

---

---

---

---

---

CentreCOM®  
**8216FXL/SC・8224XL・9006SX/SC**

---

# 追加機能マニュアル

# はじめに

本書は、CentreCOM 8216FXL/SC、CentreCOM 8224XL、CentreCOM 9006SX/SC (以下、8216FXL/SC、8224XL、9006SX/SC)のオペレーションマニュアルに記載されていない追加機能について説明したものです。

各機能と対応ソフトウェアバージョンについては下表をご覧ください。  
ソフトウェアの最新バージョンは弊社ホームページよりダウンロード可能です。  
<http://www.allied-telesis.co.jp>

また、各製品ごとのリリースノート、およびオペレーションマニュアルもあわせてご覧ください。

機能	機種	8216FXL/SC	8224XL	9006SX/SC
ポートセキュリティ		2.0.0J 以降	2.0.0J 以降	2.0.0J 以降
RRPスヌーピング		2.0.0J 以降	2.0.0J 以降	2.0.0J 以降
マルチプルVLAN		2.0.0J 以降	2.0.0J 以降	
MACテーブルの消去		2.0.0J 以降	2.0.0J 以降	2.0.0J 以降
マネージメントポートの VLAN割当て		2.0.0J 以降	1.2.12J 以降	1.0.5J 以降
IGMPスヌーピング エージングタイム		マニュアル記載済	1.2.9J 以降	マニュアル記載済
プライオリティウエイト		マニュアル記載済	1.2.4J 以降	マニュアル記載済
VLAN ID設定値の拡大		2.0.0J 以降	2.0.0J 以降	2.0.0J 以降
トランキンググループの複数設定		2.0.0J 以降	2.0.0J 以降	
メニュー構造の変更		2.0.0J 以降	2.0.0J 以降	2.0.0J 以降

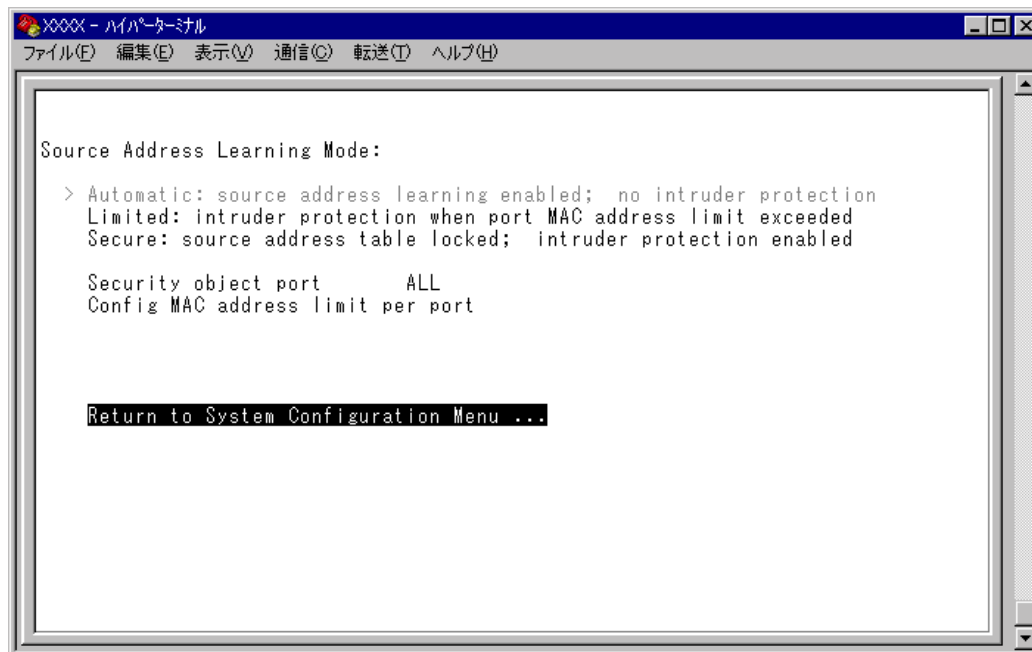
## 目次

はじめに .....	2
ポートセキュリティ .....	3
RRP スヌーピング .....	9
マルチプル VLAN .....	12
MAC テーブルの消去 .....	17
マネージメントポートの VLAN 割当て .....	18
IGMP スヌーピングエージングタイム .....	19
プライオリティウエイト .....	20
その他の追加項目 .....	21
VLAN ID 設定値の拡大 .....	21
トランキンググループの複数設定 .....	21
メニュー構造の変更 .....	21

# ポートセキュリティ

## Security/Source Address Table

[ Main Menu ] -> [ System configuration ] -> [ Security/Source Address Table ] とすすみ、次の画面を表示します。



この画面では、登録済みのMACアドレスと異なるMACアドレスを持つ端末が接続された場合に、不正進入とみなしてパケットをフィルタリングするセキュリティ機能についての設定を行います。

通常、MACアドレステーブルは継続的に更新される状態で使用しますが、このオプションを使用すると、MACアドレステーブルの学習機能を停止することができます。これにより、MACアドレステーブルに登録されていないMACアドレスを持つパケットをフィルタリングし、端末を特定のMACアドレスに制限します。セキュリティ機能の対象となるポートの指定ができ、未登録のMACアドレスを検出してセキュリティが機能した場合に、システムに対してどのような処理を行わせるかを設定するオプションもあります。各オプションを上から順に説明します。

---

### Source Address Learning Mode: Automatic/Limited/Secure

MACアドレステーブルを学習機能モードにするか、セキュリティ機能モードにするかを設定します。デフォルトはAutomaticで、セキュリティ機能は無効となっています。

#### Automatic

MACアドレステーブルは通常の学習機能モードになります。

このモードでは、未学習のMACアドレスを持つ端末からパケットを受信するたびに、MACアドレスと受信ポートの対応を登録します。

また、エージング機能によって、一定時間内にパケットの送信がない端末の情報はMACアドレステーブルから自動的に削除されます。

#### Limited

条件付きのセキュリティ機能モードになります。

このモードでは、あらかじめ設定しておいた数までMACアドレスを学習し、学習済みのMACアドレス以外のMACアドレスはフィルタリングします。

オプション選択後、MACアドレステーブルは一度消去され、各ポートごとに設定された数までMACアドレスを学習します。学習されたMACアドレス以外のMACアドレスを持つパケットは不正進入とみなし、MACアドレスの登録を行いません。

また、設定数まで学習されたMACアドレスは、エージング機能によって削除されません。MACアドレステーブルから削除する場合は、システムをリセットします。

#### Secure

セキュリティ機能モードになります。


このモードでは、オプション選択時にMACアドレステーブルがロックされた状態となり、その時点で学習済みのMACアドレス以外のMACアドレスはフィルタリングします。

オプション選択時に学習済みのMACアドレスは、エージング機能やシステムのリセットによって削除されません。MACアドレステーブルから削除する場合は、一度 [ Automatic ] を選択します。

---

### Security object port

セキュリティ機能モードの対象となるポートを指定します。デフォルトはALLです。セキュリティ機能モードを特定のポートで動作させる場合は、Limited/Secureを選択する前に、あらかじめこのオプションで対象ポートを設定しておきます。対象外のポートは [ Automatic ] と同様、通常の学習機能モードとなります。

 本機能では、登録されたMACアドレスを持つ端末のパケットは、Security object port で指定されているすべてのポートで受信します。

---

### Config MAC address limit per port

セキュリティ機能モードを Limited にした場合、ポートごとに MAC アドレスの最大登録数を設定します。設定数まで学習された MAC アドレス以外の MAC アドレスに対してはセキュリティ機能が動作し、MAC アドレスの登録を行いません。デフォルトは  $\alpha$  (ゼロ) で、MAC アドレスの最大登録数は設定されません。

---

### Intruder Protection: Transmit an SNMP Trap/No SNMP Trap


セキュリティ機能モード時に未登録の MAC アドレスを検出した場合、SNMP マネージャーに Trap メッセージを送信するかどうかを設定します。デフォルトは No SNMP Trap です。

