NETGEAR®

GS716T/GS724T/GS748T
ギガビットスマートスイッチ
ソフトウェア管理マニュアル

September 2013

202-11263-01（英文参照マニュアル）

350 East Plumeria Drive

San Jose, CA 95134

USA

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。

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（http://www.netgear.com/about/regulatory/ ）を参照してください。（英語）。

製品型番	ファームウェア
GS716T-300AJS	6.3.1.11
GS724T-400AJS	6.3.1.11
GS748T-500AJS	6.3.1.11

目次

はじめに

このマニュアルは GS716T-300AJS/GS724T-400AJS/GS748T-500AJS 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。この文書では GS716T-300AJS/GS724T-400AJS/GS748T-500AJS をネットギアスイッチと呼びます。この文書の情報は断りがない限りこれらのスイッチ 3 機種に適用されます。

ネットギアスイッチを使う

この章ではネットギア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。

スイッチ管理インターフェース

ネットギアスイッチ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。ネットギアスイッチ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 ユーティリティを参照してください。

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。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参照してください。

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。詳しくは、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参照してください。

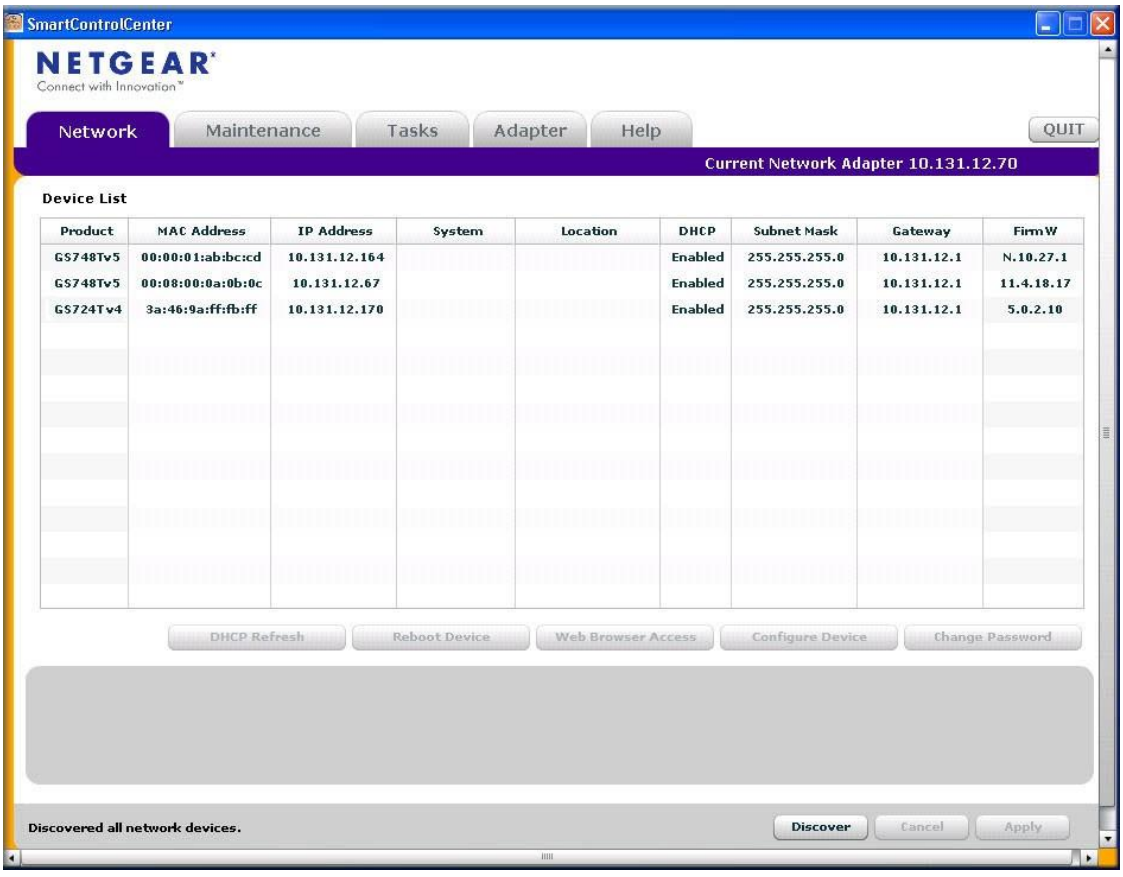
ローカルホストから接続して固定設定をする—Smart Control Center を使わずに固定アドレス設定をするには、192.168.0.0/24 のネットワークのホスト(管理システム)からスイッチに接続し、スイッチの Web 管理インターフェースを使って設定を変更できます。

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

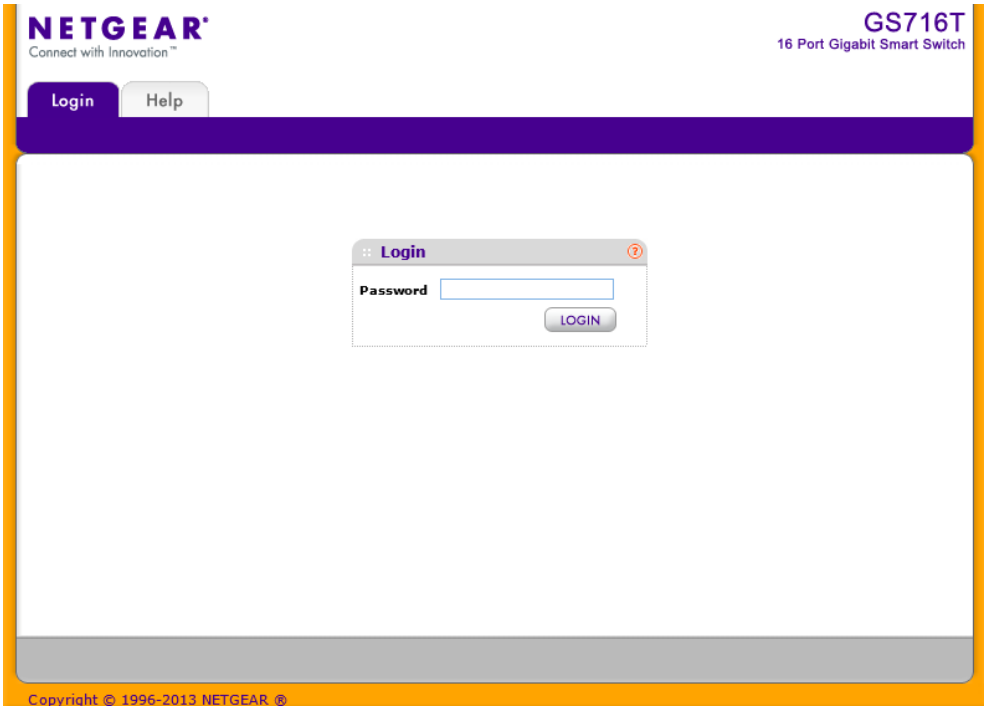
1. DHCP サーバーのあるネットワークにスイッチを接続する。
2. スイッチに電源ケーブルを接続して電源を入れます。
3. Windows コンピュータに Smart Control Center をインストールします。
4. Smart Control Center を起動します。
5. **Discover** ボタンを クリックしてスイッチを検索します。下の図のような画面が表示されます。



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）

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。
Smart Switch Control Center が Web ブラウザを起動し、Login 画面を表示します。



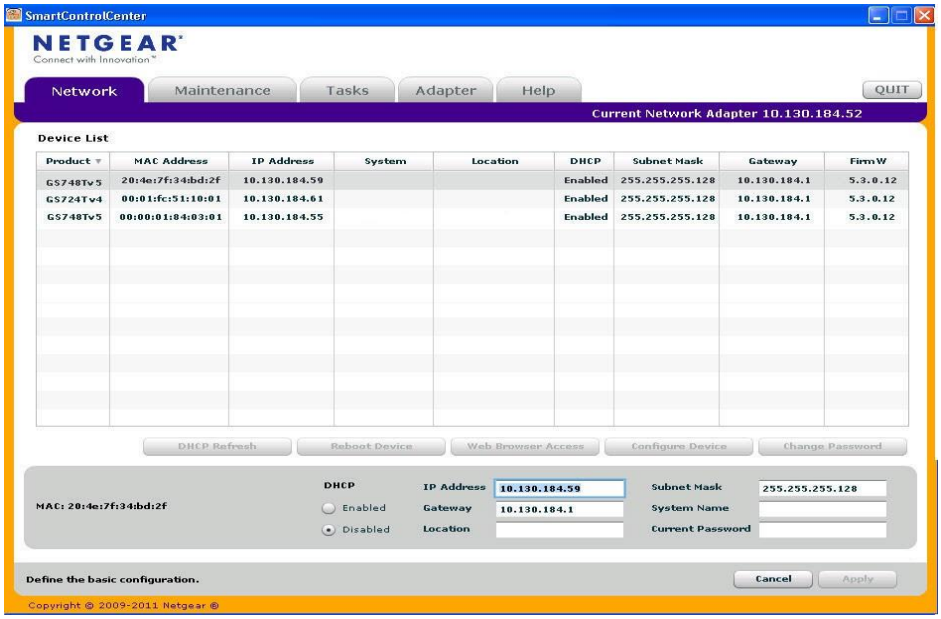
Web ブラウザを使ってスイッチを管理します。デフォルトのパスワードは **password** です。

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

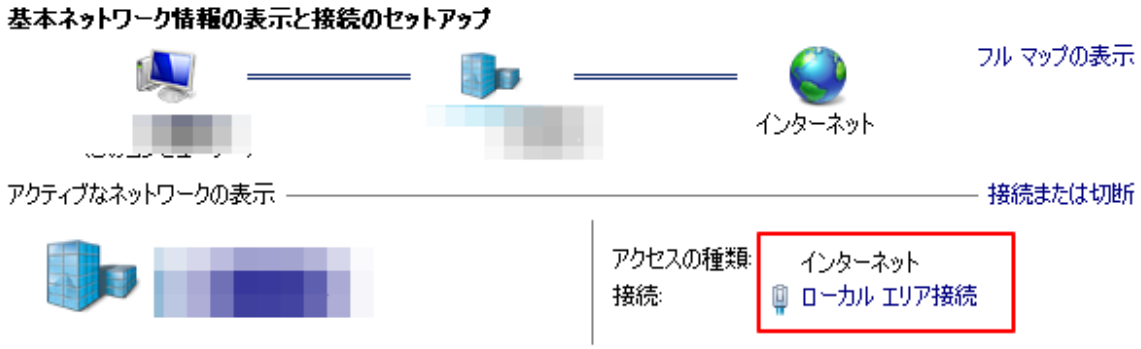
1. ネットワークにスイッチを接続します。
2. スイッチに電源コードを接続して電源を入れます。
3. Windows コンピュータに Smart Control Center をインストールします。
4. Smart Control Center を起動します。
5. **Discover** ボタンを クリックしてスイッチを検索します。**Smart Control Center** はレイヤー2 Discovery パケットをブロードキャストドメインにブロードキャストして、スイッチを発見します。
6. スイッチを選択し、**Configure Device** ボタンをクリックします。図のように画面の下の方に追加の情報を表示します。
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。
9. **Current Password** 欄にパスワードを入力します。



10. Apply ボタンをクリックしてスイッチのネットワーク設定を適用します。
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

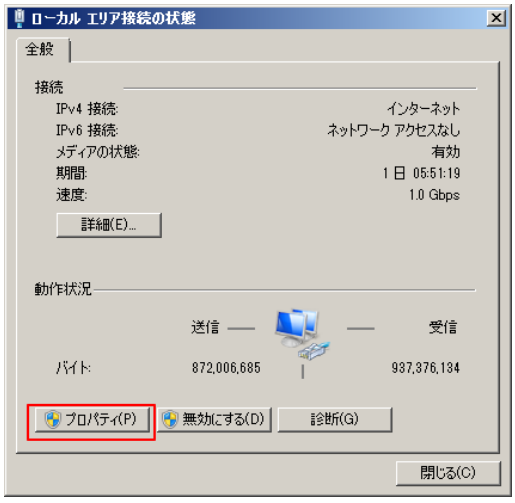
Smart Control Center を使わずにスイッチのネットワーク情報を設定するには、PC やラップトップコンピュータのような管理システムからスイッチに直接接続します。管理システムの IP アドレスはスイッチのデフォルト IP アドレスと同じサブネットにある必要があります。多くのネットワークでは、管理システムの IP アドレスをスイッチのデフォルト IP アドレス(192.168.0.239)と同じサブネットに変更することになります。



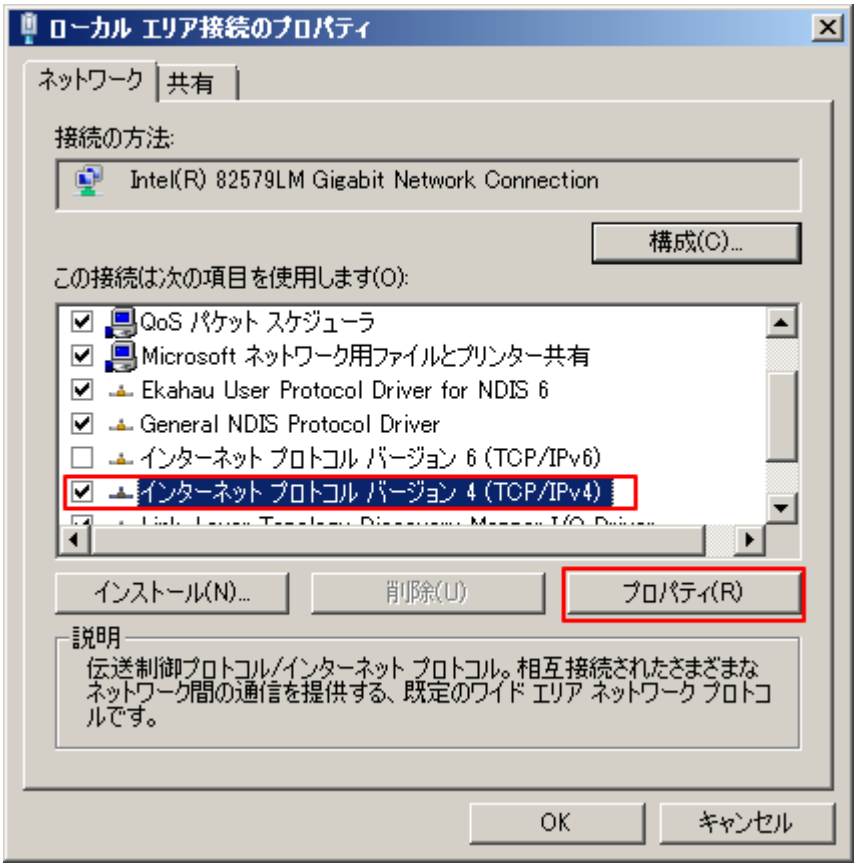
管理システムの IP アドレス設定を変更する方法はオペレーティングシステムのバージョンにより異なります。Windows で動作する管理システムの IP アドレスを変更するには、Windows の管理者権限が必要です。以下にマイクロソフト Windows 7 で動作するコンピュータの固定 IP アドレスを変更する方法を示します。

Windows で動作する管理システムのネットワーク設定を変更する

1. コントロールパネルを開き、**ネットワークと共有センター**オプションをクリックします。
2. **ローカルエリア接続**リンクをクリックします。



3. ローカルエリア接続の状態ウィンドウでプロパティボタンをクリックします。
ローカルエリア接続のプロパティウィンドウが開きます。



4. インターネット プロトコル バージョン4(TCP/IPv4)オプションを選択し、プロパティボタンをクリックします。

5. **次の IP アドレスを使う**ラジオボタンをクリックし、管理システムの IP アドレスを 192.168.0.0 ネットワーク中のアドレス、たとえば 192.168.0.200 と設定します。
IP アドレスはスイッチとは異なるアドレスである必要がありますが、スイッチと同じサブネットにある必要があります。

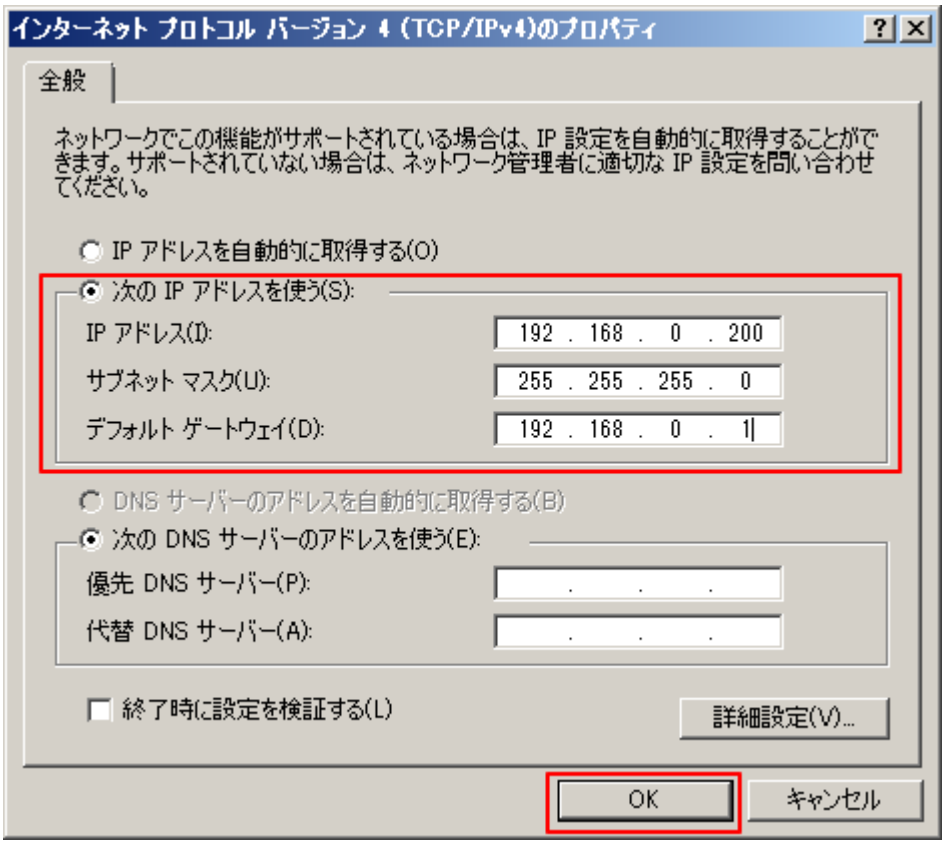
警告！
管理システムの IP アドレスを変更すると、他のネットワークへの接続が失われます。設定を変更する前に、現在のネットワークアドレス設定をメモしておいてください。

6. OK ボタンをクリックします。

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スイッチ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。

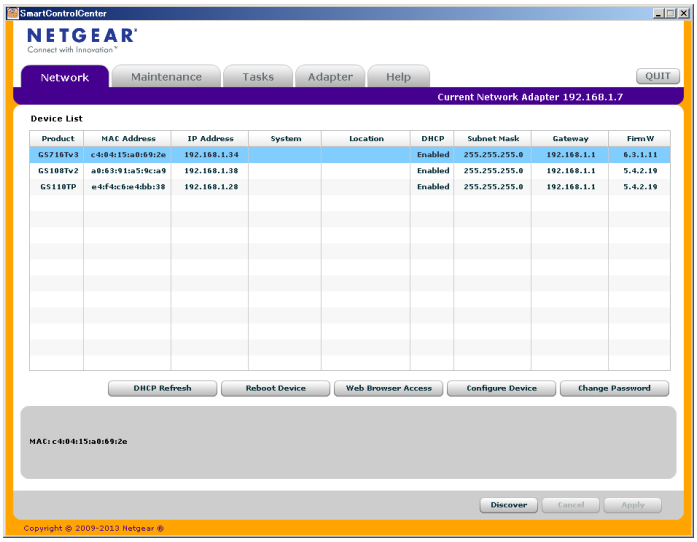


4. スイッチのネットワーク設定を変更後、管理システムのネットワーク設定を以前の設定に戻します。

Web ブラウザで管理インターフェースにアクセスする

ネットギアスイッチ の管理インターフェースにアクセスするには、以下の方法のうち一つをお使いください。:

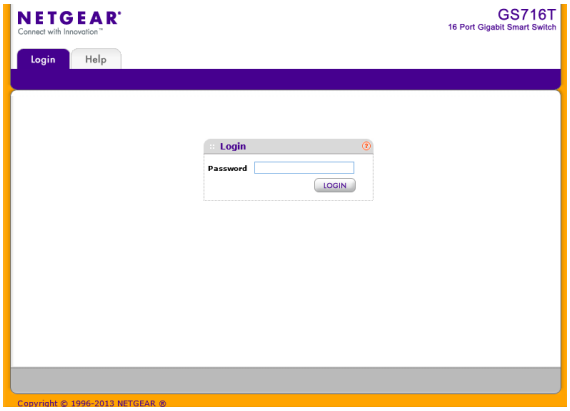
- Smart Control Center を使い、スイッチを選択して Web Browser Access ボタンをクリックする。



- 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、ネットギアスイッチの 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。



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。

このマニュアルは 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

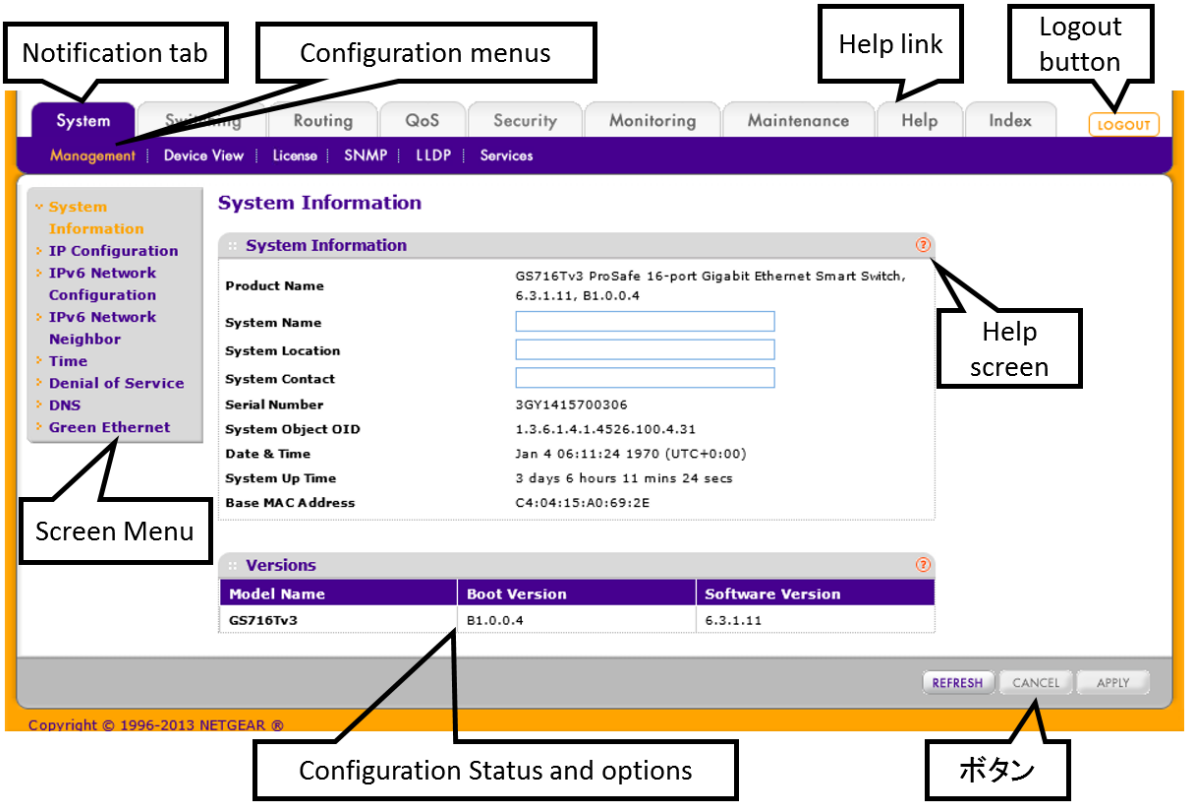
Web ブラウザを使ってスイッチにアクセスするには、ブラウザは以下のソフトウェア要素を満たす必要があります。

- 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。
   Login 画面が表示されます。
2. **Password** 欄に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。パスワードは大文字と小文字を区別します。
3. **Login** ボタンをクリックします。
4. 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。次の図がス

マートスイッチ Web インターフェース画面です。

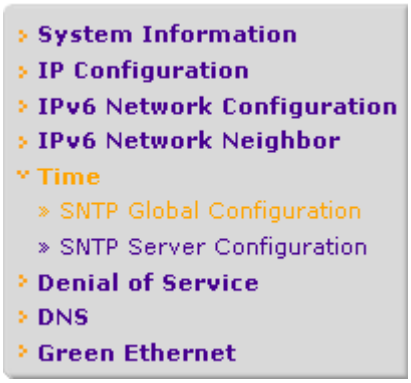


ナビゲーションタブ、設定メニューとスクリーンメニュー

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。

設定とステータスオプション（Configuration and Status Options）

設定メニューの真下とリンク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。

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ボタンを示します。

表 1 コマンドボタン

ボタン	機能
ADD	入力した情報を追加する。
APPLY	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	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	選択した項目を削除します。
REFRESH	バイスの最新の情報を表示させます。
LOGOUT	セッションを終了します。
CLEAR	すべての情報をクリアしスイッチをデフォルト設定に戻します。

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一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。

ポートの状態に応じて、Device View でのポートの色は、赤、緑、黄色または黒です。緑または黄色の場合はポートが有効です。赤の場合はポートでエラーが発生しているか、無効にされているかです。黒の場合は、リンクが存在しません。

リンクが存在する場合、Device View のポートの色は緑または黄色です。

緑のときはリンク速度が 1Gbps（1000Mbps）です。

黄色の時はリンク速度が 10M または 100Mbps です。

メモ：SFP ポートの速度は 1000Mbps(1Gbps)のみです。

システム LED はフロントパネルの左側にあります。

電源/ステータス LED(Power/Status LED)

Power LED は 2 色の LED で電源表示とその診断状態を示します。

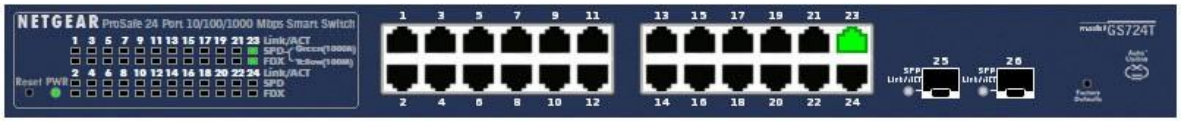
- **緑点灯**：スイッチに電源が供給され、正常状態。
- **黄色点灯**：起動途中
- **消灯**：電源が供給されていない。

ファンステータス LED（FAN Status LED）

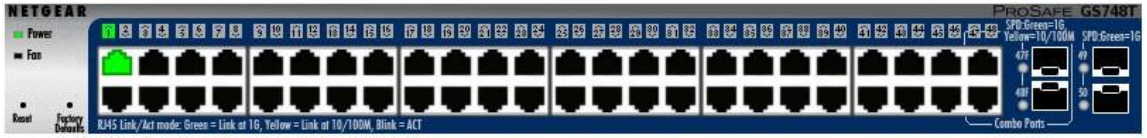
- **黄色点灯**：ファン故障。
- **消灯**：ファン正常。

GS716T の Device View

GS724T の Device View



GS748T の Device View



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。

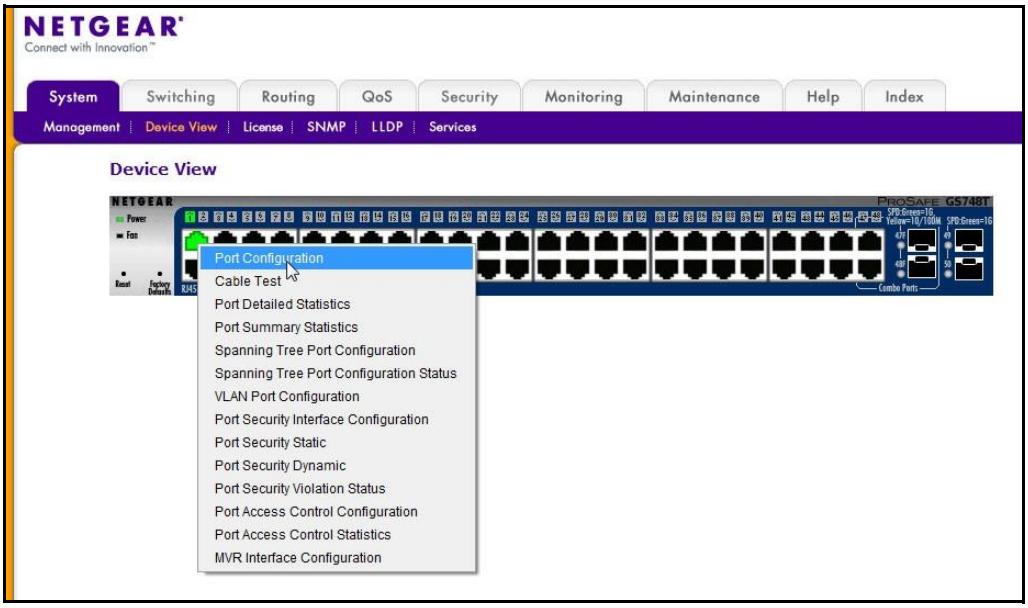


図 5. Device View Port Menu

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。

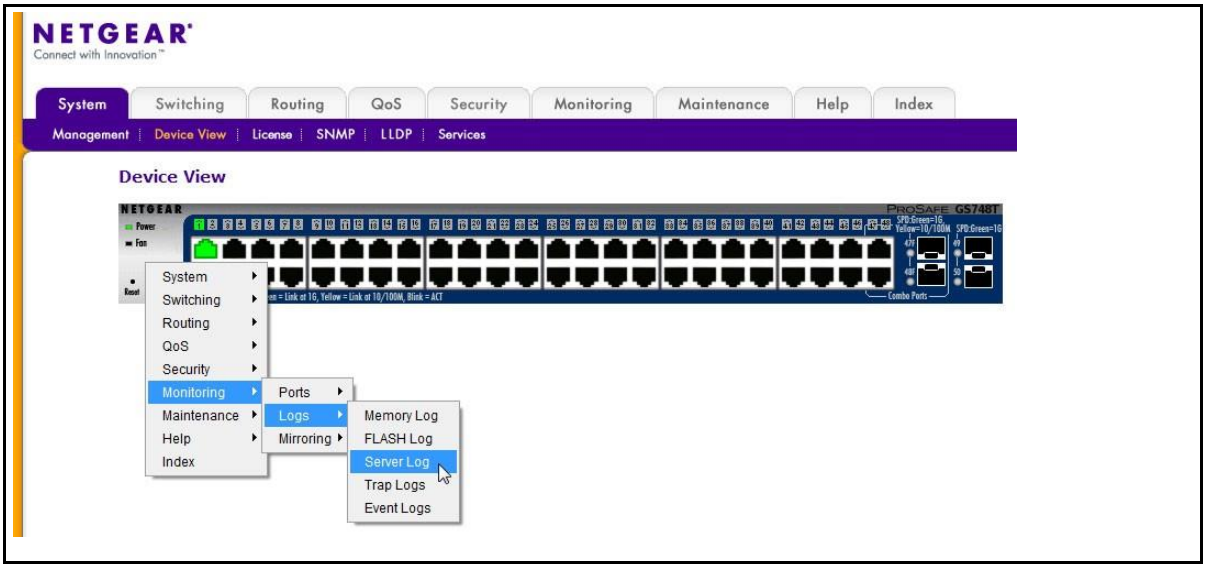


図 6. Device View Main Menu

Help Access

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  があります。

ユーザー定義フィールド(User-Defined Fields)

ユーザーが定義可能なフィールドは断りがない限り 1-159 文字まで入力可能です。以下の文字を除くすべての英数字と特殊文字が使用可能です。

表 2.使用出来ない文字

文字	定義
¥	Backslash
/	Forward slash
*	Asterisk
?	Question mark
<	Less than
>	Greater than
|	Pipe

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。すべての物理ポートは以下のとおりです。

1. **GS716T**:.ポート 1-16 はギガビットのメタルポートです。ポート 17-18 はギガビット SFP ポートです。
2. **GS724T**:ポート 1-24 はギガビットのメタルポートです。ポート 25-26 はギガビット SFP ポートです。
3. **GS748T**:ポート 1-46 はギガビットのメタルポートです。47-48 はコンボポートでメタルまたは SFP ポートして使用出来ます。

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できます。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。

表 3 インターフェース命名規則

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。	l1, l2, l3 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

インターフェース設定

いくつかの機能でインターフェース設定をします。同じ設定を同時に以下のものに対して設定することができます。

- 一つのポート
- 複数のポート
- すべてのポート
- 一つの LAG
- 複数の LAG
- すべての LAG
- 複数のポートと LAG
- すべてのポートと LAG

多くの画面ですべてのポート、すべての LAG、およびすべてのポートと LAG を設定、表示をすることができます。

図 7. Links to Display Interfaces

以下のリンクを使います。

1：すべてのポートを表示します。

LAGS：すべての LAG を表示します。

All：すべてのポートと LAG を表示します。

このセクションでは設定するポートと LAG の選択方法を示します。

Go To Interface 欄を使って一つのポートを設定する

1. 画面にすべてのポートが表示されていることを確認します。
2. **Go To Interface**：ポート番号を入力します。（例：g4）
3. **Go** ボタンをクリックします。
   関連するインターフェースのチェックボックスが選択され、その行がハイライトされます。

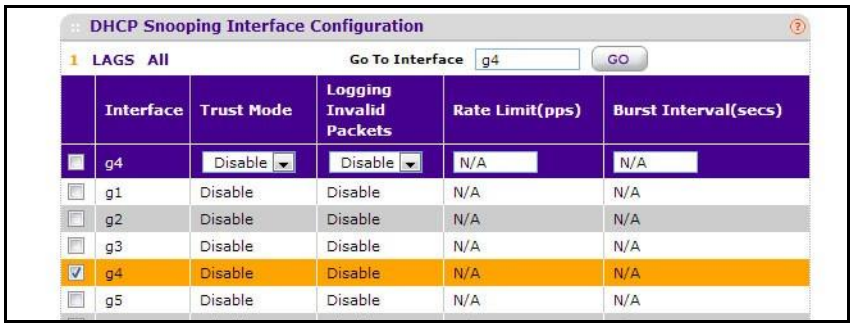
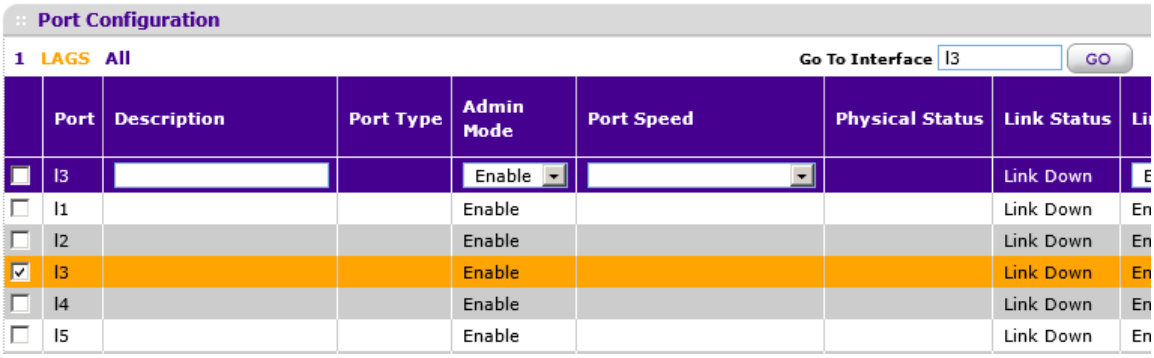


図 8. Go To Interface

4. 設定をします。
5. **Apply** ボタンをクリックします。
   選択したインターフェースに設定が適用されます。

Go To Interface 欄を使って一つの LAG を設定する

1. **LAGS** または **All** リンクをクリックして LAG を表示します。
2. **Go To Interface**：LAG 番号を入力します。（例：l3）
3. **Go** ボタンをクリックします。



関連するインターフェースのチェックボックスが選択され、その行がハイライトされます。

4. 設定をします。
5. **Apply** ボタンをクリックします。
   選択したインターフェースに設定が適用されます。

一つのポートを設定する

1. 画面にすべてのポートが表示されていることを確認します。
2. 設定をするポートのチェックボックスを選択します。
   選択した行がハイライトされます。

3. 設定をします。
4. Apply ボタンをクリックします。
   選択したインターフェースに設定が適用されます。

一つの LAG を設定する

1. LAGS または All リンクをクリックして LAG を表示します。
2. 設定する LAG を選択します。
   関連するインターフェースのチェックボックスが選択され、その行がハイライトされます。
3. 設定をします。
4. Apply ボタンをクリックします。
   選択したインターフェースに設定が適用されます。

複数のポートを設定する

1. 画面にすべてのポートが表示されていることを確認します。
2. 設定をするポートのチェックボックスを選択します。
   選択した行がハイライトされます。

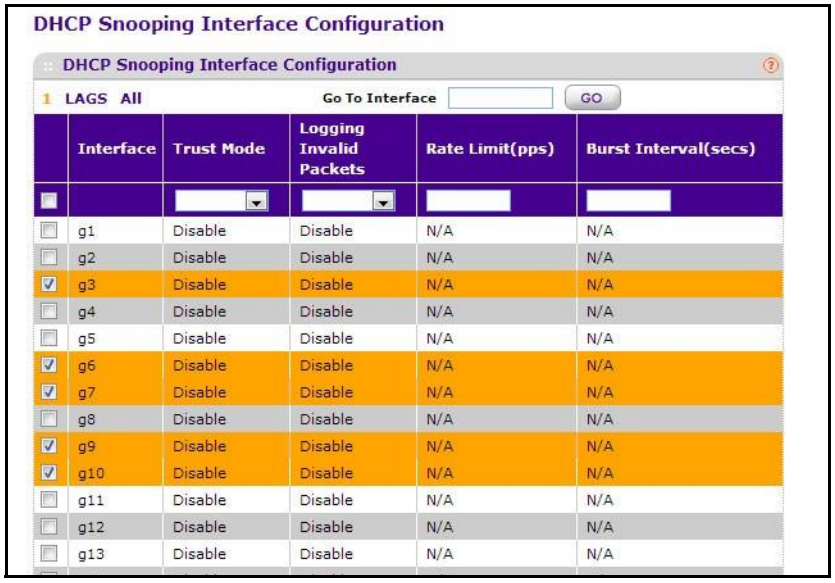


図 9. Select multiple ports

3. 設定をします。
4. Apply ボタンをクリックします。
   選択したインターフェースに設定が適用されます。

複数の LAG を設定する

1. LAGS または All リンクをクリックして LAG を表示します。
2. 設定する LAG を選択します。
   関連するインターフェースのチェックボックスが選択され、その行がハイライトされます。
3. 設定をします。
4. Apply ボタンをクリックします。
   選択したインターフェースに設定が適用されます。

すべてのポートを設定する

1. 画面にすべてのポートが表示されていることを確認します。
2. 一番上のチェックボックスを選択します。
   すべてのポートのチェックボックスが選択され、すべての行がハイライトされます。

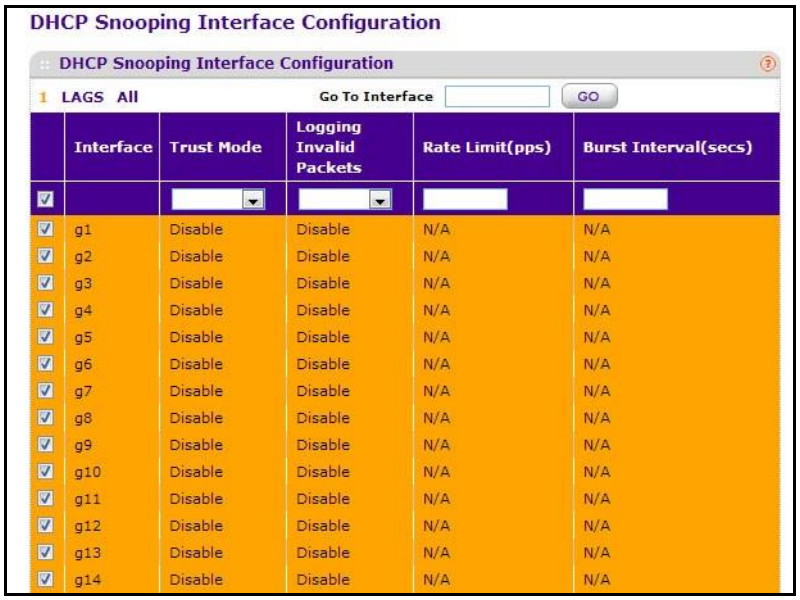


図 10. Select all ports

3. 設定をします。
4. Apply ボタンをクリックします。
   選択したインターフェースに設定が適用されます。

すべての LAG を設定する

1. LAGS リンクをクリックして LAG のみを表示します。
2. 一番上のチェックボックスを選択します。

すべての LAG のチェックボックスが選択され、すべての行がハイライトされます。

3. 設定をします。
4. Apply ボタンをクリックします。
   選択したインターフェースに設定が適用されます。

複数のポートと LAG を設定する

1. All リンクをクリックしてすべてのポートと LAG を表示します。
2. 設定するポートと LAG を選択します。
   関連するインターフェースのチェックボックスが選択され、その行がハイライトされます。
3. 設定をします。
4. Apply ボタンをクリックします。
   選択したインターフェースに設定が適用されます。

すべてのポートと LAG を設定する

1. All リンクをクリックしてすべてのポートと LAG を表示します。
2. 一番上のチェックボックスを選択します。
   すべてのポートと LAG のチェックボックスが選択され、すべての行がハイライトされます。
3. 設定をします。
4. Apply ボタンをクリックします。
   選択したインターフェースに設定が適用されます。

システム情報設定

System ナビゲーションタブの機能を使ってスイッチと環境との関係を定義します。

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、管理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。

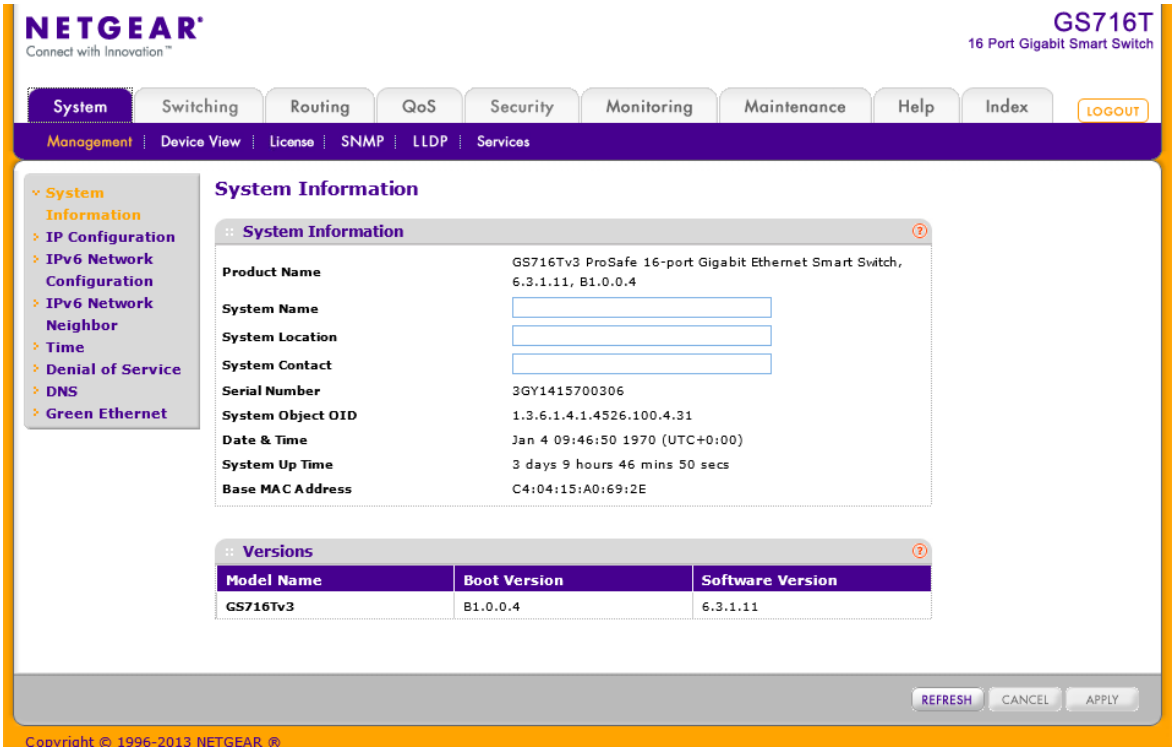
システム情報(System Information)

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。

システム情報を設定する

1. System > Management > System Information を選択して System Information ページを表示します。
2. 以下の項目を記入します。
   - 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。
   - 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。
   - 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。



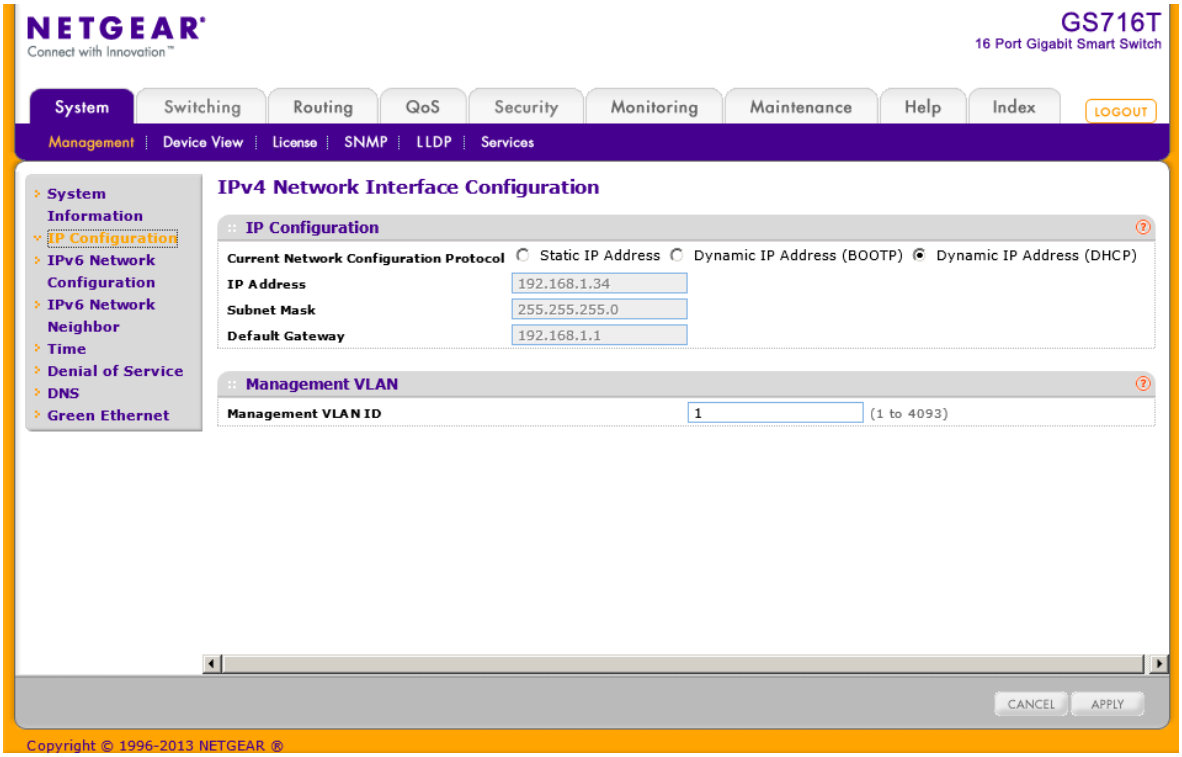
項目	説明
Product Name	スイッチの製品名
Serial Number	スイッチのシリアル番号
System Object ID	スイッチのエンタープライズ MIB のベースオブジェクト ID
Date & Time	現在の日時
System Up Time	再起動時からの稼働時間
Base MAC Address	システムの MAC アドレス
Fan Status	ファンの状態。(OK/Failure/Not Present)
Model Name	スイッチのモデル名
Boot Version	スイッチのブートコードバージョン
Software Version	スイッチのソフトウェアバージョン

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。

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 サーバーからスイッチの 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。

   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. 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。
6. 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。
7. キャンセルする場合は **Cancel** ボタンをクリックします。

IPv6 ネットワーク設定（IPv6 Network Configuration）

IPv6Network Configuration 画面を使い、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。

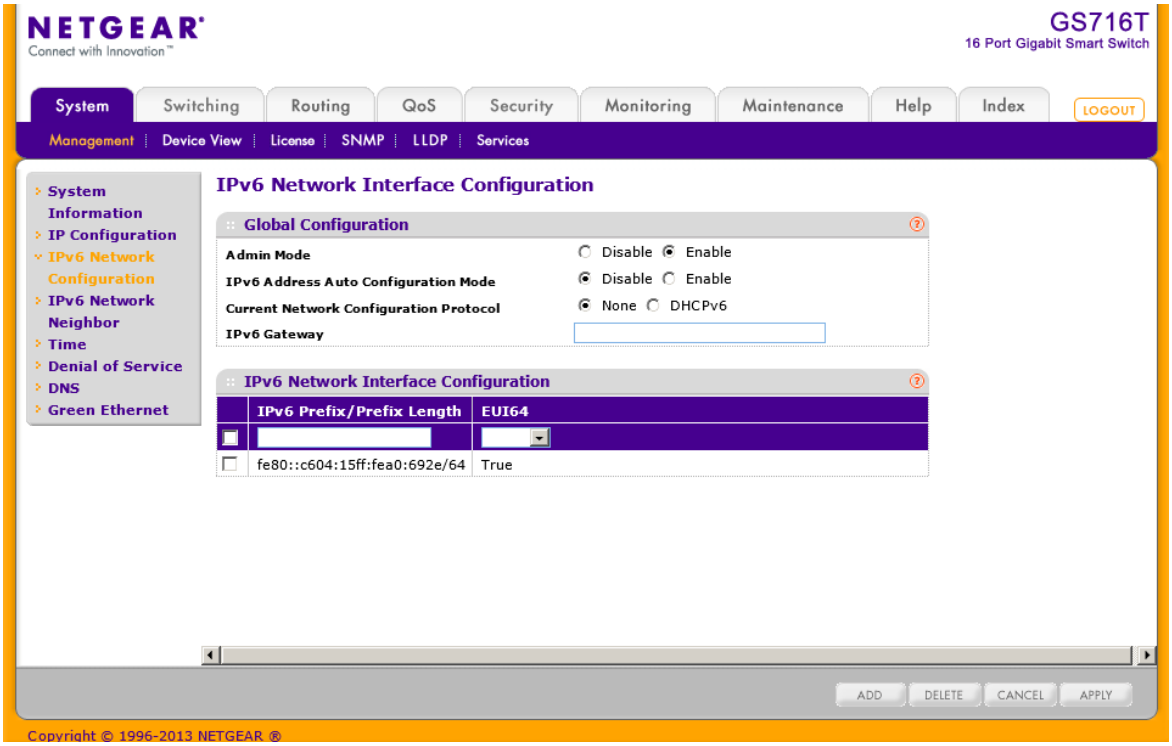
IPv6 ネットワークを介してスイッチにアクセスするには、最初にスイッチに IPV6 情報（IPv6 prefix, prefix length, default gateway）を設定する必要があります。IPv6 は以下のオプションで設定できます。

- IPv6 auto configuration
- DHCPv6

インバンド接続が確立された時、IPv6 情報が SNMP ベースの管理あるいは Web ベースの管理を使って変更することができます。

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。



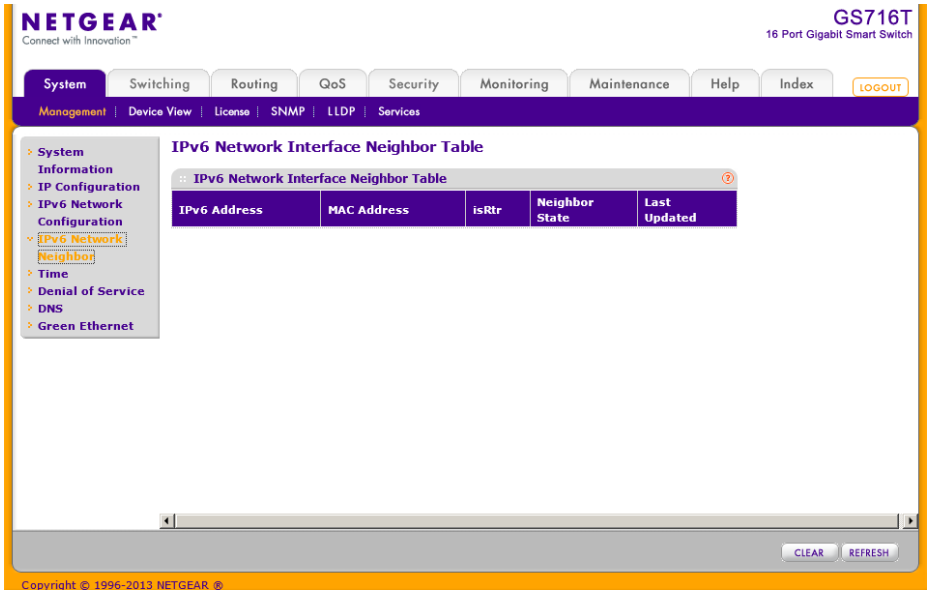
2. **Admin Mode**：有効（Enable）を選択します。
3. スイッチがどのようにして IPv6 アドレスを取得するか決定します。
   - **IPv6 Address Auto Configuration Mode**：このモードを有効（**Enable**）にすると、IPv6 アドレスを IPv6 NDP(Neighbor Discovery Protocol)およびルーターアドバータイズメントメッセージの使用で取得します。
     このモードを無効にすると、ネットワークインターフェースはネイティブの IPv6 Auto Configuration 機能を使って IPv6 アドレスの取得を行いません。DHCPv6 がスイッチのどの管理インターフェースでも有効になっていない時に限って Auto configuration を有効にできます。
   - **DHCPv6**：スイッチは DHCPv6 サーバーから IPv6 アドレスの取得を試みます。**None** を選択すると DHCPv6 クライアントをネットワークインターフェースで無効にします。
     DHCPv6 が有効になると、DHCPv6 サーバーにメッセージを送信する際に DHCPv6 Client NUID フィールドで DHCPv6 クライアントが使う client identifier を表示します。
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。

ゲートウェイのアドレスは、IPv6 グローバルまたはリンクローカルアドレスフォーマットのどちらかです。

6. （オプション）管理インターフェースに固定 IPv6 アドレスを設定することができます。
   a. **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。
   b. **EUI64**:EUI(Extended Universal Identifier)フラグを有効にするには **True** を選択します。
   c. **Add** ボタンをクリックします。
   d. **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 Network Neighbor

IPv6 Network Neighbor ページを使い、スイッチが NDP(Neighbor Discovery Protocol)を使って発見した IPv6 の近隣情報を確認することができます。



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。

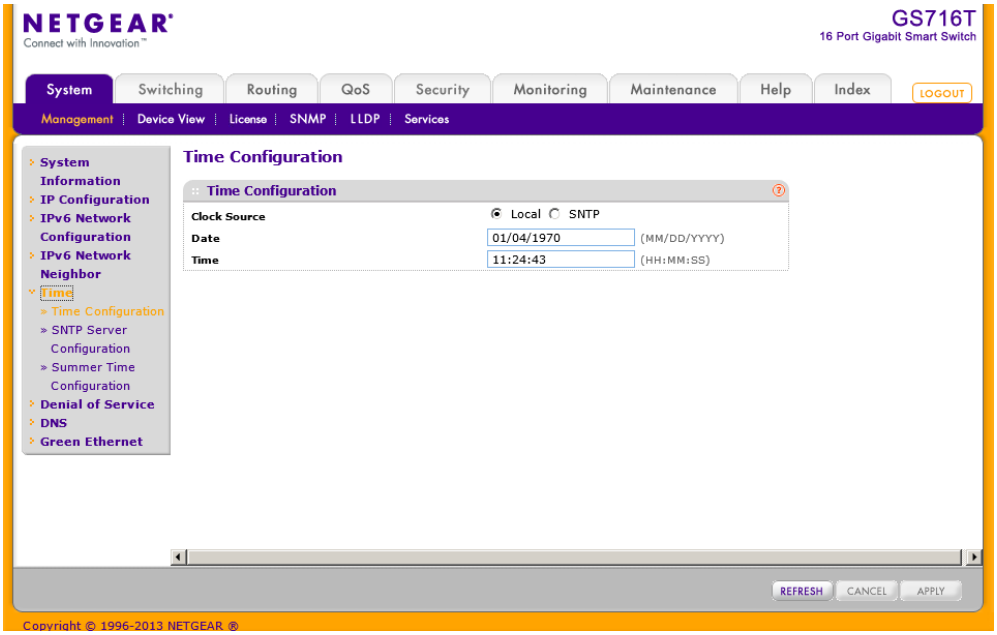
デバイスは自発的に要求、あるいは定期的にポーリング要求をして得られた情報を使って同期情報を取得します。

時間設定（Time Configuration）

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

スイッチの時間をクロックソースとして使う

1. **System** > **Management** > **Time** > **Time Configuration** を選択して **Time Configuration** ページを表示します。



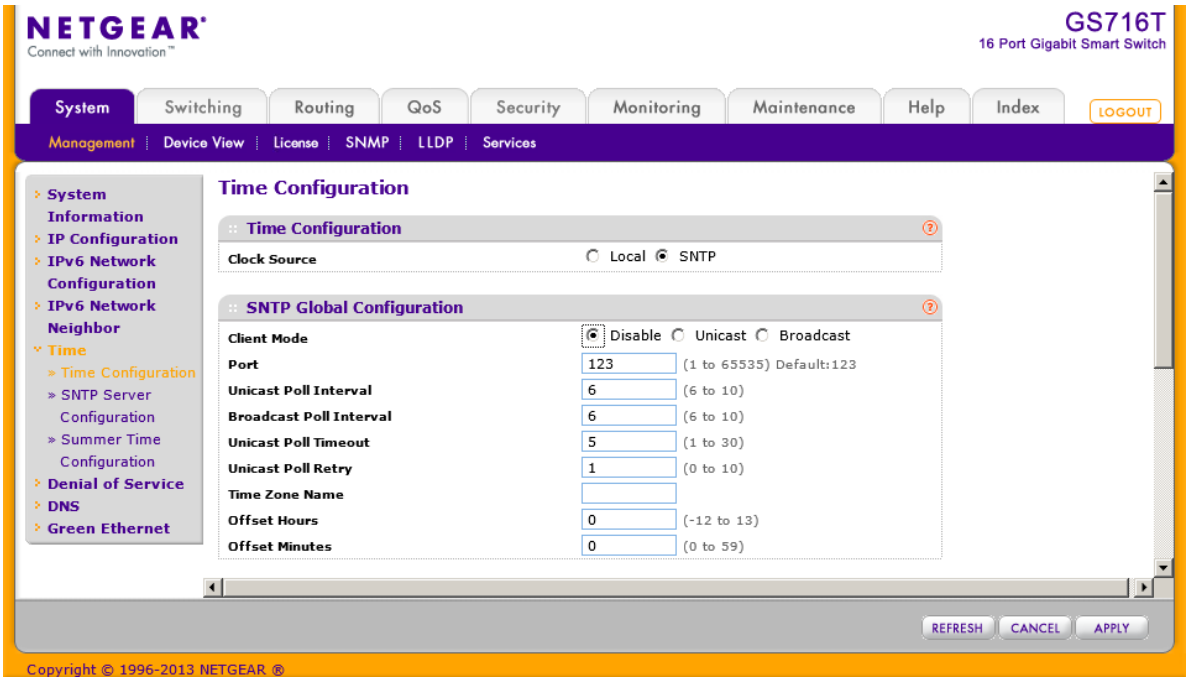
2. **Clock Source**: Local を選択します。
3. **Date**: DD/MM/YYYY 形式で年月日を記入します。
4. **Time**: HH:MM:SS 形式で時間を記入します。

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。

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

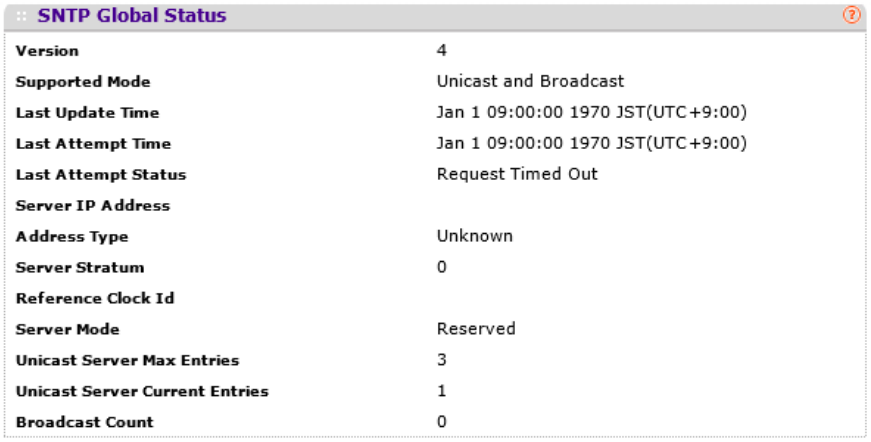
1. System > Management > Time > Time Configuration を選択して Time Configuration ページを表示します。
2. Clock Source 欄で SNTP.を選択します。
   Clock Source(時間基準)を SNTP に設定すると、追加の設定画面が表示されます。



3. Client Mode：SNTP クライアントのモードを選択します。
   - Disable：SNTP は動作していません。（デフォルト）
   - Unicast：SNTP がポイント-ポイントで動作します。クライアントはサーバーのユニキャストアドレス宛に要求メッセージを送信し応答メッセージを受信し、時間、往復時間、ローカル時間オフセット等を決定します。
   - Broadcast：ブロードキャストアドレスを使います。ブロードキャストアドレスは一つのサブネットで動作します。
4. Port：SNTP クライアントが使う UDP ポート番号。(1-65535)デフォルトは 123。
5. Unicast Poll Interval：ユニキャストの問い合わせ間隔。（6-10 秒）デフォルトは 6 秒。
6. Broadcast Poll Interval：ブロードキャストの問い合わせ間隔。（6-10 秒）デフォルトは 6 秒。

7. **Unicast Poll Timeout**：ユニキャストのタイムアウト時間。(0-30 秒)デフォルトは 5 秒。
8. **Unicast Poll Retry**：ユニキャストの再送回数。(0-10 回)デフォルトは 1 回。
9. **Time Zone Name**：タイムゾーン名を記入します。デフォルトは UTC.。
10. **Offset Hours**：UTC との時間差。(-12 から 13 まで)デフォルトは 0
11. **Offset Minutes**：UTC との時間差(分)(0-59)デフォルトは 0 分。
12. **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。
13. **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。
14. **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。
以下の表は SNTP Global Status の項目について記します。



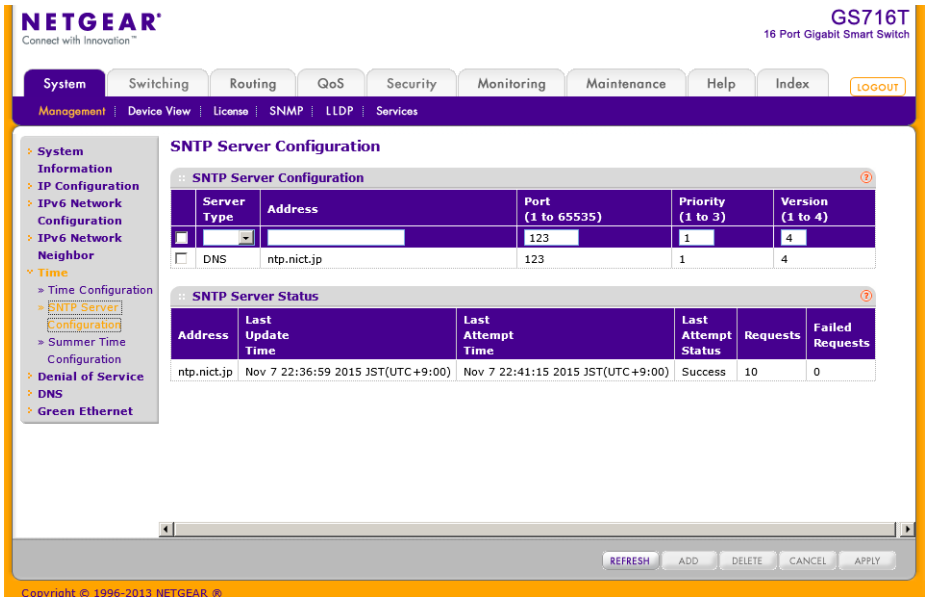
項目	説明
Version	クライアントのサポートする SNTP バージョン。
Supported Mode	クライアントのサポートする SNTP バージョン。複数のモードがサポートされる場合もあります。
Last Update Time	SNTP クライアントの最新のシステムクロック更新時間。
Last Attempt Time	最新の SNTP 要求メッセージの送信あるいは応答メッセージの受信時間。

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。 • **Version Not Supported**: SNTP サーバーのバージョンがクライアントのサポートしているバージョンに一致しない。 • **Server Unsynchronized**: SNTP サーバーはピアと同期していません。これは SNTP メッセージの'leap indicator'で表示されます。 • **Server Kiss Of Death**: SNTP サーバーが要求を受信しないことを示しています。サーバーから受信したメッセージの stratum フィールドを 0 にすることで表現されます。
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。



新しい SNTP サーバーを設定する

1. System > Management > Time > SNTP Server Configuration を選択して SNTP Server Configuration ページを表示します。
2. 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。IPv4 アドレス(IPv4) 、IPv6 アドレス(IPv6)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。デフォルト値は 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。
3. Add.をクリックして SNTP サーバー設定を追加します。
4. 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。
5. 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。

6. 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。
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。

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。

Address	Last Update Time	Last Attempt Time	Last Attempt Status	Requests	Failed Requests
ntp.nict.jp	Nov 7 22:36:59 2015 JST(UTC+9:00)	Nov 7 22:48:43 2015 JST(UTC+9:00)	Success	17	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。 • **Version Not Supported**: SNTP サーバーのバージョンがクライアントのサポートしているバージョンに一致しない。 • **Server Unsynchronized**: SNTP サーバーはピアと同期していません。これは SNTP メッセージの'leap indicator'で表示されます。 • **Server Kiss Of Death**: SNTP サーバーが要求を受信しないことを示しています。サーバーから受信したメッセージの stratum フィールドを 0 にすることで表現されます。
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。

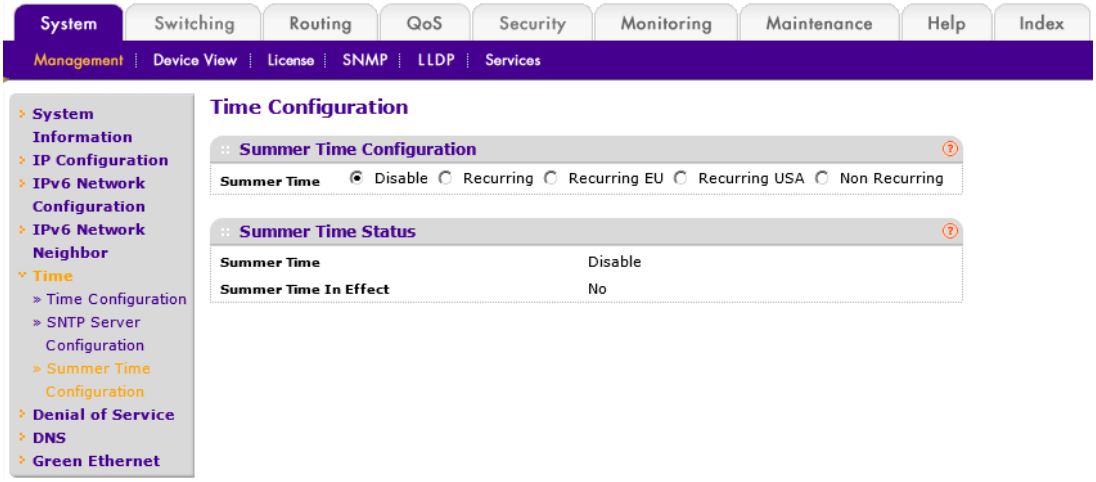
Refresh ボタンをクリックしてページの表示情報を最新に更新します。

サマータイム設定（Summer Time Configuration）

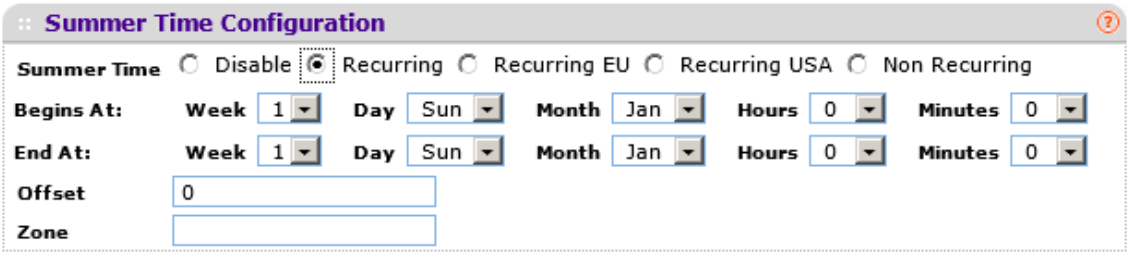
Summer Time Configuration 画面を使ってサマータイム設定をします。デイライトセービングタイムとも呼ばれます。

サマータイム設定をする

1. **System** > **Management** > **Time** > **Summer Time Configuration** を選択して **Summer Time Configuration** ページを表示します。



2. Summer Time 設定を以下の中から選択します。
   - Recurring：サマータイムの開始日と終了日が毎年同じ場合に選択します。
   - Recurring EU：EU でのサマータイムで使用します。
   - Recurring USA：USA（アメリカ合衆国）でのサマータイムで使用します。
   - Non Recurring：サマータイムの開始日と終了日を一度だけ設定する場合。翌年には再設定が必要です。
3. Summer Time の設定が Recurring、Non Recurring の場合は開始日と終了日を設定します。
   - Begins At：開始日を設定します。
   - Ends At：終了日を設定します。



4. Offset：サマータイムで変更する時間を分単位で設定します。
5. Zone：タイムゾーンを記入します。（JST 等）
6. Apply ボタンをクリックします。

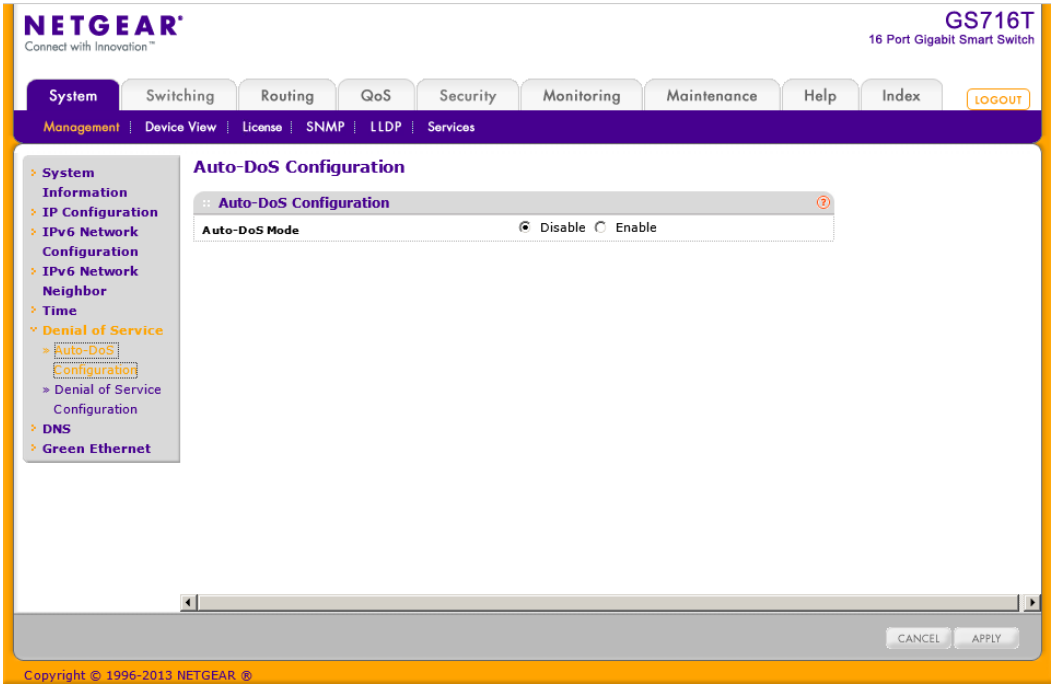
   Summer Time Status 欄はサマータイムの設定と状態を示します。

DoS(Denial of Service)

DoS(Denial of Service)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。

自動 DoS 設定(Configure Auto-DoS)

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。



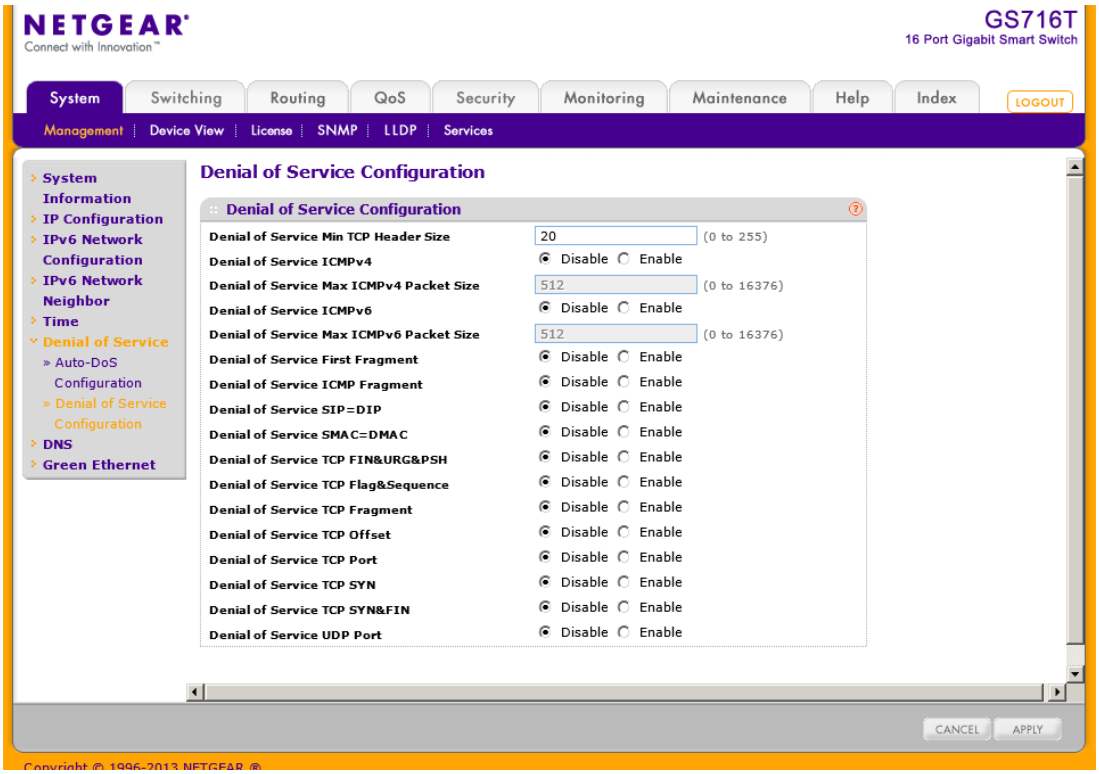
Auto-DoS 機能を設定する

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。攻撃が検知された場合、警告メッセージがログに記録され、Syslog サーバーに送信されます。同時に、ポートは無効にされ、管理者はポートを有効にすることができます。
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。
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(Denial of Service Configuration)

Denial of Service 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。



DoS 設定をする

1. System > Management > Denial of Service > Denial of Service Configuration をクリックして Denial of Service 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 Min TCP Header Size**:最小 TCP ヘッダーサイズを指定します。DoS TCP 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 ICMPv4**:ICMPv4 packet size よりも大きなサイズの ICMPv4 Ping (ECHO_REQ)パケットを廃棄します。デフォルトは無効(Disabled)です。
   - **Denial of Service Max ICMPv4 Packet Size**:最大の ICMPv4 パケットサイズを指定します。(0-16376 バイト)デフォルトは 512 バイトです。
   - **Denial of Service ICMPv6**:ICMPv6 packet size よりも大きなサイズの ICMPv6 Ping (ECHO_REQ)パケットを廃棄します。デフォルトは無効(Disabled)です。

