS パケット数。

ページ下部のボタンを使って以下の操作をします。

- Clear Counters ボタンをクリックして値を初期化します。
- Refresh ボタンをクリックしてスイッチの最新情報を表示させます。

TACACS+設定(Configuring TACACS+)

TACACS+は RADIUS や他の認証方式との一貫性を保ちつつ集中ユーザー管理システムを提供します。TACACS+は以下のサービスを提供します。

- **認証(Authentication)**: ログインの最中とユーザー名とユーザー作成のパスワードでの 認証を提供します。
- **承認(Authorization)**: ログイン時に実行されます。認証が完了した時、認証されたユーザー名 を使って承認セッションが開始します。TACACS+サーバーはユーザー権限を確認します。

TACACS+プロトコルはデバイスとTACACS+サーバーの間で暗号化したプロトコル通信でネットワークセキュリティを確実にします。

TACACS+フォルダは以下の機能へのリンクを含んでいます。

- TACACS+設定(TACACS+ Configuration)
- TACACS+サーバー設定(TACACS+ Server Configuration)

TACACS+設定(TACACS+ Configuration)

TACACS+ Configuration ページはインバンド管理ポートを介してスイッチと TACACS+サーバーとの間の通信のための TACACS+設定をします。

NETGEAR					8 Port Giga	GS108T abit Smart Switch
System Swite	hing QoS	Security	Monitoring	Maintenance	Help	LOGOUT
Management Security	Access Port Authentice	ation Traffic	Control ACL	20		
User Configuration	TACACS+ Config	uration				
RADIUS TACACS+	TACACS+ Config	uration		0		
* TACACS+	Key String	•••••		(0 to 128)		
Configuration	Connection Timeout	5		(1 to 30)		
Configuration						
Authentication List						
	<					>
					CA	NGEL APPLI

グローバル TACACS+設定をする

- 1. Security > Management Security > TACACS+ > TACACS+ Configuration を選択して TACACS+ Configuration ページを表示します。
- Key String:スイッチと TACACS+サーバー間の通信のための暗号化キーを指定します。0-128 文 字です。
- **3. Connection Timeout**: スイッチと TACACS+サーバー間の TCP コネクション確立のための最大時 間(秒)(1-30 秒)
- 4. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。
- 5. Apply ボタンをクリックして設定をスイッチに適用します。

TACACS+サーバー設定(TACACS+ Server Configuration)

TACACS+ Server Configuration ページでスイッチが通信する TACACS+サーバーを 5 つまで設定 できます。

NETGEAR Connect with Innovation				8 Port	GS110TP I Gigabit PoE Smart Switch with 2 Fiber SFP
System Switc	hing QoS	Security Moni	toring Mainter	iance Help	LOGOUT
Management Security	Access Port Authentica	tion Traffic Control	ACL		
User Configuration PADTUS	Server Configura	tion			^
* TACACS+	Server Configurat	tion		1	
 TACACS+ Configuration Server Configuration Authentication List 	TACACS+ Server Server Address	Add			E
	<				DELETE APPLY

TACACS+サーバー設定をする

- 1. Security > Management Security > TACACS+ > Server Configuration を選択して Server Configuration ページを表示します。
- 新しい TACACS+サーバーを追加するには、TACACS+ Server 欄で Add を選択し、Server Address 欄に TACACS+サーバーの IP アドレスを記入してから Apply ボタンをクリックします。

メモ: Add は TACACS+サーバー設定が 5 未満の場合に選択可能であり、Server Address 欄は Add が選択された時のみ表示されます。

TACACS+サーバーを追加すると、追加の欄が表示されます。

3			
Server Configuration	on		0
TACACS+ Server	192.1	168.2.34	~
Priority	0	(0 to 65535)	
Port	49	(0 to 65535)	
Key String		••	(0 to 128 characters)
Connection Timeout	5	(1 to 30)	

- Priority: TACACS+サーバーが使われる優先順位を記入します。(0-65535) 0 の優先度が最高です。
- Port: TACACS+セッションで使用する認証ポート番号を指定します。デフォルトは 49 で範囲 は 0-65535 です。
- 5. Key String:スイッチと TACACS+サーバーの間で使われる認証と暗号のキーを指定します。有 効な長様 0-128 文字です。
- 6. Connection Timeout: デバイスとTACACS+サーバー間の通信タイムアウト値(秒)を指定しま す。範囲は 1-30(秒)です。
- 7. 設定を変更あるいは追加した場合は、Apply ボタンをクリックして変更を適用します。
- 8. TACACS+サーバーを削除するには、削除する TACACS+サーバーをメニューから選択し、Delete ボタンをクリックします。

認証リスト設定(Authentication List Configuration)

Authentication List ページでデフォルトログインリストを設定します。 ログインリストは admin ユー ザーのためのスイッチあるいはポートへアクセスするための認証方式について記します。

メモ: Admin はシステムで唯一のユーザーで、defaultList という削除不可能なリ ストに割り当てられています。

								- 9	
System	Switch	ning	QoS S	ecurity	Monitoring	Maintenance	Help		.060
Managemen	Security	Acces	s Port Authenticat	ion Traffic	Control ACL				
User Config	guration	Aut	nentication Lis	st					
TACACS+		A	uthentication List	t				(?)	
Authentica	tion List		List Name	1		2	3		
				L	ocal 💌	None	No	ne ⊻	
			defaultList	Lo	ocal	None	Non	e	
						Ē.			

defaultList の認証方式を変更する

- 1. Security > Management Security > Authentication List を選択して Authentication List ページを 表示します。
- 2. defaultList のチェックボックスを選択します。
- 3. Use the drop down menu in the 1 の欄のドロップダウンメニューで認証ログインリストの最初に現 れる認証方式を選択します。'local'のようなタイムアウトしない方式を選択した場合、複数の方式 を指定しても他の方式は使われません。新しいログインリストを作成した場合はこのパラメータは 表示されません。選択した順番に認証方式は発生します。方式は以下の通り。
 - Local:ローカルに保存されたユーザーID とパスワードが認証に使われます。ローカル方式は タイムアウトしないため、これを選択した場合は以降の方式は選択されていたとしても使われ ません。
 - RADIUS:ユーザーID とパスワードは RADIUS サーバーを使って認証されます。RADIUS または TACACS+を最初の方式に選択し、認証時にエラーが発生した場合には、次の認証方式が使われます。
 - TACACS+:ユーザーID とパスワードは TACACS+サーバーを使って認証されます。RADIUS または TACACS+を最初の方式に選択し、認証時にエラーが発生した場合には、次の認証方式が使われます。
 - None:認証方式なし。この選択肢は第2または第3の方式として選択可能です。
- 4. 2,3の欄についても選択します。
- 5. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。
- 6. Apply ボタンをクリックして設定をスイッチに適用します。

管理アクセス設定(Configuring Management Access)

Access ページでスイッチの管理インターフェースへの HTTP と HTTPS アクセスの設定ができます。アクセスコンロロールプロファイルとアクセスルールの設定もできます。

Security > Access タブは以下のフォルダーを含みます。

- HTTP 設定(HTTP Configuration)
- HTTPS 設定(Secure HTTP Configuration)
- 証明書ダウンロード(Certificate Download)
- アクセスプロファイル設定(Access Profile Configuration)
- アクセスルール設定(Access Rule Configuration)

HTTP 設定(HTTP Configuration)

HTTP Configuration ページで HTTP サーバー設定をします。

NETGEA Connect with Innovation	R'			8 Port G	GS110TP igabit PoE Smart Switch with 2 Fiber SFP
System S	witching QoS Security	Monitoring	Maintenance	Help	LOGOUT
Management Secur	ity Access Port Authentication Tr	affic Control ACL			
*HTTP	HTTP Configuration				-
Configuration	HTTP Configuration		(?)		
HTTPS	Java Mode	O Disable 💿 Enable			
Access Control	HTTP Session Soft Timeout (Minutes)	5	(0 to 60)		
	HTTP Session Hard Timeout (Hours)	24	(0 to 168)		
	Maximum Number of HTTP Sessions	16	(0 to 16)		
					L
	<				>
					CANCEL APPLY
Convright @ 1006.00	110 Notacar @				

HTTP サーバー設定をする

- 1. Security tab, then click Access > HTTP > HTTP Configuration を選択して HTTP Configuration ペ ージを表示します。
- Java Mode: Web の Java モードの有効(enable)、無効(disable)を選択します。この設定は HTTP、 HTTPS 接続の両方に適用されます。表示されている選択が現在の状態です。デフォルト設定は 有効(enable)です。
- HTTP Session Soft Timeout: HTTP セッションタイムアウトを設定します。(0-60分) 設定した時間セッションがアイドルになっていると、自動的にログアウトされ、管理インターフェー スにアクセスするには再度パスワードを入力する必要があります。デフォルト値は5(分)です。表 示されている値が現在の値です。
- 4. HTTP Session Hard Timeout: HTTP セッションのハードタイムアウトを設定します。ハードタイムアウトはセッションのアクティビティ状況には依存しません。範囲は 0-168 時間です。デフォルトは 24 時間です。0 は無限を示します。表示されている値が現在の値です。
- 5. Maximum Number of HTTP Sessions:同時に可能な HTTP セッション数を指定します。値は 0 - 16 です。デフォルトは 16 です。表示されている値が現在の値です。
- 6. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。
- 7. Apply ボタンをクリックして設定をスイッチに適用します。

HTTPS 設定(Secure HTTP Configuration)

HTTPS は暗号化された SSL(Secure Socket Layer)や TLS(Transport Layer security)上で HTTP 接続を可能にします。HTTPS 接続で Web インターフェースを使うと、管理システムとスイッチの間の通信を守り、のぞき見や中間者攻撃を防御します。

HTTPS Configuration ページでスイッチと管理端末間の HTTPS 接続を設定します。

NETGE	A R'					GS108
nnect with Innovatio	on "				8 Port Gig	abit Smart Swite
System	Switching QoS Security	Moni	itoring	Maintenance	Help	LOGOUT
Management Se	curity Access Port Authentication T	raffic Control	ACL			
нттр	HTTPS Configuration					
HTTPS * HTTPS	HTTPS Configuration			(?)		
	HTTPS Admin Mode	Oisable	O Enable			
» Certificate	SSL Version 3	O Disable	Enable			
Download	TLS Version 1	O Disable	 Enable 			
Control	HTTPS Port	443				
	HTTPS Session Soft Timeout (Minutes)	5		(1 to 60)		
	HTTPS Session Hard Timeout (Hours)	24		(1 to 168)		
	Maximum Number of HTTPS Sessions	2		(0 to 2)		
	<					>
					c	
					C.	AITE

HTTPS 設定をする

- 1. Security > Access > HTTPS > HTTPS Configuration を選択して HTTPS Configuration ページ を表示します。
- HTTPS Admin Mode: HTTPS モードの有効(enable)、無効(disable)を設定します。表示されている設定が現在の設定です。デフォルトは無効(disable)です。ルート証明書がダウンロードされていない状態で HTTPS Admin Mode が enable の場合は、 SSL Version 3 ど TLS Version 1 の設定を変更することはできません。
- 3. SSL Version 3:SSL バージョン 3.0 の有効(enable)、無効(disable)を設定します。表示されている設定が現在の設定です。デフォルトは有効(enable)です。
- 4. TLS Version 1: TLS バージョン 1.0 の有効(enable)、無効(disable)を設定します。表示されている設定が現在の設定です。デフォルトは有効(enable)です。
- 5. HTTPS Port: HTTPS で使うポート番号を指定します。範囲は 1-65535 で、デフォルトは 443 で す。表示されている値が現在の値です。
- HTTPS Session Soft Timeout: HTTPS セッションタイムアウトを設定します。(1-60分) 設定した時間セッションがアイドルになっていると、自動的にログアウトされ、管理インターフェー スにアクセスするには再度パスワードを入力する必要があります。デフォルト値は 5(分)です。 表示されている値が現在の値です。
- 7. HTTPS Session Hard Timeout: HTTPS セッションのハードタイムアウトを設定します。ハードタイムアウトはセッションのアクティビティ状況には依存しません。範囲は 1-168 時間です。デフォルトは 24 時間です。表示されている値が現在の値です。
- 8. Maximum Number of HTTPS Sessions: 同時に可能な HTTPS セッション数を指定します。値は 0-2 です。デフォルトは 2 です。表示されている値が現在の値です。
- 9. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。
- **10. Apply** ボタンをクリックして設定をスイッチに適用します。

証明書ダウンロード(Certificate Download)

スイッチ上の Web サーバーとして管理端末から HTTPS 接続を受け入れるために、Web サーバー は公開鍵証明書が必要です。外部で証明書を作成してスイッチにダウンロードすることができま す。

SSL 証明書のダウンロード(Downloading SSL Certificates)

証明書をスイッチにダウンロードする前に、以下の条件が揃っている必要があります。

- TFTP サーバーに証明書ファイルが設定されている。
- 証明書ファイルが正しい形式である。
- スイッチと TFTP サーバーは接続可能である。

System S	witching QoS	Security Monitori	ng Maintenance	Help	LOGO
Management Secur	ity Access Port Aut	hentication Traffic Control A	ACL		
НТТР	Certificate Dow	nload			
HTTPS	Certificate Dow	nload	0		
 Configuration Certificate Download 	File Type TFTP Server IP Remote File Name	SSL Trusted Root Certificate 0.0.0.0	PEM File		
Access Control		Start File Transfer			
ſ	e]				

HTTP セッション用の証明書ダウンロード設定をする

- 1. Security > Access >HTTPS > Certificate Download を選択して Certificate Download ページを表示します。
- 2. File Type:以下の中からダウンロードする SSL 証明書のタイプを選択します。
 - **SSL Trusted Root Certificate PEM File**: SSL Trusted Root Certificate File (PEM Encoded).
 - SSL Server Certificate PEM File: SSL Server Certificate File (PEM Encoded).
 - SSL DH Weak Encryption Parameter PEM File: SSL Diffie-Hellman Weak Encryption Parameter File (PEM Encoded).
 - SSL DH Strong Encryption Parameter PEM File: SSL Diffie-Hellman Strong Encryption Parameter File (PEM Encoded).
- 3. TFTP Server IP: TFTP サーバーのアドレスを入力します。形式は x.x.x.x またはホスト名です。フ ァイルが TFTP サーバーからダウンロード可能であることを確認してください。
- Remote File Name:ファイル名を指定します。必要ならばパスも含めてください。最大 32 文字まで 入力可能です。
- 5. Start File Transfer:: チェックボックスをチェックします。
- 6. Apply ボタンをクリックしてダウンロードを開始します。ダウンロードの最中と完了時に状態メッ セージが表示されます。
- 7. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。

アクセスプロファイル設定(Access Profile Configuration)

Access Profile Configuration ページでスイッチへの管理アクセス制御設定をします。アクセスプロファイル設定は3段階で行います。

- 1. Access Profile Configuration ページでアクセスプロファイルを作成します。プロファイルにルール を追加するには、アクセスプロファイルが無効(デフォルト)である必要があります。
- 2. Access Rule Configuration ページでアクセスルールをプロファイルに追加します。
- 3. Access Profile Configuration ページに戻り、プロファイルを有効化します。

C.ustam C		0-5		Maathatian	Maintenance	Hale		100
System 3	witching	Qos Se	curity	Moniforing	Maintenance	Help	p	(100
Management Secu	ity Access	Port Authentication	n Traff	ic Control ACL				
нттр	Access Pr	ofile Configu	ration					
HTTPS Access	Access P	rofile Configura	ation				0	
Control Access Profile	Access Pro	file Name	Activat	e Profile	Deactivate Pro	file	Remove Profile	
Configuration Access Rule								
Configuration								
	Profile S	ummary					۲	
	Rule Type	Service Type		Source IP Address	Mask	Priority		

アクセスプロファイルを設定する

- 1. Security > Access > Access Control > Access Profile Configuration を選択して Access Profile Configuration ページを表示します。
- 2. Access Profile Name: 追加するアクセスプロファイル名を入力します。32 文字まで入力可能で す。
- 3. Activate Profile: アクセスプロファイルを有効化するにはこのチェックボックスを選択します。アクセスプロファイルが有効の場合はルールを追加することはできません。
- 4. Deactivate Profile: アクセスプロファイルを無効化するにはこのチェックボックスを選択します。
- 5. Remove Profile: アクセスプロファイルを削除するにはこのチェックボックスを選択します。アクセスプロファイルを削除するには、アクセスプロファイルを無効化してください。
- 6. Apply ボタンをクリックしてダウンロードを開始します。ダウンロードの最中と完了時に状態メッ セージが表示されます。
- 7. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。

Profile Summary の表はプロファイルに設定されたルールを示し、以下の情報を表示します。

項目	説明
Rule Type	ルールが決める操作を示します。Permit または Deny です。
Service Type	スイッチ管理インターフェースをアクセスするサービスタイプを示します。 ● SNMP ● HTTP ● HTTPS
Source IP Address	管理トラフィックを発生するデバイスの IP アドレスを指定します。
Mask	IP アドレスのサブネットマスク。
Priority	ルールの優先度を表示します。小さい値が優先されます。ルールが一致すると それ以降のルールは無視されます。

Refresh ボタンをクリックしてスイッチの最新情報を表示させます。

アクセスルール設定(Access Rule Configuration)

Access Rule Configuration ページでスイッチの管理インターフェースをアクセスするルールとプロト コルを設定します。

NETGEA Connect with Innovation	R.					8 Port Gigab	GS110TI bit PoE Smart Swite with 2 Fiber SF
System	Switching	QoS	Security	Monitoring	Maintenance	Help	LOGOUT
Management Secu	urity Access	Port Authen	tication Traffic	Control ACL			
• HTTP	Access R	le Config	guration				
> HTTPS * Access Control	Access F	tule Config	uration			(?)	
» Access Profile	Rule T	уре	Service Type	Source IP Addres	s Mask	Priority	
» Access Rule		M	M				
Configuration							
							
						ADD DELETE CAM	NCEL APPLY
Copyright © 1996-2	010 Netgear ®						

アクセスルールを作成する前に、以下を確認してください。

- アクセスプロファイルが存在する。
- アクセスプロファイルは無効になってい

る。

アクセスプロファイルルールを設定する

- 1. Security > Access > Access Control > Access Rule Configuration を選択して Access Rule Configuration ページを表示します。
- 2. アクセスプロファイルルールを追加するには、以下の設定を行い、Add ボタンをクリックしま す。
 - Rule Type: ルールがスイッチの管理インターフェースにアクセスすることを許可(permit)あるいは拒否(deny)するかを設定します。
 - **Permit**: ルールに一致したトラフィックが管理インターフェースにアクセスすることを許可します。一致しないものは拒否されます。
 - Deny: ルールに一致したトラフィックが管理インターフェースにアクセスすることを拒否します。一致しないものは許可されます。MAC ACL や IP ACL とは異なり、ルールの最後に deny all は含まれていません。
 - Service Type:管理インターフェースのアクセスを許可または拒否するサービスタイプ。
 - SNMP
 - HTTP
 - HTTPS
 - Source IP Address:管理インターフェースにアクセスする端末の IP アドレスを設定します。
 - Mask: IP アドレス用のサブネットマスクを設定します。

- Priority: ルールの優先度を表示します。小さい値が優先されます。 ルールが一致するとそれ 以降のルールは無視されます。
- 3. アクセスルールを変更するには、変更するアクセスルールのチェックボックスを選択し、設定を 変更した後に Apply ボタンをクリックします。
- 4. アクセスルールを削除するには、削除するアクセスルールのチェックボックスを選択し、Delete ボタンをクリックします。
- 5. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。

ポート認証(Port Authentication)

ポートベース認証モードでは、802.1X がグローバルで有効になっており、ポートに接続されたサプ リカントでポート認証が成功すれば制限なしにポートを利用することができます。いつでも、このモ ードでの一つのポートでは一つのサプリカントのみが認証をすることができます。このモードでは ポートは双方向について制御されます。これがデフォルトの認証モードです。

802.1X ネットワークは3つの構成要素からなります。

- Authenticators:オーセンティケータ。アクセスを許可する前に認証されるポート。
- Supplicants:サプリカント。システムへのアクセスを要求する認証されたポートへ接続されたホスト。
- Authentication Server:オーセンティケータの代わりに認証を行い、ユーザーがシステムのサービスに認証されるかどうかを判断する RADIUS サーバーのような外部サーバー。

