



Sun Fire™ B1600 ブレードシステムシャーシ スイッチ管理マニュアル

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054
U.S.A.

Part No. 817-1893-10
2003 年 4 月, Revision A

コメントの宛先: docfeedback@sun.com

Copyright 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, CA 95054 U.S.A. All rights reserved.

米国 Sun Microsystems, Inc. (以下、米国 Sun Microsystems 社とします)は、本書に記述されている製品に採用されている技術に関する知的所有権を有しています。これら知的所有権には、<http://www.sun.com/patents>に掲載されているひとつまたは複数の米国特許、および米国ならびにその他の国におけるひとつまたは複数の特許または出願中の特許が含まれています。

本書およびそれに付属する製品は著作権法により保護されており、その使用、複製、頒布および逆コンパイルを制限するライセンスのもとにおいて頒布されます。サン・マイクロシステムズ株式会社の書面による事前の許可なく、本製品および本書のいかなる部分も、いかなる方法によっても複製することが禁じられます。

本製品のフォント技術を含む第三者のソフトウェアは、著作権法により保護されており、提供者からライセンスを受けているものです。

本製品の一部は、カリフォルニア大学からライセンスされている Berkeley BSD システムに基づいていることがあります。UNIX は、X/Open Company Limited が独占的にライセンスしている米国ならびに他の国における登録商標です。

本製品は、株式会社モリサワからライセンス供与されたリュウミン L-KL (Ryumin-Light) および中ゴシック BBB (GothicBBB-Medium) のフォント・データを含んでいます。

本製品に含まれる HG 明朝 L と HG ゴシック B は、株式会社リコーがリョービマジクス株式会社からライセンス供与されたタイプフェースマスタをもとに作成されたものです。平成明朝体 W3 は、株式会社リコーが財団法人日本規格協会 文字フォント開発・普及センターからライセンス供与されたタイプフェースマスタをもとに作成されたものです。また、HG 明朝 L と HG ゴシック B の補助漢字部分は、平成明朝体 W3 の補助漢字を使用しています。なお、フォントとして無断複製することは禁止されています。

Sun、Sun Microsystems、AnswerBook2、docs.sun.com、Sun Fire は、米国およびその他の国における米国 Sun Microsystems 社の商標もしくは登録商標です。サンロゴマークおよび Solaris は、米国 Sun Microsystems 社の登録商標です。

すべての SPARC 商標は、米国 SPARC International, Inc. のライセンスを受けて使用している同社の米国およびその他の国における商標または登録商標です。SPARC 商標が付いた製品は、米国 Sun Microsystems 社が開発したアーキテクチャーに基づくものです。

OPENLOOK、OpenBoot、JLE は、サン・マイクロシステムズ株式会社の登録商標です。

ATOK は、株式会社ジャストシステムの登録商標です。ATOK8 は、株式会社ジャストシステムの著作物であり、ATOK8 にかかる著作権その他の権利は、すべて株式会社ジャストシステムに帰属します。ATOK Server/ATOK12 は、株式会社ジャストシステムの著作物であり、ATOK Server/ATOK12 にかかる著作権その他の権利は、株式会社ジャストシステムおよび各権利者に帰属します。

本書で参照されている製品やサービスに関しては、該当する会社または組織に直接お問い合わせください。

OPEN LOOK および Sun Graphical User Interface は、米国 Sun Microsystems 社が自社のユーザーおよびライセンス実施権者向けに開発しました。米国 Sun Microsystems 社は、コンピュータ産業用のビジュアルまたはグラフィカル・ユーザーインタフェースの概念の研究開発における米国 Xerox 社の先駆者としての成果を認めるものです。米国 Sun Microsystems 社は米国 Xerox 社から Xerox Graphical User Interface の非独占的ライセンスを取得しており、このライセンスは米国 Sun Microsystems 社のライセンス実施権者にも適用されます。

Use, duplication, or disclosure by the U.S. Government is subject to restrictions set forth in the Sun Microsystems, Inc. license agreements and as provided in DFARS 227.7202-1(a) and 227.7202-3(a) (1995), DFARS 252.227-7013(c)(1)(ii) (Oct. 1998), FAR 12.212(a) (1995), FAR 52.227-19, or FAR 52.227-14 (ALT III), as applicable.

本書は、「現状のまま」をベースとして提供され、商品性、特定目的への適合性または第三者の権利の非侵害の黙示の保証を含みそれに限定されない、明示的であるか黙示的であるかを問わない、なんらの保証も行われぬものとします。

本書には、技術的な誤りまたは誤植のある可能性があります。また、本書に記載された情報には、定期的に変更が行われ、かかる変更は本書の最新版に反映されます。さらに、米国サンまたは日本サンは、本書に記載された製品またはプログラムを、予告なく改良または変更することがあります。

本製品が、外国為替および外国貿易管理法 (外為法) に定められる戦略物資等 (貨物または役務) に該当する場合、本製品を輸出または日本国外へ持ち出す際には、サン・マイクロシステムズ株式会社の事前の書面による承諾を得ることのほか、外為法および関連法規に基づく輸出手続き、また場合によっては、米国商務省または米国所轄官庁の許可を得ることが必要です。

原典:	Sun Fire B1600 Blade System Chassis Switch Administration Guide Part No: 816-3365-11 Revision A
-----	---



Adobe PostScript

Copyright (c) 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, CA 95054 U.S.A. All rights reserved. この製品は、ひとつまたは複数の米国特許によって保護されています。特許出願中。

この製品は、第三者が開発した製品とともに頒布される場合があります。

Sun、Sun Microsystems、Java、Sun Fire、100% Pure Java ロゴマークは、米国およびその他の国における米国 Sun Microsystems 社の商標もしくは登録商標です。サン・のロゴマークおよび Solaris は、米国 Sun Microsystems 社の登録商標です。

すべての SPARC 商標は、米国 SPARC International, Inc. のライセンスを受けて使用している同社の米国およびその他の国における商標または登録商標です。SPARC 商標が付いた製品は、米国 Sun Microsystems 社が開発したアーキテクチャーに基づくものです。

この製品は、米国の輸出規制法に従うものであり、その他の国の輸出または輸入に関する法律が適用される場合もあります。核またはミサイル、生物化学兵器、核の海上での最終使用または最終使用者は、直接的または間接的にかかわらず厳重に禁止されています。米国の通商禁止対象国、または拒否された人物および特別認定国リストに限らず、米国の輸出禁止リストに指定されている実体への輸出または再輸出は、厳重に禁止されています。

予備の CPU の使用または交換は、米国の輸出法に従って輸出された製品に対する CPU の修理または 1 対 1 の交換に制限されています。米国政府の許可なしに、製品のアップグレードに CPU を使用することは、厳重に禁止されています。

目次

はじめに xvii

1. 概要 1-1

1.1 製品の概要 1-1

1.1.1 スイッチのアーキテクチャー 1-2

1.1.2 スイッチ管理アプリケーションへのアクセス方法 1-2

1.2 ハードウェアの説明 1-3

1.2.1 Ethernet ポート 1-3

1.2.1.1 アップリンクポート 1-3

1.2.1.2 内部ポート 1-3

1.2.2 状態表示 LED 1-4

1.3 スイッチの機能 1-5

1.4 デフォルト設定 1-8

2. 初期設定 2-1

2.1 スイッチのインタフェースへの接続 2-2

2.1.1 設定オプション 2-2

2.1.1.1 組み込み型スイッチインタフェースを使用したスイッチの設定 2-2

2.2 SNMP 管理アクセスを使用可能にする方法 2-4

2.2.1 コミュニティ文字列 2-4

2.2.2	トラップの受信	2-5
3.	管理作業の概要	3-1
3.1	Web インタフェースの使用	3-2
3.1.1	Web ブラウザインタフェースのナビゲーション	3-3
3.1.1.1	ホームページ	3-3
3.1.1.2	設定オプション	3-4
3.1.2	パネル表示	3-4
3.1.3	メインメニュー	3-5
3.2	基本的な設定	3-8
3.2.1	システム情報の表示	3-8
3.2.2	IP アドレスの設定	3-11
3.2.2.1	手動による設定	3-13
3.2.2.2	DHCP および BOOTP の使用	3-15
3.2.3	スイッチソフトウェアのバージョンの表示	3-17
3.2.4	ファームウェアの管理	3-19
3.2.4.1	サーバーからのシステムソフトウェアのダウンロード	3-19
3.2.5	設定情報の保存および復元	3-22
3.2.5.1	サーバーからの設定情報のダウンロード	3-22
3.2.6	ユーザー認証の設定	3-24
3.2.7	SNMP の設定	3-28
3.2.7.1	SNMP プロトコルへのアクセス権の設定	3-29
3.2.7.2	トラップマネージャーおよびトラップタイプの指定	3-30
3.3	グローバルなネットワークプロトコルの設定	3-33
3.3.1	VLAN の設定	3-33
3.3.1.1	基本的な VLAN 情報の表示	3-36
3.3.1.2	GVRP の使用可能および使用不可の切り替え (グローバル設定)	3-38
3.3.1.3	VLAN の設定	3-39

3.3.1.4	VLAN への静的メンバーの追加	3-42
3.3.2	マルチキャスト設定	3-45
3.3.2.1	IGMP スヌープパラメタの設定	3-46
3.3.2.2	マルチキャストルーターに接続するインタフェースの指定	3-49
3.3.2.3	マルチキャストサービスの設定	3-52
3.3.3	ブロードキャストストームの抑制 (グローバル設定)	3-55
3.3.4	スパニングツリーアルゴリズムの設定	3-57
3.3.4.1	基本的な STA 設定	3-57
3.3.4.2	STA の拡張設定	3-63
3.3.5	サービスクラスの設定	3-65
3.3.5.1	インタフェースのデフォルトの優先順位の設定	3-65
3.3.5.2	CoS 値の送信キューへの割り当て	3-67
3.3.5.3	トラフィッククラスのサービス加重の設定	3-70
3.3.5.4	レイヤー 3 および 4 の優先順位の CoS 値への割り当て	3-71
3.3.5.5	IP 優先順位 (Precedence) の割り当て	3-73
3.3.5.6	DSCP 優先順位の割り当て	3-75
3.3.6	アドレステーブルの設定	3-77
3.3.6.1	アドレステーブルの表示	3-77
3.3.6.2	有効期限の変更	3-79
3.4	ポートの設定	3-80
3.4.1	接続ステータスの表示	3-80
3.4.2	インタフェース接続の設定	3-84
3.4.3	ポートトランクの設定	3-88
3.4.3.1	LACP によるトランクの動的な設定	3-89
3.4.3.2	トランクの静的な設定	3-91
3.4.4	インタフェースの VLAN 動作の設定	3-93
3.4.5	静的アドレスの設定	3-99
3.4.6	スパニングツリーアルゴリズムのインタフェースの管理	3-102

3.4.6.1	STA の現在のインタフェース設定の表示	3-102
3.4.6.2	インタフェースの STA の設定	3-106
3.4.6.3	インタフェースの STA プロトコルステータスの確認	3-109
3.4.7	管理ポートのトラフィックのフィルタリング	3-110
3.5	ポートおよび管理トラフィックの監視	3-114
3.5.1	ポートのミラー化の設定	3-114
3.5.2	ポートの統計情報の表示	3-116
3.5.3	SNMP 統計情報の表示	3-125
3.5.4	メッセージログの設定	3-128
4.	コマンド行リファレンス	4-1
4.1	コマンド行インタフェースの使用	4-1
4.1.1	CLI へのアクセス	4-1
4.1.1.1	コンソール接続	4-1
4.1.1.2	telnet 接続	4-2
4.1.2	コマンドの入力	4-3
4.1.2.1	キーワードおよび引数	4-3
4.1.2.2	最小限の省略語	4-4
4.1.2.3	コマンドの補完	4-4
4.1.2.4	コマンドのヘルプの表示	4-4
4.1.2.5	コマンドの表示	4-5
4.1.2.6	省略したキーワードの検索	4-6
4.1.2.7	コマンドの機能を無効にする方法	4-6
4.1.2.8	コマンド履歴の使用	4-6
4.1.2.9	コマンドモードについて	4-7
4.1.2.10	実行コマンド	4-7
4.1.2.11	設定コマンド	4-8
4.1.2.12	コマンド行の入力	4-9
4.2	コマンドグループ	4-10

4.3 コマンドの詳細な説明	4-11
4.3.1 一般コマンド	4-11
4.3.1.1 enable	4-12
4.3.1.2 disable	4-13
4.3.1.3 configure	4-13
4.3.1.4 show history	4-14
4.3.1.5 reload	4-15
4.3.1.6 end	4-16
4.3.1.7 exit	4-16
4.3.1.8 quit	4-17
4.3.2 フラッシュ/ファイルコマンド	4-17
4.3.2.1 copy	4-18
4.3.2.2 delete	4-20
4.3.2.3 dir	4-21
4.3.2.4 whichboot	4-22
4.3.2.5 boot system	4-23
4.3.3 システム管理コマンド	4-24
4.3.3.1 hostname	4-25
4.3.3.2 username	4-25
4.3.3.3 enable password	4-26
4.3.3.4 ip http port	4-27
4.3.3.5 ip http server	4-28
4.3.3.6 jumbo-frame	4-29
4.3.3.7 logging on	4-30
4.3.3.8 logging history	4-30
4.3.3.9 clear logging	4-32
4.3.3.10 show logging	4-32
4.3.3.11 show startup-config	4-34

- 4.3.3.12 show running-config 4-36
- 4.3.3.13 show system 4-38
- 4.3.3.14 show users 4-39
- 4.3.3.15 show version 4-39
- 4.3.4 認証コマンド 4-41
 - 4.3.4.1 authentication login 4-42
 - 4.3.4.2 radius-server host 4-43
 - 4.3.4.3 radius-server port 4-43
 - 4.3.4.4 radius-server key 4-44
 - 4.3.4.5 radius-server retransmit 4-44
 - 4.3.4.6 radius-server timeout 4-45
 - 4.3.4.7 show radius-server 4-46
 - 4.3.4.8 tacacs-server host 4-46
 - 4.3.4.9 tacacs-server port 4-47
 - 4.3.4.10 tacacs-server key 4-47
 - 4.3.4.11 show tacacs-server 4-48
- 4.3.5 SNMP コマンド 4-49
 - 4.3.5.1 snmp-server community 4-49
 - 4.3.5.2 snmp-server contact 4-50
 - 4.3.5.3 snmp-server location 4-51
 - 4.3.5.4 snmp-server host 4-51
 - 4.3.5.5 snmp-server enable traps 4-52
 - 4.3.5.6 show snmp 4-53
- 4.3.6 回線コマンド 4-55
 - 4.3.6.1 line 4-56
 - 4.3.6.2 login 4-57
 - 4.3.6.3 password 4-58
 - 4.3.6.4 exec-timeout 4-59

- 4.3.6.5 password-thresh 4-60
- 4.3.6.6 silent-time 4-61
- 4.3.6.7 show line 4-62
- 4.3.7 IP コマンド 4-63
 - 4.3.7.1 ip address 4-63
 - 4.3.7.2 ip dhcp restart 4-65
 - 4.3.7.3 ip dhcp client-identifier 4-66
 - 4.3.7.4 ip default-gateway 4-67
 - 4.3.7.5 show ip interface 4-67
 - 4.3.7.6 show ip redirects 4-68
 - 4.3.7.7 ping 4-69
 - 4.3.7.8 ip filter 4-70
 - 4.3.7.9 show ip filter 4-74
- 4.3.8 インタフェースコマンド 4-75
 - 4.3.8.1 interface 4-75
 - 4.3.8.2 description 4-76
 - 4.3.8.3 speed-duplex 4-77
 - 4.3.8.4 negotiation 4-78
 - 4.3.8.5 capabilities 4-79
 - 4.3.8.6 flowcontrol 4-81
 - 4.3.8.7 shutdown 4-82
 - 4.3.8.8 switchport broadcast packet-rate 4-83
 - 4.3.8.9 clear counters 4-84
 - 4.3.8.10 show interfaces status 4-84
 - 4.3.8.11 show interfaces counters 4-85
 - 4.3.8.12 show interfaces switchport 4-87
- 4.3.9 アドレステーブルコマンド 4-88
 - 4.3.9.1 mac-address-table static 4-89

- 4.3.9.2 clear mac-address-table dynamic 4-90
- 4.3.9.3 show mac-address-table 4-90
- 4.3.9.4 mac-address-table aging-time 4-91
- 4.3.9.5 show mac-address-table aging-time 4-92
- 4.3.10 ポートセキュリティコマンド 4-92
 - 4.3.10.1 port security 4-93
- 4.3.11 スパニングツリーコマンド 4-94
 - 4.3.11.1 spanning-tree 4-95
 - 4.3.11.2 spanning-tree mode 4-96
 - 4.3.11.3 spanning-tree forward-time 4-97
 - 4.3.11.4 spanning-tree hello-time 4-98
 - 4.3.11.5 spanning-tree max-age 4-98
 - 4.3.11.6 spanning-tree priority 4-99
 - 4.3.11.7 spanning-tree pathcost method 4-100
 - 4.3.11.8 spanning-tree transmission-limit 4-100
 - 4.3.11.9 spanning-tree cost 4-101
 - 4.3.11.10 spanning-tree port-priority 4-102
 - 4.3.11.11 spanning-tree edge-port 4-103
 - 4.3.11.12 spanning-tree protocol-migration 4-104
 - 4.3.11.13 spanning-tree link-type 4-104
 - 4.3.11.14 show spanning-tree 4-105
- 4.3.12 VLAN コマンド 4-108
 - 4.3.12.1 vlan database 4-109
 - 4.3.12.2 vlan 4-109
 - 4.3.12.3 interface vlan 4-110
 - 4.3.12.4 switchport mode 4-111
 - 4.3.12.5 switchport acceptable-frame-types 4-112
 - 4.3.12.6 switchport ingress-filtering 4-113

- 4.3.12.7 switchport native vlan 4-114
- 4.3.12.8 switchport allowed vlan 4-115
- 4.3.12.9 switchport forbidden vlan 4-116
- 4.3.12.10 show vlan 4-117
- 4.3.13 GVRP およびブリッジ拡張機能コマンド 4-118
 - 4.3.13.1 switchport gvrp 4-118
 - 4.3.13.2 show gvrp configuration 4-119
 - 4.3.13.3 garp timer 4-120
 - 4.3.13.4 show garp timer 4-121
 - 4.3.13.5 bridge-ext gvrp 4-122
 - 4.3.13.6 show bridge-ext 4-123
- 4.3.14 IGMP スヌープコマンド 4-124
 - 4.3.14.1 ip igmp snooping 4-125
 - 4.3.14.2 ip igmp snooping vlan static 4-126
 - 4.3.14.3 ip igmp snooping version 4-126
 - 4.3.14.4 show ip igmp snooping 4-127
 - 4.3.14.5 show mac-address-table multicast 4-128
 - 4.3.14.6 ip igmp snooping querier 4-129
 - 4.3.14.7 ip igmp snooping query-count 4-130
 - 4.3.14.8 ip igmp snooping query-interval 4-131
 - 4.3.14.9 ip igmp snooping query-max-response-time 4-131
 - 4.3.14.10 ip igmp snooping router-port-expire-time 4-132
 - 4.3.14.11 ip igmp snooping vlan mrouter 4-133
 - 4.3.14.12 show ip igmp snooping mrouter 4-134
- 4.3.15 優先順位コマンド 4-135
 - 4.3.15.1 switchport priority default 4-136
 - 4.3.15.2 queue bandwidth 4-137
 - 4.3.15.3 queue cos-map 4-138

- 4.3.15.4 show queue bandwidth 4-139
- 4.3.15.5 show queue cos-map 4-140
- 4.3.15.6 map ip precedence (グローバル設定) 4-140
- 4.3.15.7 map ip precedence (インタフェース設定) 4-141
- 4.3.15.8 map ip dscp (グローバル設定) 4-142
- 4.3.15.9 map ip dscp (インタフェース設定) 4-143
- 4.3.15.10 show map ip precedence 4-144
- 4.3.15.11 show map ip dscp 4-145
- 4.3.16 ミラーポートコマンド 4-146
 - 4.3.16.1 port monitor 4-146
 - 4.3.16.2 show port monitor 4-147
- 4.3.17 ポートトランクコマンド 4-148
 - 4.3.17.1 channel-group 4-149
 - 4.3.17.2 lacp 4-150
- A. 管理情報ベース A-1
 - A.1 サポートする MIB A-1
 - A.2 サポートトラップ A-3
- B. 障害追跡 B-1
 - B.1 スイッチのインジケータによる診断 B-1
 - B.2 ポート接続の診断 B-2
 - B.3 管理インタフェースへのアクセス B-2
 - B.4 システムログの使用 B-3
 - B.4.1 ログメッセージ B-4
 - B.5 エラーメッセージ B-5
 - B.5.1 コマンド行エラーの検出 B-5
 - B.5.2 システムエラー B-5
 - B.5.3 コマンド行エラー B-6

B.5.4 Web インタフェースエラー B-8

C. 仕様 C-1

C.1 スイッチアーキテクチャー C-1

C.2 管理機能 C-2

C.3 物理仕様 C-2

C.4 電源 C-3

C.5 動作環境 C-3

C.6 標準規格 C-3

用語集 用語集-1

索引 索引-1

はじめに

このマニュアルでは、Sun Fire™ B1600 システムシャーシが実装する SSC (スイッチ/システムコントローラ) モジュール内のスイッチを理解して使用するために必要な事項について説明します。スイッチへのインタフェースには、コマンド行インタフェースと Web インタフェースの 2 つがあります。このマニュアルでは、両方のインタフェースについて説明します。

このマニュアルは、システムシャーシを管理するネットワーク管理者を対象としています。ローカルエリアネットワークの動作に関する知識があり、ネットワークプロトコルを熟知していることを前提とします。

お読みになる前に

スイッチの設定を始める前に、『Sun Fire B1600 ブレードシステムシャーシハードウェア設置マニュアル』および『Sun Fire B1600 ブレードシステムシャーシソフトウェア設定マニュアル』の手順に従って、システムシャーシを設置してください。

内容の紹介

第 1 章では、管理方法、ハードウェアの機能、スイッチの機能、デフォルト設定などの、スイッチの概要について説明します。

第 2 章では、スイッチコンソールまたは Web インタフェースに接続する方法について説明します。

第 3 章では、スイッチの重要な機能について説明し、Web インタフェースまたはコンソールインタフェースによってそれらの機能を設定する方法を示します。また、SNMP 管理アプリケーションが使用する、各機能に対応する MIB 変数のリストも示します。

第 4 章では、すべてのコンソールインタフェースコマンドおよびパラメタについて詳細に説明します。

付録 A では、このスイッチがサポートする管理情報ベース (Management Information Base : MIB) およびトラップについて説明します。

付録 B では、システム LED およびポート LED の意味、管理インタフェースにアクセスできなくなる問題の解決方法、システムログの使用方法などの、基本的な障害追跡情報について説明します。

付録 C では、スイッチの詳細な仕様について説明します。

用語集では、語句とその定義のリストを示します。

索引では、このマニュアルで説明する重要な事項の参照先ページを示します。

書体と記号について

書体または記号	意味	例
AaBbCc123	コマンド名、ファイル名、ディレクトリ名、画面上のコンピュータ出力、コード例。	システムファイルを表示します。 すべてのファイルを一覧表示するには、 <code>dir</code> を使用します。
AaBbCc123	ユーザーが入力する文字を、画面上のコンピュータ出力と区別して表します。	>enable Password:
AaBbCc123 またはゴシック	コマンド行の可変部分。実際の名前や値と置き換えてください。	<code>rm filename</code> と入力します。 <code>rm ファイル名</code> と入力します。
『 』	参照する書名を示します。	『Solaris ユーザーマニュアル』
「 」	参照する章、節、または、強調する語を示します。	第 6 章「データの管理」を参照。 この操作ができるのは「スーパーユーザー」だけです。
\	枠で囲まれたコード例で、テキストがページ行幅をこえる場合に、継続を示します。	% <code>grep `^#define` \</code> <code>XV_VERSION_STRING'</code>

関連マニュアル

用途	タイトル	Part No.
設置	『Sun Fire B1600 ブレードシステムシャーシハードウェア設置マニュアル』	817-1904
シャーシソフトウェアの設定	『Sun Fire B1600 ブレードシステムシャーシソフトウェア設定マニュアル』	817-1888
シャーシの管理	『Sun Fire B1600 ブレードシステムシャーシ管理マニュアル』	817-1898

Sun のオンラインマニュアル

各言語対応版を含むサンの各種マニュアルは、次の URL から表示または印刷、購入できます。

<http://www.sun.com/documentation>

Solaris およびその他のマニュアルは下記 URL より参照できます。

<http://docs.sun.com>

コメントをお寄せください

弊社では、マニュアルの改善に努力しており、お客様からのコメントおよびご忠告をお受けしております。コメントは下記宛に電子メールでお送りください。

docfeedback@sun.com

電子メールの表題にはマニュアルの Part No. (817-1893-10) を記載してください。

なお、現在日本語によるコメントには対応できませんので、英語で記述してください。

PART I ご使用の前に

ここでは、Sun Fire B1600 ブレードシステムシャーシの概要およびネットワークスイッチの基本概念について説明します。また、管理インターフェースにアクセスするための基本設定についても説明します。

概要

初期設定

第1章

概要

Sun Fire B1600 ブレードシステムシャーシは、スイッチ/システムコントローラ (SSC) モジュールを 2 台実装しています。SSC は、高性能の Gigabit Ethernet スイッチを搭載しています。このスイッチは、16 個の内部用の全二重 Gigabit ポートによってシャーシ内で大容量通信を実現するとともに、8 個の外部用の全二重 Gigabit ポートによって広域のネットワークに接続します。

1.1 製品の概要

2 つのスイッチは、Sun Fire B1600 ブレードシステムシャーシに Gigabit Ethernet 接続を提供します。一方のスイッチに障害が発生した場合でも、もう一方のスイッチによって動作が継続されます。シャーシ内のすべてのコンポーネント (ブレード、SSC、PSU) は、共通のミッドプレーンに接続します。このミッドプレーンによって、コンポーネント間のあらゆる相互接続を実現します。

16 台のサーバーブレードは、ブレードの主な入出力手段である Gigabit Ethernet リンクを使用して、それぞれが各スイッチの 1 つのポートに接続します。各 SSC 内のスイッチには、外部との接続に使用する 8 つの外部リンク、およびすべてのブレードをまとめて接続する Gigabit Ethernet ファブリックがあります。各ブレードは、単純なシリアルリンクを使用して各 SSC 内のシステムコントローラ (SC) に接続します。SC を使用すると、シャーシに実装されたコンポーネントを管理および監視できます。また、スイッチのコマンド行インタフェース、およびシャーシに取り付けられている各サーバーブレードのコンソールにアクセスすることもできます。

1.1.1 スイッチのアーキテクチャー

このスイッチは、高速スイッチングファブリックを採用しているため、すべてのポートで短時間に複数パケットを同時転送できます。また、データの完全性を向上させるために蓄積転送 (Store-and-Forward) 方式を採用しています。このモードでは、必ずパケット全体をポートバッファに格納して、有効性を確認した上で転送します。こうして、エラーがネットワーク全体に伝播されることを防ぎます。

1.1.2 スイッチ管理アプリケーションへのアクセス方法

このスイッチには RJ-45 ジャックを使用したシリアルコンソールポートがあり、設置場所で SC にアクセスして管理できるようになっています。システムシャーシに電源を入れると、SC へのインタフェースが表示されます。スイッチのコマンド行インタフェースにアクセスする方法については、2-2 ページの「設定オプション」または『Sun Fire B1600 ブレードシステムシャーシソフトウェア設定マニュアル』を参照してください。

このコマンド行インタフェースには、SSC の 100BASE-TX RJ-45 管理ポート (NETMGT) を介して telnet で直接アクセスすることもできます。

Web ブラウザまたは SNMP/RMON ソフトウェアを使用して、ネットワーク経由でこのポートに接続してスイッチを管理することもできます。

Web ブラウザを介して接続する場合は、グラフィカルユーザーインタフェースを使用した HTTP 管理アクセスが可能です。

SNMP から提供される情報は、適切に設定した SNMP 対応管理アプリケーションを使用して表示できます。

1.2 ハードウェアの説明

SSC は、スイッチボードおよび SC、冷却用ファン、ミッドプレーンコネクタ、背面パネルコネクタで構成されます。SC は、サーバーシャーシおよびスイッチボードにアクセスして管理する機能を提供します。また、システムインジケータを制御して、Sun Fire B1600 ブレードシステムシャーシの前面および背面に同じ情報を表示します。

1.2.1 Ethernet ポート

1.2.1.1 アップリンクポート

8 個の外部 RJ-45 ポートは、IEEE 802.3x で規定された、速度およびデュプレックスモード、フロー制御の自動ネゴシエーションをサポートしています。各ポートは 10 Mbps、100 Mbps、1000 Mbps の全二重または半二重で動作し、データストリームを制御してバッファのオーバーフローを防ぎます。このアップリンクポートは、カテゴリ 5 より対線ケーブルを使用して、100 m (328 フィート) 以内にある IEEE 802.3ab 1000BASE-T に準拠する装置に接続できます。また、このポートは自動 MDI/MDI-X 操作をサポートするため、すべての接続でストレートケーブルを使用できます。アップリンクポートは、設定インタフェースでは NETP0 ~ 7 という名前で示されます。

注 - 自動ネゴシエーションを使用するとき、接続する装置もこの機能に対応していれば、速度および伝送方式、フロー制御は自動的に設定されます。それ以外の場合は、各接続に対してこれらの項目を手動で設定します。

注 - MDI/MDI-X ピン配列の自動設定機能を使用する場合は、自動ネゴシエーションを使用可能にする必要があります。

1.2.1.2 内部ポート

このスイッチは、シャーシ内のサーバーブレードとの接続に使用する 16 個の 1000BASE-X Gigabit Ethernet 内部ポートも実装しています。このポートは、1000 Mbps、全二重の設定に固定されています。内部ポートは、設定インタフェースでは SNP0 ~ 15 という名前で示されます。

また、このスイッチは、NETMGT と呼ばれる 10/100BASE-TX 内部ポートも実装しています。NETMGT は、内蔵のハブを介して SC のネットワークポートおよび SSC の正面パネル上にある外部管理用のポートに接続します。

1.2.2 状態表示 LED

SSC モジュールには、スイッチの状態を示すインジケータが付いています。また、SSC の背面パネル上の 1000BASE-T アップリンクポートおよび 10/100BASE-TX 管理ポートには、リンクおよび速度の状態を示すインジケータが付いています。

図 1-1 SSC の外部のパネル

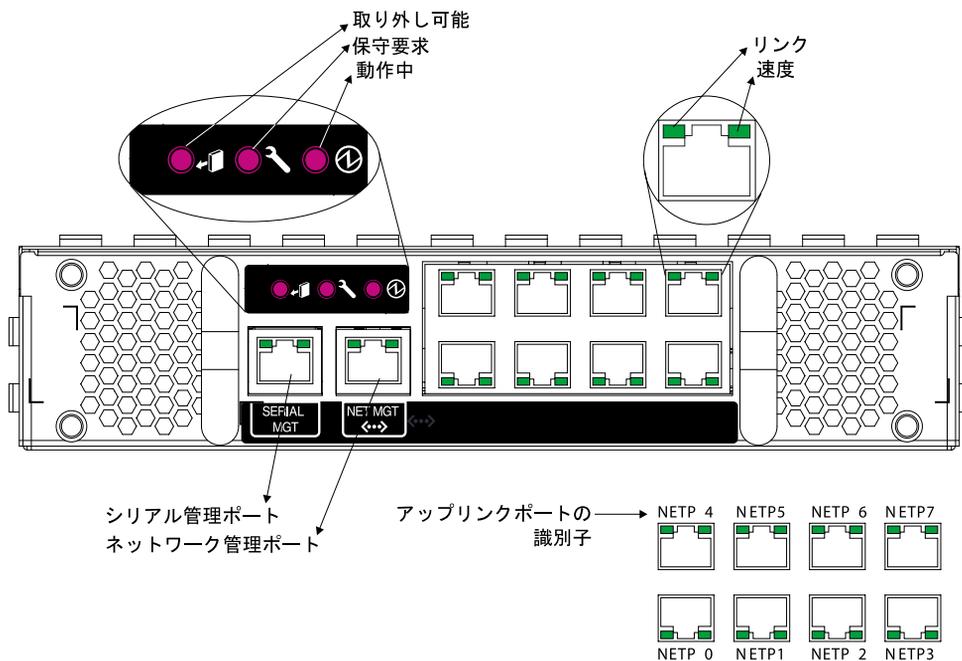


表 1-1 ポート LED

LED	条件	状態
SSC		
動作中	点灯 (緑色)	SSC は正常に動作しています。
保守要求	点灯 (オレンジ色)	SSC の保守作業が必要です。
取り外し可能	点灯 (青色)	SSC を取り外すことができます。
RJ-45 ポート		
リンク	点灯 (緑色)	ポートが有効なネットワーク接続を確立しました。
速度	点灯 (オレンジ色)	リンクは 1 Gbps で動作しています。
	消灯	リンクは 1 Gbps 未満で動作しています。

1.3 スイッチの機能

このスイッチは、性能を向上させるためにさまざまな先進機能を提供しています。マルチキャストフィルタリングにより、リアルタイムネットワークアプリケーションのサポートが可能です。ポートベースのタグ付き VLAN に加えて、GVRP による VLAN の自動登録もサポートしているため、トラフィックセキュリティを維持しながらネットワーク帯域幅を効率よく使用できます。QoS 優先制御キューイングによって、リアルタイムマルチメディアデータをネットワーク上で伝送するときの遅延が最小限に抑えられます。フロー制御は、ポートの飽和に起因するボトルネックによってパケット損失が発生することを防ぎます。また、ブロードキャストストームの抑制機能によって、ブロードキャストトラフィックストームによって発生するネットワークの混乱を防ぎます。次に、主な管理機能の概要を示します。

IEEE 802.1D ブリッジ – IEEE 802.1D の透過ブリッジをサポートします。アドレステーブルを使用して、学習したアドレスによってデータスイッチングを行い、この情報に基づいてトラフィックをフィルタリングまたは転送します。このアドレステーブルは、最大 8000 アドレスをサポートします。

蓄積転送 (Store-and-Forward) スwitching – スイッチは、別のポートに転送する前に、各フレームをメモリーにコピーします。これによって、すべてのフレームが Ethernet の標準のサイズであることを確認し、巡回冗長検査 (CRC) によって完全性を確認します。そのため、不良フレームをネットワークに送出して帯域幅をむだに使用することがなくなります。

トラフィック量の多いポートでフレーム損失が発生しないように、各ポートには 128K バイトのフレームバッファが用意されています。このバッファに、混雑するネットワークへの伝送を待機するパケットを蓄積できます。

スパニングツリープロトコル – 次のスパニングツリープロトコルをサポートしています。

スパニングツリープロトコル (STP、IEEE 802.1D) – 1組の LAN セグメントの間に複数の冗長接続を実現することで耐障害性を向上させるプロトコルです。セグメント間に複数の物理パスがある場合に、このプロトコルは1つのパスを除くすべてのパスを使用不可にして、ネットワーク上の任意の2台のステーション間のルートを1つに限定します。これによって、ネットワークループが形成されることを防ぎます。選択したパスに何らかの問題が発生した場合には、代替パスがアクティブになって接続が維持されます。

高速スパニングツリープロトコル (RSTP、IEEE 802.1w) – ネットワークトポロジーの切り替えに必要な収束 (コンバージェンス) 時間を、従来の IEEE 802.1D STP 標準に比べて約 10% に短縮します。RSTP は STP に代わるものですが、接続された装置から STP プロトコルメッセージを受信した場合には、ポートを自動的に STP 準拠モードに再構成して従来の STP 標準で動作しているスイッチとの相互運用性を維持します。

仮想 LAN – 最大 256 の仮想 LAN (VLAN) をサポートします。VLAN とは、ネットワーク上の物理的な位置や接続ポイントにかかわらず、同じコリジョンドメインを共有するネットワークノードの集合を指します。このスイッチは、IEEE 802.1Q 標準に基づくタグ付き VLAN をサポートしています。GVRP を介して VLAN グループのメンバーを動的に学習させることも、またはポートを特定の VLAN のセットに手動で割り当てることもできます。こうして、スイッチは、トラフィックをユーザーに割り当てた VLAN グループに限定することができます。ネットワークを VLAN にセグメント化することには、次の利点があります。

- フラットネットワークの性能を大きく低下させるブロードキャストストームを抑制できます。
- ノードを変更または移動するときに、ネットワーク接続を手動で変更する代わりに、ポートの VLAN メンバー構成を遠隔から変更するだけで対処できるため、ネットワーク管理が容易になります。
- 元になる VLAN へのすべてのトラフィックを制限することで、データの安全性を確保できます。ただし、ルーターまたはレイヤー 3 スイッチを使用して個々の VLAN 間の接続を設定している場合を除きます。

ポートのミラー化 – 任意のポートから監視ポートへのトラフィックを、動作に影響を与えずにミラー化できます。プロトコルアナライザまたは RMON プローブを接続することで、トラフィックを分析して接続の完全性を確認できます。

ポートのトランク化 – ポートをまとめて接続を集約できます。トランクは、手動で設定することも、または IEEE 802.3ad の LACP (Link Aggregation Control Protocol) を使用して動的に設定することもできます。ポートをまとめることによって、あらゆる接続のスループットが飛躍的に向上し、トランクに含まれるポートで障害が発生した場合でも負荷を引き継ぐことができる冗長性を実現します。このスイッチは 6 つのトランクをサポートします。各トランクには、最大 4 つのアップリンクポートまたは最大 2 つのダウンリンクポートを含めることができます。

ポートセキュリティ — ポートセキュリティ機能は、不正なユーザーがネットワークにアクセスすることを防ぎます。各ポートを介してネットワークにアクセスすることが承認されている装置の MAC アドレスのリストは、ポートが学習するか、ポートに割り当てます。ポートが受信したすべてのパケットの送信元アドレスが承認済みリストに含まれている必要があります。送信元アドレスがリストにない場合、そのパケットは破棄されます。ポートセキュリティは、デフォルトでは使用不可になっていますが、ポートごとに使用可能にすることができます。

ブロードキャスト抑制 — この機能により、ブロードキャストトラフィックによるネットワークの過負荷を防ぎます。ポートでこの機能を使用可能にすると、そのポートを通過するブロードキャスト通信のトラフィック量が制限されます。ブロードキャスト通信のトラフィック量があらかじめ定義されているしきい値を超えた場合は、しきい値を下回るまで抑制されます。

フロー制御 — 混雑中のトラフィック量を制限することで、ポートバッファのオーバーフローによるパケット損失を防ぎます。スイッチは、IEEE 802.3x 標準に基づくフロー制御をサポートします。デフォルトでは、フロー制御はすべてのポートで使用不可になっています。

トラフィックの優先制御 — 加重ラウンドロビンキューイング方式の 4 つの優先制御キューを使用して、要求されるサービスレベルに基づいて各パケットに優先順位を付けることにより、サービス品質 (Quality of Service : QoS) を向上させます。IEEE 802.1p および 802.1Q のタグを使用して、エンドステーションのアプリケーションの指定に基づいて受信トラフィックに優先順位を付けます。この機能によって、遅延が問題になるデータおよびベストエフォート型データの優先順位を個々に設定できます。

また、このスイッチは、アプリケーションの要件に合わせて、レイヤー 3 およびレイヤー 4 のトラフィックの一般的な優先制御方式もいくつかサポートしています。トラフィックには、IP フレームのサービスタイプ (Type of Service : ToS) オクテットの優先制御ビットによって優先順位を付けることができます。このサービスを使用可能にすると、スイッチはサービスクラス (Class of Service : CoS) 値に優先順位を割り当てて、対応する送信キューにトラフィックを送信します。

アドレスのフィルタリング — スwitchは CPU ポートに流入する全トラフィックに対するパケットフィルタを提供しているので、必要に応じてトラフィックを管理ネットワークに転送または経路指定することができます。パケットフィルタは、ルールおよびパターンに基づいており、一致した場合にパケットを拒否するパターンセットと、一致した場合にパケットを受理するパターンセットを定義できます。

マルチキャストスイッチング — 特定のマルチキャストトラフィックを専用の VLAN に割り当てることで、通常のネットワークトラフィックを妨害しないように設定し、この配信先 VLAN に必要な優先順位を指定してリアルタイム配信を保証します。スイッチは、IGMP スヌープおよび IGMP を使用して、マルチキャストグループ登録を制御します。

1.4 デフォルト設定

表 1-2 デフォルト設定

機能	デフォルト
システム設定	
Web 管理	使用可能
セキュリティー保護された Web 管理	使用不可
BOOTP	使用可能
DHCP	使用可能
SNMP コミュニティー	public : 読み取り専用 private : 読み取り/書き込み
SNMP トラップ	認証トラップ : 使用可能 リンクアップダウンイベント : 使用可能
ユーザー名	admin (コンソール、telnet、Web 用) guest (コンソール、telnet、Web 用)
パスワード	ログオン - ユーザー名 admin、パスワード admin ユーザー名 guest、パスワード guest 通常実行から特権実行への変更 : super
シリアルポート	ボーレート : 9600、データビット : 8、ストップビット : 1、 パリティ : なし
IP 設定	アドレス : 0.0.0.0、サブネットマスク : 255.0.0.0
ポートの接続状態	
ポートの速度	ポート SNP0 ~ 15 : 1000 Mbps ポート NETP0 ~ 7 : 10/100/1000 Mbps、 自動ネゴシエーション ポート NETMGT : 10/100 Mbps、自動ネゴシエーション
デュプレックスモード	ポート SNP0 ~ 15 : 全二重 ポート NETP0 ~ 7、NETMGT : 全二重および半二重、 自動ネゴシエーション
フロー制御	使用不可
ポートの優先制御	受信データの優先順位 : 0
ポートセキュリティー	使用不可

表 1-2 デフォルト設定 (続き)

機能	デフォルト
スパニングツリープロトコル	使用可能、デフォルト RSTP (デフォルト:すべてのパラメータは IEEE 802.1w ベース)
エッジポート (高速転送)	デフォルトでは SNP0 ~ 15 は使用可能、NETP0 ~ 7 は使用不可
アドレスの有効期限	300 秒
仮想 LAN	
GVRP	使用不可
デフォルト VLAN	PVID 1 (タグなしフレームの場合)
管理 VLAN	VLAN 2 (管理ポートの場合)
タグ付け	RX: すべてのフレーム、TX: タグなしフレーム
インGRESSフィルタリング	使用不可
マルチキャストフィルタリング	
IGMP スヌープ	使用可能
ARP	使用可能
キャッシュタイムアウト	20 分

第2章

初期設定

スイッチの初期設定手順の詳細は、『Sun Fire B1600 ブレードシステムシャーシソフトウェア設定ガイド』を参照してください。

この章は次の節で構成されています。

- 2-2 ページの 2.1 節 「スイッチのインタフェースへの接続」
- 2-4 ページの 2.2 節 「SNMP 管理アクセスを使用可能にする方法」

2.1 スイッチのインタフェースへの接続

2.1.1 設定オプション

スイッチモジュールは、管理アクセス用にコマンド行設定インタフェース (CLI) を提供します。このプログラムにアクセスするには、まずスイッチの RJ-45 シリアルコンソールポートに接続して、次に示すシステムコントローラ (SC) のコマンドプロンプトからスイッチの CLI にログインします。ここで、SSC*n* には、SSC0 または SSC1 のいずれかを指定します。

```
sc>: console sscn/swt
Username: admin
Password:

      CLI session with the Sun Fire B1600 is opened.
      To end the CLI session, enter [Exit].

Console#
```

注 – 管理ネットワーク上に DHCP サーバーを設定している場合は、スイッチへの telnet 接続または Web 接続を使用できます。スイッチが起動して DHCP 要求を発行したときに常に同じアドレスを受け取るには、DHCP サーバーに SUNW,SWITCH_ID=*serial number of chassis*, 0 (SSC0 のスイッチの場合) または SUNW,SWITCH_ID=*serial number of chassis*, 1 (SSC1 のスイッチの場合) の形式でクライアント識別子を指定する必要があります。システムシャーシをネットワークに組み込むための準備と、スイッチの初期設定のすべての手順については、『Sun Fire B1600 ブレードシステムシャーシソフトウェア設定マニュアル』を参照してください。

2.1.1.1 組み込み型スイッチインタフェースを使用したスイッチの設定

コンソール接続 – スイッチの CLI にアクセスするには、システムコントローラコマンドプロンプトで `console sscn/swt` コマンドを入力します。ここで、*ssc*n** には、SSC0 または SSC1 を指定します。

telnet 接続 – 管理ネットワーク上の telnet 接続によって、遠隔からスイッチの CLI に接続できます。

Web インタフェース – スイッチには、HTTP Web エージェントも組み込まれています。このエージェントにアクセスするには、管理ネットワーク上の任意のコンピュータで標準の Web ブラウザを使用します。

SNMP ソフトウェア – スイッチの管理エージェントは、SNMP (Simple Network Management Protocol、バージョン 1 と 2c の両方をサポート) に基づいています。この SNMP エージェントを使用すると、SunNet Manager などの管理ソフトウェアを使用して、管理ネットワーク上の任意のシステムからスイッチを管理できます。

システムの設定プログラムおよび SNMP エージェントは、次の管理機能をサポートしています。

- ポートの使用可能または使用不可への切り替え
- ポートの速度およびデュプレックスモードの設定
- SNMP パラメタの設定
- ポートのネットワーク VLAN への追加
- システム情報または統計情報の表示
- スイッチのスパニングツリーへの組み込み
- システムファームウェアのダウンロード

2.2 SNMP 管理アクセスを使用可能にする方法

スイッチは、SunNet Manager などの SNMP v1 または v2c に対応するアプリケーションからの管理コマンドを受け入れるように設定できます。また、SNMP 要求に応答したり、SNMP トラップを生成するように設定することもできます。

SNMP 管理ホストがスイッチに情報の返送またはパラメタ設定のいずれかの要求を送信すると、スイッチは要求されたデータを提供するか、または指定されたパラメタを設定します。また、SNMP マネージャーからの要求がない場合でも、スイッチがトラップメッセージを使用して SNMP マネージャーに情報を送信するように設定することもできます。トラップメッセージは、特定のイベントが発生したことを SNMP マネージャーに通知します。

2.2.1 コミュニティー文字列

コミュニティー文字列は、SNMP ホストへの管理アクセスを制御したり、SNMP ホストに SSC からのトラップメッセージを受信する権限を付与する場合に使用します。そのため、コミュニティー文字列を特定のユーザーまたはユーザーグループに割り当てて、アクセスレベルを設定する必要があります。

デフォルトのコミュニティー文字列は、次のとおりです。

- **public** – 読み取り専用アクセス。この権限が付与された管理ホストは、MIB オブジェクトの取り出しだけを行うことができます。
- **private** – 読み取り/書き込みアクセス。この権限が付与された管理ホストは、MIB オブジェクトの取り出しおよび変更の両方を行うことができます。

注 – SNMP を使用しない場合は、デフォルトのコミュニティー文字列を両方とも削除することをお勧めします。コミュニティー文字列が存在しないと、スイッチへの SNMP 管理アクセスが使用不可になります。

コミュニティー文字列を設定するには、次の手順を実行します。

1. 特権実行レベルのグローバル設定モードのプロンプトで「snmp-server community string mode」と入力します。ここで、string にはコミュニティーアクセス文字列、mode には **rw** (読み取り/書き込み) または **ro** (読み取り専用) を指定します。Enter キーを押します。

2. 既存のコミュニティ文字列を削除するには、
「no snmp-server community *string*」と入力します。ここで、*string* には、削除するコミュニティアクセス文字列を指定します。Enter キーを押します。

```
Console(config)#snmp-server community sun rw
Console(config)#no snmp-server community private
Console(config)#
```

2.2.2 トラップの受信

SSC からのトラップを受信する SNMP 管理ホストを指定することもできます。

トラップを受信するホストを設定するには、次の手順に従ってください。

1. グローバル設定モードのプロンプトで
「snmp-server host *host-address community-string*」と入力します。ここで、*host-address* にはトラップを受信するホストの IP アドレス、*community-string* にはそのホストに関連付けられている文字列を指定します。
Enter キーを押します。
2. SNMP 通知を送信するように SSC を設定するには、
snmp-server enable traps コマンドを 1 回以上実行する必要があります。
「snmp-server enable traps [*type*]」と入力します。ここで、*type* には、authentication または link-up-down のいずれかを指定します。Enter キーを押します。

```
Console(config)#snmp-server enable traps link-up-down
Console(config)#
```

3. 『Sun Fire B1600 ブレードシステムシャーシソフトウェア設定マニュアル』を参照して、設定を保存します。

PART II スイッチの設定

ここでは、スイッチの基本機能について、Web ブラウザまたはコマンド行インタフェースを使用して各機能を設定する手順の例を示しながら説明します。

管理作業の概要

コマンド行リファレンス

第3章

管理作業の概要

この章では、基本的な設定作業を実行する方法について説明します。

- 3-2 ページの 3.1 節「Web インタフェースの使用」
- 3-8 ページの 3.2 節「基本的な設定」
- 3-33 ページの 3.3 節「グローバルなネットワークプロトコルの設定」
- 3-80 ページの 3.4 節「ポートの設定」
- 3-114 ページの 3.5 節「ポートおよび管理トラフィックの監視」

3.1 Web インタフェースの使用

このスイッチには、HTTP Web エージェントが組み込まれています。Web ブラウザからスイッチを設定し、統計情報を表示してネットワークの使用状況を監視できます。Web エージェントには、ネットワークに接続されたコンピュータから、標準の Web ブラウザ (Internet Explorer 5.0 以上または Netscape Navigator 6.2 以上) を使用してアクセスできます。

注 - コマンド行インタフェース (CLI) を使用して、コンソールポートへのシリアル接続または telnet を介してスイッチを管理することもできます。CLI の使用方法については、第 4 章を参照してください。

Web ブラウザからスイッチにアクセスする前に、次の作業を実行しておく必要があります。

1. 帯域外シリアル接続または BOOTP、DHCP プロトコルを使用して、スイッチに有効な IP アドレスおよびサブネットマスク、デフォルトゲートウェイを設定します。この作業の詳細は、『Sun Fire B1600 ブレードシステムシャーシソフトウェア設定マニュアル』を参照してください。
2. 帯域外シリアル接続を使用して、ユーザー名およびパスワードを設定します。Web エージェントへのアクセスは、ボードに組み込まれた設定プログラムと同じユーザー名およびパスワードによって制御されます。この作業の詳細は、『Sun Fire B1600 ブレードシステムシャーシソフトウェア設定マニュアル』を参照してください。

注 - 管理ホストとこのスイッチの間にスパニングツリーアルゴリズムを使用する装置が設置されていない場合は、管理ホストに接続されたスイッチポートに高速転送を設定することで、Web インタフェースを介して発行した管理コマンドに対するスイッチの応答時間を短縮できます。詳細は、3-106 ページの「Admin Edge Port」を参照してください。

3. ユーザー名およびパスワードを入力すると、システム設定プログラムにアクセスできます。

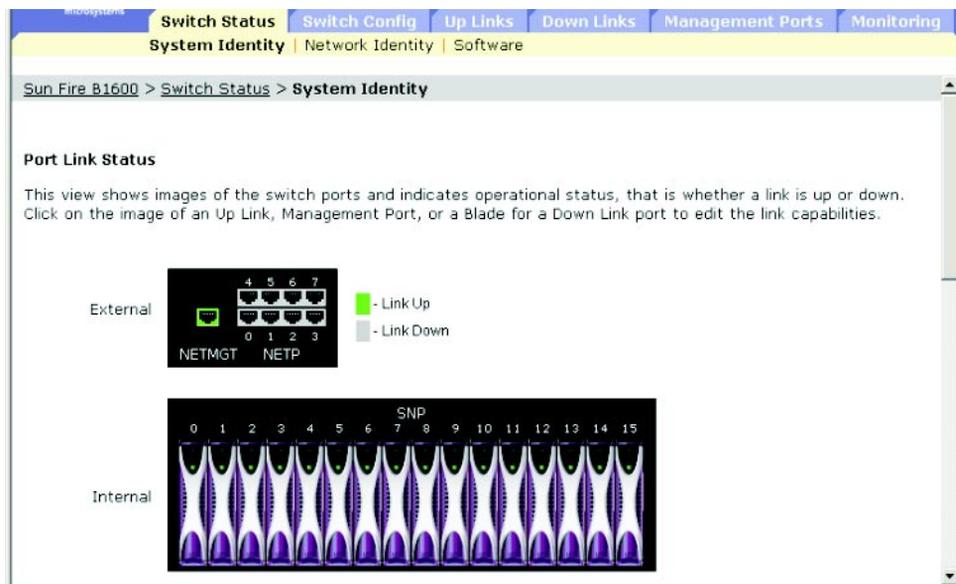
注 - パスワードは 3 回まで入力できます。パスワードを 3 回間違えると、現在の接続処理が中断されます。

3.1.1 Web ブラウザインタフェースのナビゲーション

Web ブラウザインタフェースにアクセスするには、まずユーザー名およびパスワードを入力する必要があります。管理者は、すべての構成パラメータと統計情報に対して、読み取りおよび書き込みのアクセス権を持っています。管理者のデフォルトのユーザー名およびパスワードは「admin」です。

3.1.1.1 ホームページ

Web ブラウザをスイッチの Web エージェントに接続すると、ホームページが表示されます。ページの左側のメインメニューパネルから、「Switch」を選択します。画面上部のメニュータブとこれに対応するメニュー項目 (メニュータブの下に 1 行で表示される) に、設定オプションが表示されます。メニュータブとこれに対応するメニュー項目を使用することで、設定メニューにアクセスして構成パラメータや統計情報を表示します。



3.1.1.2 設定オプション

設定できるパラメタは、ダイアログボックスまたはドロップダウンリストで表示されます。ページ上で設定を変更したら、必ず「Save」ボタンをクリックして新しい設定を確定します。次の表に、Web ページの設定ボタンの概要を示します。

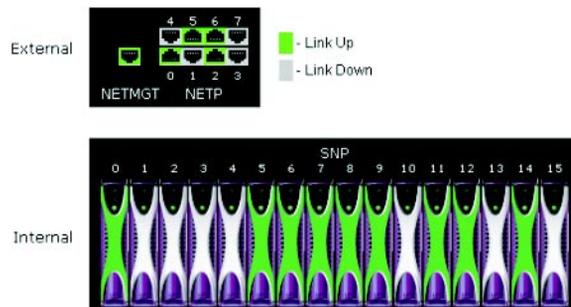
ボタン	動作
Cancel	指定した値を取り消し、現在の値に戻します。
Reset	指定した値を取り消し、現在の値に戻します。
Save	指定した値をシステムに対して設定します。

注 - 画面を適切に再表示するため、Internet Explorer 5.x の「ツール」メニューから「インターネット オプション」=>「全般」=>「インターネット一時ファイル」=>「設定」の順に選択して、「保存しているページの新しいバージョンの確認」の設定を「ページを表示するごとに確認する」にする必要があります。

注 - Internet Explorer 5.0 を使用している場合は、設定を変更したあとにブラウザの更新ボタンを押して手動で再表示する必要があります。

3.1.2 パネル表示

Web エージェントは、スイッチのアップリンクポートのイメージを表示し、各リンクがアップ (稼働) またはダウン (停止) のどちらの状態であることを示します。ポートのイメージをクリックすると、3-80 ページに示すポートの設定ページが表示されます。



3.1.3 メインメニュー

オンボード Web エージェントを使用すると、システムパラメタを定義し、スイッチおよびその全ポートの管理や制御を行い、ネットワークの状態を監視できます。次の表に、このプログラムで設定できる項目の概要を示します。

メニュー	説明	ページ
Switch Setup	基本的な設定	3-8
System Identity	位置、連絡先情報などの基本的なシステム情報を設定します。	3-8
Network Identity	DHCP または BOOTP、手動設定による管理アクセスのための IP アドレスを設定します。	3-11
Software	ファームウェアバージョンの表示と、コードおよび設定情報のダウンロードを行います。	3-17
Switch Config	グローバルなプロトコルの設定	3-33
Security	ユーザー名およびパスワードの設定のほか、RADIUS または TACACS+ による遠隔アクセス認証サービスの割り当てを指定します。	3-24
Communication	SNMP コミュニティーアクセス文字列およびトラップマネージャー、発行するトラップのタイプを設定します。	3-29
VLANs	基本的な VLAN 情報の表示、GVRP マルチキャストプロトコルの使用可能への切り替え、VLAN の設定を行います。	3-33
Static VLAN Port Membership	VLAN に静的なメンバーを追加します。	3-42
Broadcast & Multicast	ブロードキャストストームの抑制と、IGMP スヌープ、ルーターの静的なポート情報、マルチキャストサービスなどのマルチキャストプロトコル設定を行います。	3-45
IGMP Parameters	マルチキャストフィルタリングを使用可能にし、マルチキャスト照会のためのパラメタを設定します。	3-46
Multicast Router Ports	周辺のマルチキャストルーターおよびスイッチに接続されるポートを割り当てます。	3-49
Multicast Services	特定のインタフェースにマルチキャストサービスを割り当てます。	3-52
Broadcast Parameters	ブロードキャストストームのしきい値を設定します。	3-55
Spanning Tree	スパニングツリーのプロトコル設定を行います。	3-57
Basic Configuration	グローバルスパニングツリーの情報を設定します。	3-57
Advanced Configuration	RSTP の拡張情報を設定します。	3-63

メニュー	説明	ページ
Class of Service	サービスクラスを設定します。	3-65
Basic Traffic Prioritisation	デフォルトの CoS 優先順位の設定、CoS 優先順位の送信キューへの割り当て、加重ラウンドロビンキューイング設定を行います。	3-65
Layer 3/4 Traffic Prioritisation	レイヤー 3 および 4 の優先サービスの選択、IP 優先順位タグの CoS 値への割り当て、DSCP タグの CoS 値への割り当てを行います。	3-71
Address Tables	アドレスの有効期限の設定、指定されたインタフェースまたは VLAN、アドレスのエントリの表示、静的アドレスの設定を行います。	3-77
Up Links	ポートの設定	3-80
Connection Status	ポートの接続ステータスを表示します。	3-80
Connection Configuration	ポートの接続ステータスの設定、ブロードキャストストーム制御の使用可能への切り替えを行います。	3-84
Link Aggregation	LACP によってポートが動的にトランクに結合されるように設定するか、または静的にトランクにグループ化するポートを指定します。	3-88
VLANs	ポートの属性 (デフォルトの PVID、スイッチポートモード、イングレスフィルタリング、GVRP、GARP タイマー) の設定、ポートを静的に割り当てる VLAN の設定を行います。	3-93
Static Addresses	アドレステーブルの静的なエントリの表示または編集、永続エントリの学習機能の使用可能および使用不可の切り替えを行います。	3-99
Spanning Tree	グローバルスパニングツリーのポートを設定します。	3-102
Spanning Tree Protocol	グローバルスパニングツリー上のインタフェースの STA ポートレベルを設定します。	3-102
Down Links	ポートの設定	3-80
Connection Status	ポートの接続ステータスを表示します。	3-80
Connection Configuration	ポートの接続ステータスの設定、ブロードキャストストーム制御の使用可能への切り替えを行います。	3-84
Link Aggregation	LACP によってポートが動的にトランクに結合されるように設定するか、または静的にトランクにグループ化するポートを指定します。	3-88
VLANs	ポートの属性 (デフォルトの PVID、スイッチポートモード、イングレスフィルタリング、GVRP、GARP タイマー) の設定、ポートを静的に割り当てる VLAN の設定を行います。	3-93

メニュー	説明	ページ
Static Addresses	アドレステーブルの静的なエントリの表示または編集、永続エントリの学習機能の使用可能および使用不可の切り替えを行います。	3-99
Spanning Tree	グローバルスパンニングツリーのポートを設定します。	3-102
Spanning Tree Protocol	グローバルスパンニングツリー上のインタフェースの STA ポートレベルを設定します。	3-102
Management Port	ポートの設定	3-80
Connection Status	ポートの接続ステータスを表示します。	3-80
VLANs	ポートの属性 (デフォルトの PVID、スイッチポートモード、インgressフィルタリング、GVRP、GARP タイマー) の設定、ポートを静的に割り当てる VLAN の設定を行います。	3-93
Packet Filtering	アップリンクポートから管理ポートに入るトラフィックのフィルタリングを設定します。	3-110
Monitoring	監視機能の切り替え	3-114
Port Mirroring	ミラー化するソースポートおよびターゲットポートを設定します。	3-114
Port Statistics	Interfaces Group、Ethernetlike MIB、RMON MIB からの情報など、ポートのトラフィックに関する統計情報を表示します。	3-116
SNMP Statistics	SNMP メッセージに関する統計情報を表示します。	3-125
Logs	メッセージログのパラメタの設定、スイッチのメモリーに格納されているメッセージの表示を行います。	3-125

3.2 基本的な設定

3.2.1 システム情報の表示

システムの識別を容易にするために、わかりやすい名前および位置、連絡先の情報を指定します。

コマンド属性

- **Host Name** – スイッチの名前を指定します。
- **Location** – システムシャーシの位置を指定します。
- **Contact** – システムの管理者を指定します。
- **System Up Time** – 管理エージェントを起動してから経過した時間です。
- **System Description** – メーカーによるシステムハードウェアの説明です。
- **Serial Number¹** – メインボードのシリアル番号です。
- **System OID string²** – スイッチのネットワーク管理サブシステムの MIB II オブジェクト ID です。
- **MAC Address³** – スイッチの物理レイヤーアドレスです。
- **Web server²** – HTTP を介した管理アクセスが使用可能かどうかを表示します。
- **Web server port²** – Web インタフェースが使用する TCP ポート番号を表示します。
- **POST result²** – 電源投入時自己診断の結果を表示します。

1: CLIの詳細は、4-39ページの「show version」を参照してください。

2: CLIでのみ確認できます。

3: Webの詳細は、3-11ページの「IPアドレスの設定」を参照してください。

Web – 「Switch Setup」 => 「System Identity」を開きます。ホスト名および位置、システム管理者の連絡先を指定して、「Save Changes」をクリックします。

MicroSystems

Switch Status | Switch Config | Up Links | Down Links | Management Ports | Monitoring

System Identity | Network Identity | Software

System Configuration

To easily identify the switch you will need to provide a descriptive name, location and contact information for the switch, edit the following properties and press the save button to store changes on the switch.

