D-Link DGS-3200 シリーズ
Layer2+ Gigabit Managed Switch

コマンドラインインタフェース (CLI) マニュアル

ご注意

本書は、コマンドラインインタフェースの説明および設定方法を記載しています。本シリーズの仕様、設置方法など使用するために必要な基本的な取り扱い方法については、設置マニュアルおよびユーザマニュアルをご覧ください。

D-Link®
Building Networks for People

安全にお使いいただくために

安全上のご注意　必ずお守りください

本製品を安全にお使いいただくために、以下の項目をよくお読みになり必ずお守りください。

⚠警告	この表示を無視し、まちがった使いかたをすると、火災や感電などにより人身事故になるおそれがあります。
⚠注意	この表示を無視し、まちがった使いかたをすると、傷害または物損損害が発生するおそれがあります。

記号の意味　⃠ してはいけない**「禁止」**内容です。　❗ 必ず実行していただく**「指示」**の内容です。

⚠警告

分解・改造をしない
機器が故障したり、異物が混入すると、やけどや火災の原因となります。

落としたり、重いものを乗せたり、強いショックを与えたり、圧力をかけたりしない
故障の原因につながります。

発煙、焦げ臭い匂いの発生などの異常状態のまま使用しない
感電、火災の原因になります。
使用を止めて、ケーブル / コード類を抜いて、煙が出なくなってから販売店に修理をご依頼してください。

ぬれた手でさわらない
感電のおそれがあります。

水をかけたり、ぬらしたりしない
内部に水が入ると、火災、感電、または故障のおそれがあります。

油煙、湯気、湿気、ほこりの多い場所、振動の激しいところでは使わない
火災、感電、または故障のおそれがあります。

内部に金属物や燃えやすいものを入れない
火災、感電、または故障のおそれがあります。

表示以外の電圧で使用しない
火災、感電、または故障のおそれがあります。

たこ足配線禁止
たこ足配線などで定格を超えると火災、感電、または故障の原因となります。

設置、移動のときは電源プラグを抜く
火災、感電、または故障のおそれがあります。

雷鳴が聞こえたら、ケーブル / コード類にはさわらない
感電のおそれがあります。

ケーブル / コード類や端子を破損させない
無理なねじり、引っ張り、加工、重いものの下敷きなどは、ケーブル / コードや端子の破損の原因となり、火災、感電、または故障につながります。

正しい電源ケーブル、コンセントを使用する
火災、感電、または故障の原因となります。

乳幼児の手の届く場所では使わない
やけど、ケガ、または感電の原因になります。

次のような場所では保管、使用をしない
・直射日光のあたる場所
・高温になる場所
・動作環境範囲外

光源をのぞかない
光ファイバケーブルの断面、コネクタ、および製品のコネクタをのぞきますと強力な光源により目を損傷するおそれがあります。

⚠注意

静電気注意
コネクタやプラグの金属端子に触れたり、帯電したものを近づけますと故障の原因となります。

コードを持って抜かない
コードを無理に曲げたり、引っ張りますと、コードや機器の破損の原因となります。

振動が発生する場所では使用しない
接触不良や動作不良の原因となります。

付属品の使用は取扱説明書にしたがう
付属品は取扱説明書にしたがい、他の製品には使用しないでください。機器の破損の原因になります。

電波障害自主規制について

本製品は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラス A 情報技術装置です。
この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。
この場合には使用者が適切な対策を講ずるよう要求されることがあります。

このたびは、弊社製品をお買い上げいただきありがとうございます。

本書は、製品を正しくお使いいただくための取扱説明書です。必要な場合には、いつでもご覧いただけますよう大切に保管してください。
また、必ず本書、設置マニュアル、ユーザマニュアルおよび同梱されている製品保証書をよくお読みいただき、内容をご理解いただいた上で、記載事項にしたがってご使用ください。

- 本書および同梱されている製品保証書の記載内容に逸脱した使用の結果発生した、いかなる障害や損害において、弊社は一切の責任を負いません。あらかじめご了承ください。
- 本書および同梱されている製品保証書は大切に保管してください。
- 弊社製品を日本国外でご使用の際のトラブルはサポート対象外になります。

なお、本製品の最新情報やファームウェアなどを弊社ホームページにてご提供させていただく場合がありますので、ご使用の前にご確認ください。
また、テクニカルサポートご提供のためにはユーザ登録が必要となります。

http://www.dlink-jp.com/

表記規則について

本項では、本マニュアル中での表記方法について説明します。

注意 注意では、特長や技術についての詳細情報を記述します。

警告 警告では、設定の組み合わせ、イベントや手順によりネットワークの接続状態やセキュリティなどに悪影響を及ぼす恐れのある事項について説明します。

目次

第 1 章　はじめに

本スイッチは、シリアルポート、Telnet、または Web ベースマネジメントエージェントを通してスイッチの管理を行うことができます。コマンドラインインタフェース (CLI) では、シリアルポートまたは Telnet インタフェースを経由してスイッチを設定および管理することができます。本マニュアルでは CLI に含まれるコマンドに関して説明しています。Web ベースマネジメントエージェントを経由したスイッチ設定および管理については、ユーザマニュアルに記載しています。また、ハードウェア設置の詳細情報についても、ユーザマニュアルを参照してください。

シリアルポート経由でスイッチに接続する

スイッチのシリアルポートの設定は以下の通りです。

- データ速度 : 115200 ビット / 秒
- パリティ : ノーパリティ
- データビット : 8
- ストップビット : 1

VT-100 端末をエミュレート可能な端末ソフトが動作し、上記シリアルポート設定を行っているコンピュータを RS-232（D-Sub 9 ピン）ケーブルでスイッチのシリアルポートに接続します。
シリアルポートが適切に管理コンピュータに接続されると、以下の画面が表示されます。表示されない場合、Ctrl+R を押し、コンソール画面を更新してください。

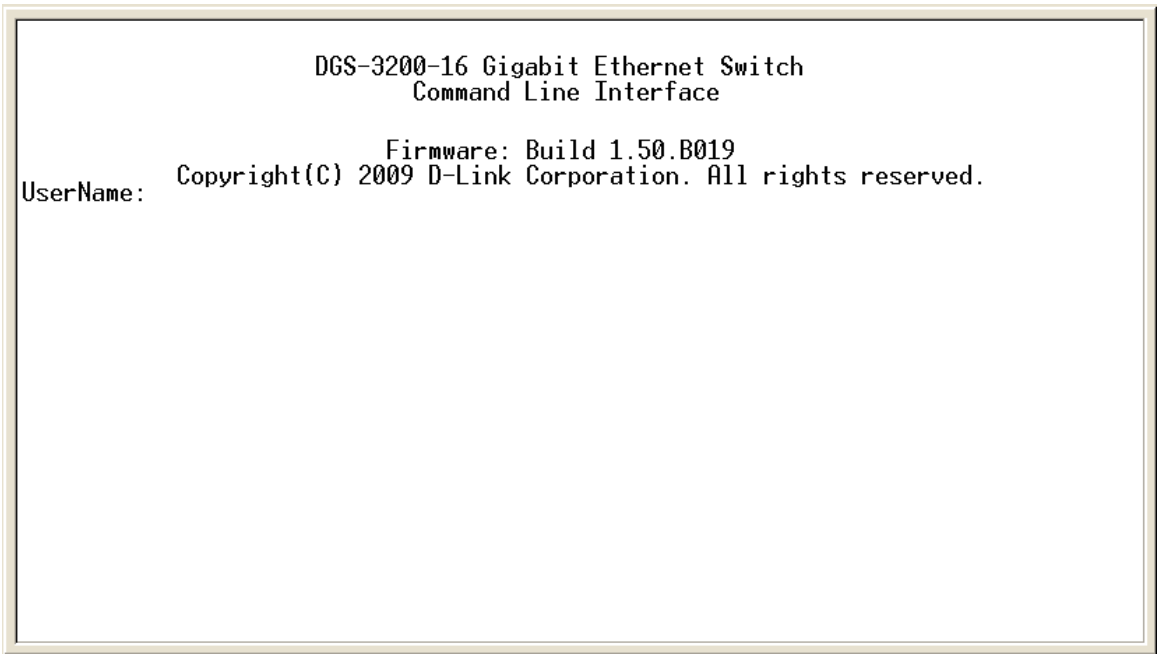


図 1-1　　初期の CLI 画面

本製品にはユーザ名とパスワードの初期値はありません。入力プロンプトに対して、2 回「Enter」キーを押すと、「DGS-3200-16: 4 #」が表示されます。これは、すべてのコマンドを入力する場合のコマンドプロンプトです。

スイッチの IP アドレス設定

各スイッチに対して、SNMP ネットワークマネージャまたは他の TCP/IP アプリケーション (例 :BOOTP、TFTP) と通信するために IP アドレスを割り当てる必要があります。本スイッチの IP アドレスの初期値は「10.90.90.90」です。この IP アドレスはご使用のネットワークのアドレス計画に基づいて変更することができます。
また、本スイッチには、出荷時に固有の MAC アドレスが割り当てられています。本 MAC アドレスを変更することはできません。初期起動時のコンソール画面に表示されます。

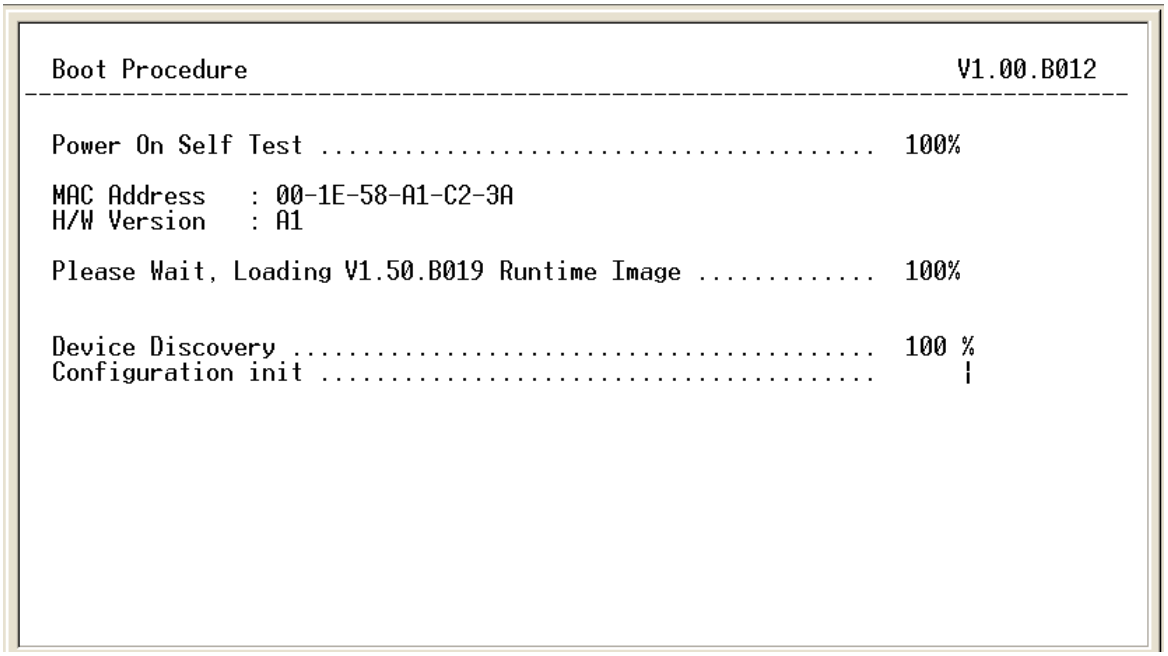


図 1-2　起動画面

本スイッチの MAC アドレスは、Web ベース管理インタフェースの「Configuration」メニューの「Device Information」画面にも表示されます。
本スイッチの IP アドレスは、Web ベース管理インタフェースの使用前に設定する必要があります。スイッチの IP アドレスは、BOOTP または DHCP プロトコルを使用して自動的に取得することもできます。この場合は、スイッチに割り当てた本来のアドレスを知っておく必要があります。
IP アドレスはコンソールから CLI を使用して、以下のように設定することができます。

1. **config ipif System ipaddress xxx.xxx.xxx.xxx/yyy.yyy.yyy.yyy**
   xxx.xxx.xxx.xxx は IP アドレスを示し、「System」と名づけた IP インタフェースに割り当てられます。
2. または、**config ipif System ipaddress xxx.xxx.xxx.xxx/z** と入力することもできます。
   yyy.yyy.yyy.yyy/z は対応するサブネットマスクを示しています。**xxx.xxx.xxx.xxx** は IP インタフェースに割り当てられた IP アドレスを示し、**z** は CIDR 表記で対応するサブネット数を表します。

本スイッチ上の「System」という名前の IP インタフェースに IP アドレスとサブネットマスクを割り当てて、管理ステーションから本スイッチの Telnet または Web ベースの管理エージェントに接続します。

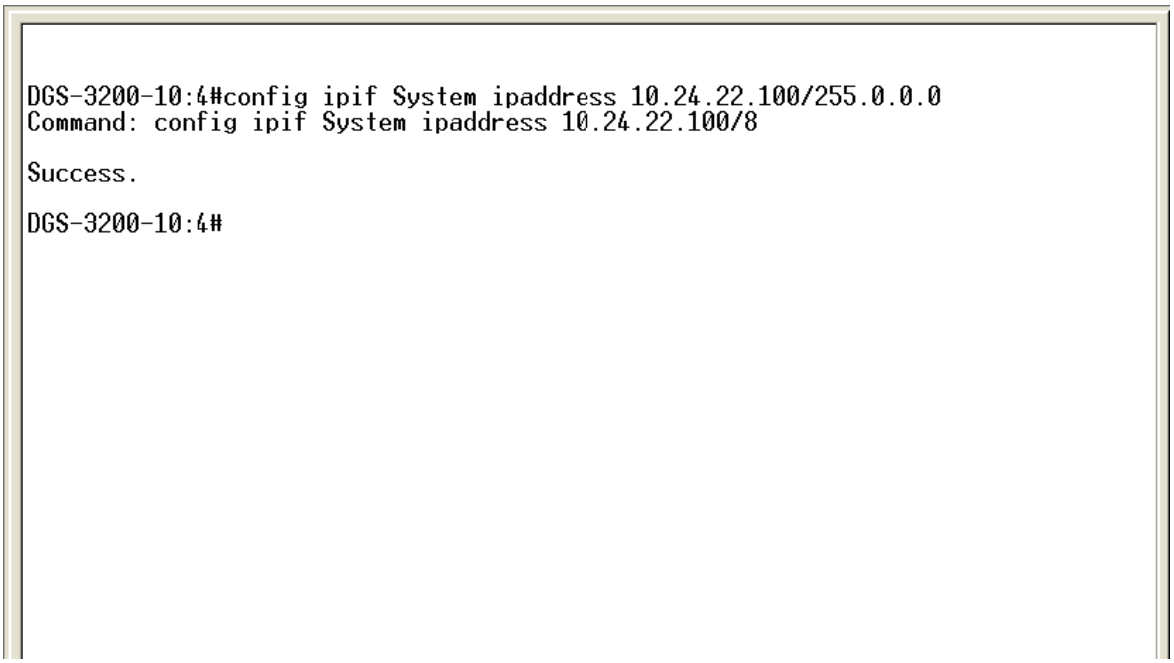


図 1-3　IP アドレスの割り当て

上記例では、スイッチに IP アドレス「10.24.22.100」とサブネットマスク「255.0.0.0」を割り当てています。「Success.」というメッセージにより、コマンドの実行が成功したことが確認できます。スイッチのアドレス設定が終了すると、Telnet、SNMP MIB ブラウザおよび CLI 経由、または上記 IP アドレスを使用した Web ベース管理エージェントによる設定と管理を開始することができます。

CLI には多くの便利な機能があります。「**?**」コマンドを入力すると、トップレベルの全コマンドリストが表示されます。

```
config 802.1x capability ports
config 802.1x guest_vlan ports
config 802.1x init
config 802.1x reauth
config access_profile profile_id
config account
config address_binding dhcp_snoop max_entry ports
config address_binding ip_mac ipaddress
config address_binding ip_mac ports
config address_binding recover_learning ports
config admin local_enable
config arp_aging time
config arp_spoofing_prevention
config arpentry
config authen application
config authen parameter attempt
config authen parameter response_timeout
config authen server_group
config authen server_host
config authen_enable
config authen_login
config authentication guest_vlan
config authentication ports
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

図 1-4　「?」コマンド

必須パラメータなしでコマンドを入力すると、CLI は「**Next possible completions**」メッセージを表示します。

```
DGS-3200-16:4#config account
Command: config account
Next possible completions:
<username>

DGS-3200-16:4#_
```

図 1-5　コマンドパラメータヘルプ例

この場合、「config account」コマンドには <username> パラメータが入力されます。CLI は、「**Next possible completions**」メッセージで <username> の入力を促します。CLI のすべてのコマンドには本機能があり、複雑なコマンドは、複数のパラメータ階層で入力を促します。
さらに、どんなコマンドも 1 スペースを付けて入力すると、引き続き、「Tab」キーを押すことで次に可能なサブコマンドのすべてを参照することができます。

コマンドプロンプトで前のコマンドを再入力するためには、矢印キーを押します。前のコマンドがコマンドプロンプトに表示されます。

図 1-6　上矢印キーを使用したコマンドの再入力

上記の例では、「config account」コマンドは必須パラメータの <username> なしで入力したため、CLI は「**Next possible completions**」を返しています。<username> プロンプトで上矢印カーソルキーを入力して、コマンドプロンプトでは前のコマンド（config account）を入力しています。適切なユーザ名を入力すると、「config account」コマンドが再実行されます。

CLI のすべてのコマンドがこのように動作します。さらに、ヘルププロンプトの構文は、本マニュアルで提供されるものと同じです。< > は数値または文字列、{} はオプションパラメータまたはパラメータの選択、[ ] は必須パラメータを示します。
CLI で認識されていないコマンドを入力すると、トップレベルのコマンドが以下の通り表示されます。

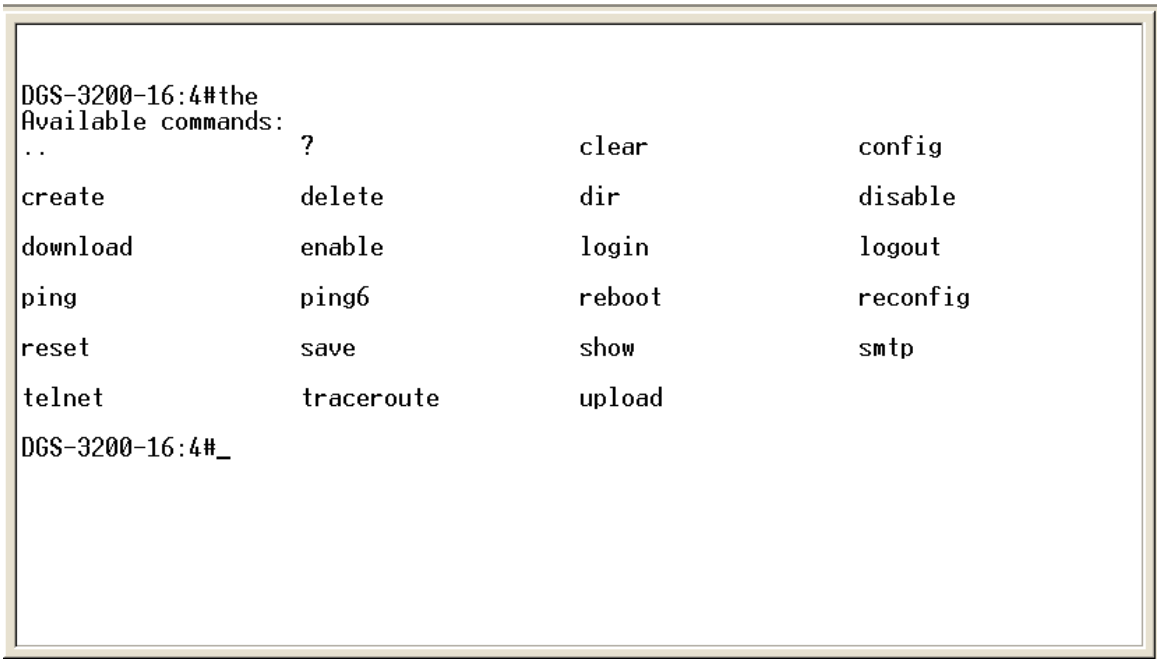


図 1-7　利用可能なコマンド

トップレベルのコマンドは「show」または「config」などがあります。これらのコマンドの多くは、トップレベルのコマンドを限定するために 1 つ以上のパラメータを必要とします。「show xxx?」または「config xxx?」とします。「xxx?」が次のパラメータです。
例えば、「show」コマンドを付加パラメータなしで入力すると、CLI は次に可能なパラメータのすべてを表示します。

```
DGS-3200-24:4#show
Command: show
Next possible completions:
802.1p                  802.1x                  access_profile          account
acct_client             address_binding         arp_spoofing_prevention
arpentry                attack_log              auth_client             auth_diagnostics
auth_session_statistics                         auth_statistics         authen
authen_enable           authen_login            authen_policy           authentication
authorization           autoconfig              bandwidth_control       command_history
config                  cpu                     cpu_filter              dhcp_local_relay
dhcp_relay              dot1v_protocol_group                            egress_filter
environment             error                   fdb                     filter
firmware                greeting_message        gvrp                    igmp
igmp_snooping           ipif                    ipif_ipv6_link_local_auto
iproute                 ipv6                    ipv6route               jumbo_frame
jwac                    lacp_port               limited_multicast_addr
link_aggregation        log                     log_save_timing         loopdetect
mac_based_access_control                        mac_based_access_control_local
mac_based_vlan          mac_notification        max_mcast_group
mcast_filter_profile                            mirror                  mld_snooping
multicast               multicast_fdb           packet                  port
port_security           ports                   power_saving            private_vlan
pvid                    radius                  router_ports            safeguard_engine
scheduling              scheduling_mechanism                            serial_port
session                 sim                     smtp                    snmp
sntp                    ssh                     ssl
storage_media_info                              stp                     switch
syslog                  system_severity         time                    time_range
traffic                 traffic_segmentation                            trusted_host
utilization             vlan                    vlan_trunk              wac
```

図 1-8　Next possible completions - show コマンド

上記例では、「show」コマンドの次に入力可能なパラメータのすべてが表示されています。「**Next possible completions**」プロンプトでは、上矢印を使用して、「show」コマンドに続いて「account」パラメータを再入力します。CLI はスイッチに設定されているユーザアカウントを表示します。

コマンド構文

以下の記号は、本マニュアルにおけるコマンドエントリの記述、および値と引数の指定を説明するために使用されます。CLI に含まれ、コンソールインタフェース経由で利用可能なオンラインヘルプは同じ構文を使用します。

注意　すべてのコマンドが大文字、小文字を区別します。大文字、小文字を変更する「Caps Lock」または他の不要な機能を無効にしてください。

< 山括弧 >

目的
　指定の必要がある変数または値を囲みます。
構文
　create account [admin | user] <username 15>
説明
　上の構文例では、<username> にユーザ名を入力する必要があります。< > は入力しません。
使用例
　create account admin newadmin1

[各括弧]

目的
　必要な値または引数を囲みます。値または引数を指定します。
構文
　create account [admin | user] <username 15>
説明
　上の構文例では、アカウントを作成するために「admin」または「user」レベルのいずれかを指定する必要があります。[ ] は入力しません。
使用例
　create account user newuser1

| 垂直線

目的
　リスト内の 2 つ以上の排他的な項目を分けて、そのうちの 1 つを入力する必要があります。
構文
　create account [admin | user] <username 15>
説明
　上の構文例では、「admin」または「user」を指定する必要があります。垂直線は入力しません。
使用例
　create account user newuser1

{ 中括弧 }

目的
　オプションの値かオプションの引数を囲みます。
構文
　reset {[config | system]}
説明
　上の構文例では、「config」または「system」を指定するオプションがあります。オプションの値を指定する必要はありませんが、システムリセットの効果は指定される値に依存します。そのため、この例では、システムリセットの実行によって 3 つの結果があります。リセットコマンドに関する詳細に関しては、30 ページの「第 5 章 基本のスイッチコマンド」を参照してください。
使用例
　reset config

変数の属性テーブル

表 1-1　変数の属性テーブル（例）

変数名	最大長	タイプ
<username>	15	文字列
<password>	15	文字列
<ipaddr>	15	ip アドレス
<netmask>	15	ip アドレス
<Gateway>	15	ip アドレス
<vlan_name>	32	文字列
<sw_name>	128	文字列
<sw_location>	128	文字列
<sw_contact>	128	文字列
<community_string 32>	32	文字列
<server_ip>	15	ip アドレス
<path_file name>	64	文字列
<macaddr>	17	MAC アドレス
<ipif>	12	文字列

行編集キーの使い方

表 1-2　行編集キー

キー	説明
Delete キー	カーソル下の文字を削除して、次に、ラインで残っている文字を左にシフトします。
Backspace キー	文字をカーソルの左方向に削除して、次に、ラインで残っている文字を左にシフトします。
Insert キーまたは Ctrl+R	オンとオフを切り替えます。オンの場合、文字を挿入し、前の文字を右にシフトします。
左矢印キー　←	左にカーソルを移動します。
右矢印キー　→	右にカーソルを移動します。
上矢印キー　↑	前に入力したコマンドを繰り返します。上矢印キーが押されるたびに表示されているものよりも前のコマンドが表示されます。このように、現在のセッションのコマンドヒストリを見直すことができます。コマンドヒストリリストを順番に追って前に進めるためには、下矢印キーを使用します。
下矢印キー　↓	下矢印キーは現在のセッションに入力されたコマンドヒストリにおいて次のコマンドを表示します。入力した通りに、各コマンドは連続して表示されます。上矢印キーを使用して、前のコマンドを見直します。
Tab キー	左にある次のフィールドにカーソルをシフトします。

ページ表示制御キー

表 1-3　ページ表示制御キー

キー	説明
スペースキー	次のページを表示します。
CTRL+C キー	複数のページが表示される場合、残りのページの表示を止めます。
ESC キー	複数のページが表示される場合、残りのページの表示を止めます。
n	次のページを表示します。
p	前のページを表示します。
q	複数のページが表示される場合、残りのページの表示を止めます。
r	現在表示されているページを更新します。
a	ページ表示を中断せずに、残りのページを表示します。
Enter キー	次の行またはテーブルエントリを表示します。

「show」コマンド出力がページの終わりに到達すると画面表示は一時停止します。

第 2 章　スイッチポートコマンド

ポート速度やフロー制御を含む、各物理ポートの属性やプロパティの設定および情報の表示を行います。

コマンドラインインタフェース（CLI）におけるスイッチポートコマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
config ports	[<portlist> | all] {medium_type [fiber | copper]} {speed [auto | 10_half | 10_full | 100_half | 100_full | 1000_full {master | slave}] | flow_control [enable | disable] | learning [enable | disable] | state[enable | disable] [description <desc 1-32> | clear_description]}
show ports	{<portlist>} {description | err_disabled}

以下のセクションで各コマンドについて詳しく記述します。

config ports

目的

スイッチのポート設定を行います。

構文

config ports [<portlist> | all] {medium_type [fiber | copper]} {speed [auto | 10_half | 10_full | 100_half | 100_full | 1000_full {master | slave}] | flow_control [enable | disable] | learning [enable | disable] | state [enable | disable] [description <desc 1-32> | clear_description]}

説明

スイッチのイーサネットポート設定を変更します。

パラメータ

パラメータ	説明
<portlist> | all	• <portlist> - 設定するポートまたはポート範囲を指定します。 • all - スイッチの全ポートに設定します。
medium_type [fiber | copper]	コンボポートにだけ適用されます。コンボポートを設定する場合、使用している通信メディアのタイプを指定します。コンボポートのメディアタイプを設定するためのオプションパラメータです。コンボポートを使用していない場合、本パラメータを指定する必要はありません。
speed [auto | 10_half | 10_full | 100_half | 100_full | 1000_full {master | slave}]	指定ポートにポートスピードを設定します。 • auto - 指定したポート範囲にオートネゴシエーションを有効にします。 • 10_half - ポートスピードを 10M ハーフデュプレックスに設定します。 • 10_full - ポートスピードを 10M フルデュプレックスに設定します。 • 100_half - ポートスピードを 100M ハーフデュプレックスに設定します。 • 100_full - ポートスピードを 100M ハーフデュプレックスに設定します。 • 1000_full {master | slave} - ポートスピードを 1000M フルデュプレックスに設定します。マスタ設定を行うと、ポートはデュプレックス、速度およびレイヤタイプに関連する能力を通知します。さらに、マスタ設定は、接続している 2 つの物理層間のマスタとスレーブの関係を決定します。この関係は 2 つの物理層間のタイミング制御を確立するために必要です。タイミング制御は、ローカルソースによってマスタの物理層に設定されます。スレーブ設定は、マスタから受信したデータストリームからタイミングを取るループタイミングを使用します。一方の接続にマスタを設定すると、他方の接続はスレーブとする必要があります。その他の設定は両ポートのリンクダウンを引き起こします。
flow_control [enable | disable]	指定ポートのフロー制御を「enable」（有効）または「disable」（無効）にします。
learning [enable | disable]	指定した範囲ポート上の MAC アドレス学習を「enable」（有効）または「disable」（無効）にします。
state [enable | disable]	指定ポート範囲を「enable」（有効）または「disable」（無効）にします。指定ポートがエラーによる無効状態である場合、本パラメータを有効にしてポートを有効状態に戻します。
description <desc 1-32>	選択したポートインタフェースを説明するために 32 文字未満の半角英数字の文字列を入力します。
clear_description	選択ポートのポート説明をクリアします。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

ギガビットポートは、1000Mbps に固定設定されており、遅い速度に設定することはできません。

使用例

スイッチのポート 3 の速度を 10Mbps、フルデュプレックス、MAC アドレス学習 / ステータス / フローコントロールを有効にします。

```
DGS-3200-10:4#config ports 1-3 speed 10_full state enable learning enable flow_control
enable
Command: config ports 1-3 speed 10_full state enable learning enable flow_control enable

Success.

DGS-3200-10:4#
```

show ports

目的

ポート範囲の現在の設定を表示します。

構文

show ports {<portlist>} {description | err_disabled}

説明

ポート範囲の現在の設定を表示します。パラメータがない場合は、すべてのポートを表示します。

パラメータ

パラメータ	説明
<portlist>	表示するポートまたはポート範囲を指定します。
description	本パラメータを追加すると、入力済みのポート説明が表示されます。
err_disabled	接続状態と無効になった原因を含む無効ポートのリストを表示します。 **注意** コンボポートがない場合、本パラメータを指定する必要はありません。

制限事項

なし。

使用例

ポート 1-4 の設定を表示します。

```
DGS-3200-10:4#show ports 1-4
Command: show ports 1-4

Port Port           Settings              Connection        Address
     State      Speed/Duplex/FlowCtrl  Speed/Duplex/FlowCtrl  Learning
---  -------  ------------------   ------------------  --------
1    Enabled   10M/Full/Enabled    Err-Disabled        Enabled
2    Enabled   10M/Full/Enabled    Link Down           Enabled
3 (C)Enabled   10M/Full/Enabled    Err-Disabled        Enabled
4 (F)Enabled   Auto/Disabled       Link Down           Enabled
```

ポート 1-4 の説明を表示します。

```
DGS-3200-10:4#show ports 1-4 description
Command: show ports 1-4 description

Port Port          Settings             Connection        Address
     State      Speed/Duplex/FlowCtrl  Speed/Duplex/FlowCtrl  Learning
---  -------  ------------------   ------------------  --------
1    Enabled  10M/Full/Enabled     Err-Disabled        Enabled
     Description:port1.
2    Enabled  10M/Full/Enabled     Err-Disabled        Enabled
     Description:port2.
3    Enabled  10M/Full/Enabled     Link Down           Enabled
     Description:port3.
4    Enabled  Auto/Disabled        Link Down           Enabled
     Description:port4.
```

注意 接続ステータスには次の状態があります。: Link Down（リンクダウン）、Speed/Duplex/FlowCtrl（速度 / デュプレックス / リンクアップ時のフローコントロール）および Err-Disabled（ストームコントロールエラー無効）。

```
DGS-3200-10:4#show ports err-disabled
Command: show ports err-disabled

Port Port      Connection Status   Reason
     State
---  -------  ------------------  -------------
1    Enabled  Err-Disabled        Storm control
     Description:port1.
8    Enabled  Err-Disabled        Storm control
     Description:port8.
```

第 3 章　ケーブル診断コマンド

コマンドラインインタフェース（CLI）におけるケーブル診断コマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
cable_diag ports	[<portlist> | all]

以下のセクションで各コマンドについて詳しく記述します。

cable_diag ports

目的

UTP ケーブルのテストを行います。ケーブルにエラーがある場合、エラーのタイプと発生箇所を診断します。

構文

cable_diag ports [<portlist> | all]

説明

UTP ケーブルの接続をテストします。10BASE-T/100BASE-TX のリンク速度である UTP ケーブルの場合、2 組のケーブルを診断し、1000BASE-T のリンク速度である UTP ケーブルの場合、4 組のケーブルを診断します。ケーブルエラーのタイプは、「open」、「short」、または「crosstalk」です。

「open」とは、エラーになっている対のケーブルが特定された箇所で接続していないことを示します。
「short」とは、エラーになっている対のケーブルが特定された箇所でショートしていることを示します。
「crosstalk」とは、エラーになっている対のケーブルが特定された箇所でクロストークの問題があることを示します。

ポートがリンクしている状態の場合、テストではケーブルの距離を取得します。リンク状態なので、ケーブルには「short」や「open」の問題はありませんが、まだ「crosstalk」の問題を検出する可能性があります。ポートがリンクダウンしている場合は、多くの要因により発生した可能性があります。ポートに正常なケーブル接続があるのに離れているリモートパートナーの電源が落ちている場合は、リモートパートナーの電源が入っているとしてケーブルの健全性を診断することができます。
ポートにケーブル接続がない場合、テストの結果はケーブルなしと表示されます。テストではエラーのタイプと発生箇所を検出します。本テストでは少規模のパケットを使用するのでご注意ください。
本テストは UTP ケーブル向けであり、光ファイバーケーブルに接続しているポートはテストの対象外です。また、ファイチップの中にはケーブル診断機能をサポートできないものがあり、それが結果に表示されます。

パラメータ

パラメータ	説明
<portlist>	ケーブル診断を行うポートまたはポート範囲を指定します。
all	すべてのポートを診断します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

指定ポートのケーブル診断を行います。

```
DGS-3200-10:4#cable_diag ports 1-4, 8
Command: cable_diag ports 1-4, 8

Perform Cable Diagnostics ...

Port Type         Link Status      Test Result        Cable Length(M)
---- ------------ ---------------- ------------------ --------------
1    1000Base_T   Link Up          OK                 4
2    1000Base_T   Link Down        No Cable           -
3    1000Base_T   Link Down        No Cable           -
4    1000Base_T   Link Down        No Cable           -
8    1000Base_T   Link Down        No Cable           -

DGS-3200-10:4#
```

第 4 章　ファイルシステムコマンド（DGS-3200-24/GE のみ）

コマンドラインインタフェース（CLI）におけるファイルシステムコマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
show storage_media_info	
md	<drive_id> <pathname 255>
rd	<drive_id> <pathname 255>
cd	{<pathname 255>}
dir	{<drive_id>} {< pathname 255>}
rename	{<drive_id>} <pathname 255> < filename 255>
erase	{ <drive_id>} <pathname 255>
del	{<drive_id>} <pathname 255>
move	{<drive_id>} <pathname 255> {<drive_id>} <pathname 255>
copy	{<drive_id>} < pathname 255> [{<drive_id>} < pathname 255> | image_id <int 1-n> | config_id <int 1-n> | prom]
copy	[image_id <int 1-n> | config_id <int 1-n> | prom | log] {<drive_id>} < pathname 255>
format	<drive> [FAT16 | FAT32] {<label_name 8>}

注意　本コマンドは、スイッチの前面パネルに SD フラッシュカードスロットを搭載する DGS-3200-24/GE にのみ対応しています。DGS-3200-10 と DGS-3200-16/GE は本機能をサポートしていません。

注意　アダプタを使用した miniSD カードや microSD カードは未対応です。

DGS-3200-24/GE 上の SD フラッシュカードスロットに SD フラッシュカードを挿入し、ファイル管理と他の管理業務を行うことができます。
ファイルシステムコマンドの設計は以下のルールに基づいています。

- ユニット上の各ストレージメディアはドライブにマップされます。そのため、ドライブのサイズはストレージメディアのサイズになります。
- 「C:」は、ファイルシステムを初めて使用する場合の初期値です。
- システムのストレージメディアであるフラッシュカードは、より高い優先順位を持ち、「C:」にマップされます。

以下のセクションで各コマンドについて詳しく記述します。

show storage_media_info

目的

ストレージメディアに関する情報を表示します。

構文

show storage_media_info

説明

ストレージメディアに関する情報を表示します。システムは 1 つ以上のメディアを持つことができます。メディア情報は、ドライブ番号とメディア識別子を含みます。スタンドアロンのデバイスの場合、ユニット番号を指定する必要はありません。

パラメータ

パラメータ	説明
<drive_id>	情報を表示するドライブ番号を指定します。ドライブ番号の指定形式は「C:」です。

制限事項

なし。

使用例

ストレージメディア情報を表示します。

```
DGS-3200-24:4#show storage_media_info
Command: show storage_media_info

Drive Media_Type Size  Label      FS_Type
----- ---------- ----- ---------- ---------------
C:\   SD Card    438MB TLD3       FAT16

DGS-3200-24:4#
```

md

目的

ストレージメディアにディレクトリを作成します。

構文

md <drive_id> <pathname 255>

説明

ストレージメディアにディレクトリを作成します。

パラメータ

パラメータ	説明
drive_id	ドライブ番号を指定します。ドライブ番号の指定形式は「C:」です。
pathname	作成するディレクトリ名。フルパス名で指定できます。

制限事項

管理者レベルユーザだけが本コマンドを実行できます。

使用例

ストレージメディアにディレクトリを作成します。

```
DGS-3200-24:4#md c:\abc
Command: md c:\abc

Process......Done.
Success.

DGS-3200-24:4#
```

rd

目的

ストレージメディアのディレクトリを削除します。

構文

rd <drive_id> <pathname 255>

説明

ストレージメディアのディレクトリを削除します。ディレクトリにファイルがある場合、本コマンドのエラーとなり、エラーメッセージを返します。

パラメータ

パラメータ	説明
drive_id	ドライブ番号を指定します。ドライブ番号の指定形式は「C:」です。
pathname	削除するディレクトリ名。フルでパス名を指定できます。

制限事項

管理者レベルユーザだけが本コマンドを実行できます。

使用例

ディレクトリを削除します。

```
DGS-3200-24:4#rd c:\abc
Command: rd c:\abc

Process......Done.
Success.

DGS-3200-24:4#
```

cd

目的

カレントディレクトリを別のディレクトリに変更します。または、カレントディレクトリのパスを表示します。

構文

cd {<pathname 255>}

説明

カレントディレクトリを変更します。作業ディレクトリを別のドライブにあるディレクトリに変更する場合、カレントドライブを希望のドライブに変更し、次に、カレントディレクトリを変える必要があります。 <pathname> を指定しないと、カレントドライブとカレントディレクトリを表示します。

パラメータ

パラメータ	説明
pathname	カレントディレクトリを本ディレクトリに変更します。フルパス名としてパス名を指定できます。

制限事項

なし。

使用例

カレントディレクトリを別のディレクトリに変更します。

```
DGS-3200-24:4#cd
Command: cd

C:\
Success.

DGS-3200-24:4#
```

dir

目的

ドライブ内のディレクトリにある全ファイルを表示します。

構文

dir {<drive_id>} {<pathname 255>}

説明

ドライブ内のディレクトリにある全ファイルを表示します。パス名を指定しないと、指定ドライブにあるファイルをすべて表示します。パラメータのいずれも指定しないと、カレントドライブにおけるファイルを表示します。

パラメータ

パラメータ	説明
drive_id	ドライブ番号を指定します。指定しないと、カレントドライブを参照します。
pathname	ディレクトリ名をパス形式で指定します。

制限事項

なし。

使用例

ドライブ内のディレクトリにある全ファイルを表示します。

```
DGS-3200-24:4#dir C:
Command: dir C:

unit 1 - C:\

2006/05/10 14:00 RUN.HAD         229,8112
2006/04/10 14:00 STARTUP.CFG        2,261
2006/03/10 14:00 LOG.TXT           46,384
2006/03/10 14:00 <DIR> LOG.TXT

total files 3
total directories 1

DGS-3200-24:4#
```

rename

目的

ファイル名を変更します。

構文

rename {<drive_id>} <pathname 255> <filename 255>

説明

ファイルシステム内のファイル名を設定します。「pathname」には変更するファイルをパス形式で指定し、「filename」には新しいファイル名を指定します。名前を変更されたファイルは同じディレクトリに残ります。スタンドアロンのデバイスの場合、ユニット番号は必要ありません。

パラメータ

パラメータ	説明
drive_id	ドライブ番号を指定します。指定しないと、カレントドライブを参照します。
pathname	変更するファイル名をパス形式で指定します。
filename	ファイルの新しい名前を指定します。

制限事項

管理者レベルユーザだけが本コマンドを実行できます。

使用例

ファイル名を変更します。

```
DGS-3200-24:4#rename c:\run.had run1.had
Command: rename c:\run.had run1.had

Process......Done.
Success.

DGS-3200-24:4#
```

erase, del

目的

システムからファイルを削除します。

構文

erase {<drive_id>} <pathname 255>

del {<drive_id>} <pathname 255>

説明

ファイルシステム内の保存されているファイルを削除します。

パラメータ

パラメータ	説明
drive_id	ドライブ番号を指定します。指定しないと、カレントドライブを参照します。
pathname	削除するファイル名をパス形式で指定します。

制限事項

管理者レベルユーザだけが本コマンドを実行できます。

使用例

ファイルを削除します。

```
DGS-3200-24:4#erase c:\run.had
Command: erase c:\run.had

Process......Done.
Success.

DGS-3200-24:4#
```

move

目的

ファイルを別の場所に移動します。

構文

move {<drive_id>} <pathname 255> {drive_id} <pathname 255>

説明

ファイルシステム内のファイル名を移動します。ユニット内のドライブにあるファイルを別のユニット内の別のドライブに移動することができます。ファイルを移動する場合、同時にファイル名の変更も指定できます。

パラメータ

パラメータ	説明
drive_id	ドライブ番号を指定します。指定しないと、カレントドライブを参照します。
pathname	ファイルを移動する場所のパス名を指定します。

制限事項

管理者レベルユーザだけが本コマンドを実行できます。

使用例

ファイルを移動します。

```
DGS-3200-24:4#move c:\log.txt c:\log1.txt
Command: move c:\log.txt c:\log1.txt

Process......Done.
Success.

DGS-3200-24:4#
```

copy

目的

ファイルをコピーします。

構文

copy {<drive_id>} <pathname 255> [{<drive_id>} <pathname 255> | image_id <int 1-n> | config_id <int 1-n> | prom]

copy [image_id <int 1-n> | config_id <int 1-n> | prom | log] {<drive_id>} <pathname 255>

説明

ファイルをファイルシステム内の別のファイル名にコピーします。フラッシュ上のファイルシステムをサポートしないプロジェクトのために、予約済みのキーワードを使用することで、本コマンド経由してファイルシステムをサポートするメディアに（から）ランタイムイメージ、コンフィグレーション、PROM、およびログなどのシステムファイルをコピーできます。ここでのキーワードは、image_id、config_id、prom、または log のことを示しています。

パラメータ

パラメータ	説明
<drive_id>	ドライブ番号を指定します。指定しないと、カレントドライブを参照します。
<pathname 255>	コピー元のファイル名をパス形式で指定します。
<pathname 255>	コピー先のファイル名をパス形式で指定します。
image_id <int 1-n>	コピーするファームウェアイメージを指定します。
config_id <int 1-n>	コピーするコンフィグレーションを指定します。
prom	指定すると PROM コードをコピーします。
log	指定すると格納済みのログをコピーします。

制限事項

管理者レベルユーザだけが本コマンドを実行できます。

使用例

ファイルをコピーします。

```
DGS-3200-24:4#copy c:\log.txt c:\log1.txt
Command: copy c:\log.txt c:\log1.txt

Process......Done.
Success.

DGS-3200-24:4#
```

イメージ番号をコピーします。

```
DGS-3200-24:4#copy c:\runtime.had image_id 1
Command: copy c:\runtime.had image_id 1
Do not Power off!
Please waite, programming Done.

Success.

DGS-3200-24:4#
```

format

目的

ドライブを初期化します。

構文

format <drive_id> [FAT16 | FAT32] {<label_name 8>}

説明

指定ドライブを初期化します。

パラメータ

パラメータ	説明
drive_id	ドライブ名を指定します。（例「C:」）
FAT16	FAT16 ファイルシステムを指定します。
FAT32	FAT32 ファイルシステムを指定します。
<label_name 8>	ドライブ名を指定します。

制限事項

管理者レベルユーザだけが本コマンドを実行できます。

使用例

メディアを初期化します。

```
DGS-3200-24:4#format c:\ FAT16
Command: format c:\ FAT16

Process.....................Done.
Success.

DGS-3200-24:4#
```

第 5 章　基本のスイッチコマンド

コマンドラインインタフェース (CLI) における基本的なスイッチコマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
create account	[admin | user] <username 15>
enable password encryption	
disable password encryption	
config account	<username 15> {encrypt [plain_text | sha_1] <password>}
show account	
delete account	<username 15>
show session	
show switch	
show environment*	
show serial_port	
config serial_port	{baud_rate [9600 | 19200 | 38400 | 115200] | auto_logout [never | 2_minutes | 5_minutes | 10_minutes | 15_minutes]}
enable clipaging	
disable clipaging	
enable telnet	<tcp_port_number 1-65535>
disable telnet	
enable web	<tcp_port_number 1-65535>
disable web	
save	{[config <config_id 1-2> | log | all]}
save**	{[config [<config_id 1-2> | <pathname 255>] | log {<pathname 255>} | all]}
reboot	
reset	{[config | system]}
login	
logout	

* DGS-3200-16/GE、DGS-3200-24/GE のみ。
** DGS-3200-24/GE のみ。

以下のセクションで各コマンドについて詳しく記述します。

create account

目的
　ユーザアカウント作成します。
構文
　create account [admin | user] <username 15>
説明
　ユーザアカウントを作成します。admin と user を含む 8 個までのユーザアカウントを作成できます。
パラメータ

パラメータ	説明
admin <username 15>	スイッチにすべての権利を持ってアクセスできる「admin」ユーザ（半角英数字 15 文字以内）を作成します。
user <username 15>	スイッチに一部の権利でアクセスするユーザ（半角英数字 15 文字以内）を作成します。
パスワード	15 文字以内で指定します。

制限事項
　管理者レベルユーザだけが本コマンドを実行できます。
使用例
　「dlink」というユーザ名で管理者レベルのユーザアカウントを作成します。

```
DGS-3200-10:4#create account admin dlink
Command: create account admin dlink

Enter a case-sensitive new password:****
Enter the new password again for confirmation:****
Success.

DGS-3200-10:4#
```

「System」というユーザレベルのアカウントを作成します。

```
DGS-3200-10:4#create account admin System
Command: create account admin System

Enter a case-sensitive new password:****
Enter the new password again for confirmation:****
Success.

DGS-3200-10:4#
```

enable password encryption

目的

パスワードの暗号化を有効または無効にします。

構文

enable password encryption

説明

ユーザアカウント設定情報をコンフィグレーションファイルに保存して、後にシステムに適用します。パスワードの暗号化を有効にすると、暗号化されたパスワードがコンフィグレーションファイルに保存されます。既存のユーザアカウントが暗号化されたパスワードを直接使用する場合、パスワードは暗号化形式のままとなります。

パラメータ

なし

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

パスワードの暗号化を有効にします。

```
DGS-3200-10:4#enable password encryption
Command: enable password encryption

Success.

DGS-3200-10:4#
```

disable password encryption

目的

パスワードの暗号化を有効または無効にします。

構文

disable password encryption

説明

ユーザアカウント設定情報をコンフィグレーションファイルに保存して、後にシステムに適用します。パスワードの暗号化を無効にすると、プレーンテキストのパスワードがコンフィグレーションファイルに保存されます。既存のユーザアカウントが暗号化されたパスワードを直接使用する場合、パスワードは暗号化形式のままとなります。

パラメータ

なし

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

パスワードの暗号化を有効にします。

```
DGS-3200-10:4#disable password encryption
Command: disable password encryption

Success.

DGS-3200-10:4#
```

config account

目的
　ユーザアカウントを設定します。
構文
　config account <username 15> {encrypt [plain_text | sha_1] <password>}
説明
　「create account」コマンドで作成したユーザアカウントを設定します。<password> を指定していない場合、システムはパスワード入力プロンプトを表示します。ユーザはプレーンテキスト形式でパスワードを入力します。
　<password> を指定している場合、プレーンテキスト形式または暗号化形式（SHA-1）でパスワードを入力できます。
パラメータ

パラメータ	説明
<username 15>	パスワードを変更するアカウントの新しいユーザ名を入力します。
encrypt	• plain_text - プレーンテキスト形式でパスワードを指定する場合に選択します。 • sha_1 - SHA-1 暗号化形式でパスワードを指定する場合に選択します。
<password>	ユーザアカウントのパスワード。プレーンテキスト形式および暗号化形式ではパスワード長が異なります。 • plain-text - プレーンテキスト形式のパスワードは 0-15 文字で入力します。 • sha_1 - 暗号化形式のパスワードは 35 バイトの固定長で入力します。 大文字と小文字を区別します。

制限事項
　管理者レベルユーザのみ本コマンドを実行できます。
使用例
　「dlink」というアカウントのユーザパスワードを設定します。

```
DGS-3200-10:4#config account dlink
Command: config account dlink

Enter a old password:****
Enter a case-sensitive new password:****
Enter the new password again for confirmation:****
Success.

DGS-3200-10:4#
```

　「administrator」というアカウントのユーザパスワードを設定します。

```
DGS-3200-10:4#config account administrator encrypt sha_1 *@&cRDtpNCeBiq15KOQsKVyrA0sAiCIZQwq
Command: config account administrator encrypt sha_1 *@&cRDtpNCeBiq15KOQsKVyrA0sAiCIZQwq

Success.

DGS-3200-10: 4#
```

show account

目的
　ユーザアカウントを表示します。
構文
　show account
説明
　スイッチに作成済みのすべてのユーザアカウントを表示します。
パラメータ
　なし。
制限
　なし。
使用例
　スイッチに作成済みのすべてのユーザアカウントを表示します。

```
DGS-3200-10:4#show account
Command: show account

Current Accounts:
Username        Access Level
--------        -----------
System          User
dlink           Admin

Total Entries : 1

DGS-3200-10:4#
```

delete account

目的
　設定済みのユーザアカウントを削除します。
構文
　delete account <username 15>
説明
　「create account」コマンドを使用して作成したユーザアカウントを削除します。
パラメータ

パラメータ	説明
<username 15>	削除するユーザアカウント名を入力します。

制限
　管理者レベルユーザのみ本コマンドを実行できます。アクティブな admin ユーザが存在する必要があります。
使用例
　「System」というユーザアカウントを削除します。

```
DGS-3200-10:4#delete account System
Command: delete account System

Success.

DGS-3200-10:4#
```

show session

目的
　現在ログインしているユーザのリストを表示します。
構文
　show session
説明
　コマンドを実行した時に CLI セッションにログインしている現在のユーザリストを表示します。
パラメータ
　なし
制限事項
　管理者レベルユーザのみ本コマンドを実行できます。
使用例
　現在ログインしているユーザのリストを表示します。

```
DGS-3200-10:4#show session
Command: show session

 ID Live Time    From            Level Name
 -- ------------ --------------- ----- ---------
 8  22:33:44.555 Serial Port     4     Anonymous

Total Entries:1

CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

show switch

目的

スイッチに関する一般的な情報を表示します。

構文

show switch

説明

スイッチに関する情報を表示します。

パラメータ

なし。

制限事項

なし。

使用例

スイッチに関する情報を表示します。

```
DGS-3200-10:4#show switch
Command: show switch

Device Type              : DGS-3200-10 Gigabit Ethernet Switch
MAC Address              : 00-00-00-01-02-00
IP Address               : 10.90.90.90 (Manual)
VLAN Name                : default
Subnet Mask              : 255.0.0.0
Default Gateway          : 0.0.0.0
Boot PROM Version        : Build 1.00.B012
Firmware Version         : Build 1.50.B019
Hardware Version         : A2
Serial Number            : P4CK183000001
System Name              :
System Location          :
System Contact           :
Device Uptime            : 8 days, 5 hours, 4 minutes, 26 seconds
Spanning Tree            : Disabled
GVRP                     : Disabled
IGMP Snooping            : Disabled
MLD Snooping             : Disabled
VLAN Trunk               : Disabled
Telnet                   : Enabled (TCP 23)
Web                      : Enabled (TCP 80)
SNMP                     : Enabled
RMON                     : Disabled
Safeguard Engine         : Disabled
SSL Status               : Disabled
SSH Status               : Disabled
802.1x                   : Disabled
Jumbo Frame              : Off
CLI Paging               : Enabled
MAC Notification         : Disabled
Port Mirror              : Disabled
SNTP                     : Disabled
DHCP Local Relay         : Disabled
Syslog Global State      : Disabled
Single IP Management     : Disabled
Dual Image               : Supported

Password Encryption Status     : Disabled

DGS-3200-10:4#
```

show environment

目的
　デバイス内部の温度を表示します。
構文
　show environment
説明
　デバイスの内部温度と DGS-3200-16/GE、DGS-3200-24/GE のファンの状態、および DGS-3200-24/GE の内部電源 / 外部電源の状態を表示します。
　DGS-3200-10 はサポートしていませんのでご注意ください。
パラメータ
　なし。
制限事項
　本機能は、DGS-3200-16/GE、DGS-3200-24/GE のみサポートします。
使用例
　スイッチ内部の温度状況を表示します。（DGS-3200-16/GE）

```
DGS-3200-16:4#show environment
Command: show environment

Side Fan         Temperature
                  (Celsius)
--------         ----------
 OK                 47

Note : The warning temperature is above 83 degrees.
```

　スイッチ内部の温度、ファン、内部電源 / 外部電源の状態を表示します。（DGS-3200-24/GE）

```
DGS-3200-24:4#show environment
Command: show environment

Internal Power   External Power   Left Fan   Temperature
                                            (Celsius)
--------------   --------------   --------   -----------
        Active             Fail         OK          34

Note: The warning temperature is above 80 degrees.
```

show serial_port

目的
　現在のシリアルポート設定を表示します。
構文
　show serial_port
説明
　現在のシリアルポート設定を表示します。
パラメータ
　なし。
制限事項
　なし
使用例
　シリアルポート設定を表示します。

```
DGS-3200-10:4#show serial_port
Command: show serial_port

Baud Rate   :115200
Data Bits   :8
Parity Bits :None
Stop Bits   :1
Auto-Logout :10 mins

DGS-3200-10:4#
```

config serial_port

目的

シリアルポートを設定します。

構文

config serial_port {baud_rate [9600 | 19200 | 38400 | 115200] | auto_logout [never | 2_minutes | 5_minutes | 10_minutes | 15_minutes]}

説明

管理ホストと通信するのに使用されるシリアルビットレートと無通信状態に対する自動ログアウト時間を設定します。

パラメータ

パラメータ	説明
baud_rate [9600 | 19200 | 38400 | 115200]	管理ホストと通信を行うために使用されるシリアルボーレート。次の 4 つのオプションがあります。9600、19200、38400、115200。初期値は 115200 です。
auto_logout	never - コンソールはユーザからの入力がなくなってもタイムアウトは発生しません。 • 2_minutes - コンソールはユーザからの入力がなくなってから、2 分経過すると自動的にログアウトします。 • 5_minutes - コンソールはユーザからの入力がなくなってから、5 分経過すると自動的にログアウトします。 • 10_minutes - コンソールはユーザからの入力がなくなってから、10 分経過すると自動的にログアウトします。 • 15_minutes - コンソールはユーザからの入力がなくなってから、15 分経過すると自動的にログアウトします。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

ボーレートを設定します。

```
DGS-3200-10:4#config serial_port baud_rate 9600
Command: config serial_port baud_rate 9600

Success.

DGS-3200-10:4#
```

enable clipaging

目的

コマンドが 1 ページ以上を表示する時、コンソール画面のスクローリングを一時停止します。

構文

enable clipaging

説明

コンソール画面で複数ページがすぐにスクロールしてしまう場合に使用します。本コマンドは、ページごとに一時停止します。初期値は有効です。

パラメータ

なし。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

出力がページの終わりに到達すると画面表示は一時停止します。

```
DGS-3200-10:4#enable clipaging
Command: enable clipaging

Success.

DGS-3200-10:4#
```

disable clipaging

目的

コマンドが 1 ページ以上を表示する時、コンソール画面のスクローリングを一時停止する機能を無効にします。

構文

disable clipaging

説明

複数ページに渡る情報を表示する場合に各ページの終わりでコンソール画面を一時停止する機能を無効にします。

パラメータ

なし。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

コマンド出力がページの終わりに達する場合に、画面表示を一時停止する機能を無効にします。

```
DGS-3200-10:4#disable clipaging
Command: disable clipaging

Success.

DGS-3200-10:4#
```

enable telnet

目的

Telnet プロトコルを使用したスイッチとの通信および管理を有効にします。

構文

enable telnet <tcp_port_number 1-65535>

説明

Telnet を有効にし、ポート番号を設定します。

パラメータ

パラメータ	説明
<tcp_port_number 1-65535>	TCP ポート番号。TCP ポート番号は 1-65535 です。Telnet プロトコルの一般的な TCP ポート番号は 23 です。 初期値では TCP ポート番号は 23 で有効となっています。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

Telnet を有効にし、ポート番号を設定します。

```
DGS-3200-10:4#enable telnet 23
Command: enable telnet 23

Success.

DGS-3200-10:4#
```

disable telnet

目的
　Telnet プロトコルを無効にします。
構文
　disable telnet
説明
　Telnet プロトコルを無効にします。
パラメータ
　なし。
制限事項
　管理者レベルユーザのみ本コマンドを実行できます。
使用例
　スイッチの Telnet プロトコルを無効にします。

```
DGS-3200-10:4#disable telnet
Command: disable telnet

Success.

DGS-3200-10:4#
```

enable web

目的
　スイッチの HTTP ベースの管理ソフトウェアを有効にします。
構文
　enable web <tcp_port_number 1-65535>
説明
　HTTP を有効にし、ポート番号を設定します。
パラメータ

パラメータ	説明
<tcp_port_number 1-65535>	TCP ポート番号。TCP ポート番号は 1-65535 です。Web ベース管理ソフトウェアの一般的な TCP ポート番号は 80 です。初期値では TCP ポート番号は 80 で有効となっています。

制限事項
　管理者レベルユーザのみ本コマンドを実行できます。
使用例
　HTTP を有効にし、ポート番号を設定します。

```
DGS-3200-10:4#enable web 80
Command: enable web 80

Note : SSL will be disabled if web is enabled.
Success.

DGS-3200-10:4#
```

disable web

目的
　HTTP ベース管理ソフトウェアを無効にします。
構文
　disable web
説明
　HTTP ベース管理ソフトウェアを無効にします。
パラメータ
　なし。
制限事項
　管理者レベルユーザのみ本コマンドを実行できます。
使用例
　HTTP を無効にします。

```
DGS-3200-10:4#disable web
Command: disable web

Success.

DGS-3200-10:4#
```

save

目的
　NV-RAM にスイッチ設定の変更を保存します。
構文
　save {[config <config_id 1-2> | log | all]}
　save {[config [<config_id 1-2> | <pathname 255>] | log {<pathname 255>} | all]}（DGS-3200-24/GE のみ）
説明
　NV-RAM に現在のスイッチ設定を保存します。保存されたスイッチ設定は、スイッチが再起動するたびにスイッチのメモリにロードされます。
パラメータ

パラメータ	説明
config <config_id 1-2> | log | all | <pathname 255>	• config <config_id 1-2> - コンフィグレーションファイルに現在の設定を保存します。 • log - 現在アクティブなコンフィグレーションに変更とログを保存します。 • all - すべてのコンフィグレーション設定とログを保存します。 • <pathname 255> - デバイスのファイルシステムにおけるパス名を指定します。（DGS-3200-24/GE のみ） 「save」の後に何も指定しないと、現在アクティブなコンフィグレーションファイルに変更を保存します。

制限事項
　管理者レベルユーザのみ本コマンドを実行できます。
使用例
　NV-RAM に現在のスイッチ設定を入力します。

```
DGS-3200-10:4#save
Command: save

Saving all configurations to NV-RAM.........Done.

DGS-3200-10:4#
```

　NV-RAM にコンフィグレーション 1 を保存します。

```
DGS-3200-10:4#save config 1
Command: save config 1

Saving configurations 1 to NV-RAM.........Done.

DGS-3200-10:4#
```

NV-RAM にログを保存します。

```
DGS-3200-10:4#save log
Command: save log
Saving all System logs to NV-RAM.........Done.

DGS-3200-10:4#
```