Port Authentication リンクから以下のページにアクセスできます。

- Basic:
 - 802.1X 設定(802.1X Configuration)
- Advanced:
 - ポート認証(Port Authentication)
 - ポートサマリー(Port Summary)

802.1X 設定(802.1X Configuration)

802.1X Configuration ページを使ってシステムのポートアクセス制御を有効、無効にします。

Connect with Innovation	A R'			8 P	ort Gigabit Pol w	E Smart Switch ith 2 Fiber SFP
System	Switching QoS	Security	Monitoring	Maintenance	Help	LOGOUT
Management See	curity Access Port A	thentication Traffi	c Control ACL			
~Basic	802.1X Configur	ation				_
> 802.1X Configuration	802.1X Configur	ation		3		
> Advanced	Port Based Authentica Guest Vlan Vlan Assignment Mode	tion State	e O Enable e O Enable e O Enable			
	<u> </u>				CANCEL	APPLY

グローバル 802.1X 設定をする

- 1. Security > Port Authentication > Basic > 802.1X Configuration を選択して 802.1X Configuration ページを表示します。
- 2. Port Based Authentication State 欄のラジオボタンを選択してスイッチの 802.1X 管理モードを 有効・無効にします。
 - Enable:ポートベース認証が有効。

メモ:802.1X が有効になると、認証は RADIUS サーバーで実施されます。これは第 一の認証方法は RADIUS である必要があることを意味します。

Security > Management Security > Authentication List を選択し、 defaultList で RADIUS を第一の方式に設定します。

- Disable:スイッチはポートにトラフィックを受け入れる前に 802.1X 認証を行いません。
- 3. Guest VLAN 欄のラジオボタンを選択してスイッチのゲスト VLAN サプリカントモードを有効・ 無効にします。
 - Enabled:ポートで 802.1X サプリカントが認証されていない時に、認証サーバーで設定された ゲスト VLAN へ.限定的なネットワークアクセスを提供します。
 - Disabled:認証されていないポートでゲスト VLAN を使うことができません。
- 4. VLAN Assignment Mode 欄のラジオボタンを選択してスイッチの VLAN の割当モードを有効・ 無効にします。デフォルト設定は無効(disable)です。
- 5. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。
- 6. Apply ボタンをクリックして設定をスイッチに適用します。

ポート認証(Port Authentication)

Port Authentication ページでポートアクセス制御を設定します。

メモ:水平スクロールバーを使って画面を表示してください。以下の画面は左右に分割した画面となっています。

System Switch	ing	QoS	Security	Monitorin	g M	aintenance H	elp	
Basic Advanced > 802.1X Configuration	Por	t Authe	entication					
 Port Authentication Port Summary 		Port	Port Control	Guest VLAN ID	Guest VLAN Period	Periodic Reauthentication	Reauthentication Period	Quiet Period
			×	1		×		
		g1	Auto	0	90	Disable	3600	60
		g2	Auto	0	90	Disable	3600	60
		g3	Auto	0	90	Disable	3600	60
		g4	Auto	0	90	Disable	3600	60
		g5	Auto	0	90	Disable	3600	60
		g6	Auto	0	90	Disable	3600	60
		g7	Auto	0	90	Disable	3600	60
		g8	Auto	0	90	Disable	3600	60
		g9	Auto	0	90	Disable	3600	60
		g10	Auto	0	90	Disable	3600	60

							8	Port Gigabit	GS110 PoE Smart Sv with 2 Fiber	TF witc SF
Maintena	nce H	lelp							LOGO	UT
										ļ
									1	
									(
							GOTOTN	TERFACE	GO	
Resending EAP	Max EAP Requests	Supplicant Timeout	Server Timeout	Control Direction	Protocol Version	PAE Capabilities	Authenticator PAE State	Backend State	EAPOL Flood Mode	
									~	
30	2	30	30	Both	1	Authenticator	Initialize	Initialize	Disable	
30	2	30	30	Both	1	Authenticator	Initialize	Initialize	Disable	
30	2	30	30	Both	1	Authenticator	Initialize	Initialize	Disable	
30	2	30	30	Both	1	Authenticator	Initialize	Initialize	Disable	
30	2	30	30	Both	1	Authenticator	Initialize	Initialize	Disable	
30	2	30	30	Both	1	Authenticator	Initialize	Initialize	Disable	
30	2	30	30	Both	1	Authenticator	Initialize	Initialize	Disable	
30	2	30	30	Both	1	Authenticator	Initialize	Initialize	Disable	
30	2	30	30	Both	1	Authenticator	Initialize	Initialize	Disable	
30	2	30	30	Both	1	Authenticator	Initialize	Initialize	Disable	
							GO TO IN	TERFACE	GO	
										hand
					Ш				[>
						INITIAL	ZE REAUTHENTIC	ATE CANC	EL APPLY	0

ポートの 802.1X 設定をする

- 1. Security > Port Authentication > Advanced > Port Authentication を選択して Port Authentication ページを表示します。
- 設定をするポートのチェックボックスを選択します。複数ポートを選択して共通設定することも可能で、一番上のチェックボックスを選択してすべてのポートに対して共通設定をすることも可能です。
- 3. 選択したポートに以下の設定をします。

- Port Control:ポートの認証状態を設定します。リンク状態がアップ(Up)の時のみモードの設定が可能です。
 - Auto:自動的にインターフェースの認証モードを検知します。
 - Authorized: インターフェースを認証なしに承認します。
 - Unauthorized:インターフェースを非承認状態にしてシステムアクセスを拒否します。
 スイッチはインターフェースを介して認証サービスを提供することができません。
- Guest VLAN ID: インターフェースにゲスト VLAN ID を設定します。有効な値は 0-4093 です。 デフォルト値は 0 です。0 を設定するとゲスト VLAN ID はリセットできます。
- Guest VLAN Period: インターフェースでゲスト VLAN の有効時間を設定します。範囲は 1-300(秒)でデフォルト値は 90(秒)です。
- Periodic Reauthentication: 再認証を有効あるいは無効にします。有効(enable)を選択して一定時間ごとの再認証を行います。 Apply ボタンをクリックして設定を有効にします。
- Reauthentication Period: 再認証の周期。範囲は 1-65535(秒) デフォルト値は 3600(秒)。
 Apply ボタンをクリックして設定を有効にします。
- Quiet Period:認証に失敗した際のアイドル時間を設定します。値の範囲は 0-65535(秒)で す。デフォルトは 60(秒)です。Apply ボタンをクリックして設定を有効にします。
- Resending EAP: ポートでの EAPOL EAP フレームの送信周期(秒)。範囲は 1-65535(秒)。デ フォルトは 30(秒)。 Apply ボタンをクリックして設定を有効にします。
- Max EAP Requests:ポートでの EAPOL EAP フレームの再送信回数。値の範囲は 1-10 (回)。デフォルト値は 2。 Apply ボタンをクリックして設定を有効にします。
- Supplicant Timeout: EAP 要求をユーザーに再送する時間。範囲は 1-65535(秒)。デフォルトは 30(秒)。 Apply ボタンをクリックして設定を有効にします。
- Server Timeout:スイッチが認証サーバーに送信する要求を再送する時間。範囲は 1-65535 (秒)。デフォルトは 30(秒)。Apply ボタンをクリックして設定を有効にします。
- Control Direction:ポートの制御方向。双方向のみで変更不可。
- Protocol Version:ポートのプロトコルバージョン。バージョン1のみで変更不可。
- PAE Capabilities: PAE(port access entity)機能。Authenticator または Supplicant。設定不可。
- Authenticator PAE State:オーセンティケータの PAE 状態。
 - Initialize
 - Disconnected
 - Connecting
 - Authenticating
 - Authenticated
 - Aborting
 - Held
 - ForceAuthorized
 - ForceUnauthorized
- Backend State:バックエンドの認証状態。
 - Request
 - Response

- Success
- Fail
- Timeout
- Initialize
- Idle
- EAPOL Flood Mode: スイッチで 802.1X が無効の時に、EAOPL パケットをフラッド(透過)する かどうかを設定します。デフォルトは無効(Disable)です。
- 4. Apply ボタンをクリックして設定をスイッチに適用します。
- 5. Initialize ボタンをクリックしてポートの認証を初期化します。このボタンは Port Control モードが Auto の時のみクリック可能です。ボタンをクリックするとすぐに初期化を開始します。
- 6. Reauthenticate ボタンをクリックしてポートの再認証を行います。このボタンは Port Control モードが Auto の時のみクリック可能です。ボタンをクリックするとすぐに再承認を開始します。
- 7. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。

ポートサマリー(Port Summary)

Port Summary ページでポートアクセス制御の情報を確認することができます。

Security > Port Authentication > Advanced > Port Summary を選択して Port Summary ページを表示 します。

							-
stem S	witching	QoS	Security	Monitoring	Maintenance	Help	Ŀ
nagement Secur	ity Acce	ss Port Au	hentication T	raffic Control ACL			
ic	Port S	ummary					
anced	Port	Summary			(1)		
onfiguration							
ert ithentication irt Summary	Port	Control Mode	Operating Control Mode	Reauthentication Enabled	Port Status		
	g1	auto	auto	false	Authorized		
	g2	auto	auto	false	Authorized		
	g3	auto	auto	false	Authorized		
	g4	auto	auto	false	Authorized		
	g5	auto	auto	false	Authorized		
	g6	auto	auto	false	Authorized		
	g7	auto	auto	false	Authorized		
	g8	auto	auto	false	Authorized		
	<						

以下に Port Summary ページに表示される情報の説明を示します。

項目	
Port	- ポート番号

Control Mode	 ポートの認証制御状態を表示します。 Auto: 自動的にインターフェースの認証モードを検知します。 Force Authorized: インターフェースを認証なしに承認します。 Force Unauthorized: インターフェースを非承認状態にしてシステムアクセスを拒否します。スイッチはインターフェースを介して認証サービスを提供することができません。
Operating Control Mode	ポートの実際の動作状態。 • ForceUnauthorized • ForceAuthorized • Auto • N/A: ポートに何も接続されていない状態でポートアクセス制御が行われて いない。
Reauthentication Enabled	再認証が可能か否か。
Port Status	ポートの認証状態。

Refresh ボタンをクリックしてスイッチの最新情報を表示させます。

トラフィック制御(Traffic Control)

Traffic Control リンクで、MAC フィルタ(MAC Filters)、ストームコントロール(Storm Control)、ポートセ キュリティ(Port Security)およびプロテクトポート(Protected Port)設定ができます。 **Security > Traffic Control** を選択して表示します。

Traffic Control フォルダは以下の機能へのリンクを含んでいます。

- MAC Filter:
 - MAC フィルター設定(MAC Filter Configuration)
 - MAC フィルターサマリー(MAC Filter Summary)
 - ポートセキュリティ設定(Port Security Configuration)
 - ポートセキュリティインターフェース設定(Port Security Interface Configuration)
 - セキュリティ MAC アドレス (Security MAC Address)
- ストームコントロール(Storm Control)
- Port Security
 - ポートセキュリティ設定(Port Security Configuration)
 - ポートセキュリティインターフェース設定(Port Security Interface Configuration)
 - セキュリティ MAC アドレス (Security MAC Address)
- プロテクトポート(Protected Ports Membership)

MAC フィルター設定(MAC Filter Configuration)

MAC Filter Configuration ページで MAC フィルターを設定することができます。

NETGEA	R'				8 Port 0	GS110TF Gigabit PoE Smart Swite with 2 Fiber SF
System Sv	vitching QoS	Security	Monitoring	Maintenance	Help	LOGOUT
Management Securit	y Access Port Au	hentication Traffi	c Control ACL			
MAC Filter MAC Filter Configuration MAC Filter Summary Storm Control Port Security Protected Ports	MAC Filter Con # MAC Filter Con MAC Filter MAC Address Source Port Member Destination Port Me	figuration figuration Create Filter s	VLAN	IID		
	<]				DELETE	CANCEL APPLY

MAC フィルター設定をする

- 1. Security > Traffic Control > MAC Filter > MAC Filter Configuration を選択して MAC Filter Configuration ページを表示します。
- 2. MAC フィルターを設定するには、:
 - a. MAC Filter: Create Filter を選択します。
 - **b.** VLAN ID: MAC フィルターを行う VLAN ID を選択します。 VLAN ID はフィルターを作成する ときのみ変更・設定可能です。
 - MAC Address:フィルターする MAC アドレスを(00:01:1A:B2:53:4D)形式で指定します。フィルターを作成するときのみ変更・設定可能です。
 以下の MAC アドレスを設定することはできません。
 - 00:00:00:00:00
 - 01:80:C2:00:00:00 ~ 01:80:C2:00:00:0F
 - 01:80:C2:00:00:20 ~ 01:80:C2:00:00:21
 - FF:FF:FF:FF:FF
 - c. オレンジ色のバーをクリックして、ポートとLAGを表示し、入力方向(Inbound)のフィルターを適用するポートとLAGを指定します。設定されていない MAC アドレスと VLAN ID のパケットが受信された場合には廃棄されます。
 - d. オレンジ色のバーをクリックして、ポートとLAGを表示し、出力方向(Outbound)のフィルターを 適用するポートとLAGを指定します。リストに含まれている MAC アドレスと VLAN ID のパケ ット飲みが送信されます。宛先 MAC アドレスはマルチキャストフィルターのみに含まれます。
- 3. MAC フィルターを削除するには、削除する MAC フィルターのチェックボックスを選択し、Delete ボタンをクリックします。
- 4. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。
- 5. Apply ボタンをクリックして設定をスイッチに適用します。
MAC フィルターサマリー(MAC Filter Summary)

MAC Filter Summary ページで MAC フィルターの状態を確認することができます。

Security > Traffic Control > MAC Filter > MAC Filter Summary を選択して MAC Filter Summary ページを表示します。

NETGEA Connect with Innovation	R'				81	G: Port Gigabit Sm	S108T
System S	witching Qo	S Security	Monitoring	Maintenance	Help	on again on	
 Management Security MAC Filter MAC Filter 	MAC Filter Su	Immary	ffic Control ACL				•
Configuration MAC Filter Summary Storm Control	MAC Filter S	ummary VLAN ID Sou	urce Port Members	Destination	Port Members		
 Port Security Protected Ports 							
	<						•

以下に MAC Filter Summary ページに表示される情報の説明を示します。

項目	説明
MAC Address	フィルターした MAC アドレス。
VLAN ID	フィルターする MAC アドレス。
Source Port Members	入力方向のフィルターに含まれるポート。
Destination Port Members	出力方向のフィルターに含まれるポート。

Refresh ボタンをクリックしてスイッチの最新情報を表示させます。

ストームコントロール(Storm Control)

ブロードキャストストームは過度なブロードキャストメッセージが同時にネットワークに送信されることから発生します。転送されたメッセージへの応答がネットワークを飽和状態にし、ネットワークタイムアウトを引き起こしたりします。

スイッチは、ポートに入力されるブロードキャスト/マルチキャスト/未知のユニキャストパケットの速度をポート単位に観測し、設定した速度を上回る場合にパケットを廃棄します。ストームコントロールはインターフェース単位に、パケットタイプや速度を設定できます。

NETGEA Connect with Innovation*	R.			8 Port Gig	GS110TP abit PoE Smart Switch with 2 Fiber SFP
System Sw	ritching QoS	Security	Monitoring Maintenance	Help	LOGOUT
Management Security	y Access Port Au	thentication Traffic	Control ACL		
> MAC Filter	Storm Control				<u>~</u>
Port Security	· Storm Control		0		
> Protected Ports	Ingress Control Mode	Status	Threshold		
	Disable	∽			
	Port Settings		0		
		GO	TO INTERFACE GO		
	Port	Status	Threshold		
		× 11			
		Disable			=
		Disable			
	94	Disable			
	g 5	Disable			
	 96	Disable			
	g 7	Disable			
	g 8	Disable			
	99	Disable			
	g10	Disable			
		GO 1			
G	e]				×
	• I				
				C	ANCEL APPLY
Copyright © 1996-201	0 Netgear ®				

ストームコントロールを設定する

- 1. Security > Traffic Control > Storm Control を選択して Storm Control ページを表示します。
- 設定をするポートのチェックボックスを選択します。複数のポートを選択して共通の設定をすることもできます。一番上のチェックボックスですべてのポートを選択することもできます。
- 3. Ingress Control Mode メニューからストームコントロールで制御するブロードキャストのモード を選択します。
 - Disable:ストームコントロールを使用しない。
 - Unknown Unicast: インターフェースに入力される不明の L2 ユニキャスト(宛先不明)トラフィックの速度が設定されたスレッショルド値を超えるとトラフィックが廃棄されます。
 - Multicast: インターフェースに入力される L2 マルチキャストトラフィックの速度が設定されたスレッショルド値を超えるとトラフィックが廃棄されます。
 - Broadcast: インターフェースに入力される L2 ブロードキャストトラフィックの速度が設定された スレッショルド値を超えるとトラフィックが廃棄されます。
- 4. Threshold:パケットが転送される最大速度を設定します。範囲はインターフェース速度の 0-100% です。デフォルト値は 5%です。
- 5. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。
- 6. Apply ボタンをクリックして設定をスイッチに適用します。

ポートセキュリティ設定(Port Security Configuration)

ポートセキュリティ(Port Security)機能を使ってスイッチのポートをロックします。ポートがロックされると、許可された送信元 MAC アドレスを持つパケットのみが転送されます。他のパケットは廃棄 されます。

NETGEA	R'						GS108
onnect with Innovation						8 Port G	igabit Smart Switc
System S	Switching	QoS	Security	Monitoring	Maintenance	Help	LOGOUT
Management Secu	rity Access	Port Auth	ontication Traff	ic Control ACL			
MAC Filter	Port Sec	curity Co	nfiguration				
Storm Control	Port Se	ecurity Co	nfiguration		۲		
	Port Secur	ity Mode	💿 Disabl	e OEnable			
 Interface Configuration 	Port S	ecurity Vie	lations		1		
» Security MAC Address	Port	La	st Violation MA	c	VLAN ID		
Protected Ports							
	<						
						(APPROVAL)	

グローバルポートセキュリティモードを設定する

- 1. Security > Traffic Control > Port Security > Port Security Configuration を選択して Port Security Configuration ページを表示します。
- 2. Port Security Mode:ポートセキュリティの有効(Enable)・無効(Disable)を選択します。
- 3. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。
- 4. Apply ボタンをクリックして設定をスイッチに適用します。

Port Security Violation の表はポートセキュリティが有効なポートで発生した違反の情報を表示します。

以下に Port Security Violation 欄に表示される情報の説明を示します。

Field	Description
Port	違反が発生したポート。
Last Violation MAC	最後に廃棄されたパケットの送信元 MAC アドレス。
VLAN ID	違反が発生した最後のパケットの VLAN ID。

Refresh ボタンをクリックしてスイッチの最新情報を表示させます。

ポートセキュリティインターフェース設定(Port Security Interface Configuration)

MAC アドレスが受け入れ可能かどうかはダイナミックかスタティックのどちらか一方で決定することができます。ポートがロックされるときに両方の方法が使われます。

ポートセキュリティのダイナミックロッキングは最初に到達したものを優先する方式を使用していま

す。ポートで学習できる MAC アドレス数を設定します。設定したアドレス数に達するまで、MAC ア ドレスを学習して転送されます。最大数に達するとそれ以上の MAC アドレスは学習されません。 学習されていない送信元 MAC アドレスを持つフレームは廃棄されます。最大数を0に設定するこ とによって、ダイナミックロック機能を無効化することができます。

スタティックロックではポートで許容できる MAC アドレスを設定することができます。設定された送 信元 MAC アドレスを持つフレームに対する処理はダイナミックロックの場合と同じく転送されま す。

System Sw	itchi	ng	QoS S	ecurity N	Aonitoring	Maintenance	Help	LOG
anagement Securit	11	ccess	Port Authenticat	ion Traffic Cor	ntrol ACL			
AC Filter	Int	erfac	e Configurat	ion				
torm Control		Interfa	ce Configuratio	on		0		
Port Security	POF	TS I	AGS All	GO TO I	TERFACE	GO		
Configuration				Max	Max			
Interface Configuration Security MAC		Port	Port Security	Allowed Dynamically Learned	Allowed Statically Locked	Enable Violation Traps		
rotected Ports				MAC	MAC			
			×			× 1		
		g1	Disable	600	20	No		
		g2	Disable	600	20	No		
		g3	Disable	600	20	No		
		g4	Disable	600	20	No		
		go	Disable	600	20	No		
		g6	Disable	600	20	No		
		97	Disable	600	20	No		
		g0 09	Disable	600	20	No		
		a10	Disable	600	20	No		
	POF	UTS I	LAGS All	GO TO I	TERFACE	GO		