- **Denial of Service Max ICMPv6 Packet Size**：最大の ICMPv6 パケットサイズを指定します。(0-16376 バイト)デフォルトは 512 バイトです。
- **Denial of Service First Fragment**：最初のフラグメント IP パケットの DoS オプションを確認します。それ以外をスイッチは無視します。
- **Denial of Service ICMP Fragment.**：フラグメントした ICMP パケットを廃棄します。
- **Denial of Service SIP=DIP**：送信元 IP アドレスと宛先 IP アドレスが同じパケットを廃棄します。
- **Denial of Service SMAC=DMAC**：送信元 MAC アドレスと宛先 MAC アドレスが同じパケットを廃棄します。
- **Denial of Service TCP FIN&URG&PSH**：TCP Flags FIN, URG, and PSH set and TCP sequence number equal to 0 のパケットを廃棄します。
- **Denial of Service TCP Flag&Sequence**：TCP control flags set to 0 and TCP sequence number set to 0 のパケットを廃棄します。
- **Denial of Service TCP Fragment**：TCP ヘッダーサイズが規定より短いパケットを廃棄します。
- **Denial of Service TCP Offset**：TCP ヘッダーオフセットが 1 のパケットを廃棄します。
- **Denial of Service TCP Port**：TCP 送信元ポートと TCP 宛先ポートが同じパケットを廃棄します。
- **Denial of Service TCP SYN**：TCP フラグで SYN が設定されているパケットを廃棄します。
- **Denial of Service TCP SYN&FIN**：TCP フラグで SYN と FIN が設定されているパケットを廃棄します。

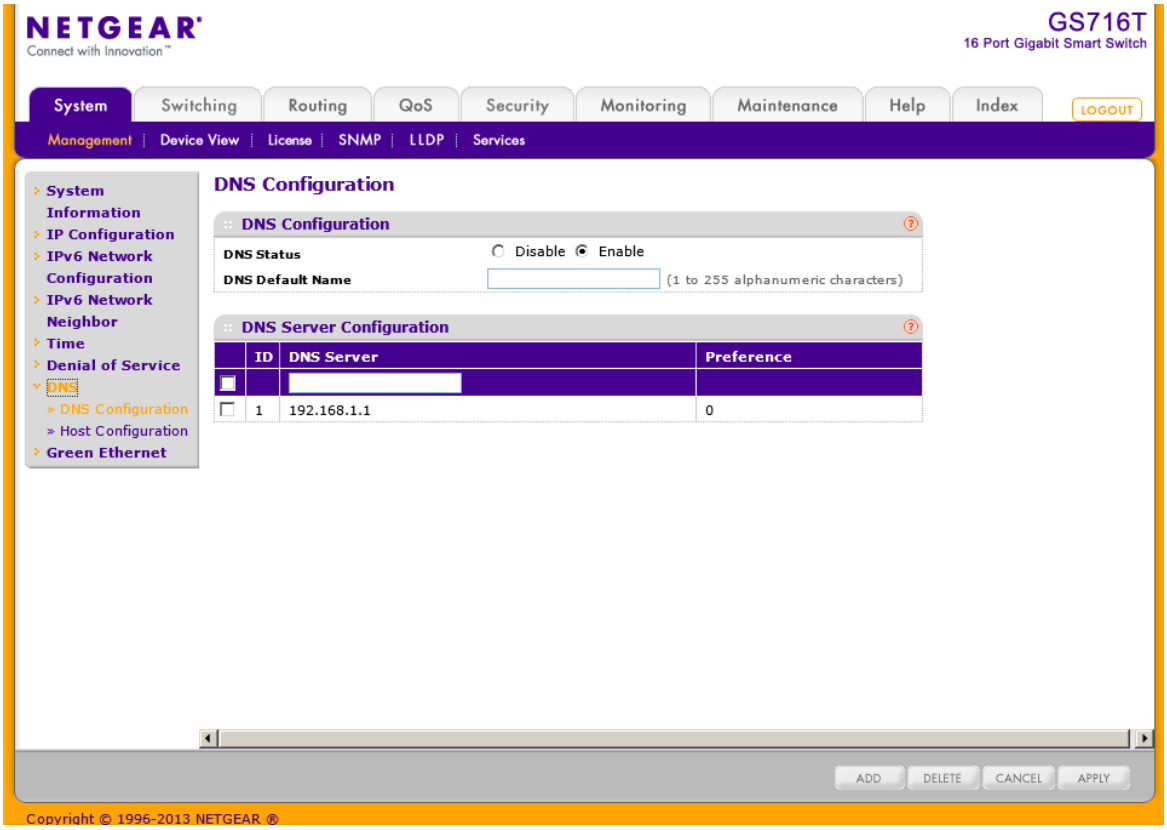
3. **Apply**.ボタンをクリックして変更した DoS 設定をスイッチに適用します。
4. **Cancel** ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。

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。



DNS 設定をする

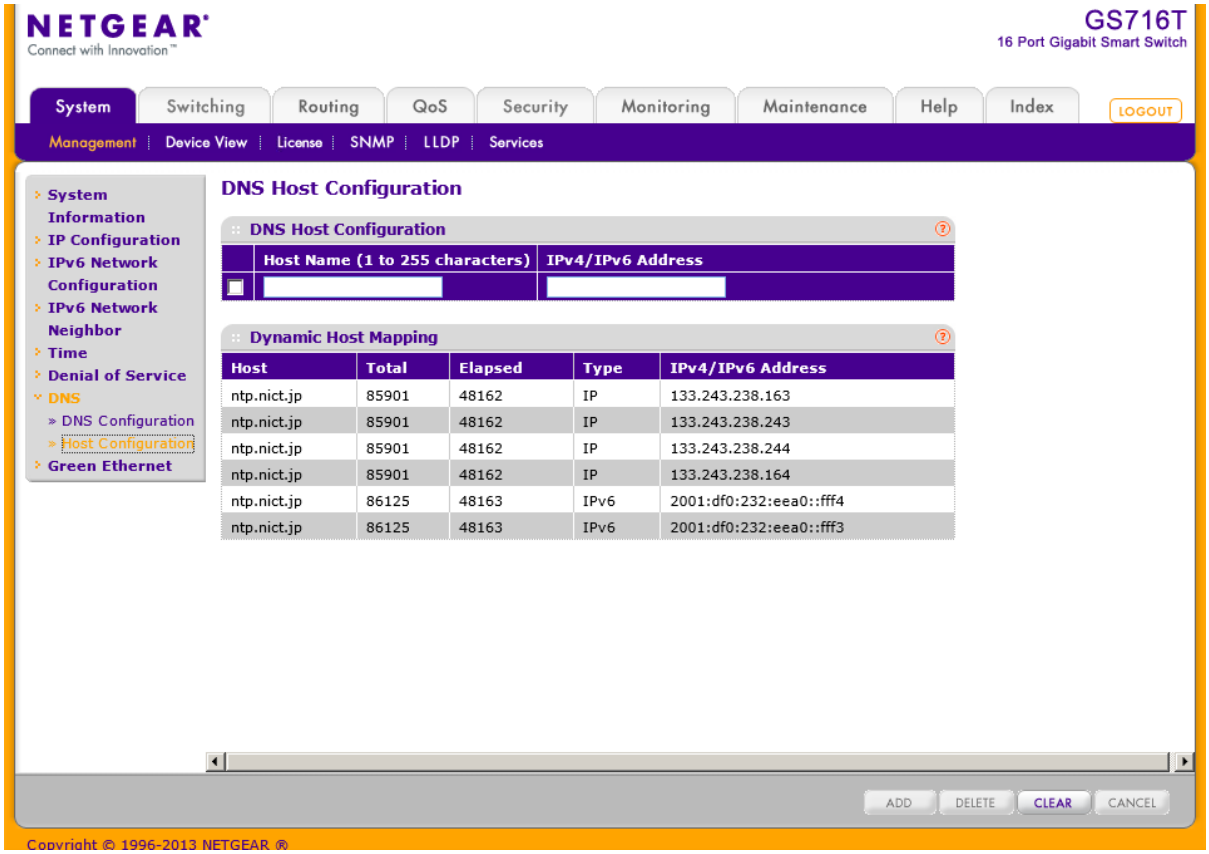
1. System > Management > DNS > DNS Configuration を選択して DNS Configuration ページを表示します。
2. DNS Status でスイッチの DNS クライアント機能を有効にします。
   - Enable：有効にしてスイッチが DNS サーバーに DNS クエリを送信して DNS ドメインネームを解決します。
   - Disable：無効にしてスイッチが DNS クエリを送信しないようにします。
3. システムがルックアップを実行する際に DNS default domain name がドメイン名として提供されます。(test 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 Preference 値が割り当てられます。設定は 8 つまで可能です。
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。



DNS テーブルに固定設定を追加する

1. System > Management > DNS > Host Configuration を選択して 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 255 文字です。
3. IPv4/IPv6 Address:ホスト名に関連付けたい IP アドレス(IPv4/IPv6)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。

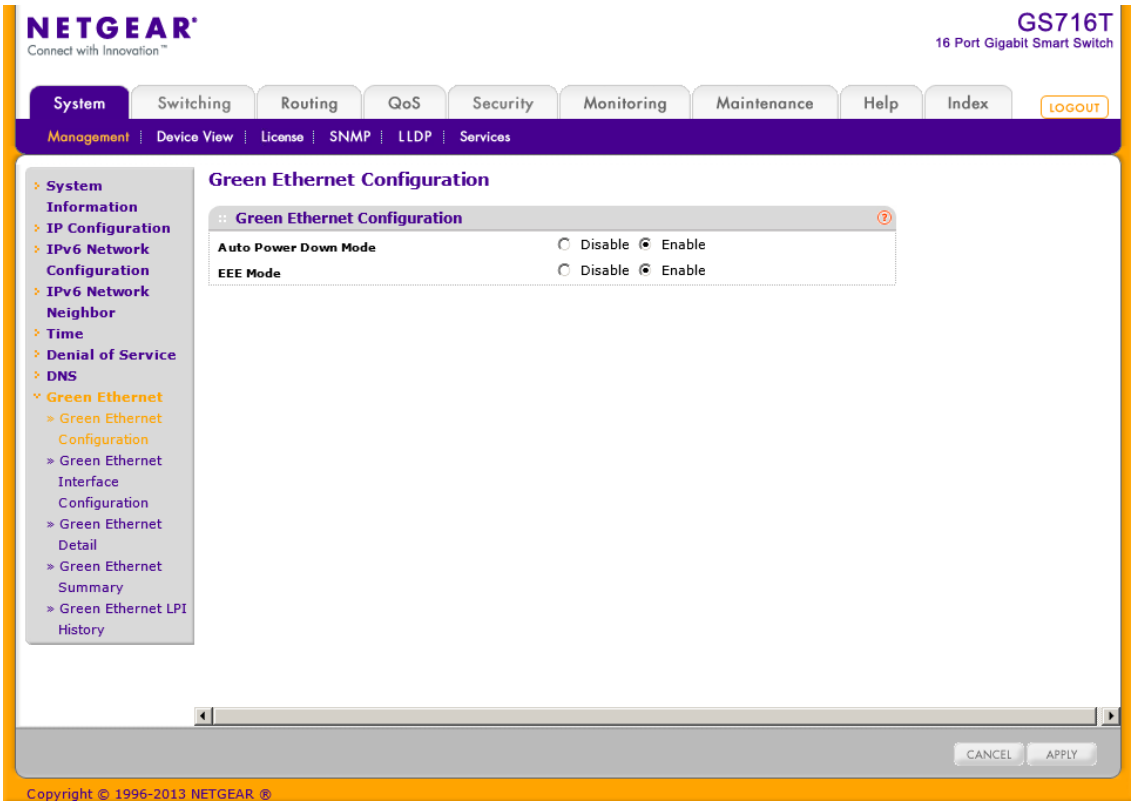
Dynamic Host Mapping table はスイッチが学習したホスト名と IP アドレスの関係を表示します。以下に **Dynamic Host Mapping** の表の項目の説明を示します。

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。
Type	追加された情報のタイプ。
Addresses	IP アドレス。

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（Green Ethernet）

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。



グリーンイーサネット（Green Ethernet）を設定する。

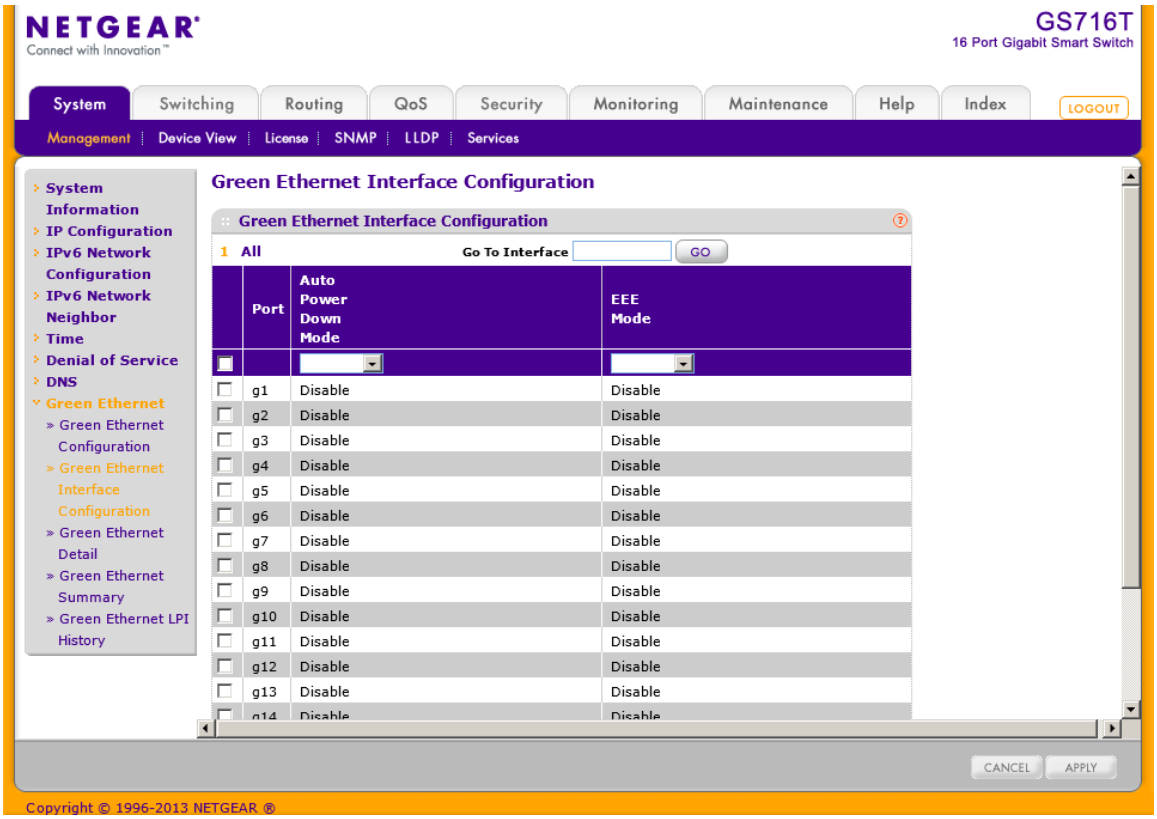
1. System > Management > Green Ethernet > Green Ethernet Configuration を選択して Green Ethernet Configuration ページを表示します。
2. Auto Power Down Mode を設定する。
   - Enable：ポートのリンクがダウンした時、ポートは自動的にポートをダウンして時々リンクパルスを確認します。
   - Disable：リンクダウン時でもポートに最大電力を供給します。
3. EEE Mode を設定する。
   - Enable：ポートの負荷が軽い場合にポートを低電力モードに移行します。
   - Disable：負荷によらずポートに最大電力を供給します。
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。

グリーンイーサネットインターフェース設定

このページでポート単位のグリーンイーサネット設定をします。

グリーンイーサネットインターフェース設定をする

1. System > Management > Green Ethernet > Green Ethernet Interface Configuration を選択して Green Ethernet Interface Configuration ページを表示します。



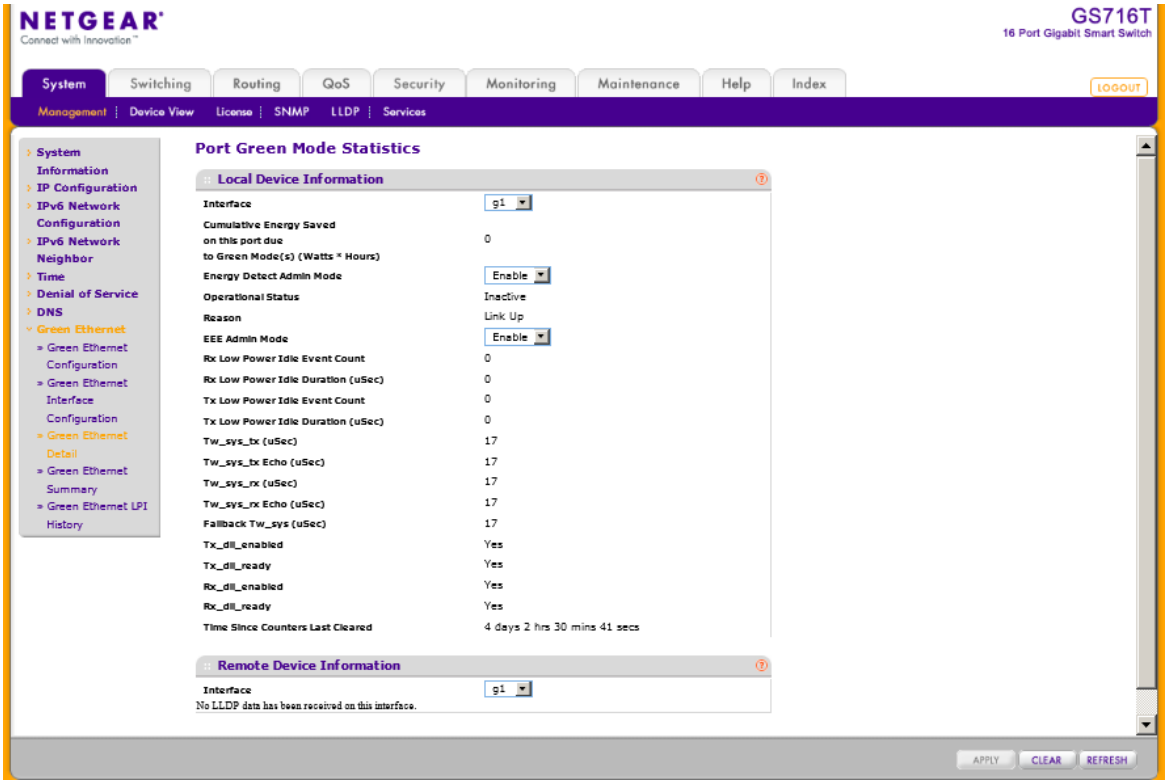
2. 設定するポートを選択します。
   - 一つのポートを選択するには、ポートのチェックボックスを選択するか、Go To Interface 欄にポート番号を入力し、Go ボタンをクリックします。
   - 複数のポートを選択するには、各ポートのチェックボックスを選択します。
   - すべてのポートを選択するには、一番上のチェックボックスを選択します。
3. 選択したポートにグリーンイーサネット設定を行います。
   - Auto Power Down Mode：ポートのリンクがダウンした時、ポートは自動的にポートをダウンして時々リンクパルスを確認します。
   - EEE Mode：ポートの負荷が軽い場合にポートを低電力モードに移行します。
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。

グリーンイーサネット詳細(Green Ethernet Detail)

この画面でポート単位の詳細なグリーンイーサネット情報の確認と設定をすることができます。

ポートのグリーンイーサネット詳細

1. System > Management > Green Ethernet > Green Ethernet Detail を選択して Green Ethernet Detail ページを表示します。



2. Interface でインターフェースを選択します。
3. ポートでグリーンイーサネット設定をします。
   - Energy Detect Admin Mode:ポートのリンクがダウンした時、ポートは自動的にポートをダウンして時々リンクパルスを確認します。
   - EEE Mode:ポートの負荷が軽い場合にポートを低電力モードに移行します。
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。

Local Device Information はポートのグリーンイーサネット情報と統計を表示します。

Green Ethernet local device information

項目	説明

Cumulative Energy Saved on this port due to Green Mode(s) (Watts * Hours)	ポート単位のエネルギー削減量（1 時間あたり）
Operational Status	グリーンモード状態。Inactive/Active
Reason	理由。Inactive/Active
Rx Low Power Idle Event Count	低電力状態になった回数。
Rx Low Power Idle Duration (uSec)	低電力アイドル状態の累積時間。単位 uSec。増加単位 10ms。
Tx Low Power Idle Event Count	リンクパートナーが低電力状態になった回数。
Tx Low Power Idle Duration (uSec)	リンクパートナーの低電力アイドル状態の累積時間。単位 uSec。増加単位 10ms。
Tw_sys_tx (uSec)	ローカルシステムがサポートできる Tw_sys 値。この値は EEE DLL Transmitter state diagram によって更新されます。
Tw_sys_tx Echo (uSec)	リモートシステムの Tw_sys 値。
Tw_sys_rx (uSec)	リモートシステムから要求する Tw_sys 値。この値は EEE Receiver L2 state diagram.によって更新されます。
Tw_sys_rx Echo (uSec)	リモートシステムの受信 Tw_sys 値。

Fallback Tw_sys (uSec)	フォールバック Tw_sys。
Tx_dll_enabled	ローカルシステムの EEE transmit Data Link Layer 管理機能の初期化状態。
Tx_dll_ready	データリンクレイヤーの送信準備状態。
Rx_dll_enabled	EEE 能力のネゴシエーション状態。
Rx_dll_ready	受信データリンクレイヤーの準備状態。
Time Since Counters Last Cleared	前回のカウンタークリアからの時間。

Green Ethernet Summary

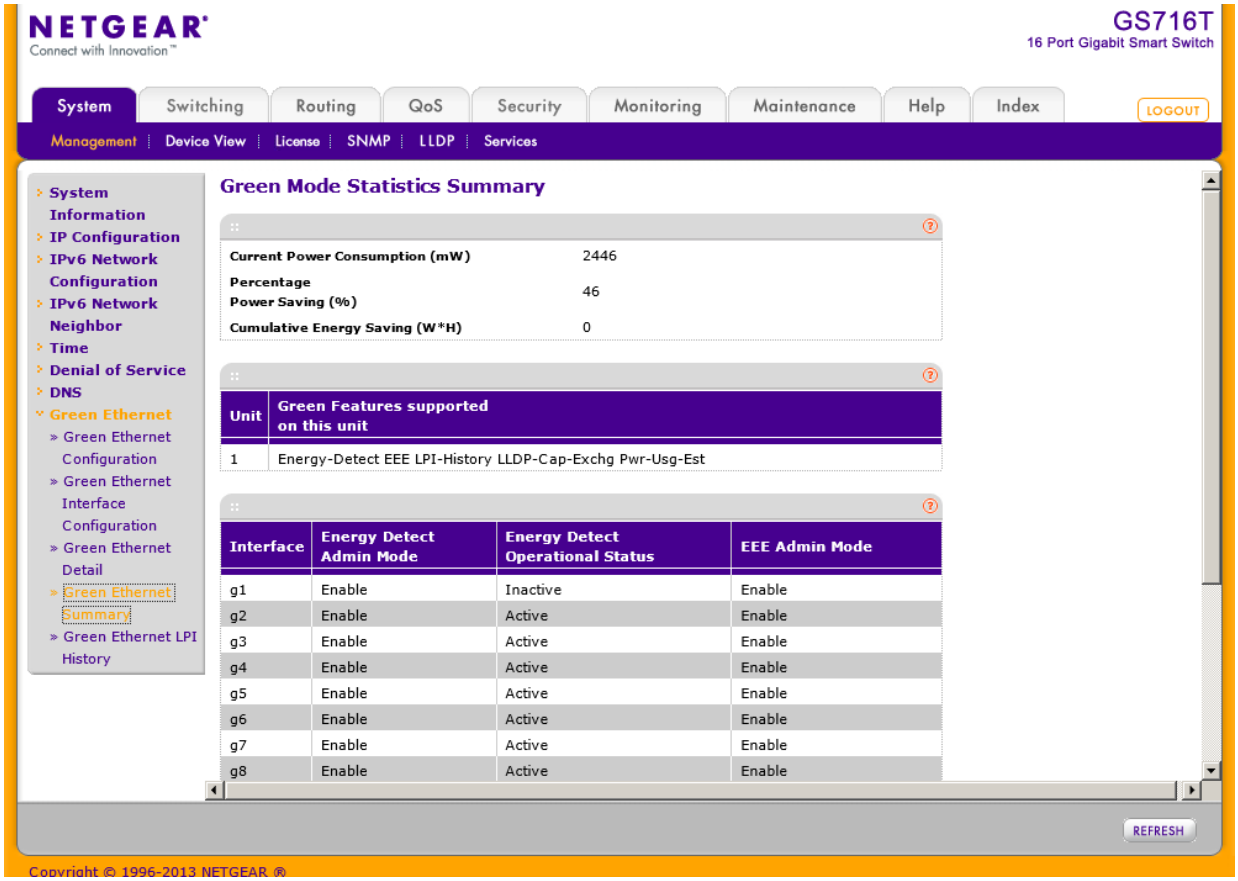
この画面で現在のグリーンイーサネットのサマリーを表示します。

System > Management > Green Ethernet > Green Ethernet Summary を選択して **Green Ethernet Summary** ページを表示します。

以下に Green Mode Statistics Summary ページで表示される情報を示します。

Green Ethernet power saving information

項目	説明
Current Power Consumption	全ポートでの総消費電力量(mW)
Estimated	推定削減電力(%)



Percentage Power Saving	
Cumulative Energy Saving per (Watts*Hours)	累積削減電力(WH)。

項目	説明
Unit	ユニット ID 番号。常に 1
Green Features supported on this unit	スイッチがサポートしているグリーンイーサネット機能。

項目	説明
Interface	インターフェース。
Energy Detect Admin Mode	Energy Detect Admin Mode の状態。
Energy Detect Operational Status	Energy Detect 機能の状態。
EEE Admin Mode	EEE Admin Mode の状態。

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。

グリーンイーサネット LPI ヒストリーを確認する

この画面でグリーンイーサネット LPI(Low Power Idle)ヒストリーを設定、確認できます。

LPI 設定をする

1. **System** > **Management** > **Green Ethernet** > **Green Ethernet LPI History** を選択して **Green Ethernet LPI History** ページを表示します。
2. **Sampling Interval field**:EEE LPI データ取得周期。グローバル設定ですべてのインターフェースに適用されます。(30-36000 秒)デフォルトは 3600 秒。
3. **Max Samples to keep**:最大保存データ量。グローバル設定ですべてのインターフェースに適用されます。(1-168)デフォルトは 168。
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. **Interface** でインターフェースを選択し、インターフェースごとの情報を表示します。

以下に表の項目の説明を記します。

表 13. LPI history information

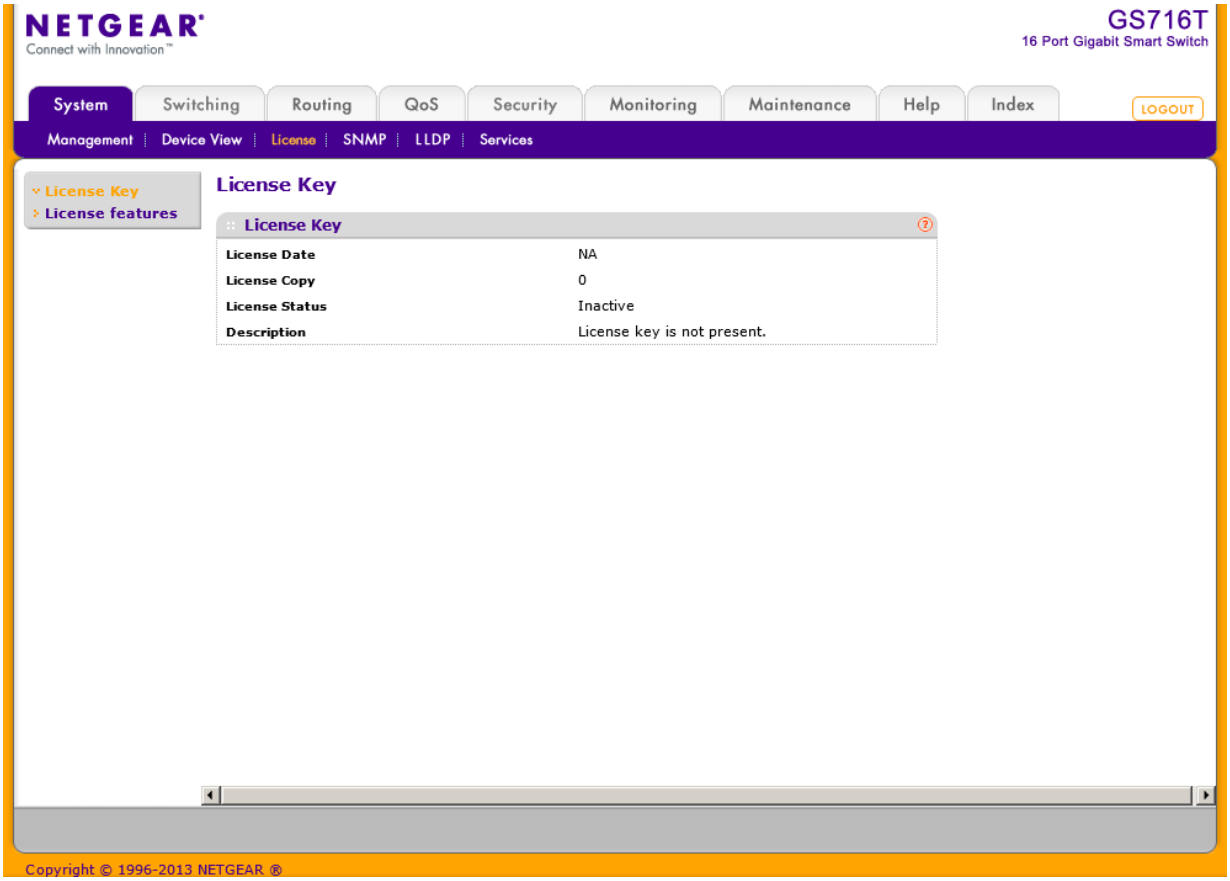
項目	説明
Percentage LPI time	LPI モードで動作した時間の割合。
Sample No.	現在のサンプル数。最大に達した後1から開始されます。
Time Since The Sample Was Recorded	前回の記録からの時間。
Percentage Time spent in LPI mode since last sample	前回の記録以降で LPI モードの時間。
Percentage Time spent in LPI mode	前回の再起動からの LPI 時間の割合。

since last reset	

ライセンス（License）

スイッチの機能によってはライセンスが必要なものがあります。このページでライセンス情報を確認することができます。

System > License > License Key を選択して License Key ページを表示します。



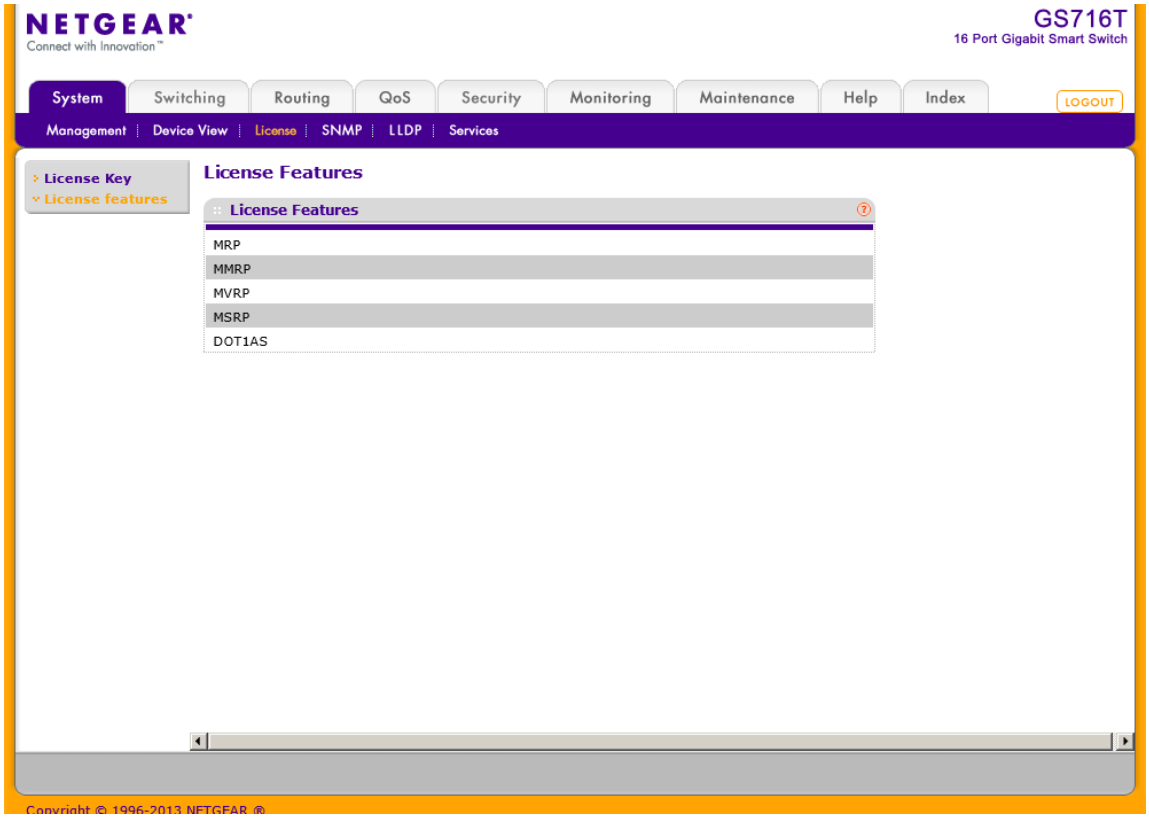
License Key ページで表示される情報の説明を以下に示します。

表 14. License Key information

項目	説明
License Date	ライセンス購入日。
License Copy	スイッチにあるライセンス数。

License Status	ライセンスの状態。
Description	ライセンスキーの情報。

System > License > License Features を選択して License Features を表示できます。



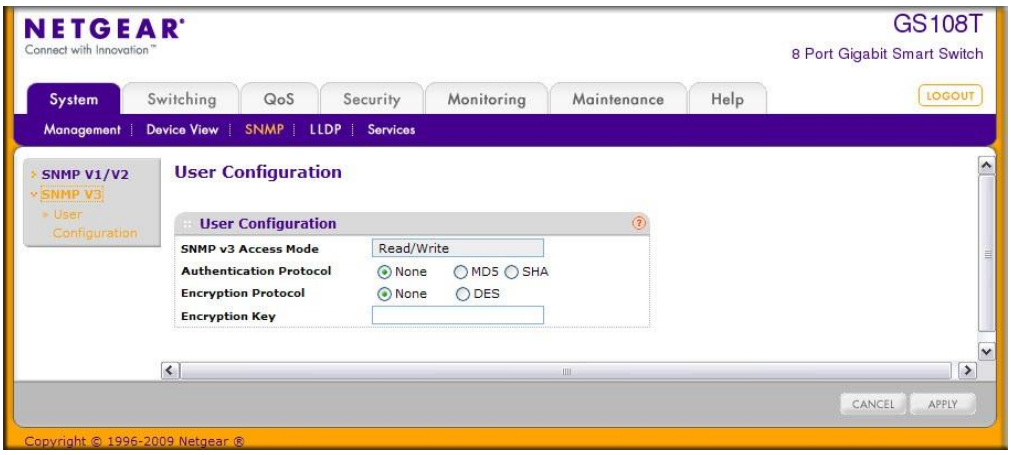
SNMP

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。

SNMPv1/v2 コミュニティ設定

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

ここでは SNMPv3 の設定をします。



SNMPv3 Access Mode は変更不可の情報でユーザー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 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 グループとユーザーの設定をサポートしています。

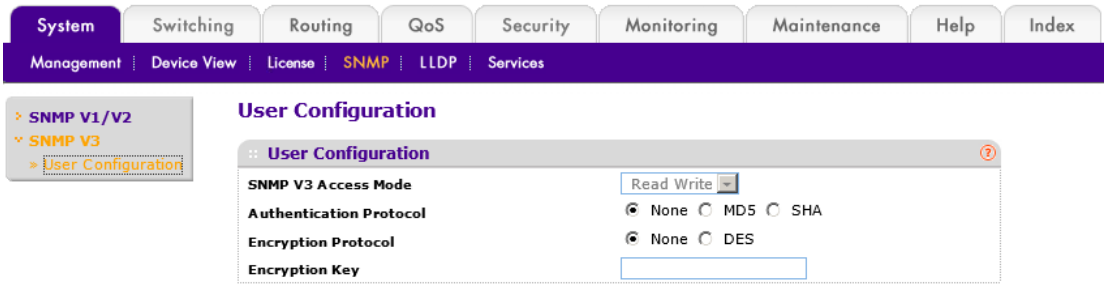
スイッチは標準的な機能のためのスタンダード public MIB と追加のスイッチ機能をサポートする private MIB の両方を使います。すべての private MIB は”-“の文字から始まります。メインのインターフェース設定オブジェクトは private MIB である-SWITCHING-MIB に含まれます。いくつかのインターフェース設定は public MIB である IF-MIB に含まれます。

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 インターフェースで SNMPv3 設定をする

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



2. SNMPv3 Access Mode はユーザーカウントのアクセス権限を示し、この情報は変更不可です。Admin アカウントは常に Read/Write 権限で、その他のアカウントは Read Only です。
3. 認証を有効にするために、Authentication Protocol オプションを選択します。
4. Authentication Protocol が MD5 または SHA の場合、ユーザーログインパスワードが SNMPv3 認証パスワードとして使われます。
5. 暗号化を有効にするために Encryption Protocol 欄で DES を選択して SNMPv3 パケットを DES で暗号化します。
6. Encryption Key：英数 8 文字以上の文字を記入します。
7. Apply ボタンクリックします。

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。

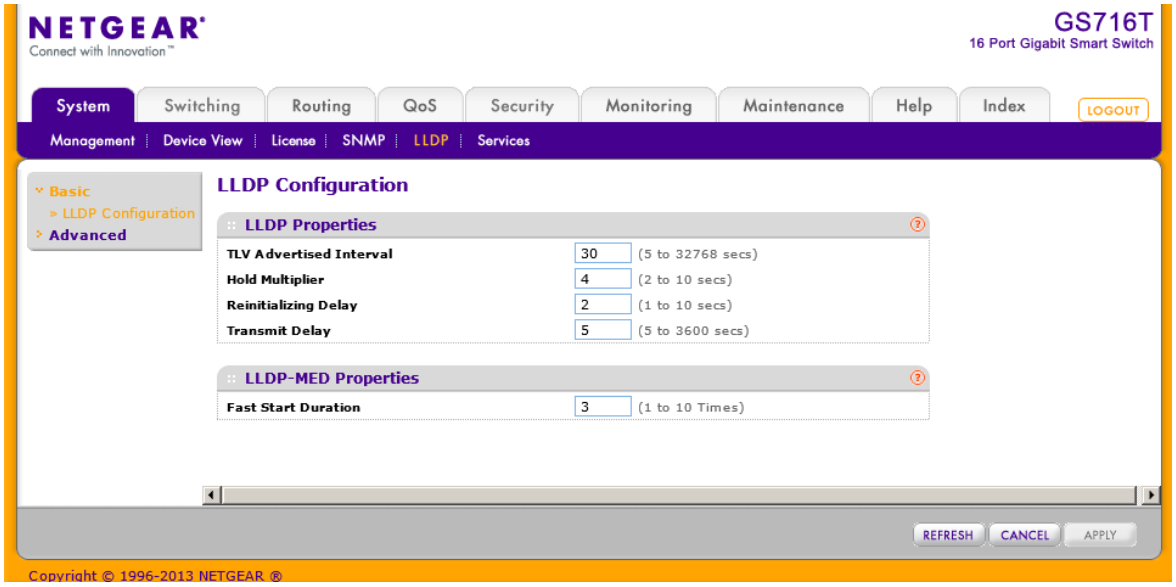
LLDP は一方向のプロトコルで、要求・応答というような通信はありません。情報はこの機能を送信する機能を実装している機器から送信(advertise)され、受信機能を実装している機器によって受信・処理されます。送信・受信の機能はポート単位に設定できます。デフォルト設定では、送信・受信共に無効になっています。

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。

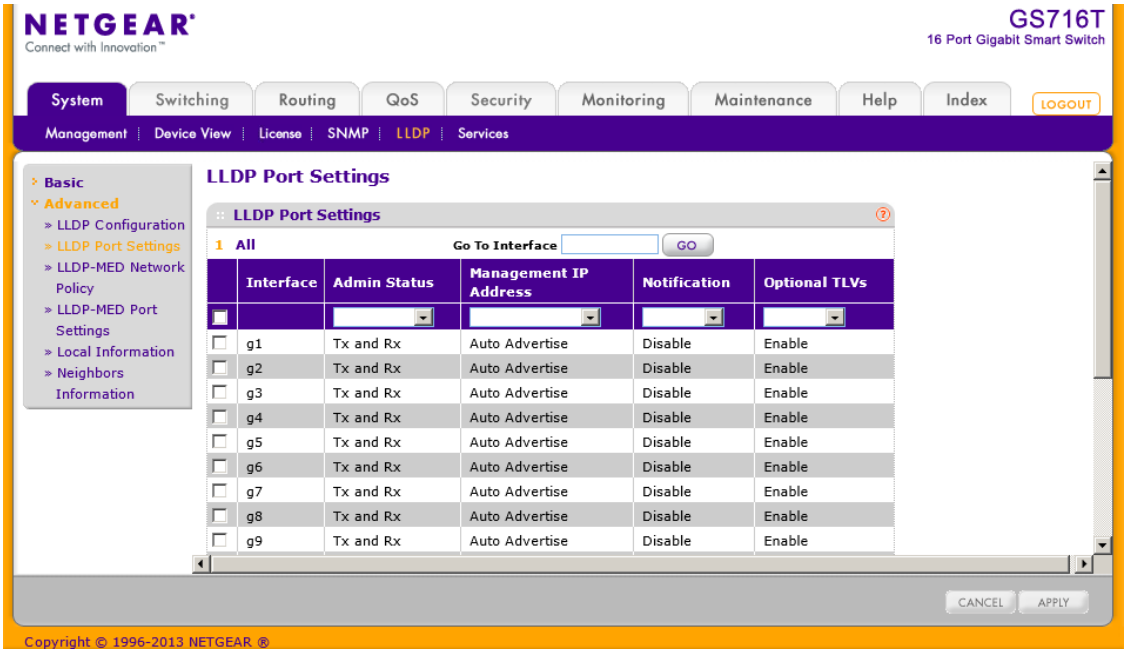


グローバル LLDP(Global LLDP)設定をする

1. 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 5-32768(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。
   - 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。
3. LLDP-MED properties の Fast Start Duration は、LLDP-MED 対応機器を検出し、LLDP－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。



LLDP ポート設定をする

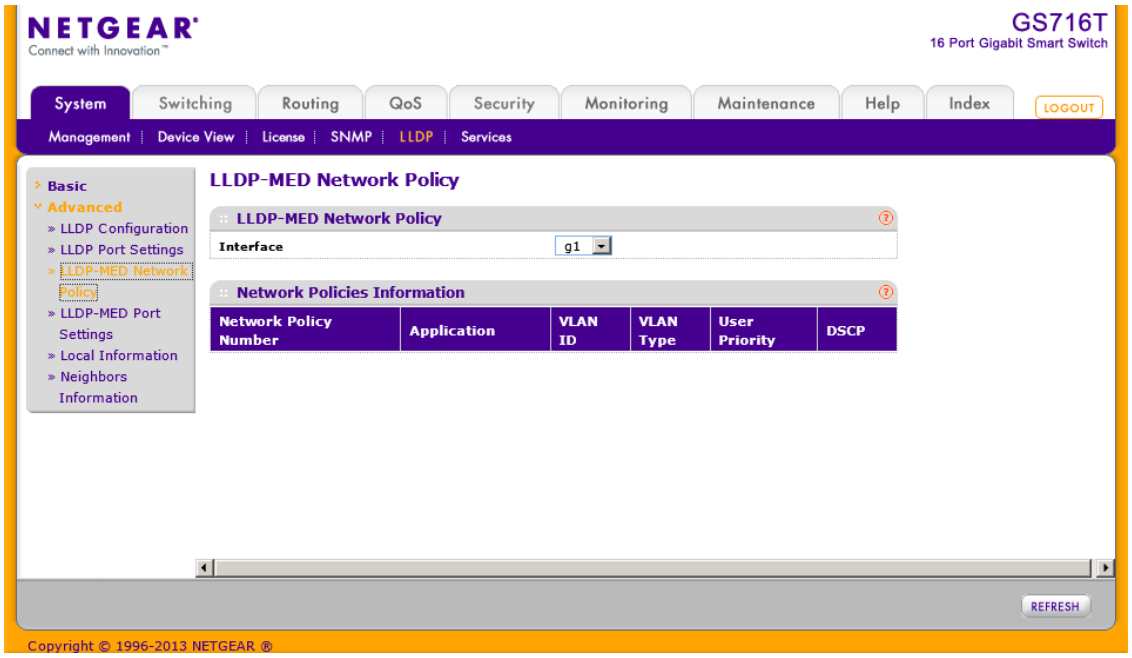
1. System > LLDP > Advanced > LLDP Port Settings を選択して LLDP Port Settings ページを表示します。
2. 以下の LLDP ポート設定を変更します。
   - Interface：LLDP 設定を変更するポートを選択します。
   - Admin Status：LLDP パケットの送信・受信の設定をします。
     - Tx Only:：指定したポートで LLDP パケットの送信のみをします。
     - Rx Only：指定したポートで LLDP パケットの受信のみをします。
     - Tx and Rx:：指定したポートで 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。



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。

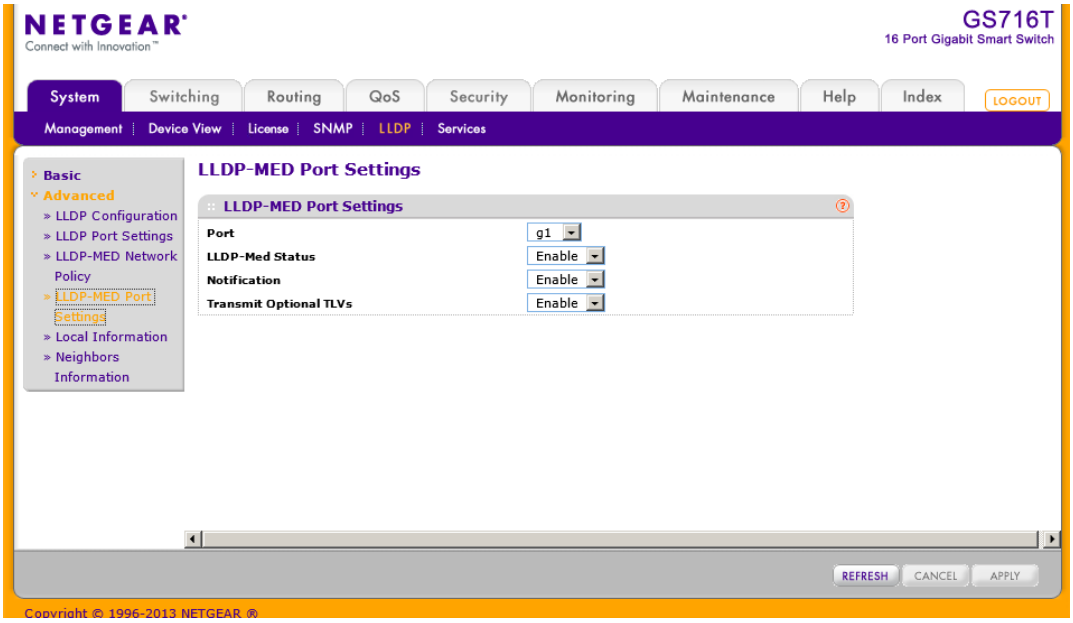
項目	説明

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 ポート設定(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。



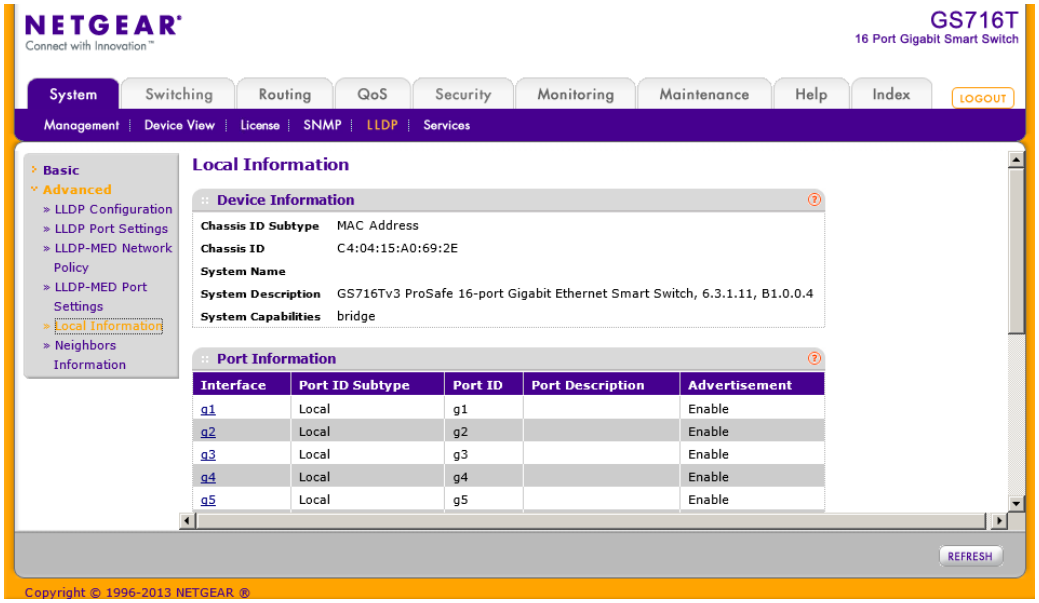
ポートに LLDP-MED 設定(LLDP-MED Settings)をする

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。
4. 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。



LLDP > Local Information.を選択して、LLDP Local Information ページを表示します。LLDP が有効なインターフェースのみが表示されます。

Local Information ページで表示される Device Information の説明は以下の通りです。

項目	説明
Chassis ID Subtype	Chassis ID 欄に表示される情報のタイプ。
Chassis ID	Chassis ID
System Name	システム名
System Description	システム詳細
System Capabilities	システム能力

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。

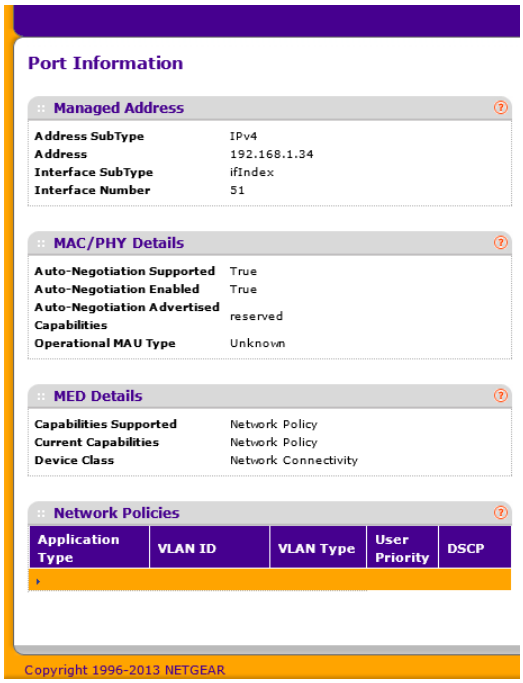
項目	説明
Interface	インターフェース番号

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。

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。



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。

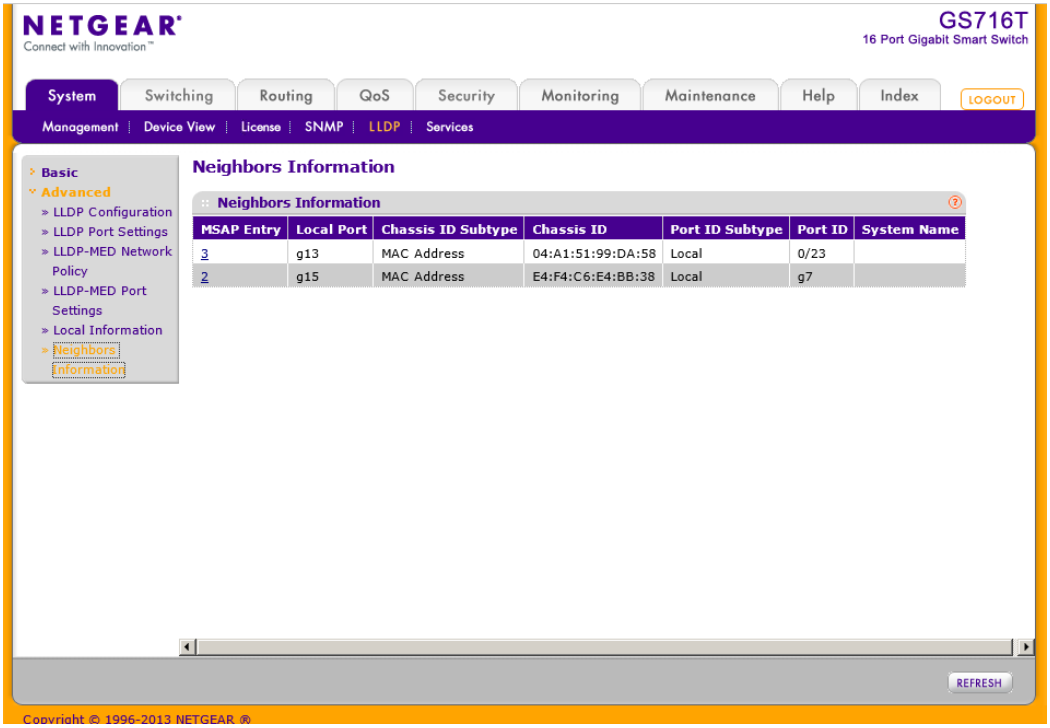
項目	説明
Managed Address	
Address SubType	管理インターフェースが使っているアドレスのタイプ。たとえば IPv4 アドレス。
Address	管理用に使われるアドレス。
Interface SubType	ポートのタイプ。
Interface Number	ポートの番号。
MAC/PHY Details	

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。
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。



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

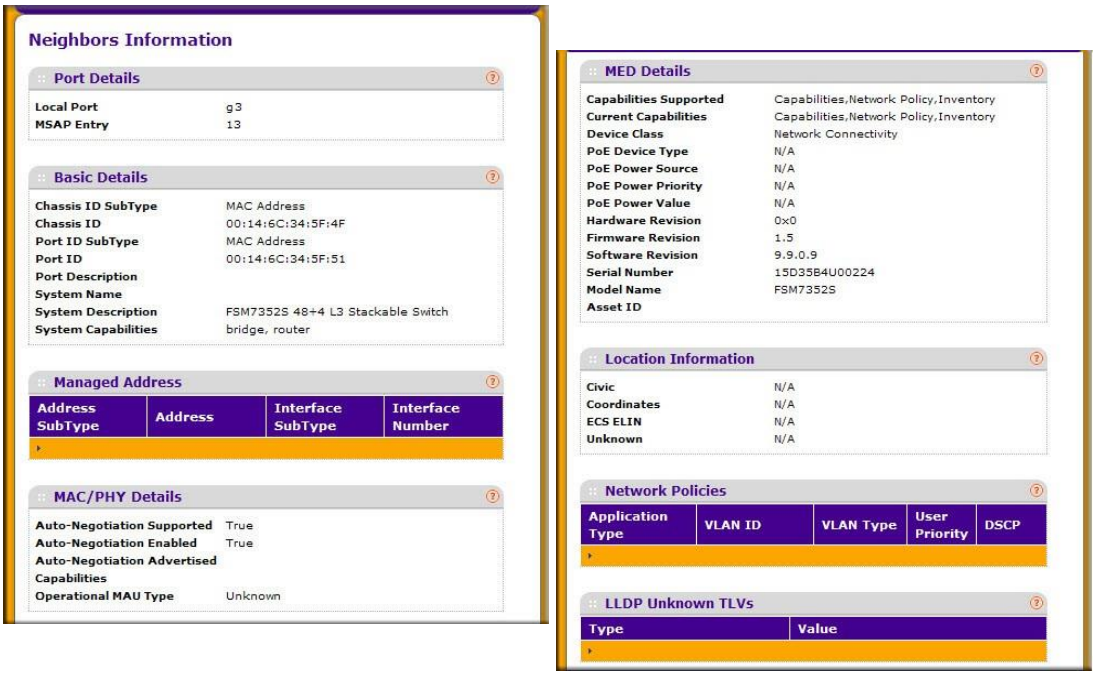
ポートで受信された LLDP の情報の説明は以下の表のとおりです。

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。



項目	説明
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 Capabilities	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)のタイプ。
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、レイヤー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。
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	
Type	不明の TLV タイプ。
Value	不明の TLV 値。

サービス(Services)

この章では DHCP スヌーピングと DAI(Dynamic ARP Inspection)の設定方法について記します。DHCP スヌーピングと DAI はトラフィックを検査してスイッチやネットワークに対する偶然または悪意のある攻撃を防ぐためにトラフィックを検査するレイヤー2 のセキュリティ機能です。サービスメニューから以下の 2 つの機能にアクセスできます。

- DHCP Snooping
- Dynamic ARP Inspection

DHCP スヌーピング(DHCP Snooping)

DHCP スヌーピングは信頼できない DHCP メッセージをフィルタし、DHCP スヌーピングバインディングテーブルを作成、維持することによってセキュリティを提供する役に立つ機能です。信頼出来ないメッセージはネットワークやファイヤーウォールの外から受信されたメッセージであり、ネットワークに対するトラフィック攻撃の原因となるものです。DHCP スヌーピングバインディングテーブルは MAC アドレス、IP アドレス、リースタイム、バインディングタイプ、VLAN 番号、およびスイッの信頼できないインターフェースのインターフェース情報を含みます。信頼できないインターフェース(Untrusted interface)は外部のネットワークやファイヤーウォールからメッセージを受信するように設定されています。信頼できるインターフェースは、ネットワーク内部のみからメッセージを受信するように設定されています。

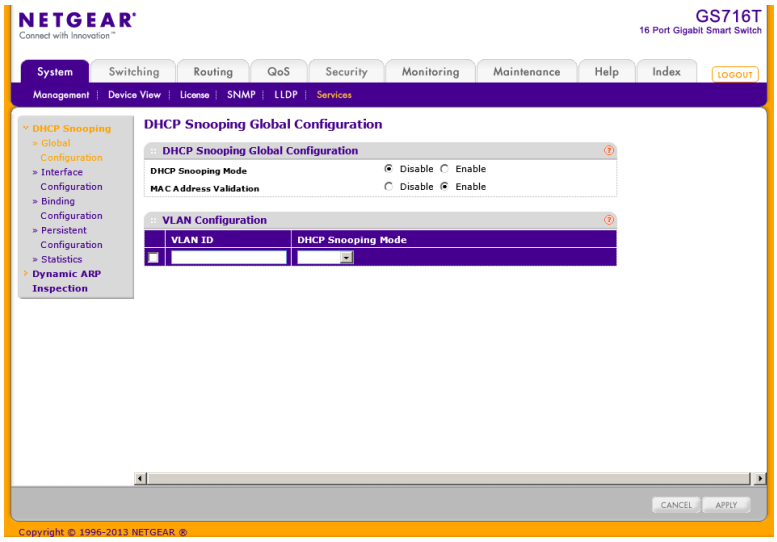
DHCP スヌーピングは信頼できないホスト(Untrusted Hosts)と DHCP サーバーの間のファイヤーウォールのように動作します。また、エンドユーザーと接続されている信頼出来ないインターフェースと DHCP サーバーや他のスイッチと接続されている陰雷できるインターフェースを区別する方法も提供します。

グローバル設定(Global Configuration)

このページで DHCP スヌーピングのグローバル設定をします。

DHCP スヌーピンググローバル設定をする

1. **System** > **Services** > **DHCP Snooping** > **Global Configuration** を選択して **Global Configuration** ページを表示します。
2. **DHCP Snooping Mode**:Enable(有効)を選択します。
3. **MAC Address Validation**:Enable(有効)、Disable(無効)を選択します。
   有効にすると、信頼できないインターフェースで受信したパケットの MAC アドレスと DHCP クライアントの MAC アドレスを比較し、一致しない場合はパケットを廃棄します。デフォルトは有効です。



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、設定は保存されます。
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。

VLAN 内で DHCP スヌーピングを有効にする

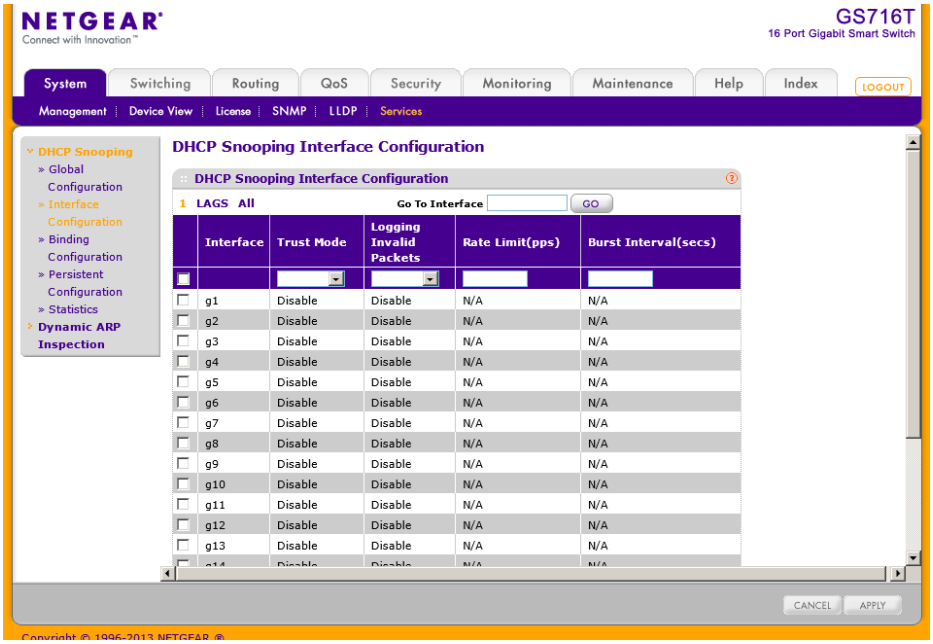
1. **VLAN ID**：DHCP スヌーピングを有効にする VAN を選択します。
2. **DHCP Snooping Mode**：Enable(有効)を選択します。
3. **Apply** ボタンをクリックして設定をスイッチに適用します。設定は即時に有効になり、設定は保存されます。
4. **Cancel** ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。

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。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。

DHCP スヌーピングインターフェース設定をする

1. System > Services > DHCP Filtering > Interface Configuration を選択して Interface Configuration を表示します。



2. 1/LAGS/ALL をクリックして、インターフェースを表示して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。複数の選択も可能です。
3. Trust Mode：モードを選択します。
   - Enable：(Trusted)インターフェースは信頼できるとみなされ、DHCP サーバーメッセージは検証なしに転送されます。
   - Disable：(Unstusted):インターフェースは信頼できないとみなされ、ネットワーク攻撃に使われる可能性があります。DHCP サーバーメッセージはバインディングデータベースと照合されます。
     信頼できないポート(untrusted port)では、DHCP スヌーピング機能は以下のセキュリティルールを適用します。
     - DHCP サーバーからのパケット（DHCP OFFER/DHCP ACK/DHCP NACK/DHCP RELEASE QUERY）は廃棄されます。
     - MAC アドレスがスヌーピングデータベースに存在するが、バインディングインターフェースと異なる場合は DHCP RELEASE/DHCP DECLINE パケットは廃棄されます。
5. Logging Invalid Packets：Enable（有効）にすると、インターフェースで不正なパケットを受信し、廃棄された際にログメッセージが保存されます。
6. Rate Limit(pps)：受信される DHCP パケットの速度が Burst Interval 時間内でこの値を超えた時に、ポートはシャットダウンされます。無効の場合は、DHCP パケットの速度によらず、ポートはシャットダ

ウンされません。

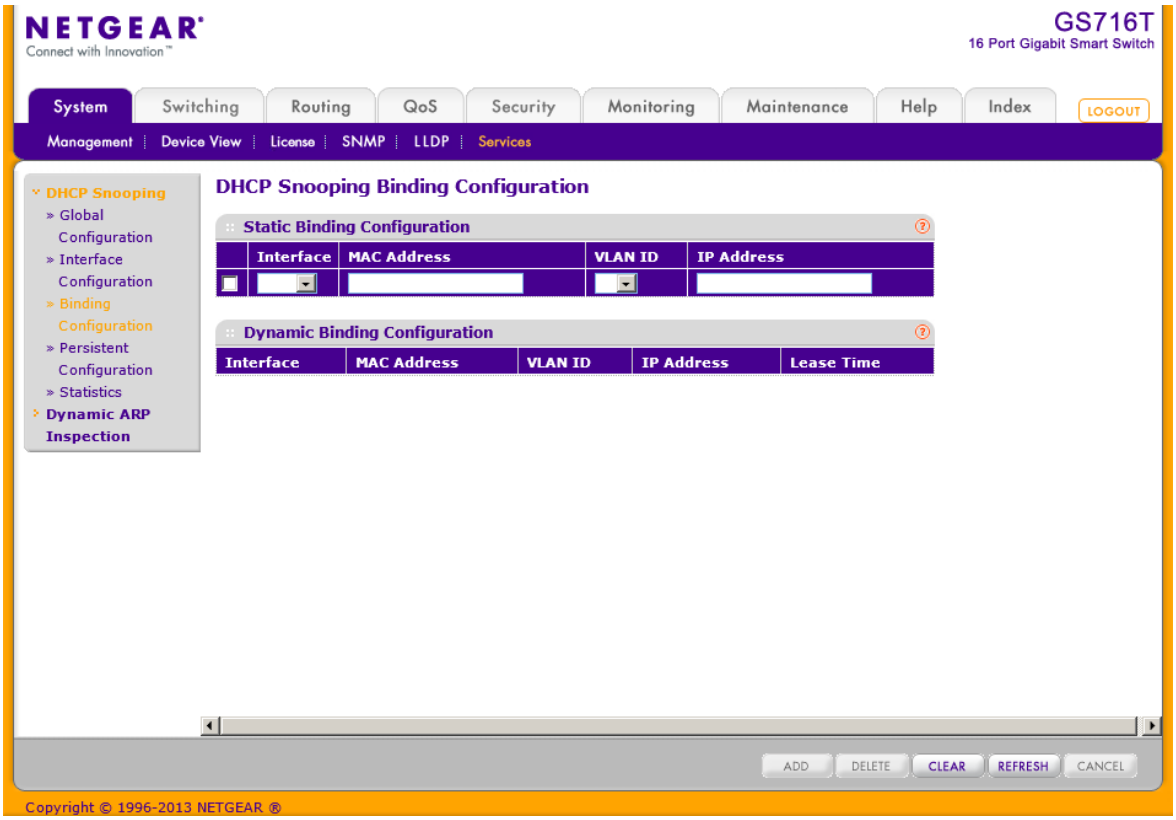
7. **Burst Interval(secs)**：Rate Limit のための時間（秒）を設定します。
8. **Apply** ボタンをクリックして設定をスイッチに適用します。設定は即時に有効になり、設定は保存されます。
9. **Cancel** ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。

バインディング設定（Binding Configuration）

この画面で DHCP スヌーピングバインディングデータベースへのスタティックバインディングの確認、追加、削除およびバインディングテーブルのダイナミックバインディングの確認およびクリアをすることができます。

スタティック DHCP バインディングの設定

1. **System** > **Services** > **DHCP Snooping** > **Binding Configuration** を選択して **Binding Configuration** ページを表示します。



2. **Interface**：DHCP クライアントを許可するインターフェースを指定します。
3. **MAC Address**：バインディングする MAC アドレスを指定します。この情報がバインディングデータベースの鍵となります。

4. **VLAN ID**：VLAN ID を指定します。
5. **IP Address**：クライアントの IP アドレスを指定します。
6. **Add** ボタンをクリックします。
   DHCP スヌーピングバインディングがデータベースに追加されます。

Dynamic Binding Configuration は DHCP スヌーピングが有効になっているインターフェースで学習した DHCP バインディング情報を示します。以下の表はダイナミックバインディング情報を示します。

表 21. DHCP snooping dynamic binding information

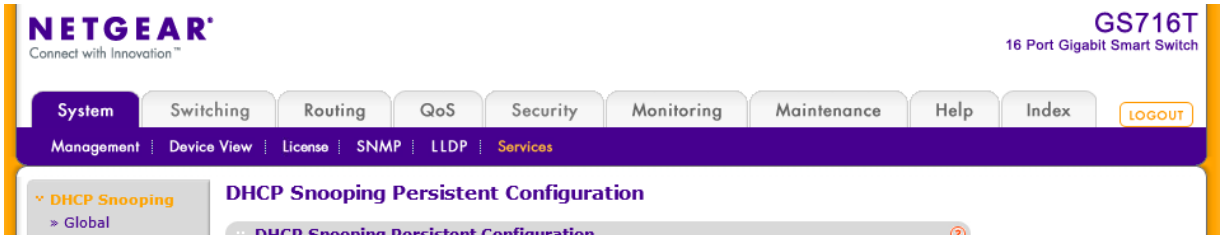
項目	説明
Interface	DHCP クライアントメッセージを受信したインターフェース。
MAC Address	メッセージを送信した DHCP クライアントの MAC アドレス。この情報がバインディングデータベースの鍵です。
VLAN ID	クライアントインターフェースの VLAN ID。
IP Address	DHCP サーバーがクライアントに割り当てた IP アドレス。
Lease Time	クライアントの IP アドレスの残リースタイム。

永続的設定（Persistent Configuration）

この画面を使って DHCP スヌーピングバインディングデータベースの永続的な位置を設定します。バインディングデータベースはスイッチにローカルに保存されるか、ネットワーク上のどこかのリモートシステムに保管されます。デバイスはバインディング情報をリモートデータベースに送るためにリモートシステムの IP アドレスに到達できる必要があります。

DHCP スヌーピング永続設定をする

1. **System** > **Services** > **DHCP Snooping** > **Persistent Configuration** を選択して **Persistent Configuration** ページを表示します。
2. **Store**：DHCP スヌーピングバインディングデータベースの場所を指定します。
   - **Local**：バインディングテーブルはスイッチに保管されます。
   - **Remote**：バインディングテーブルはリモートの TFTP サーバーに保管されます。



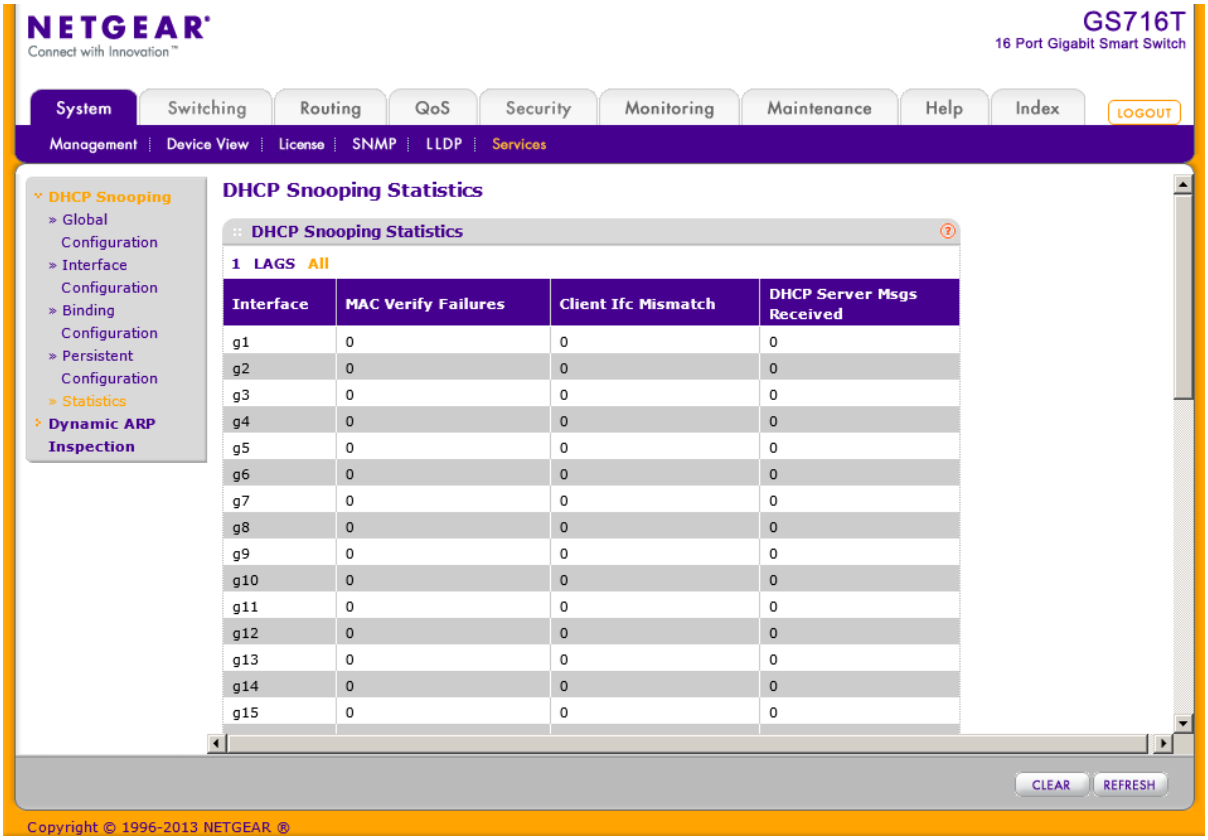
3. **Remote IP Address**：バインディングテーブルがリモートに保管される場合に、TFTP サーバーの IP アドレスを指定します。
4. **Remote File Name**：バインディングテーブルがリモートに保管される場合に、DHCP スヌーピングバインディングデータベースのファイル名。
5. **Write Delay**：バインディング情報を永続ファイルに記録するまでの待ち時間を指定します。（15-86400 秒）デフォルトは 300 秒。
   この遅延によりよりデバイスは多くの情報を集めることができます。
6. **Apply** ボタンをクリックします。

統計（Statistics）

この画面を使って信頼できないインターフェースで DHCP スヌーピング機能によってフィルターされた DHCP メッセージのインターフェース単位の統計を確認、クリアします。

DHCP スヌーピング統計を確認、クリアする

1. **System** > **Services** > **DHCP Snooping** > **Statistics** を選択して **DHCP Snooping Statistics** ページを表示します。



2. **Clear** をクリックしてすべてのインターフェースの統計情報をクリアします。

以下に **DHCP snooping statistics** 表の情報の説明を示します。

表 22. DHCP snooping statistics

項目	説明
Interface	インターフェース
MAC Verify Failures	送信元 MAC アドレスとクライアントハードウェアアドレスが一致しないために廃棄された DHCP メッセージ数。MAC Address Verification はグローバル設定です。
Client Ifc Mismatch	パケットが受信された VLAN 情報とインターフェースが一致しないために DHCP スヌーピングにより廃棄されたパケット数。
DHCP Server Msgs Received	Untrusted ポートで廃棄された DHCP サーバーメッセージ (DHCPOFFER, DHCPACK, DHCPNAK, DHCPRELEASEQUERY)。

ダイナミック ARP 検査(Dynamic ARP Inspection)

DAI(Dynamic ARP Inspection:ダイナミック ARP 検査)は不正で悪意のある ARP パケットを拒否します。DAI は非友好的な端末が他の端末向けのトラフィックを横取りし、ARP キャッシュを汚染するような中間者攻撃を防止します。悪意のある攻撃者は他の端末の IP アドレスと自分の MAC アドレスを対応付ける ARP 要求や応答を送信します。

DAI を有効にすると、送信元 MAC アドレスと送信元 IP アドレスが DHCP スヌーピングバインディングデータベースの情報に一致しない ARP パケットを廃棄します。追加の ARP パケット検証を設定することもできます。