NV-RAM にコンフィグレーションおよびログファイルのすべてを保存します。

```
DGS-3200-10:4#save all
Command: save all
Saving configuration and logs to NV-RAM...... Done.

DGS-3200-10:4#
```

reboot

目的

スイッチを再起動します。

構文

reboot

説明

スイッチを再起動します。

パラメータ

なし。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

スイッチを再起動します。

```
DGS-3200-10:4#reboot
Command: reboot

Are you sure you want to proceed with the system reboot?(y|n)
Please wait, the switch is rebooting...
```

reset

目的

スイッチを工場出荷時設定に戻します。

構文

reset {[config | system]}

説明

スイッチの設定を工場で割り当てられた初期設定に戻します。

パラメータ

パラメータ	説明
config	IPアドレス、ユーザアカウント、スイッチヒストリおよびバナーなどのパラメータが工場出荷時設定にリストアされます。スイッチは保存または再起動しません。
system	すべての工場出荷時設定がスイッチにリストアされます。スイッチの設定が初期値に変更された後、保存および再起動が行われます。再起動するとフォワーディングデータベース内のすべてのエントリがクリアされます。 パラメータを指定しないと、IP アドレス、ユーザアカウント、およびヒストリログを除き、すべてのパラメータが初期設定にリセットされます。スイッチは保存または再起動しません。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

IP アドレス、ヒストリログ、ユーザアカウント、およびグリーティングバナーを除くすべてのスイッチパラメータをリセットします。

```
DGS-3200-10:4#reset
Command: reset

Are you sure you want to proceed with system reset except IP address, log, user
account and banner?(y/n) y

Success.

DGS-3200-10:4#
```

システムコンフィグレーション設定をリセットします。

```
DGS-3200-10:4#reset config
Command: reset config

Are you sure you want to proceed with system reset?(y/n) y

Success.

DGS-3200-10:4#
```

すべてのシステムパラメータをリセットして、保存を行い、スイッチを再起動します。

```
DGS-3200-10:4#reset system
Command: reset system

Are you sure you want to proceed with system reset?(y/n)
   y-(reset all include configure, save, reboot)
   n-(cancel Command) y

Loading factory default configuration… Done.

Saving all configuration to NV-RAM… Done.
Please wait, the switch is rebooting…
```

login

目的
　スイッチのコンソールにログインします。
構文
　login
説明
　ログインを開始します。ユーザ名とパスワードプロンプトが表示されます。
パラメータ
　なし。
制限事項
　なし。
使用例
　ログインを開始します。

```
DGS-3200-10:4#login
Command: login

UserName:
```

logout

目的
　スイッチコンソールからログアウトします。
構文
　logout
説明
　スイッチコンソールの現在のユーザセッションを終了します。
パラメータ
　なし。
制限事項
　なし。
使用例
　スイッチコンソールの現在のユーザセッションを終了します。

```
DGS-3200-10:4#logout
Command: logout


***********
* Logout  *
***********

                        DGS-3200-10 Gigabit Ethernet Switch
                              Command Line Interface
                             Firmware: Build 1.50.B019
           Copyright(C) 2009 D-Link Corporation. All rights reserved.

UserName:
```

第 6 章　スイッチユーティリティコマンド

コマンドラインインタフェース（CLI）におけるスイッチユーティリティコマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
download	[firmware_fromTFTP [<ipaddr> | <ipv6addr>] <path_filename 64> [image_id <int 1-2>] | cfg_fromTFTP [<ipaddr> | <ipv6addr>] <path_filename 64> {[<config_id 1-2> | increment]}]
download *	firmware_fromTFTP [<ipaddr> | <ipv6addr>] <path_filename 64> <pathname 255>
download *	cfg_fromTFTP [<ipaddr> | <ipv6addr>] <path_filename 64> <pathname 255>
upload log_toTFTP	[<ipaddr> | <ipv6addr>] <path_filename 64>
upload cfg_toTFTP	[<ipaddr> | <ipv6addr>] <path_filename 64> {<config_id 1-2>}
upload attack_log_toTFTP	[<ipaddr> | <ipv6addr>] <path_filename 64>
config firmware	image_id <int 1-2> [delete | boot_up]
config firmware *	<pathname 255> [boot_up]
config configuration	<config_id 1-2> [boot_up | delete | active]
config configuration *	<pathname 255> [boot_up | active]
show firmware information	
show config	[current_config | config_in_nvram <config_id 1-2> | information]
ping	<ipaddr> {times <value 1-255>} {timeout <sec 1-99>}
ping6	<ipv6addr> {times <value 1-255>| size <value 1-6000> | timeout <value 1-10>}
traceroute	<ipaddr> {ttl <value 1-60>} {port <value 30000-64900>} {timeout <sec 1-65535>} {probe <value 1-9>}
telnet	<ipaddr> {tcp_port <value 0-65535>}

* DGS-3200-24/GE のみ

「Interface」フィールドは、Link-Local ネットワークのアドレスに使用されます。Link-local の IPv6 アドレスには、明確なインタフェース名を入力することをお勧めします。グローバル IPv6 アドレスの場合、フィールドは省略されることがあります。例えば以下のようになります。

```
DGS-3200-10:4#upload cfg_toTFTP fe80::20d:88ff:fe11:7b6c%System DGS-3200.cfg
```

以下のセクションで各コマンドについて詳しく記述します。

download

目的

TFTP サーバから新しいファームウェアまたはスイッチのコンフィグレーションファイルをダウンロードしてインストールします。

構文

download [firmware_fromTFTP [<ipaddr> | <ipv6addr>] <path_filename 64> [image_id <int 1-2>] | cfg_fromTFTP [<ipaddr> | <ipv6addr>] <path_filename 64> {[<config_id 1-2> | increment]}]

download firmware_fromTFTP [<ipaddr> | <ipv6addr>] <path_filename 64> <pathname 255>（DGS-3200-24/GE のみ）

download cfg_fromTFTP [<ipaddr> | <ipv6addr>] <path_filename 64> <pathname 255>（DGS-3200-24/GE のみ）

説明

TFTP サーバから新しいファームウェアまたはスイッチのコンフィグレーションファイルをダウンロードします。ファームウェアは image_id または config_id に応じて、異なるセクションにロードできます。DGS-3200-24/GE の場合には、SD カードにもダウンロードすることができます。

パラメータ

パラメータ	説明
firmware_fromTFTP	新しいファームウェアを TFTP サーバからスイッチにダウンロードしてインストールします。 • <ipaddr> - TFTP サーバの IP アドレス。 • <ipv6addr> - TFTP サーバの IPv6 アドレス。 • <path_filename 64> - TFTP サーバ上のファームウェアファイルの DOS パスとファイル名（64 文字以内）。例 : c: \dgs3427.had • image_id <int 1-2> - スイッチメモリにおけるファームウェアのイメージ番号を指定します。スイッチのメモリには 2 個のファームウェアイメージを格納できます。変更されない限り、ID1 が初期設定の起動用ファームウェアです。
cfg_fromTFTP	新しいコンフィグレーションファイルを TFTP サーバからスイッチにダウンロードしてインストールします。 • <ipaddr> - TFTP サーバの IP アドレス。 • <ipv6addr> - TFTP サーバの IPv6 アドレス。 • <path_filename 64> - TFTP サーバ上のコンフィグレーションの DOS パスとファイル名（64 文字以内）。例 : c: \dgs3427.had • config_id <int 1-2> - スイッチは、セクション ID で指定される 2 つのコンフィグレーションファイルを保持することができます。config_id が指定されないと、ダウンロードされるコンフィグレーションは、システムに適用されます。config_id が指定されると、ダウンロードされるコンフィグレーションは、選択したセクション（1 か 2）のフラッシュメモリだけに保存され、システムに適用されません。「config configuration」コマンドを使用して変更しない限り、config_id が起動用コンフィグレーションであることにご注意ください。 • increment - 部分的なスイッチコンフィグレーションファイルのダウンロードが可能です。コンフィグレーションファイル内に明記されているスイッチパラメータだけを変更するようにファイルをダウンロードすることができます。他のすべてのスイッチパラメータは変更されないで残ります。 • <pathname 255> - SD カードファイルシステムのファイルを指定します。ファイルシステムをサポートしていない場合には指定する必要はありません。（DGS-3200-24/GE のみ）

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

ファームウェアファイルをダウンロードします。

```
DGS-3200-10:4#download firmware_fromTFTP 10.90.90.90 dgs3200_Run_1_5_B019.had
Command: download firmware_fromTFTP 10.90.90.90 dgs3200_Run_1_5_B019.had

Connecting to server...................Done.
Download firmware.....................Done.  Do not power off !
Please wait, programming flash.........Done.

DGS-3200-10:4#
```

DGS-3200-24/GE に挿入した SD カードにファームウェアをダウンロードします。

```
DGS-3200-24:4#download firmware_fromTFTP 10.90.90.1 dgs3200.had c:\image.had
Command: download firmware_fromTFTP 10.90.90.1 dgs3200.had c:\image.had

Connecting to server................... Done.
Download firmware..................... Done.  Do not power off !
Success.

DGS-3200-24:4#
```

upload

目的

スイッチのコンフィグレーションファイルまたはスイッチのヒストリログを TFTP にアップロードします。

構文

upload log_toTFTP [<ipaddr> | <ipv6addr>] <path_filename 64>
upload cfg_toTFTP [<ipaddr> | <ipv6addr>] <path_filename 64> {<config_id 1-2>}
upload attack_log_toTFTP [<ipaddr> | <ipv6addr>] <path_filename 64>

説明

スイッチの現在のコンフィグレーションファイルまたはスイッチのヒストリログを TFTP にアップロードします。

パラメータ

パラメータ	説明
log_toTFTP	スイッチヒストリログを TFTP サーバにアップロードします。 • <ipaddr> - TFTP サーバの IP アドレス。TFTP サーバはスイッチと同じ IP サブネットにある必要があります。 • <ipv6addr> - TFTP サーバの IPv6 アドレス。TFTP サーバはスイッチと同じ IP サブネットにある必要があります。 • <path_filename 64> - スイッチコンフィグレーションファイルの場所を TFTP サーバに指定します。本ファイルはスイッチからアップロードされたファイルと交換されます。
cfg_toTFTP	スイッチの現在の設定を TFTP にアップロードします。 • <ipaddr> - TFTP サーバの IPv4 アドレス。TFTP サーバはスイッチと同じ IP サブネットにある必要があります。 • <ipv6addr> - TFTP サーバの IPv6 アドレス。TFTP サーバはスイッチと同じ IP サブネットにある必要があります。 • <path_filename 64> - スイッチコンフィグレーションファイルの場所を TFTP サーバに指定します。本ファイルは、スイッチからアップロードされたファイルと交換されます。 • <config_id 1-2> - コンフィグレーションの ID 番号を指定します。
attack_log_toTFTP	スイッチアタックログを TFTP サーバにアップロードします。 • <ipaddr> - TFTP サーバの IPv4 アドレス。TFTP サーバはスイッチと同じ IP サブネットにある必要があります。 • <ipv6addr> - TFTP サーバの IPv6 アドレス。TFTP サーバはスイッチと同じ IP サブネットにある必要があります。 • <path_filename 64> - スイッチアタックログの場所を TFTP サーバに指定します。本ファイルは、スイッチからアップロードされたファイルと交換されます。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

TFTP サーバにコンフィグレーションファイルをアップロードします。

```
DGS-3200-10:4#upload cfg_toTFTP 10.48.74.121 c:\cfg\DGS-3200-10\cfg config_id 1
Command: upload cfg_toTFTP 10.48.74.121 c:\cfg\DGS-3200-10\cfg config_id 1

Connecting to server...Done.
Upload configuration...Done.

DGS-3200-10:4#
```

TFTP サーバにシステムログをアップロードします。

```
DGS-3200-10:4#upload log_toTFTP 10.48.74.121 c:\cfg\DGS-3200-10\log
Command: upload log_toTFTP 10.48.74.121 c:\cfg\DGS-3200-10\log

Connecting to server...Done.
Upload log...Done.

DGS-3200-10:4#
```

config firmware

目的

ブートアップイメージとして指定したファームウェアを設定、または削除します。

構文

config firmware image_id <int 1-2> [delete | boot_up]

config firmware <pathname 255> [boot_up]（DGS-3200-24/GE のみ）

説明

ファームウェアセクションを設定します。ファームウェアセクションの削除またはブートアップセクション設定を選択できます。

パラメータ

パラメータ	説明
image_id <int 1-2>	動作しているセクションを指定します。スイッチは 2 つのファームウェアバージョンを保持し、イメージ ID を指定することで選択できます。 設定するスイッチメモリのファームウェアの ID 番号を選択します。
delete	本パラメータを入力し、指定したファームウェアセクションを削除します。
boot_up	本パラメータを入力し、起動セクションとしてファームウェアイメージ ID を指定します。
<pathname 255>	SD カードファイルシステムのファームウェアファイルを指定します。ファイルシステムをサポートしていない場合には指定する必要はありません。(DGS-3200-24/GE のみ)

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

起動セクションとして指定したファームウェアのセクション 2 を削除します。

```
DGS-3200-10:4#config firmware image_id 2 delete
Command: config firmware image_id 2 delete

Are you sure you want to delete firmware image_id 2?(y/n) y
Please wait, deleting image ...........Done.

Success.

DGS-3200-10:4#
```

ブートアップイメージとして指定したファームウェアを設定します。

```
DGS-3200-10:4#config firmware image_id 1 boot_up
Command: config firmware image_id 1 boot_up

Success.

DGS-3200-10:4#
```

ブートアップイメージとして SD カード内のファームウェアを設定します。（DGS-3200-24/GE のみ）

```
DGS-3200-24:4#config firmware c:\run3.had boot_up
Command: config firmware c:\run3.had boot_up

Success.

DGS-3200-24:4#
```

config configuration

目的

指定したコンフィグレーションをブートアップまたはアクティブ用に設定するか、または削除します。

構文

config configuration <config_id 1-2> [boot_up | delete | active]

config configuration <pathname 255> [boot_up | active]（DGS-3200-24/GE のみ）

説明

指定したコンフィグレーションをブートアップまたはアクティブ用に設定するか、または削除します。

パラメータ

パラメータ	説明
<config_id 1-2>	設定または削除されるセクションを指定します。
boot_up	起動用セクションとしてコンフィグレーションセクションを指定します。
delete	指定されたセクションに関する内容を削除します。
active	アクティブセクションとしてコンフィグレーションセクションを指定します。
<pathname 255>	SD カードファイルシステムのコンフィグレーションファイルを指定します。ファイルシステムをサポートしていない場合には指定する必要はありません。(DGS-3200-24/GE のみ)

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

指定のコンフィグレーションを削除します。

```
DGS-3200-10:4#config configuration 2 delete
Command: config configuration 2 delete

Success.

DGS-3200-10:4#
```

SD カード内のコンフィグレーションを再起動用に設定します。（DGS-3200-24/GE のみ）

```
DGS-3200-24:4#config configuration c:\config.cfg boot_up
Command: config configuration 2 delete

Success.

DGS-3200-24:4#
```

show firmware information

目的

ファームウェア情報を表示します。

構文

show firmware information

説明

ファームウェア情報を表示します。

パラメータ

なし。

制限事項

なし。

使用例

スイッチの現在のファームウェア情報を表示します。

```
DGS-3200-24:4# show firmware information
Command: show firmware information

Image ID : 1(Boot up firmware)
    Version     : 1.50.B019
    Size        : 3713664 Bytes
    Update Time : 2000/01/01 00:57:40
    From        : 10.5.2.5(Console)
    User        : Anonymous

Image ID : 2
    Version     : (Empty)
    Size        :
    Update Time :
    From        :

DGS-3200-24:4#
```

show config

目的

スイッチのコンフィグレーション設定の現在または保存されているバージョンを表示します。

構文

show config [current_config | config_in_nvram <config_id 1-2> | information]

説明

NV RAMに保存されているすべてのコンフィグレーション設定を表示します。または、現在設定されているコンフィグレーション設定を表示します。

パラメータ

パラメータ	説明
current_config	現在設定されているコンフィグレーション設定を表示します。
config_in_nvram <config_id 1-2>	NV RAM に保存されているコンフィグレーションを表示するセクションを指定します。
information	NV RAM に保存されているすべてのコンフィグレーション設定を表示します。

制限事項

なし。

使用例

現在のコンフィグレーション設定を参照します。

```
DGS-3200-10:4#show config information
Command: show config information

ID : 1(Current active configuration)
-------------- ------------ ----------------------------
Version     : 1.50.B019
Size        : 14964 Bytes
Updata Time : 2000/01/01 00:32:25
From        : Local save(Console)
User        : Anonymous
Boot Up     : Yes

ID : 2
-------------- ------------ ----------------------------
Version     : 1.00B006
Size        : 5 Bytes
Updata Time : 2000/01/01 00:02:40
From        : Local save(Console)
User        : Anonymous
Boot Up     : No

DGS-3200-10:4#
```

ping

目的

ネットワークデバイス間の接続性をテストします。

構文

ping <ipaddr> {times <value 1-255>} {timeout <sec 1-99>}

説明

Ping コマンドはリモート IP アドレスに Internet Control Message Protocol（ICMP）エコーメッセージを送信します。その後、リモート IP アドレスは、「エコー」するか、またはメッセージを返します。これは、スイッチとリモートデバイス間の接続性を確認するために使用されます。

パラメータ

パラメータ	説明
<ipaddr>	ホストの IP アドレスを指定します。
times <value 1-255>	送信する各 ICMP エコーメッセージ数（1-255）。指定しないと ICMP エコーメッセージを継続的に送信します。
timeout <sec 1-99>	リモートデバイスからの応答を待つ時間を定義します。1-99（秒）を指定します。初期値は 1（秒）です。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

ICMP エコーメッセージを IP アドレス「10.51.17.1」に 4 回送信します。

```
DGS-3200-10:4#ping 10.51.17.1 times 4
Command: ping 10.51.17.1 times 4

Reply from 10.51.17.1, time<10ms
Reply from 10.51.17.1, time<10ms
Reply from 10.51.17.1, time<10ms
Reply from 10.51.17.1, time<10ms
Ping Statistics for 10.51.17.1
Packets: Sent =4, Received =4, Lost =0

DGS-3200-10:4#
```

ping6

目的

IPv6 を使用してネットワークデバイス間の接続性をテストします。

構文

ping6 <ip6addr> {times <value 1-255> | size <value 1-6000> | timeout <value 1-10>}

説明

ICMP(Internet Control Message Protocol) エコーメッセージをリモート IP アドレスに送信します。その後、リモート IP アドレスは、「エコー」するか、またはメッセージを返します。これは、スイッチとリモートデバイス間の接続性を確認するために使用されます。

パラメータ

パラメータ	説明
<ip6addr>	ホストの IPv6 アドレスを指定します。
times <value 1-255>	送信する各 ICMP エコーメッセージ数（1-255）。0 の値は ICMP エコーメッセージを継続的に送信します。
size <value 1-6000>	サイズ（1-6000）を定義します。
timeout <value 1-10>	リモートデバイスからの応答を待つ時間を定義します。1-10（秒）を指定します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

「3FFE:2::D04D:7878:66D:E5BC」に ICMP エコーメッセージを 10 回送信します。

```
DGS-3200-10:4#ping6 3FFE:2::D04D:7878:66D:E5BC times 10 size 6000 timeout 10
Command: ping6 3FFE:2::D04D:7878:66D:E5BC times 10 size 6000 timeout 10

Reply from 3FFE:2::D04D:7878:66D:E5BC, bytes=6000 time<10 ms
Reply from 3FFE:2::D04D:7878:66D:E5BC, bytes=6000 time<10 ms
Reply from 3FFE:2::D04D:7878:66D:E5BC, bytes=6000 time<10 ms
Reply from 3FFE:2::D04D:7878:66D:E5BC, bytes=6000 time<10 ms
Reply from 3FFE:2::D04D:7878:66D:E5BC, bytes=6000 time<10 ms
Reply from 3FFE:2::D04D:7878:66D:E5BC, bytes=6000 time<10 ms
Reply from 3FFE:2::D04D:7878:66D:E5BC, bytes=6000 time<10 ms
Reply from 3FFE:2::D04D:7878:66D:E5BC, bytes=6000 time<10 ms
Reply from 3FFE:2::D04D:7878:66D:E5BC, bytes=6000 time<10 ms
Reply from 3FFE:2::D04D:7878:66D:E5BC, bytes=6000 time<10 ms
Ping Statistics for 3FFE:2::D04D:7878:66D:E5BC
Packets: Sent =10, Received =10, Lost =0

DGS-3200-10:4#
```

traceroute

目的

スイッチと宛先のエンドステーション間の経路をトレースします。

構文

traceroute <ipaddr> {ttl <value 1-60>} {port <value 30000-64900>} {timeout <sec 1-65535>} {probe <value 1-9>}

説明

ネットワーク上のスイッチとホスト間の経路をトレースします。

パラメータ

パラメータ	説明
<ipaddr>	ホストの IP アドレスを指定します。
ttl <value1-60>	トレースルートリクエストが有効な回数。これはルータの最大数です。本コマンドは 2 つのデバイス間のネットワーク経路を検索する間行き交います。
port <value 30000-64900>	ポート番号。値の範囲は、30000-64900 です。
timeout <sec 1-65535>	デバイスからの応答を待つ時間を定義します。範囲は 1-65535（秒）です。
probe <value 1-9>	プローブの数。範囲は、1-9 です。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

スイッチと 10.48.74.121 間の経路をトレースします。

```
DGS-3200-10:4#traceroute 10.48.74.121 probe 3
Command: traceroute 10.48.74.121 probe 3

<10 ms. 10.48.74.121
<10 ms. 10.48.74.121
<10 ms. 10.48.74.121

DGS-3200-10:4#
```

telnet

目的

Telnet をサポートするホストにログインします。

構文

telnet <ipaddr> {tcp_port <value 0-65535>}

説明

ファームウェア情報を表示します。

パラメータ

パラメータ	説明
<ipaddr>	ログインするホストの IP アドレスを指定します。
tcp_port <value 0-65535>	Telnet ポート。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

ホストに Telnet します。

```
DGS-3200-10:4#telnet 10.90.90.90
Command: telnet 10.90.90.90

Connecting to 10.90.90.90...
[Press Ctrl+Y to disconnect.]

DGS-3200-10:4#Welcome to Microsoft Telnet Service

login: administrator
password:

*===============================================================
Welcome to Microsoft Telnet Server.
*===============================================================

C:\Documents and Settings\Administrator>exit
Connection to host lost.

DGS-3200-10:4#
```

第 7 章　省電力コマンド

コマンドラインインタフェース（CLI）における省電力コマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
config power_saving	{state [enable | disable] | length_detection [enable | disable]}
show	power_saving

以下のセクションで各コマンドについて詳しく記述します。

config power_saving

目的

省電力のためにグローバルな状態とケーブル長検出を設定します。

構文

config power_saving {state [enable | disable] | length_detection [enable | disable]}

説明

省電力のためにグローバルステータスとケーブル長検出を設定します。

パラメータ

パラメータ	説明
state	省電力機能におけるリンク状態を有効または無効にします。初期値は有効です。
length_detection	省電力機能におけるケーブル長検出を有効または無効にします。初期値は有効です。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

省電力機能を設定します。

```
DGS-3200-10:4#config power_saving state enable
Command: config power_saving state enable

Success.

DGS-3200-10:4#
```

省電力機能のグローバルステータスとケーブル長検出を設定します。

```
DGS-3200-10:4#config power_saving state enable length_detection enable
Command: config power_saving state enable length_detection enable

Success.

DGS-3200-10:4#
```

show power_saving

目的

省電力機能の設定情報を表示します。

構文

show power_saving

説明

省電力機能の設定情報を表示します。

パラメータ

なし。

制限事項

なし。

使用例

省電力機能の設定情報を表示します。

```
DGS-3200-10:4#show power_saving
Command: show power_saving

Power  Saving    State : Enabled
Length Detection State : Enabled

DGS-3200-10:4#
```

第 8 章　SNMPv1/v2 コマンド

SNMP（Simple Network Management Protocol）は、OSI 参照モデルの第 7 層（アプリケーション層）のプロトコルで、ネットワークデバイスの管理や監視を行います。ネットワーク管理デバイスは、SNMP を利用してゲートウェイ、ルータ、およびその他のネットワークデバイスの設定状態を確認または変更します。また、SNMP を利用してスイッチやスイッチ群、またはネットワークに対し、正常な動作を行うためのシステム設定、パフォーマンスの監視、問題の検出を行います。

SNMP をサポートする管理デバイスは、スイッチ上で動作する SNMP エージェントと呼ばれるソフトウェアを実装しています。SNMP エージェントが管理する定義された変数（管理オブジェクト）により、デバイスの管理を行います。これらのオブジェクトは MIB（Management Information Base）内に定義され、デバイス上の SNMP エージェントにより管理される情報表示の基準を（管理側のデバイスに）伝えます。SNMP では、MIB の仕様と、ネットワークを経由してこれらの情報にアクセスするために使用するプロトコルのフォーマットを定義しています。

DGS-3200 シリーズは、SNMP バージョン 1（SNMP v1）、2c（SNMP v2c）、および 3（SNMP v3）をサポートしています。スイッチの監視と制御に使用する SNMP バージョンを選択することができます。これらの 3 つのバージョンでは、管理ステーションとネットワークデバイス間に適用されるセキュリティのレベルに違いがあります。

SNMP バージョン 1 と 2 では、ユーザ認証はパスワードに良く似た「コミュニティ名」を使用して行われます。リモートユーザの SNMP アプリケーションとスイッチの SNMP は同じコミュニティ名を使用する必要があります。認証が行われていない SNMP パケットを受信した場合、そのパケットは廃棄されます。

SNMP バージョン 1 と 2 を使用するスイッチのコミュニティ名の初期値は次の通りです。

- public -（ネットワークデバイス SNMP 管理ソフトに）MIB オブジェクトの読み取り権限が許可されているコミュニティ名です。
- private - MIB オブジェクトの読み取りと書き込みの権限を与えられているコミュニティ名です。

SNMP バージョン 3 では、さらに高度な認証プロセスを採用し、そのプロセスは 2 つのパートに分かれます。最初のパートは SNMP マネージャとして動作することのできるユーザとその属性を掲載したリストを保持し、次のパートではリスト上のユーザの SNMP マネージャとしての権限を記載しています。

スイッチではユーザグループをリストにまとめ、権限を設定します。SNMP のバージョンは SNMP マネージャのグループごとに設定可能です。そのため、SNMP マネージャを “SNMP バージョン 1 を使用して読み取り専用の情報とトラップの受信のみを可能にするグループ” や、“SNMP バージョン 3 を使用して高いセキュリティレベルを与え、読み書き可能にするグループ” など、グループごとに登録することができます。

個別のユーザや SNMP マネージャグループに SNMP バージョン 3 を使用すると、特定の SNMP 管理機能を許可または制限できるようになります。そのような管理機能の許可または制限は、各 MIB に関連付けられる OID（Object Identifier）を使用して定義します。SNMP バージョン 3 では SNMP メッセージを暗号化することにより、さらに強固なセキュリティを実現できます。スイッチでの SNMP バージョン 3 の設定方法については次のセクションを参照してください。

トラップ

トラップとは、スイッチ上で発生したイベントを、ネットワーク管理者に警告するためのメッセージです。イベントには、再起動（誰かが誤ってスイッチの電源を切ってしまった）などの重大なものから、ポートの状態変化を知らせる軽微なものまで幅広い種類があります。スイッチはトラップを生成してトラップ受信者（またはネットワークマネージャ）に送信します。典型的なトラップには、認証の失敗、トポロジの変化、ブロードキャスト / マルチキャストストーム発生などがあります。

MIB

スイッチの MIB には管理情報およびカウンタ情報が格納されています。本スイッチは標準 MIB-II モジュールを使用し、MIB オブジェクトの値は SNMP ベースのネットワーク管理ソフトウェアから読み出されます。標準 MIB-II に加えて、拡張 MIB としてベンダ固有の MIB もサポートします。MIB OID の指定によってもベンダ固有の MIB を取得することができます。MIB の値は読み取り専用、または読み書き可です。

DGS-3200 シリーズは、スイッチの環境に合わせた柔軟性のある SNMP 管理機能を採用しています。SNMP 管理機能は、ネットワークの要求やネットワーク管理者の好みに合わせてカスタマイズすることができます。

DGS-3200 シリーズは、SNMP バージョン 1、2c、および 3 をサポートします。管理者は、スイッチの監視と制御にどの SNMP バージョンを使用するかを指定できます。これらの 3 つのバージョンでは、管理ステーションとネットワークデバイス間に適用されるセキュリティのレベルに違いがあります。3 つの SNMP バージョンのセキュリティ機能は以下の通りです。

SNMP バージョン	認証方式	説明
v1	コミュニティ名	NoAuthNoPriv - コミュニティ名が認証に使用されます。
v2c	コミュニティ名	NoAuthNoPriv - コミュニティ名が認証に使用されます。
v3	ユーザ名	NoAuthNoPriv - ユーザ名が認証に使用されます。
v3	MD5 または SHA	AuthNoPriv - 認証は HMAC-MD5 または HMAC-SHA アルゴリズムに基づきます。
v3	MD5 DES または SHA DES	AuthPrivDES - 認証は HMAC-MD5 または HMAC-SHA アルゴリズムに基づきます。 56 ビット暗号方式が CBC-DES（DES-56）標準規格に基づいて追加されます。

コマンドラインインタフェース（CLI）における SNMPv1/v2 コマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
create snmp community	<community_string 32> view <view_name 32> [read_only | read_write]
delete snmp community	<community_string 32>
show snmp community	

以下のセクションで各コマンドについて詳しく記述します。

注意 56 ページの「第 9 章 SNMPv3 コマンド」が使用されている場合、SNMPv1/v2 コマンドは必要ありません。

create snmp community

目的

SNMP マネージャとエージェントとの関係を定義するために SNMP コミュニティ名を作成します。コミュニティ名は、スイッチ上のエージェントへのアクセスを行う際のパスワードの役割をします。以下の特性はコミュニティ名と関係します。

- アクセスリストはコミュニティ名を使用して、スイッチ上の SNMP エージェントにアクセスを行う SNMP マネージャの IP アドレスが掲載されています。
- SNMP コミュニティにアクセス可能な MIB オブジェクトには「read_write」（読み書き可能）または「read_only」（読み出しのみ可能）のレベルがあります。

構文

create snmp community <community_string 32> view <view_name 32> [read_only | read_write]

説明

SNMP コミュニティ名を作成し、このコミュニティ名にアクセス制限を行う文字列を割り当てます。

パラメータ

パラメータ	説明
<community_string 32>	スイッチの SNMP コミュニティのメンバを識別します（32 文字までの半角英数字）。本コミュニティ名は、リモートの SNMP マネージャが、スイッチの SNMP エージェント内の MIB オブジェクトにアクセスする際にパスワードのように使用します。
<view_name 32>	SNMP ビュー名（32 文字以内の半角英数字）。
[read_only | read_write]	リモート SNMP マネージャがスイッチにアクセスできる MIB オブジェクトのグループを指定します（32 文字までの半角英数字）。 • read_only - 本コマンドを使用して作成したコミュニティ名を使用する SNMP コミュニティメンバは、スイッチの MIB オブジェクトの内容を読み出しが可能です。初期値は「public」です。 • read_write - 本コマンドを使用して作成したコミュニティ名を使用する SNMP コミュニティメンバは、スイッチの MIB オブジェクトの内容を読み出しおよび書き込みが可能です。初期値は「private」です。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。4 つまでのコミュニティ名を指定できます。

使用例

SNMP コミュニティ名「System」を作成します。

```
DGS-3200-10:4#create snmp community System view readwrite read_write
Command: create snmp community System view readwrite read_write

Success.

DGS-3200-10:4#
```

delete snmp community

目的

スイッチから特定の SNMP コミュニティ名を削除します。

構文

delete snmp community <community_string 32>

説明

スイッチから定義済みの SNMP コミュニティ名を削除します。

パラメータ

パラメータ	説明
<community_string 32>	削除する SNMP コミュニティのメンバを指定します（32 文字までの半角英数字）。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

SNMP コミュニティ名「System」を削除します。

```
DGS-3200-10:4#delete snmp community System
Command: delete snmp community System

Success.

DGS-3200-10:4#
```

show snmp community

目的

スイッチの設定されている SNMP コミュニティ設定を表示します。

構文

show snmp community {<community_string 32>}

説明

SNMP コミュニティ名、ビュー名およびアクセス権などの情報を表示します。

パラメータ

パラメータ	説明
<community_string 32>	スイッチの SNMP エージェントへのアクセスを希望するユーザの認証に使用される文字列 (半角英数字 32 文字以内)。

制限事項

なし。

使用例

現在入力されている SNMP コミュニティ設定を表示します。

```
DGS-3200-10:4#show snmp community
Command: show snmp community

SNMP Community Table
Community Name  View Name       Access Right
--------------  --------------- -----------
private         CommunityView   read_write
public          CommunityView   read_only

Total Entries :2

DGS-3200-10:4#
```

第 9 章　SNMPv3 コマンド

本スイッチシリーズは、SNMP（Simple Network Management Protocol ）バージョン1、2cおよび3をサポートしています。SNMPの3つのバージョンは、管理ステーションとネットワークデバイス間に提供するセキュリティレベルが異なります。SNMP バージョンのセキュリティ機能は以下の通りです。

SNMP バージョン	認証方式	説明
v1	コミュニティ名	NoAuthNoPriv - コミュニティ名が認証に使用されます。
v2c	コミュニティ名	NoAuthNoPriv - コミュニティ名が認証に使用されます。
v3	ユーザ名	NoAuthNoPriv - ユーザ名が認証に使用されます。
v3	MD5 または SHA	AuthNoPriv - 認証は HMAC-MD5 または HMAC-SHA アルゴリズムに基づきます。
v3	MD5 DES または SHA DES	AuthPrivDES - 認証は HMAC-MD5 または HMAC-SHA アルゴリズムに基づきます。 56 ビット暗号方式が CBC-DES（DES-56）標準規格に基づいて追加されます。

コマンドラインインタフェース（CLI）における SNMPv3 のコマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
create snmp group	<groupname 32> [v1 | v2c | v3 [noauth_nopriv | auth_nopriv | auth_priv]] {read_view <view_name 32> | write_view <view_name 32> | notify_view <view_name 32>}
delete snmp group	<groupname 32>
create snmp user	<user_name 32> <groupname 32> {encrypted [by_password auth [md5 <auth_password 8-16> | sha <auth_password 8-20>] priv [none | des <priv_password 8-16>] | by_key auth [md5 <auth_key 32-32>| sha <auth_key 40-40>] priv [none | des <priv_key 32-32>]]}
delete snmp user	<user_name 32>
show snmp user	
show snmp groups	
create snmp view	<view_name 32> <oid> view_type [included | excluded]
delete snmp view	<view_name 32> [all | <oid>]
show snmp view	<view_name 32>
create snmp community	<community_string 32> view <view_name 32> [read_only | read_write]
delete snmp community	<community_string 32>
show snmp community	<community_string 32>
config snmp engineID	<snmp_engineID 10-64>
show snmp engineID	
create snmp host	[host <ipaddr> | v6host <ipv6addr>] [v1 | v2c | v3 [noauth_nopriv | auth_nopriv | auth_priv] <auth_string 32>]
delete snmp host	[host <ipaddr> | v6host <ipv6addr>]
show snmp v6host	{<ipv6addr>}
show snmp host	{<ipaddr>}
show snmp traps	

以下のセクションで各コマンドについて詳しく記述します。

注意　本コマンドを使用すると、53 ページの「第 8 章 SNMPv1/v2 コマンド」は必要ありません。

create snmp group

目的

新しい SNMP グループ、または SNMP ユーザを SNMP ビューにマップするテーブルを作成します。

構文

create snmp group <groupname 32> [v1 | v2c | v3 [noauth_nopriv | auth_nopriv | auth_priv]] {read_view <view_name 32> | write_view <view_name 32> | notify_view <view_name 32>}

説明

新しい SNMP グループ、または SNMP ユーザを SNMP ビューにマップするテーブルを作成します。

パラメータ

パラメータ	説明
<groupname 32>	新しい SNMP ユーザが関連する SNMP グループを指定します（32 文字までの半角英数字）。
v1	SNMP バージョン 1 が使用されます。Simple Network Management Protocol（SNMP）バージョン 1 は、モニタする手段と制御ネットワークデバイスを提供するネットワーク管理プロトコルです。
v2c	SNMP バージョン 2c が使用されます。SNMP v2c は、ネットワークマネジメント管理を中央に集結して、提供します。SNMP バージョン 1 と比較して SMI（Structure of Management Information）およびセキュリティ機能が強化されています。
v3	SNMP バージョン 3 が使用されます。SNMP v3 は、ネットワーク上で認証とパケットの暗号化を併用することにより、デバイスへの安全なアクセスを提供します。SNMP v3 では以下のパラメータを追加します。 • noauth_nopriv - スイッチとリモート SNMP マネージャ間に送信されるパケットには許可も暗号化もありません。 • auth_nopriv - スイッチとリモート SNMP マネージャ間には認証は必要ですが、送信パケットには暗号化はありません。 • auth_priv - スイッチとリモート SNMP マネージャ間には認証と送信パケットの暗号化が必要です。 • read_view - 作成された SNMP グループが、SNMP メッセージを要求するように指定します。 • write_view - 作成された SNMP グループが、書き込み権を持つように指定します。 • notify_view - 作成された SNMP グループが、スイッチの SNMP エージェントによって生成された SNMP トラップメッセージを受信するように指定します。 • <view_name 32> - リモート SNMP マネージャがスイッチにアクセスできる MIB オブジェクトのグループを指定します（32 文字までの半角英数字）。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

SNMP グループ名「D-Link_group」を作成します。

```
DGS-3200-10:4#create snmp group D-Link_group v3 noauth_nopriv notify_view dlink
Command: create snmp group D-Link_group v3 noauth_nopriv notify_view dlink

Success.

DGS-3200-10:4#
```

delete snmp group

目的

スイッチから SNMP グループを削除します。

構文

delete snmp group <groupname 32>

説明

スイッチから SNMP グループを削除します。

パラメータ

パラメータ	説明
<groupname 32>	削除する SNMP グループ名（32 文字以内の半角英数字）を指定します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

「D-Link_group」という名前の SNMP グループを削除します。

```
DGS-3200-10:4#delete snmp group D-Link_group
Command: delete snmp group D-Link_group

Success.

DGS-3200-10:4#
```

create snmp user

目的

作成した SNMP グループに新しい SNMP ユーザを追加します。

構文

create snmp user <user_name 32> <groupname 32> {encrypted [by_password auth [md5 <auth_password 8-16> | sha <auth_password 8-20>] priv [none | des <priv_password 8-16>] | by_key auth [md5 <auth_key 32-32>| sha <auth_key 40-40>] priv [none | des <priv_key 32-32>]]}

説明

新しい SNMP ユーザを作成し、作成した SNMP グループにユーザを追加します。パスワードまたはキーによる認証を選択します。SNMP は以下の項目を保証します。

- メッセージの保全 - パケットが送信中に変更されていないことを保証します。
- 認証 - SNMP メッセージが有効な送信元から来ているかどうかを判断します。
- 暗号化 - 未認証の送信元によって参照されることを防ぐために、メッセージの内容にスクランブルをかけます。

パラメータ

パラメータ	説明
<user_name 32>	新しい SNMP ユーザを識別する名前。（半角英数字 32 文字以内。）
<groupname 32>	新しい SNMP ユーザが対応付けされる SNMP グループを識別する名前。（半角英数字 32 文字以内。）
encrypted	SNMP を使用した認証のタイプを選択します。 • by_password - 認証とプライバシーのために SNMP ユーザにパスワードを入力するように要求します。パスワードは、以下で「auth_password」を指定することによって定義されます。この方式を推奨します。 • by_key - 認証とプライバシーのために SNMP ユーザに暗号化キーを入力するように要求します。キーは、以下で 16 進形式により指定することによって定義されます。この方式は推奨されません。
auth	SNMP ユーザを認証するために使用される認証アルゴリズムのタイプを選択します。 • md5 - HMAC-MD5-96 認証レベルを使用します。md5 は、以下の 1 つを入力することによって、利用されます。 - <auth password 8-16> - ホストに対するパケットを受信するためにエージェントを認可するために使用されるパスワードです。半角英数字 8-16 文字。 - <auth_key 32-32> - ホストに対するパケットを受信するためにエージェントを認可するために使用されるキーです。16 進数形式 32 文字。 • sha - HMAC-SHA-96 認証レベルを使用します。 - <auth password 8-20> - ホストに対するパケットを受信するためにエージェントを認可するために使用されるパスワードです。半角英数字 8-20 文字。 - <auth_key 40-40> - ホストに対するパケットを受信するためにエージェントを認可するために使用されるキーです。16 進数形式 40 文字。 • priv - priv（プライバシー）パラメータを追加すると、より高いセキュリティために認証アルゴリズムに加えて、暗号化も可能になります。 - des - 本パラメータを追加すると、56 ビットの暗号化のための DES-56 標準の使用が可能となります。 ・ <priv_password 8-16> - ホストがエージェントに送信するメッセージの内容を暗号化するために使用されます。半角英数字 8-16 文字の文字列。 ・ <priv_key 32-32> - ホストがエージェントに送信するメッセージの内容を暗号化するために使用されます。16 進数形式 32 文字。 - none - 本パラメータを追加すると、暗号化を行いません。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

作成した SNMP グループに新しい SNMP ユーザを追加します。

```
DGS-3200-10:4#create snmp user dlink D-Link_group encrypted by_password auth md5
12345678 priv des 12345678
Command: create snmp user dlink D-Link_group encrypted by_password auth md5 12345678
priv des 12345678

Success.

DGS-3200-10:4#
```

delete snmp user

目的

SNMP グループから SNMP ユーザを削除し、また、関連する SNMP グループも削除します。

構文

delete snmp user <user_name 32>

説明

SNMP グループから SNMP ユーザを削除し、また、関連する SNMP グループも削除します。

パラメータ

パラメータ	説明
<user_name 32>	削除する SNMP ユーザを特定する文字列（半角英数字 32 文字以内）。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

スイッチに設定済みの SNMP ユーザを削除します。

```
DGS-3200-10:4#delete snmp user dlink
Command: delete snmp user dlink

Success.

DGS-3200-10:4#
```

show snmp user

目的

SNMP グループのユーザ名テーブル内の各 SNMP ユーザ名に関する情報を表示します。

構文

show snmp user

説明

SNMP グループのユーザ名テーブル内の各 SNMP ユーザ名に関する情報を表示します。

パラメータ

なし。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

スイッチに現在設定されている SNMP ユーザ情報を表示します。

```
DGS-3200-10:4#show snmp user
Command: show snmp user

Username  Group Name  Ver Auth Prive
--------  ----------  -------------
initial   initial     V3  None None

Total Entries:1

DGS-3200-10:4#
```

show snmp groups

目的

スイッチに現在設定されている SNMP グループのグループ名を表示します。また、各グループのセキュリティモデル / レベルおよびステータスを表示します。

構文

show snmp groups

説明

現在のスイッチに設定した SNMP グループ名を表示します。また、各グループのセキュリティモデル / レベルおよびステータスを表示します。

パラメータ

なし。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

スイッチの現在設定されている SNMP グループを表示します。

```
DGS-3200-10:4#show snmp groups
Command: show snmp groups

Vacm Access Table Settings

Group Name       :public
ReadView Name    :CommunityView
WriteView Name   :
Notify View Name :CommunityView
Securiy Model    :SNMPv1
Securiy Level    :NoAuthNoPriv

Group Name       :public
ReadView Name    :CommunityView
WriteView Name   :
Notify View Name :CommunityView
Securiy Model    :SNMPv2
Securiy Level    :NoAuthNoPriv

Group Name       :initial
ReadView Name    :restricted
WriteView Name   :
Notify View Name :restricted
Securiy Model    :SNMPv3
Securiy Level    :NoAuthNoPriv

Group Name       :private
ReadView Name    :CommunityView
WriteView Name   :CommunityView
Notify View Name :CommunityView
Securiy Model    :SNMPv1
Securiy Level    :NoAuthNoPriv

Group Name       :private
ReadView Name    :CommunityView
WriteView Name   :WriteView Name :
Notify View Name :CommunityView
Securiy Model    :SNMPv2
Securiy Level    :NoAuthNoPriv

Group Name       :ReadGroup
ReadView Name    :CommunityView
WriteView Name   :
Notify View Name :CommunityView
Securiy Model    :SNMPv1
Securiy Level    :NoAuthNoPriv

Group Name       :ReadGroup
ReadView Name    :CommunityView
WriteView Name   :
Notify View Name :CommunityView
Securiy Model    :SNMPv1
Securiy Level    :NoAuthNoPriv
```

```
Group Name        :ReadGroup
ReadView Name     :CommunityView
WriteView Name    :
Notify View Name  :CommunityView
Securiy Model     :SNMPv2
Securiy Level     :NoAuthNoPriv

ReadView Name     :CommunityView
WriteView Name    :CommunityView
Notify View Name  :CommunityView
Securiy Model     :SNMPv1
Securiy Level     :NoAuthNoPriv

Group Name        :WriteGroup
ReadView Name     :CommunityView
WriteView Name    :CommunityView
Notify View Name  :CommunityView
Securiy Model     :SNMPv1
Securiy Level     :NoAuthNoPriv

Group Name        :WriteGroup
ReadView Name     :CommunityView
WriteView Name    :CommunityView
Notify View Name  :CommunityView
Securiy Model     :SNMPv2
Securiy Level     :NoAuthNoPriv

Group Name        :D-Link_group
ReadView Name     :CommunityView
WriteView Name    :CommunityView
Notify View Name  :CommunityView
Securiy Model     :SNMPv3
Securiy Level     :authPriv

Total Entries:10

DGS-3200-10:4#
```

create snmp view

目的

MIB オブジェクトと SNMP マネージャのアクセスを制限するために、コミュニティ名にビューを割り当てます。

構文

create snmp view <view_name 32> <oid> view_type [included | excluded]

説明

SNMP マネージャがアクセス可能な MIB オブジェクトを制限するために、コミュニティ名にビューを割り当てます。

パラメータ

パラメータ	説明
<view_name 32>	32 文字までの半角英数字を入力します。新しい SNMP ビューを登録し、識別する際に使用します。
<oid>	SNMP マネージャがアクセス可能な範囲であるかを指定するオブジェクトツリー（MIB ツリー）を識別するオブジェクト ID。
view_type	以下のビュータイプを選択します。 • included - SNMP マネージャがアクセスできるオブジェクトのリストにこのオブジェクトを含めます。 • excluded - SNMP マネージャがアクセスできるオブジェクトのリストからこのオブジェクトを除外します。

使用例

SNMP ビューを作成します。

```
DGS-3200-10:4#create snmp view dlinkview 1.3.6 view_type included
Command: create snmp view dlinkview 1.3.6 view_type included

Success.

DGS-3200-10:4#
```

delete snmp view

目的

スイッチに作成済みの SNMP ビューエントリを削除します。

構文

delete snmp view <view_name 32> [all | <oid>]

説明

スイッチに作成 SNMP ビューエントリを削除します。

パラメータ

パラメータ	説明
<view_name 32>	削除する SNMP ビュー名（32 文字以内の半角英数字）。
all	スイッチの SNMP ビューすべてを削除します。
<oid>	スイッチから削除されるオブジェクトツリー（MIB ツリー）を示すオブジェクト ID。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

スイッチから設定した SNMP ビューを削除します。

```
DGS-3200-10:4#delete snmp view dlinkview all
Command: delete snmp view dlinkview all

Success.

DGS-3200-10:4#
```

show snmp view

目的

スイッチに作成済みの SNMP ビューを表示します。

構文

show snmp view {<view_name 32>}

説明

スイッチに作成済みの SNMP ビューを表示します。

パラメータ

パラメータ	説明
<view_name 32>	削除する SNMP ビュー名が表示されます（32 文字以内の半角英数字）。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

SNMP ビュー設定を表示します。

```
DGS-3200-10:4#show snmp view
Command: show snmp view

Vacm View Table Settings
View Name       Subtree             View Type
-------------   ------------------- ---------
restricted      1.3.6.1.2.1.1       Included
restricted      1.3.6.1.2.1.11      Included
restricted      1.3.6.1.6.3.10.2.1  Included
restricted      1.3.6.1.6.3.11.2.1  Included
restricted      1.3.6.1.6.3.15.1.1  Included
CommunityView   1                   Included
CommunityView   1.3.6.1.6.3         Excluded
CommunityView   1.3.6.1.6.3.1       Included

Total Entries:8

DGS-3200-10:4#
```

create snmp community

目的

SNMP マネージャとエージェントとの関係を定義するために SNMP コミュニティを作成します。コミュニティ名は、スイッチ上のエージェントへのアクセスを行う際のパスワードの役割をします。以下の特性はコミュニティ名と関係します。1 つ以上指定することができます。

- アクセスリストはコミュニティ名を使用して、スイッチ上の SNMP エージェントにアクセスを行う SNMP マネージャの IP アドレスが掲載されています。
- MIB ビューは SNMP コミュニティにアクセス可能なすべての MIB オブジェクトのサブセットを定義します。
- SNMP コミュニティにアクセス可能な MIB オブジェクトには「read_write」（読み書き可能）または「read_only」（読み出しのみ可能）のレベルがあります。

構文

create snmp community <community_string 32> view <view_name 32> [read_only | read_write]

説明

SNMP コミュニティ名を作成し、このコミュニティ名にアクセス制限を行う文字列を割り当てます。

パラメータ

パラメータ	説明
<community_string 32>	スイッチの SNMP コミュニティのメンバを識別します（32 文字までの半角英数字）。本コミュニティ名は、リモートの SNMP マネージャが、スイッチの SNMP エージェント内の MIB オブジェクトにアクセスする際にパスワードのように使用します。
<view_name 32>	SNMP マネージャがアクセス可能な範囲であるかを指定するオブジェクトツリー（MIB ツリー）を識別するオブジェクト ID。
view type [read_only | read_write]	リモート SNMP マネージャがスイッチにアクセスできる MIB オブジェクトのグループを指定します（32 文字までの半角英数字）。 • read_only - 本コマンドを使用して作成したコミュニティ名を使用する SNMP コミュニティメンバは、スイッチの MIB オブジェクトの内容を読み出しが可能です。 • read_write - 本コマンドを使用して作成したコミュニティ名を使用する SNMP コミュニティメンバは、スイッチの MIB オブジェクトの内容を読み出しおよび書き込みが可能です。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

SNMP コミュニティ名「dlink」を作成します。

```
DGS-3200-10:4#create snmp community dlink view CommunityView read_write
Command: create snmp community dlink view CommunityView read_write

Success.

DGS-3200-10:4#
```

delete snmp community

目的

スイッチから特定の SNMP コミュニティ名を削除します。

構文

delete snmp community <community_string 32>

説明

スイッチから定義済みの SNMP コミュニティ名を削除します。

パラメータ

パラメータ	説明
<community_string 32>	スイッチの SNMP コミュニティのメンバを識別します（32 文字までの半角英数字）。本コミュニティ名は、リモートの SNMP マネージャが、スイッチの SNMP エージェント内の MIB オブジェクトにアクセスする際にパスワードのように使用します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

SNMP コミュニティ名「dlink」を削除します。

```
DGS-3200-10:4#delete snmp community dlink
Command: delete snmp community dlink

Success.

DGS-3200-10:4#
```

show snmp community

目的

スイッチの設定されている SNMP コミュニティ設定を表示します。

構文

show snmp community <community_string 32>

説明

スイッチに設定されている SNMP コミュニティ設定を表示します。

パラメータ

パラメータ	説明
<community_string 32>	スイッチの SNMP コミュニティのメンバを識別します（32 文字までの半角英数字）。コミュニティ名を指定しないと、すべてのコミュニティ名情報を表示します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

現在入力されている SNMP コミュニティ名を表示します。

```
DGS-3200-10:4#show snmp community
Command: show snmp community

SNMP Community Table
Community Name  View Name       Access Right
--------------  -------------   ------------
private         CommunityView   read_write
public          CommunityView   read_only

Total Entries:2

DGS-3200-10:4#
```

config snmp engineID

目的

スイッチの SNMP エンジンに名前を設定します。

構文

config snmp engineID <snmp_engineID 10-64>

説明

スイッチの SNMP エンジンに名前を設定します。各 SNMP エンティティに固有のエンジン ID で関連付けます。

パラメータ

パラメータ	説明
<snmp_engineID 10-64>	スイッチの SNMP エンジンを指定します。（10-64 文字の 16 進数 0-9、A-F）

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

「1023457890」という名前をスイッチの SNMP エージェントに付与します。

```
DGS-3200-10:4#config snmp engineID 1023457890
Command: config snmp engineID 1023457890

Success.

DGS-3200-10:4#
```

show snmp engineID

目的

スイッチの SNMP エンジンの識別子を表示します。

構文

show snmp engineID

説明

スイッチの SNMP エンジンの識別子を表示します。

パラメータ

なし。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

SNMP エンジンの現在の名前を表示します。

```
DGS-3200-10:4#show snmp engineID
Command: show snmp engineID

SNMP Engine ID :1023457890

DGS-3200-10:4#
```

create snmp host

目的

スイッチの SNMP エージェントによって生成される SNMP トラップの受信者を作成します。

構文

create snmp [host <ipaddr> | v6host <ipv6addr>] [v1 | v2c | v3 [noauth_nopriv | auth_nopriv | auth_priv] <auth_string 32>]

説明

スイッチの SNMP エージェントによって生成される SNMP トラップの受信者を作成します。

パラメータ

パラメータ	説明
host <ipaddr>	トラップの対象となる受信者の IP アドレスを指定します。
v6host <ipv6addr>	トラップの対象となる受信者の IPv6 アドレスを指定します。
v1	SNMP バージョン 1 を使用します。Simple Network Management Protocol（SNMP）バージョン 1 は、モニタする手段と制御ネットワークデバイスを提供するネットワーク管理プロトコルです。
v2c	SNMP バージョン 2c を使用します。SNMP v2c は、ネットワークマネジメント管理を中央に集結して、提供します。SNMP バージョン 1 と比較して SMI（Structure of Management Information）およびセキュリティ機能が強化されています。
v3	SNMP バージョン 3 が使用されます。SNMP v3 は、ネットワーク上で認証とパケットの暗号化を併用することにより、デバイスへの安全なアクセスを提供します。SNMP v3 では以下のパラメータを追加します。最もセキュアなモデルです。 • メッセージの保全 - パケットが送信中に変更されていないことを保証します。 • 認証 - SNMP メッセージが有効な送信元から来ているかどうかを判断します。 • 暗号化 - 未認証の送信元によって参照されることを防ぐために、メッセージの内容にスクランブルをかけます。
noauth_nopriv	スイッチとリモート SNMP マネージャ間に送信されるパケットには許可も暗号化もありません。
auth_nopriv	スイッチとリモート SNMP マネージャ間には認証は必要ですが、送信パケットには暗号化はありません。
auth_priv	スイッチとリモート SNMP マネージャ間には認証と送信パケットの暗号化が必要です。
<auth_string 32>	スイッチの SNMP エージェントがスイッチにアクセスするためにリモートの SNMP マネージャを認可するために使用する文字列。（32 文字までの半角英数字。）

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

SNMP メッセージを受信するために SNMP IPv4 ホストを作成します。

```
DGS-3200-10:4#create snmp host 10.48.74.100 v3 noauth_nopriv initial
Command: create snmp host 10.48.74.100 v3 noauth_nopriv initial

Success.

DGS-3200-10:4#
```

delete snmp host

目的

スイッチの SNMP エージェントによって生成された SNMP トラップの受信者を削除します。

構文

delete snmp [host <ipaddr> | v6host <ipv6addr>]

説明

スイッチの SNMP エージェントによって生成された SNMP トラップの受信者を削除します。

パラメータ

パラメータ	説明
host <ipaddr>	スイッチの SNMP ホストとして動作するリモート管理ステーションの IPv4 アドレス。
v6host <ipv6addr>	スイッチの SNMP ホストとして動作するリモート管理ステーションの IPv6 アドレス。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

SNMP ホストエントリを削除します。

```
DGS-3200-10:4#delete snmp host 10.48.74.100
Command: delete snmp host 10.48.74.100

Success.

DGS-3200-10:4#
```

show snmp host

目的

スイッチの SNMP エージェントによって生成される SNMP トラップの受信者を表示します。

構文

show snmp host {<ipaddr>}

説明

スイッチの SNMP エージェントによって生成される SNMP トラップの受信者として選出されたリモート SNMP マネージャの IP アドレスおよび設定情報を表示します。

パラメータ

パラメータ	説明
<ipaddr>	スイッチの SNMP エージェントによって生成された SNMP トラップを受け取るリモート SNMP マネージャの IP アドレス。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

スイッチに現在設定されている SNMP ホストを表示します。

```
DGS-3200-10:4#show snmp host
Command: show snmp host

SNMP Host Table
Host IP Address  SNMP Version     Community Name/SNMPv3 User Name
---------------  ---------------  ------------------------------
10.48.74.100     V3 noauthnopriv  initial
10.51.17.1       V2c              public

Total Entries:2

DGS-3200-10:4#
```

show snmp v6host

目的

スイッチの SNMP エージェントによって生成される SNMP トラップの受信者を表示します。

構文

show snmp v6host {<ipv6addr>}

説明

スイッチの SNMP エージェントによって生成される SNMP トラップの受信者として選出されたリモート SNMP マネージャの IP アドレスおよび設定情報を表示します。

パラメータ

パラメータ	説明
<ipv6addr>	スイッチの SNMP エージェントによって生成された SNMP トラップを受け取るリモート SNMP マネージャの IP アドレス。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

スイッチに現在設定されている SNMP ホストを表示します。

```
DGS-3200-10:4#show snmp v6host
Command: show snmp v6host

SNMP Host Table
--------------------------------------------------------------------------
Host IPv6 Address               : FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
SNMP Version                    : V3 na/np
Community Name/SNMPv3 User Name : 123456789101234567890
Host IPv6 Address               : FECO:1A49:2AA:FF:FE34:CA8F
SNMP Version                    : V3 a/np
Community Name/SNMPv3 User Name : abcdefghijk

Total Entries : 2

DGS-3200-10:4#
```

show snmp traps

目的

スイッチの SNMP トラップと認証トラップの状態を表示します。

構文

show snmp traps

説明

スイッチの SNMP トラップサポートを表示します。

パラメータ

なし。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

現在の SNMP トラップサポートを参照します。

```
DGS-3200-10:4#show snmp traps
Command: show snmp traps

SNMP Traps        : Enabled
Authenticate Trap : Enabled
Linkchange Traps  : Enabled
Coldstart Traps   : Enabled
Warmstart Traps   : Enabled

DGS-3200-10:4#
```

第 10 章　ネットワーク管理コマンド

コマンドラインインタフェース（CLI）におけるネットワーク管理コマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
enable snmp	
disable snmp	
create trusted_host	[<ipaddr> | network <network_address>]
delete trusted_host	[ipaddr <ipaddr> | network <network_address> | all]
show trusted_host	<ipaddr>
config snmp system_name	<sw_name>
config snmp system_location	<sw_location>
config snmp system_contact	<sw_contact>
enable rmon	
disable rmon	
enable snmp traps	
disable snmp traps	
enable snmp authenticate_traps	
disable snmp authenticate_traps	
enable snmp linkchange_traps	[<ipaddr> | network <network_address>]
disable snmp linkchange_traps	[<ipaddr> | network <network_address>]
config snmp coldstart_traps	[enable | disable]
config snmp warmstart_traps	[enable | disable]
config snmp linkchange_traps	ports [all | <portlist>] [enable | disable]
show snmp traps	{linkchange_traps {ports <portlist>}}

以下のセクションで各コマンドについて詳しく記述します。

enable snmp

目的

SNMP を有効にします。

構文

enable snmp

説明

SNMP 機能を有効にします。SNMP 機能を無効にすると、ネットワークマネージャは SNMP MIB オブジェクトにアクセスできなくなります。また、デバイスもトラップや通知をネットワークマネージャに送信しなくなります。

パラメータ

なし。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

スイッチの SNMP を有効にします。

```
DGS-3200-10:4#enable snmp
Command: enable snmp

Success.

DGS-3200-10:4#
```

disable snmp

目的

SNMP インタフェースアクセス機能を無効にします。

構文

disable snmp traps

説明

スイッチの SNMP 無効にします。SNMP 機能を無効にすると、ネットワークマネージャは SNMP MIB オブジェクトにアクセスできなくなります。また、デバイスもトラップや通知をネットワークマネージャに送信しなくなります。

パラメータ

なし。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

スイッチの SNMP を無効にします。

```
DGS-3200-10:4#disable snmp
Command: disable snmp

Success.

DGS-3200-10:4#
```

create trusted_host

目的

トラストホストを作成します。

構文

create trusted_host [<ipaddr> | network <network_address>]

説明

トラストホストを作成します。8 個までの IP アドレスが SNMP または Telnet ベースの管理ソフトウェア経由でスイッチを管理することができます。これらの IP アドレスは、マネジメント VLAN に所属する必要があります。IP アドレスを指定しないと、ユーザがユーザ名およびパスワードを知っていても、どの IP アドレスからのスイッチアクセスもできません。

パラメータ

パラメータ	説明
<ipaddr>	指定 IP アドレスのトラストホストを作成します。
network <network_address>	トラストネットワークのアドレス。ネットワークアドレスの形式は xxx.xxx.xxx.xxx/y です。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

トラストホストを作成します。

```
DGS-3200-10:4#create trusted_host 10.48.74.121
Command: create trusted_host 10.48.74.121

Success.

DGS-3200-10:4#
```

delete trusted_host

目的

上記「create trusted_host」コマンドで作成したトラストホストエントリを削除します。

構文

delete trusted _host [ipaddr <ipaddr> | network <network_address> | all]