Host Name:

Location:

Contact:

System Uptime: 0 days, 0 hours, 7 minutes, and 50.79 seconds

System Description: Sun Fire B1600

Serial Number: 1

CLI – ホスト名および位置、連絡先を指定します。

```
Console(config)#hostname R&D 5                                4-25
Console(config)#snmp-server location WC 9                    4-51
Console(config)#snmp-server contact Bill                     4-50
Console#show system                                          4-38
System description: Sun Fire B1600
System OID string: 1.3.6.1.4.1.674.10895.4
System information
System Up time: 0 days, 0 hours, 55 minutes, and 54.91 seconds
System Name          : [NONE]
System Location      : [NONE]
System Contact       : [NONE]
MAC address          : 00-00-e8-00-00-01
Web server           : enable
Web server port      : 80
Web secure server    : enable
Web secure server port : 443
POST result

--- Performing Power-On Self Tests (POST) ---
UART Loopback Test ..... PASS
Timer Test ..... PASS
DRAM Test ..... PASS
I2C Initialization ..... PASS
Runtime Image Check ..... PASS
PCI Device Check ..... PASS
Switch Driver Initialization ..... PASS
----- DONE -----
Console#
```

SNMP – 対応する MIB 変数

フィールド名	MIB 変数	アクセス	値の範囲	デフォルト値
System Name (ホスト名)	MIB-II. system. sysName	読み取り / 書き込み	文字列 (長さ 0 ~ 255)	
System Location	MIB-II. system. sysLocation	読み取り / 書き込み	文字列 (長さ 0 ~ 255)	
System Contact	MIB-II. system. sysContact	読み取り / 書き込み	文字列 (長さ 0 ~ 255)	
System UP Time	MIB-II. system. sysUpTime	読み取り 専用	時間間隔 (センチ秒単位)	
System Description	MIB-II. system. sysDescr	読み取り 専用	文字列 (長さ 0 ~ 255)	
System Object Identification	MIB-II. system. sysObjectID	読み取り 専用	オブジェクト識別子	
MAC Address	MIB-II. interfaces. ifTable.ifEntry. ifPhysAddress	読み取り 専用	物理アドレス	
HTTP State (Web サーバー)	sun... ipMgt. ipHttpState	読み取り / 書き込み	使用可能 (1)、 使用不可 (2)	使用可能
HTTP Port (Web サーバー ポート)	sun... ipMgt. ipHttpPort	読み取り / 書き込み	整数 (1 ~ 65535)	80
HTTPS State (セキュリティー 保護された サーバー)	sun... ipMgt. ipHttpsState	読み取り / 書き込み	使用可能 (1)、 使用不可 (2)	使用可能
HTTPS Port (セキュリティー 保護された サーバーポート)	sun... ipMgt. ipHttpsPort	読み取り / 書き込み	整数 (1 ~ 65535)	443

3.2.2 IP アドレスの設定

デフォルトでは、スイッチは、DHCP を使用して IP アドレスおよびデフォルトゲートウェイ、ネットマスクを取得します。

IP アドレスは、手動で設定することも、装置を設定して BOOTP または DHCP サーバーから取得させることもできます。有効な IP アドレスは、ピリオドで区切った 0 ~ 255 の 4 つの 10 進数で構成されます。この設定ソフトウェアは、これ以外の形式を受け入れません。

注 – スwitchの IP アドレスは、実際には、管理ポート (NETMGT) が含まれている VLAN の IP アドレスです。デフォルトでは、管理ポートは VLAN 2 上にあります。そのため、VLAN 2 に IP アドレスを割り当てることによって、スイッチへのネットワークアクセスを設定します。IP アドレスは、管理ポートを含む VLAN にだけ割り当てる必要があります。IP アドレスを任意の VLAN に割り当てると、元の IP アドレスが無効になり、ただちに新しいアドレスが有効になります。

コマンド属性

- **Current IP Address** – 管理アクセスを許可されている VLAN インタフェースの現在のアドレスです。
- **MAC Address¹** – このスイッチの物理レイヤーアドレスです。
- **Management VLAN** – スwitchを管理するために使用できる唯一の VLAN です。デフォルトでは、管理ポート (NETMGT) は、この VLAN (VLAN 2) のメンバーとして設定されています。管理 VLAN を変更する場合は、NETMGT ポートを新しい VLAN のメンバーとして設定しておかないと、スイッチに対して管理アクセスができなくなります。スイッチにアクセスできなくなった場合は、コンソールインタフェースを使用して、新しく設定した管理 VLAN に NETMGT ポートを追加する必要があります。詳細は、4-115 ページの「switchport allowed vlan」を参照してください。

1: CLI の詳細は、3-8 ページの「システム情報の表示」を参照してください。

- **IP Address Mode** – 手動による静的な設定、または動的ホスト構成プロトコル (Dynamic Host Configuration Protocol : DHCP)、ブートプロトコル (BOOTP) のどの方法で IP 機能を使用可能にするかを指定します。DHCP または BOOTP を使用可能にする場合は、サーバーからの応答を受信するまで IP は機能しません。IP 設定情報の要求は、スイッチによって定期的にブロードキャストされます。DHCP または BOOTP の値には、IP アドレスおよびサブネットマスク、デフォルトゲートウェイを設定できます。
- **DHCP** – DHCP を使用します。
 - **Enable Client ID** – DHCP サーバーとのすべての通信でクライアント識別子を記述します。
 - **Text/Hex** – クライアント ID をテキスト文字列 (1 ~ 15 文字) または 16 進数のいずれのデータ型で入力するかを指定します。指定するデータ型は、使用する DHCP サーバーの要件によって異なります。

注 – このメニューで指定したクライアント ID は、システムまたはスイッチを次に再起動したときに、SC によって上書きされます。ファームウェアの次のバージョンでは、Client ID フィールドは廃止される予定です。

- **BOOTP** – BOOTP を使用します。
- **Manual** – 管理インタフェースに特定の値を設定します。
 - **IP Address** – 管理アクセスが許可される VLAN インタフェースのアドレスです。有効な IP アドレスは、ピリオドで区切った 0 ~ 255 の 4 つの数値で構成されます (デフォルト : 0.0.0.0)。
 - **Subnet Mask** – 特定のサブネットへのルーティングに使用するホストアドレスビットを識別するためのマスクです (デフォルト : 255.0.0.0)。
 - **Broadcast Address²** – この IP アドレスに関連付けられているインタフェースでデータグラムを送信するために使用する IP ブロードキャストアドレスです。この値は、スイッチが使用するサブネットおよびネットワークの両方のブロードキャストアドレスに適用されます (デフォルト : 0.0.0.1)。
 - **Gateway IP Address** – ほかのネットワークセグメント上の、装置と管理ホストの間にあるゲートウェイルーターの IP アドレスです (デフォルト : 0.0.0.0)。

2: Web でのみ確認できます。

3.2.2.1 手動による設定

Web – 「Switch Setup」 => 「Network Identity」を開きます。管理インタフェースを選択して、「Manual」ラジオボタンをクリックし、IP アドレスおよびサブネットマスク、デフォルトゲートウェイを指定して、「Save」をクリックします。

microsystems

Switch Status | Switch Config | Up Links | Down Links | Management Ports | Monitoring

System Identity | Network Identity | Software

Sun Fire B1600 > Switch Status > Network Identity

To change the VLAN used for managing the switch, you will need to change the Management VLAN. Note: To prevent loss of connection to the switch, ensure that the Management Port is configured as a member of the new VLAN.

Current IP Address: 10.1.0.2

MAC Address: 00-00-E8-66-66-72

Management VLAN: 2 MgtVlan

Use the radio buttons to select whether the switch IP address is manually configured or dynamically configured by a DHCP or BOOTP Server on your network. The switch will broadcast a request for IP configuration settings on the next power Cancel. Otherwise, you can click the Request Address button to immediately request a new address.

Select IP Address Mode:

DHCP Client

Enable Client ID :

Text Hex

BOOTP

Restart DHCP/BOOTP for changes to take effect: **Save and Restart**

Manual

IP Address: 10.1.0.2

Subnet Mask: 255.255.255.0

Broadcast Address: 0.0.0.1

Gateway IP Address: 0.0.0.0

Save **Cancel**

注 – 入力したデータが無効であるというエラーメッセージが表示された場合は、それぞれの IP アドレスが正しく指定されているかどうかを確認してください。

CLI – 管理インタフェースおよび IP アドレス、デフォルトゲートウェイを指定します。

```

Console#config
Console(config)#interface vlan 2                                4-75
Console(config-if)#ip address 10.1.0.2 255.255.255.0          4-63
Console(config-if)#exit
Console(config)#ip default-gateway 10.1.0.254                 4-67
Console(config)#

```

SNMP – 対応する MIB 変数

フィールド名	MIB 変数	アクセス	値の範囲	デフォルト値
Management VLAN	sun... switchMgt. switchManagementVlan	読み取り/ 書き込み	整数 (1 ~ 4094)	1
IP Address Mode	sun... vlanMgt. vlanTable.vlanEntry. vlanAddressMethod	読み取り/ 書き込み	user (1)、 bootp (2)、 dhcp (3)	user
IP Address Configuration	MIB-II. ip.ipAddrTable. ipAddrEntry. ipAdEntAddr	読み取り/ 書き込み	IP アドレス	
Subnet Mask Configuration	MIB-II. ip.ipAddrTable. ipAddrEntry. ipAdEntNetMask	読み取り/ 書き込み	IP アドレス	
Broadcast Address	MIB-II. ip.ipAddrTable. ipAddrEntry. ipAdEntBcastAddr	読み取り 専用	整数 (0 ~ 1)	1
Default Gateway Configuration	sun... ipMgt. netDefaultGateway	読み取り/ 書き込み	IP アドレス	

3.2.2.2 DHCP および BOOTP の使用

デフォルトでは、スイッチは DHCP または BOOTP サービスを使用して IP 設定情報を取得します。

Web – 「Switch Setup」 => 「Network Identity」を開きます。管理インタフェースを選択し、「DHCP」ラジオボタンまたは「BOOTP」ラジオボタンをクリックします。

デフォルトでは、シャーシのシステムコントローラがスイッチにクライアント識別子を提供します。クライアント識別子は、スイッチが SSC0 または SSC1 のどちらにあるかによって、SUNW,SWITCH_ID=*serial number of chassis*,0 または SUNW,SWITCH_ID=*serial number of chassis*,1 になります。クライアント識別子は「Enable Client ID」チェックボックスで指定できますが、この値が有効になるのはシステムコントローラを次にリセットまたは再起動したときです。しかし、この方法による指定はお勧めできません。ファームウェアの次のバージョンでは、「Enable Client ID」は廃止される予定です。

microsystems

Switch Status | Switch Config | Up Links | Down Links | Management Ports | Monitoring

System Identity | Network Identity | Software

Current IP Address: 10.1.0.1

MAC Address: 00-00-E8-66-66-72

Management VLAN: 2 MgtVlan

Use the radio buttons to select whether the switch IP address is manually configured or dynamically configured by a DHCP or BOOTP Server on your network. The switch will broadcast a request for IP configuration settings on the next power Cancel. Otherwise, you can click the Request Address button to immediately request a new address.

Select IP Address Mode:

DHCP Client

Enable Client ID :

Text Hex

0010b55169f7

BOOTP

Restart DHCP/BOOTP for changes to take effect: **Save and Restart**

注 – 管理接続ができなくなった場合は、コンソール接続で `show ip interface` と入力して新しいスイッチアドレスを指定してください。

注 – このメニューで指定したクライアント ID は、システムまたはスイッチを次に再起動したときに、SC によって上書きされます。ファームウェアの次のバージョンでは、Client ID フィールドは廃止される予定です。

CLI – 管理インタフェースを指定し、IP アドレスモードに DHCP または BOOTP を設定して、`ip dhcp restart` コマンドを実行します。

```

Console#config
Console(config)#interface vlan 2                                4-75
Console(config-if)#ip address dhcp                             4-63
Console(config-if)#ip dhcp client-id hex 00-00-e8-66-65-72    4-66
Console(config-if)#end
Console#ip dhcp restart                                        4-65
Console#show ip interface                                     4-67
IP address and netmask: 10.1.0.54 255.255.255.0 on VLAN 2,
  and address mode: DHCP.
Console#

```

DCHP の更新 – DHCP は、クライアントに無期限または期限付きでアドレスを割り当てます。アドレスの有効期限が切れるか、スイッチが別のネットワークエージェントに移された場合は、スイッチへの管理アクセスができなくなります。この場合は、スイッチを再起動するか、クライアント要求を送信して DHCP サービスを再起動します。

Web – DHCP によって割り当てられたアドレスが機能なくなると、Web インタフェースを介して IP 設定を更新できなくなります。現在のアドレスが有効な場合のみ、Web インタフェースを介して DHCP サービスを再起動できます。

CLI – DHCP サービスを再起動するには、次のコマンドを実行します。

```

Console#ip dhcp restart                                        4-65

```

SNMP – 対応する MIB 変数

フィールド名	MIB 変数	アクセス	値の範囲	デフォルト値
Management VLAN	sun... switchMgt. switchManagementVlan	読み取り/ 書き込み	整数 (1 ~ 4094)	1
IP Address Mode	sun... vlanMgt. vlanTable.vlanEntry. vlanAddressMethod	読み取り/ 書き込み	user (1)、 bootp (2)、 dhcp (3)	dhcp
DHCP Client ID	sun... ipMgt. dhcpClientIfClientId	読み取り/ 書き込み	オクテット文字列 (MAC アドレス)	
DHCP Restart	sun... ipMgt. ipDhcpRestart	読み取り/ 書き込み	restart (1)、 noRestart (2)	noRestart

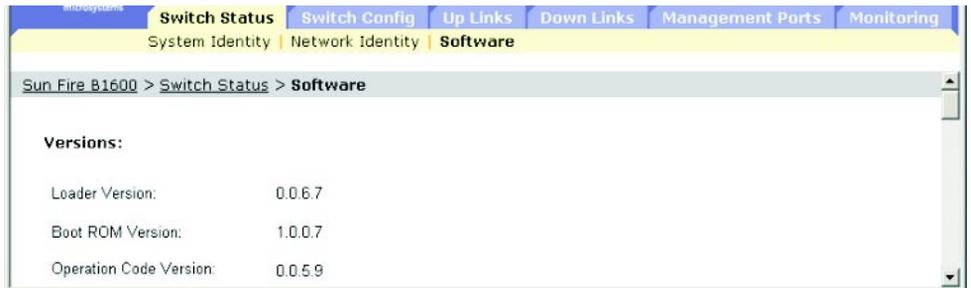
3.2.3 スイッチソフトウェアのバージョンの表示

コマンド属性

- **Loader Version** – ロダーコードのバージョン番号です。
- **Boot-Rom Version** – 起動コードのバージョン番号です。
- **Operation Code Version** – 実行時コードのバージョン番号です。
- **Unit ID*** – アクティブなスイッチの ID で、この値は常に 1 です。

* CLI でのみ確認できます。Sun Fire B1600 ブレードシステムシャーシのスイッチの現在のバージョンでは、Unit ID の値は重要ではありません。

Web – 「Switch Setup」 => 「Software」 を開きます。



CLI – バージョン情報を表示するには、次のコマンドを実行します。

```
Console#show version 4-39
Unit1
  Serial number      :1
  Service tag        :
  Hardware version   :R0B
  Number of ports    :25
  Main power status  :up
  Redundant power status :not present
Agent(master)
  Unit id            :1
  Loader version     :0.0.6.5
  Boot rom version   :0.0.7.3
  Operation code version :1.0.0.1
Console#
```

SNMP – 対応する MIB 変数

フィールド名	MIB 変数	アクセス	値の範囲	デフォルト値
Switch Serial Number	SUN. switchMgt. switchInfoTable. switchInfoEntry. swSerialNumber	読み取り 専用	表示文字列 (長さ 0 ~ 80)	
Switch Hardware Version	SUN. switchMgt. switchInfoTable. switchInfoEntry. swHardwareVer	読み取り 専用	表示文字列 (長さ 0 ~ 20)	
Switch Port Number	SUN. switchMgt. switchInfoTable. switchInfoEntry. swPortNumber	読み取り 専用	整数	25
Switch Unit Index	SUN. switchMgt. switchInfoTable. switchInfoEntry. swUnitIndex	アクセス 不可	整数	1
Switch Loader Version	sun... switchMgt. switchInfoTable. switchInfoEntry. swLoaderVer	読み取り 専用	文字列 (長さ 0 ~ 20)	
Switch Boot Rom Version	sun... switchMgt. switchInfoTable. switchInfoEntry. swBootRomVer	読み取り 専用	文字列 (長さ 0 ~ 20)	
Switch Operation Code Version	sun... switchMgt. switchInfoTable. switchInfoEntry. swOpCodeVer	読み取り 専用	文字列 (長さ 0 ~ 20)	

3.2.4 ファームウェアの管理

ファームウェアは、TFTP サーバーを使用してアップロードおよびダウンロードすることができます。TFTP サーバー上のファイルに実行時コードを保存しておくこと、あとでそのファイルをスイッチにダウンロードして動作を回復できます。また、前のバージョンのファームウェアを上書きすることなく、新しいファームウェアを使用するようにスイッチを設定することもできます。

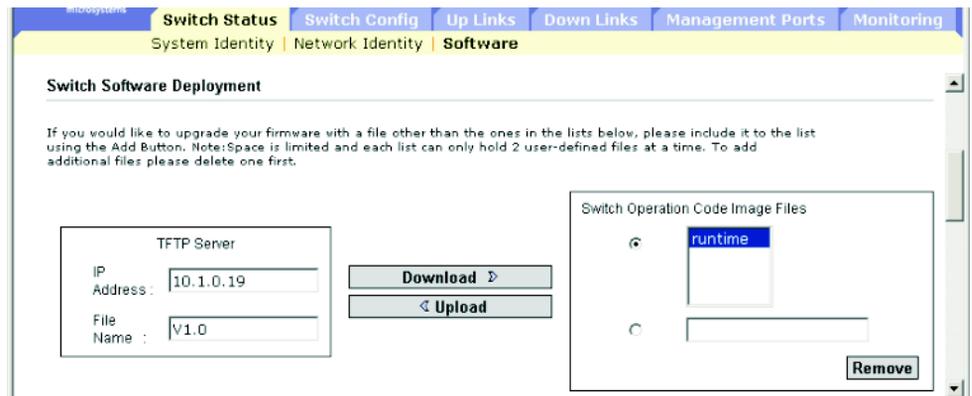
コマンド属性

- 対象ファイル名にはスラッシュ (\ または /) を使用できません。ファイル名の先頭の文字はピリオド (.) 以外にする必要があります。ファイル名は、TFTP サーバーでは 127 文字以内、スイッチでは 32 文字以内で指定します。使用できる文字は、A ~ Z および a ~ z、0 ~ 9、「.」、「-」、「_」です。
- スwitch上のファイルディレクトリには、システムソフトウェアファイル (実行時ファームウェアを含む) を 2 つだけ格納できます。起動用に指定されているファイルは削除できません。システムソフトウェアファイル 2 つ存在する場合は、起動用に指定されていない方のファイルを削除して新しいファイルに置き換えるか、新しいファイルを既存のファイル名で同じディレクトリにコピーします。また、起動ファイルの指定を解除してそのファイルを削除し、新しいバージョンのシステムソフトウェアファイルを同じディレクトリにコピーして起動ファイルに指定することもできます。

3.2.4.1 サーバーからのシステムソフトウェアのダウンロード

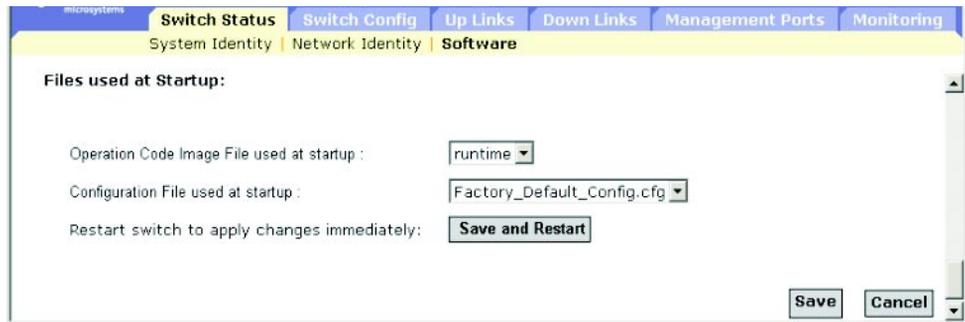
実行時コードをダウンロードするときは、対象ファイル名を指定して現在のイメージと置き換えるか、いったん現在の実行時コードファイルとは別の名前でファイルをダウンロードした上で、新しいファイルを起動ファイルとして設定します。

Web - 「Switch Status」 => 「Software」を開きます。TFTP サーバーの IP アドレスとダウンロードするソフトウェアのファイル名を入力し、スイッチ上の上書きするファイルを選択するか、新しいファイル名を指定して、「Download」をクリックします。



注 – 入力したデータが無効であるというエラーメッセージが表示された場合は、入力した IP アドレスまたはファイル名が誤っているか、あるいは TFTP 転送を行うための正しいアクセス権を持っていない可能性があります。また、スイッチ上の使用可能なメモリーが不足している可能性もあります。

新しいファイル名でダウンロードした場合は、起動時に使用するオペレーションコードのファイルをドロップダウンボックスから選択し、「Save」をクリックします。新しいファームウェアを起動するには、「Save and Restart」をクリックしてシステムを再起動する必要があります。



CLI – TFTP サーバーの IP アドレスを入力して `config` または `opcode` のいずれかのファイルタイプを選択し、ソースファイル名と対象ファイル名を入力し、新しいファイルでシステムを起動するように設定して、スイッチを再起動します。

```
Console#copy tftp file 4-18
TFTP server ip address: 10.1.0.99
Choose file type:
  1. config:  2. opcode: <1-2>: 2
Source file name: v10.bix
Destination file name: V10000
\Write to FLASH Programming.
-Write to FLASH finish.
Success.

Console#config
Console(config)#boot system opcode: V10000 4-23
Console(config)#exit
Console#reload 4-15
```

新しいファームウェアを起動するには、`reload` コマンドを実行してシステムを再起動する必要があります。

SNMP – 対応する MIB 変数

フィールド名	MIB 変数	アクセス	値の範囲
Switch Operation Code Image Files	未定義		
TFTP Server IP Address	sun... tftpMgt. tftpServer	読み取り / 書き込み	IP アドレス
TFTP File Type	sun... tftpMgt. tftpFileType	読み取り / 書き込み	opcode (1)、 config (2)
TFTP Source File Name	sun... tftpMgt. tftpSrcFile	読み取り / 書き込み	文字列 (長さ 0 ~ 127)
TFTP Destination File Name	sun... tftpMgt. tftpDestFile	読み取り / 書き込み	文字列 (長さ 0 ~ 127)
TFTP Action	sun... tftpMgt. tftpAction	読み取り / 書き込み	notDownloading (1)、 downloadToPROM (2)、 downloadToRAM (3) (未サポート) upload (4)
TFTP Status	sun... tftpMgt. tftpStatus	読み取り / 書き込み	tftpSuccess (1)、 tftpStatusUnknown (2)、 tftpGeneralError (3)、 tftpNoResponseFromServer (4)、 tftpDownloadChecksumError (5)、 tftpDownloadIncompatible Image(6)、 tftpTftpFileNotFound(7)、 tftpTftpAccessViolation(8)
Restart Operation Code File	sun... restartMgt. restartOpCodeFile	読み取り / 書き込み	表示文字列 (長さ 0 ~ 127)
Restart Action	sun... restartMgt. restartControl	読み取り / 書き込み	running (1)、 warmBoot (2)、 coldBoot (3)

3.2.5 設定情報の保存および復元

設定情報は、TFTP サーバーを使用してアップロードまたはダウンロードすることができます。構成ファイルを保存しておくこと、あとでスイッチにダウンロードして設定を復元することができます。

コマンド属性

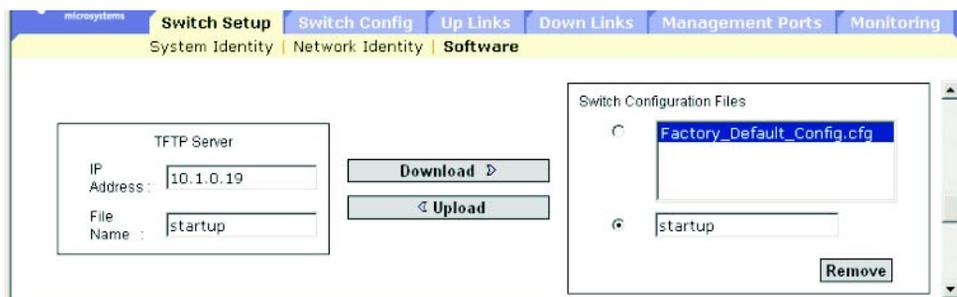
- 対象ファイル名にはスラッシュ (\ または /) を使用できません。ファイル名の先頭の文字はピリオド (.) 以外にする必要があります。ファイル名は、TFTP サーバーでは 127 文字以内、スイッチでは 32 文字以内で指定します。使用できる文字は、A～Z および a～z、0～9、「.」、「-」、「_」です。
- ユーザー定義構成ファイルの最大数は、使用可能なメモリー容量によって制限されます。

3.2.5.1 サーバーからの設定情報のダウンロード

構成ファイルは、新しいファイル名でダウンロードして起動ファイルとして設定することも、現在の起動構成ファイルを指定して直接置き換えることもできます。

Factory_Default_Config.cfg は TFTP サーバーにコピーすることはできませんが、スイッチの対象ファイルとして使用することはできません。

Web – 「Switch Setup」 => 「Software」を開きます。TFTP サーバーの IP アドレスとダウンロードするファイルの名前を入力し、スイッチ上の上書きするファイルを選択するか、新しいファイル名を指定して、「Download」をクリックします。



新しいファイル名でダウンロードした場合は、新しいファイル名をドロップダウンボックスから選択し、「Save」をクリックします。新しい設定を使用するには、「Save and Restart」をクリックしてシステムを再起動する必要があります。



CLI – TFTP サーバーの IP アドレスを入力し、サーバー上のソースファイル名とスイッチ上の起動ファイル名を設定して、スイッチを再起動します。

```

Console#copy tftp startup-config                               4-18
TFTP server ip address: 192.168.1.19
Source configuration file name: startup2.0
Startup configuration file name [startup] : startup2.0
\Write to FLASH Programming.
-Write to FLASH finish.
Success.

Console#reload
System will be restarted, continue <y/n>?y

```

起動構成ファイルを新しいファイル名でダウンロードした場合は、あとでこのファイルを起動ファイルとして設定して、スイッチを再起動します。

```

Console#config
Console(config)#boot system config: startup-new             4-23
Console(config)#exit
Console#reload                                             4-15
System will be restarted, continue <y/n>?y

```

SNMP – 対応する MIB 変数

フィールド名	MIB 変数	アクセス	値の範囲
TFTP Server IP Address	sun... tftpMgt. tftpServer	読み取り/ 書き込み	IP アドレス
TFTP File Type	sun... tftpMgt. tftpFileType	読み取り/ 書き込み	opcode (1)、 config (2)
TFTP Source File Name	sun... tftpMgt. tftpSrcFile	読み取り/ 書き込み	表示文字列 (長さ 0 ~ 127)
TFTP Action	sun... tftpMgt. tftpAction	読み取り/ 書き込み	notDownloading (1)、 downloadToPROM (2)、 downloadToRAM (3)、 upload (4)
TFTP Status	sun... tftpMgt. tftpStatus	読み取り/ 書き込み	tftpSuccess (1)、 tftpStatusUnknown (2)、 tftpGeneralError (3)、 tftpNoResponseFromServer (4)、 tftpDownloadChecksumError (5)、

フィールド名	MIB 変数	アクセス	値の範囲
			tftpDownloadIncompatibleImage(6)、 tftpTftpFileNotFound(7)、 tftpTftpAccessViolation(8)
Restart Configuration File	sun... restartMgt. restartConfigFile	読み取り / 書き込み	表示文字列 (長さ 0 ~ 127)
Restart Action	sun... restart.Mgt. restartControl	読み取り / 書き込み	running (1)、 warmBoot (2)、 coldBoot (3)

3.2.6 ユーザー認証の設定

指定したユーザー名およびパスワードに基づいて管理アクセスを制限するには、「Security」メニューを使用します。スイッチのアクセス権は、手動で設定することも、RADIUS または TACACS+ プロトコルに対応する遠隔アクセス認証サーバーを使用して設定することもできます。

アクセス権には、通常 (Normal) および特権 (Privileged) の 2 つのレベルがあります。通常レベルでは使用できるコマンドは制限されていますが、特権レベルではすべてのコマンドを使用できます。デフォルトの管理者アカウントには、オンボードエージェントを管理するすべてのパラメタに対する書き込みアクセス権が付与されています。そのため、すぐにパスワードを割り当てて、安全な場所に保管する必要があります。

注 – デフォルトの管理者名は「admin」で、パスワードは「admin」です。

コマンドの使用法

- デフォルトでは、管理アクセスは、常にローカルのスイッチに格納されている認証データベースと照合して確認されます。遠隔認証サーバーを使用している場合は、認証シーケンスおよび指定した遠隔認証プロトコルのそれぞれに対応するパラメタを設定する必要があります。
- RADIUS (Remote Authentication Dial-in User Service) および TACACS (Terminal Access Controller Access Control System) はログオン認証プロトコルです。これらのプロトコルは、中央サーバー上で動作するソフトウェアを使用して、ネットワーク上の RADIUS または TACACS 対応装置へのアクセスを管理します。認証サーバーにはデータベースがあり、スイッチへの管理アクセスを必要とするユーザーまたはグループのそれぞれに割り当てられたユーザー名およびパスワードの組と、それに関連する特権レベルが格納されています。

注 - RADIUS または TACACS サーバーで特権レベルを設定する場合、レベル 0 を設定すると、ゲスト (通常実行) としてスイッチにアクセスできます。レベル 15 を設定した場合にだけ、管理者アクセス (特権実行) が可能になります。

- RADIUS は UDP を、TACACS は TCP を使用します。UDP はベストエフォート型の通信しか提供しませんが、TCP はコネクション型トランスポートを提供します。また、RADIUS ではクライアントからサーバーへのアクセス要求パケットのパスワードだけが暗号化されますが、TACACS ではパケットの本体全体が暗号化されます。
- RADIUS および TACACS ログオン認証では、コンソールポートまたは Web ブラウザ、telnet を介して管理アクセスを制御します。これらのアクセス方法は、認証サーバー上で設定する必要があります。
- RADIUS および TACACS ログオン認証では、ユーザー名およびパスワードの組のそれぞれに対して特権レベルが割り当てられます。ユーザー名およびパスワード、特権レベルは、認証サーバー上で設定する必要があります。
- 各ユーザーに対して、認証シーケンスを示す 1 ~ 3 通りの認証方法を指定できます。たとえば、(1) RADIUS、(2) ローカルの順序で選択すると、RADIUS サーバーのユーザー名とパスワードが最初に確認されます。RADIUS サーバーが使用できない場合は、ローカルのユーザー名とパスワードが確認されます。

コマンド属性

- Authentication Mechanisms
 - Require User Authentication - 認証が必要かどうかを指定します。
 - Preference - ここに指定した順序でスイッチがユーザー認証を行います。
- Authentication Server Settings
 - Server IP Address - 認証サーバーのアドレスです (デフォルト : 10.1.0.1)。
 - Server Port Number - 認証メッセージに使用される認証サーバーのネットワーク (UDP) ポートです (範囲 : 1 ~ 65535、デフォルト : 1812)。
 - Encryption Key - クライアントへのログオンアクセスの認証に使用される暗号化鍵です。文字列には空白文字を使用しないでください (最大長 : 20 文字)。
 - No. of Retries* - スイッチが認証サーバーによってログインアクセスを認証する回数です (範囲 : 1 ~ 30、デフォルト : 2)。
 - Timeout for reply* - スイッチが要求を再送する前に応答を待つ秒数です (範囲 : 1 ~ 65535、デフォルト : 5)。
- Local Access Authentication
 - User Account - ユーザーの名前です (最大長 : 8 文字、最大ユーザー数 : 5)。
 - Access Level - ユーザーのレベルを指定します (オプション : Normal および Privileged)。
 - Password - ユーザーのパスワードを指定します (最大長 : 8 文字のプレーンテキスト、大文字小文字を区別)。

* RADIUS サーバー認証にのみ適用されます。

Web - 「Switch Config」 => 「Security」を開きます。ローカル認証または遠隔認証の優先順位を設定するには、認証シーケンス (1 ~ 3 通りの方法) を指定し、その認証方法のパラメタを指定して「Save」をクリックします。

The screenshot shows the 'Switch Config' page for 'Security'. The 'Authentication Mechanisms' section has 'Require User Authentication' checked. The preferences are set to TACACS+ (First-preference), RADIUS (Second-preference), and Local (Third-preference). The 'Authentication Server Settings' section includes RADIUS and TACACS settings. RADIUS settings: Server IP Address: 10.11.12.13, No. of Retries: 2, Server Port Number: 1812, Timeout for reply: 5, Encryption Key: *****. TACACS settings: Server IP Address: 192.160.1.25, Server Port Number: 38, Encryption Key: *****. 'Save' and 'Cancel' buttons are at the bottom right.

ローカルアクセスのための認証パラメタを設定するには、ユーザー名およびパスワード、アクセスレベルを指定して「Add」をクリックします。

The screenshot shows the 'Local Access Authentication' section. It has two tables for user accounts. The first table lists 'admin' (Privileged) and 'guest' (Normal) with 'Change Password...' and 'Remove' buttons. The second table has a 'User' field with 'bot', an 'Access Level' dropdown set to 'Privileged', and a 'password:' field with '*****', followed by an 'Add' button.

CLI — ユーザー名とアクセスレベルを割り当て (0 : Normal、15 : Privileged)、パスワードを指定します。次に、RADIUS および TACACS 遠隔クライアント認証に必要な項目を設定します。

```

Console(config)#username bob access-level 15          4-25
Console(config)#username bob password smith
Console(config)#authentication login local tacacs radius 4-42
Console(config)#tacacs-server host 192.168.1.24      4-46
Console(config)#tacacs-server port 181              4-47
Console(config)#tacacs-server key green              4-47
Console(config)#radius-server host 192.168.1.25      4-43
Console(config)#radius-server port 181              4-43
Console(config)#radius-server key white              4-44
Console(config)#radius-server retransmit 5           4-44
Console(config)#radius-server timeout 10             4-45
Console(config)#

```

SNMP — 対応する MIB 変数

フィールド名	MIB 変数	アクセス	値の範囲	デフォルト値
User Name	未定義			
Password	未定義			
Access Level	未定義			
Authentication Sequence	未定義			
RADIUS Server Address	sun... securityMgt.radiusMgt. radiusServerAddress	読み取り / 書き込み	IP アドレス	10.11.12.13
RADIUS Server Port Number	sun... securityMgt.radiusMgt. radiusServerPortNumber	読み取り / 書き込み	整数 (1 ~ 65535)	1812
RADIUS Server Encryption Key	sun... securityMgt.radiusMgt. radiusServerKey	読み取り / 書き込み (読み取りの 場合は常に 0 が戻る)	文字列 (長さ 0 ~ 20)	
RADIUS Server Retransmit	sun... securityMgt.radiusMgt. radiusServerRetransmit	読み取り / 書き込み	整数 (1 ~ 65535)	2
RADIUS Server Timeout	sun... securityMgt.radiusMgt. radiusServerTimeout	読み取り / 書き込み	整数 (1 ~ 65535) 秒	5

フィールド名	MIB 変数	アクセス	値の範囲	デフォルト値
TACACS Server Address	sun... securityMgt.tacacsMgt. tacacsServerAddress	読み取り / 書き込み	IP アドレス	
TACACS Server Port Number	sun... securityMgt.tacacsMgt. tacacsServerPortNumber	読み取り / 書き込み	整数 (1 ~ 65535)	
TACACS Server Encryption Key	sun... securityMgt.tacacsMgt. tacacsServerKey	読み取り / 書き込み (読み取りの 場合は常に 0 が戻る)	文字列 (長さ 0 ~ 20)	

3.2.7 SNMP の設定

SNMP (Simple Network Management Protocol) は、ネットワーク上の装置やその他の要素を管理するための通信プロトコルです。一般的に、SNMP では、スイッチ、ルーター、ホストコンピュータなどの装置を管理します。SNMP を使用して、これらの装置がネットワーク環境で正しく動作するように設定したり、装置を監視して性能を評価し、潜在的な問題を検出します。

スイッチにはオンボード SNMP エージェントが組み込まれています。このエージェントによって、スイッチのハードウェアの状態と、スイッチのポートを通過するトラフィックが常時監視されます。ネットワーク管理ホストは、SunNet Manager などのソフトウェアを使用して、この情報にアクセスできます。オンボードエージェントへのアクセス権は、コミュニティ文字列によって制御されます。スイッチとの通信では、管理ホストは、最初に認証のための有効なコミュニティ文字列を送信する必要があります。以降の節では、コミュニティ文字列と関連するトラップ機能の設定オプションについて説明します。

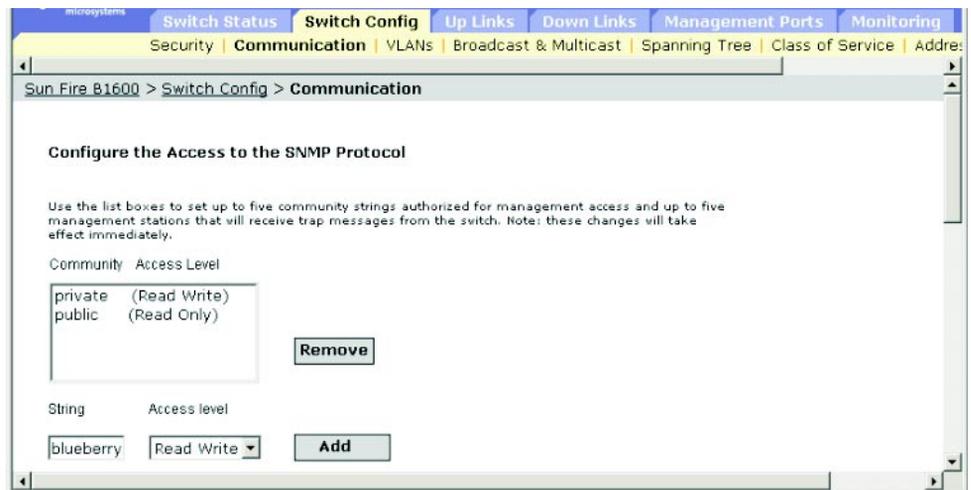
3.2.7.1 SNMP プロトコルへのアクセス権の設定

管理アクセスのための認証されたコミュニティ文字列は、最大で5つ設定できます。セキュリティのため、デフォルトの文字列は削除してください。

コマンド属性

- **Community** – コミュニティ文字列はパスワードのように機能するもので、SNMP プロトコルへのアクセスを許可します。
デフォルトの文字列：「public」（読み取り専用アクセス）、「private」（読み取りおよび書き込みアクセス）
 - 範囲：1～32文字、大文字と小文字を区別
 - デフォルト：「public」（読み取り専用アクセス）、「private」（読み取りおよび書き込みアクセス）
- **Access Level**
 - **Read Only** – 読み取り専用アクセスを指定します。認証された管理ホストは、MIB オブジェクトの取り出しだけを行うことができます。
 - **Read/Write** – 読み取りおよび書き込みアクセスを指定します。認証された管理ホストは、MIB オブジェクトの取り出しおよび変更の両方を行うことができます。

Web – 「Switch Config」=>「Communication」を開きます。必要に応じて新しいコミュニティ文字列を追加し、「Access Level」ドロップダウンリストからアクセス権を選択して「Add」をクリックします。



CLI – 次に、読み取りおよび書き込みアクセス権を持つ文字列「blueberry」を追加する例を示します。

```
Console(config)#snmp-server community blueberry rw
Console(config)#
```

4-49

SNMP – 対応する MIB 変数

この機能に対応する MIB 変数はありません。

3.2.7.2 トラップマネージャーおよびトラップタイプの指定

状態の変更を示すトラップは、スイッチから指定されたトラップマネージャーに対して発行されます。トラップマネージャーを指定して、SunNet Manager などのネットワーク管理プラットフォームによって、スイッチから管理ホストに重要なイベントを通知する必要があります。スイッチからトラップメッセージを受信する管理ホストは、最大で 5 台指定できます。このスイッチがサポートするトラップのリストについては、A-3 ページの「サポートトラップ」を参照してください。

コマンド属性

- **IP Address** – ホスト (受信側) のインターネットアドレスです (ホストアドレスの最大数: トラップの送信先の IP アドレスエントリ 5 つ)。
- **Community** – 通知操作で送信される、パスワードのように機能するコミュニティー文字列です。この文字列は、トラップマネージャーのリストに設定できませんが、SNMP プロトコルのリストにも定義することをお勧めします (最大長: 32 文字)。
- **Version** – ホストで動作している SNMP がバージョン 1 またはバージョン 2c のどちらであることを示します。
- **Generate SNMP notification for**
 - **Port link up and down events** – ポートリンクが確立または切断されたときにトラップメッセージを発行します。
 - **Authentication traps** – SNMP アクセス認証処理で無効なコミュニティー文字列が送信された場合にトラップメッセージを発行します。

Web – 「Switch Setup」 => 「Communications」を開きます。メッセージを受信する各トラップマネージャーの IP アドレスとコミュニティ文字列を設定し、「Add」をクリックします。必要に応じて、「Port link up and link down events」チェックボックスまたは「Authentication traps」チェックボックスをオンにして「Save」をクリックします。

Specify TrapManagers

IP Address	Community	Version
192.168.2.6	private	1
192.168.2.7	private	1

Remove

IP Address: 192.168.2.8 String: private Version: 1 Add

Specify Trap Types

To disable the switch from sending link-up, link-down or authentication traps, you should uncheck these check boxes and press the save button to store the changes on the switch.

Generate SNMP notification for :

link up and down events

Authentication traps

Save Cancel

CLI – 次に、トラップマネージャーを追加して、リンクの接続および切断と、認証トラップの通知を使用可能にする例を示します。

```
Console(config)#snmp-server host 10.1.0.19 private version 1 4-51
Console(config)#snmp-server enable traps link-up-down 4-52
Console(config)#snmp-server enable traps authentication
```

SNMP – 対応する MIB 変数

フィールド名	MIB 変数	アクセス	値の範囲	デフォルト値
Trap Destination Address	sun... trapDestMgt. trapDestTable. trapDestEntry. trapDestAddress	アクセス なし	IP アドレス	
Trap Destination Community	sun... trapDestMgt. trapDestTable. trapDestEntry. trapDestCommunity	読み取り / 作成	文字列 (長さ 0 ~ 127)	
Trap Destination Version	sun... trapDestMgt. trapDestTable. trapDestEntry. trapDestStatus	読み取り / 作成	version 1 (1)、 version 2 (2)	
Trap Destination Status	sun... trapDestMgt. trapDestTable. trapDestEntry. trapDestStatus	読み取り / 作成	valid (1)、 invalid (2)	
Enable Link-up-down Traps	MIB-II ifMIB.ifMIBObjects. ifXTable.ifXEntry. ifLinkUpDownTrapEnable	読み取り / 書き込み	enabled (1)、 disabled (2)	enabled

3.3 グローバルなネットワークプロトコルの設定

この節では、仮想 LAN (VLAN)、マルチキャストサービス、スパンニングツリーアルゴリズム、サービスクラスの要件に基づくデータ処理、アドレステーブルの表示または静的アドレスの設定のための、グローバルなスイッチ設定について説明します。

3.3.1 VLAN の設定

ルーターを使用する従来型のネットワークでは、ブロードキャストトラフィックは複数のドメインに分割されています。スイッチは、本来はブロードキャストドメインをサポートしていません。そのため、IPX や NetBeui などのトラフィックを処理する大規模ネットワークでは、ブロードキャストストームが発生する可能性があります。IEEE 802.1Q に準拠する VLAN を使用すると、ネットワークノードのグループを個別のブロードキャストドメインに分割して管理できるため、ブロードキャストトラフィックを送信元グループだけに制限できます。こうしてネットワーク環境が整理されて、より安全になります。

IEEE 802.1Q VLAN とは、ネットワーク内のどの場所に配置しても、同じ物理セグメントに属している場合と同様に通信できるポートのグループです。

VLAN を使用すると、物理的な接続を変更することなく装置を新しい VLAN 環境に移行できるため、ネットワーク管理が容易になります。VLAN は、部署ごとのグループ (営業部、研究開発部など)、用途別のグループ (電子メール用など)、マルチキャストグループ (ビデオ会議などのマルチメディアアプリケーションが使用) などに合わせて簡単に構成できます。

VLAN では、ブロードキャストトラフィックが減少するため、ネットワーク効率が大きく向上します。また、ネットワークを変更するときに、IP アドレスや IP サブネットを変更する必要がありません。VLAN では、設定したレイヤー 3 リンクを通して別の VLAN にトラフィックを送信するため、高レベルのネットワークセキュリティが保証されます。

このスイッチは、次の VLAN 機能をサポートしています。

- IEEE 802.1Q 標準に準拠した最大 255 の VLAN をサポート
- 明示的または暗黙的なタグ付けと GVRP プロトコルによって、複数のスイッチに渡る分散 VLAN を学習
- 1 つのポートが複数の VLAN に参加できるポートオーバーラッピング
- エンドステーションの複数の VLAN への接続
- VLAN 対応装置と VLAN 非対応装置との間のトラフィックの通過
- 優先順位別のタグ付け

ポートの VLAN への割り当て

スイッチで VLAN を使用可能にする前に、各ポートを対応する VLAN グループに割り当てる必要があります。デフォルトでは、すべてのポートはタグなしポートとして VLAN 1 に割り当てられています。中間のネットワーク装置および接続先のホストが VLAN をサポートしている場合、ポートから 1 つ以上の VLAN にトラフィックを配信するには、ポートをタグ付きポートとして追加します。次に、このトラフィックを配信するパス上に配置された VLAN 対応ネットワーク装置のポートを、GVRP を使用して動的に、または手動で、同じ VLAN に割り当てます。中間のネットワーク装置および接続先のホストが VLAN をサポートしていない場合に、このスイッチのポートを 1 つ以上の VLAN に参加させるには、ポートをタグなしポートとして VLAN に追加する必要があります。

注 – VLAN タグ付きフレームは、VLAN 対応および VLAN 非対応のどちらのネットワーク相互接続装置でも通過しますが、VLAN タグをサポートしていないエンドノードホストには送信しないようにしてください。

VLAN の分類 – フレームを受信すると、スイッチは、2 つの方法のいずれかによってフレームを分類します。フレームにタグが付いていない場合は、受信ポートの PVID に基づいて、関連する VLAN にこのフレームを割り当てます。フレームにタグが付いている場合は、そのタグの VLAN ID を使用して、フレームのポートブロードキャストドメインを識別します。

ポートオーバーラッピング – ポートオーバーラッピングを使用すると、ファイルサーバー、プリンタなどの、異なる VLAN グループ間で共有されているネットワークリソースにアクセスできます。オーバーラップしない VLAN を実装していて、通信を行う必要がある場合は、レイヤー 3 のルーターまたはスイッチを使用することでその VLAN に接続できます。

ポートベース VLAN – ポートベースの (静的な) VLAN は、特定のポートに手動で割り当てられています。スイッチは、宛先の MAC アドレスとそれに関連するポートに基づいて転送先を決定します。そのため、転送またはフラッドリング (洪水) を正しく決定するには、スイッチが、MAC アドレスと関連するポートとの実行時点での関係 (つまり VLAN との関係) を学習する必要があります。GVRP が使用可能になっていると、この処理は自動的に行われます。

VLAN の自動登録 – GARP VLAN Registration Protocol (GVRP) は、各エンドステーションの割り当て先の VLAN を、スイッチが自動的に学習するためのシステムを規定するものです。IEEE 802.1Q VLAN プロトコルをサポートするエンドステーションまたはそのネットワークアダプタは、参加を希望する VLAN グループを示すメッセージをネットワークにブロードキャストするように設定できます。スイッチは、このメッセージを受信すると、その受信ポートを自動的に指定された VLAN に割り当てて、それ以外のすべてのポートにこのメッセージを転送します。GVRP をサポートする別のスイッチがこのメッセージを受信すると、そのスイッチも受信したポートを指定された VLAN に割り当てて、それ以外のすべてのポートにこのメッ

セージを転送します。VLAN の要求は、この方法でネットワーク全体に伝播されません。こうして、GVRP 対応装置は、エンドステーションの要求だけに基づいて、自動的に VLAN グループとして設定されます。

ネットワークに GVRP を実装するには、まずオペレーティングシステムまたはほかのアプリケーションソフトウェアによって必要な VLAN にホスト装置を追加して、この VLAN がネットワークに伝播されるようにします。このホストに直接接続するエッジスイッチと、ネットワークのコアスイッチのどちらも、その装置間のリンクで GVRP を使用できるようにします (3-93 ページの「インタフェースの VLAN 動作の設定」を参照)。また、ネットワーク内のセキュリティの境界を定めて、通知の伝播を制限するエンドステーションのポートで GVRP を使用不可にするか、VLAN へのポートの参加を禁止する必要があります。

注 – GVRP をサポートしないホスト装置がある場合は、この装置に接続するスイッチポートに静的に VLAN を設定します (3-42 ページの「VLAN への静的メンバーの追加」を参照)。ただし、このエッジスイッチおよびネットワークのコアスイッチの GVRP は使用可能にする必要があります。

タグ付きフレームおよびタグなしフレームの転送

1 つのスイッチに直接接続する装置で小規模なポートベースの VLAN を作成する場合は、ポートを同じタグなし VLAN に割り当てることができます。しかし、複数のスイッチに渡る VLAN グループに割り当てするには、このグループ用の VLAN を作成してすべてのポートでタグに対応する必要があります。

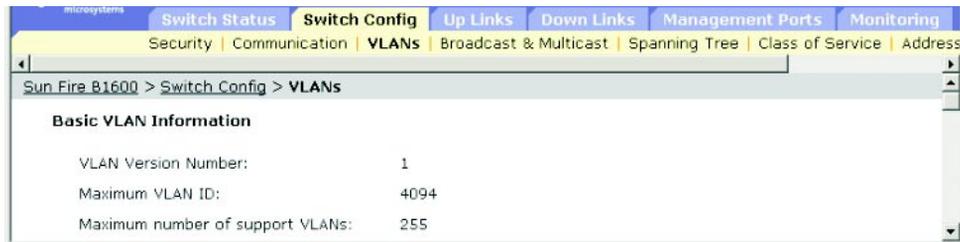
ポートは、タグ付きまたはタグなしの複数の VLAN に割り当てることができます。そのため、スイッチの各ポートは、タグ付きおよびタグなしの両方のフレームを通過させることができます。スイッチは、VLAN 対応装置が接続されたパスにフレームを転送する場合には、VLAN タグを挿入します。また、VLAN 対応装置 (宛先ホストを含む) が接続されていないパスにフレームを転送する場合には、フレームを転送する前に VLAN タグを外します。スイッチは、タグ付きフレームを受信したときには、フレームのタグに示された VLAN にこのフレームを転送します。VLAN 非対応装置からタグなしフレームを受信したときには、まずそのフレームの転送先を決定し、受信ポートのデフォルトの VID に基づいて VLAN タグを挿入します。

3.3.1.1 基本的な VLAN 情報の表示

コマンド属性

- **VLAN Version Number** – スイッチが使用する IEEE 802.1Q 標準で規定された VLAN のバージョン
- **Maximum VLAN ID** – スイッチが認識する VLAN ID の最大長
- **Maximum Number of Supported VLANs** – スイッチで設定できる VLAN の最大数

Web – 「Switch Config」 => 「VLANs」を開きます。



CLI – 次のコマンドを実行します。

```
Console#show bridge-ext 4-123  
Max support vlan numbers: 32  
Max support vlan ID: 4094  
Extended multicast filtering services: No  
Static entry individual port: Yes  
VLAN learning: IVL  
Configurable PVID tagging: Yes  
Local VLAN capable: Yes  
Traffic classes: Enabled  
Global GVRP status: Disabled  
GMRP: Disabled  
Console#
```

SNMP – 対応する MIB 変数

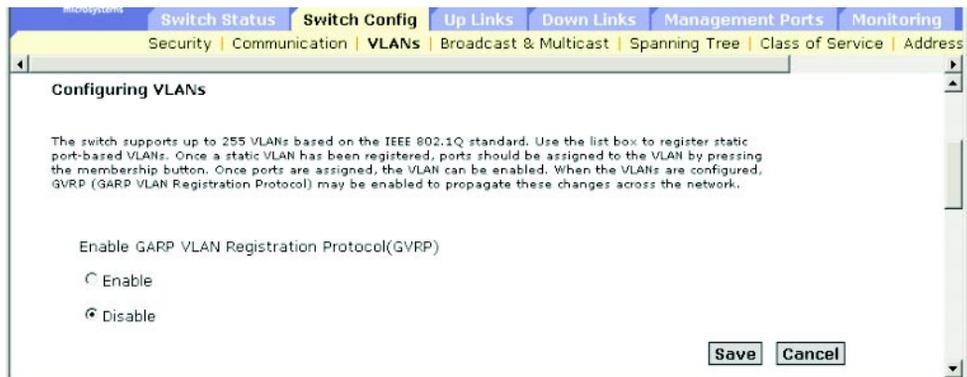
フィールド名	MIB 変数	アクセス	値の範囲	デフォルト値
VLAN Version Number	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qBase. dot1qVlanVersion- Number	読み取り専用	version1 (1)	version1

フィールド名	MIB 変数	アクセス	値の範囲	デフォルト値
Maximum VLAN ID	MIB-II. dot1dBridge. BridgeMIB. BridgeMIBObjects. dot1qBase. dot1qMaxVlanId	読み取り専用	整数	4094
Maximum Number of Supported VLANs	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qBase. dot1qMaxSupportedVlans	読み取り専用	整数	255
Device Capabilities	MIB-II. dot1dBridge. pBridgeMIB. pBridgeMIBObjects. dot1dExtBase. dot1dDeviceCapabilities	読み取り専用	ビット列 – ExtendedFiltering dot1dServices (0)、 dot1dTrafficClasses (1)、 StaticEntry dot1dIndividualPort (2)、 dot1dIVLCapable (3)、 dot1dSVLCapable (4)、 dot1dHybridCapable (5)、 dot1dConfigurablePvid dot1dTagging (6)、 dot1dLocalVlanCapable (7)	2、3、6、7
Traffic Classes Enabled	MIB-II. dot1dBridge. pBridgeMIB. pBridgeMIBObjects. dot1dExtBase. dot1dTrafficClasses- Enabled	読み取り/ 書き込み	true (1)、 false (2)	true
GMRP Status	MIB-II. dot1dBridge. pBridgeMIB. pBridgeMIBObjects. dot1dExtBase. dot1dGmrpStatus	読み取り/ 書き込み	enabled (1)、 disabled (2)	disabled
GVRP Status	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qBase. dot1qGvrpStatus	読み取り/ 書き込み	enabled (1)、 disabled (2)	disabled

3.3.1.2 GVRP の使用可能および使用不可の切り替え (グローバル設定)

GVRP は、ネットワーク上のポートで VLAN メンバーを登録するために、スイッチが VLAN 情報を交換する方法を規定したものです。VLAN は、ホスト装置からネットワーク全体に伝播される Join メッセージに基づいて動的に設定されます。VLAN の自動登録を可能にし、ローカルスイッチを超える VLAN をサポートするには、GVRP を使用可能にする必要があります。

Web — 「Switch Config」 => 「VLANs」を開きます。GVRP を使用可能または使用不可にして「Save」をクリックします。



CLI — 次に、スイッチに対して GVRP を使用可能にする例を示します。

```
Console(config)#bridge-ext gvrp 4-122
Console(config)#
```

SNMP — 対応する MIB 変数

フィールド名	MIB 変数	アクセス	値の範囲	デフォルト値
GVRP Status	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qBase. dot1qGvrpStatus	読み取り / 書き込み	enabled (1)、 disabled (2)	disabled

3.3.1.3 VLAN の設定

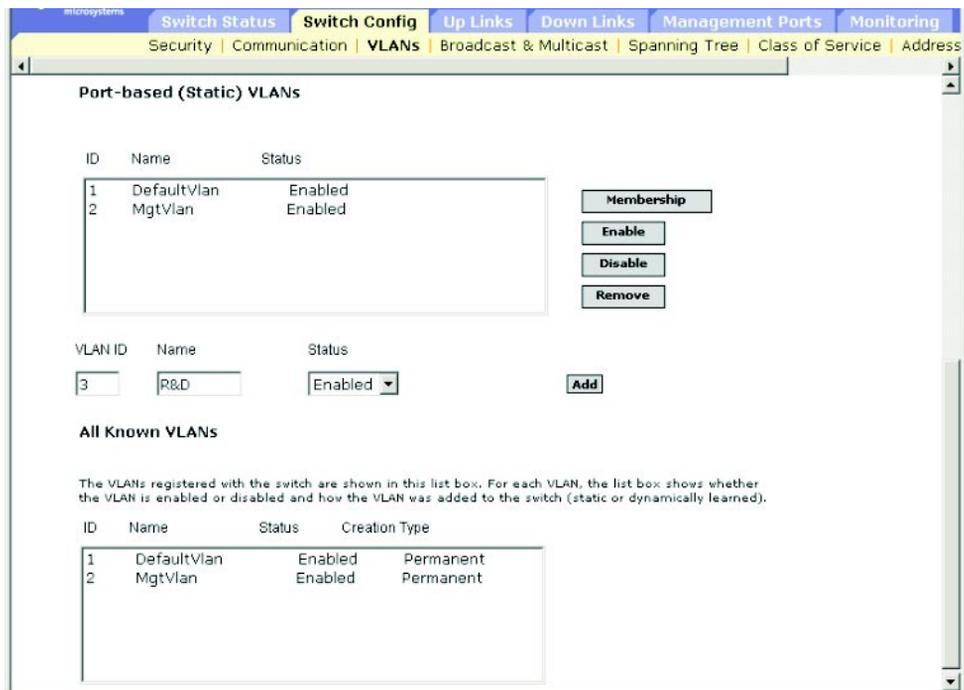
コマンド属性

- ID – 設定する VLAN の ID (1 ~ 4094) です。
- Name – VLAN の名前 (1 ~ 15 文字) です。
- Status – VLAN が使用可能または使用不可のどちらであることを示します。
 - Enable (Active*) – VLAN は動作しています。
 - Disable (Suspend*) – VLAN は停止中で、パケットの送受信を行っていません。
- Creation Type – VLAN のスイッチへの追加方法を表示します。
 - Dynamic GVRP (Dynamic*) : GVRP によって自動的に学習されました。
 - Permanent (Static*) : 静的エントリとして追加されました。
- Ports/Channel groups* – VLAN インタフェースのメンバーを表示します。

* CLI ではこの用語で表示されます。

Web – 「Switch Config」=>「VLANs」を開きます。新しい VLAN を作成するには、VLAN ID と名前を入力し、ステータスを「Enabled」または「Disabled」に設定して「Add」をクリックします。既存の VLAN を変更するには、1 つ以上のエントリを選択し、「Enable」または「Disable」、「Remove」をクリックします。

VLAN にインタフェースを追加するには、エントリを選択して「Membership」をクリックします。詳細は、3-42 ページの「VLAN への静的メンバーの追加」を参照してください。



CLI ー次に、新しい VLAN を作成し、すべての VLAN 情報を表示する例を示します。

```

Console(config)#vlan database                                4-109
Console(config-vlan)#vlan 3 name R&D media ethernet state active 4-109
Console(config-vlan)#
Console#show vlan                                           4-117
VLAN Type      Name           Status    Ports/Channel groups
-----
 1  Static      DefaultVlan   Active    SNP0   SNP1   SNP2   SNP3   SNP4
                                         SNP5   SNP6   SNP7   SNP8   SNP9
                                         SNP10  SNP11  SNP12  SNP13  SNP14
                                         SNP15  NETP0  NETP1  NETP2  NETP3
 2  Static      MgtVlan      Active    NETMGT
 3  Static      R&D          Active
Console#

```

SNMP – 対応する MIB 変数

フィールド名	MIB 変数	アクセス	値の範囲	デフォルト値
VLAN ID	MIB-II.dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanCurrentTable. dot1qVlanCurrentEntry. dot1qVlanIndex	アクセスなし	整数	1
VLAN Name	MIB-II.dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanStaticTable. dot1qVlanStaticEntry. dot1qVlanStaticName	読み取り / 作成	オクテット文字列 (長さ 0 ~ 32)	
VLAN Status	MIB-II.dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanStaticTable. dot1qVlanStaticEntry. dot1qVlanStatic. RowStatus	読み取り / 作成	enable(1)、 disable(2)	
VLAN Type	MIB-II.dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanCurrentTable. dot1qVlanCurrentEntry. dot1qVlanStatus	読み取り専用	other(1)、 permanent(2)、 dynamicGvrp(3)	
VLAN Ports	MIB-II.dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanCurrentTable. dot1qVlanCurrentEntry. dot1qVlanCurrent- EgressPorts	読み取り専用	オクテット文字列 (ポートリスト)	

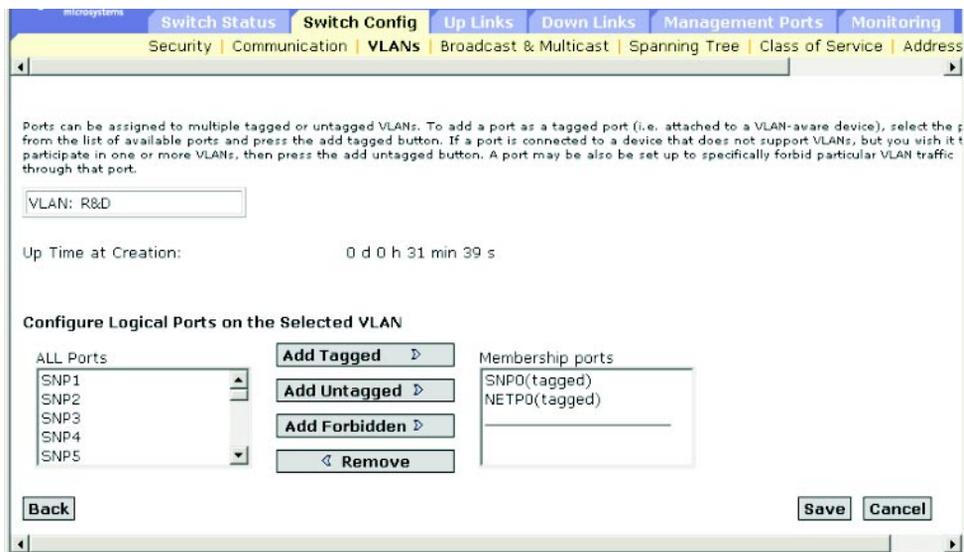
3.3.1.4 VLAN への静的メンバーの追加

コマンド属性

- **Name** – VLAN の名前です。
- **Up Time at Creation** – VLAN が作成された時刻です。
- **Status*** – VLAN のスイッチへの追加方法を表示します。
 - **Dynamic** : GVRP によって自動的に学習されました。
 - **Static** : 静的エントリとして追加されました。
- **All Ports** – ポート識別子またはトランク識別子です。
- **Membership Ports** – 選択した VLAN にタグ付きまたはタグなしとして追加されたインタフェース、あるいは GVRP による自動追加が制限されたインタフェースです。
- **Membership Type** – 必要なインタフェースを選択し、適切な「Add」ボタンをクリックすることによって、VLAN のメンバーを指定します。
 - **Add Tagged** : インタフェースを VLAN のメンバーにします。この VLAN 上のポートは、すべてのパケットにタグを付けて送信します。タグを付けることで、VLAN または CoS 情報が配信されます。
 - **Add Untagged** : インタフェースを VLAN のメンバーにします。ポートは、すべてのパケットをタグを付けずに送信します。タグが付かないため、VLAN または CoS 情報が配信されません。
 - **Add Forbidden** : GVRP によってインタフェースが VLAN に自動参加することを禁止します。詳細は、3-34 ページの「VLAN の自動登録」を参照してください。
 - **Remove** : 選択されたインタフェースをこの VLAN から削除します。

* CLI でのみ確認できます。

Web – 「Switch Config」 => 「VLANs」を開きます。静的リストで1つのVLANを選択して、「Membership」をクリックします。ポートメンバーシップのページで、「All Ports」リスト(ポートまたはトランク)からインタフェースを1つ選択し、「Add Tagged」または「Add Untagged」、「Add Forbidden」(このインタフェースがGVRPによって追加されないようにする)をクリックします。インタフェースを削除するには、「Membership Ports」リストからエントリを1つ選択し、「Remove」をクリックします。



CLI – 次に、複数のインタフェースを追加してからVLANメンバーを表示する例を示します。

```

Console(config)#interface ethernet NETP1                                4-75
Console(config-if)#switchport allowed vlan add 3 tagged                4-115
Console(config-if)#exit
Console(config)#interface ethernet NETP2
Console(config-if)#switchport allowed vlan add 3 untagged
Console(config-if)#exit
Console(config)#interface ethernet SNP13
Console(config-if)#switchport forbidden vlan add 3
Console(config-if)#end
Console#show vlan id 3
VLAN Type      Name                Status        Ports/Channel groups
-----
    3  Static      R&D               Active        NETP1  NETP2
Console#

```

SNMP – 対応する MIB 変数

フィールド名	MIB 変数	アクセス	値の範囲	デフォルト値
VLAN ID	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanStaticTable. dot1qVlanStaticEntry. dot1qVlanIndex	インデックス	行	
VLAN Name	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanStaticTable. dot1qVlanStaticEntry. dot1qVlanStaticName	読み取り / 作成	オクテット文字列 (長さ 0 ~ 32)	
Up Time at Creation	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanCurrentTable. dot1qVlanCurrentEntry. dot1qVlanCreationTime	読み取り専用	時間間隔 (センチ秒単位)	
VLAN Status	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanCurrentTable. dot1qVlanCurrentEntry. dot1qVlanStatus	読み取り専用	other(1)、 permanent(2)、 dynamicGvrp(3)	
Tagged Ports, Untagged Ports (VLAN を許可)	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanTable. dot1qVlanEntry. dot1qVlanStatic- UntaggedPorts	読み取り / 作成	オクテット文字列 (ポートリスト)	

フィールド名	MIB 変数	アクセス	値の範囲	デフォルト値
VLAN Forbidden Ports	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qPortVlanTable. dot1qPortVlanEntry. dot1qVlanForbidden- EgressPorts	読み取り / 作成	オクテット文字列 (ポートリスト)	
Port Trunk Index (チャンネルグループ プ)	sun... portMgt. portTable portEntry. portTrunkIndex	読み取り専用	整数	
VLAN Static Row Status	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanStaticTable. dot1qVlanStaticEntry. dot1qVlanStatic- RowStatus	読み取り / 作成	enable(1)、 disable(2)	

3.3.2 マルチキャスト設定

ビデオ会議、ストリーミングオーディオなどのリアルタイムアプリケーションは、マルチキャストを使用します。マルチキャストサーバーは、クライアントごとに接続を確立する必要はありません。マルチキャストサーバーは、そのサービスをネットワークにブロードキャストするだけで、そのマルチキャストサービスを受信するホスト側がローカルマルチキャストスイッチ/ルーターを登録します。この方法では、マルチキャストサーバーに必要なネットワーク負荷は軽減されますが、サービスに登録したホストにだけトラフィックが渡るように、経路上のすべてのマルチキャストスイッチ/ルーターでブロードキャストトラフィックのルーティングを行う必要があります。

このスイッチは、IGMP (Internet Group Management Protocol) を使用して、特定のマルチキャストサービスへの参加を要求する接続ホストを照会します。スイッチは、サービスを要求するホストに接続するポートを識別し、そのポートだけにデータを送信します。次に、継続してマルチキャストサービスを受信できるように、隣接するマルチキャストスイッチ/ルーターにサービス要求を伝播します。この方法は、マルチキャストフィルタリングと呼ばれています。

IP マルチキャストフィルタリングの目的は、サブネット (VLAN) の全ポートにトラフィックをフラディングするのではなく、マルチキャストグループのホストまたはマルチキャストスイッチ/ルーターに接続するポートだけにマルチキャストパケットを転送して、スイッチ制御ネットワークの性能を最適化することです。

3.3.2.1 IGMP スヌープパラメタの設定

スイッチは、マルチキャストトラフィックを効率的に転送するように設定できます。スイッチは、IGMP 照会およびレポートメッセージに基づいて、マルチキャストトラフィックを要求するポートだけにトラフィックを転送します。これによって、スイッチが全ポートにトラフィックをブロードキャストすることで、ネットワークの性能を低下させることがなくなります。

コマンドの使用法

- **IGMP Snooping** – スイッチは、IP マルチキャストスイッチ/ルーターと IP マルチキャストホストグループとの間で送受信される IGMP 照会パケットおよびレポートパケットに対して受動的にスヌープを行って、IP マルチキャストグループのメンバーを識別します。スイッチは、スイッチを通過する IGMP パケットを監視してグループ登録情報を取り出し、その情報に従ってマルチキャストフィルタを設定します。
- **IGMP Querier** – ルーターまたはマルチキャスト対応スイッチは、定期的にホストに問い合わせ、ホストがマルチキャストトラフィックの受信を要求しているかどうかを確認します。IP マルチキャストを実行する LAN に複数のルーターまたはスイッチがある場合は、その装置のいずれか 1 台が照会元 (Querier) になって、グループメンバーに代わって LAN に対する照会を行います。次に、マルチキャストサービスの受信が継続されるように、アップストリームマルチキャストスイッチ/ルーターにサービス要求を伝播します。

注 – マルチキャストルーターは、この情報を DVMRP などのマルチキャストルーティングプロトコルとともに使用して、インターネット全体の IP マルチキャストをサポートします。

コマンド属性

- **IGMP Snooping** – この属性を使用可能にすると、スイッチはネットワークトラフィックを監視することで、マルチキャストトラフィックの受信を要求するホストを決定します (デフォルト: Disabled)。
- **IGMP Protocol Version** – ネットワーク上のほかの装置と互換性のあるプロトコルバージョンを設定します (デフォルト: 2、範囲: 1 ~ 2)。
- **IGMP Querier** – この属性を使用可能にすると、スイッチは照会元として機能し、ホストがマルチキャストトラフィックの受信を要求しているかどうかを問い合わせます (デフォルト: Disabled)。

- **Query Count** – 照会の最大発行回数を設定します。ここで設定した回数分の照会を行っても応答がない場合、照会元は、マルチキャストグループからそのクライアントを除外します (デフォルト: 2、範囲: 2 ~ 10)。
- **Query Interval** – スイッチが IGMP ホスト照会メッセージを送信する時間間隔を設定します (デフォルト: 125 秒、範囲: 60 ~ 125)。
- **Query Report Delay** – ポートである IP マルチキャストアドレスに対する IGMP レポートを受信するまでの間隔を設定します。この時間を過ぎると、スイッチはそのポートに IGMP 照会を送信して、リストからエントリを削除します (デフォルト: 10 秒、範囲: 5 ~ 25)。
- **Router Port Expire Time** – 前の照会元が照会を停止してから、スイッチが待機する時間を設定します。この時間を過ぎると、スイッチは、その照会パケットを受信していたインタフェースは照会元に接続しなくなったと判断します (デフォルト: 300 秒、範囲: 300 ~ 500)。

注 – サブネット上のすべてのシステムが、同じバージョンをサポートする必要があります。IGMP Report Delay、Router Port Expire Time などのように、IGMP バージョン 2 でのみ設定できる属性もあります。

Web – 「Switch Config」=>「Broadcast & Multicast」=>「IGMP Parameters」をクリックします。必要に応じて IGMP の設定を変更し、「Save」をクリックします。

The screenshot shows the configuration page for IGMP Parameters on a Sun Fire B1600 switch. The breadcrumb navigation is: Sun Fire B1600 > Switch Config > Broadcast & Multicast. The 'View' dropdown is set to 'IGMP Parameters'. The page title is 'Configuring IGMP Parameters'. Below the title, there is explanatory text: 'To configure the switch to use IGMP (Internet Group Management Protocol) for multicast filtering, you will need to enable IGMP Snooping. You can also configure the switch to act as an IGMP Querier, which will make it responsible for propagating multicast traffic to other switches or routers on the network.' The configuration options are:

- IGMP Snooping Enabled
- IGMP Protocol Version:
 - Version 2
 - Version 1
- IGMP Querier Enabled
- Query Count (1-2):
- Query Interval(60-125)secs:
- Query Report Delay (5-30)secs:
- Router Port Expire Time (300-500)secs:

 At the bottom right, there are 'Save' and 'Cancel' buttons.