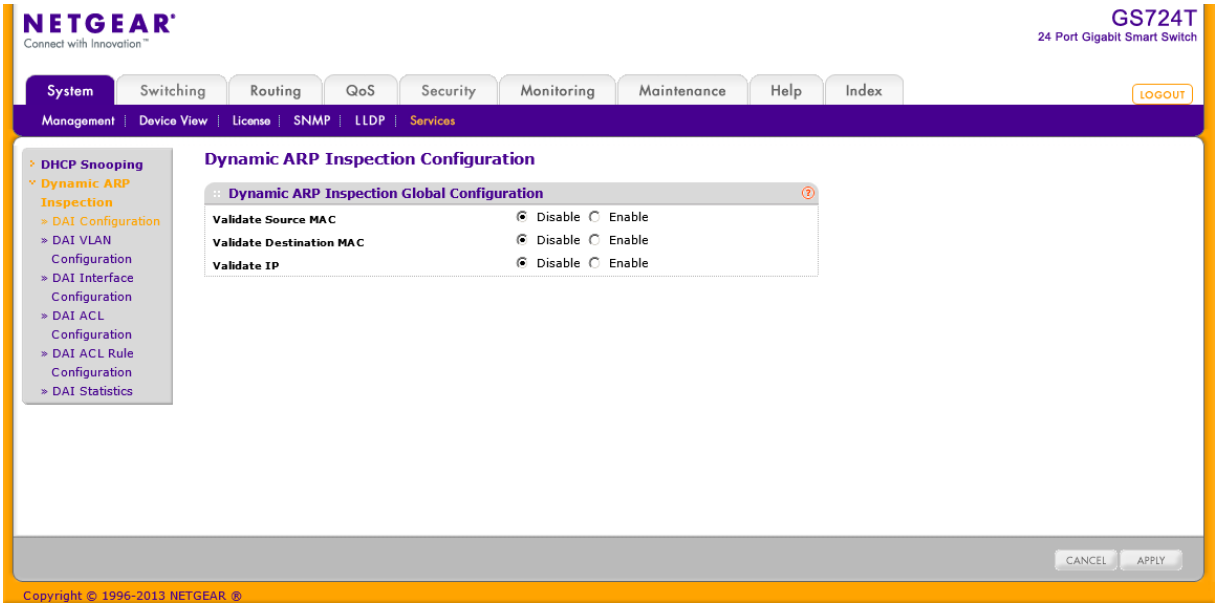
VLAN で DAI を有効にすると、VLAN のメンバーインターフェース(ポートまたは LAG)で DAI が有効になります。個々のインターフェースは信頼できる(trusted)または信頼出来ない(unstrusted)と設定できます。DAI の信頼設定と HDCP スヌーピングの信頼設定は独立です。

DAI グローバル設定をする

この画面では DAI のグローバル設定をします。

1. **System** > **Services** > **Dynamic ARP Inspection** > **DAI Configuration** を選択して **DAI**

Configuration ページを表示します。



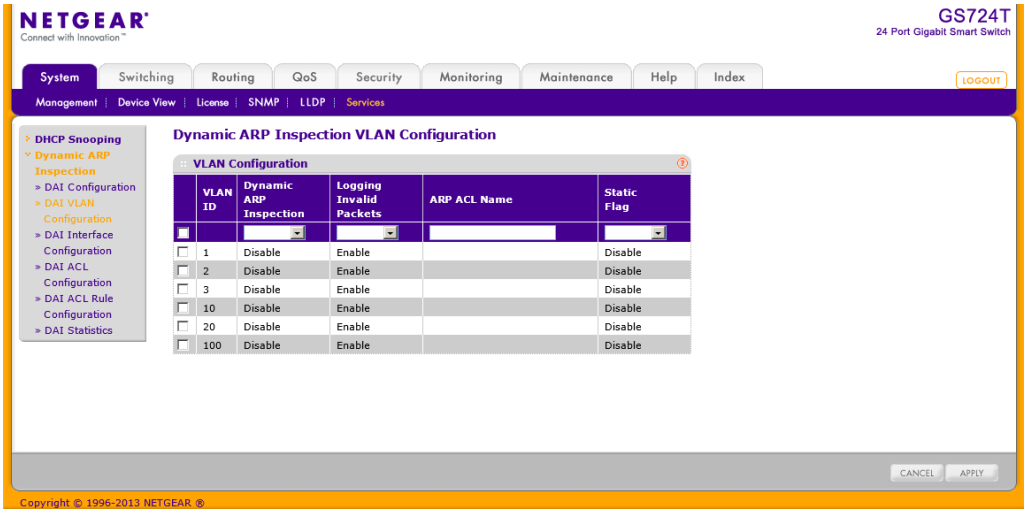
2. 以下の項目を設定します。
3. **Validate Source MAC**：有効(Enable)にすると、ARP パケットの送信元 MAC アドレスを検証します。デフォルトは無効（Disable）です。
4. **Validate Destination MAC**：有効(Enable)にすると、ARP 応答パケットの宛先 MAC アドレスを検証します。デフォルトは無効（Disable）です。
5. **Validate IP**：有効(Enable)にすると、ARP パケットの IP アドレスを検証します。デフォルトは無効（Disable）です。
6. **Apply** ボタンをクリックして設定をスイッチに適用します。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。

DAI VLAN 設定をする

この画面では DAI の VLAN 設定をします。

1. **System** > **Services** > **Dynamic ARP Inspection** > **DAI VLAN Configuration** を選択して **DAI VLAN Configuration** ページを表示します。

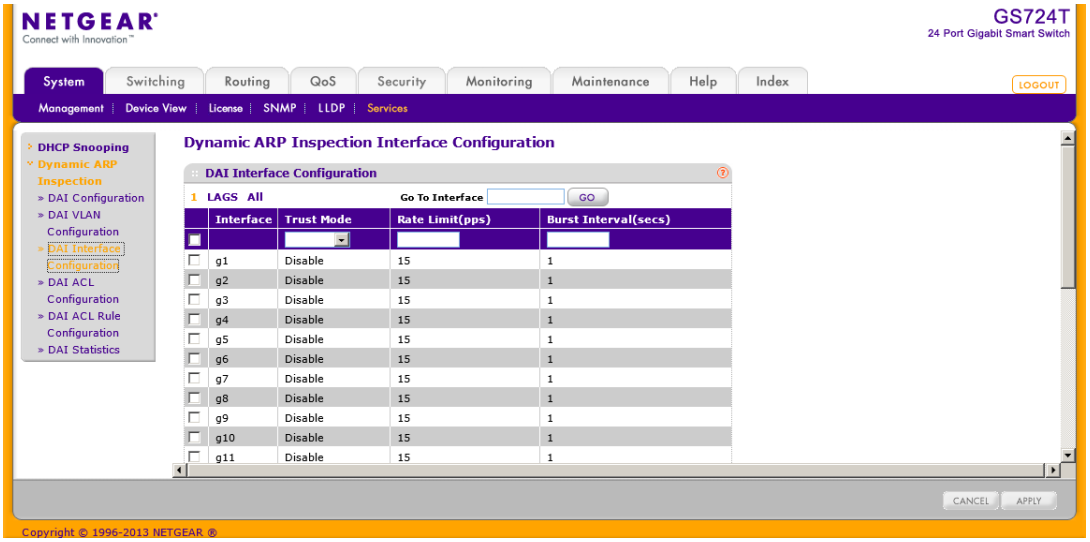
2. 以下の項目を設定します。
3. **VLAN ID**：DAI を設定する VLAN の VLAN ID を選択します。
4. **Dynamic ARP Inspection**：DAI を VLAN で有効にする場合に有効（Enable）にします。デフォルトは無効（Disable）です。



5. **Logging Invalid Packets**：不正な ARP パケットのログを記録する場合に有効（Enable）にします。デフォルトは有効（Enable）です。
6. **ARP ACL Name**：適用する DAI ACL を記入します。DAI ACL は DAI ACL 設定で作成します。
7. **Statc Flag**：ARP ACL が一致しなかった場合に DHCP スヌーピングデータベースによる検査を実行するかどうかを設定します。
8. **Enable**：ARP ACL 検証のみが実行されます。
9. **Disable**：ARP ACL 検証の後に DHCP スヌーピングデータベースによる検証が実行されます。
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。設定は即時に有効になり、設定は保存されます。
11. **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します。

DAI インターフェース設定をする

1. System > Services > Dynamic ARP Inspection > DAI Interface Configuration を選択して DAI Interface Configuration ページを表示します。



2. 1/LAGS/ALL をクリックして、インターフェースを表示して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。複数の選択も可能です。
3. 以下の項目を設定します。
   - **Trust Mode**：DAI としてインターフェースが信頼できる（Trusted）かどうかを指定します。有効（Enable）の場合、ARP パケットは検査されずに転送されます。無効（Disable）の場合、ARP パケットは検査されます。デフォルトは無効（Disable）です。
   - **Rate Limit(pps)**：入力される ARP パケットの速度(pps)が Burst Interval 時間を超えて継続した場合、ARP パケットは廃棄されま。None または-1 と指定した場合は非制限となります。範囲は 0-300 秒です。デフォルトは１５秒です。
   - **Burst Interval(secs)**：ARP パケットを連続受信する場合、連続受信可能な時間（秒）を設定します。None の場合は非制限となります。範囲は 1-15 秒でデフォルトは１秒です。
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、設定は保存されます。
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。

DAI ACL を設定する

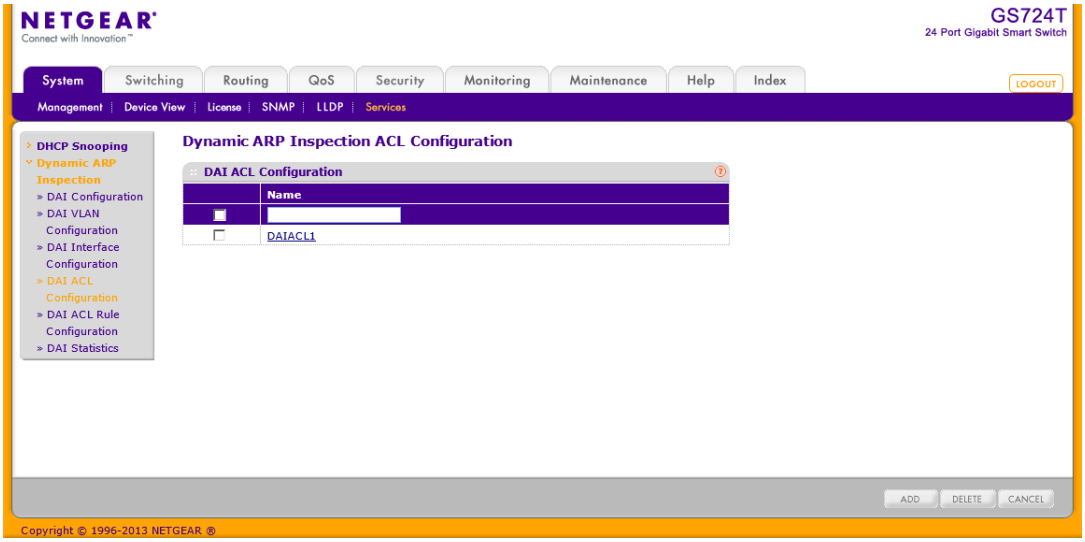
DAI は ARP パケットを検査するために DHCP スヌーピングバインディングデータベースの情報を使用します。DHCP を使わず、スタティック（固定）IP アドレスを使用しているネットワークでは、DAI ACL(アクセスコントロールリスト)を使って VLAN 中の IP アドレスと MAC アドレスを固定的に

関連付けることができます。固定 IP アドレスの場合、DHCP スヌーピング機能はバインディングデータベースを構築することができません。DAI ACL は他のスイッチが DAI を実行しない場合にも役に立ちます。

DAI は DHCP スヌーピングバインディングデータベースに問い合わせる前に、DAI ACL に設定された固定的な組み合わせを問い合わせます。もしも、VLAN で Static Flag 設定が有効になっている場合、DAI ACL は ARP ACL のみの検証を行い、DHCP スヌーピングバインディングデータベースの問い合わせは行いません。

DAI ACL 設定をする

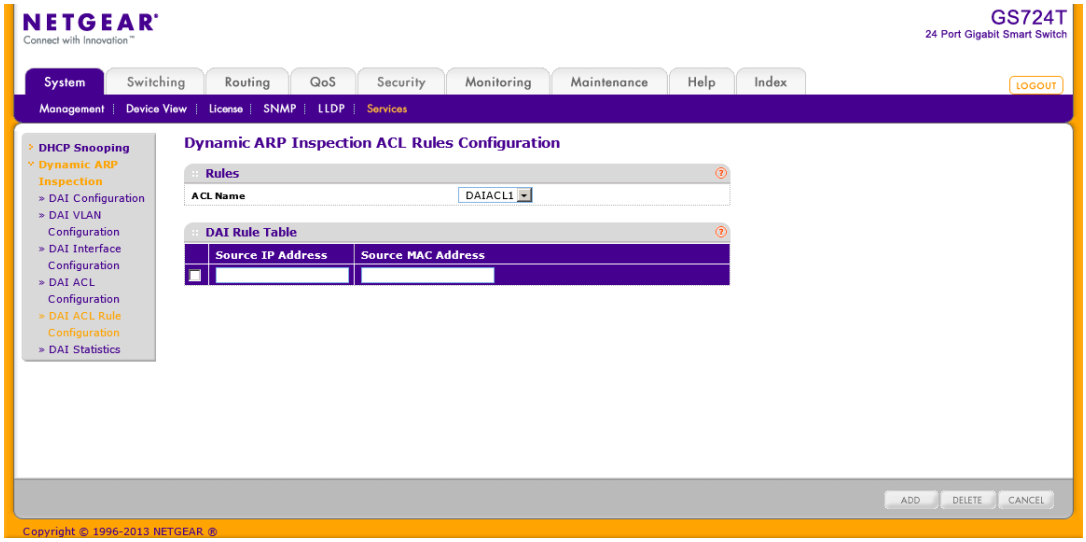
1. **System** > **Services** > **Dynamic ARP Inspection** > **DAI ACL Configuration** を選択して **DAI ACL Configuration** ページを表示します。



2. **Name**：DAI ACL の名前を入力します。
3. **Add** ボタンをクリックして DAI ACL を追加します。
4. DAI ACL を削除するには、削除する DAI 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. **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。

DAI ACL ルールを設定する

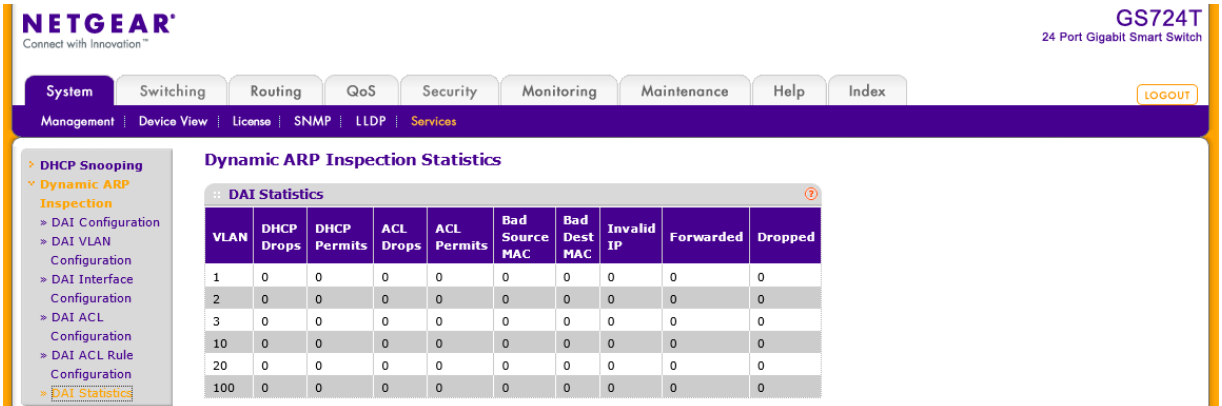
1. System > Services > Dynamic ARP Inspection > DAI ACL Rules Configuration を選択して DAI ACL Rules Configuration ページを表示します。



2. ACL Name：DAI ACL を選択します。
3. Dai Rule Table で以下の情報を入力します。
   - Source IP Address：デバイスの MAC アドレスを入力します。
   - Source MAC Address：IP アドレスに対応する MAC アドレスを入力します。
4. Add ボタンをクリックして DAI Rule を追加します。
5. 必要に応じて 3.4.を繰り返します。
6. DAI Rule を削除するには、削除する DAI Rule 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
8. DAI VLAN 設定で VLAN に DAI ACL を割り当てます。

DAI 統計を確認する

System > Services > Dynamic ARP Inspection > DAI Statistics を選択して DAI Statistics ページを表示します。



DAI Statistics は DAI の統計情報を表示します。

以下に **DAI Statistics** の表の項目の説明を示します。

項目	説明
VLAN	統計情報を表示する VLAN ID
DHCP Drops	DHCP スヌーピングバインディングに一致せず廃棄された ARP パケット数。
DHCP Permits	DHCP スヌーピングバインディングに一致し転送された ARP パケット数。
ACL Drops	ARP ACL ルールに一致せず廃棄された ARP パケット数。
ACL Permits	ARP ACL ルールに一致し転送された ARP パケット数。
Bad Source MAC	送信元 MAC アドレスに一致せず廃棄された ARP パケット数。
Bad Dest MAC	宛先 MAC アドレスに一致せず廃棄された ARP パケット数。
Invalid IP	無効な IP アドレスとして廃棄された ARP パケット数。
Forwarded	有効な ARP パケットとして転送された ARP パケット数。
Dropped	無効な ARP パケットして廃棄された ARP パケット数。

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。

スイッチング設定

スイッチングタブからアクセスできる機能を使ってレイヤー2 機能を定義します。スイッチングタブは以下の機能を含みます。

- ポート（Ports）
- リンクアグリゲーショングループ（Link Aggregation Groups）
- VLAN
- オート VoIP 設定（Auto-VoIP Configuration）
- スパニングツリープロトコル（Spanning Tree Protocol）
- マルチキャスト（Multicast）
- MVR 設定（MVR Configuration）
- アドレステーブル（Address Table）
- Multiple Registration Protocol Configuration
- 802.1AS

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)

Port Configuration ページでスイッチの物理インターフェースと LAG を設定します。

Port Configuration

Port Configuration

1 LAGS All Go To Interface GO

	Port	Description	Port Type	Admin Mode	Port Speed	Physical Status	Link Status	Link Trap	Maximum Frame Size (1518 to 9216)	MAC Address	PortList Bit Offset	ifindex
☐	g1			Enable	Auto	1000 Mbps	Link Up	Enable	1518	C4:04:15:A0:69:30	1	1
☐	g2			Enable	Auto		Link Down	Enable	1518	C4:04:15:A0:69:30	2	2
☐	g3			Enable	Auto		Link Down	Enable	1518	C4:04:15:A0:69:30	3	3
☐	g4			Enable	Auto		Link Down	Enable	1518	C4:04:15:A0:69:30	4	4
☐	g5			Enable	Auto		Link Down	Enable	1518	C4:04:15:A0:69:30	5	5
☐	g6			Enable	Auto		Link Down	Enable	1518	C4:04:15:A0:69:30	6	6
☐	g7			Enable	Auto		Link Down	Enable	1518	C4:04:15:A0:69:30	7	7
☐	g8			Enable	Auto		Link Down	Enable	1518	C4:04:15:A0:69:30	8	8
☐	g9			Enable	Auto		Link Down	Enable	1518	C4:04:15:A0:69:30	9	9
☐	g10			Enable	Auto		Link Down	Enable	1518	C4:04:15:A0:69:30	10	10
☐	g11			Enable	Auto		Link Down	Enable	1518	C4:04:15:A0:69:30	11	11
☐	g12			Enable	Auto		Link Down	Enable	1518	C4:04:15:A0:69:30	12	12
☐	g13			Enable	Auto	1000 Mbps	Link Up	Enable	1518	C4:04:15:A0:69:30	13	13
☐	g14			Enable	Auto		Link Down	Enable	1518	C4:04:15:A0:69:30	14	14
☐	g15			Enable	Auto	1000 Mbps	Link Up	Enable	1518	C4:04:15:A0:69:30	15	15
☐	g16			Enable	Auto		Link Down	Enable	1518	C4:04:15:A0:69:30	16	16
☐	g17			Enable	Auto		Link Down	Enable	1518	C4:04:15:A0:69:30	17	17
☐	g18			Enable	Auto		Link Down	Enable	1518	C4:04:15:A0:69:30	18	18

1 LAGS All Go To Interface 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. 1 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、LAG(Link Aggregation Group)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。
     - Trunk Member：ポートは LAG の、メンバーです。

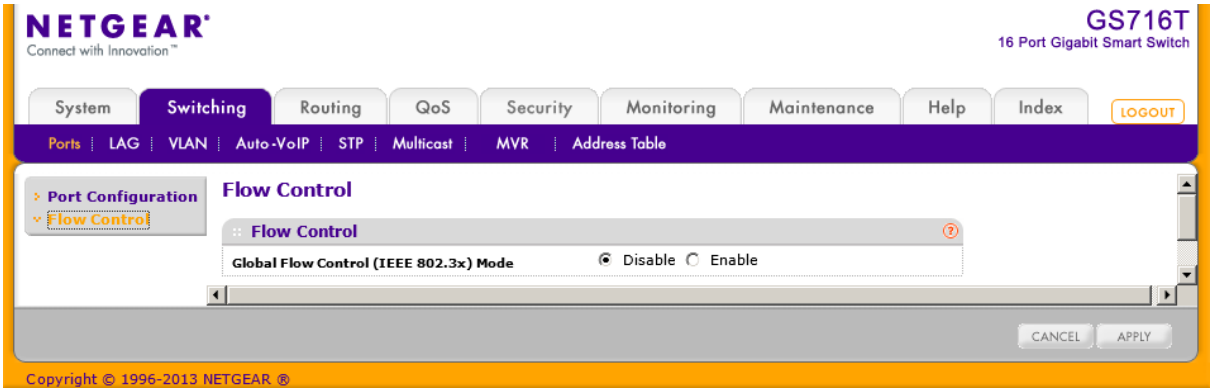
- **Mirrored**：ポートはミラーされるポートです。
- **Probe**：ポートはモニターポートです。

- **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。
- **Physical Status**：物理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**：リンクのアップ（**Link Up**）、リンクのダウン（**Link Down**）を表示します。
- **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。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。



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。

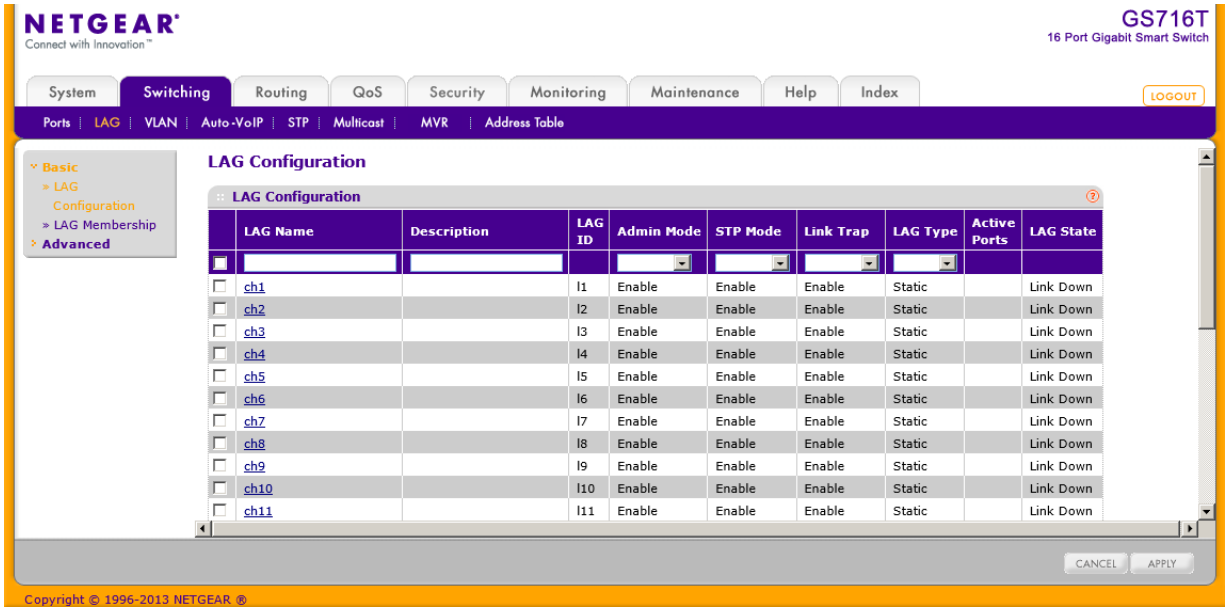
スタティック LAG の場合、LAG PDU の送受信はしません。ネットギアスイッチは最大 26 の LAG をサポートしています。(GS716T の場合は 9、GS724T の場合は 13、GS748T の場合は 26 となります)

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。

LAG 設定をする

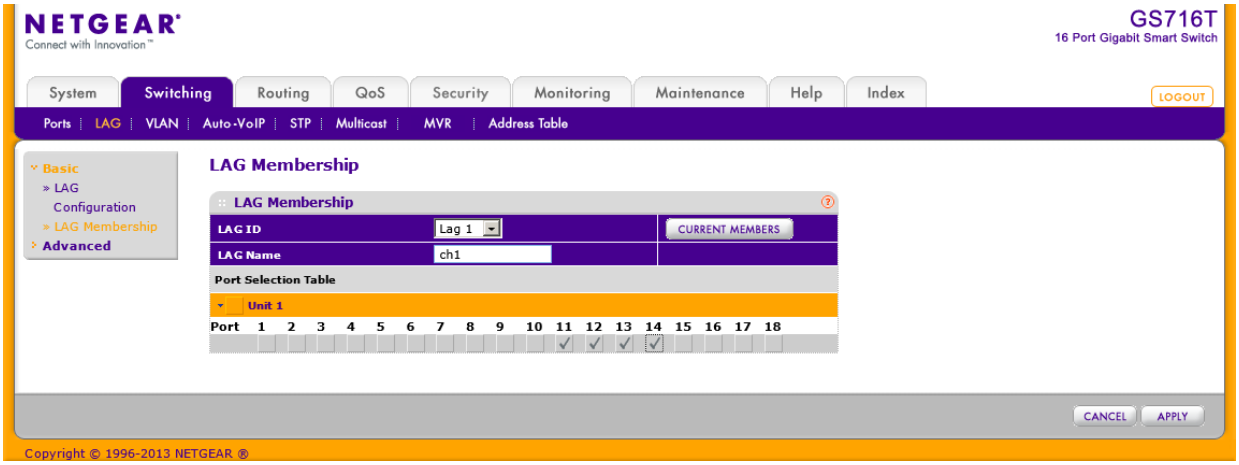
1. Switching > LAG > Basic > LAG Configuration を選択して LAG Configuration ページを表示します。
2. 設定をする LAG のチェックボックスを選択します。複数を選択して共通項目の設定をすることもできます。
3. 以下の項目を確認および設定をします。
   - LAG Name：LAG の名前を記入します。長さは英数 15 文字までです。
   - Description：LAG の説明を記入します。長さは英数 64 文字までです。
   - LAG ID：LAG に割り当てられた番号を表示します。この欄は読み取りのみです。
   - 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（Enable）です。
   - STP Mode：LAG の STP モードを設定します。
   - 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。デフォルトは有効(Enable)です。
   - 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 8 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)

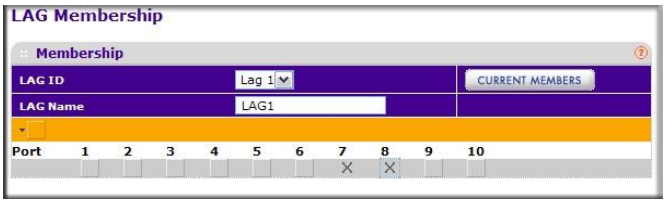
LAG Membership ページを使って LAG を構成します。

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。

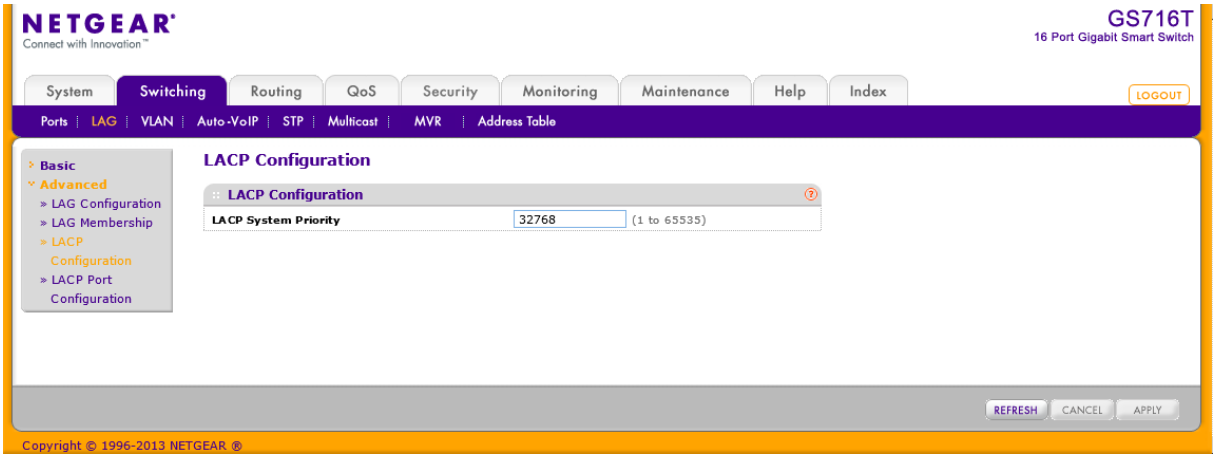


2. LAG ID: 設定する LAG を選択します。
3. LAG Name: LAG の名前を記入します。英数 15 文字までです。
4. オレンジのバーを選択してポートを表示します。
5. LAG にするポートの下のボックスをクリックして選択します。以下の図はポート 7 と 8 を LAG にする例です。



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)

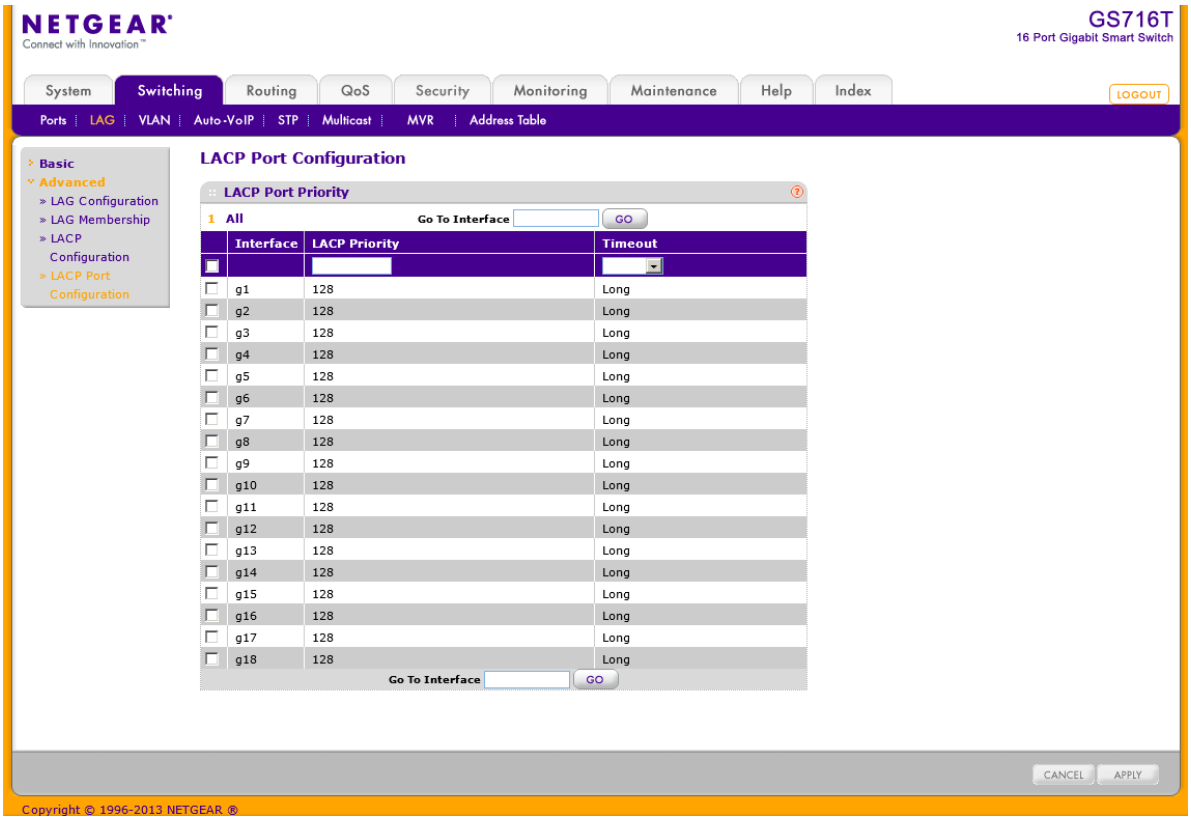


LACP を設定する

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)

LACP ポート設定ページでポートの LCAP プライオリティ値と LACP タイムアウト値を設定します。



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 ヘッダー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）

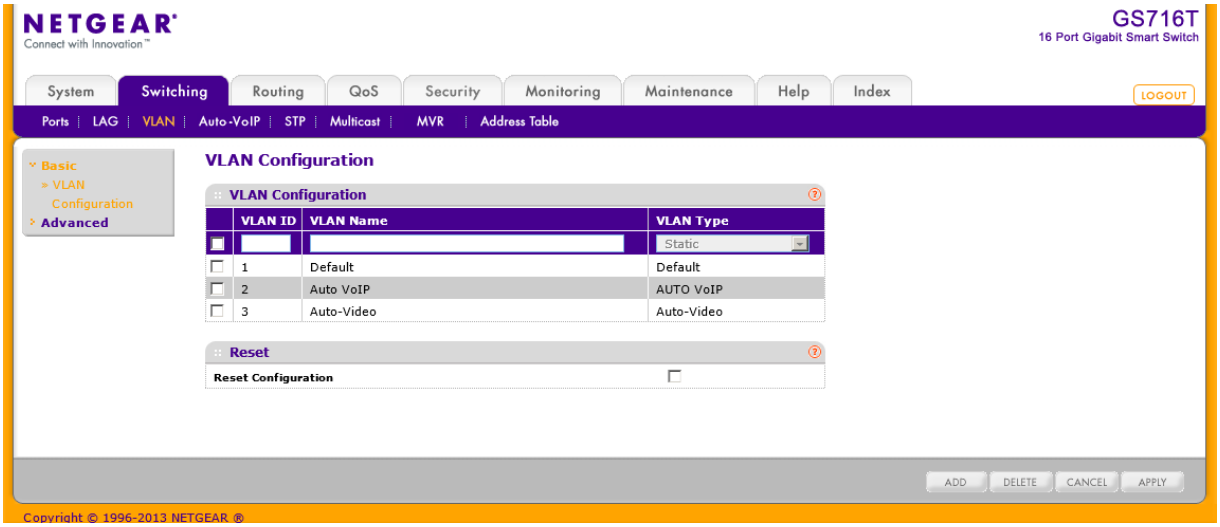
基本 VLAN 設定(Basic VLAN Configuration)

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。ネットギアスイッチは最大 256 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、すべてのポートはタグ無し(Untagged)メンバーです。VLAN タイプは常に **Static** です。

- **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。

VLAN を追加する

1. Switching > VLAN > Basic > VLAN Configuration を選択して. VLAN Configuration ページを表示します。



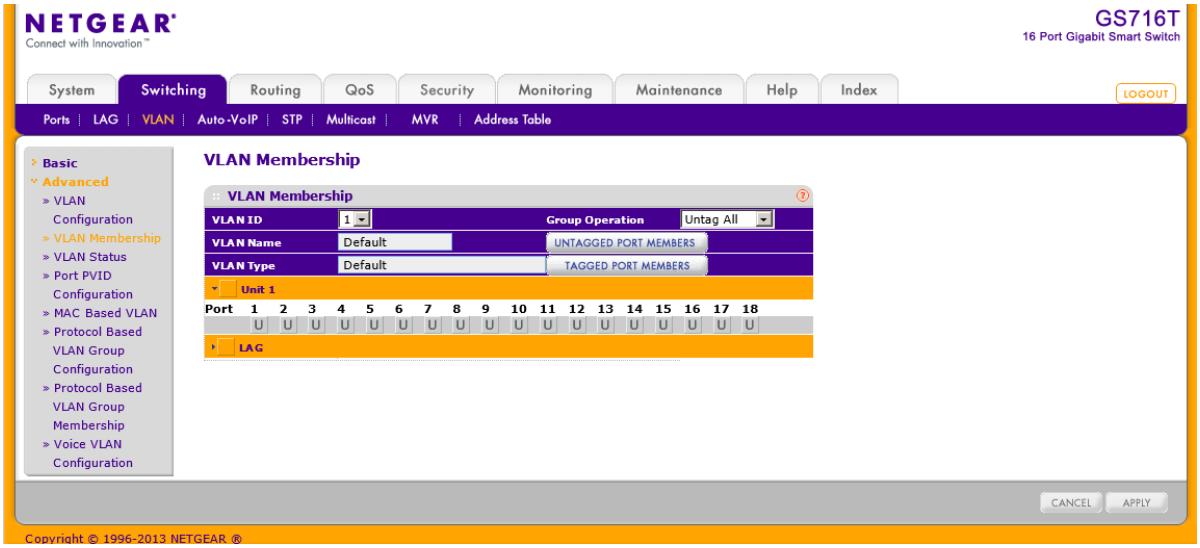
2. VLAN を追加するには、VLAN ID、VLAN 名（VLAN Name）、VLAN タイプ（VLAN Type）を設定し、Add ボタンをクリックします。
   - VLAN ID：新しい VLAN ID を入力します。VLAN ID の範囲は 1-4093 です。
   - VLAN Name：VLAN 名を記入できます。英数字の 32 文字までです。空白でも構いません。デフォルトは空白です。VLAN ID 1 の VLAN 名は常に Default です。
   - VLAN Type：VLAN のタイプを指定します。タイプは Static のみが設定可能です。デフォルトの3つの 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

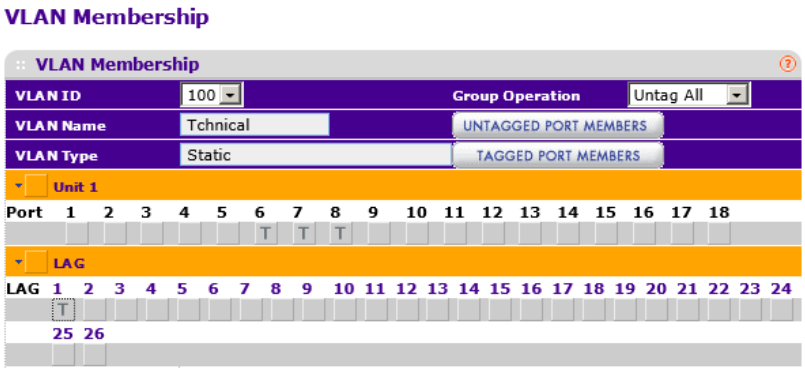
VLAN メンバーシップを設定する

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。

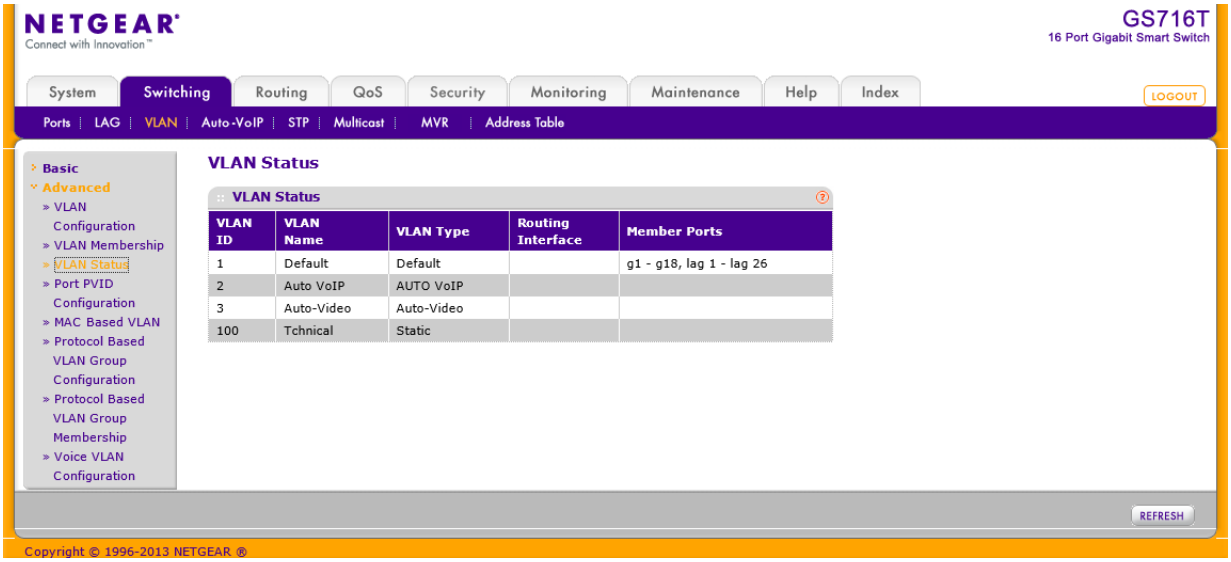
以下の図で、ポート g6, g7, g8 および LAG 1 が VLAN100 のタグ付きポートに設定されています。



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 Al：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。

VLAN ステータス（VLAN Status）

VLAN Status 画面で現在設定された VLAN 状態を確認することができます。



VLAN ステータスを確認する

1. Switching > VLAN > Advanced > VLAN Status を選択して VLAN Status ページを表示します。
2. 以下の VLAN ステータス情報を確認します。
   - VLAN ID：VLAN ID。範囲は 1-4093。
   - VLAN Name：VLAN の名前。VLAN 1 は常に Default です。
   - VLAN Type：VLAN のタイプ。
   - Default：（VLAN ID = 1）常に存在します。

- **Static**：管理者が作成・設定した VLAN。
- **Dynamic**：GVRP(Generic VLAN Registration Protocol)の登録によって作成された VLAN。以下のタイプは Dynamic です。
  AUTO VoIP, MVRP, L2 Tunnel, IP VLAN, DOT1X, OPENFLOW, Auto-Video
- **Routing Interface**：ルーティングインターフェース。
- **Member Ports**：VLAN に含まれるポート。

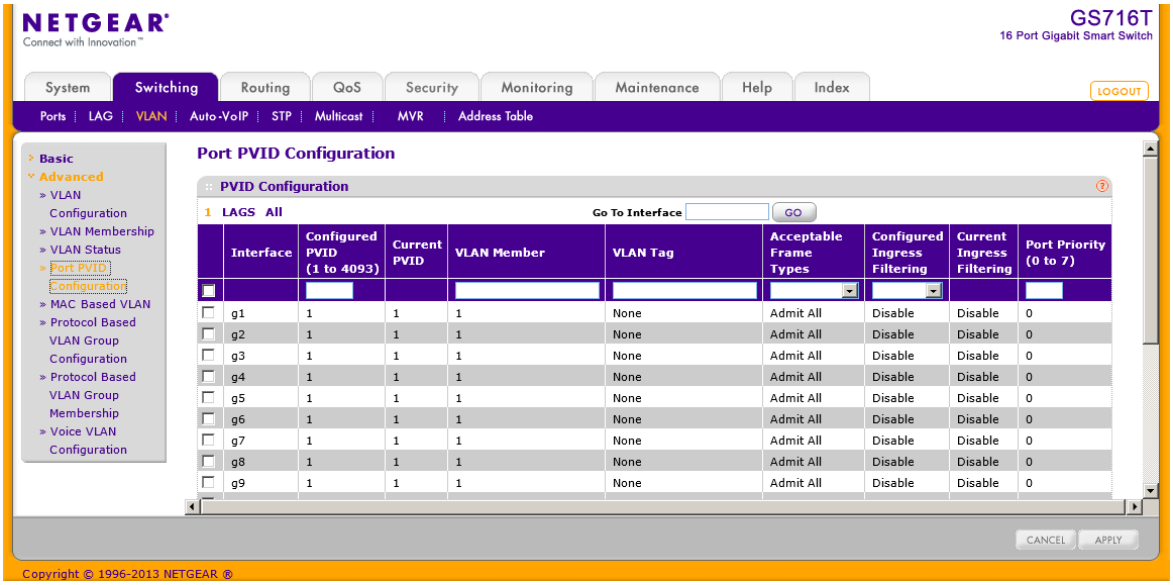
ポート VLAN 設定（Port VLAN ID Configuration）

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。
PVID にはいくつかの要件があります。

- 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。

PVID 情報を設定する

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. 1 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。
7. VLAN Member:ポートがメンバーの VLAN ID または VLAN のリストを設定します。VLAN ID の範囲は 1-4093 です。範囲で指定する場合は VLAN ID 間を"-"で結びます。(例:10-20)複数の VLAN ID を指定するには","で区切ります。(例:3,7,8,9)デフォルトは1です。
8. VLAN Tag:ポートでタグをつけたフレームを送信したい場合に設定します。範囲で指定する場合は VLAN ID 間を"-"で結びます。(例:10-20)複数の VLAN ID を指定するには","で区切ります。(例:3,7,8,9)デフォルトに戻す場合、タグを使わない場合は None を入力します。
9. 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。
10. Configured 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。
11. 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。
12. 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。
13. 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。

MAC ベース VLAN(MAC-Based VLAN)

MAC ベース VLAN 機能は受信するタグ無しパケットの送信元 MAC アドレスを使ってトラフィックを分類し、パケットを適切な VLAN に割り当てます。

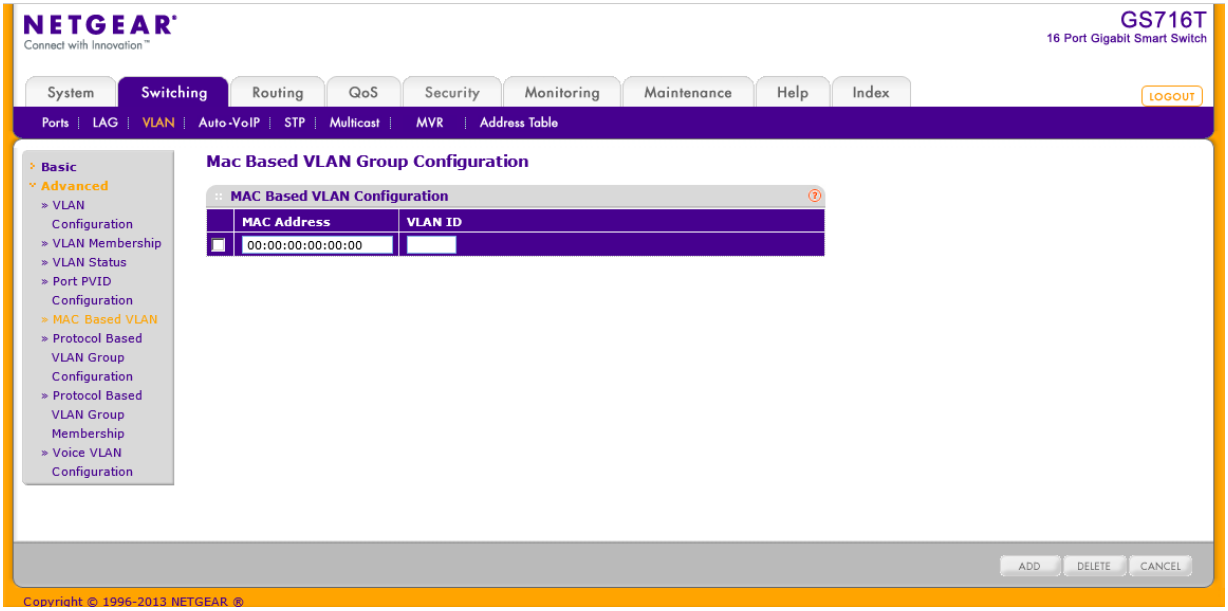
MAC と VLAN のマッピングは MAC to VLAN テーブルを設定することに定義されます。テーブル要素は送信元 MAC アドレスとそれに対応する VLAN ID で記述されます。MAC to VLAN 設定はスイッチのすべてのポートで共有されます。

タグ付きあるいはプライオリティタグのみのパケットがスイッチに到達し、パケットの送信元 MAC アドレスが MAC to VLAN に存在する場合、パケットの送信元 MAC アドレスが検索されます。一

致した場合は、対応する VLAN ID がパケットに割り当てられます。プライオリティタグ付きのパケットの場合、この値は保持されます。それ以外の場合、プライオリティは 0 に設定されます。割り当てられた VLAN ID が VLAN ID テーブルで検証されます。もしも VLAN が有効ならば、入力パケットの処理は継続され、それ以外の場合、パケットは廃棄されます。システムで作成されていない VLAN へのマッピングを設定することも可能です。

MAC ベース VLAN を設定する

1. **Switching** > **VLAN** > **Advanced** > **MAC Based VLAN** を選択して **MAC Based VLAN** ページを表示します。



2. **MAC Address**：VLAN ID に関連付ける MAC アドレスを指定します。
タグなしのパケットでこの送信元 MAC アドレスを持つパケットは VLAN に関連付けられます。
3. **VLAN ID**：関連付ける VLAN ID を指定します。
タグなしのパケットでこの送信元 MAC アドレスをポートまたは LAG で受信した場合に、この VLAN ID のタグが付与されます。
4. **Add** ボタンをクリックします。

プロトコルベース VLAN グループ設定（Protocol-Based VLAN Group Configuration）

タグなしのパケットの分類にプロトコルベース VLAN を使うことができます。デフォルトでは、タグなしのパケットは VLAN 1 に割り当てられます。ポートベース VLAN あるいはプロトコルベース VLAN を設定することによって、この動作を変更することができます。タグ付きのパケットはプロト

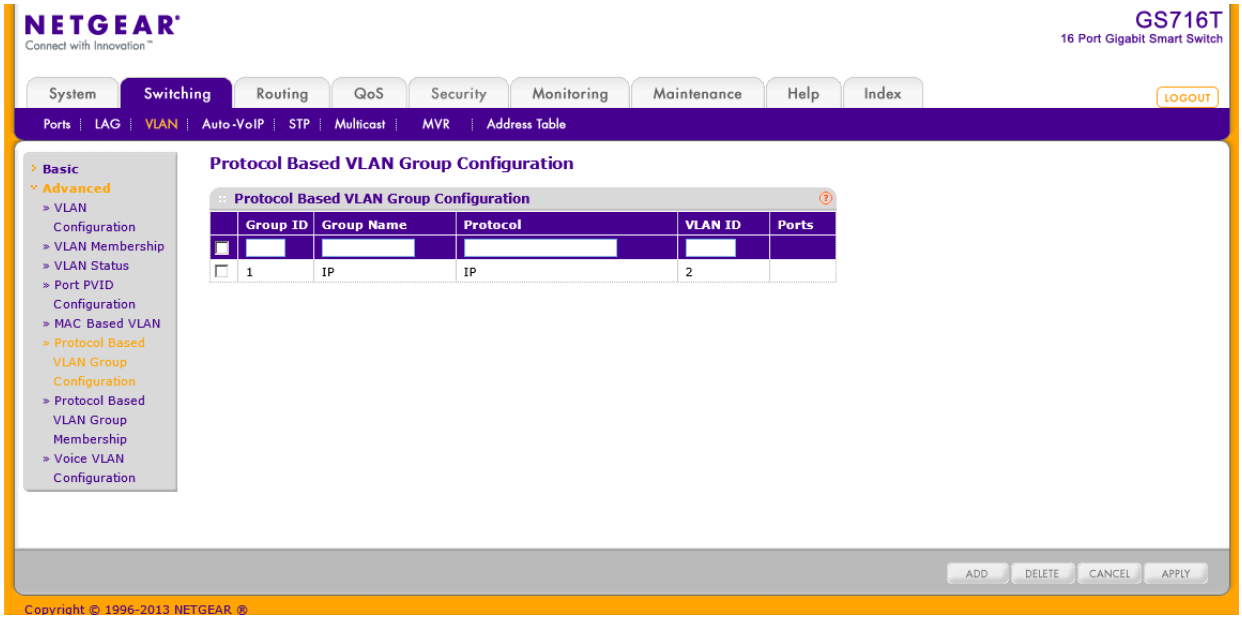
コル VLAN ではなく、IEEE802.1Q にしたがって処理されます。

ポートを特定のプロトコルに対してプロトコル VLAN に割り当てると、ポートで受信されたそのプロトコルのタグなしのフレームには設定されたプロトコルベース VLAN ID が割り当てられます。ポートで受信されたその他のプロトコルのフレームはデフォルト PVID(1)あるいはポート VLAN 設定で指定した VLAN ID が割り当てられます。

グループを作ることによってプロトコルベース VLAN を定義します。それぞれのグループは VLAN ID とは一対一の関連が付けられ、1～3 個プロトコル設定を持ち、複数のポートを含みます。グループを作成するときに、名前を選択し、グループ ID は自動的に割り当てられます。

プロトコルベース VLAN グループを設定する

1. **Switching** > **VLAN** > **Advanced** > **Protocol-Based VLAN Group Configuration** を選択して **Protocol-Based VLAN Group Configuration** ページを表示します。



2. **Group ID**：グループを識別する番号を設定します。範囲は 1-128 です。
3. **Group Name**：グループ名を指定します。英数 16 文字までです。
4. **Protocol**：プロトコル VLAN に含めるプロトコルを指定します。
   入力可能なものは、”IP”, “ARP”,”IPX”および 16 進または 10 進のイーサタイプ値（0x0600(1536)-0xFFFF(65535)）です。プロトコルを”,”で区切って複数指定することができます。
5. **VLAN ID**：プロトコルベース VLAN に割り当てる VLAN ID を指定します。
   グループのポートで受信したタグなしのフレームでこのグループに含めたプロトコルのものに VLAN ID が割り当てられます。
6. **Ports**：グループに属するメンバーポートを表示します。

7. Add ボタンをクリックします。

プロトコルベース VLAN を変更する

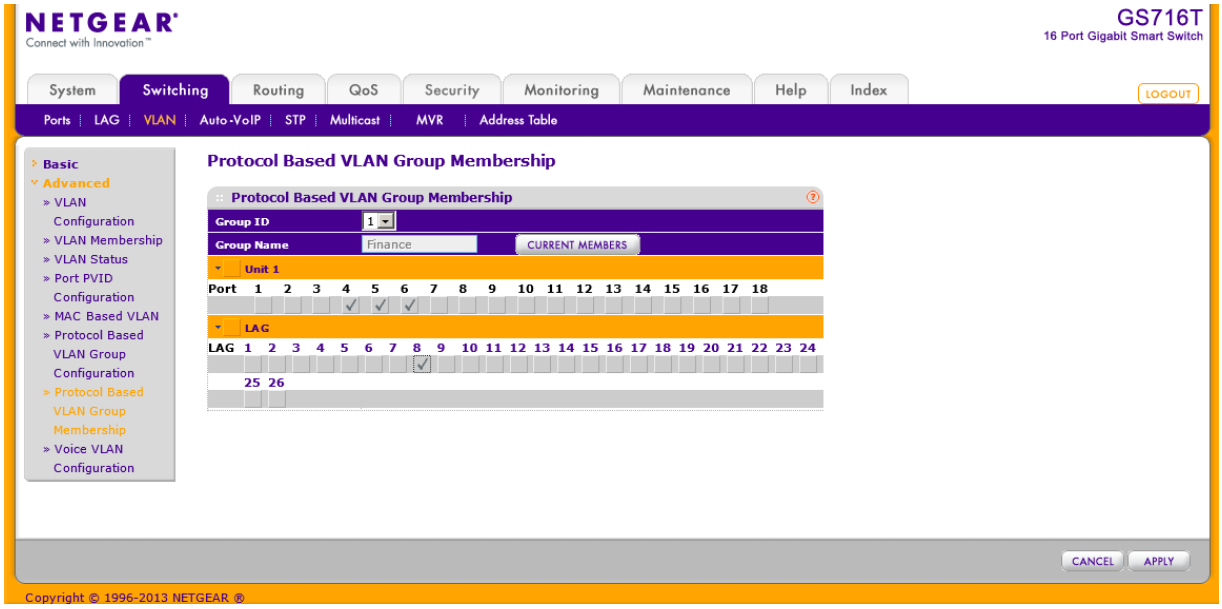
8. 更新するプロトコルベース VLAN のチェックボックスを選択します。
9. 項目を変更します。
10. Apply ボタンをクリックします。

プロトコルベース VLAN グループを削除する

11. 削除するプロトコルベース VLAN のチェックボックスを選択します。
12. Delete ボタンをクリックします。

プロトコルベース VLAN グループメンバーシップを設定する

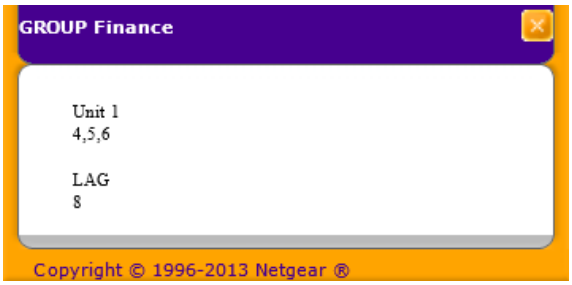
1. Switching > VLAN > Advanced > Protocol-Based VLAN Group Membership を選択して Protocol-Based VLAN Group Membership ページを表示します。
2. Group ID：プロトコル VALN グループ ID を選択します。
3. オレンジのバーをクリックしてインターフェースのリストを表示します。
   プロトコルベース VLAN グループに追加するインターフェースを選択します。



一つのインターフェースは一つのグループにのみ所属できます。

4. Group Name：グループ名が表示されます。
5. Apply ボタンをクリックします。

6. **Current Members** ボタンをクリックして選択したプロトコルベース VLAN グループのメンバーを表示できます。

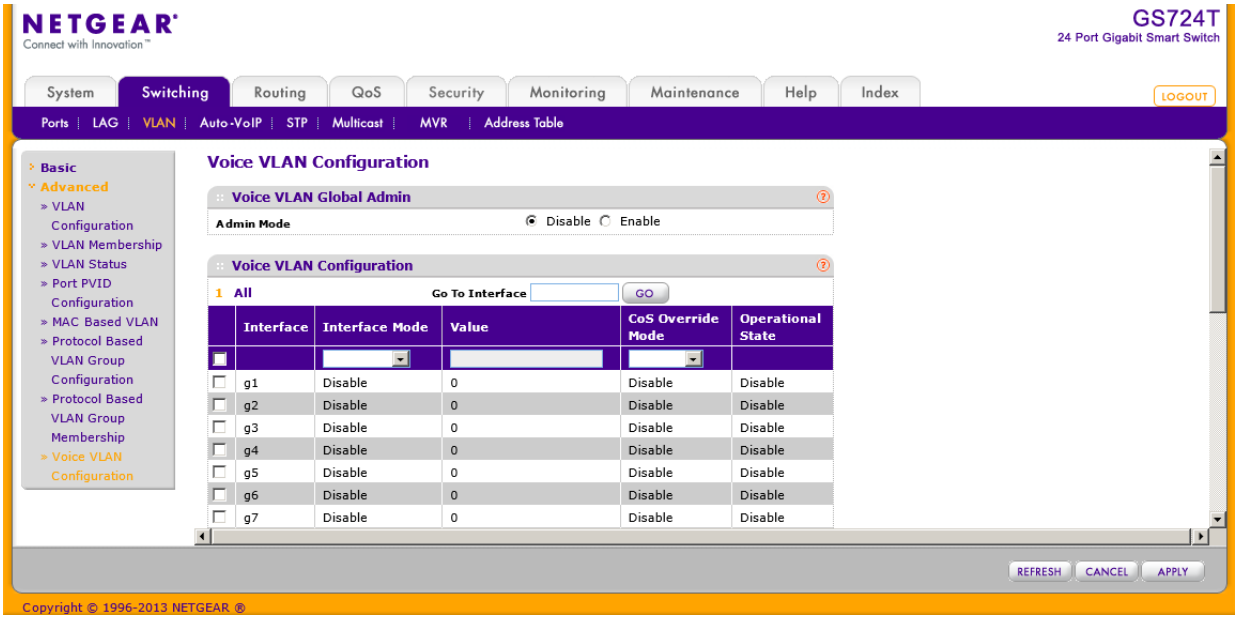


ボイス VLAN(Voice VLAN)

IP 電話機からのトラフィックを運ぶポートに対してボイス 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。

ボイス VLAN を設定する

1. **Switching** > **VLAN** > **Advanced** > **Voice VLAN Configuration** を選択して **Voice VLAN Configuration** ページを表示します。



2. **Admin Mode** でスイッチのボイス VLAN のグローバル設定を有効(Enable)にします。
3. 設定をするインターフェースをチェックボックスで選択します。
4. **Interface Mode**:Voice VLAN モードを以下から選択します。
   - **Disable**:無効(デフォルト)
   - **None**:IP 電話機にタグなしの音声トラフィックを送信させます。

- **VLAN ID**：ボイス VLAN ID を Value 欄に指定します。
- **Dot1p**：802.1p プライオリティを Value 欄に指定します。
- **Untagged**：タグなしトラフィックを使用します。

5. **Value**：VLAN ID または dot1p 値を設定します。
6. **CoS Override Mode**：以下から選択します。
   - **Enable**：ポートはイーサネットフレームの 802.1p 設定を無視します。
   - **Disable**：ポートは受信したフレームの 802.1p 設定を信頼します。
7. **Apply** ボタンをクリックします。

オート VoIP 設定(Auto-VoIP Configuration)

VoIP(Voice over Intenet Iprotocol)はデータネットワーク上での電話を可能にします。音声はデータトラフィックよりも遅延に敏感なので、オート VoIP 機能は音声パケットに対して分類する仕組みを提供し、より良い QoS(Quality of Service)を提供するためにデータパケットよりも優先することを可能にします。オート VoIP 機能で、呼制御プロトコル(SIP,SCCP,H.323)あるいは OUI ビットに基づいて、音声の優先が提供されます。

プロトコルベースのオート VoIP 設定をする

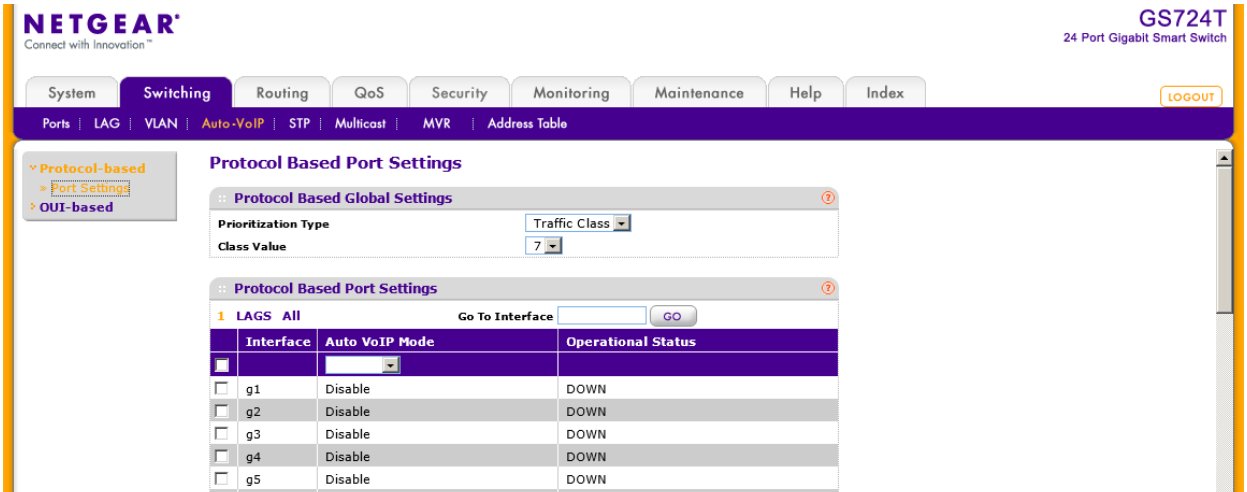
時間に敏感な音声トラフィックを優先するために、プロトコルベースのオート VoIP は以下の VoIP プロトコルを運ぶパケットを検出します。

- SIP(Session Initiation Protocol)
- H.323
- SCCP(Signalling Connection Control Part)

オート VoIP 機能が有効にされたポートで受信された VoIP フレームは特定の CoS 値に設定されます。

プロトコルベースポート設定をする

1. **Switching** > **Auto-VoIP** > **Protocol-Based** > **Port Settings** を選択して **Protocol Based Port Settings** ページを表示します。
2. **Prioritization Type**:呼制御プロトコル VoIP トラフィックを優先させる方式を選択します。
   - **Remark**:.入力インターフェースで音声トラフィックに指定した 802.1p プライオリティを再設定します。
   - **Traffic Class**:出力インターフェースで VoIP トラフィックに特定のトラフィッククラスを割り当てます。
3. **Class Value**:Remark CoS が設定された時、受信された音声パケットに割り当てる CoS タグ値を設定します。
4. Protocol Based Port Setting 欄で設定するインターフェースを選択します。
5. **Auto VoIP Mode**:Enable(有効)を選択してオート VoIP を有効にします。



6. Operational Status：インターフェースの状態を示します。
7. **Apply** ボタンをクリックします。

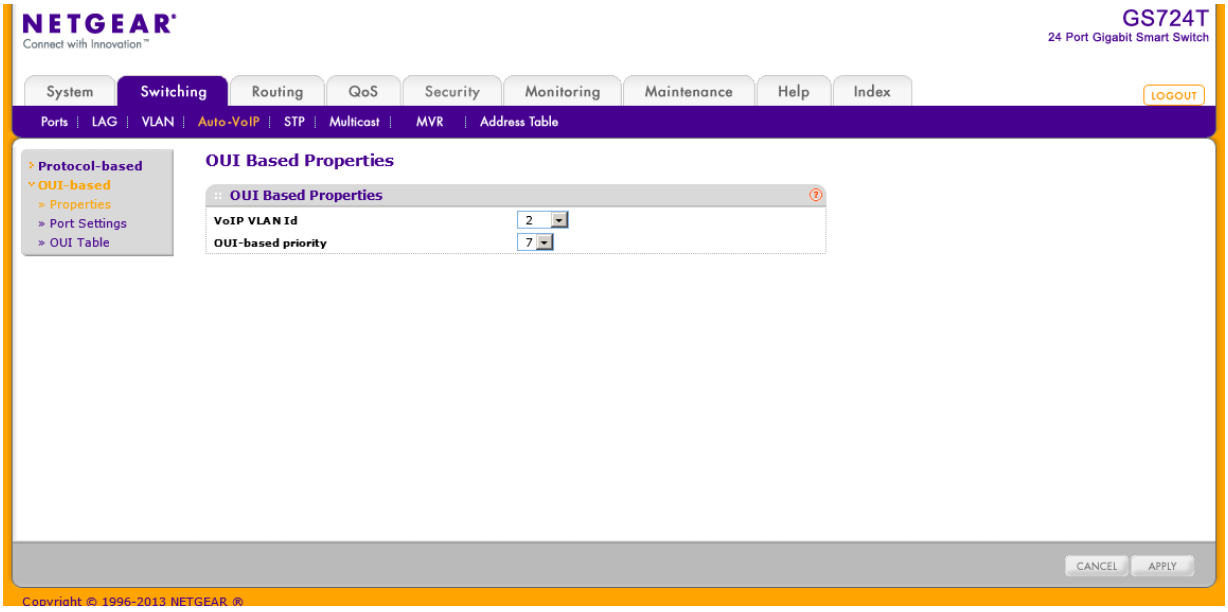
OUI ベースのオート VoIP 設定

OUI ベースのオート VoIP で、OUI ビットに基づいた音声の優先を提供します。

OUI ベースのオート VoIP 設定をする

1. **Switching** > **Auto-VoIP**> **OUI-based** > **Properties** を選択して **OUI Based Properties** ページを表示します。
2. **VoIP VLAN ID**：音声用の VLAN ID を選択します。
   OUI リストに一致する VoIP トラフィックは VoIP VLAN に割り当てられます。
3. **OUI-based priority**：OUI リストに一致したトラフィックに割り当てる 802.1p 優先度を選択します。
   オート VoIP モードが有効で、インターフェースで OUI が一致した場合、トラフィックにこの優先度を割り当てます。高いトラフィッククラスの値は一般的に時間に敏感なトラフィックに使われます。
4. **Apply** ボタンをクリックします。

OUI ポート設定（OUI Port Settings）



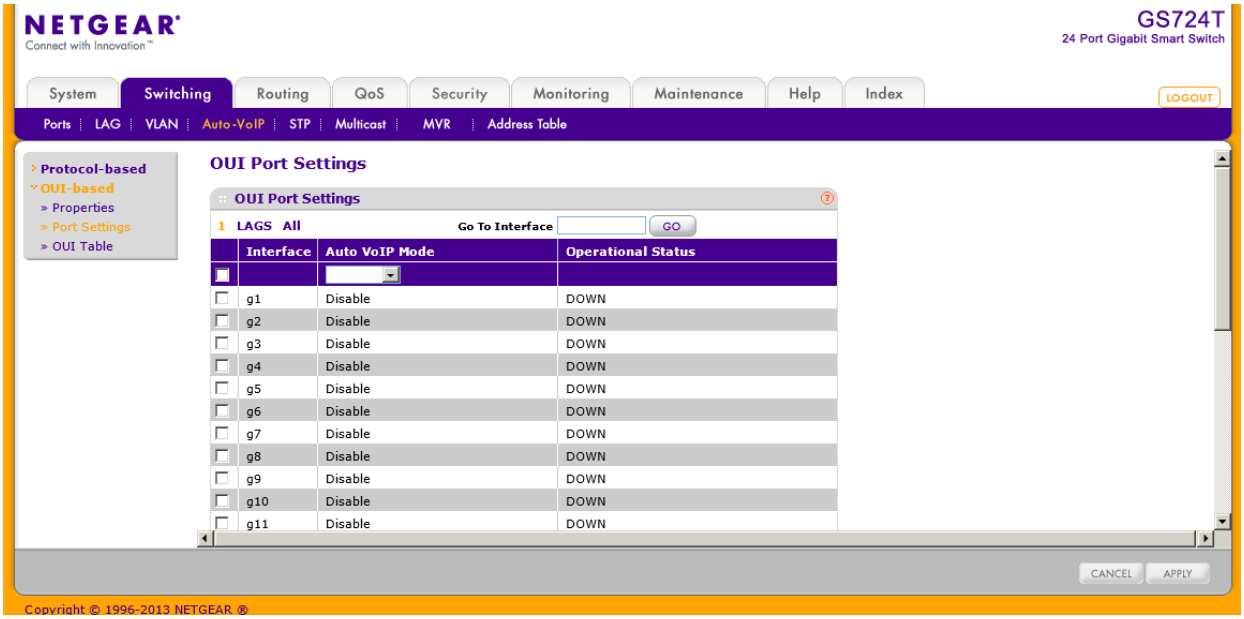
OUI Port Settings 画面で OUI ポート設定をします。

OUI ポート設定をする

1. Switching > Auto-VoIP > OUI-based > Port Settings を選択して OUI Port Settings ページを表示します。
2. 設定するインターフェースをチェックボックスで選択します。
3. Auto VoIP Mode：Enable（有効）を選択してインターフェースでオート VoIP を有効にします。
4. Operational Status：インターフェースのオート VoIP 状態を示します。
5. Apply をクリックします。

OUI テーブル（OUI Table）

デバイスハードウェアメーカーはハードウェアデバイスを認識するためにネットワークアダプター



に OUI(Organizationally Unique Identifier)を含めることができます。OUI は IEEE に登録された一意の 24 ビットの番号です。IP 電話メーカーを識別するために、スイッチには以下の OUI が設定されています。

- 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
- 00:04:13: SNOM

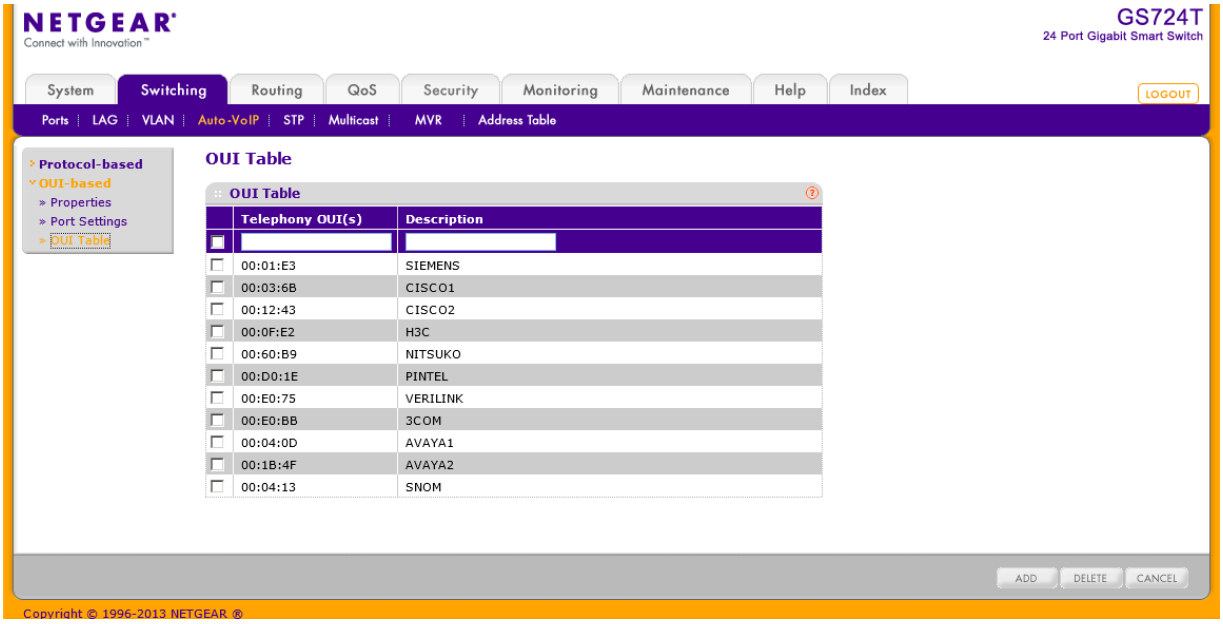
新しい OUI の設定や、OUI の情報を変更することができます。

OUI を追加する

1. **Switching** > **Auto-VoIP**> **OUI-based** > **OUI Table** を選択して **OUI Table** ページを表示します。
2. **Telephony OUI(s)**:OUI プレフィックスを指定します。
   OUI プレフィックスの形式は AA:BB:CC です。
3. **Description**:OUI に対応するメーカー名等を記入します。英数字 32 文字までです。
4. **Add** ボタンをクリックします。

OUI プレフィックスを削除する

5. 削除する OUI プレフィックスのチェックボックスを選択する。



6. **Delete** ボタンをクリックする。

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。

クラッシック 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。

MSTP(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。

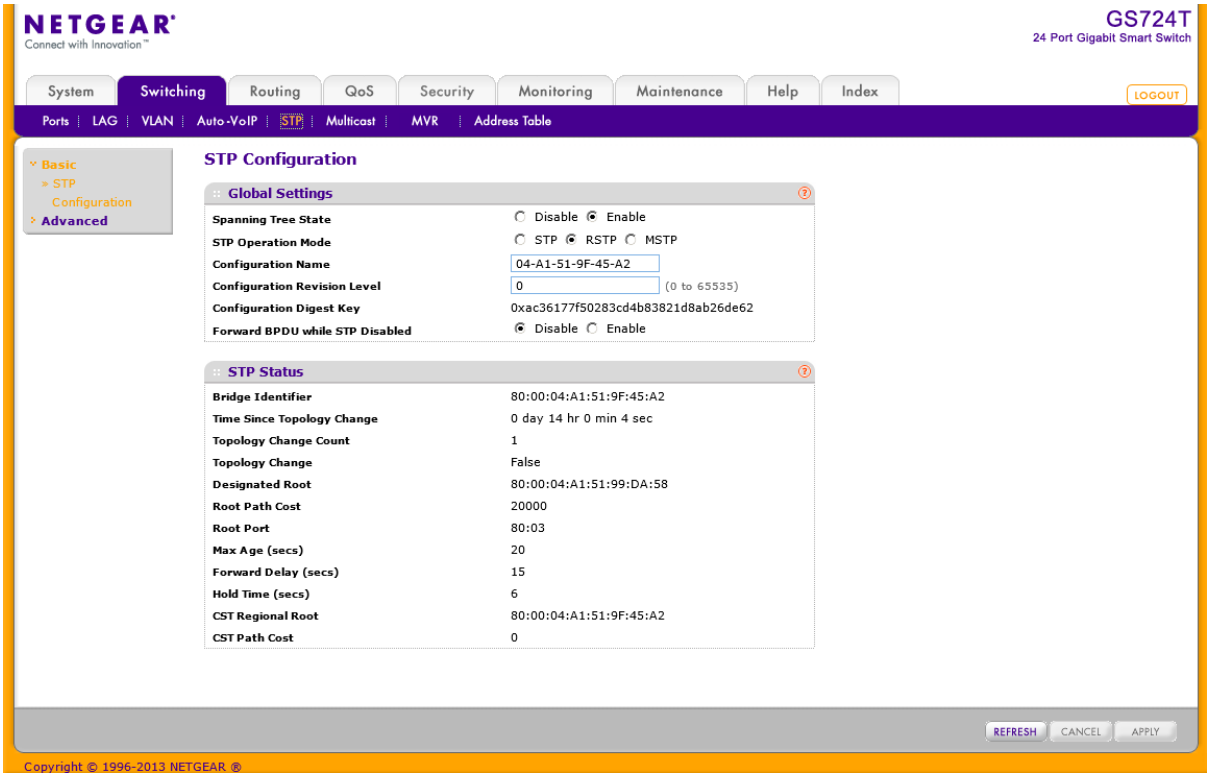
メモ: 2つのブリッジが混在する場合、動作するバージョンは 802.1s であるべきであり、設定、名前、digest key, revision level は一致するべきです。