ポートセキュリティ設定をする

- 1. Security > Traffic Control > Port Security > Interface Configuration を選択して Interface Configuration ページを表示します。
- 2. PORTS をクリックして、物理ポートのポートセキュリティ設定をします。
- 3. LAGS をクリックして、LAG (Link Aggregation Group)のポートセキュリティ設定をします。
- 4. ALL をクリックして、物理ポートとLAG (Link Aggregation Group)の両方のポートセキュリティ設定をします。
- 5. 設定をしたいポートまたは LAG の横のチェックボックスをクリックして選択をします。複数の選択 をして共通の設定をすることも可能です。一番上のチェックボックスをクリックするとすべてのイン ターフェースの設定ができます。
- 6. 以下の項目の設定をします。
 - Port Security: 選択したインターフェースでのポートセキュリティの有効(Enable),無効(Disable)
 を設定します。
 - Max Allowed Dynamically Learned MAC:選択したインターフェースでのダイナミックに学習で きる MAC アドレス数を指定します。有効な値は 0-600 です。
 - Max Allowed Statically Locked MAC: 選択したインターフェースでのスタティック MAC アドレス 数を指定します。有効な値は 0-20 です。

- Enable Violation Traps:許可されない MAC アドレスがインターフェースで受信した時にトラップを送信するかを設定します。
- 7. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。
- 8. Apply ボタンをクリックして設定をスイッチに適用します。

セキュリティ MAC アドレス (Security MAC Address)

Security MAC Address ページでダイナミックに学習した MAC アドレスをスタティック MAC アドレス に変換することができます。

NETGEA	R'					GS1087
onnect with Innovation"					8 Port G	igabit Smart Switc
System Sv	witching QoS	Security	Monitoring	Maintenance	Help	LOGOUT
Management Securi	ty Access Port A	uthentication Tra	ffic Control ACL		ñ A	
MAC Filter	Security MAC	Address				
 Storm Control Port Security 	Port Security	Settings		1		
 » Port Security Configuration » Interface 	Convert Dynamic A Number of Dynami	ddress to Static	earned:			
Configuration	· Dynamic MAC	Address Table		0		
	Port List	g1		~		
Protected Ports	VLAN ID	MAC A	ddress			
	<u>x</u>]				REFRESH	CANCEL APPLY

学習した MAC アドレスを変換する

- 1. Security > Traffic Control > Port Security > Security MAC Address を選択して Security MAC Address ページを表示します。
- 2. Convert Dynamic Address to Static チェックボックスを選択します。
- 3. Apply ボックスをクリックすると、ダイナミックに学習された MAC アドレスが昇順にスタティック MAC アドレスに変換されて最大数に達するまで登録されます。

Dynamic MAC Address Table 欄は選択したポートで学習された MAC アドレスを VLAN 毎に表示 します。Port List 欄で情報を表示したいインターフェースを選択します。

項目	説明
VLAN ID	VLAN ID。
MAC Address	インターフェースで学習された MAC アドレス。

Refresh ボタンをクリックしてスイッチの最新情報を表示させます。

プロテクトポート(Protected Ports Membership)

ポートをプロテクトポートとして設定すると、スイッチは他のプロテクトポートへトラフィックは転送しませんが、プロテクトポート以外のポートへは転送します。Protected Ports Membership ページで プロテクトポート設定をします。

								8 Por	t Gigabit PoE wit	Smart Switc h 2 Fiber SF
vitching	QoS	Securit	y M	onitoring	٨	Aainte	nance	Help		LOGOUT
y Access	Port Au	thentication	Traffic Con	rol ACL						
Protect	ted Port	ts								(
Prote	cted Por	ts Membersh	ip						(?)	
Port	1 2	34	5	57	8	9	10			
		d	in in the second se							
<										>
								REFRESH	CANCEL	APPLY
	ritching Protect Protect Prote Port	ritching QoS Access Port Au Protected Port Protected Port Port 1 2 Access Port Au Port 1 2 Access Port Au Port 1 2	ritching QoS Securi Access Port Authentication Protected Ports Protected Ports Membersh Port 1 2 3 4 (ritching QoS Security Ma Access Port Authentication Traffic Cont Protected Ports Protected Ports Membership Port 1 2 3 4 5 4 (QoS Security Monitoring / Access Port Authentication Traffic Control ACL Protected Ports	Protected Ports Port 1 2 3 4 5 6 7 8	Image: Solution of the second seco	Image: Solution of the second seco	Image: Solution of the second dependence of the second	Protected Ports Port 1 2 3 4 5 6 7 8 9 10

プロテクトポート設定をする

- 1. Security > Traffic Control > Protected Ports を選択して Protected Ports ページを表示します。
- 2. オレンジのバーをクリックしてポートを表示します。
- プロテクトポート設定をするポートを選択します。プロテクトポート間ではトラフィックは転送されません。
- 4. Refresh ボタンをクリックしてスイッチの最新情報を表示させます。
- 5. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。
- 6. Apply ボタンをクリックして設定をスイッチに適用します。すぐに設定変更がされます。

ACL を設定する(Configuring Access Control Lists)

ACL(Access Control Lists)は、期待しないアクセスを防ぎながら、許可されたユーザーだけが特定 のリソースにアクセスすることを確実にします。ACL はトラフィックフローコントロールを提供、ルー ティングアップデートのコンテンツの制限、トラフィックタイプ毎に転送するかの決定、そして何より も IPv4 と IPv6 ACL をサポートするネットワークスイッチソフトウェアにセキュリティを提供します。

最初に IPv4 ベースまたは MAC ベースの ACL ID を作成します。次に、ルールを作成しそれを ACL ID に割り当てます。最後に、ACL ID を使って ACL をポートまたは LAG に割り当てます。

Security > ACL フォルダーは以下の機能へのリンクを含みます。

- ACL ウィザード (ACL Wizard)
 - Basic:
 - MAC ACL
 - MAC JL—JL (MAC Rules)
 - MAC バインディング設定(MAC Binding Configuration)
 - MAC バインディングテーブル (MAC Binding Table)
- Advanced:
 - IP ACL
 - ・ IP ルール(IP Rules)
 - IP 拡張ルール(IP Extended Rule)

- IP バインディング設定(IP Binding Configuration)
- IP バインディングテーブル(IP Binding Table)

ACL ウィザード(ACL Wizard)

ACL ウィザード(ACL Wizard)は ACL ルール設定を簡単にします。ウィザードは permit((許可)ある いは deny(拒否)できるいくつかのリストを含んでいます。Permit あるいは deny を選択すると、自 動的に設定がされたページに移動します。

メモ:ACL ウィザードを使ってルールを設定する前に、ルールを含めることができ る MAC ACL あるいは標準 IP ACL、あるいは拡張 IP ACL を作成する必要があり ます。

		8 Port Gigabit Smart Switch
System	Switching QoS Security Monitoring Main	tenance Help
Management Sec	urity Access Port Authentication Traffic Control ACL	
ACL Wizard	ACL Wizard	[
Basic Advanced	# ACL Wizard	۲
	Select Devices Based on Source MAC Address	Permit Denv
	Select Devices Based on Destination MAC Address	Permit Deny
	Select Devices Based on Source IP Address	Permit Deny
	Select Devices Based on Destination IP Address	Permit Deny
	Select Devices Based on TCP/UDP Source Port ID	Permit Deny
	Select Devices Based on TCP/UDP Destination Port ID	Permit Deny
	<]	>

ACL ウィザードを使う

- 1. Security > ACL を選択して ACL ページを表示します。
- 2. 設定する ACL のタイプを選択し、MAC ACL または Standard IP ACL、Extended IP ACL を作成します。

- 送信元 MAC アドレスを元にトラフィックを許可・拒否するには、MAC ACL を作成します。
- 宛先 MAC アドレスを元にトラフィックを許可・拒否するには、MAC ACL を作成します。
- 送信元 IP アドレスを元にトラフィックを許可・拒否するには、Standard ACL を作成します。
- 宛先 IP アドレスを元にトラフィックを許可・拒否するには、Extended ACL を作成します。
- 送信元 TCP/UDP ポートを元にトラフィックを許可・拒否するには、Extended ACL を作成します。
- 宛先 TCP/UDP ポートを元にトラフィックを許可・拒否するには、Extended ACL を作成します。
- 送信元 TCP/UDP ポートを元にトラフィックを許可・拒否するには、Extended ACL を作成します。
- 3. ACL Wizard ページで設定する ACL の Permit または Deny リンクをクリックします。

スイッチはいくつかの項目が事前に設定された ACL ルールを設定するためのページを表示します。例えば、Select Devices Based on Source IP Address の Permit リンクを選択すると、送信元 IP アドレスルールページが表示され、設定すべき項目は送信元 IP アドレスとアドレスマスクだけです。

4. ルールを設定します。

5. Apply ボタンをクリックしてルールを保存します。

MAC ACL

MAC ACL はパケットに対して連続的に一致したルールのセットから成り立ちます。パケットがルールの条件に一致した場合、ルールの動作(Permit/Deny)が実行され、それ以上のルールへの一致確認はされません。

MAC ACLを定義してスイッチに適用するには複数の手順があります。

- 1. MAC ACL ページで ACL ID を作成します。
- 2. MAC Rules ページで ACL のルールを作成します。
- 3. MAC Binding Configuration ページで ACL ID を使ってポートに ACL を割り当てます。
- 4. (任意) MAC Binding Table ページで設定を確認します。

NETGEA Connect with Innovation	R.					8 Port Gigabil	GS110TP PoE Smart Switch with 2 Fiber SFP
System S	witching QoS	Security	Monitoring	g Mainten	ance H	elp	LOGOUT
Management Secu	rity Access Port Authenti	cation Traff	c Control AC	CL .			
 ACL Wizard Basic MAC ACL MAC Rules MAC Binding Configuration Binding Table Advanced 	MAC ACL MAC ACL Current Number of ACL Maximum ACL MAC ACL Table Name	0	Rules	() Direction	2		=
	<]						~
					ADD	DELETE CANC	EL APPLY
Copyright © 1996-2	010 Netgear ®						

MAC ACL テーブルは現在スイッチで設定されている ACL の数と設定可能な ACL の最大数を表

示します。現在の数は IPv4 ACL と MAC ACL を足したものです。

MAC ACL を設定する

- 1. Security > ACL. > Basic > MAC ACL を選択して MAC ACL ページを表示します。
- MAC ACL を追加するには、Name 欄に MAC ACL の名前を記入し Add ボタンをクリックします。 Name 欄に使える文字は、英数字と"-", "_"," "(スペース)のみです。Name はアルファベットで始 まる必要があります。

各 ACL は以下の情報を表示します。

- Rules:現在設定されている MAC ACL の数を表示します。
- Direction: MAC ACL が適用されているパケットトラフィックの方向を示します。Inbound(受信方 向)あるいは空白です。
- 3. MAC ACL を削除するには、削除する MAC ACL のチェックボックスを選択し、Delete ボタンをクリックします。
- 4. MAC ACL の名前を変更するには、変更する MAC ACL のチェックボックスを選択し、名前を変更し、Apply ボタンをクリックします。
- 5. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。

MAC J L - J L (MAC Rules)

MAC Rules ページで MAC ベース ACL のルールを設定します。アクセスリスト設定は一致するトラ イフィックが通常通りに転送されるか廃棄されるかを示すルールを含みます。デフォルトですべて のルールの最後に'deny all'があります。

progement Security Access	Port Auther	rication	Troffic Contr	JI ACL	Home	endince	nap							
CL Wizard	MAC	Rules												
MAC ACL	Rul	les												- 4
MAC Binding	ACL Na	ana .			V									
Configuration Binding Table	Rul	e Table	0											0
dvanced	1	D (1 to 0)	Action	Assign Queue	Redirect Interface	Hatch Every	CoS	Destination MAC	Destination MAC Mask	EtherType Key	EtherType User Value (0600 to FFFF hex)	Source MAC	Source MAC Hask	VLAN
										×				

MAC ACL ルールを設定する

- 1. Security > ACL > Basic > MAC Rules を選択して MAC Rules ページを表示します。
- 2. ACL Name 欄から、ルールを適用する MAC ACL を選択します。新しい MAC ACL は MAC ACL ページで作成します。
- 3. 新しいルールを追加するには、ルールに ID をつけ、以下の項目の設定をして Add ボタンをクリック します。
 - Action: ルールに一致した場合に実行される操作を指定します。
 - Permit: ACL に一致したパケットを転送します。
 - Deny: ACL に一致したパケットを廃棄します。

- Assign Queue: ACL ルールに一致したパケットを処理するハードウェア出力キューID を指定します。0-3 を設定します。
- Match Every:パケットがこの ACL の条件に一致する必要があります。ドロップダウンメニューから Ture または False を選択します。Match-Every で True を選択すると他のルールは設定できなくなります。
- CoS:パケットの CoS(Class Of Service)がここでの CoS 値と一致する必要があります。CoS の値(0-7)を入力します。
- Destination MAC: イーサネットフレームの宛先 MAC アドレスがここのアドレスと一致する必要があります。表記形式は xx:xx:xx:xx: です。
- Destination MAC Mask: 宛先 MAC アドレスのマスクを入力します。MAC アドレスマスクはイー サネットフレームの宛先 MAC アドレスのどのビットを比較するかを指定します。Fと0を MAC マスクで使い、ワイルドカード形式で使います。Fの部分は比較されず、0の部分は一致する 必要があります。例えば、MAC アドレスが aa:bb:cc:dd:ee:ff でマスクが 00:00:0ff:ff:ff:ff:ff である場 合、aa:bb:xx:xx:xx(x は任意の 16 進数)の MAC アドレスが一致したものとなります。マスク が 00:00:00:00:00:00 の場合は一つの MAC アドレスとなります。
- EtherType Key:パケットのイーサタイプが指定したイーサタイプと一致する必要があります。 ドロップダウンメニューからイーサタイプを選択します。User Value を選択すると、EtherType の値を入力出来ます。
- EtherType User Value: Ether Type で User Value を選択した場合に、入力が出来ます。 値の 範囲は 0x0600-0xFFFF です。
- Source MAC: イーサネットフレームの送信元 MAC アドレスがここのアドレスと一致する必要 があります。表記形式は xx:xx:xx:xx:xx です。
- Source MAC Mask:送信元 MAC アドレスのマスクを入力します。MAC アドレスマスクはイー サネットフレームの送信元 MAC アドレスのどのビットを比較するかを指定します。Fと0を MAC マスクで使い、ワイルドカード形式で使います。Fの部分は比較されず、0の部分は一致 する必要があります。例えば、MAC アドレスが aa:bb:cc:dd:ee:ff でマスクが 00:00:0ff:ff:ff:ff:ff であ る場合、aa:bb:xx:xx:xx(x は任意の 16 進数)の MAC アドレスが一致したものとなります。マ スクが 00:00:00:00:00:00 の場合は一つの MAC アドレスとなります。
- VLAN.:パケットの VLAN ID が一致する必要があります。値の範囲は 0-4093 です。
- 4. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。
- 5. ルールを削除するには、削除するルールのチェックボックスを選択し、Delete ボタンをクリックします。
- 6. ルールを変更するには、変更するルールのチェックボックスを選択し、項目を変更後、Apply ボ タンをクリックします。

MAC バインディング設定 (MAC Binding Configuration)

ACL がインターフェースに結び付けられるとき、すべての設定されたルールが選択されたインターフェースに適用されます。MAC Binding Configuration ページを使って MAC ACL を ACL の優先度 とインターフェースに割り当てます。

NETGE	AR'						8 Port Giga	GS110T bit PoE Smart Swite with 2 Fiber SF
System	Switching	QoS	Security	Monitoring	Maintena	nce Help		LOGOUT
Management Se	curity Access	Port Authentic	ation Traff	ic Control ACL				
ACL Wizard	MAC Bind	ding Config	uration					
Basic MAC ACL	Binding	Configuratio	n				(2)	
» MAC Rules	ACL ID		~	Directi	on	Inbound 🔽		
	Sequence N	Number	1	(1 to 4	294967295)			
» Binding Table	Port Selecti	ion Table						
Advanced	• <u>•</u>							
	LAG							
	Interfa	ce Binding St	atus				0	
	Interface	Direction	A(CL TD	Sea No		
	<				1111			>
							CA	NCEL APPLY

MAC ACL インターフェースバインディングを設定する

- 1. Security > ACL > Basic > MAC Binding Configuration を選択して MAC Binding Configuration ペー ジを表示します。
- ACL ID メニューから MAC ACL を選択します。
 ACL のパケットのフィルターの方向はインバンド、すなわち MAC ACL はポートに入力する トラフィックに適用されます。
- 3. Sequence Number(任意): インターフェースに割り当てられた他のアクセスリストとの順番をつけ るために番号を振ります。小さい数字が優先されます。値が入力されなかった場合は、一番大き な番号に1を加えた数字になります。値の範囲は 1-4294967295 です。
- 4. オレンジ色のバーをクリックして、ポートとLAGを表示します。
 - ポートまたは LAG に ACL を追加するには。ポートまたは LAG の下のボックスをクリックして X を表示させます。
 - ポートまたは LAG から ACL を削除するには。ポートまたは LAG の下のボックスをクリックして X を消去します。
- 5. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。
- 6. Apply ボタンをクリックして設定をスイッチに適用します。

MAC バインディングテーブル (MAC Binding Table)

MAC Binding Table ページで MAC ACL バインディングを確認、削除します。

Security > ACL > Basic > Binding Table を選択して MAC Binding Table ページを表示します。

								5
System	Switching	QoS	Security	Monit	oring	Maintenance	Help	LOGOL
Management Sec	urity Access	Port Authe	ntication Tra	ffic Control	ACL			
ACL Wizard	MAC Bin	ding Tab	le					
* MAC ACL	MAC B	inding Tabl	e			()		
» MAC Rules » MAC Binding	Inte	rface D	irection A	CL Type	ACL	Seq No		
Configuration					ID.			
* Binding Table Advanced								
	<					ш] [

以下に MAC Binding Table 欄に表示される情報の説明を示します。

項目	説明
Interface	MAC ACL がバインドされるインターフェース。
Direction	ACL のパケットフィルタの方向。Inbound(ポートに入力される方向)のみ有 効。
ACL Type	インターフェールと方向に割り当てられた ACL のタイプ。
ACL ID	インターフェールと方向に割り当てられた ACL ID。
Seq No	ACL の順序を決めるためにインターフェールと方向に割り当てられた番号。

MAC ACL とインターフェースとのバインディングを削除するには、削除するインターフェースのチェックボックスを選択して Delete ボタンをクリックします。

IP ACL

IP ACLを使って特定の入力ポートでのトラフィックの分類とルールを設定することが出来ます。パ ケットは入力(Ingress)ポートのみでフィルター可能です。フィルタールールが一致すると、パケット の廃棄やポートの無効化が出来ます。例えば、あるポートで TCP パケットを受信できるように ACL ルールを設定すると、UDP パケットは廃棄されます。

ACL は ACE(access control entries)とトラフィック分類を決定するフィルターを含むフィルターからなります。

IP ACL Configuration ページで IP ベースの ACL を追加・削除します。

NETGEA Connect with Innovation	R'				GS110TI 8 Port Gigabit PoE Smart Swite with 2 Fiber SF
System	iwitching QoS	Security Monit	oring Maintenance	Help	LOGOUT
Management Secu	rity Access Port Authentico	tion Traffic Control	ACL	ů.	
 ACL Wizard Basic Advanced IP ACL IP Rules IP Extended Rules IP Binding Configuration Binding Table 	IP ACL IP ACL Current Number of ACL Maximum ACL IP ACL Table IP ACL ID	0 100 Rules	Type		
	<		Ш		
					ADD DELETE CANCEL

IP ACL 欄は現在の ACL の数と最大設定可能な ACL の数を表示します。Current Number of ACL は IPv4 と MAC ACL の合計となります。最大値は 100 です。