CLI — 次に、マルチキャストフィルタリングの設定を変更してから、現在の設定内容を表示する例を示します。

```

Console(config)#ip igmp snooping 4-125
Console(config)#ip igmp snooping querier 4-129
Console(config)#ip igmp snooping query-count 10 4-130
Console(config)#ip igmp snooping query-interval 100 4-131
Console(config)#ip igmp snooping query-max-response-time 20 4-131
Console(config)#ip igmp router-port-expire-time 300 4-132
Console(config)#ip igmp snooping version 2 4-126
Console(config)#exit
Console#show ip igmp snooping 4-127
  Igmp Snooping Configuration
-----
Service status          : Enabled
Querier status          : Enabled
Query count              : 10
Query interval          : 100 sec
Query max response time : 20 sec
Query time-out          : 300 sec
IGMP snooping version   : Version 2
Console#

```

SNMP — 対応する MIB 変数

フィールド名	MIB 変数	アクセス	値の範囲	デフォルト値
Snooping Status	sun... igmpSnoopMgt. igmpSnoopStatus	読み取り/ 書き込み	enabled (1)、 disabled (2)	enabled
Snooping Querier	sun... igmpSnoopMgt. igmpSnoopQuerier	読み取り/ 書き込み	enabled (1)、 disabled (2)	enabled
Snooping Query Count	sun... igmpSnoopMgt. igmpSnoopQueryCount	読み取り/ 書き込み	整数 (2 ~ 10)	2
Snooping Query Interval	sun... igmpSnoopMgt. igmpSnoop- QueryInterval	読み取り/ 書き込み	整数 (60 ~ 125) 秒	125
Snooping Query Max Response Time	sun... igmpSnoopMgt. igmpSnoopQuery- MaxResponseTime	読み取り/ 書き込み	整数 (5 ~ 25) 秒	10

フィールド名	MIB 変数	アクセス	値の範囲	デフォルト値
Snooping Router Port Expire Time	sun... igmpSnoopMgt. igmpSnoopRouterPort- ExpireTime	読み取り/ 書き込み	整数 (300 ~ 500) 秒	300
Snooping Version	sun... igmpSnoopMgt. igmpSnoopVersion	読み取り/ 書き込み	整数 (1 ~ 2)	2

3.3.2.2 マルチキャストルーターに接続するインタフェースの指定

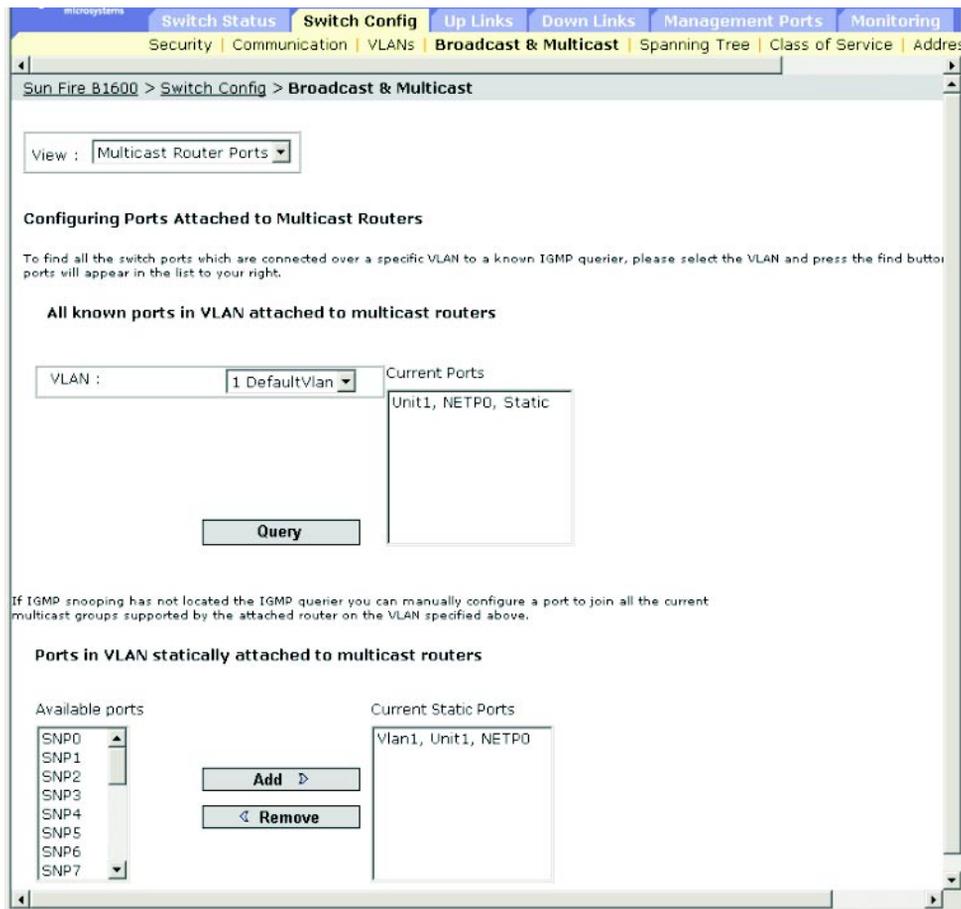
マルチキャストルーターは、IGMP 照会で取得した情報を DVMRP などのマルチキャストルーティングプロトコルとともに使用して、インターネット全体の IP マルチキャストリングをサポートします。マルチキャストルーターは、スイッチによって動的に検出されるか、またはスイッチのインタフェースに静的に割り当てられます。

ネットワーク接続によっては、IGMP スヌープでは IGMP 照会元を検出できない場合があります。そのため、IGMP 照会元がネットワークを介してスイッチのインタフェース (ポートまたはトランク) に接続された既知のマルチキャストルーター/スイッチである場合には、そのルーターがサポートする現在のすべてのマルチキャストグループに、インタフェース (および指定された VLAN) を手動で追加します。これによって、マルチキャストトラフィックがスイッチ内のすべての適切なインタフェースに渡されるようになります。

コマンド属性

- All known ports in VLAN attached to multicast routers —
 - VLAN — スイッチ上の VLAN を選択します。
スクロールダウンリストに VLAN ID および名前が表示されます。
 - Interface — マルチキャストルーターに接続されたインタフェースと、その設定が静的 (Static) または動的 (IGMP) のどちらであるかを表示します。
- Ports in VLAN statically attached to multicast routers —
 - Available Ports — 選択した VLAN にマルチキャストルーターのポートとして割り当てられていないインタフェースを表示します。
 - Current Static Ports — 選択した VLAN にマルチキャストルーターのポートとして割り当てられているインタフェースを表示します。

Web – 「Switch Config」 => 「Broadcast & Multicast」 => 「Multicast Router Ports」をクリックします。「VLAN」を選択し、「Query」をクリックして、マルチキャストルーターに接続する VLAN 内のすべてのインタフェースを表示します。または、「Add」および「Remove」ボタンを使用して、マルチキャストルーターにインタフェースを静的に設定します。



CLI – 次に、ポート NETP0 を VLAN 1 内のマルチキャストルーターのポートとして設定する例を示します。

```

Console(config)#ip igmp snooping vlan 1 mrouter ethernet NETP0 4-133
Console(config)#exit
Console#show ip igmp snooping mrouter vlan 1 4-134
VLAN M'cast Router Port Type
-----
1 NETP0 Static

```

SNMP – 対応する MIB 変数

フィールド名	MIB 変数	アクセス	値の範囲
Snooping Multicast Router Current VLAN	sun... igmpSnoopMgt. igmpSnoopRouterCurrentTable. igmpSnoopRouterCurrentEntry. dot1qVlanIndex	インデックス	整数
VLAN Name	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanStaticTable. dot1qVlanStaticEntry. dot1qVlanStaticName	読み取り/ 作成	オクテット文字列 (長さ 0 ~ 32)
Snooping Multicast Router Current Ports	sun... igmpSnoopMgt. igmpSnoopRouterCurrentTable. igmpSnoopRouterCurrentEntry. igmpSnoopRouterCurrentPorts	読み取り専用	オクテット文字列 (ポートリスト)
Snooping Multicast Router Static Vlan Index	sun... igmpSnoopMgt. igmpSnoopRouterStaticTable. igmpSnoopRouterStaticEntry. dot1qVlanIndex	インデックス	整数
Snooping Multicast Router Static Ports	sun... igmpSnoopMgt. igmpSnoopRouterStaticTable. igmpSnoopRouterStaticEntry. igmpSnoopRouterStaticPorts	読み取り/ 作成	オクテット文字列 (ポートリスト)
Snooping Multicast Router Static Status	sun... igmpSnoopMgt. igmpSnoopRouterStaticTable. igmpSnoopRouterStaticEntry. igmpSnoopRouterStaticStatus	読み取り/ 作成	valid(1)、 invalid(2)

3.3.2.3 マルチキャストサービスの設定

3-46 ページの「IGMP スヌープパラメタの設定」で説明したように、IGMP スヌープおよび IGMP 照会メッセージを使用すると、マルチキャストフィルタリングを動的に設定できます。より厳密な制御を必要とするアプリケーションには、マルチキャストサービスを特定のインタフェースに手動で割り当てる必要があります。まず、参加するホストに接続するすべてのポートを共通の VLAN に追加し、次に、この VLAN グループにマルチキャストサービスを割り当てます。

コマンドの使用法

- 静的なマルチキャストアドレスは、失効することがありません。
- マルチキャストアドレスを特定の VLAN のインタフェースに静的に割り当てると、対応するトラフィックはこの VLAN 内のポートだけに転送されます。

コマンド属性

- All known ports and Multicast Services supported on VLAN –
 - VLAN – このスイッチ上の VLAN を選択します。
スクロールダウンリストに VLAN ID および名前が表示されます。
 - IP Address – 特定のマルチキャストサービス用の IP アドレスです。
 - Interface – マルチキャストルーターに接続されたインタフェースと、その設定が静的 (User) または動的 (IGMP) のどちらであるかを表示します。
- Ports and Multicast Services statically configured on VLAN –
 - IP Address – 特定のマルチキャストサービス用の IP アドレスです。
 - Available Ports – 選択した VLAN にマルチキャストサービスをサポートするためのインタフェースとして割り当てられていないポートを表示します。
 - Current Static Ports (IP Addresses) – 選択した VLAN にマルチキャストサービスを伝播するためのインタフェースとしてすでに割り当てられているポートを表示します。また、このインタフェースに割り当てられている IP アドレスも表示します。

Web - 「Switch Config」 => 「Broadcast & Multicast」 => 「Multicast Support」 をクリックします。特定のマルチキャストサービスを伝播するスイッチインタフェースを表示するには、スクロールダウンリストからマルチキャストサービス用の VLAN ID および IP アドレスを選択し、「Query」をクリックします。特定のインタフェースにマルチキャストサービスを手動で割り当てるには、スクロールダウンリストから「VLAN」を選択し、テキストボックスにマルチキャストサービス用の IP アドレスを入力し、「Add」をクリックします。

View : Multicast Services

Configuring Multicast Services

To find all the switch ports which propagate a specific multicast address, please select the VLAN , select an IP address for a multicast service. The list of ports will appear in the list to your right

All known ports and muticast Services supported on VLAN

VLAN : 1 DefaultVlan
IP Address: 224.0.1.3
Ports Creation Type: Unit1, NETPO, User

Query

To manually assign a multicast service on the selected VLAN to a specific port, type the IP address for the multicast service in the text box, select the port from the list of switch ports to your left and press the add button. The port will then appear in the list of multicast services supported by that VLAN to your right.

Ports and multicast services statically configured on VLAN

Available Ports	IP Address:	Current Static Ports (IP Addresses)
SNP0 SNP1 SNP2 SNP3 SNP4 SNP5 SNP6 SNP7	0.0.0.0	VLAN 1, 224.0.1.3, Unit 1, NETPO

Add **Remove**

注 - 入力したデータが無効であるというエラーメッセージが表示された場合は、それぞれの IP アドレスが正しく指定されているかどうかを確認してください。

CLI - 次に、ポート NETP0 にマルチキャストアドレスを割り当ててから、VLAN 1 でサポートされている既知のマルチキャストサービスをすべて表示する例を示します。

```

Console(config)#ip igmp snooping vlan 1 static 224.0.0.12 ethernet NETP0 4-126
Console(config)#exit
Console#show mac-address-table multicast vlan 1 4-128
VLAN M'cast IP addr. Member ports Type
-----
    1      224.0.0.12      NETP1      IGMP
    1      224.1.2.3        NETP0      USER
Console#

```

SNMP - 対応する MIB 変数

フィールド名	MIB 変数	アクセス	値の範囲
Snooping Multicast Router Static Vlan Index	sun... igmpSnoopMgt. igmpSnoopMulticastStaticTable. igmpSnoopMulticastStaticEntry. dot1qVlanIndex	インデックス	整数
Snooping Multicast Static IP Address	sun... igmpSnoopMgt. igmpSnoopMulticastStaticTable. igmpSnoopMulticastStaticEntry. igmpSnoopMulticastStaticIPAddress	インデックス	IP アドレス
Snooping Multicast Static Port List	sun... igmpSnoopMgt. igmpSnoopMulticastStaticTable. igmpSnoopMulticastStaticEntry. igmpSnoopMulticastStaticPorts	読み取り/ 作成	オクテット文字列 (ポートリスト)
Snooping Multicast Router Static Status	sun... igmpSnoopMgt. igmpSnoopRouterStaticTable. igmpSnoopRouterStaticEntry. igmpSnoopRouterStaticStatus	読み取り/ 作成	valid(1)、 invalid(2)

3.3.3 ブロードキャストストームの抑制 (グローバル設定)

ネットワーク上の装置に障害がある場合や、アプリケーションプログラムが正しく設計および設定されていない場合には、ブロードキャストストームが発生することがあります。ネットワークのブロードキャストトラフィックが多すぎると、性能が著しく低下したり、すべての機能が完全に停止することがあります。

ネットワークをブロードキャストストームから保護するには、すべてのポートに適用するブロードキャストトラフィックのしきい値を設定した上で、必要なポートに対してブロードキャストストーム制御を使用可能にします。

指定したしきい値を超えるブロードキャストパケットは、破棄されます。

コマンドの使用法

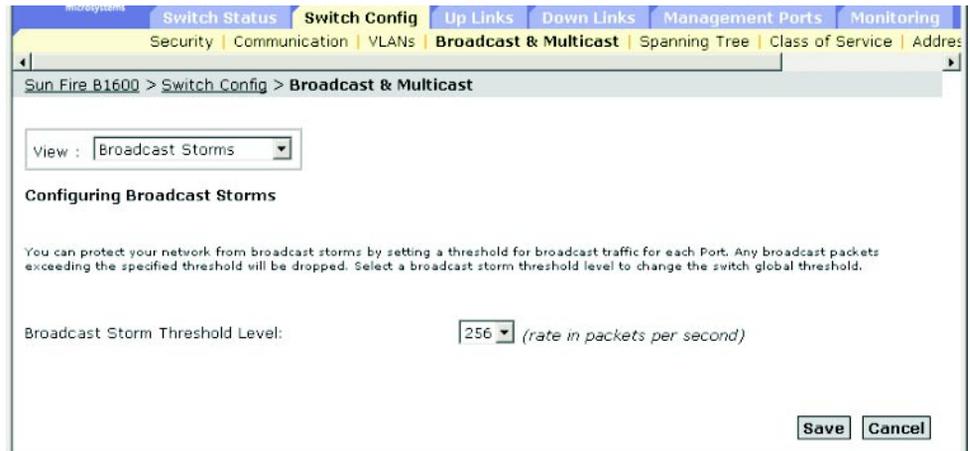
- ブロードキャストストーム制御は、デフォルトで使用可能になっています。
- ブロードキャストストーム制御は、IP マルチキャストトラフィックには影響を与えません。

コマンド属性

- **Broadcast Storm Threshold Level*** – 1 秒あたりのパケット数で表したしきい値です (範囲 : 16、64、128、256、デフォルト : 256)。

* CLI では「Broadcast Storm Limit」と表示されます。

Web – 「Switch Config」 => 「Broadcast & Multicast」 => 「Broadcast Parameters」を開きます。しきい値レベルを設定して、「Save」をクリックします。



CLI – 次に、ブロードキャストしきい値を 1 秒あたり 64 パケットに設定する例を示します。

注 - `switchport broadcast` コマンドを実行すると、指定したインタフェースのブロードキャストストーム制御が使用可能になりますが、ブロードキャストしきい値はスイッチのすべてのインタフェースに設定されます。

```

Console(config)#interface ethernet NETP7                                4-75
Console(config-if)#switchport broadcast packet-rate 64                 4-83
Console(config-if)#end
Console#show interfaces status ethernet NETP7                          4-84
Information of NETP7
  Basic information:
    Port type: 1000T
    Mac address: 00-00-E8-66-66-83
  Configuration:
    Name: External RJ-45 connector NET7
    Port admin: Up
    Speed-duplex: Auto
    Capabilities: 10half, 10full, 100half, 100full, 1000full,
    Broadcast storm: Enabled
    Broadcast storm limit: 256 packets/second
    Flow control: Disabled
    LACP: Disabled
  Current status:
    Link status: Up
    Port operation status: Up
    Operation speed-duplex: 1000full
    Flow control type: None
Console#

```

SNMP - 対応する MIB 変数

フィールド名	MIB 変数	アクセス	値の範囲	デフォルト値
Broadcast Storm Packet Rate	sun... bcastStormMgt. bcastStormTable. bcastStormEntry. bcastStormPktRate	読み取り/ 書き込み	整数 (16、64、128、256)	256
Broadcast Storm Status	sun... bcastStormMgt. bcastStormTable. bcastStormEntry. bcastStormStatus	読み取り/ 書き込み	enabled (1)、 disabled (2)	enabled

3.3.4 スパニングツリーアルゴリズムの設定

スパニングツリーアルゴリズム (STA) を使用すると、ネットワークループを検出して解消したり、スイッチまたはブリッジ、ルーターの間にバックアップリンクを設定できます。STA によってスイッチがネットワーク上のその他のブリッジ装置 (STA に準拠するスイッチまたはブリッジ、ルーター) と情報を交換できるようになるため、ネットワーク上の任意の 2 台のステーション間にルートが 1 つだけ存在するようになり、一次リンクがダウンしたときには一次リンクのタスクを自動的に引き継ぐバックアップリンクを提供できます。

このスイッチがサポートする STA のバージョンは、次のとおりです。

- STP – スパニングツリープロトコル (IEEE 802.1D)
- RSTP – 高速スパニングツリープロトコル (IEEE 802.1w)

RSTP は、処理速度の遅い従来の STP に代わるプロトコルとして設計されています。RSTP は、アクティブなポートが学習を始める前の状態変更の回数を削減し、ノードまたはポートに障害があった場合に使用する代替ルートを事前定義し、再設定時にツリー構造内の変化を認識しにくいポートのために転送データベースを保持することによって、再設定をより迅速に (STP を使用した場合の約 10 分の 1 の時間で) 行います。

3.3.4.1 基本的な STA 設定

グローバル設定はスイッチ全体に適用されます。

コマンドの使用法

- 高速スパニングツリープロトコル (RSTP)

RSTP は、次に説明するように、受信プロトコルメッセージを監視し、RSTP ノードが転送するプロトコルメッセージのタイプを動的に調整することによって、STP および RSTP のどちらのノードへの接続もサポートします。

- STP モード – スイッチがポートの移行遅延タイマーの期限が過ぎたあとに 802.1D BPDU (STP BPDU) を受信した場合、スイッチは 802.1D ブリッジに接続されていると推測して、802.1D BPDU だけを使用するようになります。
- RSTP モード – RSTP がポート上で 802.1D BPDU を使用していて、移行遅延の期限が過ぎたあとに RSTP BPDU を受信した場合、RSTP は移行遅延タイマーを再開して、そのポートでは RSTP BPDU を使用するようになります。

コマンド属性

基本的なグローバル設定

次のグローバル属性を設定できます。

- **Enable Spanning Tree** – スイッチの STA を使用可能または使用不可にします。
- **Spanning Tree Protocol** – スイッチで使用するスパニングツリーのタイプを指定します。
 - **STP**: スパニングツリープロトコル (IEEE 802.1D) を使用します。このタイプを選択すると、スイッチは、強制的に STP 互換モードに設定された RSTP を使用するようになります。
 - **RSTP**: 高速スパニングツリー (IEEE 802.1w) を使用します。

次のグローバル属性は固定されていて変更できません。

- **Bridge ID** – 装置の優先順位および MAC アドレスです。
- **Designated Root** – スイッチがルートデバイスとして受け入れたスパニングツリー内の装置の優先順位および MAC アドレスです。
 - **Root Port** – このスイッチ上にあるルートにもっとも近いポートの番号です。このスイッチは、このポートを介してルートデバイスとの通信を行います。ルートポートがない場合は、このスイッチがスパニングツリーネットワークのルートデバイスとして受け入れられます。
 - **Root Path Cost** – スイッチのルートポートからルートデバイスまでのパスコストです。
 - **Root Hello Time** – 装置が設定メッセージを送信する時間間隔 (秒単位) です。
 - **Root Maximum Age** – 装置が設定メッセージを受信するまで待機する時間 (秒単位) です。この時間を過ぎると、装置は再設定を試みます。指定ポート以外のすべての装置のポートでは、定期的に設定メッセージを受信する必要があります。前回の設定メッセージによって提供されたルートポートの STA 情報の期限が切れると、ネットワークに接続されている装置のポートの中から新しいルートポートが選択されます。この節では、ポートとはインタフェースを意味し、ポートおよびトランクの両方を指します。
 - **Root Forward Delay** – 装置が状態を (破棄から学習、転送へ) 変更する前に待機する時間 (秒単位) です。すべての装置は、フレームの転送を開始する前にトポロジの変更に関する情報を受信する必要があるため、この遅延が必要となります。また、各ポートには、競合情報を待機する時間が必要です。競合情報を受信すると、ポートは破棄状態に戻ります。この待機時間がないと、一時データのループが発生することがあります。
 - **Root Hold Time** – このノードが 2 つ以下の構成情報 BPDU を送信する時間の間隔 (秒単位)。

ルートデバイス設定

次のグローバル属性を設定できます。

- **Priority** — ルート装置およびルートポート、指定ポートの選択に使用するブリッジの優先順位です。優先順位の高い装置が STA ルート装置になります。ただし、すべての装置の優先順位が同じ場合は、MAC アドレス番号がもっとも小さい装置が STA ルート装置になります。
 - デフォルト：32768
 - 範囲：0 ~ 61440、4096 ずつ増分
 - オプション：0、4096、8192、12288、16384、20480、24576、28672、32768、36864、40960、45056、49152、53248、57344、61440
- **Hello Time** — 装置が設定メッセージを送信する間隔 (秒単位) です。
 - デフォルト：2
 - 最小値：1
 - 最大値：10 または [(メッセージの最大有効期限/2) - 1] の小さい方の値
- **Maximum Age** — 装置が設定メッセージを受信するまで待機する時間 (秒単位) です。この時間を過ぎると、装置は再設定を試みます。指定ポート以外のすべての装置のポートでは、定期的に設定メッセージを受信する必要があります。前回の設定メッセージによって提供された STA 情報の期限が切れたポートは、接続されている LAN の指定ポートになります。このポートがルートポートの場合は、ネットワークに接続されている装置のポートの中から新しいルートポートが選択されます。この節では、ポートとはインタフェースを意味し、ポートおよびトランクの両方を指します。
 - デフォルト：20
 - 最小値：6 または [2 × (Hello Time + 1)] の大きい方の値
 - 最大値：40 または [2 × (Forward Delay - 1)] の小さい方の値
- **Forward Delay** — 装置が状態を (破棄から学習、転送へ) 変更する前に待機する時間 (秒単位) です。すべての装置は、フレームの転送を開始する前にトポロジの変更に関する情報を受信する必要があるため、この遅延が必要となります。また、各ポートには、競合情報を待機する時間が必要です。競合情報を受信すると、ポートは破棄状態に戻ります。この待機時間がないと、一時データのループが発生することがあります。
 - デフォルト：15
 - 最小値：4 または [(メッセージの最大有効期限/2) + 1] の大きい方の値
 - 最大値：30

スパニングツリーの統計情報

次のグローバル属性は統計情報値を表示します。これらの属性は変更できません。

- **Number of Topology Changes** — スパニングツリーの再設定が行われた回数です。
- **Last Topology Change** — スパニングツリーの再設定が最後に行われてからの時間です。

Web – 「Switch Config」 => 「Spanning Tree」 => 「Basic Configuration」を開きます。必要な属性を変更して、「Save」をクリックします。

The screenshot shows the 'Spanning Tree' configuration page. At the top, there are navigation tabs: 'Switch Status', 'Switch Config', 'Up Links', 'Down Links', 'Management Ports', and 'Monitoring'. Below these are sub-tabs: 'Security', 'Communication', 'VLANs', 'Broadcast & Multicast', 'Spanning Tree', 'Class of Service', and 'Address'. The main content area is titled 'Spanning Tree' and includes several sections:

- Basic Configuration:** Includes links for 'Advanced Configuration', 'MST Instance Configuration', and 'MSTI VLAN Configuration'. A checkbox 'Enable Spanning Tree' is checked. A dropdown menu 'Select Spanning Tree Protocol:' is set to 'RSTP'. A note states: 'The Spanning Tree root device is selected using the bridge priority and MAC address. If there is no root port, then this has been accepted as the root device.'
- Configuration Parameters:**

Bridge ID:	32768.0000E8666672
Designated Root:	32768.0000E8666672
Root Port:	0
Root Path Cost:	0
Root Hello Time (secs):	2
Root Maximum Age (secs):	20
Root Forward Delay (secs):	15
Root Hold Time (secs):	1
- Root Device Configuration:**

Priority (0-61440):	32768
Hello Time (1-10) secs:	2
Maximum Age (6-40) secs:	20
Forward Delay (4-30) secs:	15
- Spanning Tree Statistics:**

Number of Topology Changes:	0
Last Topology Change:	0 d 1 h 12 min 59 s

注 – 入力したデータが無効であるというエラーメッセージが表示された場合は、「Priority」および「Hello Time」、「Maximum Age」、「Forward Delay」に指定した値が、各パラメタの所定の範囲内にあるかどうかを確認してください。

CLI – このコマンドを実行すると、STA のグローバル設定が表示され、続けて各ポートの設定が表示されます。

```
Console#show spanning-tree 4-105  
Spanning-tree information  
-----  
Spanning tree mode :RSTP  
Spanning tree enable/disable :enable  
Priority :32768  
Bridge Hello Time (sec.) :2  
Bridge Max Age (sec.) :20  
Bridge Forward Delay (sec.) :15  
Root Hello Time (sec.) :2  
Root Max Age (sec.) :20  
Root Forward Delay (sec.) :15  
Designated Root :32768.0000E8666672  
Current root port :0  
Current root cost :0  
Number of topology changes :0  
Last topology changes time (sec.):9142  
Transmission limit :3  
Path Cost Method :4308020  
.   
.   
.
```

注 – この装置がネットワークに接続されていないときは、current root port および current root cost に **0** が表示されます。

次に、スパニングツリーモードに **RSTP** を設定してスパニングツリーを使用可能にし、各属性を設定する場合の例を示します。

```
Console(config)#spanning-tree mode rst 4-96  
Console(config)#spanning-tree 4-95  
Console(config)#spanning-tree priority 40000 4-99  
Console(config)#spanning-tree hello-time 5 4-98  
Console(config)#spanning-tree max-age 40 4-98  

```

SNMP – 対応する MIB 変数

フィールド名	MIB 変数	アクセス	値の範囲	デフォルト値
STA System Status	sun...staMgt. staSystemStatus	読み取り / 書き込み	enabled (1)、 disabled (2)	enabled
STA Protocol Type	sun...staMgt. staProtocolType	読み取り / 書き込み	stp (1)、 rstp (2)、	rstp
Bridge ID	ブリッジの優先順位および MAC アドレスで構成される			
Designated Root	sun...xstMgt. mstInstanceCfgTable. mstInstanceCfgEntry. mstInstanceCfg- DesignatedRoot	読み取り専用	オクテット文字列	
Root Port	sun...xstMgt. mstInstanceCfgTable. mstInstanceCfgEntry. mstInstanceCfgRootPort	読み取り専用	整数	
Root Cost	sun...xstMgt. mstInstanceCfgTable. mstInstanceCfgEntry. mstInstanceCfgRootCost	読み取り専用	整数	
Hello Time	sun...staMgt.xstMgt. mstInstanceCfgTable. mstInstanceCfgEntry. mstInstanceCfg- HelloTime	読み取り専用	整数	200 センチ秒
Maximum Age	sun...staMgt.xstMgt. mstInstanceCfgTable. mstInstanceCfgEntry. mstInstanceCfgMaxAge	読み取り専用	整数	2000 センチ秒
Forward Delay	sun...staMgt.xstMgt. mstInstanceCfgTable. mstInstanceCfgEntry. mstInstanceCfg- ForwardDelay	読み取り専用	整数	1500 センチ秒
Priority	sun...staMgt.xstMgt. mstInstanceCfgTable. mstInstanceCfgEntry. mstInstanceCfgPriority	読み取り / 書き込み	整数 (0 ~ 61440)	32768
Bridge Hello Time	MIB-II. dot1dStp. dot1dStp- BridgeHelloTime	読み取り / 書き込み	整数 (100 ~ 1000) センチ秒	200 センチ秒

フィールド名	MIB 変数	アクセス	値の範囲	デフォルト値
Bridge Maximum Age	MIB-II. dot1dStp. dot1dStpBridgeMaxAge	読み取り / 書き込み	整数 (600 ~ 4000) センチ秒	2000 センチ秒
Bridge Forward Delay	MIB-II. dot1dStp. dot1dStp- BridgeForwardDelay	読み取り / 書き込み	整数 (400 ~ 3000) センチ秒	1500 センチ秒
STA Configuration Changes	MIB-II. dot1dBridge.dot1dStp. dot1dStpTopChanges	読み取り専用	カウンタ	
STA Last Topology Change	MIB-II. dot1dBridge.dot1dStp. dot1dStpTimeSince- TopologyChange	読み取り専用	整数	

3.3.4.2 STA の拡張設定

ここでは、RSTP の拡張設定について説明します。

コマンド属性

- **Path Cost Method** — パスコストは、装置間の最適なパスを決定するために使用されます。パスコスト方式によって、各インタフェースに割り当てることができる値の範囲を決定します。
 - **Long** : 1 ~ 200,000,000 の 32 ビットベースの値を指定する
 - **Short** : 1 ~ 65535 の 16 ビットベースの値を指定する
- **Transmission Limit** — 連続するプロトコルメッセージの転送間隔の最小値を設定することによって、BPDU の最高転送速度を指定します (範囲 : 1 ~ 10、デフォルト : 3)。

Web — 「Switch Config」 => 「Spanning Tree」 => 「Advanced Configuration」を開きます。必要な属性を変更して、「Save」をクリックします。



注 - 入力したデータが無効であるというエラーメッセージが表示された場合は、**Transmisson Limit** の値が所定の範囲内にあるかどうかを確認してください。

CLI - 次に、スパンニングツリーのパスコスト方式および転送制限を設定する例を示します。

Console(config)#spanning-tree pathcost method long	4-100
Console(config)#spanning-tree transmission-limit 4	4-100
Console(config)#	

SNMP - 対応する MIB 変数

フィールド名	MIB 変数	アクセス	値の範囲	デフォルト値
RSTP Path Cost Method	sun... staMgt. staPathCostMethod	読み取り/ 書き込み	short (1)、 long (2)	long
RSTP Transmission Hold Count	sun.. staMgt. staTxHoldCount	読み取り/ 書き込み	整数 (1 ~ 10)	3

3.3.5 サービスクラスの設定

サービスクラス (CoS) を使用すると、回線が混雑してトラフィックがスイッチのバッファに入っているときの、データパケットの優先度を指定できます。このスイッチは、ポートごとに 4 つの優先順位キューを持つことで CoS をサポートしています。ポートの優先順位が高いキューのデータパケットは、優先順位が低いキューのデータパケットより先に送信されます。各インタフェースにデフォルトの優先順位を設定して、スイッチの優先順位キューにフレームの優先順位タグを割り当てることができます。

3.3.5.1 インタフェースのデフォルトの優先順位の設定

スイッチの各インタフェースには、デフォルトのポート優先順位を指定できます。スイッチが受信するすべてのタグなしパケットは、指定したデフォルトのポート優先順位によってタグを付けられて、送信ポートの該当する優先順位キューに格納されます。

コマンドの使用法

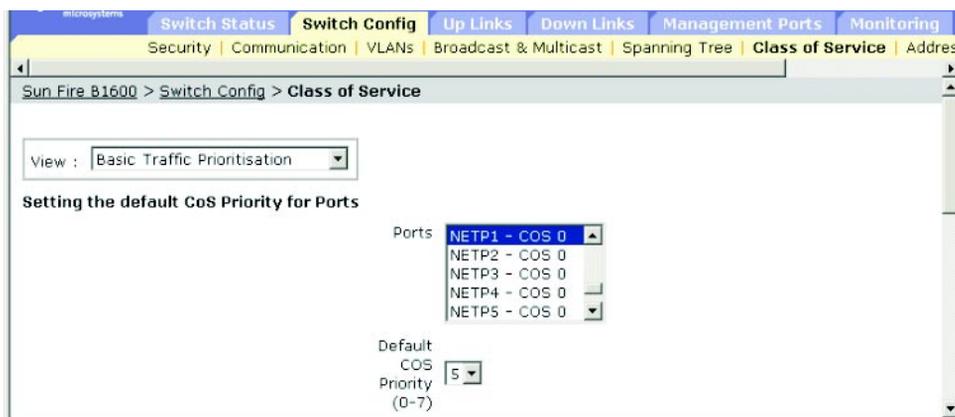
- このスイッチには、ポートごとに 4 つの優先順位キューがあります。スイッチは、加重ラウンドロビン方式で、Head-of-Queue ブロックエッジを防ぎます。
- デフォルトの優先順位は、すべてのフレームタイプ (タグなし、タグ付きの両方のフレーム) を受け入れるように設定されたポートが受信したタグなしフレームに適用されます。この優先順位は、IEEE 802.1Q VLAN タグ付きフレームには適用されません。受信したフレームが IEEE 802.1Q VLAN タグ付きフレームの場合は、IEEE 802.1p のユーザー優先順位ビットを使用します。
- 送信ポートが、関連する VLAN のタグなしのメンバーである場合は、送信前にフレームの VLAN タグを外します。

コマンド属性

- **Ports** – インタフェース (ポートまたはトランク) およびそのインタフェースに割り当てられたデフォルトの CoS 優先順位です。
- **Default COS Priority*** – 指定したインタフェースが受信するタグなしフレームに割り当てる優先順位です (範囲: 0 ~ 7、デフォルト: 0)。

* CLI では「Priority for untagged traffic」と表示されます。

Web – 「Switch Config」 => 「Class of Service」 => 「Basic Traffic Prioritisation」を開きます。「Setting the Default CoS Priority for Ports」までスクロールします。「Ports」リストからインタフェースを選択し、デフォルトの優先順位を修正して、「Save」をクリックします。



CLI – 次に、ポート NETP1 にデフォルト優先順位 5 を割り当てる例を示します。

```

Console(config)#interface ethernet NETP1                                4-75
Console(config-if)#switchport priority default 5                       4-136
Console#show interfaces switchport ethernet NETP1                      4-87
Information of NETP1
Broadcast threshold: Enabled, 256 packets/second
Lacp status: Disabled
VLAN membership mode: Hybrid
Ingress rule: Disabled
Acceptable frame type: All frames
Native VLAN: 1
Priority for untagged traffic: 5
Gvrp status: Enabled
Allowed Vlan:    1(u),
Forbidden Vlan:
Console#

```

SNMP – 対応する MIB 変数

フィールド名	MIB 変数	アクセス	値の範囲	デフォルト値
Port Default User Priority	MIB-II. dot1dBridge. pBridgeMIB. pBridgeMIBObjects. dot1dPriority. dot1dPortPriorityTable. dot1dPortPriorityEntry. dot1dPortDefault- UserPriority	読み取り / 書き込み	整数 (0 ~ 7)	0

3.3.5.2 CoS 値の送信キューへの割り当て

このスイッチは、CoS 優先順位のタグが付いたトラフィックを、各ポートの 4 つの優先順位キューを使用して、加重ラウンドロビン方式 (3-70 ページ) に基づくサービススケジュールに従って処理します。IEEE 802.1p には、最大 8 つのトラフィックの優先順位が定義されています。デフォルトの優先レベルは、次の表に示す IEEE 802.1p 標準の推奨事項に従って割り当てられます。

		キュー			
		0	1	2	3
優先順位	0		0		
	1				
	2				
	3		3		
	4			4	
	5			5	
	6				6
	7				7

次の表に、IEEE 802.1p が推奨する、ネットワークの用途別の優先レベルを示します。使用するネットワークトラフィックの状況に合わせて、スイッチの送信キューに優先レベルを割り当ててください。

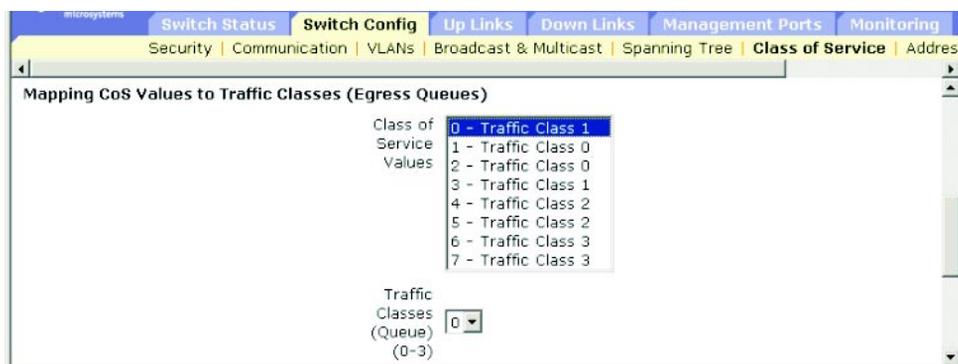
優先レベル	トラフィックタイプ
1	バックグラウンド
2	(予約)
0 (デフォルト)	ベストエフォート
3	エクセレントエフォート
4	負荷制御 (Controlled Load)
5	レイテンシおよびジッターが 100 ミリ秒未満のビデオ
6	レイテンシおよびジッターが 10 ミリ秒未満のビデオ
7	ネットワーク制御

コマンド属性

- **Class of Service Values** – CoS 値です (範囲 : 0 ~ 7、7 がもっとも高い優先順位)。
- **Traffic Classes (Queue)*** – 送信キューのバッファです (範囲 : 0 ~ 3)。

* CLI では「Queue ID」と表示されます。

Web – 「Switch Config」 => 「Class of Service」 => 「Basic Traffic Prioritisation」を開きます。「Mapping CoS Values to Traffic Classes (Egress Queues)」までスクロールします。「Class of Service Values」リストから優先順位を選択し、「Traffic Classes」スクロールダウンリストから送信キューを選択して「Save」をクリックします。



CLI ー次に、CoS 値 0、1、2 を CoS 優先順位キュー 0 に、CoS 値 3 を CoS 優先順位キュー 1 に、CoS 値 4、5 を CoS 優先順位キュー 2 に、CoS 値 6、7 を CoS 優先順位キュー 3 に割り当てる例を示します。

```

Console(config)#interface ethernet NETP0                                4-75
Console(config)#queue cos-map 0 0 1 2                                  4-138
Console(config)#queue cos-map 1 3
Console(config)#queue cos-map 2 4 5
Console(config)#queue cos-map 3 6 7
Console(config)#exit
Console#show queue cos-map ethernet NETP0                               4-140
Information of NETP0
Queue ID   Class of service
-----
0          0 1 2
1          3
2          4 5
3          6 7
Console#

```

SNMP ー 対応する MIB 変数

フィールド名	MIB 変数	アクセス	値の範囲	デフォルト値
Traffic Class Priority	MIB-II. dot1dBridge. pBridgeMIB. pBridgeMIBObjects. dot1dPriority. dot1dTrafficClassTable. dot1dTrafficClassEntry. dot1dTrafficClassPriority	アクセス不可	整数 (0 ~ 7)	
Traffic Class	MIB-II. dot1dBridge. pBridgeMIB. pBridgeMIBObjects. dot1dPriority. dot1dTrafficClassTable. dot1dTrafficClassEntry. dot1dTrafficClass	読み取り/ 書き込み	整数 (0 ~ 7)	3-67 ページを 参照

3.3.5.3 トラフィッククラスのサービス加重の設定

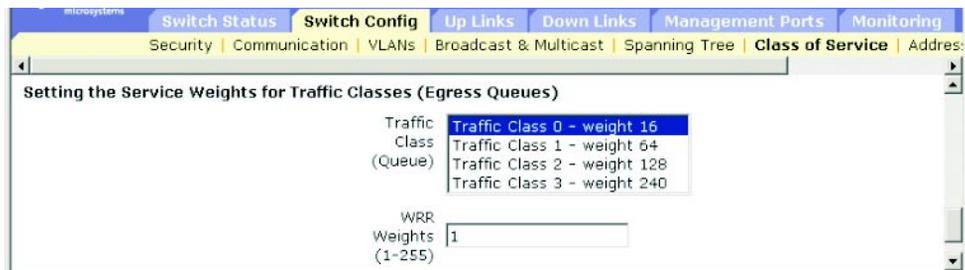
このスイッチは、加重ラウンドロビン (Weighted Round Robin : WRR) アルゴリズムを使用して、各優先順位キューのサービス間隔を決定します。3-67 ページの「CoS 値の送信キューへの割り当て」で説明したように、トラフィッククラスは、各ポートの 4 つの送信キューのいずれかに割り当てられています。このキュー (つまり各キューに対応するトラフィックの優先順位) に、加重を割り当てることができます。加重によって各キューに対するサービスのポーリング間隔が設定されるので、その結果、優先順位を割り当てられたソフトウェアアプリケーションの応答時間が変化します。

コマンド属性

- **Traffic Class (Queue)*** – 各トラフィッククラスの加重リストを表示します。
- **WRR Weights** – 選択したトラフィッククラスに新しい加重を設定します (範囲: 1 ~ 255)。

* CLI では「Queue ID」と表示されます。

Web – 「Switch Config」=> 「Class of Service」=> 「Basic Traffic Prioritisation」を開きます。「Setting the Service Weights for Traffic Classes (Egress Queues)」までスクロールします。トラフィッククラス (送信キュー) を選択し、加重値を入力して「Save」をクリックします。



CLI – 次に、CoS 優先順位キュー 0、1、2、3 に、WRR 加重 1、4、16、64 を割り当てる例を示します。

```
Console(config)#queue bandwidth 1 4 16 64          4-137
Console(config)#exit
Console#show queue bandwidth                        4-139
  Queue ID Weight
  -----
      0         1
      1         4
      2        16
      3        64
Console#
```

SNMP – 対応する MIB 変数

フィールド名	MIB 変数	アクセス	値の範囲	デフォルト値
WRR Traffic Class (Queue ID)	sun... priorityMgt. prioWrrTable. prioWrrEntry. prioWrrTrafficClass	インデックス	整数 (0 ~ 7)	
WRR Weight	sun... priorityMgt. prioWrrTable. prioWrrEntry. prioWrrWeight	読み取り/ 書き込み	整数 (1 ~ 255)	キュー 0 の場合 : 16 キュー 1 の場合 : 64 キュー 2 の場合 : 128 キュー 3 の場合 : 240

3.3.5.4 レイヤー 3 および 4 の優先順位の CoS 値への割り当て

このスイッチでは、アプリケーションの要求に応じて、レイヤー 3 および 4 のトラフィックに優先順位を付けるいくつかの一般的な方式をサポートしています。サービスタイプ (ToS) オクテットの優先順位ビットを使用して、トラフィックの優先順位をフレームの IP ヘッダーに指定できます。優先順位ビットを使用する場合は、ToS オクテットに、IP 優先順位 (Precedence) の 3 ビットの値、または Differentiated Services Code Point (DSCP) サービスの 6 ビットの値がセットされます。これらのサービスを使用可能にすると、スイッチは優先順位を CoS 値に割り当てて、対応する送信キューにトラフィックを送信します。

トラフィックに異なる優先順位情報が含まれることがあるため、このスイッチは、次の方法で優先順位値を送信キューに割り当てます。

- 優先順位は、IP 優先順位または IP DSCP、次にデフォルトのポート優先順位の順に割り当てられます。
- IP 優先順位および DSCP 優先順位を両方とも使用可能にすることはできません。優先順位タイプ的一方を使用可能にすると、もう一方のタイプは自動的に使用不可になります。

コマンド属性

- **Enable Priority Services** – CoS 値に対するレイヤー 3 および 4 の優先順位の割り当てを使用可能または使用不可にします (デフォルト : 使用不可)。
- **IP Precedence** – IP 優先順位を使用して、レイヤー 3 および 4 の優先順位を割り当てます。
- **Differentiated Services Code Point Mapping (DSCP)** – DSCP を使用してレイヤー 3 および 4 の優先順位を割り当てます。

Web – 「Switch Config」 => 「Class of Service」 => 「Layer 3/4 Traffic Prioritisation」を開きます。「Enable Priority Services」をオンにし、「IP Precedence」または「DSCP」を選択して「Save」をクリックします。



CLI – 次に、スイッチの IP 優先順位サービスを使用可能にする例を示します。

```
Console(config)#map ip precedence 4-140
Console(config)#
```

レイヤー 3 および 4 のトラフィック優先順位を完全に使用不可にするには、次のコマンドを実行します。

```
Console(config)#no map ip precedence 4-140
Console(config)#no map ip dscp 4-142
```

SNMP – 対応する MIB 変数

フィールド名	MIB 変数	アクセス	値の範囲	デフォルト値
IP Precedence/ DSCP Status	sun... priorityMgt. prioIpPrecDscpStatus	読み取り/ 書き込み	disabled (1)、 precedence (2)、 dscp (3)	disabled

3.3.5.5 IP 優先順位 (Precedence) の割り当て

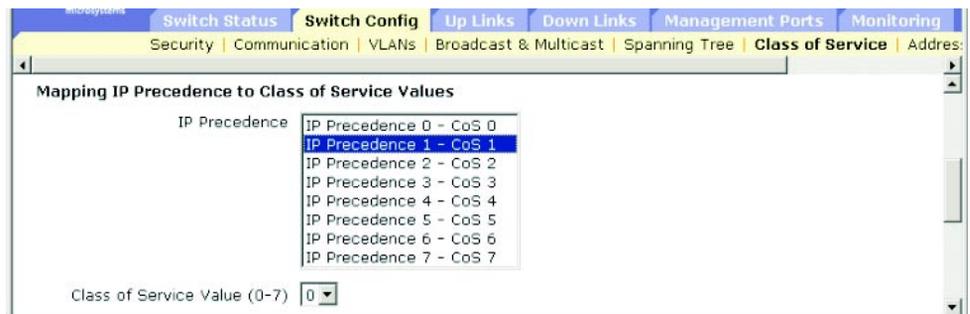
IPv4 ヘッダーの ToS オクテットには 3 ビットの優先順位ビットが含まれていて、ネットワーク制御パケット用のもっとも高い優先順位から、通常のトラフィック用のもっとも低い優先順位まで、8 つの優先順位を定義できます。デフォルトの IP 優先順位の値は、CoS 値に 1 対 1 で割り当てられます (たとえば、優先順位値 0 は CoS 値 0 に割り当てられます)。ビット 6 および 7 は、ネットワーク制御用に使用され、その他のビットもさまざまな用途に使用されます。次の表に、ToS ビットの定義を示します。

優先レベル	トラフィックタイプ
7	ネットワーク制御
6	インターネットワーク制御
5	重要
4	優先速報
3	速報
2	即時
1	優先
0	通常

コマンド属性

- **IP Precedence** – IP 優先順位と CoS の対応付けを表示します。
- **Class of Service Value** – 選択した IP 優先順位に CoS 値を割り当てます。0 は優先順位がもっとも低く、7 は優先順位がもっとも高くなります。

Web – 「Switch Config」 => 「Class of Service」 => 「Layer 3/4 Traffic Prioritisation」を開きます。「Mapping IP Precedence to Class of Service Values」までスクロールします。「IP Precedence」リストからエントリを選択し、「Class of Service Value」フィールドに値を指定して「Save」をクリックします。



CLI - 次に、ポート SNP5* の CoS 値 0 に IP 優先順位値 1 を割り当て、そのポートの IP 優先順位設定をすべて表示する例を示します。

```

Console(config)#interface ethernet SNP5                                4-75
Console(config-if)#map ip precedence 1 cos 0                          4-141
Console(config-if)#end
Console#show map ip precedence ethernet SNP5                          4-144
Precedence mapping status: disabled

  Port      Precedence COS
  -----
      SNP5          0    0
      SNP5          1    0
      SNP5          2    2
      SNP5          3    3
      SNP5          4    4
      SNP5          5    5
      SNP5          6    6
      SNP5          7    7
Console#

```

* IP 優先順位への値の割り当てにはインタフェース設定コマンドを使用しますが、変更内容はスイッチ上のすべてのインタフェースに適用されます。

SNMP - 対応する MIB 変数

フィールド名	MIB 変数	アクセス	値の範囲	デフォルト値
IP Precedence Value	sun... priorityMgt. prioIpPrecTable. prioIpPrecEntry. prioIpPrecValue	アクセス不可	整数 (0 ~ 7)	
IP Precedence CoS	sun... priorityMgt. prioIpPrecTable. prioIpPrecEntry. prioIpPrecCos	読み取り/ 書き込み	整数 (0 ~ 7)	1 対 1 の割り 当て

3.3.5.6 DSCP 優先順位の割り当て

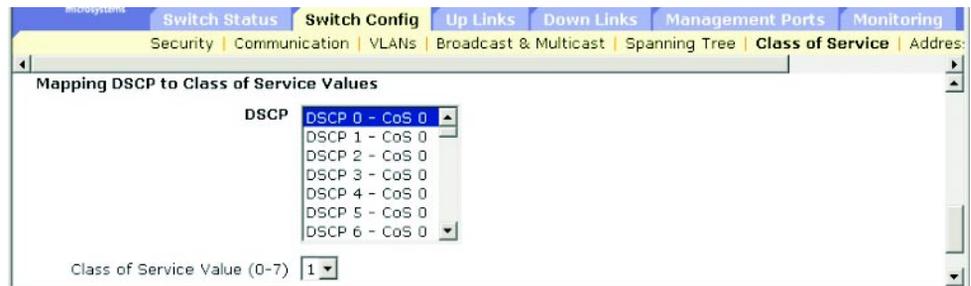
DSCP のビット幅は 6 ビットで、最大で 64 通りの転送動作をコーディングできます。DSCP は ToS ビットに代わるものですが、3 ビットの優先順位ビットに対する下位互換性があるため、DSCP に準拠していない ToS 対応の装置でも DSCP 割り当てとの競合が発生することはありません。ネットワークポリシーに基づいて、さまざまなタイプのトラフィックにさまざまな転送方法を指定できます。次の表に、DSCP のデフォルト値を示します。次の表に示されていない DSCP 値は、CoS 値 0 に割り当てられます。

IP DSCP 値	CoS 値
0	0
8	1
10、12、14、16	2
18、20、22、24	3
26、28、30、32、34、36	4
38、40、42	5
48	6
46、56	7

コマンド属性

- **DSCP** – DSCP 優先順位と CoS の対応付けを表示します。
- **Class of Service Value** – 選択した DSCP 優先順位の値に CoS 値を割り当てます。0 は優先順位がもっとも低く、7 は優先順位がもっとも高くなります。

Web – 「Switch Config」 => 「Class of Service」 => 「Layer 3/4 Traffic Prioritisation」を開きます。「Mapping DSCP to Class of Service Values」までスクロールします。「DSCP」リストからエントリを選択し、「Class of Service Value」フィールドに値を入力して「Save」をクリックします。



CLI - 次に、ポート SNP5* の CoS 値 1 に DSCP 値 0 を割り当て、そのポートの DSCP 優先順位設定をすべて表示する例を示します。

```

Console(config)#interface ethernet SNP5                                4-75
Console(config-if)#map ip dscp 0 cos 1                                4-143
Console(config-if)#end
Console#show map ip dscp ethernet SNP5                                4-145
DSCP mapping status: disabled

  Port          DSCP  COS
  -----
          SNP1      0    1
          SNP1      1    0
          SNP1      2    0
          SNP1      3    0
.
.
.
          SNP1     61    0
          SNP1     62    0
          SNP1     63    0
Console#

```

* IP DSCP への値の割り当てにはインタフェース設定コマンドを使用しますが、変更内容はスイッチ上のすべてのインタフェースに適用されます。

SNMP - 対応する MIB 変数

フィールド名	MIB 変数	アクセス	値の範囲	デフォルト値
IP DSCP Value	sun... priorityMgt. prioIpDscpTable. prioIpDscpEntry. prioIpDscpValue	アクセス不可	整数 (0 ~ 63)	
IP DSCP CoS	sun... priorityMgt. prioIpDscpTable. prioIpDscpEntry. prioIpDscpCos	読み取り/ 書き込み	整数 (0 ~ 7)	3-75 ページを 参照

3.3.6 アドレステーブルの設定

スイッチは、既知のすべての装置のアドレスを保持しています。この情報を使用して、受信ポートと送信ポートの間で直接トラフィックの経路指定が行われます。トラフィックを監視して学習したすべてのアドレスは、動的アドレステーブルに格納されます。特定のポートに割り当てる静的アドレスを、手動で設定することもできます。

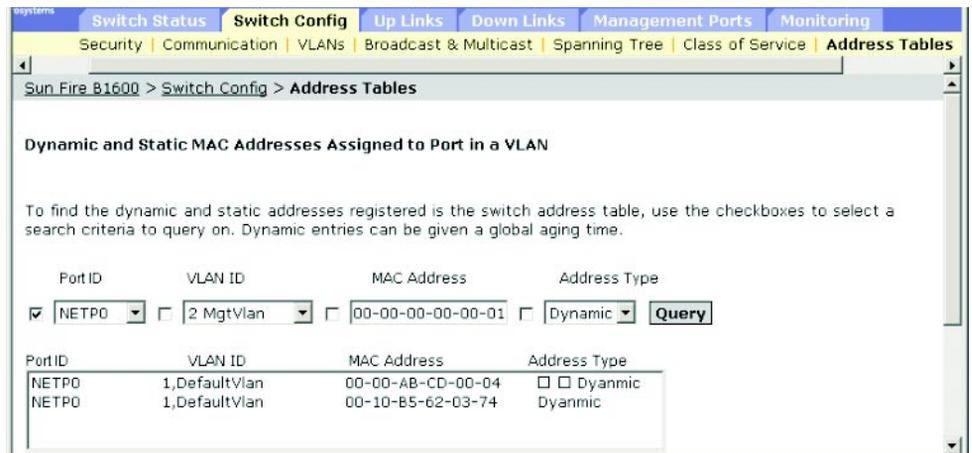
3.3.6.1 アドレステーブルの表示

アドレステーブルには、スイッチが受信したトラフィックの送信元アドレスを監視することで動的に学習した MAC アドレスが格納されます。受信トラフィックの宛先アドレスがデータベースに格納されている場合、そのアドレスに送信するパケットは、関連するポートに直接転送されます。そうでない場合は、すべてのポートにトラフィックがフラディングされます。アドレステーブルには、特定のポートに関連付けられた静的な MAC アドレスも格納されます。詳細は、3-99 ページの「静的アドレスの設定」を参照してください。

コマンド属性

- **Port ID (Interface*)** – ポートまたはトランクです (アップリンクポート : NETP0 ~ 7、ダウンリンクポート : SNP0 ~ 15、NETMGT の MAC アドレステーブルは表示されません)。
- **VLAN ID** – VLAN 識別子です (1 ~ 4094)。このフィールドに VLAN ID および名前が表示されます。
- **MAC Address** – このインタフェースに関連付けられた MAC アドレスです。
- **Address Type** – 学習したアドレスか、静的に設定されたアドレスかを示します。

Web – 「Switch Config」 => 「Address Tables」を開きます。検索条件に、インタフェース、VLAN、MAC アドレス、アドレスタイプを任意の組み合わせで指定し、「Query」をクリックします。



Port ID	VLAN ID	MAC Address	Address Type
NETP0	1,DefaultVlan	00-00-AB-CD-00-04	<input type="checkbox"/> Dynamic
NETP0	1,DefaultVlan	00-10-B5-62-03-74	Dynamic

CLI - 次に、ポート NETP1 のアドレステーブルエントリの例を示します。

```

Console#show mac-address-table interface ethernet NETP1      4-90
Interface   Mac Address          Vlan Type
-----
          NETP0 00-20-9c-23-cd-61 1    Dynamic
Console#

```

SNMP - 対応する MIB 変数

フィールド名	MIB 変数	アクセス	値の範囲
Interface	MIB-II. dot1dBridge.dot1dTp. dot1dTpFdbTable.dot1dTpFdbEntry. dot1dTpFdbPort	読み取り専用	not learned (0)、 ポートリスト (1 ~ 24)
MAC Address	MIB-II. dot1dBridge.dot1dTp. dot1dTpFdbTable.dot1dTpFdbEntry. dot1dTpFdbAddress	読み取り専用	MAC アドレス
VLAN	MIB-II. dot1dBridge.qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanStaticTable. dot1qVlanStaticEntry. dot1qVlanIndex	アクセス不可	整数
Type	MIB-II. dot1dBridge.dot1dTp. dot1dTpFdbTable.dot1dTpFdbEntry. dot1dTpFdbStatus	読み取り専用	other (1)、 invalid (2)、 learned (3)、 self (4)、 mgmt (5)

3.3.6.2 有効期限の変更

動的アドレステーブルのエントリに対して、有効期限を設定できます。

コマンド属性

- **Aging Time** — 動的に取得したエントリを破棄するまでの時間です (範囲 : 18 ~ 2184 秒、デフォルト : 300 秒)。

Web — 「Switch Config」 => 「Address Tables」 をクリックします。新しい有効期限を指定し 「Save」 をクリックします。



CLI — 次に、有効期限を 400 秒に設定する例を示します。

```
Console(config)#mac-address-table aging-time 400 4-91
Console(config)#
```

SNMP — 対応する MIB 変数

フィールド名	MIB 変数	アクセス	値の範囲	デフォルト値
Aging Time	MIB-II dot1dBridge.dot1dTp. dot1dTpAgingTime	読み取り/ 書き込み	整数 (18 ~ 2184) 秒	300 秒

3.4 ポートの設定

この節では、ダウンリンクポートおよびアップリンクポート、管理ポートのための設定メニューについて説明します。メニューのほとんどの項目は、すべてのポートタイプに適用されます。ただし、管理ポートは、いくつかの基本的なメニュー項目だけを使用します。また、パケットフィルタリング機能 (3-110 ページ) を使用できるのは、管理ポートだけです。

注 - この節のメニューで使用するポート識別子は、アップリンクポートは NETP0 ~ 7、ダウンリンクポートは SNP0 ~ 15、管理ポートは NETMGT です。

3.4.1 接続ステータスの表示

ポートステータスのページでは、リンク状態、速度およびデュプレックスモード、フロー制御、自動ネゴシエーション、ブロードキャストストーム制御などの、現在の接続ステータスを表示できます。

コマンド属性

- **Port Type** - ポートタイプを表示します (1000Base-SX または 1000Base-T、10/100Base-TX)。
- **Port** - ポートまたはトランクです (アップリンクポート : NETP0 ~ 7、ダウンリンクポート : SNP0 ~ 15、管理ポート : NETMGT)。
- **Description** - インタフェースのラベルです。
- **Admin Status** - インタフェースが使用可能または使用不可のどちらであることを表示します。
Web - 「Enabled」または「Disabled」を表示します。
CLI - 「Port Admin」に「up」または「down」を表示します。
- **Link Status** - リンクがアップまたはダウンのどちらの状態であることを表示します。
- **Port Operation Status** - ポートの状態の詳細情報を表示します。
CLI で、リンクのアップ時にだけ、この項目を確認できます。
- **Speed/Duplex** - 現在の速度およびデュプレックスモードを表示します。
- **Flow Control** - フロー制御が使用可能または使用不可のどちらであることを表示します。
Web - 「IEEE 802.3x」または「Back-Pressure」、「None」を表示します。
CLI - 「Enabled」または「Disabled」を表示します。「Flow Type」には、「IEEE 802.3x」または「Back-Pressure」、「None」を表示します。
- **Auto-negotiation** - 自動ネゴシエーションが使用可能または使用不可のどちらであることを表示します。

- **Protect Status** – このインタフェースでブロードキャストストーム制御が使用可能であるかどうかを表示します。しきい値の設定方法については、3-55 ページの「ブロードキャストストームの抑制 (グローバル設定)」を参照してください。
- **MAC Address** – このポートの物理レイヤーアドレスです。CLI でのみ確認できません。Web でこの項目を確認する方法については、3-11 ページの「IP アドレスの設定」を参照してください。
- **Port Capabilities*** – 自動ネゴシエーションで通知するポートの機能を指定します。次の機能をサポートしています。
 - 10half – 10 Mbps 半二重動作をサポート
 - 10full – 10 Mbps 全二重動作をサポート
 - 100half – 100 Mbps 半二重動作をサポート
 - 100full – 100 Mbps 全二重動作をサポート
 - 1000full – 1000 Mbps 全二重動作をサポート
 - Sym – フロー制御のためにポーズフレームを送受信
 - FC – フロー制御をサポート
- **LACP Status** – このポートで Link Aggregation Control Protocol (LACP) が使用可能であるかどうかを表示します (CLI のみ)。

* Web でこの項目を確認する方法については、3-84 ページの「インタフェース接続の設定」を参照してください。

Web – 「Up Links」 / 「Down Links」 / 「Management Port」 => 「Status」をクリックします。1 つ以上のインタフェースの接続を設定するときは、設定するエントリの横のチェックボックスをオンにして「Configure」をクリックします。詳細は、3-84 ページの「インタフェース接続の設定」を参照してください。

The screenshot shows the 'Up Links' configuration page in a web browser. The breadcrumb navigation is 'Sun Fire B1600 > Up Links > Connection Status'. Below the navigation, there is a 'Port Type: 1000Base-TX' label and a descriptive paragraph about Up Links. A 'Configure...' button is visible above a table of port configurations.