STP リンクから以下の機能にアクセスできます。

- STP 設定(STP 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 設定（STP 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。



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。デフォルトは 0 です。

5. **Configuration Digest Key**:設定を特定するための情報。(読み取りのみ)
6. **Forward BPDU While STP Disabled**:STP が無効の際に、スパニングツリーBPDU を転送するかを指定します。この機能を有効(Enable)にすると、受信した BPDU パケットを他のポートにフラッディングされます。無効(Disable)にすると、受信した BPDU は転送されません。
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。

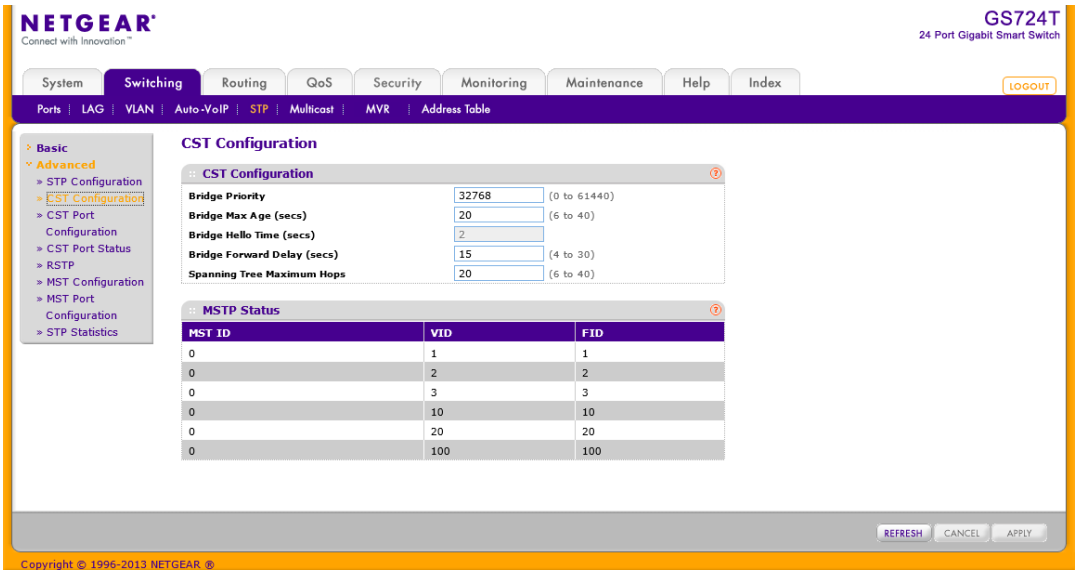
以下の表に **STP Status** 欄に表示される情報の説明を示します。

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 のルートへ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)

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



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。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 6-40 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。

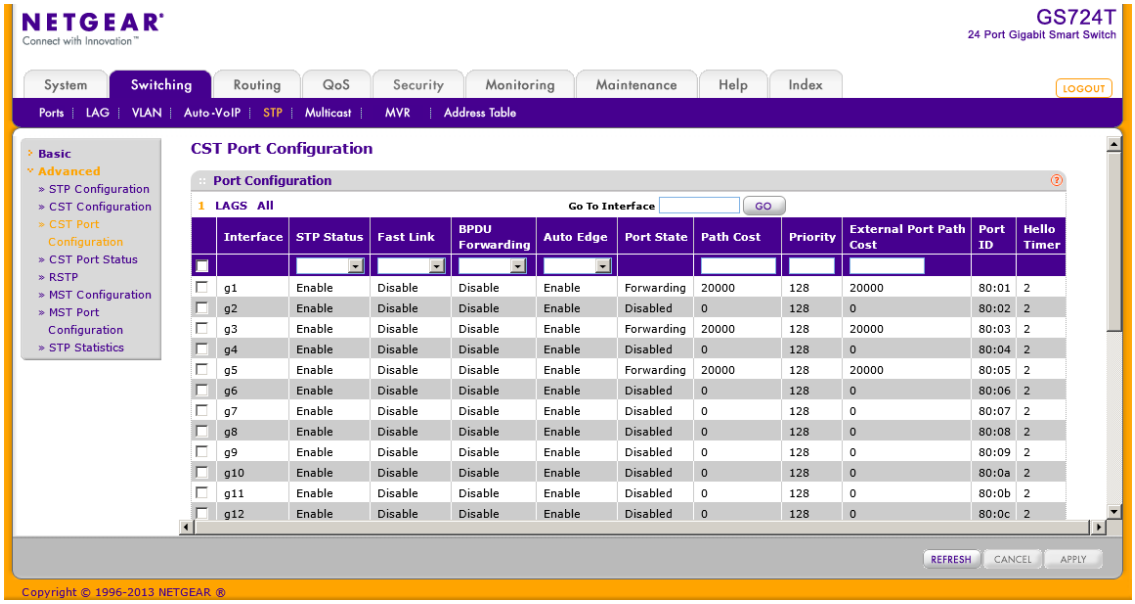
以下に **CST Configuration** ページの **MSTP Status** 欄に表示される情報の説明を示します。

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。



CST ポート設定をする。

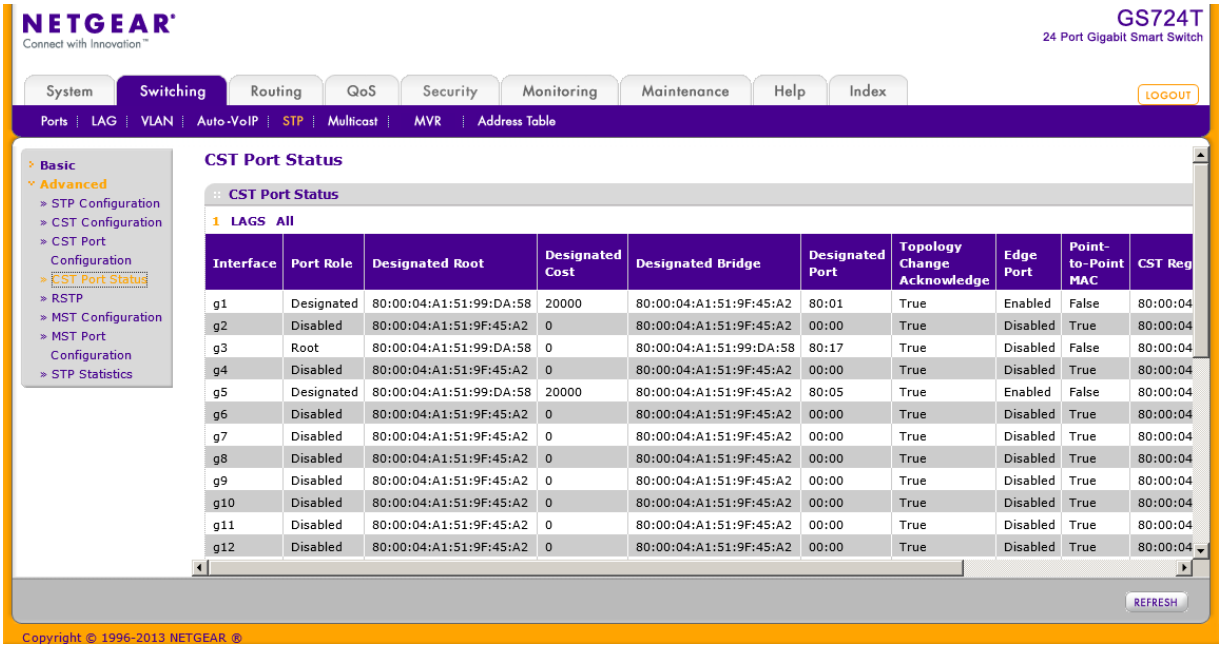
1. **Switching** > **STP** > **Advanced** > **CST Port Configuration** を選択して **CST Port Configuration** ページを表示します。
2. **1** をクリックして、物理ポートの CST 設定をします。
3. **LAGS** をクリックして、Link Aggregation Group (LAG)の CST 設定をします。
4. **ALL** をクリックして、物理ポートと Link Aggregation Group (LAG)の両方の CST 設定をします。
5. 設定をしたいポートまたは LAG 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。
   - **BPDU Forwarding**:スパニングツリーが無効の場合、BPDU を透過(Enable)するか透過しない(Disable)を設定します。
   - **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。範囲は 2-240 です。デフォルトは 128 です。
   - **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。



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。

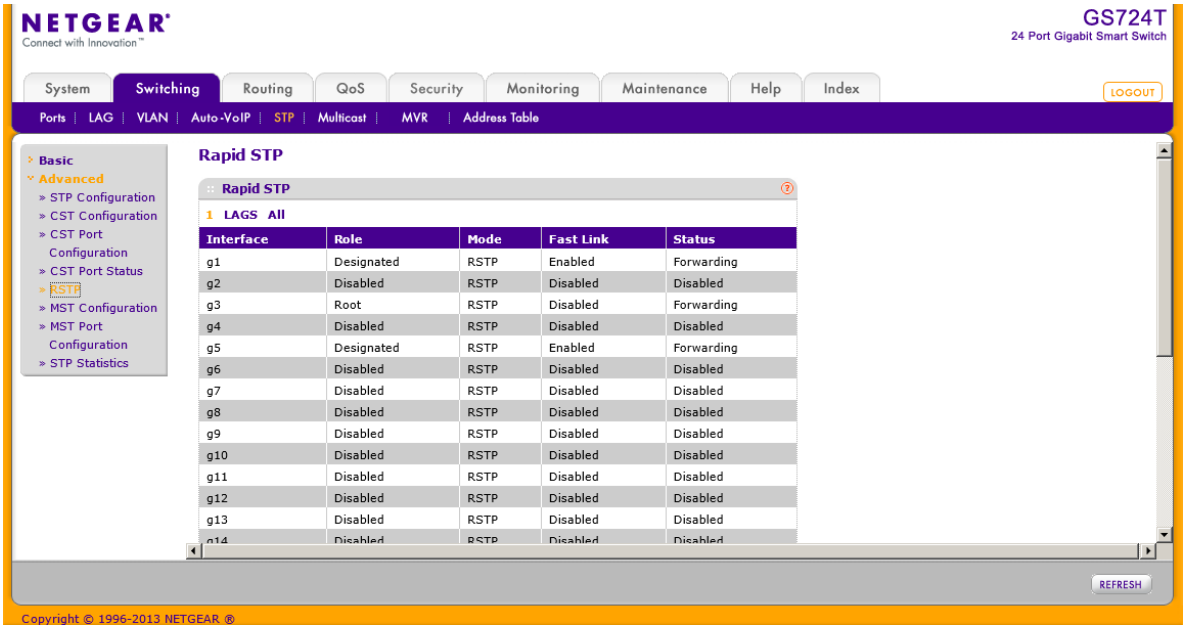
項目	説明
Interface	スイッチのインターフェース番号。
Port Role	ポートロール。以下のうちの一つ。Root Port, Designated Port, Alternate Port, Backup Port, Master Port, Disabled Port.
Designated Root	ルートブリッジ ID。
Designated Cost	STP トポロジーに参加しているポートのコスト。
Designated Bridge	ルートポートに接続されているブリッジのブリッジ ID。
Designated Port	ルートポートのポート ID。
Topology Change 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。



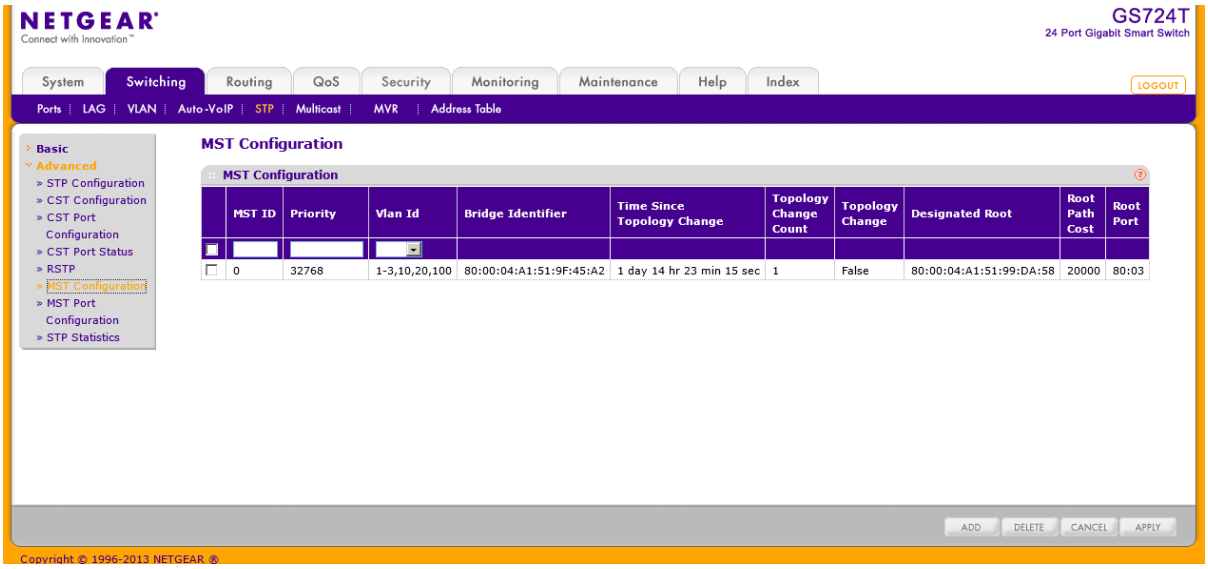
以下に Rapid STP 欄に表示される情報の説明を示します。

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。



MST を設定する。

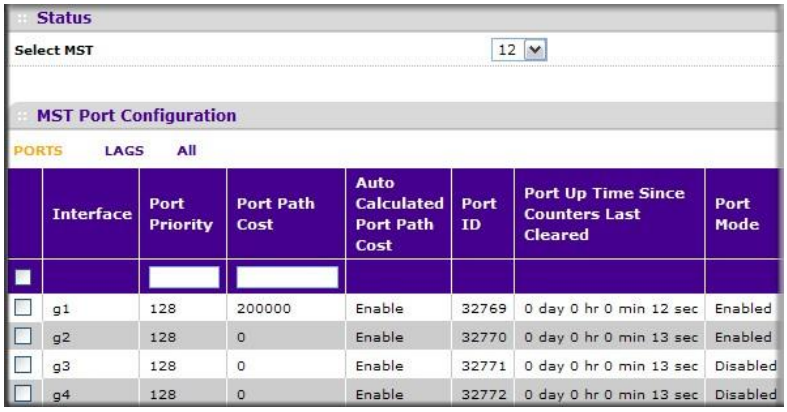
1. Switching > STP > Advanced > MST Configuration を選択して MST Configuration ページを表示します。
2. MST を追加するには、以下の情報を設定して Add ボタンをクリックします。
   - MST ID:MST ID を 1-4094 の範囲で記入します。
   - Priority:MST のブリッジプライオリティを設定します。BPDU の交換後一番小さなプライオリティのスイッチがルートブリッジになります。ブリッジプライオリティは 4096 の倍数になります。4096 の倍数以外に設定した場合は、その値より小さくかつ近い 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。

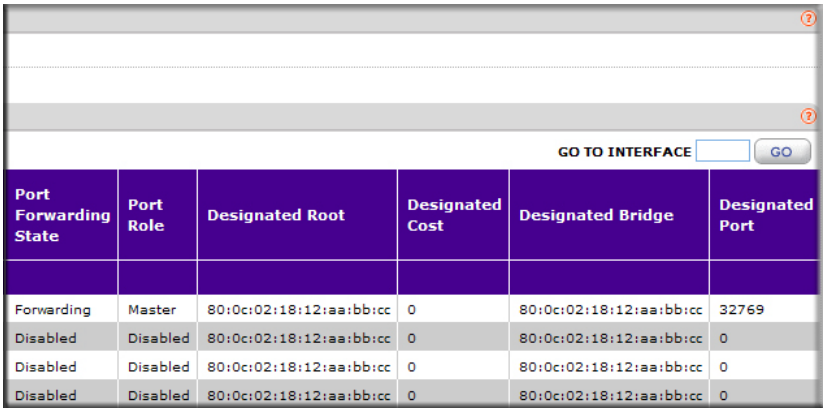
以下に MST Configuration 欄に表示される情報の説明を示します。

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。
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。





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。

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. 1 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。

項目	説明
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）。

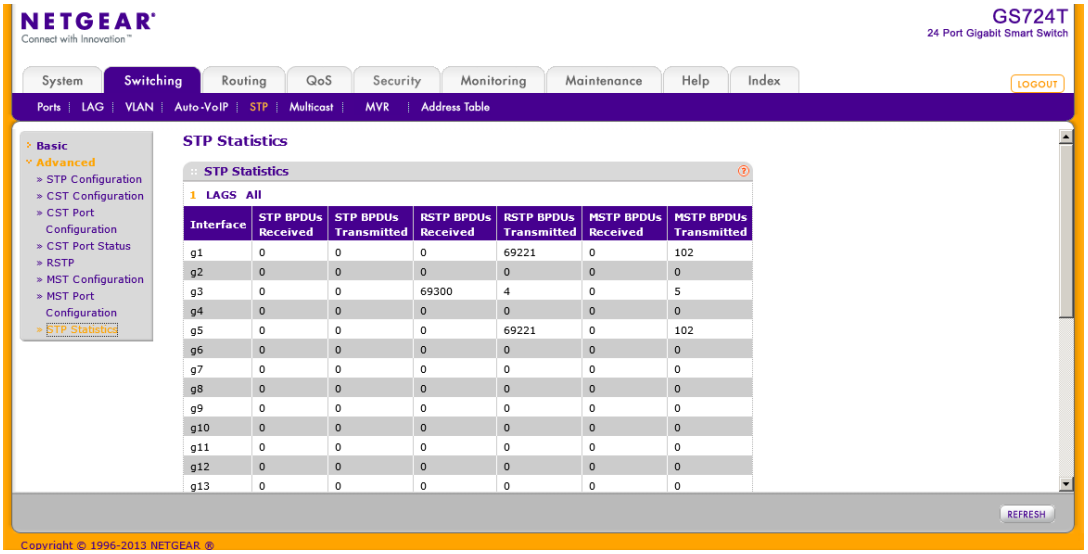
Port Forwarding State	ポートの STP 状態。 • Disabled • Blocking • Listening • Learning • Forwarding
Port Role	MST のポートロール。Root Port, Designated Port, Alternate Port, Backup Port, Master Port, または Disabled Port.
Designated Root	MST のルートブリッジ ID。
Designated Cost	STP トポロジーに参加しているポートのコスト。
Designated Bridge	ルートポ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。



以下に STP Statistics 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。IPv4 の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)を使います。IPv6 のホストグループはプレフィクス ff00::/8 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。

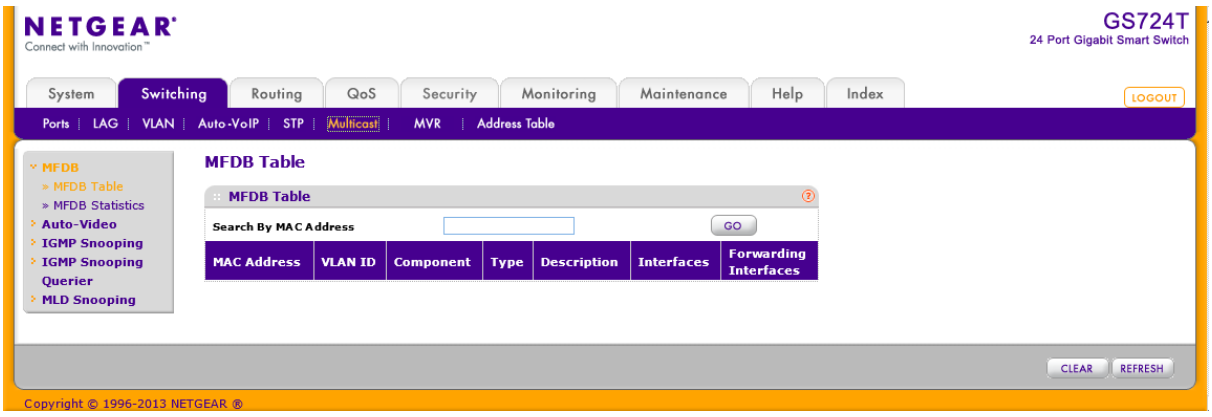
- MFDB Table
- MFDB Statistics
- Auto-Video
- IGMP Snooping
- IGMP Snooping Querier
- MLD Snooping

MFDB テーブル(MFDB Table)

MFDB(マルチキャストフォワーディングデータベース)はすべての有効なすべてのマルチキャストアドレスエントリーのためのポートメンバーシップ情報を保持します。鍵となる情報は VLAN ID と MAC アドレスの組み合わせです。エントリーは複数のプロトコルデータを含むことができます。

MFDB テーブルを検索する

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



2. Search By MAC Address:検索する MAC アドレスを入力します。
   以下の形式で入力します。
   00:01:24:43:45:67
3. Go ボタンをクリックして検索します。

以下に MFDB Table 欄に表示される情報の説明を示します。

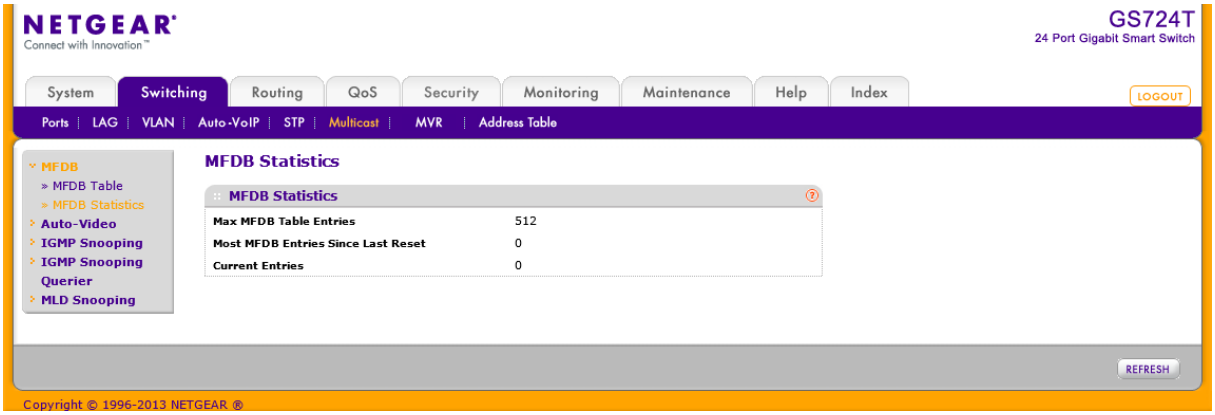
項目	説明
MAC Address	マルチキャスト MAC アドレス。MAC アドレスで検索する場合は、コロン(:)で 2 桁ごとに区切られた 12 桁の 16 進数(例: 01:00:5e:45:67:89)を入力し Go ボタンをクリックします。完全に一致する必要があります。
VLAN ID	MAC アドレスに関連する VLAN ID。
Component	このフォワーディングデータベースに入力された方法。IGMP Snooping または Static Filtering。
Type	タイプ。スタティック(Static)あるいはダイナミック(Dynamic)。
Description	マ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。

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 MFDB 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。

項目	項目
Max MFDB Table Entries	テーブルの最大容量。

Most MFDB Entries Since Last Reset	前回の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。

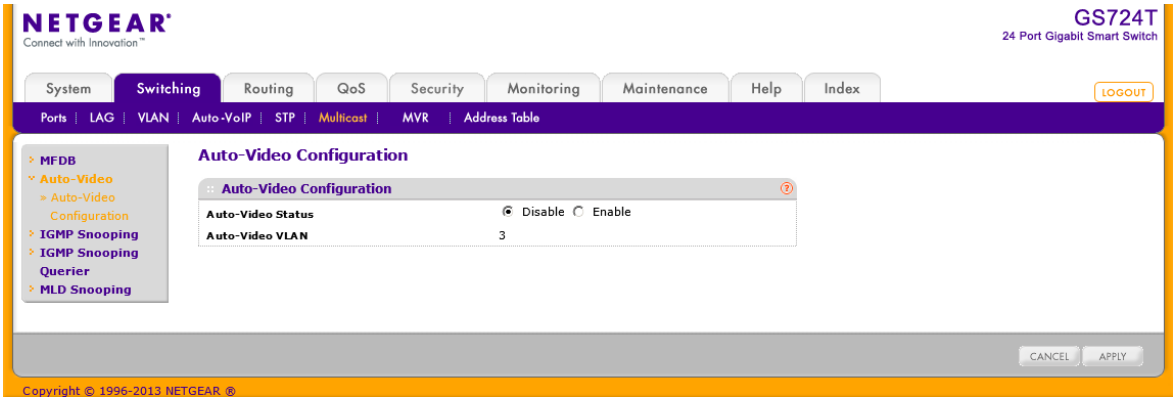
Refresh ボタンをクリックしてスイッチの最新情報を表示させます。

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。

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. Auto Video Status:オートビデオ機能を有効、無効にします。
   - Enable: オートビデオ機能をグローバルで有効にします。
   - Disable:オートビデオ機能をグローバルで無効にします。
3. Auto Video VLAN:オートビデオ VLAN の VLAN ID を示します。
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. 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。

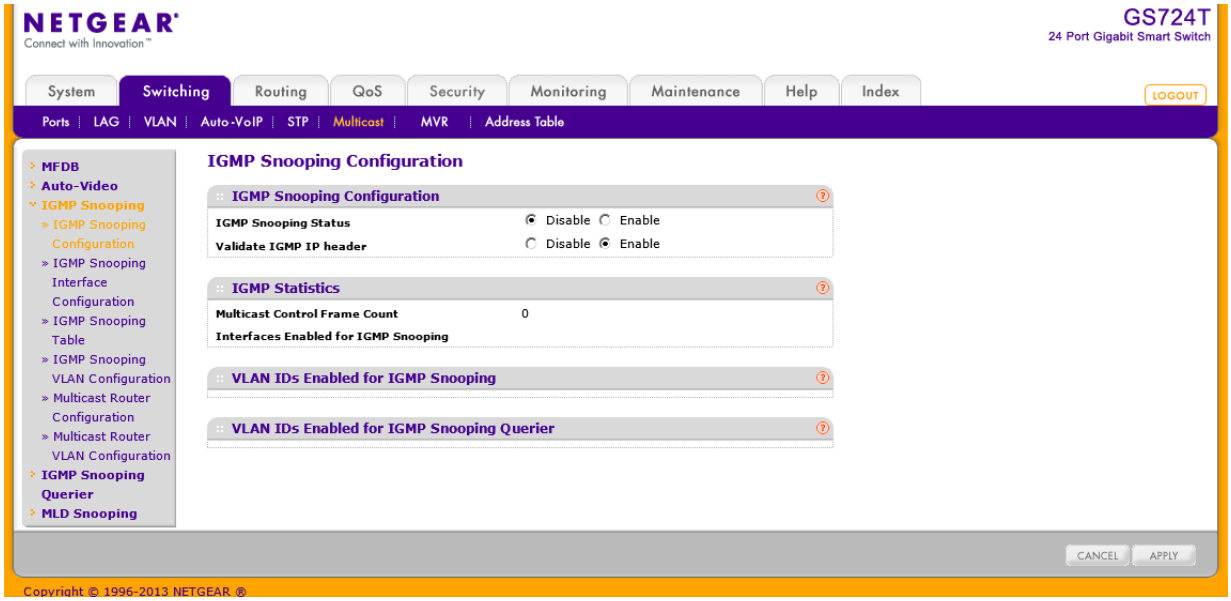
伝統的なイーサネットは多くの機器を一つの共有ネットワークに接続することを避けるために異なるネットワークセグメントに分割していました。ブリッジやスイッチがそれらのセグメントをつなげています。ブロードキャストやマルチキャストの宛先アドレスを持ったパケットを受信すると、スイッチは IEEE MAC ブリッジ標準にもとづきパケットのコピーをそのポート以外のネットワークへ転送します。その結果、ネットワークに接続されているすべてのノードがパケットをアクセスする事ができます。

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。



IGMP スヌーピングを設定する

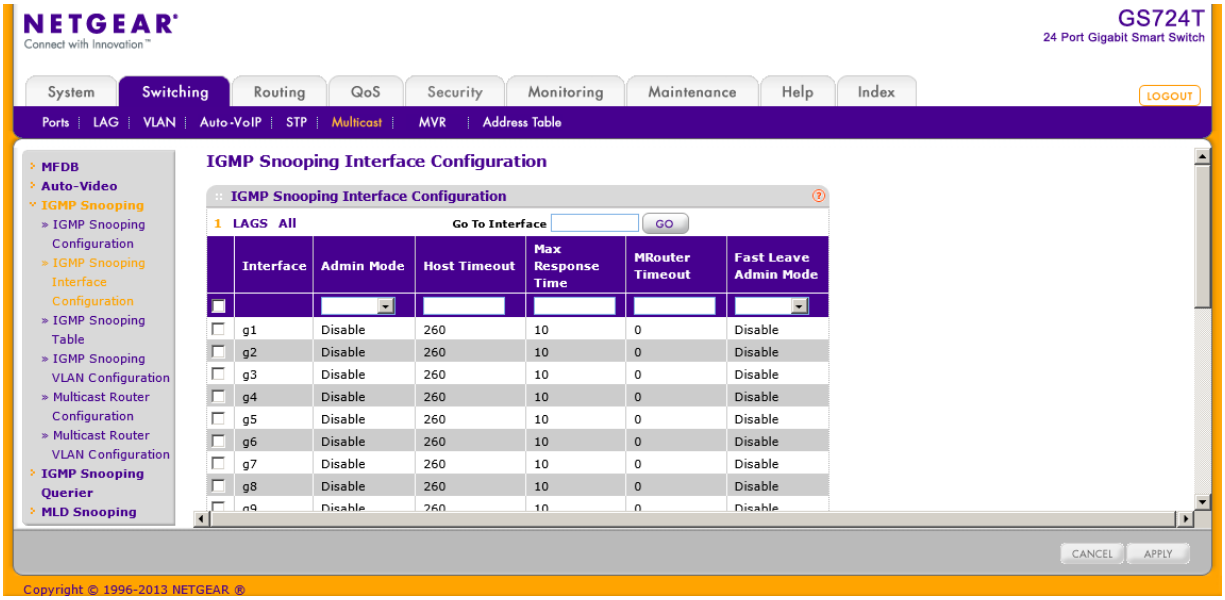
1. Switching > Multicast > IGMP Snooping > IGMP Snooping Configuration を選択して IGMP Snooping Configuration ページを表示します。
2. IGMP Snooping Status：スイッチで IGMP スヌーピングを有効にします。
   - Enable：IGMP スヌーピングを有効にし、スイッチはすべての IGMP パケットをスヌープしてパケットを送信するグループアドレスの存在するネットワークを決定します。
   - Disable：スイッチは IGMP パケットをスヌープしません。
3. Validate 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. 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. 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 欄とその下の欄に表示される情報の説明を示します。

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。
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。

IGMP スヌーピングインターフェース設定

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。



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。
2. 1 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

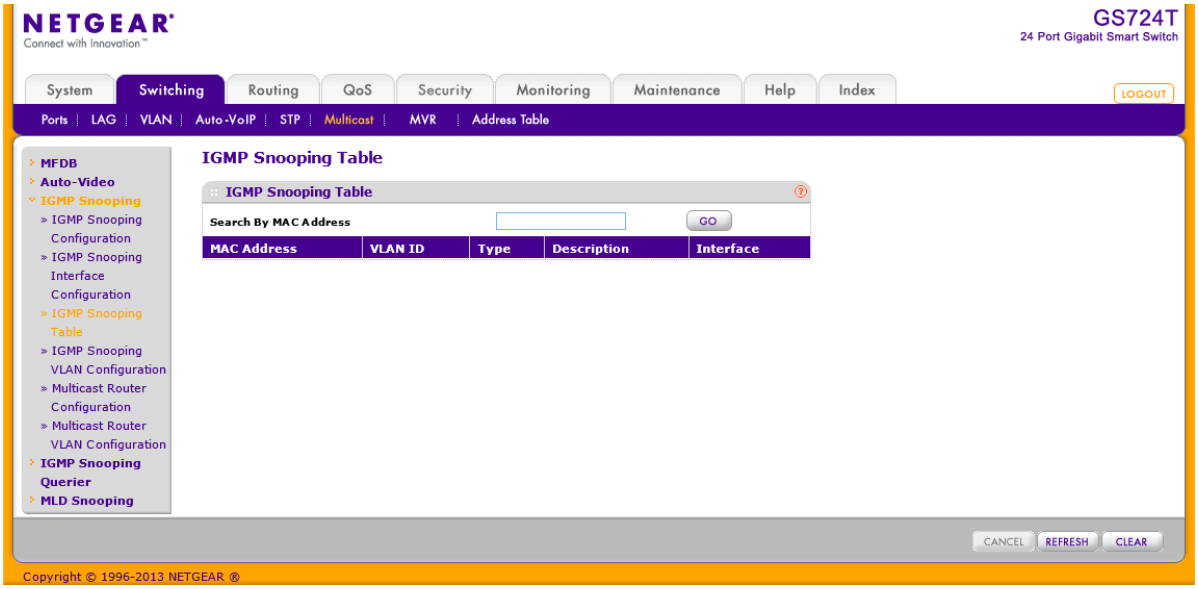
す。

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。MAC アドレスで検索ができます。



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:
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。
Type	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。

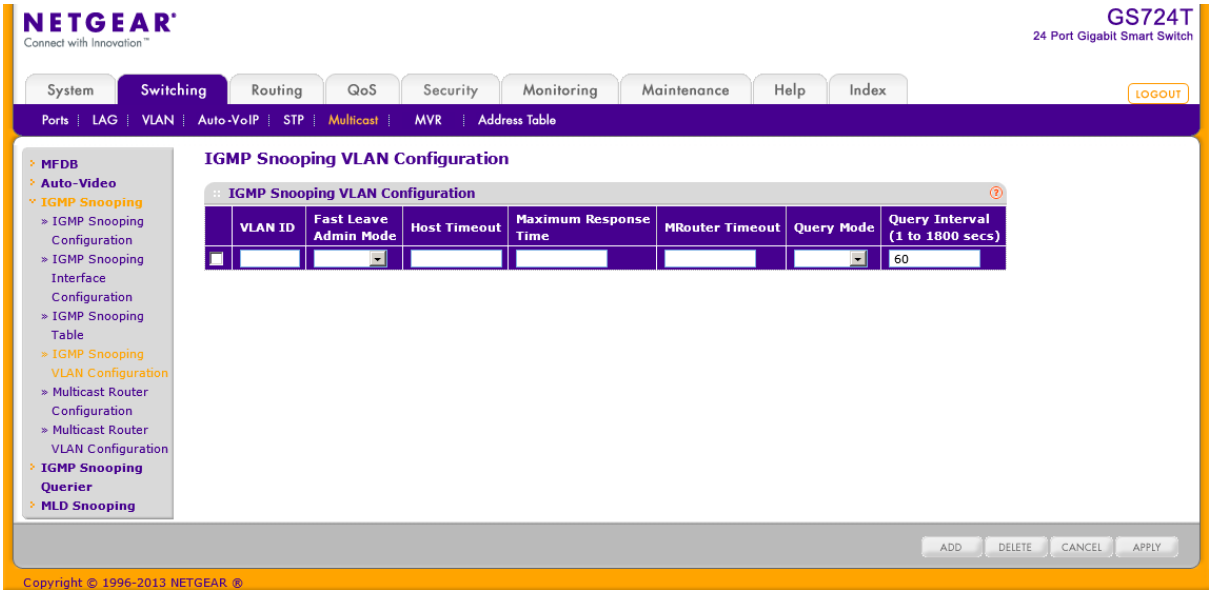
画面下部のボタンを使って以下の動作をすることができます。

- 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。

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。



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）。

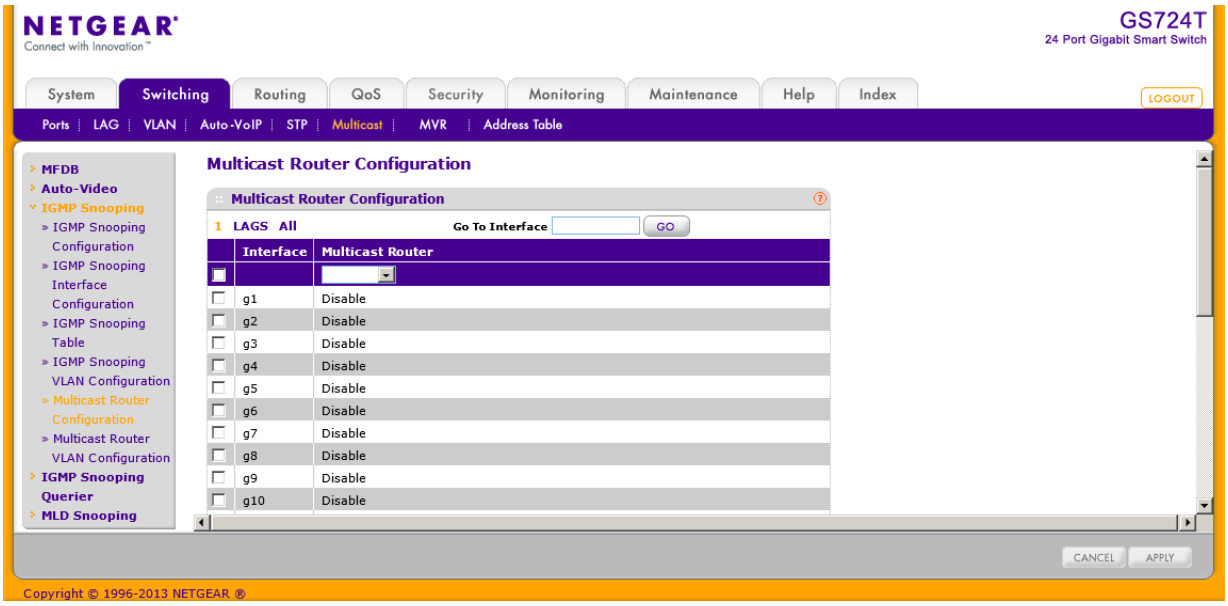
3. VLAN の IGMP を削除するには、削除する IGMP のチェックボックスを選択し、**Delete** ボタンをクリックします。
4. VLAN の IGMP を変更するには、変更する IGMP のチェックボックスを選択し、変更をします。変更後、**Apply** ボタンをクリックします。
5. **Cancel** ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。

マルチキャストルーター設定（Multicast Router Configuration）

マルチキャストルーターがスイッチに接続されているときは、スイッチはルーターの存在を動的に認識します。マルチキャストルーターあるいは IGMP クエリアに接続され、マルチキャストトラフィックを受信するインターフェースをマルチキャストルーターインターフェースと静的に設定することもできます。このページでインターフェースを静的なマルチキャストルーターインターフェースとして設定します。スイッチがスヌープしたすべての IGMP パケットはこのインターフェースに接続されているマルチキャストルーターに転送されます。スイッチが自動的にマルチキャストルーターの存在を検知し、IGMP パケットを転送するため、多くの場合、設定は不要です。複雑なネットワークで、マルチキャストルーターが常に IGMP パケットを受信できるようにしたい場合には必要となります。

インターフェースにマルチキャストルーターモードを設定する

1. **Switching** > **Multicast** > **IGMP Snooping** > **Multicast Router Configuration** を選択して **Multicast Router Configuration** ページを表示します。



2. 設定するインターフェースを選択します。

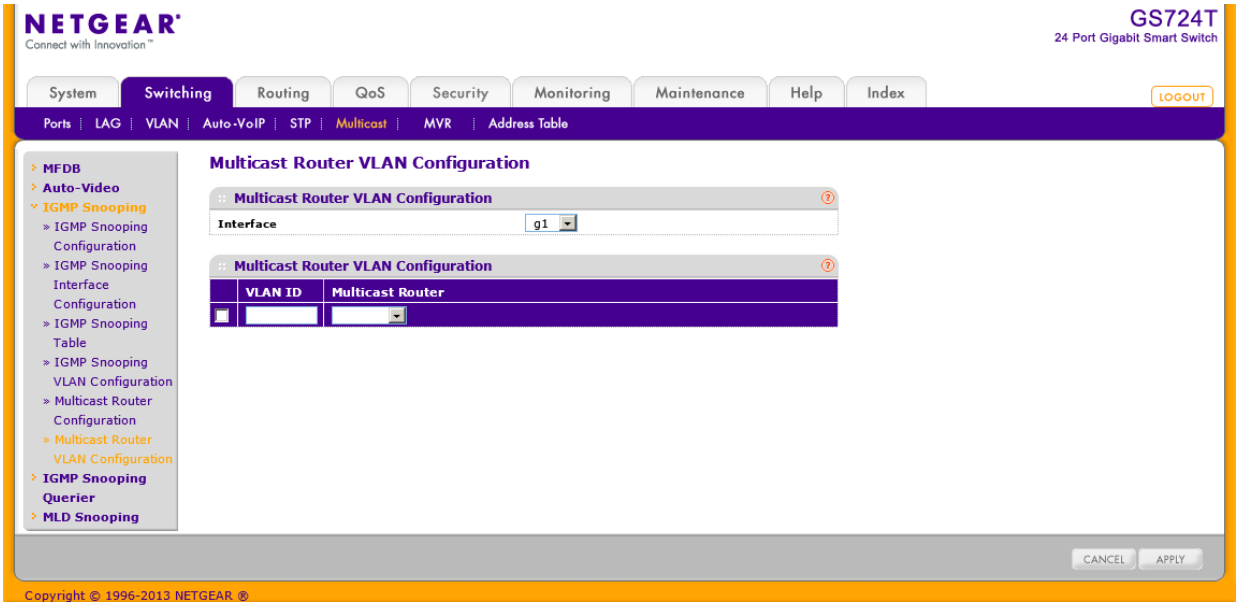
3. **Multicast Router** で有効(Enable),無効(Disable)を選択します。
4. **Apply** ボタンをクリックします。

マルチキャストルーターVLAN 設定(Multicast Router VLAN Configuration)

この画面で VLAN ID からスヌープした IGMP パケットをマルチキャストルーターが接続されたインターフェースへ転送するインターフェースを設定します。スイッチが自動的にマルチキャストルーターの存在を検知し、IGMP パケットを転送するため、多くの場合、設定は不要です。複雑なネットワークで、マルチキャストルーターが常に IGMP パケットを受信できるようにしたい場合には必要となります。

マルチキャストルーティング VLAN を設定する

1. **Switching** > **Multicast** > **IGMP Snooping** > **Multicast Router VLAN Configuration** を選択して **Multicast Router VLAN Configuration** ページを表示します。



2. 設定するインターフェースを選択します。
3. **VLAN ID**:マルチキャストルーターモードを有効にする VLAN ID を設定します。
4. **Multicast Router**:有効(Enable)、無効(Disable)を選択します。
5. **Apply** ボタンをクリックします。

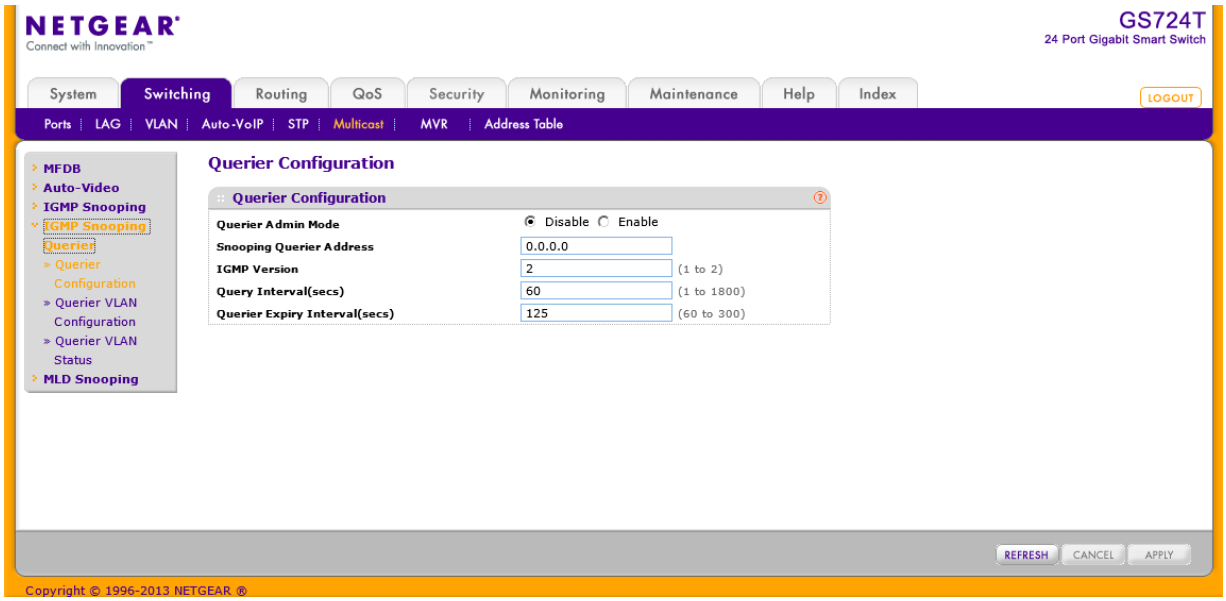
IGMP スヌーピングクエリア(IGMP Snooping Querier)

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

このページで IGMP スヌーピングクエリア設定をします。



IGMP スヌーピングクエリア設定をする

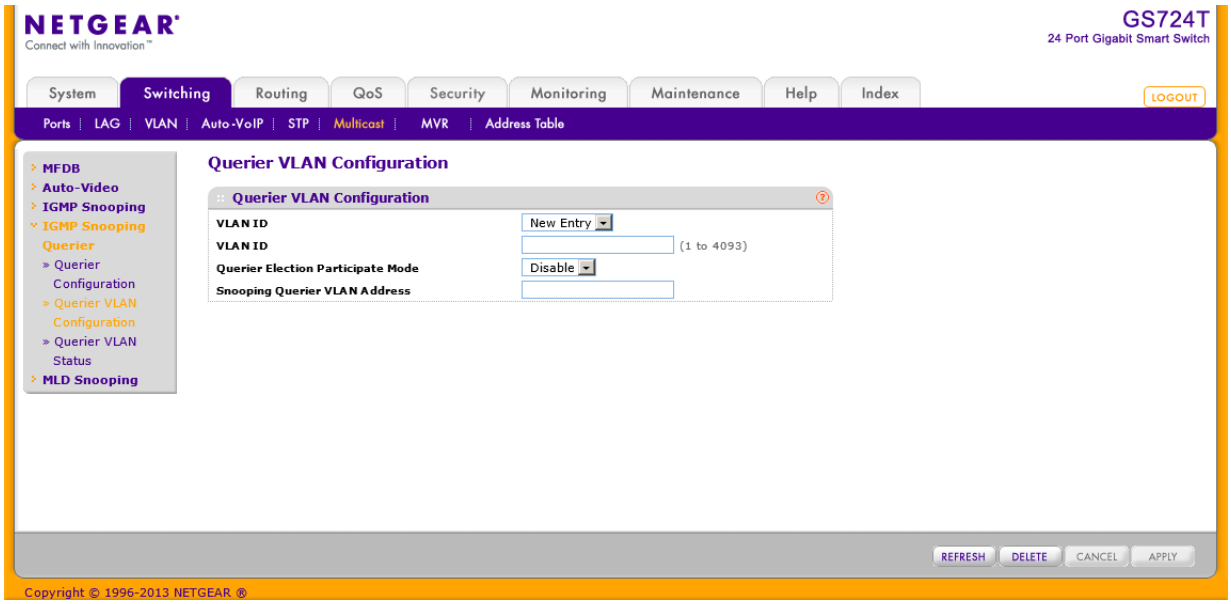
1. Switching > Multicast > IGMP Snooping Querier > IGMP Snooping > Querier Configuration を選択して Querier Configuration ページを表示し、以下の項目を設定します
   - **Querier Admin Mode**:IGMP スヌーピングクエリアを有効(Enable),無効(Disable)にします。
   - **Snooping Querier Address**:IGMP クエリを送信する IP アドレスを設定します。
   - **IGMP Version**:IGMP ク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 125(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。

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。

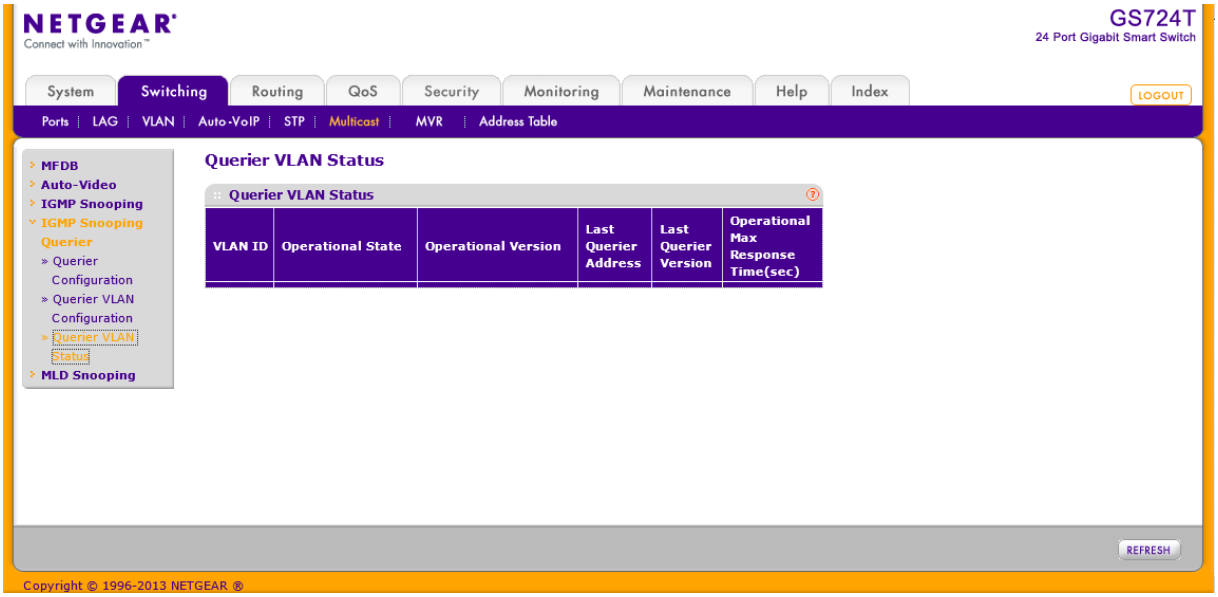


2. IGMP スヌーピング用の新しい VLAN ID を作成するには VLAN ID 欄で **New Entry** を選択し、以下の情報を設定します。
   - **VLAN ID**:IGMP スヌーピングを有効にする VLAN ID を入力します。(1-4093)
   - **Querier Election Participate Mode**:
     - **Disabled**:VLAN 中でバージョンが同じクエリを発見すると、クエリを停止します。
     - **Enabled**:クエリアの選抜に参加します。VLAN 中で IP アドレスが一番小さなものがクエリアになります。
   - **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** 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。

項目	説明
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)

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。

MLD スヌーピング(MLD Snooping)

MLD(Multicast Listener Discovery)は IPv6 マルチキャストルーターによって使われる直接接続さ

れたリンク上のマルチキャスト受信者（IPv6 マルチキャストパケットの受信を希望するノード）を発見し、どのマルチキャストパケットが隣接ノードに興味が持たれているかを発見するプロトコルです。MLD は IGMP から派生しています。MLD バージョン 1（MLDv1）は IGMPv2 と、MLD バージョン 2（MLDv2）は IGMPv3 と同等です。MLD は ICMPv6 のサブプロトコルであり、MLD メッセージは ICMPv6 メッセージのサブセットで、IPv6 パケット内で先頭の Next Header 値 58 により識別されます。

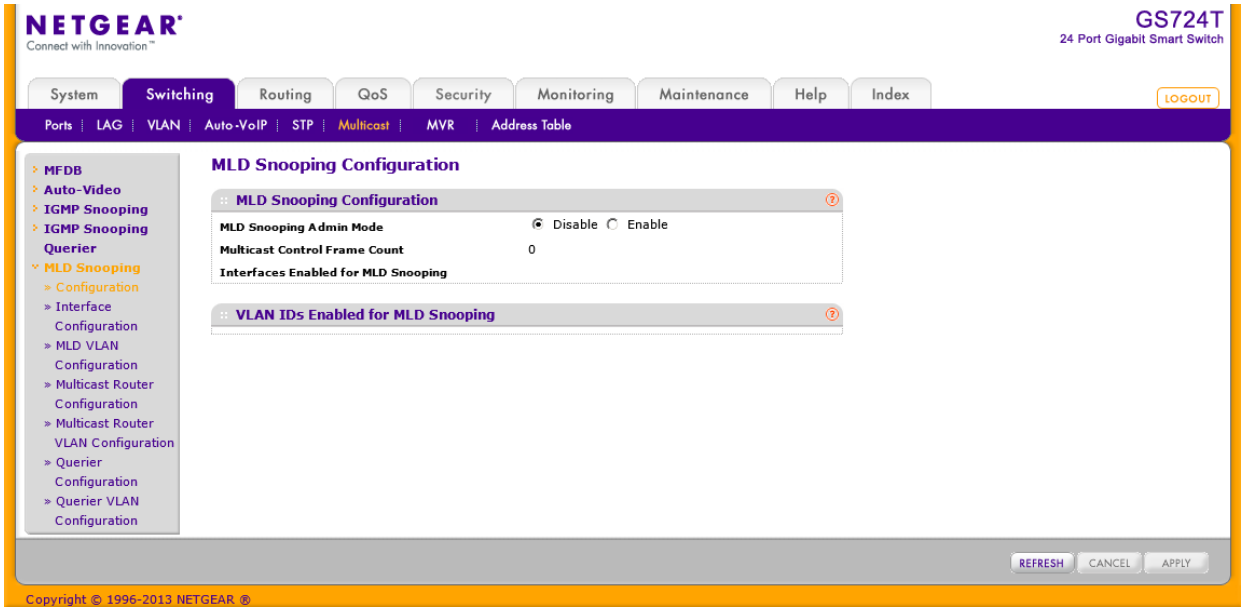
スイッチは MLDv1 と MLDv2 プロトコルパケットをスヌープし、宛先 IPv6 マルチキャスト MAC アドレスをもとに、IPv6 マルチキャストデータをブリッジします。スイッチは MLD スヌーピングおよび IGMP スヌーピングの両方を同時に実行するように設定できます。

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

IPv4 では、レイヤー2 スイッチは IGMP スヌーピングを使ってマルチキャストトラフィックが IP マルチキャストアドレスに関連付けられたインターフェースだけに転送されるように動的にレイヤー2 インターフェースを設定することによってマルチキャストトラフィックのフラッディングを制限することができます。IPv6 では、MLD スヌーピングが同様に機能します。MLD スヌーピングでは、IPv6 マルチキャストデータは、VLAN の全ポートにフラッディングされるのではなく、データを受信したいポートだけに選択的に転送されます。このポートのリストは IPv6 制御パケットをのぞきみすることにより作成されます。

MLD スヌーピングを設定する

1. **Switching** > **Multicast** > **MLD Snooping** > **MLD Snooping Configuration** を選択して **MLD Snooping Configuration** ページを表示します。



2. **MLD Snooping Admin Mode**：Enable を選択してスイッチの MLD スヌーピングを有効にします。

3. Apply ボタンをクリックします。

以下に MLD Snooping Configuration ページに表示される情報の説明を示します。

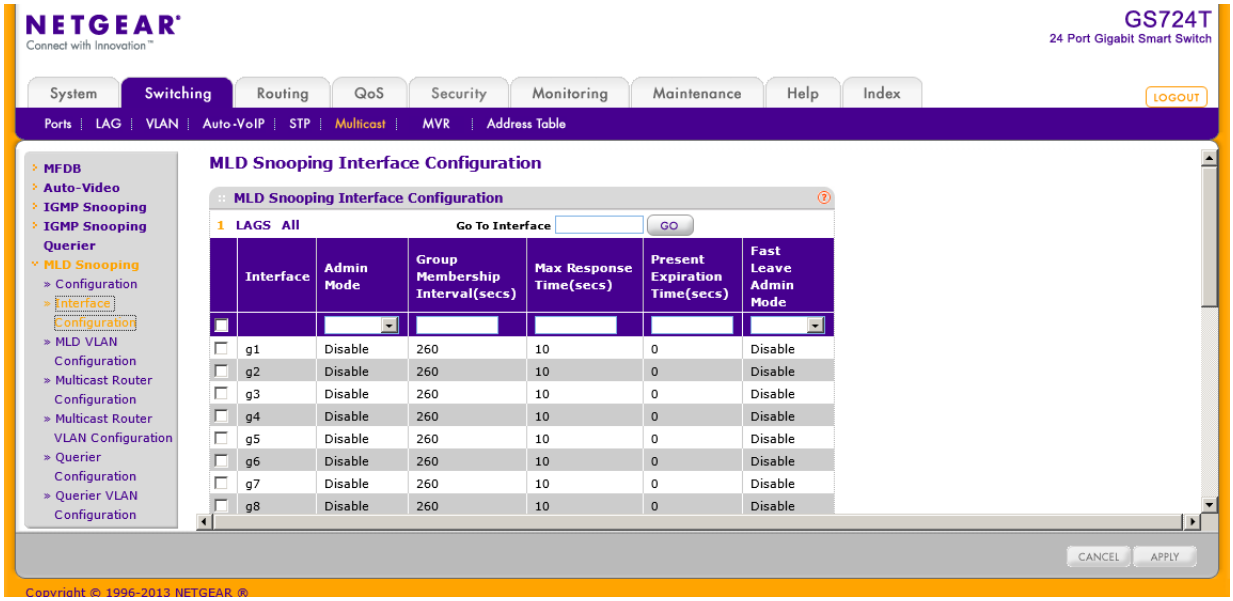
項目	説明
Multicast Control Frame Count	処理したマルチキャスト制御フレームの数。
Interfaces Enabled for MLD Snooping	MLD スヌーピングが有効なインターフェースのリスト。
VLAN IDs Enabled For MLD Snooping	転送されたデータフレームの数。

MLD インターフェース設定

MLD スヌーピングをインターフェースで有効にするには、グローバル（スイッチ）とインターフェースの両方で有効にする必要があります。

MLD スヌーピングインターフェース設定をする

1. Switching > Multicast > MLD Snooping > Interface Configuration を選択して MLD Snooping Interface Configuration ページを表示します。.
2. 設定インターフェースを選択します。
3. 選択したポートまたは LAG の MLD スヌーピング設定をします。



- **Admin Mode:**インターフェースで MLD 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。
- **Group Membership Interval(secs):** MLD 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(secs):**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）。
- **Present Expiration Time:**ルーターのメッセージ受信の待ち時間。有効な値は 0-3600（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。

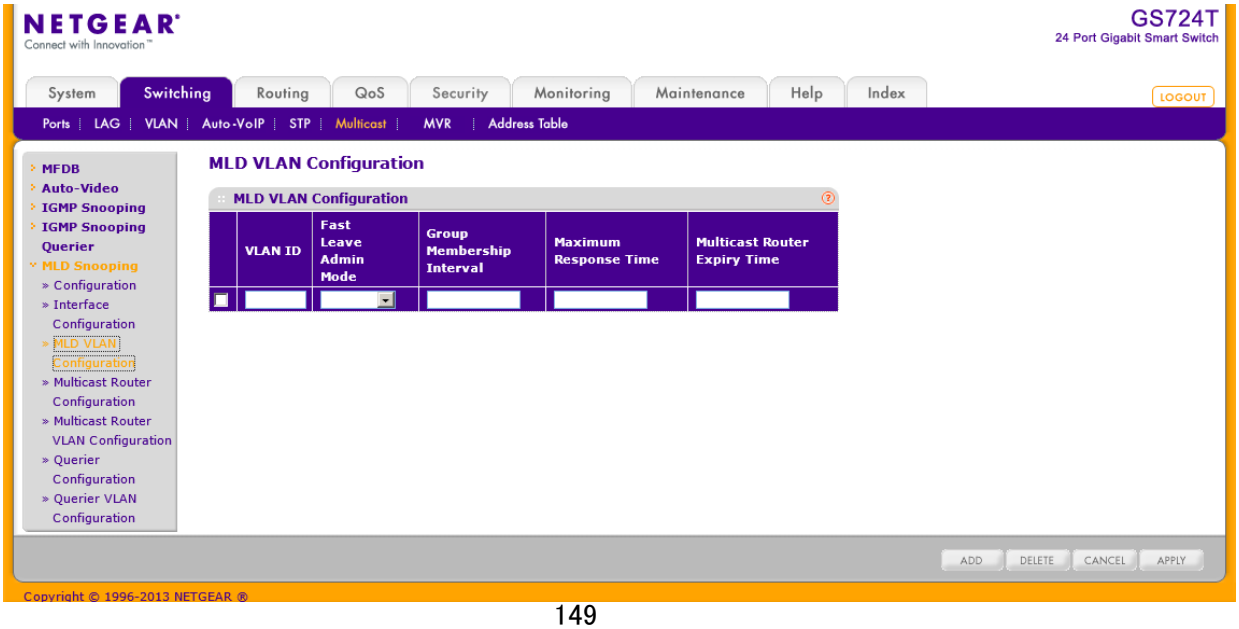
4. **Cancel** ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。
5. **Apply** ボタンをクリックして設定をスイッチに適用します。すぐに設定変更がされます。

MLD VLAN 設定（MLD VLAN Configuration）

MLD スヌーピングは VLAN のみで有効にできます。設定を有効にし、削除するためには、VLAN に所属するインターフェースを意識する必要があります。

MLD VLAN を設定する

1. **Switching** > **Multicast** > **MLD Snooping** > **MLD VLAN Configuration** を選択して **MLD VLAN Configuration** ページを表示します。
2. NLD スヌーピング設定する 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。



Fast Leave モードを有効にして、スイッチが MLDLeave 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レイヤー2 フォワーディングテーブルから削除します。

- **Group Membership Interval**: MLD 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)。
- **Maximum Response Time**:VLAN がクエリを送信することを待つ最大時間。1 以上 Group Membership Interval 未満。
- **Multicast Router Expiry**:VLAN のメッセージ受信の待ち時間。有効な値は 0-3600(秒)。

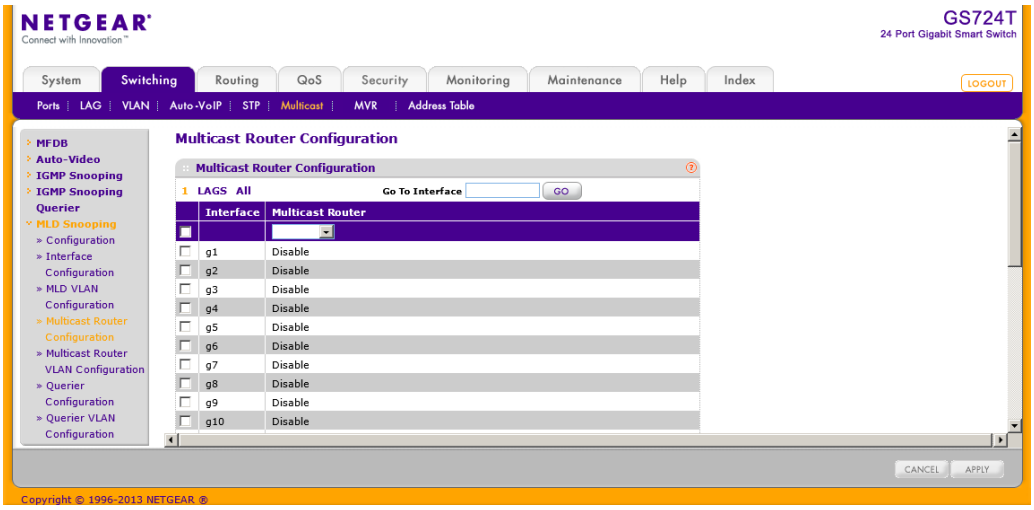
3. VLAN の MLD を削除するには、削除する IGMP のチェックボックスを選択し、**Delete** ボタンをクリックします。
4. VLAN の MLD を変更するには、変更する IGMP のチェックボックスを選択し、変更をします。変更後、**Apply** ボタンをクリックします。
5. **Cancel** ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。

マルチキャストルーター設定(Multicast Router Configuration)

スヌーピングスイッチは、マルチキャストグループメンバーシップのリストを作成し維持することに加えて、マルチキャストルーターのリストも維持します。マルチキャストパケットを転送するときに、パケットは MLD/IGMP を使ってジョインしたポートおよびマルチキャストルーターが接続されているポートにも転送されるべきです。MLD と MGMP では、有効なクエリアは一つだけです。これはネットワーク上の他のすべてのルーターは抑えられスイッチには認識されません。もし、クエリーが一定時間(multicast router present expiration time)インターフェースで受信されなかった場合はマルチキャストルーターが接続されているインターフェースのリストからインターフェースが削除されます。マルチキャストルーターの存在の有効期間は設定可能です。マルチキャストルーターの登録のタイマーデフォルト値は 0、すなわちタイムアウトしない設定となっています。

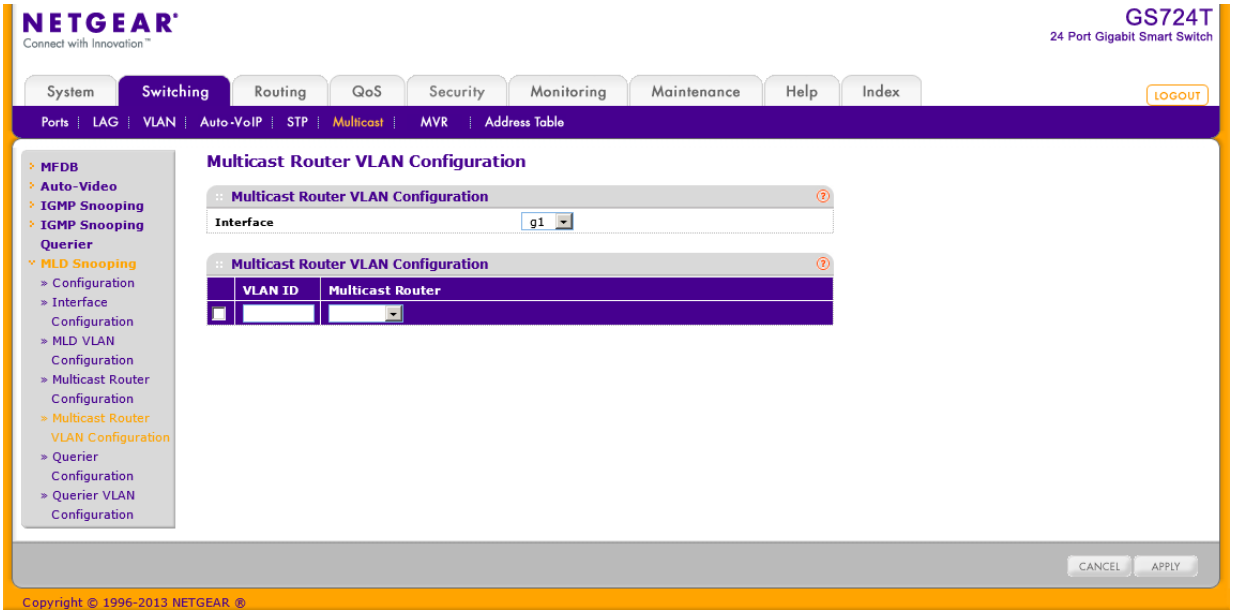
マルチキャストルーターを設定する

1. **Switching** > **Multicast** > **MLD Snooping** > **Multicast Router Configuration** を選択して **Multicast Router Configuration** ページを表示します。
2. 設定するインターフェースを選択します。
3. **Multicast Router** で有効(Enable),無効(Disable)を選択します。
4. **Apply** ボタンをクリックします。



マルチキャストルーターVLAN 設定(Multicast Router VLAN Configuration)

VLAN やインターフェースに接続されている静的に設定されたルーターは、インターフェースが有効で VLAN のメンバーであるならば、学習されたマルチキャストルーターが接続されたインターフェースリストに追加されます。以前のファームウェアのように、インターフェースで動的な学習モードを有効にする必要はありません。動的な学習モードは動的に学習したマルチキャストルーター情報(クエリアからのクエリ)のみの場合に適用されます。



マルチキャストルーティング VLAN を設定する

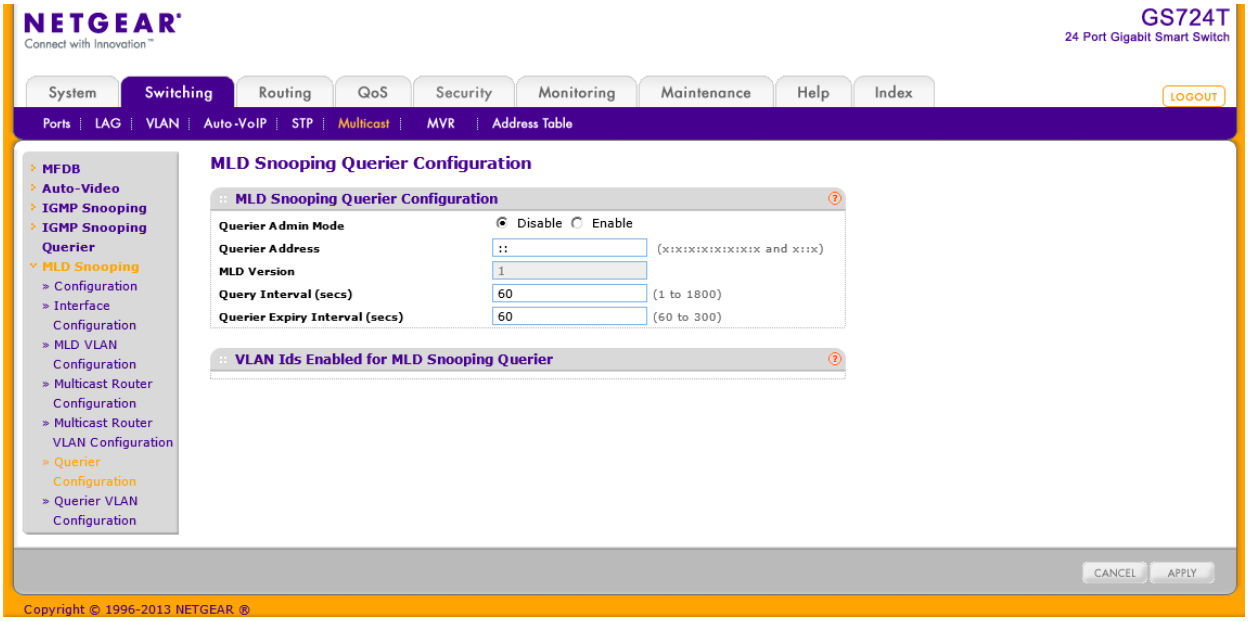
1. Switching > Multicast > MLD Snooping > Multicast Router VLAN Configuration を選択して Multicast Router VLAN Configuration ページを表示します。
2. 設定するインターフェースを選択します。

3. VLAN ID:マルチキャストルーターモードを有効にする VLAN ID を設定します。
4. Multicast Router:有効(Enable)、無効(Disable)を選択します。
5. Apply ボタンをクリックします。

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

このページで MLD スヌーピングクエリア設定をします。

MLD クエリア設定をする

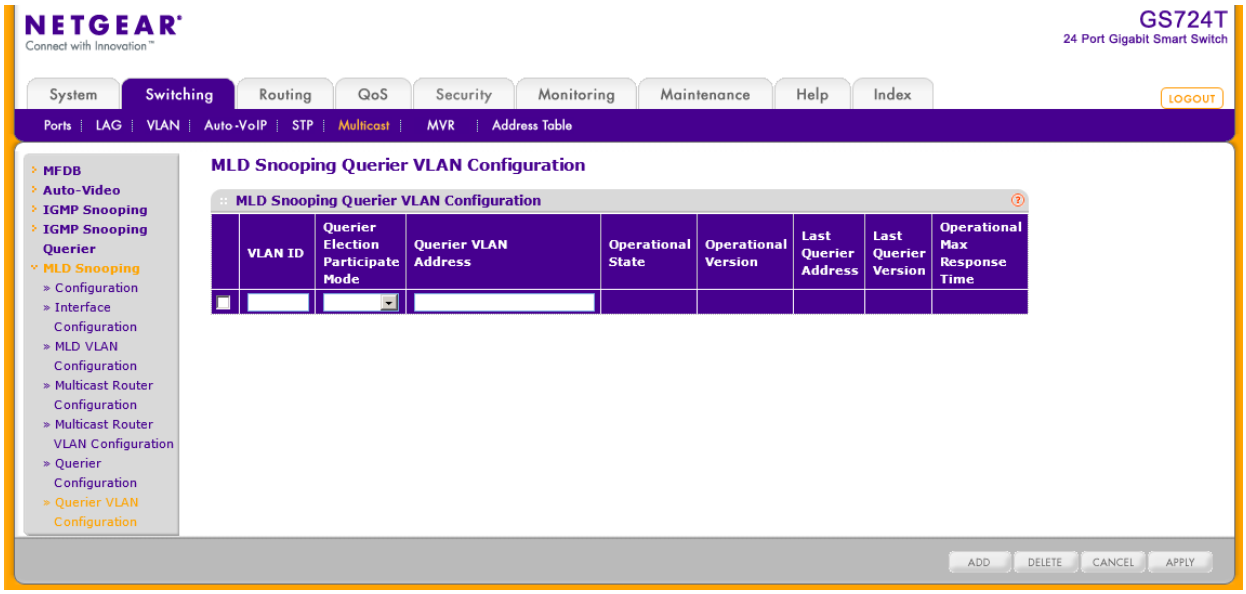


1. Switching > Multicast > MLD Snooping > Querier Configuration を選択して MLD Snooping Querier Configuration ページを表示し、以下の項目を設定します。
   - Querier Admin Mode:MLD スヌーピングクエリアを有効(Enable),無効(Disable)にします。
   - Snooping Querier Address:MLD クエリを送信する IP アドレスを設定します。
   - MLD Version:MLD クエリを送信する時に使う MLD のバージョン。1 のみ。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

MLD クエリア VLAN 設定(MLD Querier VLAN Configuration)

VLAN で MLD クエリアを使う設定をします。

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. MLD スヌーピング用の VLAN を設定します。
   - **VLAN ID**:MLD 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。
   - **Querier VLAN Address**:VLAN 中で使う MLD 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 MLD スヌーピングクエリアを削除するには、削除するクエリアの VLAN ID 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. **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 MLD Snooping VLAN Querier Configuration ページに表示される情報の説明を示します。

項目	説明
Operational State	VLAN 中の MLD スヌーピングクエリアの状態。 • Querier: MLD スヌーピングクエリアとして動作している。 • Non-Querier: MLD スヌーピングクエリアとして動作していない。 • Disabled: MLD スヌーピングクエリアは無効である。
Operational Version	動作中の MLD スヌーピングクエリアのバージョン。
Last Querier Address	VLAN 中の MLD 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）

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。

MVR 設定（MVR Configuration）

メンバーポートが同じ VLAN に属する場合に、IGMP スヌーピングはマルチキャストトラフィックの削減に役立ちますが、ポートが異なる VLAN に属している場合には、マルチキャストグループのメンバーポートを持つ VLAN それぞれにマルチキャストストリームが送信されます。MVR（Multicast VLAN Registration）はマルチキャストグループメンバーが異なる VLAN に属している場合にマルチキャストトラフィックを重複する必要性を取り除きます。

MVR は専用のマルチキャスト VLAN を使って L2 ネットワーク上でマルチキャストトラフィックを転送します。一つのスイッチで一つの MVLAN のみが設定可能であり、異なる VLAN に属するクライアントに対するマルチキャストストリームの重複を防ぐために IPTV のような特定のマルチキャストトラフィックのために使われます。クライアントは他の VLAN のメンバーシップに干渉することなしに動的にマルチキャスト VLAN への Join と Leave が可能です。