#### Transmit an SNMP Trap

未登録の MAC アドレスを検出した場合に、SNMP マネージャーに対して Trap メッセージを送信します。

Trap メッセージには、SNMP MIB 情報が含まれているため、不正進入が発生したポート、および不正進入とみなされた端末の MAC アドレスを確認することができます。

このオプションを使用する場合は、あらかじめ IP パラメーターの設定を行っておく必要があります。

 「オペレーションマニュアル / IP パラメーター」

#### No SNMP Trap

未登録の MAC アドレスを検出した場合も、SNMP マネージャーに対して Trap メッセージは送信しません。

---

### Intruder Protection: Disable the port/Port state unchanged


セキュリティ機能モード時に未登録の MAC アドレスを検出した場合、ポートを使用不可の状態にするかどうかを設定します。デフォルトは Port state unchanged です。

#### Disable the port

未登録の MAC アドレスを検出した場合に、不正進入が発生したポートを自動的に切り離し、送受信ができない状態にします。



不正進入によって使用不可の状態 (Disabled) となったポートは、手動で使用可の状態 (Enabled) に戻さない限り、使用不可のままとなりますので、ご注意ください。

 「オペレーションマニュアル / 2 ポート設定」

#### Port state unchanged

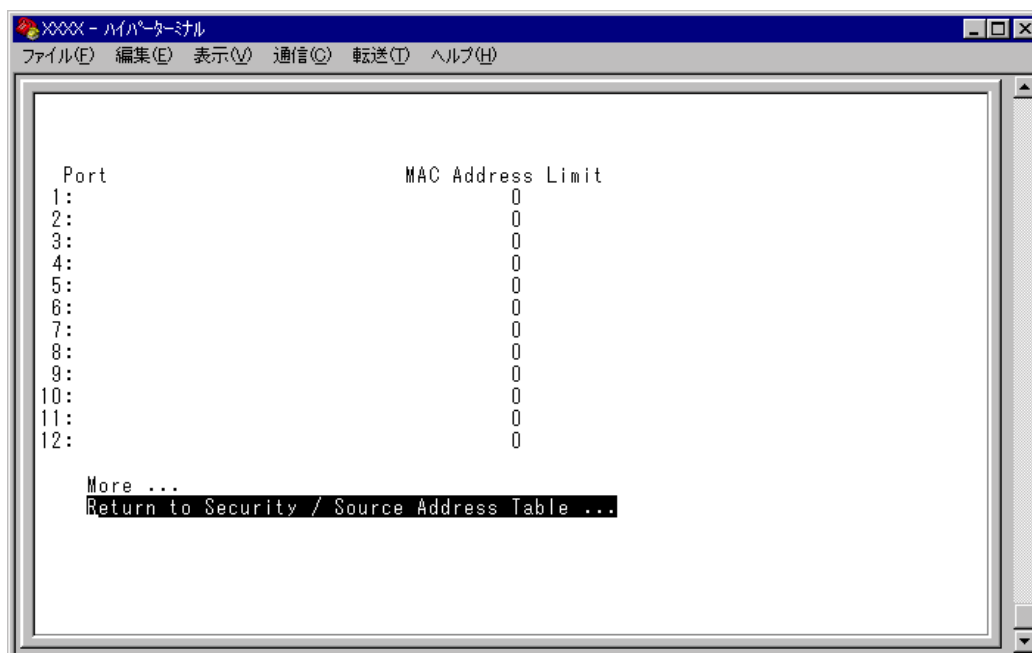
未登録の MAC アドレスを検出した場合も、ポートの切り離しは行わず、ステータスは変わりません。

## ▶ Limited/Secure モードの設定

- 1 [ Security object port ] オプションで、Limited/Secure モードの対象となるポートを指定します。  
Sを入力して、Security object port の入力フィールドにカーソルを移動します。
- 2 **[Enter]** キーを押して、「->」プロンプトを表示します。
- 3 「->」プロンプトに続けて半角英数字を入力し、**[Enter]** キーを押します。

### ポートの指定方法

- 連続しない複数のポートを設定する場合は、「1,3,5」のようにカンマで区切って指定します。
  - 連続する複数のポートを設定する場合は、「1-5」のようにハイフンを使って指定します。
  - すべてのポートを設定する場合は「all」と入力します。
  - 1行以内で入力してください。
- 4 Limitedモードの場合は、[ Config MAC address limit per port ] オプションで、ポートごとに MAC アドレスの最大登録数を設定します。  
Cを入力して**[Enter]** キーを押すと、次の画面が表示されます。



- 5 ポート番号を選択して、「Port MAC Address Limit Menu」画面を表示し、[ MAC Address Limit ( Apply this limit to all ports ) ] オプションの設定を行います。



---

### MAC Address Limit

MACアドレスの最大登録数を設定します。

- 1 **[M]**を入力して、入力フィールドにカーソルが移動します。
- 2 **[Enter]**キーを押すと「->」プロンプトが表示されます。  
「->」プロンプトに続けて0～255の半角数字を入力し、**[Enter]**キーを押します。0（ゼロ）に設定した場合は、Limitedモードは無効となり、MACアドレステーブルは通常の学習機能モードとなります。ただし、学習済みのMACアドレスはエイジング機能によって削除されません。