IP ACL を設定する

- 1. Security > ACL > Advanced > IP ACL を選択して IP ACL ページを表示します。
- 2. IP ACL Table 欄の各項目を設定します。
- 3. IP ACL ID: ACL ID を入力します。 ACL ID は整数で以下の範囲を使います。
 - 1-99:送信元 IP アドレスからのトラフィックを許可、廃棄する IP Standard ACL を作成します。
 - 100-199:送信元 IP アドレスから宛先 IP アドレスへの特定のレイヤー3、レイヤー4トラフィックを許可または廃棄する IP Extended ACL を作成します。このタイプの ACL は IP Standard ACL よりも細かくフィルターをすることが出来ます。

それぞれの設定された ACL は以下の情報を表示します。

- Rules: IP ACL に設定されているルールの数を表示します。
- **Type**.: ACL のタイプ (Standard IP ACL または Extended IP ACL)を示します。
- 4. IP ACL を削除するには、削除する IP ACL のチェックボックスを選択し、Delete ボタンをクリックします。
- 5. IP ACL の名前を変更するには、変更する IP ACL のチェックボックスを選択し、名前を変更後、 Apply ボタンをクリックします。
- 6. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。

IP ルール(IP Rules)

IP Rules ページで IP ベースの Standard ACL を設定します。アクセスリスト設定は一致するトラフィックを転送するか廃棄するかを指定するルールを含みます。

メモ:ACL リストの最後には暗黙の "deny all"ルールが存在します。ACL がパケットに適用され、明示的に設定されたルールのどれにも一致しなかった場合は暗黙の"deny all"ルールによりパケットは廃棄されます。

NETGEA Connect with Innovation	R'					8 Po	GS108T ort Gigabit Smart Switch
System S	iwitching	QoS	Security	Monitoring	Maintenance	e Help	LOGOUT
Management Secu	rity Access	Port Authentic	ation Traffic	Control ACL			
> ACL Wizard > Basic * Advanced	IP Rules IP Rule	5					0
 » IP ACL » IP Rules » IP Extended Rules 	ACL ID Basic A	None	e				0
 » IP Binding Configuration » Binding Table 	Rule ID	Action	Assign Queue Id	Match Every	Source IP Address	Source IP Mask	
		×					-
	<				Ш		► ►
						ADD DELETE	CANCEL APPLY

IP ACL ルールを設定する

- 1. Security > ACL > Advanced > IP Rules を選択して IP Rules ページを表示します。
- 2. 新しい IP ACL ルールを追加するには、ルールを追加する ACL ID を選択し、以下の項目の設定を して Add ボタンをクリックします。
 - Rule ID: 1-10 の番号をつけます。各 ACL に作成できるルールは 10 個までです。
 - Action: ルールに一致した場合に実行される操作を指定します。
 - Permit: ACL に一致したパケットを転送します。
 - Deny: ACL に一致したパケットを廃棄します。
 - Assign Queue: ACL ルールに一致したパケットを処理するハードウェア出力キューID を指定します。0-3 を設定します。
 - Match Every:パケットがこの ACL の条件に一致する必要があります。ドロップダウンメニューから Ture または False を選択します。Match-Every で True を選択すると他のルールは設定できなくなります。
 - Source IP Address: パケットの送信元 IP アドレスがここのアドレスと一致する必要がありま す。指定形式は x.x.x.x です。
 - Source IP Mask::パケットの送信元 IP アドレスのワイルドカードマスクを入力します。ワイルドカードマスクはどのビットが使われどのビットが無視されるかを指定します。255.255.255.255のワイルドカードは、すべてのビットが重要ではないことを意味します。0.0.0.0 のワールドカードはすべてのビットが重要であることを意味します。ACL のワイルドカードマスクとサブネットマスクの動作は異なります。基本的にワイルドカードマスクはサブネットマクスの逆になります。 例えば、192.168.1.0/24 サブネットのすべてのホストにルールを適用するには、Source IP Mask 欄に 0.0.0.255 と入力します。Source IP Address を入力した時に、この欄にも入力する必要があります。
- 3. IP ACL ルールを削除するには、削除するルールのチェックボックスを選択し、Delete ボタンをクリックします。
- IP ACL ルールを変更するには、変更するルールのチェックボックスを選択し、設定を変更後、 Apply ボタンをクリックします。Rule ID を変更することはできません。
- 5. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。
- 7. ページの設定を変更した場合、Apply ボタンをクリックして設定を適用します。すぐに設定変更が

されます。

IP 拡張ルール(IP Extended Rule)

IP Extended Rules ページで IP ベースの拡張 ACL を設定します。アクセスリスト設定は一致するトラフィックを転送するか廃棄するかを指定するルールを含みます。

メモ:ACLリストの最後には暗黙の "deny all"ルールが存在します。ACL がパケットに適用され、明示的に設定されたルールのどれにも一致しなかった場合は 暗黙の"deny all"ルールによりパケットは廃棄されます。

NETGEAR Connect with Innovation	2											8 Port C	Gigabit	GS110 PoE Smart S with 2 Fibe	Swi er S
System Swi	tching	QoS	s s	ecurity		Monitoring	Maint	enance	Help	>				LOGO	out
Management Security	Acces	s Port /	Authentica	tion Ti	raffic C	ontrol ACL	1998) 1998								
ACL Wizard Basic Advanced » IP ACL » IP Rules	IP Ex IP ACL II	ctendec Extendec D	l Rules d Rules	None	2									0	
 IP Extended Rules 	:: Ex	tended A	CL Rule	Table										?	1
 » IP Binding Configuration » Binding Table 		Rule ID Ac	tion Qu	sign M Jeue E	latch very	CPU Notification Mode	Protocol Type	Src IP Address	Src IP Mask	Src L4 Port	Dst IP Address	Dst IP Mask	Dst L4 Port	Service Type	
6	د]														
U											_	ADD	DELETE	CANC	EL

IP ACL の拡張ルールを設定する

- 1. Security > ACL > Advanced > IP Extended Rules を選択して IP Extended Rules ページを表示します。
- IP ACL ルールを追加するには、ルールを追加する ACL ID を選択し、Extended ACL Rule table の チェックボックスを選択して Add ボタンをクリックします。以下のような Extended ACL Rule Configuration ページが表示されます。

System Switching QoS Security Monitoring Maintenance Help Locot Management Security Access Port Authentication Traffic Control ACL ACL Wizard Basic Extended ACL Rule Configuration 100-199) Image: Configuration Image: Configuration<	onnect with Innovation"	ĸ		8 Port Gigabit PoE Smart Swi with 2 Fiber S
Management Security Access Port Authentication Taffic Control Acl ACL Wizard Basic Extended ACL Rule Configuration Extended ACL Rule Configuration(100-199) Image: Configuration (100-199) Image: Configurati	System Sv	witching QoS Sect	rity Monitoring Maintenance Help	LOGOUT
ACL Wizard Basic Advanced > IP ACL > IP AcL > IP Extended ACL Rule Configuration(100-199) () ACL ID Rule ID (1 to 10) Action > Binding Table Action Action Action Action Action Action Action Action Action Action Action Action Action Permit Egress Queue (0 to 3) O to 3) O to 3) Ser IP Address Sr IP Address Sr IP Mask Sr L4 Port Det IP Address Det IP Mask Det IP Address Det IP Mask Det IA Port Det IP Mask Det IA Port Det IP Mask Det IA Port Det IP Mask Det	Management Securi	ty Access Port Authentication	Traffic Control ACL	
* IP AcL * IP AcL * IP AcL * IP Extended Rules * IP Binding Configuration * Binding Table * To Binding Table * The Binding Tab	ACL Wizard Basic	Extended ACL Rule Co	nfiguration	
ACL ID 101 I P Extended Rules I P Binding Configuration Binding Table Match Every False M CPU Notification Mode Protocol Type Src IP Address Src IP Mask Src L4 Port Det IP Mask Dst L4 Port Dst L4 Port Service Type I P DSCP af11 (0 to 63) I P Precedence (0 to 7) I P TOS (0 to 6ff)	Advanced	Extended ACL Rule Con	iguration(100-199)	•
IP Extended Rules P Binding Configuration > Binding Table Match Every False CPU Notification Mode Protocol Type All Src IP Address Src IP Mask Dst IP TOS IP Procedence (0 to 65535)	» IP ACL » IP Rules	ACLID	101	
Action Permit Egress Queue (0 to 3) Onfiguration Deny Match Every False CPU Notification Mode Protocol Type All (0 to 255) Src IP Address Src L4 Port Dst IP Address Dst IP Mask Dst L4 Port IP DSCP af11 (0 to 65535) Service Type IP Procedence (0 to 7) IP TOS (0 to 6ff) IP TOS (0 to 6ff) IP TOS (0 to ff) IP TOS <li< td=""><td></td><td>Rule ID (1 to 10)</td><td>0</td><td></td></li<>		Rule ID (1 to 10)	0	
Binding Table Match Every False For the form of the	» IP Binding Configuration	Action	Permit Egress Queue (0 to Denv	3)
CPU Notification Mode Protocol Type All O to 255) Src IP Address Src IP Mask Dst IP Address Dst IP Mask Dst L4 Port O to 65535) Service Type IIP DSCP afi1 (0 to 63) IIP Precedence O to 7) IIP TOS O (00-ff)	» Binding Table	Match Every	False M	
Protocol Type All Protocol Type All O to 255) Src IP Address Src IP Mask Src L4 Port O to 65535) Dst IP Mask Dst L4 Port O to 65535) Service Type O IP DSCP af11 (0 to 63) IP Precedence O to 7) IP TOS O (00-ff)		CPU Notification Mode		
Src IP Address Src IP Mask Src L4 Port Dst IP Mask Dst L4 Port Dst L4 Port Dst P Mask Dst L4 Port Dst		Protocol Type	All (0 to 255)	
Src L4 Port (0 to 65535) Dst IP Mask Dst IP Mask Dst L4 Port (0 to 65535) Service Type IP DSCP af11 (0 to 63) IP Precedence (0 to 7) IP TOS (00-ff)		Src IP Address		
Dst IP Address Dst IP Mask Dst L4 Port O to 65535) Service Type O IP DSCP afi1 (0 to 63) IP Precedence O (0 to 7) IP TOS O (00-ff)		Src I 4 Port	(0 to 65535)	
Dst IP Mask Dst L4 Port Ot to 65535) Service Type Ot IP DSCP afi1 (0 to 63) IP Precedence (0 to 7) IP TOS (00-ff)		Dst IP Address		
Dst L4 Port Image: Constraint of the state		Dst IP Mask		
Service Type IP DSCP afi1 (0 to 63) IP Precedence (0 to 7) (0 to 7) IP TOS (00-ff)		Dst L4 Port	(0 to 65535)	
IP Precedence (0 to 7) IP TOS (00-ff)		Service Type	O IP DSCP af11 (0 to 63)	
(00-ff)			O IP Precedence (0 to 7)	
K			O IP TOS (00-ff)	
		<		>

- 3. 新しいルールを設定します。
 - Rule ID: 1-10 の番号をつけます。各 ACL に作成できるルールは 10 個までです。
 - Action: ルールに一致した場合の転送動作を指定します。
 - Permit: ACL に一致したパケットを転送します。
 - Deny: ACL に一致したパケットを廃棄します。
 - Egress Queue: ACL ルールに一致したパケットを処理するハードウェア出力キューID を指定します。0-3 を設定します。
 - Match Every:パケットがこの ACL の条件に一致する必要があります。ドロップダウンメニューから Ture または False を選択します。Match-Every で True を選択すると他のルールは設定できなくなります。
 - Protocol Type:パケットのプロトコルタイプを指定します。Other を指定してプロトコル番号(0-255)を指定することもできます。
 - Source IP Address:パケットの送信元 IP アドレス(A.B.C.D 形式)を指定します。
 - Src IP Mask.:パケットの送信元 IP アドレスのワイルドカードマスクを入力します。ワイルドカ ードマスクはどのビットが使われどのビットが無視されるかを指定します。255.255.255.255 の ワイルドカードは、すべてのビットが重要ではないことを意味します。0.0.0.0 のワールドカード はすべてのビットが重要であることを意味します。ACL のワイルドカードマスクとサブネットマ スクの動作は異なります。基本的にワイルドカードマスクはサブネットマクスの逆になります。 例えば、192.168.1.0/24 サブネットのすべてのホストにルールを適用するには、Source IP Mask 欄に 0.0.0.255 と入力します。Source IP Address を入力した時に、この欄にも入力する 必要があります。
 - Src L4 Port:送信元 TCP/UDP ポートを指定します。以下の情報を指定します。
 - Source L4 Keyword:送信元のポートリストからレイヤ4のキーワードを選択します。
 - Source L4 Port Number: Source L4 keyword が Other の場合、ポート番号を指定しま す。
 - Destination IP Address: 宛先 IP アドレス(A.B.C.D 形式)を指定します。

- Destination Mask: 宛先 IP アドレスマスクを指定します。
- Destination L4 Port: 宛先 TCP/UDP ポート番号を指定します。 Other を指定してポート番号 を直接設定することもできます。
- Dst IP Address: パケットの宛先 IP アドレス(A.B.C.D 形式)を指定します。
- Dst IP Mask: パケットの宛先 IP アドレスのワイルドカードマスクを入力します。ワイルドカードマスクはどのビットが使われどのビットが無視されるかを指定します。255.255.255.255 のワイルドカードは、すべてのビットが重要ではないことを意味します。0.0.0.0 のワールドカードはすべてのビットが重要であることを意味します。ACL のワイルドカードマスクとサブネットマスクの動作は異なります。基本的にワイルドカードマスクはサブネットマクスの逆になります。例えば、192.168.1.0/24 サブネットのすべてのホストにルールを適用するには、Source IP Mask 欄に 0.0.0.255 と入力します。Source IP Address を入力した時に、この欄にも入力する必要があります。
- Dst L4 Port:宛先 TCP/UDP ポートを指定します。以下の情報を指定します。
 - Destination L4 Keyword: 宛先のポートリストからレイヤ 4 のキーワードを選択します。
 - Destination L4 Port Number: Destination L4 keyword が Other の場合、ポート番号を指定します。
- Service Type: 拡張 IP ACL ルールのためのサービスタイプの一つを選択します。選択肢は IP,DSCP,IP Precedence および IP TOS です。サービスタイプを選択後、タイプ毎の設定をしま す。
 - IP DSCP: IP DSCP(DiffServ Code Point)値を指定します。DSCP は IP ヘッダーのサービスタイプオクテットの上位 6 ビットに定義されています。メニューから IP DSCP 値を選択します。数値で指定するときは Other を選択し、0-63 の整数を入力します。
 - IP Precedence::IP Precedence は IP ヘッダーのサービスタイプオクテットの上位 3 ビット に定義されています。値の範囲は 0-7 です。
 - IP TOS Bits:パケットの IP ヘッダーの ToS ビット(16 進 2 桁)を指定します。最初の TOS 欄には 16 進 2 桁を設定します。2 つ目の欄は、パケットの IP TOS を比較するための TOS マスクです。TOS マスクは 00-ff の 16 進 2 桁のワイルドカードマスクです。例えば、 IP TOS フィールドでビット 7 と 5 が 1 の場合(7 が最高位ビット)、TOS 値は a0 で TOS マ スクは 00 になります。
- 4. IP ACL ルールを削除するには、削除するルールのチェックボックスを選択し、Delete ボタンをクリックします。
- 5. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。
- 6. IP ACL ルールを変更するには、変更するルールの Rule ID をクリックします。数字は Extended ACL Rule Configuration ページへのハイパーリンク担っています。

IP バインディング設定(IP Binding Configuration)

ACL がインターフェースに結び付けられるとき、すべての設定されたルールが選択されたインターフェースに適用されます。IP Binding Configuration ページを使って IP ACL を ACL の優先度とインターフェースに割り当てます。

						with 2 Fiber
System	Switching QoS	Security	Monitoring	Maintenance	Help	LOGOU
Management Secu	urity Access Port Aut	nentication Traff	fic Control ACL			
ACL Wizard	IP Binding Config	juration				
Basic	Binding Configura	ation			Ó	D
» IP ACL	ACL ID		Direction	Inbo	und 💌	
» IP Rules	Sequence Number	0	(1 to 429	1967295)		
Rules	Port Selection Table					
	•					
» Binding Table	LAG					
binding rabid						
	Interface Binding	Status			(D.
	Interface Direc	tion ACI	Type AC	L ID Seq	No	
						10
	<					

IP ACL インターフェースバインディングを設定する

- 1. Security > ACL > > IP Binding Configuration を選択して IP Binding Configuration ページを 表示します。
- 2. ACL ID メニューから IP ACL を選択します。ACL のパケットフィルターの方向は Inbound(入 力方向)です。すなわちポートに入力されるトラフィックに IP ACL ルールが適用されます。
- Sequence Number(任意): インターフェースに割り当てられた他のアクセスリストとの順番をつけるために番号を振ります。小さい数字が優先されます。値が入力されなかった場合は、一番大きな番号に1を加えた数字になります。値の範囲は1-4294967295です。
- 4. オレンジ色のバーをクリックして、ポートとLAGを表示します。
 - ポートまたは LAG に ACL を追加するには。ポートまたは LAG の下のボックスをクリックして X を表示させます。
 - ポートまたは LAG から ACL を削除するには。ポートまたは LAG の下のボックスをクリックして X を消去します。
- 5. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。
- 6. Apply ボタンをクリックして設定をスイッチに適用します。

IP バインディングテーブル(IP Binding Table)

IP Binding Table ページで IP ACL バインディングを確認・削除します。

Security > ACL > Advanced > Binding Table を選択して IP Binding Table ページを表示します。

IETGE/	A R'						GS108T
onnect with Innovatio	n ""					8 Port	Gigabit Smart Switc
System	Switching	QoS Se	curity Ma	onitoring	Maintenance	Help	LOGOUT
Management Sec	urity Access	Port Authenticati	on Traffic Cont	rol ACL			
ACL Wizard	IP Bindin	g Table					
Basic Advanced	IP Bindi	ng Table			0		
» IP ACL » IP Rules	Inter	face Direct	ion ACL Typ	e ACL ID	Seq No		
» IP Extended Rules					ander fan in fan in fan in fan in fan in fan i		
» IP Binding Configuration							
» Binding Table							
	<			Ш			>
							DELETE CANCEL

以下に IP Binding Table 欄に表示される情報の説明を示します。

項目	
Interface	IP ACL がバインドされるインターフェース。
Direction	IP ACL のパケットフィルタの方向。Inbound(ポートに入力される方向)のみ有 効。
ACL Type	インターフェールと方向に割り当てられた ACL のタイプ。
ACL ID	インターフェールと方向に割り当てられた ACL ID。
Seq No.	ACLの順序を決めるためにインターフェールと方向に割り当てられた番号。

IP ACL とインターフェースとのバインディングを削除するには、削除するインターフェースのチェックボックスを選択して Delete ボタンをクリックします。

6.システム監視

Monitoring タブの機能を使って、スイッチとポートの様々な情報を表示し、スイッチがイベントをどのように監視するかを設定できます。Monitoring タブは以下の機能へのリンクを含みます。

- ・ ポート(Ports)
- システムログ(System Logs)
- ポートミラーリング(Port Mirroring)

ポート(Ports)

Ports リンクはスイッチで送受信されるトラフィックの量やタイプについての様々な情報へのリンクを含みます。Ports リンクから以下のページへアクセスできます。

- スイッチ統計(Switch Statistics)
- ポート統計(Port Statistics)
- ポート詳細統計(Port Detailed Statistics)
- EAP 統計(EAP Statistics)

スイッチ統計(Switch Statistics)