説明

トラストホストエントリを削除します。

パラメータ

パラメータ	説明
ipaddr <ipaddr>	削除するトラストホストの IP アドレス。
network <network_address>	トラストネットワークのアドレス。ネットワークアドレスの形式は xxx.xxx.xxx.xxx/y です。
all	すべてのトラストホストが対象になります。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

IP アドレス「10.48.74.121」を持つトラストホストを削除します。

```
DGS-3200-10:4#delete trusted_host ipaddr 10.48.74.121
Command: delete trusted_host ipaddr 10.48.74.121

Success.
DGS-3200-10:4#
```

show trusted_host

目的

上記「create trusted_host」コマンドでスイッチに作成したトラストホストのリストを表示します。

構文

show trusted_host <ipaddr>

説明

ラストホストのリストを表示します。

パラメータ

パラメータ	説明
<ipaddr>	参照するトラストホストの IP アドレス。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

トラストホストのリストを表示します。

```
DGS-3200-10:4#show trusted_host
Command: show trusted_host

Management Stations

IP Address
-----------
10.48.93.100
10.51.17.1
10.50.95.90

Total Entries:3

DGS-3200-10:4#
```

config snmp system_name

目的

スイッチに名前を設定します。

構文

config snmp system_name <sw_name>

説明

スイッチに名前を設定します。

パラメータ

パラメータ	説明
<sw_name>	255 文字まで使用できます。名前を指定しない場合、入力する必要はありません。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

スイッチ名に「DGS-3200-10 Gigabit Ethernet Switch」を設定します。

```
DGS-3200-10:4#config snmp system_name DGS-3200-10 Gigabit Ethernet Switch
Command: config snmp system_name DGS-3200-10 Gigabit Ethernet Switch

Success.

DGS-3200-10:4#
```

config snmp system_location

目的

スイッチの設置場所の説明を入力します。

構文

config snmp system_location <sw_location>

説明

スイッチの設置場所の説明を入力するために使用されます。

パラメータ

パラメータ	説明
<sw_location>	半角英数字 255 文字までを使用できます。設置場所名を指定しない場合は、入力する必要はありません。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

スイッチ設置場所に「HQ5F」を設定します。

```
DGS-3200-10:4#config snmp system_location HQ 5F
Command: config snmp system_location HQ 5F

Success.

DGS-3200-10:4#
```

config snmp system_contact

目的
　スイッチの問い合わせ先を入力します。
構文
　config snmp system_contact <sw_contact>
説明
　スイッチの問い合わせ先を識別する名前および（または）情報（半角英数字 255 文字以内）を入力します。
パラメータ

パラメータ	説明
<sw_contact>	255 文字までを使用できます。コンタクト先がない場合は、入力する必要はありません。

制限事項
　管理者レベルユーザのみ本コマンドを実行できます。
使用例
　スイッチのコンタクトパーソンに "MIS Department II" を設定します。

```
DGS-3200-10:4#config snmp system_contact "MIS Department II"
Command: config snmp system_contact "MIS Department II"

Success.

DGS-3200-10:4#
```

enable rmon

目的
　スイッチの RMON 機能を有効にします。
構文
　enable rmon
説明
　スイッチでリモートモニタリング機能（RMON）を有効にします。
パラメータ
　なし。
制限事項
　管理者レベルユーザのみ本コマンドを実行できます。
使用例
　RMON を有効にします。

```
DGS-3200-10:4#enable rmon
Command: enable rmon

Success.

DGS-3200-10:4#
```

disable rmon

目的
　スイッチの RMON 機能を無効にします。
構文
　disable rmon
説明
　スイッチのリモートモニタリング機能（RMON）を無効にします。
パラメータ
　なし。
制限事項
　管理者レベルユーザのみ本コマンドを実行できます。
使用例
　RMON を無効にします。

```
DGS-3200-10:4#disable rmon
Command: disable rmon

Success.

DGS-3200-10:4#
```

enable snmp traps

目的
　SNMP トラップサポートを有効にします。
構文
　enable snmp traps
説明
　スイッチの SNMP トラップサポートを有効にします。
パラメータ
　なし。
制限事項
　管理者レベルユーザのみ本コマンドを実行できます。
使用例
　スイッチの SNMP トラップサポートを有効にします。

```
DGS-3200-10:4#enable snmp traps
Command: enable snmp traps

Success.

DGS-3200-10:4#
```

disable snmp traps

目的
　スイッチの SNMP トラップサポートを無効にします。
構文
　disable snmp traps
説明
　スイッチの SNMP トラップサポートを無効にします。
パラメータ
　なし。
制限事項
　管理者レベルユーザのみ本コマンドを実行できます。
使用例
　スイッチの SNMP トラップサポートを有効にします。

```
DGS-3200-10:4#disable snmp traps
Command: disable snmp traps

Success.

DGS-3200-10:4#
```

enable snmp authenticate_traps

説明

スイッチの SNMP 認証トラップサポートを有効にします。

構文

enable snmp authenticate_traps

パラメータ

なし。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

SNMP 認証トラップサポートを有効にします。

```
DGS-3200-10:4#enable snmp authenticate_traps
Command: enable snmp authenticate_traps

Success.

DGS-3200-10:4#
```

disable snmp authenticate_traps

目的

SNMP 認証トラップサポートを無効にします。

構文

disable snmp authenticate_traps

説明

スイッチの SNMP 認証トラップサポートを無効にします。

パラメータ

なし。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

SNMP 認証トラップサポートを無効にします。

```
DGS-3200-10:4#disable snmp authenticate_traps
Command: disable snmp authenticate_traps

Success.

DGS-3200-10:4#
```

enable snmp linkchange_traps

目的
　リンクチェンジトラップの送信を設定します。
構文
　enable snmp linkchange_traps
説明
　SNMP リンクチェンジトラップを有効にします。
パラメータ
　なし。
制限事項
　管理者レベルユーザのみ本コマンドを実行できます。
使用例
　SNMP リンクチェンジトラップを有効にします。

```
DGS-3200-10:4#enable snmp linkchange_traps
Command: enable snmp linkchange_traps

Success.

DGS-3200-10:4#
```

disable snmp linkchange_traps

目的
　SNMP リンクチェンジトラップを無効にします。
構文
　disable snmp linkchange_traps
説明
　SNMP リンクチェンジトラップを無効にします。
パラメータ
　なし。
制限事項
　管理者レベルユーザのみ本コマンドを実行できます。
使用例
　SNMP リンクチェンジトラップを無効にします。

```
DGS-3200-10:4#disable snmp linkchange_traps
Command: disable snmp linkchange_traps

Success.

DGS-3200-10:4#
```

config snmp coldstart_traps

目的

コールドスタートイベントのトラップを設定します。

構文

config snmp coldstart_traps [enable | disable]

説明

コールドスタートイベントのトラップを設定します。

パラメータ

パラメータ	説明
enable	コールドスタートイベントのトラップを有効にします。（初期値）
disable	コールドスタートイベントのトラップを無効にします。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

コールドスタートイベントに対してトラップ状態を設定します。

```
DGS-3200-10:4#config snmp coldstart traps enable
Command: config snmp coldstart traps enable

Success.

DGS-3200-10:4#
```

config snmp warmstart_traps

目的

ウォームスタートイベントのトラップを設定します。

構文

config snmp warmstart_traps [enable | disable]

説明

ウォームスタートイベントのトラップを設定します。

パラメータ

パラメータ	説明
enable	ウォームスタートイベントのトラップを有効にします。（初期値）
disable	ウォームスタートイベントのトラップを無効にします。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

ウォームスタートイベントに対してトラップ状態を設定します。

```
DGS-3200-10:4#config snmp warmstart_traps enable
Command: config snmp warmstart_traps enable

Success.

DGS-3200-10:4#
```

config snmp linkchange_traps ports

目的

リンクチェンジトラップの送信とチェンジトラップの送信に対する各ポートの制御を設定します。

構文

config snmp linkchange_traps ports [all | <portlist>] [enable | disable]

説明

リンクチェンジトラップの送信とチェンジトラップの送信に対する各ポートの制御を設定します。

パラメータ

パラメータ	説明
[all | <portlist>]	• all - すべてのポートを指定します。 • <portlist> - ポート範囲を指定します。
[enable | disable]	• enable - このポートに対するリンクチェンジトラップの送信を有効にします。 • disable - このポートに対するリンクチェンジトラップの送信を無効にします。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

リンクチェンジトラップの送信とチェンジトラップの送信に対する各ポートの制御を設定します。

```
DGS-3200-10:4#config snmp linkchange_traps ports 1-4 enable
Command: config snmp linkchange_traps ports 1-4 enable

Success.

DGS-3200-10:4#
```

show snmp traps

目的

SNMP トラップと認証トラップの状態を表示します。

構文

show snmp traps {linkchange_traps {ports <portlist>} }

説明

トラップステータスを表示します。

パラメータ

パラメータ	説明
linkchange_traps	本リストにリンクチェンジトラップを表示します。
ports <portlist>	本リストにポート情報を表示します。 • <portlist> - 表示するポート範囲を指定します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

SNMP トラップと認証トラップの状態を表示します。

```
DGS-3200-10:4#show snmp traps
Command: show snmp traps

SNMP Traps        : Enabled
Authenticate Trap : Enabled
Linkchange Traps  : Enabled
Coldstart Traps   : Enabled
Warmstart Traps   : Enabled

DGS-3200-10:4#
```

リンクチェンジトラップの状態を表示します。

```
DGS-3200-10:4#show snmp traps linkchange_traps
Command: show snmp traps linkchange_traps

Linkchange Traps : Enabled

Port 1 : Enabled
Port 2 : Enabled
Port 3 : Enabled
Port 4 : Enabled
Port 5 : Enabled
Port 6 : Enabled
Port 7 : Enabled
Port 8 : Enabled
Port 9 : Enabled
Port 10: Enabled

DGS-3200-10:4#
```

第 11 章　ネットワークモニタリングコマンド

スイッチのポート使用率、パケットエラー等の情報を取得することができます。

コマンドラインインタフェース（CLI）におけるネットワークモニタリングコマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
show packet ports	<portlist>
show error ports	<portlist>
show utilization	[ports | cpu]
clear counters	{ports <portlist>}
clear log	
show log	{index <value_list>}
enable syslog	
disable syslog	
show syslog	
create syslog host	<index 1-4> ipaddress <ipaddr> {severity [informational | warning | all] | facility [local 0|local 1|local 2|local 3|local 4|local 5|local 6|local 7] | udp_port <udp_port_number> | state [enable | disable]}
config syslog host	[all |<index 1-4>] {severity [informational |warning | all] | facility [local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7] | udp_port <udp_port_number> | ipaddress <ipaddr> | state [enable |disable]}
delete syslog host	[<index 1-4> | all]
show syslog host	{<index 1-4>}
config log_save_timing	[time_interval <min 1-65535> | on_demand | log_trigger]
show log_save_timing	

以下のセクションで各コマンドについて詳しく記述します。

show packet ports

目的

スイッチが送受信したパケットに関する統計情報を表示します。

構文

show packet ports <portlist>

説明

指定されたポートごとに送受信されたパケットに関する統計情報を表示します。

パラメータ

パラメータ	説明
<portlist>	表示するポートまたは範囲を指定します。

制限事項

なし。

使用例

ポート 7 のパケット分析を表示します。

```
DGS-3200-10:4#show packet ports 7
Command: show packet ports 7

Port number : 7
================================================================
Frame Size/Type Frame Counts  Frames/sec
--------------- ------------- ----------
64              572           27
65-127          151            5
128-255          39            0
256-511          65            0
512-1023          7            0
1024-1518         0            0
Unicast RX        4            0
Multicast RX    162            1
Broadcast RX    568           31

Frame Type      Total         Total/sec
----- ------    ------------- ---------
RX    Bytes     81207         2237
RX    Frames      734           32
TX    Bytes      8432            0
TX    Frames      100            0
```

show error ports

目的

ポート範囲のエラー統計情報を表示します。

構文

show error ports <portlist>

説明

スイッチが指定ポートに対してパケットエラー統計情報を表示します。

パラメータ

パラメータ	説明
<portlist>	表示するポートまたは範囲を指定します。

制限事項

なし。

使用例

ポート 3 のエラーを表示します。

```
DGS-3200-10:4#show error ports 3
Command: show error ports 3

Port number :3
              RX Frames                       TX Frames
              ---------                       ---------
CRC Error     0           Excessive Deferral  0
Undersize     0           CRC Error           0
Oversize      0           Late Collision      0
Fragment      0           Excessive Collision 0
Jabber        0           Single Collision    0
Drop Pkts     0           Collision           0
Symbol Error  0
```

show utilization

目的

リアルタイムにポートと CPU の使用率統計情報を表示します。

構文

show utilization [ports | cpu]

説明

スイッチのリアルタイムにスイッチのポートと CPU の使用率統計情報を表示します。

パラメータ

パラメータ	説明
cpu	スイッチの現在の CPU 使用率を表示します。
ports	スイッチの現在のポート使用率を表示します。

制限事項

なし。

使用例

ポート使用率の統計情報を表示します。

```
DGS-3200-10:4#show utilization ports
Command: show utilization ports

Port TX/sec RX/sec Util
---- ------ ------ ----
1    0      0      0
2    0      0      0
3    0      0      0
4    0      0      0
5    0      0      0
6    0      0      0
7    0      0      0
8    0      0      0
```

現在の CPU 使用率を表示します。

```
DGS-3200-10:4#show utilization cpu
Command: show utilization cpu

CPU utilization :
-------------------------------------------------------------
Five seconds-  20%    One minute-  10%   Five minutes-  70%
```

clear counters

目的

スイッチの統計情報カウンタをクリアします。

構文

clear counters {ports <portlist>}

説明

スイッチが使用するカウンタをクリアします。

パラメータ

パラメータ	説明
ports <portlist>	クリアするポートまたは範囲を指定します。パラメータを指定しないと、システムはすべてのポートカウンタをクリアします。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

カウンタをクリアします。

```
DGS-3200-10:4#clear counters ports 7-9
Command: clear counters ports 7-9

Success.

DGS-3200-10:4#
```

clear log

目的

スイッチのヒストリログをクリアします。

構文

clear log

説明

スイッチのヒストリログをクリアします。

パラメータ

なし。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

ログ情報をクリアします。

```
DGS-3200-10:4#clear log
Command: clear log

Success.

DGS-3200-10:4#
```

show log

目的

スイッチのヒストリログを表示します。

構文

show log {index <value_list>}

説明

スイッチのヒストリログの内容を表示します。

パラメータ

パラメータ	説明
index <value_list>	2 つの値間のヒストリログを表示します。例えば「show log index 1-5」は 1 から始まり、5 で終わるヒストリログを表示します。パラメータを指定しないと、すべてのヒストリログエントリを表示します。

制限事項

なし。

使用例

スイッチのヒストリログの内容を表示します。

```
DGS-3200-10:4#show log index 1-5
Command: show log index 1-5

Index Date       Time     Log Text
----- ------------------- --------------------------------------------------
5     2000-01-01 00:00:41 Port 5 link down
4     2000-01-01 00:00:31 Port 3 link up, 100Mbps FULL duplex
3     2000-01-01 00:00:31 Successful login through Console (Username:Anonymous)
2     2000-01-01 00:00:31 Console session timed out (Username: dlink)
1     2000-01-01 00:00:31 Spanning Tree Protocol is disabled

DGS-3200-10:4#
```

enable syslog

目的

システムログがリモート Syslog サーバに送信される機能を有効にします。

構文

enable syslog

説明

システムログがリモート Syslog サーバに送信される機能を有効にします。

パラメータ

なし。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

スイッチの Syslog 機能を有効にします。

```
DGS-3200-10:4#enable syslog
Command: enable syslog

Success.

DGS-3200-10:4#
```

disable syslog

目的
　システムログがリモート Syslog サーバに送信される機能を無効にします。
構文
　disable syslog
説明
　システムログがリモート Syslog サーバに送信される機能を無効にします。
パラメータ
　なし。
制限事項
　管理者レベルユーザのみ本コマンドを実行できます。
使用例
　スイッチの Syslog 機能を無効にします。

```
DGS-3200-10:4#disable syslog
Command: disable syslog

Success.

DGS-3200-10:4#
```

show syslog

目的
　Syslog 機能のグローバルな現在の動作状態を表示します。
構文
　show syslog
説明
　スイッチの Syslog 機能のグローバルな現在の動作状態を表示します。
パラメータ
　なし。
制限事項
　なし。
使用例
　Syslog 機能のグローバルな現在の動作状態を表示します。

```
DGS-3200-10:4#show syslog
Command: show syslog

Syslog Global State: Enabled

DGS-3200-10:4#
```

create syslog host

目的

新しい Syslog ホストを作成します。

構文

create syslog host <index 1-4> ipaddress <ipaddr> {severity [informational | warning | all] | facility [local 0|local 1|local 2|local 3|local 4|local 5|local 6|local 7] | udp_port <udp_port_number> | state [enable | disable]}

説明

新しい Syslog ホストを作成します。

パラメータ

パラメータ	説明	
index <1-4>	コマンドを適用する Syslog ホストのインデックスを指定します。1-4 の 4 つのインデックスが利用可能です。	
ipaddress <ipaddr>	syslog メッセージを送信されるリモートホストの IP アドレスを指定します。	
severity	3 つの Severity レベル（メッセージレベル）をサポートしています。	
	メッセージレベル	説明
	informational warning all	情報メッセージをリモートホストに送信します。 警告メッセージをリモートホストに送信します。 スイッチに生成される現在サポートしている syslog メッセージのすべてをリモートホストに送信します。
facility	いくつかのオペレーティングシステムデーモンおよびプロセスはファシリティ値を割り当てられています。ファシリティを割り当てていないプロセスとデーモンの場合は「local use」（アプリケーション用の汎用）のいずれかを使用するか、「user-level」を使用します。指定できるファシリティは以下の通りです。	
	コード	ファシリティ
	local0 local1 local2 local3 local4 local5 local6 local7	ローカル使用 0（local 0） ローカル使用 1（local 1） ローカル使用 2（local 2） ローカル使用 3（local 3） ローカル使用 4（local 4） ローカル使用 5（local 5） ローカル使用 6（local 6） ローカル使用 7（local 7）
udp_port <udp_port_number>	syslog プロトコルがメッセージをリモートホストに送信するために使用する UDP ポート番号（514 または 6000-65535）を指定します。	
state [enable	disable]	リモートホストへの syslog メッセージの送信を「enable」（有効）または「disable」（無効）にします。	

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

Syslog ホストを作成します。

```
DGS-3200-10:4#create syslog host 1 ipaddress 192.168.1.12 severity all facility local0
Command: create syslog host 1 ipaddress 192.168.1.12 severity all facility local0

Success.

DGS-3200-10:4#
```

config syslog host

目的

Syslog プロトコルを設定し、システムログデータをリモートホストに送信します。

構文

config syslog host [all | <index 1-4>] { severity [informational | warning | all] | facility [local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7] | udp_port <udp_port_number> | ipaddress <ipaddr> | state [enable | disable]}

説明

syslog プロトコルを設定し、システムログ情報をリモートホストに送信します。

パラメータ

パラメータ	説明	
host [all | <index 1-4>]	コマンドを適用する Syslog ホストのインデックスを指定します。1-4 の 4 つのインデックスが利用可能です。「all」を指定すると、すべてのホストを対象とします。	
severity	３つの Severity レベル（メッセージレベル）をサポートしています。	
	メッセージレベル	説明
	informational warning all	情報メッセージをリモートホストに送信します。 警告メッセージをリモートホストに送信します。 スイッチに生成される現在サポートしている syslog メッセージのすべてをリモートホストに送信します。
facility	いくつかのオペレーティングシステムデーモンおよびプロセスはファシリティ値を割り当てられています。ファシリティを割り当てていないプロセスとデーモンの場合は「local use」（アプリケーション用の汎用）のいずれかを使用するか、「user-level」を使用します。指定できるファシリティは以下の通りです。	
	コード	ファシリティ
	local0 local1 local2 local3 local4 local5 local6 local7	ローカル使用 0（local 0） ローカル使用 1（local 1） ローカル使用 2（local 2） ローカル使用 3（local 3） ローカル使用 4（local 4） ローカル使用 5（local 5） ローカル使用 6（local 6） ローカル使用 7（local 7）
udp_port <udp_port_number>	syslog プロトコルがメッセージをリモートホストに送信するために使用する UDP ポート番号を指定します。	
ipaddress <ipaddr>	syslog メッセージを送信されるリモートホストの IP アドレスを指定します。	
state [enable | disable]	リモートホストへの syslog メッセージの送信を「enable」（有効）または「disable」（無効）にします。	

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

Syslog ホストを設定します。

```
DGS-3200-10:4#config syslog host all severity all
Command: config syslog host all severity all
Success.

DGS-3200-10:4#
```

delete syslog host

目的

設定した Syslog ホストをスイッチから削除します。

構文

delete syslog host [<index 1-4> | all]

説明

スイッチから定義済みの Syslog ホストを削除します。

パラメータ

パラメータ	説明
<index 1-4>	コマンドを適用する Syslog ホストのインデックスを指定します。1-4 の 4 つのインデックスが利用可能です。
all	すべてのホストに本コマンドを適用します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

定義済みの Syslog ホストを削除します。

```
DGS-3200-10:4#delete syslog host 4
Command: delete syslog host 4

Success.

DGS-3200-10:4#
```

show syslog host

目的

スイッチに現在設定されている Syslog ホストを表示します。

構文

show syslog host {<index 1-4>}

説明

スイッチに設定されている Syslog ホストを表示します。

パラメータ

パラメータ	説明
<index 1-4>	コマンドを適用する Syslog ホストのインデックスを指定します。1-4 の 4 つのインデックスが利用可能です。パラメータが指定されないと、すべてのホストが表示されます。

制限事項

なし。

使用例

Syslog ホスト情報を表示します。

```
DGS-3200-10:4#show syslog host
Command: show syslog host

Syslog Global State:Disabled

Host Id  Host IP Address Severity Facility UDP port Status
-------  --------------- -------- -------- -------- --------
1        10.1.1.2        All      Local0   514      Disabled
2        10.40.2.3       All      Local0   514      Disabled
3        10.21.13.1      All      Local0   514      Disabled

Total Entries :3

DGS-3200-10:4#
```

config log_save_timing

目的

スイッチのフラッシュメモリにログファイルを保存するタイミングを設定します。

構文

config log_save_timing [time_interval <min 1-65535> | on_demand | log_trigger]

説明

スイッチのフラッシュメモリにログファイルを保存する際に使用されるタイミングを設定します。

パラメータ

パラメータ	説明
time_interval <min 1-65535>	ログファイルの保存を実行する間隔を設定します。ログファイルは、ここで設定した時間（分）ごとに保存されます。
on_demand	「save」または「save log」コマンドを使用して、手動でスイッチに保存した場合にだけログファイルを保存します。（初期値）
log_trigger	スイッチにログイベントが発生すると、スイッチにログファイルを保存します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

ログを保存する方法を設定します。

```
DGS-3200-10:4# config log_save_timing on_demand
Command: config log_save_timing on_demand

Success.

DGS-3200-10:4#
```

show log_save_timing

目的

スイッチのフラッシュメモリにログファイルを保存するタイミングを表示します。

構文

show log_save_timing

説明

スイッチのフラッシュメモリにログファイルを保存するために設定されたタイミングを表示します。

パラメータ

なし。

制限事項

なし。

使用例

ログファイルの保存のためのタイミングを表示します。

```
DGS-3200-10:4#show log_save_timing
Command: show log_save_timing

Saving log method: on_demand

DGS-3200-10:4#
```

第 12 章　システムメッセージレベルコマンド

スイッチは、アラートが発生した場合、ログとして記録するか、または SNMP エージェントにトラップとして送信するか、またはその両方を選択することができます。また、アラートの発生がログイベント、またはトラップメッセージをトリガにするレベルも指定することができます。本コマンドを使用して、アラートの基準を設定します。

コマンドラインインタフェース（CLI）におけるシステムメッセージレベルコマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
config system_severity	[trap | log | all] [critical | warning | information]
show system_severity	

以下のセクションで各コマンドについて詳しく記述します。

config system_severity

目的

ログエントリまたはトラップメッセージに必要とされるアラートのメッセージレベルを設定します。

構文

config system_severity [trap | log | all] [critical | warning | information]

説明

本コマンドは、スイッチのシステムメッセージレベルを設定します。イベントがスイッチに発生する時、SNMP エージェント（トラップ）、スイッチのログまたは両方にメッセージは送信されます。スイッチに発生するイベントは 3 つの主なカテゴリに分けられます。これらのカテゴリは同じ名前のパラメータと厳密には同じではありません（以下参照）。

- information - information として分類されるイベントは、スイッチの様々な機能を有効または無効にするなどの問題とは見なされないようなスイッチにおける基本的なイベントです。
- warning - warning として分類されるイベントは、ダウンロード / アップロードの失敗やログインの失敗などスイッチの全般的な機能にとって総括的機能に重要でないが、注意を必要とする問題の多いイベントです。
- critical - critical として分類されるイベントは、ハードウェアの故障やスプーフィング攻撃などのスイッチに発生する致命的なイベントです。

パラメータ

以下のパラメータから 1 つを選び、送信されるシステムメッセージレベルを指定します。

パラメータ	説明
trap	スイッチに発生するどのイベントが分析のために SNMP エージェントに送られるかを定義します。
log	スイッチに発生するどのイベントが分析のためにスイッチのログに送信されるかを定義します。
all	スイッチに発生するどのイベントが分析のために SNMP エージェントとスイッチのログに送られるかを定義します。

以下のパラメータから 1 つを選び、どのシステム警告レベルが上で入力された宛先に送信されるかを指定します。

パラメータ	説明
critical	上で記述したように適切な宛先とともに本パラメータを入力すると、本スイッチのログまたは SNMP エージェントに critical イベントだけを送付します。
warning	上で記述したように適切な宛先とともに本パラメータを入力すると、本スイッチのログまたは SNMP エージェントに warning イベントおよび critical イベントを送付します。
information	上で記述したように適切な宛先とともに本パラメータを入力すると、本スイッチのログまたは SNMP エージェントに informational イベント、warning イベントおよび critical イベントを送付します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

システムメッセージレベル設定を重要なトラップだけに設定します。

```
DGS-3200-10:4#config system_severity trap information
Command: config system_severity trap information

Success.

DGS-3200-10:4#
```

show system_severity

目的

システムのシステムメッセージレベル制御を表示します。

構文

show system_severity

説明

システムのシステムメッセージレベル制御を表示します。

パラメータ

なし。

制限事項

なし。

使用例

システムのシステムメッセージレベル制御を表示します。

```
DGS-3200-10:4#show system_severity
Command: show system_severity

System Severity Trap : warning
System Severity Log  : information

DGS-3200-10:4#
```

第 13 章　コマンドヒストリリストコマンド

コマンドラインインタフェース（CLI）におけるコマンドヒストリリストコマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
?	
show command_history	
config command_history	<value 1-40>

以下のセクションで各コマンドについて詳しく記述します。

?

目的

コマンドラインインタフェース (CLI) におけるすべてのコマンド、および各コマンドの構文と記述情報を表示します。

構文

?{command}

説明

コマンドラインインタフェース (CLI) におけるすべてのコマンド、および各コマンドの構文と記述情報を表示します。

パラメータ

パラメータ	説明
{command}	適切なコマンドと共に「?」を入力すると、指定コマンドに対応するすべてのパラメータの一覧がコマンド機能の簡単な説明とコマンド内に同じ用語を持つ類似のコマンドと共に表示されます。パラメータが指定されないと、システムはすべてのコマンドを表示します。

制限事項

なし。

使用例

CLI に含まれるすべてのコマンドを表示します。

```
DGS-3200-10:4#?
Command: ?


..
?
cable_diag ports
clear
clear address_binding dhcp_snoop binding_entry ports
clear arptable
clear attack_log
clear counters
clear fdb
clear igmp_snooping data_driven_group
clear log
clear mac_based_access_control auth_mac
clear port_security_entry port
clear wac auth_state
config 802.1p default_priority
config 802.1p user_priority
Config 802.1x auth_failover
config 802.1x auth_mode
config 802.1x auth_parameter ports
config 802.1x auth_protocol
config 802.1x capability ports
config 802.1x guest_vlan ports

CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

show command_history

目的
　コマンドヒストリを表示します。
構文
　show command_history
説明
　コマンドヒストリを表示します。
パラメータ
　なし。
制限事項
　なし。
使用例
　コマンドヒストリを表示します。

```
DGS-3200-10:4#show command_history
Command: show command_history

?
?
show traffic_segmentation 1-6
config traffic_segmentation 1-6 forward_list 7-8
config radius delete 1
config radius add 1 10.48.74.121 key dlink default
config 802.1x reauth port_based ports all
config 802.1x init port_based ports all
config 802.1x auth_mode port_based
config 802.1x auth_parameter ports 1-50 direction both
config 802.1x capability ports 1-5 authenticator
show 802.1x auth_configuration ports 1
show 802.1x auth_state ports 1-5
enable 802.1x
show 802.1x auth_state ports 1-5
show igmp_snooping
enable igmp_snooping

DGS-3200-10:4#
```

config command_history

目的
　コマンドヒストリを設定します。スイッチは入力した最後の 40 個のコマンドを記憶しています。スイッチが再度呼び出しを行うコマンド数を設定することができます。
構文
　config command_history <value 1-40>
説明
　スイッチが再度呼び出しを行うコマンド数を設定します。
パラメータ

パラメータ	説明
<value 1-40>	スイッチが再度呼び出しを行うコマンド数（1-40）

制限事項
　管理者レベルユーザのみ本コマンドを実行できます。
使用例
　コマンドヒストリを設定します。

```
DGS-3200-10:4#config command_history 20
Command: config command_history 20

Success.

DGS-3200-10:4#
```

第 14 章　バナーとプロンプトの編集コマンド

コマンドラインインタフェース（CLI）におけるバナーとプロンプトの編集コマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
config greeting_message	{default}
config command_prompt	[<string 16> | username | default]
show greeting_message	

以下のセクションで各コマンドについて詳しく記述します。

config greeting_message

目的

ログインバナー（グリーティングメッセージ）を設定します。

構文

config greeting _message {default}

説明

バナーエディタを使用してログインバナー（グリーティングメッセージ）を編集します。

パラメータ

パラメータ	説明
default	本パラメータを追加すると、バナーは工場出荷時設定のバナーにリセットされます。
バナーエディタ	情報を入力し、バナーエディタに記述されているコマンドを使用してバナーに表示します。 - 保存しないで終了 - Ctrl+C - 保存して終了 - Ctrl+W - カーソルの移動 - Left/Right/Up/Down - ラインの削除 - Ctrl+D - 全設定の消去 - Ctrl+X - オリジナルの設定のリロード - Ctrl+L

制限事項

管理者レベルユーザのみ本コマンドを実行できます。他の制限は以下の通りです。

- 「reset/reset config」コマンドが実行されると、変更されたバナー設定は残ります。しかし、「reset system」コマンドは工場出荷時設定のバナーにリセットします。
- バナーは 6 行以内で指定します（1 行に 80 文字まで）。
- Ctrl+W は DRAM に変更されたバナーを保存するだけです。「save」コマンドを使用してフラッシュメモリに保存する必要があります。
- しきい値内で有効です。

使用例

バナーを編集します。

```
DGS-3200-10:4#config greeting_message
Command: config greeting_message

Greeting Message Editor
================================================================================

                      DGS-3200-10 Gigabit Ethernet Switch
                            Command Line Interface

                           Firmware: Build 1.50.B019
          Copyright(C) 2009 D-Link Corporation. All rights reserved.

================================================================================

   <Function Key>                  <Control Key>
   Ctrl+C     Quit without save    left/right/
   Ctrl+W     Save and quit        up/down       Move cursor
                                   Ctrl+D        Delete line
                                   Ctrl+X        Erase all setting
                                   Ctrl+L        Reload original setting
--------------------------------------------------------------------------------

Success.

DGS-3200-10:4#
```

応答メッセージ

1. 「Success.」
   有効なグリーティングメッセージを入力、設定がデバイスに受理された場合に表示されます。

2. 「Quit without saving.The current greeting message will not be changed.」
   「Ctrl+C」ファンクションキーを押すことによって、バナーエディタを終了した場合に表示されます。この場合、編集内容は保存されず、現在のグリーティングメッセージは変更されません。

3. 「Fail ! Settings failed.」
   入力された設定がデバイスによって受理されなかった場合に表示されます。

config command_prompt

目的

コマンドプロンプトを設定します。

構文

config command_prompt [<string 16> | username | default]

説明

管理者レベルのユーザが本コマンドを使用して、コマンドプロンプトを編集することができます。
現在のコマンドプロンプトは 4 つの部分で構成されています。「product name」+「:」+「user level」+「#」（例 :「DGS-3200-10:4#」）最大 16 文字から成る文字列を持つ最初の部分（1.「product name」）を変更します。また、ログインユーザ名と交換します。

パラメータ

パラメータ	説明
<string 16>	半角英数字 16 文字以内の新しい名前を入力することで、コマンドプロンプトを変更します。
username	コマンドプロンプトをログインユーザ名に変更します。
default	工場出荷時コマンドプロンプトにリセットします。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。他の制限は以下の通りです。

- 「reset」コマンドが実行されると、変更されたコマンドプロンプトは残ります。しかし、「reset system/config」コマンドは工場出荷時設定のバナーにリセットします。

使用例

コマンドプロンプトを「AtYourService」に変更します。

```
DGS-3200-10:4#config command_prompt AtYourService
Command: config command_prompt AtYourService

Success.

AtYourService:4#
```

応答メッセージ

1. 「Success.」
   入力された設定がデバイスによって受理された場合に表示されます。

2. 「Next possible completions: <string 16> username default.」
   入力したプロンプト文字列が最大文字数 (16 文字) を超えた場合に表示されます。

show greeting_message

目的

スイッチに設定されている現在のグリーティングメッセージを参照します。

構文

show greeting_message

説明

スイッチに設定されている現在のグリーティングメッセージを参照します。

パラメータ

なし。

制限事項

なし。

使用例

設定済みのグリーティングメッセージを参照します。

```
DGS-3200-10:4#show greeting_message
Command: show greeting_message

================================================================================
                    DGS-3200-10 Gigabit Ethernet Switch
                        Command Line Interface

                        Firmware:Build 1.50.B019
          Copyright(C) 2009 D-Link Corporation.All rights reserved.
================================================================================

DGS-3200-10:4#
```

第 15 章　SNTP 設定コマンド

SNMP（Simple Network Time Protocol）は、コンピュータのクロックにスイッチを同期させるために使用されます。

コマンドラインインタフェース（CLI）における Simple Network Time Protocol（SNTP）（Network Time Protocol（NTP）準拠）コマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
config sntp	{primary <ipaddr> | secondary <ipaddr> | poll-interval <int 30-99999>}
show sntp	
enable sntp	
disable sntp	
config time	<date ddmthyyyy> <time hh:mm:ss>
config time_zone	{operator [+ | -] | hour <gmt_hour 0-13> | min <minute 0-59>}
config dst	[disable | repeating {s_week <start_week 1-4,last> | s_day <start_day sun-sat> | s_mth <start_mth 1-12> | s_time <start_time hh:mm> | e_week <end_week 1-4,last> | e_day <end_day sun-sat> | e_mth <end_mth 1-12> | e_time <end_time hh:mm> | offset [30 | 60|90|120]} | annual {s_date <start_date 1-31> | s_mth <start_mth 1-12> | s_time <start_time hh:mm> | e_date <end_date 1-31> | e_mth <end_mth 1-12> | e_time <end_time hh:mm> | offset [30 | 60 | 90 | 120]}]
show time	

以下のセクションで各コマンドについて詳しく記述します。

config sntp

目的

SNTP サービスを設定します。

構文

config sntp {primary <ipaddr> | secondary <ipaddr> | poll-interval <int 30-99999>}

説明

SNTP サーバから SNTP サービスを設定します。SNTP を使用するためには、本コマンドで SNTP を有効にする必要があります（「enable sntp」参照）。

パラメータ

パラメータ	説明
primary<ipaddr>	SNTP 情報を取得するプライマリサーバの IP アドレス。
secondary<ipaddr>	プライマリサーバが使用できない場合に SNTP 情報を取得するセカンダリサーバの IP アドレス。
poll-interval <int 30-99999>	SNTP の更新情報をリクエストする間隔。ポーリング間隔は 30-99999（秒）。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。SNTP を使用するためには、SNTP を有効にする必要があります（「enable sntp」コマンド参照）。

使用例

SNTP パラメータを設定します。

```
DGS-3200-10:4#config sntp primary 10.1.1.1 secondary 10.1.1.2 poll-interval 30
Command: config sntp primary 10.1.1.1 secondary 10.1.1.2 poll-interval 30

Success.

DGS-3200-10:4#
```

show sntp

目的
　SNTP 情報を表示します。
構文
　show sntp
説明
　送信元 IP アドレス、時間、およびポーリング間隔を含む SNTP 設定情報を表示します。
パラメータ
　なし。
制限事項
　なし。
使用例
　SNTP 設定情報を表示します。

```
DGS-3200-10:4#show sntp
Command: show sntp

Current Time Source :System Clock
SNTP :Disabled
SNTP Primary Server   :10.1.1.1
SNTP Secondary Server :10.1.1.2
SNTP Poll Interval    :30 sec

DGS-3200-10:4#
```

enable sntp

目的
　SNTP サーバサポートを有効にします。
構文
　enable sntp
説明
　SNTP サポートを有効にします。SNTP サービスは分けて設定する必要があります（「config sntp」コマンド参照）。SNTP サポートを有効にして、設定すると、手動で設定したすべてのシステム時間設定が上書きされます。
パラメータ
　なし。
制限事項
　管理者レベルユーザのみ本コマンドを実行できます。SNTP パラメータは SNTP が機能するように設定される必要があります（「config sntp」コマンド参照）。
使用例
　SNTP 機能を有効にします。

```
DGS-3200-10:4#enable sntp
Command: enable sntp

Success.

DGS-3200-10:4#
```

disable sntp

目的
　SNTP サーバサポートを無効にします。
構文
　disable sntp
説明
　SNTP サポートを無効にします。SNTP サービスは分けて設定される必要があります（「config sntp」コマンド参照）。
パラメータ
　なし。
制限事項
　管理者レベルユーザのみ本コマンドを実行できます。
使用例
　SNTP を無効にします。

```
DGS-3200-10:4#disable sntp
Command: disable sntp

Success.

DGS-3200-10:4#
```

config time

目的
　手動でシステム時間と日付の設定を行います。
構文
　config time <date ddmthyyyy> <time hh:mm:ss>
説明
　システム時間と日付の設定を行います。SNTP が設定され、有効にされると、これらは上書きされます。
パラメータ

パラメータ	説明
date	システムクロック日付。日付には 2 桁の数字、月には英字 3 文字、年には 4 桁の数字を使用して表します。例 : 03aug2003
time	システムクロックタイム。システム時間は hh:mm:ss 形式で表します（hh: 時、mm: 分、ss: 秒は 2 桁の数字、24 時制）。例 :19:42:30

制限事項
　管理者レベルユーザのみ本コマンドを実行できます。SNTP が有効になると、手動で設定したシステム時間と日付設定は上書きされます。
使用例
　システム時間と日付の設定を手動で行います。

```
DGS-3200-10:4#config time 30jun2003 16:30:30
Command: config time 30jun2003 16:30:30

Success.

DGS-3200-10:4#
```

config time_zone

目的
　使用するタイムゾーンを決定し、システムクロックを調整します。
構文
　config time_zone {operator [+ | -] | hour <gmt_hour 0-13> | min <minute 0-59>}
説明
　タイムゾーンに応じて、システムクロック設定を調整します。そのため、タイムゾーン設定は SNTP 情報を調整します。
パラメータ

パラメータ	説明
operator	グリニッジ標準時に対するタイムゾーンの調整を（+）または（-）でそれぞれ時間をプラスおよびマイナスします。
hour	グリニッジ標準時との差分の時間を指定します。
min	プラスまたはマイナスする差分の時間（分）を指定し、タイムゾーンを調整します。

制限事項
　管理者レベルユーザのみ本コマンドを実行できます。

使用例

タイムゾーン設定を設定します。

```
DGS-3200-10:4#config time_zone operator + hour 2 min 30
Command: config time_zone operator + hour 2 min 30

Success.

DGS-3200-10:4#
```

config dst

目的

サマータイム（DST : Savings Time）を有効にし、時間調整を設定します。

構文

config dst [disable
| repeating {s_week <start_week 1-4,last>
| s_day <start_day sun-sat>
| s_mth <start_mth 1-12>
| s_time <start_time hh:mm>
| e_week <end_week 1-4,last>
| e_day <end_day sun-sat>
| e_mth <end_mth 1-12>
| e_time <end_time hh:mm>
| offset [30 | 60|90|120]}
| annual {s_date <start_date 1-31>
| s_mth <start_mth 1-12>
| s_time <start_time hh:mm>
| e_date <end_date 1-31>
| e_mth <end_mth 1-12>
| e_time <end_time hh:mm>
|offset [30 | 60 | 90 | 120]}]

説明

DST を有効にして、設定します。有効にする場合、どの DST 要求にも応じるようにシステムクロックの調整をします。DST 調整は手動による設定した時間および SNTP サービスを利用して設定した時間の両方のシステム時間に作用します。

パラメータ

パラメータ	説明
disable	スイッチの DST 季節時間の調整を無効にします。
repeating	リピートモードを使用すると、DST の季節の時間調整が有効になります。リピートモードでは、DST（サマータイム）の設定を指定する期間が必要となります。例えば、サマータイムを 4 月の第 2 週の土曜日から、10 月の最終週の日曜日までと指定することができます。
annual	アニュアルモードでは、DST の季節の時間調整は有効になります。アニュアルモードでは、DST（サマータイム）の設定を指定する詳細な期日が必要になります。例えば、サマータイムを 4 月 3 日から、10 月 14 日までと指定することができます。
s_week	DST が開始する週を設定します。 • <start_week 1-4,last> - DST が開始する週の番号。1 は第 1 週目、2 は第 2 週目と続き、last は月の最終週。
e_week	DST が終了する週を設定します。 • <end_week 1-4,last> - DST が終了する週の番号。1 は第 1 週目、2 は第 2 週目と続き、last は月の最終週
s_day	DST が開始する曜日を設定します。 • <start_day sun-sat> - 3 桁の英字を使用して表された DST が開始する曜日。（sun, mon, tue, wed, thu, fri, sat）
e_day	DST が終了する曜日を設定します。 • <end_day sun-sat> - 3 桁の英字を使用して表された DST が終了する曜日。（sun, mon, tue, wed, thu, fri, sat）
s_mth	DST が開始する月を設定します。 • <start_mth 1-12> - DST が開始する月番号。
e_mth	DST が終了する月を設定します。 • <end_mth 1-12> - DST が終了する月番号。
s_time	DST が開始する時刻を設定します。 • <start_time hh:mm> - 24 時制で時刻（hh: 時、mm: 分）を表します。
e_time	DST が終了する時刻を設定します。 • <end_time hh:mm> - 24 時制で時刻（hh: 時、mm: 分）を表します。

パラメータ	説明
s_date	DST が開始する特定日（月日）を設定します。 • <start_date 1-31> - 開始日を数字で表します。
e_date	DST が終了する特定日（月日）を設定します。 • <end_date 1-31> - 終了日を数字で表します。
offset [30 | 60 | 90 | 120]	サマータイムによる調整時間（プラスまたはマイナス）を指定します。可能なオフセット時間は、30、60、90、120 です。初期値は 60 です。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

15:30 に 15:00 に 4 月第 2 週の火曜日に開始し、10 月第 2 週の水曜日に終了するサマータイムの設定を行います。

```
DGS-3200-10:4#config dst repeating s_week 2 s_day tue s_mth 4 s_time 15:00 e_week 2 e_day wede_
mth 10 e_time 15:30 offset 30
Command: config dst repeating s_week 2 s_day tue s_mth 4 s_time 15:00 e_week 2 e_day wed e_mth
10 e_time 15:30 offset 30

Success.

DGS-3200-10:4#
```

show time

目的

現在の時刻設定と状態を表示します。

構文

show time

説明

現在のシステム時間と共に日付と時刻を表示します。

パラメータ

なし。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

現在スイッチに設定されている時間設定を表示します。

```
DGS-3200-10:4#show time
Command: show time

Current Time Source  : System Clock
Boot Time            : 1 Jan 2000 00:00:00
Current Time         : 1 Jan 2000 07:26:28
Time Zone            : +00:00
Daylight Saving Time : Disabled
Offset in Minutes    : 60
    Repeating From   : Apr 2nd Tue 15:00
               To    : Oct last Sun 00:00
    Annual     From  : 29 Apr 00:00
               To    : 12 Oct 00:00

DGS-3200-10:4#
```

第 16 章　ジャンボフレームコマンド

ジャンボフレームにより、同じデータを少ないフレームで転送することができます。これによりオーバヘッド、処理時間、割り込みを確実に減らすことができます。本スイッチはジャンボフレーム（標準のイーサネットサイズの 1536 バイトより長いフレーム）をサポートしています。最大 9K（およびタグ付きで 10240 バイト）までのフレームを送信するために、ジャンボフレームコマンドを有効にすることで MTU サイズを初期値の 1536 バイトから増やすことができます。

コマンドラインインタフェース（CLI）におけるジャンボフレームコマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
enable jumbo_frame	
disable jumbo_frame	
show jumbo_frame	

以下のセクションで各コマンドについて詳しく記述します。

enable jumbo_frame

目的
　ジャンボフレーム機能を有効にします。
構文
　enable jumbo_frame
説明
　ジャンボフレーム機能を有効にします。
パラメータ
　なし。
制限事項
　ジャンボフレーム機能を有効にします。
使用例
　ジャンボフレーム機能を有効にします。

```
DGS-3200-10:4#enable jumbo_frame
Command: enable jumbo_frame

The maximum size of Jumbo Frame is 10240 Bytes.
Success.

DGS-3200-10:4#
```

disable jumbo_frame

目的
　ジャンボフレーム機能を無効にします。
構文
　disable jumbo_frame
説明
　ジャンボフレーム機能を無効にします。
パラメータ
　なし。
制限事項
　管理者レベルユーザのみ本コマンドを実行できます。
使用例
　ジャンボフレーム機能を無効にします。

```
DGS-3200-10:4#disable jumbo_frame
Command: disable jumbo_frame

Success.

DGS-3200-10:4#
```

show jumbo_frame

目的

ジャンボフレーム機能の状態を表示します。

構文

show jumbo_frame

説明

スイッチのジャンボフレーム機能の状態を表示します。

パラメータ

なし。

制限事項

なし。

使用例

スイッチに設定されているジャンボフレームの現在の状態を参照します。

```
DGS-3200-10:4#show jumbo_frame
Command: show jumbo_frame

Jumbo Frame State  :Disabled
Maximum Frame Size :1536 Bytes

DGS-3200-10:4#
```

第 17 章　D-Link シングル IP マネジメントコマンド

シングル IP マネジメント（SIM）の概要

D-Link シングル IP マネジメントとは、スタックポートまたはモジュールを使用する代わりにイーサネット経由でスイッチをスタックする方法です。シングル IP マネジメント機能を利用する利点を以下に示します。

1. ネットワークを拡大し、増大する帯域幅に対する要求に対処しながら、小規模のワークグループや、ワイヤリングクローゼット（ユーザ接続エリア）を簡単に管理できるようになります。
2. ネットワークに必要な IP アドレス数を減らします。
3. スタック接続のために特別なケーブル配線を必要とせず、他のスタック技術ではトポロジ上の問題になる距離的制限を取り除きます。

D-Link シングル IP マネジメント（以下 SIM と呼びます）機能を搭載するスイッチには、以下の基本的なルールがあります。

- SIM はスイッチのオプション機能であり、CLI または Web インタフェース経由で簡単に有効 / 無効にできます。また、SIM グループはご使用のネットワーク内でスイッチの操作に影響を与えることはありません。
- SIMには3つのクラスのスイッチがあります。Commander Switch（CS）はグループのマスタスイッチ、Member Switch（MS）はCSによってSIMグループのメンバとして認識されるスイッチ、Candidate Switch（CaS）は SIM グループに物理的にリンクはしているが、SIM グループのメンバとして認識されていないスイッチです。
- 1 つの SIM グループには、Commander Switch（CS）を 1 つだけ持つことができます。
- 特定の SIM グループ内にあるすべてのスイッチは、同じ IP サブネット（ブロードキャストドメイン）内にある必要があります。ルータを越えた位置にあるメンバの設定はできません。
- 1 つの SIM グループには、Commander Switch（番号：0）を含めずに、最大 32 台のスイッチ（番号：1-32）が所属できます。
- 同じ IP サブネット（ブロードキャストドメイン）内の SIM グループ数に制限はありませんが、各スイッチは、1 つの SIM グループにしか所属することができません。
- マルチプル VLAN が設定されていると、SIM グループはスイッチ上のデフォルト VLAN だけを使用します。
- SIMはSIMをサポートしていないデバイスを経由することができます。そのためCSから1ホップ以上はなれたスイッチを管理することができます。

SIM グループは 1 つのエンティティとして管理されるスイッチのグループです。SIM スイッチは 3 つの異なる役割を持っています。

1. Commander Switch（CS）- グループの管理用デバイスとして手動で設定されるスイッチで、以下の特長を持っています。
   - IP アドレスを 1 つ持つ。
   - 他のシングル IP グループの CS や MS ではない。
   - マネジメント VLAN 経由で MS に接続する。

2. Member Switch（MS）- シングル IP グループに所属するスイッチで、CS からアクセスが可能です。MS は以下の特徴を持ちます。
   - 他のシングル IP グループの CS や MS ではない。
   - CS マネジメント VLAN 経由で CS に接続する。

3. Candidate Switch（CaS）- SIM グループに参加する準備が整っているが、まだ MS ではないスイッチです。CaS を SIM グループ内の MS として、本スイッチの機能を使用して手動で登録することが可能です。CaS として登録されたスイッチは、SIM グループには所属せず、以下の特長を持っています。
   - 他のシングル IP グループの CS や MS ではない。
   - CS マネジメント VLAN 経由で CS に接続する。

上記の役割には、以下のルールを適用します。

- 各デバイスは、まず CS の状態から始まります。
- CS は、はじめに CaS に、その後 MS となり、SIM グループの MS へと遷移します。つまり CS から MS へ直接遷移することはできません。
- ユーザは、CS から CaS へ手動で遷移させることができます。
- 以下のような場合に MS から CaS に遷移します。
  - CS を介して CaS として設定される時。
  - CS から MS への Report パケットがタイムアウトになった時。
- ユーザが手動で CaS から CS に遷移するように設定できます。
- CS を介して CaS は MS に遷移するように設定されます。

SIM グループの CS として運用するスイッチを 1 台登録した後、スイッチを手動によりグループに追加して MS とします。CS はその後 MS へのアクセスのためにインバンドエントリポイントとして動作します。CS の IP アドレスがグループのすべての MS への経路になり、CS の管理パスワードや認証によって、SIM グループのすべての MS へのアクセスを制御します。

SIM 機能を有効にすると、CS 内のアプリケーションはパケットを処理する代わりに、リダイレクト（宛先変更）します。アプリケーションは管理者からのパケットを復号化し、データの一部を変更し、MS へ送信します。処理後、CS は MS から Response パケットを受け取り、これを符号化して管理者に返送します。

CS が MS に遷移すると、自動的に CS が所属する最初の SNMP コミュニティ（リード権 / ライト権、リード権だけを含む）のメンバになります。しかし、自身の IP アドレスを持つ MS は、グループ内の他のスイッチ（CS を含む）が所属していない SNMP コミュニティに加入することができます。

バージョン 1.61 へのアップグレード

SIM 管理機能強化の目的で、本スイッチは本リリースにおいて、バージョン 1.61 にアップグレードしています。本バージョンでは以下の改善点が加わりました。

1. CS は、再起動または Web での異常検出によって、SIM グループから抜けたメンバスイッチを自動的に再検出する機能が搭載しました。この機能は、以前設定された SIM メンバが再起動の後に発行する Discovery パケットと Maintain パケットを使用することにより実現されます。一度 MS の MAC アドレスとパスワードが CS のデータベースに記録され、MS が再起動を行うと、CS はこの MS の情報をデータベースに保存し、MS が再検出された場合、これを SIM ツリーに自動的に戻します。これらのスイッチを再検出するために設定を行う必要はありません。

一度保存を行った MS の再検出ができないという場合もあります。例えば、スイッチの電源がオンになっていない場合、他のグループのメンバとなっている場合、または CS スイッチとして設定された場合は再検出処理をすることができません。

2. 本バージョンでは、以下のファームウェア、コンフィグレーションファイル、およびログファイルのアップロードやダウンロードを複数スイッチに対して行う機能が追加されました。

- ファームウェア : TFTP サーバから複数の MS に対するファームウェアダウンロードがサポートされました。
- コンフィグレーションファイル : TFTP サーバを使用した複数のコンフィグレーションのダウンロード / アップロード（コンフィグレーションの復元やバックアップ用）が可能になりました。
- ログ : 複数のログファイルを TFTP サーバにアップロード可能になりました。

コマンドラインインタフェース（CLI）における SIM コマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
enable sim	
disable sim	
show sim	{[candidate {<candidate_id 1-100>} | members {<member_id 1-32>} | group {commander_mac <macaddr>} | neighbor]}
reconfig	{member_id <value 1-32> | exit}
config sim_group	[add <candidate_id 1-100> {<password>} | delete <member_id 1-32>]
config sim	[[commander {group_name <groupname 64>} | candidate] | dp_interval <30-90> | hold_time <sec 100-255>]
download sim_ms	[firmware_from_tftp | configuration_from_tftp] <ipaddr> <path_filename> {[members <mslist 1-32> | all]}
upload sim_ms	[configuration_to_tftp | log_to_tftp] <ipaddr> <path_filename> {[members <mslist> | all]}
config sim trap	[enable | disable]

以下のセクションで各コマンドについて詳しく記述します。

enable sim

目的

スイッチのシングル IP マネジメント（SIM）を有効にします。

構文

enable sim

説明

スイッチの SIM 機能をグローバルに有効にします。本機能が有効にしないと、SIM 機能は適切に機能しません。

パラメータ

なし。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

スイッチで SIM を有効にします。

```
DGS-3200-10:4#enable sim
Command: enable sim

Success.

DGS-3200-10:4#
```

disable sim

目的

スイッチのシングル IP マネジメント（SIM）を無効にします。

構文

```
disable sim
```

説明

スイッチの SIM 機能をグローバルに無効にします。

パラメータ

なし。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

スイッチで SIM を無効にします。

```
DGS-3200-10:4#disable sim
Command: disable sim

Success.

DGS-3200-10:4#
```

show sim

目的

スイッチの SIM グループに関する現在の情報を表示します。

構文

show sim {[candidate { <candidate_id 1-100>} | members {<member_id 1-32>} | group {commander_mac <macaddr>} | neighbor]}

説明

CaS、MS、グループおよび Neighbor を含む以下のようなスイッチの SIM グループに関する現在の情報を表示します。

- SIM バージョン - スイッチの現在の SIM バージョンを表示します。
- ファームウェアバージョン - スイッチに設定されているファームウェアバージョンを表示します。
- デバイス名 - スイッチのユーザ定義デバイス名を表示します。
- MAC アドレス - スイッチの MAC アドレスを表示します。
- Capabilities - スイッチのタイプ（レイヤ 2 : L2 またはレイヤ 3 : L3）を表示します。
- SIM State - 現在のスイッチの SIM 状態が有効または無効であるかを表示します。
- Role State - CS、MS、CaS を含むスイッチの現在の役割を表示します。スタンドアロンスイッチは、いつも CS です。
- Discovery Interval - スイッチがネットワークに Discovery パケットを送信する間隔（秒）を表示します。
- Hold time - 廃棄または使用する前にスイッチが検出結果を保持する時間（秒）を表示します。

パラメータ

パラメータ	説明
<candidate_id 1-100>	SIM グループの CaS に関する情報を表示します。特定の CaS を参照する場合は、CaS ID 番号（1-100）を入力します。
members <member_id 1-32>	SIM グループのメンバに関する情報を表示します。特定のメンバを参照するためには、1-32 までのメンバ ID を入力します。
group {commander_mac <macaddr>}	SIM グループに関する情報を表示します。特定のグループを見るためには、グループの CS の MAC アドレスを入力します。
neighbor	スイッチの Neighbor デバイスを表示します。Neighbor は SIM スイッチに物理的に接続していても SIM グループのメンバではないスイッチとして定義されます。以下の結果が生成されます。 • Port - Neighbor スイッチにアップリンクしている CS の物理ポート番号を表示します。 • MAC Address - Neighbor スイッチの MAC アドレスを表示します。 • Role - Neighbor スイッチの役割（CS、CaS、MS）を表示します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

詳細な SIM 情報を参照します。

```
DGS-3200-10:4#show sim
Command: show sim

SIM Version         : VER-1.61
Firmware Version    : Build 1.50.B019
Device Name         :
MAC Address         : 00-35-26-11-11-00
Capabilities        : L2
Platform            : DGS-3200-10 L2 Switch
SIM State           : Disabled
Role State          : Candidate
Discovery Interval  : 30 sec
Hold Time           : 100 sec
Trap                : Enabled

DGS-3200-10:4#
```

サマリ内の CaS 情報を表示します。

```
DGS-3200-10:4#show sim candidate
Command: show sim candidate

ID  MAC Address       Platform /              Hold  Firmware  Device Name
                      Capability              Time  Version
--- ----------------- ----------------------- ----- --------- ----------------
 1  00-01-02-03-04-00 DGS-3200-10 L2 Switch    40   1.50-B019 aaaaaaaaaaaaaaa
 2  00-55-55-00-55-00 DES-3326SR L3 Switch     140   4.00-B15  default master

Total Entries: 2

DGS-3200-10:4#
```

サマリ内のメンバ情報を表示します。

```
DGS-3200-10:4#show sim members
Command: show sim members

ID  MAC Address       Platform /              Hold  Firmware  Device Name
                      Capability              Time  Version
--- ----------------- ----------------------- ----- --------- ----------------
1  00-01-02-03-04-00  DGS-3200-10 L2 Switch    40   1.50-B019 aaaaaaaaaaaaaaa
2  00-55-55-00-55-00  DES-3326SR L3 Switch     140   4.00-B15  default master

Total Entries: 2

DGS-3200-10:4#
```

グループが指定された場合、サマリ内のグループ情報を表示します。

```
DGS-3200-10:4#show sim group
Command: show sim group

SIM Group Name : default

ID  MAC Address       Platform /               Hold  Firmware  Device Name
                      Capability               Time  Version
--- ----------------- ------------------------ ----- --------- ----------------
*1  00-01-02-03-04-00 DGS-3200-10 L2 Switch     40   1.10-B021 aaaaaaaaaaaaaaa
 2  00-55-55-00-55-00

SIM Group Name : SIM2

ID  MAC Address       Platform /               Hold  Firmware  Device Name
                      Capability               Time  Version
--- ----------------- ------------------------ ----- --------- ----------------
*1  00-01-02-03-04-00 DGS-3200-10 L2 Switch     40   1.50-B019 aaaaaaaaaaaaaaa
 2  00-55-55-00-55-00

'*' means commander switch.

DGS-3200-10:4#
```

SIM Neighbor を参照します。

```
DGS-3200-10:4#show sim neighbor
Command: show sim neighbor

Neighbor Table

Port    MAC Address         Role
------  ------------------  ---------
23      00-35-26-00-11-99   Commander
23      00-35-26-00-11-91   Member
24      00-35-26-00-11-90   Candidate

Total Entries: 3

DGS-3200-10:4#
```

reconfig

目的

Telnet を使用して、CS から MS に接続します。

構文

reconfig {member_id <value 1-32 | exit}

説明

Telnet を使用して MS に再接続します。

パラメータ

パラメータ	説明
member_id <value 1-32>	設定する MS の ID 番号を指定します。
exit	MS の管理を終了し、CS の管理に戻ります。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

MS に接続します。

```
DGS-3200-10:4#reconfig member_id 1
Command: reconfig member_id 1

DGS-3200-10:4#
Login:
```

config sim_group

目的

SIM グループから CaS の追加、またはメンバの削除を行います。

構文

config sim_group [add <candidate_id 1-32> {<password>} | delete <member_id 1-32>]

説明

ID 番号によって SIM グループから CaS の追加、またはメンバの削除を行います。

パラメータ

パラメータ	説明
add <candidate_id 1-32> {<password>}	CaS を SIM グループの MS 変更します。（必要であれば）、CaS は ID 番号とパスワードによって定義することも可能です。
delete <member_id 1-32>	SIM グループのメンバを削除します。MS は ID 番号によって指定します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

メンバを追加します。

```
DGS-3200-10:4#config sim_group add 2
Command: config sim_group add 2

Please wait for ACK!!!
SIM Config Success !!!

Success.

DGS-3200-10:4#
```

メンバを削除します。

```
DGS-3200-10:4#config sim_group delete 1
Command: config sim_group delete 1

Please wait for ACK!!!
SIM Config Success!!!

Success.