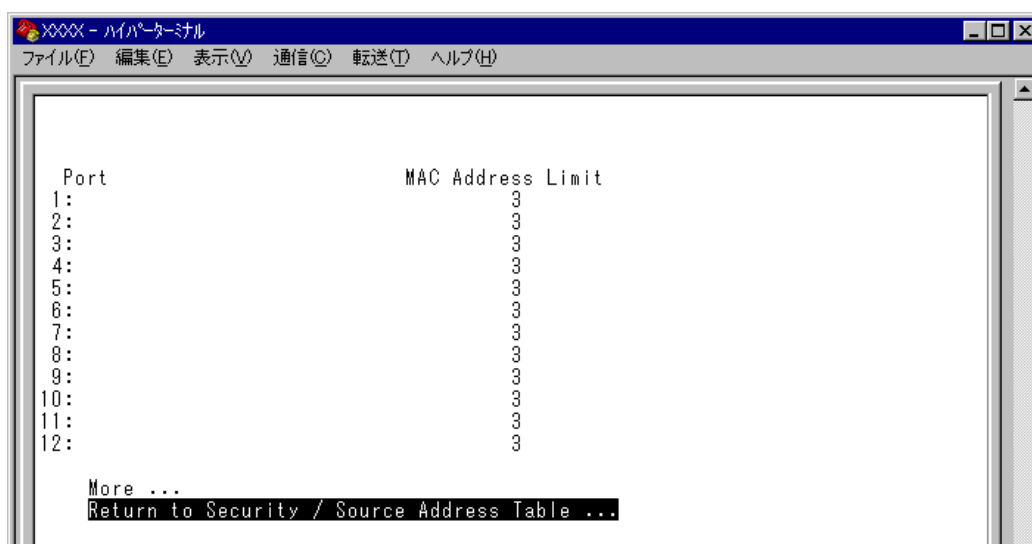
---

### Apply this limit to all ports

現在選択しているポートの最大登録数を、他のすべてのポートに適用します。

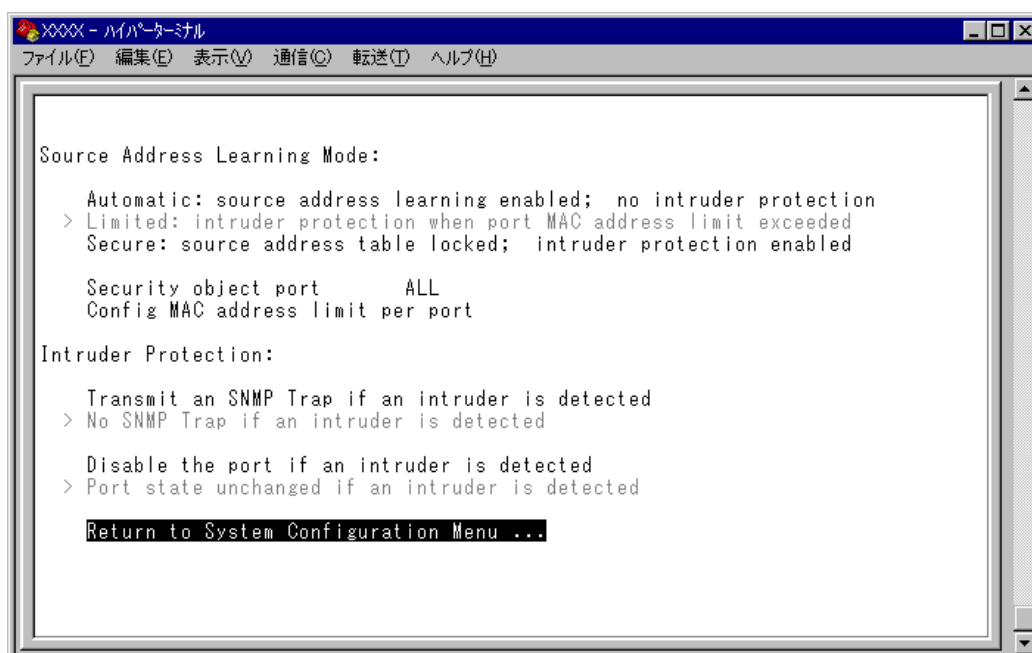
**[A]**を入力後、**[Enter]**キーを押します。

前の画面に戻り、MACアドレスの最大登録数がすべてのポートに適用されていることを確認します。



## ポートセキュリティ

- i** ▶ MACアドレスの最大登録数の設定は、Security object portで対象ポートとして設定したポートに対してのみ有効となります。
- 6 「Source Address Learning Mode:」で、Secureモードの場合は[ Secure ]を、Limitedモードの場合は[ Limited ]を選択して、セキュリティ機能モードを有効にします。
  - 7 [ Limited/Secure ] オプションを選択すると、「Intruder Protection:」の追加オプションが表示されます。未登録のMACアドレスを検出したときに、SNMPマネージャーにTrapメッセージを送信する場合は[ Transmit an SNMP Trap ]を、ポートを使用不可の状態にする場合は[ Disable the port ]を選択します。



- !** ▶ ポートセキュリティ機能と以下の機能を同一ポートに設定することはできません。

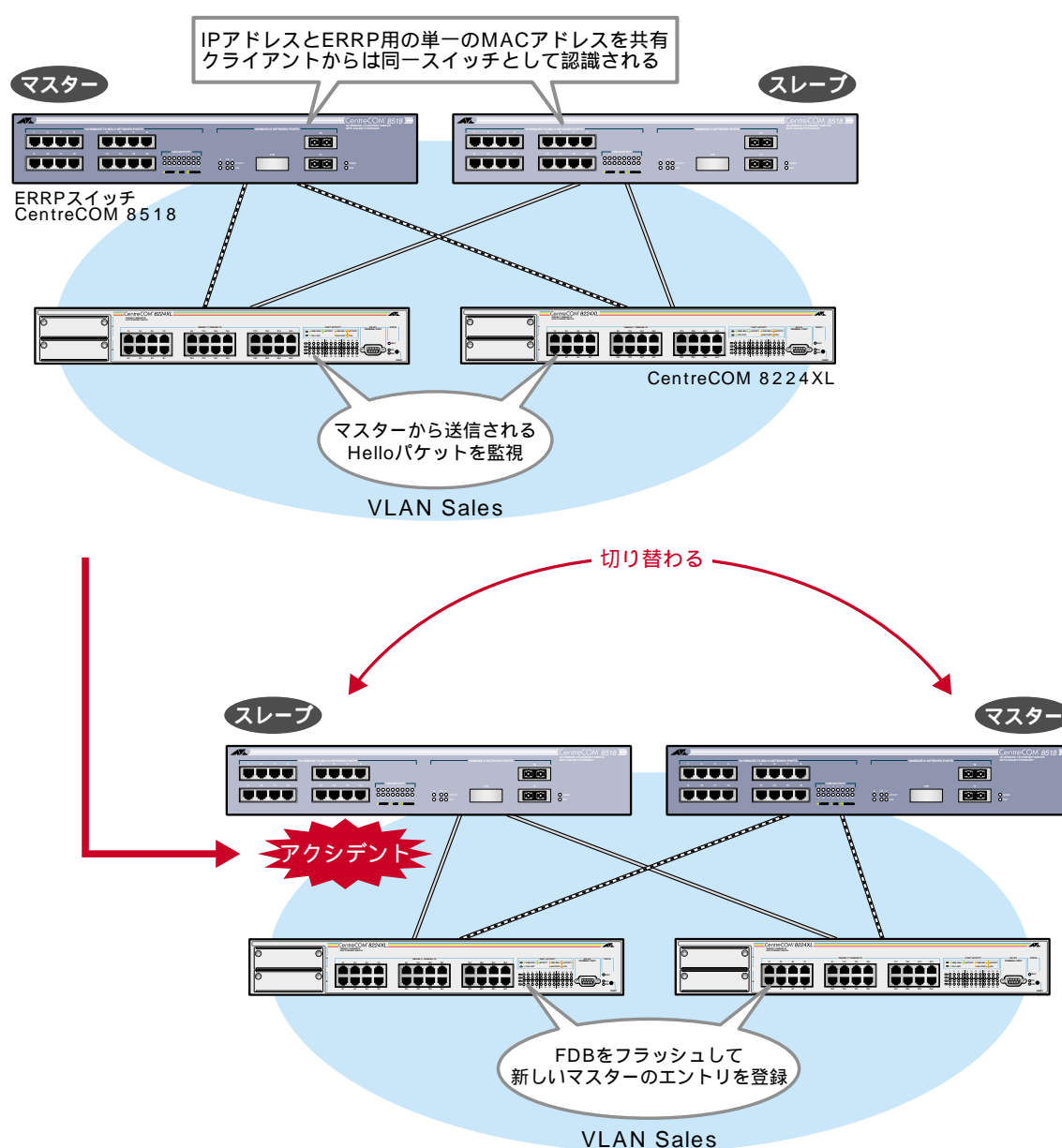
ポートランキング機能( Port Trunking in the 10/100M Speed Port )  
RRP スヌーピング機能( Router Redundancy Protocol Snooping )  
マルチプル VLAN 機能( Multiple Vlan Mode )



# RRP スヌーピング

## Router Redundancy Protocol Snooping

本製品と弊社CentreCOM 8500シリーズなどを連携させ、高速な冗長性を実現するためのERRP(Enterprise Router Redundancy Protocol)に関する設定を行います。本製品をERRPおよび同等機能を持つ製品の下位に配置し、接続ポートにRRPスヌーピングを設定すると、本製品はマスタールーターから定期的送信されるHelloパケットをVLANごとに監視し、どのポートがマスターかを記憶します。マスタールーターに障害が発生して、スレーブに切り替わると、システム全体のフォワーディングデータベース(FDB)をフラッシュしてスレーブルーターのエントリがすぐに登録されるようにします。これによって、ERRPに対応していないスイッチを下位に接続するよりも、はるかに短い時間で通信を再開することができます。



## RRP スヌーピング

前ページの図は、VLAN Sales 内において、本製品を ERRP イネーブルな 2 台の CentreCOM 8518 (以下、8518) に対して、それぞれ RRP Snooping を設定したポートを用いて接続した例です。

2 台の 8518 は互いに ERRP Hello パケット (実際は、規定のソース MAC アドレス) を交換し、どちらがマスターになるかを決定します。マスターになった 8518 は VLAN Sales に対してスイッチング (ルーティング) のサービスを提供します。一方、スタンバイ (スレーブ) 側の 8518 はまったくパケットの転送を行わず、これによりブリッジループを回避します。

本製品は 8518 の間で交換される ERRP Hello パケットを常に監視しており、マスターの障害発生を検知するとただちに自らのフォワーディングデータベース (FDB) をフラッシュして、新しいマスターのエントリがすぐに登録されるようにします。これにより 4 ~ 9 秒という高速な切り替えを実現します。