Switch Statistics ページでスイッチが扱うトラフィックの統計情報を確認することができます。

Monitoring > Ports > Switch Statistics を選択して Switch Statistics ページを表示します。

System Switching Ports Logs Port Mirroring switch Statistics Port Statistics Switch Statistics Port Detailed Statistics EAP Statistics Switch Statistics	QoS Security Mon B Switch Statistics Switch Statistics Statistics ifIndex Octets Received Packets Received Packets Received Multicast Packets Received Broadcast Packets Received Broadcast Packets Received	itoring Maintenance Image: Transmission of transmissi of transmissico of transmission of transmission of transmissico	Help	
Ports Logs Port Mirroring Switch Statistics S Port Statistics S Port Detailed Statistics E PAP Statistics S	Switch Statistics Statistics ifIndex Octets Received Packets Received Without Error Unicast Packets Received Multicast Packets Received Broadcast Packets Received	13 671967 4825 2491 28		
Switch Statistics Port Statistics Port Detailed Statistics EAP Statistics	Switch Statistics :: Statistics ifIndex Octets Received Packets Received Without Error Unicast Packets Received Multicast Packets Received Broadcast Packets Received	13 671967 4825 2491 28		
Switch Statistics Port Statistics Port Detailed Statistics EAP Statistics	Statistics Statistics ifIndex Octets Received Packets Received Multicast Packets Received Broadcast Packets Received	13 671967 4825 2491 28		
Port Detailed Statistics EAP Statistics	Statistics ifIndex Octets Received Packets Received Without Error Unicast Packets Received Multicast Packets Received Broadcast Packets Received	 3 671967 4825 2491 28 		
EAP Statistics	ifIndex Octets Received Packets Received Without Error Unicast Packets Received Multicast Packets Received Broadcast Packets Received	13 671967 4825 2491 28		
	Octets Received Packets Received Without Error Unicast Packets Received Multicast Packets Received Broadcast Packets Received	671967 4825 2491 28		
	Packets Received Without Error Unicast Packets Received Multicast Packets Received Broadcast Packets Received	4825 2491 28		
	Unicast Packets Received Multicast Packets Received Broadcast Packets Received	2491 28		
	Multicast Packets Received Broadcast Packets Received	28		
	Broadcast Packets Received			
		2306		
	Receive Packets Discarded	0		
	Octets Transmitted	1826982		
	Packets Transmitted Without Errors	2201		
	Unicast Packets Transmitted	2178		
	Multicast Packets Transmitted	0		
	Broadcast Packets Transmitted	23		
	Transmit Packets Discarded	0		
	Most Address Entries Ever Used	28		
	Address Entries in Use	22		
	Maximum VLAN Entries	64		
	Most VLAN Entries Ever Used	3		
	Static VLAN Entries	0		
	VLAN Deletes	0		
	Time Since Counters Last Cleared	0 day 3 hr 32 min 7 sec		
<				

Switch Statistics ページの Statistics 欄に表示される情報の説明を示します。

項目	説明
ifIndex	インターフェースの ifIndex 数。
Octets Received	プロセッサーが受信するデータオクテット数。
Packets Received Without Errors	プロセッサーが受信した正常パケット数(マルチキャスト、ブロードキャストを 含む)。
Unicast Packets Received	プロセッサーが受信したユニキャストパケット数。

GS108T/GS110TP スマートスイッチソフトウェア管理マニュアル

Multicast Packets Received	プロセッサーが受信したマルチキャストパケット数。ブロードキャストパケットは 含みません。
Broadcast Packets Received	プロセッサーが受信したブロードキャストパケット数。マルチキャストパケット は含みません。
Receive Packets Discarded	プロセッサーが受信したパケットで廃棄されたパケット数。原因としては受信バッ ファーの不足等があります。
Octets Transmitted	インターフェースから送信されたオクテット数。
Packets Transmitted Without Errors	インターフェースから送信されたパケット数。
Unicast Packets Transmitted	送信されたユニキャストパケット数。
Multicast Packets Transmitted	送信されたマルチキャストパケット数。
Broadcast Packets Transmitted	送信されたブロードキャストパケット数。
Transmit Packets Discarded	廃棄された送信パケット数。
Most Address Entries Ever Used	最大 FDB(MAC アドレス)エントリー数。
Address Entries in Use	現在の FDB(MAC アドレス)エントリー数。
Maximum VLAN Entries	

項目	
Most VLAN Entries Ever Used	スイッチでの最大 VLAN 数。
Static VLAN Entries	スタティック VLAN 数。
Dynamic VLAN Entries	ダイナミック VLAN 数。
VLAN Deletes	削除された VLAN 数。
Time Since Counters Last Cleared	カウンターがクリアされてからの経過時間。

ページの下部のボタンを使って以下の操作をします。

- Clear:カウンターの値をクリアします。廃棄されたパケット数はクリアされません。
- Refresh:カウンターを最新状態に更新します。

ポート統計(Port Statistics)

Port Statistics ページでポートごとのトラフィック統計情報を表示します。

Monitoring > Ports > Port Statistics を選択して Port Statistics ページを表示します。 GS108T

System Switching		QoS	Security	Monito	ring M	aintenance	Help		LO
Ports Logs Port Mirrori	ng								
Switch Statistics	Port	Statistic	s						
Port Statistics Port Detailed Statistics	s	tatus							(2)
EAP Statistics	PORT	IS LAGS A			N (
	•	Interface	Total Packets received without Errors	Packets received with Errors	Broadcast Packets received	Packets transmitted without Errors	Transmit Packet Errors	Collision Frames	Time since counters last cleared
		g1	369412	0	110012	12233	0	0	2 day 7 hr 0 min 50 sec
		g2	0	0	0	0	0	0	2 day 7 hr 0 min 51 sec
		g3	0	0	0	0	0	0	2 day 7 hr 0 min 51 sec
		g4	0	0	0	0	0	0	2 day 7 hr 0 min 51 sec
		g5	0	0	0	0	0	0	2 day 7 hr 0 min 51 sec
		g6	0	0	0	0	0	0	2 day 7 hr 0 min 51 sec
						111			

以下に Port Statistics ページの Status 欄に表示される情報の説明を示します。

項目	説明
Interface	インターフェース。
Total Packets Received Without Errors	エラー無しに受信したパケット数。
Packets Received With Error	受信したエラーパケット数。
Broadcast Packets Received	受信したブロードキャストパケット数。マルチキャストパケットは含みません。
Packets Transmitted Without Errors	ポートから送信したパケット数。
Transmit Packet Errors	ポートから送信したエラーパケット数。
Collision Frames	コリジョンが発生したフレーム数。
Time Since Counters Last Cleared	カウンターがクリアされてからの経過時間。

ページ下部のボタンを使って以下の操作をします。

- Clear:カウンターの値をクリアします。一番上のチェックボックスを選択してすべてのポートのカウンターをクリアするか、個々のポートを選択してポートのカウンターをクリアします。
- Refresh:カウンターを最新状態に更新します。

ポート詳細統計(Port Detailed Statistics)

Port Detailed Statistics ページでポート単位の様々な統計情報を表示できます。

Monitoring > Ports > Port Detailed Statistics を選択して Port Detailed Statistics ページを表示します。

nnect with Innovation "			8 Port Gigabit PoE Smart S with 2 Fibe
System Switching	QoS Security Monito	ning Maintenance	Help
Ports Logs Port Mirroring			
Switch Statistics	Port Detailed Statistics		
Port Statistics Port Detailed Statistics	Detailed Statistics		(?)
EAP Statistics	-		-
	Interface	g1 📉	
	MSTID	CST	
	ifIndex	1	
	Port Type		
	Port Channel ID	Disable	
	Port Role	Disabled	
	STP Mode		
	STP State	Manual forwarding	
	Admin Mode	Enable	
	LACP Mode	Enable	
	Physical Mode	Auto	
	Physical Status	1000 Mbps Full Duplex	
	Link Status	Link Up	
	Link Trap	Enable	
	Packets RX and TX 64 Octets	1182	
	Packets RX and TX 65-127 Octets	12664	
	Packets RX and TX 128-255 Octets	685	
	Packets RX and TX 256-511 Octets	727	
	Packets RX and TX 512-1023 Octets	527	
	Packets RX and TX 1024-1518 Octets	1216	
	Packets RX and TX > 1522 Octets	0	
	Octets Received	1560220	
	Packets Received 64 Octets	1152	
	Packets Received 65-127 Octets	12273	
	Packets Received 128-255 Octets	386	
	Packets Received 256-511 Octets	593	
	Packets Received 512-1023 Octets	314	
	Packets Received 1024-1518 Octets	0	
	Packets Received > 1522 Octets	0	
	Iotal Packets Received Without Errors	14/18	
	Unicast Packets Received	2022	
	Multicast Packets Received	2215	
	Total Deckets Received with MAC From	2515	
	Total Packets Received with MAC Errors	0	
	Jappers Received	v	
<			

以下に Detailed Statistics 欄に表示される情報の説明を示します。

Interface メニューで確認したいポートを選択します。

項目	設定
Interface	ドロップダウンメニューから表示したいインターフェースを選択します。
MST ID	MST を選択します。
ifIndex	インターフェースの ifIndex を表示します。

項目	設定
Port Type	通常は空白です。以下の場合に表示されます。 • Mirrored:ポートミラーリングの参照元ポート。 • Probe:ポートミラーリングの宛先ポート。 • Port Channel:LAG を構成するポート。
Port Channel ID	ポートに LAG が設定されている場合はポートチャネル ID が表示されます。それ 以外の場合は Disable と表示されます。
Port Role	スパニングツリーの場合のポートロール。Root Port, Designated Port, Alternate Port, Backup Port, Master Port, あるいは Disabled Port.

STP Mode	STP の状態。 ● Enable:ポートでスパニングツリーが有効です。 ● Disable:ポートでスパニングツリーが無効です。
STP State	ポートのスパニングツリー状態。 Disabled Blocking Listening Learning Forwarding Broken
Admin Mode	ポートの状態。 Enable:ポートが有効(利用可能)(デフォルト) Disable:ポートが無効で利用不可。
LACP Mode	LACP のモードを表示します。 Enable:LAG 構成可能(デフォルト設定) Disable:LAG 構成不可。
Physical Mode	ポートの速度とデュープレックス設定。
Physical Status	ポートの速度とデュープレックス状態。
Link Status	リンクの状態。Up または Down。

項目	設定
Link Trap	リンクの状態が変化した時にトラップを送信するかどうかを表示します。デ フォルトは Enable です。
Packets RX and TX 64	パケットサイズが 64 バイトの送受信したパケット数(不良パケットも含む)。IFG,プリ
Octets	アンブルは含まず、FCS を含みます。
Packets RX and TX 65–127	パケットサイズが 65-128 バイトの送受信したパケット数(不良パケットも含む)。
Octets	IFG,プリアンブルは含まず、FCS を含みます。
Packets RX and TX	パケットサイズが 128-255 バイトの送受信したパケット数(不良パケットも含む)。
128–255 Octets	IFG,プリアンブルは含まず、FCS を含みます。
Packets RX and TX	パケットサイズが 256-511 バイトの送受信したパケット数(不良パケットも含む)。
256–511 Octets	IFG,プリアンブルは含まず、FCS を含みます。
Packets RX and TX	パケットサイズが 512-1023 バイトの送受信したパケット数(不良パケットも含む)。
512–1023 Octets	IFG,プリアンブルは含まず、FCS を含みます。
Packets RX and TX 1024–1518 Octets	パケットサイズが 1024-1518 バイトの送受信したパケット数(不良パケットも含む)。IFG,プリアンブルは含まず、FCS を含みます。
Packets RX and TX > 1522 Octets	

Octets Received	受信総オクテット数(不良パケットも含む)。IFG,プリアンブルは含まず、FCS を含 みます。イーサネットの利用率を推定する事ができます。正確には、 etherStatsPkts および etherStatsOctets の値を一定間隔で取得して速度を計算 します。
Packets Received 64	パケットサイズが 64 バイトの受信したパケット数(不良パケットも含む)。IFG,プ
Octets	リアンブルは含まず、FCS を含みます。
Packets Received 65–127	パケットサイズが 65-128 バイトの受信したパケット数(不良パケットも含む)。
Octets	IFG,プリアンブルは含まず、FCS を含みます。
Packets Received 128–255	パケットサイズが 128-255 バイトの受信したパケット数(不良パケットも含む)。
Octets	IFG,プリアンブルは含まず、FCS を含みます。
Packets Received 256–511	パケットサイズが 256-511 バイトの受信したパケット数(不良パケットも含む)。
Octets	IFG,プリアンブルは含まず、FCS を含みます。

項目	設定
Packets Received 512–1023 Octets	パケットサイズが 512-1023 バイトの受信したパケット数(不良パケットも含む)。 IFG,プリアンブルは含まず、FCS を含みます。
Packets Received 1024–1518 Octets	パケットサイズが 1024-1518 バイトの受信したパケット数(不良パケットも含む)。 IFG,プリアンブルは含まず、FCS を含みます。
Packets Received > 1522 Octets	パケットサイズが 1522 バイト以上の受信したパケット数(不良パケットも含む)。IFG,プリアンブルは含まず、FCS を含みます。
Total Packets Received Without Errors	受信した総パケット数。(エラーパケットは含まず)
Unicast Packets Received	受信したユニキャストパケット数。(エラーパケットは含まず)
Multicast Packets Received	受信したマルチキャストパケット数。(エラーパケット、ブロードキャストパケットは 含まず).
Broadcast Packets Received	受信したブロードキャストパケット数。(エラーパケット、マルチキャストパケットは含まず).
Total Packets Received with MAC Errors	受信したエラーパケット数。
Jabbers Received	パケット長が 1518 オクテット以上のジャバー(FCS エラー)パケット数。
Fragments Received	64 オクテット未満の受信 CRC エラーパケット数。
Undersize Received	64 オクテット未満の受信 CRC 正常パケット数。
Alignment Errors	64-1518 バイトの受信パケット数で FCC エラーがあり、パケット長がオクテットの整 数倍でないもの。
Rx FCS Errors	

GS108T/GS110TP スマートスイッチソフトウェア管理マニュアル

Overruns	オーバーランとして廃棄されたパケット数。
Total Received Packets Not Forwarded	受信したパケットで転送されずに廃棄されたもの。

項目	設定
Local Traffic Frames	転送段階で宛先アドレスが存在しないため廃棄されたフレーム数。
802.3x Pause Frames Received	802.3x Pause フレームの受信数。
Unacceptable Frame Type	許容できないフレームタイプとして廃棄されたフレーム数。
Multicast Tree Viable Discards	マルチキャストツリーが変更されている最中に廃棄されたマルチキャストフレ ーム数。
Reserved Address Discards	IEEE802.1 で予約済みでシステムでサポートされていないアドレス宛の廃棄された フレーム数。
Broadcast Storm Recovery	ブロードキャストストームコントロールが有効にされた結果廃棄されたブロード キャストフレーム数。(宛先 MAC アドレスが FF:FF:FF:FF:FF:FF)
CFI Discards	CFI ビットが設定されていて RFI 中のアドレスが非カノニカルフォーマットで廃棄 されたフレーム数。
Upstream Threshold	パケットのプライオリティレベルに応じたセルディスクリプタ不足で廃棄されたフ レーム数。
Total Packets Transmitted (Octets)	送信総オクテット数(不良パケットも含む)。IFG、プリアンブルは含まず、FCS を含 みます。イーサネットの利用率を推定する事ができます。正確には、 etherStatsPkts および etherStatsOctets の値を一定間隔で取得して速度を計算 します。
Packets Transmitted 64 Octets	パケットサイズが 64 バイトの送信したパケット数(不良パケットも含む)。IFG,プリ アンブルは含まず、FCS を含みます。
Packets Transmitted 65–127 Octets	パケットサイズが 65-127 バイトの送信したパケット数(不良パケットも含む)。 IFG,プリアンブルは含まず、FCS を含みます。
Packets Transmitted 128–255 Octets	パケットサイズが 128-255 バイトの送信したパケット数(不良パケットも含む)。 IFG,プリアンブルは含まず、FCS を含みます。
Packets Transmitted 256–511 Octets	パケットサイズが 256-511 バイトの送信したパケット数(不良パケットも含む)。 IFG,プリアンブルは含まず、FCS を含みます。
Packets Transmitted 512–1023 Octets	
Packets Transmitted 1024–1518 Octets	

項目	設定

Packets Transmitted 1519–1522 Octets	パケットサイズが 1519-1512 バイトの送信したパケット数(不良パケットも含む)。 IFG,プリアンブルは含まず、FCS を含みます。
Total Packets Transmitted Successfully	正常に送信されたパケット数。
Unicast Packets Transmitted	送信されたユニキャストパケット数。
Multicast Packets Transmitted	送信されたマルチキャストパケット数。
Broadcast Packets Transmitted	送信されたブロードキャストパケット数。
Total Transmit Errors	送信エラーパケット数。
Tx FCS Errors	64-1518 バイトの送信パケット数で FCC エラーがあり、パケット長がオクテットの 整数倍であるもの。
Tx Oversized	最大フレーム長を超えたフレーム数。
Underrun Errors	アンダーランエラーフレーム数。
Total Transmit Packets Discarded	廃棄された送信フレーム数。
Single Collision Frames	単一衝突後正常に送信されたフレーム数。
Multiple Collision Frames	複数衝突後正常に送信されたフレーム数。
Excessive Collision Frames	過度の衝突後送信できなかったフレーム数。
Port Membership Discards	送信フィルタによって廃棄されたフレーム数。
STP BPDUs Received	ポートでの受信 STP BPDU 数。
STP BPDUs Transmitted	ポートでの送信 STP BPDU 数。
RSTP BPDUs Received	ポートでの受信 RSTP BPDU 数。
RSTP BPDUs Transmitted	ポートでの送信 RSTP BPDU 数。
MSTP BPDUs Received	ポートでの受信 MSTP BPDU 数。
MSTP BPDUs Transmitted	ポートでの送信 MSTP BPDU 数。

項目	設定
802.3x Pause Frames Transmitted	802.3 ポーズフレーム送信数。
EAPOL Frames Received	EAPOL フレーム受信数。
EAPOL Frames Transmitted	EAPOL フレーム送信数。
Time Since Counters Last Cleared	カウンターがクリアされてからの時間。

ページ下部のボタンを使って以下の操作をします。

- Clear:カウンターの値をクリアします。
- Refresh:カウンターを最新状態に更新します。

EAP 統計(EAP Statistics)

EAP Statistics ページでポートが受信した EAP パケットの情報を確認できます。

Monitoring > Por	ts > EAF	Statistics	を選択して E/	AP Statistics	ページを表示します。
------------------	----------	------------	----------	---------------	------------

System Swit	hing	QoS	Security	Monitor	ing M	aintenance	He	p						10
orts Logs Port	Airroring													
witch Statistics	E/	P Stal	listics											
ort Statistics ort Detailed Statis	ics	EAP Statistics (6)												
AP Statistics	P	20175	LAGS	All										
				yı 6		EAPOL						EAP		7
		Ports	Frames Received	Frames Transmitted	Start Frames Received	Logoff Frames Received	Last Frame Version	Last Frame Source	Invalid Frames Received	Length Error Frames Received	Response/ID Frames Received	Response Frames Received	Request/1D Frames Transmitted	Request Frames Transmitte
	E	g1	0	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0
	C	92	0	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0
		g3	a	0	0	0	0	00:00:00:00:00:00	0	0	D	0	0	0
	C	g4	0	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0
	E	g5	0	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0
		96	0	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0
	E	97	0	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0
		98	0	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0
	10	ORTS	LAGS	All .										