Port	Description	Admin Status	Link Status	Speed Duplex	Flow Control	AutoNeg	Protect Status
<input type="checkbox"/> NETP0	External RJ-45 connector NET0	Enabled	Up	100full	None	Enabled	Enabled
<input type="checkbox"/> NETP1	External RJ-45 connector NET1	Enabled	Down	1000full	None	Enabled	Enabled
<input type="checkbox"/> NETP2	External RJ-45 connector NET2	Enabled	Down	1000full	None	Enabled	Enabled
<input type="checkbox"/> NETP3	External RJ-45 connector NET3	Enabled	Down	1000full	None	Enabled	Enabled
<input type="checkbox"/> NETP4	External RJ-45 connector NET4	Enabled	Down	1000full	None	Enabled	Enabled
<input type="checkbox"/> NETP5	External RJ-45 connector NET5	Enabled	Down	1000full	None	Enabled	Enabled
<input type="checkbox"/> NETP6	External RJ-45 connector NET6	Enabled	Down	1000full	None	Enabled	Enabled
<input type="checkbox"/> NETP7	External RJ-45 connector NET7	Enabled	Down	1000full	None	Enabled	Enabled

CLI - 次に、ポート NETP7 の接続ステータスの例を示します。

```

Console#show interfaces status ethernet NETP7
Information of NETP7
Basic information:
  Port type: 1000T
  Mac address: 00-00-E8-66-66-83
Configuration:
  Name: External RJ-45 connector NET7
  Port admin: Up
  Speed-duplex: Auto
  Capabilities: 10half, 10full, 100half, 100full, 1000full,
  Broadcast storm: Enabled
  Broadcast storm limit: 256 packets/second
  Flow control: Disabled
  LACP: Disabled
Current status:
  Link status: Up
  Port operation status: Up
  Operation speed-duplex: 1000full
  Flow control type: None
Console#
  
```

SNMP - 対応する MIB 変数

フィールド名	MIB 変数	アクセス	値の範囲	デフォルト値
Port Type	sun... portMgt. portTable. portEntry. portType	読み取り専用	other(1)、 hundredBaseTX(2)、 hundredBaseFX(3)、 thousandBaseSX(4)、 thousandBaseLX(5)、 thousandBaseT(6)、 thousandBaseMiniGBIC(7) thousandBaseSFP(8)	
MAC Address	MIB-II. interfaces. ifTable.ifEntry. ifPhysAddress	読み取り専用	物理アドレス	
Port	sun... portMgt. portTable. portEntry	インデックス	整数 (1 ~ 25)	

フィールド名	MIB 変数	アクセス	値の範囲	デフォルト値
Port Name	sun... portMgt. portTable. portEntry. portName	読み取り/ 書き込み	表示文字列 (長さ 0 ~ 64)	
Administrative Status	MIB-II. interfaces. ifTable.ifEntry. ifAdminStatus	読み取り/ 書き込み	up (1)、 down (2)、 testing (3)	up
Link Status	MIB-II. interfaces. ifTable.ifEntry. ifOperStatus	読み取り専用	up (1)、 down (2 ~ 7)、	
Operational Status	MIB-II. interfaces. ifTable.ifEntry. ifOperStatus	読み取り専用	up (1)、 down (2)、 testing (3)、 unknown (4)、 dormant (5)、 notPresent (6)、 lowerLayerDown (7)	
Port Speed Duplex Status	sun... portMgt. portTable.portEntry. portSpeedDpxStatus	読み取り専用	error(1)、 halfDuplex10(2)、 fullDuplex10(3)、 halfDuplex100(4)、 fullDuplex100(5)、 halfDuplex1000(6)、 fullDuplex1000(7)	
Port Capabilities	sun... portMgt. portTable.portEntry. portCapabilities	読み取り/ 書き込み	Bits { portCap10half (0)、 portCap10full (1)、 portCap100half (2)、 portCap100full (3)、 portCap1000half (4)、 portCap1000full (5)、 reserved6 ~ 13 (6 ~ 13)、 portCapSym (14)、 portCapFlowCtrl (15)}	
Port Flow Control Status	sun... portMgt. portTable.portEntry. portFlowCtrlStatus	読み取り専用	error (1)、 backPressure(2)、 dot3xFlowControl(3)、 none (4)	なし

フィールド名	MIB 変数	アクセス	値の範囲	デフォルト値
LACP Port Status	sun... lacpMgt. lacpPortTable. lacpPortEntry. lacpPortStatus	読み取り/ 書き込み	enabled (1)、 disabled (2)	disabled
Port Auto-negotiation	sun... portMgt. portTable.portEntry. portAutonegotiation	読み取り/ 書き込み	enabled (1)、 disabled (2)	enabled
Broadcast Storm Status	sun... bcastStormMgt. bcastStormTable. bcastStormEntry. bcastStormStatus	読み取り/ 書き込み	enabled (1)、 disabled (2)	enabled

3.4.2 インタフェース接続の設定

ポート設定のページでは、インタフェースの使用可能と使用不可を切り替えます。また、自動ネゴシエーションと通知するインタフェース機能を設定するか、手動で速度およびデュプレックスモード、フロー制御を静的に設定します。

コマンド属性

- **Port/s** — ポートまたはトランクです (アップリンク : NETP0 ~ 7、ダウンリンク : SNP0 ~ 15)。
- **Port Description** — インタフェースにラベルを付けます (範囲 : 1 ~ 64 文字、デフォルト — アップリンク : 「External RJ-45 connector NETn」、ダウンリンク : 「Blade Slot n」、管理ポート : 「External RJ-45 connector NETMGT」)。
- **Administrative Status** — 手動でインタフェースを使用不可にします。衝突が多すぎるなどの動作が異常なインタフェースを使用不可にして、問題の解決後に再び使用可能にできます。また、セキュリティーのためにインタフェースを使用不可にすることもできます。
- **Negotiate Link Capabilities¹** — 自動ネゴシエーションを使用可能または使用不可に設定します。自動ネゴシエーションを使用可能に設定する場合は、通知する機能を指定する必要があります。自動ネゴシエーションを使用不可に設定する場合は、手動で設定した速度およびモード、フロー制御が有効になります。次の機能をサポートしています。
 - 10half — 10 Mbps 半二重動作をサポート
 - 10full — 10 Mbps 全二重動作をサポート
 - 100half — 100 Mbps 半二重動作をサポート
 - 100full — 100 Mbps 全二重動作をサポート
 - 1000half — 1000 Mbps 半二重動作をサポート
 - 1000full — 1000 Mbps 全二重動作をサポート

- **symmetric (Gigabit 専用)** – この項目をオンにすると、ポーズフレームが送受信されます。オフにすると、非対称ポーズフレームの送信側および受信側の自動ネゴシエーションが行われます。このスイッチは、対称ポーズフレームだけをサポートします。
- **flowcontrol** – フロー制御をサポートします。
フロー制御は、バッファがいっぱいになったときに、スイッチに直接接続されたエンドステーションまたはセグメントからのトラフィックを「ブロッキング」することでフレーム損失を防ぎます。使用可能にすると、半二重動作にはバックプレッシャーが、全二重動作には IEEE 802.3x が使用されます。

注 – Sun Fire B1600 ブレードシステムシャーシの統合スイッチは、相互に接続する 2 つのスイッチチップで構成されています。使用可能にできるのは、同じスイッチチップ上の 2 つのポート間のフロー制御だけです。ポート NETP0 および NETP1、NETP4、NETP5、SNP8 ~ 15 は、一方のスイッチチップ上にあります。ポート NETP2 および NETP3、NETP6、NETP7、SNP0 ~ 7 は、もう一方のスイッチチップ上にあります (SSC の背面パネルの右側にあるすべてのポートが一方のチップ上に、左側にあるすべてのポートがもう一方のチップ上にあります)。

- **Speed/Duplex²** – 自動ネゴシエーションを使用不可にした場合に、ポートの速度およびデュプレックスモードを手動で設定できます。

注 – 自動ネゴシエーションを使用不可にした場合は、アップリンクポートに 10 Mbps または 100 Mbps だけを設定できます。ポートを 1 Gbps 全二重で動作させる場合は、自動ネゴシエーションを使用可能にして、ポートの伝送速度に 1000full だけを設定します。

- **Flow Control²** – 自動ネゴシエーションを使用不可にした場合は、フロー制御を使用可能または使用不可に設定する必要があります。ハブに接続するポートでは、問題の解決に必要な場合を除き、フロー制御を使用しないでください。ハブに接続するポートでフロー制御を使用すると、バックプレッシャーの妨害信号によって、ハブに接続されたセグメントの全体的な性能が低下することがあります。
- **Broadcast storm suppression** – 選択したポートに対して、ブロードキャストストーム制御を使用可能にします。ブロードキャストストーム制御またはブロードキャストしきい値レベルの設定方法については、3-55 ページの「ブロードキャストストームの抑制 (グローバル設定)」を参照してください。

1. ダウンリンクポートの自動ネゴシエーションを使用不可にすることはできません。ダウンリンクポートは、1000 Mbps 全二重に固定されています。
2. インタフェースに特定の速度またはデュプレックスモード、フロー制御オプションを設定するには、アップリンクポートの自動ネゴシエーションを使用不可にしておく必要があります。

Web – 「Up Links」 / 「Down Links」 => 「Status」画面を開きます。設定するインタフェースのチェックボックスをオンにして「Configure」をクリックします。必要なインタフェース設定を変更して「Save」をクリックします。

Microsystem
Switch Setup | Switch Config | **Up Links** | Down Links | Management Ports | Monitoring

Status | Link Aggregation | VLANs | Address Filtering | Spanning Tree

Port/s:NETP0

Port Description: External RJ-45 connect

Set Port Administrative Status:

Enable
 Disable

Enable port auto-negotiation capabilities:

Auto-negotiation enabled
Select link parameter capabilities to advertise

1000full 1000half
 100full 100half
 10full 10half
 flowcontrol symmetric

Auto-negotiation disable
Select link parameters to use

1000full 1000half
 100full 100half
 10full 10half

Flow control enabled

Set Broadcast storm Suppression:

Enable
 Disable

CLI – インタフェースを選択して、必要な設定値を入力します。

```

Console#Console(config)#interface ethernet NETP1           4-75
Console(config-if)#description RD SW#17                    4-76
Console(config-if)#shutdown                                4-82
.
.
.
Console(config-if)#no shutdown
Console(config-if)#negotiation
Console(config-if)#capabilities 1000full                   4-79
Console(config-if)#capabilities 1000full                   4-79
Console(config-if)#capabilities flowcontrol
.
.
.
Console(config-if)#no negotiation                           4-78
Console(config-if)#speed-duplex 100half                    4-77
Console(config-if)#flowcontrol                              4-81
Console(config-if)#

```

SNMP – 対応する MIB 変数

フィールド名	MIB 変数	アクセス	値の範囲	デフォルト値
Port Name	sun... portMgt. portTable.portEntry. portName	読み取り / 書き込み	表示文字列 (長さ 0 ~ 64)	3-84 ページ を参照
Administrative Status	MIB-II. interfaces. ifTable.ifEntry. ifAdminStatus	読み取り / 書き込み	up (1)、 down (2)、 testing (3)	up
Port Auto- negotiation	sun... portMgt. portTable.portEntry. portAutonegotiation	読み取り / 書き込み	enabled(1)、 disabled(2)	enabled
Port Capabilities	sun... portMgt. portTable.portEntry. portCapabilities	読み取り / 書き込み	Bits { portCap10half (0)、 portCap10full (1)、 portCap100half (2)、 portCap100full (3)、 portCap1000half (4)、 portCap1000full (5)、 reserved6 ~ 13 (6 ~ 13)、 portCapSym (14)、 portCapFlowCtrl (15)}	
Port Speed Duplex Configuration	sun... portMgt. portTable.portEntry. portSpeedDpxCfg	読み取り / 書き込み	reserved(1)、 halfDuplex10(2)、 fullDuplex10(3)、 halfDuplex100(4)、 fullDuplex100(5)、 halfDuplex1000(6)、 fullDuplex1000(7)	
Port Flow Control Configuration	sun... portMgt. portTable.portEntry. portFlowCtrlCfg	読み取り / 書き込み	enabled(1)、 disabled(2)、 backPressure(3)、 dot3xFlowControl(4)	

3.4.3 ポートトランクの設定

装置間には、1つの仮想的な集約されたリンクとして機能する、複数のリンクを作成できます。ポートトランクを使用すると、ボトルネックのあるネットワークセグメントの帯域幅を大幅に拡張し、2台の装置間に耐障害性の高いリンクを作成できます。トランクは、一度に6つまで作成できます。

スイッチは、静的なトランクおよび動的な Link Aggregation Control Protocol (LACP) の両方をサポートします。LACP が設定されたポートは、LACP が設定されたほかの装置のポートとの間で、自動的にトランクリンクのネゴシエーションを行います。スイッチのアップリンクポートは、静的なトランクに設定されていないかぎり、いくつでも LACP に設定できます。ほかにポートに LACP が設定された装置があれば、スイッチとその装置はトランクリンクのネゴシエーションを行います。LACP のトランクが5つ以上のポートで構成されている場合、5つ目以降のポートはスタンバイモードになります。トランクの中の1つのリンクに障害が発生すると、スタンバイモードのポートが自動的にアクティブになって処理を続けます。

コマンドの使用法

追加のポートがあると、トランク内の各ポートに負荷を分散できるだけでなく、ポートに障害が発生した場合に負荷を引き継ぐ冗長性を確保できます。これには、装置を物理的に接続する前に、Web インタフェースまたは CLI を使用して、両端にある装置のトランクを設定しておく必要があります。ポートトランクを使用するときは、次の点に注意してください。

- ループが形成されないように、スイッチ間の対応するネットワークケーブルを接続する前に、ポートトランクの設定を終了しておく必要があります。
- スイッチには最大6つのトランクを作成し、各トランクには最大4つのポートを設定できます。
- 接続の両端のポートをトランクポートとして設定する必要があります。
- トランクの両端のポートは、通信モード (速度およびデュプレックスモード、フロー制御)、VLAN 割り当て、CoS 設定などの設定内容を同一にする必要があります。
- ターゲットスイッチの接続ポートでも LACP が使用可能になっていると、トランクは自動的にアクティブになります。
- LACP を使用してほかのスイッチとトランクを形成すると、自動的に次に使用できるトランク ID が割り当てられます。
- 同じターゲットスイッチに5つ以上のポートを接続して LACP が使用可能になっている場合、5つ目以降の追加ポートはスタンバイモードになり、アクティブなリンクが接続に失敗した場合にのみ使用可能になります。
- VLAN に対する移動または追加、削除を行う場合は、トランク内のすべてのポートをまとめて取り扱う必要があります。
- STP および VLAN、IGMP は、トランク全体に対してのみ設定できます。

3.4.3.1 LACP によるトランクの動的な設定

Web – 「Up Links」 / 「Down Links」 => 「Link Aggregation」をクリックします。「Link Aggregation」リストから必要なポートを選択して「Enable LACP」または「Disable LACP」ボタンをクリックします。

注 – ボタンをクリックすると、ただちに処理が行われます。ネットワーク上にループが形成されないように、LACP を使用可能にしてからポートを接続するか、ポートの接続を外してから LACP を使用不可にしてください。詳細は、3-88 ページの「コマンドの使用法」を参照してください。



CLI – 次に、ポート NETP0 および NETP1 の LACP を使用可能にする例を示します。このポートを、ほかのスイッチの LACP に対応する 2 つのトランクポートに接続するとトランクが形成されます。

```
Console(config)#interface ethernet NETP0                                4-75
Console(config-if)#lACP                                                4-150
Console(config-if)#exit
Console(config)#interface ethernet NETP1
Console(config-if)#lACP
Console(config-if)#end
Console#show interfaces status port-channel 1                          4-84
Information of Trunk 1
Basic information:
  Port type: 1000T
  Mac address: 00-00-E8-66-66-83
```

```

Configuration:
  Name:
  Port admin: Up
  Speed-duplex: Auto
  Capabilities: 10half, 10full, 100half, 100full, 1000full,
  Flow control status: Disabled
Current status:
  Created by: Lacp
  Link status: Up
  Port operation status: Up
  Operation speed-duplex: 1000full
  Flow control type: None
  Member Ports: NETP0, NETP1,
  Console#

```

SNMP - 対応する MIB 変数

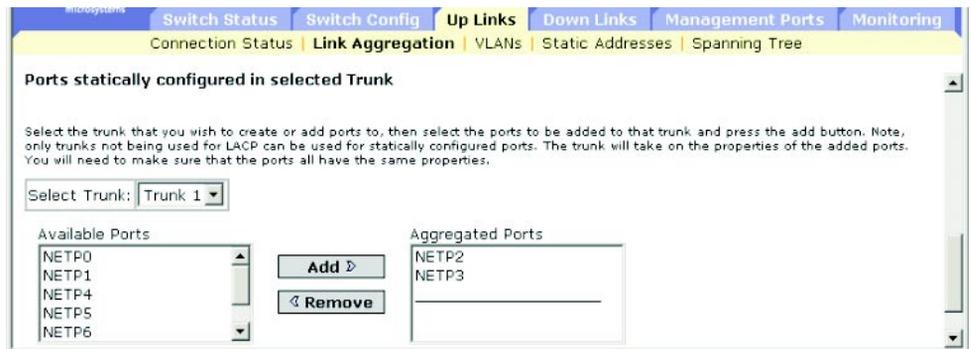
フィールド名	MIB 変数	アクセス	値の範囲	デフォルト値
Trunk Maximum ID	sun... trunkMgt. trunkMaxId	読み取り専用	整数	6
Trunk Valid Number	sun... trunkMgt. trunkValidNumber	読み取り専用	整数 (1 ~ 6)	
Trunk Index	sun... trunkMgt. trunkTable.trunkEntry. trunkIndex	インデックス	整数	
Trunk Ports	sun... trunkMgt. trunkTable.trunkEntry. trunkPorts	読み取り / 作成	オクテット文字列 (ポートリスト)	
Trunk Creation	sun... trunkMgt. trunkTable.trunkEntry. trunkCreation	読み取り専用	static (1)、 lacp (2)	
Trunk Status	sun... trunkMgt. trunkTable.trunkEntry. trunkStatus	読み取り / 作成	valid (1)、 invalid (2)	
LACP Port Status	sun... lacpMgt. lacpPortTable. lacpPortEntry. lacpPortStatus	読み取り / 書き込み	enabled (1) disabled (2)	

ほかの CLI 変数については、3-80 ページの「接続ステータスの表示」を参照してください。

3.4.3.2 トランクの静的な設定

Web – 「Up Links」 / 「Down Links」 => 「Link Aggregation」 をクリックします。ドロップダウンリストからトランクを選択し、必要なポートを選択して「Add」または「Remove」 をクリックします。

注 – ボタンをクリックすると、ただちに処理が行われます。ネットワーク上にループが形成されないように、設定インターフェースで静的にトランクを追加してからポートを接続するか、ポートの接続を外してからトランクを削除してください。詳細は、3-88 ページの「コマンドの使用法」を参照してください。



CLI – 次に、ポート NETP2 および NETP3 を含む Trunk2 を作成する例を示します。このポートを、ほかのスイッチの 2 つの静的なトランクポートに接続するとトランクが形成されます。

```
Console(config)#interface port-channel 2                                4-75
Console(config-if)#exit
Console(config)#interface ethernet NETP2                                4-75
Console(config-if)#channel-group 2                                     4-149
Console(config-if)#exit
Console(config)#interface ethernet NETP3
Console(config-if)#channel-group 2
Console(config-if)#end
Console#show interfaces status port-channel 2                            4-84
Information of Trunk 2
Basic information:
  Port type: 1000t
  Mac address: 00-00-E8-66-66-83
Configuration:
Port admin status: Up
Speed-duplex: Auto
Capabilities: 10half, 10full, 100half, 100full, 1000full,
Flow control status: Disabled
```

```

Current status:
Created by: User
Link status: Up
Port operation status: Up
Operation speed-duplex: 1000full
Flow control type: None
Member Ports: NETP2, NETP3,
Console#

```

SNMP - 対応する MIB 変数

フィールド名	MIB 変数	アクセス	値の範囲	デフォルト値
Trunk Maximum ID	sun... trunkMgt.trunkMaxId	読み取り専用	整数	6
Trunk Valid Number	sun... trunkMgt. trunkValidNumber	読み取り専用	整数 (1 ~ 6)	
Trunk Index	sun... trunkMgt.trunkTable. trunkEntry.trunkIndex	インデックス	整数	
Trunk Ports	sun... trunkMgt.trunkTable. trunkEntry.trunkPorts	読み取り / 作成	オクテット文字列 (ポートリスト)	
Trunk Creation	sun... trunkMgt. trunkTable.trunkEntry. trunkCreation	読み取り専用	static (1)、 lACP (2)	
Trunk Status	sun... trunkMgt.trunkTable. trunkEntry.trunkStatus	読み取り / 作成	valid (1)、 invalid (2)	

ほかの CLI 変数については、3-80 ページの「接続ステータスの表示」を参照してください。

3.4.4 インタフェースの VLAN 動作の設定

インタフェースには、デフォルトの VLAN 識別子 (PVID)、受け入れられるフレームタイプ、イングレスフィルタリング、GVRP ステータス、GARP タイマーなどの VLAN 動作を設定できます。

コマンドの使用法

- **GVRP** – GARP VLAN Registration Protocol は、ネットワーク全体のインタフェースの VLAN メンバーを自動的に登録するために、スイッチが VLAN 情報を交換する方法を定義します。
- **GARP** – Group Address Registration Protocol は、GVRP によって、ブリッジ接続された LAN 内のクライアントサービスのクライアント属性を登録または削除するために使用されます。GARP タイマーのデフォルト値は、媒体アクセス方式またはデータ転送速度には依存しません。GVRP の登録または削除処理で問題が発生した場合以外は、このデフォルト値を変更しないでください。

コマンド属性

- **Port** – ポートまたはトランクです (アップリンク : NETP0 ~ 7、ダウンリンク : SNP0 ~ 15、管理 : NETMGT)。
- **Default VLAN for Port (PVID)** – インタフェースが受信したタグなしフレームに割り当てられる VLAN ID です (デフォルト – アップ/ダウンリンク : 1、NETMGT : 2)。

注 – インタフェースが VLAN 1 のメンバーではない場合に、そのインタフェースの PVID を VLAN 1 にすると、インタフェースはタグなしメンバーとして VLAN 1 に自動的に追加されます。その他の VLAN の場合は、最初にインタフェースをタグなしメンバーとして設定してから、PVID にそのグループを設定します。

- **Acceptable Frame Types** – インタフェースが受け入れるフレームタイプを設定します。タグ付きとタグなしのすべてのフレームを受け入れるか、タグ付きフレームだけを受け入れるかを指定できます。すべてのフレームタイプを受信するように設定した場合、受信したタグなしフレームはデフォルトの VLAN に割り当てられます (オプション : すべて、タグ付きのみ、デフォルト : すべて)。
- **Switch Port Mode** – ポートの VLAN メンバーシップモードを設定します (デフォルト : トランク)。
 - **Trunk** – ポートを VLAN トランクの終端として指定します。トランクとは、2つのスイッチ間の直接リンクです。そのため、ポートは、送信元の VLAN を識別できるタグ付きフレームを転送します。
 - **Hybrid** – ハイブリッド VLAN インタフェースを指定します。ポートは、タグ付きフレームまたはタグなしフレームを転送します。

注 – スイッチポートのモードを「Trunk」に設定すると、そのポートのデフォルトの VLAN (PVID に関連付けられた VLAN) に属するフレームはタグなしで送信されますが、その他のフレームには割り当てられた VLAN ID のタグが付きます。

- **Ingress Filtering** — イングレスフィルタリングを使用可能にすると、この入口ポートがメンバーに含まれていない VLAN の受信フレームは、入口ポートで破棄されます (デフォルト: 使用不可)。

注 —

- イングレスフィルタリングは、タグ付きフレームだけに影響を与えます。
 - イングレスフィルタリングを使用不可にすると、ポート上で明示的に禁止されている VLAN を除いて、スイッチが認識している VLAN と一致するタグの付いた VLAN タグ付きフレームはすべて受け入れられるようになります。
 - イングレスフィルタリングを使用可能にすると、この入口ポートがメンバーに含まれていない VLAN のタグ付き受信フレームは破棄されます。
 - イングレスフィルタリングは、GVRP、STP などの VLAN に依存しない BPDU フレームには影響を与えません。ただし、GMRP などの VLAN に依存する BPDU フレームには影響を与えます。
-
- **GVRP** — インタフェースに対して GVRP を使用可能または使用不可にします。この設定を有効にするには、事前にスイッチのグローバル設定によって GVRP を使用可能にしておく必要があります (3-38 ページ)。使用不可を設定すると、このポートが受信する GVRP パケットは破棄されて、GVRP の登録情報がほかのポートから伝播されなくなります (デフォルト: 使用不可)。
 - **GARP Join Timer** — VLAN グループへの参加の要求および照会を送信する間隔です (範囲: 20 ~ 1000 センチ秒、デフォルト: 20 センチ秒)。
 - **GARP Leave Timer** — ポートが VLAN グループを離脱するまで待機する間隔です。この値は、Join Timer の 2 倍以上にする必要があります。これによって、Leave または LeaveAll メッセージを発行してグループメンバーが再参加したあとで、ポートがグループを離脱するようにします (範囲: 60 ~ 3000 センチ秒、デフォルト: 60 センチ秒)。
 - **GARP LeaveAll Timer** — VLAN グループメンバーに LeaveAll 照会メッセージを送信してから、ポートがグループを離脱するまでの間隔です。グループに再参加するノードによって生成されるトラフィック量を最小限に抑えるため、この間隔は Leave Timer よりかなり長くする必要があります (範囲: 500 ~ 18000 センチ秒、デフォルト: 1000 センチ秒)。
 - **VLAN on Selected Port** — 指定した VLAN にポートを静的に割り当てます。
 - **Membership Type** — ポートの静的な VLAN メンバーシップを設定します。
 - **Tagged**: インタフェースは VLAN のメンバーです。この VLAN 上のポートが送信するすべてのパケットにタグが付いて、このタグによって VLAN または CoS 情報が配信されます。
 - **Untagged**: インタフェースは VLAN のメンバーです。この VLAN 上のポートが送信するすべてのパケットからタグが外されるので、VLAN または CoS 情報は配信されません。
 - **Forbidden**: インタフェースは、GVRP を介して VLAN に自動的に参加することを禁止されています。詳細は、3-34 ページの「VLAN の自動登録」を参照してください。
 - **Remove**: 選択したインタフェースをこの VLAN から削除します。

Web – 「Up Links」 / 「Down Links」 / 「Management Port」 => 「VLANs」 をクリックします。各インタフェースで必要な設定を行い「Save」をクリックします。

The screenshot shows the 'VLANs' configuration page for a selected port. The breadcrumb path is 'Sun Fire 81600 > Up Links > VLANs'. A dropdown menu for 'Select Port:' is set to 'NETP4'. The page contains several configuration sections:

- Default VLAN for Port (PVID):** A dropdown menu is set to '4, Finance'.
- Acceptable Frame Types:** Radio buttons for 'All Frame Types' (selected), 'Tagged Only', and 'Switch Port Mode'.
- Switch Port Mode:** Radio buttons for 'Trunk' and 'Hybrid' (selected).
- Ingress Filtering Enabled:** A checkbox that is currently unchecked.
- Enable GARP VLAN Registration Protocol (GVRP):** Radio buttons for 'Enable' (selected) and 'Disable'.
- Configure Group Address Registration Protocol(GARP) Parameters:** Input fields for 'GARP Join Timer' (20), 'GARP Leave Timer' (60), and 'GARP LeaveAll Timer' (1000).

At the bottom right, there are 'Save' and 'Cancel' buttons.

VLAN メンバーシップのリストまでスクロールし、選択したインタフェースに必要な VLAN を設定します。

The screenshot shows the 'Configure VLANs on Selected Port' page. The breadcrumb path is 'Sun Fire 81600 > Up Links > VLANs'. The page contains the following sections:

- All VLANs:** A list box containing '3, R&D' and '5, Marketing'.
- Membership VLANs:** A list box containing '1, DefaultVlan, Allow(untagged)', '2, MgtVlan, Forbidden', and '4, Finance, Allow(tagged)'.
- Buttons:** 'Add Tagged', 'Add Untagged', 'Add Forbidden', and 'Remove' buttons are located between the two list boxes.

At the bottom right, there are 'Save' and 'Cancel' buttons.

CLI ー 次に、ポート NETP4 でタグ付きフレームだけを受信するように設定し、ネイティブ VLAN ID として PVID 4 を割り当て、GVRP を使用可能にし、GARP タイマーを設定し、スイッチポートのモードをハイブリッドに設定する例を示します。

```

Console(config)#interface ethernet NETP4                                4-75
Console(config-if)#switchport acceptable-frame-types tagged           4-112
Console(config-if)#no switchport ingress-filtering                    4-113
Console(config-if)#switchport allowed vlan add 4 tagged               4-115
Console(config-if)#switchport native vlan 4                           4-114
Console(config-if)#switchport gvrp                                    4-118
Console(config-if)#garp timer join 10                                  4-120
Console(config-if)#garp timer leave 90                                4-120
Console(config-if)#garp timer leaveall 2000                           4-120
Console(config-if)#switchport mode hybrid                              4-111
Console(config-if)#switchport forbidden vlan add 3                    4-116
Console(config-if)#

```

SNMP ー 対応する MIB 変数

フィールド名	MIB 変数	アクセス	値の範囲	デフォルト値
Port PVID	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qPortVlanTable. dot1qPortVlanEntry. dot1qPvid	読み取り/ 書き込み	整数 (1 ~ 4094)	1
Port Acceptable Frame Type	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qPortVlanTable. dot1qPortVlanEntry. dot1qPortAcceptable- FrameTypes	読み取り/ 書き込み	admitAll (1)、 admitOnlyVlan- Tagged (2)	admitAll
Port Mode	sun... vlanMgt. vlanPortTable. vlanPortEntry. vlanPortMode	読み取り/ 書き込み	hybrid (1)、 dot1qTrunk (2)	hybrid

フィールド名	MIB 変数	アクセス	値の範囲	デフォルト値
Port Ingress Filtering	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qPortVlanTable. dot1qPortVlanEntry. dot1qPortIngressFiltering	読み取り/ 書き込み	true (1)、 false (2)	false
Port GVRP Status	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qPortVlanTable. dot1qPortVlanEntry. dot1qPortGVRPStatus	読み取り/ 書き込み	enabled (1)、 disabled (2)	disabled
GARP Join Time	MIB-II. dot1dBridge. pBridgeMIB. pBridgeMIBObjects. dot1dGarp. dot1dPortGarpTable. dot1dPortGarpEntry. dot1dPortGarpJoinTime	読み取り/ 書き込み	整数 (20 ~ 1000) センチ秒	20 センチ秒
GARP Leave Time	MIB-II. dot1dBridge. pBridgeMIB. pBridgeMIBObjects. dot1dGarp. dot1dPortGarpTable. dot1dPortGarpEntry. dot1dPortGarpLeaveTime	読み取り/ 書き込み	整数 (60 ~ 3000) センチ秒	60 センチ秒
GARP Leave All Time	MIB-II. dot1dBridge. pBridgeMIB. pBridgeMIBObjects. dot1dGarp. dot1dPortGarpTable. dot1dPortGarpEntry. dot1dPortGarp- LeaveAllTime	読み取り/ 書き込み	整数 (500 ~ 18000) センチ秒	1000 センチ秒

フィールド名	MIB 変数	アクセス	値の範囲	デフォルト値
VLAN Static Name	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanStaticTable. dot1qVlanStaticEntry. dot1qVlanStaticName	読み取り / 作成	オクテット文字列 (長さ 0 ~ 32)	
VLAN Static Row Status	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanStaticTable. dot1qVlanStaticEntry. dot1qVlanStaticRowStatus	読み取り / 作成	enable (1), disable (2)	
Tagged Ports, Untagged Ports (VLAN 許可)	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanTable. dot1qVlanEntry. dot1qVlanStatic- UntaggedPorts	読み取り / 作成	オクテット文字列 (ポートリスト)	
VLAN Forbidden Ports	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qPortVlanTable. dot1qPortVlanEntry. dot1qVlanForbidden- EgressPorts	読み取り / 作成	オクテット文字列 (ポートリスト)	

3.4.5 静的アドレスの設定

アドレスのフィルタリング機能によって、特定のポートおよび VLAN に割り当てる静的アドレスを設定し、受信トラフィックを現在アドレステーブルに設定されているエントリ (動的または静的アドレス) に制限するポートセキュリティーを使用可能にできます。

コマンドの使用法

- **静的アドレスの設定** — このスイッチの特定のインタフェースに、静的アドレスを割り当てることができます。現在いずれかのインタフェースに割り当てられている静的アドレスを別のインタフェースに割り当てても、インタフェースはそのアドレスでデータの送受信を行うことができないので、アドレスはアドレステーブルに追加されません。
- **ポートセキュリティーの設定** — ポートセキュリティーを使用可能にすると、スイッチは、指定されたポートでの新しいアドレスの動的な学習を停止します。送信元アドレスがすでに動的アドレステーブル内に保存されている受信トラフィックだけが受け入れられます。ポートセキュリティーを使用するには、まず、初期の学習期間としてインタフェースが受信したフレームの <送信元 MAC アドレス、VLAN> の組をスイッチに動的に学習させてから、ポートセキュリティーを使用可能にしてアドレスの学習を停止します。学習機能を使用可能にする期間は十分にとって、選択したインタフェースに有効な VLAN メンバーがすべて登録されるようにしてください。

あとで新しい VLAN メンバーを追加する場合は、静的アドレスを手動で追加するか、ポートセキュリティーをオフに設定して、新しい VLAN メンバーを登録するために必要な期間だけ学習機能を再び使用可能にします。安全のため、必要に応じて、学習機能を再び使用不可にします。

コマンド属性

- **Port** — インタフェースです (ポートまたはトランク)
(アップリンクポート : NETP0 ~ 7、ダウンリンクポート : SNP0 ~ 15)。
- **Secure Port** — ポートセキュリティーを使用可能または使用不可にします (デフォルト : 使用不可)。
セキュリティー保護されたポートには、次の制限があります。
 - ポートの監視機能を使用できません。
 - マルチ VLAN インタフェースにすることはできません。
 - ネットワークの相互接続装置には接続できません。
 - トランクポートにすることはできません。
- **Number of Static Addresses*** — 手動で設定したアドレスの数です。
- **VLAN** — 設定する VLAN の ID (1 ~ 4094) および名前です。
- **MAC Address** — このインタフェースに関連付けられた MAC アドレスです。
- **Duration** — アドレスは、次のタイプに設定できます。
 - **Permanent** — 割り当ては永続的で、スイッチのリセット後に復元されます。
 - **Delete on Reset** — スイッチがリセットされるまで割り当てられます。

* Web でのみ確認できます。

Web – 「Up Links」 / 「Down Links」 => 「Address Filtering」をクリックします。インターフェースを指定します。「Secure Port」チェックボックスをオンにしてポートセキュリティーを使用可能にします。次に、VLAN および MAC アドレス、有効期間を入力して、「Add」をクリックします。

The screenshot shows the 'Static Addresses' configuration page in the Sun Fire B1600 web interface. The breadcrumb trail is 'Sun Fire B1600 > Up Links > Static Addresses'. The 'Select Port' dropdown is set to 'NETP4'. Below this, there is a note: 'A static address can be assigned to a specific interface on the switch. Static addresses are bound to the assigned interface and will not be moved. When a static address is seen on another interface, the address will be ignored and will not be written to the address table.' The 'Secure port to prevent dynamic learning of new addresses:' section has 'Unsecured' selected. The 'Number of Static Addresses:' input field contains the value '2'. At the bottom right of this section are 'Save' and 'Cancel' buttons. Below this is the 'Static MAC Addresses Assigned to Port in a VLAN' section, which contains a table with two entries: '1, DefaultVlan, 00-80-C8-00-00-01, Permanent' and '1, DefaultVlan, 00-80-C8-00-00-02, Delete on Reset'. A 'Remove' button is located to the right of the table. At the bottom, there are input fields for 'VLAN:' (set to '1, DefaultVlan'), 'MAC Address:', and 'Duration:' (set to 'Delete on Reset'), followed by an 'Add' button.

CLI – 次に、同じ項目を静的アドレステーブルに追加する例を示します。

```

Console(config)#interface ethernet NETP4
Console(config-if)#port security                                4-93
Console(config-if)#exit
Console(config)#mac-address-table static 00-80-c8-00-00-01
  interface ethernet NETP4 vlan 1 permanent                    4-89
Console(config)#mac-address-table static 00-80-c8-00-00-02
  interface ethernet NETP4 vlan 1 delete-on-reset
Console(config)#exit
Console#show mac-address-table ethernet NETP4                  4-90
  Interface   Mac Address          Vlan Type
  -----
           NETP4 00-80-C8-00-00-01    1 Permanent
           NETP4 00-80-C8-00-00-02    1 Delete-on-reset
Console#

```

SNMP – 対応する MIB 変数

フィールド名	MIB 変数	アクセス	値の範囲	デフォルト値
Static Receive Port	MIB-II. dot1dBridge. dot1dStatic. dot1dStaticTable. dot1dStaticEntry. dot1dStaticReceivePort	読み取り / 書き込み	整数	
Port Security Status	sun... securityMgt. portSecurityMgt portSecPortTable. portSecPortEntry. portSecPortStatus	読み取り / 書き込み	enabled (1)、 disabled (2)	disabled
Number of Static Addresses	未定義			
VLAN Index	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanStaticTable. dot1qVlanStaticEntry. dot1qVlanIndex	インデックス	整数	
Static Address	MIB-II. dot1dBridge. dot1dStatic. dot1dStaticTable. dot1dStaticEntry. dot1dStaticAddress	読み取り / 書き込み	MAC アドレス	
Static Status	MIB-II. dot1dBridge. dot1dStatic. dot1dStaticTable. dot1dStaticEntry. dot1dStaticStatus	読み取り / 書き込み	other(1)、 invalid(2)、 permanent(3)、 deleteOnReset(4)、 deleteOnTimeout(5)	permanent

3.4.6 スパニングツリーアルゴリズムのインタフェースの管理

インタフェースに、ポートの優先順位、パスコスト、リンクタイプ、エッジポートなどの RSTP 属性を設定できます。同じ媒体タイプのポートに異なる優先順位またはパスコストを指定して優先するパスを示したり、リンクタイプを指定してポイントツーポイント接続と共有媒体への接続のどちらであるかを示したり、エッジポートを指定して接続された装置が高速転送をサポートするかどうかを示すことができます。

3.4.6.1 STA の現在のインタフェース設定の表示

コマンド属性

- **Port** — ポートだけに設定できます。トランクまたはトランクポートのメンバーには設定できません。
(アップリンクポート: NETP0 ~ 7, ダウンリンクポート: SNP0 ~ 15)
- **STA Status** — 指定したポートのスパニングツリー上での現在のステータスを表示します。
 - **Discarding** — ポートは STA 設定メッセージを受信していますが、パケットは転送されません。
 - **Learning** — ポートは、Forward Delay パラメタで設定した間隔で設定メッセージを送信し、矛盾する情報は受信していません。ポートアドレステーブルを消去して、アドレスの学習を開始します。
 - **Forwarding** — ポートはパケットを転送して、アドレスの学習を継続しています。
- **Priority** — ポートの STA での優先順位を設定します。スイッチ上のすべてのポートのパスコストが同一である場合は、この優先順位がもっとも高い (値がもっとも小さい) ポートがスパニングツリー内のアクティブなリンクとして設定されます。これによって、STA がネットワークループを検出したときに、優先順位の高いポートがブロックされる可能性を低くします。複数のポートにもっとも高い優先順位が割り当てられている場合は、識別子にもっとも小さい番号が付いているポートが使用可能になります。
- **Path Cost** — STA は、このパラメタを使用して装置間の最適なパスを決定します。そのため、速い媒体に接続するポートには小さい値を、遅い媒体に接続するポートには大きい値を割り当てます。Path Cost は、Priority より優先されます。
- **Designated Cost** — パケットがこのポートから現在のスパニングツリー設定のルートに達するまでのコストです。媒体の伝送速度が遅いほど、コストは高くなります。
- **Designated Bridge** — このポートがスパニングツリーのルートと通信を行うときに経由する装置の優先順位および MAC アドレスです。
- **Designated Port** — このスイッチがスパニングツリーのルートと通信を行うときに経由するブリッジ装置のポートの優先順位および番号です。

- **Link Type (Admin Link type*)** – このインタフェースに接続するリンクのタイプです。
 - **Point-to-Point** – 1 台のブリッジだけに接続されています。
 - **Shared** – 複数のブリッジに接続されています。
 - **Auto** – スイッチによって、ポイントツーポイントリンクと共有媒体のどちらに接続されているかを自動的に検出します。
- **Edge Port (Admin Edge Port*)** – インタフェースが、ブリッジ接続された LAN の境界にある LAN セグメントまたはエンドノードに接続している場合には、このオプションを使用可能に設定できます。エンドノードが転送ループを発生させることはないため、すぐスパンニングツリーの転送状態になります。エッジポートを指定すると、ワークステーション、サーバーなどの装置をすばやく収束 (コンバージェンス) し、現在の転送処理が使用しているデータベースを保持することで再構成時のアドレステーブル再作成に必要なフレームフラッディングの量を削減します。また、インタフェースの状態が変わってもスパンニングツリーが再構成を開始しなくなります。STA 関連のタイムアウト問題にも対処できます。ただし、エッジポートは、エッジノード装置に接続されたポートでのみ使用可能にしてください。

* CLI ではこの用語で表示されます。

次のパラメータは、CLI だけに表示されます。

- **Admin status** – インタフェースで STA が使用可能であるかどうかを表示します。
- **Role** – ポートが、ブリッジをルートブリッジに接続するアクティブトポロジの一部か (ルートポート)、ブリッジを介して LAN をルートブリッジに接続しているか (指定ポート)、あるいはほかのブリッジまたはブリッジポート、LAN に障害が発生するか取り外された場合に接続を引き継ぐ代替ポートまたはバックアップポートになっているかに応じて、ポートに役割を割り当てます。スパンニングツリー内でポートに役割が割り当てられていない場合は使用不可が設定されます (無効ポート)。
- **Designated root** – スイッチがルート装置として受け入れたスパンニングツリー内の装置の優先順位および MAC アドレスです。
- **Forward transitions** – このポートが学習状態から転送状態に切り替わった回数です。
- **Oper edge port** – このパラメータは「Admin Edge Port」の設定 (真または偽) に初期化されますが、BPDU を受信すると、設定は偽になります。
- **Oper Link type** – インタフェースに接続する LAN セグメントの、動作時の二地点間の状態です。このパラメータは、「Admin Link Type」で説明したように、手動または自動で設定できます。

Web – 「Up Links」 / 「Down Links」 => 「Spanning Tree」 => 「Spanning Tree Protocol」 をクリックします。

Port	STA Status	Priority	Path Cost	Designated Cost	Designated Bridge	Designated Port	Link Type	Edge Port Status
<input type="checkbox"/> NETP0	Forwarding	128	100000	0	32768.0.0000E8666672	128.17	Point-to-Point	Disabled
<input type="checkbox"/> NETP1	Broken	128	10000	0	32768.0.0000E8666672	128.18	Point-to-Point	Disabled
<input type="checkbox"/> NETP2	Broken	128	10000	0	32768.0.0000E8666672	128.19	Point-to-Point	Disabled
<input type="checkbox"/> NETP3	Broken	128	10000	0	32768.0.0000E8666672	128.20	Point-to-Point	Disabled

CLI – 次に、ポート NETP4 の STA 属性の例を示します。

```

Console#show spanning-tree ethernet NETP4                                     4-105
SNP0 information
-----
Admin status           : enable
Role                   : designate
State                  : forwarding
Path cost              : 10000
Priority                : 128
Designated cost       : 10000
Designated port       : 128.1
Designated root       : 32768.00209C23C267
Designated bridge     : 32768.0000E8666672
Forward transitions   : 0
Admin edge port       : disable
Oper edge port        : disable
Admin Link type       : point-to-point
Oper Link type        : point-to-point
Console#

```

SNMP – 対応する MIB 変数

フィールド名	MIB 変数	アクセス	値の範囲	デフォルト値
Port	sun...xstMgt. mstInstancePortTable. mstInstancePortEntry	インデックス	整数 (1 ~ 25)	
STA Port State	sun...xstMgt. mstInstancePortTable. mstInstancePortEntry. mstInstancePortState	読み取り専用	discarding (1)、 learning (2)、 forwarding (3)	
STA Port Priority	sun...xstMgt. mstInstancePortTable. mstInstancePortEntry. mstInstancePortPriority	読み取り / 書き込み	整数 (0 ~ 240)	128
STA Port Path Cost	sun...xstMgt. mstInstancePortTable. mstInstancePortEntry. mstInstancePortPathCost	読み取り / 書き込み	整数 (long : 1 ~ 200,000,000、 short : 1 ~ 65,535)	3-106 ページを 参照
STA Port Designated Cost	sun...xstMgt. mstInstancePortTable. mstInstancePortEntry. mstInstancePort- DesignatedCost	読み取り専用	整数	
STA Port Designated Bridge	sun...xstMgt. mstInstancePortTable. mstInstancePortEntry. mstInstancePort- DesignatedBridge	読み取り専用	オクテット文字列	
STA Port Designated Port	sun...xstMgt. mstInstancePortTable. mstInstancePortEntry. mstInstancePort- DesignatedPort	読み取り専用	オクテット文字列	
STA Port Admin Point to Point	sun...staMgt. staPortTable. staPortEntry. staPortAdminPointTo- Point	読み取り / 書き込み	forceTrue (0) forceFalse (1) auto (2)	auto
STA Port Admin Edge Port	sun...staMgt. staPortTable. staPortEntry. staPortAdminEdgePort	読み取り / 書き込み	true (1)、 false (2)	false

フィールド名	MIB 変数	アクセス	値の範囲	デフォルト値
STA Port Enable (管理ステータス)	sun...mstMgt. mstInstancePortTable. mstInstancePortEntry. mstInstancePortEnable	読み取り/ 書き込み	enabled (1)、 disabled (2)	enabled
STA Port Role	sun...mstMgt. mstInstancePortTable. mstInstancePortEntry. mstInstancePortPortRole	読み取り専用	disabled (1)、 root (2)、 designated (3)、 alternate (4)、 backup (5)	
STA Port Designated Root	sun...mstMgt. mstInstancePortTable. mstInstancePortEntry. mstInstancePort- DesignatedRoot	読み取り専用	オクテット文字列	
STA Port Forward Transitions	sun...mstMgt. mstInstancePortTable. mstInstancePortEntry. mstInstancePort- ForwardTransitions	読み取り専用	カウンタ	

3.4.6.2 インタフェースの STA の設定

ここで説明する設定は、スイッチの設定が強制 STP 互換モード (3-57 ページ) および RSTP になっている場合に有効になります。

コマンド属性

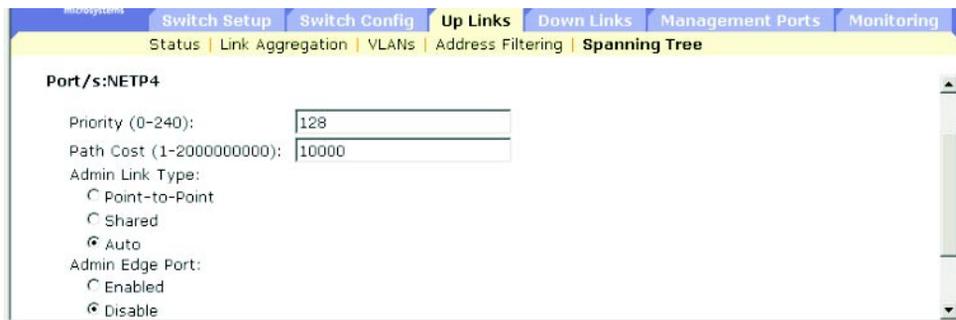
- **Priority** — ポートの STA での優先順位を設定します。スイッチ上のすべてのポートのパスコストが同一である場合は、この優先順位がもっとも高い (値がもっとも小さい) ポートがスパニングツリー内のアクティブリンクとして設定されます。これによって、STA がネットワークループを検出したときに、優先順位の高いポートがブロックされる可能性を低くします。複数のポートにもっとも高い優先順位が割り当てられている場合は、識別子にもっとも小さい番号が付いているポートが使用可能になります。
 - デフォルト : 128
 - 範囲 : 0 ~ 240、16 ずつ増分
- **Path Cost** — STA は、このパラメータを使用して装置間の最適なパスを決定します。そのため、速い媒体に接続するポートには小さい値を、遅い媒体に接続するポートには大きい値を割り当てます。Path Cost は、Priority より優先されます。
 - 範囲 —
 - Ethernet : 200,000 ~ 20,000,000
 - Fast Ethernet : 20,000 ~ 2,000,000
 - Gigabit Ethernet : 2,000 ~ 200,000

- デフォルト –
 - Ethernet – 半二重 : 2,000,000、全二重 : 1,000,000、トランク : 500,000
 - Fast Ethernet – 半二重 : 200,000、全二重 : 100,000、トランク : 50,000
 - Gigabit Ethernet – 全二重 : 10,000、トランク : 5,000

注 – Path Cost Method に short を設定している場合 (3-63 ページ)、パスコストの最大値は 65,535 になります。

- **Admin Link Type** – インタフェースに接続するリンクのタイプです (デフォルト : Auto)。
 - Point-to-Point – 1 台のブリッジだけに接続されています。
 - Shared – 複数のブリッジに接続されています。
 - Auto – スイッチによって、ポイントツーポイントリンクと共有媒体のどちらに接続されているかを自動的に検出します。
- **Admin Edge Port** – インタフェースが、ブリッジ接続された LAN の境界にある LAN セグメントまたはエンドノードに接続している場合には、このオプションを使用可能に設定できます。エンドノードは、転送ループを発生させることがないため、すぐスパンニングツリーの転送状態になります。エッジポートを指定すると、ワークステーション、サーバーなどの装置をすばやく収束 (コンバージェンス) し、現在の転送用のデータベースを保持することで再構成時のアドレステーブル再作成に必要なフレームフラッディングの量を削減します。また、インタフェースの状態が変わってもスパンニングツリーが再構成を開始しなくなります。STA 関連のタイムアウト問題にも対処できます。ただし、エッジポートは、エッジノード装置に接続されたポートでのみ使用可能にしてください (デフォルト : NETP0 ~ 7 : 使用不可、SNP0 ~ 15 : 使用可能に固定)。

Web – 「Up Links」 / 「Down Links」 => 「Spanning Tree」 => 「Spanning Tree Protocol」をクリックします。STP (IEEE 802.1D) のインタフェース設定を行うには、必要なインタフェースのチェックボックスをオンにして「Configure」をクリックします。必要な属性を変更して「Save」をクリックします。



CLI - 次に、ポート NETP5 の STP 属性を設定する例を示します。

```

Console(config)# interface ethernet NETP5                4-75
Console(config-if)#spanning-tree port-priority 128      4-102
Console(config-if)#spanning-tree cost 19                4-101
Console(config-if)#spanning-tree link-type auto         4-104
Console(config-if)#no spanning-tree edge-port          4-103

```

SNMP - 対応する MIB 変数

フィールド名	MIB 変数	アクセス 値の範囲	デフォルト値
STA Port Priority	sun...mstMgt. mstInstancePortTable. mstInstancePortEntry. mstInstancePortPriority	読み取り / 整数 (0 ~ 240) 書き込み	128
STA Port Path Cost	sun...mstMgt. mstInstancePortTable. mstInstancePortEntry. mstInstancePortPathCost	読み取り / 整数 書き込み (long : 1 ~ 200,000,000、 short : 1 ~ 65,535)	3-106 ページ を参照
STA Port Admin Link Type	sun...staMgt. staPortTable. staPortEntry. staPortAdmin- PointToPoint	読み取り / forceTrue (0)、 書き込み forceFalse (1)、 auto (2)	auto
STA Port Admin Edge Port	sun...staMgt. staPortTable. staPortEntry. staPortAdminEdgePort	読み取り / true (1)、 書き込み false (2)	false

3.4.6.3

インタフェースの STA プロトコルステータスの確認

スイッチは、構成情報 (Configuration) BPDU、トポロジ変更通知 (Topology Change Notification) BPDU などの STP BPDU を検出すると、選択されたインタフェースを強制 STP 互換モードに設定します。また、「Protocol Migration」ボタンを使用して、そのインタフェースでの送信に適した BPDU の形式 (RSTP または STP 互換形式) を手動で再確認することもできます。

Web - 「Up Links」 / 「Down Links」 => 「Spanning Tree」 => 「Spanning Tree Protocol」 をクリックします。必要なインタフェースを選択して 「Protocol Migration」 ボタンをクリックします。



Port	STA Status	Priority	Path Cost	Designated Cost	Designated Bridge	Designated Port	Link Type	Edge Port Status
<input checked="" type="checkbox"/> NETP4	Broken	128	10000	0	32768.0.0000E8666672	128.21	Point-to-Point	Disabled

CLI - 次に、protocol migration コマンドを使用して、このインタフェースに送信されるスパニングツリーメッセージのタイプ (RSTP または STP 互換) を検証する例を示します。

```
Console(config)interface ethernet NETP4
Console(config-if)#spanning-tree protocol-migration      4-104
Console(config-if)#
```

SNMP - 対応する MIB 変数

フィールド名	MIB 変数	アクセス	値の範囲	デフォルト値
STA Port Protocol Migration	sun...staMgt. staPortTable. staPortEntry. staPortProtocolMigration	読み取り / 書き込み	true (1)、 false (2)	true

3.4.7 管理ポートのトラフィックのフィルタリング

特定の IP トラフィックがダウンリンクポートから内部管理ポート (NETMGT) に到達することを防ぐために、パケットフィルタリングを設定できます。なお、アップリンクポートから管理ポートへのトラフィックの送信は許可されていません。

コマンドの使用法

- デフォルトでは、内部管理ポート (NETMGT) とダウンリンクポートとの間の通過を許可された IP パケットはありません。管理ポートを介してサーバーブレードにアクセスする必要がある場合は、管理ポートとダウンリンクポート間で特定のパケットの通過を許可するようにフィルタを設定します。
- デフォルトでは、ダウンリンクポートから管理ポート (NETMGT) への通過を許可された IP パケットはありません。サーバーブレードから管理ポート (NETMGT) を介して管理ネットワークにアクセスする必要がある場合は、ダウンリンクポートから管理ポートへの特定のフレームの送信を許可するようにフィルタを設定します。

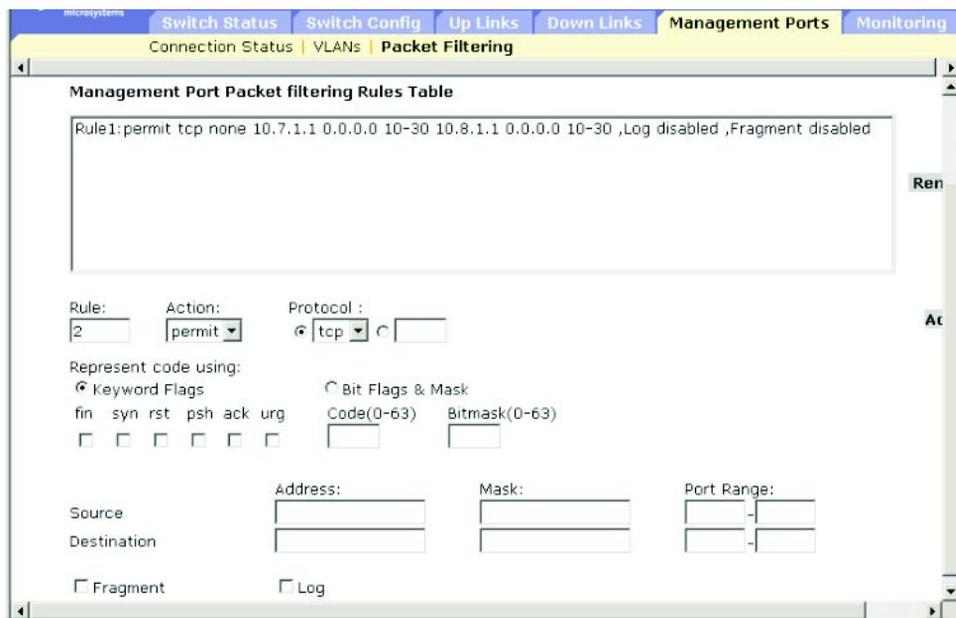
注 — アップリンクポートと管理ポートの間のトラフィックは許可されません。

コマンド属性

- **Rule** — リストの指定した位置にフィルタルールを挿入し、その位置以降に既存のフィルタルールがあれば下に移動させます。ルール番号に、リスト内で次に使用できる番号より大きい数字を指定することはできません。ルール番号を指定しないと、新しい内容は、ルールリストの終わりに追加されます (範囲: 1 ~ 128)。
- **Action** — ダウンリンクポートから管理ポートへのパケットの送信をブロックまたは許可します。(オプション: `permit`、`deny`)
- **Protocol** — プロトコル (TCP、UDP、Any) またはプロトコル番号 (0 ~ 255) を選択します。
- **Keyword Flags** (コードシーケンス) — TCP ヘッダーの 14 バイト目のフラグを指定します。これによって、コードシーケンスを指定できるようになります (選択する場合は ON、選択しない場合は OFF)。記号名およびそれに対応するビットは、次のとおりです。
 - `fin` (1) — 完了
 - `syn` (2) — 同期
 - `rst` (4) — リセット
 - `psh` (8) — プッシュ
 - `ack` (16) — 承認
 - `urg` (32) — 緊急ポインタ
- **Code** — TCP ヘッダーの 14 バイト目のフラグビットを、ビット文字列を表す 10 進数で指定します (範囲: 0 ~ 63)。
- **Bitmask** — コードに適用するビットマスクを表す 10 進数です。有効にするビットには 2 進数のビット「1」を、無視するビットには「0」を設定して、それと等価の 10 進数を入力します。次の各ビットを指定できます。
32 (urg)、16 (ack)、8 (psh)、4 (rst)、2 (syn)、1 (fin)

- **Source** – フレームの TCP/UDP 送信元アドレスおよびネットマスク、ポートの範囲です (ポートの範囲 : 0 ~ 65535)。
- **Destination** – フレームの TCP/UDP 送信先アドレスおよびネットマスク、ポートの範囲です (ポートの範囲 : 0 ~ 65535)。
- **Fragment** – ルールは、More Fragments (MF) ビットが設定されているパケットまたはフラグメントオフセットが 0 より大きいパケットだけに適用されます。フラグメントを設定しない場合は、フラグメントパケットとフラグメントなしのパケットの両方に適用されます。
- **Log** – 一致したパケットをログバッファに記録します。ログバッファに格納できるエントリの最大数は 64 です。バッファがいっぱいになると、先頭に戻ってもっとも古いエントリが上書きされます。ログは RAM に格納されているため、スイッチをリセットすると消去されます。

Web – 「Management Port」 => 「Packet Filtering」をクリックします。必要なルールを入力して「Add」をクリックします。この例のルールは、TCP ポート 10 ~ 30 を使用する、送信元アドレス 10.7.1.1 から送信先アドレス 10.8.1.1 に送信される TCP トラフィックを許可しています。



CLI – 次に、すべてのパケットがフィルタを通過するように、すべてのプロトコルタイプを許可し、送信元アドレスと送信先アドレスの両方に空のアドレスおよびネットワークマスクを使用する例を示します。この例の詳細なリストについては、4-70 ページの「ip filter」を参照してください。

```
Console(config)#ip filter permit any 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 4-70
Console(config)#
```

SNMP – 対応する MIB 変数

フィールド名	MIB 変数	アクセス	値の範囲	デフォルト値
Index	sun... securityMgt. packetFilterUnitMgt. pfuRuleTable. pfuRuleEntry. pfuRuleIndex	アクセスなし	整数 (1 ~ 128)	
Action	sun... securityMgt. packetFilterUnitMgt. pfuRuleTable. pfuRuleEntry. pfuRuleAction	読み取り / 作成	permit (1)、 deny (2)	
Protocol	sun... securityMgt. packetFilterUnitMgt. pfuRuleTable. pfuRuleEntry. pfuRuleProtocol	読み取り / 作成	整数 (0 ~ 256、 256 は任意のプロトコ ルを示す)	
Source IP Address & Bitmask	sun... securityMgt. packetFilterUnitMgt. pfuRuleTable. pfuRuleEntry. pfuRuleSrcIpAddr & pfuRuleSrcIpBitmask	読み取り / 作成	IP アドレス	
Source IP Port Range	sun... securityMgt. packetFilterUnitMgt. pfuRuleTable. pfuRuleEntry. pfuRuleSrcPortRange1 & pfuRuleSrcPortRange2	読み取り / 作成	整数 (1 ~ 65536)	
Destination IP Address & Bitmask	sun... securityMgt. packetFilterUnitMgt. pfuRuleTable. pfuRuleEntry. pfuRuleDstIpAddr & pfuRuleDstIpBitmask	読み取り / 作成	IP アドレス	

フィールド名	MIB 変数	アクセス	値の範囲	デフォルト値
Destination IP Port Range	sun... securityMgt. packetFilterUnitMgt. pfuRuleTable. pfuRuleEntry. pfuRuleDstPortRange1 & pfuRuleDstPortRange2	読み取り / 作成	整数 (1 ~ 65536)	
TCP Code	sun... securityMgt. packetFilterUnitMgt. pfuRuleTable. pfuRuleEntry. pfuRuleTcpCode	読み取り / 作成	整数 (0 ~ 63)	
TCP Code Bitmask	sun... securityMgt. packetFilterUnitMgt. pfuRuleTable. pfuRuleEntry. pfuRuleTcpCodeBitmask	読み取り / 作成	整数 (0 ~ 63)	
Fragments	sun... securityMgt. packetFilterUnitMgt. pfuRuleTable. pfuRuleEntry. pfuRuleFragments	読み取り / 作成	enabled (1)、 disabled (2)	disabled
Log	sun... securityMgt. packetFilterUnitMgt. pfuRuleTable. pfuRuleEntry. pfuRuleLog	読み取り / 作成	enabled (1)、 disabled (2)	disabled

3.5 ポートおよび管理トラフィックの監視

この節では、分析用にトラフィックを監視ポートにミラー化する機能、ポートの詳細なネットワーク統計情報を表示する機能、管理ポートを通過する SNMP トラフィックの主な統計情報を表示する機能などの、スイッチを監視するための機能について説明します。

注 – Sun Fire B1600 ブレードシステムシャーシの統合スイッチは、相互に接続する 2 つのスイッチチップで構成されています。あるポートのトラフィックは、同じスイッチチップ上の別のポートだけにミラー化できます。ポート NETP0 および NETP1、NETP4、NETP5、SNP8 ~ 15 は、一方のスイッチチップ上にあります。ポート NETP2 および NETP3、NETP6、NETP7、SNP0 ~ 7 は、もう一方のスイッチチップ上にあります (SSC の背面パネルの右側にあるすべてのポートが一方のチップ上に、左側にあるすべてのポートがもう一方のチップ上にあります)。

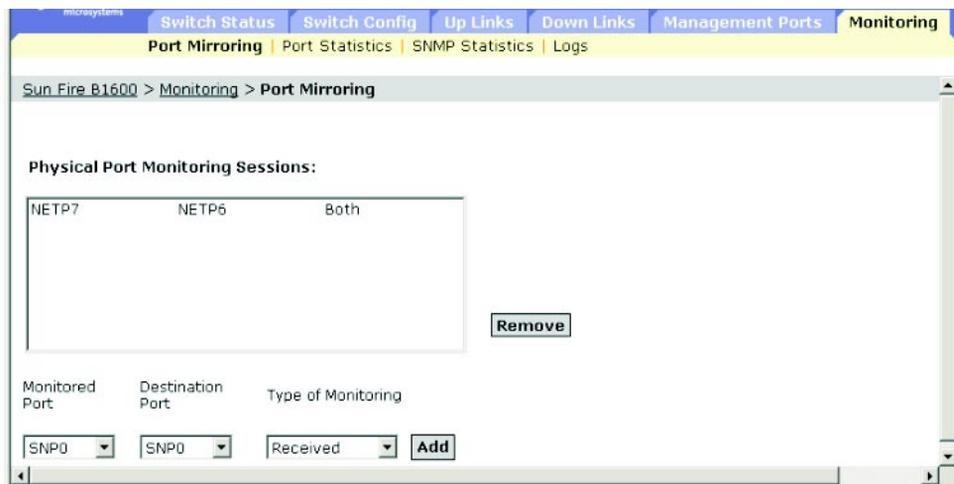
3.5.1 ポートのミラー化の設定

リアルタイム分析を行うために、ソースポートのトラフィックをターゲットポートにミラー化できます。ミラー化したターゲットポートにロジックアナライザまたは RMON プロンプを設置すると、運用に影響を与えることなく、ソースポートを通過するトラフィックを調査できます。

コマンドの使用法

- 監視ポートの速度は、ソースポートの速度と同じか、それ以上である必要があります。そうでない場合は、監視ポートからトラフィックが失われることがあります。
- ポートのトラフィックをミラー化するときには、ターゲットポートをソースポートと同じ VLAN に含める必要があります。

Web – 「Monitoring」 => 「Port Mirror」を開きます。ソースポートおよびミラー化するトラフィックのタイプ、監視ポートを指定して「Add」をクリックします。



CLI - interface コマンドを使用して監視ポートを選択し、port monitor コマンドを使用してソースポートを指定します。CLI では、デフォルトで受信パケットと送信パケットの両方のミラー化が設定されています。

```

Console(config)#interface ethernet NETP7                                4-75
Console(config-if)#port monitor ethernet NETP6                          4-146
Console(config-if)#

```

SNMP - 対応する MIB 変数

フィールド名	MIB 変数	アクセス	値の範囲	デフォルト値
Mirror Source Port	sun... mirrorMgt. mirrorTable.mirrorEntry. mirrorSourcePort	アクセス不可	整数	
Mirror Destination Port	sun... mirrorMgt. mirrorTable.mirrorEntry. mirrorDestinationPort	アクセス不可	整数	
Mirror Type	sun... mirrorMgt. mirrorTable.mirrorEntry. mirrorType	読み取り / 作成	rx (1)、 tx (2)、 both (3)	both
Mirror Status	sun... mirrorMgt. mirrorTable.mirrorEntry. mirrorStatus	読み取り / 作成	valid (1)、 invalid (2)	

3.5.2 ポートの統計情報の表示

Interfaces グループおよび **Ethernetlike MIB** のネットワークトラフィックに関する標準の統計情報と、**RMON MIB** に基づくトラフィックの詳細情報を表示できます。

Interfaces および **Ethernetlike** 統計情報には、各ポートを通過するトラフィックのエラーが表示されます。この情報は、ポートの障害や過負荷などの、スイッチの潜在的な問題を識別するために使用できます。**RMON** 統計情報は、各ポートを通過するサイズやタイプが異なるフレームの総数などの、さまざまな統計情報を提供します。表示されるすべての値は、システムの再起動後の累積値で、1 秒ごとの件数として表示されます。デフォルトでは、統計情報は 20 秒ごとに再表示されます。

注 – **RMON** グループ 2 および 3、9 には、**SNMP** を使用した場合にのみアクセスできます。

コマンド属性

パラメタ	説明
インタフェース統計情報	
Received Octets	フレーミング文字を含む、インタフェースが受信したオクテットの総数です。
Received Unicast Packets	上位レイヤープロトコルに配信された、サブネットワークのユニキャストパケットの数です。
Received Multicast Packets	上位 (サブ) レイヤーに配信された、このサブレイヤーでマルチキャストアドレスが指定されたパケットの数です。
Received Broadcast Packets	上位 (サブ) レイヤーに配信された、このサブレイヤーでブロードキャストアドレスが指定されたパケットの数です。
Received Discarded Packets	エラーは検出されなかったが、上位レイヤーのプロトコルに配信しないように破棄された受信パケットの数です。バッファ領域を空けるなどの理由で、パケットが破棄されることがあります。
Received Unknown Packets	未知または未サポートのプロトコルであるために破棄された、このインタフェースの受信パケットの数です。
Received Errors	上位レイヤーのプロトコルに配信できないエラーを含む受信パケットの数です。
Transmit Octets	フレーミング文字を含む、インタフェースから送信されたオクテットの総数です。
Transmit Unicast Packets	上位プロトコルによって、サブネットワークのユニキャストアドレスへの送信が要求されたパケットの総数です。破棄されたパケットや送信されなかったパケットも含む数です。
Transmit Multicast Packets	上位プロトコルによって送信が要求された、このサブレイヤーでマルチキャストアドレスが指定されたパケットの総数です。破棄されたパケットや送信されなかったパケットも含む数です。
Transmit Broadcast Packets	上位プロトコルによって送信が要求された、このサブレイヤーでブロードキャストアドレスが指定されたパケットの総数です。破棄されたパケットや送信されなかったパケットも含む数です。
Transmit Discarded Packets	エラーは検出されなかったが、送信しないように破棄された送信パケットの数です。バッファ領域を空けるなどの理由で、パケットが破棄されることがあります。
Transmit Errors	エラーのために送信されなかった送信パケットの数です。

パラメタ	説明
Etherlike 統計情報	
Alignment Errors	アライメントエラー (同期を失ったデータパケット) の数です。
Late Collisions	パケットの送信で 512 ビット以上送信したあとに衝突が検出された回数です。
FCS Errors	インタフェースが受信した、フレーム長はオクテット整数だが FCS チェックをパスしなかったフレームの数です。フレームが長すぎるまたは短かすぎるエラーを含まない数です。
Excessive Collisions	過度の衝突によってインタフェースでの送信に失敗したフレームの数です。インタフェースが全二重モードで動作しているときには、この値はカウントされません。
Single Collision Frames	衝突によって 1 回だけ送信が妨げられた、正常に転送されたフレームの数です。
Internal MAC Transmit Errors	内部 MAC サブレイヤーの送信エラーによってインタフェースでの送信に失敗したフレームの数です。
Multiple Collision Frames	衝突によって複数回の送信が妨げられた、正常に転送されたフレームの数です。
Carrier Sense Errors	フレームを送信しようとしたときにキャリアセンスが失われたか、アサートされなかった回数です。
SQE Test Errors	インタフェースで、PLS サブレイヤーによって SQE TEST ERROR メッセージが生成された回数です。
Frames Too Long	インタフェースが受信した、許容される最大フレームサイズを超えたフレームの数です。
Deferred Transmissions	媒体がビジー状態であったため、インタフェースでの最初の転送で遅延が発生したフレームの数です。
Internal MAC Receive Errors	内部 MAC サブレイヤーの受信エラーにより、インタフェースでの受信が失敗したフレームの数です。
RMON 統計情報	
Drop Events	リソース不足により、パケットを損失した総数です。
Jabbers	受信したフレームのうち、(フレーミングビットは含まず、FCS オクテットを含む) 長さが 1518 オクテットを超え、FCS エラーまたはアライメントエラーがあるフレームの総数です。
Received Bytes	ネットワークで受信したデータの総バイト数です。この統計情報は、Ethernet 利用率の適切な指針として使用できます。
Collisions	この Ethernet セグメントでの衝突総数の最善の見積もり値です。

パラメタ	説明
Received Frames	受信したフレーム (エラーデータおよびブロードキャスト、マルチキャスト) の総数です。
Broadcast Frames	送信先がブロードキャストアドレスになっている、正常な受信フレームの総数です。マルチキャストパケットは含まない数です。
Multicast Frames	送信先がマルチキャストアドレスになっている、正常な受信フレームの総数です。
CRC/Alignment Errors	CRC/アライメントエラー (FCS またはアライメントエラー) の数です。
Undersize Frames	受信フレームのうち、(フレーミングビットは含まず、FCS オクテットを含む) 長さが 64 オクテットに満たない、それ以外の形式には問題のないフレームの総数です。
Oversize Frames	受信フレームのうち、(フレーミングビットは含まず、FCS オクテットを含む) 長さが 1518 オクテットを超える、それ以外の形式には問題のないフレームの総数です。
Fragments	受信フレームのうち、(フレーミングビットは含まず、FCS オクテットを含む) 長さが 64 オクテットに満たない、FCS またはアライメントエラーがあるフレームの総数です。
64 Bytes Frames	(フレーミングビットは含まず、FCS オクテットを含む) 長さが 64 オクテットの送受信フレーム (エラーパケットを含む) の総数です。
65-127 Byte Frames	(フレーミングビットは含まず、FCS オクテットを含む) オクテット数が規定の範囲内である送受信フレーム (エラーパケットを含む) の総数です。
128-255 Byte Frames	
256-511 Byte Frames	
512-1023 Byte Frames	
1024-1518 Byte Frames	
1519-1536 Byte Frames	

Web – 「Monitoring」 => 「Statistics」 をクリックします。必要なインタフェースを選択して「Select」 をクリックします。また、ページの下部にある「Refresh」 ボタンを使用して画面を更新することもできます。

The screenshot shows the web management interface for a Sun Fire B1600 system. The top navigation bar includes tabs for 'Switch Status', 'Switch Config', 'Up Links', 'Down Links', 'Management Ports', and 'Monitoring'. Under 'Monitoring', there are sub-links for 'Port Mirroring', 'Port Statistics', 'SNMP Statistics', and 'Logs'. The breadcrumb path is 'Sun Fire B1600 > Monitoring > Port Statistics'. A dropdown menu for 'Physical Port:' is set to 'NETPO'. Below this, there are two tables: 'Interface Statistics' and 'Etherlike Statistics'.