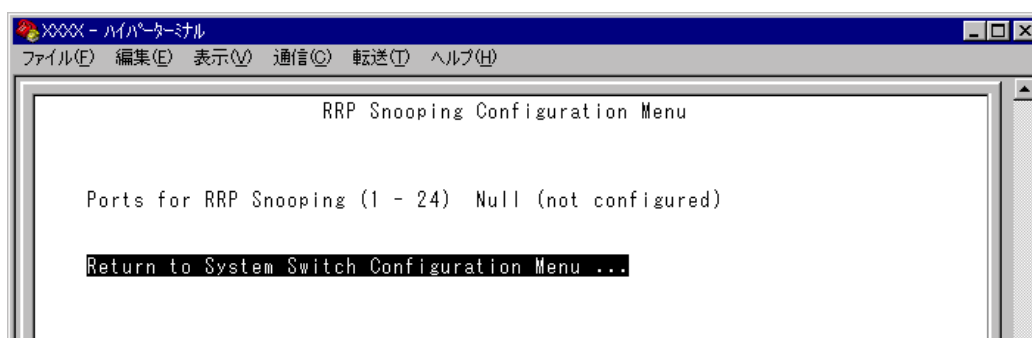
本製品がスヌーピングする Hello パケットのソース MAC アドレスは下記の通りです。

```
00:e0:2b:00:00:80  
00:a0:d2:eb:ff:80
```

左の図は 1 つの VLAN に対する多重化の例ですが、複数の VLAN に対して RRP スヌーピングを設定することも可能です。

### ▶ RRP スヌーピング設定

- 1 [ Main Menu ]->[ System configuration ]->[ System Switch configuration ]->[ Router Recuncancy Protocol Snooping (RRPS) ] とすすみ、次の画面を表示します。

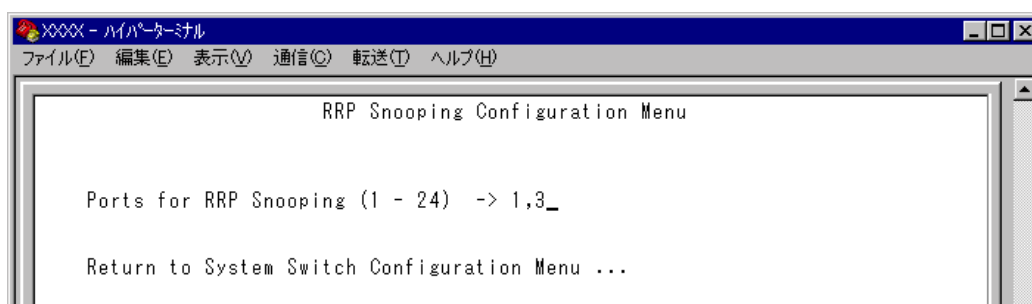


- 2 **[P]** を押して、Ports for RRP Snooping の入力フィールドにカーソルを移動します。
- 3 **[Enter]** キーを押して「->」プロンプトを表示します。

- 4 「->」プロンプトに続けて、RRP スヌーピングを設定するポートを入力し、**[Enter]** キーを押します。

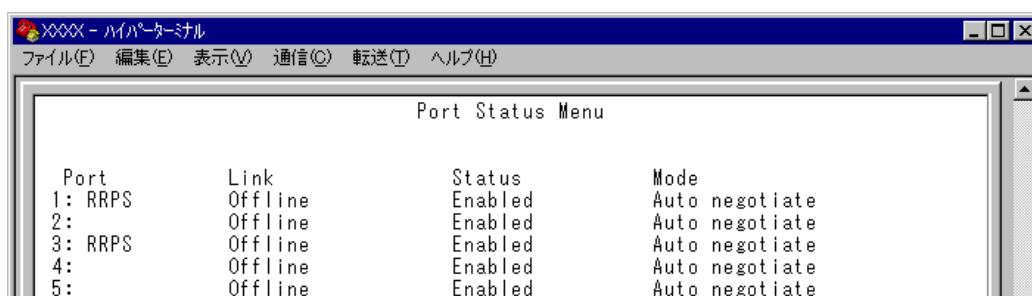
ポートの指定方法

- 連続しない複数のポートを設定する場合は、「1,3,5」のようにカンマで区切って指定します。
- 連続する複数のポートを設定する場合は、「1-5」のようにハイフンを使って指定します。
- すべてのポートを設定する場合は「all」と入力します。
- 1ポートのみの入力はできません。
- 1行以内で入力してください。



RRP スヌーピングポートを「Null (not configured)」に戻す場合は、「->」プロンプトに続けて(すでに設定してあるポート番号の上から) **[スペース]**を入力し、**[Enter]** キーを押します。

**i** RRP スヌーピングを設定した場合は、ポート名として「RRPS」が自動的に登録されます。



**!** RRPスヌーピング機能と以下の機能を同一ポートに設定することはできません。

- ポートセキュリティ機能 (Security/Source Address)
- ポートトラッキング機能 (Port Trunking in the 10/100M Speed Port)
- マルチプル VLAN 機能 (Multiple Vlan Mode)
- スパニングツリー機能 (Port spanning tree configuration)

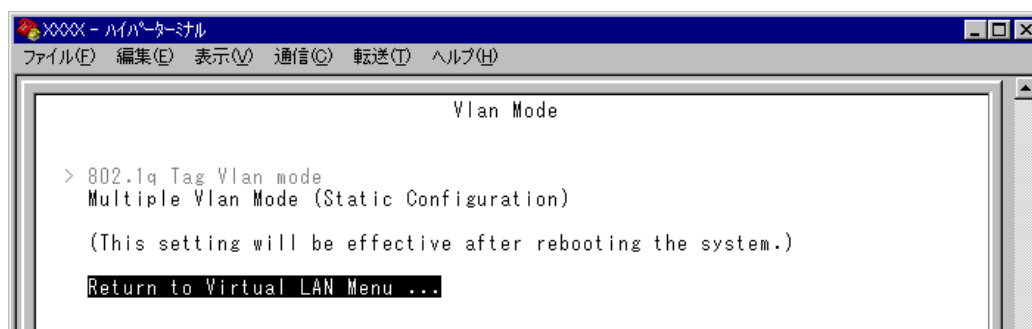
**!** 必要なポート以外に RRP スヌーピングを設定しないでください。

# マルチプル VLAN

## Multiple Vlan Mode

特定のポートを複数のVLANに所属させることにより、インターネットマンションなどのネットワーク構成に対応するマルチプルVLANの設定方法、および仕様と用例について説明します。

[ Main Menu ] -> [ Virtual LANs/QoS ] -> [ Change The Vlan Mode( 802.1Q Vlan or Multiple Vlan ) ] とすすみ、次の画面を表示します。



---

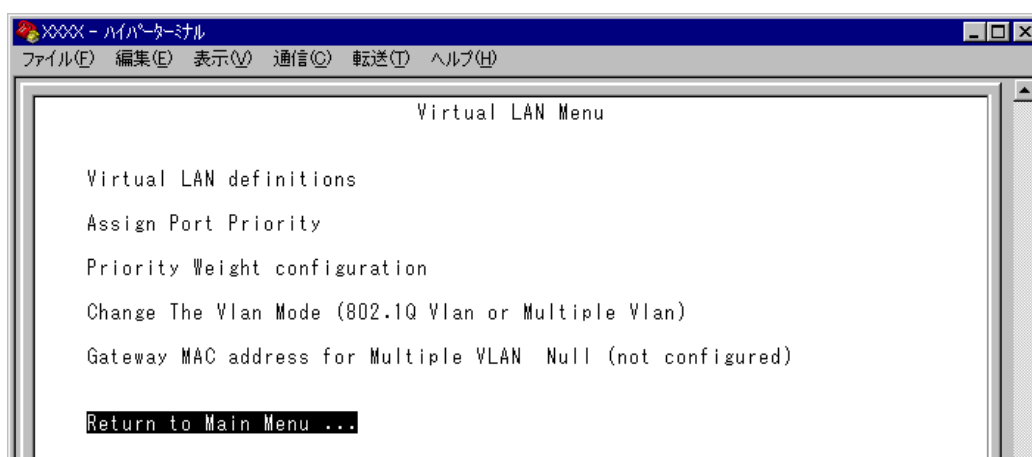
### 802.1Q Tag Vlan mode/Multiple Vlan Mode