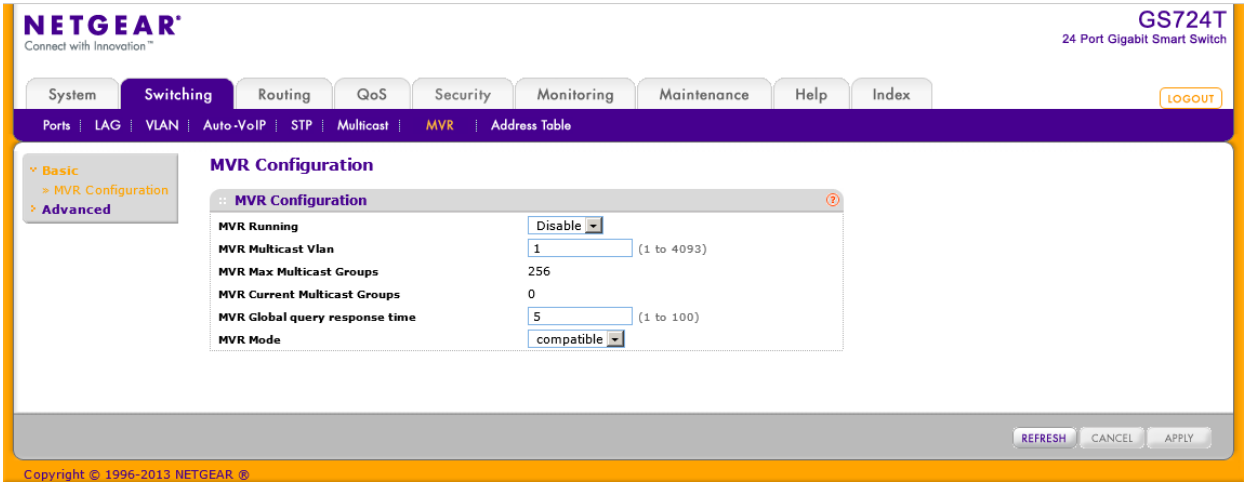
MVR は IGMP と同様にマルチキャストグループメンバーシップを学習するために IGMP メッセージをチェックします。

MVR 設定(MVR Configuration)

MVR Configuration 画面で MVR を有効にし、スイッチの MVR グローバル設定を行います。

基本 MVR 設定をする

1. Switching > MVR > Basic > MVR Configuration を選択して MVR Configuration ページを表示します。



2. MVR Running:有効にするには Enable を選択します。
3. MVR Multicast VLAN:MVR マルチキャストデータを受信する VLAN を指定します。すべての送信元ポートはこの VLAN に所属します。範囲は 1-4093。デフォルト値は 1 です。
4. MVR Global query response time:IGMP レポートの受信待機時間。(単位は 1/10 秒)。範囲は 1-100。(0.1 秒－10 秒)デフォルトは 5(0.5 秒)。
この時間はポートリーブ処理のためのレシーバーに見に適用されます。IGMP クエリーが受信ポートから送信されたとき、スイッチは IGMP グループメンバーシップレポートを MVR query time 時間待ってからポートをマルチキャストグループメンバーシップから削除します。
5. MVR Mode:MVR モードを選択します。
   - Dynamic:MVR スイッチは IGMP クエリをスヌープし、IGMP レポートをマルチキャスト VLAN 中の IGMP ルーターに転送することによって既存のマルチキャストグループを学習します。
   - Compatible:MVR スイッチはマルチキャストグループを学習しません。MVR は IGMP レポートを転送しないため、グループを設定する必要があります。このモードで動作させるためにはすべての必要なマルチキャストストリームは MVR スイッチに対して転送されるように IGMP ルーターを静的に設定する必要があります。

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

表 37. MVR status

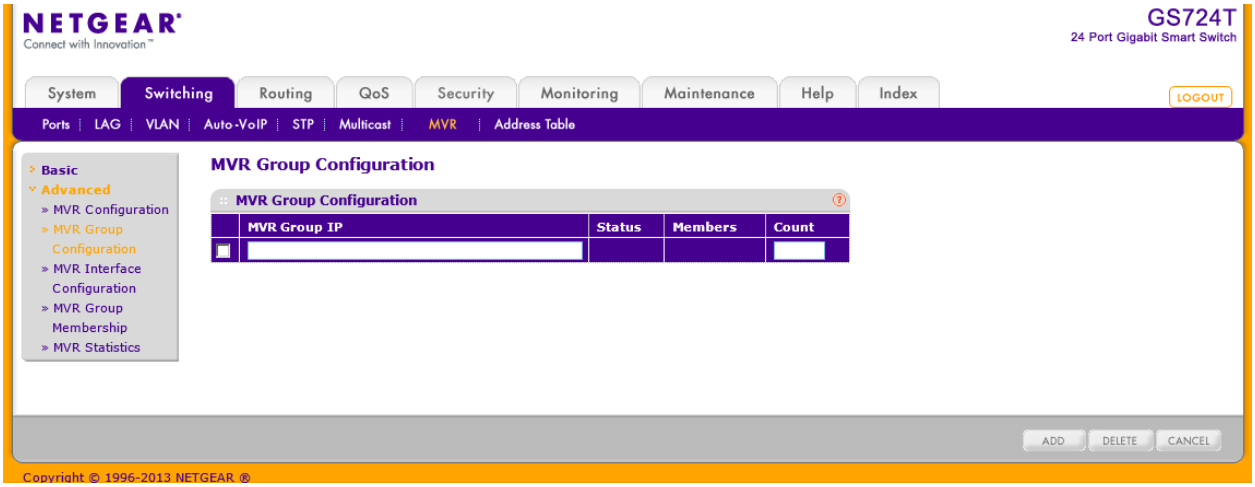
項目	説明
MVR Max Multicast Groups	MVR がサポート可能な最大マルチキャストグループ数。
MVR Current Multicast Groups	現在の MVR グループ数。

MVR グループ設定（MVR Group Configuration）

MVR Group Configuration 画面でスイッチに MVR グループを作成し、設定することができます。この例では、5 つの MVR グループを作成します。複数の MVR グループを作るには、連続した IP アドレス（239.1.1.1, 239.1.1.2, 239.1.1…）を持つ必要があります。

5 つの連続した MVR グループを作成する

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



2. MVR Group IP：MVR Group Configuration：MVR グループアドレスの IP アドレスの最小の値を記入します。
3. Count：連続して生成するアドレス（グループ）数を記入します。
例では 5 を入力しています。
4. Add ボタンをクリックして 5 つの新しい MVR グループが作成されます。
以下の図は 5 つの MVR グループが作成された例です。

以下に **MVR GroupConfiguration** ページに表示される情報の説明を示します。

表 38. MVR group status information

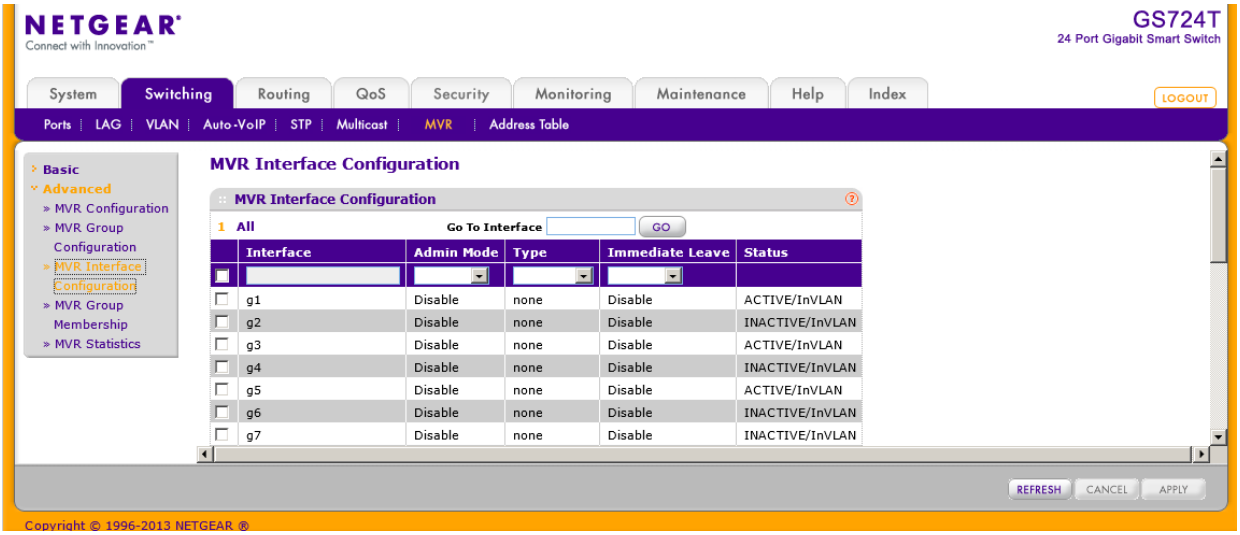
項目	説明
Status	MVR グループの状態。Inactive/Active。
Members	MVR グループに属しているポートのリスト。

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

MVR Interface Configuration 画面で MVR グループに属するポートの設定とグループ内での役割を設定します。

MVR インターフェースを設定する

1. **Switching** > **MVR** > **Advanced** > **MVR Interface Configuration** を選択して **MVR Interface Configuration** ページを表示します。



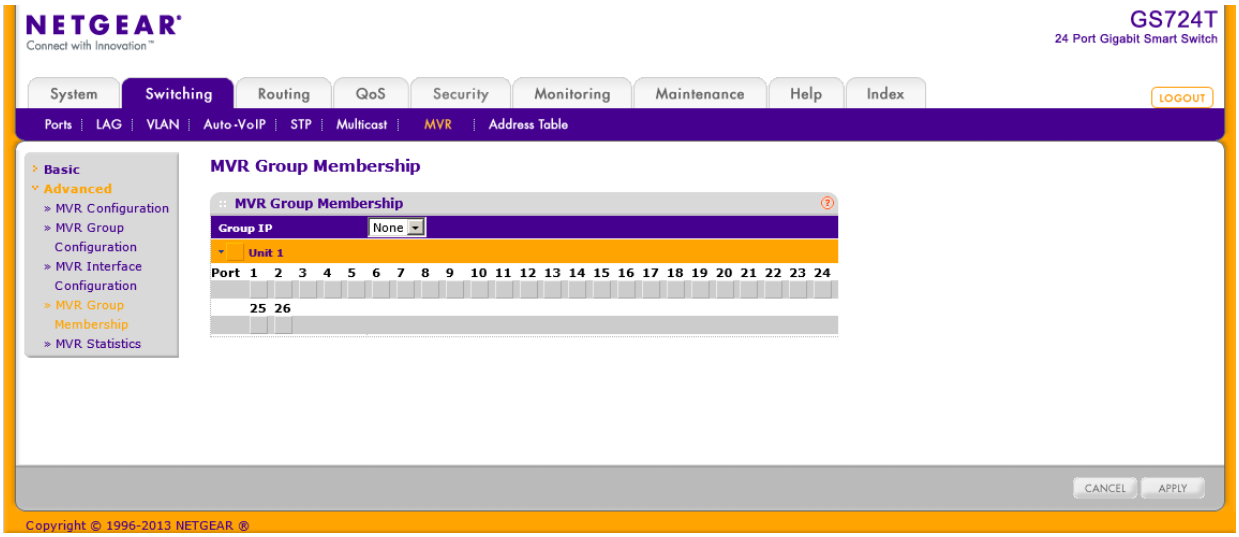
2. 設定するポートを選択します。
3. **Admin Mode**：ポートで MVR を有効にするには Enable を選択します。
4. **Type**：ポートの MVR タイプを選択します。
    - **Source**：マルチキャスト VLAN を使ってマルチキャストトラフィックが流れるポート。
    - **Receiver**：リスニングホストが接続されているポート。
5. **Immediate Leave**：有効（Enable）にすると、IGMP Leave メッセージが受信されると Receiver ポートがマルチキャストグループメンバーシップから削除されます。
6. **Apply** ボタンをクリックします。

MVR グループメンバーシップ（MVR Group Membership）

MVR Configuration 画面で MVR グループからポートの削除及び追加をします。

MVR グループメンバーシップを設定する

1. **Switching** > **MVR** > **Advanced** > **MVR Group Membership** を選択して **MVR Group Membership** ページを表示します。

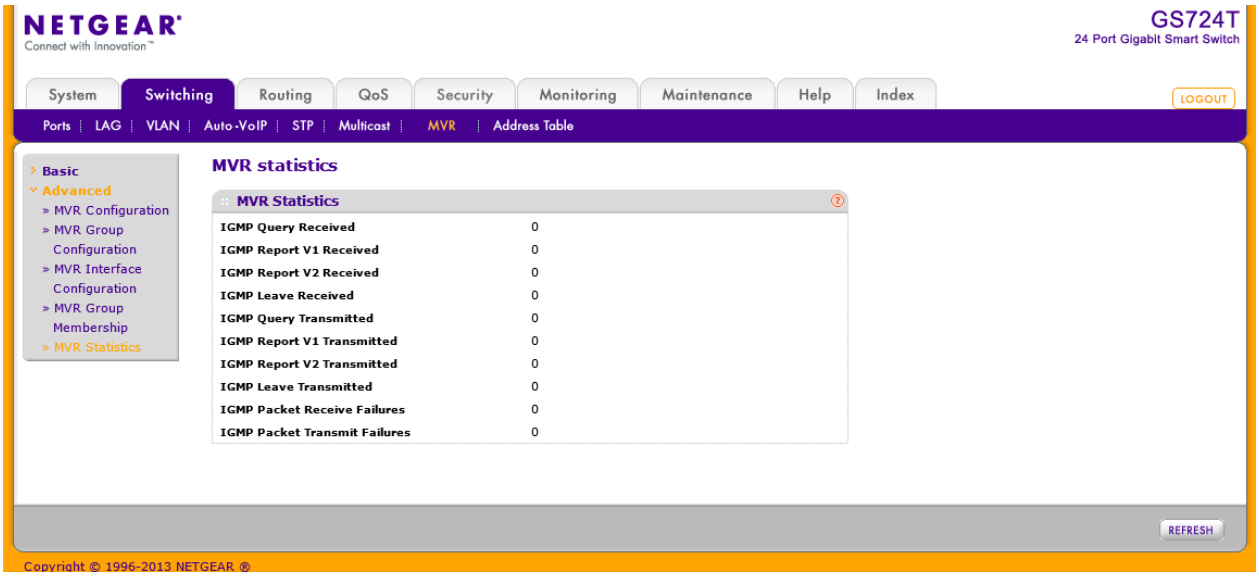


2. **Group IP**：設定する VMR グループの IP アドレスを選択します。
3. オレンジのバーをクリックしてポートを表示します。
4. MVR グループに追加するポートを選択します。
5. **Apply** ボタンをクリックします。

MVR 統計（MVR Statistics）

MVR Statistics 画面でスイッチが送受信した IGMP パケットと IGMP メッセージの情報を表示できます。

Switching > MVR > Advanced > MVR Statistics を選択して MVR Statistics ページを表示します。



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

表 39. MVR statistics

項目	設定
IGMP Query Received	受信した IGMP クエリ数。
IGMP Report V1 Received	受信した IGMP レポート V1 数。
IGMP Report V2 Received	受信した IGMP レポート V2 数。
IGMP Leave Received	受信した IGMP Leave 数。
IGMP Query Transmitted	送信した IGMP クエリ数。
IGMP Report V1 Transmitted	送信した IGMP レポート V1 数。
IGMP Report V2 Transmitted	送信した IGMP レポート V2 数。

IGMP Leave Transmitted	送信した IGMP Leave 数。
IGMP Packet Receive Failures	IGMP パケット受信失敗数。
IGMP Packet Transmit Failures	IGMP パケット送信失敗数。

アドレステーブル（Address Table）

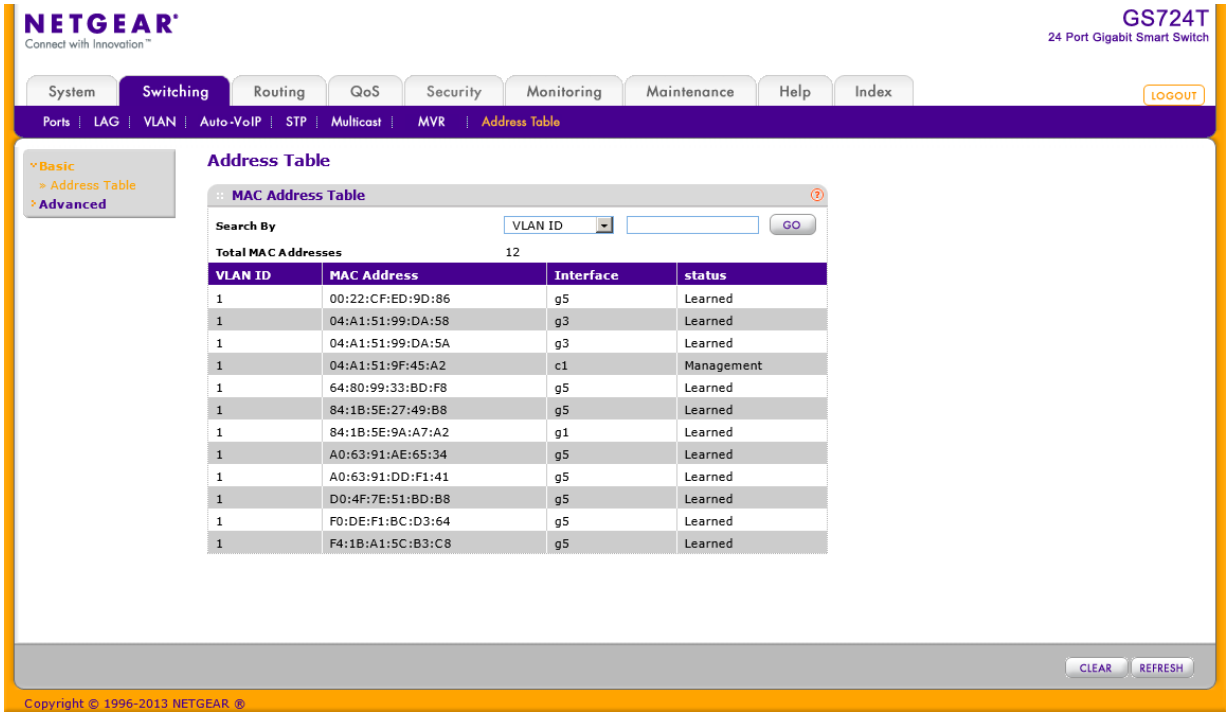
アドレステーブルは MAC アドレスを受信した後に MAC アドレスのリストを管理します。トランスペアレントブリッジ機能はフォワーディングデータベースエントリーを使って受信したフレームをどう転送するかを判断します。

MAC アドレステーブル（MAC Address Table）

MAC アドレステーブル（MAC Address Table）はスイッチが転送あるいはフィルターするユニキャスト MAC アドレスの情報を含みます。この情報が受信したフレームをどのように伝搬するかを判断するためにトランスペアレントブリッジング機能によって使われます。テーブルの入力情報を表示するために MAC アドレステーブルの検索機能を使います。

MAC アドレステーブルで検索をする

1. **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**：検索する項目を指定します。
   - **MAC Address**：メニューで MAC Addres を選択し、検索**する** MAC アドレスを入力します。00:11:22:33:44:55 の形式で入力し、**Go** ボタンをクリックして検索します。アドレは完全一致する必要があります。
   - **VLAN ID**：メニューで VLAN ID を選択し VLAN ID を入力ます。**Go** ボタンをクリックして検索し

ます。

- **Interface**：メニューで Interface を選択し、インターフェース番号を入力します。**Go** ボタンをクリックして検索します。

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。

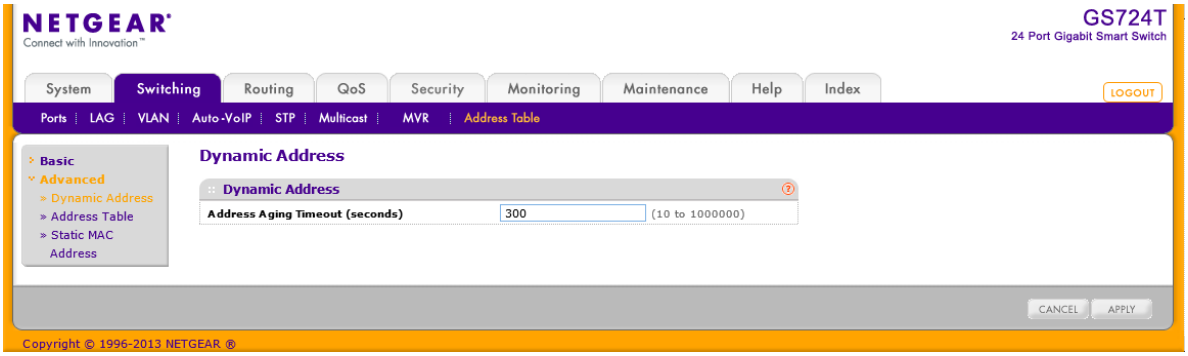
項目	説明
VLAN ID	MAC アドレスが存在する VLAN の VLAN ID。
MAC Address	スイッチが転送あるいはフィルタしたユニキャスト MAC アドレス。コロン(:)で 2 桁ごとに区切られた 12 桁の 16 進数で表されます。（例： 00:0F:89:AB:CD:EF）
Interface	この MAC アドレスが学習されたポート。このポートからこの MAC アドレスに到達することができます。
Status	テーブルエントリーの状態。 **Static**：スタティック設定。 **Learned**：学習したアドレス。 **Management**：システム MAC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



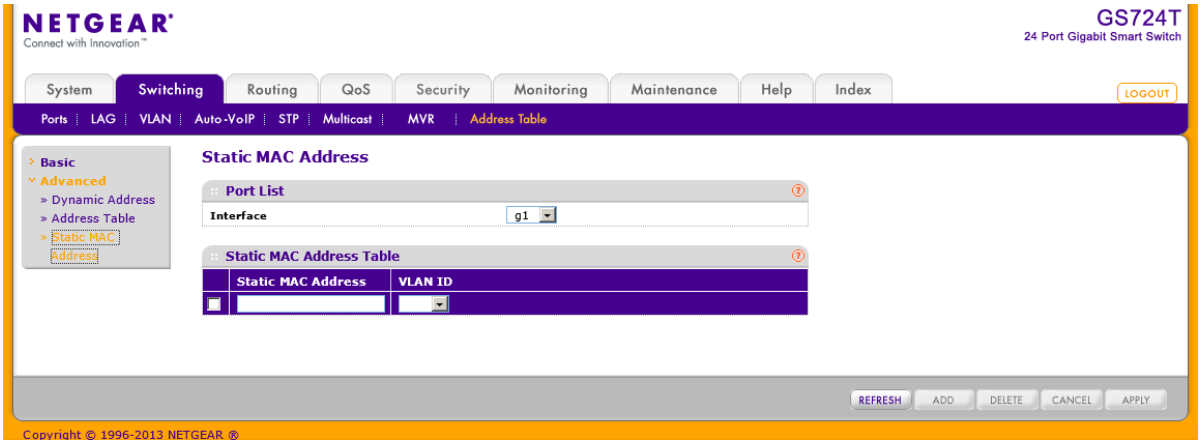
2. Address Aging Timeout (seconds): IEEE 802.1D-1990 は 300 秒を推奨しています。設定範囲は 10-1000000(秒)です。デフォルトは 300(秒)です。
3. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。
4. Apply ボタンをクリックして設定をスイッチに適用します。すぐに設定変更がされます。

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。

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. **Interface:**インターフェースを選択します。

b. **Static MAC Address:**MAC アドレスを入力します。

c. **VLAN ID:**MAC アドレスを設定したい **VLAN ID** 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。

ルーティング設定

スイッチは IP ルーティングをサポートしています。Routing タブ中のメニューを使ってスイッチのルーティングを管理します。

パケットがスイッチに入力されると、設定されたルーティングインターフェースと一致するかどうか宛先 MAC アドレスが検査されます。一致した場合、スイッチはホストテーブルで宛先 IP アドレスを探します。宛先 IP アドレスが見つかったら、パケットはホストにルートされます。一致しなかった場合は、スイッチはロンゲストプレフィックスマッチを宛先 IP アドレスで実行します。エントリーが発見された場合は、パケットはネクストホップにルートされます。一致がなかった場合にはパケットはデフォルトルートに指定されているネクストホップへルートされます。デフォルトルートが設定されていない場合、パケットはソフトウェアに渡され適切な処理がされます。

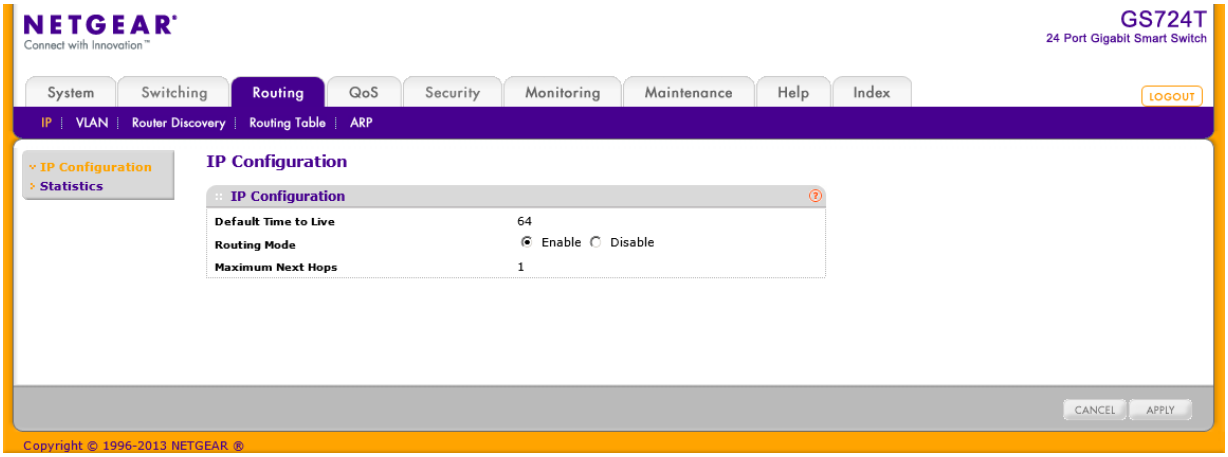
ルーティングテーブルは静的あるいはルーティングプロトコルにより動的にエントリーが追加されます。ホストテーブルは静的あるいは ARP をつかって動的に追加されたエントリーを持ちます。

IP 設定(IP Configuration)

IP Configuration 画面でスイッチのルーティングパラメータを設定します。

スイッチでルーティングを有効にする

1. Routing > IP > IP Configuration を選択して IP Configuration ページを表示します。



2. Routing Mode: Enable を選択してルーティングを有効にします。
   最初にスイッチでルーティングを有効にしてからインターフェースでのルーティング設定をしてください。
   ルーティングは VLAN インターフェース単位でも有効、無効にできます。デフォルトは Disable(無効)です。
3. Apply ボタンをクリックします。

以下の表に IP Configuration 画面の情報を示します。

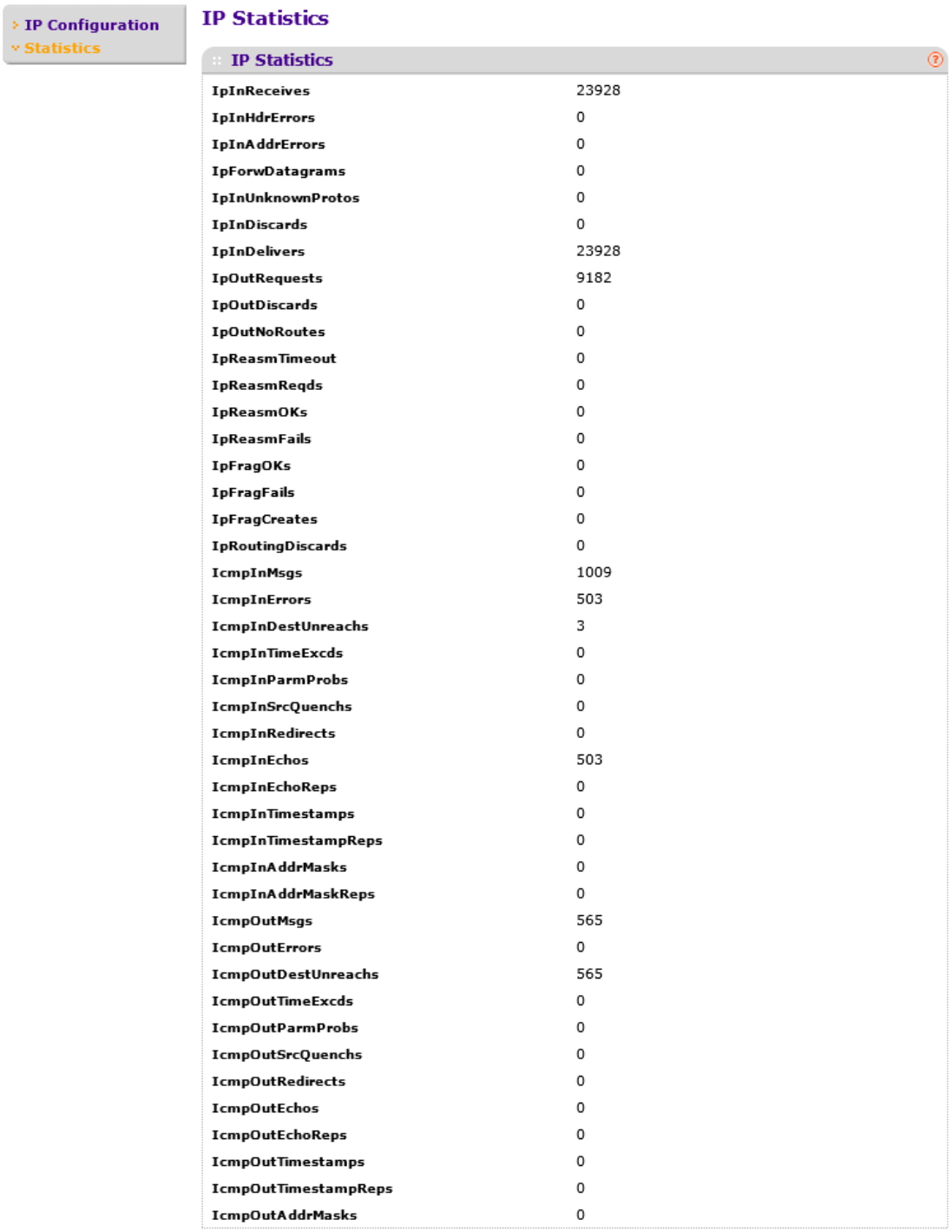
表 50. Global IP status information

項目	説明
Default Time to Live	デフォルト Time To Live 値。デフォルトは 64。
Maximum Next Hops	スイッチの最大ホップ。固定で 1。

IP 統計(IP Statistics)

IP Statistics ページに表示される統計情報は RC1213 に定義されています。

Routing > IP >Statistics を選択して IP Statistics ページを表示します。



IpInReceives	23928
IpInHdrErrors	0
IpInAddrErrors	0
IpForwDatagrams	0
IpInUnknownProtos	0
IpInDiscards	0
IpInDelivers	23928
IpOutRequests	9182
IpOutDiscards	0
IpOutNoRoutes	0
IpReasmTimeout	0
IpReasmReqds	0
IpReasmOKs	0
IpReasmFails	0
IpFragOKs	0
IpFragFails	0
IpFragCreates	0
IpRoutingDiscards	0
IcmpInMsgs	1009
IcmpInErrors	503
IcmpInDestUnreachs	3
IcmpInTimeExcds	0
IcmpInParmProbs	0
IcmpInSrcQuenchs	0
IcmpInRedirects	0
IcmpInEchos	503
IcmpInEchoReps	0
IcmpInTimestamps	0
IcmpInTimestampReps	0
IcmpInAddrMasks	0
IcmpInAddrMaskReps	0
IcmpOutMsgs	565
IcmpOutErrors	0
IcmpOutDestUnreachs	565
IcmpOutTimeExcds	0
IcmpOutParmProbs	0
IcmpOutSrcQuenchs	0
IcmpOutRedirects	0
IcmpOutEchos	0
IcmpOutEchoReps	0
IcmpOutTimestamps	0
IcmpOutTimestampReps	0
IcmpOutAddrMasks	0

以下の表に **IP Statistics** 画面の情報を示します。

表 51. IP routing statistics

項目	説明
IpInReceives	エラーも含め、インターフェースに到着した全ての受信データグラムの総数。
IpInHdrErrors	チェックサムエラー、バージョン番号エラー、フォーマットエラー、TTL エラー、IP オプションエラーなど、IP ヘッダーにエラーがある為に捨てられた受信データグラムの数。
IpInAddrErrors	IP ヘッダーの宛先フィールドの IP アドレスが、このエンティティでは受け取っても意味のない値になっている受信データグラムの数。このカウンタは、無効であるアドレス(例えば 0.0.0.0) や、サポートしていない IP アドレスクラス(例えば クラス E)を持っているデータグラムの数も含む。IP ゲートウェイでないエンティティ、つまりデータグラムをフォワードしないエンティティでは、宛先アドレスがローカルのアドレスではない為に破棄されたデータグラムの数を含む。
IpForwDatagrams	このエンティティが最終の IP 宛先ではない受信データグラムの数。データグラムを最終の宛先に送る為、経路を探すことによってこのエンティティが最終の IP 宛先ではないことが分かる。IP ゲートウェイとして動作しないエンティティでは、このカウンターは、このエンティティ経由のソースルートのパケットでソースルートオプションの処理が正常終了したものの数だけを含む。
IpInUnknownProtos	受信は成功したが、未知もしくはサポートされていないプロトコルの為に捨てられたローカルアドレスのデータグラムの数。

IpInDiscards	以後の処理を続けるのに問題はないが、捨てられた IP データグラム(例えば、バッファスペース不足)の数。データグラムの組み立て中に捨てられたデータグラムの数は含まない事に注意されたし。
IpInDelivers	IP のユーザープロトコル(ICMP も含む)へ配送が成功した受信データグラムの総数。
IpOutRequests	ローカルの IP のユーザープロトコル(ICMP も含む)から、送信するために、IP に渡された IP データグラムの総数。この値には ipForwDatagrams でカウントされたデータグラムの数はカウントされない事に注意されたし。
IpOutDiscards	送信するのに問題はないが捨てられた(例えば、バッファスペース不足)送信 IP データグラムの数。このカウンターが ipForwDatagrams でカウントされたデータグラムの中で、このように捨てられたものもカウントしている事に注意。

Field	Description
IpOutNoRoutes	宛先に転送する為の経路が判明しなかった為に廃棄された IP データグラムの数。ipForwDatagrams でカウントされていて"no-route"規準に当てはまるパケットもカウントされる事に注意。全てのデフォルトゲートウェイがダウンしている為にホストがルーティング出来なかったデータグラムも含む事に注意。
IpReasmTimeout	このエンティティで、受け取ったデータグラムを組み立てるために、フラグメントを保持する最大の秒数。

IpReasmReqds	受け取った IP フラグメントの中で、このエンティティで再組み立てが必要なものの数。
IpReasmOKs	再組み立てに成功した IP データグラムの数。
IpReasmFails	IP 再組み立ての過程で検出された不具合(例えば、タイムアウト、エラーなど)の数。このカウンターの値は捨てられた IP フラグメントの数である必要はない。なぜなら受け取ったフラグメントを結合し、フラグメントの数が分からなくなっても良いアルゴリズムもある為である。(RFC815 に記してある)
IpFragOKs	このエンティティでフラグメント化に成功した IP データグラムの数。
IpFragFails	このエンティティでフラグメント化する必要があったのにフラグメント化できなくて、捨てられた IP データグラムの数。例えば、IP データグラムの"Don'tFragment"フラグがセットされていた場合などがそう。
IpFragCreates	このエンティティでフラグメント化した結果生成された IP データグラムフラグメントの数。
IpRoutingDiscards	有効だが放棄されたルーティングエントリーの数。理由としては、他のルーティングエントリーのためのバッファスペースが足りなくなった。
IcmpInMsgs	エンティティが受け取った ICMP メッセージの総数。これは icmpInErrors でカウントされるものも含む。
IcmpInErrors	エンティティが受け取った、ICMP エラーのある ICMP メッセージの数。(ICMP チェックサムエラ

	ーやレングスエラーなど）
IcmpInDestUnreachs	受信した ICMPDestinationUnreachable メッセージの数。
IcmpInTimeExcds	受信した ICMPTimeExceeded メッセージの数。
IcmpInParmProbs	受信した ICMPParameterProblem メッセージの数。
IcmpInSrcQuenchs	受信した ICMPSourceQuench メッセージの数。
IcmpInRedirects	受信した ICMPRedirect メッセージの数。
IcmpInEchos	受信した ICMPEcho(request)メッセージの数。
IcmpInEchoReps	受信した ICMPEchoReply メッセージの数。
IcmpInTimestamps	受信した ICMPTimeStamp メッセージの数。

項目	説明
IcmpInTimestampReps	受信した ICMPTimeStampReply メッセージの数。
IcmpInAddrMasks	受信した ICMPAddressMaskRequest メッセージの数。
IcmpInAddrMaskReps	受信した ICMPAddressMaskReply メッセージの数。

IcmpOutMsgs	エンティティが送信した ICMP メッセージの総数。これは icmpOutErrors でカウントされるものも含む。
IcmpOutErrors	バッファーが足りないというような ICMP で発見された問題の為にエンティティが送出しなかった ICMP メッセージの数。IP がデータグラムをルーティングできないという様な、ICMP の外の層で発見されたエラーは、この値には含まれない。
IcmpOutDestUnreachs	送信した ICMPDestinationUnreachable メッセージの数。
IcmpOutTimeExcds	送信した ICMPTimeExceeded メッセージの数。
IcmpOutParmProbs	送信した ICMPParameterProblem メッセージの数。
IcmpOutSrcQuenchs	送信した ICMPSourceQuench メッセージの数。
IcmpOutRedirects	送信した ICMPRedirect メッセージの数。ホストは redirects メッセージを出せないのでこのオブジェクトの値は常に 0 となる。
IcmpOutEchos	送信した ICMPEcho(request)メッセージの数。
IcmpOutEchoReps	送信した ICMPEchoReply メッセージの数。
IcmpOutTimestamps	送信した icmpOutTimestamps メッセージの数。

IcmpOutTimestampReps	送信した ICMPTimeStampReply メッセージの数。
IcmpOutAddrMasks	送信した icmpOutAddrMasks メッセージの数。
IcmpOutAddrMaskReps	送信した icmpOutAddrMaskReps メッセージの数。

VLAN ルーティング設定（Configure VLAN Routing）

あるポートでは VLAN、あるポートではルーティングをサポートしているようにスイッチソフトウェアを設定することができます。VLAN 上のトラフィックが、VLAN がルーターポートであるように扱われるようにソフトウェアを設定することもできます。

ポートがルーティングよりもブリッジング（デフォルト）として有効にされると、入力されるパケットに対してすべての通常のブリッジングの処理がされ、VLAN に割り当てられます。宛先 MAC アドレス（MAC DA）と VLAN ID が MAC アドレステーブルの検索に使われます。ルーティングが VLAN で有効になっており、入力されるユニキャストパケットの宛先 MAC アドレスがになっているとパケットはルートされます。入力されるマルチキャストパケットは VLAN 中のすべてのポートと、パケットがルーティングされる VLAN で受信された場合は内部ブリッジルーターインターフェースにも転送されます。

ポートは一つ以上の VLAN に属するように設定できるので、VLAN ルーティングはポート上のすべての VLAN あるいはサブネットで有効にできます。VLAN ルーティングは一つ以上の物理ポートが一つのサブネットに存在することを許容するように使えます。VLAN が複数の物理ネットワークに渡る場合や追加の分割やセキュリティが必要な場合にも使うことができます。この章ではスイッチソフトウェアで VLAN ルーティングをサポートする方法を示します。ポートは VLAN ポートまたはルーターポートになることはできますが、同時に両方になることはできません。しかし、VLAN ポートはルーターポートである VLAN の一部となることはできます。

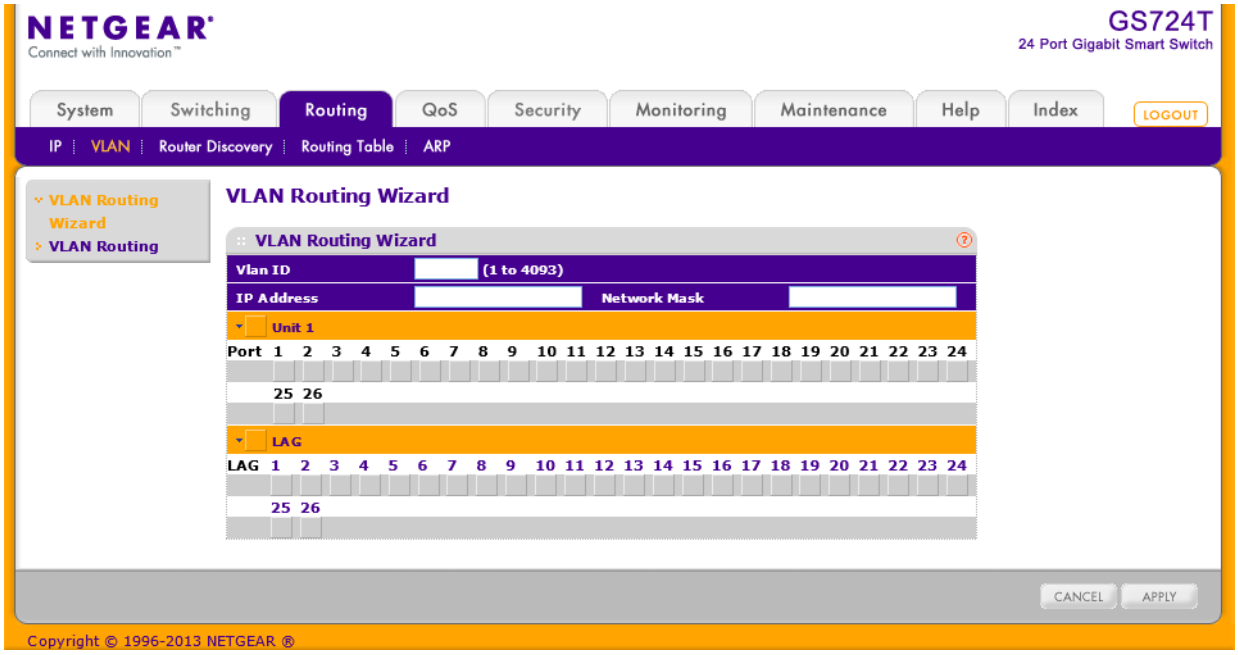
VLAN ルーティングウィザード（VLAN Routing Wizard）

VLAN ルーティングウィザード（VLAN Routing Wizard）は VLAN ルーティングインターフェースを作り、インターフェースの IP アドレスとサブネットマスクを設定し、選択したポートまたは LAG を VLAN に追加します。ウィザードを使って、以下のことができます。

- VLAN を作成し、VLAN に名前をつける。
- 選択したポートを新しく作成した VLAN に追加し、デフォルト VLAN から削除する。
- LAG を作成し、選択したポートを LAG に追加し、LAG を新しく作成した VLAN に追加する。
- ポートが他の VLAN に存在する場合は、選択したポートにタグを設定する。選択したポートが他の VLAN に存在しない場合はタグを無効にする。
- VLAN から選択されていないポートを除外する。
- 入力した IP アドレスとサブネットマスクを使って VLAN でルーティングを有効にする。

VLAN ルーティングウィザードを使って VLAN ルーティングを設定する

1. **Routing** > **VLAN** > **VLAN Routing Wizard** を選択して **VLAN Routing Wizard** ページを表示します。
2. **Vlan ID**：VLAN ID を指定します。



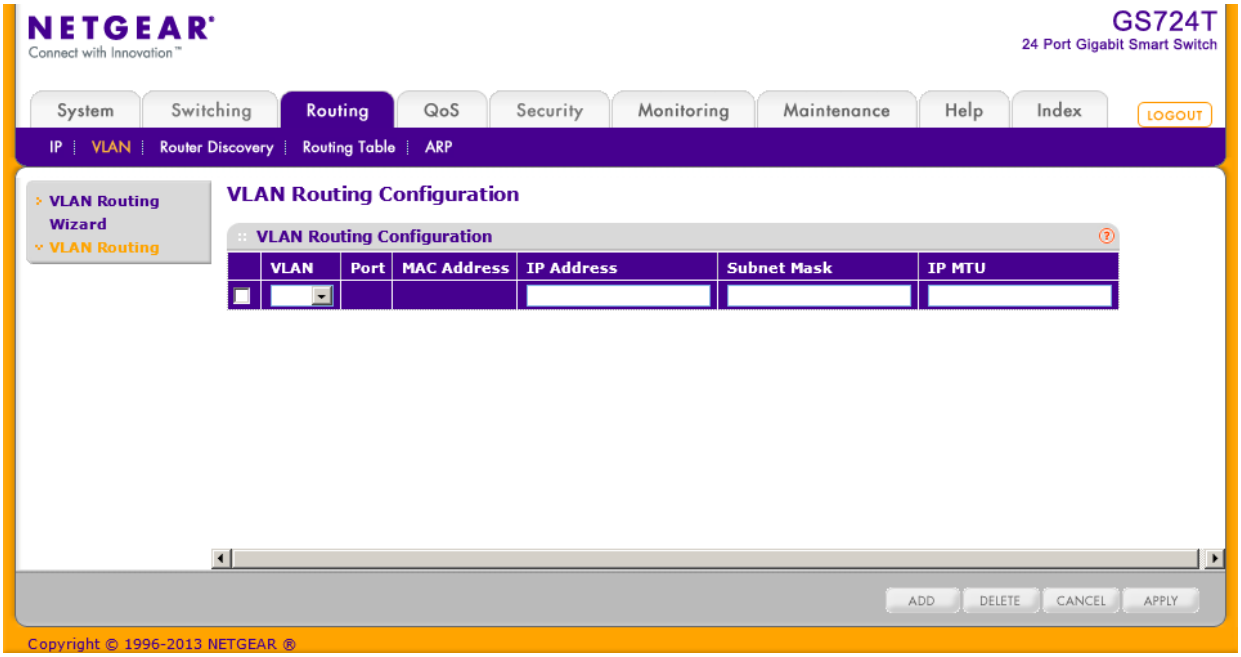
3. **IP Address**：VLAN インターフェースの IP アドレスを指定します。
4. **Network Mask**：VLAN インターフェースのサブネットマスクを指定します。
5. オレンジのバーをクリックしてポートと LAG を表示します。
6. VLAN メンバーに追加するポート LAG を選択します。
   ポートと LAG は3つのモードを持ちます。
   - **T(Tagged)**：タグ付きポートとして設定して、VLAN に含めます。
   - **U(Untagged)**：タグなしポートとして VLAN に含めます。
   - **空白(Autodetect)**：GVRP を使って動的にこの VLAN に含めます。この VLAN から除外する設定です。
7. **Apply** ボタンをクリックします。

VLAN ルーティング設定（VLAN Routing Configuration）

VLAN Routing Configuration 画面で VLAN ルーティングインターフェースの情報を表示し、VLAN に IP アドレスとサブネットマスクを設定します。

VLAN ルーティングを設定する

1. Routing > VLAN > VLAN Routing を選択して VLAN Routing Configuration ページを表示します。



2. VLAN：設定する VLAN を選択します。
3. IP address：VLAN インターフェースの IP アドレスを指定します。
4. Subnet Mask：VLAN インターフェースのサブネットマスクを指定します。
5. IP MTU：インターフェースの IP MTU サイズを指定します。
   有効な値は68バイトからリンク MTU までです。デフォルトは 1500 バイトです。0 を指定すると未設定として、リンク MTU の値を使用します。
6. Add ボタンをクリックします。

以下の表に VLAN Routing Configuration 画面の情報を示します。

表 52. VLAN Routing Configuration

項目	説明
Port	VLAN ルーティングインターフェースに割り当てられたポート番号。
MAC Address	VLAN ルーティングインターフェースに割り当てられた MAC アドレス。

ルーターディスカバリー設定（Configure Router Discovery）

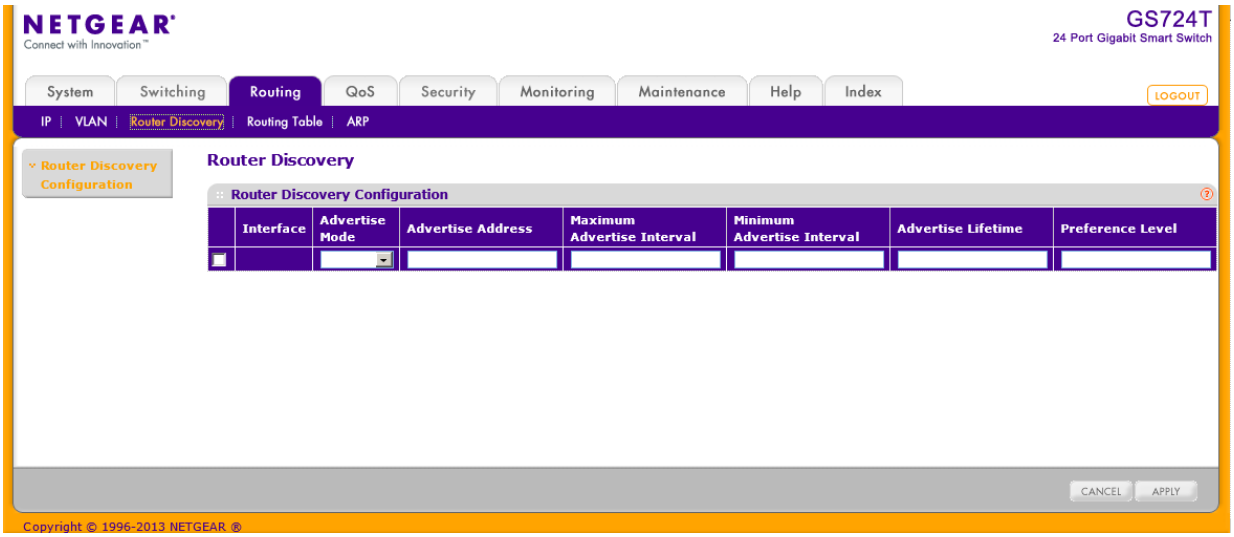
ルーターディスカバリープロトコル（Router Discovery protocol）はサブネットで動作するルーターを認識するためにホストによって使用されます。

ルーターディスカバリーメッセージはルーターアドバタイズメント（Router Advertisements）とルーター要請（Router Solicitations）の 2 つのタイプがあります。すべてのルーターは定期的に IP アドレスをアドバタイズすることを必須としています。ホストはこれらのアドバタイズメントをリスン（listen）し、近隣ルートを発見します。

Router Discovery Configuration 画面でルーターディスカバリー設定を入力、変更します。

ルーターディスカバリー設定をする

1. Routing > Router Discovery を選択して Router Discovery Configuration ページを表示します。



2. 設定するルーターインターフェースを選択します。
3. Advertise Mode: Enable を選択してインターフェースからルーターアドバタイズを送信します。
4. Advertise Address：アドバタイズするルーターの IP アドレスを指定します。
5. Maximum Advertise Interval：ルーターアドバタイズメントの最大送信間隔を設定します。範囲は 4－1800 秒です。デフォルトは 600 秒です。
6. Minimum Advertise Interval：ルーターアドバタイズメントの最小送信間隔を設定します。範囲は 3－1800 秒です。デフォルトは 450 秒です。
7. Advertise Lifetime：ルーターアドバタイズメントの値の有効時間を設定します。範囲は 4－9000 秒です。デフォルトは 1800 秒です。

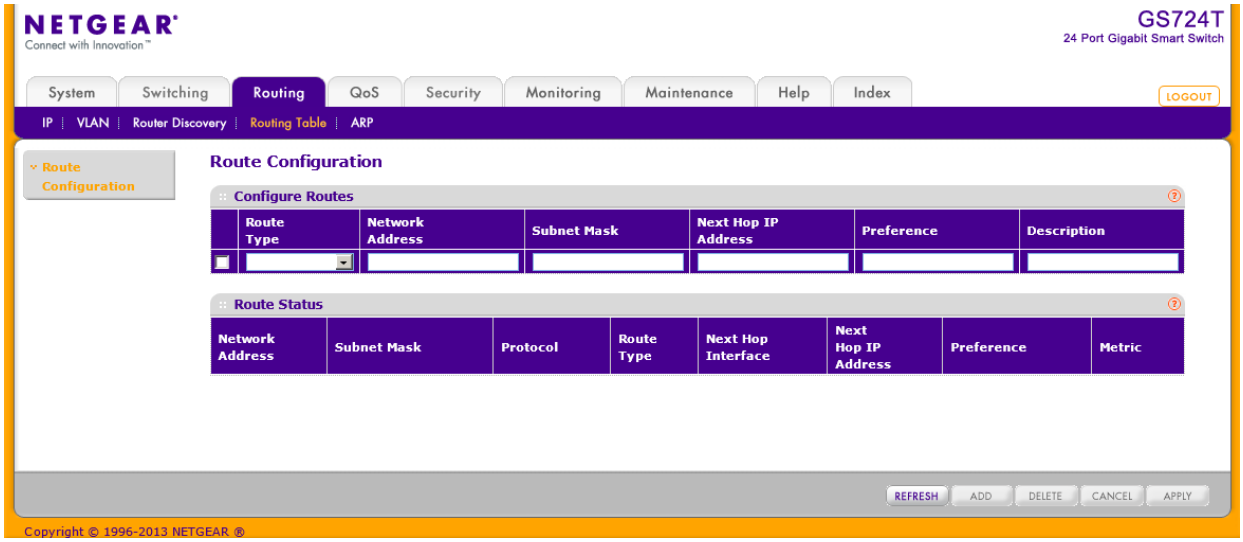
8. **Preference Level**：デフォルトルーターとしての同じサブネット中の他のルーターとの相対的な優先レベルを指定します。大きな値が優先されます。整数を入力する必要があります。値の範囲は-2147483648 から 2147483647 です。デフォルトは 0 です。
9. **Apply** ボタンをクリックします。

ルートの設定と表示（Configure and View Routes）

Route Configuration 画面でスタティックルートとデフォルトルートを設定し、スイッチが学習したルートを表示できます。

ルートを設定する

1. **Routing** > **Routing Table** > **Route Configuration** を選択して **Route Configuration** ページを表示します。



2. **Route Type**：設定するルートのタイプを選択します。
   - **Static**：スタティックルートを設定するときに選択します。
   - **Default Route**：デフォルトルートを設定するときに選択します。デフォルトルートを設定するときに入力する必要があるのは、Next Hop Address と Preference です。デフォルトルートの Preference は 1 です。
3. **Network Address**：IP ルートプレフィクスを指定します。
   ルートを作成するには、有効なルーティングインターフェースが存在する必要があり、ネクストホップ IP アドレスはルーティングインターフェースと同じサブネットにある必要があります。
4. **Subnet Mask**：サブネットマスクを指定します。
   隣接ネットワークの IP アドレスの一部を表します。
5. **Next Hop IP Address**：ネクストホップ IP アドレスを指定します。

ルートを作成するには、ネクストホップ IP はルーティングインターフェースと同じサブネットにある必要があります。有効なネクストホップ IP アドレスは Route Status テーブルに載っています。

6. **Preference**：ルートの優先度を指定します。
同じ宛先のルートの中で一番小さな Preference の値のルートがフォワーディングデータベースにルートとして登録されます。スタティックルートに Preference を設定することによって、スタティックルートの優先度を設定することができます。
7. **Description**：（オプション）ルートの説明を記入します。英数 31 文字までです。
8. **Add** ボタンをクリックしてルートを追加します。
9. ルートを削除するには、削除するルートを選択し、**Delete** ボタンをクリックします。
10. ルートを変更するには、変更するルート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。
11. **Refresh** ボタンをクリックして最新情報を表示させます。
12. **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。

次の **Route Status** 表はスイッチのスタティックルートと動的に学習したルートを表示します。

表 53. Route Status

項目	説明
Route Type	ルートのタイプ。Static または Default route。
Network Address	IP ルートプレフィクス
Subnet Mask	サブネットマスク。
Protocol	ルート作成のプロトコル。 • Local • Static
Route Type	ルートタイプ。Connected、Static、Dynamic。

Next Hop Interface	ネクストホップのインターフェース。
Next Hop IP Address	ネクストホップ IP アドレス。
Preference	ルートの優先度。(1-255)
Metric	宛先までのパスコスト。

ARP 設定（Configure ARP）

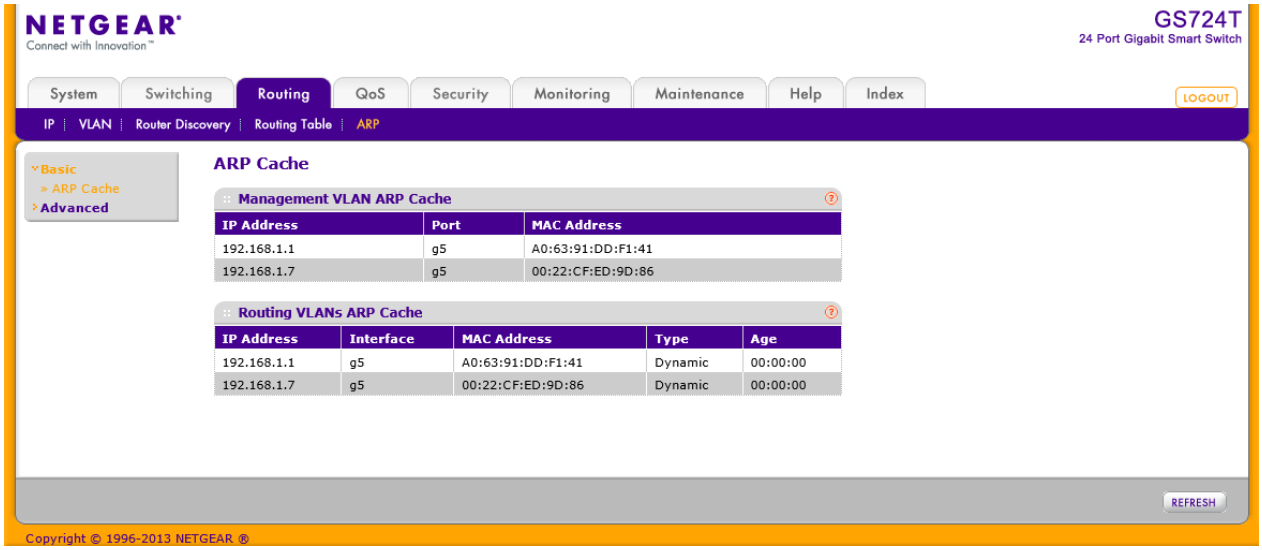
ARP(Address Resolution Protocol)はレイヤー2MAC アドレスとレイヤー3IPv4 アドレスを関連付けます。スイッチソフトウェアは動的および静的な ARP 設定をサポートしています。マニュアル ARP 設定では、静的に ARP テーブルにエントリーを追加できます。

ARP は IP(Internet Protocol)の必須プロトコルであり、IP アドレスをイーサネットのような LAN(Local Area Network)のメディアアドレス（MAC）へ変換するために使われます。IP パケットを送信する必要のあるすケーションは IP 宛先、あるいは宛先が同じサブネット上にない場合はネクストホップルーターの MAC アドレスを知る必要があります。これは ARP 要求パケットをブロードキャストし、受信者が ARP 応答に自分の MAC アドレスをユニキャストで返信することによって実現されます。一度学習した後、IP パケットの前につけられるレイヤー2 ヘッダー中の宛先アドレスとして MAC アドレスが使われます。

ARP キャッシュはネットワーク上の各ステーションによって維持されるテーブルです。ARP キャシュエントリーは ARP 要求、ARP 応答のタイプによらず、ARP パケットの送信元アドレスを検査することによって学習されます。このようにして、ARP 要求が LAN セグメントまたは VLAN のすべてのステーションにブロードキャストされ、それぞれの受信者は ARP キャッシュに送信者の IP アドレスと MAC アドレスを保存することができます。ユニキャストの ARP 応答は通常要求者にのみ見え、要求者は送信者情報を ARP キャッシュに保存します。新しい情報は ARP キャッシュの既存の情報を更新します。

スイッチは動的、静的合わせて 512 の ARP エントリーをサポートします。

デバイスはネットワーク内で移動することがあり、MAC アドレスと関連付けられていた IP アドレスは異なる MAC アドレスを使っていたり、ネットワークから消えてしまっている事があります。周期的に更新されないと ARP キャッシュ中の情報の陳腐化へとつながります。



ARP キャッシュ（ARP Cache）

ARP Cache 画面でリモート接続のテーブルである ARP テーブルのエントリーを表示します。

Routing > **ARP** > **Basic** > **ARP Cache** を選択して **ARP Cache** ページを表示します。

以下の表は **Management VLAN ARP Cache** ページの情報を示します。

表 54. **Management VLAN ARP Cache**

項目	説明
IP Address	マネージメント VLAN に接続されているデバイスの IP アドレス。
Port	デバイスが接続されているポート。
MAC Address	デバイスの MAC アドレス。

以下の表は **Routing VLANs ARP Cache** ページの情報を示します。

表 55. **Routing VLANs ARP Cache**

項目	説明
Interface	ARP エントリーと関連付けられているルーティングインターフェース。
IP Address	ルーティングインターフェースに接続されているデバイスの IP アドレス。
MAC Address	デバイスの MAC アドレス。
Type	ARP エントリーのタイプ。 • **Local**：ローカルインターフェース。 • Gateway：ルーター。 • **Static**：スタティック。

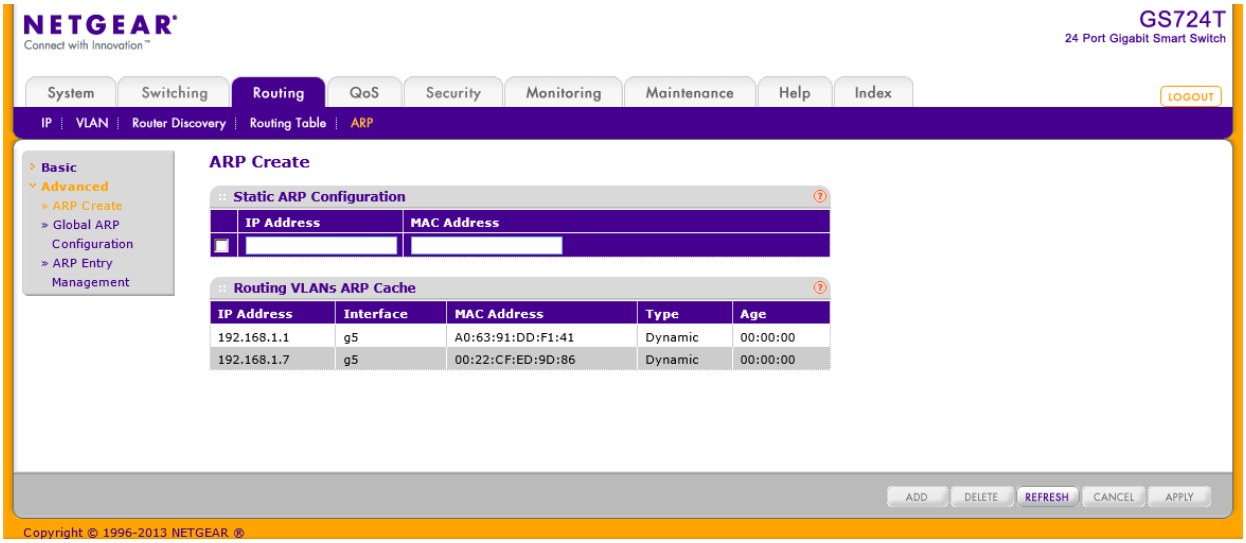
	• Dynamic：ダイナミック。
Age	ARP テーブルで更新されてからの時間。形式は hh:mm:ss。

スタティック ARP エントリーを作る（Create a Static ARP Entry）

この画面で ARP テーブルにスタティックエントリーを追加します。

ARP テーブルにエントリーを追加する

1. **Routing** > **ARP** > **Advanced** > **ARP Create** を選択して **ARP Create** ページを表示します。



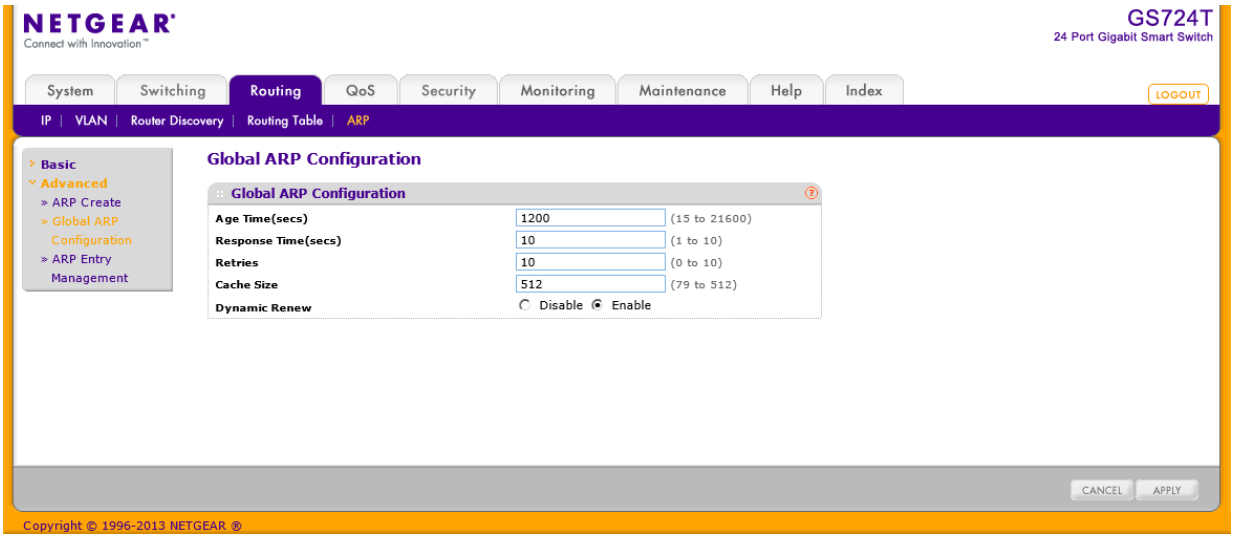
2. **IP Address**：追加する IP アドレスを記入します。スイッチのルーティングインターフェースと同じサブネットの IP アドレスを追加します。
3. **MAC Address**：デバイスの MAC アドレスを記入します。形式は 00:06:29:32:81:40（例）です。
4. **Add** ボタンをクリックします。

グローバル ARP 設定（Configure Global ARP Settings）

Global ARP Configuration 画面で ARP テーブル設定を表示、設定します。

ARP テーブルを表示、設定する

1. Routing > ARP > Advanced > Global ARP Configuration を選択して Global ARP Configuration ページを表示します。



2. Age Time(secs): ARP エントリーのエージアウトタイム（秒）。範囲は 15-21600 秒。デフォルトは 1200 秒。
3. Response Time(secs): ARP 応答タイムアウト。範囲は 1-10 秒。デフォルトは 10 秒。
4. Retries: ARP 要求の再送回数。範囲は 0-10。デフォルトは 10。
5. Cache Size: ARP キャッシュの最大エントリー数。範囲は 79-512。デフォルトは 512。
6. Dynamic Renew: Enable を選択すると、ダイナミック ARP エントリーがエージアウトした際に自動的に更新を試みます。
7. Apply ボタンをクリックします。

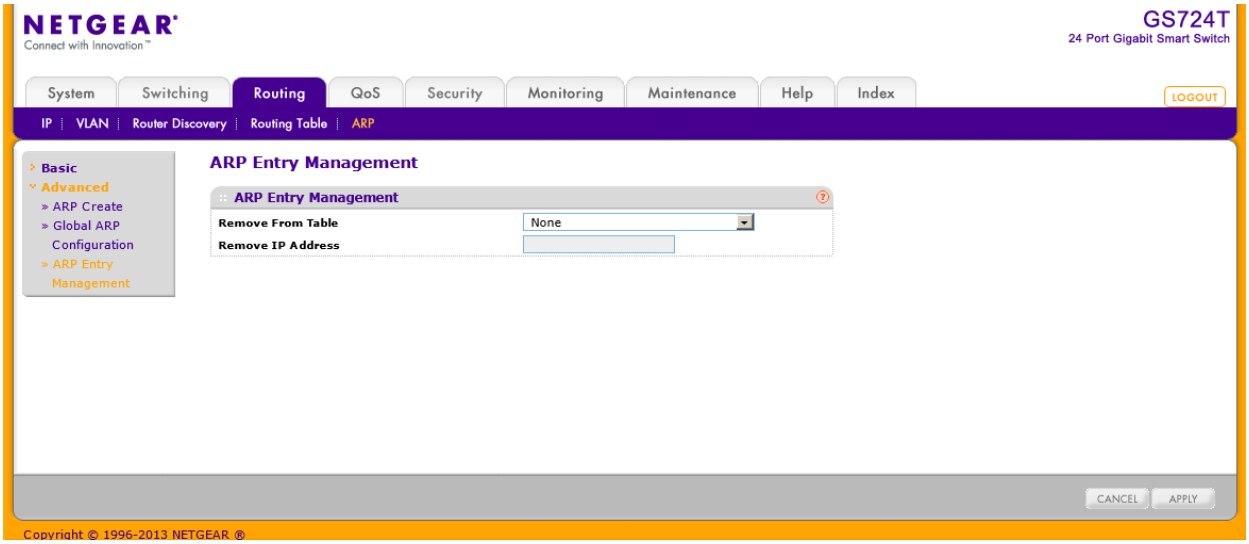
ARP キャッシュから ARP エントリーを削除する

この画面で ARP テーブルからエントリーを削除します。

ARP テーブルからエントリーを削除する

1. Routing > ARP > Advanced > ARP Entry Management を選択して ARP Entry Management ページを表示します。
2. Remove From Table: 削除する ARP エントリータイプを以下から選択します。
   - All Dynamic Entries
   - All Dynamic and Gateway Entries

- Specific Dynamic/Gateway Entry
- Specific Static Entry
- None：ARP テーブルのエントリーから削除をしない場合に選択します。



3. Remove IP Address：Specific Dynamic/Gateway Entry または Specific Static Entry を選択した時は、エントリーの IP アドレスを記入して ARP テーブルから削除します。
4. Apply ボタンをクリックします。

QoS 設定

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ることができます。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ため、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。

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)

CoS（Class of Service）

CoS（Class of Service)キューイング機能で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によ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。

スイッチではポート毎に 8 つのキューがサポートされています。

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

- CoS 設定(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）

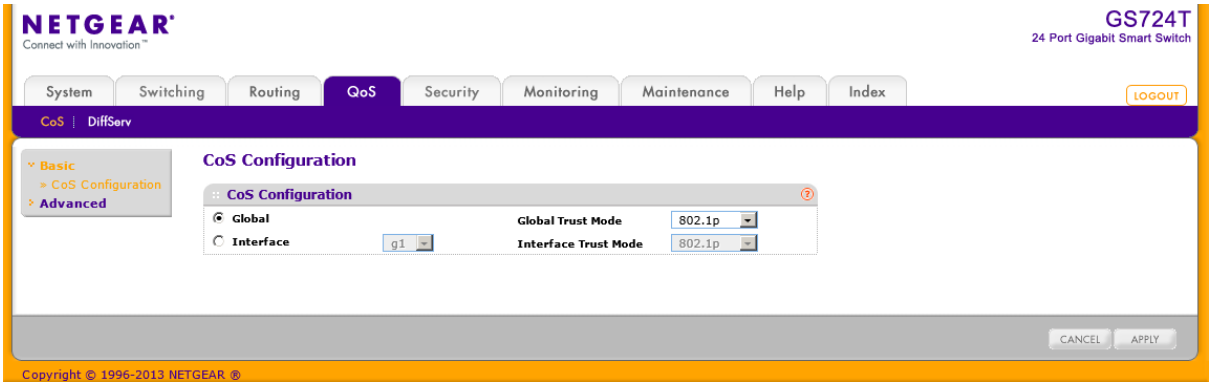
CoS 設定(CoS Configuration)

CoS Configuration ページで、インターフェースの 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 に割り当てることを含みます。

あるいは、ポートがアントラスト(untrusted)と設定されていると、受信したパケットのプライオリティを信頼せず、かわりにポートの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。

インターフェースに CoS トラストモード設定をする

1. **QoS > Basic > CoS Configuration** を選択して **CoS Configuration** ページを表示します。



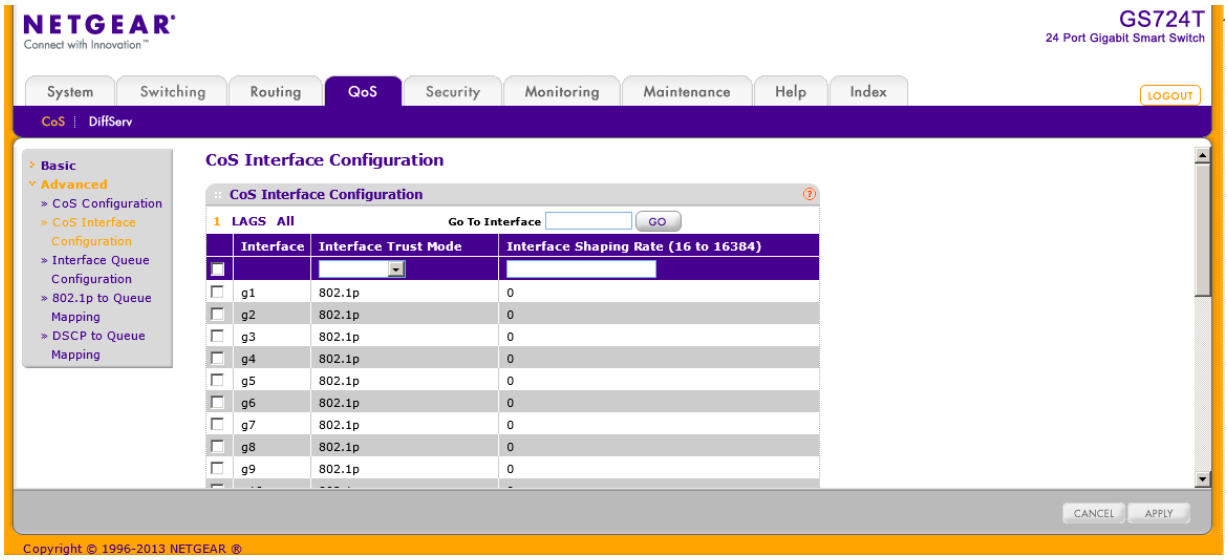
2. **Global** ラジオボタンを選択してすべてのインターフェースに適用するトラストモードを設定します。
   あるいは、**Interface** ラジオボタンを選択してトラストモード設定を個々のインターフェースに設定します。インターフェース設定はグローバル設定よりも優先されます。
3. すべてのインターフェース (Global Trust Mode)またはインターフェース(Interface Trust Mode)のどちらかのトラストモードを選択します。この設定でフレームがポートに入力した時の CoS マーキングのタイプを決定します。
   - **Untrusted**:受信パケットの CoS 設定を信頼しません。
   - **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 8 段階のハードウェアプライオリティキューにマッピングします。
   - **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。
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. **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。

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。

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. 1 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。
   - 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 8 段階のハードウェアプライオリティキューにマッピングします。
6. Interface 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。
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)