以下に EAP Statistics 欄に表示される情報の説明を示します。

項目	説明
Ports	ポート名を表示します。
Frames Received	ポートで受信した有効な EAPOL フレーム数を表示します。
Frames Transmitted	ポートから送信した EOPOL フレーム数を表示します。
Start Frames Received	ポートで受信した EAPOL Start フレーム数を表示します。
Log off Frames Received	ポートで受信した EAPOL Log off フレーム数を表示します。
Last Frame Version	最新の受信した EAPOL フレームのプロトコルバージョン。
Last Frame Source	最新の受信した EAPOL フレームの送信元 MAC アドレス。
Invalid Frames Received	ポートで受信した不正な EAPOL フレーム数。
Length Error Frames Received	ポートで受信したパケット長エラーの EAPOL フレーム数。
Response/ID Frames Received	ポートで受信した EAP 応答 ID フレーム数。
Response Frames Received	ポートで受信した有効な EAP 応答 フレーム数。
Request/ID Frames Transmitted	ポートから送信された EAP 要求 ID フレーム数。
Request Frames Transmitted	ポートから送信された EAP 要求フレーム数。

ページ下部のボタンを使って以下の操作をします。

- Clear:カウンターの値をクリアします。一番上のチェックボックスを選択してすべてのポートのカウンターをクリアするか、個々のポートを選択してポートのカウンターをクリアします。
- Refresh:カウンターを最新状態に更新します。

システムログ(System Logs)

スイッチはプラットフォーム上で発生するイベント、障害、エラーに対してメッセージを生成します。これ らのメッセージはローカルに保存され、監視目的のために集中拠点や長期保存ストレージに転送する ことができます。ローカルおよびリモートログ機能は、重要性や生成元に基づくログあるいは転送のメ ッセージのフィルタを含みます。

Monitoring > Logs タブは以下のフォルダーのリンクを含みます。

- メモリーログ(Memory Logs)
- フラッシュログ設定(FLASH Log Configuration)
- サーバーログ設定(Server Log Configuration)
- トラップログ(Trap Logs)
- イベントログ(Event Logs)

メモリーログ(Memory Logs)

メモリーログはメッセージの中身や重要性に対する設定にもとづきメモリーにメッセージをログします。Memory Logs ページでシステムバッファー中でのログのふるまいや管理状態の設定をします。これらのログメッセージはスイッチが再起動するとクリアされます。

System	Switching QoS	Security	Monitoring	Maintenance	Help	LOG		
Ports Logs	Port Mirroring							
lemory Log	Memory Log							
ELASH Log	Memory Log (Configuration		0				
Frap Logs Event Logs	Admin Status Behavior	O Disab Wrap	ole 💿 Enable					
	Memory Log			۲				
	Total number of Me	ssages 54						
	Description	Description						
	<14> Jan 01 00:00 2 %% OPENSSL: Fi	<14> Jan 01 00:00:07 0.0.0.0-1 UNKN[2181650108]: openssl_api.c(800) 2 %% OPENSSL: File dh512.pem size = 0						
	<14> Jan 01 00:00 3 %% OPENSSL: 0							
	<14> Jan 01 00:00 4 %% DH params	<14> Jan 01 00:00:07 0.0.0.0-1 UNKN[2181650108]: openssl_api.c(884) 4 %% DH params not read						
	<14> Jan 01 00:00 EDB Callback: Unit	<14> Jan 01 00:00:07 0.0.0.1 UNKN[2174399244]: edb.c(356) 5 %% EDB Callback: Unit Join: 1.						
	A 145 1 01 00:00		• NTMED1777100ED					

メモリーログ設定をする

- 1. Monitoring > Logs > Memory Log を選択して Memory Log ページを表示します。
- 2. Admin Status 欄のラジオボタンでメッセージのログをするかどうかを設定します。

- Enable:システムログを有効にします。
- Disable:システムログを無効にします。
- 3. Behavior メニューでログがいっぱいになった時の動作を設定します。
 - Wrap:バッファーがいっぱいになると、古いログメッセージが削除され、新しいメッセージがログ されます。
 - Stop on Full: バッファーがいっぱいになると、システムは新しいメッセージのログを止めて、 既に存在しているすべてのログを保持します。
- 4. 設定を変更した場合は、Apply ボタンをクリックして変更のシステムへの適用および変更の保存をします。

Memory Log の表は Memory Log ページにも表示されます。

項目	説明
Total Number of Messages	システムがメモリーにログしたメッセージ数。最新の 64 メッセージのみが 表示されます。

Descriptions 欄にはメモリーログメッセージが表示されます。ログメッセージのフォーマットはメッセ ージログ等と同じです。

以下がログメッセージの標準的なフォーマットの例です。

<14> Mar 24 05:34:05 10.131.12.183-1 UNKN[2176789276]:

main_login.c(179) 3855 %% HTTP Session 19 initiated for user admin connected from 10.27.64.122

◇で囲まれた数字は次の値から導かれるメッセージのプライオリティを表します。

プライオリティ=(ファシリティ値 × 8)+重要度の値

ファシリティ値は通常はユーザーレベルメッセージを意味する1です。したがってメッセージの重要度の値は、<>で囲まれた数字から8を引くことで求められます。

メッセージは 3 月 24 日の午前 5 時 34 分 05 秒に、IP アドレスが 10.131.12.183 のスイッチから生成さ れました。メッセージを生成した部分は不明(Unknown)ですが、main_login.c ファイルの 179 行目であ ることがわかります。スイッチが起動してから 3,855 番目にログされたメッセージです。メッセージは管 理者が IP アドレス 10.27.64.122 のホストから HTTP 管理インターフェースにログインしたことを示して います。

ページ下部のボタンを使って以下の操作をします。

- Clear: メッセージをメモリーのバッファーログからクリアします。
- Refresh:ログ中のメッセージを最新状態に更新します。
- Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。

フラッシュログ設定(FLASH Log Configuration)

フラッシュログ(FLASH log)はスイッチが再起動しても維持される固定記憶域に保存されるログです。

1番目のログタイプは system startup log です。System startup log はシステム再起動後の最初に受信した N 個のメッセージを保存します。このログは常にいっぱいになった際に保存を停

止し、最大 32 メッセージを保存できます。

 2 つ目のログタイプは system operation log です。System operation log はシステム動作時の最 後に受信した N 個のメッセージを保存します。このログはいっぱいになった時に上書きをし、最 大 1000 メッセージを保存できます。

System startup log または System operation log はログサブシステムが受信したメッセージを保存しますが、両方を保存するわけではありません。システム起動時に、Startup log が設定されていると、メッ セージを制限数まで保存します。Operation log が設定されていると、メッセージを保存開始します。

FLASH Log Configuration ページでフラッシュログ設定をします。

NETGE	AR'			GS108
Connect with Innovatio	n "		8 Port Giga	bit Smart Swit
System	Switching QoS Security Monitoring	Maintenance	Help	LOGOU
Ports Logs	Port Mirroring	C.		
Memory Log	FLASH Log			
FLASH Log Server Log	FLASH Log Configuration	1		
Trap Logs Event Logs	Admin Status Image: Openable Severity Filter Alert			
	: FLASH Logs	(2)		
	Number of FLASH Messages 0			
	Description			
	[〈]][;
		CLEAR	R REFRESH CA	NCEL APPLY

フラッシュログ設定をする

- 1. Monitoring > Logs > FLASH Log を選択して FLASH Log ページを表示します。
- 2. Admin Status 欄のラジオボタンを選択します。
 - Enable:フラッシュログを有効にします。
 - Disable:フラッシュログを無効にします。
- 3. Severity Filter:記録するログメッセージのタイプを指定します。ログは設定したレベルとそれ以 上のレベルのメッセージを記録します。例えば、Errorを選択すると、Error, Critical, Alert, および Emergency レベルが記録されます。デフォルトのレベルは Alert(1)です。
 - Emergency (0):最高の警告レベル。デバイスがダウンあるいは正常に動作していない場合に使用されます。
 - Alert (1):2 番目の警告レベル。即座に対応が必要です。
 - Critical (2):3 番目の警告レベル。致命的な状態。
 - Error (3):3 番目の警告レベル。ポートがオフラインになったようなデバイスのエラーが 発生。
 - Warning (4): 最低レベルの警告。
 - Notice (5): 正常だが重要な情報。デバイスの情報をネットワーク管理者に提供します。
 - Info (6): デバイス情報を提供します。
 - Debug (7): デバッグ用の詳細な情報を提供します。資格があるサポート担当者が使うべき レベルです。
- 4. 設定を変更した場合は、Apply ボタンをクリックして変更のシステムへの適用をします。

Descriptions 欄にはフラッシュログメッセージが表示されます。

ページ下部のボタンを使って以下の操作をします。

- Clear:メッセージをメモリーのバッファーログからクリアします。
- Refresh:ログ中のメッセージを最新状態に更新します。
- Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。

サーバーログ設定(Server Log Configuration)

Server Log Configuration ページでリモートのログサーバーにメッセージを送信する設定をします。

NETGEA Connect with Innovation	AR'				8 F	CS110TP Port Gigabit PoE Smart Switch with 2 Fiber SFP
System	Switching QoS	Security Mo	nitoring	Maintenance	Help	LOGOUT
Ports Logs	Port Mirroring					
Memory Log	Server Log					^
FLASH Log Server Log	Server Log Configur	ration				2
 Trap Logs Event Logs 	Admin Status Local UDP Port	S14	isable (Enable (1 to 65535)		
	Messages Relayed	0				
	Server Configuratio	n			(2
	Host Address	Status	514	1 to 65535)	Severity Filter	
	<					
					ADD DELET	E CANCEL APPLY
Copyright © 1996-2	2010 Netgear ®					

ローカルログサーバー設定をする

- 1. Monitoring > Logs > Server Log を選択して Server Log ページを表示します。
- 2. Admin Status 欄のラジオボタンを選択します。
 - Enable:メッセージは設定されたホストに送信されます。
 - Disable:設定されたホストへのメッセージ送信を停止します。
- 3. Local UDP Port: Syslog メッセージを送信するポート番号を指定します。
- 4. Apply ボタンをクリックして設定を保存します。

Server Log Configuration 欄は以下の情報も表示します。

- Messages Relayed: Syslog 機能が Syslog ホストへ転送したメッセージ数。複数のホストに送信されたメッセージはそれぞれカウントされます。
- Messages Ignored: 無視されたメッセージ数。

リモートログサーバー設定をする

- 1. リモート Syslog ホスト(ログサーバー)を追加するには以下の設定をして Add ボタンをクリックします。
 - Host Address:シスログサーバーを IP アドレスまたはホスト名で指定します。
 - Port:ホストのポート番号を指定します。デフォルトは 514 です。
 - Severity Filter:ホストへ送信するログメッセージのタイプを指定します。ログは設定したレベルとそれ以上のレベルのメッセージを送信します。例えば、Errorを選択すると、Error,

Critical, Alert, および Emergency レベルが送信されます。 デフォルトのレベルは Alert(1) です。

- Emergency (0):最高の警告レベル。デバイスがダウンあるいは正常に動作していない場合に使用されます。
- Alert (1):2 番目の警告レベル。即座に対応が必要です。
- Critical (2):3 番目の警告レベル。致命的な状態。
- Error (3):3 番目の警告レベル。ポートがオフラインになったようなデバイスのエラーが発生。
- Warning (4):最低レベルの警告。
- Notice (5): 正常だが重要な情報。デバイスの情報をネットワーク管理者に提供します。
- Info (6): デバイス情報を提供します。
- Debug (7): デバッグ用の詳細な情報を提供します。資格があるサポート担当者が使う べきレベルです。
- 2. 設定されているホストを削除するには、削除するホストのチェックボックスを選択し、Delete ボタ ンをクリックします。
- 3. ホスト設定を変更するには、変更するホストのチェックボックスを選択し、変更後に Apply ボタンを クリックして変更のシステムへの適用をします。
- 4. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。

Server Configuration table の Status 欄はホストがアクティブかどうかを表示します。

トラップログ(Trap Logs)

Trap Logs ページでスイッチが生成する SNMP トラップの情報を表示します。

Monitoring > Logs > Trap Logs を選択して Trap Logs ページを表示します。

NETGE#	AR'						GS108T
Connect with Innovation	n ""					8 Port Gig	abit Smart Switch
System	Switchi	ng QoS	Security	Monitoring	Maintenance	Help	LOGOUT
Ports Logs	Port Mir	roring					
> Memory Log	Traj	o Logs					^
 FLASH Log Server Log 	Т	rap Logs	(?)				
* Trap Logs * Event Logs	Num Trap	ber of Traps Since Last Log Capacity	Reset	4 256			
	Num	ber of Traps Since Log	Last Viewed	4			
	т	rap Logs			(2)		=
	Log	System Up Time	Trap				
	0	0 days 00:00:32	0 days 00:00:32 Cold Start: Unit: 0				
	1	0 days 00:00:25	Link Up: g	1			
	2	0 days 00:00:24	Link Down	: g1			
	3	0 days 00:00:15	Link Up: g	1			
	<			III			~
1							
							CLEAR COUNTERS
Copyright © 1996-2	2009 Net	gear ®					

以下に Trap Logs 欄に表示される情報の説明を示します。

項目	説明

GS108T/GS110TP スマートスイッチソフトウェア管理マニュアル

Number of Traps Since Last Reset	スイッチが再起動してから発生したトラップ数。
Trap Log Capacity	ログに保存できる最大のトラップ数。最大数に達した場合は古いトラップが上書きされます。
Number of Traps Since Log Last Viewed	最後にトラップが表示されてからのトラップ数。表示されると0になります。

Trap Logs 欄には送信されたトラップの情報も表示されます。

項目	説明
Log	トラップの番号。
System Up Time	トラップが発生した時のスイッチが再起動してからの時間。
Тгар	トラップの情報。

Clear ボタンをクリックしてカウンターをクリアします。すべての値がデフォルト値になります。

イベントログ(Event Logs)

Event Log ページでイベントログを表示します。イベントがログされ、更新されたログがフラッシュメモリーに保存された後、スイッチはリセットされます。ログは最低 2000 まで保存され、いっぱいになった後にイベントが追加される際に消去されます。イベントログはスイッチがリセットされても保存されます。

Monitoring > Logs > Event Logs を選択して Event Logs ページを表示します。

	A R'					GS 1 8 Port Gigabit PoE Sm with 2	10T art Swi Fiber S
System	Switching Qo	S Security	Monitoring	Maintenance	Help	G	logout
Ports Logs	Port Mirroring		16		000 - DA		
Memory Log	Event Logs						
FLASH Log Server Log	Event Logs					1	
Trap Logs	Entry Type	Filename Line	Task ID	Code	Time		
Event Logs							
	<						
						CLEAR	FRESH
and the second	DOLO Notacco O						

以下に Event Logs 欄に表示される情報の説明を示します。

項目	
Entry	イベントの番号。最新が一番上。
Туре	イベントのタイプ。
Filename	ソースコードのファイル名。
Line	ソースコードの該当行番号。
Task ID	イベントを発生したタスク ID.

Code	イベント発生時のイベントコード。
Time	イベント発生時間。前回の再起動からの時間。

ページ下部のボタンを使って以下の操作をします。

- Clear:メッセージをイベントログからクリアします。
- Refresh:画面を最新状態に更新します。

ポートミラーリング(Port Mirroring)

Port Mirroring リンクでポートミラーリングの設定ができます。

マルチポートミラーリング(Multiple Port Mirroring)

ポートミラーリングはネットワークアナライザーで解析するためのネットワークトラフィックを選択しま す。スイッチの特定ポートを選択し解析できます。そのために、複数のポートを送信元ポート、一つの ポートを宛先ポートとして設定できます。送信元ポートのトラフィックをどのようにミラーするかを設定で きます。送信元ポートで受信、送受信、および送信されるトラフィックを宛先ポートにミラーすることがで きます。

宛先ポートにコピーされるパケットは送信元パケットと同じフォーマットです。送信元パケットの VLAN タグの有無も含めてコピーされます。

NETGEAR	£.						GS108
Connect with Innovation "						8 Port G	igabit Smart Sw
System Swi	tching	QoS	Security	Monitoring	Maintenanc	e Help	LOGO
Ports Logs Por	Mirroring			ana katalah sa			
• Port Mirroring	AUITIPIE P	OFT MILL	oring				
1	Status T	able			(?)		
			GO TO	INTERFACE	GO		
	Source	Port	Destination Por	Session Mode	Mirroring Port		
				×			
	g1			Disable			
	g2			Disable			
	g3			Disable			
	g4			Disable			
	g 5			Disable			
	g6			Disable			
	g7			Disable			
	g8			Disable			
			GO TO	INTERFACE	GO		
<							1
						DELETE	CANCEL APPLY

Multiple Port Mirroring ページでポートミラーリングを設定します。

ポートミラーリングを設定する

- 1. Monitoring > Port Mirroring を選択して Port Mirroring ページを表示します。
- 2. 参照するポートのチェックボックスを選択します。
- 3. Destination Port:宛先ポート名をg1,g2…という形式で記入します。宛先ポートはスイッチで1つのみとなります。
- 4. Session Mode:ポートミラーリングの有効・無効を選択します。
 - Enable:ポートミラーリングを有効にします。
 - Disable:ポートミラーリングを無効にします。
- 5. Apply ボタンをクリックして設定を適用します。ポートが参照元として設定されている場合には、 Mirroring Port 欄の表示は Mirrored となります。
- 6. 参照元ポートを削除するには、削除するポートのチェックボックスを選択し、Delete ボタンをクリックします。
- 7. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。

7.システムメインテナンス

Maintenance タブ中の機能をつかってスイッチを管理します。Maintenance タブには以下の機能の リンクを含みます。

- リセット(Reset)
- スイッチからのファイルアップロード(Upload File From Switch)
- スイッチへのファイルダウンロード(Download File To Switch)
- ファイル管理(File Management)
- トラブルシュート(Troubleshooting)

リセット(Reset)

Reset メニューは以下の機能へのリンクを含みます。

- 再起動(Device Reboot)
- ファクトリーデフォルト(Factory Default)

再起動(Device Reboot)

Device Reboot ページで GS108T/GS110TP を再起動します。

NETGI Connect with Innov	EAR'					8 Port Gig	GS108T abit Smart Switch
System	Switching	QoS	Security	Monitoring	Maintenance	Help	LOGOUT
Reset Upk	oad Download	File Manage	ement Trouble	shooting	1		
- Device Reb	oot Device	Reboot					^
> Factory Del	ault Devic	e Reboot			(7)		
	Check this	s box and clic	APPLY below t	o reboot unit(s)			
							~
	<			111			>
						(c)	ANCEL APPLY

スイッチを再起動する

- 1. Maintenance > Reset > Device Reboot.を選択して Device Reboot.ページを表示します。
- 2. チェックボックスをクリックします。
- 3. Apply.ボタンをクリックすると、スイッチは即座に再起動します。スイッチが起動し終わるまで管理 インターフェースは利用できません。スイッチ再起動後ログイン画面が表示されます。

ファクトリーデフォルト(Factory Default)

Factory Default ページでシステム設定を工場出荷時設定にリセットすることができます。

メモ:スイッチを初期化すると、IP アドレスは 192.168.0.239 になり、DHCP クライア ント機能は有効になっています。

NETGEA Connect with Innovation ^{**}	R'			81	Port Gigabit P	OE Smart Switch with 2 Fiber SFP
System Sw	vitching	QoS Security	Monitoring	Maintenance	Help	LOGOUT
Reset Upload	Download Fi	le Management Trouble	shooting			
> Device Reboot	Factory De	efault				^
* Factory Delault	Factory D	efault		(?)		
	Check this bo: configuration	x and click APPLY below t settings to default values	o return all s			=
r	. 1					· · · · · · · · · · · · · · · · · · ·
l	<u>, </u>					
					CANCEL	APPLY
Copyright © 1996-201	0 Netgear ®					

スイッチの設定を工場出荷設定に戻す

- 1. Maintenance > Reset > Factory Default を選択して Factory Default ページを表示します。
- 2. チェックボックスを選択します。
- 3. Apply.ボタンをクリックすると、スイッチは即座に再起動します。

スイッチからのファイルアップロード(Upload File From Switch)

スイッチは TFTP または HTTP でリモートシステムへのファイルアップロードをすることができます。 Upload ページで設定(ASCII)、ログ(ASCII)およびイメージ(バイナリー)ファイルをスイッチからリモート サーバーへアップロードできます。

NETGEAR Connect with Innovation					8 Port Gig	GS110TP abit PoE Smart Switch with 2 Fiber SFP
System Switch Reset Upload Dov	ning QoS wnload File Manage	Security ment Trouble	Monitoring	Maintenance	Help	LOGOUT
 * TFTP File Upload > HTTP File Upload 	TFTP File Uplo TTTP File Uplo File Type Transfer Mode Server Address Typ Server Address Transfer File Path Transfer File Name	ad ad Error Fror 0.0.0.0 Star	Log • • • • • • • • • • • •			
					c	ANCEL

スイッチから TFTP サーバーへファイルをアップロードする

- 1. Maintenance > Upload > TFTP File Upload を選択して TFTP File Upload ページを表示します。
- 2. File Type:アップロードするファイルのタイプを選択します。
 - Code:コードイメージ。
 - Text Configuration:テキスト設定ファイル。
 - Error Log:エラーログ、イベントログ。

- Buffered Log:メモリー中のバッファーログ。
- **Trap Log**:トラップログ。
- **11.** タイプが Code の場合は、image1 か image2 かを選択します。この選択肢は Code を選択した時のみ表示されます。
- 3. Transfer Mode: TFTP モードのみが選択可能です。
- 4. Server Address Type: TFTP サーバーのアドレス指定フォーマットを指定します。
 - IPv4: TFTP サーバーアドレスを x.x.x.x フォーマットで指定します。
 - DNS:TFTP サーバーをホスト名で指定します。
- 5. Server Address: TFTP サーバーの IP アドレスあるいはホスト名を Server Address Type の f-マットで指定します。
- Transfer File Path:ファイルを送信する TFTP サーバーのフォルダーパスを指定します。パスの最後にはバックスラッシュを記入してください。パス名にはスペースは使えません。ルートの場合にはブランクにしておいてください。最大 32 文字です。
- 7. Transfer File Name: ファイル名を指定します。Code の場合は"stk"としてください。最大 32 文字 です。
- 8. Start File Transfer: チェックボックスを選択します。
- 9. Apply ボタンをクリックしてファイル転送を開始します。