VLANのモードを802.1QタグVLANにするか、マルチプルVLANにするかを設定します。デフォルトは802.1Q Tag Vlan mode です。

802.1Q Tag Vlan mode  
802.1Q タグ VLAN モードになります。

#### Multiple Vlan Mode

マルチプルVLANモードになります。このオプションを選択すると、システムは自動的にマルチプルVLAN対応のVLAN構成に固定設定されます。設定はシステムのリセット後に有効となります。リセット後、[ Virtual LANs/QoS ] メニューは次のような構成になります。Assign Port Priority、Priority Weight configuration オプションについては各オペレーションマニュアル( Priority Weight configuration については本マニュアルにも記載 )を参照してください。



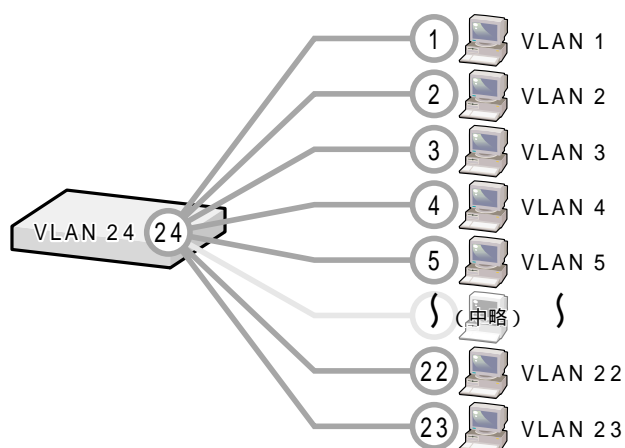
### 本製品マルチプル VLAN の仕様

Multiple Vlan Mode を選択すると、自動的にマルチプル VLAN 対応の固定 VLAN が生成されます。VLAN は物理ポート数分生成され、最終ポートがインターネット接続用のポートとしてすべてのVLANに所属します。これにより、インターネットマンションなどにおいて、部屋同士のセキュリティを確保しつつ、各部屋からのインターネット接続を実現します。

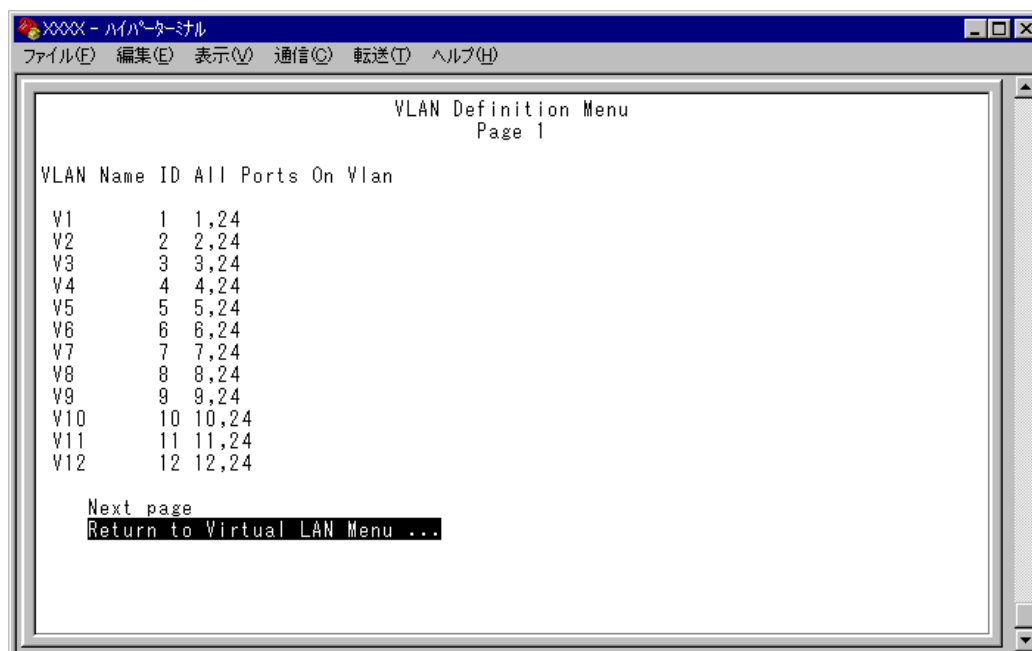
下図は8224XL( 拡張モジュールなし )で、マルチプルVLANを設定した場合のVLAN構成です。

マルチプルVLANモード時のVLAN構成  
(最終ポートがポート24の場合)

VLAN名(VLAN ID)	所属ポート
VLAN 1( 1 )	1, 24
VLAN 2( 2 )	2, 24
VLAN 3( 3 )	3, 24
VLAN 4( 4 )	4, 24
VLAN 5( 5 )	3, 24
:	:
:	:
VLAN 22( 22 )	22, 24
VLAN 23( 23 )	23, 24
VLAN 24( 24 )	ALL



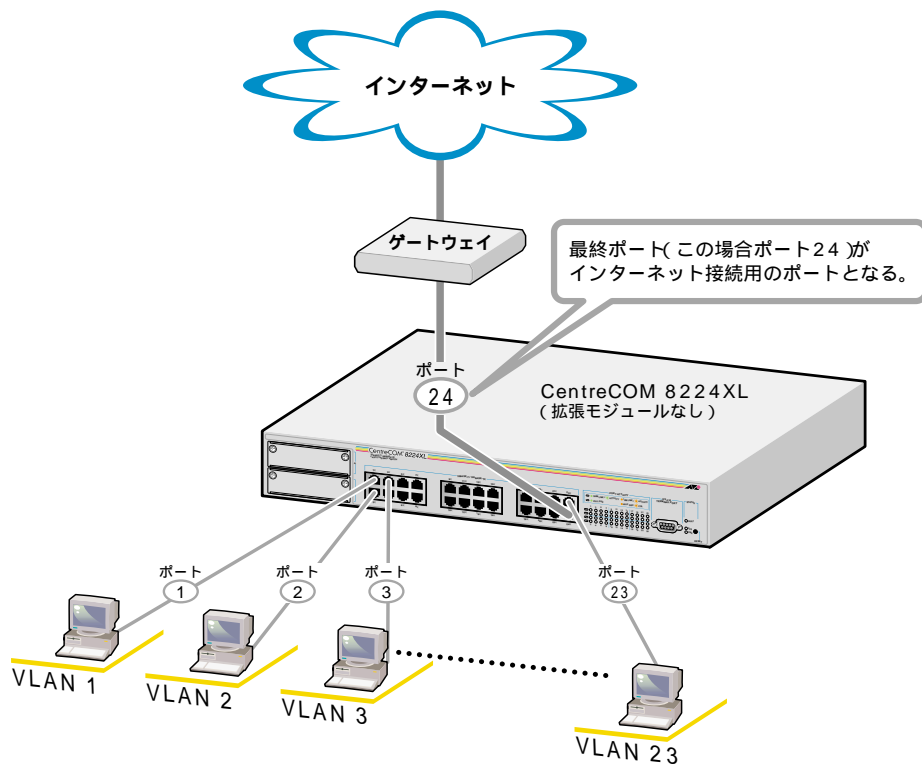
VLAN 構成は Virtual LAN definition メニューで確認することができます。