DGS-3200-10:4#
```

config sim

目的

スイッチの SIM プロトコルの役割パラメータを設定します。

構文

config sim [[commander {group_name <groupname 64>} | candidate] | dp_interval <30-90> | hold_time <sec 100-255>]

説明

SIM スイッチのパラメータを設定します。

パラメータ

パラメータ	説明
commander	CS に変更します。CS になると、グループ名を変更することができます。 • group_name <groupname 64> - グループ名を更新します。64 文字以内の半角英数字の文字列を入力して、SIM グループ名を更新します。
candidate	CS を CaS に変更します。
dp_interval <30-90>	スイッチが Discovery パケットを送信する Discovery プロトコル送信間隔（秒）を設定します。30-90（秒）の間から指定します。
hold_time <sec 100-255>	他のスイッチから「Discovery Interval」の間隔で送信された情報を CS が保持する時間（秒）を指定します。100-255（秒）の間から指定します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

CS に設定します。

```
DGS-3200-10:4#config sim commander
Command: config sim commander

Success.

DGS-3200-10:4#
```

CaS に設定します。

```
DGS-3200-10:4#config sim candidate
Command: config sim candidate

Success.

DGS-3200-10:4#
```

グループ名を更新します。

```
DGS-3200-10:4#config sim commander group_name mygroup
Command: config sim commander group_name mygroup

Success.

DGS-3200-10:4#
```

Discovery プロトコルの間隔を変更します。

```
DGS-3200-10:4#config sim dp_interval 30
Command: config sim dp_interval 30

Success.

DGS-3200-10:4#
```

Discovery プロトコルの保持時間を変更します。

```
DGS-3200-10:4#config sim hold_time 200
Command: config sim hold_time 200

Success.

DGS-3200-10:4#
```

download sim_ms

目的

ファームウェアまたはコンフィグレーションファイルを指定デバイスにダウンロードします。

構文

download sim_ms [firmware_from_tftp | configuration_from_tftp] <ipaddr> <path_filename> {[members <mslist 1-32> | all]}

説明

TFTP サーバから新しいファームウェアまたはスイッチのコンフィグレーションファイルを指定デバイスにダウンロードして、インストールします。

パラメータ

パラメータ	説明
firmware_from_tftp	SIM グループのメンバにファームウェアをダウンロードします。
configuration_from_tftp	SIM グループのメンバにスイッチのコンフィグレーションをダウンロードします。
<ipaddr>	TFTP サーバの IP アドレスを入力します。
<path_filename>	TFTP サーバのファームウェアまたはスイッチのパス名およびファイル名を入力します。
members	ファームウェアまたはスイッチのコンフィグレーションファイルをダウンロードする先のメンバを指定します。以下のパラメータから 1 つを追加することによって、メンバを指定します。 • <mslist 1-32> - 値を入力し、ファームウェアまたはスイッチのコンフィグレーションファイルを受け取る SIM グループのメンバを指定します。 • all - ファームウェアまたはスイッチのコンフィグレーションファイルを SIM グループのすべてのメンバが受け取ります。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

ファームウェアをダウンロードします。

```
DGS-3200-10:4#download sim_ms configuration_from_tftp 10.55.47.1 D:\dwl600x.tfpmembers 1
Commands: download sim_ms configuration_from_tftp 10.55.47.1 D:\dwl600x.tfp members 1

This device is updating firmware.  Please wait...

Download Status :

ID   MAC Address        Result
---  ----------------- ----------------
1    00-01-02-03-04-00  Success
2    00-07-06-05-04-03  Fail
3    00-07-06-05-04-04  Fail

DGS-3200-10:4#
```

コンフィグレーションファイルをダウンロードします。

```
DGS-3200-10:4#download sim_ms configuratin_from_tftp 10.55.47.1 D:\test.txt 1
Commands: download sim_ms configuratin_from_tftp 10.55.47.1 D:\test.txt 1
<new page>

This device is updating configuration.  Please wait...

Download Status :

ID   MAC Address        Result
---  ----------------  ----------------
1    00-01-02-03-04-00   Success
2    00-07-06-05-04-03   Fail
3    00-07-06-05-04-04   Fail

DGS-3200-10:4#
```

upload sim_ms

目的

SIM グループの指定メンバから TFTP サーバにコンフィグレーションファイルまたはログファイルをアップロードします。

構文

upload sim_ms [configuration_to_tftp | log_to_tftp] <ipaddr> <path_filename> {[members <mslist> | all]}

説明

SIM グループの指定メンバから TFTP サーバにコンフィグレーションファイルまはたログファイルをアップロードします。

パラメータ

パラメータ	説明
configuration_to_tftp | log_to_tftp	SIM グループのメンバから TFTP サーバにスイッチのコンフィグレーションをアップロードします。
<ipaddr>	TFTP サーバの IP アドレスを入力します。
<path_filename>	ファイルをアップロードする TFTP サーバのユーザ定義パスとファイル名を入力します。
members <mslist> | all	スイッチコンフィグレーションまたはログファイルをアップロードする先のメンバを指定します。以下のパラメータから 1 つを追加することによって、メンバを指定します。 • <mslist> - 値を入力し、スイッチのコンフィグレーションファイルまたはログファイルをアップロードする SIM グループのメンバを指定します。 • all - スイッチのコンフィグレーションファイルまたはログファイルを SIM グループのすべてのメンバがアップロードします。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

TFTP サーバにコンフィグレーションファイルをアップロードします。

```
DGS-3200-10:4#upload sim_ms configuration_to_tftp 10.55.47.1 D:\configuration.
txt members 1
Command: upload sim_ms configuration_to_tftp 10.55.47.1 D:\configuration.txt
members 1

Done.

DGS-3200-10:4#
```

config sim trap

目的

メンバスイッチから発行されるトラップの送信を制御します。

構文

config sim trap [enable | disable]

説明

メンバスイッチから発行されるトラップの送信を制御します。

パラメータ

パラメータ	説明
[enable | disable]	トラップのステータスを「Enable」(有効) または「Disable」(無効) にします。初期値は有効です。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

SIM トラップを無効にします。

```
DGS-3200-10:4#config sim trap disable
Command: config sim trap disable

Success.

DGS-3200-10:4#
```

第 18 章　セーフガードエンジンコマンド

ネットワーク上の悪意のあるホストがスイッチに対して、パケットフラッディング（ARP ストーム）などを利用して、周期的に攻撃してくることがあります。これらの攻撃はスイッチに能力以上の負荷を加える可能性があります。このような問題を軽減するために、本スイッチのソフトウェアにセーフガードエンジン機能を付加しました。

セーフガードエンジンは、攻撃が行われている間、スイッチの稼働を最小化して、スイッチ全体の操作性を保ち、限られたリソース内で必要不可欠なパケットの送受信を可能にします。スイッチが（a）処理能力を超えた量のパケットを受信した場合、または（b）メモリ使用率が高すぎる場合には、「Exhausted」モードに遷移します。本モードでは、スイッチの稼働を最小化するために、以下のタスクを実行します。

1. 受信 ARP パケットの帯域幅を制限します。「config safeguard_engine」コマンドを使用して 2 つの方法で実行することができます。

- 「strict」を選択すると、スイッチはスイッチに到達しない ARP パケットの受信を中止します。これにより、不必要な ARP パケットをすべて排除し、必要な ARP パケットを不可欠の ARP パケットをスイッチの CPU にパススルーします。

- 「fuzzy」を選択すると、スイッチに到着するかどうかに関わらず、すべての ARP パケットの帯域を調整することによって、スイッチが受信する ARP パケットの帯域を最小化します。スイッチは、内部アルゴリズムを使用し、スイッチに到着する ARP パケットのために確保するように高い割合で ARP パケットをフィルタします。

2. スイッチが受信する IP パケットの帯域幅を制限します。「config safeguard_engine」コマンドを使用して 2 つの方法で実行することができます。

- 「strict」を選択すると、ブロードキャスト IP パケットの高受信レートによって高 CPU 使用率が発生しなくても、スイッチは不必要なブロードキャスト IP パケットの受信を中止します。

- 「fuzzy」を選択すると、IP パケットの帯域の調整、ユニキャストおよびブロードキャスト両方への受信帯域の設定を行うことによって、スイッチが受信する IP パケットの帯域を最小化します。スイッチは、内部アルゴリズムを使用して、ダイナミックに帯域幅を調整中に IP パケットをフィルタします。

また、IP パケットは、受け入れる特定の IP アドレスを設定することで、スイッチに制限されます。前セクションで記述した CPU インタフェースフィルタリングメカニズムを通してこの方式を実行することができます。一度許可する IP アドレスを設定すると、異なる IP アドレスを含む他のパケットは、スイッチに廃棄され、その結果、IP パケットの帯域幅を制限します。処理を高速に保つためには、許可する IP アドレスとそのパケットを受け付ける多くの条件を追加しないように注意してください。多くの条件は CPU の使用率を制限します。

一度セーフガードエンジンは Exhausted モードになると、パケットフローは本モード開始時の半分のレベルまで減少させます。Normal モードに戻ると、パケットを 25% ずつ増加させます。スイッチは、その後間隔をチェックし、スイッチのオーバロードを避けるように動的に通常のパケットフローに戻します。

注意 セーフガードエンジンが有効の場合、本スイッチは FFP（Fast Filter Processor）メータリングテーブルを使用し、各トラフィックフロー（ARP、IP）に帯域を割り当て、CPU 使用率を制御することでトラフィックを制限します。これは、ネットワーク上のトラフィックのルーティング速度を制限します。

コマンドラインインタフェース（CLI）におけるセーフガードエンジンコマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
config safeguard_engine	{state [enable | disable] | utilization {rising <value 20-100> | falling <value 20-100>} | trap_log [enable | disable] | mode [strict | fuzzy]}
show safeguard_engine	

以下のセクションで各コマンドについて詳しく記述します。

config safeguard_engine

目的

セーフガードエンジンを設定します。

構文

config safeguard_engine {state [enable | disable] | utilization {rising <value 20-100> | falling <value 20-100>} | trap_log [enable | disable] | mode [strict | fuzzy]}

説明

システムにセーフガードエンジンを設定します。

パラメータ

パラメータ	説明
state [enable | disable]	セーフガードエンジン機能の実行状態を有効または無効にします。
utilization [rising <value 20-100> | falling <value 20-100>]	セーフガードエンジン機能のトリガーとなり、以下の実行に基づいて有効になります。 • rising <value 20-100> - セーフガードエンジン機能のトリガーとなるライジング CPU 使用率の割合を設定します。CPU 使用率がこの割合に上昇するとセーフガードエンジンメカニズムは開始し、スイッチは「Exhausted」モードに入ります。 • falling <value 20-100> - セーフガードエンジン機能のトリガーとなるフォーリング CPU 使用率の割合を設定します。CPU 使用率がこの割合に下がるとセーフガードエンジンメカニズムは終了し、スイッチは「Normal」モードに入ります。
trap_log [enable | disable]	セーフガードエンジン機能が CPU 高使用率で作動すると、デバイスの SNMP エージェントとスイッチのログへのメッセージ送信を有効または無効にします。 • enable - トラップとログは CPU 保護の現在のモードが変更されるとアクティブになります。 • disable - 現在のモード変更がトラップとログイベントのトリガーになりません。
mode [strict | fuzzy]	CPU 高使用率に到達した際に起動するセーフガードエンジンのタイプを選択します。以下のパラメータを選択することができます。 • strict - すべてのトラフィックフローに対し平等にダイナミックな帯域割り当てを行うことで CPU に対する IP と ARP トラフィックフローを最小化します。 • fuzzy - ストームがおさまるまで本スイッチ行きではないすべての ARP パケットの受信をストップし、不必要なブロードキャスト IP パケットの受信をストップします。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

スイッチにセーフガードエンジンエンジンを設定します。

```
DGS-3200-10:4#config safeguard_engine state enable utilization rising 50 falling 30 trap_log enable
Command: config safeguard_engine state enable utilization rising 50 falling 30 trap_log enable

Success.

DGS-3200-10:4#
```

show safeguard_engine

目的

現在のセーフガードエンジン設定を表示します。

構文

show safeguard_engine

説明

現在設定されているセーフガードエンジンのステータスとタイプを表示します。

パラメータ

なし。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

セーフガードエンジン状態を表示します。

```
DGS-3200-10:4#show safeguard_engine
Command: show safeguard_engine

Safeguard Engine State           : Enabled
Safeguard Engine Current Status  : Exhausted Mode
================================================================================
CPU Utilization Information:
Rising Threshold  : 30%
Falling Threshold : 20%
Trap/Log State    : Disabled
Mode              : Fuzzy

DGS-3200-10:4#
```

注意 セーフガードエンジン状態には、2 つのモード（「Exhausted」、「Normal」）があります。

第 19 章　マルチプルスパニングツリー（MSTP）コマンド

本スイッチは 3 つのバージョンのスパニングツリープロトコル（802.1D STP、802.1w Rapid STP、802.1s MSTP）をサポートしています。MSTP（Multiple Spanning Tree Protocol）は IEEE 委員会により定義された標準規格で、複数の VLAN を 1 つのスパニングツリーインスタンスにマッピングし、ネットワーク中に複数の経路を提供します。また、ロードバランシングを可能にし、1 つのインスタンスに障害が発生した場合でも、広い範囲で影響を与えないようにすることができます。障害発生時には障害が発生したインスタンスに代わって新しいトポロジを素早く収束します。これら VLAN 用のフレームは、これらの 3 つのスパニングツリープロトコル（STP、RSTP、MSTP）のいずれかを使用して、素早く適切に相互接続されたブリッジを通して処理されます。本プロトコルでは、BPDU（Bridge Protocol Data Unit）パケットにタグ付けを行い、受信するデバイスが、スパニングツリーインスタンス、スパニングツリーリージョン、およびそれらに関連付けられた VLAN を区別できるようにしています。これらのインスタンスは Instance_ID によって分類されます。MSTP では、複数のスパニングツリーを CIST（Common and Internal Spanning Tree）で接続します。CIST は自動的に各 MSTP リージョンとその最大範囲を決定し、1 つのスパニングツリーを構成する 1 つの仮想ブリッジのように見せかけます。そのため、異なる VLAN を割り当てられたフレームは、ネットワーク上の管理用に設定されたリージョン中の異なるデータ経路を通ります。ネットワーク上の MSTP を使用しているスイッチは、以下の 3 つの属性を持つ 1 つの MSTP 構成を持ちます。

a）32 文字までの半角英数字で定義された「Configuration 名」（「config stp mst_config_id」コマンドでの name <string> として設定済み）。
b）「Configuration Revision 番号」（「Revision Level」として設定済み）。
c）4096 件のエレメントテーブル（「VID range」として設定済み）。スイッチがサポートする 4096 件までの VLAN とインスタンスとの関連付けです。

スイッチで MSTP 機能を利用するためには、以下の手順を実行します。

a）スイッチに MSTP 設定を行います（「config stp version」コマンド）。
b）MSTP インスタンスに適切なスパニングツリープライオリティを設定します（「config stp priority」コマンド）。
c）共有する VLAN を MSTP Instance ID に追加する必要があります（「config stp instance_id」コマンド）。

コマンドラインインタフェース（CLI）におけるマルチプルスパニングツリーコマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
show stp	
show stp instance	<value 0-15>
show stp ports	{<portlist>}
show stp mst_config id	
create stp instance_id	<value 1-15>
delete stp instance_id	<value 1-15>
config stp instance _id	<value 1-15> [add_vlan | remove_vlan] <vidlist>
config stp mst_config_id	{revision_level <int 0-65535> | name <string 1-32>}
enable stp	
disable stp	
config stp version	[mstp | rstp | stp]
config stp priority	<value 0-61440> instance_id <value 0-15>
config stp	{maxage <value 6-40> | maxhops <value 6-40> | hellotime <value 1-2> | forwarddelay <value 4-30> | txholdcount <value 1-10> | fbpdu [enable | disable]}
config stp ports	<portlist> {externalCost [auto | <value 1-200000000>] | hellotime <value 1-2> | migrate [yes | no] | edge [true | false |auto] | restricted_tcn [true | false] | restricted_role [true | false] | p2p [true | false | auto] | state [enable | disable] | fbpdu [enable | disable]}
config stp mst_ports	<portlist> instance_id <value 0-15> {internalCost [auto | <value 1-200000000>] | priority <value 0-240>}
config stp trap	{new_root [enable | disable] | topo_change [enable | disable]}

以下のセクションで各コマンドについて詳しく記述します。

show stp

目的
　スイッチの現在のグローバルな STP 設定を表示します。（CIST または msti ID=0）
構文
　show stp
説明
　スイッチの現在の STP 設定を表示します。
パラメータ
　なし。
制限事項
　なし。

使用例

スイッチの現在の STP 設定を表示します。

```
DGS-3200-10:4#show stp
Command: show stp

STP Bridge Global Settings
------------------------------
STP Status           : Enabled
STP Version          : MSTP
Max Age              : 20
Forward Delay        : 15
Max Hops             : 20
TX Hold Count        : 3
Forwarding BPDU      : Enabled
New Root Trap        : Enabled
Topology Change Trap: Disabled

DGS-3200-10:4#
```

show stp instance

目的

スイッチの STP インスタンス設定を表示します。

構文

show stp instance <value 0-15>

説明

スイッチの現在の STP インスタンス設定と STP インスタンスの動作状態を表示します。値がインスタンス ID を意味し、入力しない場合、すべてのインスタンス設定を表示します。

パラメータ

パラメータ	説明
<value 0-15>	スイッチに設定済みのインスタンス ID1-15 の範囲から指定します。インスタンス 0 は、スイッチの内部に設定されている CIST に対する STP 設定を表示します。

制限事項

なし。

使用例

スイッチのインスタンス 0（内部 CIST）に対する STP インスタンス設定を表示します。

```
DGS-3200-10:4#show stp instance
Command: show stp instance

STP Instance Settings
---------------------------
Instance Type           : CIST
Instance Status         : Enabled
Instance Priority       : 32768(bridge priority : 32768, SYS ID Ext : 0 )

STP Instance Operational Status
-------------------------------
Designated Root Bridge : 32768/00-22-22-22-22-00
External Root Cost     : 0
Regional Root Bridge   : 32768/00-22-22-22-22-00
Internal Root Cost     : 0
Designated Bridge      : 32768/00-22-22-22-22-00
Root Port              : None
Max Age                : 20
Forward Delay          : 15
Last Topology Change   : 2430
Topology Changes Count : 0

DGS-3200-10:4#
```

show stp ports

目的

スイッチの現在の STP ポート設定を表示します。

構文

show stp ports {<portlist>}

説明

スイッチにおける STP ポート設定と現在実行されている STP ポートの動作状態を表示します。ポートリストが入力されないと、すべてのポートを表示します。複数のインスタンスがこのスイッチにある場合、それぞれのインスタンスのポートパラメータが表示されます。

パラメータ

パラメータ	説明
<portlist>	表示するポートまたは範囲を指定します。

制限事項

なし

使用例

STP にポートを表示します。

```
DGS-3200-10:4#show stp ports
Command: show stp ports

MSTP Port Information
---------------------
Port Index        : 1     ,  Hello Time       : 2 /2 ,  Port STP : Enabled,
External PathCost : Auto/200000   ,  Edge Port : No /No ,  P2P    : False/No
Port RestrictedRole : False,  Port RestrictedTCN : False
Port Forward BPDU : Enabled
MSTI   Designated Bridge   Internal PathCost  Prio  Status      Role
-----  ------------------  -----------------  ----  ----------  ----------
0      N/A                 200000             128   Disabled    Disabled
2      N/A                 200000             128   Disabled    Disabled

DGS-3200-10:4#
```

show stp mst_config_id

目的

MSTP 設定 ID を表示します。

構文

show stp mst_config_id

説明

コンフィグレーション名、リビジョンレベルおよび MST 設定テーブルを含む MSTP 設定 ID を表示します。デフォルトのコンフィグレーション名はスイッチの MAC アドレスです。

パラメータ

なし。

制限事項

なし。

使用例

現在スイッチに設定されている MSTI ID を表示します。

```
DGS-3200-10:4#show stp mst_config_id
Command: show stp mst_config_id

Current MST Configuration Identification
---------------------------------------

Configuration Name : 00-22-22-22-22-00                      Revision Level :0
MSTI ID     Vid list
-------     -----------
   CIST     1-4094

DGS-3200-10:4#
```

create stp instance_id

目的

MSTP に STP インスタンス ID を作成します。

構文

create stp instance_id <value 1-15>

説明

デフォルトインスタンス CIST（インスタンス 0）とは別の新しい MST インスタンスを作成します。MST インスタンスを作成後に、135 ページの「第 23 章 VLAN コマンド」を使用して、VLAN を設定する必要があります。または、新たに作成された MST インスタンスを無効状態とします。スイッチには 16 個のインスタンス（1 つは CIST で変更できません。）があり、15 個のインスタンス ID を作成することができます。

パラメータ

パラメータ	説明
<value 1-15>	スイッチに STP インスタンスを指定するために 1-15 の範囲から指定します。インスタンス 0 はデフォルトインスタンスの CIST を表しています。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

STP インスタンス 2 を作成します。

```
DGS-3200-10:4#create stp instance_id 2
Command: create stp instance_id 2

Warning:There is no VLAN mapping to this instance_id!
Success.

DGS-3200-10:4#
```

delete stp instance_id

目的

指定した STP インスタンスを削除します。

構文

delete stp instance_id <value 1-15>

説明

指定した STP インスタンスを削除します。CIST（インスタンス 0）は削除できません。一度に 1 つのインスタンスずつ削除します。

パラメータ

パラメータ	説明
<value 1-15>	削除する STP インスタンス ID。インスタンス 0 はデフォルトインスタンスの CIST を表しています。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

スイッチからインスタンス ID 2 を削除します。

```
DGS-3200-10:4#delete stp instance_id 2
Command: delete stp instance_id 2

Success.

DGS-3200-10:4#
```

config stp instance_id

目的

STP インスタンス ID の追加または削除をします。

構文

config stp instance_id <value 1-15> [add_vlan | remove_vlan] <vidlist>

説明

スイッチにインスタンス _ID を作成することによって、VID（VLANID）を設定済みの STP インスタンスにマップします。STP インスタンスは、同じ MSTP 設定を持つ複数メンバを持っています。ネットワークにおける、STP 範囲の数には制限はありませんが、各範囲は、最大 16 個の STP インスタンス（1 つは変更できないデフォルトエントリ）をサポートしています。VID は一度に 1 つの STP インスタンスにだけ所属することができます。同様に同じ STP インスタンス _ID を持つ同じ STP 範囲にあるスイッチがマップされ、同じ設定のリビジョンレベル番号と同じ名前を持つ必要があることに注意してください。

パラメータ

パラメータ	説明
<value 1-15>	スイッチに STP インスタンスを指定するために 1-15 の範囲から指定します。スイッチは 0 として設定されている変更できないデフォルトインスタンス ID を含め 16 個の STP 範囲をサポートしています。
add_vlan	<vidlist> パラメータと共に、設定済みの STP インスタンス ID に VID を追加します。
remove_vlan	<vidlist> パラメータと共に、設定済みの STP インスタンス ID から VID を削除します。
<vidlist>	スイッチに登録済みの VLAN の中から、VID の範囲を指定します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

インスタンス ID 2 を設定し、VID を追加します。

```
DGS-3200-10:4#config stp instance_id 2 add_vlan 1-3
Command: config stp instance_id 2 add_vlan 1-3

Success.

DGS-3200-10:4#
```

インスタンス ID2 から VID 2 を削除します。

```
DGS-3200-10:4#config stp instance_id 2 remove_vlan 2
Command: config stp instance_id 2 remove_vlan 2

Success.

DGS-3200-10:4#
```

config stp mst_config_id

目的

MST コンフィグレーション ID の名前またはリビジョンレベルを変更します。

構文

config stp mst_config_id {revision_level <int 0-65535> | name <string 1-32>}

説明

MST コンフィグレーション ID の名前またはリビジョンレベルを変更します。デフォルトコンフィグレーション名はスイッチの MAC アドレスです。

パラメータ

パラメータ	説明
revision_level <int 0-65535>	0-65535 の値を入力し、MSTP 範囲を識別します。本値は「name」と共に、スイッチに設定した MSTP リージョンを識別します。初期値は 0 です。
name <string 1-32>	32 文字以内の半角英数字の文字列を入力して、スイッチの MSTP 範囲を識別します。本値は revision_level と共に、スイッチに設定した MSTP リージョンを識別します。「name」が入力されないと、デフォルト名はデバイスの MAC アドレスになります。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

MST コンフィグレーション ID の名前とリビジョンレベルを変更します。

```
DGS-3200-10:4#config stp mst_config_id name R&D_BlockG revision_level 1
Commands: config stp mst_config_id name R&D_BlockG revision_level 1

Success.

DGS-3200-10:4#
```

enable stp

目的

スイッチの STP をグローバルに有効にします。初期値では無効になっています。

構文

enable stp

説明

スイッチの STP をグローバルに有効にします。

パラメータ

なし。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

スイッチの STP をグローバルに有効にします。

```
DGS-3200-10:4#enable stp
Command: enable stp

Success.

DGS-3200-10:4#
```

disable stp

目的

スイッチの STP をグローバルに無効にします。（初期値）

構文

disable stp

説明

スイッチの STP をグローバルに無効にします。

パラメータ

なし。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

スイッチの STP をグローバルに無効にします。

```
DGS-3200-10:4#disable stp
Command: disable stp

Success.

DGS-3200-10:4#
```

config stp version

目的

スイッチの STP バージョンをグローバルに設定します。

構文

config stp version [mstp | rstp | stp]

説明

STP バージョンを設定します。初期値は RSTP です。

パラメータ

パラメータ	説明
mstp	MSTP がグローバルに使用されます。
rstp	RSTP がグローバルに使用されます。
stp	STP がグローバルに使用されます。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

スイッチに MSTP をグローバルに設定します。

```
DGS-3200-10:4#config stp version mstp
Command: config stp version mstp

Success.

DGS-3200-10:4#
```

config stp priority

目的

MSTI に MSTP に関連付ける優先度を設定します。

構文

config stp priority <value 0-61440> instance_id <value 0-15>

説明

MSTI に MSTP に関連付ける優先度を設定します。

パラメータ

パラメータ	説明
priority <value 0-61440>	0-61440 の値を選択し、送信パケットに対して指定されたインスタンス ID に優先度を指定します。数字が低いほど、優先度は高くなります。このエントリは 4096 の倍数とする必要があります。
instance_id <value 0-15>	異なる STP インスタンス間の識別子です。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

instance_id 0 に対する優先度値に 61440 を指定します。

```
DGS-3200-10:4#config stp priority 61440 instance_id 0
Command: config stp priority 61440 instance_id 0

Success.

DGS-3200-10:4#
```

config stp

目的

スイッチに STP ステータスを設定します。

構文

config stp {maxage <value 6-40> | maxhops <value 6-40> | hellotime <value 1-2> | forwarddelay <value 4-30> | txholdcount <value 1-10> | fbpdu [enable | disable]}

説明

スイッチに MSTP ステータスを設定します。

パラメータ

パラメータ	説明
maxage <value 6-40>	本値は古い情報がネットワーク内の冗長パスを永遠に循環し、新しい有効な情報の伝播を妨げるのを防ぐために設定します。ルートブリッジによりセットされるこの値は、スイッチと他の Bridged LAN（ブリッジで相互接続された LAN）内のデバイスが持っているスパニングツリー設定値が矛盾していないかを確認するための値です。本値が経過した時にルートブリッジからの BPDU パケットが受信されていなければ、スイッチは自分で BPDU パケットを送信し、ルートブリッジになる許可を得ようとします。この時点でスイッチのブリッジ識別番号が一番小さければ、スイッチはルートブリッジになります。6-40 の範囲から指定します。初期値は 20 です。
maxhops <value 1-20>	スイッチが送信した BPDU パケットが破棄される前のスパニングツリー範囲内のデバイス間のホップ数を設定します。値が 0 に到達するまで、各スイッチは 1 つずつホップカウントを減らしていきます。スイッチは、その後 BPDU パケットを破棄し、ポートに保持していた情報を解放します。ホップカウントは 1-20 で指定します。初期値は 20 です。
hellotime <value 1-2>	STP のルートデバイス、または RSTP の代表ルータによるコンフィグレーションメッセージの送信間隔を 1-2（秒）で設定します。このようにして、スイッチがまだ機能していることをと通知します。初期値は 2（秒）です。 MSTP では、スパニングツリーがポートごとに設定されるため、MSTP を使用するスイッチには「config stp ports」コマンドを使用して hellotime が設定される必要があります。
forwarddelay <value 4-30>	状態を変更する前にルートデバイスが待機する最大時間（4-30 秒）。初期値は 15（秒）です。
txholdcount <value 1-10>	間隔ごとに送信される BPDU Hello パケットの最大数。初期値は 3（秒）です。
fbpdu [enable	disable]	STP を無効にすると、STP BPDU パケットが他のネットワークデバイスから送信されます。初期値は「enable」です。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

STP を設定します。

```
DGS-3200-10:4#config stp maxage 10 maxhops 6 forwarddelay 15
Command: config stp maxage 10 maxhops 6 forwarddelay 15

Success.

DGS-3200-10:4#
```

config stp ports

目的

ポートレベルで STP を設定します。

構文

config stp ports <portlist> {externalCost [auto | <value 1-200000000>] | hellotime <value 1-2> | migrate [yes | no] | edge [true | false |auto] | restricted_role [true | false] | restricted_tcn [true | false] | p2p [true | false | auto] | state [enable | disable] | fbpdu [enable | disable]}

説明

Internal Path Cost と Port Priority を除くポートパラメータのすべてを設定します。2 つのパラメータ（Internal Path Cost と Port Priority）は、MSTP の特別なケースであり、使用するためには「config stp mst_ports」コマンドを使用します。

パラメータ

パラメータ	説明
<portlist>	表示するポートまたは範囲を指定します。CLI Value タイプの 1 つであり、ポートの入力値とフォーマットを制限します。
externalCost [auto|<value 1-200000000>]	設定対象のポートに対し、パケット送信のためのコストを表すメトリックを定義します。ポートコストは、自動設定、あるいは手動でメトリック値を指定できます。CIST レベルに使用されます。初期値は「auto」です。 • auto - 指定したポートに対して、最適なパケット送信スピードを自動的に設定します。デフォルトポートコスト : 100Mbps ポートの場合は 200000、ギガビットポートの場合は 20000。 • <value 1-200000000> - 1-200000000 の範囲から指定します。小さい数字を指定すると、パケット送出ポートとして選出される確率が上がります。
hellotime <value 1-2>	指定ポートが Bridged LAN（ブリッジにより接続される LAN）上の他のデバイスに Configuration メッセージを送信する間隔。このようにして、スイッチがまだ機能していることをと通知します。1-2（秒）の範囲から指定します。初期値は 2（秒）です。
migrate [yes | no]	「yes」を設定すると、STP 設定に関する情報をリクエストする他のブリッジに BPDU パケットをポートが送信するように設定します。スイッチが RSTP に設定されると、ポートは 802.1D STP から 802.1w RSTP まで移行することができます。スイッチが MSTP に設定されると、ポートは 802.1D STP から 802.1s MSTP まで移行することができます。RSTP と MSTP は標準の STP と共存できますが、RSTP と MSTP の利点は 802.1D ネットワークが 802.1w または 802.1s が有効なネットワークに接続するポート上では実現されません。セグメントのすべてまたは一部において 802.1w RSTP または 802.1s にアップグレード可能なネットワークステーションまたはセグメントに接続したポートでは本パラメータを「yes」とします。
edge [true | false | auto]	• true - 選択ポートをエッジポートとして指定します。しかし、トポロジの変更によってループ発生の可能性が生じると、エッジポートはエッジポートとしての資格を失います。エッジポートは通常 BPDU パケットを受け取りません。もし、BPDU パケットが受信されると、そのポートはエッジポートの資格を失います。 • false - そのポートにエッジポートの資格がないことを示しています。 • auto - 指定したポートに対して適切に設定します。「auto」モードでは、ブリッジ BPUD を受信しないと、ブリッジは、エッジポートになる期間を遅らせます。（初期値）
restricted_role [true | false]	• true - CIST またはすべての MSTI に対して、ポートはルートポートとして選択されなくなり、最適なスパニングツリープライオリティの要素を持ちます。このようなポートは、ルートポートが選択されると、代理のポートとして選択されます。 • false - スパニングツリーのアクティブなトポロジに影響し、管理者の完全な制御下にないネットワークのコアリージョンに対する外部ブリッジを防ぐために設定します。選択するとスパニングツリーの接続性が低下します。（初期値）
restricted_tcn [true | false]	• true - ポートは、トポロジ変更通知または別のポートに対するトポロジ変更を伝達しません。 • false - スパニングツリーのアクティブなトポロジに変更を行うと不正確に学習されたステーションのロケーション情報が継続するなど接続性の一時的な低下が発生します。ブリッジが管理者の完全な制御下または MAC 操作による LAN 変更を頻繁に行うような環境下ではない場合、そのリージョン内のアドレスフラッシュを引き起こすなどのネットワークのコアリージョンに対する外部ブリッジを防ぎます。（初期値）
p2p [true | false | auto]	• true - 選択ポートを P2P ポートとして指定します。P2P ポートはエッジポートと似ていますが、P2P ポートは全二重モードでのみ動作する点で異なります。RSTP の特長は、エッジポート同様、P2P ポートは迅速に Forwarding 状態に遷移します。 • false - そのポートに P2P ポートの資格がないことを示しています。 • auto - ポートはいつでも可能な時に（「true」を指定した時と同様に）P2P ポートとして動作します。 ポートの資格を失う時（例えば、半二重モードを指定された時など）、自動的に「false」を指定した時と同様になります。初期値は「auto」です。
state [enable | disable]	ポートリストに指定されたポートに STP 機能を「enable」（有効）または「disable」（無効）にします。初期値は「enable」です。
fbpdu [enable | disable]	本パラメータを有効にすると、STP がポートで無効である場合に STP BPDU パケットが他のネットワークデバイスから送信されます。初期値は「enable」（有効）です。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

STP ポートを設定します。

```
DGS-3200-10:4#config stp ports 1 externalCost auto
Command: config stp ports 1 externalCost auto

Success.

DGS-3200-10:4#
```

config stp mst_ports

目的

MSTP インスタンスのポート設定を更新します。

構文

config stp mst_ports <portlist> instance_id <value 0-15> {internalCost [auto | <value 1-200000000>] | priority <value 0-240>}

説明

STP instance_id のポート設定を更新します。ループが発生すると、MSTP 機能はポートプライオリティを使用して、Forwarding 状態に遷移させるインタフェースを選択します。最初に選択させたいインタフェースには高いプライオリティ（小さい数値）を与え、最後に選択させたいインタフェースには低いプライオリティ（大きい数値）を与えます。プライオリティ値が同じインスタンスでは、MSTP 機能は最小のポート番号を Forwarding 状態にし、他のインタフェースをブロックします。低優先度値がフォワーディングパケットのために、より高いプライオリティを意味することにご注意ください。

パラメータ

パラメータ	説明
<portlist>	設定するポートまたはポート範囲を指定します。
instance_id <value 0-15>	スイッチに設定済みの instance_id を識別するために 1-15 の範囲から指定します。0 のエントリは CIST（Common and Internal Spanning Tree）を示します。
internalCost	インタフェースが STP インスタンス内で選択される場合、指定ポートへの送信パケットの相対的なコストを設定します。初期値は「auto」です。 • auto - インタフェースに自動的に最適な最速ルートを設定します。初期値はインタフェースのメディアスピードに基づきます。 • 1-2000000 - ループが発生した場合、1-2000000 の範囲の値を持つコストを使用して最速ルートを設定します。コストが小さいほど高速で伝送されます。
priority <value 0-240>	ポートインタフェースのプライオリティを 0-240 の範囲から指定します。最初に選択させたいインタフェースには高いプライオリティ（小さい数値）を与え、最後に選択させたいインタフェースには低いプライオリティ（大きい数値）を与えます。16 の倍数で指定します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

STP MST ポートを設定します。

```
DGS-3200-10:4#config stp mst_ports 1 instance_id 0 internalCost auto
Command: config stp mst_ports 1 instance_id 0 internalCost auto

Success.

DGS-3200-10:4#
```

config stp trap

目的

STP トラップの送信ステータスを設定します。

構文

config stp trap {new_root [enable | disable] topo_change [enable | disable]}

説明

STP トラップの送信ステータスを設定します。

パラメータ

パラメータ	説明
new_root [enable | disable]	新しいルートトラップの送信を有効または無効にします。初期値は有効です。
topo_change [enable | disable]	トポロジチェンジトラップの送信を有効または無効にします。初期値は有効です。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

STP トラップの送信ステータスを設定します。

```
DGS-3200-10:4#config stp trap new_root disable
Command: config stp trap new_root disable

Success.

DGS-3200-10:4#
```

第 20 章　レイヤ 2 フォワーディングデータベースコマンド

コマンドラインインタフェース（CLI）におけるレイヤ 2 フォワーディングデータベースコマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
create fdb	<vlan_name 32> <macaddr> port <port>
create multicast_fdb	<vlan_name 32> <macaddr>
config multicast_fdb	<vlan_name 32> <macaddr> [add | delete] <portlist>
config fdb aging_time	<sec 10-875>
config multicast vlan_filtering_mode	[vlanid <vidlist>| vlan <vlan_name 32> |all] [forward_unregistered_groups|filter_unregistered_groups]
delete fdb	<vlan_name 32> <macaddr>
clear fdb	[vlan <vlan_name 32> | port <port> | all]
show multicast_fdb	{vlan <vlan_name 32> | mac_address <macaddr>}
show fdb	{port <port> | vlan <vlan_name 32> | mac_address <macaddr> | static | aging_time}
show multicast vlan_filtering_mode	{vlanid <vidlist>|vlan <vlan_name 32>}

以下のセクションで各コマンドについて詳しく記述します。

create fdb

目的

ユニキャスト MAC アドレスフォワーディングテーブル（データベース）にスタティックなエントリを作成します。

構文

create fdb <vlan_name 32> <macaddr> port <port>

説明

ユニキャスト MAC アドレスフォワーディングテーブル（データベース）にエントリを作成します。

パラメータ

パラメータ	説明
<vlan_name 32>	MAC アドレスが存在する VLAN 名。半角英数字 32 文字以内。
<macaddr>	フォワーディングテーブルに追加される MAC アドレス。
port<port>	宛先 MAC アドレスに対応するポート番号を入力します。スイッチはこのポートを通じ、いつも指定されたデバイスにトラフィックを送信します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

ユニキャスト MAC アドレスフォワーディングテーブルを作成します。

```
DGS-3200-10:4#create fdb default 00-00-00-00-01-02 port 5
Command: create fdb default 00-00-00-00-01-02 port 5

Success.

DGS-3200-10:4#
```

create multicast_fdb

目的

マルチキャスト MAC アドレスフォワーディング（データベース）にスタティックなエントリを作成します。

構文

create multicast_fdb <vlan_name 32> <macaddr>

説明

マルチキャスト MAC アドレスフォワーディングテーブル（データベース）にエントリを作成します。

パラメータ

パラメータ	説明
<vlan_name 32>	MAC アドレスが存在する VLAN 名。
<macaddr>	スタティックフォワーディングテーブルに追加される MAC アドレス。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

マルチキャスト MAC フォワーディングを作成します。

```
DGS-3200-10:4#create multicast_fdb default 01-00-5E-00-00-00
Command: create multicast_fdb default 01-00-5E-00-00-00

Success.

DGS-3200-10:4#
```

config multicast_fdb

目的

スイッチのマルチキャスト MAC アドレスフォワーディングデータベースを設定します。

構文

config multicast_fdb <vlan_name 32> <macaddr> [add | delete] <portlist>

説明

マルチキャスト MAC アドレスフォワーディングテーブルを設定します。

パラメータ

パラメータ	説明
<vlan_name 32>	MAC アドレスが存在する VLAN 名。半角英数字 32 文字以内。
<macaddr>	マルチキャストフォワーディングテーブルに追加または削除される MAC アドレス。
[add | delete]	• add - ポートをテーブルに追加します。 • delete - マルチキャストフォワーディングテーブルからポートを削除します。
<portlist>	表示するポートまたは範囲を指定します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

マルチキャスト MAC フォワーディングを追加します。

```
DGS-3200-10:4#config multicast_fdb default 01-00-5E-00-00-00 add 1-5
Command: config multicast_fdb default 01-00-5E-00-00-00 add 1-5

Success.

DGS-3200-10:4#
```

config fdb aging_time

目的

フォワーディングデータベースのエージングタイムを設定します。

構文

config fdb aging_time <sec 10-875>

説明

ダイナミックユニキャスト MAC アドレスフォワーディングテーブル（データベース）にエージングタイムを設定します。

エージングタイムは、スイッチの学習プロセスに影響します。送信元 MAC アドレスと対応するポート番号で構成されるダイナミックフォワーディングテーブルエントリが、エージングタイム内にアクセスされないと、テーブルから削除されます。エージングタイムは 10-875 秒で指定します。エージングタイムが非常に長い場合、古いか既に存在しないダイナミックフォワーディングテーブルエントリとなってしまします。これはスイッチに不正確なパケット転送決定を引き起こす可能性があります。しかし、エージングタイムが短すぎると、多くのエントリが非常に早く削除されてしまいます。これは送信元アドレスがフォワーディングテーブルで見つけられないパケットを受信する高い確率をもたらし、その場合、スイッチはすべてのポートにパケットをブロードキャストするため、スイッチが持つ利点の多くを無駄にしてしまいます。

パラメータ

パラメータ	説明
<sec 10-875>	ダイナミックに学習された MAC アドレスが、データベーステーブルから削除される前にアクセスされないでスイッチの MAC アドレスフォワーディングテーブルに保持される時間（秒）を設定します。10-875（秒）。初期値は 300（秒）です。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

MAC アドレスエージングタイムを設定します。

```
DGS-3200-10:4#config fdb aging_time 300
Command: config fdb aging_time 300

Success.

DGS-3200-10:4#
```

config multicast vlan_filtering_mode

目的

指定した VLAN にマルチキャストパケットフィルタリングモードを設定します。

構文

config multicast vlan_filtering_mode [vlanid <vidlist>| vlan <vlan_name 32> |all] [forward_unregistered_groups|filter_unregistered_groups]

説明

指定した VLAN のスイッチにマルチキャストパケットフィルタリングモードを設定します。

パラメータ

パラメータ	説明
vlanid <vidlist>	設定する VLAN ID リストを指定します。
vlan <vlan_name 32>	設定を行う VLAN に VLAN 名を指定します。
all	すべての VLAN に適用されます。
forward_unregistered_groups	未登録のグループを送信します。
filter_unregistered_groups	未登録のグループをフィルタします。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

すべての VLAN で未登録のグループをフィルタするために、マルチキャストフィルタリングモードを設定します。

```
DGS-3200-10:4#config multicast vlan_filtering_mode all forward_unregistered_groups
Command: config multicast port filtering_mode all forward_unregistered_groups

Success.

DGS-3200-10:4#
```

delete fdb

目的

スイッチのフォワーディングデータベースのエントリを削除します。

構文

delete fdb <vlan_name 32> <macaddr>

説明

スイッチの MAC アドレスフォワーディングデータベースのエントリを削除します。

パラメータ

パラメータ	説明
<vlan_name 32>	MAC アドレスが存在する VLAN 名。
<macaddr>	マルチキャストフォワーディングテーブルから削除される MAC アドレス。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

パーマネント FDB エントリを削除します。

```
DGS-3200-10:4#delete fdb default 00-00-00-00-01-02
Command: delete fdb default 00-00-00-00-01-02

Success.

DGS-3200-10:4#
```

clear fdb

目的

すべてのダイナミックに学習された MAC アドレスをスイッチのフォワーディングデータベースから削除します。

構文

clear fdb [vlan <vlan_name 32> | port <port> | all]

説明

スイッチのフォワーディングデータベースにダイナミックに学習されたエントリをクリアします。

パラメータ

パラメータ	説明
vlan <vlan_name 32>	MAC アドレスが存在する VLAN 名。
port<port>	宛先 MAC アドレスに対応するポート番号を入力します。
all	フォワーディングデータベースのすべてのダイナミックエントリをクリアします。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

スイッチの FDB ダイナミックエントリをクリアします。

```
DGS-3200-10:4#clear fdb all
Command: clear fdb all

Success.

DGS-3200-10:4#
```

show multicast_fdb

目的

スイッチのマルチキャストフォワーディングデータベースの内容を表示します。

構文

show multicast_fdb { vlan <vlan_name 32> | mac_address <macaddr>}

説明

マルチキャスト MAC アドレスフォワーディングデータベースの現在の内容を表示します。

パラメータ

パラメータ	説明
vlan <vlan_name 32>	MAC アドレスが存在する VLAN 名。
mac_address <macaddr>	フォワーディングテーブルにある MAC アドレス。

パラメータを指定しないと、すべてのマルチキャスト FDB エントリを表示します。

制限事項

なし。

使用例

マルチキャスト MAC アドレステーブルを表示します。

```
DGS-3200-10:4#show multicast_fdb vlan default
Command: show multicast_fdb vlan default

VLAN Name    :default
MAC Address  :01-00-5E-00-00-00
Egress Ports :1-5
Mode         :Static

Total Entries :1

DGS-3200-10:4#
```

show fdb

目的

現在のユニキャスト MAC アドレスフォワーディングデータベースを表示します。

構文

show fdb {port <port> | vlan <vlan_name 32> | mac_address <macaddr> | static | aging_time}

説明

現在のユニキャスト MAC アドレスフォワーディングデータベースを表示します。

パラメータ

パラメータ	説明
port <port>	宛先 MAC アドレスに対応するポート番号を入力します。スイッチはこのポートを通じ、いつも指定されたデバイスにトラフィックを送信します。
vlan <vlan_name 32>	指定 VLAN のエントリを表示します。
mac_address<macaddr>	指定 MAC アドレスのエントリを表示します。
static	すべてのパーマネントエントリを表示します。
aging_time	ユニキャスト MAC アドレスのエージングタイムを表示します。

パラメータが指定されないと、システムはすべてのユニキャスト MAC アドレステーブルを表示します。

制限事項

なし。

使用例

ユニキャスト MAC アドレステーブルを表示します。

```
DGS-3200-10:4#show fdb
Command: show fdb

Unicast MAC Address Aging Time = 300

VID VLAN Name MAC Address        Port Type
--- --------- -----------------  ---- ---------
1   default   00-00-00-00-01-02  5    Permanent
1   default   00-01-02-03-04-00  CPU  Self

Total Entries :2

DGS-3200-10:4#
```

show multicast vlan_filtering_mode

目的

VLAN に設定されているマルチキャストパケットフィルタリングモードを表示します。

構文

show multicast vlan_filtering_mode {[vlanid <vidlist>|vlan <vlan_name 32>]}

説明

指定した VLAN またはすべての VLAN に対するスイッチの現在のマルチキャストパケットフィルタリングモードを表示します。

パラメータ

パラメータ	説明
vlanid <vidlist>	表示する VLAN ID リストを指定します。
vlan <vlan_name 32>	マルチキャストフィルタリングステータスを表示する VLAN を指定します。

制限事項

なし。

使用例

すべての VLAN に対するマルチキャストフィルタリングモードを表示します。

```
DGS-3200-10:4#show multicast vlan_filtering_mode
Command: show multicast vlan_filtering_mode

VLAN Name     Multicast Filter Mode
---------     -------------------------
default       filter_unregistered_groups

DGS-3200-10:4#
```

第 21 章　MAC 通知コマンド

MAC Notification（通知）は、学習によりフォワーディングデータベースに記録された MAC アドレスの監視を行うために使用します。

注意 本機能をご使用になる場合、NMS 側で MAC Notification Trap を受信できる環境が必要になります。E-mail や Syslog での通知には対応しておりません。

コマンドラインインタフェース（CLI）における MAC 通知コマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
enable mac_notification	
disable mac_notification	
config mac_notification	{interval <int 1-2147483647> | historysize <int 1-500>}
config mac_notification ports	[<portlist> | all] [enable | disable]
show mac_notification	
show mac_notification ports	<portlist>

以下のセクションで各コマンドについて詳しく記述します。

enable mac_notification

目的
　スイッチでグローバルな MAC アドレステーブル通知を有効にします。
構文
　enable mac_notification
説明
　設定変更せずに、MAC アドレス通知を有効にします。
パラメータ
　なし。
制限事項
　管理者レベルユーザのみ本コマンドを実行できます。
使用例
　基本設定を変更しないで、MAC 通知を有効にします。

```
DGS-3200-10:4#enable mac_notification
Command: enable mac_notification

Success.

DGS-3200-10:4#
```

disable mac_notification

目的
　スイッチでグローバルな MAC アドレステーブル通知を無効にします。
構文
　disable mac_notification
説明
　設定を変更せずに、MAC アドレス通知を無効にします。
パラメータ
　なし。
制限事項
　管理者レベルユーザのみ本コマンドを実行できます。
使用例
　基本設定を変更しないで、MAC 通知を無効にします。

```
DGS-3200-10:4#disable mac_notification
Command: disable mac_notification

Success.

DGS-3200-10:4#
```

config mac_notification

目的

MAC アドレス通知を設定します。

構文

config mac_notification {interval <int 1-2147483647> | historysize <int 1-500>}

説明

MAC アドレス通知を設定します。

パラメータ

パラメータ	説明
interval <int 1-2147483647>	通知間隔（秒）。間隔は 1-2147483647（秒）から選択します。
historysize <1-500>	通知に使用されるヒストリログに一覧表示されるエントリの最大数。最大 500 のエントリを指定できます。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

スイッチの MAC アドレステーブル通知のグローバルパラメータを設定します。

```
DGS-3200-10:4#config mac_notification interval 1 historysize 500
Command: config mac_notification interval 1 historysize 500

Success.

DGS-3200-10:4#
```

config mac_notification ports

目的

MAC アドレス通知状態を設定します。

構文

config mac_notification ports [<portlist> | all] [enable | disable]

説明

MAC アドレス通知状態を設定します。

パラメータ

パラメータ	説明
<portlist> | all	設定するポートまたはポート範囲を指定します。「all」はシステムのすべてのポートを設定します。
[enable | disable]	• enable - ポートの MAC アドレステーブル通知を有効にします。 • disable - ポートの MAC アドレステーブル通知を無効にします。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

ポート 7 の MAC アドレステーブル通知を有効にします。

```
DGS-3200-10:4#config mac_notification ports 7 enable
Command: config mac_notification ports 7 enable

Success.

DGS-3200-10:4#
```

show mac_notification

目的
　スイッチの MAC アドレステーブル通知のグローバルパラメータを表示します。
構文
　show mac_notification
説明
　スイッチの MAC アドレステーブル通知のグローバルパラメータを表示します。
パラメータ
　なし。
制限事項
　なし。
使用例
　MAC アドレステーブル通知のグローバル設定を表示します。

```
DGS-3200-10:4#show mac_notification
Command: show mac_notification

Global Mac Notification Settings

State           : Enabled
Interval        : 1
History Size    : 500

DGS-3200-10:4#
```

show mac_notification ports

目的
　スイッチの MAC アドレステーブル通知状態の設定を表示します。
構文
　show mac_notification ports <portlist>
説明
　スイッチの MAC アドレステーブル通知状態の設定を表示します。
パラメータ

パラメータ	説明
<portlist>	設定するポートまたはポート範囲を指定します。パラメータなしでこのコマンドを入力すると、全ポートに対する MAC 通知テーブルを表示します。

制限事項
　なし
使用例
　すべての MAC アドレステーブル通知状態の設定を表示します。

```
DGS-3200-10:4#show mac_notification ports 1-10
Command: show mac_notification ports 1-10

Port #  MAC Address Table Notification State
------  ----------------------------------
1                 Disabled
2                 Disabled
3                 Disabled
4                 Disabled
5                 Disabled
6                 Disabled
7                 Disabled
8                 Disabled
9                 Disabled
10                Disabled

CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

第 22 章　ポートミラーリングコマンド

スイッチはポート上で送受信したフレームをコピーし、別のポートに転送します。スニファーや RMON probe のようなモニタデバイスをミラーポートに接続し、最初のポートを通過するパケット情報を参照できます。ネットワーク監視とトラブルシューティングの目的で使用します。

コマンドラインインタフェース（CLI）におけるポートミラーリングコマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
config mirror port	<port> [add | delete] source ports <portlist> [rx | tx | both]
enable mirror	
disable mirror	
show mirror	

以下のセクションで各コマンドについて詳しく記述します。

config mirror port

目的

スイッチにミラーポートとソースポートのペアを設定します。どのソースポートからターゲットポートまでのトラフィックもリアルタイム分析のためにミラーリングできます。ロジックアナライザや RMON プローブを接続し、ソースポートを通過するトラフィックを調べることができます。

構文

config mirror port <port> [add | delete] source ports <portlist> [rx | tx | both]

説明

ポート範囲は、代表ポートに送信されるすべてのトラフィックを持つことが可能で、ネットワークスニファーや他のデバイスがネットワークトラフィックをモニタすることができます。さらに、1 方向または両方向に送受信されるトラフィックだけがターゲットポートにミラーリングされるような指定も可能です。

パラメータ

パラメータ	説明
<port>	ミラーされたパケットを受信するターゲットポート指定します。ターゲットポートは、ソースポートと同じ VLAN に設定され、ソースポートと同じ速度で動作する必要があります。ターゲットポートがより低速で動作していると、ソースポートは、ターゲットポートに一致するように動作速度を落とします。
[add | delete]	ソースポートパラメータに設定されるミラーポートの追加または削除をします。
source ports <portlist>	ミラーされるポート（範囲）を指定します。これにはターゲットポートを含むことはできません。
rx	ポートまたはポートリスト内のポートが受信するパケットだけをミラーリングします。
tx	ポートまたはポートリスト内のポートが送信するパケットだけをミラーリングします。
both	ポートまたはポートリスト内のポートが送受信するすべてのパケットをミラーリングします。

制限事項

ターゲットポートはソースポートにはできません。管理者レベルユーザのみ本コマンドを実行できます。

使用例

ミラーリングポートを追加します。

```
DGS-3200-10:4#config mirror port 5 add source ports 1-4 both
Command: config mirror port 5 add source ports 1-4 both

Success.

DGS-3200-10:4#
```

enable mirror

目的

入力したポートミラーリング設定を有効にします。

構文

enable mirror

説明

本コマンドは以下の「disable mirror」と組み合わせて、スイッチにポートミラーリング設定を入力した後に、設定を変更せずにミラーリングを有効または無効にすることができます。

注意　ターゲットポートが設定されていないと、本コマンドは使用できません。

パラメータ
　なし。
制限事項
　管理者レベルユーザのみ本コマンドを実行できます。
使用例
　ミラーリング設定を有効にします。

```
DGS-3200-10:4#enable mirror
Command: enable mirror

Success.

DGS-3200-10:4#
```

disable mirror

目的
　設定したポートミラーリング設定を無効にします。
構文
　disable mirror
説明
　本コマンドは以下の「enable mirror」と組み合わせて、スイッチにポートミラーリング設定を入力した後に、設定を変更せずにミラーリングを有効または無効にすることができます。
パラメータ
　なし。
制限事項
　管理者レベルユーザのみ本コマンドを実行できます。
使用例
　ミラーリング設定を無効にします。

```
DGS-3200-10:4#disable mirror
Command: disable mirror

Success.

DGS-3200-10:4#
```

show mirror

目的
　スイッチの現在のポートミラーリング設定を表示します。
構文
　show mirror
説明
　スイッチの現在のポートミラーリング設定を表示します。
パラメータ
　なし。
制限事項
　なし。
使用例
　ミラーリング設定を表示します。

```
DGS-3200-10:4#show mirror
Command: show mirror

Current Settings
Mirror Status :Disabled
Target Port   :7
Mirrored Port
            RX:
            TX:1-5

DGS-3200-10:4#
```

第 23 章　VLAN コマンド

IEEE 802.1p プライオリティについて

プライオリティのタグ付けは、IEEE 802.1p 標準規格で定義され、何種類ものデータが同時に送受信されるようなネットワーク内のトラフィックを管理するための方法です。本機能は混雑したネットワーク上でのタイムクリティカルなデータの伝送時に発生する問題を解決するために開発されました。例えばビデオ会議のような、データに依存するタイプのアプリケーションの品質は、ほんの少しの伝送遅延にも多大な影響を受けてしまいます。

IEEE 802.1p 標準規格に準拠するネットワークデバイスは、データパケットのプライオリティレベル（優先度）を認識することができます。また、これらのデバイスはパケットに対してプライオリティレベルやタグを割り当てることができ、パケットからタグを取り外すことも可能です。このプライオリティタグ（優先タグ）は、パケットの緊急度を決定し、またそのパケットがどのキューに割り当てられるかを決定します。

プライオリティタグは、0 から 7 までの値で示され、0 が最も低い優先度、7 が最も高い優先度を表します。一般的に、7 番のプライオリティタグは、少しの遅延にも影響されやすい音声や映像に関わるデータに対して、またはデータ転送速度が保証されているような特別なユーザに対して使用されます。プライオリティを与えられないパケットはキュー 0 に割り当てられ、最も低い送信優先度となります。

スイッチは Strict モードと WRR（重み付けラウンドロビン）システムをサポートし、それによりキューからパケットを送信する速度を決定します。速度の対比は 4 : 1 と設定されています。これは、最高のプライオリティのキュー（キュー 7）が 4 つのパケットを送信する間に、キュー 0 では 1 つのパケットを送信することを意味しています。

プライオリティキューの設定はスイッチ上のすべてのポートに対して行われるため、スイッチに接続されるすべてのデバイスがその影響を受けることに注意してください。このプライオリティキューイングシステムは、ご使用のネットワークがプライオリティタグ割り当て機能をサポートする場合、この機能は特にその効果を発揮します。

VLAN について

VLAN（Virtual Local Area Network : 仮想 LAN）とは、物理的なレイアウトではなく、論理的なスキームに従って構成されるネットワークトポロジです。VLAN は LAN セグメントの集まりを自律的なユーザグループへと結合させて、1 つの LAN のように見せるために使用します。また VLAN は VLAN 内のポート間にのみパケットが送信されるように、ネットワークを異なるブロードキャストドメインに論理的に分割します。一般的には 1 つの VLAN は 1 つのサブネットと関連付けられますが、必ずしもそうである必要はありません。

VLAN では、帯域を浪費せずにパフォーマンスを強化し、トラフィックを特定のドメイン内に制限することにより、セキュリティを増強します。

VLAN はエンドノードを物理的位置ではなく、論理的に束ねた集合体です。頻繁に通信を行うエンドノード同士は、それらのネットワーク上の物理的位置に関わらず、同じ VLAN を割り当てます。論理的には、VLAN とブロードキャストドメインは等しいと言えます。これは、ブロードキャストパケットはブロードキャストが行われた VLAN 内のメンバにのみ送信されるためです。

本スイッチにおける VLAN について

本スイッチにおける VLAN の特長は以下の通りです。

- どんな方法でエンドノードの識別を行い、エンドノードに VLAN メンバシップを割り当てたとしても、VLAN 間にルーティング機能を持つネットワークデバイスが存在しない限り、パケットは VLAN に所属しないポートに送信されることはありません。
- 本スイッチは IEEE 802.1Q VLAN をサポートします。ポートアンタギング機能は、パケットヘッダから 802.1Q タグを取り外すことにより、タグを理解しないデバイスとの互換性を保ちます。
- スイッチの初期状態では、すべてのポートに「default」と名付けられた 802.1Q VLAN が割り当てられています。
- 「default」VLAN の VID は 1 です。

コマンドラインインタフェース（CLI）における VLAN コマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
create vlan	<vlan_name 32> tag <vlanid 2-4094> {type [1q_vlan {advertisement} | private_vlan]}
create vlan	vlanid <vlanid_list> {type [1q_vlan | private_vlan] {advertisement}}
delete vlan	<vlan_name 32> | vlanid <vidlist>
config vlan	[vlanid<vidlist> | <vlan_name 32>] {[add [tagged | untagged | forbidden] | delete] <portlist> | advertisement [enable | disable]}
config gvrp	[<portlist> | all] {state [enable | disable] | ingress_checking [enable | disable] | acceptable_frame [tagged_only | admit_all] | pvid<vlanid 1-4094>}
enable gvrp	
disable gvrp	
show vlan	{<vlan_name 32> | vlanid<vidlist> | ports <portlist>}
show gvrp	{<portlist>}
enable pvid auto_assign	
disable pvid auto_assign	
show pvid auto_assign	
config private_vlan	[<vlan_name 32> | vid <vlanid 1-4094>] [add [isolated | community] | remove] [<vlan_name 32> | vlanid <vidlist>]
show private_vlan	{[vlan_name 32> | vlanid <vidlist>]}

以下のセクションで各コマンドについて詳しく記述します。

create vlan

目的

スイッチに VLAN を作成します。

構文

create vlan <vlan_name 32> tag <vlanid 2-4094> {type [1q_vlan {advertisement} | private_vlan]}

create vlan vlanid <vlanid_list> {type [1q_vlan | private_vlan] {advertisement}}

説明

スイッチに VLAN を作成します。VLAN を作成するためには VLAN ID を指定する必要があります。

パラメータ

パラメータ	説明
<vlan_name 32>	作成する VLAN 名。
vlanid <vlanid_list>	作成する VLAN の VLAN ID。
tag <vlanid 2-4094>	作成する VLAN の VLAN ID。2-4094 で指定します。
type	パケットヘッダの「type」フィールドを使用して、パケットのプロトコルと宛先 VLAN を決定します。 • 1q_vlan {advertisement} - 外への通知が可能であるとして VLAN を指定します。 • private_vlan - プライベート VLAN を作成します。最大 24 個のプライベート VLAN をスイッチに作成できます。 何も指定しないと作成済みの VLAN が通常の VLAN となります。
advertisement	通知を出すことができるように VLAN を指定します。