Port Statistics:

Physical Port: NETPO

Interface Statistics:

Property	
Received Octets:	232957
Received Unicast Packets:	110
Received Multicast Packets:	2671
Received Broadcast Packets:	28
Received Discarded Packets:	0
Received Unknown Packets:	0
Received Errors:	0
Transmit Octets:	173628
Transmit Unicast Packets:	0
Transmit Multicast Packets:	2706
Transmit Broadcast Packets:	0
Transmit Discarded Packets:	0
Transmit Errors:	0

Etherlike Statistics

Property	
Alignment Errors:	0
Late Collisions:	0
FCS Errors:	0
Excessive Collisions:	0
Single Collision Frames:	0
Internal MAC Transmit Errors:	0
Multiple Collision Frames:	0
Carrier Sense Errors:	0
SQE Test Errors:	0
Frames Too Long:	0
Deferred Transmissions:	0
Internal MAC Receive Errors:	0

RMON Statistics	
Property	
Drop Events:	0
Jabbers:	0
Received Bytes:	438662
Collisions:	0
Received Frames:	0
64 Bytes Frames:	5859
Broadcast Frames:	29
65-127 Bytes Frames:	97
Multicast Frames:	5869
128-255 Bytes Frames:	14
CRC/Alignment Errors:	0
256-511 Bytes Frames:	0
Undersize Frames:	0
512-1023 Bytes Frames:	2
Oversize Frames:	0
1024-1518 Bytes Frames:	40
Fragments:	0

CLI ー 次に、ポート SNP13 の統計情報の例を示します。

```

Console#show interfaces counters ethernet SNP13
Ethernet 13
Iftable stats:
  Octets input: 868453, Octets output: 3492122
  Unicast input: 7315, Unicast output: 6658
  Discard input: 0, Discard output: 0
  Error input: 0, Error output: 0
  Unknown protos input: 0, QLen output: 0
Extended iftable stats:
  Multi-cast input: 0, Multi-cast output: 17027
  Broadcast input: 231, Broadcast output: 7
Ether-like stats:
  Alignment errors: 0, FCS errors: 0
  Single Collision frames: 0, Multiple collision frames: 0
  SQE Test errors: 0, Deferred transmissions: 0
  Late collisions: 0, Excessive collisions: 0
  Internal mac transmit errors: 0, Internal mac receive errors: 0
  Frame too longs: 0, Carrier sense errors: 0
RMON stats:
  Drop events: 0, Octets: 4422579, Packets: 31552
  Broadcast pkts: 238, Multi-cast pkts: 17033
  Undersize pkts: 0, Oversize pkts: 0
  Fragments: 0, Jabbers: 0
  CRC align errors: 0, Collisions: 0
  Packet size <= 64 octets: 25568, Packet size 65 to 127 octets: 1616
  Packet size 128 to 255 octets: 1249, Packet size 256 to 511 octets: 1449
  Packet size 512 to 1023 octets: 802, Packet size 1024 to 1518 octets: 871
Console#

```

SNMP – 対応する MIB 変数

フィールド名	MIB 変数	アクセス	範囲
インタフェース統計情報			
In Octets	MIB-II. interfaces.ifNumber.ifTable.ifEntry.ifInOctets	読み取り専用	整数
In Unicast Packets	MIB-II. interfaces.ifNumber.ifTable.ifEntry. ifInUcastPkts	読み取り専用	整数
In Multicast Packets	MIB-II. ifMIB.ifMIBObjects.ifXTable.ifXEntry. ifInMulticastPkts	読み取り専用	整数
In Broadcast Packets	MIB-II. ifMIB.ifMIBObjects.ifXTable.ifXEntry. ifInBroadcastPkts	読み取り専用	整数
In Discards	MIB-II. interfaces.ifTable.ifEntry.ifInDiscards	読み取り専用	整数
In Unknown Protocols	MIB-II. interfaces.ifTable.ifEntry.ifInUnknownProtos	読み取り専用	整数
In Errors	MIB-II. interfaces.ifTable.ifEntry.ifInErrors	読み取り専用	整数
Out Octets	MIB-II. interfaces.ifTable.ifEntry.ifOutOctets	読み取り専用	整数
Out Unicast Packets	MIB-II. interfaces.ifTable.ifEntry.ifOutUcastPkts	読み取り専用	整数
Out Multicast Packets	MIB-II. ifMIB.ifMIBObjects.ifXTable.ifXEntry. ifOutMulticastPkts	読み取り専用	整数
Out Broadcast Packets	MIB-II. ifMIB.ifMIBObjects.ifXTable.ifXEntry. ifOutBroadcastPkts	読み取り専用	整数
Out Discards	MIB-II. interfaces.ifTable.ifEntry.ifOutDiscards	読み取り専用	整数
Out Errors	MIB-II. interfaces.ifTable.ifEntry.ifOutErrors	読み取り専用	整数

フィールド名	MIB 変数	アクセス	範囲
Etherlike の統計情報			
Alignment Errors	MIB-II. transmission.dot3StatsTable.dot3StatsEntry. dot3StatsAlignmentErrors	読み取り専用	整数
Late Collisions	MIB-II. transmission.dot3StatsTable.dot3StatsEntry. dot3StatsLateCollisions	読み取り専用	整数
FCS Errors	MIB-II. transmission.dot3StatsTable.dot3StatsEntry. dot3StatsFCSErrors	読み取り専用	整数
Excessive Collisions	MIB-II. transmission.dot3StatsTable.dot3StatsEntry. dot3Stats-ExcessiveCollisions	読み取り専用	整数
Single Collision Frames	MIB-II. transmission.dot3StatsTable.dot3StatsEntry. dot3StatsSingleCollisionFrames	読み取り専用	整数
Internal Mac Transmit Errors	MIB-II. transmission.dot3StatsTable.dot3StatsEntry. dot3StatsInternalMacTransmitErrors	読み取り専用	整数
Multiple Collision Frames	MIB-II. transmission.dot3StatsTable.dot3StatsEntry. dot3StatsMultipleCollisionFrames	読み取り専用	整数
Carrier Sense Errors	MIB-II. transmission.dot3StatsTable.dot3StatsEntry. dot3StatsCarrierSenseErrors	読み取り専用	整数
SQE Test Errors	MIB-II. transmission.dot3StatsTable.dot3StatsEntry. dot3StatsSQETestErrors	読み取り専用	整数
Frames Too Long	MIB-II. transmission.dot3StatsTable.dot3StatsEntry. dot3StatsFrameTooLongs	読み取り専用	整数
Deferred Transmissions	MIB-II. transmission.dot3StatsTable.dot3StatsEntry. dot3StatsDeferredTransmissions	読み取り専用	整数
Internal MAC Receive Errors	MIB-II. transmission.dot3StatsTable.dot3StatsEntry. dot3StatsInternalMacReceiveErrors	読み取り専用	整数

フィールド名	MIB 変数	アクセス	範囲
RMON 統計情報			
Drop Events	MIB-II. rmon.statistics.etherStatsTable.etherStatsEntry .etherStatsDropEvents	読み取り専用	整数
Jabbers	MIB-II. rmon.statistics.etherStatsTable.etherStatsEntry .etherStatsJabbers	読み取り専用	整数
Received Octets	MIB-II. rmon.statistics.etherStatsTable.etherStatsEntry .etherStatsOctets	読み取り専用	整数
Collisions	MIB-II. rmon.statistics.etherStatsTable.etherStatsEntry .etherStatsCollisions	読み取り専用	整数
Received Packets	MIB-II. rmon.statistics.etherStatsTable.etherStatsEntry .etherStatsPkts	読み取り専用	整数
Broadcast Packets	MIB-II. rmon.statistics.etherStatsTable.etherStatsEntry .etherStatsBroadcastPkts	読み取り専用	整数
Multicast Packets	MIB-II. rmon.statistics.etherStatsTable.etherStatsEntry .etherStatsMulticastPkts	読み取り専用	整数
CRC/Alignment Errors	MIB-II. rmon.statistics.etherStatsTable.etherStatsEntry .etherStatsCRCAAlignErrors	読み取り専用	整数
Undersize Packets	MIB-II. rmon.statistics.etherStatsTable.etherStatsEntry .etherStatsUndersizePkts	読み取り専用	整数
Oversize Packets	MIB-II. rmon.statistics.etherStatsTable.etherStatsEntry .etherStatsOversizePkts	読み取り専用	整数
Fragments	MIB-II. rmon.statistics.etherStatsTable.etherStatsEntry .etherStatsFragments	読み取り専用	整数
64 Bytes Frames	MIB-II. rmon.statistics.etherStatsTable.etherStatsEntry .etherStatsPkts64Octets	読み取り専用	整数
X-Y Byte Frames	MIB-II. rmon.statistics.etherStatsTable.etherStatsEntry .etherStatsPktsXtoYOctets	読み取り専用	整数

3.5.3 SNMP 統計情報の表示

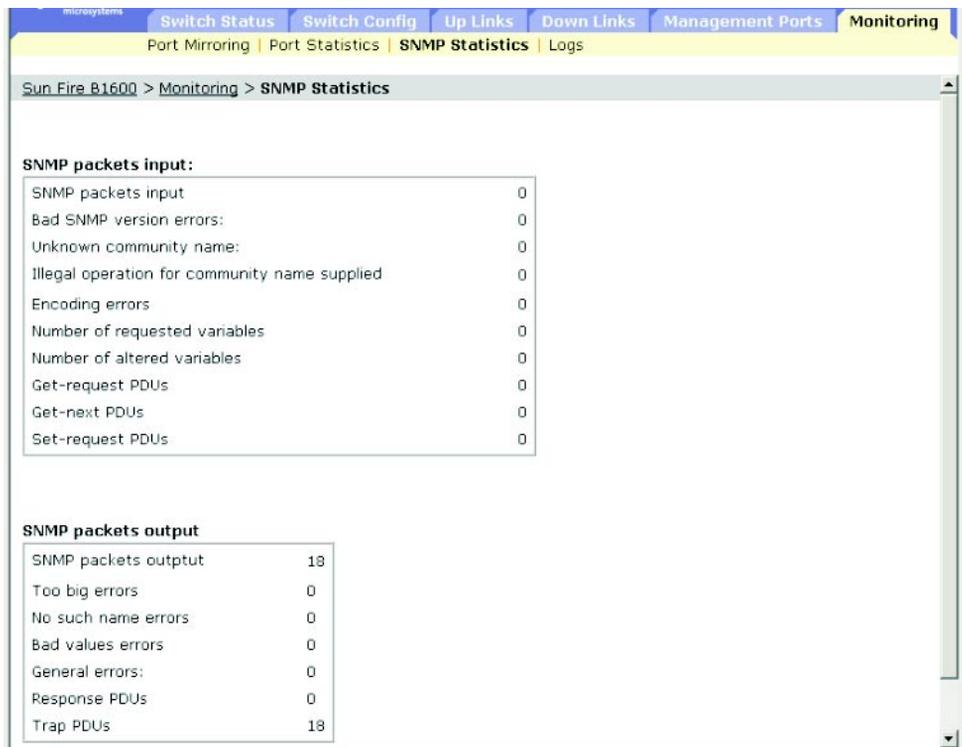
管理ポートを通過する SNMP トラフィックに関する統計情報を表示できます。この情報は、SNMP エラーのデバッグや、スイッチによって処理した SNMP トラフィックの総量および SNMP を介したスイッチへの不正アクセスを表示するために使用できます。

コマンド属性

パラメタ	説明
SNMP パケットの受信	
SNMP packets input	トランスポートサービスから SNMP エンティティに配信されたメッセージの総数です。
Bad SNMP version errors	SNMP プロトコルエンティティに配信された、サポートされていない SNMP バージョンを持つ SNMP メッセージの総数です。
Unknown community name	SNMP プロトコルエンティティに配信された、エンティティにとって未知の SNMP コミュニティ名を持つ SNMP メッセージの総数です。
Illegal operation for community name supplied	SNMP プロトコルエンティティに配信された、メッセージに示された SNMP コミュニティによって許可されていない SNMP 操作を表す SNMP メッセージの総数です。
Encoding errors	受信した SNMP メッセージを復号化したときに SNMP プロトコルエンティティによって検出された ASN.1 または BER エラーの総数です。
Number of requested variables	有効な SNMP Get-Request および Get-Next PDU が受信された結果、SNMP プロトコルエンティティによって正常に取り出された MIB オブジェクトの総数です。
Number of altered variables	有効な SNMP Set-Request PDU が受信された結果、SNMP プロトコルエンティティによって正常に変更された MIB オブジェクトの総数です。
Get-request PDUs	SNMP プロトコルエンティティによって受信および処理された SNMP Get-Request PDU の総数です。
Get-next PDUs	SNMP プロトコルエンティティによって受信および処理された SNMP Get-Next PDU の総数です。
Set-request PDUs	SNMP プロトコルエンティティによって受信および処理された SNMP Set-Request PDU の総数です。

パラメタ	説明
SNMP パケットの送信	
SNMP packets output	SNMP プロトコルエンティティからトランスポートサービスに渡された SNMP メッセージの総数です。
Too big errors	SNMP プロトコルエンティティに配信された、エラーステータスが「tooBig」である SNMP PDU の総数です。
No such name errors	SNMP プロトコルエンティティに配信された、エラーステータスが「noSuchName」である SNMP PDU の総数です。
Bad values errors	SNMP プロトコルエンティティに配信された、エラーステータスが「badValue」である SNMP PDU の総数です。
General errors	SNMP プロトコルエンティティに配信された、エラーステータスが「genErr」である SNMP PDU の総数です。
Response PDUs	SNMP プロトコルエンティティによって生成された、SNMP Get-Response PDU の総数です。
Trap PDUs	SNMP プロトコルエンティティによって生成された、SNMP Trap PDU の総数です。

Web – 「Monitoring」 => 「SNMP Statistics」をクリックします。また、ページの下部にある「Refresh」ボタンを使用して画面を更新することもできます。



CLI – 次に、スイッチの SNMP 統計情報の例を示します。

```
Console#show snmp 4-53

SNMP traps:
  Authentication: enable
  Link-up-down: enable

SNMP communities:
  1. private, and the privilege is read/write
  2. public, and the privilege is read-only

11 SNMP packets input
  0 Bad SNMP version errors
  0 Unknown community name
  8 Illegal operation for community name supplied
  0 Encoding errors
  0 Number of requested variables
  1 Number of altered variables
  0 Get-request PDUs
  0 Get-next PDUs
  3 Set-request PDUs
11 SNMP packets output
  0 Too big errors
  0 No such name errors
  0 Bad values errors
  2 General errors
  3 Response PDUs
  0 Trap PDUs

SNMP logging: disabled
Console#
```

SNMP – 対応する MIB 変数

フィールド名	MIB 変数	アクセス	範囲
SNMP パケットの受信			
In Packets	MIB-II.snmp.snmpInPkts	読み取り専用	整数
In Bad Versions	MIB-II.snmp.snmpInBadVersions	読み取り専用	整数
In Bad Community Names	MIB-II.snmp.snmpInBadCommunityNames	読み取り専用	整数
In Bad Community Uses	MIB-II.snmp.snmpInBadCommunityUses	読み取り専用	整数
In ASN Parse Errors	MIB-II.snmp.snmpInASNParseErrs	読み取り専用	整数

フィールド名	MIB 変数	アクセス	範囲
In Total Request Variables	MIB-II.snmp.snmpInTotalReqVars	読み取り専用	整数
In Total Set Variables	MIB-II.snmp.snmpInTotalSetVars	読み取り専用	整数
In Get Requests	MIB-II.snmp.snmpInGetRequests	読み取り専用	整数
In Get Nexts	MIB-II.snmp.snmpInGetNexts	読み取り専用	整数
In Set Requests	MIB-II.snmp.snmpInSetRequests	読み取り専用	整数
Silent Drops	MIB-II.snmp.snmpSilentDrops	読み取り専用	整数
Proxy Drops	MIB-II.snmp.snmpProxyDrops	読み取り専用	整数
SNMP パケットの送信			
Out Packets	MIB-II.snmp.snmpOutPkts	読み取り専用	整数
Out Too Bigs	MIB-II.snmp.snmpOutTooBigs	読み取り専用	整数
Out No Such Names	MIB-II.snmp.snmpOutNoSuchNames	読み取り専用	整数
Out Bad Values	MIB-II.snmp.snmpOutBadValues	読み取り専用	整数
Out General Errors	MIB-II.snmp.snmpOutGenErrs	読み取り専用	整数
Out Get Responses	MIB-II.snmp.snmpOutGetResponses	読み取り専用	整数
Out Traps	MIB-II.snmp.snmpOutTraps	読み取り専用	整数

3.5.4 メッセージログの設定

スイッチのメモリーに保存するシステムログメッセージを、重要度に応じて制限できます。

コマンド属性

- **Enable Logging** – デバッグメッセージまたはエラーメッセージのスイッチメモリーへのロギングを使用可能にします (デフォルト: 使用不可)。
- **Logging Level** – スイッチメモリーに保存されるシステムログメッセージを、重要度に応じて制限します。選択したレベルからレベル 0 までのメッセージが保存されます (範囲: 7 ~ 0、デフォルト – Flash: 3 ~ 0、RAM: 7 ~ 0)。

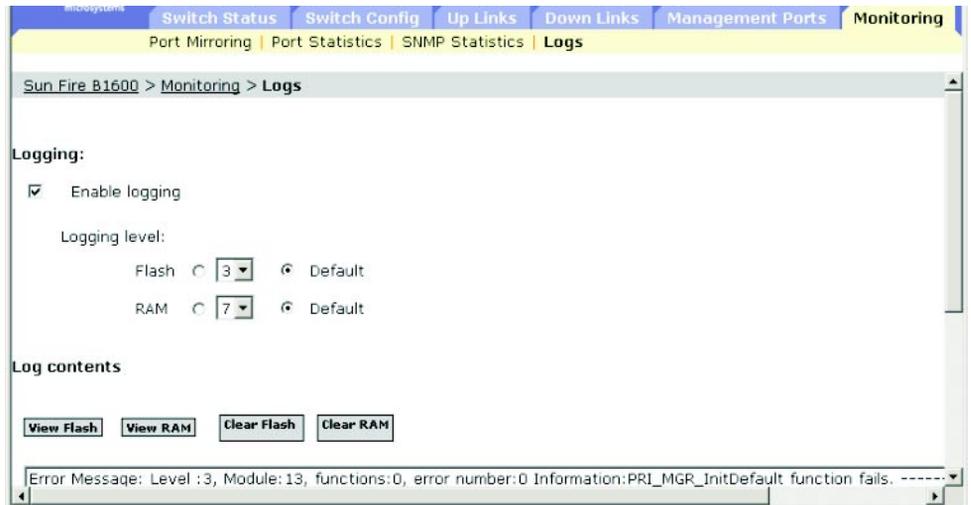
表 3-1 エラーレベル

レベル引数	レベル	説明
debugging	7	デバッグ用メッセージ
informational	6	情報メッセージのみ (すべてのトラップ)
notifications	5	コールドスタートなどの、正常だが通知が必要な状態
warnings	4	警告 (false が返された、予期せぬ結果が返されたなど)
errors	3	エラー (無効な入力が行われた、デフォルトが使用されたなど)
critical	2	重大な問題 (記憶域割り当てエラー、リソース不足による空きメモリーエラーなど)
alerts	1*	即時に対処が必要
emergencies	0*	システムは使用不可

*現在のバージョンのファームウェアには、レベル0およびレベル1のエラーメッセージはありません。

- **Log contents** – フラッシュメモリー (システムを再起動してもデータが保持される非揮発性メモリー) または RAM (システムを再起動するとデータが失われるランダムアクセスメモリー) に保存されているシステムメッセージおよびイベントメッセージを一覧表示するためのボタンや、フラッシュメモリーまたは RAM のログメッセージを消去するボタンがあります。

Web – 「Monitoring」 => 「Logs」 をクリックします。ロギングを使用可能にして「flash」または「RAM」をクリックし、ログのメッセージレベル (選択したレベルからレベル0まで) を選択して、「Save Changes」をクリックします。表示されたメッセージを更新するには、「View Flash」または「View RAM」をクリックします。



CLI – 次に、ロギングを使用可能にし、フラッシュメモリーに記録するメッセージをレベル 3 (errors) に設定してから、フラッシュメモリーに格納されたログメッセージを表示する例を示します。

```

Console(config)#logging on                                4-30
Console(config)#logging history flash 3                  4-30
Console#show logging flash                               4-32
Syslog logging: Enable
History logging in FLASH: level errors
[0] 0:0:5 1/1/1
    "PRI_MGR_InitDefault function fails."
    level: 3, module: 13, function: 0, and event no.: 0
Console#

```

SNMP – 対応する MIB 変数

フィールド名	MIB 変数	アクセス	値の範囲	デフォルト値
Log Status	sun... sysLogMgt. sysLogStatus	読み取り/ 書き込み	enabled (1)、 disabled (2)	
History Flash Level	sun... sysLogMgt. sysLogStatus.sysLog. HistoryFlashLevel	読み取り/ 書き込み	整数 (0 ~ 7)	
History RAM Level	sun... sysLogMgt. sysLogStatus.sysLog. HistoryRAMLevel	読み取り/ 書き込み	整数 (0 ~ 7)	
Log Messages	未定義			

第4章

コマンド行リファレンス

この章では、コマンド行インタフェース (CLI) の使用方法について説明します。

4.1 コマンド行インタフェースの使用

4.1.1 CLI へのアクセス

サーバーのコンソールポートへの直接接続または telnet 接続を介してスイッチの管理インタフェースにアクセスすると、プロンプトでコマンドキーワードおよびパラメータを入力してスイッチを管理できます。スイッチの CLI の使用 방법은、UNIX システムでのコマンド入力によく似ています。

4.1.1.1 コンソール接続

コンソールポートを使用してスイッチにアクセスするには、次の手順を実行します。

1. コンソールプロンプトで、ユーザー名およびパスワードを入力します。デフォルトのユーザー名は「admin」および「guest」で、それぞれに対応するパスワードは「admin」および「guest」です。管理者ユーザー名およびパスワードを入力すると、CLI に Console# プロンプトが表示され、特権アクセスモード (特権実行) になります。また、ゲストユーザー名およびパスワードを入力すると、Console> プロンプトが表示され、通常アクセスモード (通常実行) になります。
2. 作業に必要なコマンドを入力します。
3. 作業が完了したら、quit コマンドまたは exit コマンドを実行してセッションを終了します。

コンソールポートを介してシステムに接続すると、次のようなログイン画面が表示されます。

```
User Access Verification

Username: admin
Password:

      CLI session with the Sun Fire B1600 is opened.
      To end the CLI session, enter [Exit].

Console#
```

4.1.1.2 telnet 接続

telnet は、IP トラnsポートプロトコル上で動作します。この環境では、管理ホストおよびネットワーク上で管理するネットワーク装置に、有効な IP アドレスが必要になります。有効な IP アドレスは、ピリオドで区切られた 0 ~ 255 の 4 つの数字で構成されます。各アドレスは、ネットワーク部とホスト部で構成されます。たとえば、IP アドレス 10.1.0.1 のネットワーク部は 10.1.0 で、ホスト部は 1 になります。

注 - デフォルトでは、ブレードシステムシャーシのスイッチには IP アドレスは割り当てられていません。管理ポート (NETMGT) は、VLAN 2 に割り当てられています。このポートを、アップリンクポートまたはダウンリンクポートを含む VLAN に割り当てることはできません。

telnet セッションを使用してスイッチにアクセスするには、最初にスイッチの IP アドレスを設定する必要があります。また、異なる IP サブネットからスイッチを管理する場合は、デフォルトゲートウェイを設定する必要があります。たとえば、次のように設定します。

```
Console(config)#interface vlan 2
Console(config-if)#ip address 10.1.0.1 255.255.255.0
Console(config-if)#exit
Console(config)#ip default-gateway 10.1.0.254
```

企業ネットワークがオフィスの外部にある別のネットワークまたはインターネットに接続されている場合は、登録されている IP アドレスを使用する必要があります。また、独立したネットワークに接続されている場合は、サイトのネットワークポリシーに適合した任意の IP アドレスを使用できます。

スイッチの IP アドレスを設定したあと、telnet セッションを開くには、次の手順を実行します。

1. 遠隔ホストから、telnet コマンドおよびアクセス先の装置の IP アドレスを入力します。
2. プロンプトで、ユーザー名およびシステムパスワードを入力します。管理者に対しては、Vty-0# プロンプトが表示され、特権アクセスモード (特権実行) を使用していることが示されます。一方、ゲストに対しては、Vty-0> が表示され、通常アクセスモード (通常実行) を使用していることが示されます。
3. 作業に必要なコマンドを入力します。
4. 作業が完了したら、quit コマンドまたは exit コマンドを実行してセッションを終了します。

telnet コマンドを入力すると、次のようなログイン画面が表示されます。

```
Username: admin
Password:

          CLI session with the Sun Fire B1600 is opened.
          To end the CLI session, enter [Exit].

Vty-0#
```

注 - telnet を介して、装置に対して最大 4 つのセッションを開くことができます。

4.1.2 コマンドの入力

ここでは、CLI コマンドの入力方法について説明します。

4.1.2.1 キーワードおよび引数

CLI コマンドは、一連のキーワードと引数で構成されます。キーワードはコマンドを特定し、引数は構成パラメタを指定します。たとえば、コマンド `show interfaces status ethernet SNP5` では、`show interfaces` および `status` がキーワードで、`ethernet` はインタフェースのタイプを指定する引数、`SNP5` はポートを指定する引数です。

コマンドは、次のように入力します。

- 単純なコマンドを入力するには、コマンドキーワードを入力します。

- 複数のコマンドを入力するには、それぞれのコマンドを適切な順序で入力します。たとえば、特権実行コマンドモードを使用可能にし、起動設定を表示するには、次のように入力します。

```
Console>enable  
Console#show startup-config
```

- パラメタを必要とするコマンドを入力するには、コマンドキーワードのあとに必要なパラメタを入力します。たとえば、管理者のパスワードを設定するには、次のように入力します。

```
Console(config)#username admin password 0 smith
```

4.1.2.2 最小限の省略語

CLI では、最小限の文字数でコマンドを特定することができます。たとえば、コマンド `logging history` は「`logging h`」と入力できます。入力が 2 通り以上に解釈できる場合は、さらに入力を求めるプロンプトが表示されます。

4.1.2.3 コマンドの補完

Tab キーを押して入力を終了した場合は、一意に定まるところまで省略したキーワードの残りの文字が出力されます。たとえば、`logging history` を入力するときには、「`log`」と入力してから Tab キーを押すと「`logging`」まで出力されます。

4.1.2.4 コマンドのヘルプの表示

ヘルプシステムの簡単な説明を表示するには、`help` コマンドを入力します。また、「`?`」文字を付けてコマンド構文を入力すると、キーワードまたはパラメタのリストが表示されます。

4.1.2.5 コマンドの表示

コマンドプロンプトで「?」と入力すると、現在のコマンドクラス (通常実行または特権実行) あるいは設定クラス (グローバルまたはインタフェース、回線、VLAN データベース) に対応するキーワードの最初のレベルが表示されます。また、特定のコマンドに対して有効なキーワードのリストを表示することもできます。たとえば、コマンド「show ?」を入力すると、候補となる show コマンドのリストが表示されます。

```
Console#show ?
  bridge-ext      Bridge extend information
  garp             Garp property
  gvrp            Show gvrp information of interface
  history         Information of history
  interfaces      Information of interfaces
  ip              Ip
  line            TTY line information
  logging         Show the contents of logging buffers
  mac-address-table Set configuration of the address table
  map             Map priority
  port            Characteristics of the port
  queue          Information of priority queue
  radius-server   Radius server information
  running-config  The system configuration of running
  snmp            SNMP statistics
  spanning-tree   Specify spanning-tree
  startup-config  The system configuration of starting up
  system         Information of system
  tacacs-server   Login by tacacs server
  users           Display information about terminal lines
  version         System hardware and software status
  vlan           Switch VLAN Virtual Interface
Console#show
```

コマンド「show interfaces ?」を入力すると、次の情報が表示されます。

```
Console>show interfaces ?
  counters      Information of interfaces counters
  status        Information of interfaces status
  switchport    Information of interfaces switchport
```

4.1.2.6 省略したキーワードの検索

省略したキーワードに疑問符を付けて入力を終了すると、先頭の文字列と一致するキーワードの候補が表示されます。コマンドと疑問符の間には空白文字を挿入しないでください。たとえば、「s?」と入力すると「s」で始まるすべてのキーワードが表示されます。

```
Console#show s?  
snmp          spanning-tree  startup-config  system
```

4.1.2.7 コマンドの機能を無効にする方法

多くの設定コマンドでは、接頭辞キーワード「no」を入力して、コマンドの機能を無効にするか、設定をデフォルト値にリセットできます。たとえば、logging コマンドを実行すると、システムメッセージをホストサーバーに記録できます。この logging コマンドを無効にするには、no logging コマンドを実行します。このマニュアルでは、無効にできるコマンドについては、その方法も説明しています。

4.1.2.8 コマンド履歴の使用

CLI は、入力されたコマンドの履歴を保持します。上矢印キーを押すと、コマンド履歴を上方にスクロールできます。履歴リストに表示されているコマンドは、再度実行できます。また、変更して実行することもできます。

show history コマンドを実行すると、最近実行されたコマンドの長いリストが表示されます。

4.1.2.9 コマンドモードについて

コマンドセットは、実行クラスと設定クラスに分類されます。実行コマンドは、通常、システムの状態に関する情報の表示や、統計カウンタの消去に使用します。設定コマンドは、インタフェースパラメタの変更や、特定のスイッチング機能を使用可能にするために使用します。これらのクラスは、さらに異なるモードに分類されます。使用できるコマンドは、選択するモードによって異なります。プロンプトで疑問符「?」を入力すると、現在のモードで使用できるコマンドのリストが表示されます。次の表に、コマンドクラスと関連するモードを示します。

クラス	モード
実行	通常 特権
設定*	グローバル インタフェース 回線 VLAN データベース

* 設定モードにアクセスするには、実行クラスが特権実行モードになっている必要があります。

4.1.2.10 実行コマンド

「guest」のユーザー名およびパスワードでスイッチの新しいコンソールセッションを開始すると、システムが通常実行コマンドモード (ゲストモード) になり、Console> コマンドプロンプトが表示されます。このモードで使用できるコマンドは制限されます。すべてのコマンドにアクセスできるのは、特権実行コマンドモード (管理者モード) の場合だけです。特権実行モードにアクセスするには、「admin」のユーザー名およびパスワードで新しいコンソールセッションを開始します。これによって、Console# コマンドプロンプトが表示されます。また、enable コマンドで特権レベルパスワード「super」を入力して、通常実行モードから特権実行モードに移行することもできます (4-26 ページ)。

特権実行モードに移行するには、次のユーザー名およびパスワードを入力します。

```
Username: admin
Password: [admin login password]

      CLI session with the Sun Fire B1600 is opened.
      To end the CLI session, enter [Exit].

Console#
```

```
Username: guest
Password: [guest login password]
```

```
CLI session with the Sun Fire B1600 is opened.
To end the CLI session, enter [Exit].
```

```
Console>enable
Password: [privileged level password]
Console#
```

4.1.2.11 設定コマンド

設定コマンドは、スイッチ設定を変更するために使用する特権レベルのコマンドです。設定コマンドでは、動作中の設定だけが変更されて、スイッチを再起動すると変更内容は保存されていません。動作中の設定を非揮発性の記憶装置に格納するには、`copy running-config startup-config` コマンドを使用します。

設定コマンドのモードは、次のとおりです。

- グローバル設定 — システムレベルの設定を変更します。hostname、snmp-server community などのコマンドがあります。
- インタフェース設定 — ポートの設定を変更します。speed-duplex、negotiation などのコマンドがあります。
- 回線設定 — コンソールポートおよび telnet の設定を変更します。exec-timeout、silent-time などのコマンドがあります。
- VLAN 設定 — VLAN グループを作成するコマンドなどがあります。

グローバル設定モードに移行するには、特権実行モードで `configure` コマンドを入力します。システムプロンプトが `Console(config)#` に変更されて、すべてのグローバル設定コマンドへのアクセス権が付与されます。

```
Console#configure
Console(config)#
```

その他のモードに移行するには、設定プロンプトで次のコマンドを入力します。設定モードに戻るには `exit` コマンドを使用し、特権実行モードに戻るには `end` コマンドを入力します。

モード	コマンド	プロンプト	ページ
インタフェース	<code>interface {ethernet port port-channel id vlan id}</code>	Console(config-if)#	4-75
回線	<code>line {console vty}</code>	Console(config-line)#	4-56
VLAN	<code>vlan database</code>	Console(config-vlan)	4-109

たとえば、次のようにコマンドを実行すると、インタフェース設定モードに移行したあと特権実行モードに戻ることができます。

```

Console(config)#interface ethernet SNP5
.
.
.
Console(config-if)#exit
Console(config)

```

4.1.2.12 コマンド行の入力

コマンドの大文字小文字は区別されません。コマンドおよびパラメタは、現在使用できるほかのコマンドまたはパラメタと区別できるだけの文字が含まれていれば、以降は省略可能です。Tab キーを使用して省略したコマンドを完成させるか、省略したコマンドのあとに「?」文字を入力して一致するコマンドの候補を表示できます。コマンド行の入力には、次の編集用のキーストロークを使用することもできます。

キーストローク	機能
Ctrl-A	カーソルをコマンド行の先頭に移動します。
Ctrl-B	カーソルを 1 文字左に移動します。
Ctrl-E	カーソルをコマンド行の末尾に移動します。
Ctrl-F	カーソルを 1 文字右に移動します。
Ctrl-P	直前のコマンドを表示します。
Ctrl-U	行全体を削除します。
Ctrl-W	最後に入力した単語を削除します。
Delete キーまたは Backspace キー	コマンドの入力誤りを消去します。

4.2 コマンドグループ

システムコマンドは、機能的に次のグループに分類されます。

コマンドグループ	説明	ページ
一般	特権アクセスモードへの移行、システムの再起動、CLI の終了などの基本的なコマンドです。	4-11
フラッシュ/ファイル	コードイメージまたはスイッチ構成ファイルを管理します。	4-17
システム管理	システムログおよびシステムパスワード、ユーザー名、ブラウザ管理オプションなど、さまざまなシステム情報を制御します。	4-24
認証	ローカルまたは RADIUS、TACACS メソッドを使用したログオンアクセスの認証を設定します。	4-41
SNMP	認証障害トラップを使用可能にします。また、コミュニティアクセス文字列およびトラップ管理を設定します。	4-49
回線	パスワードの確認および回線のパスワード、コンソールのタイムアウトなど、シリアルポートおよび telnet の接続オプションを設定します。	4-55
IP	管理アクセスのための IP アドレスおよびゲートウェイの設定、またはデフォルトゲートウェイの表示、指定した装置への ping を行います。	4-63
インタフェース	すべての Ethernet ポートおよび集約リンク、VLAN の接続パラメタを設定します。	4-75
アドレステーブル	指定したアドレスのフィルタリング、現在のエントリの表示、テーブルの内容の消去、保持時間の設定を行うためのアドレステーブルを設定します。	4-88
ポートセキュリティ	ポートにセキュリティ保護されたアドレスを設定します。	4-92
スパニングツリー	スイッチのスパニングツリーの設定を行います。	4-94
VLAN	VLAN の設定を行い、VLAN グループのポートメンバーを定義します。	4-108
GVRP およびブリッジ拡張機能	GVRP 設定を、自動 VLAN 学習を使用可能にするように設定します。また、ブリッジ拡張 MIB の設定を表示します。	4-118
IGMP スヌープ	IGMP マルチキャストフィルタリング、照会元としての役割、照会パラメタを設定し、マルチキャストルーターに接続されているポートを指定します。	4-124
優先順位	タグの付いていないフレームのポート優先順位および各優先順位キューの相対的加重、使用可能なキューの最大数を設定し、IP 優先度および DSCP の優先順位も設定します。	4-135

コマンドグループ	説明	ページ
ミラーポート	データの通過または監視するポートの性能に影響を与えることなく分析を行うために、別のポートにデータをミラー化します。	4-146
ポートトランクおよび LACP	複数のポートを 1 つの論理トランクに静的にグループ化します。また、ポートトランクの Link Aggregation Control Protocol を設定します。	4-148

この章の表に記載するアクセスモードは、次の略語で示します。

- NE (Normal Exec : 通常実行)
- PE (Privileged Exec : 特権実行)
- GC (Global Configuration : グローバル設定)
- IE (Interface Configuration : インタフェース設定)
- LC (Line Configuration : 回線設定)
- VC (VLAN Database Configuration : VLAN データベース設定)

4.3 コマンドの詳細な説明

4.3.1 一般コマンド

コマンド	機能	モード	ページ
enable	特権モードを有効にします。	NE	4-12
disable	特権モードから通常モードに切り替えます。	PE	4-13
configure	グローバル設定モードを有効にします。	PE	4-13
show history	コマンド履歴バッファを表示します。	NE、PE	4-14
reload	システムを再起動します。	PE	4-15
end	特権実行モードに戻ります。	GC、IC、LC、VC	4-16
exit	直前の設定モードに戻るか、CLI を終了します。	任意	4-16
quit	CLI セッションを終了します。	NE、PE	4-17
help	ヘルプの使用方法を表示します。	任意	なし
?	コマンド補完のオプションを表示します。 (コンテキストに依存)	任意	なし

4.3.1.1 enable

このコマンドは、特権実行モードを有効にするために使用します。特権モードでは、使用できるコマンドが増え、一部のコマンドに追加情報が表示されるようになります。詳細は、4-7 ページの「コマンドモードについて」を参照してください。

構文

enable [*level*]

level – 装置にログインするための特権レベルを指定します。
装置の特権レベルには、0 (通常実行) および 15 (特権実行) の 2 つのレベルがあります。特権実行モードにアクセスするには、レベル 15 を入力します。

デフォルト設定

レベル 15

コマンドモード

通常実行

コマンドの使用法

- 「super」は、コマンドモードを通常実行から特権実行に変更するために必要なデフォルトのパスワードです。このパスワードの設定については、4-26 ページの `enable password` コマンドを参照してください。
- プロンプトの末尾に「#」文字が付加されて、システムが特権アクセスモードになっていることが示されます。

例

```
Console>enable
Password: [privileged level password]
Console#
```

関連コマンド

`disable` (4-13 ページ)

`enable password` (4-26 ページ)

4.3.1.2 disable

このコマンドは、特権モードから通常実行モードに切り替えるために使用します。通常アクセスモードでは、スイッチ設定または **Ethernet** 統計に関する基本情報だけを表示できます。すべてのコマンドへのアクセス権を取得するには、特権モードを使用する必要があります。詳細は、4-7 ページの「コマンドモードについて」を参照してください。

デフォルト設定

なし

コマンドモード

特権実行

コマンドの使用法

プロンプトの末尾に「>」文字が付加されて、システムが通常アクセスモードになっていることが示されます。

例

```
Console#disable
Console>
```

関連コマンド

enable (4-12 ページ)

4.3.1.3 configure

このコマンドは、グローバル設定モードを有効にするために使用します。スイッチ設定を変更するには、このモードになっている必要があります。また、インタフェース設定および回線設定、**VLAN** データベース設定など、ほかのいくつかの設定モードを使用する場合にも、最初にグローバル設定モードに移行する必要があります。詳細は、4-7 ページの「コマンドモードについて」を参照してください。

デフォルト設定

なし

コマンドモード

特権実行

例

```
Console#configure
Console(config)#
```

関連コマンド

end (4-16 ページ)

4.3.1.4 show history

このコマンドは、コマンド履歴バッファの内容を表示するために使用します。

デフォルト設定

なし

コマンドモード

通常実行、特権実行

コマンドの使用法

履歴バッファサイズは固定されており、実行コマンドおよび設定コマンドはそれぞれ 10 件まで表示できます。

例

次に、show history コマンドによるコマンド履歴バッファの内容の表示例を示します。

```
Console#show history
Execution command history:
 2 config
 1 show history

Configuration command history:
 4 interface vlan 1
 3 exit
 2 interface vlan 1
 1 end

Console#
```

通常実行モードまたは特権実行モードで ! コマンドを使用すると、実行コマンド履歴バッファのコマンドが再実行され、設定モードのいずれかで ! コマンドを使用すると、設定コマンド履歴バッファのコマンドが再実行されます。次の例では、!2 コマンドによって、実行履歴バッファ内の 2 番目のコマンド (config) が再実行されます。

```
Console#!2
Console#config
Console(config)#
```

4.3.1.5 reload

このコマンドは、システムを再起動するために使用します。

注 – システムの再起動時には、必ず電源投入時自己診断が実行されます。また、`copy running-config startup-config` コマンドによって非揮発性メモリーに格納されたすべての設定情報は保持されます。

デフォルト設定

なし

コマンドモード

特権実行

コマンドの使用法

このコマンドはシステム全体をリセットします。

例

次に、スイッチのリセット方法を示します。

```
Console#reload
System will be restarted, continue <y/n>? y
```

4.3.1.6 end

このコマンドは、特権実行モードに切り替えるために使用します。

デフォルト設定

なし

コマンドモード

グローバル設定、インタフェース設定、回線設定、VLAN データベース設定、ルーター設定

例

次に、インタフェース設定モードから特権実行モードに戻る方法を示します。

```
Console(config-if)#end
Console#
```

4.3.1.7 exit

このコマンドは、直前の設定モードに戻るか、設定プログラムを終了するために使用します。

デフォルト設定

なし

コマンドモード

任意

例

次に、グローバル設定モードから特権実行モードに切り替えたあとで CLI セッションを終了する方法を示します。

```
Console(config)#exit
Console#exit

Press ENTER to start session

User Access Verification

Username:
```

4.3.1.8 quit

このコマンドは、CLI セッションを終了するために使用します。

デフォルト設定

なし

コマンドモード

通常実行、特権実行

コマンドの使用法

quit コマンドと exit コマンドのどちらを使用しても、設定プログラムを終了できます。

例

次に、CLI セッションの終了方法を示します。

```
Console#quit

Press ENTER to start session

User Access Verification

Username:
```

4.3.2 フラッシュ/ファイルコマンド

これらのコマンドは、システムコードまたは構成ファイルを管理するために使用します。

コマンド	機能	モード	ページ
copy	フラッシュメモリまたは TFTP サーバーとの間でコードイメージまたはスイッチ設定をコピーします。	PE	4-18
delete	ファイルまたはコードイメージを削除します。	PE	4-20
dir	フラッシュメモリ内のファイルのリストを表示します。	PE	4-21
whichboot	起動されたファイルを表示します。	PE	4-22
boot system	システムの起動に使用されるファイルまたはイメージを指定します。	GC	4-23

4.3.2.1 copy

このコマンドは、スイッチのフラッシュメモリと TFTP サーバー間でコードイメージまたは構成ファイルを移動 (アップロードまたはダウンロード) するために使用します。システムコードまたは設定内容を TFTP サーバー上のファイルに保存しておく、あとでこのファイルをスイッチにダウンロードしてシステム動作を復元できます。ファイル転送が正常に行われるかどうかは、TFTP サーバーにアクセスできるかどうかと、ネットワーク接続の品質によって決まります。

構文

```
copy file {file | running-config | startup-config | tftp}
copy running-config {file | startup-config | tftp}
copy startup-config {file | running-config | tftp}
copy tftp {file | running-config | startup-config}
copy tftp https-certificate
```

- **file** - ファイルのコピーを行うためのキーワードです。
- **running-config** - 現在の動作中設定のコピーを行うためのキーワードです。
- **startup-config** - システムの初期化に使用される設定です。
- **tftp** - TFTP サーバーに対してコピーを行うためのキーワードです。
- **https-certificate** - 認識されている認証局の証明書および非公開鍵、パスワードを指定するためのオプションです。

デフォルト設定

なし

コマンドモード

特権実行

コマンドの使用法

- **copy** コマンドの実行に必要なデータの入力を求めるプロンプトが表示されます。
- 対象となる構成ファイル名にはスラッシュ (\ または /) を使用できません。ファイル名の先頭の文字はピリオド (.) 以外にする必要があります。ファイル名は、TFTP サーバーでは 127 文字以内、スイッチ上のファイルでは 32 文字以内で指定します。使用できる文字は、A ~ Z および a ~ z、0 ~ 9、「.」、「-」、「_」です。
- フラッシュメモリのサイズには制限があるため、スイッチは 2 つのオペレーションコードファイルだけをサポートします。
- ユーザー定義の構成ファイルの最大数は、使用可能なメモリー容量によって決まります。
- **Factory_Default_Config.cfg** をコピー元に指定して出荷時のデフォルト構成ファイルをコピーすることはできますが、このファイルをコピー先に指定することはできません。

- コピー先に startup-config を指定すると、起動設定を置換できます。
- 起動 ROM およびローダーコードを TFTP サーバーからアップロードまたはダウンロードすることはできません。起動 ROM またはローダーコードの変更は、サンの保守技術者が行う必要があります。

例

次に、設定内容を TFTP サーバー上のファイルにアップロードする方法を示します。

```
Console#copy file tftp
Choose file type:
 1. config:  2. opcode: <1-2>: 1
Source file name: startup
TFTP server ip address: 10.1.0.99
Destination file name: startup.01
TFTP completed.
Success.

Console#
```

次に、動作中の設定をファイルにコピーする方法を示します。

```
Console#copy running-config file
destination file name : startup
Write to FLASH Programming.
\Write to FLASH finish.
Success.

Console#
```

次に、構成ファイルのダウンロード方法を示します。

```
Console#copy tftp startup-config
TFTP server ip address: 10.1.0.99
Source configuration file name: startup.01
Startup configuration file name [startup]:
Write to FLASH Programming.
\Write to FLASH finish.
Success.

Console#
```

次に、セキュリティー保護されたサイト証明書を TFTP サーバーに格納する方法を示します。格納後、スイッチを再起動して証明書を有効にします。

```
Console#copy tftp https-certificate

      TFTP server ip address: 10.1.0.19
      Source certificate file name:SS-certificate

      Source private file name:SS-private
      Private password: *****

Success.
Console#reload
System will be restarted, continue <y/n>? y
```

4.3.2.2 delete

このコマンドは、ファイルまたはイメージを削除するために使用します。

構文

delete *filename*

filename — 構成ファイルの名前またはイメージの名前を指定します。

デフォルト設定

なし

コマンドモード

特権実行

コマンドの使用法

- 起動 ROM のファイル、またはシステムの起動に使用されるファイルは削除できません。
- Factory_Default_Config.cfg は削除できません。

例

次に、フラッシュメモリーから **test2.cfg** 構成ファイルを削除する例を示します。

```
Console#delete test2.cfg
Console#
```

関連コマンド

dir (4-21 ページ)

4.3.2.3 dir

このコマンドは、フラッシュメモリー内のファイルのリストを表示するために使用します。

構文

dir [boot-rom | config | opcode [:filename]]

表示するファイルまたはイメージには、次のタイプがあります。

- **boot-rom** – 起動 ROM
- **config** – 構成ファイル
- **opcode** – ファイルまたはイメージの名前。このファイルが存在していても、エラーがある場合は、このファイルの情報を表示することはできません。
- **filename** – 表示するファイルの名前

デフォルト設定

なし

コマンドモード

特権実行

コマンドの使用法

- パラメタを指定しないでコマンド **dir** を入力すると、すべてのファイルが表示されます。
- 次に、ファイル情報を示します。

表 4-1 ファイル情報

列ヘッダー	説明
file name	ファイルの名前
file type	ファイルタイプ: 起動 ROM およびオペレーションコード、構成ファイル
startup	システムの起動時にこのファイルが使用されるかどうかを示します。
size	ファイルの長さ (バイト数)

例

次に、すべてのファイル情報を表示する例を示します。

```
Console#dir
-----
          file name      file type startup size (byte)
-----
          diag_0060 Boot-Rom image      Y      111360
          run_01642 Operation Code      N      1074304
          run_0200 Operation Code      Y      1083008
Factory_Default_Config.cfg Config File      N      2574
          startup Config File      Y      2710
-----
Total free space:      0
Console#
```

4.3.2.4 whichboot

このコマンドは、システムの電源投入時に起動されたファイルを表示するために使用します。

デフォルト設定

なし

コマンドモード

特権実行

コマンドの使用法

このコマンドが表示するファイル情報については、4-21 ページの表 4-1 を参照してください。

例

次に、whichboot コマンドにより表示される情報の例を示します。

```
Console#whichboot
-----
          file name      file type startup size (byte)
-----
          diag_0060 Boot-Rom image      Y      111360
          run_0200 Operation Code      Y      1083008
          startup Config File      Y      2710
Console#
```

4.3.2.5 boot system

このコマンドは、システムの起動に使用されるファイルまたはイメージを指定するために使用します。

構文

```
boot system {boot-rom | config | opcode};filename
```

デフォルトとして設定されたファイルまたはイメージのタイプは、次のとおりです。

- **boot-rom** - 起動 ROM
- **config** - 構成ファイル
- **opcode** - 実行時オペレーションコード

コロンの(:)は必須です。

filename - 構成ファイルの名前またはイメージの名前

デフォルト設定

なし

コマンドモード

グローバル設定

コマンドの使用法

- 指定したファイルタイプのあとにはコロンの(:)が必要です。
- ファイルにエラーがある場合、このファイルをデフォルトファイルとして設定することはできません。

例

```
Console(config)#boot system config: startup  
Console(config)#
```

関連コマンド

[dir \(4-21 ページ\)](#)

[whichboot \(4-22 ページ\)](#)

4.3.3 システム管理コマンド

次のコマンドは、システムログ、パスワード、ユーザー名、ブラウザ設定オプションを制御し、ほかのさまざまなシステム情報を表示または設定するために使用します。

コマンド	機能	モード	ページ
装置記述コマンド			
hostname	装置のホスト名を指定または変更します。	GC	4-25
ユーザーアクセスコマンド			
username	ログイン時にユーザー名に基づく認証システムを確立します。	GC	4-25
enable password	特権実行レベルへのアクセスを制御するためのパスワードを設定します。	GC	4-26
Web サーバーコマンド			
ip http port	Web ブラウザインタフェースが使用するポートを指定します。	GC	4-27
ip http server	スイッチをブラウザから監視または設定できるようにします。	GC	4-28
ジャンボフレームコマンド			
jumbo-frame	ジャンボフレームのサポートを可能にします。	GC	4-29
イベントロギングコマンド			
logging on	エラーメッセージのロギングを制御します。	GC	4-30
logging history	スイッチメモリーに保存される syslog メッセージを重要度に応じて制限します。	GC	4-30
clear logging	ロギングバッファからメッセージを消去します。	PE	4-32
show logging	ロギングの状態を表示します。	PE	4-32
システムステータスコマンド			
show startup-config	システムの起動時に使用される、フラッシュメモリーに格納された構成ファイルの内容を表示します。	PE	4-25
show running-config	現在使用されている設定データを表示します。	PE	4-25
show system	システム情報を表示します。	NE、PE	4-25
show users	ユーザー名、アイドル時間、telnet クライアントの IP アドレスなど、アクティブなすべてのコンソールおよび telnet セッションの情報を表示します。	NE、PE	4-25
show version	システムのバージョン情報を表示します。	NE、PE	4-25

4.3.3.1 hostname

このコマンドは、この装置のホスト名を指定または変更するために使用します。デフォルトのホスト名に戻す場合は、no 形式を使用します。

構文

```
hostname name  
no hostname
```

name — このホストの名前 (最大長 : 255 文字) を指定します。

デフォルト設定

なし

コマンドモード

グローバル設定

例

```
Console(config)#hostname Server_Chassis_35  
Console(config)#
```

4.3.3.2 username

このコマンドは、名前付きユーザーの追加、ログイン時の認証の要求、ユーザーのパスワードの指定または変更 (またはパスワードが不要であることの指定)、ユーザーのアクセスレベルの指定または変更を行うために使用します。ユーザー名を削除する場合は、no 形式を使用します。

構文

```
username name {access-level level | nopassword | password {0 | 7}  
password}  
no username name
```

- *name* — ユーザーの名前を指定します (最大長 : 8 文字、最大ユーザー数 : 5)。
- **access-level** *level* — ユーザーのレベルを指定します。
装置には、次の 2 つの特権レベルがあらかじめ定義されています。
0 : 通常実行、15 : 特権実行 (レベル 1 ~ 14 は未使用)。
- **nopassword** — これを指定すると、ユーザーがログインするときにパスワードが不要になります。
- {**0** | **7**} — 0 はプレーンパスワードの入力、7 は暗号化パスワードの入力を表します。
- **password** *password* — ユーザーの認証パスワードを指定します (最大長 : プレーンテキストの場合は 8 文字、暗号化テキストの場合は 32 文字、大文字小文字を区別)。

デフォルト設定

- デフォルトのアクセスレベルは、通常実行です。
- デフォルトのパスワードは、通常実行モードでは「guest」、特権実行モードでは「admin」です。

ユーザー名およびパスワードの出荷時のデフォルトは、次のとおりです。

表 4-2 デフォルトのユーザー名およびパスワード

ユーザー名	アクセスレベル	パスワード
guest	0	guest
admin	15	admin

コマンドモード

グローバル設定

コマンドの使用法

暗号化パスワードをコマンド行で指定する必要はありません。スイッチは、システム起動時に内部でオプション 7 を使用して、構成ファイルに格納されている暗号化パスワードを読み取ります。

例

次に、ユーザーのアクセスレベルおよびパスワードの設定の例を示します。

```
Console(config)#username bob access-level 15
Console(config)#username bob password 0 smith
Console(config)#
```

4.3.3.3 enable password

システムにはじめてログオンしたときには、特権実行パスワードを設定する必要があります。パスワードは安全な場所に記録しておいてください。このコマンドは、通常実行レベルから特権実行レベルへのアクセスを制御するために使用します。デフォルトのパスワードにリセットする場合は、no 形式を使用します。

構文

```
enable password [level level] {0 | 7} password
no enable password [level level]
```

- **level level** – 特権実行の場合はレベル 15 です (レベル 0 ~ 14 は未使用)。
- **{0 | 7}** – 0 はプレーンパスワードの入力、7 は暗号化パスワードの入力を表します。
- *password* – この特権レベルのパスワードを指定します (最大長 : プレーンテキストの場合は 8 文字、暗号化テキストの場合は 32 文字、大文字小文字を区別)。

デフォルト設定

- デフォルトはレベル 15 です。
- デフォルトのパスワードは「super」です。

コマンドモード

グローバル設定

コマンドの使用法

- NULL パスワードを設定することはできません。enable コマンド (4-12 ページ) を使用して通常実行から特権実行にコマンドモードを変更するには、パスワードを入力する必要があります。
- コマンド行で暗号化パスワードを指定する必要はありません。スイッチは、システム起動時に内部でオプション 7 を使用して、構成ファイルに格納されている暗号化パスワードを読み取ります。

例

```
Console(config)#enable password level 15 0 admin
Console(config)#
```

関連コマンド

enable (4-12 ページ)

4.3.3.4 ip http port

このコマンドは、Web ブラウザインタフェースが使用する TCP ポート番号を指定するために使用します。デフォルトポートを使用する場合は、no 形式を使用します。

構文

```
ip http port port-number
no ip http port
```

port-number — ブラウザインタフェースが使用する TCP ポートを指定します (範囲: 1 ~ 65535)。

デフォルト設定

80

コマンドモード

グローバル設定

例

```
Console(config)#ip http port 769
Console(config)#
```

関連コマンド

ip http server (4-28 ページ)

4.3.3.5 ip http server

このコマンドは、ブラウザによる装置の監視または設定を可能にするために使用します。この機能を使用不可にする場合は、no 形式を使用します。

構文

```
ip http server
no ip http server
```

デフォルト設定

使用可能

コマンドモード

グローバル設定

例

```
Console(config)#ip http server
Console(config)#
```

関連コマンド

ip http port (4-27 ページ)

4.3.3.6 jumbo-frame

このコマンドは、ジャンボフレームのサポートを可能にするために使用します。使用不可にする場合は、no 形式を使用します。

構文

```
jumbo-frame  
no jumbo-frame
```

デフォルト設定

使用不可

コマンドモード

グローバル設定

コマンドの使用法

- このスイッチでは、最大 9000 バイトのジャンボフレームをサポートすることで、大容量の連続データ転送のスループットを効率化します。最大 1.5K バイトの標準の Ethernet フレームに比べて、ジャンボフレームでは、プロトコルカプセル化フィールドの処理に必要なパケットあたりのオーバーヘッドが大幅に削減されます。
- ジャンボフレームを使用するには、送信元と送信先の両方のエンドノード (コンピュータ、サーバーなど) でこの機能をサポートする必要があります。また、接続が全二重で動作している場合は、ネットワークの 2 つのエンドノード間にあるすべてのスイッチで拡張フレームサイズに対応する必要があります。半二重接続では、コリジョンドメイン内のすべての装置でジャンボフレームをサポートする必要があります。
- ジャンボフレームを使用可能にすると、ブロードキャストストーム制御の最大しきい値が 1 秒あたり 64 パケットに制限されます。詳細は、4-83 ページの switchport broadcast コマンドを参照してください。

例

```
Console(config)#jumbo-frame  
Console(config)#
```

4.3.3.7 logging on

このコマンドは、エラーメッセージのロギングを制御するために使用します。このコマンドによって、デバッグメッセージまたはエラーメッセージをスイッチメモリに送信できます。ロギングプロセスを使用不可にする場合は、no 形式を使用します。

構文

```
logging on
no logging on
```

デフォルト設定

なし

コマンドモード

グローバル設定

コマンドの使用法

ロギングプロセスは、スイッチメモリに保存するエラーメッセージを制御します。logging history コマンドを使用すると、格納するエラーメッセージのタイプを制御できます。

例

```
Console(config)#logging on
Console(config)#
```

関連コマンド

```
logging history (4-30 ページ)
clear logging (4-32 ページ)
```

4.3.3.8 logging history

このコマンドは、スイッチメモリに保存する syslog メッセージを重要度に応じて制限するために使用します。syslog メッセージのロギングをデフォルトレベルに戻す場合は、no 形式を使用します。

構文

```
logging history {flash | ram} level
no logging history {flash | ram}
```

- **flash** — フラッシュメモリ (永続メモリ) に格納されているイベント履歴を指定します。
- **ram** — 一時 RAM (電源リセット時に消去されるメモリ) に格納されているイベント履歴を指定します。

- **level** - 0 ~ 7 で指定します。選択したレベルからレベル 0 までのメッセージが保存されます。

表 4-3 エラーレベル

レベル引数	レベル	説明
debugging	7	デバッグ用メッセージ
informational	6	情報メッセージのみ
notifications	5	コールドスタートなどの、正常だが通知が必要な状態
warnings	4	警告状態 (false が返された、予期せぬ結果が返されたなど)
errors	3	エラー (無効な入力が行われた、デフォルトが使用されたなど)
critical	2	重大な問題 (記憶域割り当てエラー、リソース不足による空きメモリーエラーなど)
alerts	1	即時に対処が必要
emergencies	0	システムは使用不可