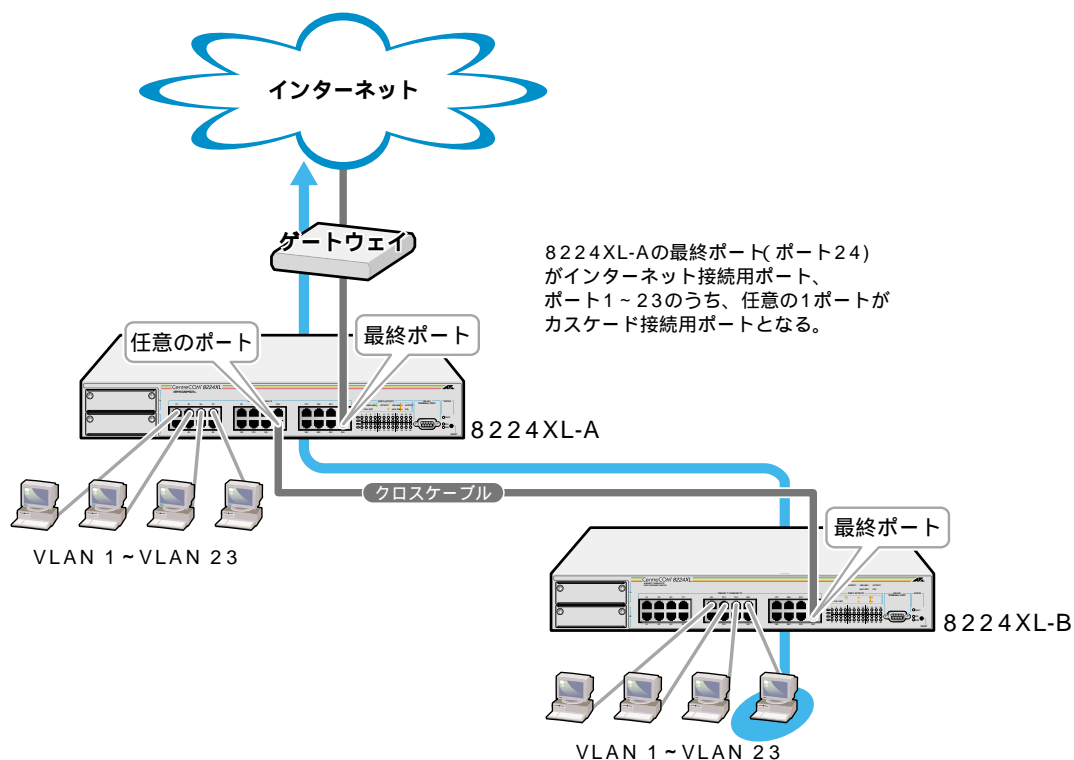
# マルチプルVLAN

マルチプルVLANを使用したネットワーク構成例を8224XL(拡張モジュールなし)をもとに示します。

## 例 1 スタンドアローンの場合



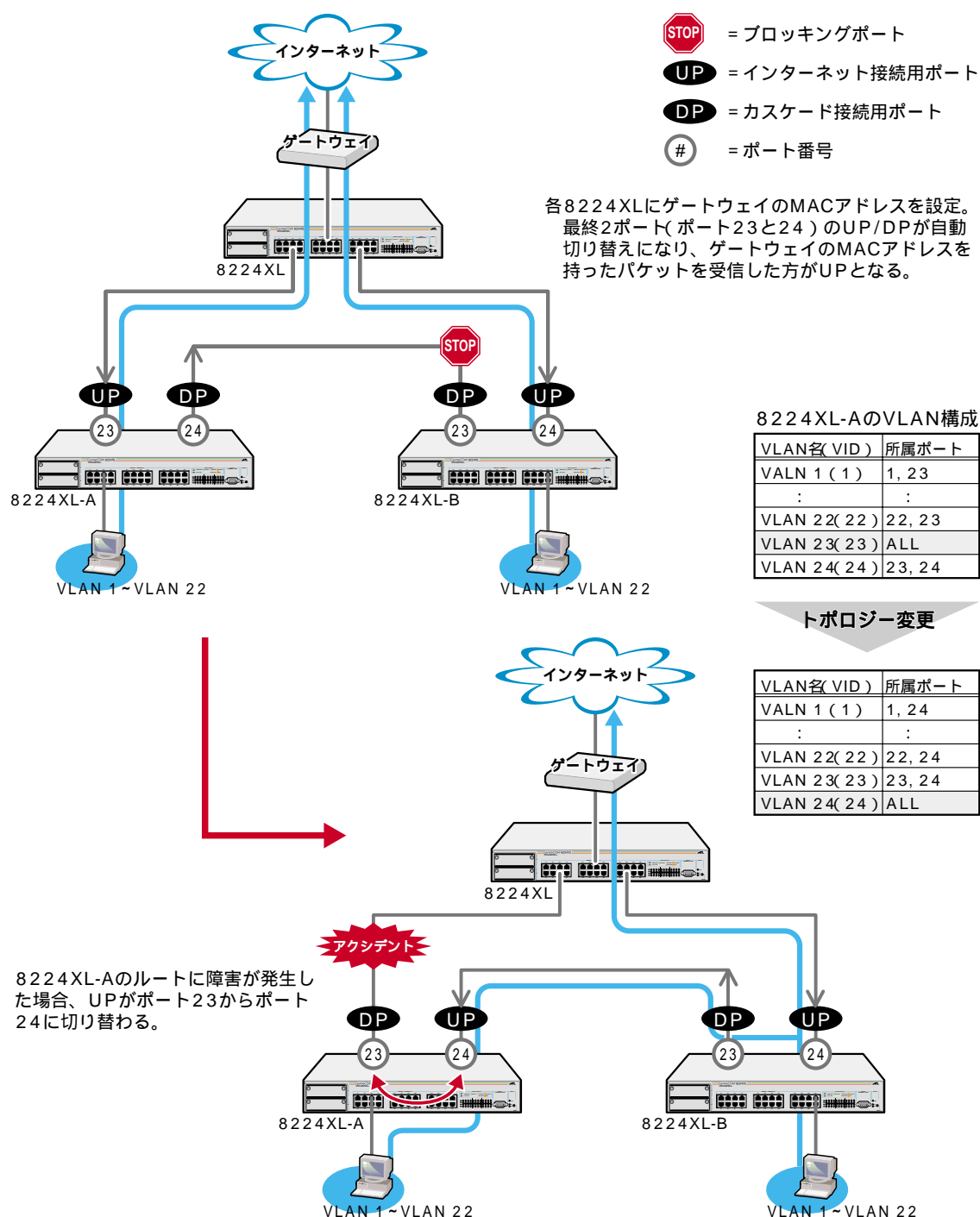
## 例 2 カスケード接続の場合



### 例 3 スパニングツリー構成の場合

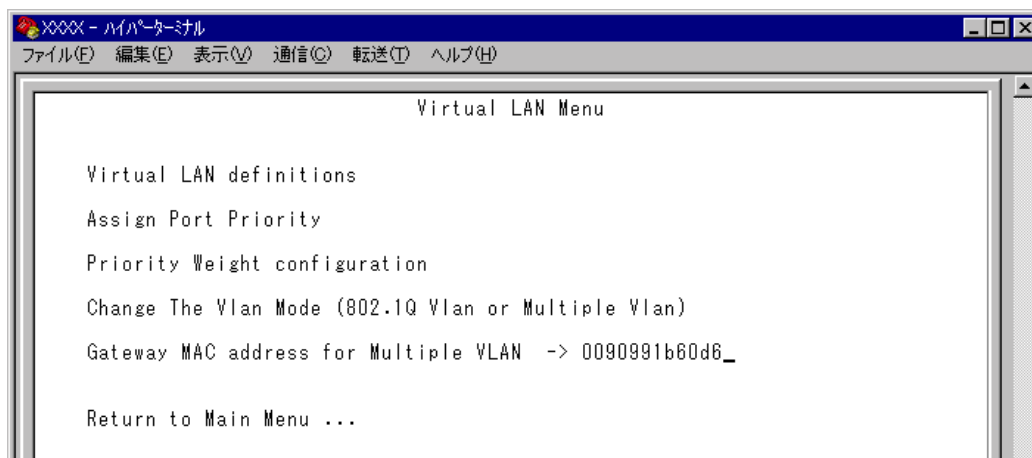
下図のようなスパニングツリー構成を組む場合は、各 8224XL にルーター(ゲートウェイ)の MAC アドレスを設定することにより、最終 2 ポートをインターネット接続用(Up Port)とカスケード接続用(Down Port)の自動切替ポートとします。ルーターの MAC アドレスを持つパケットを受信したポートが Up Port となる仕様により、トポロジの変更で Down Port 側からルーターの MAC アドレスを受信した場合、自動的に Up Port と Down Port が入れ替わり、VLAN 構成も変更されます。