制限事項

各 VLAN 名は 32 文字以内で指定します。タグが VLAN に付与されない場合、それはポートベースの VLAN になります。管理者レベルユーザのみ本コマンドを実行できます。

使用例

VLAN「v2」、「VLAN ID 2」の VLAN を作成します。

```
DGS-3200-10:4#create vlan v2 tag 2 type 1q_vlan advertisement
Command: create vlan v2 tag 2 type 1q_vlan advertisement

Success.

DGS-3200-10:4#
```

VLAN「v3」、「VLAN ID 3」のプライベート VLAN を作成します。

```
DGS-3200-10:4#create vlan v3 tag 3 type private_vlan
Command: create vlan v3 tag 3 type private_vlan

Success.

DGS-3200-10:4#
```

delete vlan

目的

スイッチに設定済みの VLAN を削除します。

構文

delete vlan <vlan_name 32> | vlanid <vidlist>

説明

スイッチに設定済みの VLAN を削除します。802.1Q VLAN がプライベート VLAN として追加されている場合、削除することはできません。

パラメータ

パラメータ	説明
<vlan_name 32>	削除する VLAN 名。
vlanid <vidlist>	削除する VLAN の VLAN ID。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

VLAN「v1」を削除します。

```
DGS-3200-10:4#delete vlan v1
Command: delete vlan v1

Success.

DGS-3200-10:4#
```

config vlan

目的

設定済みの VLAN にポートを追加します。

構文

config vlan [vlanid<vidlist> | <vlan_name 32>] {[add [tagged | untagged | forbidden] | delete] <portlist> | advertisement [enable | disable]}

説明

設定済みの VLAN のポートリストにポートを追加します。タグ付き、タグなし、禁止ポートとして追加ポートを設定します。初期値は「untagged」（タグなし）としてポートを割り当てます。

パラメータ

パラメータ	説明
vlanid<vidlist>	ポートを追加する VLAN ID。
<vlan_name 32>	ポートを追加する VLAN 名。
add	VLAN にポートを追加します。追加するポートには 3 つのタイプがあります。 • tagged - 追加ポートをタグ付きとします。 • untagged - 追加ポートをタグなしとします。 • forbidden - 追加ポートを禁止ポートにします。
delete	指定した VLAN からポートを削除します。
<portlist>	指定した VLAN に（から）追加、または削除するポートまたは範囲を指定します。
advertisement [enable | disable]	指定 VLAN 上の GVRP を「enable」（有効）または「disable」（無効）にします。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

VLAN v1 にタグ付きポート（ポート 4-8）を追加します。

```
DGS-3200-10:4#config vlan v1 add tagged 4-8
Command: config vlan v1 add tagged 4-8

Success.

DGS-3200-10:4#
```

VLAN v1 からポート 4 から 8 を削除します。

```
DGS-3200-10:4#config vlan v1 delete 4-8
Command: config vlan v1 delete 4-8

Success.

DGS-3200-10:4#
```

VLAN デフォルト Advertisement を有効にします。

```
DGS-3200-10:4#config vlan default advertisement enable
Command: config vlan default advertisement enable

Success.

DGS-3200-10:4#
```

config gvrp

目的

スイッチに GVRP を設定します。

構文

config gvrp [<portlist> | all] {state [enable | disable] | ingress_checking [enable | disable] | acceptable_frame [tagged_only | admit_all] | pvid<vlanid 1-4094>}

説明

スイッチに GVRP を設定します。Ingress チェック、GVRP 情報の送受信、およびポート VLAN ID（PVID）を設定します。

パラメータ

パラメータ	説明
<portlist>	GVRP を有効にするポートまたは範囲を指定します。ポートの範囲は、「-」(ダッシュ) を使用して指定します。
all	スイッチのすべてのポートを指定します。
state [enable | disable]	ポートリストに指定されたポートに GVRP 機能を「enable」（有効）または「disable」（無効）にします。
ingress_checking [enable | disable]	指定ポートに対する Ingress チェックを「enable」（有効）または「disable」（無効）にします。
acceptable_frame [tagged_only | admit_all]	本機能のためにスイッチが受け入れるフレームタイプを示します。 • tagged_only - タグ付きの VLAN フレームだけを受け入れることを示します。 • admit_all - タグ付きおよびタグなしフレームを受け入れることを示します。
pvid <vlanid 1-4094>	ポートに関連するデフォルト VLAN ID を指定します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

Ingress チェック状態、GVRP 情報の送受信を設定します。

```
DGS-3200-10:4#config gvrp 5 gvrp_state enable ingress_checking enable acceptable_frame tagged_only
pvid 2
Command: config gvrp 5 gvrp_state enable ingress_checking enable acceptable_frame tagged_only pvid
2

Success.

DGS-3200-10:4#
```

enable gvrp

目的
　スイッチの GVRP を有効にします。
構文
　enable gvrp
説明
　スイッチの GVRP を有効にします。初期値は無効です。
パラメータ
　なし。
制限事項
　管理者レベルユーザのみ本コマンドを実行できます。
使用例
　GVRP を有効にします。

```
DGS-3200-10:4#enable gvrp
Command: enable gvrp

Success.

DGS-3200-10:4#
```

disable gvrp

目的
　スイッチの GVRP を無効にします。
構文
　disable gvrp
説明
　スイッチの GVRP を無効にします。
パラメータ
　なし。
制限事項
　管理者レベルユーザのみ本コマンドを実行できます。
使用例
　GVRP を無効にします。

```
DGS-3200-10:4#disable gvrp
Command: disable gvrp

Success.

DGS-3200-10:4#
```

show vlan

目的

スイッチの現在の VLAN 設定を表示します。

構文

show vlan {<vlan_name 32> | vlanid<vidlist> | ports {<portlist>}}

説明

VLAN ID、VLAN 名、タグ付き / タグなしステータス、および VLAN のメンバである各ポートの Member/Non-member/Forbidden ステータスを含む各 VLAN に関するサマリ情報を表示します。

パラメータ

パラメータ	説明
<vlan_name 32>	サマリ設定を表示する VLAN 名。
vlanid<vidlist	サマリ設定を表示する VLAN ID。
ports <portlist>	サマリ設定を表示するポート番号。

制限事項

なし。

使用例

スイッチの現在の VLAN 設定を表示します。

```
DGS-3200-10:4#show vlan
Command: show vlan

VID           :1                VLAN Name         :default
VLAN Type     :Static           Advertisement     :Enabled
Member Ports            :1-7
Static Ports            :1-6
Current Tagged Ports    :
Current Untagged Ports :1-7
Static Tagged Ports     :
Static Untagged Ports   :1-6
Forbidden Ports         :

Total Static VLAN Entries : 1
Total GVRP VLAN Entries   : 0

DGS-3200-10:4#
```

スイッチにおけるポート 6 の現在の VLAN 設定を表示します。

```
DGS-3200-10:4#show vlan ports 1-2
Command: show vlan ports 1-2

Port VID     Untagged Tagged Dynamic Forbidden
---- ------- -------- ------ ------- ---------
1    1       X        -      -       -
2    1       X        -      -       -

DGS-3200-10:4#
```

show gvrp

目的

スイッチのポートリストに対する GVRP ステータスを表示します。

構文

show gvrp {<portlist>}

説明

スイッチのポートリストに対する現在の GVRP ステータスを表示します。

パラメータ

パラメータ	説明
<portlist>	GVRP ステータスを表示するポートまたは範囲を指定します。パラメータが指定されないと、システムはすべてのポートの GVRP 情報を表示します。

制限事項

なし。

使用例

802.1q ポート設定を表示します。

```
DGS-3200-10:4#show gvrp 1-6
Command: show gvrp 1-6

Global GVRP :Enabled

Port PVID GVRP     Ingress Checking Acceptable Frame Type
---- ---- -------- ---------------- ----------------------
1    2    Enabled  Enabled          Only VLAN-tagged Frames
2    2    Enabled  Enabled          Only VLAN-tagged Frames
3    2    Enabled  Enabled          Only VLAN-tagged Frames
4    2    Enabled  Enabled          Only VLAN-tagged Frames
5    2    Enabled  Enabled          Only VLAN-tagged Frames
6    1    Disabled Enabled          All Frames

Total Entries :6

DGS-3200-10:4#
```

enable pvid auto_assign

目的

PVID の自動割り当てを有効にします。

構文

enable pvid auto_assign

説明

PVID の自動割り当てを有効にすると、PVID は PVID 設定または VLAN 設定で変更可能です。ポートを VLAN x のタグなしメンバに設定する場合、このポートの PVID は VLAN x に更新されます。VLAN コマンドでは、PVID は VLAN コマンド構文の最後のパラメータを指定することで更新されます。

PVID の VLAN におけるタグなしメンバからポートを削除すると、ポートの PVID は「default VLAN」に割り当てられます。初期値は有効です。

パラメータ

なし。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

PVID の自動割り当てを有効にします。

```
DGS-3200-10:4#enable pvid auto_assign
Command: enable pvid auto_assign

Success.

DGS-3200-10:4#
```

disable pvid auto_assign

目的
　PVID の自動割り当てを無効にします。
構文
　disable pvid auto_assign
説明
　PVID の自動割り当てを無効にすると、PVID はユーザによる PVID 設定だけで変更可能です。VLAN 設定により自動的に PVID を変更することはできません。初期値は有効です。
パラメータ
　なし。
制限事項
　管理者レベルユーザのみ本コマンドを実行できます。
使用例
　PVID の自動割り当てを無効にします。

```
DGS-3200-10:4#disable pvid auto_assign
Command: disable pvid auto_assign

Success.

DGS-3200-10:4#
```

show pvid auto_assign

目的
　PVID の自動割り当てステータスを表示します。
構文
　show pvid auto_assign
説明
　PVID の自動割り当てステータスを表示します。
パラメータ
　なし。
制限事項
　なし。
使用例
　PVID の自動割り当てステータスを表示します。

```
DGS-3200-10:4#show pvid auto_assign
Command: show pvid auto_assign

PVID Auto-assignment:  Enabled

DGS-3200-10:4#
```

config private_vlan

目的

プライベート VLAN に (から) セカンダリ VLAN を追加または削除します。

構文

config private_vlan [<vlan_name 32> | vid <vlanid 1-4094>] [add [isolated | community] | remove] [<vlan_name 32> | vlanid <vidlist>]

説明

プライベート VLAN に (から) セカンダリ VLAN を追加または削除します。

プライベート VLAN はプライマリ VLAN、Isolated VLAN、および多くのコミュニティ VLAN で作成されます。プライベート VLAN ID はプライマリ VLAN の VLAN ID によって示されます。
プライマリ VLAN の目的は、混在するポートから独立したコミュニティホストのポートまたは他の混在するポートに単方向のトラフィックのダウンストリームを転送することです。

本スイッチは 2 種類のセカンダリ VLAN とコミュニティ VLAN をサポートしています。プライマリ VLAN メンバポートは、同時にセカンダリ VLAN メンバであることはできません。また、逆もまた同様です。セカンダリ VLAN は、タグなしのメンバポートを含むことだけはできます。ポートは、同時に 1 つ以上のセカンダリ VLAN のメンバであることはできません。

パラメータ

パラメータ	説明
<vlan_name 32>	プライベート VLAN 名。
vid <vlanid 1-4094>	プライベート VLAN の VLAN ID。
add [isolated | community]	プライベート VLAN にセカンダリ VLAN を追加します。 • isolated - セカンダリ VLAN を Isolated VLAN になるように指定します。Isolated VLAN は、ポートに接続しているすべてのホストがレイヤ 2 で隔離されるという異なる特性を持つセカンダリ VLAN です。Isolated VLAN の第一の長所は、プライベート VLAN が 2 つの VLAN 識別子を使用するだけでポートの分離を行い、多くのエンドユーザにサービスを提供することができるということです。プライベート VLAN は、1 つの Isolated VLAN のみサポートしています。 • community - セカンダリ VLAN をコミュニティ VLAN とするように指定します。コミュニティ VLAN は、信頼関係を持つエンドデバイスの特定の「コミュニティ」に接続するポートグループに関連付けるセカンダリ VLAN です。プライベート VLAN ドメインには、複数の異なるコミュニティ VLAN が存在することができます。
remove	プライベート VLAN からセカンダリ VLAN を削除します。
<vlan_name 32> | vlanid <vidlist>	• <vlan_name 32> - プライベート VLAN に追加または削除するセカンダリ VLAN 名。 • <vidlist> - プライベート VLAN に追加または削除するセカンダリ VLAN の範囲。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

プライベート VLAN p1 にセカンダリ VLAN を関連させます。

```
DGS-3200-10:4#config private_vlan p1 add community vlanid 2-5
Command: config private_vlan p1 add community vlanid 2-5

Success.

DGS-3200-10:4#
```

show private_vlan

目的

プライベート VLAN の情報を表示します。

構文

show private_vlan {vlan <vlan_name 32> | vlanid <vidlist>}

説明

プライベート VLAN の情報を表示します。

パラメータ

パラメータ	説明
<vlan_name 32>	プライベート VLAN 名またはセカンダリ VLAN 名。
<vidlist>	プライベート VLAN またはセカンダリ VLAN の VLAN ID。

制限事項

なし。

使用例

プライベート VLAN の設定を表示します。

```
DGS-3200-10:4#show private_vlan
Command: show private_vlan

Private VLAN 100
-------------------------
     Promiscuous Ports: 1
     Trunk Ports      : 2
     Isolated Ports   : 3-5        Isolated VLAN : 20
     Community Ports  : 6-8        Community VLAN: 30
     Community Ports  : 9-10       Community VLAN: 40

Private VLAN 200
-------------------------
     Promiscuous Ports:
     Trunk Ports :

Total Entries: 2

DGS-3200-10:4#
```

第 24 章　プロトコル VLAN コマンド

本スイッチは、通常の VLAN 設定をはじめプロトコル VLAN など先進的な技術を利用することにより、ネットワークプロバイダは規模の大きい包括的な VLAN の中に、顧客用の VLAN を設置し、VLAN 構成に新しい階層を導入することで可能となり、その規模を拡張することができます。基本的には大規模な ISP のネットワーク内に、レイヤ 2 の VPN（Virtual Private Network）および、顧客用の透過型 LAN を配置することにより、クライアント側の構造を複雑にすることなく、複数の顧客の LAN を接続します。構造の複雑化が回避できるだけでなく、4000 以上の VLAN を定義できるようになるため、VLAN ネットワークを大幅に拡張することができます。

本機能は ISP VLAN 認識と分類のために既存の VLAN フレームに VLAN フレームを追加します。デバイス通知を確実にするため、tpid として知られているこの追加 VLAN フレーム（イーサネットカプセル化）が、さらにフレームに追加されます。デバイスは、この tpid を認識して、プロバイダ VLAN タグが追加されたかどうかを確認するために VLAN のタグ付きパケットをチェックします。その場合、パケットの宛先への迅速で信頼性の高いルーティングを保証するために、同様の設定を持つさらに小規模の VLAN を含むこのプロバイダ VLAN を経由してパケットは送信されます。

コマンドラインインタフェース（CLI）における VLAN コマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
create dot1v_protocol_group	group_id <id 1-8> {group_name <name 1-32>}
config dot1v_protocol_group	[group_id <id 1-8> | group_name <name 1-32>] add protocol [ethernet_2 | ieee802.3_snap | ieee802.3_llc] <protocol_value>
config dot1v_protocol_group	[group_id <id 1-8> | group_name <name 1-32>] delete protocol [ethernet_2 | ieee802.3_snap | ieee802.3_llc] <protocol_value>
delete dot1v_protocol_group	[group_id <id 1-8> | group_name <name 1-32> | all]
show dot1v_protocol_group	{group_id <id 1-8> | group_name <name 1-32>}
config port dot1v ports	[<portlist> | all] [add protocol_group [group_id <id 1-8> | group_name <name 1-32>] [vlan< vlan_name 32> | vlanid <vlanid 1-4094>] {priority <value 0-7>} | delete protocol_group [group_id <id 1-8> | all]]
show port dot1v	{ports <portlist>}

以下のセクションで各コマンドについて詳しく記述します。

create dot1v_protocol_group

目的

プロトコル VLAN のプロトコルグループを作成します。

構文

create dot1v_protocol_group group_id <id 1-8> {group_name <name 1-32>}

説明

プロトコル VLAN のプロトコルグループを作成します。

パラメータ

パラメータ	説明
group_id <id 1-8>	多くのプロトコルを識別するために使用されるプロトコルグループの ID。
group_name <name 1-32>	プロトコルグループ名（半角英数字 32 文字以内）。グループ名が指定されないと、「ProtocolGroup+group_id」というグループ名が自動的に生成されます。例えば、group_id が 2 の場合に自動生成される名前は、「ProtocolGroup2」となります。自動生成された名前が既存のグループと重複すると、「ProtocolGroup+group_id+ALT+num」という代替名が使用されます。「num」は 1 から開始します。さらに重複すると、その次の数が代わりに使用されます。 例 : group_id が 1 の場合に自動生成される名前は、「ProtocolGroup1」となります。この名前が既に存在していると、「ProtocolGroup1ALT1」が代わりに使用されます。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

プロトコル VLAN のプロトコルグループを作成します。

```
DGS-3200-10:4#create dot1v_protocol_group group_id 4 group_name General_Group
Command: create dot1v_protocol_group group_id 4 group_name General_Group

Success.

DGS-3200-10:4#
```

config dot1v_protocol_group add protocol

目的

プロトコルグループにプロトコルを追加します。

構文

config dot1v_protocol_group [group_id <id 1-8> | group_name <name 1-32>] add protocol [ethernet_2 | ieee802.3_snap | ieee802.3_llc] <protocol_value>

説明

プロトコルグループにプロトコルを追加します。プロトコルは、定義済みプロトコルタイプまたはユーザ定義プロトコルから選択します。

パラメータ

パラメータ	説明
group_id <id 1-8>	追加するグループ ID を指定します。
group_name <name 1-32>	プロトコルグループ名。
protocol [ethernet_2 | ieee802.3_snap | ieee802.3_llc] <protocol_value>	プロトコル値は、指定されたフレームタイプのプロトコルを識別するために使用されます。オクテット文字列は、フレームタイプによって、以下に示す値の 1 つを持っています。入力形式は 0x0 から 0xffff です。 • ethernet_2 - 16 ビット (2 オクテット) の 16 進数です。 - 使用例 : IPv4 は 0800、IPv6 は 86DD、ARP は 0806 などです。 • ieee802.3_snap - 16 ビット (2 オクテット) の 16 進数です。 - 使用例 : IPv4 は 0800、IPv6 は 86DD、ARP は 0806 などです。 • ieee802.3_llc - 2 オクテットの IEEE 802.2 Link Service Access Point (LSAP) ペアです。はじめのオクテットは、DSAP (Destination Service Access Point) のための値であり、2 番目のオクテットは送信元のための値です。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

プロトコルグループにプロトコルを追加します。

```
DGS-3200-10:4#config dot1v_protocol_group group_id 4 add protocol ethernet_2 86dd
Command: config dot1v_protocol_group group_id 4 add protocol ethernet_2 86DD

Success.

DGS-3200-10:4#
```

config dot1v_protocol_group delete protocol

目的

プロトコルグループからプロトコルを削除します。

構文

config dot1v_protocol_group [group_id <id 1-8> | group_name <name 1-32>] delete protocol [ethernet_2 | ieee802.3_snap | ieee802.3_llc] <protocol_value>

説明

プロトコルグループからプロトコルを削除します。

パラメータ

パラメータ	説明
group_id <id 1-8>	削除するグループ ID を指定します。
group_name <name 1-32>	プロトコルグループ名。
protocol [ethernet_2 | ieee802.3_snap | ieee802.3_llc] <protocol_value>	プロトコル値は、指定されたフレームタイプのプロトコルを識別するために使用されます。オクテット文字列は、フレームタイプによって、以下に示す値の 1 つを持っています。入力形式は 0x0 から 0xffff です。 • ethernet_2 - 16 ビット (2 オクテット) の 16 進数です。 - 使用例 : IPv4 は 0800、IPv6 は 86DD、ARP は 0806 などです。 • ieee802.3_snap - 16 ビット (2 オクテット) の 16 進数です。 - 使用例 : IPv4 は 0800、IPv6 は 86DD、ARP は 0806 などです。 • ieee802.3_llc - 2 オクテットの IEEE 802.2 Link Service Access Point (LSAP) ペアです。はじめのオクテットは、DSAP (Destination Service Access Point) のための値であり、2 番目のオクテットは送信元のための値です。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

プロトコルグループからプロトコルを削除します。

```
DGS-3200-10:4#config dot1v_protocol_group group_id 4 delete protocol ethernet_2
86dd
Command: config dot1v_protocol_group group_id 4 delete protocol ethernet_2 86DD

Success.

DGS-3200-10:4#
```

delete dot1v_protocol_group

目的

プロトコルグループからプロトコルを削除します。

構文

delete dot1v_protocol_group [group_id <id 1-8> | group_name <name 1-32> | all]

説明

プロトコルグループからプロトコルを削除します。

パラメータ

パラメータ	説明
group_id<id 1-8>	削除するグループ ID を指定します。
group_name <name 1-32>	プロトコルグループ名。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

プロトコルグループからプロトコルを削除します。

```
DGS-3200-10:4#delete dot1v_protocol_group group_id 4
Command: delete dot1v_protocol_group group_id 4

Success.

DGS-3200-10:4#
```

show dot1v_protocol_group

目的

プロトコルグループに定義したプロトコルを表示します。

構文

show dot1v_protocol_group {group_id <id 1-8> | group_name <name 1-32>}

説明

プロトコルグループに定義したプロトコルを表示します。

パラメータ

パラメータ	説明
group_id <id 1-8>	表示するグループ ID を指定します。グループ ID を指定しないと、設定されているすべてのプロトコルグループを表示します。
group_name <name 1-32>	プロトコルグループ名。

制限事項

なし。

使用例

プロトコルグループに定義したプロトコルを表示します。

```
DGS-3200-10:4#show dot1v_protocol_group group_id 4
Command: show dot1v_protocol_group group_id 4

 Protocol Group ID     Protocol Group Name      Frame Type       Protocol Value
 ------------------    --------------------    -------------    ------------------
 4                     General Group           EthernetII             86DD

Total Entries: 1

DGS-3200-10:4#
```

config port dot1v

目的

設定されているプロトコルグループに基づいてポートリストから Ingress タグなしパケット用の VLAN を割り当てます。

構文

config port dot1v ports [<portlist> | all] [add protocol_group [group_id <id 1-8> | group_name <name 1-32>] [vlan <vlan_name 32> | vlanid <vlanid 1-4094>] {priority <value 0-7>} | delete protocol_group [group_id <id 1-8> | all]]

説明

設定されているプロトコルグループに基づいてポートリストから入力タグなしパケット用の VLAN を割り当てます。この割り当ては、「delete protocol_group」オプションを使用することで削除できます。プライオリティがコマンド内に指定されない場合、ポートのデフォルトプライオリティが、プロトコル VLAN によって分類されたタグなしパケットのためのプライオリティになります。

パラメータ

パラメータ	説明
portlist	本コマンドを適用するポート範囲。
group_id <id 1-8>	プロトコルグループのグループ ID。
group_name <name 1-32>	プロトコルグループ名。
vlan <vlan_name 32>	ポート上のプロトコル VLAN に割り当てる VLAN。
vlan_id <vlanid 1-4094>	VLAN ID。
priority <vlanid 1-4094>	プロトコルによって指定した VLAN に分類されたパケットに割り当てるプライオリティ。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

プロトコルグループに定義したプロトコルを表示します。

```
DGS-3200-10:4#config port dot1v ports 3 add protocol_group group_id 4 vlan VLAN2
Command: config port dot1v ports 3 add protocol_group group_id 4 vlan VLAN2

Success.

DGS-3200-10:4#
```

show port dot1v

目的

設定されているプロトコルグループに基づいてポートリストから Ingress タグなしパケット用と共に割り当てられた VLAN を表示します。

構文

show port dot1v {ports <portlist>}

説明

設定されているプロトコルグループに基づいてポートリストから Ingress タグなしパケット用と共に割り当てられた VLAN を表示します。

パラメータ

パラメータ	説明
portlist	表示するポートまたはポート範囲を指定します。ポートを指定しない場合、すべてのポートの情報を表示します。

制限事項

なし。

使用例

ポート 1-3 について Ingress タグなしパケット用と共に割り当てられた VLAN を表示します。

```
DGS-3200-10:4#show port dot1v ports 1-2
Command: show port dot1v ports 1-2

Port: 1
Protocol Group ID         VLAN Name               Priority
------------------   --------------------   ----------------
1                    default                        -
2                    vlan_2                         -
3                    vlan_3                         -
4                    vlan_4                         -

Port: 2
Protocol Group ID         VLAN Name               Priority
------------------   --------------------   ----------------
1                    vlan_2                         -
2                    vlan_3                         -
3                    vlan_4                         -
4                    vlan_5                         -

Total Entries : 2

DGS-3200-10:4#
```

第 25 章　VLAN トランキングコマンド

コマンドラインインタフェース（CLI）における VLAN トランキングコマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
enable vlan_trunk	
disable vlan_trunk	
config vlan_trunk ports	[<portlist> | all] state [enable | disable]
show vlan_trunk	

以下のセクションで各コマンドについて詳しく記述します。

enable vlan_trunk

目的
　VLAN トランキング機能を有効にします。
構文
　enable vlan_trunk
説明
　VLAN トランキング機能を有効にします。VLAN トランキング機能を有効にすると、VLAN トランキングポートはどの VID でも、VID を持つタグ付きフレームのすべてを送信することができます。
パラメータ
　なし。
制限事項
　管理者レベルユーザのみ本コマンドを実行できます。
使用例
　VLAN トランキング機能を有効にします

```
DGS-3200-10:4#enable vlan_trunk
Command: enable vlan_trunk

Success.

DGS-3200-10:4#
```

disable vlan_trunk

目的
　VLAN トランキング機能を無効にします。
構文
　disable vlan_trunk
説明
　VLAN トランキング機能を無効にします。
パラメータ
　なし。
制限事項
　管理者レベルユーザのみ本コマンドを実行できます。
使用例
　VLAN トランキング機能を無効にします。

```
DGS-3200-10:4#disable vlan_trunk
Command: disable vlan_trunk

Success.

DGS-3200-10:4#
```

config vlan_trunk

目的

ポートを VLAN トランクポートとして設定します。

構文

config vlan_trunk ports [<portlist> | all] | state [enable | disable]

説明

ポートを VLAN トランキングポートとして設定します。初期値では、スイッチのポートは VLAN トランキングポートには設定されていません。VLAN トランキングポートと非 VLAN トランキングポートをリンクアグリゲートとして分類することはできません。リンクアグリゲーションの VLAN トランキング設定を変更するためには、マスタポートにコマンドを適用する必要があります。しかし、リンクアグリゲーションが切断されるとこの設定はなくなり、各ポートの VLAN トランキング設定はポートの元の設定になります。

マスタポート以外のリンクアグリゲーションのメンバポートにこのコマンドを適用すると、コマンドは拒否されます。異なる VLAN 設定のポートは、リンクアグリゲーションを形成することはできません。VLAN トランキングポートに指定されている場合は、リンクアグリゲートが可能です。

VLAN トランキングポートに関しては、パケットが迂回できる VLAN は、その特定ポート上の GVRP に通知されることはありません。しかし、これらの VLAN 上のトラフィックが送信されるので、この VLAN トランキングポートはこれらの VLAN に関連づけられた MSTP インスタンスに加わることになります。

パラメータ

パラメータ	説明
<portlist> | all	• <portlist> - 設定するポートまたはポートリストを指定します。 • all - すべてのポートに設定します。
[enable | disable]	• enable - 指定ポートを VLAN トランキングポートとして設定します。 • disable - 指定ポートを VLAN トランキングポートとしません。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

ポート 1-5 を VLAN トランキングポートとして設定します。

```
DGS-3200-10:4#config vlan_trunk ports 1-5 state enable
Command: config vlan_trunk ports 1-5 state enable

Success.

DGS-3200-10:4#
```

ポート 6 を LA-1（リンクアグリケーション -1）のメンバポートとして、ポート 7 を LA-2（リンクアグリケーション -2）のマスタポートとして設定します。

```
DGS-3200-10:4#config vlan_trunk ports 6-7 state enable
Command: config vlan_trunk ports 6-7 state enable

The link aggregation member port cannot be configured.
Fail.

DGS-3200-10:4#config vlan_trunk ports 7 state disable
Command: config vlan_trunk ports 7 state disable

Success.

DGS-3200-10:4#config vlan_trunk ports 6-7 state disable
Command: config vlan_trunk ports 6-7 state disable

The link aggregation member port cannot be configured.
Fail.

DGS-3200-10:4#
```

ポート 6 を LA-1（リンクアグリケーション -1）のメンバポートとして、ポート 7 を LA-1（リンクアグリケーション -1）のマスタポートとして設定します。

```
DGS-3200-10:4#config vlan_trunk ports 6-7 state enable
Command: config vlan_trunk ports 6-7 state enable

Success.

DES-3028P:4#
```

ポート 6 と 7 は、VLAN トランキング機能を有効にする前に別々の VLAN 設定を持っています。ポート 6 を LA-1(リンクアグリケーション -1) のメンバポートとして、ポート 7 を LA-1(リンクアグリケーション -1) のマスタポートとして設定します。

```
DGS-3200-10:4#config vlan_trunk ports 7 state disable
Command: config vlan_trunk ports 7 state disable

Success.

DGS-3200-10:4#
```

ポート 6 と 7 は、VLAN トランキング機能を有効にする前に同じ VLAN 設定を持っています。ポート 6 を LA-1（リンクアグリケーション -1）のメンバポートとして、ポート 7 を LA-1（リンクアグリケーション -1）のマスタポートとして設定します。

```
DGS-3200-10:4#config vlan_trunk ports 7 state disable
Command: config vlan_trunk ports 7 state disable

Success.

DGS-3200-10:4#config vlan_trunk ports 6-7 state disable
Command: config vlan_trunk ports 6-7 state disable

Success.

DGS-3200-10:4#
```

show vlan_trunk

目的

VLAN トランキング設定を参照します。

構文

show vlan_trunk

説明

VLAN トランキング設定を参照します。

パラメータ

なし。

制限事項

なし。

使用例

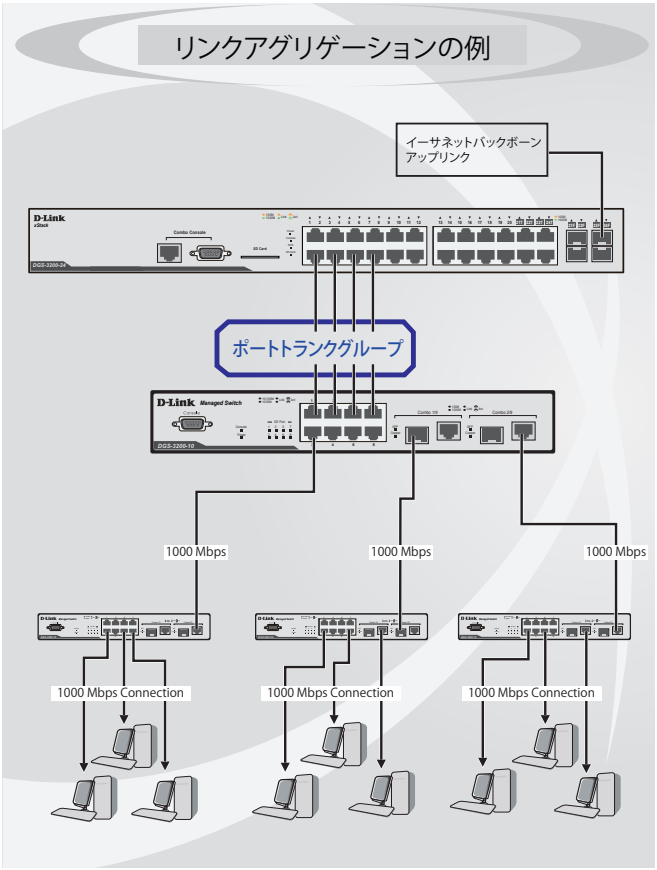
VLAN トランク情報を表示します。

```
DGS-3200-10:4#show vlan_trunk
Command: show vlan_trunk

VLAN Trunk Status    :Enable
Member Ports         :1-5,7

DGS-3200-10:4#
```

第 26 章　リンクアグリゲーションコマンド

ポートトランクグループについて

ポートトランクグループは、複数のポートを結合して 1 つの広帯域のデータパイプラインとして利用する機能です。スイッチは 2 から 8 のポートを束ねたトランクグループをサポートします。この機能により最大 8000Mbps の通信速度が実現されます。



ポートトランクグループの例

スイッチはトランクグループ内のすべてのポートを 1 つのポートと見なします。あるホスト（宛先アドレス）へのデータ転送は、トランクグループ内のいつも同じポートから行われます。これにより、データが送信された順に受け取られるようになります。

注意　トランクグループ内のあるポートが接続不可になると、そのポートが処理するパケットは他のリンクアグリゲーション（集約）グループ内の他のポート間でロードシェアされます。

リンクアグリゲーション機能により、1 つのグループとして束ねられたポートは、1 つのリンクの働きをします。この時、1 つのリンクの帯域は、束ねられたポート分拡張されます。

リンクアグリゲーションは、サーバやバックボーンなど、広帯域を必要とするネットワークデバイスにおいて広く利用されています。

本スイッチでは、2 から 8 のリンク（ポート）で構成するリンクアグリゲーショングループをサポートします。ギガビットポート（オプション）だけは、1 つのリンクアグリゲーショングループに所属します。1 つのグループ内にある ポートのすべては同じ VLAN に属し、それぞれのスパニングツリープロトコル（STP）ステータス、スタティックマルチキャスト、トラフィックコントロール、トラフィックセグメンテーション、および 802.1p デフォルトプライオリティの設定は同じである必要があります。
また、ポートロッキング、ポートミラーリング、および 802.1X は有効化されていてはなりません。さらに、集約するリンクはすべて同じ速度で、全二重モードで設定されている必要があります。

グループのマスタポートの設定はユーザにより行われます。また、マスタポートに適用される VLAN 設定を含むすべての設定オプションは、グループ内全体に適用されます。

グループ内のポート間では自動的にロードバランスが行われ、グループ内でのリンク断によって発生するネットワークトラフィックは、グループ内の他のリンクに振り分けられます。

スパニングツリープロトコル（STP）は、スイッチレベルにおいて、リンクアグリゲーショングループを 1 つのリンクとしてとらえます。ポートレベルでは STP はマスタポートのポートパラメータを使用してポートコストを計算し、リンクアグリゲーショングループの状態を決定します。スイッチ上に 2 つのリンクアグリゲーショングループが冗長して設定された場合、STP は冗長リンクを持つポートのブロックを行うのと同様に、1 つのグループをブロックします。

コマンドラインインタフェース（CLI）におけるリンクアグリゲーションコマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
create link_aggregation group_id	<value> {type [lacp | static]}
delete link_aggregation group_id	<value>
config link_aggregation group_id	<value> {master_port <port> | ports <portlist> | state [enable | disable]}
config link_aggregation algorithm	[mac_source_dest | ip_source_dest]
show link_aggregation	{group_id <value> | algorithm}

以下のセクションで各コマンドについて詳しく記述します。

create link_aggregation group_id

目的

リンクアグリゲーショングループを作成します。

構文

create link_aggregation group_id <value> {type [lacp | static]}

説明

固有の識別子を持つリンクアグリゲーショングループを作成します。

パラメータ

パラメータ	説明
<value>	グループ ID を指定します。グループ ID は各グループを識別します。DGS-3200-10 には 1-5、DGS-3200-16/GE には 1-8、DGS-3200-24/GE には 1-12 を指定します。
type [lacp | static]	グループに使用されるリンクアグリゲーションのタイプを指定します。タイプが指定されないと、初期値は「static」になります。 • lacp - ポートグループを LACP 準拠として指定します。これにより LACP は集約されたポートグループに動的な変更を行います。 • static - アグリゲーションポートグループをスタティックに指定します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

リンクアグリゲーショングループを作成します。

```
DGS-3200-10:4#create link_aggregation group_id 1 type lacp
Command: create link_aggregation group_id 1 type lacp

Success

DGS-3200-10:4#
```

注意 LACP またはスタティックタイプのリンクアグリゲーションを使用する場合、接続の両端が同じ速度とデュプレックス設定であることを確認してください。

delete link_aggregation group_id

目的

定義済みのリンクアグリゲーショングループを削除します。

構文

delete link_aggregation group_id <value>

説明

既存のリンクアグリゲーショングループを削除します。

パラメータ

パラメータ	説明
<value>	削除するグループ ID を指定します。グループ ID は各グループを識別します。DGS-3200-10 には 1-5、DGS-3200-16/GE には 1-8、DGS-3200-24/GE には 1-12 を指定します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

リンクアグリゲーショングループを削除します。

```
DGS-3200-10:4#delete link_aggregation group_id 3
Command: delete link_aggregation group_id 3

Success.

DGS-3200-10:4#
```

config link_aggregation group_id

目的

既存のリンクアグリゲーショングループを設定します。

構文

config link_aggregation group_id <value> {master_port <port> | ports <portlist> | state [enable | disable]}

説明

既存のリンクアグリゲーショングループを設定します。

パラメータ

パラメータ	説明
<value>	グループ ID を指定します。グループ ID は各グループを識別します。DGS-3200-10 には 1-5、DGS-3200-16/GE には 1-8、DGS-3200-24/GE には 1-12 を指定します。
master_port <port>	マスタポート番号。マスタポートになるリンクアグリゲーショングループのポート番号を指定します。リンクアグリゲーショングループのすべてのポートは、マスタポートと共にポート設定を共有します。
ports<portlist>	リンクアグリゲーショングループに所属するポートまたは範囲を指定します。
state [enable | disable]	指定されたリンクアグリゲーショングループを「enable」（有効）または「disable」（無効）にします。LACP グループを設定すると、ポートのステートマシンが始動します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。リンクアグリゲーショングループは重複することはできません。

使用例

ポートの負荷分散グループ、グループ ID1、マスタポート 7 をグループメンバポート 5-7 と共に定義します。

```
DGS-3200-10:4#config link_aggregation group_id 1 master_port 7 ports 5-7 state enable
Command: config link_aggregation group_id 1 master_port 7 ports 5-7 state enable

Success.

DGS-3200-10:4#
```

config link_aggregation algorithm

目的

リンクアグリゲーションアルゴリズムを設定します。

構文

config link_aggregation algorithm [mac_source_dest | ip_source_dest]

説明

送信の負荷分散データに対して Egress ポートを選択する場合、スイッチに検証されるパケットの部分を設定します。この機能は、アドレスベースの負荷分散アルゴリズムを使用することで有効になります。

パラメータ

パラメータ	説明
mac_source_dest	スイッチは MAC 送信元および送信先アドレスを調べます。
ip_source_dest	スイッチは IP 送信元および送信先アドレスを調べます。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

mac-source-dest にリンクアグリゲーションアルゴリズムを設定します。

```
DGS-3200-10:4#config link_aggregation algorithm mac_source_dest
Command: config link_aggregation algorithm mac_source_dest

Success.

DGS-3200-10:4#
```

show link_aggregation

目的

スイッチの現在のリンクアグリゲーショングループを表示します。

構文

show link_aggregation {group_id <value> | algorithm}

説明

スイッチの現在のリンクアグリゲーショングループを表示します。

パラメータ

パラメータ	説明
<value>	グループ ID を指定します。グループ ID は各グループを識別します。DGS-3200-10 には 1-5、DGS-3200-16/GE には 1-8、DGS-3200-24/GE には 1-12 を指定します。
algorithm	使用中のアルゴリズムで指定されるリンクアグリゲーションを表示します。パラメータが指定されないと、システムはすべてのリンクアグリゲーション情報を表示します。

制限事項

なし。

使用例

リンクアグリゲーション設定（有効）を表示します。

```
DGS-3200-10:4#show link_aggregation
Command: show link_aggregation

Link Aggregation Algorithm = MAC_Source_Dest

Group ID      : 1
Type          : LACP
Master Port   : 1
Member Port   : 1-8
Active Port   : 7
Status        : Enabled
Flooding Port : 7

DGS-3200-10:4#
```

リンクアグリゲーション設定（無効）を表示します。

```
DGS-3200-10:4#show link_aggregation
Command: show link_aggregation

Link Aggregation Algorithm = MAC-Source-Dest

Group ID      : 1
Type          : LACP
Master Port   : 1
Member Port   : 1-8
Active Port   :
Status        : Disabled
Flooding Port :

DGS-3200-10:4#
```

第 27 章　LACP 設定コマンド

スイッチにポートトランキンググループを作成するために使用します。

コマンドラインインタフェース（CLI）におけるリンクアグリゲーションコマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
config lacp_port	<portlist> mode [active | passive]
show lacp_port	{<portlist>}

以下のセクションで各コマンドについて詳しく記述します。

config lacp_port

目的

以前に LACP ポートとして指定されたポートを設定します。

構文

config lacp_port <portlist> mode [active | passive]

説明

以前に LACP ポートとして指定されたポートを設定します（「create link_aggregation」を参照）。

パラメータ

パラメータ	説明
<portlist>	表示するポートまたは範囲を指定します。
mode [active | passive]	LACP ポートが LACP 制御フレームを処理するかどうかを決定するモードを選択します。パラメータが指定されないと、システムはすべてのポートに対する現在の LACP ステータスを表示します。 • active - Active LACP ポートは、LACP 制御フレームの処理と送信を行います。これにより LACP 準拠のデバイス同士はネゴシエーションとリンクの集約を行い、グループは必要に応じて動的に変更されます。グループへのポート追加、または削除などのグループの変更を行うためには、少なくともどちらかのデバイスで LACP ポートを「Active」に設定する必要があります。また、両方のデバイスは LACP をサポートしなければなりません。 • passive - passive に設定された LACP ポートは、LACP 制御フレームの処理だけを行い、フレームの送信を行いません。リンクするポートグループがネゴシエーションを行い、動的にグループの変更を行うには、接続のどちらか一端が「active」LACP ポートである必要があります（上記参照）。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

ポート 1-10 に LACP モードを設定します。

```
DGS-3200-10:4#config lacp_port 1-10 mode active
Command: config lacp_port 1-10 mode active

Success.

DGS-3200-10:4#
```

show lacp_port

目的

現在の LACP ポートのモード設定を表示します。

構文

show lacp_port {<portlist>}

説明

現在の LACP ポートモード設定を表示します。

パラメータ

パラメータ	説明
<portlist>	表示するポートまたは範囲を指定します。パラメータが指定されないと、システムはポートすべての現在の LACP ステータスを表示します。

制限事項

なし。

使用例

スイッチの全ポートの LACP モード設定を表示します。

```
DGS-3200-10:4#show lacp_port
Command: show lacp_port

Port    Activity
------  --------
1       Active
2       Active
3       Active
4       Active
5       Active
6       Active
7       Active
8       Active
9       Active
10      Active

DGS-3200-10:4#
```

第 28 章　トラフィックセグメンテーションコマンド

トラフィックセグメンテーション機能は、１つのポートまたはポートグループから、スイッチのポートグループに対するトラフィックの流れを制限するために使用します。トラフィックフローの分割を行うこの方法は、VLAN によるトラフィック制限に似ていますが、さらに限定的であると言えます。

コマンドラインインタフェース（CLI）におけるトラフィックセグメンテーションコマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
config traffic_segmentation	[<portlist> | all] forward_list [null | all | <portlist>]
show traffic_segmentation	{<portlist>}

以下のセクションで各コマンドについて詳しく記述します。

config traffic_segmentation

目的

スイッチにトラフィックセグメンテーションを設定します。

構文

config traffic_segmentation [<portlist> | all] forward_list [null | all | <portlist>]

説明

スイッチにトラフィックセグメンテーションを設定します。

パラメータ

パラメータ	説明
<portlist> | all	トラフィックセグメンテーションを設定するポートまたは範囲を指定します。「all」はすべてのポートを指定します。
forward_list [null | <portlist>]	上で指定されたポートからフレームを受信するポートまたはポート範囲を指定します。 • null - ポートフォワーディングドメイン範囲に null を指定します。 • <portlist> - フォワーディングリストにポート範囲を指定します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。フォワーディングドメインはブリッジトラフィックに対してだけ制限されます。

使用例

ポート 7-8 にフレームを転送するためにポート 1-6 を設定します。

```
DGS-3200-10:4#config traffic_segmentation 1-6 forward_list 7-8
Command: config traffic_segmentation 1-6 forward_list 7-8

Success.

DGS-3200-10:4#
```

show traffic_segmentation

目的

スイッチで使用中の現在のトラフィックセグメンテーション設定を表示します。

構文

show traffic_segmentation {<portlist>}

説明

スイッチの現在のトラフィックセグメンテーション設定を表示します。

パラメータ

パラメータ	説明
<portlist>	スイッチの現在のトラフィックセグメンテーションを表示するポートまたはポート範囲を指定します。パラメータが指定されないと、システムはすべてのトラフィックセグメンテーションテーブルを表示します。

制限事項

セグメンテーションのポートリストおよびフォワーディングリストは、同じスイッチにある必要があります。

使用例

現在のトラフィックセグメンテーション設定を表示します。

```
DGS-3200-10:4#show traffic_segmentation
Command: show traffic_segmentation

Traffic Segmentation Table

Port    Forward Portlist
------  ------------------------------------------------
1       1-10
2       1-10
3       1-10
4       1-10
5       1-10
6       1-10
7       1-10
8       1-10

DGS-3200-10:4#
```

第 29 章　ポートセキュリティコマンド

ポートやポート範囲を指定して、ダイナミックな MAC アドレス学習をロックすることにより、MAC アドレスフォワーディングテーブルへ、新しいソース MAC アドレスが追加されないよう設定することができます。

コマンドラインインタフェース（CLI）におけるポートセキュリティコマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
config port_security	ports [<portlist> | all] {admin_state [enable | disable] | max_learning_addr <max_lock_no 0-16> | lock_address_mode [Permanent | DeleteOnTimeout | DeleteOnReset]}
delete port_security_entry	vlan_name <vlan_name 32> port <port> mac_address <macaddr>
clear port_security_entry	port <portlist>
show port_security	{ports <portlist>}
enable port_security trap_log	
disable port_security trap_log	

以下のセクションで各コマンドについて詳しく記述します。

config port_security

目的

ポートセキュリティを設定します。

構文

config port_security ports [<portlist> | all] {admin_state [enable | disable] | max_learning_addr <max_lock_no 0-16> | lock_address_mode [Permanent | DeleteOnTimeout | DeleteOnReset]}

説明

ポートセキュリティ機能を設定します。<portlist> に示されたポートにだけ適用されます。

パラメータ

パラメータ	説明
<portlist>	設定するポートまたはポート範囲を指定します。
all	スイッチのすべてのポートにセキュリティを設定します。
admin_state [enable | disable]	リストアップされたポートへのセキュリティを「enable」（有効）または「disable」（無効）にします。
max_learning_addr <max_lock_no 0-16>	ポートへの FDB 内で動的に学習される MAC アドレス数を制限します。エントリの最大数は 64 です。
lock_address_mode [Permanent | DeleteOnTimeout | DeleteOnReset]	アドレスをロックする手段を指定します。3 つの選択肢があります。 • Permanent - ロックされたアドレスは、再起動後のエージングタイム経過後に削除されます。 • DeleteOnTimeout - ロックされたアドレスは、エージングタイム経過後に削除されます。 • DeleteOnReset - ロックされたアドレスは、リセットか再起動されるまで削除されません。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

ポートセキュリティを設定します。

```
DGS-3200-10:4#config port_security ports 6 admin_state enable max_learning_addr
10 lock_address_mode Permanent
Command: config port_security ports 6 admin_state enable max_learning_addr 16
lock_address_mode Permanent

Success.

DGS-3200-10:4#
```

delete port_security_entry

目的

MAC アドレス、ポート番号および VLAN ID ごとにポートセキュリティエントリを削除します。

構文

delete port_security_entry vlan_name <vlan_name 32> port <port> mac_address <macaddr>

説明

学習済みのポートセキュリティエントリを MAC アドレス、ポート番号および VLAN 名ごとに削除します。

パラメータ

パラメータ	説明
vlan name <vlan_name 32>	削除するポートの対応する VLAN 名を入力します。
port <port>	MAC アドレスを学習しているポート番号を入力します。
mac_address <macaddr>	ポートが学習し、削除する MAC アドレスを入力します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

ポートセキュリティエントリを削除します。

```
DGS-3200-10:4#delete port_security_entry vlan_name default mac_address 00-01-
30-10-2C-C7 port 6
Command: delete port_security_entry vlan_name default mac_address 00-01-30-10-
2C-C7 port 6

Success.

DGS-3200-10:4#
```

clear port_security_entry

目的

ポートセキュリティ機能のために指定ポートから学習した MAC アドレスエントリをクリアします。

構文

clear port_security_entry port <portlist>

説明

指定ポートごとにスイッチが学習した MAC アドレスエントリをクリアします。

パラメータ

パラメータ	説明
<portlist>	設定するポートまたはポート範囲を指定します。

制限事項

管理者レベルのみ本コマンドを実行できます。

使用例

ポートごとにポートセキュリティエントリをクリアします。

```
DGS-3200-10:4#clear port_security_entry port 6
Command: clear port_security_entry port 6

Success.

DGS-3200-10:4#
```

show port_security

目的

現在のポートセキュリティ設定を表示します。

構文

show port_security {ports <portlist>}

説明

このコマンドは、スイッチのポートに関するポートセキュリティ情報を表示するために使用されます。表示される情報には、ポートセキュリティ、Admin ステータス、学習しているアドレスの最大数およびロックモードが含まれます。

パラメータ

パラメータ	説明
<portlist>	参照するポートまたはポート範囲を指定します。

制限事項

なし。

使用例

ポートセキュリティ設定を表示します。

```
DGS-3200-10:4#show port_security ports 1-6
Command: show port_security ports 1-6

Port_security Trap/Log : Enabled

Port    Admin State  Max. Learning Addr.  Lock Address Mode
------  -----------  -------------------  -----------------
1       Disabled     1                    DeleteOnReset
2       Disabled     1                    DeleteOnReset
3       Disabled     1                    DeleteOnReset
4       Disabled     1                    DeleteOnReset
5       Disabled     1                    DeleteOnReset
6       Enabled      10                   Permanent

DGS-3200-10:4#
```

enable port_security trap_log

目的

ポートセキュリティトラップ / ログを有効にします。

構文

enable port_security trap_log

説明

ポートセキュリティトラップ / ログを有効にします。ポートセキュリティトラップが有効である場合、既に定義したポートセキュリティ設定に従わない新しい MAC アドレスがあると、トラップは MAC とポートの情報と共に送信され、関連情報がログ取得されます。

パラメータ

なし。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

ポートセキュリティトラップを有効にします。

```
DGS-3200-10:4#enable port_security trap_log
Command: enable port_security trap_log

Success.

DGS-3200-10:4#
```

disable port_security trap_log

目的

ポートセキュリティトラップ / ログを無効にします。

構文

disable port_security trap_log

説明

ポートセキュリティトラップ / ログを無効にします。ポートセキュリティトラップを無効にすると、MAC 違反に対してトラップを送信しません。

パラメータ

なし。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

スイッチから送信されるポートセキュリティトラップを無効にします。

```
DGS-3200-10:4#disable port_security trap_log
Command: disable port_security trap_log

Success.

DGS-3200-10:4#
```

第 30 章　スタティック MAC ベース VLAN コマンド

コマンドラインインタフェース（CLI）におけるスタティック MAC ベース VLAN コマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
create mac_based_vlan	mac_address <macaddr> [vlan <vlan_name 32> | vlanid <vlanid 1-4094>]
delete mac_based_vlan	{mac_address <macaddr> [vlan <vlan_name 32> | vlanid <vlanid 1-4094>] }
show mac_based_vlan	{mac_address <macaddr> | vlan <vlan_name 32> | vlanid <vlanid 1-4094>}

以下のセクションで各コマンドについて詳しく記述します。

create mac_based_vlan

目的

スタティック MAC ベース VLAN のエントリを作成します。

構文

create mac_based_vlan mac_address <macaddr> | vlan <vlan_name 32>

説明

MAC ベース VLAN をサポートするモデル用のコマンドです。

スタティック MAC ベース VLAN のエントリを作成します。エントリがポートに作成される場合、ポートは指定した VLAN のタグ無しメンバポートに自動的になります。スタティック MAC ベース VLAN のエントリがユーザに作成されると、このユーザからのトラフィックはこのポートで動作する認証機能にかかわらず指定 VLAN の下で行われます。

パラメータ

パラメータ	説明
mac_address <macaddr>	MAC アドレス。
vlan <vlan_name 32>	MAC アドレスに関連付けされる VLAN。
<vlanid <vlanid 1-4094>	MAC アドレスに関連付けされる VLAN ID。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

スタティック MAC ベース VLAN のエントリを作成します。

```
DGS-3200-10:4#create mac_based_vlan mac_address 00-00-00-00-00-01 vlan default
Command: create mac_based_vlan mac_address 00-00-00-00-00-01 vlan default

Success.

DGS-3200-10:4#
```

delete mac_based_vlan

目的

スタティックな MAC ベース VLAN エントリを削除します。

構文

delete mac_based_vlan {mac_address <macaddr> [vlan <vlan_name 32> | vlanid <vlanid 1-4094>]}

説明

データベースエントリを削除します。MAC アドレスおよび VLAN を指定しないと、ポートに割り当てられているスタティックエントリのすべてが削除されます。

パラメータ

パラメータ	説明
mac_address <macaddr>	MAC アドレス。
vlan name <vlan_name 32>	MAC アドレスに関連付けされる VLAN。
vlanid <vlanid 1-4094>	MAC アドレスに関連付けされる VLAN ID。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

スタティック MAC ベース VLAN のエントリを削除します。

```
DGS-3200-10:4#delete mac_based_vlan mac_address 00-00-00-00-00-01 vlan default
Command: delete mac_based_vlan mac_address 00-00-00-00-00-01 vlan default

Success.

DGS-3200-10:4#
```

show mac_based_vlan

目的

スタティック MAC ベース VLAN のエントリを表示します。

構文

show mac_based_vlan {mac_address <macaddr> | vlan <vlan_name 32> | vlanid <vlanid 1-4094>}

説明

スタティック MAC ベース VLAN のエントリを表示します。

パラメータ

パラメータ	説明
mac_address <macaddr>	表示するエントリの MAC アドレス。
vlan name <vlan_name 32>	表示するエントリの VLAN 名アドレス。
vlanid <vlanid 1-4094>	表示するエントリの VLAN ID。

制限事項

なし。

使用例

以下の例では、手動で MAC アドレス「00-80-c2-33-c3-45」を VLAN 300 に割り当てます。その後、MAC-AC（MAC アドレス認証制御）により VLAN 400 に割り当てられます。MAC-AC には手動の設定よりも高い優先度があるため、手動で設定されたエントリは無効になります。

MAC ベース VLAN のエントリを表示します。

```
DGS-3200-10:4#show mac_based_vlan
Command: show mac_based_vlan

MAC Address        VLAN         Status      Type
------------------ ------------ ----------- --------
00-80-e0-14-a7-57  200          Active      Static
00-80-c2-33-c3-45  300          Inactive    Static
00-80-c2-33-c3-45  400          Active      MAC AC
00-a2-44-17-32-98  400          Active      WAC

Total Entries : 4

DGS-3200-10:4#
```

第 31 章　ポート Egress フィルタコマンド

コマンドラインインタフェース（CLI）におけるポート Egress フィルタコマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
config egress_filter	ports [<portlist> | all] {unicast [enable | disable] | multicast [enable | disable]}
show egress_filter	ports {<portlist>}

以下のセクションで各コマンドについて詳しく記述します。

config egress_filter ports

目的

　指定ポートに Egress フィルタリング機能を設定します。

portlist

unicast

multicast

構文

　config egress_filter ports [<portlist> | all] {unicast [enable | disable] | multicast [enable | disable]}

説明

　指定ポートに Egress フィルタリング機能を設定します。

パラメータ

パラメータ	説明
<portlist> | all	ポートリストを指定します。
unicast [enable | disable]	DFL(Destination Lookup Failure) パケットの Egress フィルタリングを指定します。 • enable - 未知のユニキャストパケットをフィルタし、指定ポートに送信しません。 • disable - 未知のユニキャストパケットをフィルタせずに、指定ポートに送信します。
multicast [enable | disable]	未登録のマルチキャストパケットに対する Egress フィルタリングを指定します。 • enable - 未登録のマルチキャストパケットをフィルタし、指定ポートに送信しません。 • disable - 未登録のマルチキャストパケットをフィルタせずに、指定ポートに送信します。

制限事項

　管理者レベルユーザのみ本コマンドを実行できます。

使用例

　Egress フィルタリングを設定します。

```
DGS-3200-10:4#config egress_filter ports 6 unicast enable multicast enable
Command: config egress_filter ports 6 unicast enable multicast enable

Success.

DGS-3200-10:4#
```

show egress_filter ports

目的

ポートの Egress フィルタリング設定を表示します。

構文

show egress_filter ports {<portlist>}

説明

ポートの Egress フィルタリング設定を表示します。

パラメータ

パラメータ	説明
<portlist>	Egress フィルタリング設定を表示するポートを指定します。

制限事項

なし。

使用例

ポート 6 の Egress フィルタリングを表示します。

```
DGS-3200-10:4#show egress_filter ports 6
Command: show egress_filter ports 6

Port  Unicast  Multicast
----  -------  ---------
6     Enabled  Enabled

DGS-3200-10:4#
```

第 32 章　基本的な IP コマンド（レイヤ 2）

コマンドラインインタフェース（CLI）における IP インタフェースコマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
config ipif	<ipif_name 12>[{ipaddress <network_address> | vlan <vlan_name 32> | state [enable | disable]} | bootp | dhcp | ipv6 ipv6address <ipv6networkaddr>]
create ipif	<ipif_name 12> <vlan_name 32> {state [enable | disable]}
enable ipif	[<ipif_name 12> | all]
disable ipif	[<ipif_name 12> | all]
show ipif	{<ipif_name 12>}
enable ipif_ipv6_link_local_auto	[<ipif_name 12> | all]
disable ipif_ipv6_link_local_auto	[<ipif_name 12> | all]
show ipif_ipv6_link_local_auto	{<ipif_name 12>}

以下のセクションで各コマンドについて詳しく記述します。

config ipif

目的

IP インタフェースをスイッチに設定します。

構文

config ipif <ipif_name 12>[{ipaddress <network_address> | vlan<vlan_name 32> | state [enable | disable]} | bootp | dhcp | ipv6 ipv6address <ipv6networkaddr>]

説明

IP インタフェースをスイッチに設定します。

パラメータ

パラメータ	説明
ipif_name 12	IP インタフェース名。
vlan <vlan_name 32>	IP インタフェースに対応する VLAN 名を入力します。
ipaddress <network_address>	作成する IP アドレスの IP アドレスとネットマスク。既知のフォーマット（例 :10.1.2.3/255.0.0.0 または CIDR フォーマットにおける 10.1.2.3/8）を使用して IP アドレスとマスク情報を指定します。
state [enable | disable]	IP インタフェースを「enable」（有効）または「disable」（無効）にします。
bootp	スイッチのシステム IP インタフェースに IP アドレスを割り当てるために、BOOTP プロトコルを選択します。
dhcp	スイッチのシステム IP インタフェースに IP アドレスを割り当てるために、DHCP プロトコルを選択します。
ipv6address <ipv6networkaddr>	作成する IPv6 アドレスの IPv6 アドレスとネットマスク。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

「System」IP インタフェースを設定します。

```
DGS-3200-10:4#config ipif System vlan v1
Command: config ipif System vlan v1

Success.

DGS-3200-10:4#
```

create ipif

目的

IPv6 アドレスに IPv6 インタフェースを作成します。

構文

create ipif <ipif_name 12> <vlan_name 32 > {state [enable | disable]}

説明

IPv6 アドレスに IPv6 インタフェースを作成します。本インタフェースは、IPv6 アドレスと共に設定されます。システムインタフェースにいくつかの IPv6 アドレスが既にある場合、1 つの IPv6 インタフェースだけがサポートされるため、本コマンドを実行するとエラーになります。

注意 本スイッチは、IPv6 アドレスに 1 つの IP インタフェースのみサポートします。

パラメータ

パラメータ	説明
<ipif_name 12>	作成する IP インタフェース名。12 文字以内の半角英数字を入力します。
<vlan_name 32>	IP インタフェースに関連づける VLAN 名。
state [enable | disable]	IP インタフェースを「enable」（有効）または「disable」（無効）にします。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

IP インタフェース「interface1」をスイッチに作成します。

```
DGS-3200-10:4#create ipif interface1 VLAN2
Command: create ipif ipif interface1 VLAN2

Success.

DGS-3200-10:4#
```

delete ipif

目的

インタフェースまたは IPv6 アドレスを削除します。

構文

delete ipif [<ipif_name 12> {ipv6address <ipv6networkaddr>} | all]

説明

指定のインタフェースから IPv6 インタフェースまたは IPv6 アドレスを削除します。

パラメータ

パラメータ	説明
<ipif_name 12>	削除する作成済みの IP インタフェース名。IP インタフェースを定義するためには、12 文字以内の半角英数字を入力します。
ipv6address <ipv6networkaddr>	本インタフェースに対する IPv6 アドレスを削除します。
all	システムインタフェースを除く現在スイッチに設定されているすべての IP インタフェースを削除します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