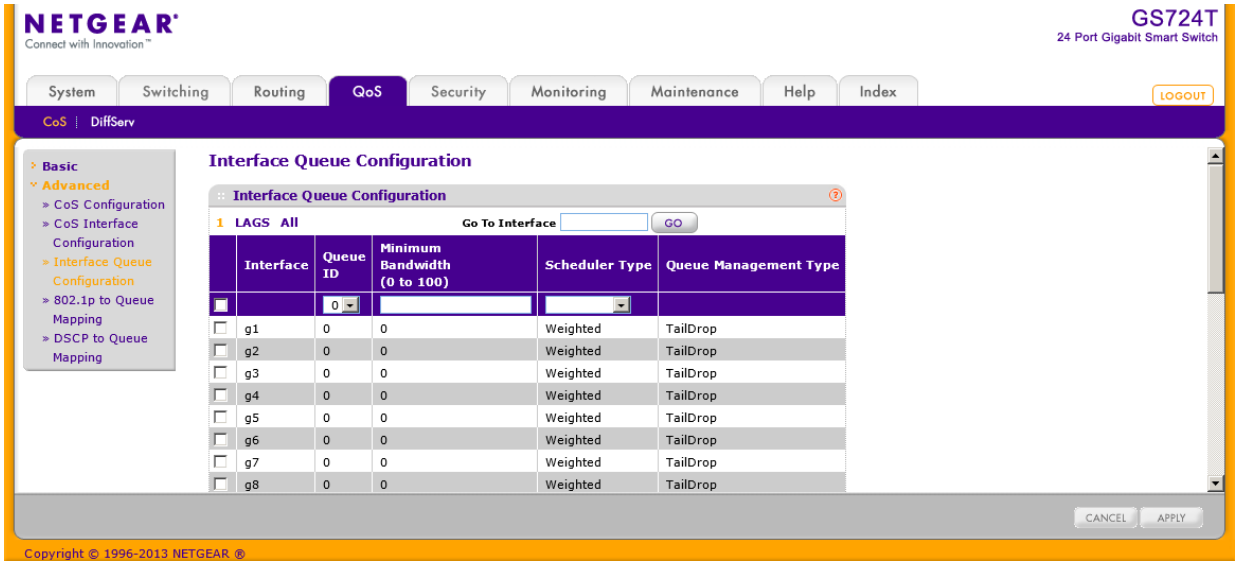
Interface Queue Configuration ページでスイッチ出力(Egress)キューを設定することによって特定のキュー動作を定義することができます。設定可能なパラメータは、キューが利用可能な帯域、

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または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。

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. 1 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。
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. 以下の項目の設定をします。
   - **Queue ID**:0-7 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。(Taildrop、テールドロップ)

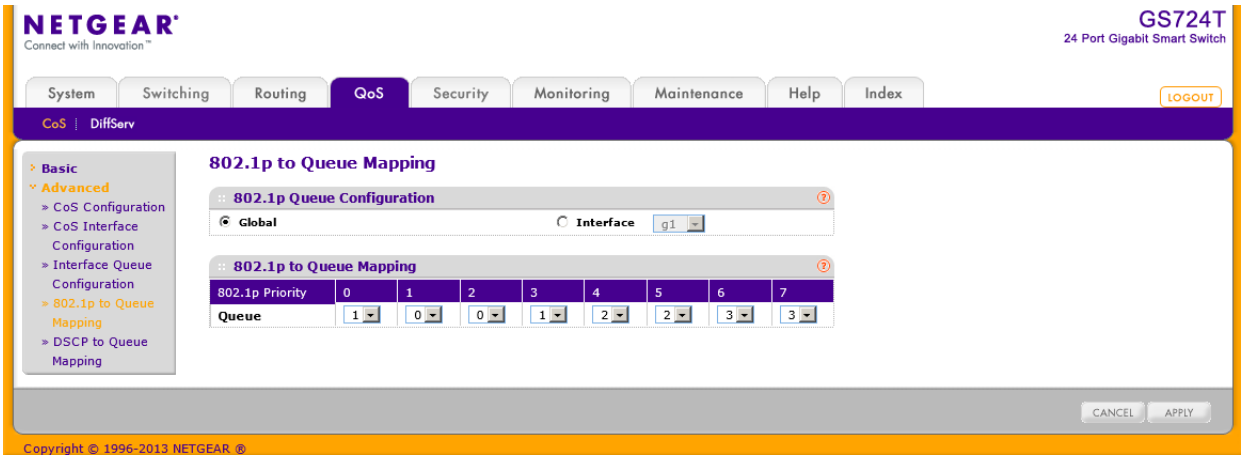
7. **Cancel** ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。
8. **Apply** ボタンをクリックして設定をスイッチに適用します。

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。

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。



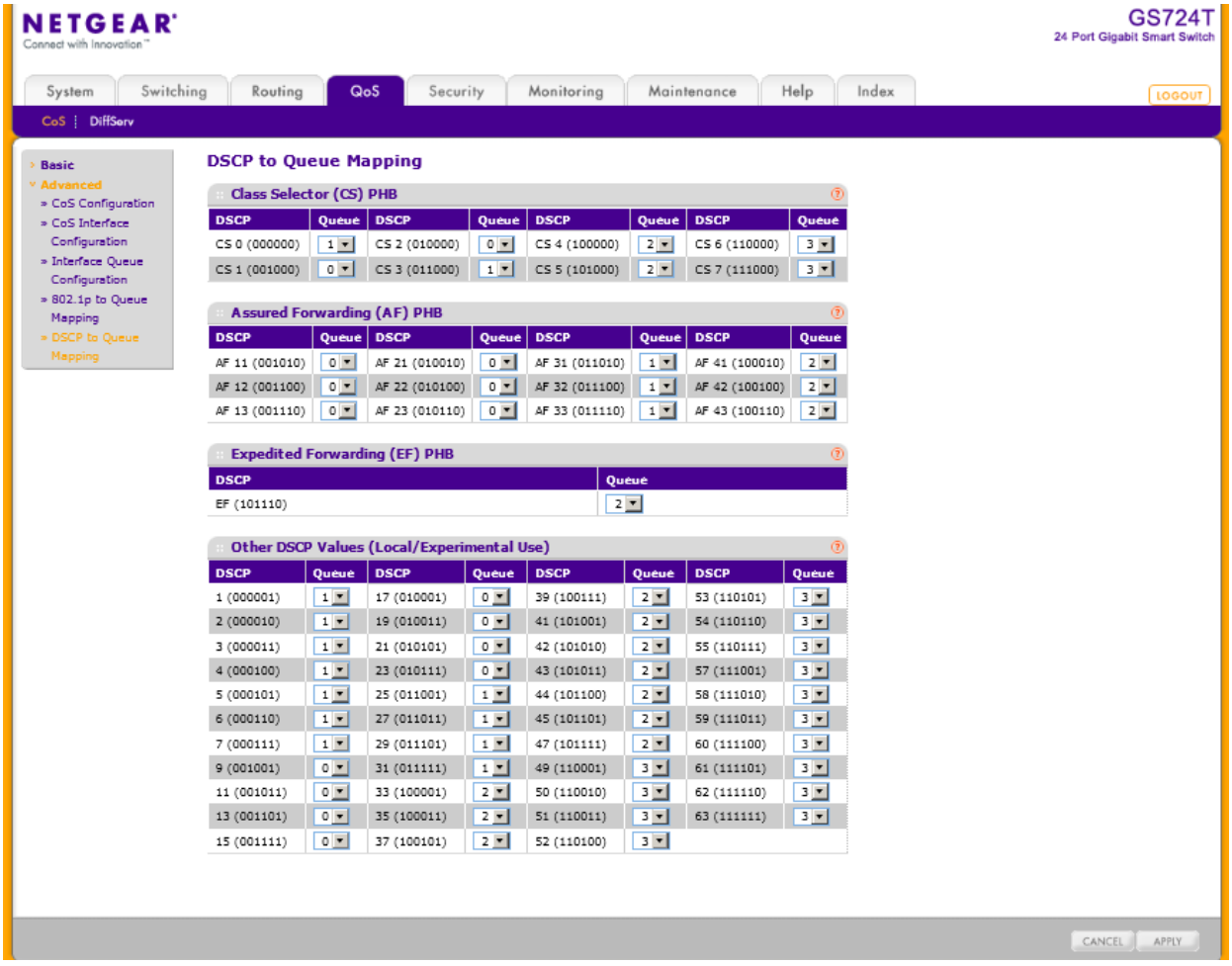
2. **Global** ラジオボタンを選択してすべてのインターフェースに同じ 802.1p プライオリティから CoS へのマッピングをするか、インターフェース単位にマッピングするかを選択します。あるいは、**Interface** ラジオボタンを選択してインターフェース単位に 802.1p プライオリティから CoS へのマッピングを設定します。インターフェース設定はグローバル設定よりも優先されます。
3. **802.1p to Queue Mapping**:802.1p プライオリティに対して、対応するキューを選択します。802.1p Priority 行は 8 つの 802.1p 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、7 が最高となります。トラフィッククラス 0-7 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。

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。



2. 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 0-7 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、7 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。

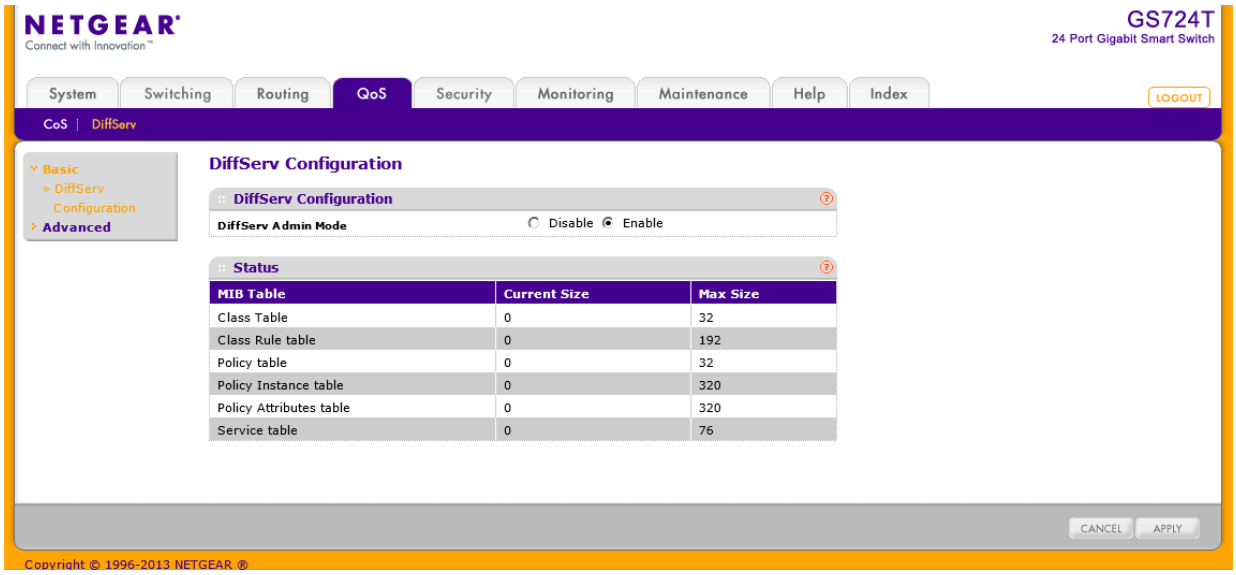
- DiffServ 設定(Diffserv Configuration)
- クラス設定(Class Configuration)
- IPv6 クラス設定(IPv6 Class Configuration)
- ポリシー設定(Policy Configuration)
- サービス設定(Service Configuration)
- サービス統計(Service Statistics)

DiffServ 設定(Diffserv Configuration)

Diffserv Configuration ページでは、現在の情報および DiffServ プライベート MIB テーブルの現在および最大行数を確認することができます。

グローバル DiffServ モードを設定する

1. QoS > DiffServ > Advanced > Diffserv Configuration を選択して Diffserv Configuration ページを表示します。



2. DiffServ Admin Mode: 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 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
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。

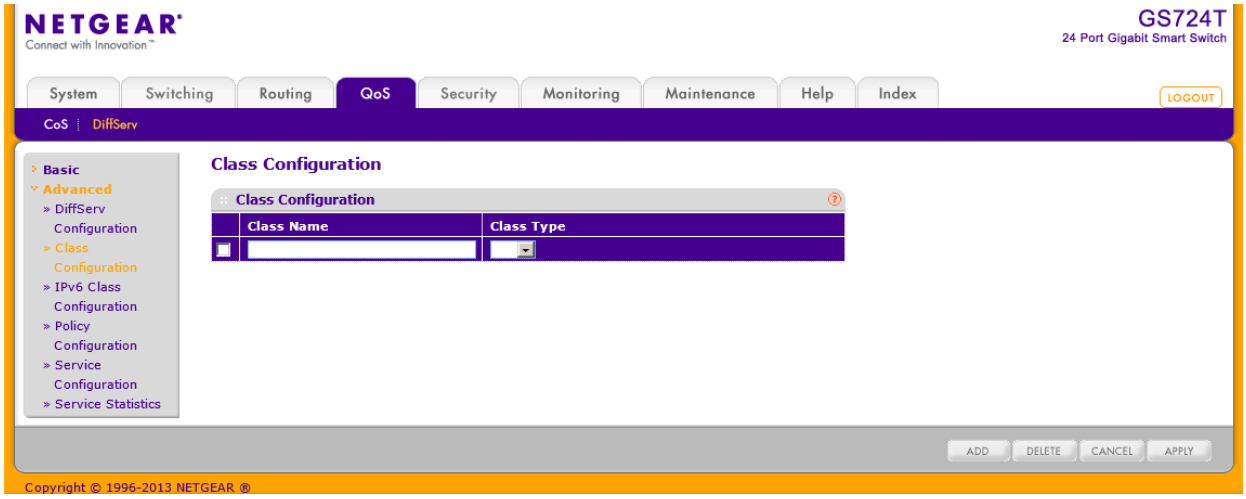
Refresh ボタンをクリックしてスイッチの最新情報を表示させます。

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。

DiffServ クラスを設定する

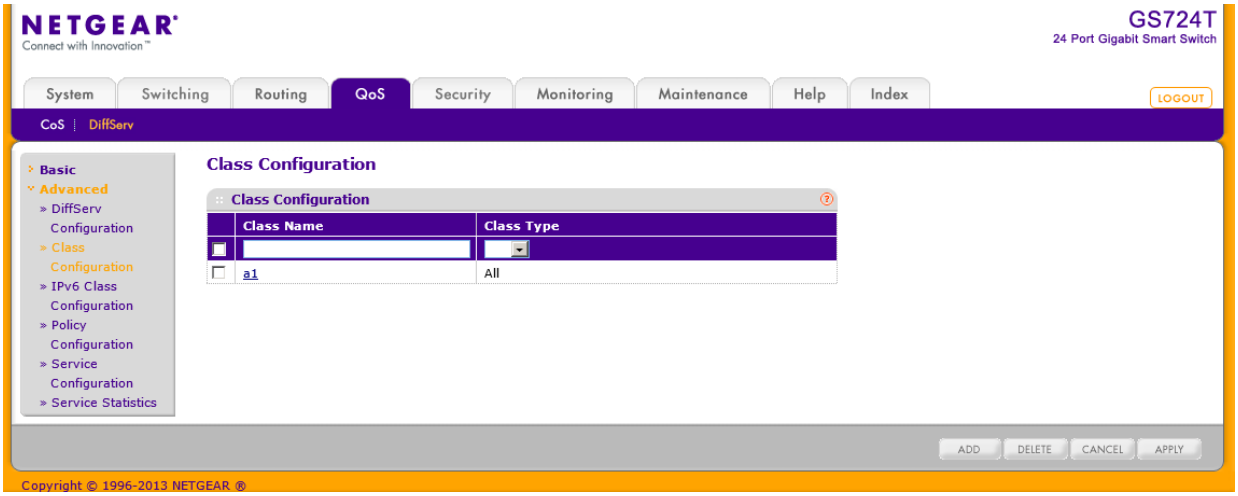
1. QoS > DiffServ > Advanced > Class Configuration を選択して Class Configuration ページを表示します。



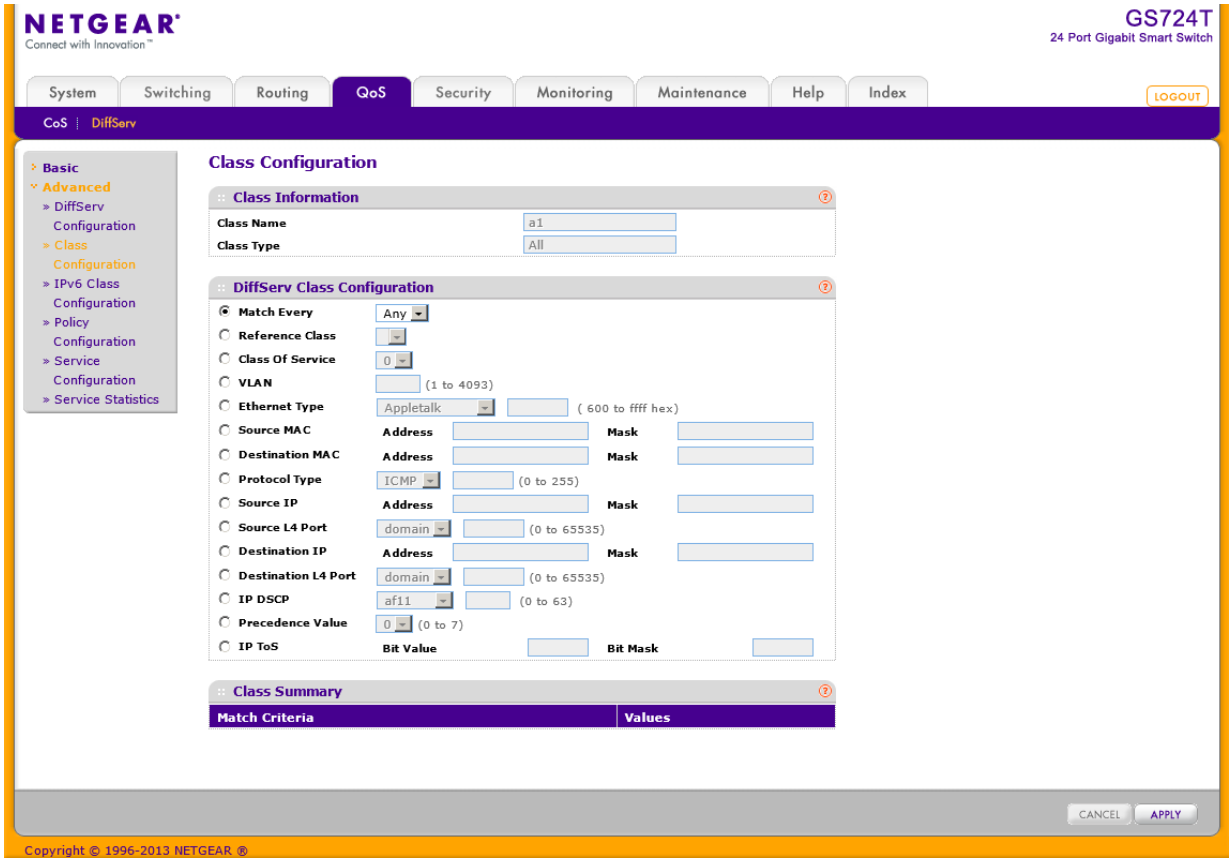
2. 新しいクラスを作成するには、クラス名を Class Name 欄に記入し、Class Type を指定して Add ボタンをクリックします。
   スイッチのサポートしている Class Type は All のみです。
3. 既存のクラス名を変更するには、変更するクラスのチェックボックスを選択し、変更をします。変更後、Apply ボタンをクリックします。
4. クラスを削除するには、削除するクラスのチェックボックスを選択し、Delete ボタンをクリックします。
5. Refresh ボタンをクリックしてスイッチの最新情報を表示させます。
6. Cancel ボタンをクリックして設定画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



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。



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。

- **Match Every**:**Any**:すべてのパケットがクラスに属する時に使います。
- **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 Address**: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 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 Address**: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 IP 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 IP 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 Class Configuration で IPv6 パケット識別を行うことによって、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。IPv6 アクセスリストは IPv4 アクセスリスト同様に機能します。

IPv6 クラス機能以前には、どの DiffServ クラス定義も IPv4 パケットに適用されていました。すなわち、クラスのマッチアイテムは IPv4 ヘッダーとして解釈されていました。IPv6 マッチ機能の導入によって、クラスルールが IPv4 用か IPv6 用かを指定することが必要となりました。この違いを容易にするために、クラスが IPv4 パケットストリームか IPv6 パケットストリームに適用されるかを指定するクラス設定パラメータが追加されました。

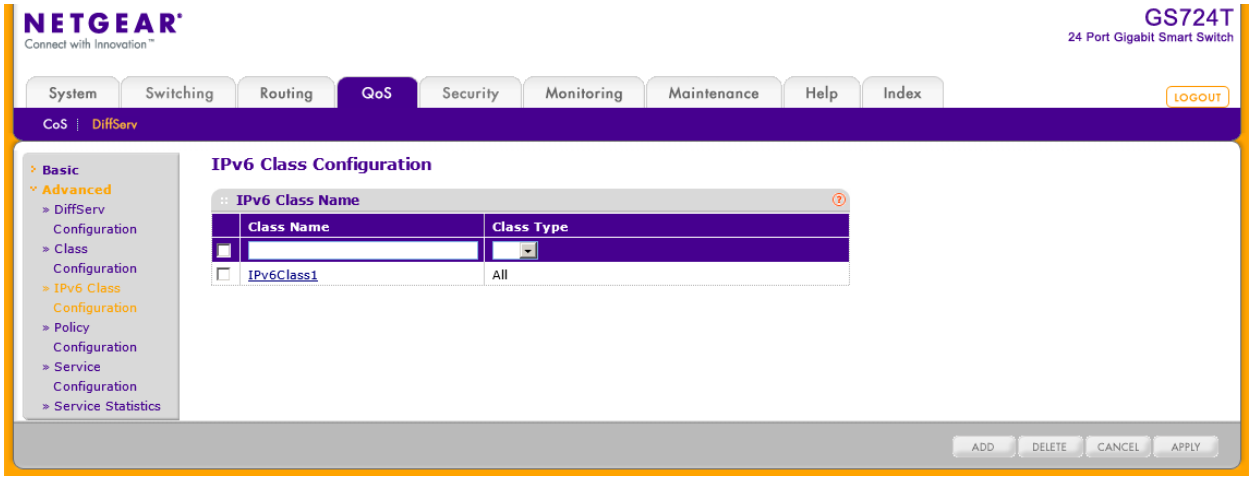
宛先と送信元の IPv6 アドレスはマスクの代わりにプレフィクス値を使います。エンドステーションが使う IPv6 パケットを区別するフローラベルはルーターでの QoS 処理の形態意味づける 20 ビットの値です。

IPv6 識別に一致するパケットは 802.1p（CoS）値あるいは Traffic Class オクテットの IP DSCP 値のみを使ってマーキングされます。IP Precedence は IPv6 には定義されていません。

IPv6 ACL/DiffServ 割当は LAG インターフェースにも適用できます。ACL や DiffServ ポリシーに説明されている手順も同様に LAG インターフェースに適用可能です。

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。



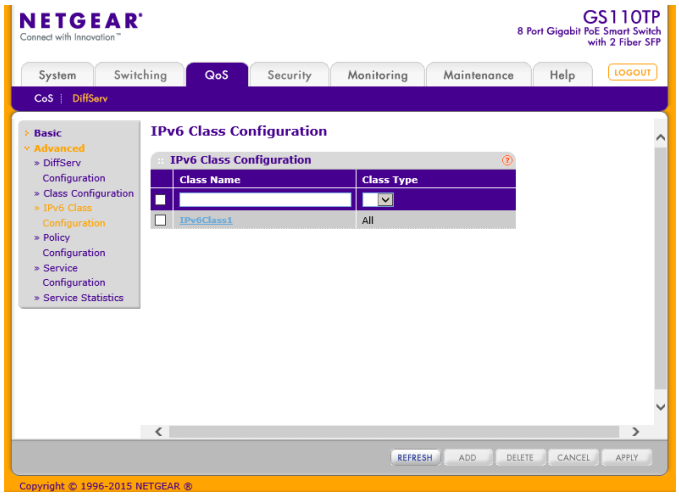
2. 新しいクラスを作成するには、クラス名を **Class Name** 欄に記入し、**Class Type** を指定して **Add** ボタンをクリックします。
   スイッチのサポートしている **Class Type** は **All** のみです。
3. 既存のクラス名を変更するには、変更するクラスのチェックボックスを選択し、変更をしま

す。変更後、Apply ボタンをクリックします。

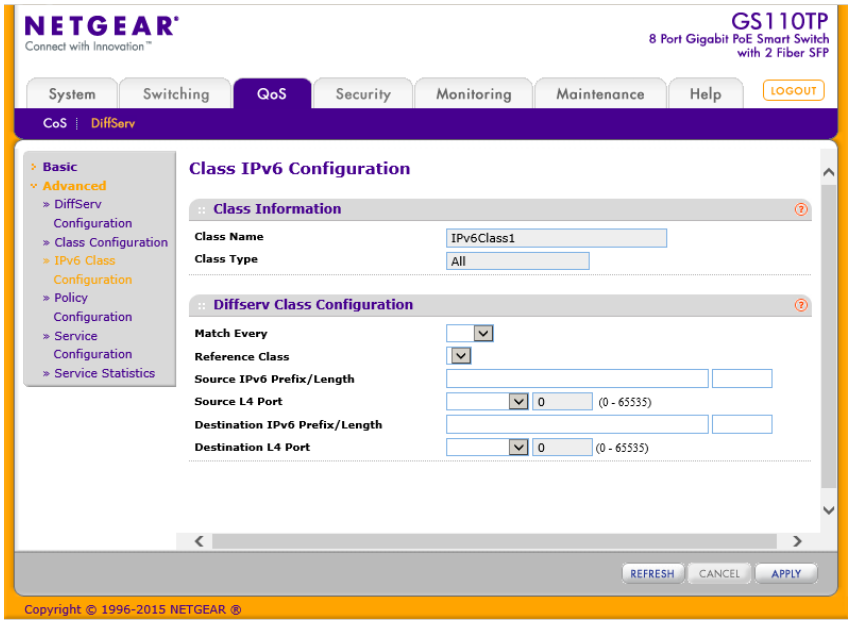
4. クラスを削除するには、削除するクラスのチェックボックスを選択し、Delete ボタンをクリックします。
5. Refresh ボタンをクリックしてスイッチの最新情報を表示させます。
6. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。

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。



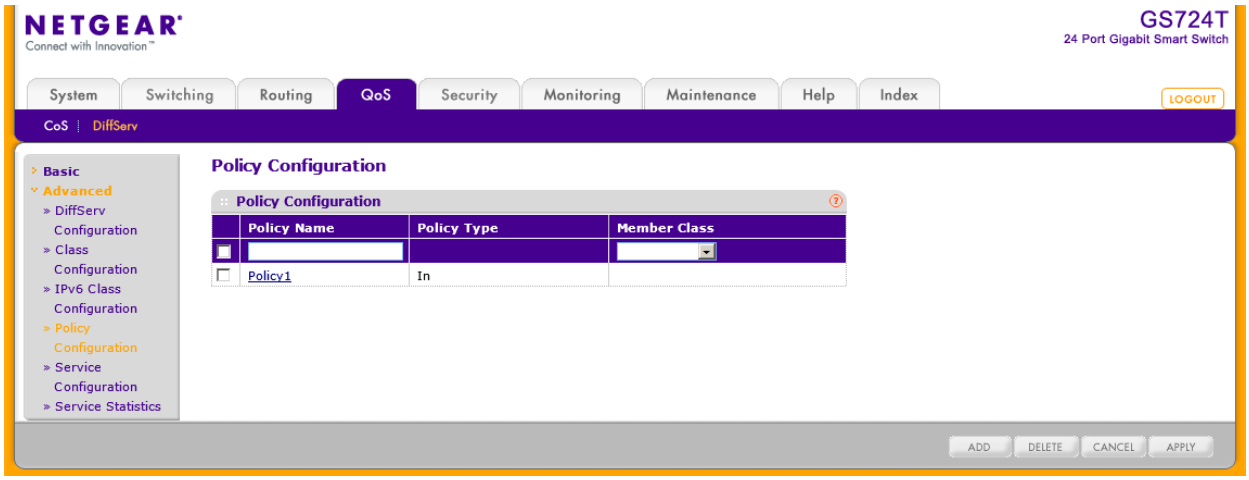
クラス名はハイパーリンクになっており、以下のような DiffServ Class Configuration 画面が表示されます。



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。

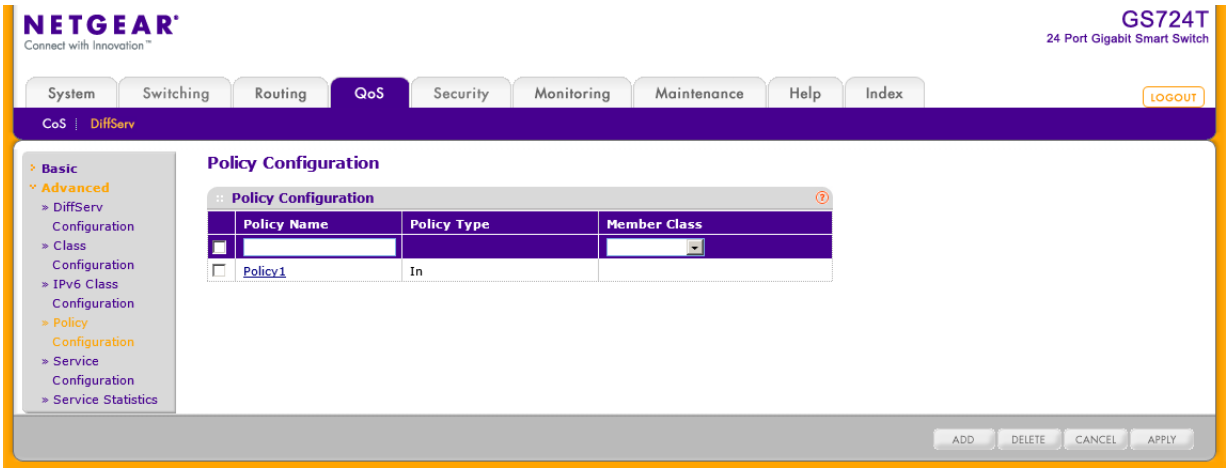
ポリシー設定(Policy Configuration)

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。



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。

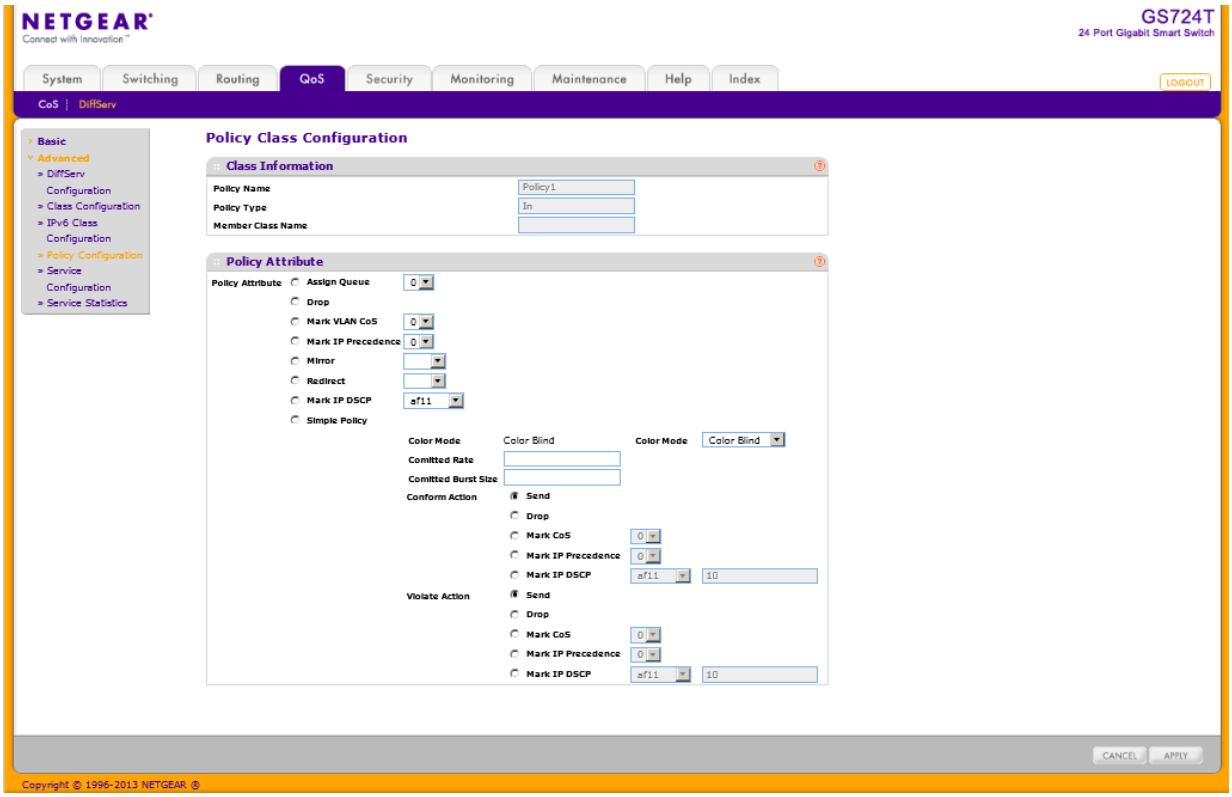


2. ポリシーを作成するには、Policy Selector 欄にポリシー名を入力し、Member Class 欄でクラスを選択します。Add ボタンをクリックしてポリシーを作成します。
ポリシータイプ（Policy Type）は In のみであり、受信方向のトラフィックにのみ有効です。この設定は変更不可です。
3. 既存のポリシー名を変更するには、変更するポリシーのチェックボックスを選択し、変更をします。変更後、Apply ボタンをクリックします。
4. ポリシーを削除するには、削除するポリシーのチェックボックスを選択し、Delete ボタンをクリックします。
5. Refresh ボタンを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。

2. 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。



3. **Policy Attribute** 項目を設定します。
   - **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。
   - **Drop**：パケットを廃棄する場合に選択します。
   - **Mark VLAN CoS**：802.1p CoS 値(0-7)を適用したい場合に選択します。
   - **Mark IP Precedence**：IP Precedence 値(0-7)を設定します。
   - **Mirror**：入力パケットを指定したポートにミラーリングします。
   - **Redirect**：入力パケットを指定したポートにリダイレクトします。
   - **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。
     - **Color Conform Class**：Color Mode で Color Aware を選択した時のみ表示されます。適用する DiffServ クラスを選択します。必ず一つ選択します。
     - **Color Mode**：.Color Mode を選択します。デフォルトは Color Blind です。
       - **Color Blind**：入力トラフィックの設定に依存しません。
       - **Color Aware**：入力トラフィックの設定に依存します。

- **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 Precedence**：IP Precedence 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 Precedence**：IP Precedence 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。

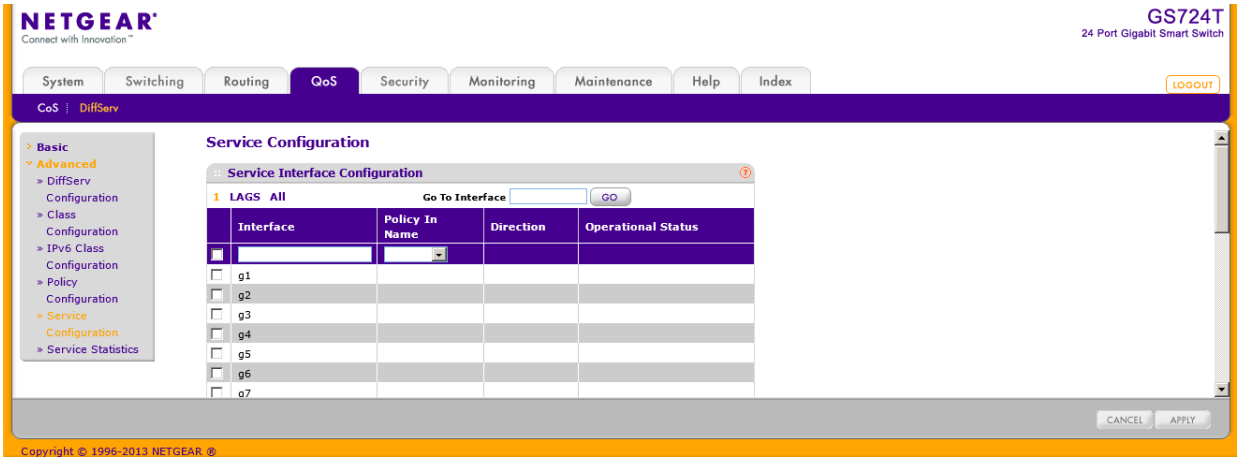
4. **Cancel** ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。
5. **Apply** ボタンをクリックして設定をスイッチに適用します。すぐに設定変更がされます。
6. **Refresh** ボタンをクリックしてスイッチの最新情報を表示させます。

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。

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。

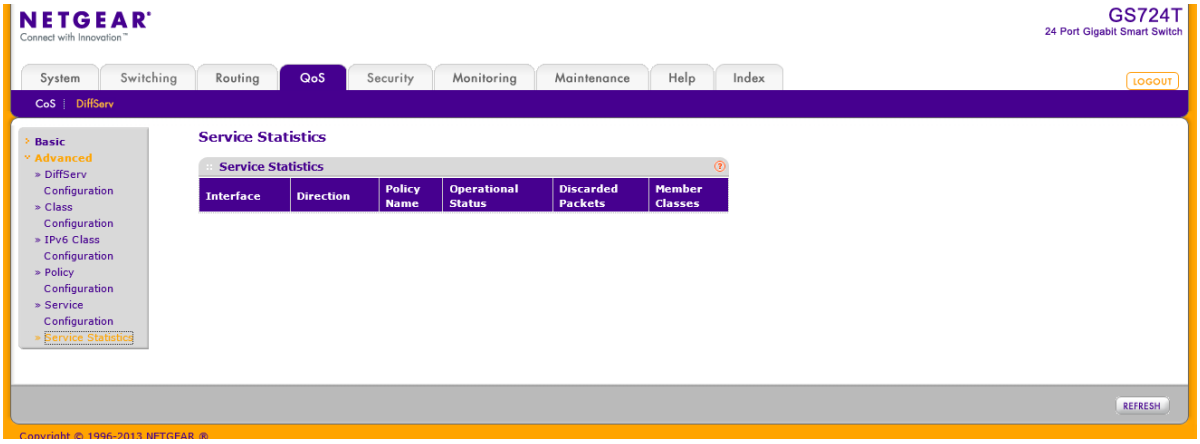


2. 1をクリックして、物理ポートの DiffServ ポリシー設定をします。
3. LAGS をクリックして、LAG（Link Aggregation Group)の DiffServ ポリシー設定をします。
4. ALL をクリックして、物理ポートと LAG（Link Aggregation Group)の両方の DiffServ ポリシー設定をします。
5. 設定をしたいポートまたは LAG の横のチェックボックスをクリックして選択をします。複数の選択をして共通の設定をすることも可能です。先頭のチェックボックスをクリックするとすべてのインターフェースを選択できます。
6. 選択したインターフェースにポリシーを適用するには、Policy In Name 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 Name 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。



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。

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。

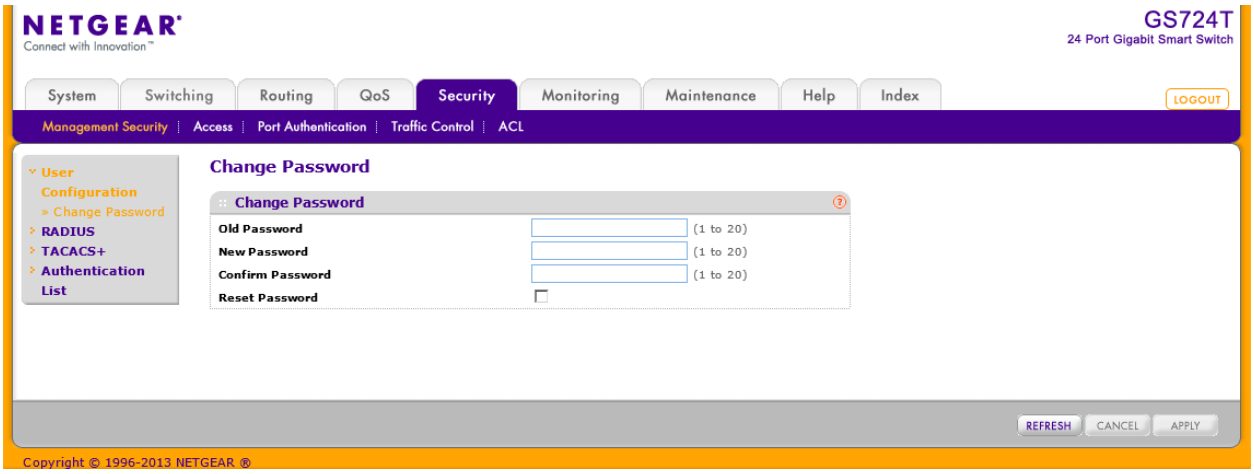
- パスワード変更(Change Password)
- RADIUS 設定(RADIUS Configuration)
- TACACS+設定(Configuring TACACS+)
- 認証リスト設定(Authentication List Configuration)

パスワード変更(Change Password)

この画面でログインパスワードを変更します。

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 **Change Password** 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(Port Access Control)

RADIUS メニュー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)

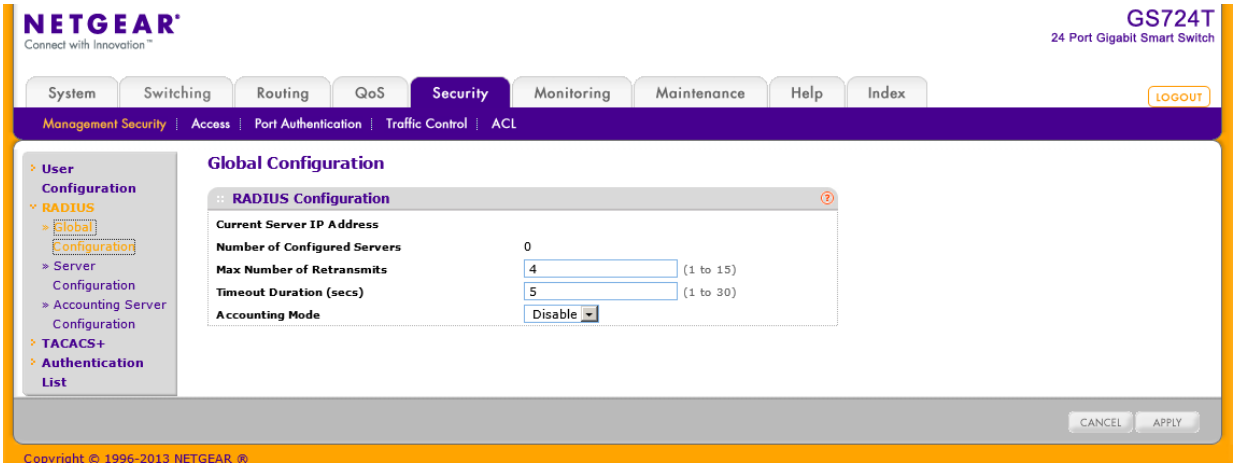
グローバル設定(Global Configuration)

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。

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。

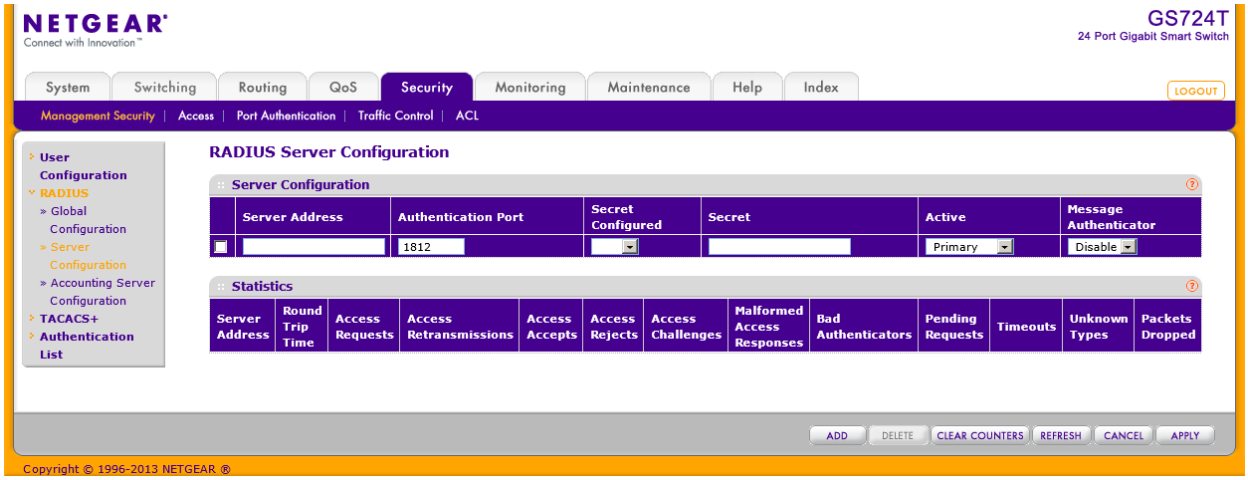
6. Apply ボタンをクリックして設定をスイッチに適用します。

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。

RADIUS サーバー設定をする

1. Security > Management Security, > RADIUS > Server Configuration を選択して RADIUS 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。
   - **Message Authenticator**:Message Authenticator の有効(Enable)、無効(Disable)を選択します。
3. 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。
4. 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。
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。

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。

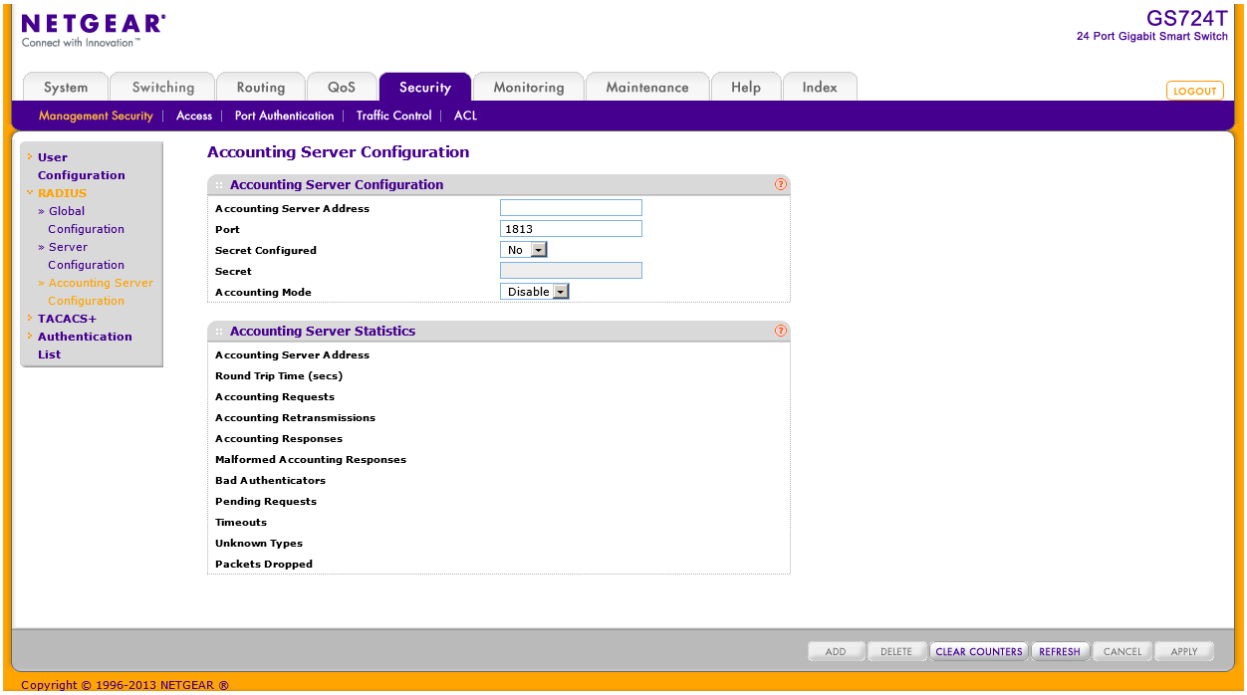
- Clear Counters ボタンをクリックして値を初期化します。
- Refresh ボタンをクリックしてスイッチの最新情報を表示させます。

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。

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) 。
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。

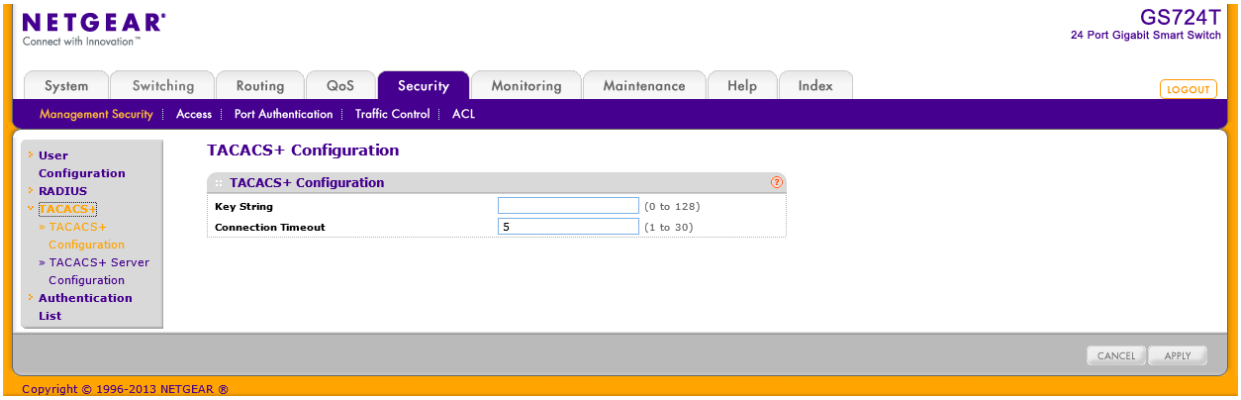
- TACACS+設定（TACACS+ Configuration）
- TACACS+サーバー設定（TACACS+ Server Configuration）

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。

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。



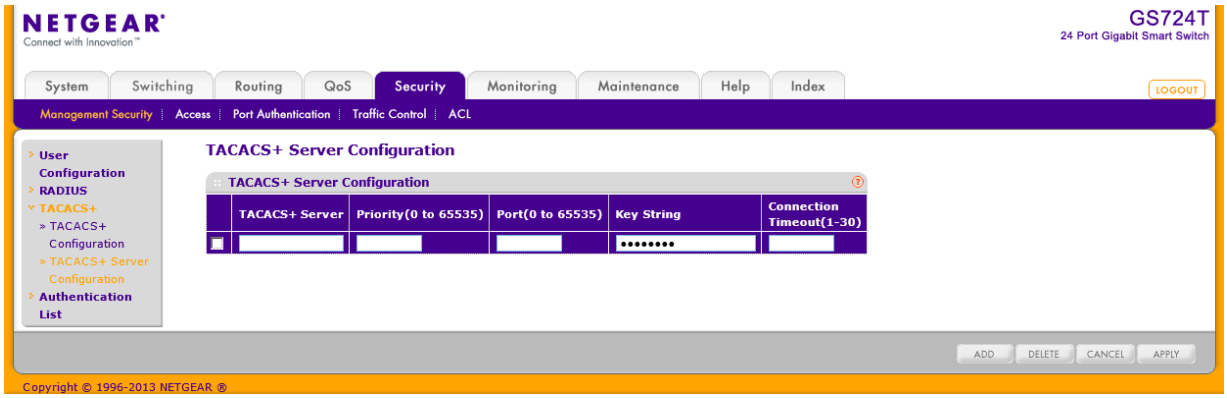
2. Key String：スイッチと TACACS+サーバー間の通信のための暗号化キーを指定します。0-128 文字です。
3. Connection Timeout：スイッチと TACACS+サーバー間の TCP コネクション確立のための最大時間（秒）（1－30 秒）デフォルトは5秒。
4. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。
5. Apply ボタンをクリックして設定をスイッチに適用します。

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。

TACACS+サーバー設定をする

1. Security > Management Security > TACACS+ > Server Configuration を選択して TACACS+ Server Configuration ページを表示します。



2. TACACS+ Server：TACACS+サーバーの IP アドレスを記入します。
3. 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。
4. 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。有効な長さは 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。デフォルトは 5 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）

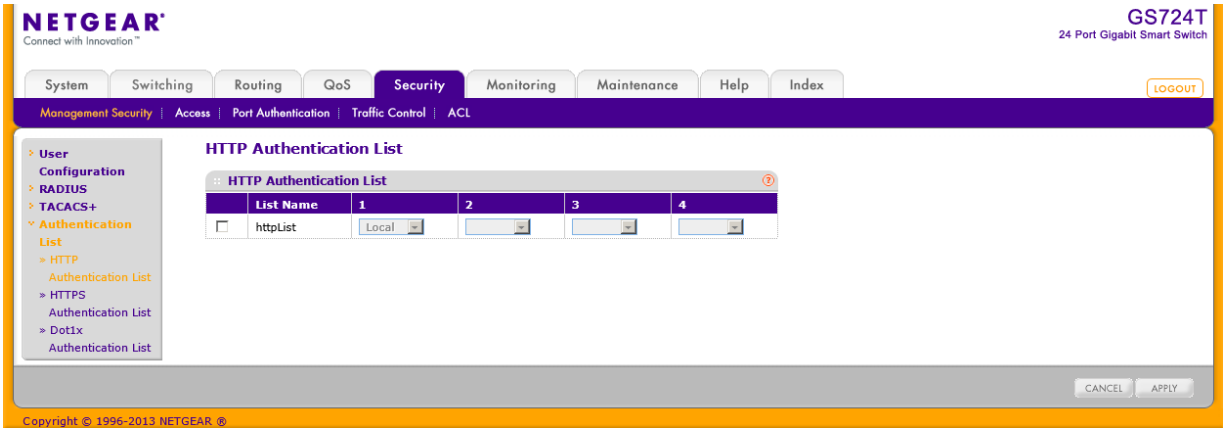
Authentication List ページでデフォルトログインリストを設定します。ログインリストは admin ユーザーのためのスイッチあるいはポートへアクセスするための認証方式について記します。

> 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。

HTTP 認証リスト

HTTP Authentication List を使ってデフォルト HTTP ログインリストを設定します。

1. Security > Management Security > Authentication List > HTTP Authentication List を選択して HTTP Authentication List ページを表示します。

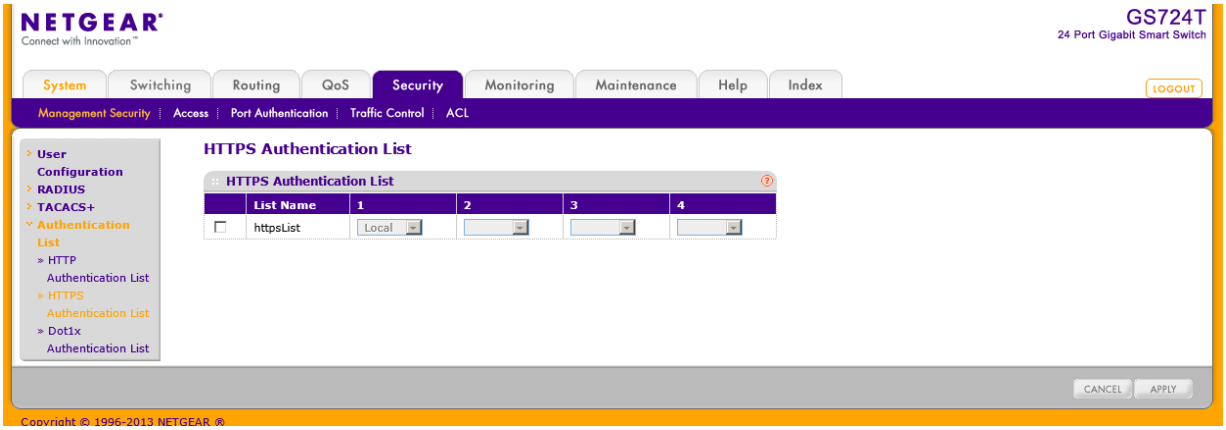


2. httpList のチェックボックスを選択します。
3. 1 の欄のドロップダウンメニューで認証ログインリストの最初に現れる認証方式を選択します。'local' のようなタイムアウトしない方式を選択した場合、複数の方式を指定しても他の方式は使われません。新しいログインリストを作成した場合はこのパラメータは表示されません。選択した順番に認証方式は発生します。方式は以下の通り。
4. Local：ローカルに保存されたユーザーID とパスワードが認証に使われます。ローカル方式はタイムアウトしないため、これを選択した場合は以降の方式は選択されていたとしても使われません。
5. RADIUS：ユーザー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。
6. 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。
7. 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。
8. 2,3,4 の欄についても選択します。
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。
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。

HTTPS 認証リスト

HTTPS Authentication List を使ってデフォルト HTTPS ログインリストを設定します。

1. Security > Management Security > Authentication List > HTTPS Authentication List を選択して HTTPS Authentication List ページを表示します。



2. httpsList のチェックボックスを選択します。
3. 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. 2,3,4 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。

Dot1x 認証リスト（Dot1x Authentication List）

Dot1x Authentication List を使ってデフォルト IEEE802.1X 認証リストを設定します。

1. Security > Management Security > Authentication List > Dot1x Authentication List を選択して Dot1x Authentication List ページを表示します。

2. Dot1xtList のチェックボックスを選択します。
3. 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。
   - None：認証方式なし。
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。

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。

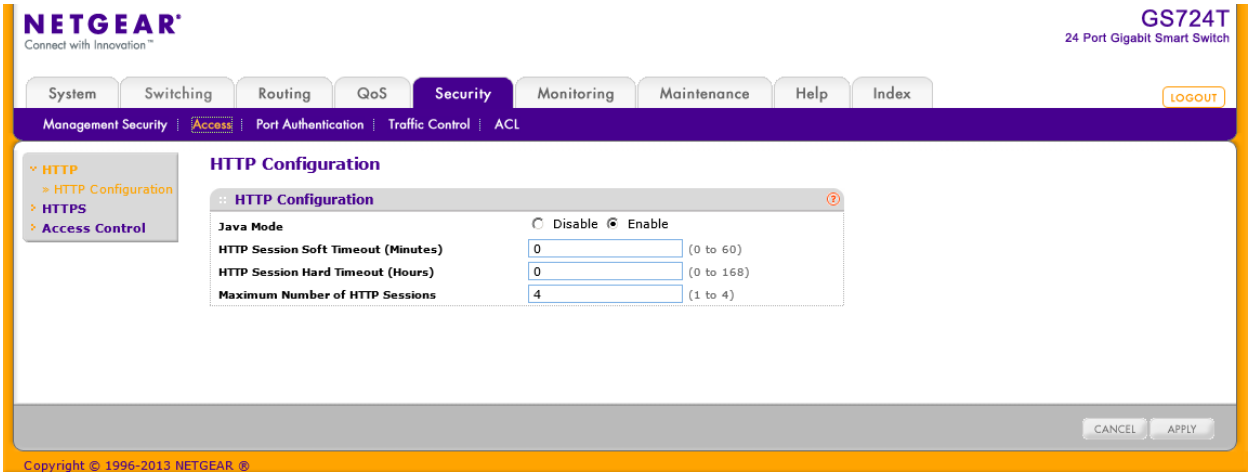
- HTTP 設定(HTTP Configuration)
- HTTPS 設定（Secure HTTP Configuration）
- 証明書管理（Certificate Management）
- 証明書ダウンロード（Certificate Download）
- アクセスコントロール（Access Control）

HTTP 設定(HTTP Configuration)

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

HTTP サーバー設定をする

1. Security > Access > HTTP > HTTP Configuration を選択して HTTP Configuration ページを表示します。



2. **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。
3. **HTTP Session Soft Timeout（Minutes）**：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。0 は無限を示します。表示されている値が現在の値です。

4. **HTTP Session Hard Timeout（Hours）**：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 1－4 です。デフォルトは 4 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。

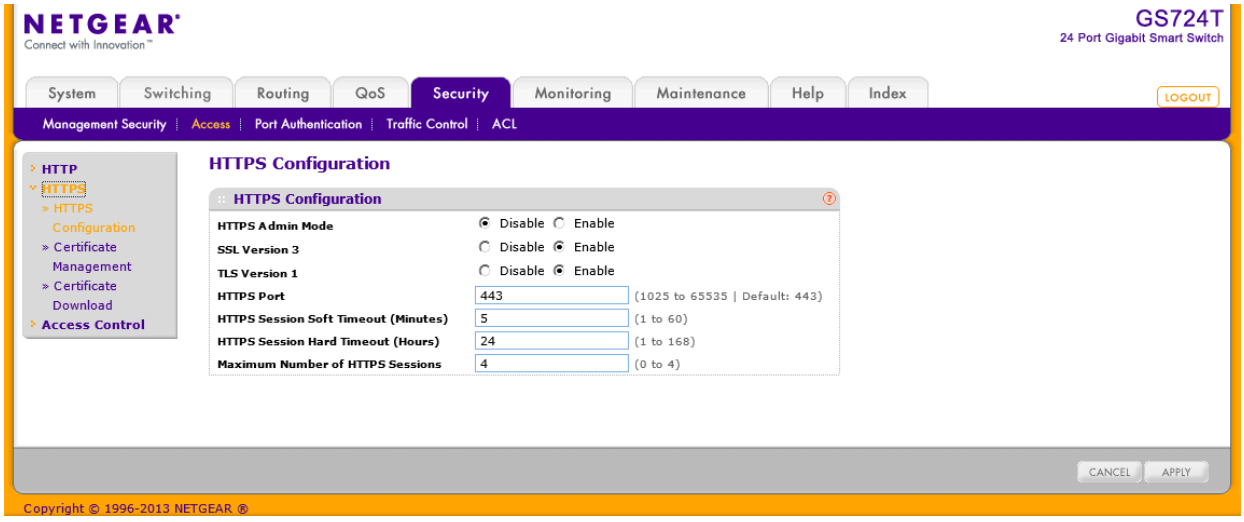
HTTPS 設定（Secure HTTP Configuration）

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。

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。



2. **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"と"TLS Version 1"の設定を変更することはできません。

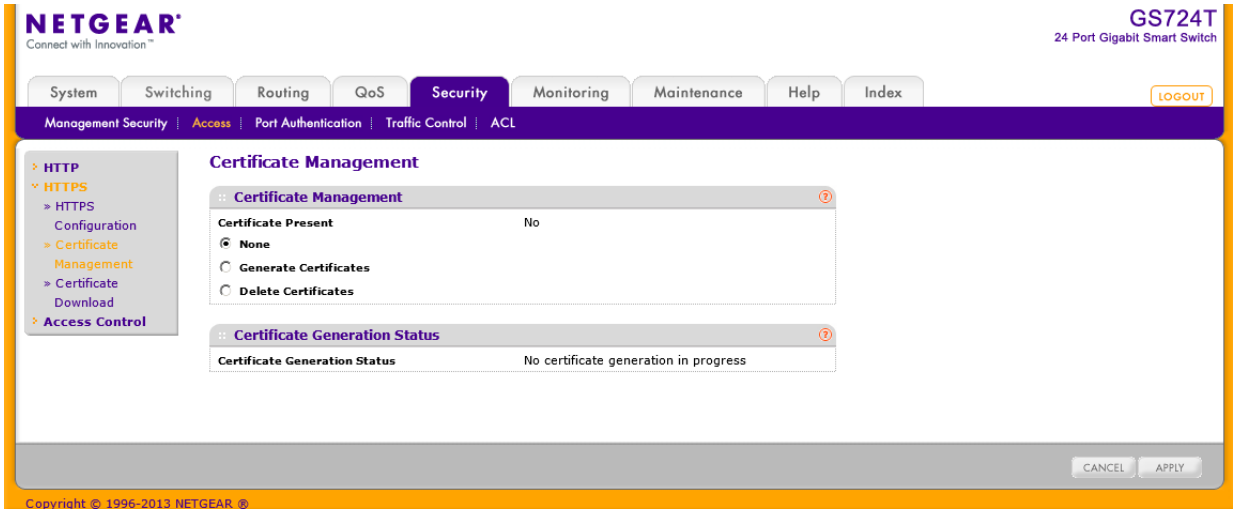
3. **SSL Version 3**：SSL バージョン 3.0 の有効(enable)、無効（disable）を設定します。表示されている設定が現在の設定です。デフォルトは有効(enable)です。
4. **TLS Version 1**：TLS バージョン 1.0 の有効(enable)、無効（disable）を設定します。表示されている設定が現在の設定です。デフォルトは有効(enable)です。
5. **HTTPS Port**：HTTPS で使うポート番号を指定します。範囲は 1025-65535 で、デフォルトは 443 です。表示されている値が現在の値です。
6. **HTTPS Session Soft Timeout(Minutes)**：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(Hours)**：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 0－4 です。デフォルトは 4 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。

証明書管理（Certificate Management）

この画面で証明書の生成、削除を行います。

SSL 証明書を生成する

1. Security > Access > HTTPS > Certificate Management を選択して Certificate Management ページを表示します。



2. Certificate Present：証明書がスイッチに存在しているか（Yes）否か（No）を示します。
3. Generate Certificates を選択して証明書を作成します。
4. Apply ボタンをクリックします。
   スイッチは SSL 証明書の生成を開始します。
   Certificate Generation Status 欄に状況が表示されます。

SSL 証明書を削除する

5. Security > Access > HTTPS > Certificate Management を選択して Certificate Management ページを表示します。
6. Certificate Present：証明書がスイッチに存在しているか（Yes）否か（No）を示します。
7. Delete Certificates を選択して証明書を削除します。
8. Apply ボタンをクリックします。

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。

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。

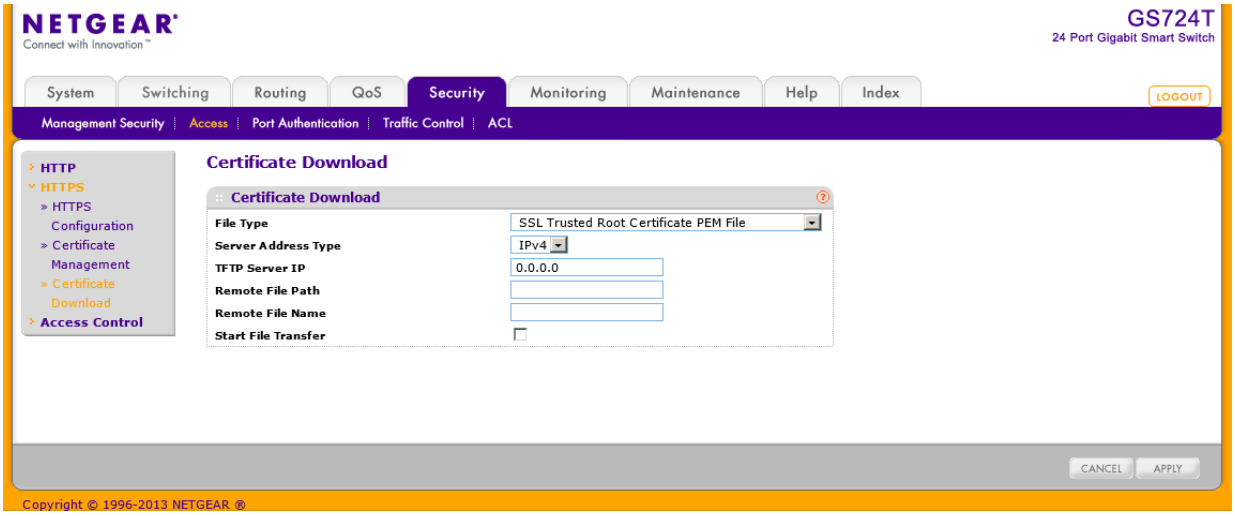
- TFTP サーバーに証明書ファイルが設定されている。

- 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。

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

HTTPS 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。
4. **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。

アクセスコントロール(Access Control)

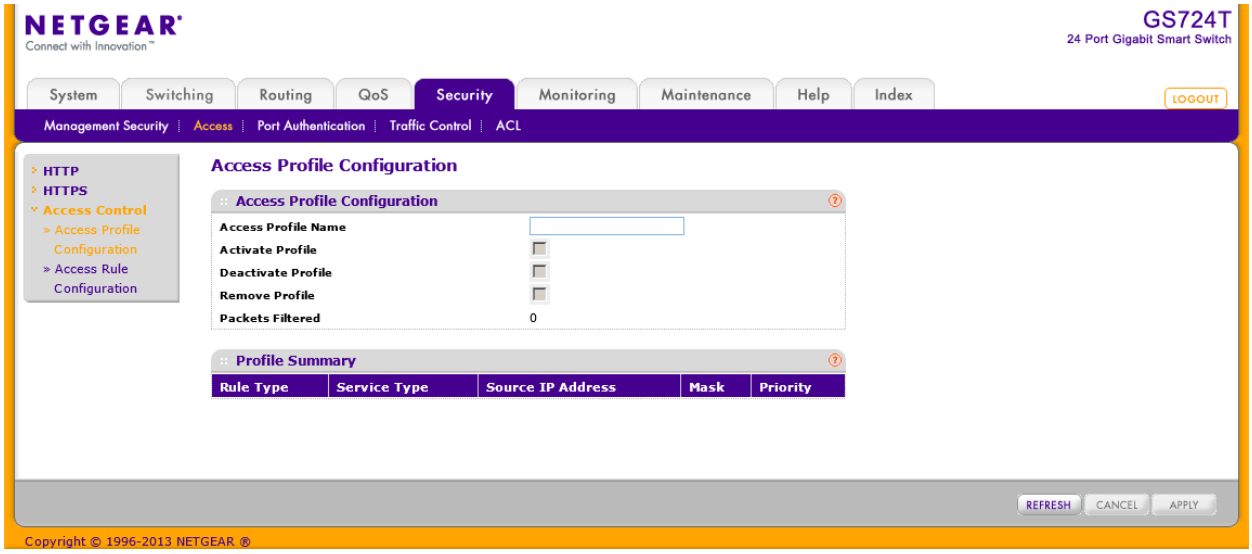
Access Control でプロファイルの設定とアクセスルールの設定ができます。

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。
   - 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。
   - 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。
   - 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。
   - Packes Filtered:フィルターされたパケットの数を表示します。
3. 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。
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。

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。

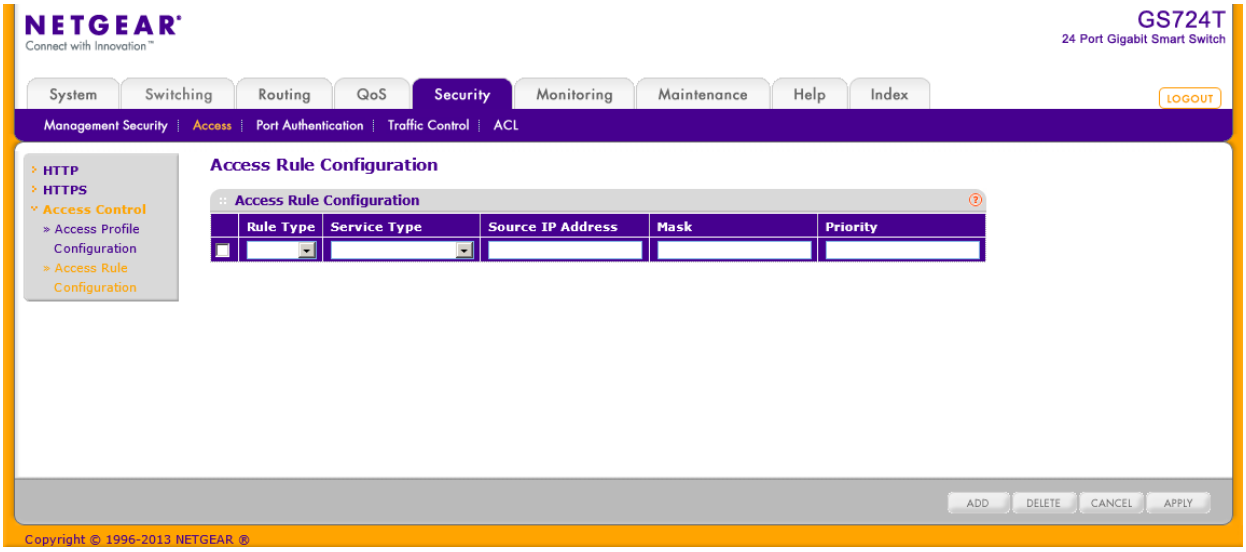
Refresh ボタンをクリックしてスイッチの最新情報を表示させます。

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。

アクセスルールを設定する

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。

3. **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。
4. **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
   - Secure HTTP(SSL)
   - HTTP
5. **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。
6. **Mask**：IP アドレス用のサブネットマスクを設定します。
7. **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。
8. 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。
9. 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。
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。

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。

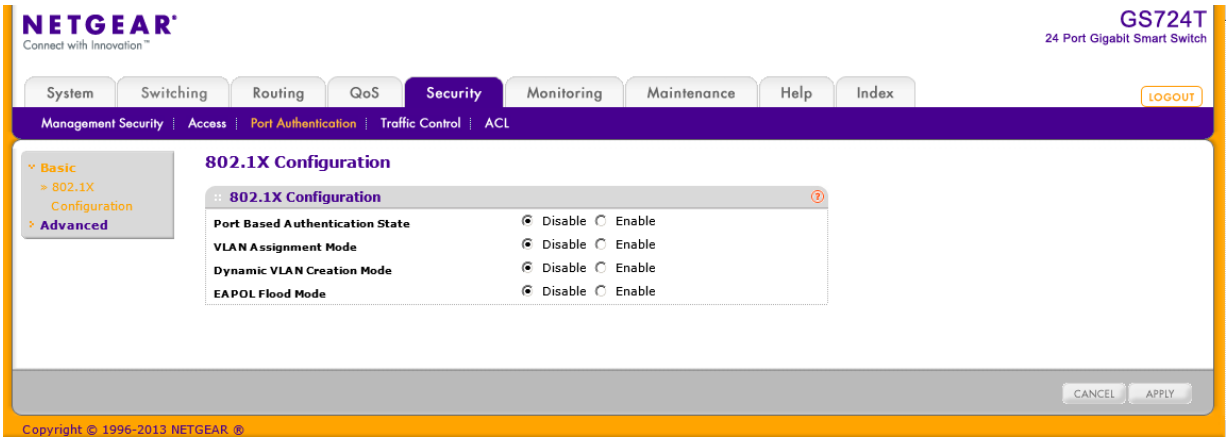
- 802.1X 設定(802.1X Configuration)
- ポート認証(Port Authentication)
- ポートサマリー(Port Summary)
- クライアントサマリー(Client Summary)

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。

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**：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。
   - **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。

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。

---

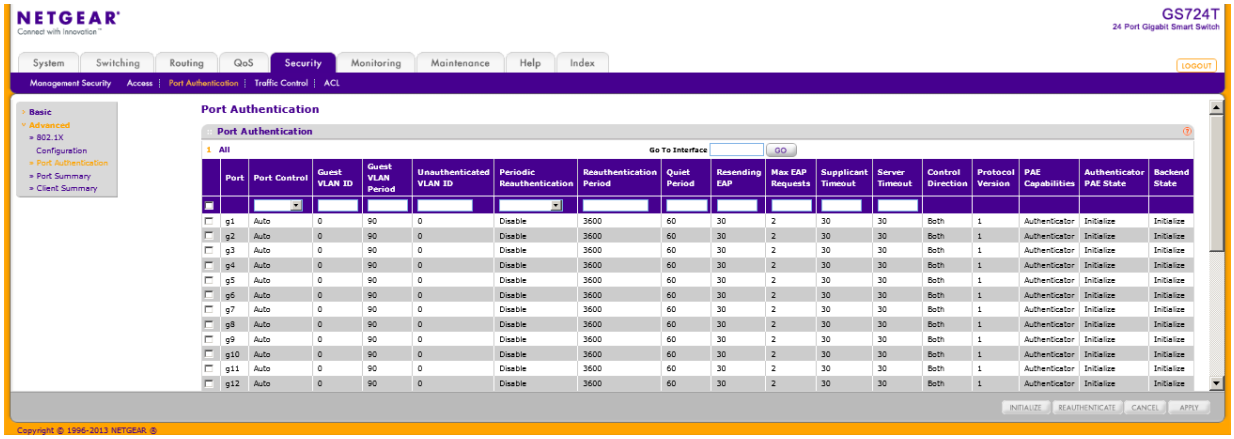
3. **VLAN Assignment Mode**：スイッチの VLAN の割当モードを有効・無効にします。デフォルト設定は無効(disable)です。
4. **Dynamic VLAN Creation Mode**：デフォルト設定は無効(disable)です。
5. **EAPOL Flood Mode**：デフォルト設定は無効(disable)です。
6. **Cancel** ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。
7. **Apply** ボタンをクリックして設定をスイッチに適用します。

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。

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。



2. 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。
  - **MAC Based**：クライアントの認証に応じて動作します。
- **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。
- **Unauthenticated VLAN ID**：インターフェースに非認証 VLAN ID を設定します。有効な値は 0-3965 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。
- **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