画面の下部にファイル転送の状態が表示されます。転送が成功あるいは失敗するまで画面 は自動的に更新されます。

スイッチから HTTP でファイルをアップロードする

NETGEAR Connect with Innovation		GS110TP 8 Port Gigabit POE Smart Switch with 2 Fiber SFP
System Switcl	ning QoS Security Monitoring Maintenan	ce Help сосоит
Reset Upload Dov	vnload File Management Troubleshooting	
> TFTP File Upload	HTTP File Upload	
v HTTP File Upload	: HTTP File Upload	0
	File Type Code Image I Image I	
		APPLY
Convright @ 1996-2015 N	ETGEAR @	APPLY

- 1. Maintenance > Upload > HTTP File Upload を選択して HTTP File Upload ページを表示し ます。
- 2. File Type:アップロードするファイルのタイプを選択します。
 - Code:コードイメージ。
 - Text Configuration: テキスト設定ファイル。
- 3. Image Name: タイプが Code の場合は、image1 か image2 かを選択します。この選択肢は Code を選択した時のみ表示されます。

- 4. Apply ボタンをクリックしてファイル転送を開始します。
- 5. ファイル保存の画面が表示されます。保存場所、名前を指定して保存をします。

image1 を開く	×
次のファイルを開こうとしています:	
🏭 image1	
ファイルの種類: application/octet-stream ファイルの場所: http://192.168.1.28	
「このファイルをどのように処理するか選んでください―――	۱ ۲
◎ プログラムで開く(<u>O</u>): 参照(<u>B</u>)	
● ファイルを保存する(S)	
今後この種類のファイルは同様に処理する(A)	
OK キャンセル	

スイッチへのファイルダウンロード(Download File To Switch)

スイッチは TFTP または HTTP でリモートシステムからのシステムファイルダウンロードをサポートしています。

Download メニューは以下の機能へのリンクを含んでいます。

- TFTP ファイルダウンロード(TFTP File Download)
- HTTP ファイルダウンロード(HTTP File Download)

TFTP ファイルダウンロード(TFTP File Download)

Download ページでデバイスソフトウェア、イメージファイル、設定ファイルおよび SSL ファイルを TFTP サーバーからスイッチへダウンロードできます。

HTTP でもダウンロードができます。

System Switching (Rosot Uplood Downlood Filk > TFTP File Download > HTTP File Download : TFTP :: TF	QoS Security Management Trouble le Download File Download	Monitoring shooting	Maintenance	Help	LOGOUT
Reset Upload Download Fil > TFTP File Download TFTP File > HTTP File Download TFTP File : TFTP	e Management Trouble le Download File Download	shooting	Ø		ļ
The Trans					
File Type Image Na Server Ac TFTP Serv Transfer I Remote F	Code image1 s Idress Type IPv4 w rer IP 0.0.0.0 File Path		×		
(۲)	Start Fi	le Transfer			

スイッチにファイルをダウンロードするには以下の条件を満たす必要があります。

- ダウンロードするファイルが TFTP サーバーのディレクトリーに存在する。
- ファイルが適切なフォーマットである。
- スイッチと TFTP サーバーが接続可能である。

TFTP サーバーからスイッチにファイルをダウンロードする

- 1. Maintenance > Download > TFTP File Download を選択して TFTP File Download ページを 表示します。
- 2. File Type:スイッチにダウンロードするファイルのタイプを指定します。
 - Code: Code は image1 および image2 という2 つのフラッシュ領域のどちらかにに保存される システム・ソフトウェアイメージです。アクティブなイメージはアクティブコピーを保存し、もうー 方はセカンドコピーを保存します。デバイスはアクティブイメージでブートし動作します。アクテ ィブイメージが破損した場合は、システムはもう一つのイメージでブートします。これはブードア ップグレード時の失敗に対する安全策です。
 - Text Configuration:テキストベースの設定ファイルはオフラインでテキストファイル(startupconfig)を編集することを可能とします。最もよく使われる方法は、動作している設定をスイッチ からアップロードして、他のスイッチ用の設定を作成して、他のスイッチにダウンロードする方 法です。
 - Boot Code:システムを自動的にブートするために使われます。ソフトウェアイメージをダウン グレードする際にブートコードをダウンロードする必要があることがあります。



スイッチと互換性のないブートコードをダウンロードすると、スイッチは利用できなく なる可能性があります。ブートコードをダウンロードする前に、ブートコードがソフト ウェアイメージバージョンと互換性があるかどうか確認してください。

- **SSL Trusted Root Certificate PEM File**: SSL Trusted Root Certificate File (PEM Encoded).
- SSL Server Certificate PEM File: SSL Server Certificate File (PEM Encoded).
- SSL DH Weak Encryption Parameter PEM File: SSL Diffie-Hellman Weak Encryption Parameter File (PEM Encoded).
- SSL DH Strong Encryption Parameter PEM File: SSL Diffie-Hellman Strong

Encryption Parameter File (PEM Encoded).

3. Image Name: Code を GS108T あるいは GS110TP にダウンロードする際には、上書きするス イッチのイメージを選択してください。File Type で Code を選択した時のみ表示されます。

メモ:アクティブイメージに上書きはしないことを推奨します。アクティブイメージに上 書きしようとするとシステムが警告メッセージを表示します。

- 4. Server Address Type: TFTP サーバーのアドレス指定フォーマットを指定します。
 - IPv4: TFTP サーバーアドレスを x.x.x.x フォーマットで指定します。
 - DNS: TFTP サーバーをホスト名で指定します。
- 5. Server Address: TFTP サーバーの IP アドレスあるいはホスト名を Server Address Type の fーマットで指定します。
- Transfer File Path:ファイルを送信する TFTP サーバーのフォルダーパスを指定します。パスの最後にはバックスラッシュを記入してください。パス名にはスペースは使えません。ルートの場合にはブランクにしておいてください。最大 32 文字です。
- 7. Remote File Name:ファイル名を指定します。最大 32 文字です。ファイル名にスペースは使えません。
- 8. Start File Transfer: チェックボックスを選択します。
- 9. Apply ボタンをクリックしてファイル転送を開始します。

画面の下部にファイル転送の状態が表示されます。転送が成功あるいは失敗するまで画面は自動的に更新されます。

スイッチにダウンロードしたソフトウェアイメージをアクティブにするには、ファイル管理を参照ください。

HTTP ファイルダウンロード(HTTP File Download)

HTTP File Download ページで様々なタイプのファイルをス HTTP セッション(Web ブラウザ)経由 でスイッチにダウンロードできます。

NETGEAR Connect with Innovation				GS110TP 8 Port Gigabit PoE Smart Switch with 2 Fiber SFP
System Switchi	ng QoS Security	Monitoring	Maintenance Help	LOGOUT
Reset Upload Down	nload File Management Trou	ubleshooting		
> TFTP File Download > HTTP File Download	HTTP File Download			
	HTTP File Download	Code		0
	Image Name Select File	image1 💌	参照	-
	NOTE: After a File transfer is st	arted, please wait till the pa	ge refreshes.	
				CANCEL

HTTP でファイルをスイッチにダウンロードする

1. Maintenance > Download > HTTP File Download を選択して HTTP File Download ページを 表示します。

- 2. File Type:スイッチにダウンロードするファイルのタイプを指定します。
 - Code: Code は image1 および image2 という2 つのフラッシュ領域のどちらかにに保存される システム・ソフトウェアイメージです。アクティブなイメージはアクティブコピーを保存し、もうー 方はセカンドコピーを保存します。デバイスはアクティブイメージでブートし動作します。アクテ ィブイメージが破損した場合は、システムはもう一つのイメージでブートします。これはブードア ップグレード時の失敗に対する安全策です。
 - Text Configuration:テキストベースの設定ファイルはオフラインでテキストファイル(startupconfig)を編集することを可能とします。最もよく使われる方法は、動作している設定をスイッチ からアップロードして、他のスイッチ用の設定を作成して、他のスイッチにダウンロードする方 法です。
 - Boot Code:システムを自動的にブートするために使われます。ソフトウェアイメージをダウン グレードする際にブートコードをダウンロードする必要があることがあります。



警告

スイッチと互換性のないブートコードをダウンロードすると、スイッチは利用できなく なる可能性があります。ブートコードをダウンロードする前に、ブートコードがソフト ウェアイメージバージョンと互換性があるかどうか確認してください。

- **SSL Trusted Root Certificate PEM File**: SSL Trusted Root Certificate File (PEM Encoded).
- SSL Server Certificate PEM File: SSL Server Certificate File (PEM Encoded).
- **SSL DH Weak Encryption Parameter PEM File**: SSL Diffie-Hellman Weak Encryption Parameter File (PEM Encoded).
- SSL DH Strong Encryption Parameter PEM File: SSL Diffie-Hellman Strong Encryption Parameter File (PEM Encoded).
- 3. Image Name: Code を GS108T あるいは GS110TP にダウンロードする際には、上書きするス イッチのイメージを選択してください。File Type で Code を選択した時のみ表示されます。

メモ:アクティブイメージに上書きはしないことを推奨します。アクティブイメージに上 書きしようとするとシステムが警告メッセージを表示します。

- 4. 参照ボタンをクリックしてダウンロードするファイルを指定します。
- 5. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。
- 6. Apply ボタンをクリックしてファイルのダウンロードを開始します。

メモ:ファイル転送が開始したら、ページが更新されるまで待ってください。ファイル選 択の表示が消えていればファイル転送は完了しています。

ファイル管理(File Management)

システムは永久記憶媒体に2つのバージョンの GS108T/GS110TP ソフトウェアを保持します。 つはアクティブイメージで、セカンドイメージはバックアップイメージです。アクティブイメージはスイ ッチの再起動後にロードされます。この機能はGS108T/GS110TP ソフトウェアをアップグレードお よびダウングレードする際に停止時間を削減します。

File Management メニューは以下のオプションへのリンクを含んでいます。

- デュアルイメージ設定(Dual Image Configuration)
- デュアルイメージ状態(Dual Image Status)

デュアルイメージ設定(Dual Image Configuration)

古いソフトウェアバージョンで動作しているシステムは新しいソフトウェアバージョンで作成された設定 ファイルを無視します。古いバージョンで動作しているシステムが新しいバージョンで作られた設定ファ イルを発見すると、システムはユーザーに対して警告を表示します。

Dual Image Configuration ページでブートイメージ設定、イメージの説明、あるいはイメージの削除を行います。

							with 2 Fiber SF
System	Switching C	QoS	Security	Monitoring	Maintenance	Help	LOGOUT
Reset Upload	Download File	e Manageme	nt Trouble	shooting			
··Dual Image	Dual Image	Configura	ation				
 Dual Image Configuration 	Dual Image	Configurat	ion		1		
» Dual Image Status	Image Name		Image	1 🗸			
	Current-active		image2				
	Image Descriptio	n	defaul	t image			
	Activate Image						
	Delete Image						
	<			1111			>

デュアルイメージ設定をする

- 1. Maintenance > File Management > Dual Image > Dual Image Configuration を選択して Dual Image Configuration ページを表示します。
- 2. Image Name: 設定するイメージを選択します。

Current-active 欄は現在アクティブなイメージを表示します。

- 3. Image Description:イメージの説明を記入します。
- 4. Active Image: 選択しているイメージをアクティブにするにはチェックボックスを選択します。

メモ:イメージをアクティブに設定した後、システムを再起動して新しいコードを動 作させる必要があります。

- 5. スイッチの永久記憶媒体からイメージを削除するには、Delete Image チェックボックスを選択します。アクティブイメージを削除することはできません。
- 6. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。
- 7. Apply ボタンをクリックして設定をスイッチに適用します。

デュアルイメージ状態(Dual Image Status)

Dual Image Status ページでデバイスのシステムイメージ状態を確認できます。

Maintenance > File Management > Dual Image > Dual Image Status を選択して Dual Image Status ペー ジを表示します。

onnect with Innovation					8 Port Gigabit	Smart Swi
System	Switching	QoS Security	Monitoring	Maintenance	Help	LOGO
Reset Upload	Download Fil	e Management Trou	bleshooting			
Dual Image	Dual Image	e Status				
» Dual Image Configuration	Dual Imag	e Status			0	
	Unit	Image1 Ver	Image2 Ver	Current-active	Next-active	
Status	1	10.26.1.32	10.28.11.23	image2	image2	
	Image2 Descrip	tion				
	<		ш			

以下に Dual Image Status ページに表示される情報の説明を示します。

項目	説明
Unit	ユニット ID.常に1。
Image1 Ver	Image1 のバージョン。
Image2 Ver	Image2 のバージョン。
Current-active	スイッチで現在アクティブなイメージ。
Next-active	次のスイッチ再起動後にアクティブになるイメージ。
Image1 Description	Image1 ファイルの説明。
Image2 Description	Image2 ファイルの説明。

Refresh:画面を最新状態に更新します。

トラブルシュート(Troubleshooting)

Troubleshooting メニューは以下の機能へのリンクを含みます。

- Ping
- Ping IPv6
- トレースルート(Traceroute)

Ping

Ping ページで IP アドレスに対して Ping を送信することができます。この機能を使って特定のホストとスイッチの接続性を確認することができます。

NETGEAR Connect with Innovation"				8 Port Gig	GS110TP gabit PoE Smart Switch with 2 Fiber SFP
System Swit	ching QoS	Security Monitoring	Maintenance	Help	LOGOUT
Reset Upload De	ownload File Mana	ement Troubleshooting			
✓ Ping> Ping IPv6	Ping				
Traceroute	Hostname / IP Ad	dress (Max 255 0	haracters/x.x.x.x)		
	Interval Size	3 (1 to 60) 0 (0 to 65507)			
	Ping				×
					CANCEL APPLY

Ping 設定をする

- 1. Maintenance > Troubleshooting > Ping を選択して Ping ページを表示します。
- 2. Hostname/IP Address: Ping 送信をしたいデバイスの IP アドレスあるいはホスト名を記入します。
- 3. 以下の設定をすることもできます。
 - Count:送信する Ping の数。1-15。
 - Interval: Pingの送信間隔(秒)。1-60。
 - Size:ICMP パケットサイズ。0-65507。
- 4. Ping:結果を表示します。
- 5. Cancel ボタンをクリックして操作を停止します。
- 6. Apply ボタンをクリックして Ping 送信を開始します。

Ping IPv6

Ping IPv6 ページで IPv6 アドレスに対して Ping IPv6 を送信することができます。この機能を使って特定のホストとスイッチの接続性を確認することができます。

GS108T/GS110TP スマートスイッチソフトウェア管理マニュアル

NETGEAR Connect with Innovation				8 Port Gigo	GS110TP abit PoE Smart Switch with 2 Fiber SFP
System Swite	ching QoS Sec	urity Monitoring	Maintenance	Help	LOGOUT
Reset Upload Do	ownload File Management	Troubleshooting			
> Ping	Ping IPv6				
 Ping IPv6 Traceroute 	·· Ping IPv6				3
	Ping	Global 💽			
	IPv6 Address/HostName		(xxxx:xxxx 255 charact	1XXXX1XXXX1XXXX1X ers)	xxxxxxxxxxx/Max
	Datagram Size	64 (48 to 2048)			
	Result				
	•				•
				C/	NCEL APPLY

Ping IPv6 設定をする

- 1. Maintenance > Troubleshooting > Ping IPv6 を選択して Ping IPv6 ページを表示します。
- 2. Ping: Global IPv6 アドレスか Link Local アドレスかを選択します。
 - Global: グローバル IPv6 アドレスに Ping します。
 - Link Local: Link Local アドレスに Ping します。
- 3. IPv6 Address/HostName: Ping 送信をしたいデバイスの IPv6 アドレスあるいはホスト名を記入します。
- 4. Datagram Size: データグラムサイズを 48-2048 バイトの範囲で設定します。
- 5. Result:結果を表示します。
- 6. Cancel ボタンをクリックして操作を停止します。
- 7. Apply ボタンをクリックして Ping 送信を開始します。

 $\mathbb{N} = \mathbb{N} = \mathbb{N} = \mathbb{N}$

Traceroute ユーティリティを使ってリモート宛先までのパケットの経路を確認することができます。

NETGEAR Connect with Innovation	GS110TF 8 Port Gigabit POE Smart Swite with 2 Fiber SF
System Swit	hing QoS Security Monitoring Maintenance Help
Reset Upload D	vnload File Management Troubleshooting
> Ping	TraceRoute
> Ping IPv6 ~ Traceroute	: Traceroute 0
	Hostname / (Max 255 Characters'x.x.x.x)
	Probes Per 3 (1 to 10) Hop
	Max TTL 30 (1 to 255)
	Init TTL 1 (0 to 255)
	Maxtail 5 (0 to 200)
	Port 33434 (1 to 65535)
	Size 0 (0 to 9192)
	TraceRoute
Convright @ 1895 2015	CANCEL APPLY

トレースルートを設定する

- 1. Maintenance > Troubleshooting > Traceroute を選択して Traceroute ページを表示します。
- 2. Hostname/IP Address: 宛先の IP アドレスまたはホスト名を指定します。
- 3. 以下の項目を設定することもできます。
 - Probes Per Hop:ホップあたりに送信する数。1-10 回。
 - MaxTTL:送出する最大の TTL。1-255 の範囲。
 - InitTTL.:送出する TTL の初期値。0-255 の範囲。
 - MaxFail:失敗可能な最大数。0-255 の範囲。
 - Interval:送出インターバル(秒)。1-60 の範囲。
 - Port: UDP の宛先ポート番号。1-65535 の範囲。
 - Size:パケットサイズ。0-9192 の範囲。
- 4. Cancel ボタンをクリックして操作を停止します。
- 5. Apply ボタンをクリックして Traceroute を開始します。結果は TraceRoute 欄に表示されます。

A.ハードウェア仕様とデフォルト設定

GS108T/ GS110TP ギガビットスマートスイッチ仕様

GS108T とGS110TP ギガビットスマートスイッチは、TCP/IP, UDP, HTTP, ICMP, TFTP, DHCP, IEEE 802.1D, IEEE 802.1p, および IEEE 802.1Q 標準に準拠しています。

GS108T 仕様

機能	仕様
インターフェース	10/100/1000 Base-T 8 ポート
PoE	PoE-Powered Device
フラッシュメモリーサイズ	16 MB
SRAM サイズとタイプ	64 MB DDR

GS110TP 仕様

機能	仕様
インターフェース	10/100/1000 Base-T 8 ポート SFP 2 ポート
PoE	ポート 1-8, IEEE 802.3af, Alternative A (MDI-X)
フラッシュメモリーサイズ	16 MB
SRAM サイズとタイプ	64 MB DDR

GS108T/GS110TP スイッチパフォーマンス

機能	仕様
スイッチング能力	ノンブロッキング、フルワイヤースピード(全パケットサイズ)
転送方式	ストア&フォワード
パケット転送速度	10M:14,880 pps/ 100M:148,810 pps/ 1G:1,488,000 pps

MAC アドレス数	4К
グリーンイーサネット	ケーブル長 10m 未満の場合の省電力 リンクダウン時の電力削減(GS110TP のみ)

GS108T/GS110TP スイッチ機能とデフォルト

ポート特性

機能	サポート単位	デフォルト
オートネゴシエーション /固定/Duplex	全ポート	Auto negotiation
Auto MDI/MDIX	N/A	有効
802.3x フローコントロール、バックプレ ッシャー	1 (システム単位)	無効
ポートミラーリング	1	無効
ポートトランキング(アグリゲーション)	4	事前設定
802.1D spanning tree	1	無効
802.1w RSTP	1	無効
802.1s spanning tree	3 インスタンス	無効
固定 802.1Q タギング	64	VID = 1 Member ports = 8 (GS108T) Member ports = 10 (GS110TP)
MAC アドレス学習	スタティックとダイナミック	ダイナミックがデフォルトで有効
PoE (GS110TP のみ)	8 ポート	有効

トラフィックコントロール

機能	サポート単位	デフォルト
ストームコントロール	全ポート	無効
ジャンボフレーム	全ポート	無効
		最大 = 9216 バイト

QoS(Quality of Service)