参照「オペレーションマニュアル / 8 ブリッジ機能」



## ▶ ゲートウェイ MAC アドレスの設定

- 1 [ Main Menu ] -> [ Virtual LANs/QoS ] とすすみ、次の画面を表示します。



- 2 **G**を入力して、Gateway MAC address for Multiple VLANの入力フィールドにカーソルを移動します。
- 3 **Enter**キーを押して、「->」プロンプトを表示します。
- 4 「->」プロンプトに続けてXXXXXXXXXXXXXの形式で16進数を入力し、**Enter**キーを押します。

「Null (not configured)」に戻す場合は、「->」プロンプトに続けて(すでに設定してあるMACアドレスの上から)「000000000000」を入力し、**Enter**キーを押します。

**i**▶ 拡張モジュールを装着した場合も、モジュールのポートを最終ポートとしてマルチプルVLANに対応可能です。

**!**▶ インターネット接続用ポート以外のポートで、管理機能(SNMPやPingなど)を使用することはできません。

**!**▶ マルチプルVLAN機能と以下の機能を併用することはできません。

ポートランキング機能 (Port Trunking in the 10/100M Speed Port )  
ポートセキュリティ機能 (Security/Source Address )  
RRP スヌーピング機能 (Router Redundancy Protocol Snooping )



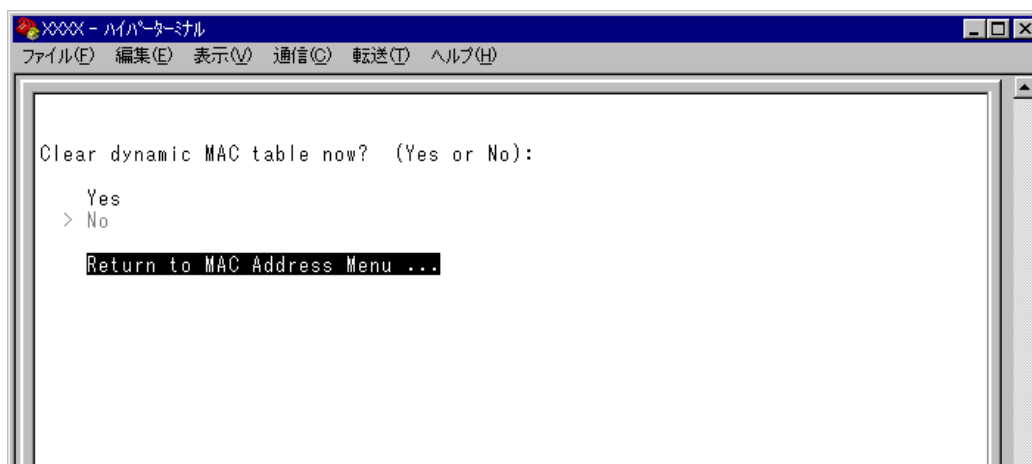
# MAC テーブルの消去

## Clear dynamic MAC table

ダイナミックに学習した MAC アドレスの登録をすべて消去します。

### ▶ MAC アドレスの消去

- 1 [ Main Menu ] -> [ MAC Address Table ] -> [ Clear dynamic MAC table ] とすすみ、次の画面を表示します。



- 2 次のオプションのどちらかを選択します。

---

### Yes/No

MAC アドレスの登録をすべて消去するかしないかを選択します。デフォルトは No で、この画面は常に No が選択された状態で表示されます。

Yes

MAC アドレスの消去が実行されます。

No

前の画面に戻ります。

# マネージメントポートの VLAN 割当て

## Assign Management Port To VLAN

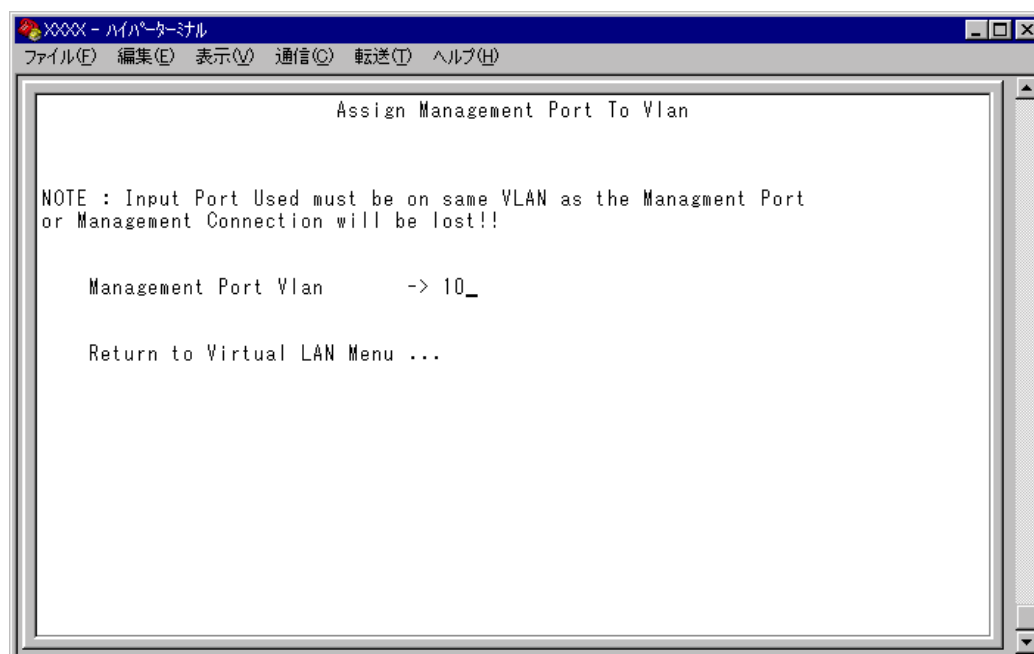
本製品は管理用のマネージメントポートを持っています。マネージメントポートは物理ポートではなく、例えば、本体にtelnetログインする場合に、ソフトウェア内部で処理される論理ポートです。

デフォルト設定では、マネージメントポートは「Default VLAN( ID = 1 )」に所属しています。Default VLAN以外のVLANにマネージメントポートを割り当てる場合に、このオプションであらかじめ定義された VLAN の ID 番号を設定します。

マネージメントポートと本体へのアクセスを行うポートは同一のVLANに属している必要があります。マネージメントポートと異なるVLANに属しているポートから本体にアクセスすることはできませんのでご注意ください。また、マネージメントポートを複数のVLANに所属させることはできません。

### ▶ マネージメントポートの VLAN 設定

- 1 [ Main Menu ] -> [ Virtual LANs/QoS ] -> [ Assign Management Port To VLAN ] とすすみ、次の画面を表示します。



- 2 **[M]**を入力して、既存の ID をハイライト表示します。
- 3 **[Enter]**キーを押して、「->」プロンプトを表示します。
- 4 「->」プロンプトに続けて、あらかじめ定義されたVLANのID番号を半角数字で入力します。