*現在のバージョンのファームウェアには、レベル 0 およびレベル 1 のエラーメッセージはありません。

デフォルト設定

フラッシュ : errors (レベル 3 ~ 0)
RAM : warnings (レベル 7 ~ 0)

コマンドモード

グローバル設定

コマンドの使用法

フラッシュメモリーに対して指定するメッセージレベルは、RAM に対して指定するレベルより高くする (数値を小さくする) 必要があります。

例

```
Console(config)#logging history ram 0
Console(config)#
```

4.3.3.9 clear logging

このコマンドは、ログバッファからメッセージを消去するために使用します。

構文

clear logging [**flash** | **ram**]

- **flash** – フラッシュメモリー (永続メモリー) に格納されているイベント履歴を指定します。
- **ram** – 一時 RAM (電源リセット時に消去されるメモリー) に格納されているイベント履歴を指定します。

デフォルト設定

フラッシュおよび RAM

コマンドモード

特権実行

例

```
Console#clear logging
Console#
```

関連コマンド

show logging (4-32 ページ)

4.3.3.10 show logging

このコマンドは、メモリーに格納されているシステムメッセージおよびイベントメッセージとともに、現在のロギング設定を表示するために使用します。

構文

show logging {**flash** | **ram**}

- **flash** – フラッシュメモリー (永続メモリー) に格納されているイベント履歴を指定します。
- **ram** – 一時 RAM (電源リセット時に消去されるメモリー) に格納されているイベント履歴を指定します。

デフォルト設定

なし

コマンドモード

特権実行

コマンドの使用法

このコマンドを使用すると、次の情報が表示されます。

- Syslog logging – logging on コマンドを使用してシステムロギングが使用可能になっているかどうか
- History logging in FLASH/RAM – logging history コマンドに基づいて通知されるメッセージのレベル
- メモリーに格納されているすべてのシステムメッセージおよびイベントメッセージ

例

次に、システムロギングが使用可能、フラッシュメモリーのメッセージレベルが「errors」（デフォルトレベル 3 ～ 0）、RAM のメッセージレベルが「debugging」（デフォルトレベル 7 ～ 0）に設定されていて、エラーが 1 つある例を示します。

```
Console#show logging flash
Syslog logging: Enable
History logging in FLASH: level errors
[0] 0:0:5 1/1/1
    "PRI_MGR_InitDefault function fails."
    level: 3, module: 13, function: 0, and event no.: 0
Console#show logging ram
Syslog logging: Enable
History logging in RAM: level debugging
[0] 0:0:5 1/1/1
    "PRI_MGR_InitDefault function fails."
    level: 3, module: 13, function: 0, and event no.: 0
Console#
```

関連コマンド

logging on (4-30 ページ)
logging history (4-30 ページ)

4.3.3.11 show startup-config

このコマンドは、システムの起動に使用される、非揮発性メモリーに格納された構成ファイルを表示するために使用します。

デフォルト設定

なし

コマンドモード

特権実行

コマンドの使用法

- このコマンドを show running-config コマンドとともに使用すると、実行中のメモリー内の情報を、非揮発性メモリーに格納されている情報と比較できます。
- このコマンドを使用すると、主なコマンドモードの設定が表示されます。各モードグループは「!」記号で区切られていて、設定モードコマンドおよび対応するコマンドが含まれています。このコマンドを使用すると、次の情報が表示されます。
 - システムの説明 (ホスト名、位置、連絡先情報)
 - SNMP コミュニティー文字列
 - ユーザー (名前、アクセスレベル、暗号化パスワード)
 - VLAN データベース (VLAN ID、名前、状態)
 - 各インタフェースの VLAN 設定
 - 管理 VLAN の IP アドレス
 - ユーザー認証シーケンスと、遠隔認証サーバーのアドレスおよび UDP ポート
 - コンソールポートおよび telnet の構成済み設定

例

```
Console#show startup-config
building startup-config, please wait.....
!
hostname R&D 5
snmp-server location WC 9
snmp-server contact Charles
!
snmp-server community private rw
snmp-server community public ro
!
username admin access-level 15
username admin password 7 21232f297a57a5a743894a0e4a801fc3
username guest access-level 0
username guest password 7 084e0343a0486ff05530df6c705c8bb4
```

```
enable password level 15 7 1b3231655cebb7a1f783eddf27d254ca
!  
vlan database  
  vlan 1 name DefaultVlan media ethernet state active  
  vlan 2 name MgtVlan media ethernet state active  
!  
!  
spanning-tree mst-configuration  
  name XSTP REGION 0  
!  
interface ethernet SNP0  
  description Blade Slot 1  
  flowcontrol  
  switchport allowed vlan add 1 untagged  
  switchport native vlan 1  
  spanning-tree edge-port  
  spanning-tree link-type auto  
.  
.  
interface vlan 2  
  ip address 0.0.0.0 255.0.0.0  
!!  
no bridge-ext gvrp!  
!  
authentication login local  
tacacs-server host 0.0.0.0  
tacacs-server port 0  
!  
line console  
!  
!  
line vty  
!  
!  
end  
Console#
```

関連コマンド

show running-config (4-36 ページ)

4.3.3.12 show running-config

このコマンドは、現在使用している設定情報を表示するために使用します。

デフォルト設定

なし

コマンドモード

特権実行

コマンドの使用法

- このコマンドを `show startup-config` コマンドとともに使用すると、実行中のメモリー内の情報を、非揮発性メモリーに格納されている情報と比較できます。
- このコマンドを使用すると、主なコマンドモードの設定が表示されます。各モードグループは、「!」記号で区切られていて、設定モードコマンドおよび対応するコマンドが含まれています。このコマンドを使用すると、次の情報が表示されます。
 - システムの説明 (ホスト名、位置、連絡先情報)
 - SNMP コミュニティ文字列
 - ユーザー (名前、アクセスレベル、暗号化パスワード)
 - VLAN データベース (VLAN ID、名前、状態)
 - 各インタフェースの VLAN 設定
 - 管理 VLAN の IP アドレス
 - ユーザー認証シーケンスと、遠隔認証サーバーのアドレスおよび UDP ポート
 - コンソールポートおよび telnet の構成済み設定

例

```
Console#show running-config
building running-config, please wait.....
!
hostname R&D 5
snmp-server location WC 9
snmp-server contact Charles
!
snmp-server community private rw
snmp-server community public ro
!
username admin access-level 15
username admin password 7 21232f297a57a5a743894a0e4a801fc3
username guest access-level 0
username guest password 7 084e0343a0486ff05530df6c705c8bb4
enable password level 15 7 1b3231655cebb7a1f783eddf27d254ca
```

```
!  
vlan database  
  vlan 1 name DefaultVlan media ethernet state active  
  vlan 2 name MgtVlan media ethernet state active  
!  
!  
!  
spanning-tree mst-configuration  
!  
interface ethernet SNP0  
  description Blade Slot 0  
  flowcontrol  
  switchport allowed vlan add 1 untagged  
  switchport native vlan 1  
  spanning-tree edge-port  
  spanning-tree link-type auto  
.  
.  
interface vlan 2  
  ip address 0.0.0.0 255.0.0.0  
!  
!  
no bridge-ext gvrp  
!  
!  
authentication login local  
tacacs-server host 0.0.0.0  
tacacs-server port 0  
!  
line console  
!  
line vty  
!  
!  
end  
Console#
```

関連コマンド

show startup-config (4-34 ページ)

4.3.3.13 show system

このコマンドは、システム情報を表示するために使用します。

デフォルト設定

なし

コマンドモード

通常実行、特権実行

コマンドの使用法

- このコマンドによって表示される項目については、3-8 ページの「システム情報の表示」を参照してください。
- POST の結果には、すべて「PASS」が表示される必要があります。「FAIL」と表示された項目があった場合は、ご購入先にご連絡ください。

例

```
Console#show system
System description: Sun Fire B1600
System OID string: 1.3.6.1.4.1.42.2.24.1
System information
  System Up time: 0 days, 0 hours, 55 minutes, and 54.91 seconds
  System Name      : [NONE]
  System Location  : [NONE]
  System Contact   : [NONE]
  MAC address      : 00-00-e8-00-00-01
  Web server       : enable
  Web server port  : 80
  Web secure server : enable
  Web secure server port : 443
POST result

--- Performing Power-On Self Tests (POST) ---
UART Loopback Test ..... PASS
Timer Test ..... PASS
DRAM Test ..... PASS
I2C Initialization ..... PASS
Runtime Image Check ..... PASS
PCI Device Check ..... PASS
Switch Driver Initialization ..... PASS
----- DONE -----
Console#
```

4.3.3.14 show users

ユーザー名、アイドル時間、telnet クライアントの IP アドレスなど、アクティブなすべてのコンソールおよび telnet セッションの情報を表示します。

デフォルト設定

なし

コマンドモード

通常実行、特権実行

コマンドの使用法

このコマンドの実行に使用されたセッションは、回線 (セッション) インデックス番号の横に「*」記号を付けて表示されます。

例

```
Console#show users
Username accounts:
  Username Privilege
  -----
    admin          15
    guest           0

Online users:
  Line      Username Idle time (h:m:s) Remote IP addr.
  -----
* 0  console  admin          0:00:00
  1  vty 0    admin          0:04:37      10.1.0.19

Console#
```

4.3.3.15 show version

このコマンドは、システムのハードウェアおよびソフトウェアのバージョン情報を表示するために使用します。

デフォルト設定

なし

コマンドモード

通常実行、特権実行

コマンドの使用法

ソフトウェア項目の詳細は、3-17 ページの「スイッチソフトウェアのバージョンの表示」を参照してください。ハードウェア項目の意味は、次のとおりです。

- Serial Number – メインボードのシリアル番号
- Service Tag – このスイッチには適用されません。
- Hardware Version – メインボードのハードウェアバージョン
- Number of Ports – スイッチのポート数
- Main Power Status – スイッチの電源の状態
- Redundant Power Status – このスイッチには適用されません。

例

```
Console#show version
Unit1
  Serial number          :1
  Service tag            :
  Hardware version       :R0B
  Number of ports        :25
  Main power status      :up
  Redundant power status :not present
Agent(master)
  Unit id                :1
  Loader version         :0.0.6.5
  Boot rom version       :0.0.7.3
  Operation code version :1.0.0.1
Console#
```

4.3.4 認証コマンド

このスイッチは、ローカルまたは RADIUS、TACACS 認証メソッドを使用して、管理アクセスのためにシステムにログインするユーザーを認証するように設定できます。

RADIUS および TACACS は、中央サーバー上で動作するソフトウェアを使用して、ネットワーク上の RADIUS または TACACS 対応装置へのアクセスを管理するログオン認証プロトコルです。認証サーバーにはデータベースがあり、スイッチへの管理アクセスを必要とするユーザーまたはグループのそれぞれに割り当てられたユーザー名およびパスワードの組と、それに関連する特権レベルが格納されています。

コマンド	機能	モード	ページ
認証メソッド			
<code>authentication login</code>	ログオン認証メソッドおよび優先度を定義します。	GC	4-42
RADIUS クライアント			
<code>radius-server host</code>	RADIUS サーバーを指定します。	GC	4-43
<code>radius-server port</code>	RADIUS サーバーのネットワークポートを設定します。	GC	4-43
<code>radius-server key</code>	RADIUS 暗号化鍵を設定します。	GC	4-44
<code>radius-server retransmit</code>	再試行回数を設定します。	GC	4-44
<code>radius-server timeout</code>	認証要求の送信間隔を設定します。	GC	4-45
<code>show radius-server</code>	現在の RADIUS 設定を表示します。	PE	4-46
TACACS クライアント			
<code>tacacs-server host</code>	TACACS サーバーを指定します。	GC	4-46
<code>tacacs-server port</code>	TACACS サーバーのネットワークポートを設定します。	GC	4-47
<code>tacacs-server key</code>	TACACS 暗号化鍵を設定します。	GC	4-47
<code>show tacacs-server</code>	現在の TACACS 設定を表示します。	PE	4-48

4.3.4.1 authentication login

このコマンドは、ログインの認証メソッドおよび優先順位を定義するために使用します。デフォルトに戻す場合は、no 形式を使用します。

構文

```
authentication login {[local] [radius] [tacacs]}  
no authentication login
```

- **local** — ローカルパスワードを使用します。
- **radius** — RADIUS サーバーパスワードを使用します。
- **tacacs** — TACACS サーバーパスワードを使用します。

認証メソッドは、任意の順序で指定できます。

デフォルト設定

なし

コマンドモード

グローバル設定

コマンドの使用法

- RADIUS は UDP を、TACACS は TCP を使用します。UDP はベストエフォート型の通信しか提供しませんが、TCP はコネクション型トランスポートを提供します。また、RADIUS ではクライアントからサーバーへのアクセス要求パケットのパスワードだけが暗号化されますが、TACACS ではパケットの本体全体が暗号化されます。
- RADIUS および TACACS ログオン認証では、コンソールポートまたは Web ブラウザ、telnet を介して管理アクセスを制御します。これらのアクセス方法は、認証サーバー上で設定する必要があります。
- RADIUS および TACACS ログオン認証では、ユーザー名およびパスワードの組のそれぞれに対して権限レベルが割り当てられます。ユーザー名およびパスワード、特権レベルは、認証サーバー上で設定する必要があります。
- 1 つのコマンドで 2 つまたは 3 つの認証メソッドを指定して、認証シーケンスを指定できます。たとえば、「authentication login radius local」と入力すると、RADIUS サーバーのユーザー名とパスワードが最初に確認されます。RADIUS サーバーが使用できない場合は、ローカルのユーザー名とパスワードが確認されます。

例

```
Console(config)#authentication login radius  
Console(config)#
```

関連コマンド

username - ローカルユーザー名およびパスワードを設定する場合 (4-25 ページ)

4.3.4.2 radius-server host

このコマンドは、RADIUS サーバーを指定するために使用します。デフォルトに戻す場合は、no 形式を使用します。

構文

```
radius-server host host_ip_address  
no radius-server host
```

host_ip_address - サーバーの IP アドレスです。

デフォルト設定

10.11.12.13

コマンドモード

グローバル設定

例

```
Console(config)#radius-server host 192.168.1.25  
Console(config)#
```

4.3.4.3 radius-server port

このコマンドは、RADIUS サーバーのネットワークポートを設定するために使用します。デフォルトに戻す場合は、no 形式を使用します。

構文

```
radius-server port port_number  
no radius-server port
```

port_number - 認証メッセージに使用する RADIUS サーバーの UDP ポートを指定します (範囲: 1 ~ 65535)。

デフォルト設定

1812

コマンドモード

グローバル設定

例

```
Console(config)#radius-server port 181
Console(config)#
```

4.3.4.4 radius-server key

このコマンドは、RADIUS 暗号化鍵を設定するために使用します。デフォルトに戻す場合は、no 形式を使用します。

構文

```
radius-server key key_string
no radius-server key
```

key_string - クライアントへのログオンアクセスの認証に使用する暗号化鍵を指定します。文字列には空白文字を使用しないでください (最大長: 20 文字)。

デフォルト設定

なし

コマンドモード

グローバル設定

例

```
Console(config)#radius-server key green
Console(config)#
```

4.3.4.5 radius-server retransmit

このコマンドは、再試行回数を設定するために使用します。デフォルトに戻す場合は、no 形式を使用します。

構文

```
radius-server retransmit number_of_retries
no radius-server retransmit
```

number_of_retries - スイッチで、RADIUS サーバーを介したログオンアクセスの認証を試行する回数を指定します (範囲: 1 ~ 30)。

デフォルト設定

2

コマンドモード

グローバル設定

例

```
Console(config)#radius-server retransmit 5
Console(config)#
```

4.3.4.6 radius-server timeout

このコマンドは、RADIUS サーバーに認証要求を転送する間隔を設定するために使用します。デフォルトに戻す場合は、no 形式を使用します。

構文

```
radius-server timeout number_of_seconds
no radius-server timeout
```

number_of_seconds — 要求を再送する前にスイッチが応答を待つ秒数を指定します (範囲: 1 ~ 65535)。

デフォルト設定

5

コマンドモード

グローバル設定

例

```
Console(config)#radius-server timeout 10
Console(config)#
```

4.3.4.7 show radius-server

このコマンドは、RADIUS サーバーの現在の設定を表示するために使用します。

デフォルト設定

なし

コマンドモード

特権実行

例

```
Console#show radius-server
Remote radius server configuration:
  Server IP address: 10.11.12.13
  Communication key with radius server: green
  Server port number: 1812
  Retransmit times: 2
  Request timeout: 5
Console#
```

4.3.4.8 tacacs-server host

このコマンドは、TACACS サーバーを指定するために使用します。デフォルトに戻す場合は、no 形式を使用します。

構文

tacacs-server host *host_ip_address*

no tacacs-server host

host_ip_address - サーバーの IP アドレスを指定します。

デフォルト設定

なし

コマンドモード

グローバル設定

例

```
Console(config)#tacacs-server host 192.168.1.25
Console(config)#
```

4.3.4.9 tacacs-server port

このコマンドは、TACACS サーバーのネットワークポートを設定するために使用します。デフォルトに戻す場合は、no 形式を使用します。

構文

```
tacacs-server port port_number  
no tacacs-server port
```

port_number — 認証メッセージに使用する TACACS サーバーの UDP ポートを指定します (範囲: 1 ~ 65535)。

デフォルト設定

なし

コマンドモード

グローバル設定

例

```
Console(config)#tacacs-server port 181  
Console(config)#
```

4.3.4.10 tacacs-server key

このコマンドは、TACACS 暗号化鍵を設定するために使用します。デフォルトに戻す場合は、no 形式を使用します。

構文

```
tacacs-server key key_string  
no tacacs-server key
```

key_string — クライアントへのログオンアクセスの認証に使用する暗号化鍵を指定します。文字列には空白文字を使用しないでください (最大長: 20 文字)。

デフォルト設定

なし

コマンドモード

グローバル設定

例

```
Console(config)#tacacs-server key green
Console(config)#
```

4.3.4.11 show tacacs-server

このコマンドは、TACACS サーバーの現在の設定を表示するために使用します。

デフォルト設定

なし

コマンドモード

特権実行

例

```
Console#show tacacs-server
Remote TACACS server configuration:
  Server IP address: 10.11.12.13
  Communication key with tacacs server: green
  Server port number: 1824
Console#
```

4.3.5 SNMP コマンド

SNMP 管理ホストからスイッチへのアクセスと、トラップマネージャーに送信するエラーのタイプを制御します。

コマンド	機能	モード	ページ
<code>snmp-server community</code>	SNMP コマンドへのアクセスを許可するためのコミュニティーアクセス文字列を設定します。	GC	4-49
<code>snmp-server contact</code>	システムの連絡先を示す文字列を設定します。	GC	4-50
<code>snmp-server location</code>	システムの位置を示す文字列を設定します。	GC	4-51
<code>snmp-server host</code>	SNMP 通知の受信者を指定します。	GC	4-51
<code>snmp-server enable traps</code>	装置の SNMP トラップの送信または要求の通知 (SNMP 通知) を可能にします。	GC	4-52
<code>show snmp</code>	SNMP 通信の状態を表示します。	NE、PE	4-53

4.3.5.1 `snmp-server community`

このコマンドは、SNMP (Simple Network Management Protocol) のコミュニティーアクセス文字列を定義するために使用します。指定したコミュニティー文字列を削除する場合は、`no` 形式を使用します。

構文

```
snmp-server community string [ro|rw]  
no snmp-server community string
```

- *string* - パスワードのように機能する、SNMP プロトコルへのアクセスを許可するコミュニティー文字列を指定します (最大長: 32 文字、大文字小文字を区別、最大文字列数: 5)。
- **ro** - 読み取り専用アクセスを指定します。認証された管理ホストは、MIB オブジェクトの取り出しだけを行うことができます。
- **rw** - 読み取りおよび書き込みアクセスを指定します。認証された管理ホストは、MIB オブジェクトの取り出しおよび変更の両方を行うことができます。

デフォルト設定

- **public** - 読み取り専用アクセス
- **private** - 読み取りおよび書き込みアクセス

コマンドモード

グローバル設定

コマンドの使用法

最初に実行した `snmp-server community` コマンドで、すべてのバージョンの SNMP (SNMPv1 および SNMPv2c) が使用可能になります。
`no snmp-server community` コマンドを実行すると、すべての SNMP バージョンが使用不可になります。

例

```
Console(config)#snmp-server community alpha rw
Console(config)#
```

4.3.5.2 snmp-server contact

このコマンドは、システムの連絡先を示す文字列を設定するために使用します。システムの絡先情報を削除する場合は、`no` 形式を使用します。

構文

```
snmp-server contact string
no snmp-server contact
```

string — システムの連絡先情報を示す文字列を指定します (最大長 : 255 文字)。

デフォルト設定

なし

コマンドモード

グローバル設定

例

```
Console(config)#snmp-server contact Paul
Console(config)#
```

関連コマンド

`snmp-server location` (4-51 ページ)

4.3.5.3 snmp-server location

このコマンドは、システムの位置を示す文字列を設定するために使用します。位置を示す文字列を削除する場合は、no 形式を使用します。

構文

```
snmp-server location text  
no snmp-server location
```

text — システムの位置を示す文字列を指定します (最大長 : 255 文字)。

デフォルト設定

なし

コマンドモード

グローバル設定

例

```
Console(config)#snmp-server location WC-19  
Console(config)#
```

関連コマンド

snmp-server contact (4-50 ページ)

4.3.5.4 snmp-server host

このコマンドは、SNMP 通知の受信者を指定するために使用します。指定したホストを削除する場合は、no 形式を使用します。

構文

```
snmp-server host host-addr community-string version version-number  
no snmp-server host host-addr
```

- *host-addr* — ホスト (対象になる受信者) の名前またはインターネットアドレスを指定します (ホストアドレスの最大数 : トラップ送信先 IP アドレスのエントリ 5 つ)。
- *community-string* — 通知操作で送信される、パスワードのように機能するコミュニティー文字列を指定します。この文字列は、snmp-server host コマンドに指定することもできますが、snmp-server host コマンドを使用する前に snmp-server community コマンドを使用して指定しておくことをお勧めします (最大長 : 32 文字)。
- *version-number* — {1 | 2c}
ホストで SNMP バージョン 1 とバージョン 2c のどちらが実行されているかを示します。

デフォルト設定

なし

コマンドモード

グローバル設定

コマンドの使用法

`snmp-server host` コマンドを実行しないと通知は送信されません。SNMP 通知を送信するようにスイッチを設定するには、1 つ以上の `snmp-server host` コマンドを実行する必要があります。複数のホストを使用可能にするには、ホストごとに `snmp-server host` コマンドを発行する必要があります。

`snmp-server host` コマンドは、`snmp-server enable traps` コマンドとともに使用します。`snmp-server enable traps` コマンドは、グローバルに送信される SNMP 通知を指定するために使用します。ホストで通知を受信するには、ホストに対して 1 つ以上の `snmp-server enable traps` コマンドおよび `snmp-server host` コマンドを実行する必要があります。

ただし、`snmp-server enable traps` コマンドでは制御できない通知タイプもあります。たとえば、一部の通知タイプは常に送信可能になっています。

例

```
Console(config)#snmp-server host 10.1.19.23 batman version 1
Console(config)#
```

関連コマンド

`snmp-server enable traps` (4-52 ページ)

4.3.5.5 `snmp-server enable traps`

このコマンドは、この装置が SNMP トラップまたは通知 (SNMP 通知) を送信できるようにするために使用します。SNMP 通知を送信不可にする場合は、`no` 形式を使用します。

構文

```
snmp-server enable traps [authentication | link-up-down]
no snmp-server enable traps [authentication | link-up-down]
```

- **authentication** — 認証エラートラップを発行するキーワードを指定します。
- **link-up-down** — リンクアップまたはリンクダウンのトラップを発行するキーワードを指定します。

デフォルト設定

認証トラップと、リンクアップおよびリンクダウントラップを発行します。

コマンドモード

グローバル設定

コマンドの使用法

`snmp-server enable traps` コマンドを実行しないと、このコマンドで制御する通知は送信されません。SNMP 通知を送信するようにこの装置を設定するには、1 つ以上の `snmp-server enable traps` コマンドを入力する必要があります。キーワードを指定しないでコマンドを実行すると、認証通知とリンクアップおよびリンクダウン通知が送信可能になります。キーワードを指定してコマンドを実行すると、そのキーワードに関連する通知タイプだけが送信可能になります。

`snmp-server enable traps` コマンドは、`snmp-server host` コマンドとともに使用します。`snmp-server host` コマンドは、SNMP 通知を受信するホストを指定するために使用します。通知を送信するには、1 つ以上の `snmp-server host` コマンドを実行する必要があります。

例

```
Console(config)#snmp-server enable traps link-up-down
Console(config)#
```

関連コマンド

`snmp-server host` (4-51 ページ)

4.3.5.6 show snmp

このコマンドは、SNMP 通信のステータスを確認するために使用します。

デフォルト設定

なし

コマンドモード

通常実行、特権実行

コマンドの使用法

このコマンドを実行すると、コミュニティアクセス文字列に関する情報、SNMP の受信および送信プロトコルデータの件数の情報、`snmp-server enable traps` コマンドによって SNMP ロギングが使用可能になっているかどうかが表示されます。

例

```
Console#show snmp

SNMP traps:
  Authentication: enable
  Link-up-down: enable

SNMP communities:
  1. private, and the privilege is read/write
  2. public, and the privilege is read-only

0 SNMP packets input
  0 Bad SNMP version errors
  0 Unknown community name
  0 Illegal operation for community name supplied
  0 Encoding errors
  0 Number of requested variables
  0 Number of altered variables
  0 Get-request PDUs
  0 Get-next PDUs
  0 Set-request PDUs
0 SNMP packets output
  0 Too big errors
  0 No such name errors
  0 Bad values errors
  0 General errors
  0 Response PDUs
  0 Trap PDUs

SNMP logging: disabled
Console#
```

4.3.6 回線コマンド

VT100 互換装置をサーバーのシリアルポートに接続すると、オンボード設定プログラムにアクセスできます。次に示すコマンドは、シリアルポートまたは **telnet** (仮想端末) の通信パラメタを設定するために使用します。

注 - シリアルインタフェースの接続パラメタは、データビット 8、ストップビット 1、パリティなし、9600 bps に固定されています。

コマンド	機能	モード	ページ
line	設定に使用する回線を指定し、回線設定モードを開始します。	GC	4-56
login	ログイン時のパスワード確認を有効にします。	LC	4-57
password	回線に対してパスワードを指定します。	LC	4-58
exec-timeout	コマンドインタプリタがユーザーからの入力を検出するまで待つ時間を設定します。	LC	4-59
password-thresh	パスワード侵害のしきい値を設定して、ログオン試行の失敗回数を制限します。	LC	4-60
silent-time*	ログオン試行の失敗回数が password-thresh コマンドで設定したしきい値を超えたあとに、管理コンソールをアクセス不可にする時間を設定します。	LC	4-61
show line	端末回線のパラメタを表示します。	NE、PE	4-62

* このコマンドは、シリアルポートでのみ適用されます。

4.3.6.1 line

このコマンドは、設定に使用する回線を指定し、回線設定コマンドの処理を開始するために使用します。

構文

line {console | vty}

- **console** – コンソール端末の回線の使用を指定します。
- **vtty** – 遠隔コンソールアクセスの仮想端末 (**telnet**) の使用を指定します。

デフォルト設定

デフォルトの回線はありません。

コマンドモード

グローバル設定

コマンドの使用法

telnet は仮想端末接続とみなされ、**show users** などの出力画面に「**Vty**」と表示されます。

例

コンソール回線モードに移行するには、次のコマンドを実行します。

```
Console(config)#line console
Console(config-line)#
```

関連コマンド

show line (4-62 ページ)
show users (4-39 ページ) [EW]

4.3.6.2 login

このコマンドは、ログイン時のパスワード確認を有効にするために使用します。パスワード確認を無効にして、パスワードなしの接続を許可する場合は、no 形式を使用します。

構文

```
login [local]  
no login
```

local — ローカルパスワード確認を有効にします。認証は、username コマンドで指定するユーザー名に基づいて行われます。

デフォルト設定

```
login local
```

コマンドモード

```
回線設定
```

コマンドの使用法

- ログイン時にスイッチが提供する認証モードには、次の 3 つがあります。
 - login を選択すると、password 回線設定コマンドで指定した単一のグローバルパスワードによって認証が行われます。この方法でログインすると、管理インタフェースは通常実行 (NE) モードで開始されます。
 - login local を選択すると、username コマンドで指定したユーザー名およびパスワードによって認証が行われます (デフォルト設定)。この方法でログインすると、管理インタフェースは、ユーザーの特権レベル (0 または 15) に応じて通常実行 (NE) モードまたは特権実行 (PE) モードで開始されます。
 - no login を選択すると、認証は行われません。この方法でログインすると、管理インタフェースは通常実行 (NE) モードで開始されます。
- このコマンドによって、スイッチを介するログイン認証を制御します。遠隔認証サーバーのユーザー名およびパスワードを設定するには、そのサーバーにインストールされている RADIUS または TACACS ソフトウェアを使用する必要があります。

例

```
Console(config-line)#login local  
Console(config-line)#
```

関連コマンド

```
username (4-25 ページ)  
password (4-58 ページ)
```

4.3.6.3 password

このコマンドは、回線のパスワードを指定するために使用します。このパスワードを削除する場合は、no 形式を使用します。

構文

```
password {0 | 7} password  
no password
```

- {0 | 7} – 0 はプレーンパスワードの入力、7 は暗号化パスワードの入力を示します。
- *password* – 回線パスワードの文字列を指定します (最大長: プレーンテキストの場合は 8 文字、暗号化テキストの場合は 32 文字、大文字小文字を区別)。

デフォルト設定

パスワードは設定されていません。

コマンドモード

回線設定

コマンドの使用法

- パスワード保護された回線で接続を開始すると、パスワードの入力を求めるプロンプトが表示されます。正しいパスワードを入力すると、システムのプロンプトが表示されます。ユーザーが不正なパスワードを複数回入力した場合に、回線接続を終了して端末をアイドル状態に戻すように設定するには、password-thresh コマンドを使用します。
- コマンド行で暗号化パスワードを指定する必要はありません。スイッチは、システム起動時に内部でオプション 7 を使用して、構成ファイルに格納されている暗号化パスワードを読み取ります。

例

```
Console(config-line)#password 0 secret  
Console(config-line)#
```

関連コマンド

login (4-57 ページ)
password-thresh (4-60 [ÉyÀ\[ÉW](#))

4.3.6.4 exec-timeout

このコマンドは、ユーザーからの入力を待つ時間を設定するために使用します。この時間が過ぎると、現在のセッションは終了します。デフォルトに戻す場合は、no 形式を使用します。

構文

```
exec-timeout [seconds]  
no exec-timeout
```

seconds - 秒数を整数で指定します (範囲 : 0 ~ 65535 秒、0 : タイムアウトなし)。

デフォルト設定

```
CLI : タイムアウトなし  
telnet : 10 分
```

コマンドモード

回線設定

コマンドの使用法

- タイムアウト時間内にユーザーからの入力を検出すると、セッションは開かれたままになります。入力が検出されなかった場合は、セッションが終了します。
- このコマンドは、シリアルコンソールと **telnet** 接続の両方に適用されます。ただし、**telnet** のタイムアウトは使用不可にできません。

例

タイムアウトを 2 分に設定するには、次のコマンドを入力します。

```
Console(config-line)#exec-timeout 120  
Console(config-line)#
```

4.3.6.5 password-thresh

このコマンドは、パスワード侵害のしきい値を設定して、ログオンの失敗回数を制限するために使用します。しきい値を削除する場合は、no 形式を使用します。

構文

```
password-thresh threshold  
no password-thresh
```

threshold – パスワードの試行を許可する回数を指定します (範囲 : 1 ~ 120、0 : しきい値なし)。

デフォルト設定

デフォルト値は、試行 3 回です。

コマンドモード

回線設定

コマンドの使用法

- コンソールポートでログオン試行のしきい値に達すると、次のログオン試行ができるようになるまで、指定した時間だけシステムインタフェースにアクセスできなくなります。アクセスを不可にする時間は、`silent-time` コマンドを使用して設定します。`telnet` でログオン試行のしきい値に達すると、`telnet` のログオンインタフェースが終了します。
- このコマンドは、ローカルコンソールと `telnet` 接続の両方に適用されます。

例

パスワードしきい値を試行 5 回に設定するには、次のコマンドを入力します。

```
Console(config-line) #password-thresh 5  
Console(config-line) #
```

関連コマンド

`silent-time` (4-61 ページ)

4.3.6.6 silent-time

このコマンドは、ログオン試行の失敗回数が password-thresh コマンドで設定されたしきい値を超えたあと、管理コンソールをアクセス不可にする時間 (サイレント時間) を設定するために使用します。サイレント時間値を削除する場合は、no 形式を使用します。

構文

```
silent-time [seconds]  
no silent-time
```

seconds — コンソールを使用不可にする秒数を指定します (範囲 : 0 ~ 65535、0 : サイレント時間なし)。

デフォルト設定

デフォルト値は、サイレント時間なしです。

コマンドモード

回線設定

例

サイレント時間を 60 秒に設定するには、次のコマンドを入力します。

```
Console(config-line)#silent-time 60  
Console(config-line)#
```

関連コマンド

password-thresh (4-60 ページ)

4.3.6.7 show line

このコマンドは、端末回線のパラメタを表示するために使用します。

構文

show line [**console** | **vty**]

- **console** – コンソール端末回線を指定します。
- **vty** – 遠隔コンソールアクセスのための仮想端末 (telnet) を指定します。

デフォルト設定

すべての回線を表示します。

コマンドモード

通常実行、特権実行

例

すべての回線の接続設定を表示するには、次のコマンドを入力します。

```
Console#show line
Console configuration:
  Password threshold: 3 times
  Interactive timeout: Disabled
  Silent time: Disabled
  Baudrate: 9600
  Databits: 8
  Parity: none
  Stopbits: 1

Vty configuration:
  Password threshold: 3 times
  Interactive timeout: 600
Console#
```

4.3.7 IP コマンド

デフォルトでは、スイッチは、DHCP を使用して IP アドレスおよびデフォルトゲートウェイ、ネットマスクを検索します。

IP アドレスは、手動で設定することも、装置を設定して BOOTP または DHCP サーバーから取得させることもできます。有効な IP アドレスは、ピリオドで区切った 0 ~ 255 の 4 つの 10 進数で構成されます。この設定ソフトウェアでは、これ以外の形式は受け入れられません。

コマンド	機能	モード	ページ
IP 設定			
<code>ip address</code>	この装置の IP アドレスを設定します。	IC	4-63
<code>ip dhcp restart</code>	BOOTP または DHCP クライアント要求を発行します。	PE	4-65
<code>ip dhcp client-identifier</code>	スイッチの DHCP クライアント識別子を指定します。システムコントローラまたはスイッチを起動するたびに、システムコントローラはスイッチにクライアント識別子を割り当てます。したがって、クライアント識別子を指定することはお勧めしません。	VC	4-66
<code>ip default-gateway</code>	帯域内管理ホストがこの装置に到達するために使用するデフォルトゲートウェイを定義します。	GC	4-67
<code>show ip interface</code>	この装置の IP 設定を表示します。	PE	4-67
<code>show ip redirects</code>	この装置に設定されているデフォルトゲートウェイを表示します。	PE	4-68
<code>ping</code>	ICMP エコー要求パケットをネットワーク上の別のノードに送信します。	NE、PE	4-69
IP パケットフィルタリング			
<code>ip filter</code>	特定の IP パケットが、ほかのスイッチポートから内部管理ポート (NETMGT) に入ることを防ぎます。	GC	4-70
<code>show ip filter</code>	フィルタルールまたは受信したパケットを表示します。	PE	4-74

4.3.7.1 ip address

このコマンドは、装置の IP アドレスを設定するために使用します。デフォルトの IP アドレスに戻す場合は、no 形式を使用します。

構文

```
ip address {ip-address netmask | bootp | dhcp}  
no ip address
```

- *ip-address* – IP アドレスを指定します。
- *netmask* – 関連付けられた IP サブネットのネットワークマスクを指定します。このマスクは、特定のサブネットへのルーティングに使用するホストアドレスビットを示すものです。
- **bootp** – BOOTP から IP アドレスを取得します。
- **dhcp** – DHCP から IP アドレスを取得します。

デフォルト設定

デフォルト設定は **dhcp** です。

コマンドモード

インタフェース設定 (VLAN)

コマンドの使用法

- IP アドレスは、手動で設定することも、装置を設定して BOOTP または DHCP サーバーから取得させることもできます。出荷時のデフォルトでは、DHCP を使用します。有効な IP アドレスは、ピリオドで区切った 0 ~ 255 の 4 つの 10 進数で構成されます。この設定プログラムは、これ以外の形式を受け入れません。
- **bootp** または **dhcp** オプションを選択した場合、IP は使用可能になりますが、BOOTP または DHCP からの応答を受信するまでは機能しません。この装置は、IP アドレスを学習する処理の中で、定期的に要求をブロードキャストします。DHCP および BOOTP の値には、IP アドレスおよびデフォルトゲートウェイ、サブネットマスクを含めることができます。
- BOOTP または DHCP への要求のブロードキャストを開始するには、`ip dhcp restart` コマンドを入力するか、スイッチを再起動します。

注 – スwitchの IP アドレスは、実際には、管理ポート (NETMGT) が含まれている VLAN の IP アドレスです。デフォルトでは、管理ポートは VLAN 2 にあります。そのため、VLAN 2 に IP アドレスを割り当てることによって、スイッチへのネットワークアクセスを設定します。IP アドレスは、管理ポートを含む VLAN にだけ割り当てる必要があります。IP アドレスを任意の VLAN に割り当てると、元の IP アドレスが無効になり、ただちに新しいアドレスが有効になります。

例

次の例では、装置に VLAN 2 内のアドレスが割り当てられます。

```
Console(config)#interface vlan 2
Console(config-if)#ip address 192.168.1.5 255.255.255.0
Console(config-if)#
```

関連コマンド

`ip dhcp restart` (4-65 ページ)

4.3.7.2 ip dhcp restart

このコマンドは、BOOTP または DHCP のクライアント要求を開始するために使用します。

デフォルト設定

なし

コマンドモード

特権実行

コマンドの使用法

- 可能な場合は、DHCP サーバーがクライアントの前回使用したアドレスを再度割り当てるように設定します。
- BOOTP または DHCP のサーバーが別のドメインに移動された場合、クライアントに提供されるアドレスのネットワーク部が新しいドメインに基づいて変更されます。

例

次の例では、装置に同じアドレスを再度割り当てています。

```
Console(config)#interface vlan 2
Console(config-if)#ip address dhcp
Console(config-if)#exit
Console#ip dhcp restart
Console#show ip interface
IP interface vlan
  IP address and netmask: 10.1.0.54 255.255.255.0 on VLAN 2,
  and address mode: DHCP.
Console#
```

関連コマンド

ip address (4-63 ページ)

4.3.7.3 ip dhcp client-identifier

このコマンドは、このスイッチの DHCP クライアント識別子を指定するために使用します。この識別子を削除する場合は、no 形式を使用します。

注 – クライアント識別子は、システムまたはスイッチを次に再起動したときに、SC によって上書きされます。ファームウェアの次のバージョンでは、client-identifier コマンドは廃止される予定です。

構文

```
ip dhcp client-identifier {text text | hex hex}  
no ip dhcp client-identifier
```

- *text* – テキスト文字列を指定します (範囲 : 1 ~ 15 文字)。
- *hex* – 16 進数の値を指定します。

デフォルト設定

DHCP クライアント識別子は、システムコントローラがスイッチをリセットするたびに、SSC のシステムコントローラによって設定されます。したがって、スイッチのコマンド行インタフェースからこの値を変更することはお勧めしません。スイッチおよびシステムシャーシのその他のコンポーネントの DHCP クライアント識別子については、『Sun Fire 1600 ブレードシステムシャーシソフトウェア設定マニュアル』を参照してください。

コマンドモード

インタフェース設定 (VLAN)

コマンドの使用法

- このコマンドは、DHCP サーバーとのすべての通信にクライアント識別子を含めるために使用します。使用するデータ型は、使用している DHCP サーバーの要件によって異なります。
- このコマンドで指定したクライアント識別子は、システムコントローラを次に再起動したときに、システムコントローラによって上書きされます。

例

```
Console(config)#interface vlan 2  
Console(config-if)#ip dhcp client-identifier hex 00-00-e8-66-65-72  
Console(config-if)#
```

関連コマンド

ip dhcp restart (4-65 ページ)

4.3.7.4 ip default-gateway

このコマンドは、装置と別のネットワークセグメントの管理ホストとの間に静的なルートを確立するために使用します。静的なルートを削除する場合は、no 形式を使用します。

構文

```
ip default-gateway gateway  
no ip default-gateway
```

gateway — デフォルトゲートウェイの IP アドレスを指定します。

デフォルト設定

静的なルータは確立されません。

コマンドモード

グローバル設定

コマンドの使用法

管理ホストが別の IP セグメントに存在する場合は、ゲートウェイを定義する必要があります。

例

次の例では、この装置のデフォルトゲートウェイを定義しています。

```
Console(config)#ip default-gateway 10.1.0.254  
Console(config)#
```

関連コマンド

show ip redirects (4-68 ページ)

4.3.7.5 show ip interface

このコマンドは、IP インタフェースの設定を表示するために使用します。

デフォルト設定

すべてのインタフェース

コマンドモード

特権実行

コマンドの使用法

このスイッチには、1つのIPアドレスだけを割り当てることができます。このアドレスは、スイッチの管理に使用されます。

例

```
Console#show ip interface
  IP address and netmask: 10.1.0.54 255.255.255.0 on VLAN 2,
  and address mode: User specified.
Console#
```

関連コマンド

`show ip redirects` (4-68 ページ)

4.3.7.6 show ip redirects

このコマンドは、この装置に設定されているデフォルトゲートウェイを表示するために使用します。

デフォルト設定

なし

コマンドモード

特権実行

例

```
Console#show ip redirects
ip default gateway 10.1.0.254
Console#
```

関連コマンド

`ip default-gateway` (4-67 ページ)

4.3.7.7 ping

このコマンドは、ネットワーク上の別のノードに ICMP エコー要求パケットを送信するために使用します。

構文

ping *host* [**count** *count*][**size** *size*]

- *host* — ホストの IP アドレスを指定します。
- *count* — 送信するパケット数を指定します (範囲: 1 ~ 16、デフォルト: 5)。
- *size* — パケット内のバイト数を指定します (範囲: 32 ~ 512、デフォルト: 32)。スイッチによってヘッダー情報が追加されるため、実際のパケットサイズは、指定したサイズよりも 8 バイト大きくなります。

デフォルト設定

このコマンドには、ホストに対するデフォルトはありません。

コマンドモード

通常実行、特権実行

コマンドの使用法

- ping コマンドは、ネットワーク上の別のサイトに到達できるかどうかを確認するために使用します。
- 次に、ping コマンドを使用した場合の結果の一部を示します。
 - 正常な応答 — 正常な応答は、ネットワークトラフィックに応じて 1 ~ 10 秒以内に返ります。
 - 宛先が応答しない — ホストが応答しない場合は、「**timeout**」と表示されます。
 - 宛先に到達できない — この宛先へのゲートウェイが、宛先に到達できないことを示しました。
 - ネットワークまたはホストに到達できない — ゲートウェイのルートテーブル内に対応するエントリがありませんでした。
- ping を停止するには、Esc キーを押します。

例

```
Console#ping 10.1.0.19
Type Ctrl-C to abort.
PING to 10.1.0.19, by 5 32-byte payload ICMP packets, timeout is 5
seconds
response time: 0 ms
response time: 0 ms
response time: 10 ms
response time: 10 ms
response time: 10 ms
Ping statistics for 10.1.0.19:
 5 packets transmitted, 5 packets received (100%), 0 packets lost (0%)
Approximate round trip times:
  Minimum = 0 ms, Maximum = 10 ms, Average = 6 ms
Console#
```

4.3.7.8 ip filter

このコマンドは、特定の IP パケットがダウンリンクポートから内部管理ポートに到達することを防ぐために使用します。フィルタテーブルからルールを削除する場合は、no 形式を使用します。

構文

```
ip filter [rule-number] action protocol {source source-bitmask}
{destination destination-bitmask} [fragments] [log]
```

ポート番号は確認しません。fragments オプションを指定できます。

```
ip filter [rule-number] action protocol {source source-bitmask} [source-port-range]
{destination destination-bitmask} [destination-port-range] [log]
```

ポート番号を確認します。つまり、source-port-range または destination-port-range を指定した場合は、fragments オプションを指定できません。

```
ip filter [rule-number] action tcp {source source-bitmask} [source-port-range]
{destination destination-bitmask} [destination-port-range]
[code {{code code-bitmask} | code-keyword-seq}] [log]
```

tcp キーワードを確認します。このキーワードがあれば、code オプションを指定できます。

```
no ip filter {all | rule-number}
```

指定したルール番号をフィルタテーブルから削除します。

- **rule-number** – テーブルの指定した位置にフィルタールールを挿入し、その位置以降に設定されていた内容があればテーブル内の下の場所に移動させます。**rule-number** に、テーブル内で次に使用できる番号より大きい数字を指定することはできません。ルール番号を指定しないと、新しい内容は、ルールテーブルの終わりに追加されます。ルールの最大数は 128 です。
- **action** – {**deny** | **permit**}
ダウンリンクポートと管理ポート (NETMGT) の間のパケットの送信をブロックまたは許可します。
- **protocol** – {**any** | **tcp** | **udp** | **number**}
任意のプロトコルまたは TCP、UDP、特定のプロトコル番号 (0 ~ 255) を指定します。
- **source source-bitmask** – フレームの送信元アドレスおよびネットマスクを指定します。
- **source-port-range** – [**number** | **start_number-end_number**]
TCP または UDP の送信元ポートまたはポート範囲を指定します (範囲 : 0 ~ 65535)。
- **destination destination-bitmask** – フレームの送信先アドレスおよびネットマスクを指定します。
- **destination-port-range** – [**number** | **start_number-end_number**]
TCP または UDP の送信先ポートまたはポート範囲を指定します (範囲 : 0 ~ 65535)。
- **code**
 - **code** – TCP ヘッダーの 14 バイト目のフラグビットを指定する 10 進数の数字 (ビット文字列) を指定します (範囲 : 0 ~ 63)。
 - **code-bitmask** – コードに適用する 10 進数 (ビットマスク) を指定します。有効にするビットには 2 進数のビット「1」を、無視するビットには「0」を設定して、それと等価の 10 進数を入力します。次の各ビットを指定できます。
 - 1 (**fin**) – 完了
 - 2 (**syn**) – 同期
 - 4 (**rst**) – リセット
 - 8 (**psh**) – プッシュ
 - 16 (**ack**) – 承認
 - 32 (**urg**) – 緊急ポインタ
 - **code-keyword-seq** – コードキーワードとして、**fin** | **syn** | **rst** | **psh** | **ack** | **urg** を指定できます。この順序で指定する必要があります。コードキーワードは、指定するとオンになり、指定しないとオフになります。
- **fragments** – ルールは、More Fragments (MF) ビットが設定されているパケットまたはフラグメントオフセットが 0 より大きいパケットにのみ適用されます。フラグメントを設定しない場合は、フラグメントパケットとフラグメントなしのパケットの両方に適用されます。
- **log** – 一致したパケットをログバッファに記録します。ログバッファに格納できるエントリの最大数は 64 です。バッファがいっぱいになると、先頭に戻ってもっとも古いエントリが上書きされます。ログは RAM に格納されているため、スイッチをリセットすると消去されます。

デフォルト設定

なし

コマンドモード

グローバル設定

コマンドの使用法

- デフォルトでは、ダウンリンクポートから管理ポート (NETMGT) への通過を許可された IP パケットはありません。サーバブレードから管理ポート (NETMGT) を介して管理ネットワークにアクセスする必要がある場合は、ダウンリンクポートから管理ポートへの特定のフレームの通過を許可するようにフィルタを設定します。アップリンクポートから管理ポートへのトラフィックは許可されません。
- フラグメントとは、MF (More Fragments) = 1 またはフラグメントオフセット > 0 のパケットです。fragments キーワードがルールに指定されていない場合は、フラグメントパケットとフラグメントなしパケットの両方がルールによって確認されます。
- コード値およびマスクを指定する場合は、 $\langle \text{value in header} \rangle \& \langle \text{mask} \rangle == \langle \text{value} \rangle \& \langle \text{mask} \rangle$ の論理式でパケットの一致を判断します。たとえば、次のフラグが設定されたパケットを得るには、次に示すコード値およびマスクを使用します。
 - SYN フラグが有効: 「code 2 2」を使用
 - SYN と ACK の両方が有効: 「code 18 18」を使用
 - SYN が有効で ACK が無効: 「code 2 18」を使用

例 - アドレスフィルタ

次に、すべてのパケットがフィルタを通過するように、すべてのプロトコルタイプを許可し、送信元と送信先の両方のアドレスに空アドレスおよびネットワークマスクを指定する例を示します。

```
Console(config)#ip filter permit any 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
Console(config)#
```

次に、送信元アドレスがサブネット 10.7.1.x 内にあるすべての受信パケットを受け入れる例を示します。たとえば、ルールに一致した場合、つまりルール (10.7.1.1 & 255.255.255.0) がマスクされたアドレス (10.7.1.2 & 255.255.255.0) と等しい場合は、パケットが通過します。

```
Console(config)#ip filter permit any 10.7.1.1 255.255.255.0 0.0.0.0
0.0.0.0
Console(config)#
```

例 - フラグメントの確認

この例では、すべてのフラグメントがブロックされ、一致したパケットがログに記録されます。

```
Console(config)#ip filter deny any 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
fragment log
Console(config)#
```

例 - コード値の確認

この例では、SYN が設定されているクラス C アドレス 192.168.1.0 からのすべての TCP パケットがブロックされます。

```
Console(config)#ip filter deny tcp 192.168.1.0 255.255.255.0 0.0.0.0
0.0.0.0 code syn
Console(config)#
```

この例でも、SYN が設定されているクラス C アドレス 192.168.1.0 からのすべての TCP パケットがブロックされます。

```
Console(config)#ip filter deny tcp 192.168.1.0 255.255.255.0 0.0.0.0
0.0.0.0 code 2 2
Console(config)#
```

例 - ポート番号の確認

この例では、クラス C アドレス 192.168.1.0 から送信先ポート 80 が設定された任意の場所への TCP パケットが許可されます。

```
Console(config)#ip filter permit tcp 192.168.1.0 255.255.255.0 0.0.0.0
0.0.0.0 80
Console(config)#
```

この例では、送信元ポートが 30 ~ 46、送信先ポートが 100 ~ 2000 の、送信元 10.7.1.1 から送信先 10.8.1.1 へのすべての TCP パケットが破棄されます。

```
Console(config)#ip filter deny tcp 10.7.1.1 255.255.255.255 30-46
10.8.1.1 255.255.255.255 100-2000
Console(config)#
```

4.3.7.9 show ip filter

このコマンドは、IP フィルタテーブル内のすべてのルールを表示するために使用します。

構文

show ip filter [*rule-number* | **log**]

- **rule-number** – テーブル内の指定した場所にあるフィルタルールを表示します (範囲: 1 ~ 128)。
- **log** – ログバッファに格納されているすべてのパケットを表示します。このバッファに格納されているパケットは、必ずフィルタテーブル内のルールに一致しています。ログバッファに格納されるエントリの最大数は 64 です。

オプションを指定しない場合は、ログバッファ内のすべてのパケットが表示されます。

デフォルト設定

なし

コマンドモード

特権実行

例

この例では、ルールが 1 つだけ設定されていて、サブネット 10.1.0.x 内のパケットが管理ポートとダウンリンクポートの間を通過できるようになっています。

```
Console#show ip filter
Ip filter:
Rule:1, Action: permit, Protocol: any, Log: disable, Fragments: disable
Source: 10.1.0.0 255.255.255.0 any
Destination: 10.1.0.0 255.255.255.0 any
```

4.3.8 インタフェースコマンド

次のコマンドは、Ethernet ポートまたは集約リンク、VLAN の通信パラメタの表示および設定に使用します。

コマンド	機能	モード	ページ
interface	インタフェースタイプを設定し、インタフェース設定モードを開始します。	GC	4-75
description	インタフェース設定に説明を追加します。	IC	4-76
speed-duplex	自動ネゴシエーションが使用不可の場合に、指定されたインタフェースの速度およびデュプレックス動作を設定します。	IC	4-77
negotiation	指定されたインタフェースの自動ネゴシエーションを使用可能にします。	IC	4-78
capabilities	自動ネゴシエーションで使用するために指定されたインタフェースの機能を通知します。	IC	4-79
flowcontrol	指定されたインタフェースのフロー制御を使用可能にします。	IC	4-81
shutdown	インタフェースを使用不可にします。	IC	4-82
switchport broadcast packet-rate	ブロードキャストストーム制御しきい値を設定します。	IC	4-83
clear counters	インタフェースの統計情報を消去します。	PE	4-84
show interfaces status	指定されたインタフェースのステータスを表示します。	NE、PE	4-84
show interfaces counters	指定されたインタフェースの統計情報を表示します。	NE、PE	4-85
show interfaces switchport	インタフェースの管理ステータスおよび動作ステータスを表示します。	NE、PE	4-87

4.3.8.1 interface

このコマンドは、インタフェースのタイプを設定して、インタフェース設定モードを開始するために使用します。

構文

```
interface interface  
no interface port-channel channel-id  
interface
```

- **ethernet** *port-name*
port-name – ダウンリンク : SNP0 ~ 15、アップリンク : NETP0 ~ 7、
 管理 : NETMGT
- **port-channel** *channel-id* (範囲 : 1 ~ 6)
- **vlan** *vlan-id* (範囲 : 1 ~ 4094)

デフォルト設定

なし

コマンドモード

グローバル設定

例

最初のアップリンクポートを指定する場合は、次のコマンドを入力します。

```
Console(config)#interface ethernet NETP0
Console(config-if)#
```

4.3.8.2 description

このコマンドは、インタフェースに説明を追加するために使用します。説明を削除する場合は、no 形式を使用します。

構文

description *string*
no description

string – このインタフェースの接続先を示すコメントまたは説明を指定します
 (範囲 : 1 ~ 64 文字)。

デフォルト設定

NETP0 ~ 7 : External RJ-45 connector NET0 ~ 7
 SNP0 ~ 15 : Blade Slot 0 ~ 15
 NETMGT : External RJ-45 connector NETMGT

コマンドモード

インタフェース設定 (Ethernet、Port Channel)

例

次に、ダウンリンクポート SNP5 の説明を設定する例を示します。

```
Console(config)#interface ethernet SNP5
Console(config-if)#description RD-SW#3
Console(config-if)#
```

4.3.8.3 speed-duplex

このコマンドは、自動ネゴシエーションが使用不可のときに、指定されたインタフェースの速度およびデュプレックスモードを設定するために使用します。デフォルトに戻す場合は、no 形式を使用します。

構文

```
speed-duplex {1000full | 100full | 100half | 10full | 10half}  
no speed-duplex
```

- **1000full** – 1000 Mbps 全二重動作を強制
- **100full** – 100 Mbps 全二重動作を強制
- **100half** – 100 Mbps 半二重動作を強制
- **10full** – 10 Mbps 全二重動作を強制
- **10half** – 10 Mbps 半二重動作を強制

デフォルト設定

- 自動ネゴシエーションは、デフォルトで使用可能になっています。
- 自動ネゴシエーションが使用不可の場合の speed-duplex のデフォルト設定は、Fast Ethernet ポートでは 100full、Gigabit Ethernet ポートでは 1000full です。

注 – 自動ネゴシエーションを使用不可にした場合は、アップリンクポートに 10 Mbps または 100 Mbps だけを設定できます。ポートを 1 Gbps 全二重で動作させる場合は、自動ネゴシエーションを使用可能にして、ポートの伝送速度に 1000full だけを設定します。

コマンドモード

インタフェース設定 (Ethernet、Port Channel)

コマンドの使用法

- 動作を speed-duplex コマンドで指定した速度およびデュプレックスモードに制限する場合は、no negotiation コマンドを使用して、選択したインタフェースの自動ネゴシエーションを使用不可にします。ただし、ダウンリンクポートの自動ネゴシエーションを使用不可にすることはできません。ダウンリンクポートは、1000 Mbps 全二重に固定されています。
- negotiation コマンドを使用して自動ネゴシエーションを使用可能にすると、capabilities コマンドの指定に基づいて最適な設定が行われます。自動ネゴシエーションの環境下で速度およびデュプレックスモードを設定するには、インタフェースの capabilities リストに必要なモードを指定する必要があります。

例

次に、ポート NETP5 を 100 Mbps、半二重動作に設定する例を示します。

```
Console(config)#interface ethernet NETP5
Console(config-if)#no negotiation
Console(config-if)#speed-duplex 100half
Console(config-if)#
```

関連コマンド

negotiation (4-78 ページ)
capabilities (4-79 ページ)

4.3.8.4 negotiation

このコマンドは、指定されたインタフェースの自動ネゴシエーションを使用可能にするために使用します。自動ネゴシエーションを使用不可にする場合は、no 形式を使用します。

構文

negotiation
no negotiation

デフォルト設定

使用可能

コマンドモード

インタフェース設定 (Ethernet、Port Channel)

コマンドの使用法

- ダウンリンクポート SNP0 ~ 15 の自動ネゴシエーションは、使用不可に固定されています。
- 自動ネゴシエーションを使用可能にした場合は、スイッチによって capabilities コマンドに基づく最適なリンク設定のネゴシエーションが行われます。自動ネゴシエーションを使用不可にした場合は、speed-duplex コマンドおよび flowcontrol コマンドを使用してリンク属性を手動で設定する必要があります。
- 自動ネゴシエーションが使用不可の場合は、アップリンクポートの MDI/MDI-X ピン配列の自動設定も使用不可になります。

例

次に、自動ネゴシエーションを使用するようにポート SNP11 を設定する例を示します。

```
Console(config)#interface ethernet SNP11
Console(config-if)#negotiation
Console(config-if)#
```

関連コマンド

capabilities (4-79 ページ)
speed-duplex (4-77 ページ)
flowcontrol (4-81 ページ)

4.3.8.5 capabilities

このコマンドは、自動ネゴシエーション中に、指定されたインタフェースのポート伝送速度を通知するために使用します。通知を停止する場合はパラメタを指定する no 形式を、デフォルト値に戻す場合はパラメタを指定しない no 形式を使用します。

構文

```
capabilities {1000full | 100full | 100half | 10full | 10half |
flowcontrol | symmetric}
no port-capabilities [1000full | 100full | 100half | 10full |
10half | flowcontrol | symmetric]
```

- **1000full** – 1000 Mbps 全二重動作をサポート
- **100full** – 100 Mbps 全二重動作をサポート
- **100half** – 100 Mbps 半二重動作をサポート
- **10full** – 10 Mbps 全二重動作をサポート
- **10half** – 10 Mbps 半二重動作をサポート
- **flowcontrol** – フロー制御をサポート
- **symmetric** (Gigabit 専用) – 指定すると、ポートでポーズフレームが送受信されます。指定しないと、ポートによって自動ネゴシエーションが行われ、非対称ポーズフレームの送信側および受信側が判別されます。現在のスイッチ ASIC は、対称ポーズフレームだけをサポートしています。

デフォルト設定

NETMGT : 10half、10full、100half、100full
NETP0 ~ 7 : 10half、10full、100half、100full、1000full、flowcontrol
SNP0 ~ 15 : 1000full

コマンドモード

インタフェース設定 (Ethernet、Port Channel)

コマンドの使用法

- SNP0 ~ 15 ダウンリンクポートの伝送速度は、1000full に固定されています。
- NETP0 ~ 7 アップリンクポートの伝送速度には、10half または 10full、100half、100full、1000full、flowcontrol、symmetric を指定します。negotiation コマンドによって自動ネゴシエーションを使用可能にした場合は、スイッチによって capabilities コマンドに基づく最適なリンク設定のネゴシエーションが行われます。自動ネゴシエーションを使用不可にした場合は、speed-duplex コマンドおよび flowcontrol コマンドを使用してリンク属性を手動で設定する必要があります。
- NETMGT ポートの伝送速度は、10half および 10full、100half、100full に固定されています。

例

次に、ポート NETP5 の伝送速度を 100half および 100full、flowcontrol に設定する例を示します。

```
Console(config)#interface ethernet NETP5
Console(config-if)#no capabilities 10half
Console(config-if)#no capabilities 10hfull
Console(config-if)#no capabilities 1000full
Console(config-if)#capabilities 100half
Console(config-if)#capabilities 100full
Console(config-if)#capabilities flowcontrol
Console(config-if)#
```

関連コマンド

negotiation (4-78 ページ)
speed-duplex (4-77 ページ)
flowcontrol (4-81 ページ)

4.3.8.6 flowcontrol

このコマンドは、フロー制御を使用可能にするために使用します。フロー制御を使用不可にする場合は、no 形式を使用します。

注 – Sun Fire B1600 ブレードシステムシャーシの統合スイッチは、相互に接続する 2 つのスイッチチップで構成されています。使用可能にできるのは、同じスイッチチップ上の 2 つのポート間のフロー制御だけです。ポート NETP0 および NETP1、NETP4、NETP5、SNP8 ~ 15 は、一方のスイッチチップ上にあります。ポート NETP2 および NETP3、NETP6、NETP7、SNP0 ~ 7 は、もう一方のスイッチチップ上にあります (SSC の背面パネルの右側にあるすべてのポートが一方のチップ上に、左側にあるすべてのポートがもう一方のチップ上にあります)。

構文

```
flowcontrol  
no flowcontrol
```

デフォルト設定

フロー制御は使用可能

コマンドモード

インタフェース設定 (Ethernet、Port Channel)

コマンドの使用法

- フロー制御は、バッファがいっぱいになったときに、スイッチに直接接続されたエンドステーションまたはセグメントからのトラフィックを「ブロッキング」することでフレーム損失を防ぎます。使用可能にすると、半二重動作にはバックプレッシャーが、全二重動作には IEEE 802.3x が使用されます。
- flowcontrol コマンドまたは no flowcontrol コマンドを使用してフロー制御を強制的にオンまたはオフにする場合は、no negotiation コマンドを使用して、選択したインタフェースの自動ネゴシエーションを使用不可にします。
- negotiation コマンドを使用して自動ネゴシエーションを使用可能にすると、capabilities コマンドの指定に基づいて最適な設定が行われます。自動ネゴシエーションの環境下でフロー制御を使用可能にするには、すべてのポートの capabilities リストに flowcontrol を指定する必要があります。
- ハブに接続するポートでは、問題の解決に必要な場合を除き、フロー制御を使用しないでください。ハブに接続するポートでフロー制御を使用すると、バックプレッシャーの妨害信号によって、ハブに接続されたセグメントの全体的な性能が低下することがあります。

例

次に、ポート NETP7 のフロー制御を使用可能にする例を示します。

```
Console(config)#interface ethernet NETP7
Console(config-if)#flowcontrol
Console(config-if)#no negotiation
Console(config-if)#
```

関連コマンド

negotiation (4-78 ページ)

capabilities (flowcontrol、symmetric) (4-79 ページ)

4.3.8.7 shutdown

このコマンドは、インタフェースを使用不可にするために使用します。インタフェースを使用不可にする場合は、no 形式を使用します。

構文

```
shutdown
no shutdown
```

デフォルト設定

すべてのインタフェースが使用可能

コマンドモード

インタフェース設定 (Ethernet、Port Channel)

コマンドの使用法

このコマンドを使用すると、衝突が多すぎるなどの動作が異常なポートを使用不可にして、問題の解決後に再び使用可能にできます。また、セキュリティーのためにポートを使用不可にすることもできます。

例

次に、Ethernet ポート SNP5 を使用不可にする例を示します。

```
Console(config)#interface ethernet SNP5
Console(config-if)#shutdown
Console(config-if)#
```

4.3.8.8 switchport broadcast packet-rate

このコマンドは、ブロードキャストストーム制御を設定するために使用します。ブロードキャストストーム制御を使用不可にする場合は、no 形式を使用します。

構文

```
switchport broadcast packet-rate rate  
no switchport broadcast
```

rate – 1 秒あたりのパケット数で表したしきい値レベル (範囲 : 16、64、128、256)

デフォルト設定

すべてのポートでブロードキャストストーム制御が使用可能
256 パケット/秒

コマンドモード

インタフェース設定 (Ethernet)

コマンドの使用法

- ブロードキャストトラフィックが指定されたしきい値を超えると、しきい値を超えたパケットは廃棄されます。
- このコマンドを使用すると、選択したインタフェースのブロードキャストストーム制御を使用可能または使用不可に設定できます。指定されたしきい値は、スイッチ全体に適用されます。
- ダウンリンクポート SNP0 ~ 15 のブロードキャストストーム制御は、使用可能に固定されています。

例

次に、ブロードキャスト制御のしきい値を 64 パケット/秒に設定する例を示します。

```
Console(config)#interface ethernet SNP5  
Console(config-if)#switchport broadcast packet-rate 64  
Console(config-if)#
```

注 – switchport broadcast コマンドを実行すると、指定したインタフェースのブロードキャストストーム制御が使用可能になりますが、ブロードキャストしきい値はスイッチのすべてのインタフェースに設定されます。

4.3.8.9 clear counters

このコマンドは、インタフェースの統計情報を消去するために使用します。

構文

clear counters *interface*

interface – **ethernet** *port-name*

port-name – ダウンリンク : SNP0 ~ 15、アップリンク : NETP0 ~ 7、
管理 : NETMGT

デフォルト設定

なし

コマンドモード

特権実行

コマンドの使用法

統計情報は、電源をリセットしたときにだけ初期化されます。このコマンドを実行すると、現在の管理セッションに表示される統計情報の基本値が 0 になります。ただし、ログアウトして管理インタフェースに戻ると、表示される統計情報は、最後に電源をリセットした時点から累積された絶対値になります。

例

次に、ポート SNP5 の統計情報を消去する例を示します。

```
Console#clear counters ethernet SNP5
Console#
```