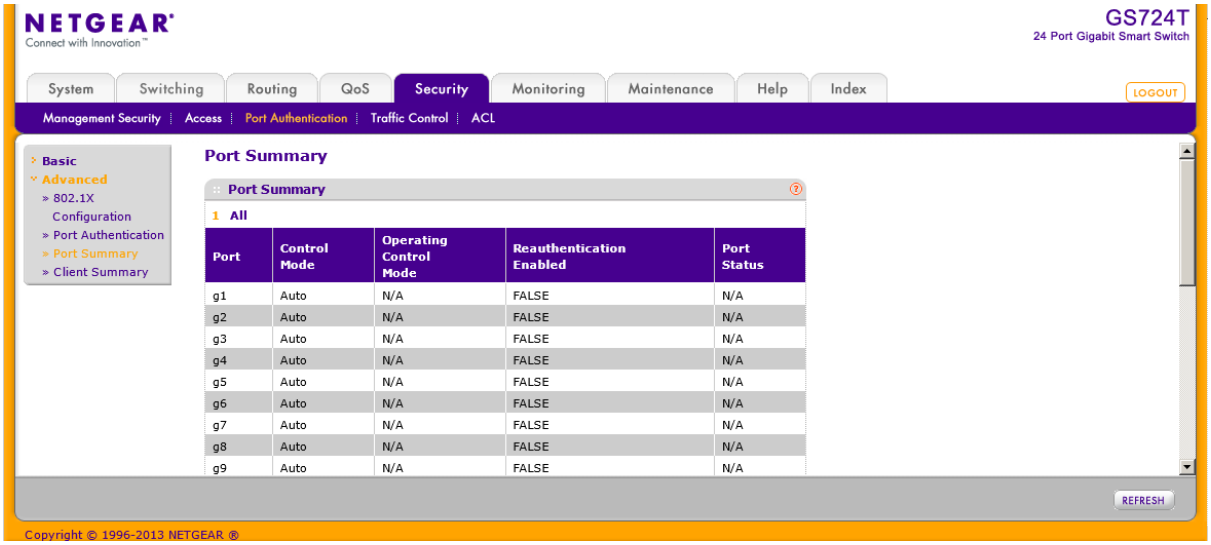
4. Apply ボタンをクリックして設定をスイッチに適用します。
5. Initialize ボタンをクリックしてポートの認証を初期化します。このボタンは Port Control モードが Auto の時のみクリック可能です。ボタンをクリックするとすぐに初期化を開始します。
6. Reauthenticate ボタンをクリックしてポートの再認証を行います。このボタンは Port Control モードが Auto の時のみクリック可能です。ボタンをクリックするとすぐに再承認を開始します。
7. Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。

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。



以下に Port Summary ページに表示される情報の説明を示します。

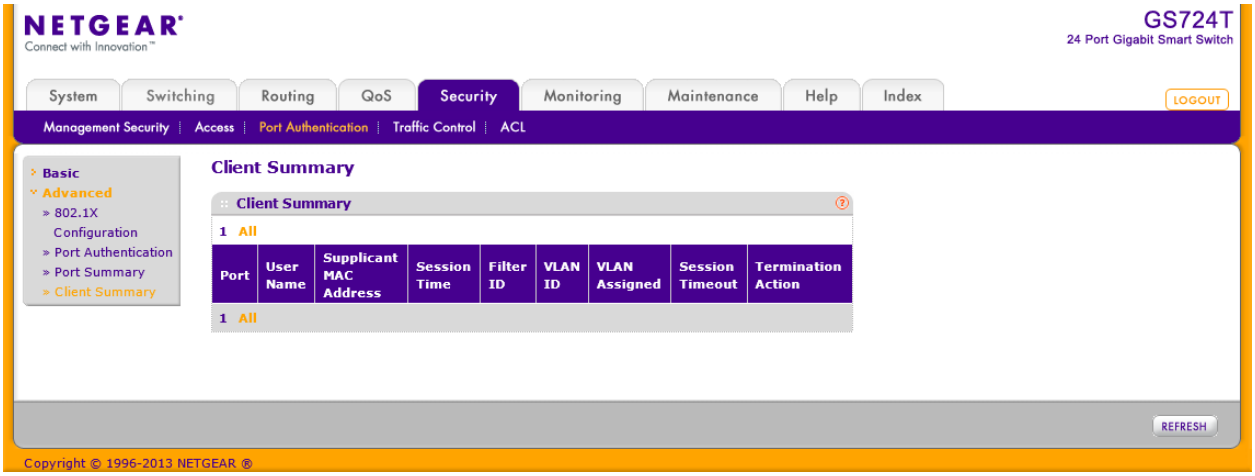
項目	説明
Port	ポート番号
Control Mode	ポートの認証制御状態を表示します。 • Auto: 自動的にインターフェースの認証モードを検知します。 • Force Authorized: インターフェースを認証なしに承認します。 • Force Unauthorized: インターフェースを非承認状態にしてシステムアクセスを拒否します。スイッチはインターフェースを介して認証サービスを提供することができません。
Operating Control Mode	ポートの実際の動作状態。 • ForceUnauthorized • ForceAuthorized • Auto • N/A: 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。

クライアントサマリー（Client Summary）

この画面でローカルオーセンティケータポートに接続されているサプリカントデバイスの情報を表示します。有効な 802.1X セッションが存在しない場合は、テーブルは空白です。

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



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

表 63. IEEE 802.1X client summary information

項目	説明
Port	ポート番号。
User Name	ユーザー名。
Supplicant MAC Address	サプリカントの MAC アドレス。
Session Time	セッション時間。
Filter ID	ポリシーフィルターID.
VLAN ID	サプリカントに割り当てられた VLAN ID。
VLAN Assigned	サプリカントが VLAN に割り当てられた理由。
Session Timeout	RADIUS サーバーが設定したセッションタイムアウト。

Termination Action	RADIUS サーバーが設定したセッションタイムアウト時の動作。

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。

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

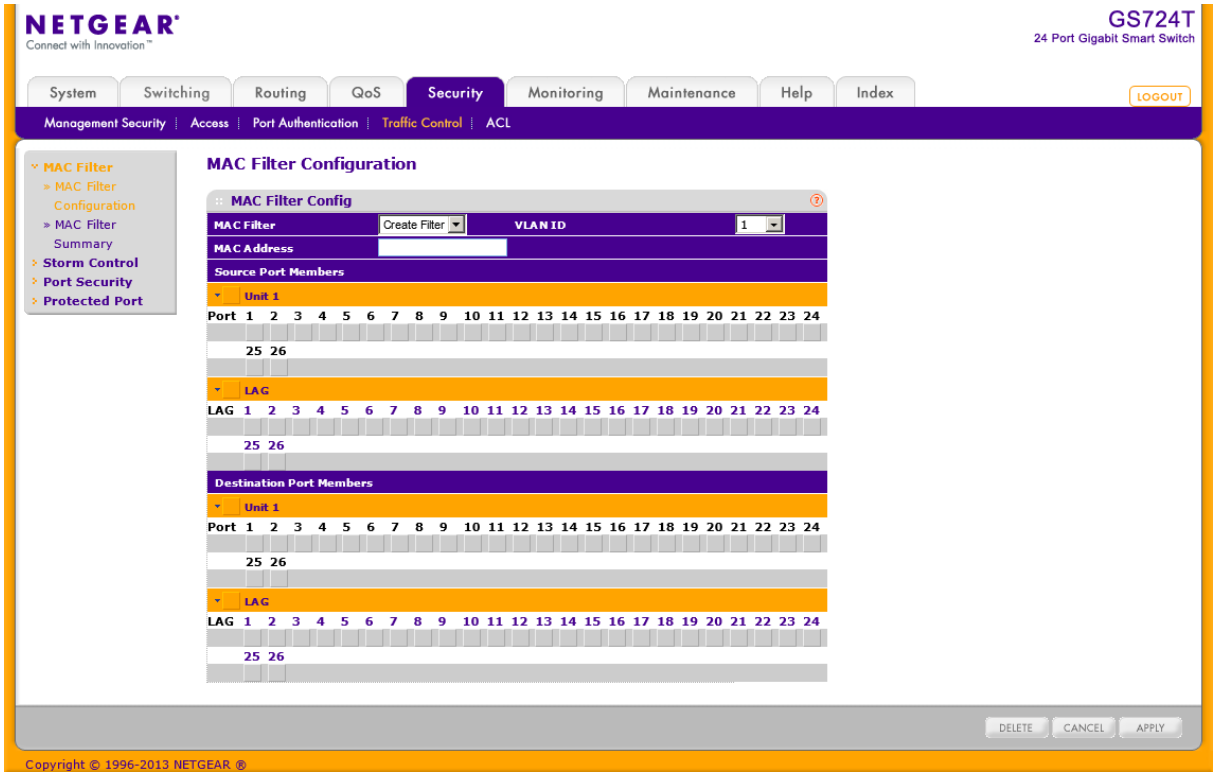
- MAC フィルター(MAC Filter)
  - MAC フィルター設定(MAC Filter Configuration)
  - MAC フィルターサマリー(MAC Filter Summary)
- ストームコントロール(Storm Control)
- ポートセキュリティ(Port Security)
  - ポートセキュリティ設定(Port Security Configuration)
  - ポートセキュリティインターフェース設定(Port Security Interface Configuration)
  - セキュリティ MAC アドレス(Security MAC Address)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

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。



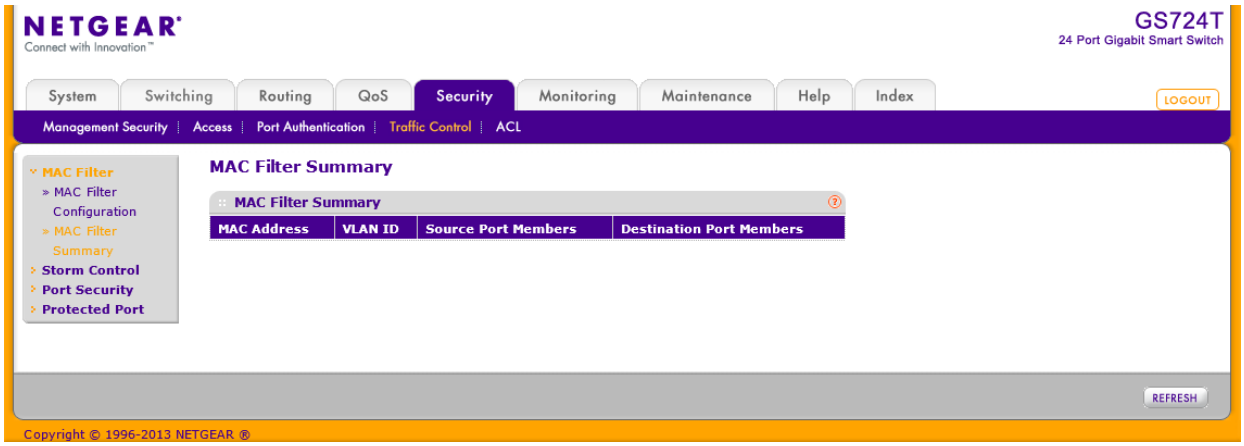
2. MAC フィルターを設定するには、:
3. **MAC Filter**: **Create Filter** を選択します。
4. **VLAN ID**:MAC フィルターを行う VLAN ID を選択します。VLAN ID はフィルターを作成するときのみ変更・設定可能です。
5. **MAC Address**:フィルターする MAC アドレスを(00:01:1A:B2:53:4D)形式で指定します。フィルターを作成するときのみ変更・設定可能です。
   以下の MAC アドレスを設定することはできません。
   - 00:00:00:00:00:00
   - 01:80:C2:00:00:00 ～ 01:80:C2:00:00:0F
   - 01:80:C2:00:00:20 ～ 01:80:C2:00:00:21
   - FF:FF:FF:FF:FF:FF
6. 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。
7. 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 のパケットのみが送信されます。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。

8. 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。
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。

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。



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	フィルターした MAC アドレスが含まれる VLAN ID。
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）

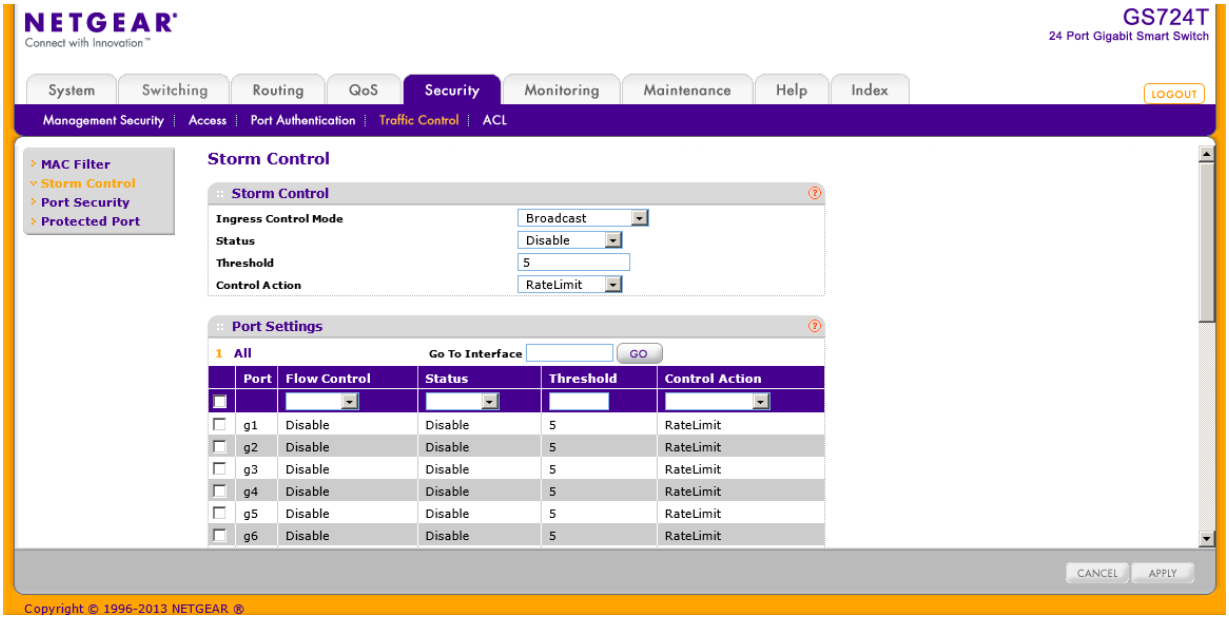
ブロードキャストストームは過度なブロードキャストメッセージが同時にネットワークに送信されることから発生します。転送されたメッセージへの応答がネットワークを飽和状態にし、ネットワークタイムアウトを引き起こしたりします。

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。

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。



2. 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。
   - Disabled：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. Status：ポートで Ingress Control Mode を有効にします。
5. 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。
6. Flow Control：IEEE802.3xフローコントロールを有効にします。

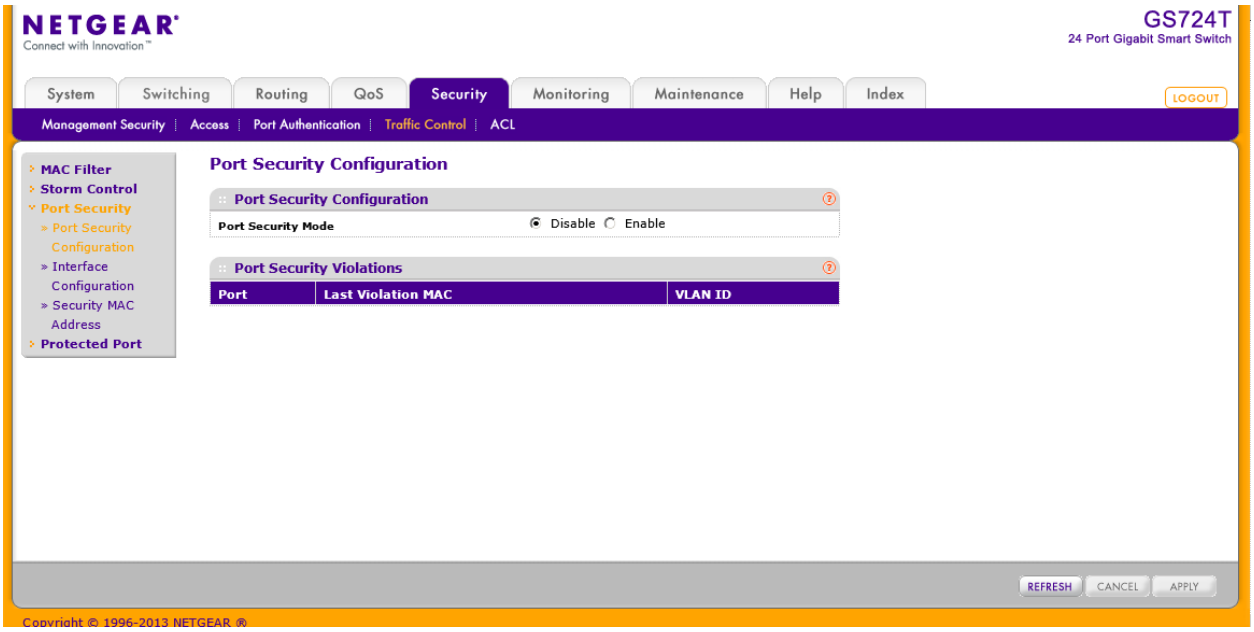
7. **Control Action**：トラフィックが Threshold に達した時のポートの動作を指定します。
   - **ShutDown**：ポートをシャットダウンします。
   - **RateLimit**：速度を制限します。（デフォルト）
8. **Cancel** ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。
9. **Apply** ボタンをクリックして設定をスイッチに適用します。

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。

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）

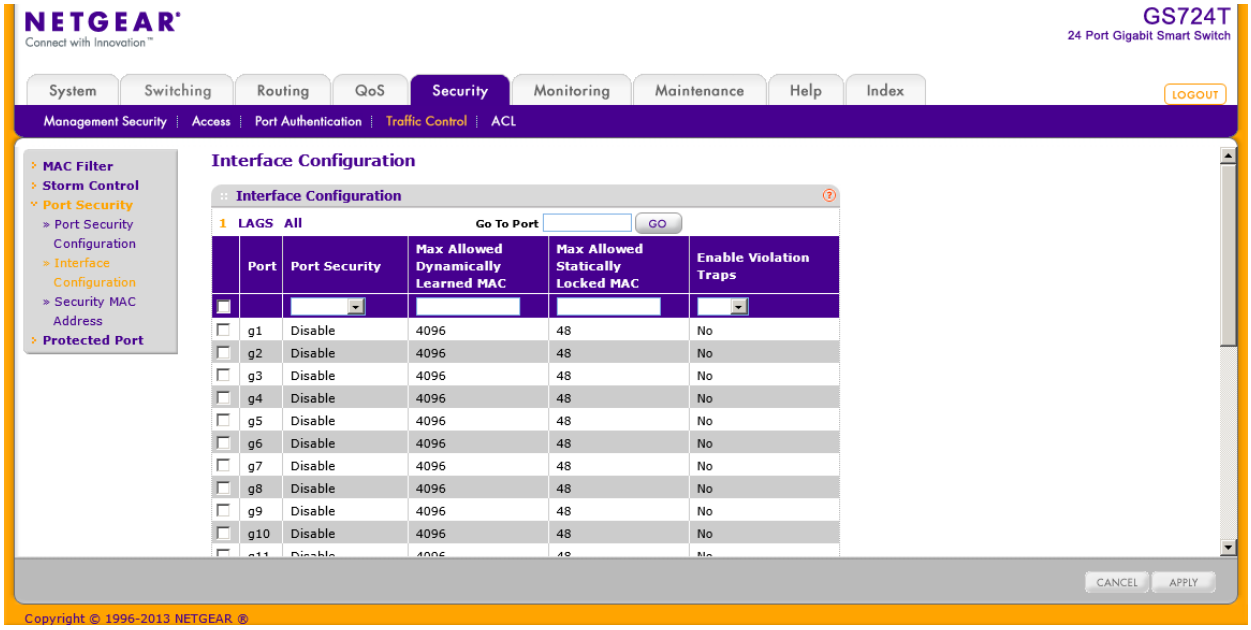
MAC アドレスが受け入れ可能かどうかはダイナミックかスタティックのどちらか一方で決定することができます。ポートがロックされているときに両方の方法が使われます。

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。

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. 1 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。
   - **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。
   - **Enable Violation Traps**:許可されない MAC アドレスを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。

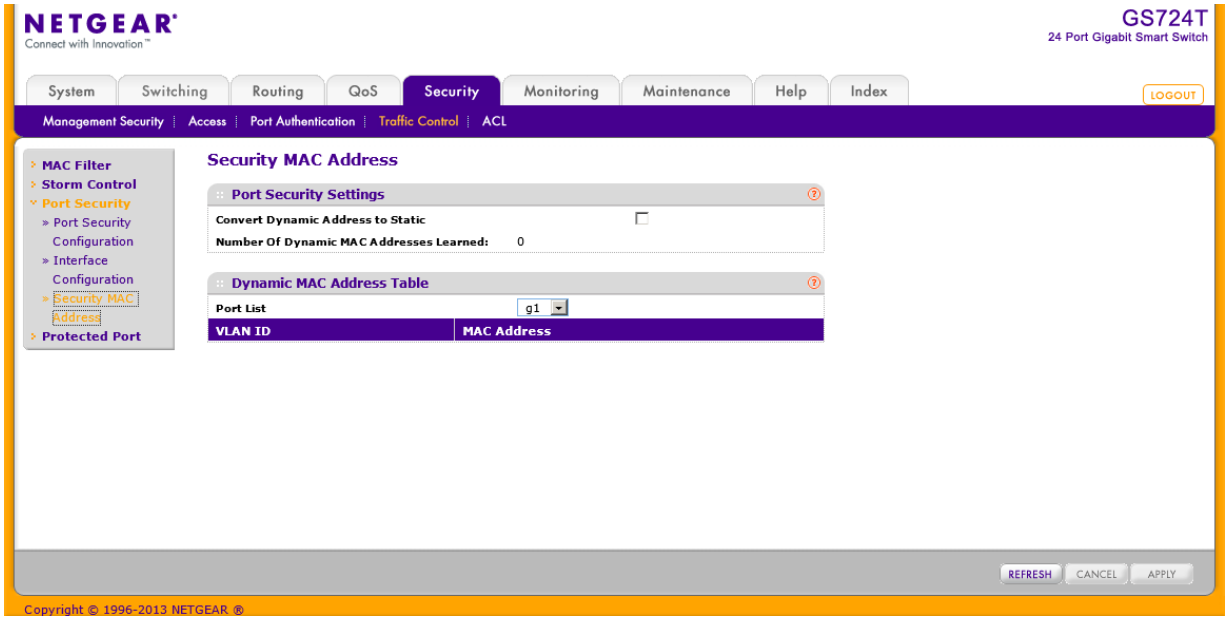
8. Apply ボタンをクリックして設定をスイッチに適用します。

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。

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。

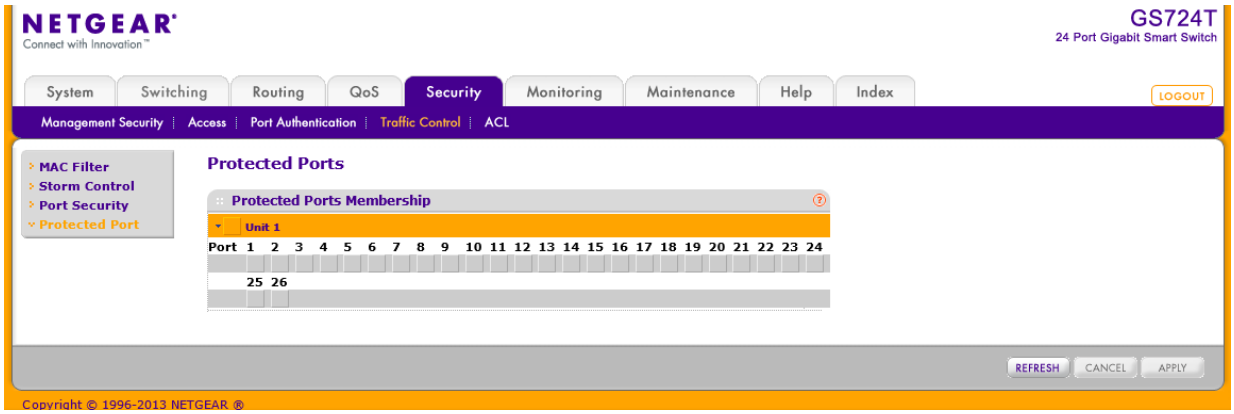
Refresh ボタンをクリックしてスイッチの最新情報を表示させます。

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を転送しませんが、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。

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。
3. 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 設定（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。

ACL 設定メニューフォルダーは以下の機能へのリンクを含みます。

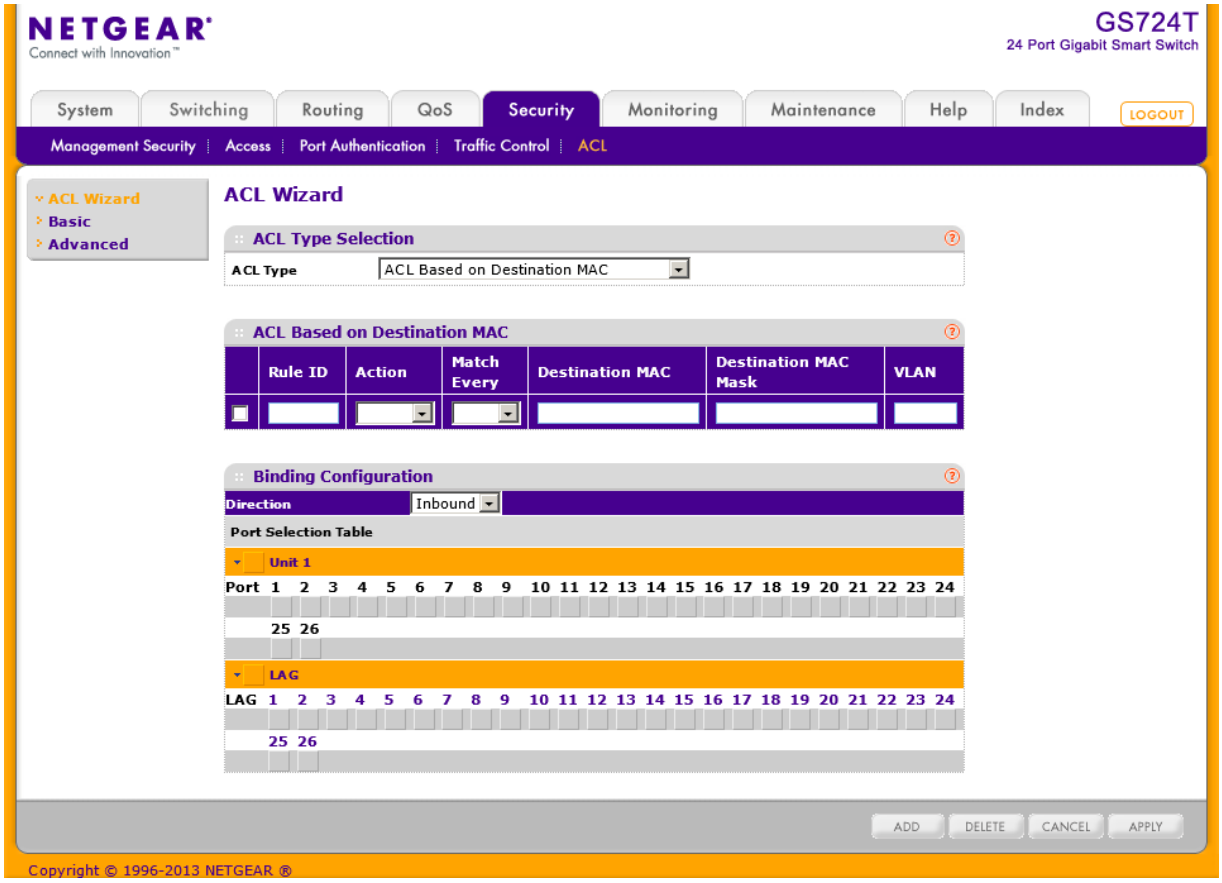
- ACL ウィザード（ACL Wizard）
- Basic
  - MAC ACL
  - MAC ルール（MAC Rules）
  - MAC バインディング設定（MAC Binding Configuration）
  - MAC バインディングテーブル（MAC Binding Table）
- Advanced:
  - IP ACL
  - IP ルール（IP Rules）
  - IP 拡張ルール（IP Extended Rules）
  - IPv6 ACL
  - IPv6 ルール(IPv6 Rules)
  - IP バインディング設定（IP Binding Configuration）
  - 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）をつかうことによって簡単な ACL を作成し、ポートに簡単にすぐに適用することができます。ACL ウィザードで ACL を作成することはできますが修正することはできません。修正に関してはルールの変更に関する記述を参照してください。

ACL ウィザードを使う

1. **Security** > **ACL** > **ACL Wizard** を選択して **ACL Wizard** ページを表示します。



2. **ACL Type**：以下の 10 のタイプの ACL を選択します。
   - **ACL Based on Destination MAC**：宛先 MAC アドレスを元にトラフィックを許可・拒否します。
   - **ACL Based on Source MAC**：送信元 MAC アドレスを元にトラフィックを許可・拒否します。
   - **ACL Based on Destination IPv4**：宛先 IPv4 アドレスを元にトラフィックを許可・拒否します。
   - **ACL Based on Source IPv4**：送信元 IPv4 アドレスを元にトラフィックを許可・拒否します。
   - **ACL Based on Destination IPv6**：宛先 IPv6 アドレスを元にトラフィックを許可・拒否します。
   - **ACL Based on Source IPv6**：送信元 IPv6 アドレスを元にトラフィックを許可・拒否します。
   - **ACL Based on Destination IPv4 L4 Port**：宛先 IPv4 レイヤー4 ポートを元にトラフィックを許可・拒否します。
   - **ACL Based on Source IPv4 L4 Port**：送信元 IPv4 レイヤー4 ポートを元にトラフィックを許可・拒否します。
   - **ACL Based on Destination IPv6 L4 Port**：宛先 IPv6 レイヤー4 ポートを元にトラフィックを許可・拒否します。
   - **ACL Based on Source IPv6 L4 Port**：送信元 IPv6 レイヤー4 ポートを元にトラフィックを許可・拒否します。
3. **Rule ID**：ルールを識別するために 1-50 の整数を記入します。
4. **Action**：ルールに一致した場合に実行される動作を選択します。

- **Permit**：パケットは宛先に転送されます。
- **Deny**：パケットは廃棄されます。

5. **Match Every**：**True** を選択すると、この ACL だけが有効になります。
6. **ACL Type** の設定に従い、以降の入力画面が変更されます。
   例えば、**ACL 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。
7. **Apply** ボタンをクリックしてルールを保存します。

以下に **ACL Type** ごとの設定項目を示します。

ACL Type（ACL Based On）	項目
Destination MAC	• Destination MAC：宛先 MAC アドレス。形式は xx:xx:xx:xx:xx:xx • Destination MAC Mask：MAC アドレスマスク。 • VLAN：VLAN ID。
Source MAC	• Source MAC：送信元 MAC アドレス。形式は xx:xx:xx:xx:xx:xx • Source MAC Mask：MAC アドレスマスク。 • VLAN：VLAN ID。
Destination IPv4	• Destination IP Address：宛先 IP アドレス。 • Destination IP Mask：宛先 IP アドレスマスク。
Source IPv4	• Source IP Address：送信元 IP アドレス。 • Source IP Mask 送信元 IP アドレスマスク。
Destination IPv6	• Destination Prefix：宛先プレフィクス。 • Destination Prefix Length 宛先プレフィクス長。
Source IPv6	• Source Prefix：送信元プレフィクス。 • Source Prefix Length. 送信元プレフィクス長。
Destination IPv4 L4 Port	• Destination L4 port (protocol)：宛先 IPv4 ポート（プロトコル） • Destination L4 port (value) ：宛先 IPv4 ポート（値）
Source IPv4 L4 Port	• Source L4 port (protocol)：送信元 IPv4 ポート（プロトコル） • Source L4 port (value)：送信元 IPv4 ポート（値）
Destination IPv6 L4 Port	• Destination L4 port (protocol)：宛先 IPv6 ポート（プロトコル） • Destination L4 port (value) ：宛先 IPv6 ポート（値）
Source IPv6 L4 Port	• Source L4 port (protocol)：送信元 IPv6 ポート（プロトコル） • Source L4 port (value) ：送信元 IPv6 ポート（値）

MAC ACL

MAC ACL はパケットに対して連続的に一致させる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。

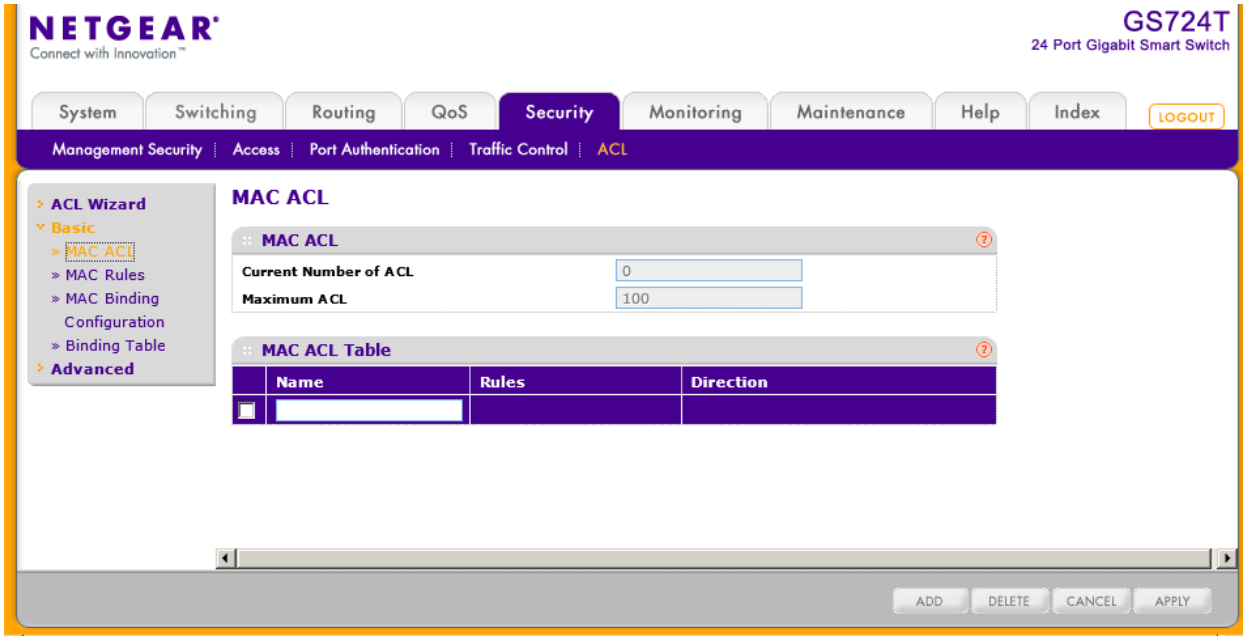
MAC ACL を定義してスイッチに適用するには複数の手順があります。

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。

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。



2. 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。

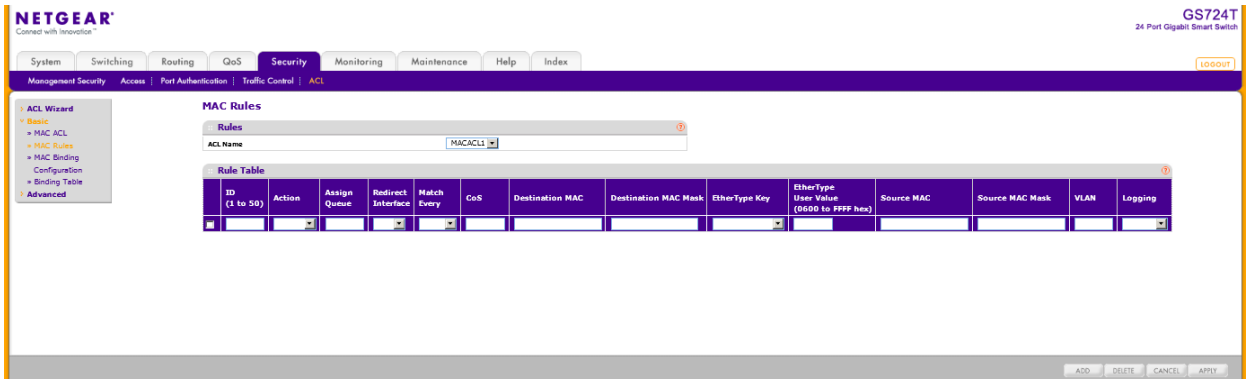
3. MAC ACL を削除するには、削除する MAC ACL のチェックボックスを選択し、**Delete** ボタンをクリックします。
4. MAC ACL の名前を変更するには、変更する MAC ACL のチェックボックスを選択し、名前を変更し、**Apply** ボタンをクリックします。
5. **Cancel** ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。

MAC ルール(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。

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。
   - **ID**:ルールを識別する値(1-50)を指定します。
   - **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。0-7 を設定します。
   - **Redirect Interface**:マッチしたトラフィックをリダイレクトするインターフェースを指定します。

- **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: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:ff:ff:ff:ff である場合、aa:bb:xx: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: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:ff:ff:ff:ff である場合、aa:bb:xx: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。
- **Logging**：有効（Enable）にするとログが有効になります。Access List Trap Flag が有効になっていれば、周期的なトラップとして何回一致したかどうかという情報が送信されます。5 分に一度送信されますが、回数が変化しない場合は送信されません。

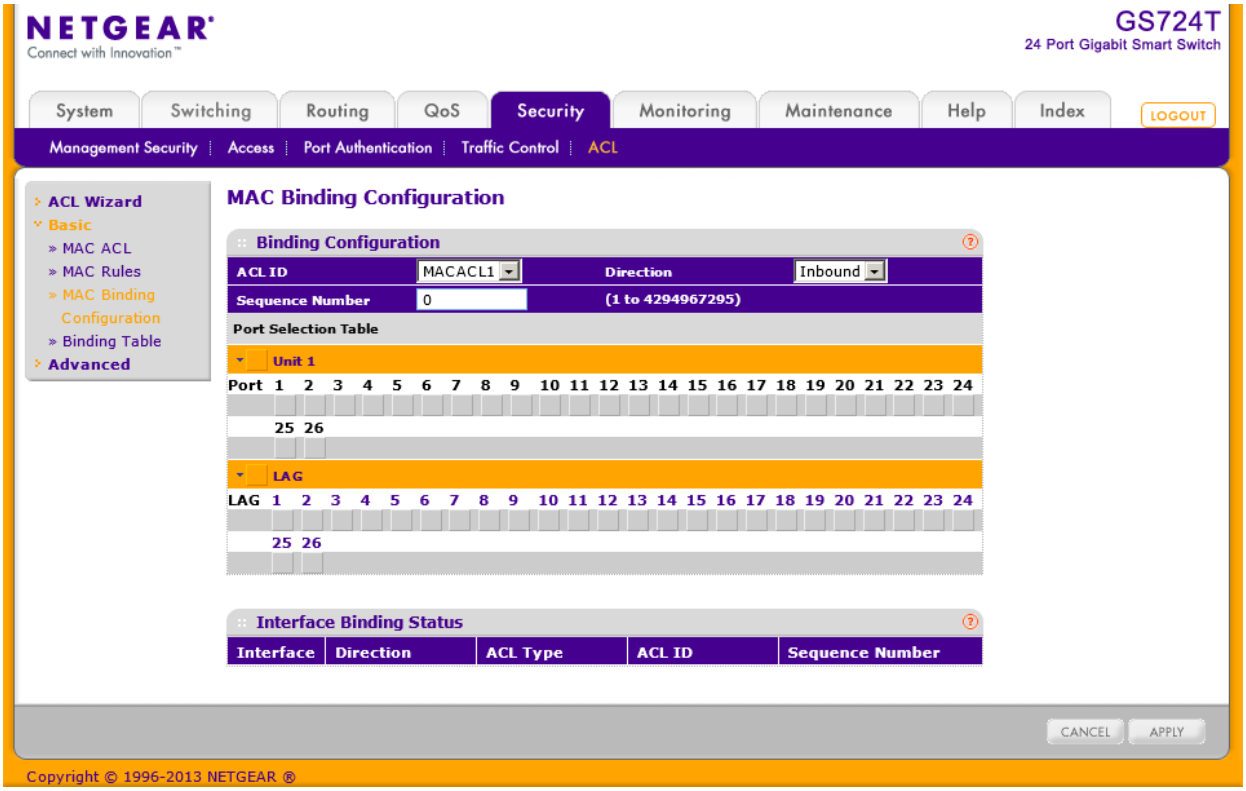
4. **Cancel** ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。
5. ルールを削除するには、削除するルールのチェックボックスを選択し、**Delete** ボタンをクリックします。
6. ルールを変更するには、変更するルールのチェックボックスを選択し、項目を変更後、**Apply** ボタンをクリックします。

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

ACL がインターフェースにバインディングされるとき、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。

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。



2. **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（**Direction**）はインバウンド（Inbound）、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 Sequence Number 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。
5. 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

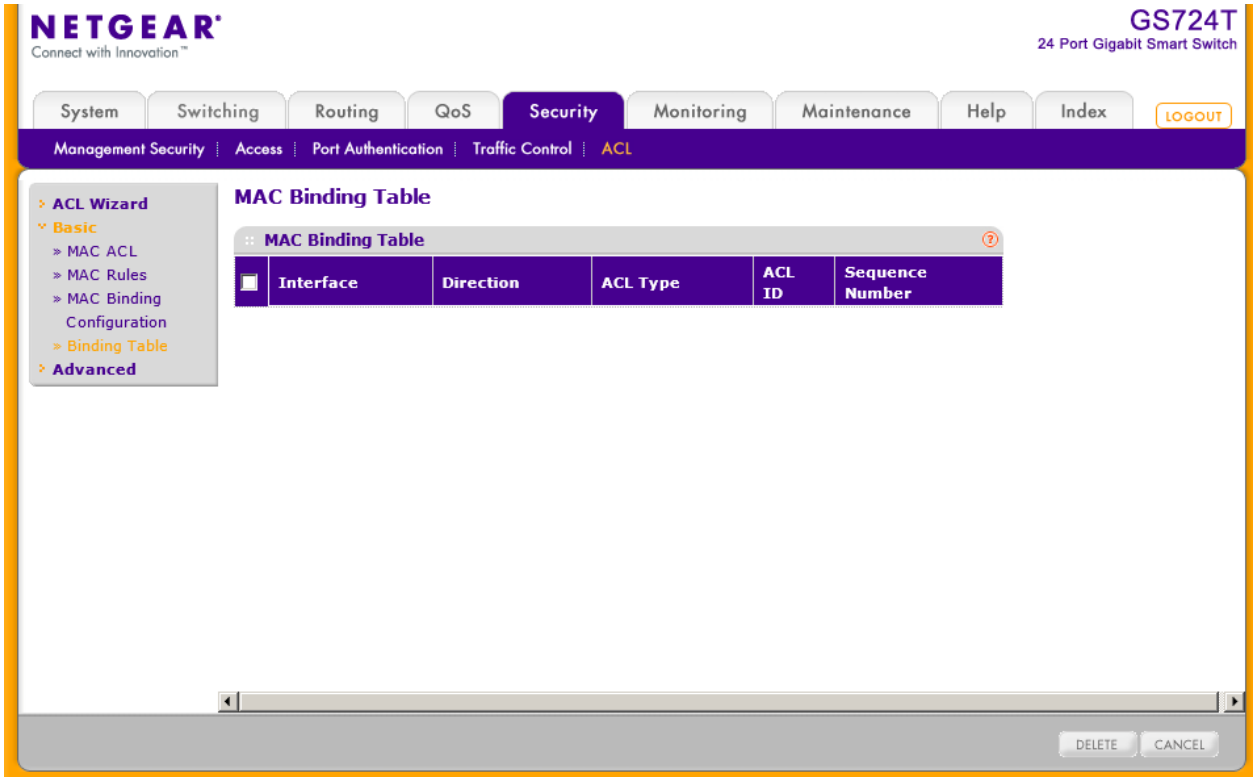
て X を表示させます。

6. 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。
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。

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。



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ーの方向。Inbound（ポートに入力される方向）のみ有効。
ACL Type	インターフェースと方向に割り当てられた ACL のタイプ。

ACL ID	インターフェース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スと方向に割り当てられた番号。

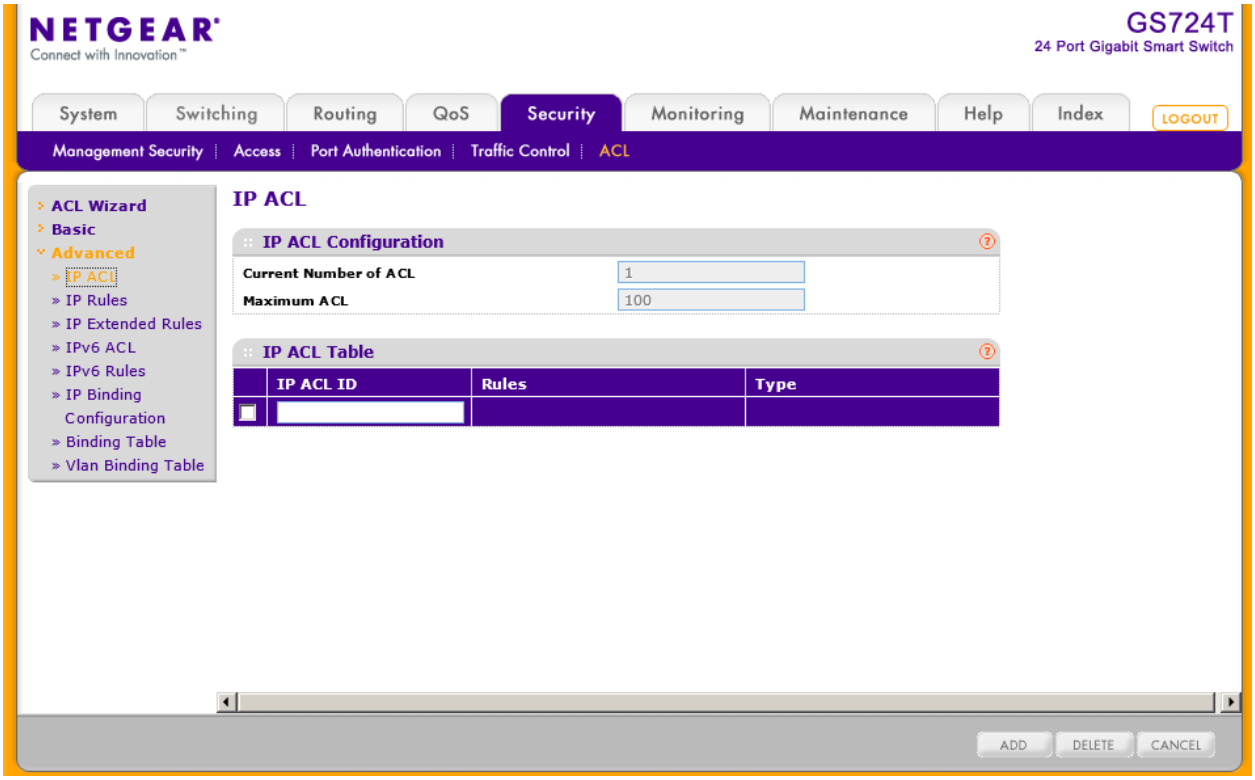
MAC ACL とインターフェースとのバインディングを削除するには、削除するインターフェースのチェックボックスを選択して **Delete** ボタンをクリックします。

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。



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。
4. 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。
5. 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。
6. 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。
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。

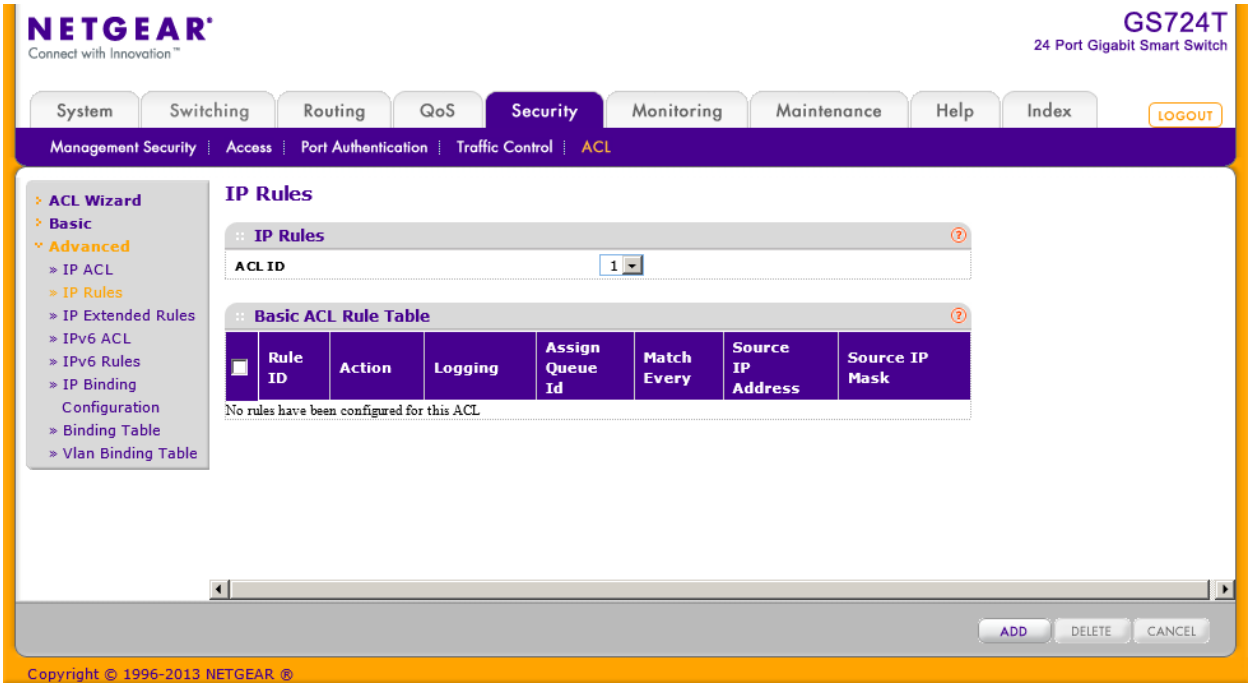
IP ルール（IP Rules）

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。

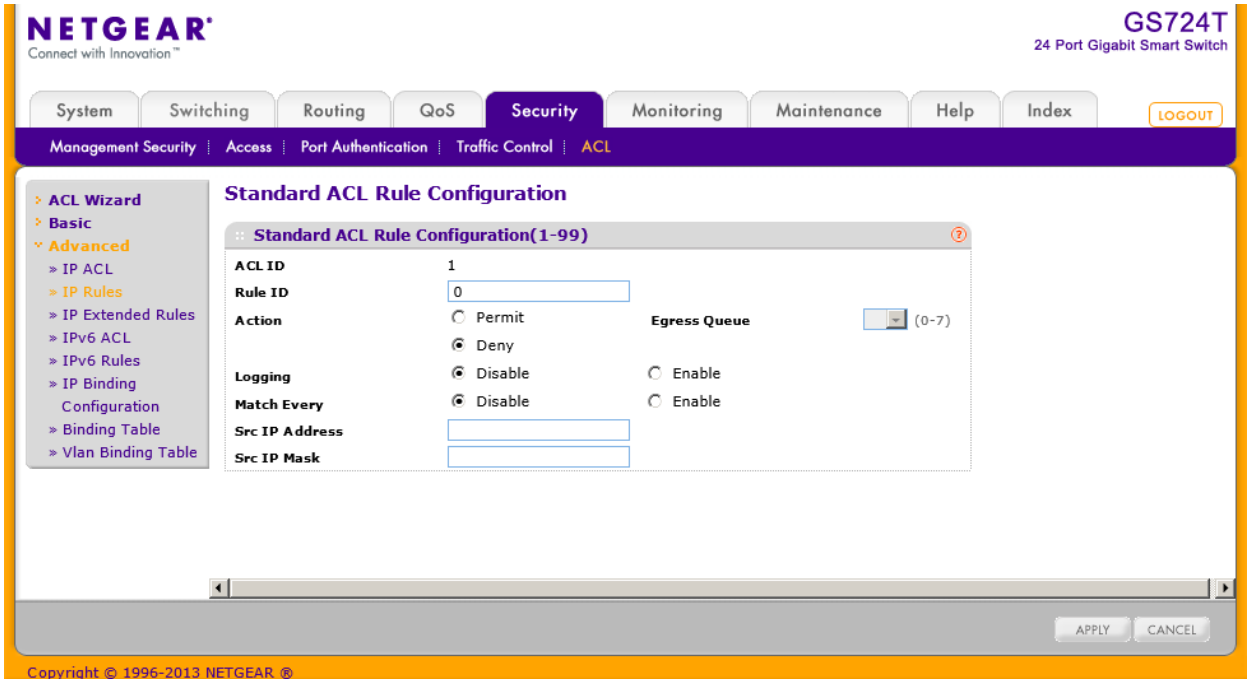
メモ：ACL リストの最後には暗黙の “deny all”ルールが存在します。ACL がパケットに適用され、明示的に設定されたルールのどれにも一致しなかった場合は暗黙の“deny all”ルールによりパケットは廃棄されます。

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。
画面が更新され、追加の入力画面が表示されます。



3. 以下の情報を入力します。
   - **Rule ID**：1-50 の番号をつけます。各 ACL に作成できるルールは 50 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。
   - **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。0-7 を設定します。
   - **Logging**：有効（Enable）にするとログが有効になります。Access List Trap Flag が有効になっていれば、周期的なトラップとして何回一致したかどうかという情報が送信されます。5 分に一度送信されますが、回数が変化しない場合は送信されません。
   - **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。
   - **Src 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。
   - **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スクの逆になります。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。
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. 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。
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. 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。

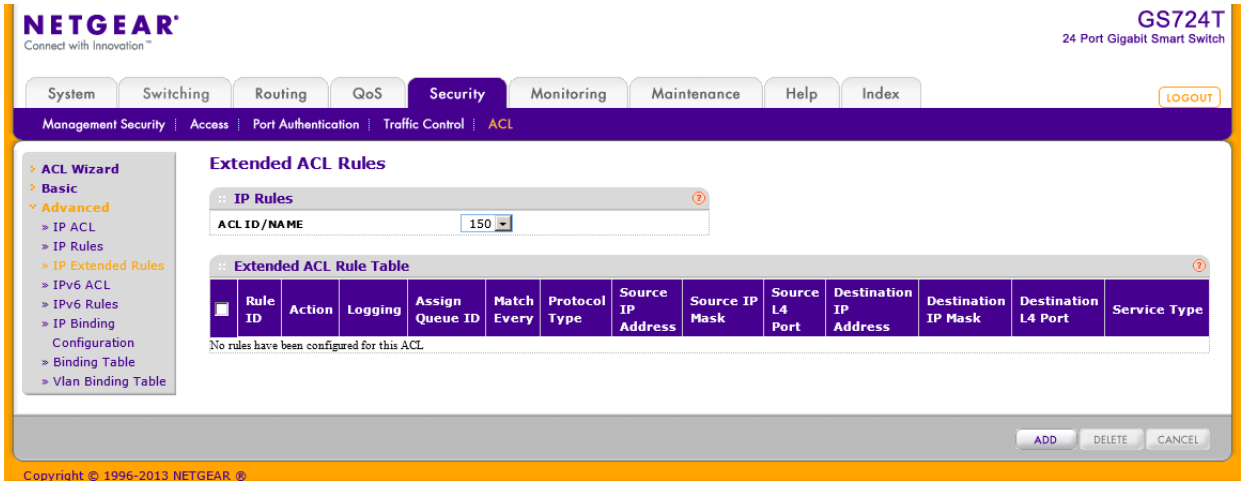
IP 拡張ルール（IP Extended Rules）

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。

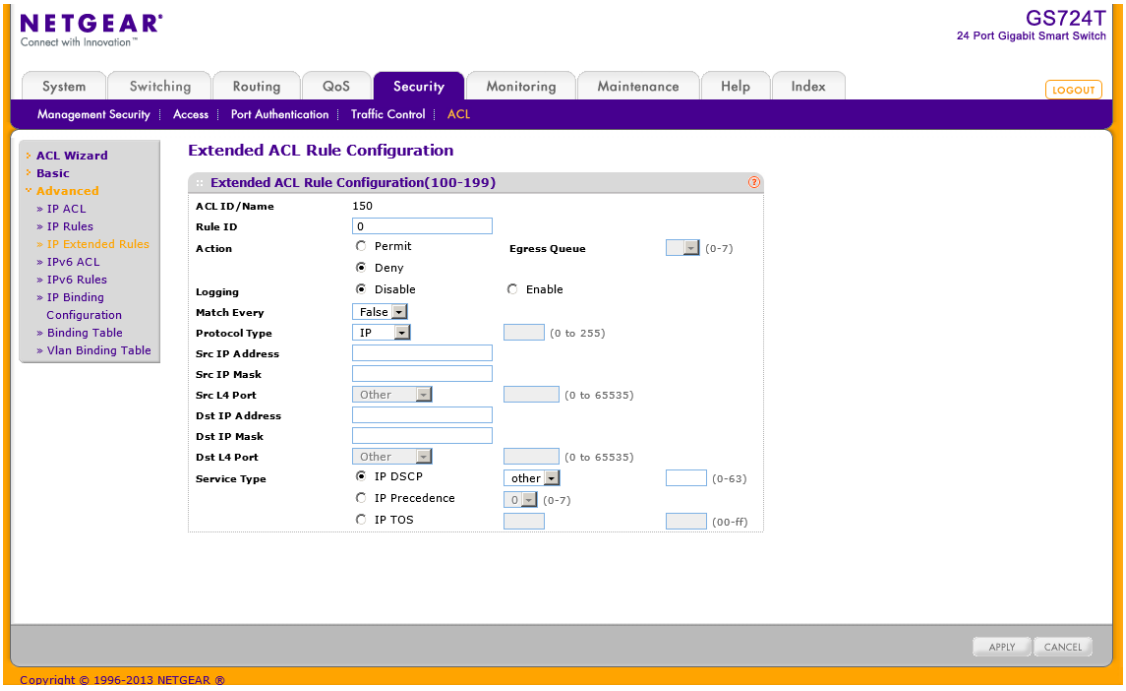
メモ：ACL リストの最後には暗黙の “deny all”ルールが存在します。ACL がパケットに適用され、明示的に設定されたルールのどれにも一致しなかった場合は暗黙の“deny all”ルールによりパケットは廃棄されます。

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 Extended ACL Rules ページを表示します。



2. 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。新しいルールを設定します。



3. 以下の情報を入力します。

- **Rule ID**：1-50 の番号をつけます。各 ACL に作成できるルールは 50 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。0-7 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。
- **Src 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スクの逆になります。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。Src 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ー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。
- **Dst IP Address**：宛先 IP アドレス（A.B.C.D 形式）を指定します。
- **Dst IP Mask**：宛先 IP アドレスマスクを指定します。
- **Dst 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スクの逆になります。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、Src 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ー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になっています。

IPv6 ACL

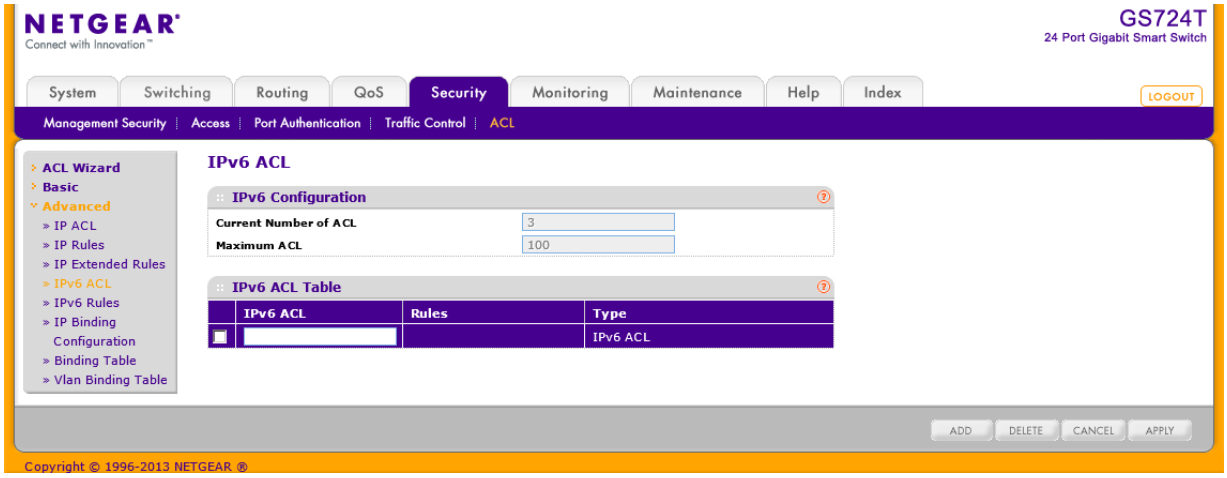
IPv6 ACL はパケットに対して連続的に一致させるルールのセットから成り立ちます。パケットがルールの条件に一致した場合、ルールの動作（Permit/Deny）が実行され、それ以上のルールへ

の一致確認はされません。IPv6ACL のためのルールは IPv6 ルール画面で設定・作成されます。

IPv6 ACL Configuration ページで IP ベースの ACL を追加・削除します。

IPv6 ACL を設定する

1. **Security** > **ACL** > **Advanced** > **IPv6 ACL** を選択して **IPv6 ACL** ページを表示します。



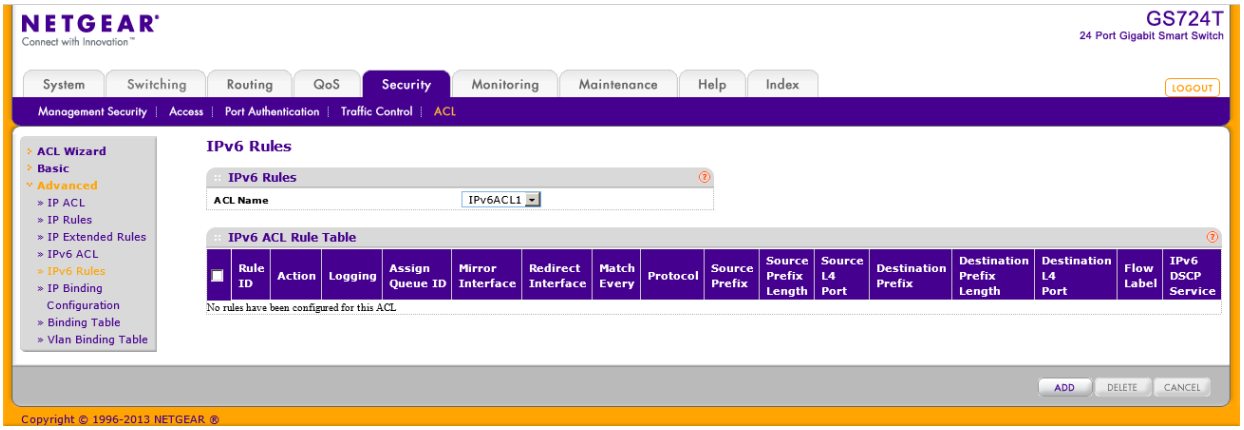
2. **Current Number of ACL** には現在設定済みの ACL の数が表示されます。
   Maximum ACL には設定可能な ACL 数が表示されています。
3. **IPv6 ACL**:IPv6 ACL の名前を指定します。
4. **Add** ボタンをクリックします。
5. 設定した IPv6 ACL を削除するには、削除する IPv6 ACL を選択して **Delete** ボタンをクリックします。

IPv6 ルール(IPv6 Rules)

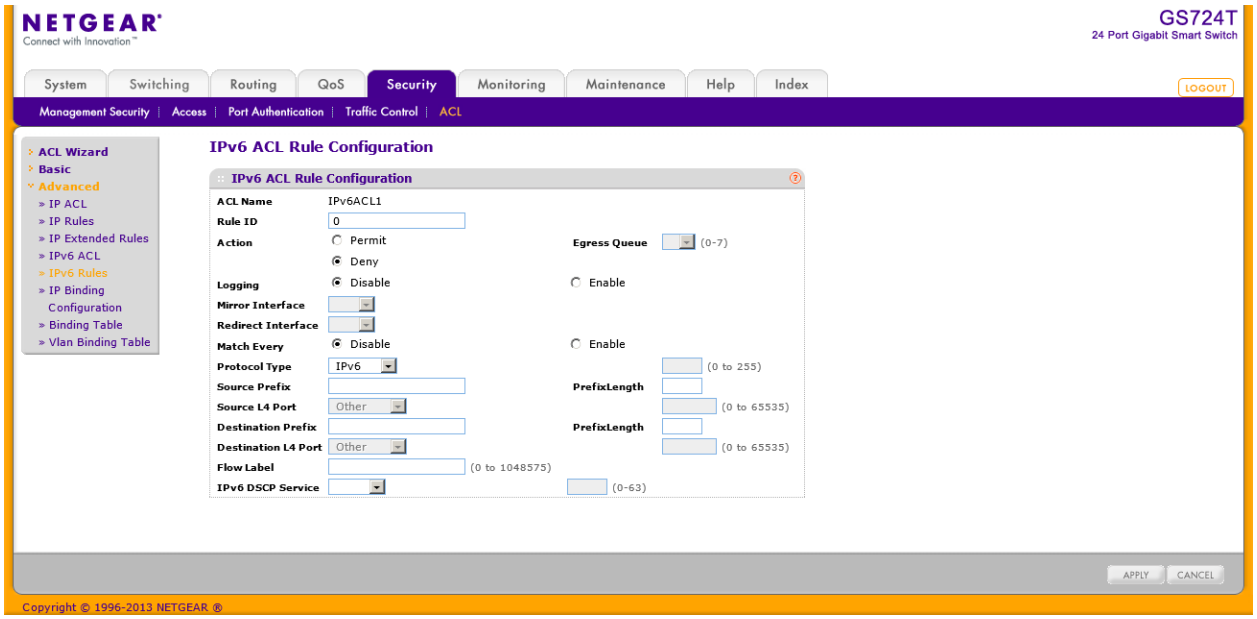
IPv6 Rules 画面で IPv6 ACL のルールを設定します。IPv6 ACL は IPv6 ACL Configuration 画面で作成します。デフォルトではどの IPv6 ACL ルールでも特定な値は有効になっていません。

IPv6 ルールを設定する

1. **Security** > **ACL** > **Advanced** > **IPv6 Rules** を選択して **IPv6 Rules** ページを表示します。



2. 新しい IPv6 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、**Add** ボタンをクリックします。



画面が更新され、追加の入力画面が表示されます。

3. 以下の情報を入力します。

- **Rule ID**：1-50 の番号をつけます。各 ACL に作成できるルールは 50 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。
- **Logging**：有効（Enable）にするとログが有効になります。Access List Trap Flag が有効になっていれば、周期的なトラップとして何回一致したかどうかという情報が送信されます。5 分に一度送信されますが、回数が変化しない場合は送信されません。

- **Egress Queues**：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。0-7 を設定します。
- **Mirror Interface**：マッチしたトラフィックを指定したインターフェースに転送します。Redirect Interface と同時には使用できません。
- **Redirect Interface**：マッチしたトラフィックは設定したインターフェースにリダイレクトされます。Mirror Interface と同時には使用できません。
- **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**：プロトコルタイプを選択するか、Other を選択して 1-255 の値を設定します。
- **Source Prefix/Prefix Length**：送信元 IPv6 アドレスのプレフィクスとプレフィクス長を指定します。Prefix Length の範囲は 1-128 です。
- **Source 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ー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 Prefix/Prefix Length**：宛先 IPv6 アドレスのプレフィクスとプレフィクス長を指定します。Prefix Length の範囲は 1-128 です。
- **Destination 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ー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。
- **Flow Label**：フローラベルは IPv6 パケットに付けられる番号です。QoS を実現するための識別のために割り当てられます。フローラベルの範囲は 0-1048575 です。
- **IPv6 DSCP Service**：DSCP 値を指定します。Other を選択した場合は、数値 0-63 を設定します。

4. IPv6 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. IPv6 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。
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. 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

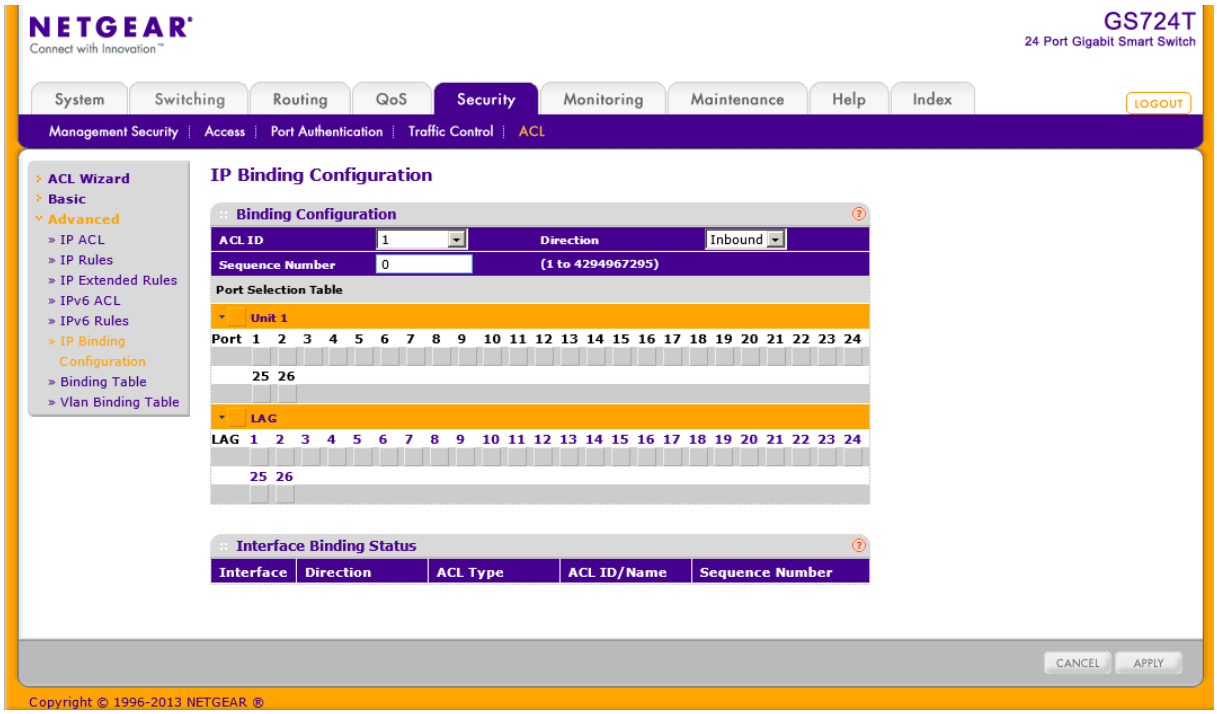
更がされます。

IP 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。

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** > **Advanced** > **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 **Direction**(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。
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 Sequence Number 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。
5. 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。
6. 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

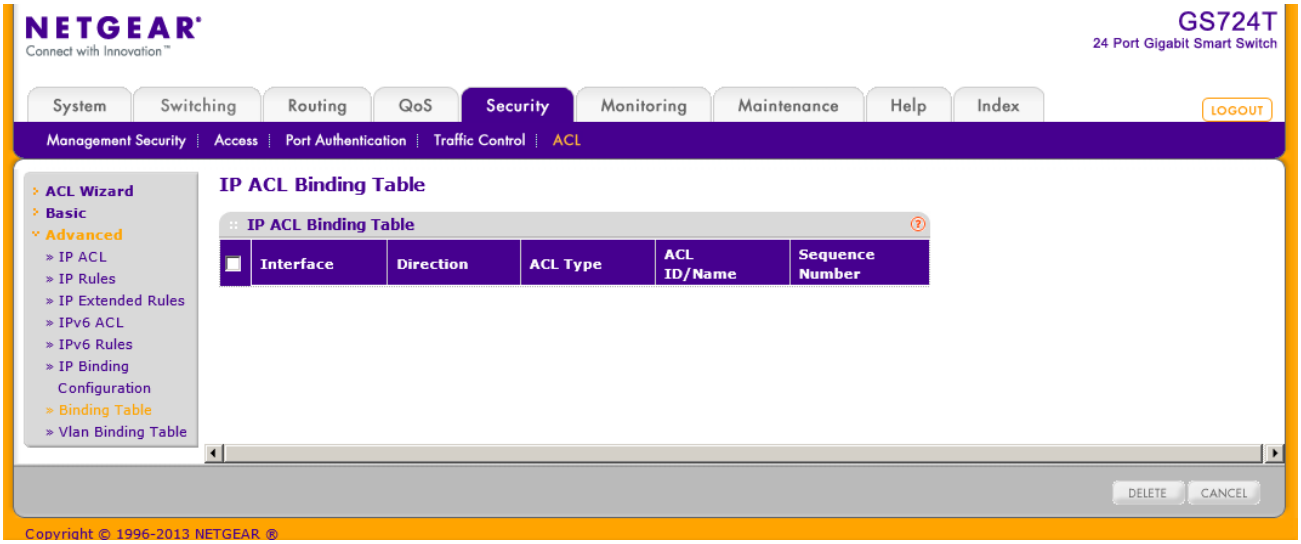
して X を消去します。

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。

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 ACL Binding Table ページを表示します。



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

項目	説明
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ーの方向。Inbound(ポートに入力される方向)のみ有効。
ACL Type	インターフェースと方向に割り当てられた ACL のタイプ。
ACL ID/Name	インターフェースと方向に割り当てられた ACL ID。
Sequence Number	ACL の順序を決めるためにインターフェース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。

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)
- ログ(Logs)
- ミラーリング(Mirroring)

ポート(Ports)

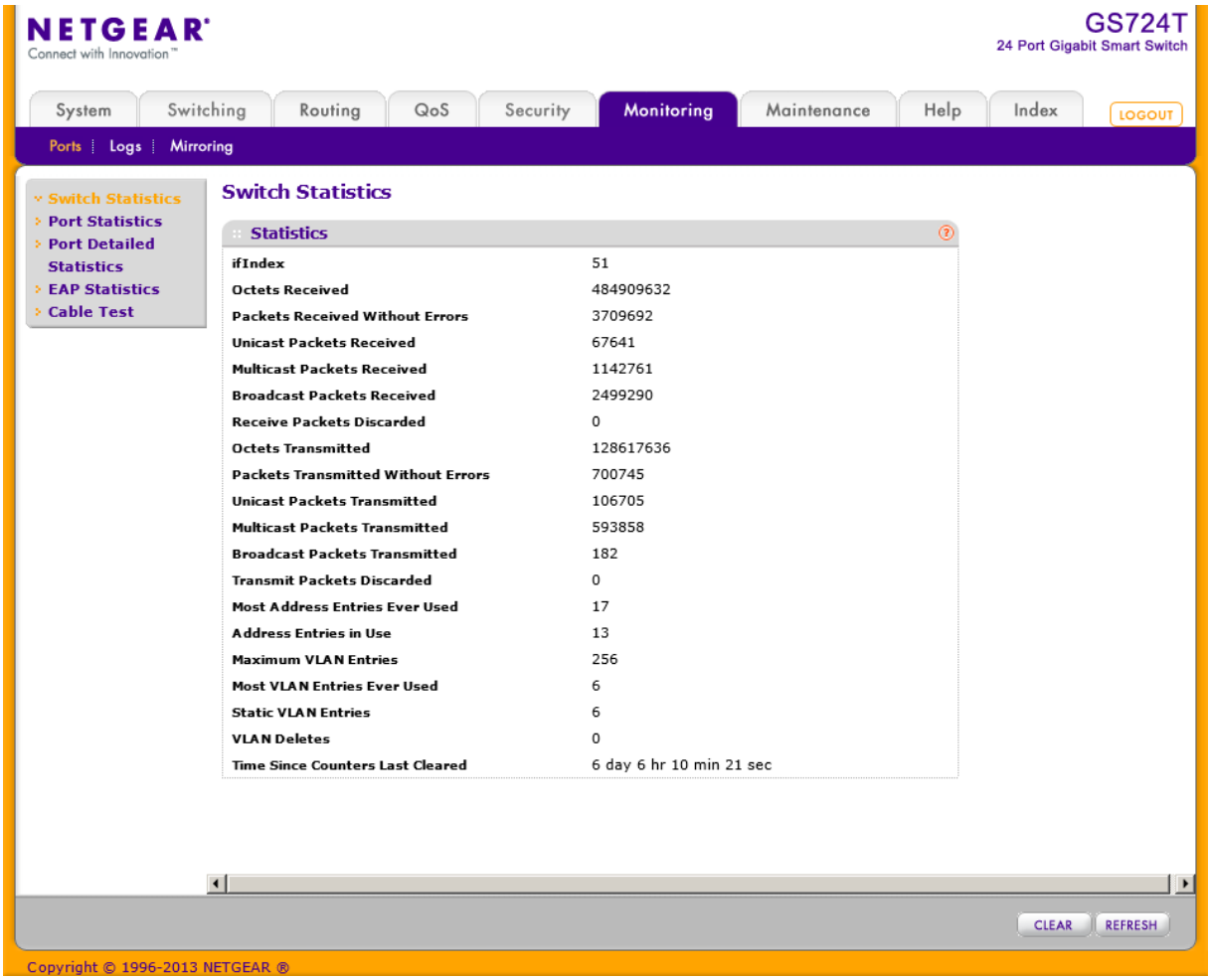
Ports リンクはスイッチで送受信されるトラフィックの量やタイプについての様々な情報へのリンクを含みます。Ports リンクから以下のページへアクセスできます。