インタフェース「interface1」を削除します。

```
DGS-3200-10:4#delete ipif interface1
Command: delete ipif interface1

Success.

DGS-3200-10:4#
```

enable ipif

目的

スイッチの IP インタフェース機能を有効にします。

構文

enable ipif [<ipif_name 12> | all]

説明

スイッチの IP インタフェース機能を有効にします。ステータスが有効である場合、IPv4 アドレスが IP インタフェースに設定されると IPv4 処理は開始します。IPv6 アドレス処理は、IPv6 アドレスが IP インタフェースに設定されると開始します。

パラメータ

パラメータ	説明
<ipif_name 12>	有効にする作成済みの IP インタフェース名。IP インタフェースを定義するためには、12 文字以内の半角英数字を入力します。
all	現在スイッチに設定されているすべての IP インタフェースを有効にします。

制限事項

管理者レベルレベルユーザのみ本コマンドを実行できます。

使用例

インタフェース「interface1」のステータスを有効にします。

```
DGS-3200-10:4#enable ipif interface1
Command: enable ipif interface1

Success.

DGS-3200-10:4#
```

disable ipif

目的

スイッチの IP インタフェース設定を無効にします。

構文

disable ipif [<ipif_name 12> | all]

説明

設定を変更せずに、スイッチの IP インタフェースを無効にします。

パラメータ

パラメータ	説明
<ipif_name 12>	無効にする作成済みの IP インタフェース名。IP インタフェースを定義するためには、12 文字以内の半角英数字を入力します。
all	現在スイッチに設定されているすべての IP インタフェースを無効にします。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

インタフェース「interface1」のステータスを無効にします。

```
DGS-3200-10:4#disable ipif interface1
Command: disable ipif interface1

Success.

DGS-3200-10:4#
```

show ipif

目的

スイッチの IP インタフェース設定を表示します。

構文

show ipif {<ipif_name 12>}

説明

スイッチの IP インタフェース設定を表示します。

パラメータ

パラメータ	説明
<ipif_name 12>	インタフェース名。パラメータが指定されないと、すべてのインタフェースが表示されます。

制限事項

なし。

使用例

IP インタフェース設定を表示します。

```
DGS-3200-10:4#show ipif
Command: show ipif

IP Interface Settings

Interface Name           : Interface1
IP Address               : 10.90.90.90 (Manual)
Subnet Mask              : 255.0.0.0
VLAN Name                : v1
Interface Admin State    : Enabled
Link Status              : LinkUP
Member Ports             : 1-10

Total Entries            :1

DGS-3200-10:4#
```

enable ipif_ipv6_link_local_auto

目的

IPv6 アドレスが設定されていない場合、Link-Local アドレスの自動設定を有効にします。

構文

enable ipif_ipv6_link_local_auto [<ipif_name 12> | all]

説明

IPv6 アドレスが事前に定義されていないと、IPv6 Link-Local アドレスを自動的にスイッチに作成します。
IPv6 アドレスが設定されると、Link-Local アドレスは自動的に設定されて IPv6 処理は開始します。IPv6 アドレスが設定されていない場合、初期値では Link-Local アドレスは設定されず、IPv6 処理は無効になります。この自動設定を有効にすることによって、Link-Local アドレスは自動的に設定されて IPv6 処理は開始します。

パラメータ

パラメータ	説明
<ipif_name 12>	IPv6 Link-Local アドレスを付与する IP インタフェース名。
all	現在スイッチに設定されているすべての IP インタフェースに IPv6 Link-Local アドレスを割り当てます。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

IP インタフェースの IPv6 Link-Local アドレス設定を有効にします。

```
DGS-3200-10:4#enable ipif_ipv6_link_local_auto interface1
Command: enable ipif_ipv6_link_local_auto interface1

Success.

DGS-3200-10:4#
```

disable ipif_ipv6_link_local_auto

目的

IPv6 アドレスが設定されていない場合、Link-Local アドレスの自動設定を無効にします。

構文

disable ipif_ipv6_link_local_auto [<ipif_name 12> | all]

説明

スイッチの IPv6 Link-Local アドレスの自動作成を無効にします。本コマンドを入力すると、選択した IP インタフェースに作成済みの IPv6 Link-Local アドレスをすべてスイッチから削除します。

パラメータ

パラメータ	説明
<ipif_name 12>	IPv6 Link-Local アドレスを無効にする IP インタフェース名。
all	現在スイッチに設定されているすべての IP インタフェースの IPv6 Link-Local アドレスを無効にします。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

IP インタフェースの IPv6 Link-Local アドレス設定を有効にします。

```
DGS-3200-10:4#disable ipif_ipv6_link_local_auto interface1
Command: disable ipif_ipv6_link_local_auto interface1

Success.

DGS-3200-10:4#
```

show ipif_ipv6_link_local_auto

目的

IPv6 Link-Local 自動設定の状態を表示します。

構文

show ipif_ipv6_link_local_auto {<ipif_name 12>}

説明

現在の IPv6 Link-Local 自動設定の状態を表示します。

パラメータ

パラメータ	説明
<ipif_name 12>	参照する IP インタフェース名。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

IP インタフェースの IPv6 Link-Local アドレス設定を有効にします。

```
DGS-3200-10:4#show ipif_ipv6_link_local_auto
Command: show ipif_ipv6_link_local_auto

IPIF : System        Automatic Link Local Address: Disabled.

DGS-3200-10:4#
```

第 33 章　自動コンフィグレーションコマンド

スイッチの DHCP 自動設定機能を有効にすると、スイッチは TFTP サーバから設定ファイルを受信します。そして、ブートアップ時に自動的に DHCP クライアントになるように設定します。本方法を使用するためには、DHCP サーバは TFTP サーバに IP アドレスと DHCP リプライパケット内の設定ファイル名情報を渡すように設定する必要があります。TFTP サーバはリクエストを受け取ると起動し、動作する必要があります。また、そのベースディレクトリ内に格納されている必要な設定を保持する必要があります。

コマンドラインインタフェース（CLI）における自動コンフィグレーションコマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
show autoconfig	
enable autoconfig	
disable autoconfig	

以下のセクションで各コマンドについて詳しく記述します。

show autoconfig

目的
　DHCP 自動設定機能の状態を表示します。
構文
　show autoconfig
説明
　DHCP 自動設定機能の状態を表示します。
パラメータ
　なし。
制限事項
　なし。
使用例
　DHCP 自動設定機能の状態を表示します。

```
DGS-3200-10:4#show autoconfig
Command: show autoconfig

Autoconfig State:Disabled.

DGS-3200-10:4#
```

enable autoconfig

目的
　DHCP の自動構成を有効にします。
構文
　enable autoconfig
説明
　DHCP の自動構成を有効にします。
パラメータ
　なし。
制限事項
　管理者レベルユーザのみ本コマンドを実行できます。
使用例
　DHCP の自動構成を有効にします。

```
DGS-3200-10:4#enable autoconfig
Command: enable autoconfig

Success.

DGS-3200-10:4#
```

disable autoconfig

目的

DHCP 自動設定機能を無効にします。

構文

disable autoconfig

説明

DHCP 自動設定機能を無効にします。

パラメータ

なし。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

DHCP 自動設定機能を無効にします。

```
DGS-3200-10:4#disable autoconfig
Command: disable autoconfig

Success.

DGS-3200-10:4#
```

第 34 章　デフォルトルートコマンド（レイヤ 2）

コマンドラインインタフェース（CLI）におけるデフォルトルートコマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
create iproute	default <ipaddr> {<metric 1-65535>}
delete iproute	default
show iproute	{static}
create ipv6route	[default] [<ipif_name 12> <ipv6addr> | <ipv6addr>] {<metric 1-65535>}
delete ipv6route	[[default] [<ipif_name 12> <ipv6addr> | <ipv6addr>] | all]
show ipv6route	

以下のセクションで各コマンドについて詳しく記述します。

create iproute

目的

スイッチにデフォルト IP ルートエントリを作成します。

構文

create iproute [default] <ipaddr> {<metric 1-65535>}

説明

スイッチにデフォルト IP ルートエントリを作成します。

パラメータ

パラメータ	説明
<ipaddr>	ネクストホップルータの IP アドレス。
<metric 1-65535>	ルーティングプロトコルのメトリック値。スイッチと上記 IP アドレス間のルータの数を表します。初期値は 1 です。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

スタティックアドレス「10.48.74.121」をルーティングテーブルに追加します。

```
DGS-3200-10:4#create iproute default 10.48.74.121
Command: create iproute default 10.48.74.121

Success.

DGS-3200-10:4#
```

delete iproute

目的

スイッチの IP ルーティングテーブルからデフォルト IP ルートエントリを削除します。

構文

delete iproute [default]

説明

スイッチの IP ルーティングテーブルから既存のデフォルトエントリを削除します。

パラメータ

なし。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

デフォルト IP ルートを削除します。

```
DGS-3200-10:4#delete iproute default
Command: delete iproute default

Success.

DGS-3200-10:4#
```

show iproute

目的

スイッチの現在の IP ルーティングテーブルを表示します。

構文

show iproute {static}

説明

スイッチの現在の IP ルーティングテーブルを表示します。

パラメータ

パラメータ	説明
{static}	スタティックアドレスを表示します。

制限事項

なし。

使用例

IP ルーティングテーブルの内容を表示します。

```
DGS-3200-10:4#show iproute
Command: show iproute

Routing Table

IP Address/Netmask  Gateway          Interface     Hops      Protocol
------------------  ---------------  ------------  --------  --------
10.0.0.0/8          0.0.0.0          System        1         Local

Total Entries : 1

DGS-3200-10:4#
```

create ipv6route

目的

スイッチの IP ルーティングテーブルに IPv6 デフォルトルートエントリを作成します。

構文

create ipv6route [default] [<ipif_name 12> <ipv6addr> | <ipv6addr>] {<metric 1-65535>}

説明

デフォルトスタティック IPv6 ルートエントリをスイッチの IP ルーティングテーブルに作成します。ネクストホップがグローバルアドレスであれば、インタフェース名を指定する必要はありません。ネクストホップがリンクローカルアドレスであれば、次にインタフェース名を指定する必要があります。

パラメータ

パラメータ	説明
[default]	デフォルトルートを指定します。
<ipif_name 12>	スタティックルートを作成するために IP インタフェースを入力します。本パラメータを指定しないでこのコマンドを指定すると、システム IP インタフェースに対してスタティックルートが設定されます。
<ipv6addr>	ネクストホップルータのゲートウェイ IPv6 アドレス。
<metric 1-65535>	ルーティングプロトコルのメトリック値。スイッチと上記 IP アドレス間のルータの数を表します。初期値は 1（秒）です。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

ルーティングテーブルにデフォルトスタティック IP アドレス「FEC0::5」を追加します。

```
DGS-3200-10:4#create ipv6route default System FEC0::5
Command: create ipv6route default System FEC0::5

Success.

DGS-3200-10:4#
```

delete ipv6route

目的

スイッチの IP ルーティングテーブルからデフォルト IPv6 ルートエントリを削除します。

構文

delete ipv6route [[default] [<ipif_name 12> <ipv6addr> | <ipv6addr>] | all]

説明

スイッチの IP ルーティングテーブルからデフォルト IPv6 スタティックルートを削除します。ネクストホップがグローバルアドレスであれば、インタフェース名を示す必要はありません。ネクストホップがリンクローカルアドレスであれば、次にインタフェース名を指定する必要があります。

パラメータ

パラメータ	説明
[default]	デフォルトルートを指定します。
<ipif_name 12>	IP インタフェース名。
<ipv6addr>	ネクストホップルータの IPv6 アドレス。
all	定義済みの IPv6 スタティックエントリのすべてを削除します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

デフォルト IP ルートを削除します。

```
DGS-3200-10:4#delete ipv6route default System FEC0::5
Command: delete ipv6route default System FEC0::5

Success.

DGS-3200-10:4#
```

show ipv6route

目的

スイッチの現在のスタティック IPv6 ルーティングテーブルを表示します。

構文

show ipv6route

説明

スイッチの現在のスタティック IPv6 ルーティングテーブルを表示します。

パラメータ

なし。

制限事項

なし。

使用例

ルーティングテーブルの IPv6 エントリを表示します。

```
DGS-3200-10:4#show ipv6route
Command: show ipv6route

IPv6 Prefix:  ::/0              Protocol: Static     Metric: 1
Next Hop   :   FEC0::5          IPIF    : System

Total Entries:1

DGS-3200-10:4#
```

第 35 章　ARP コマンド

ARP（Address Resolution Protocol）は、ホストのハードウェアアドレス (MAC アドレス) を検索するための標準規格です。ARP は、IP アドレスを物理的なアドレスに変換し、IP アドレスと MAC アドレスを対応させます。ここでは特定のデバイスに対する ARP 情報を参照、編集および削除することができます。

コマンドラインインタフェース（CLI）における ARP コマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
create arpentry	<ipaddr> <macaddr>
delete arpentry	[<ipaddr> | all]
config arpentry	<ipaddr> <macaddr>
config arp_aging time	<value 0-65535>
show arpentry	{ipif <ipif_name 12> | ipaddress <ipaddr> | static}
clear arptable	

以下のセクションで各コマンドについて詳しく記述します。

create arpentry

目的

ARP テーブルにスタティックエントリを作成します。

構文

create arpentry <ipaddr> <macaddr>

説明

スイッチの ARP テーブルに IP アドレスと対応する MAC アドレスを入力します。

パラメータ

パラメータ	説明
<ipaddr>	エンドノードまたはステーションの IP アドレス。
<macaddr>	上記 IP アドレスに対応する MAC アドレス。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

IP アドレス 10.48.74.121 と MAC アドレス「00:50:BA:00:07:36」というスタティック ARP エントリを作成します。

```
DGS-3200-10:4#create arpentry 10.48.74.121 00-50-BA-00-07-36
Command: create arpentry 10.48.74.121 00-50-BA-00-07-36

Success.

DGS-3200-10:4#
```

delete arpentry

目的

ARP テーブルのスタティック ARP エントリを削除します。

構文

delete arpentry [<ipaddr> | all]

説明

上記「create arpentry」コマンドで作成したスタティック ARP エントリを、エントリの IP アドレスまたは「all」を指定することにより削除します。「all」を指定すると、スイッチの ARP テーブルはすべてクリアされます。

パラメータ

パラメータ	説明
<ipaddr>	エンドノードまたはステーションの IP アドレス。
all	すべての ARP エントリを削除します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

IP アドレス「10.48.74.121」を持つエントリを ARP テーブルから削除します。

```
DGS-3200-10:4#delete arpentry 10.48.74.121
Command: delete arpentry 10.48.74.121

Success.

DGS-3200-10:4#
```

config arpentry

目的

ARP テーブルのスタティック ARP エントリを設定します。

構文

config arpentry <ipaddr> <macaddr>

説明

ARP テーブルにスタティックエントリを設定します。スイッチの ARP テーブルにエントリの IP アドレスと対応する MAC アドレスを入力します。

パラメータ

パラメータ	説明
<ipaddr>	エンドノードまたはステーションの IP アドレス。
<macaddr>	上記 IP アドレスに対応する MAC アドレス。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

IP アドレス 10.48.74.12 と MAC アドレス 00:50:BA:00:07:36 というスタティック ARP エントリを設定します。

```
DGS-3200-10:4#config arpentry 10.48.74.12 00-50-BA-00-07-36
Command: config arpentry 10.48.74.12 00-50-BA-00-07-36

Success.

DGS-3200-10:4#
```

config arp_aging time

目的

スイッチの ARP テーブルエントリにエージングタイマを設定します。

構文

config arp_aging time <value 0-65535>

説明

テーブルから削除される前に ARP エントリがアクセスされないまま、スイッチの ARP テーブルに保存される最大時間（分）を設定します。

パラメータ

パラメータ	説明
time <value 0-65535>	ARP エージングタイム（秒）。値は 0-65535 の範囲から指定できます。初期値は 20（分）です。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

ARP エージングタイムを設定します。

```
DGS-3200-10:4#config arp_aging time 30
Command: config arp_aging time 30

Success.

DGS-3200-10:4#
```

show arpentry

目的

ARP テーブルを表示します。

構文

show arpentry {ipif <ipif_name 12> | ipaddress <ipaddr> | static}

説明

スイッチの ARP テーブルの現在の内容を表示します。IP アドレス、インタフェース名、またはスタティックエントリで表示をフィルタすることができます。

パラメータ

パラメータ	説明
ipif <ipif_name 12>	作成された ARP テーブルのエンドノードまたはステーションが存在する IP インタフェース名。
ipaddress <ipaddr>	上記 IP インタフェースに対応するネットワークアドレス。
static	ARP テーブル内のスタティックエントリを表示します。

パラメータが指定されないと、すべての ARP エントリを表示します。

制限事項

なし。

使用例

ARP テーブルを表示します。

```
DGS-3200-10:4#show arpentry
Command: show arpentry

ARP Aging Time : 20

Interface       IP Address        MAC Address         Type
--------------  ----------------  ------------------  ---------------
System          10.0.0.0          FF-FF-FF-FF-FF-FF   Local/Broadcast
System          10.90.90.90       00-01-02-03-04-00   Local
System          10.255.255.255    FF-FF-FF-FF-FF-FF   Local/Broadcast

Total Entries: 3

DGS-3200-10:4#
```

clear arptable

目的

すべてのダイナミック ARP テーブルエントリを削除します。

構文

clear arptable

説明

スイッチの ARP テーブルからダイナミック ARP テーブルエントリを削除します。スタティック ARP テーブルエントリは影響を受けません。

パラメータ

なし。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

ARP テーブル内のダイナミックエントリを削除します。

```
DGS-3200-10:4#clear arptable
Command: clear arptable

Success.

DGS-3200-10:4#
```

第 36 章　ループバック検知コマンド

ループバック検知機能は、特定ポートに生成されたループを検出します。

コマンドラインインタフェース（CLI）におけるループバック検知コマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
config loopdetect	{recover_timer [<value 0> | <value 60-1000000>] | interval <value 1-32767> | mode [port-based | vlan-based]}
config loopdetect ports	[<portlist> | all] state [enable | disable]
enable loopdetect	
disable loopdetect	
show loopdetect	
show loopdetect ports	[all | <portlist>]
config loopdetect trap	[none | loop_detected | loop_cleared | both]

以下のセクションで各コマンドについて詳しく記述します。

config loopdetect

目的

スイッチにループバック検知機能を設定します。

構文

config loopdetect {recover_timer [<value 0> | <value 60-1000000>] | interval <value 1-32767> | mode [port-based | vlan-based]}

説明

スイッチにループバック検知機能（LBD）を設定します。

パラメータ

パラメータ	説明
recover_timer [<value 0> | <value 60-1000000>]	ループ状態がなくなったかをチェックする時間を決定するためにオートリカバリ (自動復旧) メカニズムが使用する間隔（秒）。60-1000000 で設定します。 0 は特別な値で、オートリカバリメカニズムの無効を意味します。そのため、手動で無効ポートを回復する必要があります。初期値は 60（秒）です。
interval <value 1-32767>	デバイスがループバックイベントを検出するためにすべての CTP(Configuration Test Protocol) パケットを送信する間隔（秒）。1-32767 で設定します。 初期値は 10（秒）です。
mode [port-based | vlan-based]	ループ検出動作モードを選択します。 • port-based - ポートベースモードでは、ポートはループを検知すると、無効となります。 • vlan-based - VLAN ベースモードでは、ポートは、ループを検知にかかわるポートに到達する VLAN パケットを処理することはできません。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

VLAN ベースモードで「recover_timer」を 0、「interval」を 20 に設定します。

```
DGS-3200-10:4# config loopdetect recover_timer 0 interval 20 mode vlan-based
Command: config loopdetect recover_timer 0 interval 20 mode vlan-based

Success.

DGS-3200-10:4#
```

config loopdetect ports

目的

スイッチのポートにループバック検知機能を設定します。

構文

config loopdetect ports [<portlist>| all] state [enable | disable]

説明

スイッチ上のインタフェースにループバック検知機能を設定します。

パラメータ

パラメータ	説明
ports [<portlist> | all]	• <portlist>- 設定するポートまたはポート範囲を指定します。 • all - システムのすべてのポートを設定します。
state [enable | disable]	ポートリストに指定されたポートにループバック検知機能を有効または無効にします。初期値では無効に設定されています。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

ループバック検知機能を有効にします。

```
DGS-3200-10:4# config loopdetect ports 1-5 state enable
Command: config loopdetect ports 1-5 state enable

Success.

DGS-3200-10:4#
```

enable loopdetect

目的

ループバック検知機能をグローバルに有効にします。

構文

enable loopdetect

説明

ループバック検知機能をグローバルに有効にします。初期値は有効です。

パラメータ

なし。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

ループバック検知機能をグローバルに有効にします。

```
DGS-3200-10:4#show loopdetect
Command: show loopdetect

 Loopdetect Global Settings
 ---------------------------
 Loopdetect Status         : Disabled
 Loopdetect Interval       : 10
 Recover Time              : 60
 Mode                      : Port-Based

DGS-3200-10: 4#
```

disable loopdetect

目的
　ループバック検知機能をグローバルに無効にします。
構文
　enable loopdetect
説明
　ループバック検知機能をグローバルに無効にします。初期値は有効です。
パラメータ
　なし。
制限事項
　管理者レベルユーザのみ本コマンドを実行できます。
使用例
　ループバック検知機能をグローバルに無効にします。

```
DGS-3200-10:4#disable loopdetect
Command: disable loopdetect

Success.

DGS-3200-10:4#
```

show loopdetect

目的
　スイッチの現在のループバック検知機能の設定を表示します。
構文
　show loopdetect
説明
　スイッチの現在のループバック検知機能の設定を表示します。
パラメータ
　なし。
制限事項
　なし。
使用例
　スイッチの現在のループバック検知機能の設定を表示します。

```
DGS-3200-10:4#show loopdetect
Command: show loopdetect

LBD Global Settings
------------------------------
LBD Status       : Disabled
LBD Interval     : 10
LBD Recover Time : 60
LBD Mode         : Port-Based
LBD Trap Status  : None

DGS-3200-10:4#
```

show loopdetect ports

目的

スイッチの現在のポート単位のループバック検知設定を表示します。

構文

show loopdetect ports [all | <portlist>]

説明

スイッチの現在のポート単位のループバック検知設定とステータスを表示します。

パラメータ

パラメータ	説明
ports [all | <portlist>]	• all - すべてのポートのループバック検知情報を表示します。 • <portlist> - 表示するポートまたはポート範囲を指定します。

制限事項

なし。

使用例

ポートベースモードのポート 1 から 9 のループバック検知状態を表示します。

```
DGS-3200-10:4#show loopdetect ports 1-9
Command: show loopdetect ports 1-9

Port Loopdetect State    Loop Status
---- ----------------    -----------------
1    Enabled             Normal
2    Enabled             Normal
3    Enabled             Normal
4    Enabled             Normal
5    Enabled             Loop!
6    Enabled             Normal
7    Enabled             Loop!
8    Enabled             Normal
9    Enabled             Normal

DGS-3200-10:4#
```

VLAN ベースモードのポート 1 から 9 のループバック検知状態を表示します。

```
DGS-3200-10:4#show loopdetect ports 1-9
Command: show loopdetect ports 1-9

Port Loopdetect State  Loop VLAN
---- ----------------  -----------------
1    Enabled           None
2    Enabled           None
3    Enabled           None
4    Enabled           None
5    Enabled            2
6    Enabled           None
7    Enabled            2
8    Enabled           None
9    Enabled           None

DGS-3200-10:4#
```

config loopdetect trap

目的

トラップモードを設定します。

構文

config loopdetect trap [none | loop_detected | loop_cleared | both]

説明

トラップモードを設定します。ループ状態が検出されると、ループ検出トラップが送信され、ループ状態がクリアされると、ループクリアのトラップが送信されます。

パラメータ

パラメータ	説明
none	両方の状態を検出すると、トラップを送信しません。
loop_detected	ループ状態を検出すると、トラップを送信します。
loop_cleared	ループ状態がクリアされると、トラップを送信します。
both	両方の状態を検出すると、トラップを送信します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

トラップモードを設定します。

```
DGS-3200-10:4#config loopdetect trap both
Command: config loopdetect trap both

Success.

DGS-3200-10:4#
```

第 37 章　IGMP Snooping コマンド

IGMP（Internet Group Management Protocol）Snooping 機能を利用すると、スイッチはネットワークステーションまたはデバイスと IGMP ホスト間で送信される IGMP クエリと IGMP レポートを認識するようになります。また、スイッチを通過する IGMP メッセージの情報に基づいて、指定したデバイスに接続するポートをオープン / クローズできるようになります。

コマンドラインインタフェース（CLI）における IGMP Snooping コマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
config igmp_snooping	[vlan_name <vlan_name 32> | vlanid <vidlist> | all] {host_timeout <sec 1-16711450> | router_timeout <sec 1-16711450> | leave_timer <sec 1-16711450> | state [enable | disable] | fast_leave [enable | disable] }
config igmp_snooping querier	[vlan_name <vlan_name 32> | vlanid <vidlist> | all]{ query_interval <sec 1-65535> | max_response_time <sec 1-25> | robustness_variable <value 1-255> | last_member_query_interval <sec 1-25> | state [enable | disable] version <value 1-3> }
config router_ports	<vlan_name 32> [add | delete] <portlist>
config router_ports_forbidden	<vlan_name 32> [add | delete] <portlist>
enable igmp_snooping	
disable igmp_snooping	
show igmp_snooping	{vlan <vlan_name 32> | vlanid <vidlist>}
show igmp snooping group	{vlan <vlan_name 32> | vlanid <vidlist>} {data_driven}
config igmp_snooping data_driven_learning	[vlan <vlan_name 32> | vlanid <vidlist> | all] {state [enable | disable] | aged_out [enable | disable]}
config igmp_snooping data_ driven_ learning max_learned_entry	<value 1-256>
clear igmp_snooping data_ driven_group	[all | [vlan <vlan_name 32> | vlanid <vlanid 1-4094>] [<ipaddress>| all]]
show router_ports	{vlan <vlan_name 32> | vlanid <vidlist>} {[static | dynamic | forbidden]}

以下のセクションで各コマンドについて詳しく記述します。

config igmp_snooping

目的

スイッチに IGMP Snooping を設定します。

構文

config igmp_snooping [vlan_name <vlan_name 32> | vlanid <vidlist> | all]{ host_timeout <sec 1-16711450> | router_timeout <sec 1-16711450> | leave_timer <sec 1-16711450> | state [enable | disable] | fast_leave [enable | disable] }

説明

スイッチに IGMP Snooping を設定します。

パラメータ

パラメータ	説明
vlan_name <vlan_name 32> | vlanid <vidlist> | all	• <vlan_name 32> - IGMP Snooping を設定する VLAN 名。 • vlanid<vlan_list> - IGMP Snooping を設定する VLAN ID。 • all - すべての VLAN を示します。
host_timeout <sec 1-16711450>	スイッチが Host membership report を受信しない場合に、ホストがマルチキャストグループのメンバで居続ける最大時間（秒）。初期値は 260（秒）です。
router_timeout <sec 1-16711450>	スイッチが Host membership report を受信しない場合に、ルータがマルチキャストグループのメンバで居続ける最大時間（秒）。初期値は 260（秒）です。
leave_timer <sec 1-16711450>	leave group メッセージを送信した後に、マルチキャストアドレスが削除されずにデータベースに保持される時間。初期値は 2（秒）です。
state[enable | disable]	指定された VLAN の IGMP Snooping を「enable」（有効）または「disable」（無効）にします。
fast_leave [enable | disable]	Fast Leave 機能を「enable」（有効）または「disable」（無効）にします。この機能が有効になると、スイッチが IGMP Leave Report パケットを受信する時、マルチキャストグループのメンバは（Last Member Query Time の失効を待たずに）直ちにグループから離脱します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

IGMP Snooping を設定します。

```
DGS-3200-10:4#config igmp_snooping vlan default host_timeout 250 state enable
Command: config igmp_snooping vlan default host_timeout 250 state enable

Success.

DGS-3200-10:4#
```

config igmp_snooping querier

目的

IGMP Snooping クエリアを設定します。

構文

config igmp_snooping querier [vlan_name <vlan_name 32> | vlanid <vidlist> | all]{ query_interval <sec 1-65535> | max_response_time <sec 1-25> | robustness_variable <value 1-255> | last_member_query_interval <sec 1-25> | state [enable | disable] version <value 1-3> }

説明

通常のクエリ送信の間隔（秒）、メンバからのレポートを待つ最大時間（秒）および IGMP Snooping を保証する許容パケット損失を設定します。

パラメータ

パラメータ	説明
vlan_name <vlan_name 32> | vlanid <vidlist> | all	• <vlan_name 32> - IGMP Snooping クエリアを設定する VLAN 名。 • vlanid <vidlist> - IGMP Snooping クエリアを設定する VLAN ID。 • all - すべての VLAN を示します。
query_interval <sec 1-65535>	一般的なクエリア送信間隔（秒）を指定します。初期値は 125（秒）です。
max_response_time <sec 1-25>	メンバからのレポートを待つ最大時間（秒）。初期値は 10（秒）です。
robustness_variable <value 1-255>	予想されるサブネット上のパケットの損失に応じてこの変数を調整します。Robustness Variable は以下の IGMP メッセージ間隔を計算する場合に使用されます。 • Group member interval - マルチキャストルータがネットワーク上のグループにメンバがいないと判断するまでの時間。次の計算式で計算されます。Group Listener=（Robustness Variable*Query Interval）+（1*Query Interval）。 • Querier Present Interval - マルチキャストルータがクエリアである他のマルチキャストルータがないと判断するまでの時間。次の計算式で計算されます。Querier Present Interval=（Robustness Variable*Query Interval）+（0.5*Query Response Interval）。 • Last Listener Query Count - マルチキャストルータがこのグループ内にローカルメンバがいないと見なす前に送信された Group-Specific Query 数。初期値は Robustness Variable の値です。 • 初期値では、Robustness Variable は 2 です。サブネットが高いパケット損失を持つと予想する場合には、この値を増やしたくなるかもしれません。1 は有効なエントリとして指定されますが、Robustness Variable を 1 とすると問題が生じる可能性があり、設定しないようにしてください。
last_member_query_interval <sec 1-25>	Leave Group メッセージを受け取った時に送信する Group-Specific Membership Query の最大間隔（秒）。また、同 Query の送信間隔でもあります。この間隔はルータがラストメンバグループの損失を検出するためにかかる時間をより減少するように低くします。Leave メッセージを受信する場合、ルータは、応答時間後 (last member query interval*robustness variable) に受信したレポートがないと、インタフェース上にローカルメンバがいないものと見なします。
state [enable | disable]	• enable - スイッチが IGMP クエリパケットを送信する IGMP クエリアとして選択されます。 • disable - スイッチが IGMP クエリアとしての役目を果たしません。スイッチに接続するレイヤ 3 ルータが IGMP プロキシ機能だけを提供し、マルチキャストルーティング機能を提供しない場合、この状態は無効に設定されます。そうでない場合、レイヤ 3 ルータがクエリアとして選択さないと、それは IGMP クエリパケットを送信しません。また、マルチキャストルーティングプロトコルパケットを送信しないため、ポートはルータポートとしてタイムアウトになります。
version <value 1-3>	本ポートに送信される IGMP パケットのバージョンを指定します。インタフェースが受信した IGMP パケットが指定バージョンより高いバージョンであった場合、そのパケットは破棄されます。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

IGMP Snooping クエリアを設定します。

```
DGS-3200-10:4#config igmp_snooping querier vlan default query_interval 125 state enable
Command: config igmp_snooping querier vlan default query_interval 125 state enable

Success.

DGS-3200-10:4#
```

config router_ports

目的

ルータポートとしてポートを設定します。

構文

config router_ports <vlan_name 32> [add | delete] <portlist>

説明

マルチキャストが有効なルータに接続するポート範囲を指定します。これは、宛先として本ルータが持つすべてのパケットをプロトコルなどにかかわらず、マルチキャストが有効なルータに到達するように設定します。

パラメータ

パラメータ	説明
<vlan_name 32>	ルータポートが存在する VLAN 名。
[add | delete]	指定した VLAN にルータポートを追加または削除します。
<portlist>	ポートまたはポート範囲を設定します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

スタティックルータポートを設定します。

```
DGS-3200-10:4#config router_ports default add 1-8
Command: config router_ports default add 1-8

Success.

DGS-3200-10:4#
```

config router_ports_forbidden

目的

禁止マルチキャストルータポートを設定します。

構文

config router_ports_forbidden <vlan_name 32> [add | delete] <portlist>

説明

マルチキャストが有効なルータに接続する禁止ポート（ポート範囲）を選択します。これは、マルチキャストパケットがプロトコルなどにかかわらずこのポートに送信されないようにします。

パラメータ

パラメータ	説明
<vlan_name 32>	ルータポートが存在する VLAN 名。
[add | delete]	指定された VLAN の禁止ポートを追加または削除します。
<portlist>	禁止ポートとして設定するポートまたは範囲を指定します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

ポート 1-7 をデフォルト VLAN の禁止ルータポートに設定します。

```
DGS-3200-10:4#config router_ports_forbidden default add 1-7
Command: config router_ports_forbidden default add 1-7

Success.

DGS-3200-10:4#
```

enable igmp_snooping

目的
　スイッチの IGMP Snooping を有効にします。
構文
　enable igmp_snooping
説明
　スイッチの IGMP Snooping を有効にします。
パラメータ
　なし。
制限事項
　管理者レベルユーザのみ本コマンドを実行できます。
使用例
　スイッチに IGMP Snooping を有効にします。

```
DGS-3200-10:4#enable igmp_snooping
Command: enable igmp_snooping

Success.

DGS-3200-10:4#
```

disable igmp_snooping

目的
　スイッチの IGMP Snooping を無効にします。
構文
　disable igmp_snooping
説明
　スイッチの IGMP Snooping を無効にします。
パラメータ
　なし。
制限事項
　管理者レベルユーザのみ本コマンドを実行できます。
使用例
　スイッチの IGMP Snooping を無効にします。

```
DGS-3200-10:4#disable igmp_snooping
Command: disable igmp_snooping

Success.

DGS-3200-10:4#
```

show igmp_snooping

目的

スイッチの現在の IGMP Snooping ステータスを表示します。

構文

show igmp_snooping {vlan <vlan_name 32> | vlanid <vidlist>}

説明

スイッチの現在の IGMP Snooping ステータスを表示します。

パラメータ

パラメータ	説明
vlan <vlan_name 32>	IGMP Snooping 設定を参照する VLAN 名。
vlanid <vidlist>	IGMP Snooping 設定を参照する VLAN ID。

パラメータが指定されないと、システムはすべての IGMP Snooping 設定を表示します。

制限事項

なし。

使用例

IGMP Snooping を参照します。

```
DGS-3200-10:4#show igmp_snooping
Command: show igmp_snooping

IGMP Snooping Global State : Disabled
Data Learn Max Entries     : 56

VLAN Name                  : default
Query Interval             : 125
Max Response Time          : 10
Robustness Value           : 2
Last Member Query Interval : 1
Host Timeout               : 260
Router Timeout              : 260
Leave Timer                : 2
Querier State              : Disabled
Querier Router Behavior    : Non-Querier
State                      : Disabled
Fast Leave                 : Disabled
Version                    : 3
Data Learn State           : Enabled
Data Learn Aged            : Disabled

Total Entries: 1

DGS-3200-10:4#
```

show igmp_snooping group

目的

スイッチに設定されている現在の IGMP Snooping 設定を表示します。

構文

show igmp_snooping group {[vlan <vlan_name 32> | vlanid <vidlist>]} {data_driven}

説明

スイッチに設定されている現在の IGMP Snooping グループ設定を表示します。

パラメータ

パラメータ	説明
vlan <vlan_name 32> | vlanid <vidlist>	• <vlan_name 32> - IGMP Snooping グループ情報を参照する VLAN 名。 • <vidlist> - IGMP Snooping 設定を参照する VLAN ID。 パラメータを指定しないと、システムはすべての IGMP snooping グループ設定情報を表示します。
data_driven	Data Driven 型の IGMP snooping グループエントリを表示します。

制限事項

なし。

使用例

現在の IGMP Snooping グループを参照します。

```
DGS-3200-10:4#show igmp_snooping group
Command: show igmp_snooping group

Source/Group     : NULL / 225.0.0.3
VLAN Name/VID    : default/1
Reports          : 2
Member Ports     : 8
Router Ports     : 5
Up Time          : 3
Expiry Time      : 257
Mode             : EXCLUDE

Source/Group     : NULL / 239.255.255.250
VLAN Name/VID    : default/1
Reports          : 4
Member Ports     : 8
Router Ports     : 5
Up Time          : 246
Expiry Time      : 174
Mode             : EXCLUDE

Total Entries : 2

DGS-3200-10:4#
```

config igmp_snooping data_driven_learning

目的

IGMP Snooping グループの Data Driven Learning を有効または無効にします。

構文

config igmp_snooping data_driven_learning [vlan <vlan_name 32> | vlanid <vidlist> | all] {state [enable | disable] | aged_out [enable | disable]}

説明

IGMP Snooping グループの Data Driven Learning を有効または無効にします。

Data Driven Learning が VLAN に対して有効な場合、スイッチはこの VLAN に IP マルチキャストトラフィックを受信し、IGMP Snooping グループを作成します。つまり、エントリの学習は IGMP メンバシップ登録ではなく、トラフィックによりアクティブになります。通常の IGMP Snooping エントリのために、IGMP プロトコルはエントリのエージングアウトを認めます。Data Driven エントリのために、エントリは、エージングアウトしないように指定されるか、またはエージングタイマによってエージングアウトするように指定されます。

Data Driven Learning を有効にすると、すべてのポートのマルチキャストフィルタリングモードは無視されます。これは、マルチキャストパケットがフラッドされることを意味します。Data Driven グループが作成され、IGMP メンバポートが後で学習されると、エントリは、通常の IGMP Snooping エントリになります。つまり、エージングアウトメカニズムは、通常、IGMP Snooping エントリのルールに従いします。

パラメータ

パラメータ	説明
vlan <vlan_name 32> | vlanid <vidlist> | all	• <vlan_name 32> - 設定を行う VLAN 名を指定します。 • vlanid <vidlist> - 設定を行う VLAN ID を指定します。 • all - すべての VLAN に設定します。
state [enable | disable]	IGMP Snooping グループの Data Driven Learning を有効または無効にします。初期値は「enable」です。
aged_out [enable | disable]	エントリのエージングを有効または無効にします。初期値では「disable」(無効) になっています。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

デフォルト VLAN について IGMP Snooping グループの Data Driven Learning を有効または無効にします。

```
DGS-3200-10:4#config igmp_snooping data_driven_learning vlan default state enable
Command: config igmp_snooping data_driven_learning vlan default state enable

Success.

DGS-3200-10:4#
```

config igmp_snooping data_driven_learning max_learned_entry

目的

Data Driven 方式により学習するグループの最大エントリ数を指定します。

構文

config igmp_snooping data_driven_learning max_learned_entry <value 1-256>

説明

Data Driven 方式により学習するグループの最大エントリ数を指定します。テーブルがいっぱいになると、システムは、新しい Data Driven グループの学習を中止します。新しいグループ用のトラフィックは破棄されます。

パラメータ

パラメータ	説明
max_learned_entry <value 1-256>	Data Driven 方式が学習するグループの最大エントリ数を指定します。初期値は 8 です。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

Data Driven 方式が学習するグループの最大エントリ数を指定します

```
DGS-3200-10:4#config igmp_snooping data_driven_learning max_learned_entry 50
Command: config igmp_snooping data_driven_learning max_learned_entry 50

Success.

DGS-3200-10:4#
```

clear igmp_snooping data_driven_group

目的

Data Driven 方式で学習したすべての IGMP Snooping グループを削除します。

構文

clear igmp_snooping data_ driven _group [all | [vlan <vlan_name 32> | vlanid <vlanid 1-4094>] [<ipaddress> | all]]

説明

Data Driven 方式で学習したすべての IGMP Snooping グループを削除します。

パラメータ

パラメータ	説明
all | [vlan <vlan_name 32> | vlanid <vlanid 1-4094>	• all - Data Driven 方式で学習したすべての全エントリを削除します。 • vlan <vlan_name 32> - 削除する VLAN 名を指定します。 • <vlanid 1-4094> - 削除する VLAN ID を指定します。
<ipaddress> | all	• ipaddress - 削除する IP アドレスを指定します。 • all - すべての IP アドレスを削除します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

Data Driven が学習したすべてのグループを削除します。

```
DGS-3200-10:4#clear igmp_snooping data_driven_group all
Command: clear igmp_snooping data_driven_group all

Success.

DGS-3200-10:4#
```

show router_ports

目的

スイッチに設定されている現在のルータポートを表示します。

構文

show router_ports {vlan <vlan_name 32> | vlanid <vidlist>} {[static | dynamic | forbidden]}

説明

スイッチに設定されている現在のルータポートを表示します。

パラメータ

パラメータ	説明
vlan <vlan_name 32> | vlanid <vidlist>	• vlan <vlan_name 32> - ルータポートが存在する VLAN 名。 • vlanid <vidlist> - ルータポートが存在する VLAN ID。
static | dynamic | forbidden	• static - スタティックに設定されたルータポートを表示します。 • dynamic - ダイナミックに設定されたルータポートを表示します。 • forbidden - ルータポートになることが禁止されているポートを表示します。

制限事項

なし。

使用例

ルータポートを表示します。

```
DGS-3200-10:4#show router_ports
Command: show router_ports

VLAN Name             :default
Static router port    :1-7
Dynamic router port   :
Forbidden router port :

VLAN Name             : vlan2
Static router port    :
Dynamic router port   :
Forbidden router port :

Total Entries : 2

DGS-3200-10:4#
```

第 38 章　IGMP 認証コマンド

スイッチ上の各ポートに IGMP 認証（IGMP アクセスコントロール）を設定することができます。

コマンドラインインタフェース（CLI）における IGMP 認証コマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
config igmp access_authentication	ports [all | <portlist>] state [enable | disable]
show igmp access_authentication	ports [all | <portlist>]

以下のセクションで各コマンドについて詳しく記述します。

config igmp access_authentication ports

目的

IGMP 認証ポートのステータスを設定します。

構文

config igmp access_authentication ports [all | <portlist>] state [enable | disable]

説明

指定の VLAN に対して IGMP 認証を有効または無効にします。認証を有効にして、スイッチが IGMP JOIN リクエストを受信すると、スイッチは、認証を行うために RADIUS サーバにアクセスリクエストを送信します。

パラメータ

パラメータ	説明
ports [all | <portlist>]	• <portlist> - 設定するポート範囲を指定します。 • all - すべてのポートを指定します。
state [enable | disable]	指定ポートの RADIUS 認証機能を有効または無効にします。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

すべてのポートに IGMP 認証を有効にします。

```
DGS-3200-10:4#config igmp access_authentication ports all state enable
Command: config igmp access_authentication ports all state enable

Success.

DGS-3200-10:4#
```

show igmp access_authentication ports

目的

現在の IGMP 認証設定を表示します。

構文

show igmp access_authentication ports [all |<portlist>]

説明

現在の IGMP 認証設定を表示します。

パラメータ

パラメータ	説明
all	すべてのポートを表示します。
portlist	表示するポート範囲を指定します。

ポートリストを指定しない場合、すべてのポートの情報を表示します。

制限事項

なし。

使用例

ポート 1-4 の IGMP アクセスコントロール状態を表示します。

```
DGS-3200-10:4#show igmp access_authentication ports 1-4
Command: show igmp access_authentication ports 1-4

Port  Authentication State
----- --------------------
1     Enabled
2     Disabled
3     Disabled
4     Enabled

DGS-3200-10:4#
```

第 39 章　MLD Snooping コマンド

Multicast Listener Discovery（MLD）Snooping は、IPv4 の IGMP Snooping と同じように使用される IPv6 機能です。マルチキャストデータを要求する VLAN に接続しているポートを検出するために使用されます。選択した VLAN 上のすべてのポートにマルチキャストトラフィックが流れる替わりに、MLD Snooping は、リクエストポートとマルチキャストの送信元によって生成する MLD クエリと MLD レポートを使用してデータを受信したいポートにのみマルチキャストデータを転送します。
MLD Snooping は、エンドノードと MLD ルータ間で交換される MLD コントロールパケットのレイヤ 3 部分を調査することで実行されます。ルータがマルチキャストトラフィックをリクエストしていることをスイッチが検出すると、該当ポートを IPv6 マルチキャストテーブルに直接追加し、そのポートにマルチキャストトラフィックを転送する処理を開始します。マルチキャストルーティングテーブル内のこのエントリは該当ポート、その VLAN ID、および関連する IPv6 マルチキャストグループアドレスを記録し、このポートをアクティブな Listening ポートと見なします。アクティブな Listening ポートはマルチキャストグループデータの受信だけをします。

MLD コントロールメッセージ

MLD Snooping を使用するデバイス間で 3 つのタイプのメッセージを交換します。これらのメッセージは、130、131、132 および 143 にラベル付けされた 4 つの ICMPv6 パケットヘッダによって定義されています。

1. Multicast Listener Query – IPv4 の IGMPv2 Host Membership Query（HMQ）と類似のものです。ルータは ICMPv6 パケットヘッダ内に 130 とラベル付けされた本メッセージを送信し、マルチキャストデータをリクエストしているリンクがあるかどうか問い合わせます。ルータが送信する MLD クエリメッセージには 2 つのタイプがあります。General Query は全マルチキャストアドレスに Listening ポートすべてにマルチキャストデータを送信する準備が整ったことを通知するために使用します。また、Multicast Specific query は特定のマルチキャストアドレスに送信準備が整ったことを通知するために使用します。 2 つのメッセージタイプは IPv6 ヘッダ内のマルチキャスト終点アドレス、および Multicast Listener クエリメッセージ内のマルチキャストアドレスによって区別します。
2. Multicast Listener Report Version1 – IGMPv2 の Host Membership Report（HMR）と類似のものです。Listening ポートは、Multicast Listener クエリメッセージに応じて ICMPv6 パケットヘッダ内に 131 とラベル付けされた本メッセージをクエリスイッチに送信し、マルチキャストアドレスからマルチキャストデータを受信する希望があることを伝えます。
3. Multicast Listener Done – IGMPv2 の Leave Group Message と類似のものです。マルチキャスト Listening ポートは、ICMPv6 パケットヘッダ内に 132 とラベル付けされた本メッセージを送信し、特定のマルチキャストグループアドレスからマルチキャストデータを受信せず、このアドレスからのマルチキャストデータとともに” done”（完了）した旨を伝えます。スイッチは本メッセージを受信すると、この Listening ポートには特定のマルチキャストグループアドレスからのマルチキャストトラフィックを送信しません。
4. Multicast Listener Report Version2 – IGMPv3 の Host Membership Report（HMR）と類似のものです。Listening ポートは、Multicast Listener クエリメッセージに応じて ICMPv6 パケットヘッダ内に 143 とラベル付けされた本メッセージをクエリスイッチに送信し、マルチキャストアドレスからマルチキャストデータを受信する希望があることを伝えます。

コマンドラインインタフェース（CLI）における MLD Snooping コマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
config mld_snooping	[vlan <vlan_name 32> | vlanid <vidlist> | all] {node_timeout <sec 1-16711450> | router_timeout <sec 1-16711450> | done_timer <sec 1-16711450> | state [enable | disable] | fast_done [enable | disable]}
config mld_snooping querier	[vlan <vlan_name 32> | vlanid <vidlist> | all] {query_interval <sec 1-65535> | max_response_time <sec 1-25> | robustness_variable <value 1-255> | last_listener_query_interval <sec 1-25> | state [enable | disable] | version<value 1-2>}
config mld_snooping mrouter_ports	<vlan_name 32> [add | delete] <portlist>
config mld_snooping mrouter_ports_forbidden	<vlan_name 32> [add | delete] <portlist>
enable mld_snooping	
disable mld_snooping	
show mld_snooping	{[vlan<vlan_name 32 | vlanid <vidlist>]}
show mld_snooping group	{[vlan <vlan_name 32 | vlanid <vidlist>]}
show mld_snooping mrouter_ports	{[vlan <vlan_name 32 | vlanid <vidlist>]} {[static | dynamic | forbidden]}

以下のセクションで各コマンドについて詳しく記述します。

config mld_snooping

目的

スイッチに MLD Snooping を設定します。

構文

config mld_snooping [vlan <vlan_name 32> | vlanid <vidlist> | all] {node_timeout <sec 1-16711450> | router_timeout <sec 1-16711450> | done_timer <sec 1-16711450> | state [enable | disable] | fast_done [enable | disable]}

説明

スイッチに MLD Snooping を設定します。

パラメータ

パラメータ	説明
vlan <vlan_name 32> | vlanid <vidlist> | all	• vlan <vlan_name 32> - 設定する MLD Snooping に対する VLAN 名。 • vlanid <vidlist> - 設定する MLD Snooping に対する VLAN ID。 • all - すべての VLAN を示します。
node_timeout <sec 1-16711450>	リンクノードのタイムアウト（秒）を指定します。この時間に達すると、このノードはリスニングノードとして見なされません。1 から 16711450 で設定でき、初期値は 260（秒）です。
router_timeout <sec 1-16711450>	ノードリスナーレポートなしでマルチキャストグループのリスニングノードとしてスイッチのルーティングテーブルに保持される最大の時間（秒）を設定します。1 から 16711450 で設定でき、初期値は 260（秒）です。
done_timer <sec 1-16711450>	ノードリスナーレポートなしでグループから done メッセージを受信した後にルータがスイッチに保持される最大の時間（秒）を設定します。1 から 16711450 で設定でき、初期値は 2（秒）です。
state [enable | disable]	指定された VLAN の MLD Snooping を「enable」（有効）または「disable」（無効）にします。
fast_done [enable | disable]	Fast done 機能を「enable」（有効）または「disable」（無効）にします。この機能を「enable」にするとマルチキャストグループのメンバは done メッセージがスイッチに受信されるとすぐにグループから抜けることができます。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

MLD Snooping を設定します。

```
DGS-3200-10:4#config mld_snooping vlan default node_timeout 250 state enable
Command: config mld_snooping vlan default node_timeout 250 state enable

Success.

DGS-3200-10:4#
```

config mld_snooping querier

目的

通常のクエリ送信の間隔（秒）、メンバからのレポートを待つ最大時間（秒）および IGMP Snooping を保証する許容パケット損失を設定します。

構文

config mld_snooping querier [vlan <vlan_name 32> | vlanid <vidlist> | all] {query_interval <sec 1-65535> | max_response_time <sec 1-25> | robustness_variable <value 1-255> | last_listener_query_interval <sec 1-25> | state [enable | disable] | version<value 1-2>}

説明

MLD Snooping クエリアを設定します。

パラメータ

パラメータ	説明
vlan <vlan_name 32> | vlanid <vidlist> | all	• vlan <vlan_name 32> - MLD クエリアを設定する VLAN 名を指定します。 • vlanid <vidlist> - MLD クエリアを設定する VLAN ID を指定します。 • all - MLD クエリアにすべての VLAN を指定します。
query_interval <sec 1-65535>	一般的なクエリア送信間隔（秒）を指定します。1-65535（秒）で設定します。初期値は 125（秒）です。
max_response_time <sec 1-25>	メンバからのレポートを待つ最大時間（秒）。1-25（秒）で設定します。初期値は 10（秒）です。
robustness_variable <value 1-255>	予想されるサブネット上のパケットの損失に応じてこの変数を調整します。1-255 で設定します。初期値は 2 です。サブネットにおいてパケットの損失が高いと予想できる場合、この間隔を大きくします。
last_listener_query_interval <sec 1-25>	グループ指定のクエリアメッセージ送信間隔（秒）を指定します。この間隔は、ラストリスナーグループの損失をルータが検出するためにかかる時間です。1-25（秒）で設定します。初期値は 1（秒）です。
state [enable | disable]	MLD クエリアを有効にすると、スイッチを MLS クエリアとして設定し、無効にすると Non- クエリアとして設定します。初期値は「disable」です。
version <value 1-2>	本ポートに送信される MLD パケットのバージョンを指定します。インタフェースが受信した MLD パケットが指定バージョンより高いバージョンであった場合、そのパケットは破棄されます。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

MLD Snooping クエリアを設定します。

```
DGS-3200-10:4#config mld_snooping querier vlan default query_interval 125 state enable
Command: config mld_snooping querier vlan default query_interval 125 state enable

Success.

DGS-3200-10:4#
```

注意 MLD Snooping クエリアの Robustness Variable は以下の MLD メッセージ間隔を設定する場合に使用されます。

Group Listener Interval - マルチキャストルータがネットワーク上のグループにリスナーがいないと判断するまでの時間。次の計算式で計算されます。Group Listener =（Robustness Variable*Query Interval）+（1*Query Interval）。
Querier Present Interval - マルチキャストルータが他のクエリアデバイスがないと判断するまでの時間。次の計算式で計算されます。Querier Present Interval =（Robustness Variable*Query Interval）+（0.5*Query Response Interval）。
Last Listener Query Count - マルチキャストルータがこのグループ内にローカルリスナーがいないと見なす前に送信された Group-Specific Query 数。初期値は Robustness Variable の値です。

config mld_snooping mrouter_ports

目的

スイッチのルータポートとしてポートを設定します。

構文

config mld_snooping mrouter_ports <vlan_name 32> [add | delete] <portlist>

説明

マルチキャストが有効なルータに接続するポート範囲を指定します。これは、宛先として本ルータが持つすべてのパケットをマルチキャストが有効なルータに到達するように設定します。

パラメータ

パラメータ	説明
<vlan_name 32>	ルータポートが存在する VLAN 名。
add | delete	ルータポートとしてポートを追加または削除します。
<portlist>	ルータポートとして設定するポートまたはポート範囲を指定します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

MLD Snooping マルチキャストルータを設定します。

```
DGS-3200-10:4#config mld_snooping mrouter_ports default add 1-10
Command: config mld_snooping mrouter_ports default add 1-10

Success.

DGS-3200-10:4#
```

config mld_snooping mrouter_ports_forbidden

目的

禁止ルータポートとしてスイッチのポートを設定します。

構文

config mld_snooping mrouter_ports_forbidden <vlan_name 32> [add | delete] <portlist>

説明

マルチキャストが有効なルータに接続する禁止ポート（ポート範囲）を選択します。これは、これらが、禁止ポートがルーティングパケットを送信しないように設定します。

パラメータ

パラメータ	説明
<vlan_name 32>	ルータポートが禁止される VLAN 名。
add | delete	禁止ルータポートとしてポートを追加または削除します。
<portlist>	禁止ルータポートとして設定するポートまたはポート範囲を指定します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

MLD Snooping 禁止マルチキャストルータポートを設定します。

```
DGS-3200-10:4#config mld_snooping mrouter_ports_forbidden default add 1-10
Command: config mld_snooping mrouter_ports_forbidden default add 1-10

Success.

DGS-3200-10:4#
```

enable mld_snooping

目的

スイッチで MLD Snooping をグローバルに有効にします。

構文

enable mld_snooping

説明

スイッチの MLD Snooping を有効にします。

パラメータ

なし。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

スイッチの MLD Snooping をグローバルに有効にします。

```
DGS-3200-10:4#enable mld_snooping
Command: enable mld_snooping

Success.

DGS-3200-10:4#
```

disable mld_snooping

目的

スイッチで MLD Snooping をグローバルに無効にします。

構文

disable mld_snooping

説明

スイッチの MLD Snooping を無効にします。IP マルチキャストルーティングが使用されていない場合にだけ、MLD Snooping を無効にすることができます。MLD Snooping を無効にすると、すべての MLD と IPv6 マルチキャストトラフィックは与えられた IP インタフェースでフラッドします。

パラメータ

なし。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

スイッチの MLD Snooping をグローバルに無効にします。

```
DGS-3200-10:4#disable mld_snooping
Command: disable mld_snooping

Success.

DGS-3200-10:4#
```

show mld_snooping

目的

スイッチの MLD Snooping 機能の現在のステータスを表示します。

構文

show mld_snooping {[vlan <vlan_name 32> | vlanid <vidlist>]}

説明

スイッチの MLD Snooping 機能の現在のステータスを表示します。

パラメータ

パラメータ	説明
vlan <vlan_name 32>	MLD Snooping 設定を参照する VLAN 名。
vlanid <vidlist>	MLD Snooping 設定を参照する VLAN ID。

パラメータが指定されないと、システムはすべての MLD Snooping 設定を表示します。

制限事項

なし。

使用例

MLD Snooping 設定を表示します。

```
DGS-3200-10:4#show mld_snooping
Command: show mld_snooping

MLD Snooping Global State    : Disabled
Multicast router Only        : Disabled

VLAN  Name                   : default
Query Interval               : 125
Max Response Time            : 10
Robustness Value             : 2
Last Listener Query Interval : 1
Node Timeout                 : 260
Router Timeout               : 260
Done Timer                   : 2
Querier State                : Disabled
Querier Router Behavior      : Non-Querier
State                        : Disabled
Fast Done                    : Disabled
Version                      : 2

Total Entries: 1

DGS-3200-10:4#
```

show mld_snooping group

目的

スイッチの MLD Snooping グループ設定を表示します。

構文

show mld_snooping group {vlan <vlan_name 32> | vlanid <vidlist> }

説明

スイッチの MLD Snooping グループ設定を表示します。

パラメータ

パラメータ	説明
vlan <vlan_name 32>	MLD Snooping グループ設定を参照する VLAN 名。
vlanid <vidlist>	MLD Snooping グループ設定を参照する VLAN ID。

パラメータが指定されないと、システムは現在のすべての MLD Snooping グループ設定を表示します。

制限事項

なし。

使用例

MLD Snooping グループ設定を表示します。

```
DGS-3200-10:4#show mld_snooping group
Command: show mld_snooping

Source/Group    : NULL / FF1E::1
VLAN Name/VID   : default/1
Port Member     : 8
Mode            : EXCLUDE

Total Entries: 1

DGS-3200-10:4#
```

show mld_snooping mrouter_ports

目的

スイッチの現在のルータポート設定を表示します。

構文

show mld_snooping group {[vlan <vlan_name 32> | vlanid <vidlist>]} {[static | dynamic | forbidden]}

説明

スイッチの現在のルータポート設定を表示します。

パラメータ

パラメータ	説明
vlan <vlan_name 32> | vlanid <vidlist>	• vlan <vlan_name 32> - ルータポートが存在する VLAN 名。 • vlanid <vidlist> - ルータポートが存在する VLAN ID。
static | dynamic | forbidden	• static - スタティックに設定されたルータポートを表示します。 • dynamic - ダイナミックに設定されたルータポートを表示します。 • forbidden - 禁止ポートとして設定されたルータポートを表示します。

パラメータが指定されないと、システムは現在の全ルータポート設定を表示します。

制限事項

なし。

使用例

MLD Snooping マルチキャストルータポート設定を表示します。

```
DGS-3200-10:4#mld_snooping mrouter_ports
Command: show mld_snooping mrouter_ports

VLAN Name             : default
Static Router Port    :
Dynamic Router Port   :
Forbidden Router Port :

Total Entries: 1

DGS-3200-10:4#
```

第 40 章　マルチキャスト IP アドレスの限定コマンド

IP マルチキャスト範囲の限定コマンドでは、指定したスイッチポートに受信するマルチキャストアドレスレポートを設定することができます。この機能は受信するレポート数およびスイッチに設定するマルチキャストグループ数を限定します。特定のスイッチポートに到着するレポートを受信する（Permit）またはレポートを拒否する（Deny）IP アドレス /IP アドレス範囲を設定することが可能です。

コマンドラインインタフェース（CLI）におけるマルチキャスト IP アドレスの限定コマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
create mcast_filter_profile profile_id	<value 1-24> profile_name <name 1-32>
config mcast_filter_profile	[profile_id <value 1-24> | profile_name <name 1-32>] {profile_name <name 1-32> | [add | delete] <mcast_address_list>}
delete mcast_filter_profile profile_id	[<value 1-24> | all]
delete mcast_filter_profile profile_name	<name 1-32>
show mcast_filter_profile	{profile_id <value 1-24>}
config limited_multicast_addr	[ports <portlist>] {[add | delete] [profile_id <value 1-24> | profile_name <name 1-32>] | access [permit | deny]}
show limited_multicast_addr	{ports <portlist>}
config max_mcast_group	ports <portlist> max_group <value 1-256>
show max_mcast_group	ports {<portlist>}

以下のセクションで各コマンドについて詳しく記述します。

create mcast_filter_profile

目的

マルチキャストアドレスプロファイルを作成します。

構文

create mcast_filter_profile profile_id <value 1-24> profile_name <name 1-32>

説明

マルチキャストアドレスプロファイルを作成します。プロファイルには複数のマルチキャストアドレス範囲を定義できます。

パラメータ

パラメータ	説明
profile_id <value 1-24>	プロファイルの ID。範囲は、1-24 です。
profile_name <name 1-32>	プロファイルに意味のある説明文を指定します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

MLD Snooping を設定します。

```
DGS-3200-10:4# create mcast_filter_profile profile_id 2 profile_name MOD
Command: create mcast_filter_profile profile_id 2 profile_name MOD

Success.

DGS-3200-10:4#
```

config mcast_filter_profile

目的

プロファイルへのマルチキャストアドレス範囲の追加またはプロファイルからマルチキャストアドレスを削除します。

構文

config mcast_filter_profile [profile_id <value 1-24> | profile_name <name 1-32>] {profile_name <name 1-32> | [add | delete] <mcast_address_list>}