4.3.8.10 show interfaces status

このコマンドは、インタフェースのステータスを表示するために使用します。

構文

show interfaces status [*interface*]

interface

■ **ethernet** *port-name*

port-name – ダウンリンク : SNP0 ~ 15、アップリンク : NETP0 ~ 7、
管理 : NETMGT

■ **port-channel** *channel-id* (範囲 : 1 ~ 6)

■ **vlan** *vlan-id* (範囲 : 1 ~ 4094)

デフォルト設定

すべてのインタフェースのステータスが表示されます。

コマンドモード

通常実行、特権実行

コマンドの使用法

インタフェースを指定しない場合は、すべてのインタフェースの情報が表示されます。このコマンドによって表示される項目の詳細は、3-80 ページの「接続ステータスの表示」を参照してください。

例

```
Console#show interfaces status ethernet SNP11
Information of SNP11
Basic information:
  Port type: 1000SX
  Mac address: 00-00-e8-00-00-0a
Configuration:
  Name: Blade Slot 11
  Port admin status: Up
Speed-duplex: Auto
  Capabilities: 1000full,
Broadcast storm status: Enabled
  Broadcast storm limit: 256 packets/second
  Flow control status: Enabled
  LACP status: Disabled
Current status:
  Link status: Down
  Operation speed-duplex: 1000full
  Flow control type: Dot3X
Console#
```

4.3.8.11 show interfaces counters

このコマンドは、インタフェースの統計情報を表示するために使用します。

構文

```
show interfaces counters [interface]
```

interface

- **ethernet** *port-name*

port-name – ダウンリンク : SNP0 ~ 15、アップリンク : NETP0 ~ 7、
管理 : NETMGT

- **port-channel** *channel-id* (範囲 : 1 ~ 6)

デフォルト設定

すべてのインタフェースのカウンタが表示されます。

コマンドモード

通常実行、特権実行

コマンドの使用法

インタフェースを指定しない場合は、すべてのインタフェースの情報が表示されます。このコマンドによって表示される項目の詳細は、3-116 ページの「ポートの統計情報の表示」を参照してください。

例

```
Console#show interfaces counters ethernet NETP7
NETP7:
  Iftable stats:
    Octets input: 19648, Octets output: 714944
    Unicast input: 0, Unicast output: 0
    Discard input: 0, Discard output: 0
    Error input: 0, Error output: 0
    Unknown protos input: 0, QLen output: 0
  Extended iftable stats:
    Multi-cast input: 0, Multi-cast output: 10524
    Broadcast input: 136, Broadcast output: 0
  Ether-like stats:
    Alignment errors: 0, FCS errors: 0
    Single Collision frames: 0, Multiple collision frames: 0
    SQE Test errors: 0, Deferred transmissions: 0
    Late collisions: 0, Excessive collisions: 0
    Internal mac transmit errors: 0, Internal mac receive errors: 0
    Frame too longs: 0, Carrier sense errors: 0
  RMON stats:
    Drop events: 0, Octets: 734720, Packets: 10661
    Broadcast pkts: 136, Multi-cast pkts: 10525
    Undersize pkts: 0, Oversize pkts: 0
    Fragments: 0, Jabbers: 0
    CRC align errors: 0, Collisions: 0
    Packet size <= 64 octets: 9877, Packet size 65 to 127 octets: 93
    Packet size 128 to 255 octets: 691, Packet size 256 to 511 octets: 0
    Packet size 512 to 1023 octets: 0, Packet size 1024 to 1518 octets: 0
Console#
```

4.3.8.12 show interfaces switchport

このコマンドは、インタフェースの拡張設定情報を表示するために使用します。

構文

```
show interfaces switchport [interface]
```

interface

- **ethernet** *port-name*

port-name — ダウンリンク : SNP0 ~ 15、アップリンク : NETP0 ~ 7、
管理 : NETMGT

- **port-channel** *channel-id* (範囲 : 1 ~ 6)

デフォルト設定

すべてのインタフェースが表示されます。

コマンドモード

通常実行、特権実行

コマンドの使用法

インタフェースを指定しない場合は、すべてのインタフェースの情報が表示されます。このコマンドによって、次の項目が表示されます。

- **Broadcast threshold** — ブロードキャストストーム制御が使用可能または使用不可のいずれに設定されているかを示し、使用可能に設定されている場合はしきい値レベルも示します (4-83 ページ)。
- **Lacp status** — Link Aggregation Control Protocol が使用可能または使用不可のいずれに設定されているかを示します (4-150 ページ)。
- **VLAN membership mode** — メンバーシップモードが Trunk または Hybrid のいずれに設定されているかを示します (4-111 ページ)。
- **Ingress rule** — イングレスフィルタリングが使用可能または使用不可のいずれに設定されているかを示します (4-113 ページ)。
- **Acceptable frame type** — すべての種類の VLAN フレームが許可されているか、タグ付きフレームだけが許可されているかを示します (4-112 ページ)。
- **Native VLAN** — デフォルトのポート VLAN ID を示します (4-114 ページ)。
- **Priority for untagged traffic** — タグなしフレームのデフォルトの優先順位を示します (4-136 ページ)。
- **Gvrp status** — GARP VLAN Registration Protocol が使用可能または使用不可のいずれに設定されているかを示します (4-118 ページ)。
- **Allowed vlan** — このインタフェースが参加している VLAN を示します。「(u)」はタグなし、「(t)」はタグ付きを示します (4-115 ページ)。
- **Forbidden vlan** — このインタフェースが GVRP を介して動的に参加できない VLAN を示します (4-116 ページ)。

例

次に、Ethernet ポート NETP7 の設定の例を示します。

```
Console#show interfaces switchport ethernet NETP7
Information of NETP7
Broadcast threshold: Enabled, 256 packets/second
Lacp status: Enabled
VLAN membership mode: Hybrid
Ingress rule: Disabled
Acceptable frame type: All frames
Native VLAN: 1
Priority for untagged traffic: 0
Gvrp status: Enabled
Allowed Vlan: 1(u),
Forbidden Vlan: 2,
Console#
```

4.3.9 アドレステーブルコマンド

次のコマンドは、特定のアドレスをフィルタリングするアドレステーブルの設定、および現在のエントリの表示、消去、有効期限の設定を行うために使用します。

コマンド	機能	モード	ページ
mac-address-table static	静的アドレスを VLAN のポートに割り当てます。	GC	4-89
clear mac-address-table dynamic	学習したエントリを転送用のデータベースから削除します。	PE	4-90
show mac-address-table	ブリッジ転送用のデータベースのエントリを表示します。	PE	4-90
mac-address-table aging-time	アドレステーブルの有効期限を設定します。	GC	4-91
show mac-address-table aging-time	アドレステーブルの有効期限を表示します。	PE	4-92

4.3.9.1 mac-address-table static

このコマンドは、宛先ポートに静的アドレスを割り当てるために使用します。アドレスを削除する場合は、no 形式を使用します。

構文

```
mac-address-table static mac-address {interface interface}
vlan vlan-id [action]
no mac-address-table static mac-address vlan vlan-id
```

- *mac-address* – MAC アドレス
- *interface*
 - **ethernet** *port-name*
port-name – ダウンリンク : SNP0 ~ 15、アップリンク : NETP0 ~ 7、管理 : NETMGT
 - **port-channel** *channel-id* (範囲 : 1 ~ 6)
- *vlan-id* – VLAN ID (範囲 : 1 ~ 4094)
- *action* –
 - **permanent** – 永続的な割り当て
 - **delete-on-reset** – スイッチをリセットするまでの割り当て

デフォルト設定

静的アドレスは定義されていません。デフォルトモードは **permanent** です。

コマンドモード

グローバル設定

コマンドの使用法

- 特定の VLAN 内の特定のポートに、ホスト装置の静的アドレスを割り当てることができます。このコマンドは、MAC アドレステーブルに静的アドレスを追加するために使用します。静的アドレスの特性は、次のとおりです。
 - 指定したインタフェースリンクがダウンしていると、静的アドレスはそのアドレステーブルから削除されません。
 - 静的アドレスは、割り当てられたインタフェースに固定されて移動しません。指定した静的アドレスがほかのインタフェースに割り当てられている場合、その静的アドレスは無視されて、アドレステーブルに書き込まれません。
 - このコマンドの no 形式を使用して静的アドレスを削除するまで、別のポートがそのアドレスを学習することはできません。

例

```
Console(config)#mac-address-table static 00-e0-29-94-34-de
ethernet SNP1 vlan 1 delete-on-reset
Console(config)#
```

4.3.9.2 clear mac-address-table dynamic

このコマンドは、学習したエントリを転送用のデータベースから削除し、静的エントリまたはシステムによって設定されたエントリの送受信数を消去するために使用します。

デフォルト設定

なし

コマンドモード

特権実行

例

```
Console#clear mac-address-table dynamic
Console#
```

4.3.9.3 show mac-address-table

このコマンドは、ブリッジ転送用データベース内のエントリのクラスを表示するために使用します。

構文

```
show mac-address-table [address mac-address [mask]] [interface interface] [vlan vlan-id] [sort {address | vlan | interface}]
```

- *mac-address* – MAC アドレス
- *mask* – アドレス内の無視するビット
- *interface*
 - **ethernet** *port-name*
port-name – ダウンリンク : SNP0 ~ 15、アップリンク : NETP0 ~ 7、管理 : NETMGT
 - **port-channel** *channel-id* (範囲 : 1 ~ 6)
- *vlan-id* – VLAN ID (範囲 : 1 ~ 4094)
- **sort** – アドレスまたは VLAN、インタフェースによるソート

デフォルト設定

なし

コマンドモード

特権実行

コマンドの使用法

MAC アドレステーブルには、各インタフェースに関連付けられた MAC アドレスが格納されています。Type フィールドには、次のタイプが表示されます。

- Learned — 動的なアドレスエントリ
- Permanent — 静的エントリ
- Delete-on-reset — システムのリセット時に削除される静的エントリ

例

```
Console#show mac-address-table
Interface Mac Address      Vlan Type
-----
          SNP11 00-10-b5-62-03-74    1 Learned
Console#
```

4.3.9.4 mac-address-table aging-time

このコマンドは、アドレステーブル内のエントリの有効期限を設定するために使用します。デフォルトの有効期限に戻す場合は、no 形式を使用します。

構文

```
mac-address-table aging-time seconds
no mac-address-table aging-time
```

seconds — 秒単位の時間 (18 ~ 2184)

デフォルト設定

300 秒

コマンドモード

グローバル設定

コマンドの使用法

有効期限は、動的に学習した転送情報を一定期間のあと無効にするために使用します。

例

```
Console(config)#mac-address-table aging-time 300
Console(config)#
```

4.3.9.5 show mac-address-table aging-time

このコマンドは、アドレステーブル内のエントリの有効期限を表示するために使用します。

デフォルト設定

なし

コマンドモード

特権実行

例

```
Console#show mac-address-table aging-time
Aging time: 300 sec.
Console#
```

4.3.10 ポートセキュリティーコマンド

次のコマンドを使用すると、学習機能を使用不可にして、ポートのセキュリティー保護されたアドレスを手動で指定できます。初期の学習期間中は、ポートセキュリティーをオフにして (学習機能を使用可能にして) 選択したポートに現在の VLAN メンバーをすべて登録してから、ポートセキュリティーを使用可能にし、未知の送信元 MAC アドレスや別のポートから学習した送信元 MAC アドレスを持つ受信フレームを廃棄できます。

コマンド	機能	モード	ページ
port security	セキュリティー保護されたポートを設定します。	IC	4-93
mac-address-table static	静的アドレスを VLAN のポートに割り当てます。	GC	4-89
show mac-address-table	ブリッジ転送用データベースのエントリを表示します。	PE	4-90

4.3.10.1 port security

このコマンドは、セキュリティー保護されたポートを設定するために使用します。ポートセキュリティーを無効にする場合は、no 形式を使用します。

構文

```
port security
no port security
```

デフォルト設定

すべてのポートセキュリティーが使用不可

コマンドモード

インタフェース設定 (Ethernet)

コマンドの使用法

- ポートセキュリティーを使用可能にすると、スイッチは、指定されたポートでの新しいアドレスの動的な学習を停止します。動的または静的アドレステーブル内に保存されている送信元アドレスを持つ受信トラフィックだけが受け入れられます。
- ポートセキュリティーを使用するには、まず、初期の学習期間中としてポートが受信したフレームの <送信元 MAC アドレス、VLAN> の組をスイッチに動的に学習させてから、ポートセキュリティーを使用可能にしてアドレスの学習を停止します。学習機能を使用可能にする期間は十分にとって、選択したポートに有効な VLAN メンバーがすべて登録されるようにしてください。
- あとで新しい VLAN メンバーを追加する場合は、`mac-address-table static` コマンドを使用してセキュリティー保護されたアドレスを手動で追加するか、ポートセキュリティーをオフに設定して、新しい VLAN メンバーを登録するために必要な期間だけ学習機能を再び使用可能にします。安全のため、必要に応じて、学習機能を再び使用不可にします。
- セキュリティー保護されたポートには、次の制限があります。
 - ポートの監視機能を使用できません。
 - マルチ VLAN ポートにすることはできません。
 - ネットワークの相互接続装置には接続できません。
 - トランクポートにすることはできません。

例

次に、ポート SNP5 のポートセキュリティーを使用可能にする例を示します。

```
Console(config)#interface ethernet SNP5
Console(config-if)#port security
```

関連コマンド

`mac-address-table static` (4-89 ページ)

4.3.11 スパニングツリーコマンド

ここでは、スイッチ全体にスパニングツリーアルゴリズム (STA) を設定するコマンドおよび選択されたインタフェースに STA を設定するコマンドについて説明します。

コマンド	機能	モード	ページ
spanning-tree	スパニングツリープロトコルを使用可能にします。	GC	4-95
spanning-tree mode	STP または RSTP モードを設定します。	GC	4-96
spanning-tree forward-time	スパニングツリーブリッジの転送時間を設定します。	GC	4-97
spanning-tree hello-time	スパニングツリーブリッジの hello 時間を設定します。	GC	4-98
spanning-tree max-age	スパニングツリーブリッジの最大有効期限を設定します。	GC	4-98
spanning-tree priority	スパニングツリーブリッジの優先順位を設定します。	GC	4-99
spanning-tree path-cost method	RSTP のパスコスト方式を設定します。	GC	4-100
spanning-tree transmission-limit	RSTP の転送間隔を設定します。	GC	4-100
spanning-tree cost	インタフェースのスパニングツリーパスコストを設定します。	IC	4-101
spanning-tree port-priority	インタフェースのスパニングツリー優先順位を設定します。	IC	4-102
spanning-tree edge-port	エッジポートの高速転送を使用可能にします。	IC	4-103
spanning-tree protocol-migration	適切な BPDU 形式を再確認します。	PE	4-104
spanning-tree link-type	RSTP のリンクタイプを設定します。	IC	4-104
show spanning-tree	スパニングツリー設定を表示します。	PE	4-105

4.3.11.1 spanning-tree

このコマンドは、スイッチのスパニングツリーアルゴリズムをグローバルに使用可能にするために使用します。使用不可にする場合は、no 形式を使用します。

構文

```
spanning-tree  
no spanning-tree
```

デフォルト設定

スパニングツリーは使用可能です。

コマンドモード

グローバル設定

コマンドの使用法

スパニングツリーアルゴリズム (STA) を使用すると、ネットワークループを検出して解消したり、スイッチまたはブリッジ、ルーターの間にバックアップリンクを設定できます。STA によってスイッチがネットワーク上のその他のブリッジ装置 (STA に準拠するスイッチまたはブリッジ、ルーター) と情報を交換できるようになるため、ネットワーク上の任意の 2 台のステーション間にルートが 1 つだけ存在するようになり、一次リンクがダウンしたときには一次リンクのタスクを自動的に引き継ぐバックアップリンクを提供できます。

例

次に、スイッチの STA を使用可能にする例を示します。

```
Console(config)#spanning-tree  
Console(config)#
```

4.3.11.2 spanning-tree mode

このコマンドは、スイッチのスパニングツリーモードを選択するために使用します。デフォルトに戻す場合は、no 形式を使用します。

構文

```
spanning-tree mode {stp | rstp}  
no spanning-tree mode
```

- **stp** – スパニングツリープロトコル (IEEE 802.1D)
- **rstp** – 高速スパニングツリー (IEEE 802.1w)

デフォルト設定

stp

コマンドモード

グローバル設定

コマンドの使用法

- 高速スパニングツリープロトコル (RSTP)

RSTP は、次に説明するように、受信プロトコルメッセージを監視し、RSTP ノードが転送するプロトコルメッセージのタイプを動的に調整することによって、STP および RSTP のどちらのノードへの接続もサポートします。

- STP モード – スイッチがポートの移行遅延タイマーの期限が過ぎたあとに 802.1D BPDU を受信した場合、スイッチは 802.1D ブリッジに接続されていると推測して、802.1D BPDU だけを使用するようになります。
- RSTP モード – RSTP がポート上で 802.1D BPDU を使用していて、移行遅延の期限が過ぎたあとに RSTP BPDU を受信した場合、RSTP は移行遅延タイマーを再開して、そのポートでは RSTP BPDU を使用するようになります。

例

次に、RSTP を使用するようにスイッチを設定する例を示します。

```
Console(config)#spanning-tree mode rstp  
Console(config)#
```

4.3.11.3 spanning-tree forward-time

このコマンドは、スイッチのスパニングツリーブリッジの転送時間をグローバルに設定するために使用します。デフォルトに戻す場合は、no 形式を使用します。

構文

```
spanning-tree forward-time seconds  
no spanning-tree forward-time
```

seconds – 秒単位の時間 (範囲 : 4 ~ 30 秒)
最小値は、4 または $[(\text{最大有効期限}/2) + 1]$ の大きい方の値です。

デフォルト設定

15 秒

コマンドモード

グローバル設定

コマンドの使用法

このコマンドによって、ルートの装置が状態を (破棄から学習、転送へ) 変更する前に待機する最大の時間を秒単位で設定します。すべての装置は、フレームの転送を開始する前にトポロジの変更に関する情報を受信する必要があるため、この遅延が必要となります。また、各ポートには、競合情報を待機する時間が必要です。競合情報を受信すると、ポートは破棄状態に戻ります。この待機時間がないと、一時データのループが発生することがあります。

例

```
Console(config)#spanning-tree forward-time 20  
Console(config)#
```

4.3.11.4 spanning-tree hello-time

このコマンドは、スイッチのスパニングツリーブリッジの **hello** 時間をグローバルに設定するために使用します。デフォルトに戻す場合は、no 形式を使用します。

構文

```
spanning-tree hello-time time  
no spanning-tree hello-time
```

time - 秒単位の時間 (範囲 : 1 ~ 10 秒)
最大値は、10 または [(最大有効期限/2) - 1] の小さい方の値です。

デフォルト設定

2 秒

コマンドモード

グローバル設定

コマンドの使用法

このコマンドによって、ルートの装置が設定メッセージを送信する間隔を秒単位で設定します。

例

```
Console(config)#spanning-tree hello-time 5  
Console(config)#
```

4.3.11.5 spanning-tree max-age

このコマンドは、スイッチのスパニングツリーブリッジの最大有効期限をグローバルに設定するために使用します。デフォルトに戻す場合は、no 形式を使用します。

構文

```
spanning-tree max-age seconds  
no spanning-tree max-age
```

seconds - 秒単位の時間 (範囲 : 6 ~ 40 秒)
最小値は、6 または [2 x (hello 時間 + 1)] の大きい方の値です。
最大値は、40 または [2 x (転送時間 - 1)] の小さい方の値です。

デフォルト設定

20 秒

コマンドモード

グローバル設定

コマンドの使用法

このコマンドによって、装置が設定メッセージを受信するまで待機する最大時間を秒単位で設定します。この時間を過ぎると、装置は再設定を試みます。指定ポート以外のすべての装置のポートでは、定期的に設定メッセージを受信する必要があります。前回の設定メッセージによって提供された STA 情報の期限が切れたポートは、接続されている LAN の指定ポートになります。このポートがルートポートだった場合は、ネットワークに接続されている装置のポートの中から新しいルートポートが選択されます。

例

```
Console(config)#spanning-tree max-age 40
Console(config)#
```

4.3.11.6 spanning-tree priority

このコマンドは、スイッチのスパニングツリーの優先順位をグローバルに設定するために使用します。デフォルトに戻す場合は、no 形式を使用します。

構文

```
spanning-tree priority priority
no spanning-tree priority
```

priority – ブリッジの優先順位

(範囲 – 0 ~ 61440、4096 ずつ増分。指定可能な値 : 0、4096、8192、12288、16384、20480、24576、28672、32768、36864、40960、45056、49152、53248、57344、61440)

デフォルト設定

32768

コマンドモード

グローバル設定

コマンドの使用法

ブリッジの優先順位は、ルート装置およびルートポート、指定ポートを選択するために使用されます。優先順位の高い装置が STA ルート装置になります。ただし、すべての装置の優先順位が同じ場合は、MAC アドレス番号がもっとも小さい装置が STA ルート装置になります。

例

```
Console(config)#spanning-tree priority 40000
Console(config)#
```

4.3.11.7 spanning-tree pathcost method

このコマンドは、高速スパンニングツリーが使用するパスコスト方式を設定するために使用します。デフォルトに戻す場合は、no 形式を使用します。

構文

```
spanning-tree pathcost method {long | short}  
no spanning-tree pathcost method
```

- **long** – 1 ~ 200,000,000 の 32 ビットベースの値を指定
- **short** – 1 ~ 65535 の 16 ビットベースの値を指定

デフォルト設定

short 方式

コマンドモード

グローバル設定

コマンドの使用法

パスコスト方式は、装置間の最適なパスを決定するために使用されます。そのため、速い媒体に接続するポートには小さい値を、遅い媒体に接続するポートには大きい値を割り当てます。パスコスト (4-101 ページ) は、ポートの優先順位 (4-102 ページ) よりも優先度が高くなります。

例

```
Console(config)#spanning-tree pathcost method long  
Console(config)#
```

4.3.11.8 spanning-tree transmission-limit

このコマンドは、連続する RSTP BPDU の最小転送間隔を設定するために使用します。デフォルトに戻す場合は、no 形式を使用します。

構文

```
spanning-tree transmission-limit count  
no spanning-tree transmission-limit
```

count – 秒単位の最小転送間隔 (範囲: 1 ~ 10)

デフォルト設定

3

コマンドモード

グローバル設定

コマンドの使用法

このコマンドによって、BPDU の最大転送速度が制限されます。

例

```
Console(config)#spanning-tree transmission-limit 4
Console(config)#
```

4.3.11.9 spanning-tree cost

このコマンドは、指定されたインタフェースにスパニングツリーのパスコストを設定するために使用します。デフォルトに戻す場合は、no 形式を使用します。

構文

```
spanning-tree cost cost
no spanning-tree cost
```

cost — インタフェースのパスコスト
(範囲 — 1 ~ 200,000,000)
推奨範囲 —

- Ethernet : 200,000 ~ 20,000,000
- Fast Ethernet : 20,000 ~ 2,000,000
- Gigabit Ethernet : 2,000 ~ 200,000

デフォルト設定

- Ethernet — 半二重 : 2,000,000、全二重 : 1,000,000、トランク : 500,000
- Fast Ethernet — 半二重 : 200,000、全二重 : 100,000、トランク : 50,000
- Gigabit Ethernet — 全二重 : 10,000、トランク : 5,000

コマンドモード

インタフェース設定 (Ethernet、Port Channel)

コマンドの使用法

- スパニングツリーアルゴリズムは、このコマンドを使用して装置間の最適なパスを決定します。そのため、速い媒体に接続するインタフェースには小さい値を、遅い媒体に接続するインタフェースには大きい値を割り当てます。
- パスコストは、インタフェースの優先順位より優先度が高くなります。
- スパニングツリーのパスコスト方式に short を設定している場合、パスコストの最大値は 65,535 になります。

例

```
Console(config)#interface ethernet SNP5
Console(config-if)#spanning-tree cost 50
Console(config-if)#
```

関連コマンド

`spanning-tree port-priority` (4-102 ページ)

4.3.11.10 `spanning-tree port-priority`

このコマンドは、指定したインタフェースの優先順位を設定するために使用します。デフォルトに戻す場合は、`no` 形式を使用します。

構文

```
spanning-tree port-priority priority
no spanning-tree port-priority
```

priority – インタフェースの優先順位 (範囲 : 0 ~ 240、16 ずつ増分)

デフォルト設定

128

コマンドモード

インタフェース設定 (Ethernet、Port Channel)

コマンドの使用法

- このコマンドによって、インタフェースのスパニングツリーアルゴリズム内での優先順位を定義します。スイッチ上のすべてのインタフェースのパスコストが同一である場合は、この優先順位がもっとも高い (値がもっとも小さい) インタフェースがスパニングツリー内のアクティブリンクとして設定されます。
- 複数のインタフェースにもっとも高い優先順位が割り当てられている場合は、識別子にもっとも小さい番号が付いているインタフェースが使用可能になります。

例

```
Console(config)#interface ethernet SNP5
Console(config-if)#spanning-tree port-priority 0
Console(config-if)#
```

関連コマンド

`spanning-tree cost` (4-101 ページ)

4.3.11.11 spanning-tree edge-port

このコマンドは、インタフェースをエッジポートに指定するために使用します。デフォルトに戻す場合は、no 形式を使用します。

構文

```
spanning-tree edge-port  
no spanning-tree edge-port
```

デフォルト設定

NETP0 ~ 7、NETMGT : 使用不可
SNP0 ~ 15 : 使用可能 (この設定に固定)

コマンドモード

インタフェース設定 (Ethernet、Port Channel)

コマンドの使用法

インタフェースが、ブリッジ接続された LAN の境界にある LAN セグメントまたはエンドノードに接続されている場合は、このオプションを使用可能に設定できます。エンドノードは、転送ループを発生させることがないため、すぐスパンニングツリーの転送状態になります。エッジポートを指定すると、ワークステーション、サーバーなどの装置をすばやく収束 (コンバージェンス) し、現在の転送用のデータベースを保持することで再構成時のアドレステーブル再作成に必要なフレームフラディングの量を削減します。また、インタフェースの状態が変わってもスパンニングツリーが再構成を開始しなくなります。STA 関連のタイムアウト問題にも対処できます。ただし、エッジポートは、エッジノード装置に接続されているポートでのみ使用可能にしてください。

例

```
Console(config)#interface ethernet SNP5  
Console(config-if)#spanning-tree edge-port  
Console(config-if)#
```

4.3.11.12 spanning-tree protocol-migration

このコマンドは、選択したインタフェースに送信される BPDU の形式が適切かどうかを再確認するために使用します。

構文

spanning-tree protocol-migration *interface*

interface

- **ethernet** *port-name*

port-name — ダウンリンク : SNP0 ~ 15、アップリンク : NETP0 ~ 7、
管理 : NETMGT

- **port-channel** *channel-id* (範囲 : 1 ~ 6)

コマンドモード

特権実行

コマンドの使用法

スイッチは、構成情報 (Configuration) BPDU、トポロジ変更通知 (Topology Change Notification) BPDU などの STP BPDU を検出すると、選択されたインタフェースを強制 STP 互換モードに設定します。また、**spanning-tree protocol-migration** コマンドを使用して、選択したインタフェースでの送信に適した BPDU の形式 (RSTP または STP 互換形式) を手動で再確認することもできます。

例

```
Console(config)#interface ethernet SNP5
Console(config-if)#spanning-tree protocol-migration
Console(config-if)#
```

4.3.11.13 spanning-tree link-type

このコマンドは、高速スパニングツリーのリンクタイプを設定するために使用します。デフォルトに戻す場合は、**no** 形式を使用します。

構文

spanning-tree link-type {**auto** | **point-to-point** | **shared**}

no spanning-tree link-type

- **auto** — デュプレックスモード設定から自動的に判定
- **point-to-point** — ポイントツーポイント接続
- **shared** — 共有媒体

デフォルト設定

auto

コマンドモード

インタフェース設定 (Ethernet、Port Channel)

コマンドの使用法

- インタフェースをほかの 1 台のブリッジだけに接続する場合はポイントツーポイント接続を、複数のブリッジに接続する場合は共有リンクを指定します。
- 自動検出を選択すると、スイッチはデュプレックスモードからリンクタイプを判定します。全二重インタフェースの場合はポイントツーポイント接続に、半二重インタフェースの場合は共有リンクになります。
- RSTP は、2 台のブリッジ間のポイントツーポイント接続だけで機能します。ポートを共有リンクに指定すると、RSTP は禁止されます。

例

```
Console(config)#interface ethernet SNP5
Console(config-if)#spanning-tree link-type point-to-point
Console(config-if)#
```

4.3.11.14 show spanning-tree

このコマンドは、スパニングツリーの設定を表示するために使用します。

構文

show spanning-tree [*interface*]

- *interface*
 - **ethernet** *port-name*
port-name — ダウンリンク : SNP0 ~ 15、アップリンク : NETP0 ~ 7、
管理 : NETMGT
 - **port-channel** *channel-id* (範囲 : 1 ~ 6)

デフォルト設定

なし

コマンドモード

特権実行

コマンドの使用法

- パラメタを指定せずに **show spanning-tree** コマンドを実行すると、スイッチおよびツリー内のすべてのインタフェースのスパニングツリー設定が表示されます。

- `show spanning-tree interface` コマンドを実行すると、特定のインタフェースのスパニングツリー設定が表示されます。
- 「Bridge-group information」の欄に表示される項目については、3-57 ページの「基本的な STA 設定」を参照してください。特定のインタフェースに関する項目については、3-102 ページの「スパニングツリーアルゴリズムのインタフェースの管理」を参照してください。

例

```
Console#show spanning-tree
Bridge-group information
-----
Spanning tree mode           :RSTP
Spanning tree enable/disable :enable
Priority                     :32768
Bridge Hello Time (sec.)    :2
Bridge Max Age (sec.)       :20
Bridge Forward Delay (sec.) :15
Root Hello Time (sec.)      :2
Root Max Age (sec.)         :20
Root Forward Delay (sec.)   :15
Designated Root             :8.0000E8666672
Current root port           :0
Current root cost           :0
Number of topology changes  :0
Last topology changes time (sec.):1363
Transmission limit          :3
Path Cost Mothod            :21
-----
SNP0 information
-----
Admin status      : enable
Role              : designate
State             : forwarding
Path cost         : 10000
Priority          : 128
Designated cost   : 0
Designated port   : 8.1
Designated root   : 8.0000E8666672
Designated bridge : 8.0000E8666672
Forward transitions : 0
Admin edge port   : disable
Oper edge port    : disable
Admin Link type   : point-to-point
Oper Link type    : point-to-point
.
.
.
Console#
```

4.3.12 VLAN コマンド

VLAN とは、ネットワーク内のどの場所に配置しても、同じ物理セグメントに属している場合と同様に通信できるポートのグループです。ここでは、VLAN グループの作成およびポートメンバーの追加、VLAN タグの使用方法の指定、選択したインタフェースの自動 VLAN 登録の使用可能への切り替えを行うコマンドについて説明します。

コマンド	機能	モード	ページ
VLAN グループの編集			
vlan database	VLAN を追加および変更、削除するために VLAN データベースモードを開始します。	GC	4-109
vlan	VLAN の VID、名前、状態などを設定します。	VC	4-109
VLAN インタフェースの設定			
interface vlan	指定した VLAN のインタフェース設定モードを開始します。	GC	4-110
switchport mode	インタフェースの VLAN メンバーシップモードを設定します。	IC	4-111
switchport acceptable-frame-types	インタフェースが受け入れるフレームタイプを設定します。	IC	4-112
switchport ingress-filtering	インタフェースのイングレスフィルタリングを使用可能にします。	IC	4-113
switchport native vlan	インタフェースの PVID (ネイティブ VLAN) を設定します。	IC	4-114
switchport allowed vlan	インタフェースに関連付けられた VLAN を設定します。	IC	4-115
switchport gvrp	インタフェースの GVRP を使用可能にします。	IC	4-118
switchport forbidden vlan	インタフェースの禁止 VLAN を設定します。	IC	4-116
VLAN 情報の表示			
show vlan	VLAN 情報を表示します。	NE、PE	4-117
show interfaces status vlan	指定した VLAN インタフェースのステータスを表示します。	NE、PE	4-84
show interfaces switchport	インタフェースの管理ステータスおよび動作ステータスを表示します。	NE、PE	4-87

4.3.12.1 vlan database

このコマンドは、VLAN データベースモードを開始するために使用します。このモードで入力したすべてのコマンドは、ただちに有効になります。

デフォルト設定

なし

コマンドモード

グローバル設定

コマンドの使用法

- VLAN データベースコマンドモードでは、VLAN の追加および変更、削除を実行できます。設定の変更が終了したら、`show vlan` コマンドを実行して VLAN 設定を確認できます。
- VLAN のインタフェース設定モードでは、ポートメンバーシップモードの定義および VLAN へのポートの追加または削除を実行できます。実行したコマンドの結果は、動作時設定ファイルに書き込まれ、`show running-config` コマンドによって確認できます。

例

```
Console(config)#vlan database
Console(config-vlan)#
```

関連コマンド

`show vlan` (4-117 ページ)

4.3.12.2 vlan

このコマンドは、VLAN を設定するために使用します。デフォルト設定に戻す場合や VLAN を削除する場合は、`no` 形式を使用します。

構文

```
vlan vlan-id [name vlan-name] media ethernet [state (active | suspend)]
no vlan vlan-id [name | state]
```

- *vlan-id* — 設定する VLAN の ID (範囲: 1 ~ 4094、先頭にゼロを付けない)
- **name** — キーワードに続けて VLAN 名を指定します。
 - *vlan-name* — 1 ~ 15 文字の ASCII 文字列
- **media ethernet** — 媒体タイプは Ethernet
- **state** — キーワードに続けて VLAN 状態を指定します。
 - **active** — VLAN は動作中
 - **suspend** — VLAN は停止中。パケットの送受信を行っていません。

デフォルト設定

デフォルトでは、VLAN 1 だけが存在し動作しています。

コマンドモード

VLAN データベース設定

コマンドの使用法

- **no vlan *vlan-id*** を実行すると、VLAN が削除されます。
- **no vlan *vlan-id* name** を実行すると、VLAN 名が削除されます。
- **no vlan *vlan-id* state** を実行すると、VLAN がデフォルトの状態 (active) に戻ります。
- VLAN 1 は停止できませんが、その他の VLAN は停止できます。
- スイッチには、最大で 255 の VLAN を設定できます。

例

次に、vlan-id が 105、名前が RD5 の VLAN を追加する例を示します。この VLAN は、デフォルトで動作中になります。

```
Console(config)#vlan database
Console(config-vlan)#vlan 105 name RD5 media ethernet
Console(config-vlan)#
```

関連コマンド

show vlan (4-117 ページ)

4.3.12.3 interface vlan

このコマンドは、VLAN のインタフェース設定モードを開始して、物理インタフェースを設定するために使用します。

構文

interface vlan *vlan-id*

vlan-id — 設定する VLAN の ID (範囲 : 1 ~ 4094、先頭にゼロを付けない)

デフォルト設定

なし

コマンドモード

グローバル設定

例

次に、VLAN 1 のインタフェース設定モードを開始して、この VLAN に IP アドレスを割り当てる例を示します。

```
Console(config)#interface vlan 1
Console(config-if)#ip address 192.168.1.254 255.255.255.0
Console(config-if)#
```

関連コマンド

shutdown (4-82 ページ)

4.3.12.4 switchport mode

このコマンドは、ポートの VLAN メンバーシップモードを設定するために使用します。デフォルトに戻す場合は、no 形式を使用します。

構文

```
switchport mode {trunk | hybrid}
no switchport mode
```

- **trunk** — ポートを VLAN トランクの終端として指定します。トランクとは、2つのスイッチ間の直接リンクです。そのため、ポートは、送信元の VLAN を識別できるタグ付きフレームを転送します。ただし、ポートのデフォルトの VLAN (PVID に関連付けられた VLAN) に属するフレームは、タグなしで送信されます。
- **hybrid** — ハイブリッド VLAN インタフェースを指定します。ポートは、タグ付きフレームまたはタグなしフレームを送信します。

デフォルト設定

すべてのポートがハイブリッドモードで PVID に VLAN 1 が設定されています。

コマンドモード

インタフェース設定 (Ethernet、Port Channel)

例

次に、ポート SNP1 の設定モードを開始して、スイッチポートのモードをハイブリッドに設定する例を示します。

```
Console(config)#interface ethernet SNP1
Console(config-if)#switchport mode hybrid
Console(config-if)#
```

4.3.12.5 switchport acceptable-frame-types

このコマンドは、ポートが受け入れるフレームタイプを設定するために使用します。デフォルトに戻す場合は、no 形式を使用します。

構文

```
switchport acceptable-frame-types {all | tagged}  
no switchport acceptable-frame-types
```

- **all** – ポートは、タグ付きおよびタグなしのすべてのフレームを受け入れます。
- **tagged** – ポートは、タグ付きフレームだけを受信します。

デフォルト設定

すべてのフレームタイプ

コマンドモード

インタフェース設定 (Ethernet、Port Channel)

コマンドの使用法

すべてのフレームタイプを受信するように設定すると、受信したすべてのタグなしフレームはデフォルト VLAN に割り当てられます。

例

次に、SNP1 が受信するトラフィックをタグ付きフレームに制限する例を示します。

```
Console(config)#interface ethernet SNP1  
Console(config-if)#switchport acceptable-frame-types tagged  
Console(config-if)#
```

4.3.12.6 switchport ingress-filtering

このコマンドは、インタフェースのイングレスフィルタリングを使用可能にするために使用します。デフォルトに戻す場合は、no 形式を使用します。

構文

```
switchport ingress-filtering
no switchport ingress-filtering
```

デフォルト設定

使用不可

コマンドモード

インタフェース設定 (Ethernet、Port Channel)

コマンドの使用法

- イングレスフィルタリングは、タグ付きフレームだけに影響を与えます。
- イングレスフィルタリングを使用不可にすると、ポート上で明示的に禁止されている VLAN を除いて、スイッチが認識している VLAN と一致するタグの付いた VLAN タグ付きフレームはすべて受け入れられるようになります。
- イングレスフィルタリングを使用可能にすると、この入口ポートがメンバーに含まれていない VLAN のタグ付き受信フレームは破棄されます。
- イングレスフィルタリングは、GVRP、STP などの VLAN に依存しない BPDU フレームには影響を与えません。ただし、GMRP などの VLAN に依存する BPDU フレームには影響を与えます。

例

次に、ポート SNP1 のインタフェースを設定して、イングレスフィルタリングを使用可能にする例を示します。

```
Console(config)#interface ethernet SNP1
Console(config-if)#switchport ingress-filtering
Console(config-if)#
```

4.3.12.7 switchport native vlan

このコマンドは、インタフェースに PVID (デフォルトの VID) を設定するために使用します。デフォルトに戻す場合は、no 形式を使用します。

構文

```
switchport native vlan vlan-id  
no switchport native vlan
```

vlan-id - インタフェースのデフォルト VLAN の ID (範囲 : 1 ~ 4094、先頭にゼロを付けない)

デフォルト設定

VLAN 1

コマンドモード

インタフェース設定 (Ethernet、Port Channel)

コマンドの使用法

- インタフェースが VLAN 1 のメンバーではない場合に、そのインタフェースの PVID を VLAN 1 にすると、インタフェースはタグなしメンバーとして VLAN 1 に自動的に追加されます。その他の VLAN の場合は、最初にインタフェースをタグなしメンバーとして設定してから、PVID にそのグループを設定します。
- 受け入れ可能なフレームタイプを all に設定するか、スイッチポートモードを hybrid に設定すると、入口ポートが受信するすべてのタグなしフレームに PVID が挿入されます。

例

次に、ポート SNP1 の PVID を VLAN 3 に設定する例を示します。

```
Console(config)#interface ethernet SNP1  
Console(config-if)#switchport native vlan 3  
Console(config-if)#
```

4.3.12.8 switchport allowed vlan

このコマンドは、選択されたインタフェースの VLAN グループを設定するために使用します。デフォルトに戻す場合は、no 形式を使用します。

構文

```
switchport allowed vlan {add vlan [tagged | untagged] | remove vlan}
```

- **add vlan** — 追加する VLAN の ID
- **remove vlan** — 削除する VLAN の ID

先頭にゼロを入力しないでください (範囲: 1 ~ 4094)。

```
no switchport allowed vlan
```

注 — no switchport allowed vlan コマンドは、NETMGT ポートに対して実行することはできません (実行すると、エラーメッセージが表示されます)。管理ポートを出荷時のデフォルトの VLAN (VLAN 2) に戻して、このポートに追加したすべての VLAN を削除する場合は、次のコマンドを入力します。

```
Console(config)#interface ethernet NETMGT
Console(config-if)#switchport allowed vlan add 2
Console(config-if)#switchport native vlan 2
Console(config-if)#switchport allowed vlan remove <vlan id>
```

ここで、<vlan id> には、NETMGT に追加した VLAN 2 以外の VLAN の番号を指定します。NETMGT が属している VLAN 2 以外のすべての VLAN に対して、最後のコマンドを繰り返し実行します。

デフォルト設定

- NETMGT 以外のすべてのポートは、デフォルトでは VLAN 1 に割り当てられています。NETMGT は、デフォルトでは VLAN 2 に割り当てられています。
- デフォルトのフレームタイプは、タグなしです。

コマンドモード

インタフェース設定 (Ethernet、Port Channel)

コマンドの使用法

- スイッチポートモードを trunk に設定した場合、インタフェースは、タグ付きメンバーとしてだけ VLAN グループに割り当てることができます。
- スイッチ内のフレームには、常にタグが付いています。インタフェースに VLAN を追加するときに指定するタグ付きまたはタグなしのパラメタによって、スイッチが、フレームの送信時にタグを維持するかまたは削除するかを判断します。

- 中間に位置するすべてのネットワーク装置および接続先のホストが VLAN をサポートしていない場合、その VLAN にはインタフェースをタグなしメンバーとして追加する必要があります。そうでない場合は、インタフェースを1つの VLAN のタグなしメンバーとして追加し、その VLAN をネイティブ VLAN に設定するだけですみます。
- インタフェースの禁止リストに登録されている VLAN をそのインタフェースに手動で追加すると、その VLAN は禁止リストから自動的に削除されます。

例

次に、ポート SNP1 の許可リストに、VLAN 1 および 2、5、6 をタグ付き VLAN として追加する例を示します。

```
Console(config)#interface ethernet SNP1
Console(config-if)#switchport allowed vlan add 1 tagged
Console(config-if)#switchport allowed vlan add 2 tagged
Console(config-if)#switchport allowed vlan add 5 tagged
Console(config-if)#switchport allowed vlan add 6 tagged
Console(config-if)#
```

4.3.12.9 switchport forbidden vlan

このコマンドは、禁止する VLAN を設定するために使用します。禁止する VLAN のリストを削除する場合は、no 形式を使用します。

構文

```
switchport forbidden vlan {add vlan | remove vlan}  
no switchport forbidden vlan
```

- **add *vlan*** - 追加する VLAN の ID
- **remove *vlan*** - 削除する VLAN の ID

先頭にゼロを入力しないでください (範囲: 1 ~ 4094)。

デフォルト設定

禁止リストに登録された VLAN はありません。

コマンドモード

インタフェース設定 (Ethernet、Port Channel)

コマンドの使用法

- このコマンドを使用すると、指定したインタフェースに GVRP によって VLAN が自動的に割り当てられることを禁止できます。
- VLAN をインタフェースの許可 VLAN に追加した場合は、この VLAN を同じインタフェースの禁止 VLAN に追加することはできません。

例

次に、ポート SNP1 が VLAN 3 に追加されないように設定する例を示します。

```
Console(config)#interface ethernet SNP1
Console(config-if)#switchport forbidden vlan add 3
Console(config-if)#
```

4.3.12.10 show vlan

このコマンドは、VLAN 情報を表示するために使用します。

構文

```
show vlan [id vlan-id | name vlan-name]
```

- **id** – キーワードに続けて VLAN ID を指定します。
 - *vlan-id* – 設定した VLAN の ID (範囲: 1 ~ 4094、先頭にゼロを付けない)
- **name** – キーワードに続けて VLAN 名を指定します。
 - *vlan-name* – 1 ~ 15 文字の ASCII 文字列

デフォルト設定

すべての VLAN が表示されます。

コマンドモード

通常実行、特権実行

例

次に、VLAN 1 の情報を表示する例を示します。

```
Console#show vlan id 1
VLAN Type      Name           Status  Ports/Channel groups
-----
 1 Static      DefaultVlan   Active  SNP0   SNP1   SNP2   SNP3   SNP4
                               SNP5   SNP6   SNP7   SNP8   SNP9
                               SNP10  SNP11  SNP12  SNP13  SNP14
                               SNP15  NETP0  NETP1  NETP2  NETP3
                               NETP4  NETP5  NETP6  NETP7
 2 Static      MgtVlan       Active  NETMGT
Console#
```

4.3.13 GVRP およびブリッジ拡張機能コマンド

GARP VLAN Registration Protocol (GVRP) は、ネットワーク上のインタフェースで VLAN のメンバーを自動的に登録するために、スイッチが VLAN 情報を交換する方法を規定したものです。ここでは、個々のインタフェースに対して GVRP を使用可能にする方法、およびスイッチ全体で GVRP を使用可能にする方法、ブリッジ拡張機能の MIB のデフォルト設定を表示する方法について説明します。

コマンド	機能	モード	ページ
インタフェースコマンド			
switchport gvrp	インタフェースの GVRP を使用可能にします。	IC	4-118
switchport forbidden vlan	インタフェースの禁止 VLAN を設定します。	IC	4-116
show gvrp configuration	選択したインタフェースの GVRP 設定を表示します。	NE、PE	4-119
garp timer	選択した機能の GARP タイマーを設定します。	IC	4-120
show garp timer	選択した機能の GARP タイマーを表示します。	NE、PE	4-121
グローバルコマンド			
bridge-ext gvrp	GVRP をスイッチ全体で使用可能にします。	GC	4-122
show bridge-ext	ブリッジ拡張機能の設定を表示します。	PE	4-123

4.3.13.1 switchport gvrp

このコマンドは、ポートに対して GVRP を使用可能にするために使用します。使用不可にする場合は、no 形式を使用します。

構文

```
switchport gvrp
no switchport gvrp
```

デフォルト設定

使用可能

コマンドモード

インタフェース設定 (Ethernet、Port Channel)

例

```
Console(config)#interface ethernet SNP1
Console(config-if)#switchport gvrp
Console(config-if)#
```

4.3.13.2 show gvrp configuration

このコマンドは、GVRP が使用可能または使用不可のどちらに設定されているかを確認するために使用します。

構文

show gvrp configuration [*interface*]

interface

■ **ethernet** *port-name*

port-name – ダウンリンク : SNP0 ~ 15、アップリンク : NETP0 ~ 7、
管理 : NETMGT

■ **port-channel** *channel-id* (範囲 : 1 ~ 6)

デフォルト設定

グローバル設定およびインタフェース固有の設定の両方が表示されます。

コマンドモード

通常実行、特権実行

例

```
Console#show gvrp configuration
Whole system:
GVRP configuration: Enabled
SNP0:
  Gvrp configuration: Enabled
SNP1:
  Gvrp configuration: Enabled
.
.
.
```

4.3.13.3 garp timer

このコマンドは、**join** および **leave**、**leaveall** の各タイマーに値を設定するために使用します。タイマーのデフォルト値に戻す場合は、**no** 形式を使用します。

構文

```
garp timer {join | leave | leaveall} timer_value  
no garp timer {join | leave | leaveall}
```

- {**join** | **leave** | **leaveall**} – 設定するタイマー
- *timer_value* – タイマーの値
範囲：
 - **join** : 20 ~ 1000 センチ秒
 - **leave** : 60 ~ 3000 センチ秒
 - **leaveall** : 500 ~ 18000 センチ秒

デフォルト設定

- **join** : 20 センチ秒
- **leave** : 60 センチ秒
- **leaveall** : 1000 センチ秒

コマンドモード

インタフェース設定 (Ethernet、Port Channel)

コマンドの使用法

- Group Address Registration Protocol (GARP) は、GVRP および GMRP によって、ブリッジ接続された LAN 内のクライアントサービスのクライアント属性を登録または削除するために使用されます。GARP タイマーのデフォルト値は、媒体アクセス方式またはデータ転送速度には依存しません。GMRP または GVRP の登録または削除処理で問題が発生した場合以外は、このデフォルト値を変更しないでください。
- タイマー値は、すべての VLAN のすべてのポートの GVRP に適用されます。
- タイマー値は、次の条件を満たす必要があります。
 - **leave** >= (2 x **join**)
 - **leaveall** > **leave**

注 – 同じネットワークに接続するすべてのレイヤー 2 装置の GVRP タイマーは、同じ値に設定してください。異なる値を設定すると、GVRP が正常に動作しません。

例

```
Console(config)#interface ethernet SNP1  
Console(config-if)#garp timer join 100  
Console(config-if)#
```

関連コマンド

show garp timer (4-121 ページ)

4.3.13.4 show garp timer

このコマンドは、選択したインタフェースの GARP タイマーを表示するために使用します。

構文

```
show garp timer [interface]
```

```
interface
```

```
■ ethernet port-name
```

```
port-name — ダウンリンク : SNP0 ~ 15、アップリンク : NETP0 ~ 7、  
管理 : NETMGT
```

```
■ port-channel channel-id (範囲 : 1 ~ 6)
```

デフォルト設定

すべての GARP タイマーが表示されます。

コマンドモード

通常実行、特権実行

例

```
Console#show garp timer ethernet SNP1  
SNP1 GARP timer status:  
Join timer: 20 sec.  
Leave timer: 60 sec.  
Leaveall timer: 1000 sec.  
Console#
```

関連コマンド

garp timer (4-120 ページ)

4.3.13.5 bridge-ext gvrp

このコマンドは、GVRP をスイッチ全体で使用可能にするために使用します。使用不可にする場合は、no 形式を使用します。

構文

```
bridge-ext gvrp  
no bridge-ext gvrp
```

デフォルト設定

使用可能

コマンドモード

グローバル設定

コマンドの使用法

GVRP は、ネットワーク上のポートで VLAN メンバーを登録するために、スイッチが VLAN 情報を交換する方法を規定したものです。VLAN の自動登録を可能にし、ローカルスイッチを超える VLAN をサポートするには、この機能を使用可能にする必要があります。

例

```
Console(config)#bridge-ext gvrp  
Console(config)#
```

4.3.13.6 show bridge-ext

このコマンドは、ブリッジ拡張機能コマンドの設定を表示するために使用します。

デフォルト設定

なし

コマンドモード

特権実行

コマンドの使用法

このコマンドで表示される項目の意味は、次のとおりです。

- Max support vlan numbers – IEEE 802.1Q 標準で規定されている、このスイッチが使用する VLAN のバージョンです。
- Max support vlan ID – このスイッチが認識する VLAN ID の最大の番号です。
- Extended multicast filtering services – このスイッチは、GMRP (GARP Multicast Registration Protocol) に基づく個々のマルチキャストアドレスのフィルタリングはサポートしていません。
- Static entry individual port – このスイッチは、ユニキャストアドレスおよびマルチキャストアドレスの静的フィルタリングに対応しています (4-89 ページおよび 4-126 ページ)。
- VLAN learning – このスイッチは独立 VLAN 学習機能 (Independent VLAN Learning : IVL) を使用するので、各ポートが独自のフィルタリングデータベースを保持しています。
- Configurable PVID tagging – このスイッチでは、各ポートのデフォルトのポート VLAN ID (フレームタグの PVID) および出力ステータス (VLAN-Tagged または Untagged) を上書きできます (4-114 ページ)。
- Local VLAN capable – このスイッチが複数スパンニングツリーをサポートするかどうかを示します。現在、複数スパンニングツリーはサポートしていません。
- Traffic classes – このスイッチは、複数のトラフィッククラスにユーザー優先順位を割り当てる機能を提供します (4-138 ページ)。
- Global GVRP status – GVRP は、ネットワーク上のポートで VLAN メンバーを登録するために、スイッチが VLAN 情報を交換する方法を規定したものです。ローカルスイッチを超える VLAN グループを使用するには、この機能を使用可能にする必要があります (4-122 ページ)。
- GMRP – GMRP を使用すると、ネットワーク装置はエンドステーションをマルチキャストグループに登録できます。このスイッチは GMRP をサポートしていません。このスイッチは、Internet Group Management Protocol (IGMP) を使用して、自動マルチキャストフィルタリングを行います。

例

```
Console#show bridge-ext
Max support vlan numbers: 255
Max support vlan ID: 4094
Extended multicast filtering services: No
Static entry individual port: Yes
VLAN learning: IVL
Configurable PVID tagging: Yes
Local VLAN capable: Yes
Traffic classes: Enabled
Global GVRP status: Enabled
GMRP: Disabled
Console#
```

4.3.14 IGMP スヌープコマンド

このスイッチは、IGMP (Internet Group Management Protocol) を使用して、特定のマルチキャストサービスの受信を要求する接続ホストを照会します。スイッチは、サービスを要求するホストに接続するポートを識別し、このポートだけにデータを送信します。次に、継続してマルチキャストサービスを受信できるように、隣接するマルチキャストスイッチ/ルーターにサービス要求を伝播します。

コマンド	機能	モード	ページ
基本的な IGMP コマンド			
ip igmp snooping	IGMP スヌープを使用可能にします。	GC	4-125
ip igmp snooping vlan static	マルチキャストグループのメンバーとしてインタフェースを追加します。	GC	4-126
ip igmp snooping version	スヌープの IGMP バージョンを設定します。	GC	4-126
show ip igmp snooping	IGMP スヌープ設定を表示します。	PE	4-127
show bridge multicast	IGMP スヌープの MAC マルチキャストリストを表示します。	PE	4-128
IGMP 照会元コマンド			
ip igmp snooping querier	装置が IGMP スヌープの照会元として機能するように設定します。	GC	4-129
ip igmp snooping query-count	照会の回数を設定します。	GC	4-130

コマンド	機能	モード	ページ
ip igmp snooping query-interval	照会間隔を設定します。	GC	4-131
ip igmp snooping query-max-response-time	レポートの遅延を設定します。	GC	4-131
ip igmp snooping router-port-expire-time	照会のタイムアウトを設定します。	GC	4-132
show ip igmp snooping	IGMP スヌープ設定を表示します。	PE	4-127
マルチキャストルーターコマンド			
ip igmp snooping vlan mrouter	マルチキャストルーターポートを追加します。	GC	4-133
show ip igmp snooping mrouter	マルチキャストルーターポートを表示します。	PE	4-134

4.3.14.1 ip igmp snooping

このコマンドは、スイッチ上で IGMP スヌープを使用可能にするために使用します。使用不可にする場合は、no 形式を使用します。

構文

```
ip igmp snooping
no ip igmp snooping
```

デフォルト設定

使用不可

コマンドモード

グローバル設定

例

次に、IGMP スヌープを使用可能にする例を示します。

```
Console(config)#ip igmp snooping
Console(config)#
```

4.3.14.2 ip igmp snooping vlan static

このコマンドは、マルチキャストグループにポートを追加するために使用します。ポートを削除する場合は、no 形式を使用します。

構文

```
ip igmp snooping vlan vlan-id static ip-address interface  
no ip igmp snooping vlan vlan-id static ip-address interface
```

- *vlan-id* – VLAN ID (範囲 : 1 ~ 4094)
- *ip-address* – マルチキャストグループの IP アドレス
- *interface*
 - **ethernet** *port-name*
port-name – ダウンリンク : SNP0 ~ 15、アップリンク : NETP0 ~ 7、
管理 : NETMGT
 - **port-channel** *channel-id* (範囲 : 1 ~ 6)

デフォルト設定

なし

コマンドモード

グローバル設定

例

次に、ポートのマルチキャストグループを静的に設定する例を示します。

```
Console(config)#ip igmp snooping vlan 1 static 224.0.0.12  
ethernet SNP5  
Console(config)#
```

4.3.14.3 ip igmp snooping version

このコマンドは、IGMP スヌープのバージョンを設定するために使用します。デフォルトに戻す場合は、no 形式を使用します。

構文

```
ip igmp snooping version {1 | 2}  
no ip igmp snooping version
```

- 1 – IGMP バージョン 1
- 2 – IGMP バージョン 2

デフォルト設定

IGMP バージョン 2

コマンドモード

グローバル設定

コマンドの使用法

- サブネット上のすべてのシステムが、同じバージョンをサポートする必要があります。ネットワーク内にバージョン 1 だけをサポートする従来型の装置が存在する場合は、このスイッチでもバージョン 1 を使用するように設定する必要があります。
- `ip igmp query-max-response-time`、`ip igmp query-timeout` などの一部のコマンドは、IGMP バージョン 2 でのみ使用可能です。

例

次に、IGMP バージョン 1 を使用するようにスイッチを設定する例を示します。

```
Console(config)#ip igmp snooping version 1
Console(config)#
```

4.3.14.4 show ip igmp snooping

このコマンドは、IGMP スヌープ設定を表示するために使用します。

デフォルト設定

なし

コマンドモード

特権実行

コマンドの使用法

表示項目については、3-46 ページの「IGMP スヌープパラメタの設定」を参照してください。

例

次に、現在の IGMP スヌープ設定を表示する例を示します。

```
Console#show ip igmp snooping
Service status: Enabled
Querier status: Enabled
Query count: 2
Query interval: 125 sec
Query max response time: 10 sec
Query time-out: 300 sec
IGMP snooping version: Version 2
Console#
```

4.3.14.5 show mac-address-table multicast

このコマンドは、既知のマルチキャストアドレスを表示するために使用します。

構文

```
show mac-address-table multicast [vlan vlan-id]  
[user | igmp-snooping]
```

- *vlan-id* – VLAN ID (1 ~ 4094)
- **user** – ユーザーが設定したマルチキャストエントリだけが表示されます。
- **igmp-snooping** – IGMP スヌープを使用して学習したエントリだけが表示されます。

デフォルト設定

なし

コマンドモード

特権実行

コマンドの使用法

選択するオプションによって、IGMP または USER のメンバータイプが表示されます。

例

次に、IGMP スヌープを使用して学習した、ブリッジグループ 1 の VLAN 1 に関するマルチキャストエントリを表示する例を示します。

```
Console#show mac-address-table multicast vlan 1 igmp-snooping
VLAN M'cast IP addr. Member ports Type
-----
      1      224.0.0.12      NETP0      USER
      1      224.1.2.3      NETP1      IGMP
Console#
```

4.3.14.6 ip igmp snooping querier

このコマンドは、スイッチを IGMP スヌープ照会元として使用可能にするために使用します。使用不可にする場合は、no 形式を使用します。

構文

```
ip igmp snooping querier
no ip igmp snooping querier
```

デフォルト設定

使用不可

コマンドモード

グローバル設定

コマンドの使用法

使用可能にすると、選択したスイッチは照会元として機能するようになります。照会元には、ホストがマルチキャストトラフィックの受信を要求しているかどうかを確認する役割があります。

例

```
Console(config)#ip igmp snooping querier
Console(config)#
```

4.3.14.7 ip igmp snooping query-count

このコマンドは、照会の回数を設定するために使用します。デフォルトに戻す場合は、no 形式を使用します。

構文

```
ip igmp snooping query-count count  
no ip igmp snooping query-count
```

count — 照会の最大発行回数を設定します。ここで設定した回数分の照会を行っても応答がない場合、照会元は、マルチキャストグループからそのクライアントを除外します (範囲: 2 ~ 10)。

デフォルト設定

2 回

コマンドモード

グローバル設定

コマンドの使用法

照会の回数によって、照会元が処理を行うまでに、マルチキャストクライアントからの応答を待機する時間を定義します。照会元がこのコマンドで定義した回数の照会を送信しても、クライアントからの応答がない場合は、
ip igmp snooping query-max-response-time によって定義した時間を使用してタイマーのカウントダウンが開始されます。カウントダウンが終了してもクライアントからの応答がない場合は、そのクライアントはマルチキャストグループから離脱したとみなします。

例

次に、照会の回数を 10 に設定する例を示します。

```
Console(config)#ip igmp snooping query-count 10  
Console(config)#
```

関連コマンド

ip igmp snooping query-max-response-time (4-131 ページ)

4.3.14.8 ip igmp snooping query-interval

このコマンドは、スヌープ照会の間隔を設定するために使用します。デフォルトに戻す場合は、no 形式を使用します。

構文

```
ip igmp snooping query-interval seconds  
no ip igmp snooping query-interval
```

seconds – スイッチが IGMP ホスト照会メッセージを送信する間隔の秒数 (範囲: 60 ~ 125)

デフォルト設定

125 秒

コマンドモード

グローバル設定

例

次に、照会間隔を 100 秒に設定する例を示します。

```
Console(config)#ip igmp snooping query-interval 100  
Console(config)#
```

4.3.14.9 ip igmp snooping query-max-response-time

このコマンドは、スヌープレポートの遅延を設定するために使用します。デフォルトに戻す場合は、このコマンドの no 形式を使用します。

構文

```
ip igmp snooping query-max-response-time seconds  
no ip igmp snooping query-max-response-time
```

seconds – IGMP 照会で通知するレポートの遅延の秒数 (範囲: 5 ~ 25)

デフォルト設定

10 秒

コマンドモード

グローバル設定

コマンドの使用法

- このコマンドを使用可能にするには、スイッチで IGMPv2 を使用する必要があります。
- このコマンドによって、照会後にマルチキャストクライアントからの応答を待機する期間を定義します。照会元が `ip igmp snooping query-count` によって定義した回数の照会を送信しても、クライアントからの応答がない場合は、このコマンドによって定義した値を初期値としてタイマーのカウントダウンが開始されます。カウントダウンが終了してもクライアントからの応答がない場合は、そのクライアントはマルチキャストグループから離脱したとみなします。

例

次に、最大応答時間を 20 秒に設定する例を示します。

```
Console(config)#ip igmp snooping query-max-response-time 20
Console(config)#
```

関連コマンド

`ip igmp snooping version` (4-126 ページ)
`ip igmp snooping query-max-response-time` (4-131 ページ)

4.3.14.10 ip igmp snooping router-port-expire-time

このコマンドは、スヌープ照会のタイムアウトを設定するために使用します。デフォルトに戻す場合は、このコマンドの `no` 形式を使用します。

構文

```
ip igmp snooping router-port-expire-time seconds  
no ip igmp snooping router-port-expire-time
```

seconds — 前の照会元が照会を停止してから、スイッチが待機する秒数を指定します。この時間を過ぎると、スイッチは、その照会パケットを受信していたインタフェースは照会元に接続しなくなったと判断します (範囲 : 300 ~ 500)。

デフォルト設定

300 秒

コマンドモード

グローバル設定

コマンドの使用法

このコマンドを使用可能にするには、スイッチで IGMPv2 を使用する必要があります。

例

次に、タイムアウトを 500 秒に設定する例を示します。

```
Console(config)#ip igmp snooping router-port-expire-time 500
Console(config)#
```

関連コマンド

`ip igmp snooping version` (4-126 ページ)

4.3.14.11 ip igmp snooping vlan mrouter

このコマンドは、マルチキャストルーターポートを静的に設定するために使用します。設定を削除する場合は、no 形式を使用します。

構文

```
ip igmp snooping vlan vlan-id mrouter interface  
no ip igmp snooping vlan vlan-id mrouter interface
```

- *vlan-id* – VLAN ID (範囲 : 1 ~ 4094)
- *interface*
 - **ethernet** *port-name*
port-name – ダウンリンク : SNP0 ~ 15、アップリンク : NETP0 ~ 7、
管理 : NETMGT
 - **port-channel** *channel-id* (範囲 : 1 ~ 6)

デフォルト設定

静的なマルチキャストルーターポートは設定されていません。

コマンドモード

グローバル設定

コマンドの使用法

ネットワーク接続によっては、IGMP スヌープが IGMP の照会元を検出できない場合があります。IGMP の照会元がネットワーク上でこのスイッチのインタフェース (ポートまたはトランク) に接続する既知のマルチキャストルーター/スイッチである場合は、そのインタフェースを手動で設定し、現在のすべてのマルチキャストグループに追加できます。

例

次に、VLAN 1 内のポート 11 をマルチキャストルーターポートとして設定する例を示します。

```
Console(config)#ip igmp snooping vlan 1 mrouter ethernet NETP0
Console(config)#
```

4.3.14.12 show ip igmp snooping mrouter

このコマンドは、静的に設定したマルチキャストルーターポート、および動的に学習したマルチキャストルーターポートに関する情報を表示するために使用します。

構文

```
show ip igmp snooping mrouter [vlan vlan-id]
```

vlan-id – VLAN ID (範囲 : 1 ~ 4094)

デフォルト設定

設定されたすべての VLAN のマルチキャストルーターポートが表示されます。

コマンドモード

特権実行

コマンドの使用法

マルチキャストルーターポートのタイプは、Static または Dynamic と表示されます。

例

次に、マルチキャストルーターに接続するポートを表示する例を示します。

```
Console#show ip igmp snooping mrouter
VLAN M'cast Router Ports Type
-----
   1                NETP5  Static
   2                NETP6  Dynamic
Console#
```

4.3.15 優先順位コマンド

ここで説明するコマンドを使用すると、回線が混雑してトラフィックがスイッチのバッファに入っているときの、データパケットの優先度を指定できます。このスイッチは、ポートごとに 4 つの優先順位キューを持つことで CoS をサポートしています。ポートの優先順位が高いキューのデータパケットは、優先順位が低いキューのデータパケットより先に送信されます。各インタフェースのデフォルトの優先順位、および各キューの相対的な加重、フレーム優先順位タグのスイッチ優先順位キューへの割り当てを設定できます。