機能	サポート単位	デフォルト
キューの数	4	N/A
ポートベース	N/A	N/A
802.1p	1	有効
DSCP	1	無効

GS108T/GS110TP スマートスイッチソフトウェア管理マニュアル

速度制限	全ポート	無効
オートQoS	全ポート	無効

セキュリティ

機能	サポート単位	デフォルト
802.1X	全ポート	無効
MAC ACL	100 (IP ACL と共有)	全 MAC アドレス許可
IP access list	100 (MACACL と共有)	全 IP アドレス許可
パスワードアクセス管理	1	アイドルタイムアウト 5 分 Password = "password"
管理セキュリティ	1 プロファイル、20 ルール(IP アド レスでの HTTP/HTTPS/SNMP ア クセス/サブネット管理)	全 IP アドレス許可
ポート MAC ロックダウン	全ポート	無効

システム設定

機能	サポート単位	デフォルト
ブートコードアップデート	1	N/A
DHCP/固定 IP	1	DHCP 有効/192.168.0.239
デフォルトゲートウェイ	1	192.168.0.254
システム名設定	1	NULL
設定保存·復元	1	N/A
ファームウェアアップデート	1	N/A
工場初期化	1 (Web あるいはフロントボタン経由)	N/A
デュアルイメージサポート	1	有効
ファクトリーリセット	1	N/A

管理

機能	サポート単位	デフォルト
Web マルチセッション	16	有効
SNMPv1/V2c SNMP v3	最大 5 コミュニティ	有効 (read, read-write communities)
時間	1 (ローカルまたは SNTP)	ローカル時間有効
LLDP/LLDP-MED	全ポート	無効
ログ	3 (メモリー/フラッシュ/サーバー)	メモリーログ有効
MIB サポート	1	無効

GS108T/GS110TP スマートスイッチソフトウェア管理マニュアル

Smart Control Center	N/A	有効
統計	N/A	N/A

その他の機能

機能	サポート単位	デフォルト
IGMP snooping v1/v2	全ポート	無効
Configurations upload/download	1	N/A
EAPoL flooding	全ポート	無効
BPDU flooding	全ポート	無効
Static multicast groups	8	無効
Filter multicast control	1	無効

B.設定サンプル

この章では以下の機能の設定方法について記します。

- VLAN(Virtual Local Area Networks)
- ACL(Access Control Lists)

VLAN(Virtual Local Area Networks)

LAN(Local Area Network)は一般的にはブロードキャストドメインとして定義されます。同一物理セグメ ントにあるハブ、ブリッジ、またはスイッチはすべてのエンドノードデバイスを接続します。エンドノード はルーターの必要性無しにお互いに通信ができます。ルーターは LAN を結びつけ、トラフィックを適 切なポートにルーティングします。

VLAN(バーチャル LAN)は地理的な位置以外のある決まりに従ってワークステーションを位置づける ローカルエリアネットワークです。VLAN 間にトラフィックを流すためには、VLAN が異なる2つの LAN であると同じようにルーターを介する必要があります。

VLAN は、PC、サーバー、およびその他のネットワーク機器が一つのネットワークセグメントに接続されているように見えるグループです。例えば、すべてのマーケティング部門のメンバーはビルディング中に散らばっていても、一つの VLAN に割り当てられていれば、全員が同じセグメントに接続されているように資源や帯域を共有することができます。他の部門の資源はマーケティング VLAN メンバーには見えず、IT 管理者の VLAN 設定に従って特定の担当者のみがアクセス可能となります。

VLAN には数々の利点があります。

- ネットワーク分割が簡単。頻繁に連絡を取り合うメンバーを物理的な位置によらずに共通の VLAN にグループ化できます。各グループのトラフィックはほぼ VLAN の中に収まり、過剰なトラフィックを 削減し、全体のネットワークの効率を高めます。
- 管理が簡単。ノードの追加や移動、その他の変更は、ワイヤリングクローゼットでの作業のかわり に管理インターフェース経由で簡単にできます。
- パフォーマンスの増加を提供できます。VLAN はネットワーク全体でのノード間の通信とブロードキャストを制限することにより帯域を開放します。
- ネットワークセキュリティをより強固にします。VLAN はルーター経由のみで通過可能な仮想的な 壁を作ります。標準的なルーターベースのセキュリティ対策が VLAN 間のアクセス制御に利用で きます。

スイッチで受信されたパケットは以下のように処理されます。

- タグのついていないパケットがポートで受信された場合は、自動的にポートのデフォルト VLAN ID のタグがつけられます。各ポートは設定可能なデフォルト VLAN ID (デフォルトは1)が設定されて います。デフォルト VLAN ID 設定は Port PVID 設定画面で変更できます。
- タグ付きのパケットがポートに入力された場合、パケットのタグはデフォルト VLAN ID 設定によって 変更はされません。パケットはその VLAN ID に従って VLAN の処理がされます。
- 入力されたポートに VLAN ID タグで指定された VLAN のメンバーシップが設定されていない場合は、パケットは廃棄されます。
- 入力されたポートに VLAN ID タグで指定されたものと同じ VLAN メンバーシップが設定されている 場合は、同じ VLAN ID を持つポートに転送されます。
- ポートから送信されるパケットは、そのポートの VLAN メンバーシップ設定によってタグ付きあるい はタグ無しで送信されます。あるポートが U となっている場合は、ポートから出て行くパケットはタ グなしです。逆に T が付いているポートは、そのポートの VLAN ID のタグ付きのパケットが送信さ れます。

この節の例はタグ付き VLAN を理解するために様々な設定を紹介します。

VLAN サンプル設定(VLAN Example Configuration)

この例では、いくつかの VLAN の利用形態を示し、スイッチがどのようにタグ付き、タグ無しのトラフィックを扱うかを説明します。

この例では、新しい VLAN を 2 つ作成し、デフォルト VLAN 1 のポートメンバーシップを変更し、 ポートメンバーを 2 つの新しい VLAN に割り当てます。

- 1. Basic VLAN Configuration ページで、以下の VLAN を作成します。
 - ・ VLAN ID 10の VLAN
 - VLAN ID 20 の VLAN

NETGEAR Connect with Innovation					GS108T 8 Port Gigabit Smart Switch
System Switch Ports LAG VLAN	hing Void	QoS ce VLAN Au	Security Monitoring Mainte to-VoIP STP Multicast Address Table	enance Hel	Р
* Basic > VLAN Configuration	VLA	N Configu LAN Configu	ration Iration	0	×
Advanced		VLAN ID	VLAN Name	VLAN Type	
		1	Default	Static 💌 Default	
		3	Voice VLAN Auto-Video	Default Default	
		10 20	VLAN10 VLAN20	Static Static	
	:: R Rese	eset t Configuratio	n Г	0	
		gurutk	••	ADD D	ELETE CANCEL APPLY

- 2. VLAN Membership ページで以下のように VLAN メンバーシップを指定します。
 - VLAN ID 1 のデフォルト VLAN でポート 7、ポート 8 をタグ無し(U)に設定します。

> Basic	VLAN Membership											
» VLAN	: VLAN Membership											
Configuration	VLAN I	D		1 🔹			Grou	p Opera	ation	Untag All	-	
» VLAN Membership	VLAN N	lame		Defau	Default			UNTAGGED PORT MEMBERS				
» Port PVID	VLAN T	ype		Defau	lt		T,	AGGED P	ORT MEM	BERS		
Configuration	- PC	DRT										
	Port	1	2	3	4	5	6	7 U	8 U			
		~										

• VLAN ID 10 の VLAN でポート 1, ポート 2 をタグ無し(U),ポート 3 をタグあり(T)に設定します。

: VLAN	Memb	pership									
VLAN ID			10 💌]		Grou	p Opera	ation	Untag All	-	
VLA N Nar	ne		VLAN	10		UNI	ERS				
VLAN Typ	VLAN Type Static						TAGGED PORT MEMBERS				
* POR	т										
Port	1	2	3	4	5	6	7	8			
	U	U	Т								
LAG											

VLAN ID 20 の VLAN でポート 4, ポート 6 をタグ無し(U),ポート 5 をタグあり(T)に設定します。

VLAN I	D		20 💌			Grou	up Opera	ation	Untag All	-
VLAN N	ame		VLAN2	20		UN	TAGGED	PORT MEMB	ERS	
VLAN T	ype		Static			Т	AGGED F	ORT MEMBE	RS	
• PC	ORT									
Port	1	2	3	4	5	6	7	8		
				U	Т	U				

- 3. Port PVID Configuration ページで g1 と g4 に PVID を設定して、それらのポートに入力される パケットがポート VLAN ID のタグが付くようにします。
 - Port g1: PVID 10
 - Port g4: PVID 20

Basic	Port PVID Configuration										
» VLAN	:: PVID Configuration ()										
Configuration	POF	RTS LAGS	6 All		GO TO INTERFACE GO						
» VLAN Membership » Port PVID Configuration		Interface	PVID Configured (1 to 4093)	Current PVID	Acceptable Frame Types	Ingress Filtering	Port Priority (0 to 7)				
					-	•					
		g1	10	10	Admit All	Disable	0				
		g2	1	1	Admit All	Disable	0				
		g3	1	1	Admit All	Disable	0				
		g4	20	20	Admit All	Disable	0				
		g5	1	1	Admit All	Disable	0				

- 4. 以上の VLAN 設定によって、以下のような動作をします。
 - タグなしのパケットがポート1で受信された時、スイッチはVLAN ID 10のタグをつけます。パケットはポート2とポート3に転送されます。ポート2から送信されるパケットからはタグが外されて送信されます。ポート3から送信されるパケットはVLAN ID 10のタグがついたまま送信されます。
 - VLAN ID 10 のタグ付きのパケットがポート3で受信された時、パケットはポート1と2に転送されます。ポート1とポート2から送信されるパケットからはタグが外されてタブなしパケットとして送信されます。
 - タグなしのパケットがポート4で受信された時、スイッチはパケットにVLAN ID 20のタグを付けます。パケットはポート5とポート6に転送されます。ポート5から送信されるパケットはVLAN ID 20のタグがついたまま送信されます。ポート6から送信されるパケットからはタグが外されて送信されます。

ACL(Access Control Lists)

ACL は、ネットワークリソースへの望まないアクセスを防止しながら、許可されたユーザーのみが 特定のリソースへのアクセスを確保します。

ACL はトラフィックフローコントロールの提供、ルーティングアップデートの内容の制限、トラフィックタイ プの転送、ブロックの判断、およびネットワークセキュリティの提供に使われます。ACL は通常は内部 のネットワークとインターネットのような外部のネットワークの間に置かれるファイヤーウォールやルー ターに使われます。ACL は内部ネットワークの特定の部分から出入りするトラフィックを制御するため に、2 つのネットワークの間にあるルーターにも使われます。ACL のために必要なパケット処理はスイ ッチのパフォーマンスに影響を与えません。すなわち ACL 処理はワイヤースピードで実行されます。

アクセスリストは許可(permit)と拒否(deny)条件の集まるリストです。フィルタリングクライテリア (filtering criteria)として知られている、この条件の集まりがスイッチまたはルーターで処理される各 パケットに適用されます。パケットの転送と廃棄はパケットが特定のクライテリアに一致するかどう かに基づきます。

トラフィックフィルタリングは以下の2つの基本的なステップを必要とします。

1. アクセスリスト定義をする。

アクセスリスト定義はクライテリアに一致するトラフィックが転送されるか廃棄されるかを指定するルー ルを含みます。さらに、クライテリアに一致するトラフィックを特定のキューに割り当てたり、特定のポー トに転送したりすることもできます。各リストの最後にすべてを deny するルールがあります。

2. アクセスリストをインターフェースの入力方向に適用します。

GS108T /GS110TP では ACL は物理ポートと LAG に対して適用することができます。スイッチ ソフトウェアは MAC ACL と IP ACL をサポートしています。

MAC ACL サンプル設定 (MAC ACL Example Configuration)

以下の例ではセールス部門からの特定のポートからのイーサネットトラフィックを許可し、その他のトラフィックを拒否する MAC ベース ACL 作成する方法を示します。

1. MAC ACL ページで、セールス部門のための Sales_ACL という名前の ACL を作成します。

デフォルトで ACL は入力方向のトラフィックに適用されます。すなわち、スイッチはそのポートに入

	ACL Wizard	MA	CACL				
	* Basic > MAC ACL		MAC ACL				0
	» MAC Rules	Cur	rent Number of ACL	1]	
	» MAC Binding Configuration	Max	ximum ACL	100]	
	» Binding Table						
	Advanced		MAC ACL Table				(?)
			Name		Rules	Direction	
			Sales_ACL		0		
+	も ストニフ 小力を検本	1 ±-					

カされるトラフィックを検査します。

GS108T/GS110TP スマートスイッチソフトウェア管理マニュアル

- 2. MAC Rules ページで Sales_ACL のためのルールを以下の設定で作成します。
 - ID: 1
 - Action: Permit
 - Assign Queue: 0
 - Match Every: False
 - CoS: 0
 - Destination MAC: 01:02:1A:BC:DE:EF
 - Destination MAC Mask: 00:00:00:00:FF:FF
 - Source MAC: 02:02:1A:BC:DE:EF
 - Source MAC Mask: 00:00:00:FF:FF
 - VLAN ID: 2

Management Security	Access	Port Au	thentication	Traffic Contr	ol ACL								
> ACL Wizard		МА	C Rules										
* Basic * MAC ACL			Rules										
» MAC Rules		AC	L Name			Sales_	ACL	-					
» MAC Binding													
 Binding Table 			Rule Table										
Advanced			ID (1 to		Assian	Redirect	Mat	ch					
			10)	Action	Queue	Interface	Eve	ry	CoS				
		_											
		드님						-					
			1	Permit	U		Fais	e	0				
			Destinati	on MAC	Destii Mask	nation MAC		Ethe	агТуре	Кеу	EtherType User Value (0600 to	Source MAC	Source MAC M
											FFFF hex)		
										-			
			01:02:1A:	BC:DE:EF	00:00:	00:00:FF:FF						02:02:1A:BC:DE:EF	00:00:00:00:FF

3. MAC Binding Configuration ページで、Sales_ACL をインターフェース g6,g7,g8 に割り当てます。 (Apply ポタンをクリックして適用します。)

Svetom Swit	ahing O	-S So	ourity	Annitoring	Agintongaco	Help	
Management Security		t Authentiantia			Adminiendince	Therp	
Management Security		TAunenicalic					
ACL Wizard	MAC Bind	ing Config	guration				
* Basic * MAC ACL	Binding	Configurati	on				0
» MAC Rules	ACLID		Sales_ACL 💌	Direction		Inbound 💌	
» MAC Binding	Sequence N	umber	0	(0 to 4294	1967295)		
» Binding Table	Port Selection	n Table					
Advanced	• PORT						
	Port 1	2	3 4	5 6 7	8		
					· ^		
	Interfac	e Binding S	tatus				0
	Interface	Direction	ACL Type	ACL ID		Seq No	
	g6	Inbound	MAC ACL	Sales_ACL		1	
	g7	Inbound	MAC ACL	Sales_ACL		1	
	4			G-1 401		1	

既にアクセスリストがインターフェースに定義されている場合は、シーケンス番号を設定してア

クセスリスト間の順序を設定することができます。

4. MAC Binding Table はインターフェースとMAC ACL の関係を表示します。

> ACL Wizard	MAC	Binding	Table			
» MAC ACL	8 M	AC Binding	Table			(?
» MAC Rules		Interface	Direction	ACL Type	ACL ID	Seq No
» MAC Binding Configuration		g6	Inbound	MAC ACL	Sales_ACL	1
» Binding Table		g7	Inbound	MAC ACL	Sales_ACL	1
Advanced		g8	Inbound	MAC ACL	Sales_ACL	1

Sales_ACL という ACL はルールに設定されている宛先 MAC アドレスと送信元 MAC アドレスをもつイ ーサネットフレームを見つけます。さらに、フレームはセールス部門の VLAN である VLAN ID が 2 の タグ付きである必要があります。フレームの CoS 値イーサネットフレームのデフォルトの 0 である必要 があります。以上のクライテリアに一致するフレームはポート 6,7,8 の送信キュー0(デフォルト)に割り 当てられます。他のトラフィックはインターフェースで拒否されます。他のトラフィックがこれらのポート で許可されるためには、新しい許可をするルールをインターフェース 6,7,8 に追加する必要がありま す。

スタンダード IP ACL サンプル設定(Standard IP ACL Example Configuration)

以下の例で他の部門が使っているポートへのファイナンス部門からの IP トラフィックを拒否する IP ベースの ACL の作成方法を示します。

1. IP ACL ページで IP ACL ID が 1 の新しい IP ACL を作成します。

> ACL Wizard	IP ACL		
* Basic * Advanced	II IP ACL		0
» IP ACL	Current Number of ACL	1	
» IP Rules	Maximum ACL	100	
» IP Extended Rules			
» IPv6 ACL	TD ACL Table		0
» IPV6 Kules	IP ACL Table		v
» IP binding	IP ACL ID	Rules	Туре
» Binding Table			
	1	0	Basic

- 2. IP Rules ページで以下の設定で IP ACL 1 用のルールを作成します。
 - Rule ID: 1
 - Action: Deny
 - Assign Queue ID: 0 (optional: 0 is the default value)
 - Match Every: False
 - Source IP Address: 192.168.187.0
 - Source IP Mask: 255.255.255.0

3. Add ボタンをクリックします。

> ACL Wizard	IP Rules											
* Advanced	IP Rules (
» IP ACL » IP Rules	ACL	. ID	1 -									
» IP Extended Rules » IPv6 ACL		Basic AC	L Rule Table				0					
 » IPv6 Rules » IP Binding Configuration » Binding Table 		Rule ID	Action	Assign Queue Id	Match Every	Source IP Address	Source IP Mask					
			-		-							
		1	Deny	0	False	192.168.187.0	255.255.255.0					

- 4. IP Rules ページで以下の設定で IP ACL 1 用の 2 つ目のルールを作成します。
 - Rule ID: 2
 - Action: Permit
 - Match Every: True
- 5. Add ボタンをクリックします。

> ACL Wizard	IP	IP Rules										
* Advanced	IP Rules											
» IP ACL	ACL ID 1											
» IP Rules	1											
» IP Extended Rules	» IP Extended Rules											
» IPv6 ACL	Basic ACL Rule Table ()											
» IPv6 Rules » IP Binding		Rule ID	Action	Assign Queue Id	Match Every	Source IP Address	Source IP Mask					
Configuration			-	-	-							
» Binding Table		1	Deny	0	False	192.168.187.0	255.255.255.0					
		2	Permit	0	False	0.0.0.0	0.0.0.0					

6. **IP Binding Configuration** ページで ACL ID 1、sequence number 1 をインターフェース g2,g3,g4 に 割り当てます。

デフォルトで IP ACL は入力方向に適用されるので、スイッチに入力するトラフィックを検査します。

> ACL Wizard	izard IP Binding Configuration										
* Basic * Advanced	IP Binding Configuration										?
» IP ACL	ACL ID			1 -		Direction				Inbound 💌	
» IP Rules	Sequen	ce Numb	per	1			(0 to	429490	57295)		
» IP Extended Rules » IPv6 ACL	Port Selection Table										
» IPv6 Rules	* PC	RT									
» IP Binding	Port	1	2	3	4	5	6	7	8		
Configuration			×	×	×						
» Binding Table	• 🗌 LA	G									

7. Apply ボタンをクリックします。

8. IP Binding Table ページで IP ACL とインターフェースの関係を確認します。

> ACL Wizard	IP B	inding Ta	ble								
 Basic Advanced 	: IP Binding Table										
» IP ACL		Interface	Direction	ACL Type	ACL ID	Seq No					
» IP Rules » IP Extended Rules » IPv6 ACL		g2	Inbound	IP ACL	1	1					
		g3	Inbound	IP ACL	1	1					
» IPv6 Rules » IP Binding		g4	Inbound	IP ACL	1	1					
Configuration » Binding Table											

この例の IP ACL はインターフェース 2,3,4 でファイナンス部門の送信元 IP アドレスとサブネットマスク に一致するパケットを拒否します。2 つ目のルールはファイナンス部門以外のトラフィックを許可しま す。ルールの最後にすべてを拒否する暗黙ルールが存在するために、2 つ目のルールが必要となり ます。