説明

プロファイルへのマルチキャストアドレス範囲の追加またはプロファイルからマルチキャストアドレスを削除します。

パラメータ

パラメータ	説明
profile_id <value 1-24> | profile_name <name 1-32>	• profile_id <value 1-24> - マルチキャストアドレス範囲の追加または削除するプロファイルの ID。 • profile_name <name 1-32> - マルチキャストアドレス範囲の追加または削除するプロファイル名。
profile_name <name 1-32> | [add | delete] <mcast_address_list>	• profile_name <name 1-32> - マルチキャストアドレス範囲の追加または削除するプロファイル名。 • add | delete - 追加または削除します。 • <mcast_address_list> - プロファイルに置くマルチキャストアドレスのリスト。一つのマルチキャスト IP アドレスまたはマルチキャスト IP アドレスを指定することができます。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

プロファイルへマルチキャストアドレス範囲を追加します。

```
DGS-3200-10:4#config mcast_filter_profile profile_id 2 add 225.1.1.1 - 225.1.1.1
Command: config mcast_filter_profile profile_id 2 add 225.1.1.1 - 225.1.1.1

Success.

DGS-3200-10:4#
```

delete mcast_filter_profile

目的

マルチキャストアドレスプロファイルを削除します。

構文

delete mcast_filter_profile profile_id [<value 1-24> | all]

delete mcast_filter_profile profile_name <name 1-32>

説明

マルチキャストアドレスプロファイルを削除します。

パラメータ

パラメータ	説明
profile_id [<value 1-24> | all]	• <value 1-24> - 削除するプロファイルの ID。 • all - すべてのマルチキャストアドレスプロファイルを削除します。
profile_name <name 1-32>	削除するプロファイル名を指定します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

マルチキャストアドレスプロファイルを削除します。

```
DGS-3200-10:4#delete mcast_filter_profile profile_id 3
Command: delete mcast_filter_profile profile_id 3

Success.

DGS-3200-10:4#
```

show mcast_filter_profile

目的

定義済みのマルチキャストアドレスプロファイルを表示します。

構文

show mcast_filter_profile {profile_id <value 1-24>}

説明

定義済みのマルチキャストアドレスプロファイルを表示します。

パラメータ

パラメータ	説明
<value 1-24>	プロファイルの ID。パラメータが指定されないと、すべてのプロファイルが表示されます。

制限事項

なし。

使用例

定義済みのマルチキャストアドレスプロファイルを表示します。

```
DGS-3200-10:4#show mcast_filter_profile
Command: show mcast_filter_profile

Profile ID  Name      Multicast Addresses
----------  --------  ----------------------------
1           MOD       234.1.1.1 - 238.244.244.244
                      234.1.1.1 - 238.244.244.244
2           customer  224.19.62.34 - 224.19.162.200

Total Entries :2

DGS-3200-10:4#
```

config limited_multicast_addr

目的

ポートにマルチキャストアドレスフィルタ機能を設定します。

構文

config limited_multicast_addr ports <portlist> {[add | delete] [profile_id <value 1-24> | profile_name <name 1-32>] | access [permit | deny]}

説明

ポートまたは VLAN にマルチキャストアドレスフィルタ機能を設定します。ポートまたは VLAN にプロファイルが指定されていないと、制限機能は有効になりません。

パラメータ

パラメータ	説明
<portlist>	• <portlist> - IP マルチキャストフィルタ機能を設定するポートまたはポート範囲。
add | delete	• add - ポートにマルチキャストアドレスプロファイルを追加します。 • delete - ポートからマルチキャストアドレスプロファイルを削除します。
profile_id <value 1-24>	ポートに追加されるプロファイル、またはポートから削除されるプロファイル ID。
access [permit | deny]	• permit - プロファイルテーブルに定義されたアドレスに一致するパケットを許可します。 • Deny - プロファイルテーブルに定義されたアドレスに一致するパケットを拒否します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

ポート 1 と 3 をマルチキャストアドレスプロファイル 2 に設定します。

```
DGS-3200-10:4#config limited_multicast_addr ports 1,3 add profile_id 2
Command: config limited_multicast_addr ports 1,3 add profile_id 2

Success.

DGS-3200-10:4#
```

show limited_multicast_addr

目的

IP マルチキャストアドレス範囲の制限をポートごとに表示します。

構文

show limited_multicast_addr {ports <portlist>}

説明

マルチキャストアドレスの制限するコマンドではポートまたは VLAN ごとにマルチキャストアドレス範囲を表示します。

パラメータ

パラメータ	説明
ports <portlist>	IP マルチキャスト範囲の限定機能を設定するポートまたはポート範囲。

制限事項

なし。

使用例

制限されるマルチキャストアドレス範囲を表示します。

```
DGS-3200-10:4#show limited_multicast_addr 1,3
Command: show limited_multicast_addr 1,3

Port   : 1
Access : Deny

Profile ID  Name      Multicast Addresses
----------  --------  ----------------------------
1           customer  224.19.62.34 - 224.19.162.200

Port   : 3
Access : Deny

Profile ID  Name      Multicast Addresses
----------  --------  ----------------------------
1           customer  224.19.62.34 - 224.19.162.200

DGS-3200-10:4#
```

config max_mcast_group

目的

ポートが参加可能なマルチキャストグループの最大数を設定します。

構文

config max_mcast_group ports <portlist> max_group <value 1-256>

説明

ポートが参加可能なマルチキャストグループの最大数を設定します。

パラメータ

パラメータ	説明
ports [<portlist>]	max_mcast_group を設定するポートまたはポート範囲
max_group [<value 1-256>]	マルチキャストグループの最大数（1-256）を指定します。初期値は 256 です。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

ポート 1 と 3 にマルチキャストグループの最大数を設定します。

```
DGS-3200-10:4#config max_mcast_group ports 1, 3 max_group 100
Command: config max_mcast_group ports 1, 3 max_group 100

Success.

DGS-3200-10:4#
```

show max_mcast_group

目的

ポートが参加可能なマルチキャストグループの最大数を表示します。

構文

show max_mcast_group ports {<portlist>}

説明

ポートが参加可能なマルチキャストグループの最大数を表示します。

パラメータ

パラメータ	説明
ports {<portlist>}	マルチキャストの最大数を表示するポート範囲。

制限事項

なし。

使用例

ポートが参加可能なマルチキャストグループの最大数を表示します。

```
DGS-3200-10:4#show max_mcast_group ports 1
Command: show max_mcast_group ports 1

Max Multicast Filter Group:
Port  MaxMcastGroup
----- -------------
1     256

DGS-3200-10:4#
```

第 41 章　IGMP Snooping Multicast VLAN (ISM) 設定コマンド

コマンドラインインタフェース（CLI）における IGMP Snooping Multicast VLAN コマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
create igmp_snooping multicast_vlan	<vlan_name 32> <vlanid 2-4094>
config igmp_snooping multicast_vlan	<vlan_name 32> {[add | delete] [member_port <portlist> | source_port <portlist> | tag_member_port <portlist>] | state [enable | disable] | replace_source_ip <ipaddr>}
create igmp_snooping multicast_group_profile	<profile_name 1-32>
config igmp_snooping multicast_ group_profile	<profile_name 1-32> [add | delete] <mcast_address_list>
delete igmp_snooping multicast_ group_profile	[<profile_name 1-32> | all]
show igmp_snooping multicast_ group_profile	{< profile_name 1-32>}
config igmp_snooping multicast_vlan_group	<vlan_name 32> [add | delete] profile_name <profile_name 1-32>
show igmp_snooping multicast_vlan_group	{<vlan_name 32> }
delete igmp_snooping multicast_vlan	<vlan_name 32>
enable igmp_snooping multicast_vlan	
disable igmp_snooping multicast_vlan	
show igmp_snooping multicast_vlan	{<vlan_name 32>}

以下のセクションで各コマンドについて詳しく記述します。

create igmp_snooping multicast_vlan

目的

IGMP Snooping マルチキャスト VLAN を作成します。

構文

create igmp_snooping multicast_vlan <vlan_name 32> <vlanid 2-4094>

説明

マルチキャスト VLAN を作成します。ISM（IGMP Snooping multicast）VLAN は、1Q VLAN データベース内には作成されません。複数の ISM VLAN を作成することができ、ISM VLAN の Snooping 機能は、1Q VLAN の Snooping 機能と共存します。

パラメータ

パラメータ	説明
<vlan_name 32>	作成する VLAN 名。各マルチキャスト VLAN 名は半角英数字 32 文字以内で指定します。
<vlanid 2-4094>	作成するマルチキャスト VLAN の VLAN ID（2-4094）。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

VLAN 名が mv1、vid が 2 のマルチキャスト VLAN を作成します。

```
DGS-3200-10:4#create igmp_snoop multicast_vlan mv1 2
Command: create igmp_snoop multicast_vlan mv1 2

Success.

DGS-3200-10:4#
```

config igmp_snooping multicast_vlan

目的

指定のマルチキャスト VLAN のパラメータを設定します。

構文

config igmp_snooping multicast_vlan <vlan_name 32> {[add | delete] [member_port <portlist> | source_port <portlist> | tag_member_port <portlist>] | state [enable | disable] | replace_source_ip <ipaddr>}

説明

メンバポートの追加、タグ付きメンバポートの追加、およびポートリストへの送信元ポートの追加を行います。メンバポートは自動的にマルチキャスト VLAN のタグなしメンバとなり、タグ付きメンバポートおよび送信元ポートは自動的にマルチキャスト VLAN のタグ付きメンバになります。ポートリストの変更については、「add」（追加）や「delete」（削除）を指定しなければ、新しいポートリストが古いポートリストと入れ替わります。メンバポートリストと送信元ポートリストは重複することはできませんが、マルチキャスト VLAN のメンバポートは、別のマルチキャスト VLAN と重複することが可能です。設定する前に必ずマルチキャスト VLAN を作成します。

パラメータ

パラメータ	説明
<vlan_name 32>	設定する VLAN 名。各マルチキャスト VLAN 名は半角英数字 32 文字以内で指定します。
add | delete	• add - ポートリストを追加します。 • delete - ポートリストを削除します。
member_port <portlist> | source_port <portlist> | tag_member_port <portlist>	• member_port - マルチキャスト VLAN に追加または削除するメンバポートの範囲。メンバポートは ISM VLAN のタグなしメンバポートになります。 • source_port <portlist> - マルチキャスト VLAN に追加する送信元ポートの範囲。 • tag_member_port - ISM VLAN のタグ付きメンバポートを指定します。
state [enable | disable]	選択した VLAN のマルチキャスト VLAN を有効または無効に設定します。
replace_source_ip <ipaddr>	送信元 IP アドレス置換の設定をします。IGMP Snooping 機能により、ホストが送信した IGMP Report パケットが送信元ポートに転送されます。パケットを転送する前に、join パケット内の送信元 IP アドレスをこの IP アドレスに置換する必要があります。何も指定しない場合、送信元 IP アドレスの置換は行われません。 • <ipaddr> - 置換する IP アドレスを設定します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

IGMP Snooping マルチキャスト VLAN「mv1」のメンバとしてポート 1 と 3 を追加します。

```
DGS-3200-10:4#config igmp_snooping multicast_vlan mv1 add member_port 1,3 state
enable
Command: config igmp_snooping multicast_vlan mv1 add member_port 1,3 state enable

Success.

DGS-3200-10:4#
```

create igmp_snooping multicast_group_profile

目的

スイッチにマルチキャストグループプロファイルを作成します。

構文

create igmp_snooping multicast_group_profile <profile_name 1-32>

説明

マルチキャストグループプロファイルを作成します。プロファイル名は固有である必要があります。

パラメータ

パラメータ	説明
<profile_name 1-32>	マルチキャスト VLAN プロファイル名（32 文字以内）を指定します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

マルチキャストグループプロファイルを作成します。

```
DGS-3200-10:4#create igmp_snooping multicast_group_profile Knicks
Command: create igmp_snooping multicast_group_profile Knicks

Success.

DGS-3200-10:4#
```

config igmp_snooping multicast_group_profile

目的

スイッチに IGMP Snooping マルチキャストグループプロファイルを設定します。また、プロファイルのマルチキャストアドレスの追加、または削除をします。

構文

config igmp_snooping multicast_group_profile <profile_name 1-32> [add | delete] <mcast_address_list>

説明

スイッチに IGMP Snooping マルチキャストグループプロファイルを設定します。また、プロファイルのマルチキャストアドレスの追加、または削除をします。

パラメータ

パラメータ	説明
<profile_name 1-32>	マルチキャスト VLAN プロファイル名（32 文字以内）を指定します。
add | delete	本マルチキャストグループプロファイルに (から) マルチキャストアドレスを追加、または削除します。
<mcast_address_list>	マルチキャストアドレスを指定します。マルチキャストアドレスリストには、「225.1.1.1,225.1.1.3,225.1.1.8」という連続して単一のマルチキャストアドレスや「225.1.1.1-225.2.2.2」というマルチキャストアドレス範囲、および「225.1.1.1,225.1.1.18-225.1.1.20」という両方の指定が可能です。グループはすべて指定のマルチキャスト VLAN から選択します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

プロファイル名「Knicks」にマルチキャストアドレスを追加します。

```
DGS-3200-10:4#config igmp_snooping multicast_group_profile Knicks add 225.1.1.1,
225.1.1.10-225.1.1.20
Command: config igmp_snooping multicast_group_profile Knicks add 225.1.1.1,
225.1.1.10-225.1.1.20

Success.

DGS-3200-10:4#
```

delete igmp_snooping multicast_group_profile

目的

既存の IGMP Snooping マルチキャストグループプロファイルを削除します。

構文

delete igmp_snooping multicast_group_profile [<profile_name 1-32>|all]

説明

既存の IGMP Snooping マルチキャストグループプロファイルを削除します。

パラメータ

パラメータ	説明
<profile_name 1-32> | all	• <profile_name 1-32> - マルチキャスト VLAN プロファイル名（32 文字以内）を指定します。 • all - すべてのマルチキャストグループプロファイルを削除します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

「Knicks」という名前のマルチキャストグループプロファイルを削除します。

```
DGS-3200-10:4#delete igmp_snooping multicast_group_profile Knicks
Command: delete igmp_snooping multicast_group_profile Knicks

Success.

DGS-3200-10:4#
```

show igmp_snooping multicast_group_profile

目的

IGMP Snooping マルチキャストグループプロファイルを表示します。

構文

show igmp_snooping multicast_group_profile {<profile_name 1-32>}

説明

IGMP Snooping マルチキャストグループプロファイルを表示します。

パラメータ

パラメータ	説明
<profile_name 1-32>	マルチキャスト VLAN プロファイル名（半角英数字 32 文字以内）を指定します。

制限事項

なし。

使用例

プロファイル設定を表示します。

```
DGS-3200-10:4#show igmp_snooping multicast_group_profile
Command: show igmp_snooping multicast_group_profile

Profile Name Multicast Addresses
------------ --------------------------------
Knicks       234.1.1.1 - 238.244.244.244
             239.1.1.1 - 239.2.2.2
customer     224.19.62.34 - 224.19.162.200

Total Entries : 2

DGS-3200-10:4#
```

config igmp_snooping multicast_vlan_group

目的

指定のマルチキャスト VLAN と共に学習されるマルチキャストグループを設定します。

構文

config igmp_snooping multicast_vlan_group <vlan_name 32> [add | delete] profile_name <profile_name 1-32>

説明

指定のマルチキャスト VLAN と共に学習されるマルチキャストグループを設定します。学習方法には 2 つあります。

- マルチキャストグループが設定されず、またマルチキャスト VLAN には重複するメンバポートがないと仮定します。メンバポートが受信した join パケットは、このポートが所属するマルチキャスト VLAN と共に学習されます。
- join パケットが送信先マルチキャストグループを含むマルチキャスト VLAN と共に学習されます。join パケットの送信先マルチキャストグループがこのポートが属するどのマルチキャスト VLAN にも属していない場合、join パケットはパケットの本来の VLAN と共に学習されます。

注意 異なるマルチキャスト VLAN 内において同じマルチキャストグループは重複できません。複数のマルチキャストグループを 1 つのマルチキャスト VLAN に追加することができます。

パラメータ

パラメータ	説明
<vlan_name 32>	作成するマルチキャスト VLAN 名。各マルチキャスト VLAN 名は半角英数字 32 文字以内で指定します。
add | delete	• add - マルチキャストにプロファイルを対応させます。 • delete - マルチキャストからプロファイルの対応を削除します。
profile_name <profile_name 1-32>	マルチキャスト VLAN プロファイル名を半角英数字 32 文字以内で指定します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

マルチキャスト VLAN にグループを追加します。

```
DGS-3200-10:4#config igmp_snooping multicast_vlan_group v1 add profile_name
channel_1
Command: config igmp_snooping multicast_vlan_group v1 add profile_name channel_1

Success.

DGS-3200-10:4#
```

show igmp_snooping multicast_vlan_group

目的

指定したマルチキャスト VLAN に設定されているマルチキャストグループを表示します。

構文

show igmp_snooping multicast_vlan_group {<vlan_name 32>}

説明

指定したマルチキャスト VLAN に設定されているマルチキャストグループを表示します。

パラメータ

パラメータ	説明
<vlan_name 32>	マルチキャストグループを表示するマルチキャスト VLAN 名（半角英数字 32 文字以内）を指定します。

制限事項

なし。

使用例

マルチキャスト VLAN に設定されているマルチキャストグループを表示します。

```
DGS-3200-10:4#show multicast_vlan_group mv1
Command: show multicast_vlan_group mv1

VLAN Name     VLAN ID     Multicast Group Profiles
---------     -------     ------------------------
mv1           100         Knicks

DGS-3200-10:4#
```

delete igmp_snooping multicast_vlan

目的

マルチキャスト VLAN を削除します。

構文

delete igmp_snooping multicast_vlan <vlan_name 32>

説明

マルチキャスト VLAN を削除します。

パラメータ

パラメータ	説明
<vlan_name 32>	削除するマルチキャスト VLAN 名。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

IGMP Snooping マルチキャスト VLAN を削除します。

```
DGS-3200-10:4#delete igmp_snooping multicast_vlan mv1
Command: delete igmp_snooping multicast_vlan mv1

Success.

DGS-3200-10:4#
```

enable igmp_snooping multicast_vlan

目的

マルチキャスト VLAN 機能を有効にします。

構文

enable igmp_snooping multicast_vlan

説明

マルチキャスト VLAN 機能を有効にします。ISM VLAN は、本コマンドが有効の場合に効果があります。初期値は無効です。

パラメータ

なし。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

マルチキャスト VLAN 機能を有効にします。

```
DGS-3200-10:4#enable igmp_snooping multicast_vlan
Command: enable igmp_snooping multicast_vlan

Success.

DGS-3200-10:4#
```

disable igmp_snooping multicast_vlan

目的

マルチキャスト VLAN 機能を無効にします。

構文

disable igmp_snooping multicast_vlan

説明

マルチキャスト VLAN 機能を無効にします。ISM VLAN は、本コマンドが有効の場合に効果があります。初期値は無効です。

パラメータ

なし。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

マルチキャスト VLAN 機能を無効にします。

```
DGS-3200-10:4#disable igmp_snooping multicast_vlan
Command: disable igmp_snooping multicast_vlan

Success.

DGS-3200-10:4#
```

show igmp_snooping multicast_vlan

目的

マルチキャスト VLAN の情報を表示します。

構文

show igmp_snooping multicast_vlan {<vlan_name 32>}

説明

マルチキャスト VLAN の情報を表示します。

パラメータ

パラメータ	説明
<vlan_name 32>	情報を参照するマルチキャスト VLAN 名。

制限事項

なし。

使用例

マルチキャスト VLAN の情報を表示します。

```
DGS-3200-10:4#show igmp_snooping multicast_vlan
Command: show igmp_snooping multicast_vlan

ISM VLAN Global Stae    : Disabled

VLAN Name               : mv1
VID                     : 2

Member(Untagged) Ports  : 1,3
Tagged Member Ports     : 2
Source Ports            : 4
Status                  : Enabled
Replace Source IP       : 10.1.1.100

DGS-3200-10:4#
```

第 42 章　802.1X コマンド

本スイッチは、IEEE 802.1X ポートベースおよび MAC ベースのネットワークアクセスコントロールのサーバ機能を実装しています。このメカニズムは、ポートがフレームの送受信の前に一致する必要のあるスイッチの各ポートの基準を設定することで、認証ユーザまたは他のネットワークデバイスにネットワークリソースへのアクセスを許可するものです。

コマンドラインインタフェース（CLI）における 802.1X コマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
enable 802.1x	
disable 802.1x	
create 802.1x user	<username 15>
delete 802.1x user	<username 15>
show 802.1x user	{ports <portlist>}
config 802.1x auth_protocol	[local | radius_eap]
config 802.1x auth_failover	[enable | disable]
show 802.1x	{[auth_state | auth_configuration] ports {<portlist>}}
config 802.1x capability	ports [<portlist> | all] [authenticator | none]
config 802.1x auth_parameter	ports [<auth_portlist> | all] [default | {direction both | port_control [force_unauth | auto | force_auth] | quiet_period <sec 0-65535> supp_timeout <sec 1-65535> server_timeout <sec 1-65535> max_req <value 1-10> reauth_period <sec 1-65535> enable_reauth [enable | disable]}]
config 802.1x auth_mode	[port_based | mac_based]
config 802.1x init	[port_based ports [<auth_portlist | all>] | mac_based ports [<portlist> | all] {mac_address <macaddr>}]
config 802.1x reauth	[port_based ports [<auth_portlist | all>] | mac_based ports [<auth_portlist> | all] {mac_address <macaddr>}]
create 802.1x guest_vlan	<vlan_name 32>
delete 802.1x guest_vlan	<vlan_name 32>
config 802.1x guest_vlan	ports [<portlist> | all] state [enable | disable]
show 802.1x guest_vlan	
config radius add	<server_index 1-3> [<server_ip> | <ipv6addr>] key <passwd 32> [default | {auth_port <udp_port_number 1-65535> | acct_port <udp_port_number 1-65535> | timeout <int 1-255> retransmit <int 1-255>}]
config radius delete	<server_index 1-3>
config radius	<server_index 1-3> {ipaddress [<server_ip> | <ipv6addr>] | key <passwd 32> | auth_port <udp_port_number> acct_port <udp_port_number> timeout <int 1-255> retransmit <int 1-255>}
show radius	
show auth_statistics	{ports <portlist | all>}
show auth_diagnostics	{ports <portlist | all>}
show auth_session_statistics	{ports <portlist | all>}
show auth_client	
show acct_client	

以下のセクションで各コマンドについて詳しく記述します。

enable 802.1x

目的
　スイッチの 802.1X 機能を有効にします。
構文
　enable 802.1x
説明
　スイッチの 802.1X 機能を有効にします。「config 802.1x auth_mode」コマンドを使用して、ポートベースまたは MAC ベースを選択します。
パラメータ
　なし。
制限事項
　管理者レベルユーザのみ本コマンドを実行できます。
使用例
　スイッチの 802.1X 機能を有効にします。

```
DGS-3200-10:4#enable 802.1x
Command: enable 802.1x

Success.

DGS-3200-10:4#
```

disable 802.1x

目的
　スイッチの 802.1X 機能を無効にします。
構文
　disable 802.1x
説明
　スイッチの 802.1X 機能を無効にします。「config 802.1x auth_mode」コマンドを使用して、ポートベースまたは MAC ベースを選択します。
パラメータ
　なし。
制限事項
　管理者レベルユーザのみ本コマンドを実行できます。
使用例
　スイッチの 802.1X 機能を無効にします。

```
DGS-3200-10:4#disable 802.1x
Command: disable 802.1x

Success.

DGS-3200-10:4#
```

create 802.1x user

目的
　新しく 802.1X ユーザを作成します。
構文
　create 802.1x user <username 15>
説明
　新しく 802.1X ユーザを作成します。
パラメータ

パラメータ	説明
user <username 15>	追加するユーザ名（半角英数字 15 文字以内）を指定します。

制限事項
　管理者レベルユーザのみ本コマンドを実行できます。
使用例
　802.1X ユーザ「ctsnow」を作成します。

```
DGS-3200-10:4#create 802.1x user ctsnow
Command: create 802.1x user ctsnow

Enter a case-sensitive new password:******
Enter the new password again for confirmation:******
Success.

DGS-3200-10:4#
```

delete 802.1x user

目的

スイッチの 802.1X ユーザアカウントを削除します。

構文

delete 802.1x user <username 15>

説明

スイッチに現在設定されている 802.1X ユーザを削除します。

パラメータ

パラメータ	説明
user <username 15>	削除するユーザ名（半角英数字 15 文字以内）を指定します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

802.1X ユーザ「Tiberius」を削除します。

```
DGS-3200-10:4#delete 802.1x user Tiberius
Command: delete 802.1x user Tiberius

Are you sure to delete the user?(y/n)

Success.

DGS-3200-10:4#
```

show 802.1x user

目的

スイッチの 802.1X ユーザを表示します。

構文

show 802.1x user

説明

スイッチに現在設定されている 802.1X ユーザアカウント情報を表示します。

パラメータ

なし。

制限事項

なし。

使用例

スイッチに現在設定されている 802.1X ユーザ情報を表示します。

```
DGS-3200-10:4#show 802.1x user
Command: show 802.1x user

Current Accounts:

UserName  Password
--------  -------------
ctsnow    gallinari

Total Entries : 1

DGS-3200-10:4#
```

config 802.1x auth_protocol

目的

スイッチに 802.1X 認証プロトコルを設定します。

構文

config 802.1x auth_protocol [local | radius_eap]

説明

802.1X 認証プロトコルの設定を行います。

パラメータ

パラメータ	説明
[local | radius_eap]	認証プロトコルを指定します。 • local - 認証プロトコルを local に指定します。 • radius_eap - 認証プロトコルを RADIUS EAP に指定します。

制限事項

管理者レベルのユーザのみ本コマンドを実行できます。

使用例

スイッチに認証プロトコルに 802.1X RADIUS EAP を設定します。

```
DGS-3200-10:4#config 802.1x auth_protocol radius_eap
Command: config 802.1x auth_protocol radius_eap

Success.

DGS-3200-10:4#
```

config 802.1x auth_failover

目的

802.1X 認証フェイルオーバを設定します。

構文

config 802.1x auth_failover [enable | disable]

説明

802.1X 認証フェイルオーバを設定します。初期値では認証フェイルオーバは無効です。RADIUS サーバに到達しないと、認証エラーとなります。また、認証フェイルオーバが有効な場合に RADIUS サーバ認証が未反応でとローカルデータベースが認証のために使用されます。初期値ではステータスは無効です。

パラメータ

パラメータ	説明
[enable | disable]	認証フェイルオーバを有効または無効にします。

制限事項

管理者レベルのユーザのみ本コマンドを実行できます。

使用例

802.1X 認証フェイルオーバを設定します。

```
DGS-3200-10:4#config 802.1x auth_failover enable
Command: config 802.1x auth_ failover enable

Success.

DGS-3200-10:4#
```

show 802.1x

目的

スイッチの 802.1X サーバの現在の 802.1X 認証状態および設定を表示します。

構文

show 802.1x [auth_state | auth_configuration] {ports [<portlist> | all]}

説明

スイッチの 802.1X サーバの現在の 802.1X 認証状態および設定を表示します。

パラメータ

パラメータ	説明
auth_state	指定ポートまたは全ポートの 802.1X 認証状態を表示します。
auth_configuration	指定ポートまたは全ポートの 802.1X 設定を表示します。
ports [<portlist> | all]	表示するポートまたは範囲を指定します。「all」はすべてのポートを示します。

制限事項

なし。

使用例

802.1X のグローバルな設定を表示します。

```
DGS-3200-10:4#show show 802.1x
Command: show 802.1x

802.1X                   : Enabled
Authentication Mode      : Port_based
Authentication Protocol  : Radius_EAP
Authentication Failover  : Disabled

DGS-3200-10:4#
```

ポート 1-5 の 802.1X 認証状態を表示します。

```
DGS-3200-10:4#show 802.1x auth_state ports 1-5
Command: show 802.1x auth_state ports 1-5

                                                 Assigned
Port MAC Address           State           VLAN ID  Priority
---- -----------------     -----------     ------- ------------------
1    00-00-00-00-00-01     Authenticated   4004    3
1    00-00-00-00-00-02     Authenticated   1234    -
1    00-00-00-00-00-03     Blocked         -       -
1    00-00-00-00-00-04     Authenticating  -       -
2    00-00-00-00-00-10(P)  Authenticated   1234    -
3    00-00-00-00-00-20(P)  Authenticating  -       -
3    00-00-00-00-00-21(P)  Blocked         -       -

Total Authenticating Hosts : 2
Total Authenticated Hosts  : 3

DGS-3200-10:4#
```

ポート 1 の 802.1X 認証設定を表示します。

```
DGS-3200-10:4#show 802.1x auth_configuration ports 1
Command: show 802.1x auth_configuration ports 1

802.1X                   :Enabled
Authentication Mode      :Port_based
Authentication Protocol :Radius_EAP

Port Number    :1
Capability     :None
AdminCrlDir    :Both
OpenCrlDir     :Both
Port Control   :Auto
QuietPeriod    :60 sec
TxPeriod       :30 sec
SuppTimeout    :30 sec
ServerTimeout  :30 sec
MaxReq         :2 times
ReAuthPeriod   :3600 sec
ReAuthenticate :Disabled

DGS-3200-10:4#
```

config 802.1x capability ports

目的

ポート範囲による 802.1X 認証を設定します。

構文

config 802.1x capability ports [<portlist> | all] [authenticator | none]

説明

ポート範囲による 802.1X 認証を設定します。

パラメータ

パラメータ	説明
<portlist> | all	表示するポートまたは範囲を指定します。「all」はスイッチのすべてのポートを指定します。
authenticator | none	• authenticator - ネットワークのアクセス権を取得するために認証プロセスを通過する必要があります。 • none - ポートは 802.1X 機能によって制御されません。ポートを経由する PDU（プロトコルデータユニット）のフローを許可します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

ポート 1-8 に 802.1X 機能を設定します。

```
DGS-3200-10:4#config 802.1x capability ports 1-8 authenticator
Command: config 802.1x capability ports 1-8 authenticator

Success.

DGS-3200-10:4#
```

config 802.1x auth_parameter

目的

ポート範囲に 802.1X 認証パラメータを設定します。デフォルトパラメータは、指定されている範囲内のすべてのポートをデフォルト 802.1X 設定に戻します。

構文

config 802.1x auth_parameter ports [<portlist> | all] [default | {direction both | port_control [force_unauth | auto | force_auth] | quiet_period <sec 0-65535> | tx_period <sec 1-65535> | supp_timeout <sec 1-65535> | server_timeout <sec 1-65535> | max_req <value 1-10> | reauth_period <sec 1-65535> | enable_reauth [enable | disable]}]

説明

ポート範囲に 802.1X 認証パラメータを設定します。

パラメータ

パラメータ	説明
<portlist> | all	表示するポートまたは範囲を指定します。「all」はすべてのポートを指定します。
default	指定範囲内のすべてのポートを 802.1X 設定に戻します。
direction both	制御ポートが送受信両方の通信をブロックするかどうかを決定します。
port_control	ポート範囲の認証処理における管理用の制御を設定します。以下の認証オプションがあります。 • force_auth - ポートのオーセンティケータを Authorized 状態にします。ネットワークアクセスは許可されます。 • auto - ポートステータスに認証プロセスの結果を反映します。 • force_unauth - ポートを Unauthorized 状態にします。ネットワークアクセスはブロックされます。
quiet_period <sec 0-65535>	認証に失敗した後、新しく認証を開始するまでの間隔を設定します。初期値は 60（秒）です。0-65535（秒）の範囲で設定できます。
tx_period <sec 1-65535>	EAP Request/Identity パケットを送信するためにサプリカント（ユーザ）からの応答を待つ時間を設定します。初期値は 30（秒）で 1-65535（秒）の範囲で設定できます。
supp_timeout <sec 1-65535>	Request/Identity パケットを除くすべての EAP パケットに対するサプリカント（ユーザ）からの応答を待つ時間を設定します。初期値は 30（秒）で 1-65535（秒）の範囲で設定できます。
server_timeout <sec 1-65535>	RADIUS サーバからの応答を待つ時間を設定します。初期値は 30（秒）です。1-65535（秒）の範囲で設定できます。
max_req <value 1-10>	サプリカントへのパケットの再送信回数を設定します。初期値は 2 で 1-10 の範囲で設定できます。
reauth_period <sec 1-65535>	連続する再認証の間隔を設定します。初期値は 3600（秒）です。
enable_reauth [enable | disable]	スイッチが再認証するかどうかを決定します。有効にすると、上記「reauth_period」フィールドで指定した間隔でユーザを再認証します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

ポート 1-10 に 802.1X 認証パラメータを設定します。

```
DGS-3200-10:4#config 802.1x auth_parameter ports 1-10 direction both
Command: config 802.1x auth_parameter ports 1-10 direction both

Success.

DGS-3200-10:4#
```

config 802.1x auth_mode

目的

スイッチの 802.1X 認証モードを設定します。

構文

config 802.1x auth_mode [port_based | mac_based]

説明

スイッチのポートベースまたはホストベースの 802.1X 認証機能を有効にします。

パラメータ

パラメータ	説明
[port_based | mac_based]	ポートか MAC アドレスによる 802.1X 認証をします。各モードでポートを初期化するためには、はじめに 802.1X ポートベース /MAC ベースの設定を有効にする必要があります。 • port_based - ポートだけに基づいた認証を設定します。 • mac_based - MAC アドレスだけに基づいた認証を設定します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

MAC アドレスによる 802.1X 認証を設定します。

```
DGS-3200-10:4#config 802.1x auth_mode port_based
Command: config 802.1x auth_mode port_based

Success.

DGS-3200-10:4#
```

config 802.1x init

目的

ポート範囲の 802.1X 認証を初期化します。

構文

config 802.1x init [port_based ports [<portlist> | all] | mac_based ports [<portlist> | all] {mac_address <macaddr>}]

説明

指定された範囲のポートから操作される指定ポートまたは MAC アドレス範囲の 802.1X 機能をただちに初期化します。各モードでポートを初期化するためには、はじめに 802.1X ポートベース /MAC ベースの設定を有効にする必要があります。

パラメータ

パラメータ	説明
port_based	ポートベースモードで 802.1X 機能を初期化します。初期化を承認されるポートを指定することができます。
mac_based	MAC アドレスだけに基づいた 802.1X 機能を初期化します。初期化を承認される MAC アドレスを指定することができます。
port <portlist> | all	設定するポートまたは範囲を指定します。「all」はスイッチのすべてのポートを指定します。
mac_address <macaddr>	初期化するホストの MAC アドレスを入力します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

すべてのポートの認証状態を初期化します。

```
DGS-3200-10:4#config 802.1x init port_based ports all
Command: config 802.1x init port_based ports all

Success.

DGS-3200-10:4#
```

config 802.1x reauth

目的

スイッチの 802.1X 再認証機能を設定します。

構文

config 802.1x reauth [port_based ports [<portlist> | all] |mac_based ports [<portlist> | all] {mac_address <macaddr>}]

説明

ポートに接続するデバイスを再認証します。再認証の間、再認証に失敗するまでポートの状態は「authorized」のままです。

パラメータ

パラメータ	説明
port_based	ポートだけに基づいた 802.1X 再認証機能を設定します。再認証されるポートを指定することができます。
mac_based	MAC アドレスだけに基づいた 802.1X 再認証機能を設定します。再認証される MAC アドレスを指定することができます。
ports <portlist>	再認証するポートまたは範囲を指定します。
all	スイッチのすべてのポートを指定します。
mac_address <macaddr>	認証 RADIUS クライアントの MAC アドレスを指定します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

ポートに接続するデバイスを再認証します。

```
DGS-3200-10:4#config 802.1x reauth port_based ports all
Command: config 802.1x reauth port_based ports all

Success.

DGS-3200-10:4#
```

create 802.1x guest_vlan

目的

設定済みの VLAN を 802.1X ゲスト VLAN として設定します。

構文

create 802.1x guest_vlan <vlan_name 32>

説明

設定済みの VLAN を 802.1X ゲスト VLAN として設定します。

パラメータ

パラメータ	説明
<vlan_name 32>	802.1X ゲスト VLAN として登録済みの VLAN 名を入力します（半角英数字 32 文字以内）。VLAN は前述の「create vlan」コマンドを使用して作成します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。ゲスト VLAN として設定するスタティック VLAN はあらかじめ設定される必要があります。
ゲスト VLAN に割り当てられる VLAN を削除することはできません。1 つの VLAN だけが 802.1X ゲスト VLAN として設定されます。

使用例

スタティック VLAN を 802.1X ゲスト VLAN として設定します。

```
DGS-3200-10:4#create 802.1x guest_vlan guestVLAN
Command: create 802.1x guest_vlan guestVLAN

Success.

DGS-3200-10:4#
```

delete 802.1x guest_vlan

目的

802.1X ゲスト VLAN を削除します。

構文

delete 802.1x guest_vlan <vlan_name 32>

説明

802.1X ゲスト VLAN 設定を削除します。スタティック VLAN は削除しません。

パラメータ

パラメータ	説明
<vlan_name 32>	削除する 802.1X ゲスト VLAN 名を入力します。(半角英数字 32 文字以内)。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

ゲスト VLAN が削除されると、ゲスト VLAN として有効であるすべてのポートはオリジナルの VLAN に戻ります。

使用例

802.1X ゲスト VLAN を削除します。

```
DGS-3200-10:4#delete 802.1x guest_vlan guestVLAN
Command: delete 802.1x guest_vlan guestVLAN

Success.

DGS-3200-10:4#
```

config 802.1x guest_vlan

目的

設定済みの 802.1X ゲスト VLAN にポートを設定します。

構文

config 802.1x guest_vlan ports [<portlist> | all] state [enable | disable]

説明

802.1 ゲスト VLAN を有効または無効にするために、ポートを設定します。

パラメータ

パラメータ	説明
<portlist>	設定するポートまたは範囲を指定します。
all	802.1X ゲスト VLAN にすべてのポートを設定します。
state [enable | disable]	設定するポートの VLAN ポート状態を指定します。 • enable - ゲスト VLAN に参加します。 • disable - ゲスト VLAN から離脱します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。指定ポートの状態を有効から無効に変更した場合、ポートはデフォルト VLAN に戻ります。

使用例

設定済みの 802.1X ゲスト VLAN ポートを有効に設定します。

```
DGS-3200-10:4#config 802.1x guest_vlan ports 1-8 state enable
Command: config 802.1x guest_vlan ports 1-8 state enable

Warning! The ports are move to Guest VLAN!

Success.

DGS-3200-10:4#
```

show 802.1x guest_vlan

目的

802.1x ゲスト VLAN の設定を参照します。

構文

show 802.1x guest_vlan

説明

ゲスト VLAN の情報を参照します。

パラメータ

なし。

制限事項

なし。

使用例

設定済みの 802.1X ゲスト VLAN の設定を表示します。

```
DGS-3200-10:4#show 802.1x guest_vlan
Command: show 802.1x guest_vlan

Guest VLAN Setting
---------------------------
Guest VLAN :guest
Enable Guest VLAN Ports:1-10

DGS-3200-10:4#
```

config radius add

目的

新しい RADIUS サーバを追加します。低いインデックスを持つサーバほどには、認証優先度が高くなります。

構文

config radius add <server_index 1-3> [<server_ip> | <ipv6addr>] key <passwd 32> [default | {auth_port <udp_port_number 1-65535> | acct_port <udp_port_number 1-65535> | timeout <int 1-255> | retransmit <int 1-255>}]

説明

新しい RADIUS サーバを追加します。

パラメータ

パラメータ	説明
<server_index 1-3>	RADIUS サーバに番号を割り当てます。3 つまでの RADIUS サーバ設定のグループをスイッチに入力できます。
<server_ip> | <ipv6addr>	• <server_ip> - RADIUS サーバの IP アドレス。 • <ipv6addr> - RADIUS サーバの IPv6 アドレス。
key <passwd 32>	RADIUS サーバとスイッチが使用する共有秘密鍵。32 文字以内で指定します。インターネットに送信される前にユーザの認証データを暗号化するために使用されます。
default	「auth_port」と「acct_port」設定の両方にデフォルト UDP ポート番号を使用します。「auth_port」を 1812 に、「acct_port」を 1813 に設定します。
auth_port <udp_port_number 1-65535>	認証リクエストに対する UDP ポート番号。初期値は 1812 です。
acct_port <udp_port_number 1-65535>	アカウンティングリクエストに対する UDP ポート番号。初期値は 1813 です。
timeout <int 1-255>	サーバの応答を待つ時間。初期値は 5（秒）です。
retransmit <int 1-255>	再送回数。初期値は 2 です。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

```
DGS-3200-10:4#config radius add 1 10.48.74.121 key dlink default
Command: config radius add 1 10.48.74.121 key dlink default

Success.

DGS-3200-10:4#
```

config radius delete

目的

登録済みの RADIUS サーバ設定を削除します。

構文

config radius delete <server_index 1-3>

説明

登録済みの RADIUS サーバ設定を削除します。

パラメータ

パラメータ	説明
<server_index 1-3>	RADIUS サーバの現在の設定に番号（1-3）を割り当てます。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

設定済みの RADIUS サーバ通信設定を削除します。

```
DGS-3200-10:4#config radius delete 1
Command: config radius delete 1

Success.

DGS-3200-10:4#
```

config radius

目的

スイッチの RADIUS サーバの設定を行います。

構文

config radius <server_index 1-3> {ipaddress [<server_ip> | <ipv6addr>] | key <passwd 32> | auth_port <udp_port_number 1-65535> | acct_port <udp_port_number 1-65535> | timeout <int 1-255> | retransmit <int 1-255>}

説明

スイッチの RADIUS サーバの設定を行います。

パラメータ

パラメータ	説明
<server_index 1-3>	RADIUS サーバに番号を割り当てます。3 つまでの RADIUS サーバ設定のグループをスイッチに入力できます。
ipaddress [<server_ip> | <ipv6addr>]	• <server_ip> - RADIUS サーバの IP アドレス。 • <ipv6addr> - RADIUS サーバの IPv6 アドレス。
key <passwd 32>	スイッチと RADIUS サーバ間で使用されるパスワードと暗号キーを指定します。 RADIUS サーバとスイッチが使用する共有秘密鍵。32 文字以内で指定します。インターネットに送信される前にユーザの認証データを暗号化するために使用されます。
auth_port <udp_port_number 1-65535>	認証リクエストに対する UDP ポート番号。初期値は 1812 です。
acct_port <udp_port_number 1-65535>	アカウンティングリクエストに対する UDP ポート番号。初期値は 1813 です。
timeout <int 1-255>	サーバの応答を待つ時間。初期値は 5（秒）です。
retransmit <int 1-255>	再送回数。初期値は 2 です。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

RADIUS パラメータを設定します。

```
DGS-3200-10:4#config radius 1 10.48.74.121 key dlink
Command: config radius 1 10.48.74.121 key dlink

Success.

DGS-3200-10:4#
```

show radius

目的

スイッチの現在の RADIUS 設定を表示します。

構文

show radius

説明

スイッチの現在の RADIUS 設定を表示します。

パラメータ

なし。

制限事項

なし。

使用例

スイッチの現在の RADIUS 設定を表示します。

```
DGS-3200-10:4#show radius
Command: show radius

Index 1
  IP Address : fe80:fec0:56ab:34b0:20b2:6aff:fecf:7ec6
  Auth-Port  : 1812
  Acct-Port  : 1813
  Timeout    : 5
  Retransmit : 2
  Key        : adfdslkfjefiefdkgjdassdwtgjk6y1w

Index 2
  IP Address : 172.18.211.71
  Auth-Port  : 1812
  Acct-Port  : 1813
  Timeout    : 5
  Reransmit  : 2
  Key        : 1234567

Index 3
  IP Address : 172.18.211.108
  Auth-Port  : 1812
  Acct-Port  : 1813
  Timeout    : 5
  Retransmit : 2
  Key        : adfdslkfjefiefdkgjdassdwtgjk6y1w

DGS-3200-10:4#
```

show auth_statistics

目的

現在の認証統計情報を表示します。

構文

show auth_statistics {ports [<portlist> | all] }

説明

ポートベースでスイッチの現在の認証統計情報を表示します。

パラメータ

パラメータ	説明
ports [<portlist> | all]	表示するポートまたは範囲を指定します。「all」はすべてのポートを指定します。

制限事項

なし。

使用例

ポート 1 の現在の認証統計情報を表示します。

```
DGS-3200-10:4#show auth_statistics ports 1
Command: show auth_statistics ports 1

 Port number :1

 EapolFramesRx          0
 EapolFramesTx          6
 EapolStartFramesRx     0
 EapolReqIdFramesTx     6
 EapolLogoffFramesRx    0
 EapolReqFramesTx       0
 EapolRespIdFramesRx    0
 EapolRespFramesRx      0
 InvalidEapolFramesRx   0
 EapLengthErrorFramesRx 0

 LastEapolFrameVersion  0
 LastEapolFrameSource   00-00-00-00-00-00

DGS-3200-10:4#
```

show auth_diagnostics

目的

現在の認証診断を表示します。

構文

show auth_diagnostics {ports [<portlist> | all] }

説明

ポートベースでスイッチの現在の認証診断を表示します。

パラメータ

パラメータ	説明
ports [<portlist> | all]	表示するポートを指定します。「all」はすべてのポートを指定します。

制限

管理者レベルユーザのみ本コマンドを実行できます。

使用例

ポート 1 の現在の認証診断を表示します。

```
DGS-3200-10:4#show auth_diagnostics ports 1
Command: show auth_diagnostics ports 1

 Port Number :1

 EntersConnecting                20
 EapLogoffsWhileConnecting       0
 EntersAuthenticating            0
 SuccessWhileAuthenticating      0
 TimeoutsWhileAuthenticating     0
 FailWhileAuthenticating         0
 ReauthsWhileAuthenticating      0
 EapStartsWhileAuthenticating    0
 EapLogoffWhileAuthenticating    0
 ReauthsWhileAuthenticated       0
 EapStartsWhileAuthenticated     0
 EapLogoffWhileAuthenticated     0
 BackendResponses                0
 BackendOtherRequestsToSupplicant 0
 BackendAuthSuccesses            0
 BackendAuthFails                0
```

show auth_session_statistics

目的

スイッチの現在の認証セッション統計情報を表示します。

構文

show auth_session_statistics {port [<portlist> | all]}

説明

スイッチの現在の認証セッション統計情報を表示します。

パラメータ

パラメータ	説明
ports [<portlist> | all]	表示するポートを指定します。「all」はすべてのポートを指定します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

ポート 1 の現在の認証セッション統計情報を表示します。

```
DGS-3200-10:4#show auth_session_statistics ports 1
Command: show auth_session_statistics ports 1

 Port Number :1

 SessionOctetsRx          0
 SessionOctetsTx          0
 SessionFramesRx          0
 SessionFramesTx          0
 SessionId
 SessionAuthenticMethod   Remote Authentication Server
 SessionTime              0
 SessionTerminateCause    SupplicantLogoff
 SessionUserName

DGS-3200-10:4#
```

show auth_client

目的

現在の RADIUS 認証クライアントを表示します。

構文

show auth_client

説明

スイッチに現在設定されている RADIUS 認証クライアントを表示します。

パラメータ

なし。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

RADIUS 認証クライアントを参照します。

```
DGS-3200-10:4#show auth_client
Command: show auth_client

radiusAuthClient ==>
radiusAuthClientInvalidServerAddresses   0
radiusAuthClientIdentifier               D-Link

radiusAuthServerEntry ==>
radiusAuthServerIndex :1

radiusAuthServerAddress                  0.0.0.0
radiusAuthClientServerPortNumber         X
radiusAuthClientRoundTripTime            0
radiusAuthClientAccessRequests           0
radiusAuthClientAccessRetransmissions    0
```

```
radiusAuthClientAccessAccepts            0
radiusAuthClientAccessRejects            0
radiusAuthClientAccessChallenges         0
radiusAuthClientMalformedAccessResponses 0
radiusAuthClientBadAuthenticators        0
radiusAuthClientPendingRequests          0
radiusAuthClientTimeouts                 0
radiusAuthClientUnknownTypes             0
radiusAuthClientPacketsDropped           0


radiusAuthClient ==>
radiusAuthClientInvalidServerAddresses   0
radiusAuthClientIdentifier               D-Link

radiusAuthServerEntry ==>
radiusAuthServerIndex :2

radiusAuthServerAddress                  0.0.0.0
radiusAuthClientServerPortNumber         X
radiusAuthClientRoundTripTime            0
radiusAuthClientAccessRequests           0
radiusAuthClientAccessRetransmissions    0
radiusAuthClientAccessAccepts            0
radiusAuthClientAccessRejects            0
radiusAuthClientAccessChallenges         0
radiusAuthClientMalformedAccessResponses 0
radiusAuthClientBadAuthenticators        0
radiusAuthClientPendingRequests          0
radiusAuthClientTimeouts                 0
radiusAuthClientUnknownTypes             0
radiusAuthClientPacketsDropped           0

radiusAuthClient ==>
radiusAuthClientInvalidServerAddresses   0
radiusAuthClientIdentifier               D-Link

radiusAuthServerEntry ==>
radiusAuthServerIndex :3

radiusAuthServerAddress                  0.0.0.0
radiusAuthClientServerPortNumber         X
radiusAuthClientRoundTripTime            0
radiusAuthClientAccessRequests           0
radiusAuthClientAccessRetransmissions    0
radiusAuthClientAccessAccepts            0
radiusAuthClientAccessRejects            0
radiusAuthClientAccessChallenges         0
radiusAuthClientMalformedAccessResponses 0
radiusAuthClientBadAuthenticators        0
radiusAuthClientPendingRequests          0
radiusAuthClientTimeouts                 0
radiusAuthClientUnknownTypes             0
radiusAuthClientPacketsDropped           0

DGS-3200-10:4#
```

show acct_client

目的

現在の RADIUS アカウンティングクライアントを表示します。

構文

show acct_client

説明

スイッチに現在設定されている RADIUS アカウンティングクライアントを表示します。

パラメータ

なし。

制限事項

なし。

使用例

RADIUS アカウンティングクライアントを参照します。

```
DGS-3200-10:4#show acct_client
Command: show acct_client

radiusAcctClient ==>
radiusAcctClientInvalidServerAddresses 0
radiusAcctClientIdentifier             D-Link

radiusAuthServerEntry ==>
radiusAccServerIndex : 1

radiusAccServerAddress                 0.0.0.0
radiusAccClientServerPortNumber        X
radiusAccClientRoundTripTime           0
radiusAccClientRequests                0
radiusAccClientRetransmissions         0
radiusAccClientResponses               0
radiusAccClientMalformedResponses      0
radiusAccClientBadAuthenticators       0
radiusAccClientPendingRequests         0
radiusAccClientTimeouts                0
radiusAccClientUnknownTypes            0
radiusAccClientPacketsDropped          0

radiusAcctClient ==>
radiusAcctClientInvalidServerAddresses 0
radiusAcctClientIdentifier             D-Link

radiusAuthServerEntry ==>
radiusAccServerIndex : 2

radiusAccServerAddress                 0.0.0.0
radiusAccClientServerPortNumber        X
radiusAccClientRoundTripTime           0
radiusAccClientRequests                0
radiusAccClientRetransmissions         0
radiusAccClientResponses               0
radiusAccClientMalformedResponses      0
radiusAccClientBadAuthenticators       0
radiusAccClientPendingRequests         0
radiusAccClientTimeouts                0
radiusAccClientUnknownTypes            0
radiusAccClientPacketsDropped          0

radiusAcctClient ==>
radiusAcctClientInvalidServerAddresses 0
radiusAcctClientIdentifier             D-Link

radiusAuthServerEntry ==>
radiusAccServerIndex : 3
```

```
radiusAccServerAddress                  0.0.0.0
radiusAccClientServerPortNumber         X
radiusAccClientRoundTripTime            0
radiusAccClientRequests                 0
radiusAccClientRetransmissions          0
radiusAccClientResponses                0
radiusAccClientMalformedResponses       0
radiusAccClientBadAuthenticators        0
radiusAccClientPendingRequests          0
radiusAccClientTimeouts                 0
radiusAccClientUnknownTypes             0
radiusAccClientPacketsDropped           0

DGS-3200-10:4#
```

第 43 章　アクセス認証コントロールコマンド

TACACS/ XTACACS/ TACACS+/ RADIUS コマンドは、TACACS/ XTACACS/ TACACS+ /RADIUS プロトコルを使用してスイッチへの安全なアクセスを可能にします。ユーザがスイッチへのログインや、管理者レベルの特権へのアクセスを行おうとする時、パスワードの入力を求められます。TACACS/ XTACACS/ TACACS+/ RADIUS 認証がスイッチで有効になると、スイッチは TACACS/ XTACACS/ TACACS+/ RADIUS サーバと連絡し、ユーザの確認をします。確認が行われたユーザは、スイッチへのアクセスを許可されます。

現在 TACACS セキュリティプロトコルには異なるエンティティを持つ 3 つのバージョンが存在します。本スイッチのソフトウェアは TACACS の以下のバージョンをサポートします。

- TACACS（Terminal Access Controller Access Control System）
  セキュリティのためのパスワードチェック、認証、およびユーザアクションの通知を、1 台またはそれ以上の集中型の TACACS サーバを使用して行います。パケットの送受信には UDP プロトコルを使用します。
- XTACACS（拡張型 TACACS）
  TACACS プロトコルの拡張版で、TACACS プロトコルより多種類の認証リクエストとレスポンスコードに対応します。パケットの送受信に UDP プロトコルを使用します。
- TACACS+（Terminal Access Controller Access Control System plus）
  ネットワークデバイスの認証のために詳細なアクセス制御を提供します。TACACS+ は、1 台またはそれ以上の集中型のサーバを経由して認証コマンドを使用することができます。TACACS+ プロトコルは、スイッチと TACACS+ デーモンの間のすべてのトラフィックを暗号化します。また、TCP プロトコルを使用して信頼性の高い伝達を行います。

TACACS/ XTACACS/ TACACS+/ RADIUS のセキュリティ機能が正常に動作するためには、スイッチ以外の認証サーバホストと呼ばれるデバイス上で認証用のユーザ名とパスワードを含む TACACS/ XTACACS/ TACACS+/ RADIUS サーバの設定を行う必要があります。スイッチがユーザにユーザ名とパスワードの要求を行う時、スイッチは TACACS/ XTACACS/ TACACS+/ RADIUS サーバにユーザ認証の問い合わせを行います。サーバは以下の 3 つのうちの 1 つの応答を返します。

- サーバは、ユーザ名とパスワードを認証し、ユーザにスイッチへの通常のアクセス権を与えます。
- サーバは、入力されたユーザ名とパスワードを受け付けず、スイッチへのアクセスを拒否します。
- サーバは、認証の問い合わせに応じません。この時点でスイッチはサーバからタイムアウトを受け取り、メソッドリスト中に設定された次の認証方法へと移行します。

本スイッチには TACACS、XTACACS、TACACS+、RADIUS の各プロトコル用に 4 つの認証サーバグループがあらかじめ組み込まれています。これらの認証サーバグループはスイッチにアクセスを試みるユーザの認証に使用されます。認証サーバグループ内に任意の順番で認証サーバホストを設定し、ユーザがスイッチへのアクセス権を取得する場合、1 番目の認証サーバホストに認証を依頼します。認証が行われなければ、リストの 2 番目のサーバホストに依頼し、以下同様の処理が続きます。実装されている認証サーバグループには、特定のプロトコルが動作するホストのみを登録できます。例えば TACACS 認証サーバグループは、TACACS 認証サーバホストのみを登録できます。

スイッチの管理者は、ユーザ定義のメソッドリストに 6 種類の異なる認証方法（TACACS/ XTACACS/ TACACS+/ RADIUS/ local/ none）を設定できます。これらの方法は、任意に並べ替えることが可能で、スイッチ上での通常のユーザ認証に使用されます。リストには最大 8 つの認証方法を登録できます。ユーザがスイッチにアクセスしようとすると、スイッチはリストの 1 番目の認証方法を選択して認証を行います。1 番目の方法で認証サーバホストを通過しても認証が返ってこなければ、スイッチはリストの次の方法を試みます。この手順は、認証が成功するか、拒否されるか、またはリストのすべての認証方法を試し終わるまで繰り返されます。

スイッチへのアクセス権を取得したユーザは、通常のアクセス権を与えられていることにご注意ください。管理者特権レベルの権利を取得するためには、ユーザは「Enable Admin」画面にアクセスし、スイッチに管理者により事前に設定されているパスワードの入力が必要になります。

注意　TACACS、XTACACS、TACACS+、RADIUS は独立したエンティティであり、互換性はありません。スイッチとサーバ間は、同じプロトコルを使用した全く同じ設定を行う必要があります。（例えば、スイッチに TACACS 認証を設定した場合、ホストサーバにも同様の設定を行います。）

コマンドラインインタフェース（CLI）におけるアクセス認証コントロールコマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
enable authen_policy	
disable authen_policy	
show authen_policy	
create authen_login method_list_name	<string 15>
config authen_login	config authen_login [default | method_list_name <string 15>] method {tacacs | xtacacs | tacacs+ | radius | server_group <string 15> | local | none}
delete authen_login method_list_name	<string 15>
show authen_login	[default | method_list_name <string 15> | all]
create authen_enable method_list_name	<string 15>
config authen_enable	[default | method_list_name <string 15>] method {tacacs | xtacacs | tacacs+ | radius | server_group <string 15> | local_enable | none}
delete authen_enable method_list_name	<string 15>
show authen_enable	[default | method_list_name <string 15> | all]
config authen application	[console | telnet | ssh | http |all] [login | enable] [default| method_list_name <string 15>]
show authen application	
create authen server_group	<string 15>
config authen server_group	config authen server_group [tacacs | xtacacs | tacacs+ | radius | <string 15>] [add | delete] server_host <ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius]
delete authen server_group	<string 15>
show authen server_group	<string 15>
create authen server_host	<ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius] {port <int 1-65535> | key [<key_string 254> | none] | timeout <int 1-255> | retransmit <int 1-255>}
config authen server_host	<ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius] {port <int 1-65535> | key [<key_string 254> | none] | timeout <int 1-255> | retransmit <int 1-255>}
delete authen server_host	<ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius]
show authen server_host	
config authen parameter response_timeout	<int 0-255>
config authen parameter attempt	<int 1-255>
show authen parameter	
enable admin	
config admin local_enable	<password 0-15>

以下のセクションで各コマンドについて詳しく記述します。

enable authen_policy

目的

システムアクセス認証ポリシーを有効にします。

構文

enable authen_policy

説明

管理者が定義するスイッチにアクセスするユーザのための認証ポリシーを有効にするために使用します。有効にすると、デバイスはログインメソッドリストをチェックし、ログイン時のユーザ認証に使用する認証方法を選択します。

パラメータ

なし。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

システムアクセス認証ポリシーを有効にします。

```
DGS-3200-10:4#enable authen_policy
Command: enable authen_policy

Success.

DGS-3200-10:4#
```

disable authen_policy

目的

システムアクセス認証ポリシーを無効にします。

構文

disable authen_policy

説明

管理者が定義するスイッチにアクセスするユーザのための認証ポリシーを無効にします。無効になると、スイッチはユーザ名とパスワード検証のためにローカルユーザアカウントデータベースにアクセスします。さらに、スイッチは、現在、管理者レベルの権限にアクセスを試みる普通のユーザのために認証として local enable password を受け付けます。

パラメータ

なし。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

システムアクセス認証ポリシーを無効にします。

```
DGS-3200-10:4#disable authen_policy
Command: disable authen_policy

Success.

DGS-3200-10:4#
```

show authen_policy

目的

スイッチのシステムアクセス認証ポリシー状態を表示します。

構文

show authen_policy

説明

スイッチのアクセス認証ポリシーの現在のステータスを表示します。

パラメータ

なし。

制限事項

なし。

使用例

システムアクセス認証ポリシーを表示します。

```
DGS-3200-10:4#show authen_policy
Command: show authen_policy

Authentication Policy:Enabled

DGS-3200-10:4#
```

create authen_login method_list_name

目的

ユーザがスイッチにログインする際の認証方法を規定するユーザ定義のログインメソッドリストを作成します。

構文

create authen_login method_list_name <string 15>

説明

ユーザログイン用の認証方法のリストを作成します。本スイッチは、最大 8 個のメソッドリストをサポートしていますが、1 つはデフォルトとして予約されているため、削除できません。複数のメソッドリストは、別々に作成および設定される必要があります。

パラメータ

パラメータ	説明
method_list_name <string 15>	15 文字以内の半角英数字の文字列を入力して、メソッドリストを定義します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

メソッドリストを作成します。

```
DGS-3200-10:4#create authen_login method_list_name login_list_1
Command: create authen_login method_list_name login_list_1

Success.

DGS-3200-10:4#
```

config authen_login

目的

ユーザがスイッチにログインする際の認証方法を規定するユーザ定義またはデフォルトのメソッドリストを設定します。

構文

config authen_login [default | method_list_name <string 15>] method {tacacs | xtacacs | tacacs+ | radius | server_group <string 15> | local | none}