コマンド	機能	モード	ページ
レイヤー 2 の優先順位コマンド			
switchport priority default	受信したタグなしフレームのポート優先順位を設定します。	IC	4-136
queue bandwidth	優先順位キューにラウンドロビン加重を割り当てます。	GC	4-137
queue cos map	優先順位キューにサービスクラス値を割り当てます。	IC	4-138
show queue bandwidth	優先順位キューに割り当てられたラウンドロビン加重を表示します。	PE	4-139
show queue cos-map	サービスクラス割り当てを表示します。	PE	4-140
show interfaces switchport	インタフェースの管理ステータスおよび動作ステータスを表示します。	PE	4-87
レイヤー 3 およびレイヤー 4 の優先順位コマンド			
map ip precedence	IP 優先順位のサービスクラスへの割り当てを使用可能にします。	GC	4-140
map ip precedence	サービスクラスに IP 優先順位値を割り当てます。	IC	4-141
map ip dscp	IP DSCP のサービスクラスへの割り当てを使用可能にします。	GC	4-142
map ip dscp	サービスクラスに IP DSCP 値を割り当てます。	IC	4-143
show map ip precedence	IP 優先順位割り当てを表示します。	PE	4-144
show map ip dscp	IP DSCP 割り当てを表示します。	PE	4-145

4.3.15.1 switchport priority default

このコマンドは、受信するタグなしフレームの優先順位、または指定したインタフェースに接続する装置が受信するフレームの優先順位を設定するために使用します。デフォルト値に戻す場合は、no 形式を使用します。

構文

```
switchport priority default default-priority-id  
no switchport priority default
```

default-priority-id - 受信するタグなしトラフィックの優先順位番号です。優先順位は 0 ~ 7 で指定し、もっとも高い優先順位は 7 です。

デフォルト設定

優先順位は設定されていません。インタフェースが受信するタグなしフレームのデフォルト値は 0 です。

コマンドモード

インタフェース設定 (Ethernet、Port Channel)

コマンドの使用法

- 優先順位は、IP 優先順位 (Precedence) または IP DSCP、次にデフォルトのスイッチポート優先順位の順に割り当てられます。
- デフォルトの優先順位は、すべてのフレームタイプ (タグなし、タグ付きの両方のフレーム) を受け入れるように設定されたポートが受信したタグなしフレームに適用されます。この優先順位は、IEEE 802.1Q VLAN タグ付きフレームには適用されません。受信したフレームが IEEE 802.1Q VLAN タグ付きフレームの場合は、IEEE 802.1p のユーザー優先順位ビットを使用します。
- このスイッチには、ポートごとに 4 つの優先順位キューがあります。スイッチは加重ラウンドロビン方式を使用するように設定されています。この設定は、queue bandwidth コマンドを使用して確認できます。VLAN タグが付いていない受信フレームには、受信ポートのデフォルトのユーザー優先順位がタグとして付けられて、送信ポートの適切な優先順位キューに格納されます。すべての受信ポートのデフォルトの優先順位は 0 です。したがって、優先順位タグが付いていないすべての受信フレームは、送信ポートのキュー 0 に格納されます。送信ポートが、関連付けられた VLAN のタグなしメンバーである場合は、送信前にフレームの VLAN タグが外されることに注意してください。

例

次に、ポート SNP3 のデフォルトの優先順位を 5 に設定する例を示します。

```
Console(config)#interface ethernet SNP3  
Console (config-if)#switchport priority default 5
```

4.3.15.2 queue bandwidth

このコマンドは、加重ラウンドロビン (Weighted Round Robin : WRR) の加重を 4 つのサービスクラス (CoS) 優先順位キューに割り当てるために使用します。デフォルトの加重に戻す場合は、no 形式を使用します。

構文

```
queue bandwidth weight1...weight4  
no queue bandwidth
```

weight1...weight4 – キュー 0 ~ 3 の加重比率によって、WRR スケジューラが使用する加重が決定します (範囲 : 1 ~ 255)。

デフォルト設定

キュー 0、1、2、3 には、それぞれ 16、64、128、240 の加重が割り当てられています。

コマンドモード

グローバル設定

コマンドの使用法

WRR を使用すると、指定した加重スケジューリングによって送信ポートの帯域幅を共有できます。

例

次に、CoS 優先順位キュー 0、1、2、3 に WRR 加重 1、3、5、7 を割り当てる例を示します。

```
Console(config)#queue bandwidth 1 3 5 7  
Console(config)#
```

関連コマンド

show queue bandwidth (4-139 ページ)

4.3.15.3 queue cos-map

このコマンドは、CoS 優先順位キューに CoS 値を割り当てるために使用します。CoS 割り当てをデフォルト値に戻す場合は、no 形式を使用します。

構文

```
queue cos-map queue_id [cos1 ... cosn]
no queue cos-map
```

- *queue_id* – CoS 優先順位キューのキュー ID。範囲は 0～3 で、CoS 優先順位がもっとも高いキューは 3 です。
- *cos1 .. cosn* – キュー ID に割り当てられる CoS 値。数字を空白文字で区切って指定します。CoS 値は 0～7 で、もっとも高い優先順位は 7 です。

デフォルト設定

このスイッチは、4 つの優先順位キューを使用して、ポートごとに加重ラウンドロビンキューイングを行うことでサービスクラスをサポートしています。IEEE 802.1p には、8 つの異なるトラフィッククラスが定義されています。デフォルトの優先レベルは、次の表に示す IEEE 802.1p 標準の推奨事項に従って割り当てられます。

	キュー			
	0	1	2	3
優先順位		0		
	1			
	2			
		3		
			4	
			5	
				6
				7

コマンドモード

インタフェース設定 (Ethernet、Port Channel)

コマンドの使用法

受信ポートで割り当てられた CoS 値は、送信ポートで CoS 優先順位を選択するために使用されます。

例

次に、CoS 値 0、1、2 を CoS 優先順位キュー 0 に、CoS 値 3 を CoS 優先順位キュー 1 に、CoS 値 4、5 を CoS 優先順位キュー 2 に、CoS 値 6、7 を CoS 優先順位キュー 3 に割り当てる例を示します。

```
Console(config)#interface ethernet SNP1
Console(config-if)#queue cos-map 0 0 1 2
Console(config-if)#queue cos-map 1 3
Console(config-if)#queue cos-map 2 4 5
Console(config-if)#queue cos-map 3 6 7
Console(config-if)#
```

関連コマンド

`show queue cos-map` (4-140 ページ)

4.3.15.4 show queue bandwidth

このコマンドは、4 つの CoS 優先順位キューに割り当てられた WRR 帯域幅を表示するために使用します。

デフォルト設定

なし

コマンドモード

特権実行

例

```
Console#show queue bandwidth
Queue ID Weight
-----
0          16
1          64
2         128
3         240
Console#
```

4.3.15.5 show queue cos-map

このコマンドは、サービスクラス優先順位割り当てを表示するために使用します。

構文

```
show queue cos-map [interface]
```

```
interface
```

- **ethernet** *port-name*

port-name - ダウンリンク : SNP0 ~ 15、アップリンク : NETP0 ~ 7、
管理 : NETMGT

- **port-channel** *channel-id* (範囲 : 1 ~ 6)

デフォルト設定

なし

コマンドモード

特権実行

例

```
Console#show queue cos-map ethernet SNP11
Information of SNP11
Queue ID Traffic class
-----
      0      1 2
      1      0 3
      2      4 5
      3      6 7
Console#
```

4.3.15.6 map ip precedence (グローバル設定)

このコマンドは、IP 優先順位割り当て (IP サービスタイプ) を使用可能にするために使用します。IP 優先順位割り当てを使用不可にする場合は、no 形式を使用します。

構文

```
map ip precedence
```

```
no map ip precedence
```

デフォルト設定

使用可能

コマンドモード

グローバル設定

コマンドの使用法

- 優先順位は、IP 優先順位 (Precedence) または IP DSCP、次にデフォルトのスイッチポート優先順位の順に割り当てられます。
- IP 優先順位および IP DSCP を両方とも使用可能にすることはできません。優先順位タイプ的一方を使用可能にすると、もう一方のタイプは自動的に使用不可になります。

例

次に、IP 優先順位割り当てをグローバルに使用可能にする例を示します。

```
Console(config)#map ip precedence
Console(config)#
```

4.3.15.7 map ip precedence (インタフェース設定)

このコマンドは、IP 優先順位 (IP サービスタイプの優先順位) を設定するために使用します。デフォルトの設定に戻す場合は、no 形式を使用します。

構文

```
map ip precedence ip-precedence-value cos cos-value
no map ip precedence
```

- *precedence-value* – 3 ビットの優先順位値 (範囲 : 0 ~ 7)
- *cos-value* – サービスクラス値 (範囲 : 0 ~ 7)

デフォルト設定

1 対 1 の割り当て (優先順位値 0 は CoS 値 0 にと、順に割り当てられます。)

コマンドモード

インタフェース設定 (Ethernet、Port Channel)

コマンドの使用法

- 優先順位は、IP 優先順位 (Precedence) または IP DSCP、次にデフォルトのスイッチポート優先順位の順に割り当てられます。
- IP 優先順位値は、IEEE 802.1p 標準の推奨事項に従ってデフォルトの CoS 値に 1 対 1 で割り当てられてから、キューのデフォルト値に割り当てられます。
- IP 優先順位への値の割り当てにはインタフェース設定コマンドを使用しますが、変更内容はスイッチ上のすべてのインタフェースに適用されます。

例

次に、IP 優先順位値 1 を CoS 値 0 に割り当てる例を示します。

```
Console(config)#interface ethernet SNP5
Console(config-if)#map ip precedence 1 cos 0
Console(config-if)#
```

4.3.15.8 map ip dscp (グローバル設定)

このコマンドは、IP DSCP (Differentiated Services Code Point) 割り当てを使用可能にするために使用します。IP DSCP 割り当てを使用不可にする場合は、no 形式を使用します。

構文

```
map ip dscp
no map ip dscp
```

デフォルト設定

使用可能

コマンドモード

グローバル設定

コマンドの使用法

- 優先順位は、IP 優先順位 (Precedence) または IP DSCP、次にデフォルトのスイッチポート優先順位の順に割り当てられます。
- IP 優先順位および IP DSCP を両方とも使用可能にすることはできません。優先順位タイプ的一方を使用可能にすると、もう一方のタイプは自動的に使用不可になります。

例

次に、IP DSCP 割り当てをグローバルに使用可能にする例を示します。

```
Console(config)#map ip dscp
Console(config)#
```

4.3.15.9 map ip dscp (インタフェース設定)

このコマンドは、IP DSCP (Differentiated Services Code Point) 優先順位を設定するために使用します。デフォルトの設定に戻す場合は、no 形式を使用します。

構文

```
map ip dscp dscp-value cos cos-value  
no map ip dscp
```

- *dscp-value* - 8 ビットの DSCP 値 (範囲: 0 ~ 255)
- *cos-value* - サービスクラス値 (範囲: 0 ~ 7)

デフォルト設定

次の表に、DSCP のデフォルト値を示します。次の表に示されていない DSCP 値は、CoS 値 0 に割り当てられます。

IP DSCP 値	CoS 値
0	0
8	1
10, 12, 14, 16	2
18, 20, 22, 24	3
26, 28, 30, 32, 34, 36	4
38, 40, 42	5
48	6
46, 56	7

コマンドモード

インタフェース設定 (Ethernet、Port Channel)

コマンドの使用法

- 優先順位は、IP 優先順位 (Precedence) または IP DSCP、次にデフォルトのスイッチポート優先順位の順に割り当てられます。
- DSCP 優先順位値は、IEEE 802.1p 標準の推奨事項に従ってデフォルトの CoS 値に割り当てられてから、キューのデフォルト値に割り当てられます。
- DSCP への値の割り当てにはインタフェース設定コマンドを使用しますが、変更内容はスイッチ上のすべてのインタフェースに適用されます。

例

次に、IP DSCP 値 1 を CoS 値 0 に割り当てる例を示します。

```
Console(config)#interface ethernet SNP5
Console(config-if)#map ip dscp 1 cos 0
Console(config-if)#
```

4.3.15.10 show map ip precedence

このコマンドは、IP 優先順位割り当てを表示するために使用します。

構文

show map ip precedence [*interface*]

interface

- **ethernet** *port-name*

port-name – ダウンリンク : SNP0 ~ 15、アップリンク : NETP0 ~ 7、
管理 : NETMGT

- **port-channel** *channel-id* (範囲 : 1 ~ 6)

デフォルト設定

なし

コマンドモード

特権実行

例

```
Console#show map ip precedence ethernet SNP5
Precedence mapping status: disabled

  Port          Precedence COS
  -----
          SNP5          0    0
          SNP5          1    1
          SNP5          2    2
          SNP5          3    3
          SNP5          4    4
          SNP5          5    5
          SNP5          6    6
          SNP5          7    7
Console#
```

関連コマンド

map ip precedence (グローバル設定) (4-140 ページ)
map ip precedence (インタフェース設定) (4-141 ページ)

4.3.15.11 show map ip dscp

このコマンドは、IP DSCP 優先順位割り当てを表示するために使用します。

構文

```
show map ip dscp [interface]  
interface  
  ■ ethernet port-name  
    port-name — ダウンリンク : SNP0 ~ 15、アップリンク : NETP0 ~ 7、  
    管理 : NETMGT  
  ■ port-channel channel-id (範囲 : 1 ~ 6)
```

デフォルト設定

なし

コマンドモード

特権実行

例

```
Console#show map ip dscp ethernet SNP1  
DSCP mapping status: disabled  
  
Port          DSCP COS  
-----  
SNP1          0    0  
SNP1          1    0  
SNP1          2    0  
SNP1          3    0  
:  
:  
SNP1          61   0  
SNP1          62   0  
SNP1          63   0  
Console#
```

関連コマンド

map ip dscp (グローバル設定) (4-142 ページ)
map ip dscp (インタフェース設定) (4-143 ページ)

4.3.16 ミラーポートコマンド

ここでは、ソースポートのトラフィックをターゲットポートにミラー化する方法について説明します。

コマンド	機能	モード	ページ
port monitor	ミラーセッションを設定します。	IC	4-146
show port monitor	ミラーポートの設定を表示します。	PE	4-147

4.3.16.1 port monitor

このコマンドは、ミラーセッションを設定するために使用します。ミラーセッションを消去する場合は、no 形式を使用します。

注 – Sun Fire B1600 ブレードシステムシャーシの統合スイッチは、相互に接続する 2 つのスイッチチップで構成されています。あるポートのトラフィックは、同じスイッチチップ上の別のポートだけにミラー化できます。ポート NETP0 および NETP1、NETP4、NETP5、SNP8 ~ 15 は、一方のスイッチチップ上にあります。ポート NETP2 および NETP3、NETP6、NETP7、SNP0 ~ 7 は、もう一方のスイッチチップ上にあります (SSC の背面パネルの右側にあるすべてのポートが一方のチップ上に、左側にあるすべてのポートがもう一方のチップ上にあります)。

構文

```
port monitor interface [rx | tx | both]
no port monitor interface
```

- *interface* – **ethernet** *port-name*
port-name – ダウンリンク : SNP0 ~ 15、アップリンク : NETP0 ~ 7、
管理 : NETMGT
ここで指定したインタフェースがソースポートになります。
- **rx** – 受信パケットのミラー化
- **tx** – 送信パケットのミラー化
- **both** – 受信パケットおよび送信パケットの両方をミラー化

デフォルト設定

ミラーセッションは定義されていません。使用可能にすると、デフォルトでは受信パケットおよび送信パケットの両方がミラー化されます。

コマンドモード

インタフェース設定 (Ethernet、宛先ポート)

コマンドの使用法

- リアルタイム分析を行うために、ソースポートのトラフィックを宛先ポートにミラー化できます。ミラー化した宛先ポートにロジックアナライザまたは RMON プロンプを設置すると、運用に影響を与えることなく、ソースポートを通過するトラフィックを調査できます。
- `interface` コマンドで指定した **Ethernet** インタフェースが、宛先ポートになります。

例

次に、ポート SNP6 のすべてのパケットをポート NETP2 にミラー化する例を示します。

```
Console(config)#interface ethernet NETP2
Console(config-if)#port monitor ethernet SNP6 both
Console(config-if)#
```

関連コマンド

`show port monitor` (4-147 ページ)

4.3.16.2 show port monitor

このコマンドは、ミラー化に関する情報を表示するために使用します。

構文

show port monitor [*interface*]

interface — **ethernet** *port-name*

port-name — ダウンリンク : SNP0 ~ 15、アップリンク : NETP0 ~ 7、
管理 : NETMGT

ここで指定したインタフェースがソースポートになります。

デフォルト設定

すべてのセッションが表示されます。

コマンドモード

特権実行

コマンドの使用法

このコマンドを実行すると、現在設定されているソースポートおよび宛先ポート、ミラーモード (RX、TX、RX/TX) が表示されます。

例

次に、SNP6 ポートから NETP2 ポートへのミラー化を設定する例を示します。

```
Console(config)#interface ethernet NETP2
Console(config-if)#port monitor ethernet SNP6
Console(config-if)#end
Console#show port monitor
Port Mirroring
-----
Destination port(listen port):NETP2
Source port(monitored port) :SNP6
Mode :RX/TX
Console#
```

関連コマンド

port monitor (4-146 ページ)

4.3.17 ポートトランクコマンド

ポートを1つの集約リンク(トランク)に静的にグループ化すると、ネットワーク接続の帯域幅を拡張し、障害回復力を向上できます。また、**Link Aggregation Control Protocol (LACP)** を使用して、スイッチと別のネットワーク装置との間で自動的にトランクリンクのネゴシエーションが行われるように設定することもできます。静的トランクを設定するには、同じタイプのスイッチを使用する必要があります。動的トランクを設定する場合は、LACPに準拠するスイッチを使用します。このスイッチは、最大6つのトランクをサポートします。たとえば、2つの1000 Mbpsポートで構成されるトランクを全二重モードで動作させると、4 Gbpsの集約帯域幅がサポートされます。

コマンド	機能	モード	ページ
手動設定コマンド			
interface port-channel	トランクを設定し、そのトランクのインタフェース設定モードを開始します。	GC	4-75
channel-group	ポートをトランクに追加します。	IC	4-149
動的設定コマンド			
lacp	現在のインタフェースにLACPを設定します。	IC	4-150
トランクステータス表示コマンド			
show interfaces status port-channel	トランクに関する情報を表示します。	NE、PE	4-84

トランクを作成するためのガイドライン

- ループが形成されないように、スイッチ間の対応するネットワークケーブルを接続する前に、ポートトランクの設定を終了しておく必要があります。
- 1つのトランクには、最大4つのアップリンクポート、または最大2つのダウンリンクポートを設定できます。
- 接続の両端のポートをトランクポートとして設定する必要があります。
- トランク内のすべてのポートは、通信モード (速度およびデュプレックスモード、フロー制御)、VLAN 割り当て、CoS 設定などの設定内容を同一にする必要があります。
- 特定のポートチャネルを介して VLAN に対する移動または追加、削除を行う場合は、トランク内のすべてのポートをまとめて取り扱う必要があります。
- STP および VLAN、IGMP は、特定のポートチャネルを介してトランク全体に対してのみ設定できます。

4.3.17.1 channel-group

このコマンドは、静的トランクにポートを追加するために使用します。トランクからポートを削除する場合は、no 形式を使用します。

構文

```
channel-group channel-id  
no channel-group
```

channel-id – トランクのインデックス (範囲 : 1 ~ 6)

デフォルト設定

現在のポートがこのトランクに追加されます。

コマンドモード

インタフェース設定 (Ethernet)

コマンドの使用法

- 静的トランクを設定する場合は、同じタイプのスイッチだけをリンクできます。
- トランクからポートグループを削除するには、no channel-group を使用します。
- スイッチからトランクを削除するには、no interfaces port-channel を使用します。

例

次に、トランク 1 を作成してポート NETP2 を追加する例を示します。

```
Console(config)#interface port-channel 1
Console(config-if)#exit
Console(config)#interface ethernet NETP2
Console(config-if)#channel-group 1
Console(config-if)#
```

4.3.17.2 lacp

このコマンドは、現在のインタフェースに対して 802.3ad LACP を使用可能にするために使用します。使用不可にする場合は、no 形式を使用します。

構文

```
lacp
no lacp
```

デフォルト設定

使用可能

コマンドモード

インタフェース設定 (Ethernet)

コマンドの使用法

- LACP トランクの両端のポートは、強制モードまたは自動ネゴシエーションのいずれかを使用して、全二重に設定する必要があります。
- LACP を使用してほかのスイッチとトランクを形成すると、自動的に次に使用できるポートチャネル ID が割り当てられます。
- ターゲットスイッチの接続ポートでも LACP が使用可能になっていると、トランクは自動的にアクティブになります。
- 同じターゲットスイッチに 5 つ以上のポートを接続して LACP が使用可能になっている場合、5 つ目以降の追加ポートはスタンバイモードになり、アクティブなリンクが接続に失敗した場合にのみ使用可能になります。

例

次に、ポート NETP0 ~ NETP2 上で LACP を使用可能にする例を示します。リンクのもう一方の端のポートでも LACP が使用可能になっているため、`show interfaces status port-channel 1` コマンドを実行すると、Trunk1 が確立されたことが示されます。

```
Console(config)#interface ethernet NETP0
Console(config-if)#lacp
Console(config-if)#exit
Console(config)#interface ethernet NETP1
Console(config-if)#lacp
Console(config-if)#exit
Console(config)#interface ethernet NETP2
Console(config-if)#lacp
Console(config-if)#exit
Console(config)#exit
Console#show interfaces status port-channel 1
Information of Trunk 1
Basic information:
  Port type: 1000t
  Mac address: 00-00-e8-00-00-0b
Configuration:
  Name:
  Port admin status: Up
  Speed-duplex: Auto
  Capabilities: 10half, 10full, 100half, 100full, 1000full
  Flow control status: Disabled
Current status:
  Created by: lacp
  Link status: Up
  Operation speed-duplex: 1000full
  Flow control type: None
  Member Ports: NETP0, NETP1, NETP2,
Console#
```


PART III 付録

ここでは、次の項目の追加情報について説明します。

管理情報ベース

障害追跡

仕様

付録 A

管理情報ベース

SNMP 管理ホストでは、管理情報ベース (Management Information Base : MIB) のデバイス変数を設定または読み取ることによって、ネットワーク装置を設定および監視できます。この付録では、このスイッチがサポートする重要な MIB グループのリストを示します。それぞれの設定作業で使用する具体的な MIB 変数については、第 3 章「管理作業の概要」を参照してください。

A.1 サポートする MIB

次の表に、標準的な MIB を示します。

RFC 番号	名称	サポートするグループ
1213	MIB-II	<ul style="list-style-type: none">• system グループ• interfaces グループ• ip グループ• icmp グループ• tcp グループ• udp グループ• snmp グループ
1493	Bridge MIB	<ul style="list-style-type: none">• dot1dBase グループ• dot1dStp グループ• dot1dTp グループ• dot1dStatic グループ
2863	Interfaces Evolution MIB	<ul style="list-style-type: none">• ifXTable グループ• ifStackTable グループ

RFC 番号	名称	サポートするグループ
2819	RMON MIB	<ul style="list-style-type: none"> • statistics グループ • history グループ • alarm グループ • event グループ
2618	RADIUS MIB	<ul style="list-style-type: none"> • radiusAuthClientMIB
2665	Etherlike MIB	<ul style="list-style-type: none"> • dot3StatsTable グループ
2737	Entity MIB	<ul style="list-style-type: none"> • entityPhysical グループ
2674	P-bridge	<ul style="list-style-type: none"> • dot1dExtBase グループ • dot1dPriority グループ • dot1dGarp グループ
2674	Q-bridge	<ul style="list-style-type: none"> • dot1qBase グループ • dot1qTp グループ • dot1qStatic グループ • dot1qVlan

次に、サンのプライベートエンタープライズ MIB を示します。

名称	バージョン
CSSP.MIB	01.00.00

A.2 サポートトラップ

サポートされている SNMP トラップには、次の項目が含まれています。

RFC 番号	項目
RFC 1215 (SNMPv1)、 RFC 1907 (SNMPv2c)	<ul style="list-style-type: none">• coldStart• linkDown• linkUp• authenticationFailure
RFC 1493	<ul style="list-style-type: none">• newRoot• topologyChange
RFC 2819	<ul style="list-style-type: none">• risingAlarm• fallingAlarm

サポートするサンのプライベートエンタープライズトラップには、次の項目が含まれています。

名称	項目
CSSP.MIB	<ul style="list-style-type: none">• swPowerStatusChangeTrap

付録 B

障害追跡

ネットワーク接続に問題が発生した場合は、ネットワークのケーブル配線を確認して、問題の装置がネットワークに正しく接続されているかどうかを確認します。次に、B-1 ページの「スイッチのインジケータによる診断」を参照して、スイッチの対応するポートが正常に機能しているかどうかを確認します。

管理インタフェースへの接続に問題がある場合は、B-2 ページの「管理インタフェースへのアクセス」の障害追跡手順を参照してください。

B.1 スwitchのインジケータによる診断

装置をスイッチのポートに接続したのにリンク LED が消灯したままである場合は、次の事項を確認してください。

- ケーブルがスイッチと対応する装置の両方に接続されていることを確認します。
- 適切なタイプのケーブルを使用していて、ケーブルの長さが規定の上限を超えていないことを確認します。
- 接続する装置のアダプタを確認して、ケーブルとの接合部分に不具合がないかどうかを確認します。必要に応じて、不具合のあるアダプタまたはケーブルを交換します。

すべてのシステムコンポーネントが正しく設置されていることを確認します。ネットワークのケーブル配線に不具合があった場合は、問題の部品をすべてのコンポーネントが正常に動作している別の環境に取り付けてテストします。

B.2 ポート接続の診断

ポートが正常に動作しない場合は、次の事項を確認してください。

- ケーブルがしっかりと接続されており、ケーブルがリンクの両端で正しいポートに接続されていることを確認します。
- ポートステータス (Admin) および自動ネゴシエーション機能が使用可能になっているか、リンクの両端のポートに同じ通信速度およびデュプレックスモードが設定されていることを確認します。詳細は、3-80 ページの「ポートの設定」を参照してください。

B.3 管理インタフェースへのアクセス

スイッチの管理インタフェースには、接続するネットワーク内のどこからでも、telnet または Web ブラウザ、SNMP ベースの任意のネットワーク管理ソフトウェアを使用してアクセスできます。管理インタフェースへのアクセスに問題がある場合は、次に示す障害追跡情報を参照してください。

telnet または Web ブラウザ、SNMP ソフトウェアを使用して接続できない場合は、次の事項を確認してください。

- サーバシャーシに電源が入っていることを確認します。
- 管理ホストとスイッチの間のネットワークケーブル配線を確認します。
- スイッチへのネットワーク接続が機能していて、使用するポートが使用不可になっていないことを確認します。詳細は、3-80 ページの「ポートの設定」を参照してください。
- 管理ホストとサーバシャーシの間にレイヤー 2 スイッチだけがある場合は、次の事項を確認します。
 - スイッチの管理 VLAN に有効な IP アドレスおよびサブネットマスクが設定されていること
 - 管理ホストの IP アドレスが管理 VLAN と同じサブネットに含まれていること
 - 管理ホストが管理 VLAN のメンバーであるスイッチポートに接続されていること
 - ネットワークの中間スイッチに接続するポートがタグ付きポートで、管理 VLAN のメンバーであること
- 管理ホストとサーバシャーシの間に 1 つ以上のレイヤー 3 スイッチがある場合は、次の事項を確認します。

- スイッチの管理 VLAN に有効な IP アドレスおよびサブネットマスク、デフォルトゲートウェイが設定されていること
- 管理ホストに有効な IP アドレスおよびサブネットマスク、デフォルトゲートウェイが設定されていること
- 管理ホストが管理 VLAN のメンバーであるスイッチポートに接続されていること
- ネットワークの中間スイッチおよびレイヤー 3 スイッチに接続するポートがタグ付きポートで、管理 VLAN のメンバーであること
- telnet で接続できない場合は、同時に起動できる telnet セッション数の上限を超えている可能性があります。しばらく時間をおいてから接続を試みてください。

シリアルポート接続を介してオンボードの設定プログラムに接続できない場合は、次の事項を確認してください。

- Sun Fire B1600 ブレードシャーシに付属する DB-9 - RJ-45 変換ケーブルを使用して、端末またはコンピュータを SSC モジュールのシリアルポートに接続していることを確認します。
- 端末エミュレータプログラムが VT100 互換、データビット 8、ストップビット 1、パリティなし、9600 bps に設定されていることを確認します。
- ヌルモデムシリアルケーブルが、付録 B に示すピン配列どおりであることを確認します。

B.4 システムログの使用

障害が発生した場合には、このサーバーシャーシに関するほかのマニュアルを参照して、スイッチに起因する障害であるかどうかを確認します。障害の原因がスイッチであると考えられる場合は、次の手順を実行します。

1. ログイングを使用可能にします。
2. すべてのカテゴリのエラーメッセージが報告されるように設定します。
3. エラーメッセージを受信する SNMP ホストを指定します。
4. コマンド実行などのエラーが発生する操作を繰り返します。
5. 障害が発生するコマンドや状況のリストを作成します。また、表示されるエラーメッセージのリストも作成します。
6. ご購入先に連絡します。

例

```
Console(config)#logging on
Console(config)#logging history flash 7
Console(config)#snmp-server host 10.1.0.23
.
.
.
```

B.4.1 ログメッセージ

次の表に、このスイッチが生成するログメッセージを示します。

表 B-1 ログメッセージ

メッセージ	説明	レベル*
System coldStart notification	スイッチがコールドブートしました。	5
System warmStart notification	システムがウォームブートしました。	5
Unit 1 Port YY link-up notification	ポートリンクが接続されました。	6
Unit 1 Port YY link-down notification	ポートリンクが切断されました。	6
Trunk 1 link-up notification	トランクリンクが接続されました。	6
Trunk 1 link-down notification	トランクリンクが切断されました。	6
VLAN XX link-up notification	VLAN リンクが接続されました。	6
VLAN XX link-down notification	VLAN リンクが切断されました。	6
Authentication failure notification	SNMP アクセス認証に失敗しました。	6
STA root change notification	STA ルートが変更されました。	6
STA topology change notification	STA トポロジが変更されました。	6
RMON rising alarm notification	RMON 上昇アラーム	6
RMON falling alarm notification	RMON 下降アラーム	6

「Unit 1 Port YY」は、ユニット1、ポート YY (YY:1～25) を表します。

「VLAN XX」は、VLAN ID 値 (XX:1～4094) を表します。

* Syslog メッセージのレベルです。詳細は、4-30 ページの「logging history」を参照してください。

B.5 エラーメッセージ

B.5.1 コマンド行エラーの検出

スイッチは、コマンド行で無効な入力が行われたことを検出すると、検出したエラー箇所の下に「^」を表示します。たとえば、次のように表示します。

```
Console#show interfaces status s e 1/1
                                     ^
% Invalid input detected at '^' marker.
```

B.5.2 システムエラー

次の表に、このスイッチが生成する主なエラーメッセージを示します。スイッチが出力するメッセージのレベルを制御する方法については、4-30 ページの「logging history」を参照してください。

表 B-2 システムエラーメッセージ

メッセージ	説明	レベル*
<module> create task fail.	このソフトウェアモジュールは、タスクを生成できません。	2
<module> task idle too long.	このソフトウェアモジュールは、アイドル状態になっている時間が長すぎます。	2
Allocate <string> memory fail.	<string> へのメモリーの割り当てに失敗しました。	2
Free <string> memory fail.	<string> のメモリーの解放に失敗しました。	2
<string> switch to default.	指定された値が無効であるか、サポートされていません。デフォルト値を使用します。有効な値については、オンラインヘルプまたはこのマニュアルを参照してください。	3

<module> には、スイッチのソフトウェアモジュール (STA、VLAN、XFER、TRAP、RMON など) が表示されます。
<string> には、設定時に指定された値が表示されます。

* Syslog メッセージのレベルです。詳細は、4-30 ページの「logging history」を参照してください。

B.5.3 コマンド行エラー

次の表に、スイッチがコマンド行インタフェースで生成するエラーメッセージを示します。これらのメッセージは、ログファイルには書き込まれません。

表 B-3 コマンド行エラーメッセージ

メッセージ	説明
Ambiguous command:<string>	コマンドがあいまいです。
Clear dynamic address error.	動的アドレスを消去できません。
CLI internal error - contact your local service provider.	CLI コマンドの内部エラーが発生しました。
Copy error.	コピーに失敗しました。
Exec-timeout could not be disabled for vty session.	telnet セッションでは <code>exec-timeout</code> を無効にできません。
Factory default configuration file cannot be deleted.	出荷時のデフォルト設定ファイルは削除できません。
Factory default configuration file cannot be replaced.	出荷時の構成ファイルは置換できません。
Failed to allocate resource.	リソースが不足しています。
Failed to get <string>	表示コマンドが失敗しました。
Failed to set <string>	設定コマンドが失敗しました。
Failed to write certificate file to flash.	証明書ファイルエラー、非公開鍵ファイルエラー (不正なパスフレーズなど)、非公開鍵と証明書の公開鍵との不一致のいずれかが発生しました。
Incomplete command.	コマンドが不完全です。
Insufficient memory.	メモリーが不足しています。
Insufficient memory to display or save running config.	すべての情報を収集するための容量が不足しています。
Invalid file name.	無効なファイル名が入力されました。
Invalid input.	誤ったキー入力が行われました。
Invalid input detected at '^' marker.	コマンドが無効です。
Invalid parameter.	ping のパラメタが無効です。
Invalid parameter value/range.Type "?" to get more detail information.	値または文字列長が制限を超えています。
Invalid TFTP server IP address.	TFTP の IP アドレスエラーが発生しました。
Not enough resources; please try later.	ping 機能のためのリソースがありません。

表 B-3 コマンド行エラーメッセージ (続き)

メッセージ	説明
No such file.	指定されたファイルが存在しません。
No such VLAN.	指定された VLAN が存在しません。
Port <port name> does not exist.	指定されたポート名が存在しません。
Port <port name> is an ethernet port.	指定されたポートは Ethernet ポートです。
Port <port name> is not present.	インタフェースモードに入るとき、指定されたポートが存在しませんでした。
Port <port name> unknown.	指定されたポートが不明です。
Session terminated.	CLI によって、現在のセッションが終了されました。
Session timed out.	接続セッションがタイムアウトしました。
Startup file cannot be deleted.	起動ファイルは削除できません。
This command for console only.	回線モード vty では、コンソールパラメタコマンドを使用できません。
This command is only valid for adding a single port to a trunk.	このコマンドを使用してトランクに追加できるポートは 1 つだけです。
This command is only valid for the name of a single port.	複数のポートを選択してポートの説明を設定することはできません。
This command is not supported for management port in current release.	<code>no switchport allow vlan</code> コマンドは、管理ポートには使用できません。
Trunk ID:<trunk> is out of range.	指定されたトランク ID は無効です。
Trunk <trunk> does not exist.	指定されたトランクは存在しません。
Trunk <trunk> is a normal trunk.	通常のトランクが指定されました。
Trunk with no members cannot be displayed.	トランクのメンバーを設定または表示できません。
Type "show ?" for a list of subcommands.	「show」だけを入力しました。
Unknown error.	不明なエラーが発生しました。
Unrecognized command.	認識できないコマンドを実行しました。

<string> には、コマンドで指定した値が表示されます。

B.5.4 Web インタフェースエラー

次の表に、このスイッチが生成する Web インタフェースに関するエラーメッセージを示します。これらのメッセージは、ログファイルには書き込まれません。

表 B-4 Web インタフェースエラーメッセージ

メニュー	メッセージ	説明
Switch Setup		
System Identity	User privileges are not enough to perform this operation.	権限が不十分です。
Network Identity	Current IP Address Mode is not DHCP or BOOTP.	DHCP を再起動したとき、スイッチは DHCP または BOOTP のいずれかのモードになっている必要があります。
	Data is invalid.	一般的なエラーです。
	Set DHCP Client-ID error.	DHCP クライアント ID の設定に失敗しました。
	User privileges are not enough to perform this operation.	権限が不十分です。
Software	Data is invalid.	一般的なエラーです。
	Please input a destination file.	ダウンロードまたはアップロード先のファイル名を入力してください。
	Please input a source file.	ダウンロードまたはアップロード元のファイル名を入力してください。
	Please input or select a destination file.	ダウンロードまたはアップロード先のファイル名を入力または選択してください。
	Please select a file.	ダウンロードまたはアップロード元のファイルを選択してください。
	System will be restarted...	システムが再起動されます。
	User privileges are not enough to perform this operation.	権限が不十分です。
Switch Config		
Security	Cannot add user.	ユーザー名が無効であるか、ユーザー数の上限を超えました。
	Cannot set password for user.	パスワードが無効です。
	Cannot set user privilege.	ユーザーテーブルに問題が発生しました。
	Cannot set user status.	ユーザーテーブルに問題が発生しました。
	User does not exist.	ユーザーテーブルに問題が発生しました。

表 B-4 Web インタフェースエラーメッセージ (続き)

メニュー	メッセージ	説明
Communication	Community String cannot contain spaces.	コミュニティー文字列には空白文字を使用できません。
	Community table is full or data is invalid.	コミュニティーテーブルがいっぱいであるか、データが無効です。
	Data is invalid.	一般的なエラーです。
	Illegal SNMP trap IP address.	IP アドレスの形式が不正です。
	Please select a Community String.	削除するコミュニティー文字列を選択してください。
	Please type a Community String.	追加するコミュニティー文字列を入力してください。
	Trap Manager table is full or data is invalid.	トラップマネージャーテーブルがいっぱいであるか、データが無効です。
	User privileges are not enough to perform this operation.	権限が不十分です。
Security	You must specify an IP trap community string.	追加する IP トラップコミュニティー文字列を入力してください。
	Authentication type doesn't exist.	認証タイプ Local または TACACS、RADIUS のいずれかがサポートされていません。
	Data is invalid	一般的なエラーです。
	Illegal IP address.	IP アドレスの形式が不正です。
	Number of Server Transmits is out of range.	RADIUS の再転送数が範囲外です。
	Password too long.	パスワードが最大長を超えています。
	Please input username.	新しいユーザーを追加するためのユーザー名を入力してください。
	Please select an user	削除またはパスワードを変更するユーザーを選択してください。
	RADIUS KEY is invalid	RADIUS の暗号化鍵が無効です。
	Server Port Number is out of range.	RADIUS のポート番号が範囲外です。
	Select a privilege level.	ユーザーを追加するための特権レベルを選択してください。
	TACACS PORT is invalid	TACACS のポートが無効です。
TACACS KEY is invalid	TACACS の鍵が無効です。	
Timeout is out of range.	RADIUS のタイムアウト値が範囲外です。	
User privileges are not enough to perform this operation.	権限が不十分です。	

表 B-4 Web インタフェースエラーメッセージ (続き)

メニュー	メッセージ	説明
VLAN	Cannot create VLAN.	VLAN ID が無効であるか、VLAN 数がサポートされる上限を超えています。
	Cannot set VLAN name.	VLAN 名が無効です。
	Cannot set VLAN status.	VLAN 1、または管理ポートのネイティブ VLAN (PVID) に設定されている VLAN は、使用不可にできません。
	Cannot delete VLAN.	メンバーが存在する VLAN、またはインタフェースのネイティブ VLAN (PVID) に設定されている VLAN は削除できません。
	Data is invalid	一般的なエラーです。
	User privileges are not enough to perform this operation.	権限が不十分です。
Membership	Data is invalid.	一般的なエラーです。
	User privileges are not enough to perform this operation.	権限が不十分です。
Broadcast & Multicast		
Broadcast Parameters	Threshold is out of range.	ブロードキャストストームしきい値レベルが上限を超えています。
	User privileges are not enough to perform this operation.	権限が不十分です。
IGMP Parameters	Please enter a valid version.	有効なバージョンを入力してください。
	Query count is out of range.	照会数が範囲外です。
	Query interval is out of range.	照会の間隔が範囲外です。
	Query timeout is out of range.	照会のタイムアウト値が範囲外です。
	Report delay is out of range.	レポート遅延が範囲外です。
	User privileges are not enough to perform this operation.	権限が不十分です。
Multicast Router Ports	Data is invalid.	一般的なエラーです。
	Please select a port	マルチキャストルーターに対して追加または削除するポートを選択してください。
	User privileges are not enough to perform this operation.	権限が不十分です。

表 B-4 Web インタフェースエラーメッセージ (続き)

メニュー	メッセージ	説明
Multicast Services	Data is invalid.	一般的なエラーです。
	Igmp group member is null.	IGMP グループメンバーをリストから選択してください。
	Illegal IP address.	IP アドレスの形式が不正です。
	Select a port or trunk	VLAN に対して追加または削除する静的ポートを選択してください。
Spanning Tree		
	Basic Configuration	
	Data is invalid.	一般的なエラーです。
	Priority is out of range.	優先順位が範囲外です。
Advanced Configuration	User privileges are not enough to perform this operation.	権限が不十分です。
	Data is invalid.	一般的なエラーです。
Class of Service	User privileges are not enough to perform this operation.	権限が不十分です。
Basic Traffic Prioritisation	Cos Value is out of range.	CoS 値が範囲外です。
	Data is invalid.	一般的なエラーです。
	Priority is out of range.	優先順位が範囲外です。
	Queue weight must be in a order of $Q0 \leq Q1 \leq Q2 \leq Q3$	キューの加重値が無効です。
	Traffic Class is out of range.	トラフィッククラスが範囲外です。
	User privileges are not enough to perform this operation.	権限が不十分です。
Layer 3/4 Traffic Prioritisation	Cos Value is out of range.	CoS 値が範囲外です。
	Please select IP Precedence or DSCP mode	優先順位サービスが使用可能な場合は、いずれかのオプションを選択してください。
	Traffic Class is out of range.	トラフィッククラスが範囲外です。
	User privileges are not enough to perform this operation.	権限が不十分です。
Address Tables	Aging time is out of range.	アドレスの有効期限が上限を超えています。
	User privileges are not enough to perform this operation.	権限が不十分です。

表 B-4 Web インタフェースエラーメッセージ (続き)

メニュー	メッセージ	説明
Up Links, Down Links		
Status	Cannot set port capabilities.	指定されたポートの伝送速度またはデュプレックスモードが無効です。
	Data is invalid.	一般的なエラーです。
	User privileges are not enough to perform this operation.	権限が不十分です。
Link Aggregation	Cannot add trunk.The specified trunk is full or data is invalid.	指定されているトランクがいっぱいであるか、データが無効です。
	Cannot create trunk.	トランク数が上限を超えています。
	Cannot remove trunk.	トランクテーブルに問題が発生しました。
	Cannot remove trunk member.Data is invalid.	トランクテーブルに問題が発生しました。
	Cannot set trunk status.	静的なトランクメンバーに対しては、LACP を使用可能にできません。
	Data is invalid.	一般的なエラーです。
	User privileges are not enough to perform this operation.	権限が不十分です。
VLANs	Data is invalid.	一般的なエラーです。
	Please enter a valid PVID.	PVID が無効です。正しい PVID を選択してください。
	Please enter a valid timer.	タイマー値が無効です。正しいタイマー値を選択してください。
	Table is full or data is invalid.	テーブルがいっぱいであるか、データが無効です。
	User privileges are not enough to perform this operation.	権限が不十分です。
Address Filtering	Data is invalid.	一般的なエラーです。
	Please enter a valid MAC address.	MAC アドレスが無効です。
	Please enter a valid VLAN ID.	VLAN ID が無効です。
	Table is full or data is invalid.	テーブルがいっぱいであるか、データが無効です。
	User privileges are not enough to perform this operation.	権限が不十分です。
Spanning Tree	Data is invalid.	一般的なエラーです。
	User privileges are not enough to perform this operation.	権限が不十分です。

表 B-4 Web インタフェースエラーメッセージ (続き)

メニュー	メッセージ	説明
Config	Path cost is out of range.	パスコストが範囲外です。
	Priority is out of range.	優先順位が範囲外です。
Port	Path cost is out of range.	パスコストが範囲外です。
	Priority is out of range.	優先順位が範囲外です。
	User privileges are not enough to perform this operation.	権限が不十分です。
Management Ports		
VLANs	Data is invalid.	一般的なエラーです。
	Please enter a valid PVID.	PVID が無効です。正しい PVID を選択してください。
	Please enter a valid timer.	タイマー値が無効です。正しいタイマー値を選択してください。
	Table is full or data is invalid.	テーブルがいっぱいであるか、データが無効です。
	User privileges are not enough to perform this operation.	権限が不十分です。
Packet Filtering	User privileges are not enough to perform this operation.	権限が不十分です。
Monitoring		
Port Mirroring	Data is invalid.	一般的なエラーです。
	User privileges are not enough to perform this operation.	権限が不十分です。
Logs	Data is invalid.	一般的なエラーです。
	User privileges are not enough to perform this operation.	権限が不十分です。

付録 C

仕様

C.1 スイッチアーキテクチャー

ポート

ネットワークアップリンク - 1000BASE-T × 8

ミッドプレーン - Gigabit シリアルダウンリンク × 16 (サーバーブレード用)

管理チャンネル - 10/100BASE-TX × 1、コンソールポート × 1 (シリアル RJ-45)

ネットワークインタフェース

10/100/1000Base-T ポート NETP0 ~ 7:

RJ-45 コネクタ、自動ネゴシエーション、自動 MDI/MDI-X

ケーブル: 10BASE-T: 100 オーム、UTP ケーブル、カテゴリ 3、4、5

100BASE-TX: 100 オーム、UTP ケーブル、カテゴリ 5

1000BASE-T: 100 オーム、UTP ケーブル、カテゴリ 5 または 5e

バッファアーキテクチャー

アップリンクポートおよびダウンリンクポート: 1M バイト共有

集約帯域幅

48 Gbps

スイッチングデータベース

32K MAC アドレスエントリ

LED

SSC: 動作中、保守要求、取り外し可能

Ethernet ポート: リンク/通信、速度

C.2 管理機能

帯域内管理

telnet または Web ベースの HTTP、SNMP

帯域外管理

RJ-45 コンソールポート経由の RS-232 信号

ソフトウェアインストール

帯域内では TFTP、帯域外では XModem

MIB サポート

SNMP v1/v2 (RFC 1215, 1907)、MIB II (RFC 2863)、Bridge MIB (RFC 1493)、Etherlike MIB (RFC 1643/2665)、RMON (RFC 2819 グループ 1、2、3、9)、IEEE 802.1Q VLAN (RFC 2674)、IEEE 802.3ad LACP、プライベート MIB

RMON サポート

グループ 1、2、3、9 (Statistics、History、Alarm、Event)

追加機能

ポートトランク (静的および LACP)

ポートのミラー化

ポートセキュリティ

RADIUS 認証クライアント

C.3 物理仕様

重量

2.08 kg (4.59 ポンド)

サイズ

27.5 × 20.3 × 4.3 cm (10.8 × 8.0 × 1.7 インチ)

C.4 電源

作動電圧

+12 VDC

最大電流

5.2 A

消費電力

62 W (最大)

放熱量

211 BTU/時 (最大)

C.5 動作環境

温度

動作時 : 5 ~ 45 °C (41 ~ 113 °F)

保管時 : -40 ~ 70 °C (-40 ~ 158 °F)

湿度

動作時 : 10 ~ 90 % (結露のないこと)

C.6 標準規格

IEEE 802.3 Ethernet、IEEE 802.3u Fast Ethernet、IEEE 802.3ab Gigabit Ethernet

IEEE 802.1D スパニングツリープロトコルおよびトラフィック優先制御、

IEEE 802.1w 高速化した STP (RSTP)

IEEE 802.1p 優先順位タグ、IEEE 802.1Q VLAN、IEEE 802.3ac VLAN タグ、

IEEE 802.3x 全二重フロー制御 (ISO/IEC 8802-3)

IEEE 802.3ad Link Aggregation Control Protocol (LACP)、

SNMP (RFC 1215、1907)、RMON (RFC 2819 グループ 1、2、3、9)、

MIB II (RFC 2863)、Bridge MIB (RFC 1493)、Etherlike MIB (RFC 1643/2665)、

ARP (RFC 826)、IGMP (RFC 1112)、ICMP (RFC 792)

用語集

10BASE-T	2組のカテゴリ 3 または 4、5 UTP ケーブルを使用する 10 Mbps Ethernet の IEEE 802.3 仕様。
100BASE-TX	2組のカテゴリ 5 UTP ケーブルを使用する 100 Mbps Fast Ethernet の IEEE 802.3u 仕様。
1000BASE-T	2組のカテゴリ 5、5e 100 オーム UTP ケーブルを使用する Gigabit Ethernet の IEEE 802.3ab 仕様。
1000BASE-X	8B/10B 信号に基づく 1000 Mbps Gigabit Ethernet を示す IEEE 802.3 仕様の略名。
BOOTP	ネットワークに接続された装置にオペレーティングシステムを読み込むときに使用する起動プロトコル。
CSMA/CD	Carrier Sense Multiple Access/Collision Detect (衝突検出機能付きキャリア検知多重アクセス) の略で、Ethernet および Fast Ethernet で使用される通信方式。
Ethernet	DEC および Intel、Xerox の 3 社によって開発され標準化された、ベースバンド伝送および CSMA/CD アクセス、論理バストポロジ、同軸ケーブルを使用するネットワーク通信システム。後継の IEEE 802.3 標準規格では、OSI モデルに統合するため、ファイバおよび細い同軸ケーブル、より対線ケーブル上で動作するリピータと実装方式によって、物理レイヤーおよび媒体が拡張された。
Fast Ethernet	Ethernet および CSMA/CD アクセス方式に基づく 100 Mbps のネットワーク通信システム。
GARP VLAN Registration Protocol (GVRP)	スパニングツリーに基づき、ポートに必要な VLAN メンバーを登録するために、スイッチが VLAN 情報を交換する方法を定義する。これによって、各スイッチで定義された VLAN が、自動的にスパニングツリーネットワーク上で機能するようになる。

**Generic Attribute
Registration Protocol
(GARP)**

スイッチ制御された環境で、マルチキャストグループのメンバー情報を登録および伝播するために、エンドステーションとスイッチが使用するプロトコル。これによって、マルチキャストデータフレームが、登録されたエンドステーションが含まれるスイッチ制御 LAN 部分だけに伝播されるようになる。以前は、Group Address Registration Protocol と呼ばれていた。

Gigabit Ethernet

Ethernet および CSMA/CD アクセス方式に基づく 1000 Mbps のネットワーク通信システム。

**Group Attribute
Registration Protocol**

「Generic Attribute Registration Protocol」を参照。

IEEE 802.1D

スパニングツリープロトコルを含む、MAC ブリッジの動作に関する汎用的な方式の規定。

IEEE 802.1Q

VLAN のタグ付けに関する規定。VLAN 情報を配信する Ethernet フレームタグを定義する。これによって、スイッチは、エンドステーションを異なる仮想 VLAN に割り当てることができる。また、スイッチ制御ネットワークで VLAN が通信を行うための標準方式を定義する。

IEEE 802.1p

Ethernet ネットワーク上でサービス品質 (Quality of Service : QoS) を提供するための IEEE 標準規格。この標準規格では、最大で 8 つのトラフィッククラスを定義するパケットタグを使用して、スイッチが優先順位値のタグに基づいてパケットを送信できるようにする。

IEEE 802.1w

IEEE 802.1D の後継として設計された高速スパニングツリープロトコル (RSTP) の IEEE 標準規格。RSTP によって、トポロジ変更の収束 (コンバージェンス) が大幅に高速化される。

IEEE 802.3

CSMA/CD アクセス方式および物理レイヤー仕様を定義する。

IEEE 802.3ab

1000BASE-T Fast Ethernet の CSMA/CD アクセス方式および物理レイヤー仕様を定義する。

IEEE 802.3ac

VLAN タグのフレーム拡張機能を定義する。

IEEE 802.3u

100BASE-TX Fast Ethernet の CSMA/CD アクセス方式および物理レイヤー仕様を定義する。

IEEE 802.3x

全二重リンクのフロー制御で使用する Ethernet フレームの開始および停止要求とタイマーを定義する。

IEEE 802.3z

1000BASE Gigabit Ethernet の CSMA/CD アクセス方式および物理レイヤー仕様を定義する。

IGMP スヌープ

IP マルチキャストグループのメンバーを識別するために、IP マルチキャストルーターと IP マルチキャストホストグループとの間で送受信される IGMP 照会パケットおよび IGMP レポートパケットを待機すること。

**Internet Control
Message Protocol
(ICMP)**

通常、監視用のエコーメッセージ (Ping) を送信するために使用する。

<p>Internet Group Management Protocol (IGMP)</p>	<p>ホストがマルチキャストサービス用のローカルルーターに登録するために使用するプロトコル。サブネットワークに複数のマルチキャストルーターがある場合は、ルーターの1台が「照会元」となり、グループメンバーの登録状況を追跡する役割を負う。</p>
<p>IP マルチキャスト フィルタリング</p>	<p>スイッチが参加しているホストにマルチキャストトラフィックを渡すために実行する処理。</p>
<p>LAN セグメント</p>	<p>個々の LAN またはコリジョンドメイン。</p>
<p>LED</p>	<p>装置またはネットワークの状態を監視するために使用する発光ダイオード。</p>
<p>Link Aggregation Control Protocol (LACP)</p>	<p>ポートが、別の装置上の LACP が設定されたポートとの間で自動的にトランクリンクのネゴシエーションを行うことを可能にするプロトコル。</p>
<p>Remote Authentication Dial-in User Service (RADIUS)</p>	<p>中央サーバーを使用して、ネットワーク上の RADIUS 対応装置へのアクセスを制御する認証プロトコル。RADIUS サーバーは、スイッチへの管理アクセスを求める各ユーザーまたは各グループに対応するユーザー名およびパスワードの組とそれに関連する特権レベルを複数登録したデータベースを使用してプログラミングできる。</p>
<p>Remote Monitoring (RMON)</p>	<p>RMON は、包括的なネットワーク監視機能を提供する。標準的な SNMP で要求されるポーリングを排除し、特定のエラータイプを含むさまざまなトラフィック条件に対してアラームを設定できる。</p>
<p>RJ-45 コネクタ</p>	<p>より対線ケーブル用のコネクタ。</p>
<p>Simple Network Management Protocol (SNMP)</p>	<p>インターネット対応のプロトコル群の中で、ネットワーク管理サービスを提供するアプリケーションプロトコル。</p>
<p>telnet</p>	<p>TCP/IP 上で端末装置とのインタフェースをとるための遠隔通信機能。</p>
<p>Terminal Access Controller Access Control System (TACACS)</p>	<p>中央サーバーを使用して、ネットワーク上の TACACS 対応装置へのアクセスを制御する認証プロトコル。TACACS サーバーは、スイッチへの管理アクセスを求める各ユーザーまたは各グループに対応するユーザー名およびパスワードの組とそれに関連する特権レベルを複数登録したデータベースを使用してプログラミングできる。</p>

Transmission Control Protocol/Internet Protocol (TCP/IP)	基本的なトランスポートプロトコルに TCP、ネットワーク層プロトコルに IP を含むプロトコル群。
Trivial File Transfer Protocol (TFTP)	ソフトウェアダウンロードに通常使用される TCP/IP プロトコル。
XModem	装置間でファイルを転送するために使用されるプロトコル。データは、128 バイトブロックに区切られて、エラーが修正される。
エンドステーション	ネットワーク相互接続装置として動作しないワークステーションまたはサーバー、その他の装置。
仮想 LAN (VLAN)	ネットワーク上の物理的な位置や接続ポイントにかかわらず、同じコリジョンドメインを共有するネットワークノードの集合。VLAN は、物理的な境界のない論理ワークグループとして機能する。VLAN によって、ユーザーは、1 つの LAN 内に存在するかのように情報およびリソースを共有できる。
管理情報ベース (MIB)	MIB は Management Information Base の頭字語。特定の装置に関する情報を格納したデータベースオブジェクトのセット。
コリジョンドメイン	単一の CSMA/CD LAN セグメント。
シールド付きより対線 (STP) ケーブル	過剰なノイズの侵入または放出を削減するために、外側をアルミ箔または銅の織布シールドで覆ったより対線ワイヤ。
シールドなしより対線 (UTP) ケーブル	電気的な干渉を削減するために、2 本の絶縁ワイヤを撚り合わせたケーブル。一般的な電話コードに使用されている。
自動ネゴシエーション	各ノードが接続先ノードの機能に基づいて最適な動作モード (10 Mbps または 100 Mbps、半二重または全二重など) を選択できるようにする信号方式。
衝突	ケーブルに送信されたパケットが相互に干渉する状態。干渉によって、どちらの信号も認識できなくなる。これは、半二重接続の場合にのみ当てはまる。
スイッチポート	個々のコリジョンドメインまたは LAN セグメント上のポート。
スパニングツリー プロトコル (STP)	ネットワーク内にループが発生していないかどうかを確認する手法。ループは、複雑に接続されたネットワークシステムやバックアップ接続されたネットワークシステム内で発生することが多い。スパニングツリーは、検出したデータを使用できる最短のパスに送信することによって、ネットワークの性能および効率を最適化する。
全二重	スイッチとネットワークカードが送受信を同時に実行できるようにする伝送方式。この効率化によって、リンクの帯域幅が 2 倍になる。
帯域外管理	ネットワークに接続されていないステーションから行うネットワーク管理。
帯域内管理	ネットワークに直接接続されたステーションから行うネットワーク管理。

帯域幅	ネットワーク信号に使用できる最高周波数と最低周波数との差。回線速度の同義語として使用されることもあり、この場合はケーブルの実際のデータ伝送速度を示す。
帯域幅利用率	実際に受信したパケットの総帯域幅に対する割合。
動的ホスト構成 プロトコル (DHCP)	TCP/IP ネットワーク上のホストに設定情報を渡すためのフレームワークを提供する。ブートストラップ (BOOTP) に、再利用可能なネットワークアドレスの自動割り当て機能および構成オプションを追加したものである。
ポートトランク	複数の低速な物理リンクを結合して単一の高速論理リンクを作成するネットワークリンク集約およびトランク方式の定義。
ポートのミラー化	ロジックアナライザや RMON プロブを使用して障害追跡を行うために、ターゲットポート上のデータを監視ポートにミラー化すること。これによって、ターゲットポートのデータを妨げることなく調査できる。
マルチキャスト スイッチング	スイッチが、接続するホストが登録されていないサービスへのマルチキャストフレームを受信したときに、これをフィルタリングして、指定されたマルチキャスト VLAN グループに含まれるすべてのポートに転送する処理。
メディアアクセス制御 (MAC)	伝送媒体へのアクセスを制御する、ネットワークプロトコルの一部。これによって、ネットワークノード間のデータの交換が容易になる。
リンク集約	「ポートトランク」を参照。
リンクセグメント	1 組のリピータ、または 1 台のリピータと 1 台の PC を接続するより対線ケーブルまたはファイバケーブルの長さ。
レイヤー 2	ISO の 7 層データ通信プロトコルのデータリンク層。レイヤー 2 は、ネットワーク装置のハードウェアインタフェースに直結して、MAC アドレスに基づいてトラフィックを渡す。
レイヤー 3	ISO の 7 階データ通信プロトコルのネットワーク層。レイヤー 3 は、オープンシステム間でデータをやり取りするためのルーティング機能を処理する。
ローカルエリア ネットワーク (LAN)	相互接続されたコンピュータとサポート装置のグループ。

索引

B

BOOTP, 3-15, 4-64

C

CLI, 4-1

CoS

キューの割り当て, 3-65, 4-138

サービス加重, 3-70, 4-137

設定, 3-65, 4-135

デフォルトの優先順位, 3-65, 4-136

レイヤー 3 およびレイヤー 4 の優先順位, 3-71, 4-135

D

DHCP, 3-15, 4-64

クライアント識別子, 3-12, 4-66

Differentiated Services Code Point、「DSCP」を参照

DSCP, 3-75, 4-142

G

GARP, 3-93, 4-120

タイマーの設定, 4-120

GARP VLAN Registration Protocol、「GVRP」を参照

Group Address Registration Protocol、「GARP」を参照

GVRP, 3-35, 3-93, 4-118

インタフェースの設定, 3-94, 4-118

グローバル設定, 3-38, 4-122

説明, 3-35

I

IEEE 802.1D, 3-57, 4-96

IEEE 802.1w, 3-57, 4-96

IGMP, 3-45, 4-124

Internet Group Management Protocol、「IGMP」を参照

IP アドレス

BOOTP/DHCP サービス, 3-15, 4-63

手動による設定, 3-13, 4-64

設定, 3-11, 4-63

IP 優先順位 (Precedence), 3-73, 4-141

L

LACP, 3-88, 4-150

Link Aggregation Control Protocol、「LACP」を参照

M

MIB, A-1

サポートする MIB, A-1

P

PVID, 3-93, 4-114

デフォルトの ID, 3-93, 4-114

R

RADIUS, 3-24, 4-41

Remote Authentication Dial-in User Service、
「RADIUS」を参照

RSTP, 3-57, 4-96

グローバル設定, 3-63, 4-96

説明, 3-57

S

SC, 1-1, 1-3

Simple Network Management Protocol、
「SNMP」を参照

SNMP, 2-3

コミュニティー文字列, 2-4, 3-29, 4-49

設定, 3-28, 4-49

トラップ、サポート, A-3

トラップの受信側, 2-5, 3-30, 4-51

トラップの使用可能への切り替え, 3-30, 4-52

バージョン, 2-3, 3-30, 4-51

SSC, 1-xvii, 1-1, 1-3

STA, 3-57, 4-94, 4-95

インタフェース設定の表示, 3-102, 4-106

インタフェースの設定, 3-106, 4-94

エッジポート, 3-103, 3-107, 4-103

説明, 3-57

パスコスト, 3-102, 3-106

プロトコルの移送, 3-109, 4-104

優先順位, 3-102, 3-106, 4-102

リンクタイプ, 3-103, 3-107, 4-104

STP, 3-57, 4-96

T

TACACS, 3-24, 4-41

telnet, 4-2

Terminal Access Controller Access Control
System、「TACACS」を参照

V

VLAN, 3-33, 3-93, 4-108

禁止, 3-94, 4-116

設定, 3-33, 4-108

説明, 3-33

タグ付き, 3-94, 4-115

タグなし, 3-94, 4-115

メンバーポート, 3-94, 4-115

W

Web インタフェース, 3-2

アクセス要件, 3-2

設定ボタン, 3-4

パネル表示, 3-4

ホームページ, 3-3

メニューリスト, 3-5

あ

アップリンクポート, 1-3

アドレステーブル, 3-77, 4-90

有効期限, 3-79, 4-91

暗号化パスワード, 4-26, 4-27, 4-58

い

イングレスフィルタリング, 3-94, 4-113

う

受け入れるフレームタイプ, 3-93, 4-112

え

- エッジポート、STA、3-103, 4-103
- エラーメッセージ、B-5
 - Web インタフェース、B-8
 - コマンド行エラー、B-6
 - システムエラー、B-5
 - ロギング、4-30

か

- 管理
 - インタフェース、Web、3-2
 - インタフェース、コンソール、4-1
- 管理情報ベース、「MIB」を参照
- 管理ポート、1-4
- 管理ポート、トラフィックのフィルタリング、3-110, 4-70

き

- 起動構成ファイル、作成、3-22, 4-18
- 起動ファイル
 - 設定、3-19, 4-22
 - 表示、3-19, 4-34

こ

- 高速スパニングツリープロトコル、「RSTP」を参照
- コマンド行インタフェース、「CLI」を参照
- コミュニティ文字列、2-4, 3-29, 4-49
- コンソールポート
 - 接続、4-1
 - 設定、4-55

さ

- サーバーブレード、1-1, 1-3
- サービスクラス、「CoS」を参照

し

- システムソフトウェア、3-17, 4-18
 - アップロードまたはダウンロード、3-19, 4-18
 - サーバーからのダウンロード、3-19, 4-18
- システムログ、3-128, 4-30, B-3
- ジャンボフレーム、4-29
- 仕様、C-1
- 障害追跡、B-1
 - 管理インタフェース、B-2
 - システムログの使用、B-3
 - スイッチインジケータ、B-1
 - ポート接続、B-2
- 状態表示 LED、1-4
- シリアルポート
 - 設定、4-55

す

- スイッチ/システムコントローラ、「SSC」を参照
- スイッチの仕様、C-1
- スイッチポートモード、3-93, 4-111
- スパニングツリーアルゴリズム、「STA」を参照
- スパニングツリープロトコル、「STP」を参照

せ

- 静的アドレス、設定、3-99, 4-89
- 設定内容
 - 保存、2-5
 - 保存または復元、3-22, 4-18

そ

- ソフトウェアのアップグレード、3-19, 4-18
- ソフトウェアのダウンロード、3-19, 4-18
- ソフトウェアのバージョン、表示、3-17, 4-39

た

- ダウンリンクポート、1-3

ダウンロード、ソフトウェア、3-19,4-18

と

統計情報、SNMP、3-125,4-53

統計情報、スイッチ、3-116,4-85

トラップの受信側、2-5,3-30,4-51

トラフィックのフィルタリング、管理ポート
、3-110,4-70

トランク

LACP、3-89,4-150

静的、3-91,4-148

設定、3-88,4-148

動的、3-89,4-150

は

パスコスト、3-102

パスコスト、STA、3-106,4-100,4-101

パスコスト、方式、3-63,4-100

パスワード、4-26,4-27,4-58

パスワード、設定、3-24,4-41

ふ

ファームウェア、アップグレード、3-19,4-18

ファームウェアのバージョン、表示、3-17,4-39

ブロードキャストストーム

しきい値、3-55,4-83

ポート設定、3-85,4-83

プロトコルの移送、3-109,4-104

ほ

ポート、設定、3-80,4-75

ポートセキュリティ、3-99,4-92

ポートミラー、3-114,4-146

ポート優先順位、受信ポートでのデフォルト
、3-65,4-136

ま

マルチキャスト

設定、3-45,4-124

ルーター、3-49,4-133

み

ミラーポート、設定、3-114,4-146

め

メインメニュー、3-5,4-10

ゆ

有効期限、3-79,4-91

ユーザー名、設定、3-24,4-41

優先順位、STA、3-102,3-106,4-99

優先順位、受信ポートのデフォルト、3-65,4-136

り

リンクタイプ、STA、3-103,3-107,4-104

ろ

ロギング、メッセージ、3-128,4-30

ログイン

Web インタフェース、3-3

ログオン認証、3-24,4-41

ログメッセージ、B-4