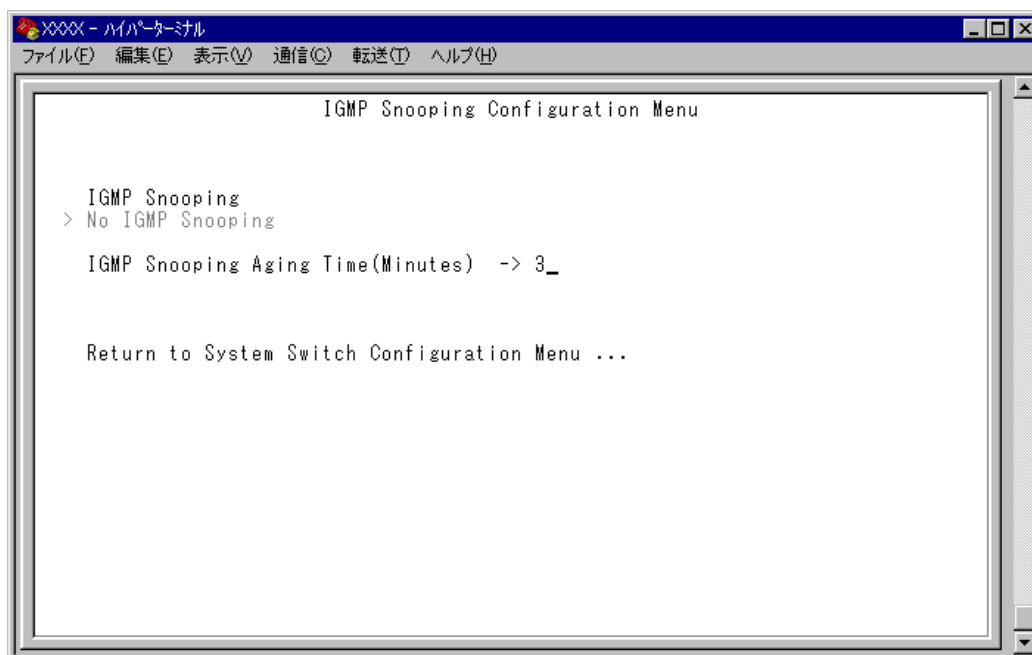
# IGMP スヌーピングエージングタイム

## IGMP Snooping Aging Time(Minutes)

IGMP パケット専用のエージングタイムを設定します。デフォルトは5(分)です。エージングタイムを設定すれば、IGMP スヌーピング機能が有効な場合、設定した時間内に IGMP パケット( レポート・メッセージ )の送信がないグループ・メンバーのポートは自動的に削除されます。

### ▶ IGMP スヌーピング エージングタイムの設定

- 1 [ Main Menu ]->[ System configuration ]->[ System Switch Configuration ]->[ IGMP Snooping configuration ] とすすみ、次の画面を表示します。
- 2 を複数回押して、IGMP Snooping Aging Time( Minutes )の入力フィールドにカーソルを移動します。



- 3 キーを押すと「->」プロンプトが表示されます。  
「->」プロンプトに続けて1～999(分)の半角数字を入力し、キーを押します。  
(ゼロ) または を入力して キーを押すと、この機能は無効となります。  
(登録されたマルチキャストパケット・ポートはシステムがリセットされるまで削除されません。)

# プライオリティウェイト

## Priority Weight configuration

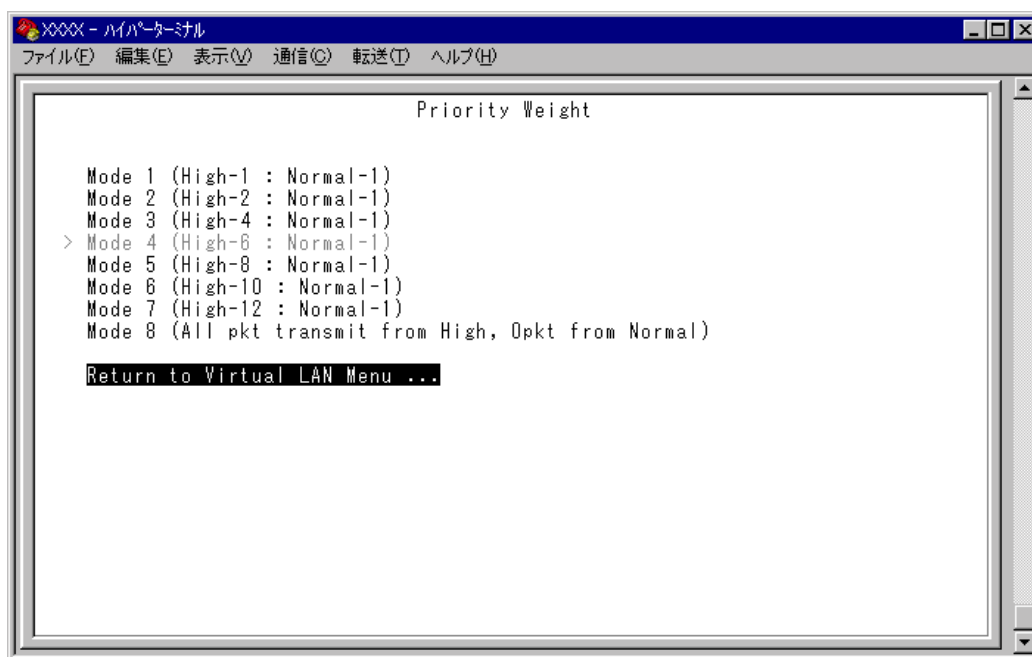
プライオリティキュー High と Normal の帯域保証の割合を 8 つのモードから選択します。デフォルトは Mode 4 ( High-6 : Normal-1 ) です。

Mode 1 ~ Mode 7 のカッコ内の表示、「High-N ( 1, 2, 4, 6, 8, 10, 12 ) : Normal-1」は、High プライオリティキューの packets を N 個送信した後、Normal プライオリティキューの packets を 1 個送信することを意味します。

「Mode 8 ( All pkt transmit from High, 0pkt from Normal )」は、High プライオリティキューの packets を全て送信した後、Normal プライオリティキューの packets を送信することを意味します。

### ▶ プライオリティウェイトの設定

- 1 [ Main Menu ] -> [ Virtual LANs/QoS ] -> [ Priority Weight configuration ] とすすみ、「Port Priority Configuration」画面からポート番号を選択し、次の画面を表示します。



- 2 **[M]** を複数回押して、選択する「Mode」へ移動し、**[Enter]** キーを押します。

## その他の追加項目

### VLAN ID 設定値の拡大

参照「オペレーションマニュアル / 7 バーチャル LAN」

VLAN ID の設定値は 2 ~ 2,047 でしたが、これを 2 ~ 4,094 としました。ただし、IGMP スヌーピング機能を使用している場合は、2 ~ 2,047 となります。

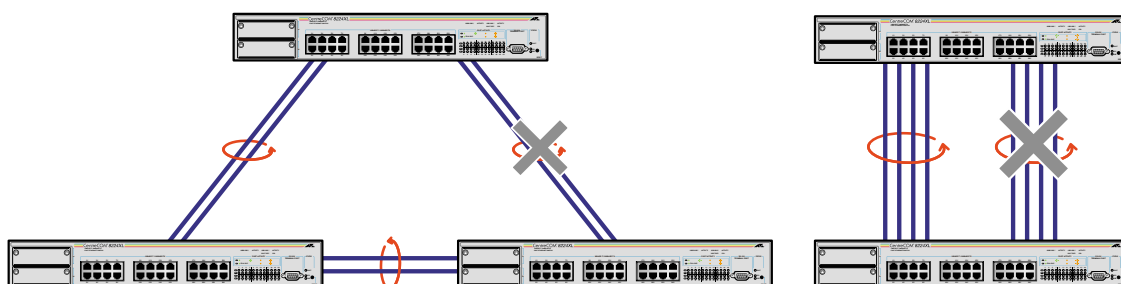
### トランキンググループの複数設定

参照「オペレーションマニュアル / ポートトランキング」

ポートトランキング機能において、トランキンググループを一台につき複数設定することが可能になりました。

8216FXL/SC ..... 4 グループまで(アップリンクポートを含む)  
8224XL ..... 5 グループまで(アップリンクポートを含む)

ただし、下図のようなネットワーク構成での設定はループが形成されるため避けてください。



**i** 本製品は、同一機種同士のトランク接続が可能です。その他のトランク接続が可能な弊社製品については、弊社ホームページの「製品 / 動作検証リスト」でご確認ください。

ホームページアドレス <http://www.allied-teleasis.co.jp>

### メニュー構造の変更

以下のオプションは、[ Main Menu ]>[ System configuration ]直下から、[ Main Menu ]> [ System configuration ] -> [ Switch Configuration ] の下に移動しました。

IGMP Snooping/No IGMP Snooping IGMP Snooping Aging Time( Minutes )  
[ Main Menu ] -> [ System configuration ] -> [ Switch Configuration ] -> [ IGMP Snooping configuration ]

Port trunking in the 10/100M Speed Port( 旧 : Port trunking )  
[ Main Menu ] -> [ System configuration ] -> [ Switch Configuration ]