- 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)
- ケーブルテスト(Cable Test)

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。



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。
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	スイッチで利用可能な最大 VLAN 数。

項目	説明
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。

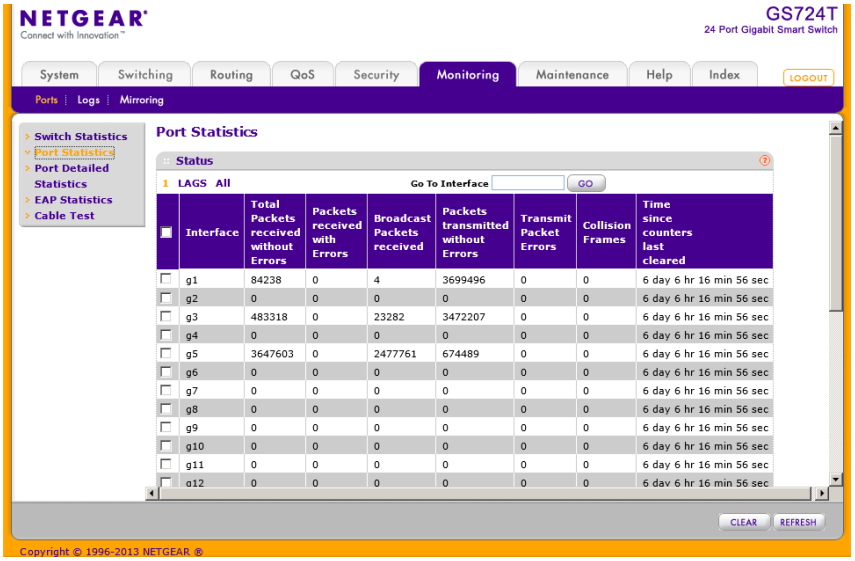
- Clear：カウンターの値をクリアします。廃棄されたパケット数はクリアされません。

- 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。



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。

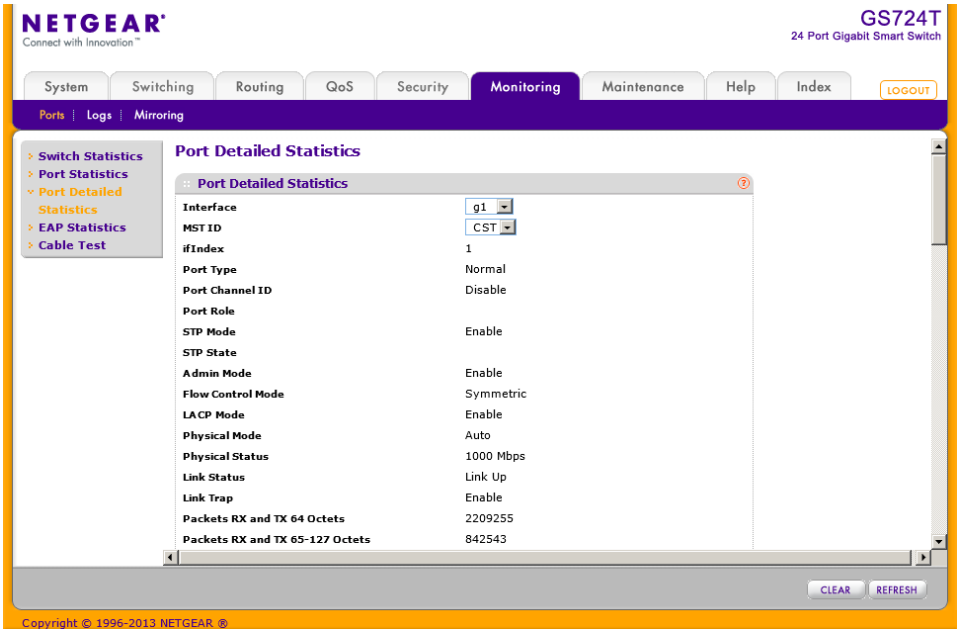
ページ下部のボタンを使って以下の操作をします。

- 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。



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。
Flow Control Mode	フローコントロールの状態。LAG インターフェースでは無効です。
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。 • **Enable**：ポート状態が変化するとトラップを送信します。 • **Disable**：ポート状態が変化してもトラップを送信しません。
Packets RX and TX 64 Octets	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,プリアンブルは含まず、FCS を含みます。
Packets RX and TX 65-127 Octets	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）。IFG,プリアンブルは含まず、FCS を含みます。
Packets RX and TX 128-255 Octets	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）。IFG,プリアンブルは含まず、FCS を含みます。
Packets RX and TX 256-511 Octets	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）。IFG,プリアンブルは含まず、FCS を含みます。
Packets RX and TX 512-1023 Octets	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）。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 1519-2047 Octets	パケットサイズが 1519-2047 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 2048-4095 Octets	パケットサイズが 2048-4095 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 4096-9216 Octets	パケットサイズが 4096-9216 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。
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 Octets	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,プリアンブルは含まず、FCS を含みます。
Packets Received 65-127 Octets	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）。IFG,プリアンブルは含まず、FCS を含みます。

Packets Received 128-255 Octets	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）。IFG,プリアンブルは含まず、FCS を含みます。
Packets Received 256-511 Octets	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）。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 > 1518 Octets	パケットサイズが 1518 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	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あるもの。
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。
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	パケットサイズが 512-1023 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 1024-1518 Octets	パケットサイズが 1024-1518 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。

項目	設定
Packets Transmitted > 1518 Octets	パケットサイズが 1519 バイト以上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。
Maximum Frame Size	最大フレーム長。デフォルトは 1518 バイト。範囲は 1518-9216 バイト。
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。
Transmit Packets Discarded	廃棄された送信パケット数。エラーパケットは含まない。
Total Transmit Errors	送信エラーパケット数。
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。
Dropped Transmit Frames	指定されたポートでの廃棄された送信フレーム数。
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。

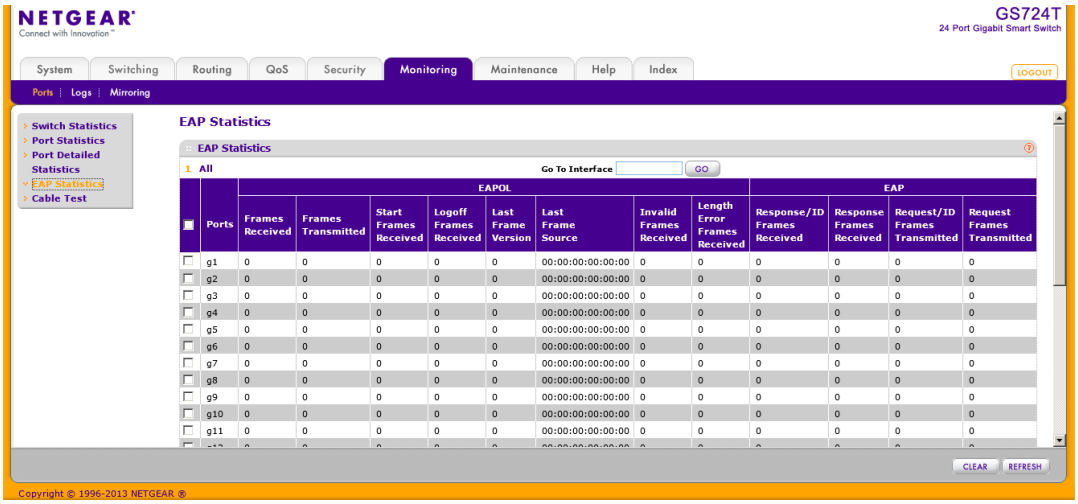
ページ下部のボタンを使って以下の操作をします。

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



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。
Logoff 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。

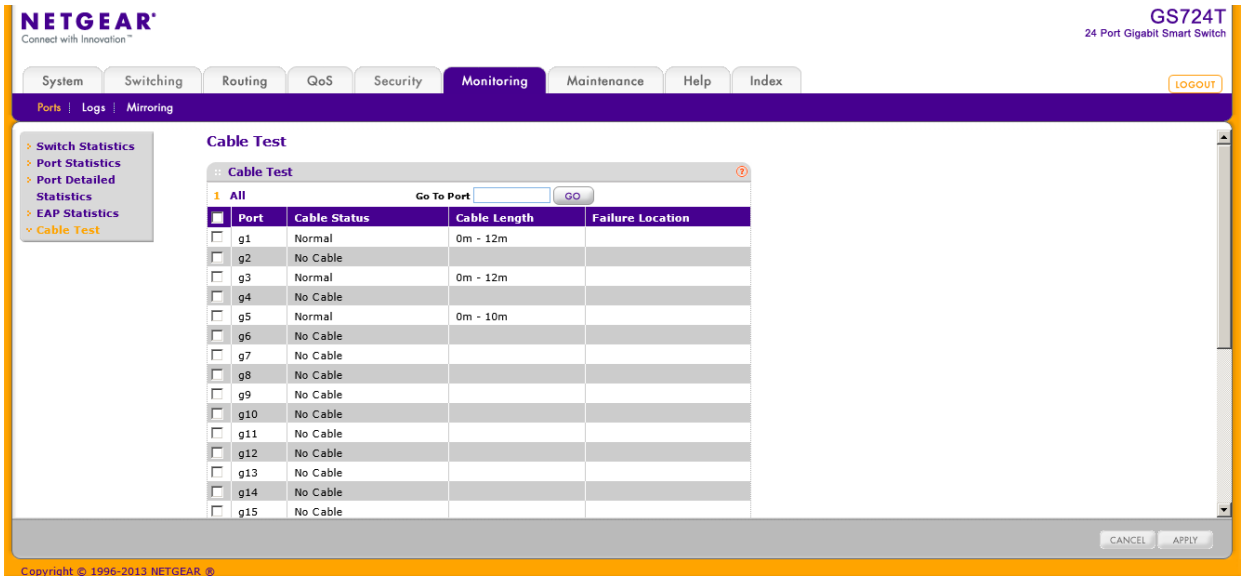
- Clear:カウンターの値をクリアします。一番上のチェックボックスを選択してすべてのポートのカウンターをクリアするか、個々のポートを選択してポートのカウンターをクリアします。
- Refresh:カウンターを最新状態に更新します。

ケーブルテスト(Cable Test)

Cable Test 画面でスイッチのポートに接続されているケーブルの情報を表示します。

ケーブルテストを実行する

1. Monitoring > Ports > Cable Test を選択して Cable Test ページを表示します。



2. ケーブルテストを実行するポートのチェックボックスを選択します。
3. Apply ボタンをクリックします。
   選択したポートでケーブルテストが実行されます。

ケーブルテストの実行に約 2 秒かかります。ポートが有効でリンクがアップしている場合の状態は Normal です。テストの結果、ケーブル長の推定値を表示します。リンクがダウンでケーブルが

10M または 100M のイーサネットアダプターに接続されている場合は、イーサネットアダプターによっては使用していない電線のペアが終端されていないあるいは接地されていないために、ケーブルの状態が Open または Short になることがあります。

以下の表はケーブルテスト画面に表示される情報の説明です。

項目	説明
Port	ポート番号
Cable Status	ケーブルの状態。 • Normal：正常。 • Open：ケーブルが接続されていないか、コネクター不良。 • Short.：ケーブルがショートしている。 • Cable Test Failed：テスト失敗。 • Unknown：テストが実行されていない。
Cable Length	推定ケーブル長。Cable Status が Normal の場合のみ表示されます。
Failure Location	推定障害箇所（m）。ポートからの長さ。Cable Status が Open または Short の場合のみ表示されます。

ログ(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ーを含みます。

Monitoring > **Logs** タブは以下のフォルダーのリンクを含みます。

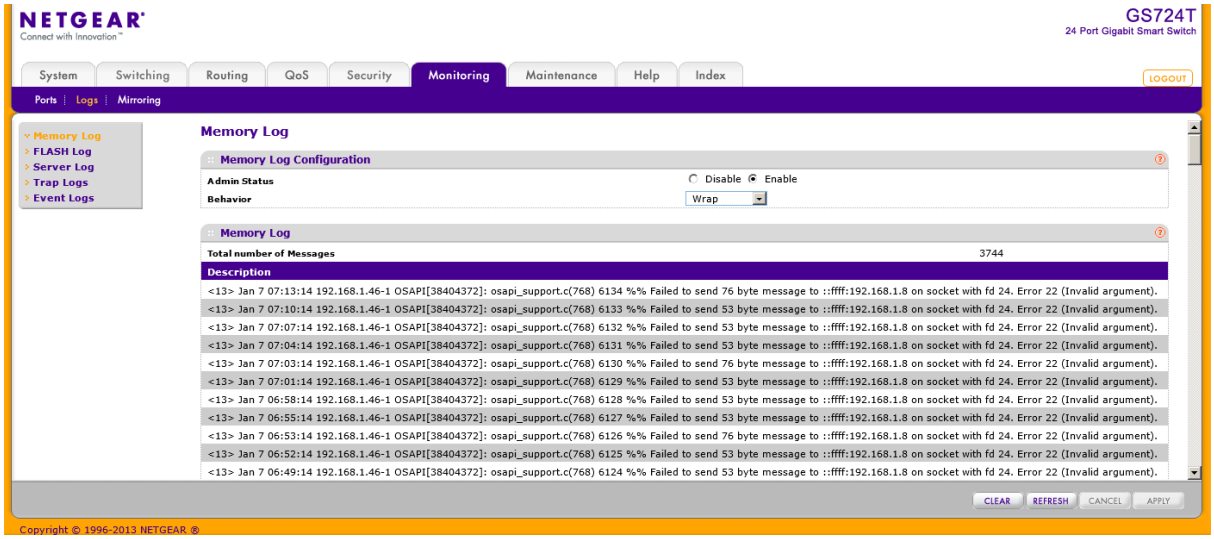
- メモリーログ(Memory Logs)
- フラッシュログ(FLASH Log)
- サーバーログ(Server Log)
- トラップログ(Trap Logs)
- イベントログ(Event Logs)

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。

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 200 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。

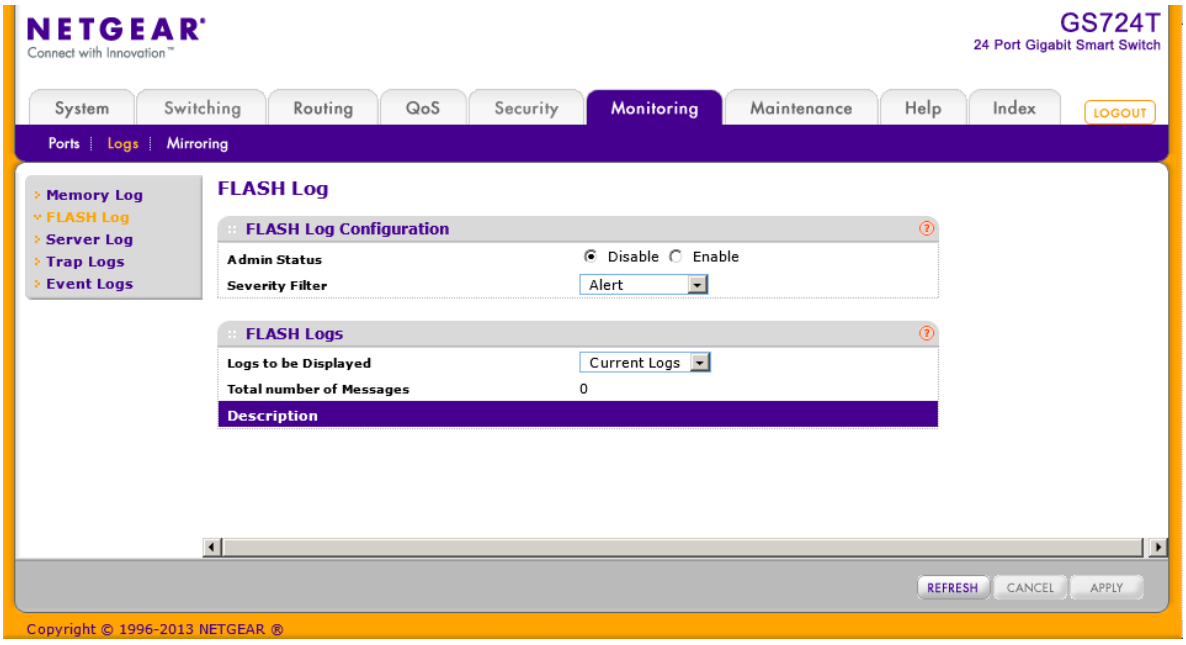
フラッシュログ（FLASH Log）

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。フラッシュログは現在の運用状況とスタートアップのログメッセージの表示、あるいは前回の再起動前の最大 64 個までのログされたメッセージを表示することができます。設定した重要度レベル（Severity Level）に一致したメッセージのみがフラッシュメモリーにログされます。

FLASH Log 画面を使って FLASH ログの設定、表示をします。

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。

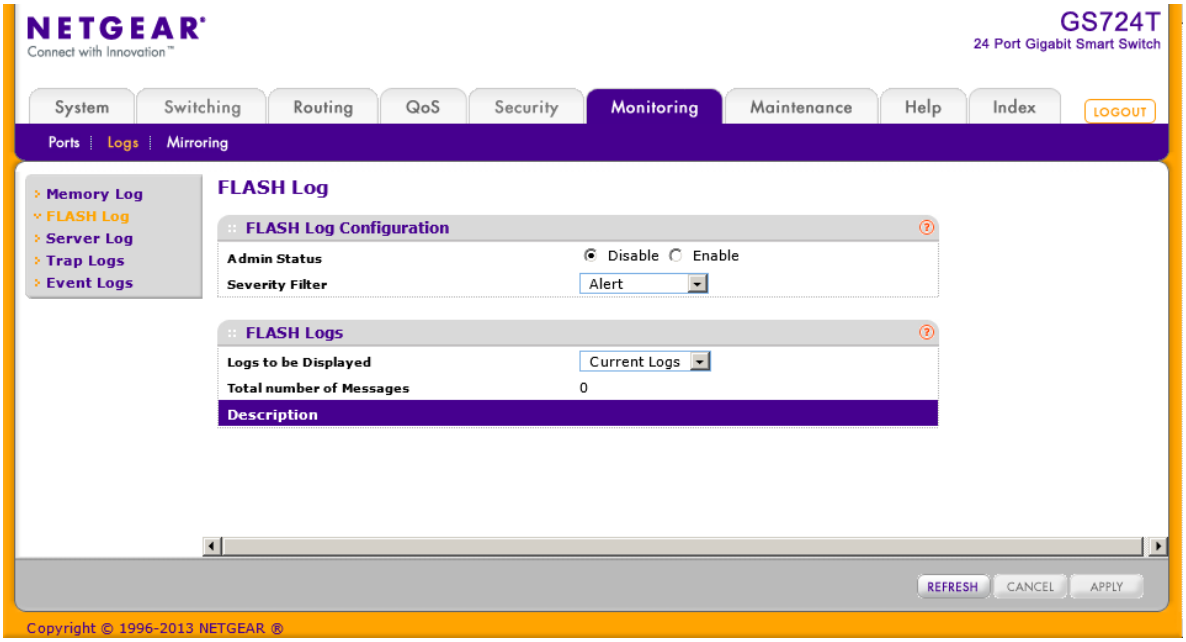
Descriptions 欄にはフラッシュログメッセージが表示されます。

ページ下部のボタンを使って以下の操作をします。

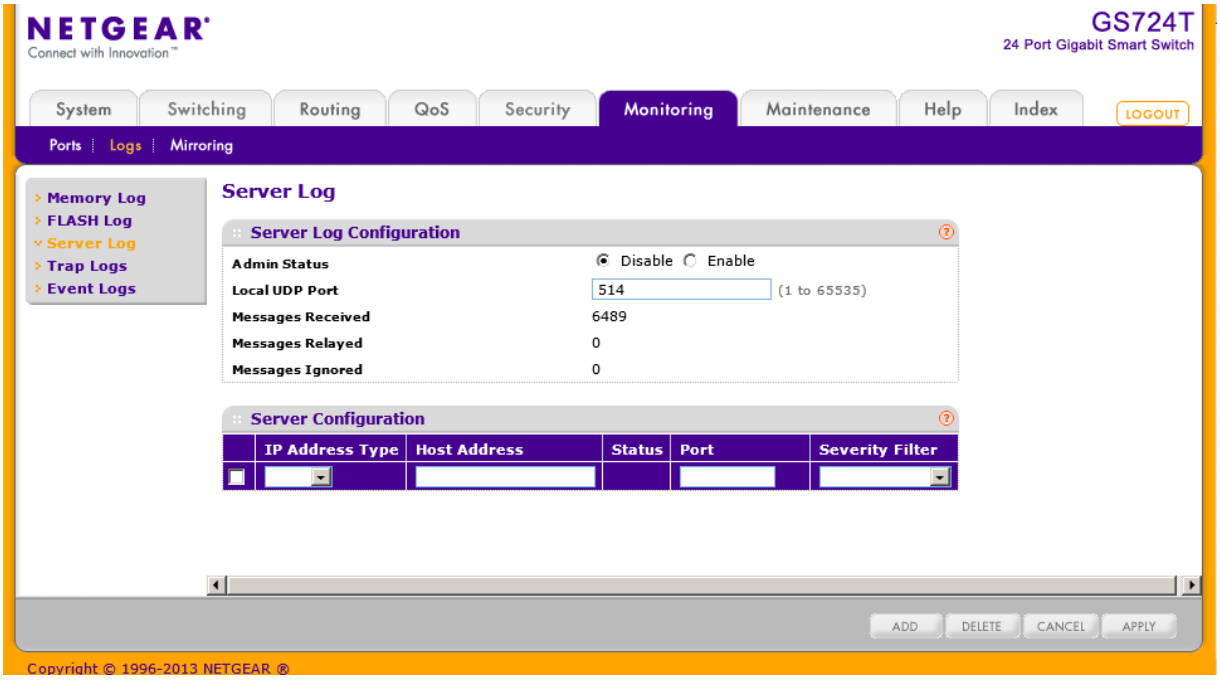
- Clear:メッセージをメモリーのバッファーログからクリアします。
- Refresh:ログ中のメッセージを最新状態に更新します。
- Cancel ボタンをクリックして設定画面の情報をキャンセルし、スイッチの最新情報を表示させます。

フラッシュログ表示をする

1. Monitoring > Logs > FLASH Log を選択して FLASH Log ページを表示します。



2. Logs to be Displayed 欄で表示するログを選択します。
   - Current Logs:現在のログを表示します。
   - Previous Logs:再起動前のログを表示します。保存された最大 64 個のログを表示します。。表示されるログは以下の 2 種類です。



- 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 32 個のメッセージを保存します。
- 2 つ目のログタイプは **system operation log** です。System operation log はシステム再起動前の最後に受信した 32 個のメッセージを保存します。

サーバーログ (Server Log)

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。

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 Received**:受信したメッセージ数。廃棄や無視されたメッセージも含みます。
- **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

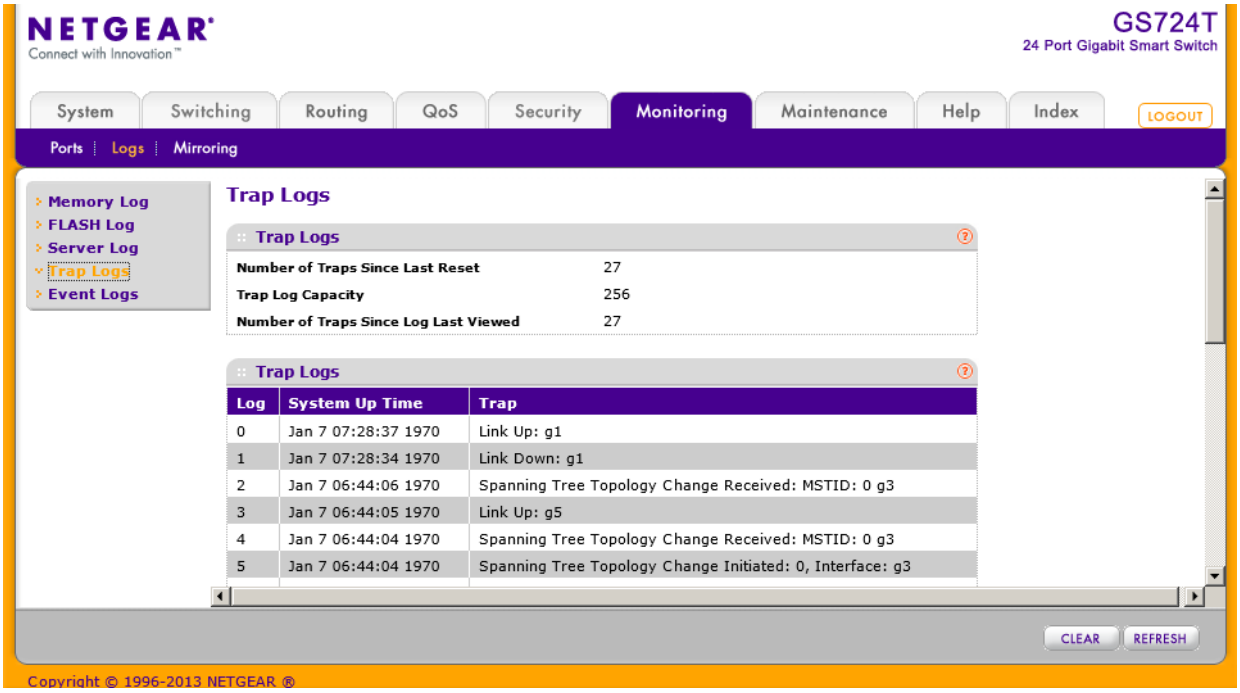
1. リモート Syslog ホスト（ログサーバー）を追加するには以下の設定をして **Add** ボタンをクリックします。
   - **Host Address**：シスログサーバーを IP アドレス(IPv4/IPv6)またはホスト名（DNS）で指定します。
   - **Port**：ホストのポート番号を指定します。デフォルトは 514 です。
   - **Severity Filter**：ホストへ送信するログメッセージのタイプを指定します。ログは設定したレベルとそれ以上のレベルのメッセージを送信します。例えば、Error を選択すると、Error, Critical, Alert, 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。



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
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。

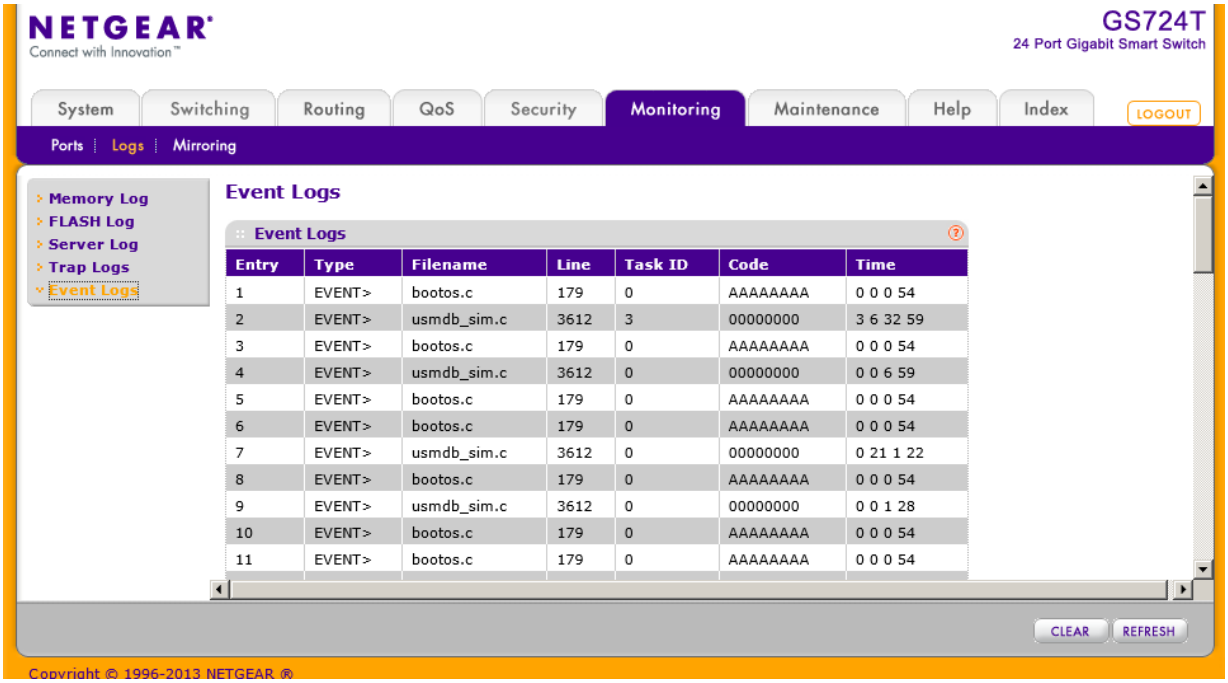
項目	説明
Log	トラップの番号。
System Up Time	トラップが発生した時のスイッチが再起動してからの時間。
Trap	トラップの情報。

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。



以下に Event Logs 欄に表示される情報の説明を示します。

項目	説明
Entry	イベントの番号。最新が一番上。
Type	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。

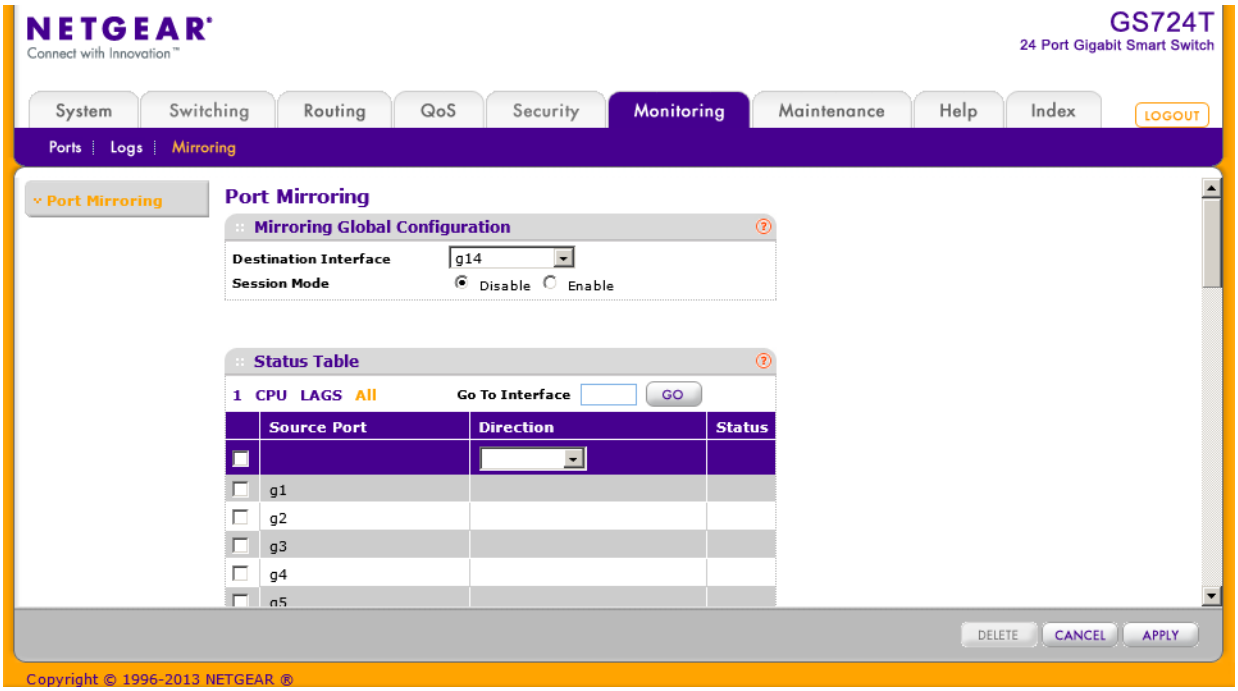
ミラーリング(Mirroring)

Port Mirroring リンクでポートミラーリングの設定ができます。

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。

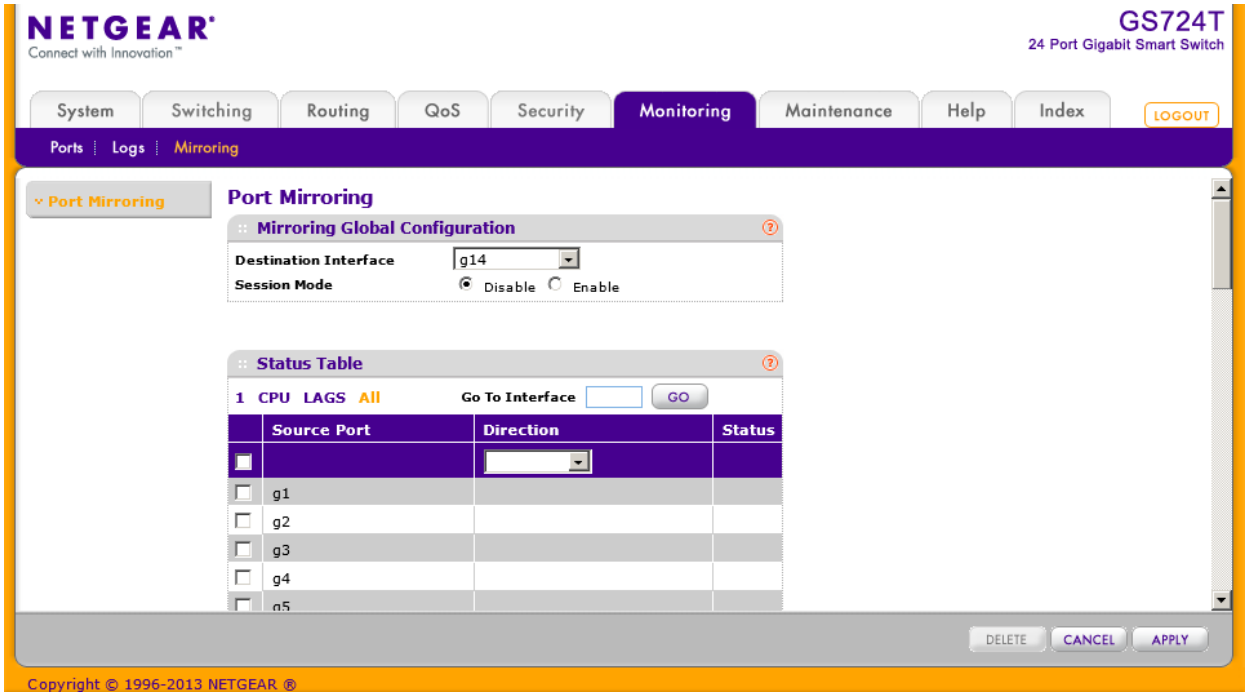
宛先ポートにコピーされるパケットは送信元パケットと同じフォーマットです。送信元パケットの VLAN タグの有無も含めてコピーされます。

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 > Mirroring > Port Mirroring を選択して Port Mirroring ページを表示します。



2. Destination Interface：宛先ポートを選択します。
3. Session Mode：ポートミラーリングの有効・無効を選択します。
   - Enable：選択したポートのポートミラーリングを有効にします。
   - Disable：選択したポートのポートミラーリングを無効にします。設定は維持されます。
4. 参照元ポートを選択します。
   複数のポート及び LAG を選択できます。CPU ポートも参照元として選択できます。
   - ポートおよび LAG を表示して参照元を設定します。
     - 1 をクリックして、物理ポートを表示します。
     - LAGS をクリックして、LAG（Link Aggregation Group）を表示します。
     - CPU をクリックして CPU ポートを表示します。
     - ALL をクリックして、すべてのインターフェースを表示します。
   - インターフェースの横のチェックボックスをクリックして選択をします。
5. Direction：参照する方向を指定します。
   - Tx and Rx：送信と受信の双方向を参照します。
   - Tx only：送信方向のみを参照します。

- **Rx only**：受信方向のみを参照します。

6. **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、**Status** 欄の表示は Mirrored となります。
7. 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。
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。

メインテナンス（Maintenance）

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）

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。

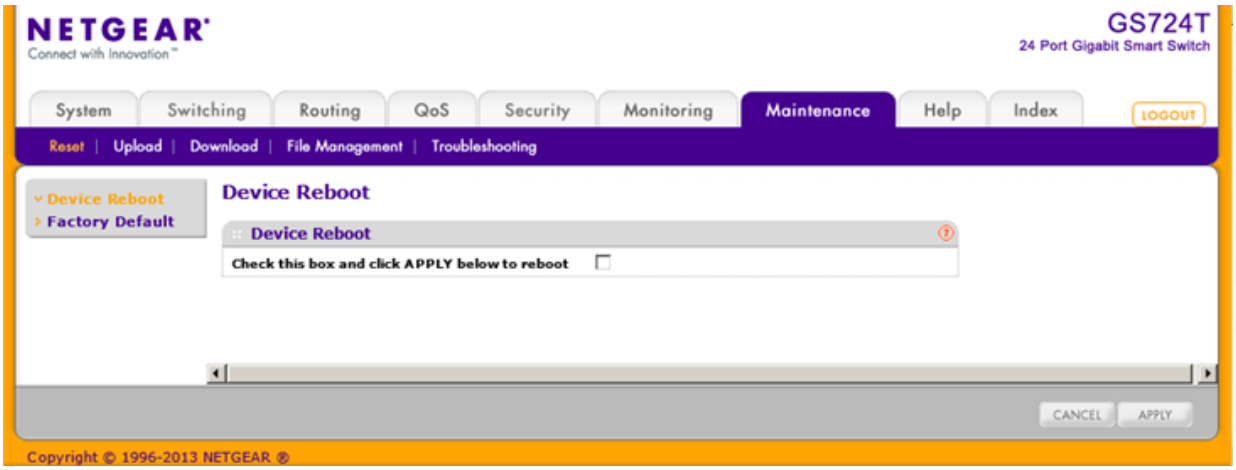
- 再起動(Device Reboot)
- ファクトリーデフォルト(Factory Default)

再起動(Device Reboot)

Device Reboot ページでスイッチを再起動します。

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。

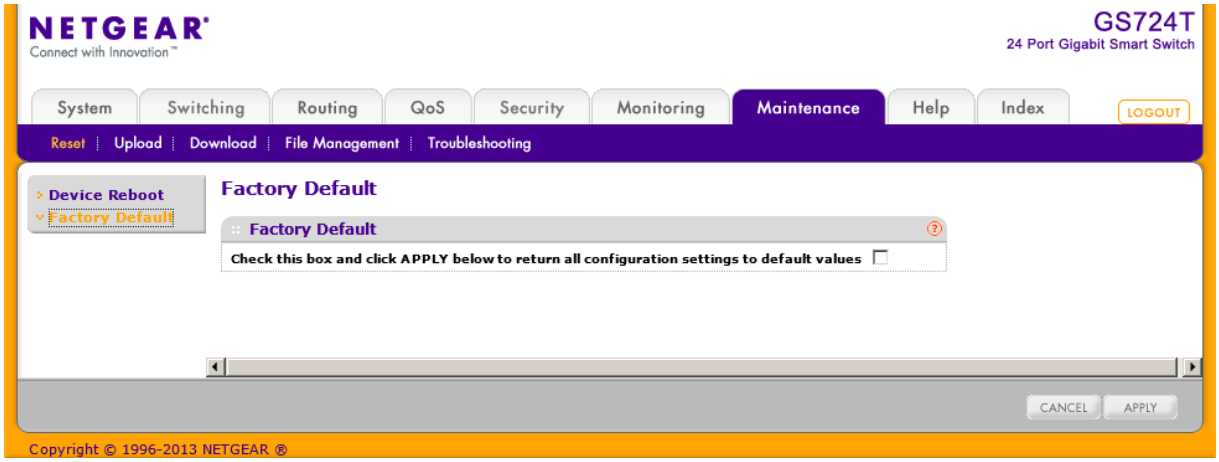
ファクトリーデフォルト(Factory Default)

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 クライアント機能が有効になっています。DHCP サーバーがあるネットワークでは DHCP サーバーから IP アドレスが割り当てられます。

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)

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。

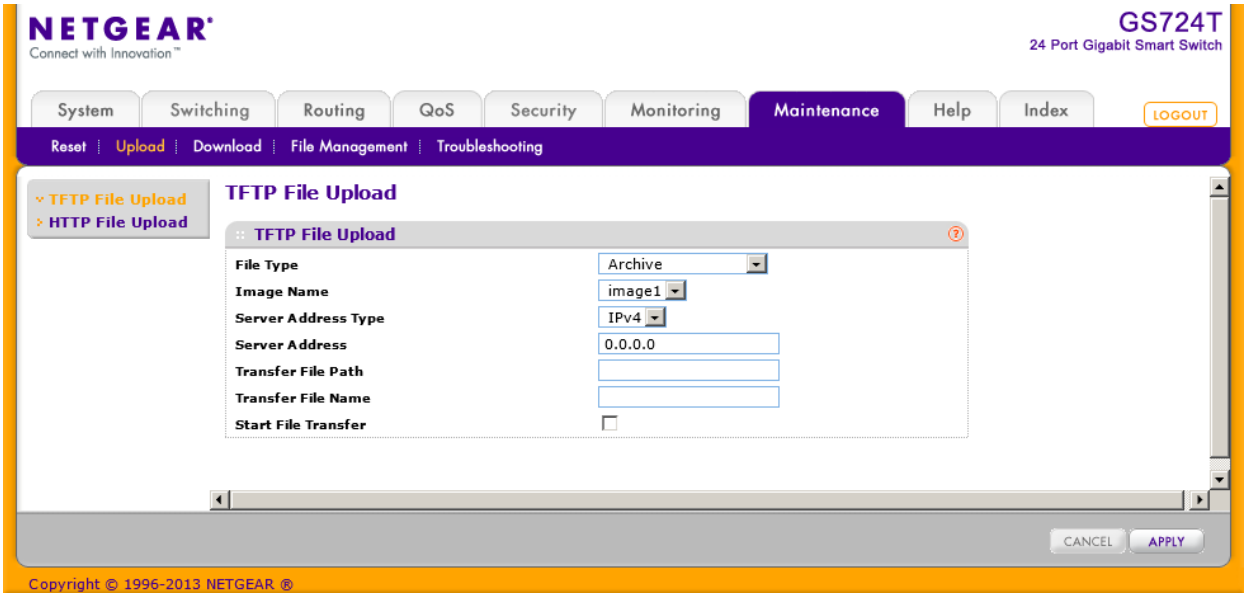
Upload メニュー以下の機能のリンクを含んでいます。

- TFTP ファイルアップロード
- HTTP ファイルアップロード

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

TFTP 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。

1. Maintenance > Upload > TFTP File Upload を選択して TFTP File Upload ページを表示します。

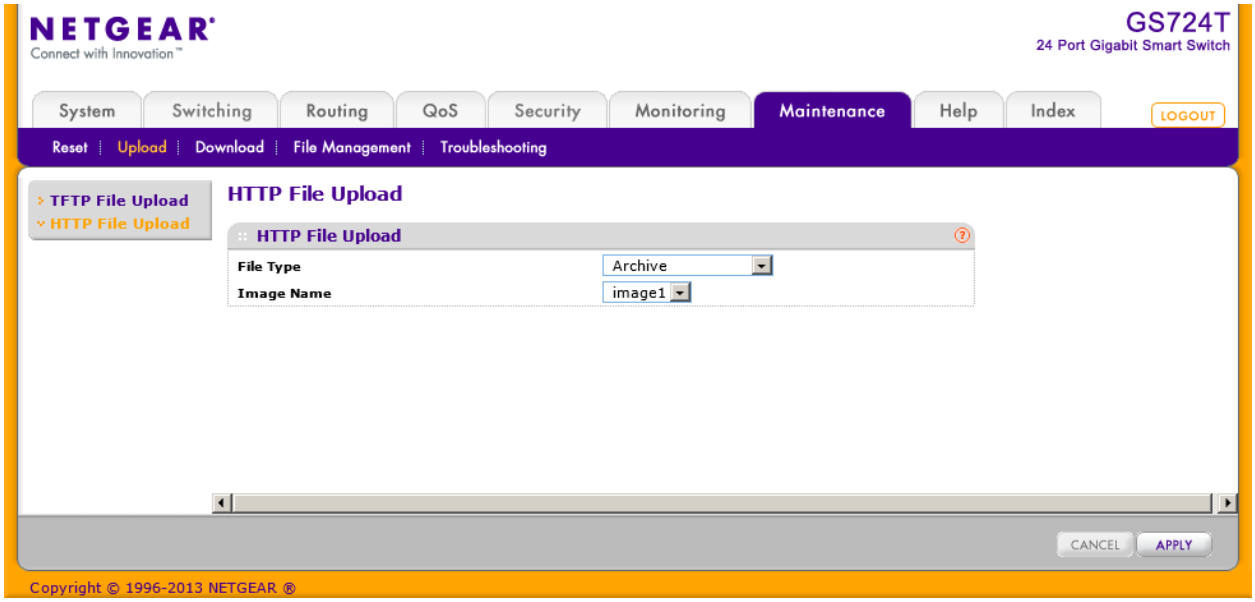


2. File Type:アップロードするファイルのタイプを選択します。
   - Archive:コードイメージ。
   - Text Configuration:テキスト設定ファイル。
   - Error Log:エラーログ、イベントログ。
   - Trap Log:トラップログ。
   - Buffered Log:メモリー中のバッファーログ。
   - Tech Support:Tech Support ファイル。トラブルシューティングの様々な情報が含まれています。

3. **Image Name List**:アップロードするイメージ名を選択します。
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 のフォーマットで指定します。
6. **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。Archive 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。
10. 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

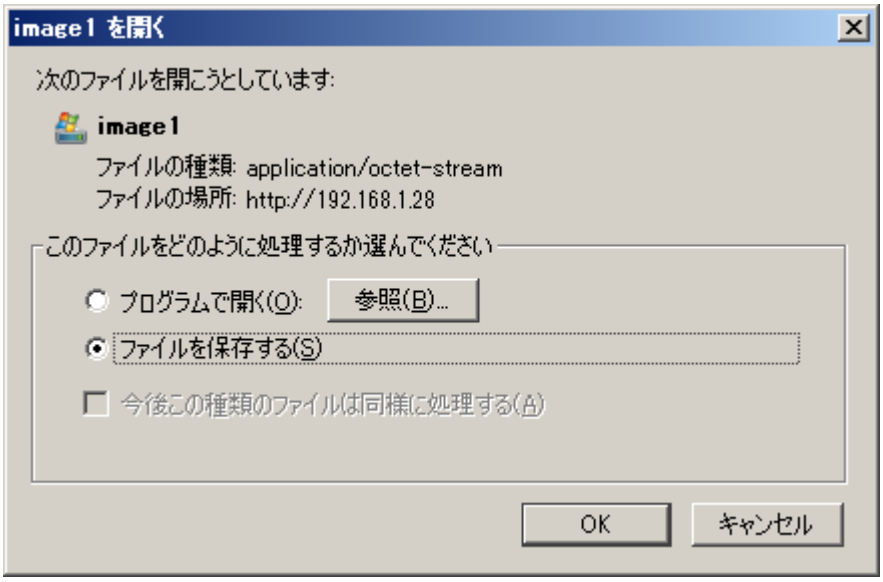
1. **Maintenance** > **Upload** > **HTTP File Upload** を選択して **HTTP File Upload** ページを表示します。



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。
   - **Archive**:コードイメージ。

- **Text Configuration**：テキスト設定ファイル。
- **Tech Support**：Tech Support ファイル。トラブルシューティングの様々な情報が含まれています。

3. **Image Name**：タイプが Archive の場合は、image1 か image2 かを選択します。この選択肢は Archive 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。
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。



スイッチへのファイルダウンロード(Download)

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。

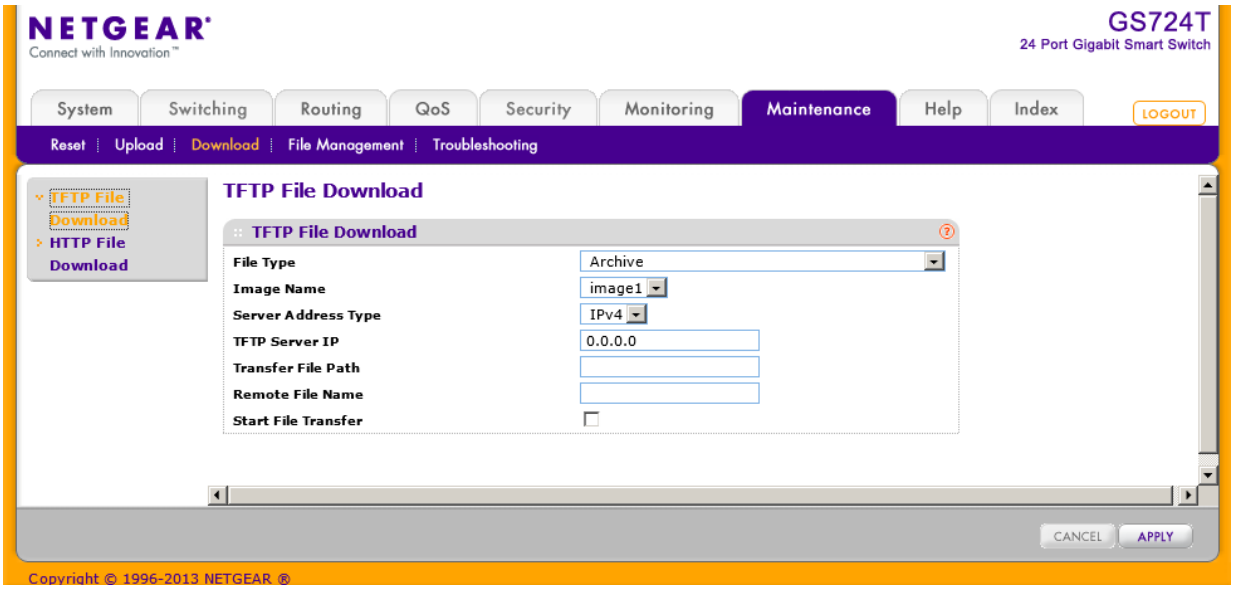
スイッチにファイルをダウンロードするには以下の条件を満たす必要があります。

- 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。

HTTP でもダウンロードができます。

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。
   - **Archive**：Archive 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、もう一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(startup-config)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。
   - **Licence Key**：特定のスイッチ機能を有効にするためのライセンスキー。
   - **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**：Archive をスイッチ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ます。File Type で Archive 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 IP**：TFTP サーバーの IP アドレスあるいはホスト名を Server Address Type のフォーマットで指定します。
6. **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。

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。
   - **Archive**:Archive 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、もう一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(startup-config)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。
   - **Licence Key**:特定のスイッチ機能を有効にするためのライセンスキー。
   - **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**:Archive をスイッチ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ます。File Type で Archive 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. Apply ボタンをクリックしてファイル転送を開始します。

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 つのバージョンのスイッチソフトウェアを保持します。一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。この機能はスイッチ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。

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。

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。

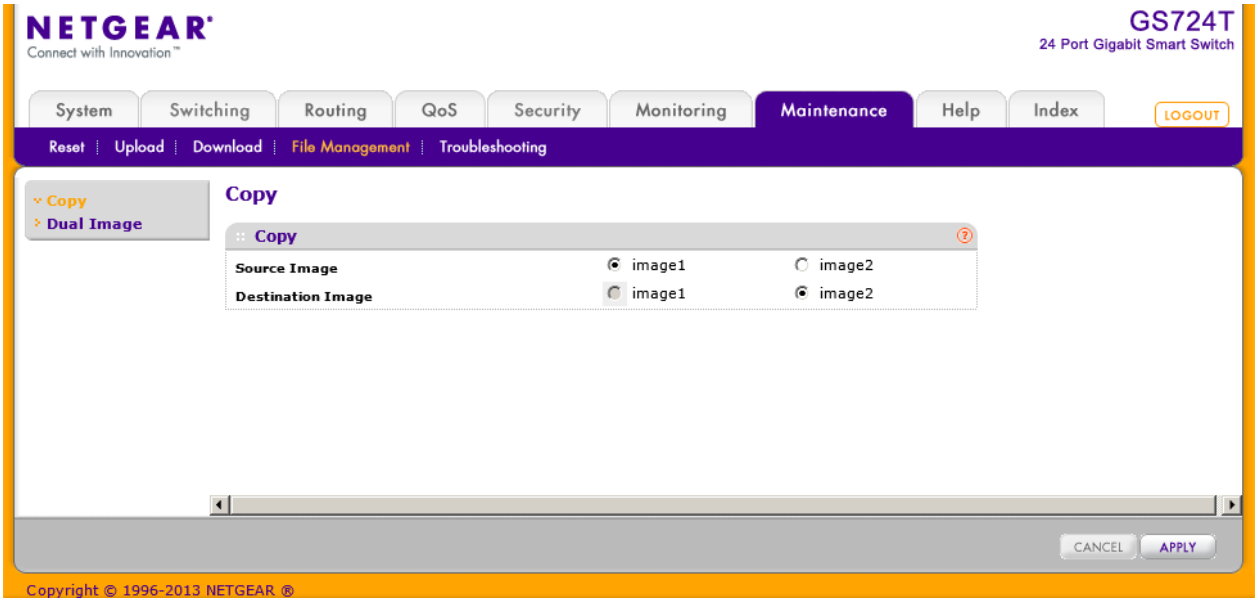
- コピー(Copy)
- デュアルイメージ設定(Dual Image Configuration)
- デュアルイメージ状態(Dual Image Status)

コピー(Copy)

Use the **Copy** 画面でイメージをコピーすることができます。(image1 と image2 の間)

イメージをコピーする

1. **Maintenance** > **File Management** > **Copy** を選択して **Copy** ページを表示します。



2. **Source Image**:コピー元ファイルを選択します。
3. **Destination Image**:コピー先ファイルを選択します。

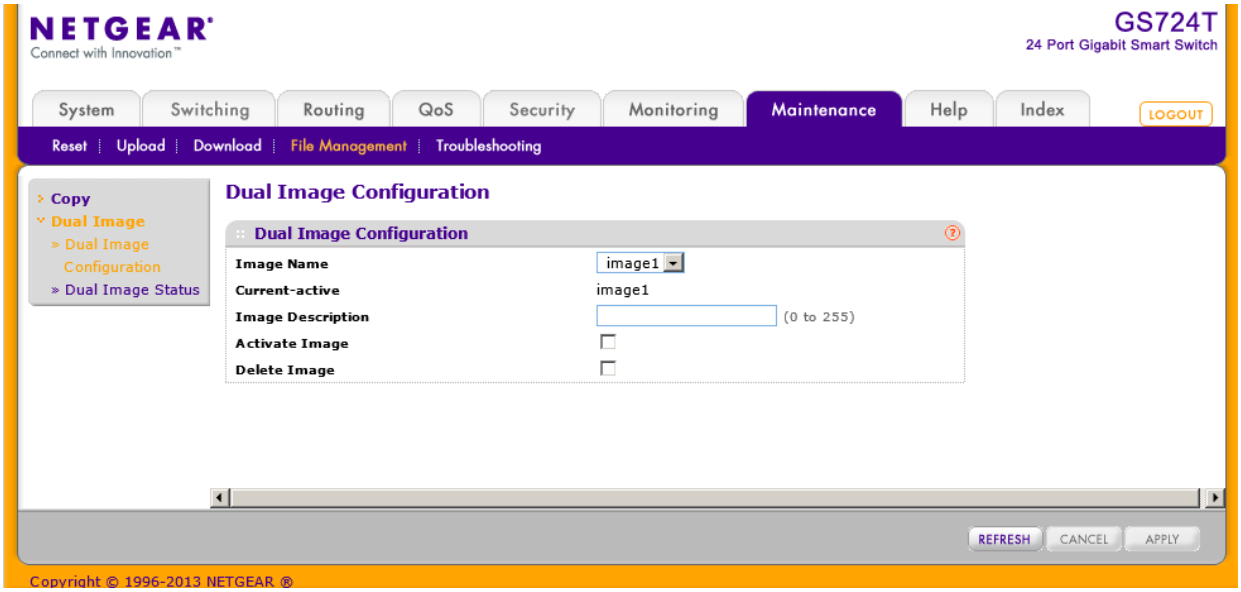
4. Apply ボタンをクリックします。

デュアルイメージ設定（Dual Image Configuration）

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。

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 ではないイメージを選択します）
3. Current-active 欄は現在アクティブなイメージを表示します。
4. Image Description：イメージの説明を記入します。
5. Activate 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。

---

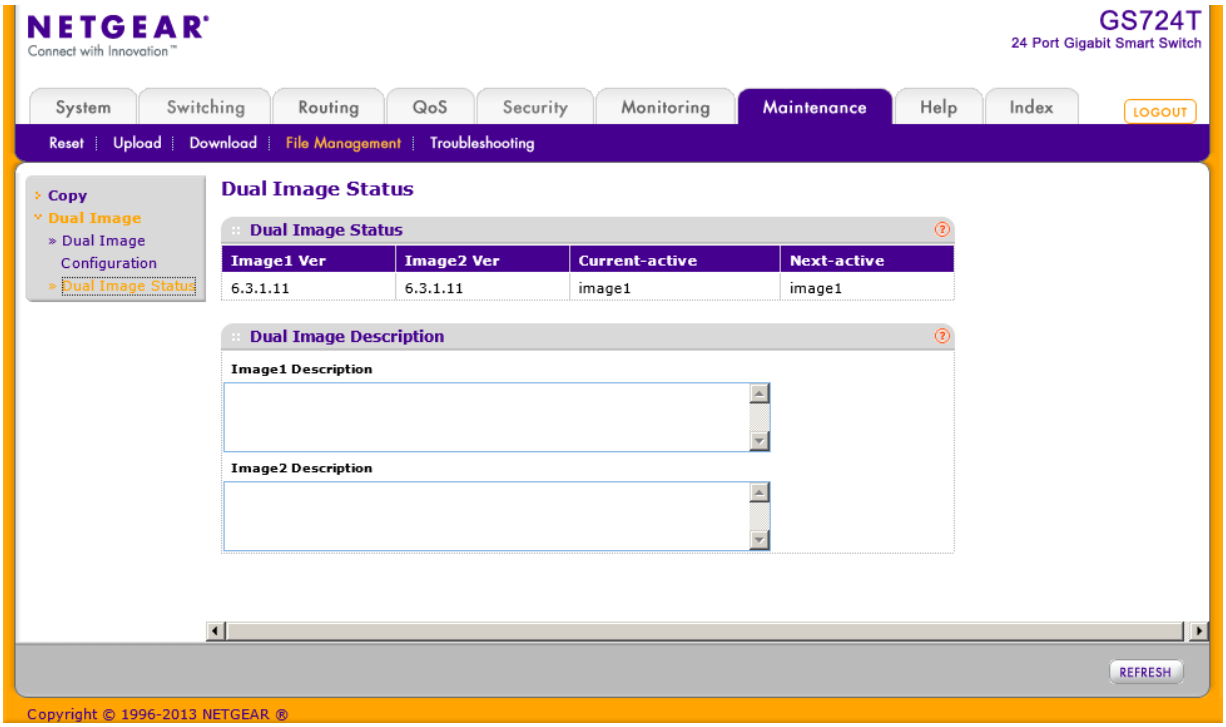
6. スイッチの永久記憶媒体からイメージを削除するには、Delete Image チェックボックスを選択します。アクティブイメージを削除することはできません。

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。

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。



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
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。

トラブルシューティング（Troubleshooting）

この章では以下の項目について記します。

- トラブルシューティング設定メニュー
- トラブルシューティングチャート

トラブルシューティング設定メニュー（Troubleshooting Configuration Menu）

このメニューで、IPv4/IPv6 アドレスへの Ping、IPv4/IPv6 ホストへのルートのトレースといった基本的なトラブルシューティング機能を実行できます。

Troubleshooting メニューは以下の機能へのリンクを含みます。

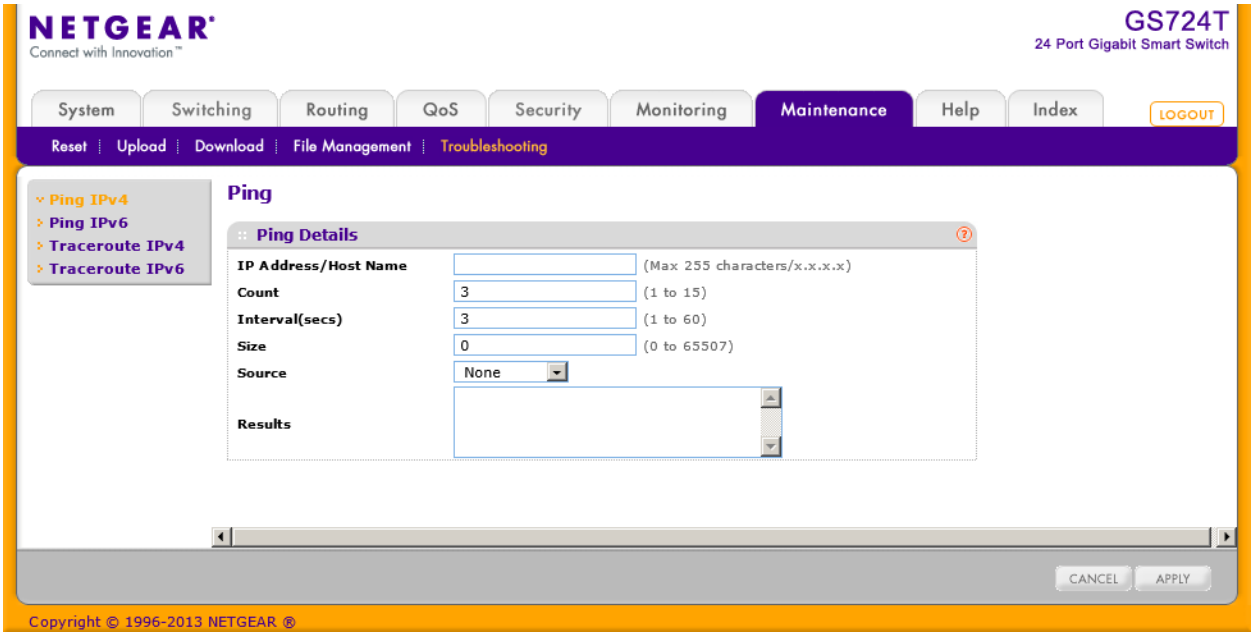
- Ping IPv4
- Ping IPv6
- トレースルート IPv4（Traceroute IPv4）
- トレースルート IPv6（Traceroute IPv6）

Ping IPv4

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。

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. IP address/Hostname：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。

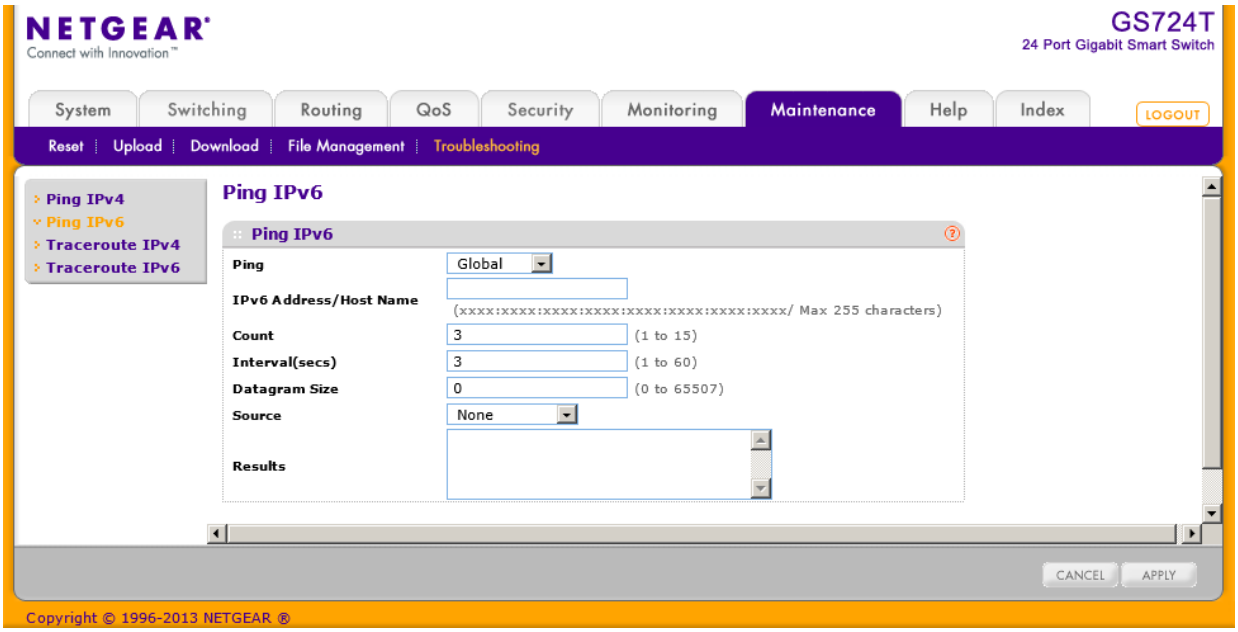
3. 以下の設定をすることもできます。
   - **Count**:送信する Ping の数。1-15。
   - **Interval**:Ping の送信間隔(秒)。1-60。
   - **Size**:Ping(ICMP)パケットサイズ。0-65507。
   - **Source**:Ping を送信する送信元を選択します。
     - **None**:デフォルトの送信インターフェース。
     - **IP Address**:IP アドレス。送信元 IP アドレスを入力する欄が表示されます。
     - **Interface**:送信するインターフェースを選択します。
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 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。

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。

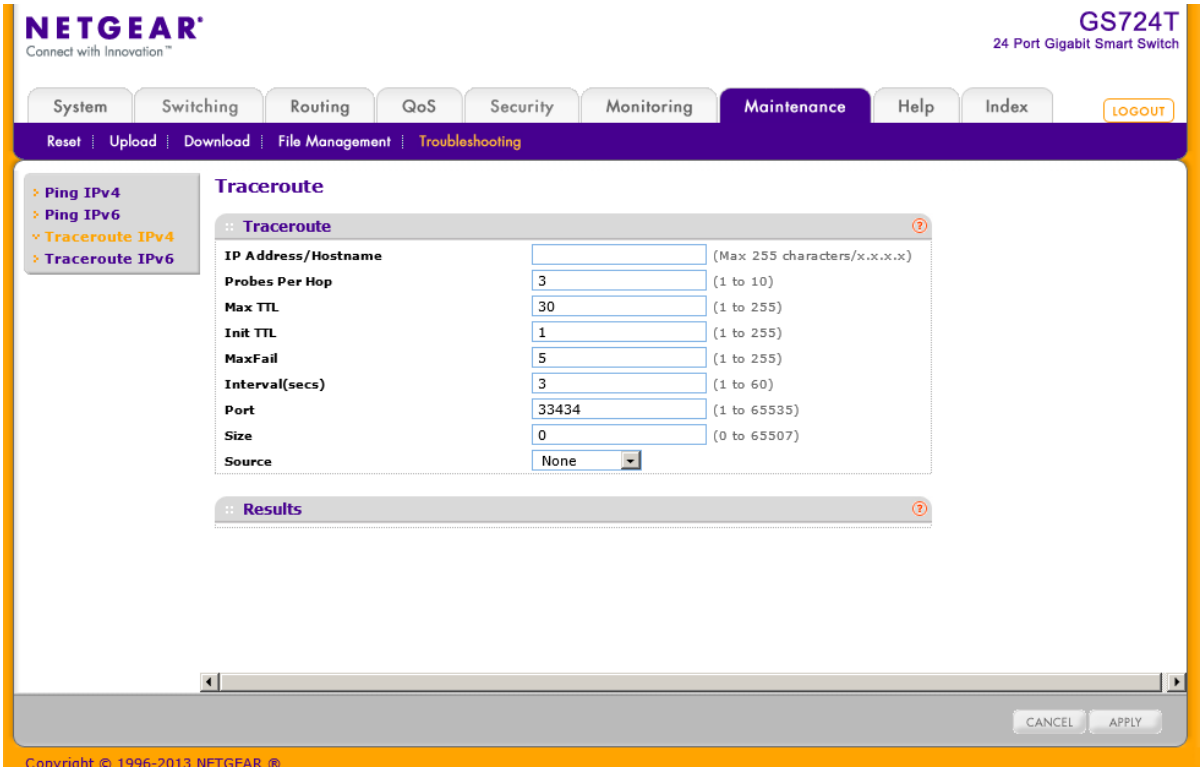
3. **IPv6 Address/Hostname**：Ping 送信をしたいデバイスの IPv6 アドレスあるいはホスト名を記入します。
4. 以下の設定をすることもできます。
   - **Count**：送信する Ping の数。1-15。
   - **Interval**：Ping の送信間隔（秒）。1-60。
   - **Datagram Size**：Ping パケットサイズ。0-65507。
   - **Source**：Ping を送信する送信元を選択します。
     - **None**：デフォルトの送信インターフェース。
     - **IP Address**：IP アドレス。送信元 IP アドレスを入力する欄が表示されます。
     - **Interface**：送信するインターフェースを選択します。
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。

トレースルート IPv4（Traceroute IPv4）

Traceroute ユーティリティを使ってリモート宛先までの IPv4 パケットの経路を確認することができます。

IPv4 アドレスまたはホストまでの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. IP Address/Hostname：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。0-65507 の範囲。
   - Source：Ping を送信する送信元を選択します。
     - None：デフォルトの送信インターフェース。
     - IP Address：IP アドレス。送信元 IP アドレスを入力する欄が表示されます。
     - Interface：送信するインターフェースを選択します。

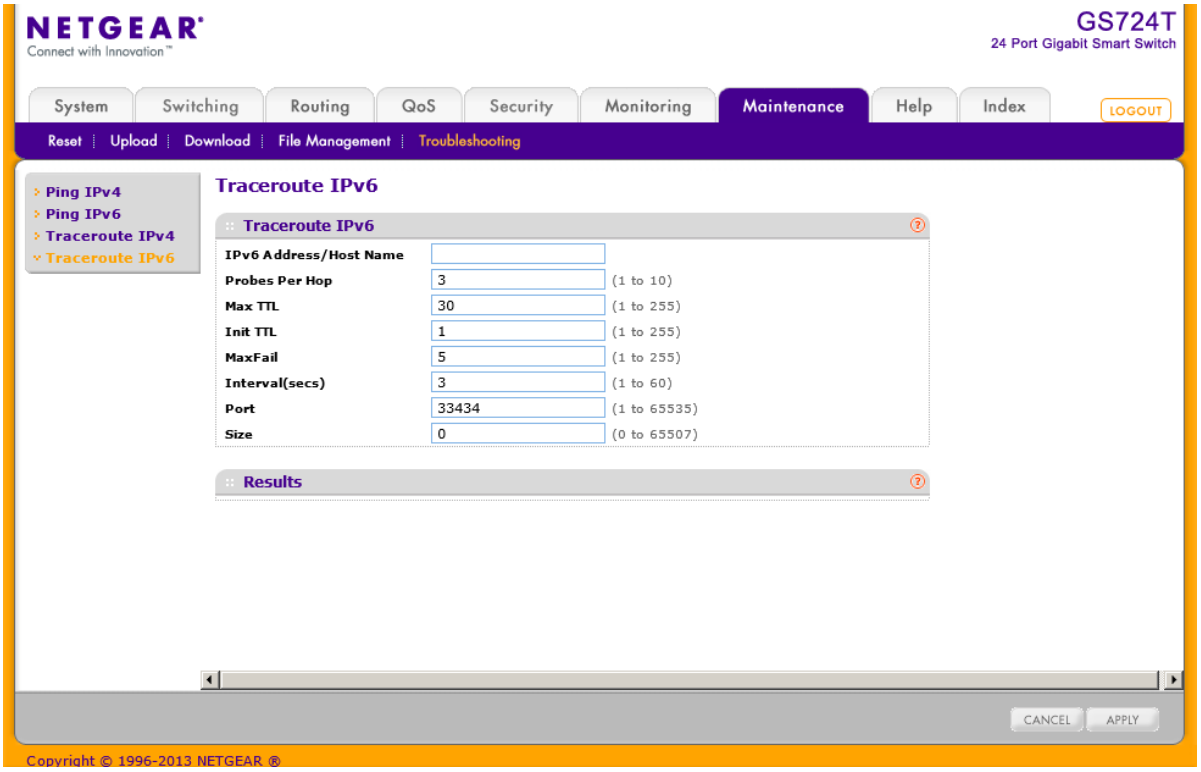
4. Cancel ボタンをクリックして操作を停止します。
5. Apply ボタンをクリックして Traceroute を開始します。結果は Results 欄に表示されます。

トレースルート IPv6（Traceroute IPv6）

Traceroute ユーティリティを使ってリモート宛先までの IPv6 パケットの経路を確認することができます。

IPv6 アドレスまたはホストまでのトレースルートを設定する

1. Maintenance > Troubleshooting > Traceroute IPv6 を選択して Traceroute IPv6 ページを表示します。



2. IPv6 Address/Hostname：宛先の IPv6 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。0-65507 の範囲。
- **Source**：Ping を送信する送信元を選択します。
  - **None**：デフォルトの送信インターフェース。
  - **IP Address**：IP アドレス。送信元 IP アドレスを入力する欄が表示されます。
  - **Interface**：送信するインターフェースを選択します。

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 **Results** 欄に表示されます。

トラブルシューティングチャート（Troubleshooting Chart）

トラブルの症状、原因、解決方法の表を以下に示します。

症状	原因	解決方法
電源 LED が消えている。	電源が入力されていません。	スイッチの電源コンセントの間の電源コード、コネクターを確認します。
デバイスとの間をイーサネットケーブルで接続したがポートの LED が点灯しない。	ポート接続が動作していない。	• コネクターがスイッチとデバイスのポートにしっかり接続されているかを確認する。 • イーサネット標準に対応したケーブルを適切に使用しているかを確認する。 • 他のデバイスと接続してデバイスが故障しているかどうかを確認する。
ファイル転送が遅い。	スイッチとデバイスのデュープレックスの不一致（全二重と半二重）	Autonegotiation 同士、あるいは固定設定になるように設定します。
セグメントまたはデバイスがネットワークの一部として認識されない。	一部のデバイスが適切に接続されていない、あるいはケーブルがイーサネット標準に準拠していない。	接続が正しいかを確認する。
Link/ACT LED が連続的に点滅していて、ネットワークが利用できない。	ネットワークループが発生している。	ループ部分を切断します。

ハードウェア仕様とデフォルト設定

スイッチ仕様（Switch Specifications）

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。

スイッチ仕様とパフォーマンス

機能	仕様
GS748T-500AJS インターフェース	10/100/1000 Base-T 46 ポート SFP/R-45 (10/100/1000 Base-T/1G/100M SFP) 2 ポート 1G SFP 2 ポート
GS724T-400AJS インターフェース	10/100/1000 Base-T 24 ポート 1G SFP 2 ポート
GS716T-300AJS インターフェース	10/100/1000 Base-T 16 ポート 1G SFP 2 ポート
フラッシュメモリー	32 MB
SRAM サイズとタイプ	128 MB DDR2 SDRAM
スイッチング能力	全パケットサイズでノンブロッキング、ワイヤースピード
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	16000

スイッチ機能とデフォルト（Switch Features and Defaults）

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）	8	事前設定
802.1D spanning tree	1	無効
802.1w RSTP	1	無効
802.1s spanning tree	4 インスタンス	無効
固定 802.1Q タギング	256	VID = 1 最大メンバーポート数はスイッチの全ポート数と同じ。
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

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	8	N/A
802.1p	1	有効
DSCP	1	無効
レートリミット	全ポート	無効

セキュリティ(Security)

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、IPv6 ACL と共有)	全 MAC アドレス許可

IP ACL	100 (IPv6 ACL、MAC ACL と共有)	全 IP アドレス許可
IPv6 ACL	100 (IP ACL、MAC ACL 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

システム管理

機能	サポート単位	デフォルト
Web マルチセッション	4	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	有効
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
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
スタティックルート数	32	N/A
Number of routed VLANs	15	N/A
Number of ARP Cache entries	512	N/A
Number of DHCP snooping bindings	8K	N/A
Number of DHCP static entries	1024	N/A
MLD Snooping	N/A	N/A
Protocol and MAC-based VLAN	N/A	N/A
Dynamic ARP Inspection	N/A	Disabled
Multiple VLAN Registration (MVR)	N/A	Disabled