説明

本コマンドでは、ユーザがスイッチにログインする際の認証方法を規定するユーザ定義または初期設定のログインメソッドリストを設定します。本メニューで設定した認証方法の順番が認証結果に影響します。例えば、ログインメソッドリストに TACACS - XTACACS - Local の順番で認証方法を指定すると、スイッチはまずサーバグループ内の 1 番目の TACACS ホストに認証リクエストを送信します。そのサーバホストから応答がない場合、2 番目の TACACS ホストに認証リクエストを送信します。このようにサーバグループ内のすべてのホストに順番に送信を試みても応答がない場合、スイッチは本メソッドリストの次の方法（XTACACS）を試します。それでも認証が行われなければ、スイッチ内に設定したローカルアカウントデータベースを使用して認証を行います。Local メソッドが使用される時、ユーザの権限はスイッチに設定されたローカルアカウントの権限に依存します。

これらの方法によって、認証に成功したユーザには「User」の権限のみが与えられます。ユーザが管理者レベルの権限に更新したい場合、「enable admin」コマンドを実行し、スイッチに管理者により事前に設定されているパスワードの入力が必要になります。（詳細については、「enable admin」の説明を参照してください。）

パラメータ

パラメータ	説明
default	ユーザに定義されたアクセス認証のためのデフォルトメソッドリスト。
method_list_name <string 15>	ユーザによって定義されたメソッドリスト名を入力します。本メソッドリストに追加する認証方法を最大 4 件まで指定します。
method	• tacacs - TACACS サーバグループリストのリモートの TACACS サーバホストから TACACS プロトコルを使用してユーザ認証を行います。 • xtacacs - XTACACS サーバグループリストのリモートの XTACACS サーバホストから XTACACS プロトコルを使用してユーザ認証を行います。 • tacacs+ - TACACS+ サーバグループリストのリモートの TACACS+ サーバホストから TACACS+ プロトコルを使用してユーザ認証を行います。 • radius - TACACS サーバグループリストのリモートの RADIUS サーバホストから RADIUS プロトコルを使用してユーザ認証を行います。 • server_group <string 15> - ユーザ定義のサーバグループを使用してユーザ認証を行います。 • local - スイッチ上のローカルユーザアカウントデータベースを使用してユーザ認証を行います。 • none - スイッチへアクセスするために認証要求はしません。

注意 認証プロトコルとして「none」または「local」を入力すると、メソッドリストまたはデフォルトメソッドリストに別の認証が上書きされます。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

認証メソッド tacacs+、tacacs および local をこの順番でユーザ定義メソッドリスト「login_list_1」に設定します。

```
DGS-3200-10:4#config authen_login method_list_name login_list_1 method tacacs+ tacacs local
Command: config authen_login method_list_name login_list_1 method tacacs+ tacacs local

Success.

DGS-3200-10:4#
```

delete authen_login method_list_name

目的

ユーザがスイッチにログインする際の認証方法を規定するユーザ定義のログインメソッドリストを削除します。

構文

delete authen_login method_list_name <string 15>

説明

ユーザログイン用の認証方法のリストを削除します。

パラメータ

パラメータ	説明
method_list_name<string 15>	15 文字以内の半角英数字の文字列を入力して、メソッドリストを削除します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

メソッドリスト「login_list_1」を削除します。

```
DGS-3200-10:4#delete authen_login method_list_name login_list_1
Command: delete authen_login method_list_name login_list_1

Success.

DGS-3200-10:4#
```

show authen_login

目的

ユーザがスイッチにログインする際の認証方法を規定するユーザ定義のログインメソッドリストを表示します。

構文

show authen_login [default | method_list_name <string 15> | all]

説明

ユーザがスイッチにログインする際の認証方法を参照します。

パラメータ

パラメータ	説明
default	ユーザがスイッチにログインする際の認証方法を規定するデフォルトのメソッドリストを表示します。
method_list_name <string 15>	15 文字以内の半角英数字の文字列で、参照するメソッドリストを入力します。
all	現在スイッチに設定されているすべての認証ログインメソッドを表示します。

画面には以下のパラメータが表示されます。

パラメータ	説明
Method List Name	設定されているメソッドリスト名。
Priority	ユーザがスイッチにログインする場合、認証のために問い合わせされるメソッドリストプロトコルの順番を定義します。優先順位は 1（最も高い）から 4（最も低い）です。
Method Name	メソッドリスト名ごとに実行されるセキュリティプロトコルを定義します。
Comment	メソッドのタイプを定義します。ユーザ定義のグループは、ユーザが定義したサーバグループを参照します。実装されているグループは、スイッチ内の普遍設定である TACACS、XTACACS、TACACS+ および RADIUS セキュリティプロトコルを参照します。キーワードは「local」（スイッチのユーザアカウント経由の認証）と「none」（スイッチのすべての機能にアクセスするために認証は必要なし）という TACACS/XTACACS/TACACS+/RADIUS の代わりの技術を使用して認証を参照します。

制限事項

なし。

使用例

「Trinity」という認証ログインメソッドリストを参照します。

```
DGS-3200-10:4#show authen_login method_list_name login_list_1
Command: show authen_login method_list_name login_list_1

Method List Name  Priority  Method Name      Comment
----------------  --------  ---------------  ------------------
login_list_1      1         tacacs+          Built-in Group
                  2         tacacs           Built-in Group
                  3         mix_1            User-defined Group
                  4         local            Keyword

DGS-3200-10:4#
```

create authen_enable method_list_name

目的

ノーマルユーザ権限を管理者権限に昇格するための認証方法を規定するユーザ定義のログインメソッドリストを作成します。

構文

create authen_enable method_list_name <string 15>

説明

スイッチで認証メソッドを使用して、ユーザの権限をユーザレベルから管理者（Admin）レベルに上げます。通常のユーザレベルの権限を取得したユーザが管理者特権を得るためには、管理者が定義した方法により認証を受ける必要があります。最大 8 件の Enable Method List がスイッチで実行されます。

パラメータ

パラメータ	説明
method_list_name<string 15>	15 文字以内の半角英数字の文字列を入力して、enable メソッドリストを作成します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

ユーザ権限を管理者権限に昇格するために「enable_list_1」という名のユーザ定義メソッドリストを作成します。

```
DGS-3200-10:4#create authen_enable method_list_name enable_list_1
Command: create authen_enable method_list_name enable_list_

Success.

DGS-3200-10:4#
```

config authen_enable

目的

スイッチでユーザの権限をユーザレベルから管理者（Admin）レベルに上げる認証メソッドのユーザ定義メソッドリストを設定します。

構文

config authen_enable [default | method_list_name <string 15>] method {tacacs | xtacacs | tacacs+ | radius | server_group <string 15> | local_enable | none}

説明

スイッチで認証メソッドを使用して、ユーザの権限をユーザレベルから管理者（Admin）レベルに上げます。通常のユーザレベルの権限を取得したユーザが管理者特権を得るためには、管理者が定義した方法により認証を受ける必要があります。最大 8 件の Enable Method List が登録できます。

本コマンドで設定した認証方法の順番が認証結果に影響します。例えば、ログインメソッドリストに tacacs-xtacacs-local_enable の順番で認証方法を指定すると、スイッチはまずサーバグループ内の 1 番目の tacacs ホストに認証リクエストを送信します。そのサーバホストから応答がない場合、2 番目の tacacs ホストに認証リクエストを送信します。このようにサーバグループ内のすべてのホストに順番に送信を試みても応答がない場合、スイッチは本メソッドリストの次の方法（xtacacs）を試します。それでも認証が行われなければ、スイッチ内に設定し local_enable password を使用して認証を行います。

これらの中のひとつの方法で認証されたユーザは、「Admin」（管理者）権限を取得することができます。

パラメータ

パラメータ	説明
default	ユーザがスイッチにログインする際の認証方法を規定するデフォルトのメソッドリストを表示します。
method_list_name <string 15>	ユーザによって定義されたメソッドリスト名を入力します。（create authen_enable） 本メソッドリストに追加する認証方法を最大 4 件まで指定します。
method	• tacacs - TACACS サーバグループリストのリモートの TACACS サーバホストから TACACS プロトコルを使用してユーザ認証を行います。 • xtacacs - XTACACS サーバグループリストのリモートの XTACACS サーバホストから XTACACS プロトコルを使用してユーザ認証を行います。 • tacacs+ - TACACS+ サーバグループリストのリモートの TACACS+ サーバホストから TACACS+ プロトコルを使用してユーザ認証を行います。 • radius - TACACS サーバグループリストのリモートの RADIUS サーバホストから RADIUS プロトコルを使用してユーザ認証を行います。 • server_group <string 15> - ユーザ定義のサーバグループを使用してユーザ認証を行います。 • local - スイッチ上のローカルユーザアカウントデータベースを使用してユーザ認証を行います。 • none - スイッチへアクセスするために認証要求はしません。

使用例

ユーザ権限を管理者権限に昇格するためにユーザ定義のメソッドリストを設定します。

```
DGS-3200-10:4#config authen_enable method_list_name enable_list_1 method tacacs+
tacacs local_enable
Command: config authen_enable method_list_name enable_list_1 method tacacs+ tacacs
local_enable

Success.

DGS-3200-10:4#
```

delete authen_enable method_list_name

目的

ノーマルユーザ権限を管理者権限に昇格するための認証方法を規定するユーザ定義のログインメソッドリストを削除します。

構文

delete authen_enable method_list_name <string 15>

説明

ノーマルユーザ権限を管理者権限に昇格するための認証方法を規定するユーザ定義のログインメソッドリストを削除します。

パラメータ

パラメータ	説明
method_list_name <string 15>	15 文字以内の半角英数字の文字列で、削除するメソッドリスト名を入力します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

ユーザ定義のメソッドリスト「enable_list_1」を削除します。

```
DGS-3200-10:4#delete authen_enable method_list_name enable_list_1
Command: delete authen_enable method_list_name enable_list_1

Success.

DGS-3200-10:4#
```

show authen_enable

目的

ノーマルユーザ権限を管理者権限に昇格するための認証方法を規定するユーザ定義のログインメソッドリストを表示します。

構文

show authen_enable [default | method_list_name <string 15> | all]

説明

ノーマルユーザ権限を管理者権限に昇格するための認証方法を規定するユーザ定義のログインメソッドリストを表示します。

パラメータ

スイッチの管理者レベルにアクセスを昇格するように試みるユーザのデフォルトメソッドリストを表示します。

パラメータ	説明
default	ユーザ権限を管理者権限に昇格するための認証方法を規定するデフォルトログインメソッドリストを表示します。
method_list_name <string 15>	15 文字以内の半角英数字の文字列で、参照するメソッドリスト名を入力します。
all	現在スイッチに設定されているすべての認証ログインメソッドを表示します。

画面には以下のパラメータが表示されます。

パラメータ	説明
Method List Name	設定されているメソッドリスト名。
Priority	ユーザがスイッチにログインする場合、認証のために問い合わせされるメソッドリストプロトコルの順番を定義します。優先順位は 1（最も高い）から 4（最も低い）です。
Method Name	メソッドリスト名ごとに実行されるセキュリティプロトコルを定義します。
Comment	メソッドのタイプを定義します。ユーザ定義のグループは、ユーザが定義したサーバグループを参照します。実装されているグループは、スイッチ内の普遍設定である tacacs、xtacacs、tacacs+ および radius セキュリティプロトコルを参照します。キーワードは local（スイッチのユーザアカウント経由の認証）と none（スイッチのすべての機能にアクセスするために認証は必要なし）という tacacs/xtacacs/tacacs+/radius の代わりの技術を使用して認証を参照します。

制限事項

なし。

使用例

ユーザ権限を管理者権限に昇格するためのすべてのメソッドリストを表示します。

```
DGS-3200-10:4#show authen_enable all
Command: show authen_enable all

Method List Name  Priority  Method Name      Comment
----------------  --------  ---------------  ------------------
enable_list_1     1         tacacs+          Built-in Group
                  2         tacacs           Built-in Group
                  3         mix_1            User-defined Group
                  4         local            Keyword

enable_list_2     1         tacacs+          Built-in Group
                  2         radius           Built-in Group

Total Entries : 2

DGS-3200-10:4#
```

config authen application

目的

設定済みのメソッドリストを使用して、認証のためにスイッチに様々なアプリケーションを設定します。

構文

config authen application [console | telnet | ssh | http |all] [login | enable] [default | method_list_name <string 15>]

説明

作成済みのメソッドリストを使用して、ユーザレベルおよび管理者レベル（authen_enable）でログインする際に使用するスイッチの設定用アプリケーション（コンソール、Telnet、SSH、Web）を設定します。

パラメータ

パラメータ	説明
application	設定するアプリケーションを選択します。以下の 5 つのオプションの 1 つを選択します。 • console - コマンドラインインタフェースログインメソッドを設定します。 • telnet - telnet ログインメソッドを設定します。 • ssh - Secure Shell ログインメソッドを設定します。 • http - Web インタフェースログインメソッドを設定します。 • all - すべてのアプリケーション（コンソール、Telnet、SSH、Web）ログインメソッドを設定します。
login	登録済みのメソッドリストを使用して、ユーザレベルの通常ログインを行うアプリケーションを設定します。
enable	登録済みのメソッドリストを使用して、通常のユーザレベルを管理者権限に昇格させるアプリケーションを設定します。
default	デフォルトメソッドリストを使用して、ユーザ認証を行うアプリケーションを設定します。
method_list_name <string 15>	登録済みのメソッドリストを使用して、ユーザ認証用のアプリケーションを設定します。15 文字以内の半角英数字の文字列を入力して、登録済みのメソッドリストを指定します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

telnet インタフェースのためにデフォルトメソッドリストを設定します。

```
DGS-3200-10:4#config authen application telnet login method_list_name login_list_1
Command: config authen application telnet login method_list_name login_list_1

Success.

DGS-3200-10:4#
```

show authen application

目的

スイッチの様々なアプリケーションのための認証方法を表示します。

構文

show authen application

説明

スイッチに現在設定されているスイッチ設定アプリケーション（コンソール、Telnet、SSH、Web）に対するすべての認証メソッドリスト（ログイン、管理者特権の有効化など）を表示します。

パラメータ

なし。

制限事項

なし。

使用例

スイッチのすべてのアプリケーションに対するログインと enable method list を表示します。

```
DGS-3200-10:4#show authen application
Command: show authen application

Application   Login Method List   Enable Method List
-----------   -----------------   ------------------
Console       default             default
Telnet        login_list_1        default
HTTP          default             default

DGS-3200-10:4#
```

create authen server_group

目的

ユーザ定義の認証サーバグループを作成します。

構文

create authen server_group <string 15>

説明

認証サーバグループを作成します。サーバグループとは、TACACS/XTACACS/TACACS+/RADIUS のサーバホストを、ユーザ定義のメソッドリスト使用の認証カテゴリにグループ分けしたものです。「config authen server_group」コマンドを使用して、8 個の認証サーバホストをこのグループに追加することができます。

パラメータ

パラメータ	説明
server_group <string 15>	15 文字以内の半角英数字の文字列を入力して、enable メソッドリストを作成します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

サーバグループ「mix_1」を作成します。

```
DGS-3200-10:4#create authen server_group mix_1
Command: create authen server_group mix_1

Success.

DGS-3200-10:4#
```

config authen server_group

目的

ユーザ定義の認証サーバグループを設定します。指定したサーバグループへ（から）認証サーバを追加または削除します。

構文

config authen server_group [tacacs | xtacacs | tacacs+ | radius | <string 15>] [add | delete] server_host <ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius]

説明

認証サーバグループを設定します。サーバグループとは、TACACS/XTACACS/TACACS+/RADIUS のサーバホストを、ユーザ定義のメソッドリスト使用の認証カテゴリにグループ分けしたものです。プロトコルによって、または定義済みのサーバグループに組み込むことによりグループ分けを行います。どのグループにも最大 8 個までの認証サーバホストを登録できます。

パラメータ

パラメータ	説明
server_group	スイッチに実装するプロトコルグループ（TACACS/XTACACS/TACACS+/RADIUS）、または「create authen server_group」コマンドで作成したユーザ定義グループによってグループを定義します。 • tacacs - スイッチに実装されている TACACS サーバプロトコルを使用します。TACACS プロトコルを使用するサーバホストだけをこのグループに追加することができます。 • xtacacs - スイッチに実装されている XTACACS サーバプロトコルを使用します。XTACACS プロトコルを使用するサーバホストだけをこのグループに追加することができます。 • tacacs+ - スイッチに実装されている TACACS+ サーバプロトコルを使用します。TACACS+ プロトコルを使用するサーバホストだけをこのグループに追加することができます • radius - スイッチに実装されている RADIUS サーバプロトコルを使用します。RADIUS プロトコルを使用するサーバホストだけをこのグループに追加することができます • <string 15> - 15 文字以内の半角英数字の文字列を入力して、作成済みのサーバグループを指定します。本グループはプロトコルにかかわらずサーバホストのどんな組み合わせも追加することができます。
[add/delete]	サーバグループからサーバホストを追加または削除します。
server_host<ipaddr>	追加または削除するリモートサーバホストの IP アドレスを入力します。
protocol	サーバホストが使用するプロトコルを入力します。以下のオプションがあります。 • tacacs - サーバホストが TACACS 認証プロトコルを使用している場合に指定します。 • xtacacs - サーバホストが XTACACS 認証プロトコルを使用している場合に指定します。 • tacacs+ - サーバホストが TACACS+ 認証プロトコルを使用している場合に指定します。 • radius - サーバホストが RADIUS 認証プロトコルを使用している場合に指定します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

サーバグループ「mix_1」に認証ホストを追加します。

```
DGS-3200-10:4#config authen server_group mix_1 add server_host 10.1.1.222 protocol tacacs+
Command: config authen server_group mix_1 add server_host 10.1.1.222 protocol tacacs+

Success.

DGS-3200-10:4#
```

delete authen server_group

目的

ユーザ定義の認証サーバホストグループを削除します。

構文

delete authen server_group <string 15>

説明

認証サーバグループを削除します。

パラメータ

パラメータ	説明
server_group <string 15>	削除するユーザ定義のサーバグループ名。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

サーバグループ「mix_1」を削除します。

```
DGS-3200-10:4#delete server_group mix_1
Command: delete server_group mix_1

Success.

DGS-3200-10:4#
```

show authen server_group

目的

スイッチの認証サーバグループを表示します。

構文

show authen server_group <string 15>

説明

スイッチに設定されている現在の認証サーバグループを表示します。

パラメータ

パラメータ	説明
server_group <string 15>	15 文字以内の半角英数字の文字列を入力して、参照するサーバグループを指定します。 本コマンドを <string> パラメータなしで入力すると、スイッチのすべての認証サーバグループを表示します。

制限事項

なし。

使用例

スイッチに現在設定している認証サーバホストを参照します。

```
DGS-3200-10:4#show authen server_group
Command: show authen server_group

Server Group : mix_1

Group Name       IP Address       Protocol
---------------  ---------------  --------
mix_1            10.1.1.222       TACACS+
radius           10.1.1.224       RADIUS
tacacs           10.1.1.225       TACACS
tacacs+          10.1.1.226       TACACS+
xtacacs          10.1.1.227       XTACACS

Total Entries : 5

DGS-3200-10:4#
```

create authen server_host

目的

認証サーバホストを作成します。

構文

create authen server_host <ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius] {port <int 1-65535> | key [<key_string 254> | none] | timeout <int 1-255> | retransmit <int 1-255>}

説明

本コマンドでは、スイッチに TACACS/ XTACACS/ TACACS+/ RADIUS セキュリティプロトコルに対応したユーザ定義の認証サーバホストを作成します。ユーザが認証ポリシーを有効にしてスイッチにアクセスを試みると、スイッチはリモートホスト上の TACACS/ XTACACS/ TACACS+/ RADIUS サーバホストに認証パケットを送信します。すると TACACS/ XTACACS/ TACACS+/ RADIUS サーバホストはその要求を認証または拒否し、スイッチに適切なメッセージを返します。1 つの物理ホスト上で複数の認証プロトコルを動作させることは可能ですが、TACACS/ XTACACS/ TACACS+/ RADIUS は別のエンティティであり、互換性を持たないことに注意が必要です。サポート可能なサーバホストは最大 16 台です。

パラメータ

パラメータ	説明
server_host <ipaddr>	追加するリモートサーバホストの IP アドレス。
protocol	サーバホストが使用するプロトコル。以下から選択します。 • tacacs - サーバホストが TACACS プロトコルを使用している場合に選択します。 • xtacacs - サーバホストが XTACACS プロトコルを使用している場合に選択します。 • tacacs+ - サーバホストが TACACS+ プロトコルを使用している場合に選択します。 • radius - サーバホストが RADIUS プロトコルを使用している場合に選択します。
port <int 1-65535>	サーバホスト上で認証プロトコルに使用する仮想ポート番号（1-65535）。ポート番号の初期値は、TACACS/ XTACACS/TACACS+ サーバの場合は 49、RADIUS サーバの場合は 1812 です。独自の番号を設定してセキュリティを向上することも可能です。
key [<key_string 254> | none]	• <key_string 254> - TACACS+ と RADIUS サーバの場合に指定する共有キー（254 文字までの半角英数字）。 • none - TACACS+ と RADIUS 認証に暗号化を使用しません。
timeout <int 1-255>	スイッチが、サーバホストからの認証リクエストへの応答を待つ時間（秒）。初期値は 5（秒）です。
retransmit <int 1-255>	サーバからの応答がない場合に、デバイスが認証リクエストを再送する回数。初期値は 2 です。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

ポート番号が 15555、タイムアウトの値が 10 秒である TACACS+ 認証サーバホストを作成します。

```
DGS-3200-10:4#create authen server_host 10.1.1.222 protocol tacacs+ port 15555 timeout 10
Command: create authen server_host 10.1.1.222 protocol tacacs+ port 15555 timeout 10

Success.

DGS-3200-10:4#
```

config authen server_host

目的

ユーザ定義の認証サーバホストを設定します。

構文

config authen server_host <ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius] {port <int 1-65535> | key [<key_string 254> | none] | timeout <int 1-255> | retransmit <int 1-255>}

説明

スイッチに TACACS/XTACACS/TACACS+/RADIUS セキュリティプロトコルに対応したユーザ定義の認証サーバホストを設定します。ユーザが認証プロトコルを有効にしてスイッチにアクセスを試みると、スイッチはリモートホスト上の TACACS/XTACACS/TACACS+/RADIUS サーバホストに認証パケットを送信します。すると TACACS/XTACACS/TACACS+/RADIUS サーバホストはその要求を認証または拒否し、スイッチに適切なメッセージを返します。1 つの物理ホスト上で複数の認証プロトコルを動作させることは可能ですが、TACACS/XTACACS/TACACS+/RADIUS は別のエンティティであり、互換性を持たないことに注意が必要です。サポート可能なサーバホストは最大 16 台です。

パラメータ

パラメータ	説明
server_host <ipaddr>	変更するリモートサーバホストの IP アドレス。
protocol	サーバホストが使用するプロトコル。以下から選択します。 • tacacs - サーバホストが TACACS プロトコルを使用している場合に選択します。 • xtacacs - サーバホストが XTACACS プロトコルを使用している場合に選択します。 • tacacs+ - サーバホストが TACACS+ プロトコルを使用している場合に選択します。 • radius - サーバホストが RADIUS プロトコルを使用している場合に選択します。
port <int 1-65535>	サーバホスト上で認証プロトコルに使用する仮想ポート番号（1-65535）。ポート番号の初期値は、TACACS/XTACACS/TACACS+ サーバの場合は 49,RADIUS サーバの場合は 1812 および 1813 です。独自の番号を設定してセキュリティを向上することも可能です。
key [<key_string 254> | none]	• <key_string 254> - TACACS+ と RADIUS サーバの場合に指定する共有キー（254 文字までの半角英数字）。 • none - TACACS+ と RADIUS 認証に暗号化を使用しません。
timeout <int 1-255>	スイッチが、サーバホストからの認証リクエストへの応答を待つ時間（秒）。 初期値は 5（秒）です。
retransmit <int 1-255>	サーバからの応答がない場合に、デバイスが認証リクエストを再送する回数。TACACS+ プロトコルは操作できません。初期値は 2 です。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

TACACS+ 認証サーバホストのキーを設定します。

```
DGS-3200-10:4#config authen server_host 10.1.1.222 protocol tacacs+ key "This is a secret"
Command: config authen server_host 10.1.1.222 protocol tacacs+ key "This is a secret"

Success.

DGS-3200-10:4#
```

delete authen server_host

目的

ユーザ定義の認証サーバホストを削除します。

構文

delete authen server_host <ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius]

説明

登録済みのユーザ定義認証サーバホストを削除します。

パラメータ

パラメータ	説明
server_host <ipaddr>	削除するリモートサーバホストの IP アドレス。
protocol	削除するサーバホストが使用するプロトコル。以下から選択します。 • tacacs - サーバホストが TACACS プロトコルを使用している場合に選択します。 • xtacacs - サーバホストが XTACACS プロトコルを使用している場合に選択します。 • tacacs+ - サーバホストが TACACS+ プロトコルを使用している場合に選択します。 • radius - サーバホストが RADIUS プロトコルを使用している場合に選択します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

認証サーバホストを削除します。

```
DGS-3200-10:4#delete authen server_host 10.1.1.222 protocol tacacs+
Command: delete authen server_host 10.1.1.222 protocol tacacs+

Success.

DGS-3200-10:4#
```

show authen server_host

目的

ユーザ定義の認証サーバホストを参照します。

構文

show authen server_host

説明

登録済みのユーザ定義認証サーバホストを参照します。

パラメータ

なし。

制限事項

なし。

使用例

スイッチに現在設定している認証サーバホストを参照します。

```
DGS-3200-10:4#show authen server_host
Command: show authen server_host

IP Address       Protocol  Port   Timeout  Retransmit  Key
---------------  --------  -----  -------  ----------  -------------------------
10.1.1.222       TACACS+   15555  10       No Use      This is a secret

Total Entries : 1

DGS-3200-10:4#
```

config authen parameter response_timeout

目的

コンソール、Telnet、および SSH アプリケーションにおいて、スイッチがタイムアウトの前にユーザからの認証のレスポンスを待つ時間を設定します。

構文

config authen parameter response_timeout <int 0-255>

説明

ユーザからの認証のレスポンスに対するスイッチの待ち時間を指定します。

パラメータ

パラメータ	説明
response_timeout <int 0-255>	コマンドラインインタフェースまたは telnet インタフェースからユーザの認証レスポンスに対するスイッチの待ち時間を指定します。0-255（秒）の範囲から指定します。0 はタイムアウトにならないことを意味します。初期値は 30（秒）です。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

60 秒のレスポンスのタイムアウトを設定します。

```
DGS-3200-10:4# config authen parameter response_timeout 60
Command: config authen parameter response_timeout 60

Success.

DGS-3200-10:4#
```

config authen parameter attempt

目的

ユーザが認証を試みることができる最大回数を設定します。

構文

config authen parameter attempt <int 1-255>

説明

コマンドラインインタフェース、Telnet または SSH インタフェースからユーザが認証を試みることができる最大回数。指定回数認証に失敗すると、そのユーザはスイッチへのアクセスを拒否され、さらに認証を試みることができなくなります。CLI ユーザは、再度認証を行うために 60 秒待つ必要があります。

パラメータ

パラメータ	説明
parameter attempt <int 1-255>	コマンドラインインタフェース、Telnet または SSH インタフェースからユーザがスイッチによる認証のために試みることができる最大回数を設定します。初期値は 3 です。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

許可される認証試みの最大数に 9 を設定します。

```
DGS-3200-10:4#config authen parameter attempt 5
Command: config authen parameter attempt 5

Success.

DGS-3200-10:4#
```

show authen parameter

目的

スイッチに現在設定されている認証パラメータを表示します。

構文

show authen parameter

説明

レスポンスタイムアウトおよびユーザ認証を試みる回数を含むスイッチに設定されている現在の認証パラメータを表示します。

パラメータ

なし。

制限事項

なし。

使用例

スイッチに現在設定している認証パラメータを参照します。

```
DGS-3200-10:4#show authen parameter
Command: show authen parameter

Response Timeout : 60 seconds
User Attempts    : 9

DGS-3200-10:4#
```

enable admin

目的

ユーザレベルから管理者レベルに権限を昇格します。

構文

enable admin

説明

通常のユーザレベルとしてスイッチにログインした後、管理者レベルに変更する場合に使用します。スイッチにログインした後のユーザにはユーザレベルの権限のみが与えられています。管理者レベルの権限を取得するためには、本コマンドを入力し、認証用パスワードを入力します。本機能における認証方法には、TACACS/XTACACS/TACACS+/RADIUS、ユーザ定義のサーバグループ、local enable（スイッチのローカルアカウント）または、認証なし（none）があります。XTACACS と TACACS は Enable の機能をサポートしていないため、ユーザはサーバホストに特別なアカウントを作成し、ユーザ名「enable」、および管理者が設定するパスワードを登録する必要があります。本機能は認証ポリシーが「disable」（無効）である場合には実行できません。

パラメータ

なし。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

スイッチで管理者レベルの権限を有効にします。

```
DGS-3200-10:4#enable admin
Password:******

DGS-3200-10:4#
```

config admin local_enable

目的

本コマンドは、通常のユーザレベルとしてスイッチにログインした後、管理者レベルに変更したい場合に使用します。スイッチにログインした後のユーザにはユーザレベルの権限のみが与えられています。管理者レベルの権限を取得するためには、本画面を開き、認証用パスワードを入力します。本機能における認証方法は、TACACS/ XTACACS/ TACACS+/ RADIUS、ユーザ定義のサーバグループ、local enable（スイッチ上のローカルアカウント）または、認証なし（none）から選択できます。XTACACS と TACACS は Enable の機能をサポートしていないため、ユーザはサーバホスト上に特別なアカウントを作成し、ユーザ名「enable」、および管理者が設定するパスワードを登録する必要があります。本機能は認証ポリシーが「disable」（無効）である場合には実行できません。

構文

config admin local_enable <password 15>

説明

「enable admin」コマンド用の Local Enable Password を設定します。ユーザがその権限をユーザレベルから管理者レベルに変更する際の認証方法に、「local_enable」を選択している場合、スイッチにローカルに登録したパスワードの入力が要求されます。

パラメータ

パラメータ	説明
<password 15>	本コマンドを入力した後、ユーザは元のパスワード、次に新しいパスワード、さらに確認のために再び新しいパスワードを入力します。パスワードは 15 文字以内の半角英数字で指定します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

「local_enable」認証方法のためのパスワードを設定します。

```
DGS-3200-10:4#config admin local_enable
Command: config admin local_enable

Enter the old password:
Enter the case-sensitive new password:******
Enter the new password again for confirmation:******
Success.

DGS-3200-10:4#
```

第 44 章　SSL コマンド

Secure Sockets Layer（SSL）とは、認証、デジタル署名および暗号化を使用して、ホストとクライアント間に安全な通信パスを提供するセキュリティ機能です。このセキュリティ機能は、認証セッションに使用する厳密な暗号パラメータ、特定の暗号化アルゴリズムおよびキー長を決定する、暗号スイートと呼ばれるセキュリティ文字列により実現しています。SSL は、以下の 3 つの段階で構成されます。

1. 鍵交換
   暗号スイート文字列の最初の部分では、使用する公開鍵アルゴリズムを規定しています。本スイッチは、RSA（Rivest Shamir Adleman）公開鍵アルゴリズムとデジタル署名アルゴリズム（DHE : DHE DSS Diffie-Hellman 公開鍵アルゴリズムとして指定）を使用します。本レベルは、鍵を交換して適合する相手を探し、暗号化のネゴシエーションを行うまでの認証を行って、次のレベルに進むというクライアント、ホスト間の最初のプロセスとなります。
2. 暗号化
   暗号スイートの次の段階は、クライアントとホスト間で送受信するメッセージの暗号化を含む暗号化方式です。本スイッチは 2 種類の暗号化アルゴリズムをサポートしています。
   - ストリーム暗号 – スイッチは 2 種類のストリーム暗号に対応します。1 つは 40 ビット鍵での RC4、もう 1 つは 128 ビット鍵での RC4 です。これらの鍵はメッセージの暗号化に使用され、最適な使用のためにはクライアントとホスト間で一致させる必要があります。
   - CRC ブロック暗号 – CBC（Cipher Block Chaining : 暗号ブロック連鎖）とは、前に暗号化したブロックの暗号文を使用して現在のブロックの暗号化を行う方法です。本スイッチは、DES（Data Encryption Standard）で定義する 3 DES EDE 暗号化コードをサポートし、暗号文を生成します。
3. ハッシュアルゴリズム
   暗号スイートの最後の段階では、メッセージ認証コードを決定するメッセージダイジェスト機能を規定します。このメッセージ認証コードは送信されたメッセージで暗号化され、整合性を提供し、リプレイアタックを防止します。本スイッチは、MD5（Message Digest 5）と SHA（Secure Hash Algorithm）の 2 種類のハッシュアルゴリズムをサポートします。

これら 3 つのパラメータは、スイッチ上での 4 つの選択肢として独自に組み合わされ、サーバとホスト間で安全な通信を行うための 3 層の暗号化コードを生成します。暗号スイートの中から 1 つ、または複数を組み合わせて実行することができますが、選択する暗号スイートによりセキュリティレベルや安全な接続時のパフォーマンスは変化します。暗号スイートに含まれる情報はスイッチには存在していないため、証明書と呼ばれるファイルを第三者機関からダウンロードする必要があります。この証明書ファイルがないと本機能をスイッチ上で実行することができません。証明書ファイルは、TFTP サーバを使用してスイッチにダウンロードできます。本スイッチは、SSLv3 および TLSv1 をサポートしています。SSL の他のバージョンは本スイッチとは互換性がないおそれがあり、クライアントからホストへの認証やメッセージ送信時に問題が発生する場合があります。

「SSL Configuration Settings」画面では、ネットワークマネージャが SSL を有効にしてスイッチに暗号スイートを設定できます。暗号スイートは認証セッションに使用する、正確な暗号のパラメータ、特定の暗号化アルゴリズム、および鍵のサイズを決定する文字列です。スイッチは SSL 機能のための 4 つの暗号スイートを持ち、初期設定ではすべてを有効にしていますが、特定の暗号スイートのみ有効にして、他のものを無効にすることも可能です。

SSL 機能が有効になると、Web の使用はできなくなります。SSL 機能を使用しながら Web ベースの管理を行うためには、Web ブラウザが SSL 暗号化をサポートし、https:// で始まる URL を使用しなければなりません。（例 : https://10.90.90.90）これを守らないと、エラーが発生し、Web ベースの管理機能にアクセスできなくなります。

本画面では、SSL を使用するための証明書ファイルを TFTP サーバからダウンロードします。証明書ファイルは、ネットワーク上のデバイスを認証するために使われるデータであり、所有者の情報や認証のための鍵やデジタル署名などの情報が格納されています。SSL 機能を最大限に活用するためには、サーバとクライアントが一致した証明書ファイルを持つ必要があります。スイッチは、拡張子 ".der" を持つ証明書のみをサポートします。スイッチは証明書が既にロードされている形で発送されますが、ユーザの環境によっては、さらにダウンロードが必要になる場合があります。

コマンドラインインタフェース（CLI）における Secure Sockets Layer（SSL）コマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
show ssl certificate	
download ssl certificate	<ipaddr> certfilename <path_filename 64> keyfilename <path_filename 64>
enable ssl	{ciphersuite {RSA_with_RC4_128_MD5 | RSA_with_3DES_EDE_CBC_SHA | DHE_DSS_with_3DES_EDE_CBC_SHA | RSA_EXPORT_with_RC4_40_MD5}}
disable ssl	{ciphersuite {RSA_with_RC4_128_MD5 | RSA_with_3DES_EDE_CBC_SHA | DHE_DSS_with_3DES_EDE_CBC_SHA | RSA_EXPORT_with_RC4_40_MD5}}
show ssl	
show ssl cachetimeout	
config ssl cachetimeout	<value 60-86400>

以下のセクションで各コマンドについて詳しく記述します。

show ssl certificate

目的

スイッチの SSL と証明書ファイルの状態を参照します。

構文

show ssl certificate

説明

スイッチで現在実行している SSL 証明書ファイル情報を参照します。

パラメータ

なし。

制限事項

なし。

使用例

スイッチの証明書ファイル情報を参照します。

```
DGS-3200-10:4#show ssl certificate
Command: show ssl certificate

Loaded with RSA Certificate!

DGS-3200-10:4#
```

download ssl certificate

目的

スイッチの SSL 機能のために証明書ファイルをダウンロードします。

構文

download ssl certificate <ipaddr> certfilename <path_filename 64> keyfilename <path_filename 64>

説明

SSL を使用するための証明書ファイルを TFTP サーバからダウンロードします。証明書ファイルは、ネットワーク上のデバイスを認証するために使われるデータであり、所有者の情報や認証のための鍵やデジタル署名などの情報が格納されています。SSL 機能を最大限に活用するためには、サーバとクライアントが一致した証明書ファイルを持つ必要があります。本スイッチは、拡張子 ".der" を持つ証明書のみをサポートします。RSA 鍵交換のためには、RSA タイプの証明書をダウンロードし、DHS_DSS のためには鍵交換に DSA 証明書を使用する必要があります。

パラメータ

パラメータ	説明
<ipaddr>	TFTP サーバの IP アドレスを指定します。
certfilename <path_filename 64>	ダウンロードする証明書ファイルのパスとファイル名を入力します。
keyfilename <path_filename 64>	ダウンロードする秘密鍵ファイルのパスとファイル名を入力します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

スイッチに証明書ファイルをダウンロードします。

```
DGS-3200-10:4#download ssl certificate 10.55.47.1 certfilename cert.der keyfilename pkey.der
Command: download ssl certificate 10.55.47.1 certfilename cert.der keyfilename pkey.der

Success.

DGS-3200-10:4#
```

enable ssl

目的

スイッチの SSL 機能と暗号スイートを有効にします。

構文

enable ssl{ ciphersuite {RSA_with_RC4_128_MD5 | RSA_with_3DES_EDE_CBC_SHA | DHE_DSS_with_3DES_EDE_CBC_SHA | RSA_EXPORT_with_RC4_40_MD5}}

説明

ネットワークマネージャが SSL を有効にしてスイッチに暗号スイートを設定できます。本コマンドをパラメータなしで入力すると、スイッチの SSL 状態は無効になります。SSL 機能が有効になると Web ベースマネジメントは無効になります。

パラメータ

パラメータ	説明
ciphersuite	暗号スイートは認証セッションに使用する、正確な暗号のパラメータ、特定の暗号化アルゴリズム、および鍵のサイズを決定する文字列です。ユーザは以下のどの組み合わせも選択できます。 • RSA_with_RC4_128_MD5 - この暗号スイートは RSA key exchange、stream cipher C4（128-bit keys）、MD5 Hash Algorithm の組み合わせです。 • RSA_with_3DES_EDE_CBC_SHA - RSA key exchange with 3DES_EDE_CBC encryption、SHA Hash Algorithm の組み合わせです。 • DHE_DSS_with_3DES_EDE_CBC_SHA - この暗号スイートは DSA Diffie Hellman key exchange、CBC Block Cipher 3DES_EDE encryption、SHA Hash Algorithm の組み合わせです。 • RSA_EXPORT_with_RC4_40_MD5 - この暗号スイートは RSA Export key exchange、stream cipher RC4（40-bit keys）、MD5 Hash Algorithm の組み合わせです。 • パラメータの指定なし - SSL 機能を有効にします。 スイッチは SSL 機能のための 4 つの暗号スイートを持ち、初期設定ではすべてを有効にしていますが、暗号スイートを持つ SSL を有効にして、他の SSL を無効にすることも可能です。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

RSA_with_RC4_128_MD5 に対して SSL 暗号スイートを有効にします。

```
DGS-3200-10:4#enable ssl ciphersuite RSA_with_RC4_128_MD5
Command: enable ssl ciphersuite RSA_with_RC4_128_MD5

Note: Web will be disabled if SSL is enabled.
Success.

DGS-3200-10:4#
```

SSL を有効にします。

```
DGS-3200-10:4#enable ssl
Command: enable ssl

Success.

DGS-3200-10:4#
```

disable ssl

目的

スイッチの SSL 機能を無効にします。

構文

disable ssl{ ciphersuite {RSA_with_RC4_128_MD5 | RSA_with_3DES_EDE_CBC_SHA | DHE_DSS_with_3DES_EDE_CBC_SHA | RSA_EXPORT_with_RC4_40_MD5}

説明

スイッチの SSL を無効にし、さらに暗号スイートのどんな組み合わせも無効にすることができます。

パラメータ

パラメータ	説明
ciphersuite	暗号スイートは認証セッションに使用する、正確な暗号のパラメータ、特定の暗号化アルゴリズム、および鍵のサイズを決定する文字列です。ユーザは以下のどの組み合わせも選択できます。 • RSA_with_3DES_EDE_CBC_SHA - RSA key exchange with 3DES_EDE_CBC encryption、SHA Hash Algorithm の組み合わせです。 • DHE_DSS_with_3DES_EDE_CBC_SHA - この暗号スイートは DSA Diffie Hellman key exchange、CBC Block Cipher 3DES_EDE encryption、SHA Hash Algorithm の組み合わせです。 • RSA_EXPORT_with_RC4_40_MD5 - この暗号スイートは RSA Export key exchange、stream cipher RC4（40-bit keys）、MD5 Hash Algorithm の組み合わせです。 • パラメータの指定なし - SSL 機能を無効にします。 スイッチは SSL 機能のための 4 つの暗号スイートを持ち、初期設定ではすべてを有効にしていますが、暗号スイートを持つ SSL を有効にして、他の SSL を無効にすることも可能です。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

スイッチの SSL 状態を無効にします。

```
DGS-3200-10:4#disable ssl
Command: disable ssl

Success.

DGS-3200-10:4#
```

暗号スイート RSA_with_RC4_128_MD5 に対して SSL 暗号スイートを無効にします。

```
DGS-3200-10:4#disable ssl ciphersuite RSA_with_RC4_128_MD5
Command: disable ssl ciphersuite RSA_with_RC4_128_MD5

Success.

DGS-3200-10:4#
```

show ssl

目的
　現在の SSL 状態とサポートする暗号スイートを表示します。
構文
　show ssl
説明
　現在の SSL 状態とサポートする暗号スイートを表示します。
パラメータ
　なし。
制限事項
　なし。
使用例
　SSL を参照します。

```
DGS-3200-10:4#show ssl
Commands: show ssl

SSL Status                                      Disabled

RSA_WITH_RC4_128_MD5                    0x0004  Enabled
RSA_WITH_3DES_EDE_CBC_SHA               0x000A  Enabled
DHE_DSS_WITH_3DES_EDE_CBC_SHA           0x0013  Enabled
RSA_EXPORT_WITH_RC4_40_MD5              0x0003  Enabled

DGS-3200-10:4#
```

show ssl cachetimeout

目的
　SSL キャッシュタイムアウトを参照します。
構文
　show ssl cachetimeout
説明
　スイッチで現在実行されている SSL キャッシュタイムアウトを参照します。
パラメータ
　なし。
制限事項
　なし。
使用例
　スイッチで現在実行されている SSL キャッシュタイムアウトを参照します。

```
DGS-3200-10:4#show ssl cachetimeout
Command: show ssl cachetimeout

Cache timeout is 600 second(s)

DGS-3200-10:4#
```

config ssl cachetimeout

目的

SSL キャッシュタイムアウトを設定します。

構文

config ssl cachetimeout <value 60-86400>

説明

クライアントとホストの間の SSL による新しい鍵交換の間隔を指定します。クライアントとホストが鍵交換をすると常に新しい SSL セッションが確立します。この値を長くすると SSL セッションによる特定のホストとの再接続には主鍵が再利用されます。それためネゴシエーション処理は速くなります。60 秒（1 分）- 86400 秒（24 時間）で指定します。初期値は 600（秒）です。

パラメータ

パラメータ	説明
timeout <value 60-86400>	60-86400（秒）でタイムアウト時間を設定します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

SSL キャッシュタイムアウト値に 60 秒を設定します。

```
DGS-3200-10:4#config ssl cachetimeout 60
Commands: config ssl cachetimeout 60

Success.

DGS-3200-10:4#
```

第 45 章　SSH コマンド

リモート PC（SSH クライアント）とスイッチ（SSH サーバ）間でセキュアな通信を行うための SSH プロトコルの設定は、以下の手順で行います。

1. 「create account admin」コマンドで管理者レベルのアクセス権を持つアカウントを作成します。本手順はスイッチに管理者レベルのユーザアカウントを作成する方法と同じで、パスワードの設定を含みます。本パスワードは、SSH プロトコルを使用した安全な通信経路が確立された後、スイッチにログインする際に使用します。

2. 「config ssh user authmode」コマンドを使用して、ユーザアカウントを設定します。この時スイッチが SSH 接続の確立を許可する際のユーザの認証方法を指定します。この認証方法には、「password」、「publickey」、「hostbased」の 3 つがあります。

3. SSH クライアントとサーバ間で送受信するメッセージの暗号化、復号化に用いる暗号化アルゴリズムを設定します。

4. 最後に「enable ssh」コマンドで、SSH を有効にします。

これらの手順が完了後、安全な帯域内の通信を使用してリモート PC 上の SSH クライアントの設定とスイッチの管理を行うことができます。

コマンドラインインタフェース（CLI）における Secure Shell（SSH）コマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
config ssh algorithm	[3DES | AES128 | AES192 | AES256| arcfour|blowfish | cast128 | twofish128 | twofish192 | twofish256 | MD5 | SHA1 | RSA | DSA] [enable | disable]
show ssh algorithm	
config ssh authmode	[password | publickey | hostbased] [enable | disable]
show ssh authmode	
config ssh user	<username 15> authmode [publickey | password | hostbased [hostname <domain_name 32> | hostname_IP <domain_name 32> <ipaddr>]]
show ssh user authmode	
config ssh server	{maxsession <int 1-8>| contimeout <sec 120-600> | authfail <int 2-20> | rekey [10min | 30min | 60min | never]}
enable ssh	
disable ssh	
show ssh server	

以下のセクションで各コマンドについて詳しく記述します。

config ssh algorithm

目的

SSH アルゴリズムを設定します。

構文

config ssh algorithm [3DES | AES128 | AES192 | AES256 | arcfour | blowfish | cast128 | twofish128 | twofish192 | twofish256 | MD5 | SHA1 | RSA | DSA] [enable | disable]

説明

認証の暗号化に使用する SSH アルゴリズムの種類を設定します。

パラメータ

パラメータ	説明
3DES	Triple_Data EtiStddtilithEncryption Standard 暗号化アルゴリズムを有効または無効にします。
AES128	AES 128 暗号化アルゴリズムを有効または無効にします。
AES192	AES 192 暗号化アルゴリズムを有効または無効にします。
AES256	AES 256 暗号化アルゴリズムを有効または無効にします。
arcfour	Arc Four 暗号化アルゴリズムを有効または無効にします。
blowfish	Blowfish 暗号化アルゴリズムを有効または無効にします。
cast128	Cast128 暗号化アルゴリズムを有効または無効にします。
twofish128	Twofish 128 暗号化アルゴリズムを有効または無効にします。
twofish192	Twofish 192 暗号化アルゴリズムを有効または無効にします。
MD5	MD5 暗号化アルゴリズムを有効または無効にします。
SHA1	Secure Hash Algorithm 暗号化を有効または無効にします。
RSA	RSA 暗号化アルゴリズムを有効または無効にします。
DSA	Digital Signature Algorithm 暗号化を有効または無効にします。
[enable | disable]	本コマンドで入力したアルゴリズムを有効または無効にします。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

SSH アルゴリズムを設定します。

```
DGS-3200-10:4#config ssh algorithm DSA enable
Command: config ssh algorithm DSA enable

Success.

DGS-3200-10:4#
```

show ssh algorithm

目的

SSH アルゴリズム設定を表示します。

構文

show ssh algorithm

説明

現在の SSH アルゴリズム設定状態を表示します。

パラメータ

なし。

制限事項

なし。

使用例

スイッチに現在設定されている SSH アルゴリズムを表示します。

```
DGS-3200-10:4#show ssh algorithm
Command: show ssh algorithm

Encryption Algorithm
--------------------------
3DES       : Enabled
AES128     : Enabled
AES192     : Enabled
AES256     : Enabled
arcfour    : Enabled
blowfish   : Enabled
cast128    : Enabled
twofish128 : Enabled
twofish192 : Enabled
twofish256 : Enabled

Data Integrity Algorithm
--------------------------
MD5        : Enabled
SHA1       : Enabled

Public Key Algorithm
--------------------------
RSA        : Enabled
DSA        : Enabled

DGS-3200-10:4#
```

config ssh authmode

目的

スイッチの SSH 認証設定を行います。

構文

config ssh authmode [password | publickey | hostbased] [enable | disable]

説明

スイッチにアクセスを試みるユーザのために SSH 認証モードを設定します。

パラメータ

パラメータ	説明
password	スイッチにおける認証にローカルに設定したパスワードを使用します。
publickey	スイッチにおける認証に SSH サーバに設定した公開鍵を使用します。
hostbased	認証にホストコンピュータを使用します。本パラメータは SSH 認証機能を必要とする Linux ユーザ向けに設定されます。ホストコンピュータには SSH プログラムがインストールされ、Linux OS が起動している必要があります。
[enable | disable]	指定された SSH 認証を有効または無効にします。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

スイッチに SSH ユーザ認証方式を設定します。

```
DGS-3200-10:4#config ssh authmode publickey enable
Command: config ssh authmode publickey enable

Success.

DGS-3200-10:4#
```

show ssh authmode

目的

SSH 認証モード設定を表示します。

構文

show ssh authmode

説明

スイッチの現在の SSH 認証設定を表示します。

パラメータ

なし。

制限事項

なし。

使用例

スイッチの現在の認証モード設定を表示します。

```
DGS-3200-10:4#show ssh authmode
Command: show ssh authmode

The SSH Authmode :
-----------------------------------------------------
Password  : Enabled
Publickey : Enabled
Hostbased : Enabled

DGS-3200-10:4#
```

config ssh user

目的

SSH 設定におけるユーザ情報を更新します。

構文

config ssh user <username 15> authmode [publickey | password | hostbased [hostname <domain_name 32> | hostname_ip <domain_name 32> <ipaddr>]]

説明

SSH 設定におけるユーザ情報を更新します。

パラメータ

パラメータ	説明
<username 15>	SSH ユーザを識別するユーザ名を 15 文字までの半角英数字で指定します。
authmode	スイッチへのログインを希望する SSH ユーザの認証モードを指定します。管理者は以下のパラメータを選択することができます。publickey、password、hostbased
publickey	SSH サーバ上の公開鍵を使用して認証を行う場合に選択します。
password	管理者定義のパスワードを使用して認証を行う場合に選択します。本パラメータを選択すると、スイッチは管理者にパスワードの入力（確認のため 2 回）を促します。
hostbased	認証用にリモート SSH サーバを使用する場合に選択します。本パラメータを選択すると、SSH ユーザの識別のために「hostname」および「hostname_ip」フィールドの入力が必要になります。本パラメータは SSH 認証機能を必要とする Linux ユーザ向けに設定されます。ホストコンピュータには SSH プログラムがインストールされ、Linux OS が起動している必要があります。
hostname <domain_name 32>	ホストのドメイン名を指定します。
hostname_IP <domain_name 32> <ipaddr>	SSH ユーザのホスト名と対応する IP アドレスを入力します。 • domain_name - ホストベースモードで設定する場合に、ホスト名を指定します。 • ipaddr - ホストベースモードで設定する場合に、ホストの IP アドレスを指定します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。ユーザアカウントを作成する必要があります。

使用例

SSH ユーザ「test」の認証モードを更新します。

```
DGS-3200-10:4#config ssh user test authmode publickey
Command: config ssh user test authmode publickey

Success.

DGS-3200-10:4#
```

show ssh user authmode

目的

SSH 認証ユーザ設定を表示します。

構文

show ssh user authmode

説明

スイッチの現在の SSH ユーザ設定を表示します。

パラメータ

なし。

制限事項

なし。

使用例

スイッチの現在の SSH ユーザ設定を表示します。

```
DGS-3200-10:4#show ssh user
Command: show ssh user

Current Accounts :
Username        Authmode    HostName HostIP
--------------  ----------  -------- ------
test            publickey

Total Entries : 1

DGS-3200-10:4#
```

注意 SSH ユーザを設定するためには、管理者はスイッチにユーザアカウントを作成する必要があります。ユーザアカウント設定に関する情報については、本マニュアル 30 ページの「第 5 章 基本のスイッチコマンド」の「create account」コマンドを参照してください。

config ssh server

目的

SSH サーバを設定します。

構文

config ssh server {maxsession <int 1-8>| contimeout <sec 120-600> | authfail <int 2-20> | rekey [10min | 30min | 60min | never] }

説明

スイッチに SSH サーバ設定のパラメータを設定します。

パラメータ

パラメータ	説明
maxsession <int 1-8>	同時にスイッチに接続できる数を 1 から 8 の数字を設定します。初期値は 8 です。
contimeout <sec 120-600>	接続のタイムアウト時間を指定します。120 から 600（秒）を設定します。初期値は 300（秒）です。
authfail <int 2-20>	ユーザが SSH サーバに対して認証を試みることができる回数を指定します。指定した回数を超えるとスイッチは接続を切り、ユーザは再度スイッチに接続する必要があります。
rekey [10min | 30min | 60min | never]	スイッチが SSH 暗号を変更する期間を設定します。「never」を指定すると、スイッチはセッションキーを再生成しません。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

SSH サーバに最大セッション 3 を設定します。

```
DGS-3200-10:4#config ssh server maxsession 3
Command: config ssh server maxsession 3

Success.

DGS-3200-10:4#
```

enable ssh

目的

SSH サーバを有効にします。

構文

enable ssh

説明

スイッチの SSH サーバサービスを有効にします。

パラメータ

なし。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。SSH を有効にすると、Telnet は無効になります。

使用例

SSH を有効にします。

```
DGS-3200-10:4#enable ssh
Command: enable ssh

Success.

DGS-3200-10:4#
```

disable ssh

目的
　SSH サーバを無効にします。
構文
　disable ssh
内容
　スイッチの SSH サーバサービスを無効にします。
パラメータ
　なし。
制限事項
　管理者レベルユーザのみ本コマンドを実行できます。
使用例
　SSH を無効にします。

```
DGS-3200-10:4#disable ssh
Command: disable ssh

Success.

DGS-3200-10:4#
```

show ssh server

目的
　SSH 認証サーバ設定を表示します。
構文
　show ssh server
説明
　スイッチの現在の SSH サーバ設定を表示します。
パラメータ
　なし。
制限事項
　なし。
使用例
　SSH サーバを表示します。

```
DGS-3200-10:4#show ssh server
Command: show ssh server

The SSH Server Configuration
Max Session         : 3
Connection Timeout  : 300
Authfail Attempts   : 2
Rekey Timeout       : 60min

DGS-3200-10:4#
```

第 46 章　IP-MAC-Port バインディング（IMPB）コマンド

IP ネットワークレイヤ（IP レベル）では 4 バイトのアドレスを使用し、イーサネットリンクレイヤ（データリンクレベル）では 6 バイトの MAC アドレスを使用します。これらの 2 つのアドレスタイプを結合させることにより、レイヤ間のデータ転送を可能にします。IP-MAC-Port バインディングの第一の目的は、スイッチにアクセスするユーザ数を制限することです。IP アドレスと MAC アドレスのペアを、事前に設定したデータベースと比較を行い、認証クライアントのみがスイッチのポートにアクセスできるようにします。未認証ユーザが IP-MAC-Port バインディングが有効なポートにアクセスしようとすると、システムはアクセスをブロックして、パケットを廃棄します。IP-MAC-Port バインディングのエントリ数はチップの能力（例えば ARP テーブルサイズ）およびデバイスのストレージサイズによって異なります。本シリーズにおける IP-MAC-Port バインディングの最大エントリ数は 512 です。認証クライアントのリストは、CLI または Web により手動で作成できます。本機能はポートベースであるため、ポートごとに本機能を有効 / 無効にすることができます。

ACL モード

IP-MAC-Port バインディングで生じたいくつかの特別なケースのために、IP-MAC-Port バインディングに特別な ACL モードを実装しています。これは、これらの問題を軽減することができます。有効にすると、スイッチはアクセスプロファイルテーブルに 2 つのエントリを作成します。スイッチに利用可能なプロファイル番号が少なくとも 2 つある場合にだけ、エントリは作成されます。そうでない場合に ACL モードが有効にされると、エラーメッセージが表示されます。ACL モードが有効にされる場合、スイッチは IP-MAC-Port バインディング設定で作成されたエントリからのパケットだけを受信します。他のすべてのパケットは破棄されます。
ACL モードを設定するためには、はじめに「create address_binding ip_mac ipaddress」コマンドで IP-MAC-Port バインディングを作成し、ACL モードを選択する必要があります。その後、「enable address_binding acl_mode」コマンドを入力することでモードを有効にする必要があります。IP-MAC-Port バインディングエントリを作成し、それを ACL モードエントリに変更する場合には、「config address_binding ip_mac ipaddress」コマンドを使用して、ACL モードを選択します。

注意 IP-MAC-Port バインディング機能の ACL モードの設定を行う時は、登録済みの ACL エントリの内容に十分ご注意ください。ACL モードエントリは、若い空き番号から 2 つの ID を使用し、またアクセスプロファイル ID は、ACL プライオリティ（優先度）を示すため、ACL モードエントリが他の ACL エントリより優先されてしまう可能性があります。ACL エントリが優先されることにより設定内容の競合が発生し、ユーザ定義の ACL パラメータが無効になる恐れがあります。ACL 設定についての詳しい情報は、340 ページの「第 58 章 アクセスコントロールリスト（ACL）コマンド」を参照してください。

注意 ACL プロファイルを IP-MAC-Port バインディング機能を通じて作成すると、それらの ACL モードアクセスプロファイルエントリに対して編集、削除または追加はできません。ACL ルールの編集、削除または追加を行うと前画面にエラーメッセージが表示されます。

注意 スイッチにコンフィグレーションファイルをアップロードする場合、ロードされる ACL 設定に注意してください。本機能によって設定された ACL モードのアクセスプロファイルは、アクセスプロファイルタイプの両方に問題を引き起こす可能性があります。

コマンドラインインタフェース（CLI）における IP-MAC-Port バインディングコマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
create address_binding ip_mac ipaddress	<ipaddr> mac_address <macaddr> {ports [<portlist> | all] | mode [arp | acl]}
config address_binding ip_mac ports	[<portlist> | all] {state [enable {[strict | loose]} | disable] | allow_zeroip [enable | disable] | forward_dhcppkt [enable | disable] | mode [arp | acl] | stop_learning_threshold <0-500>}
config address_binding ip_mac ipaddress	<ipaddr> mac_address <macaddr> {ports [<portlist> | all] | mode [arp | acl] }
delete address_binding	[ip_mac [ipaddress <ipaddr> mac_address <macaddr> | all] | blocked [all | vlan_name <vlan_name> mac_address <macaddr>]]
show address_binding	{[ip_mac [all | ipaddress <ipaddr> mac_address <macaddr>] | blocked [all | vlan_name <vlan_name> mac_address <macaddr>] | ports]}
enable address_binding trap_log	
disable address_binding trap_log	
enable address_binding dhcp_snoop	
disable address_binding dhcp_snoop	
clear address_binding dhcp_snoop binding_entry ports	[<portlist> | all]
show address_binding dhcp_snoop	{[max_entry {ports <portlist>} | binding_entry {port <portlist>}]}
config address_binding dhcp_snoop max_entry ports	[<portlist> | all] limit [<value 1-50> | no_limit]
config address_binding recover_learning ports	[<portlist> | all]
enable address_binding arp_inspection	
disable address_binding arp_inspection	

create address_binding ip_mac ipaddress

目的

IP-MAC-Port バインディングエントリを作成します。

構文

create address_binding ip_mac ipaddress <ipaddr> mac_address <macaddr> {ports [<portlist> | all] | mode [arp | acl]}

説明

IP-MAC-Port バインディングエントリを作成します。

パラメータ

パラメータ	説明
<ipaddr>	IP-MAC-Port バインディングエントリを作成するために使用する IP アドレス。
mac_address <macaddr>	IP-MAC-Port バインディングエントリを作成するために使用する MAC アドレス。
ports [<portlist> | all]	• <portlist> - アドレスバインディングを設定するポートまたはポート範囲を指定します。 • all - スイッチのすべてのポートがアドレスバインディングに設定されます。
mode [arp | acl]	以下の 2 つのモードのいずれかを選択することによって、IP-MAC-Port バインディング設定のモードを設定します。システムが ARP モードであるなら、ARP モードエントリと ACL モードエントリが有効になります。システムが ACL モードであると、ACL モードエントリだけがアクティブになり、ARP モードエントリは有効になりません。指定されないと、ARP モードが初期値となります。 • arp - 入力した IP と MAC アドレスにより、通常の IP-MAC-Port バインディングエントリを設定します。 • acl - 送信元がここで作成した IP-MAC-Port バインディングエントリであるパケットだけを許可します。異なる IP アドレスを持つそれ以外のパケットは廃棄されます。本モードは、「enable address_binding acl_mode」コマンドで ACL モードを有効にした場合にだけ使用できます。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

スイッチのアドレスバインディングを作成します。

```
GS-3200-10:4#create address_binding ip_mac ipaddress 10.1.1.1 mac_address 00-00-00-00-00-
11
Command: create address_binding ip_mac ipaddress 10.1.1.1 mac_address 00-00-00-00-00-11

Success.

DGS-3200-10:4#
```

config address_binding ip_mac ports

目的

指定されたポートに対して IP-MAC 状態を有効または無効に設定します。

構文

config address_binding ip_mac ports [<portlist> | all] {state [enable {[strict | loose]} | disable] | allow_zeroip [enable | disable] | forward_dhcppkt [enable | disable] | mode [arp | acl] | stop_learning_threshold <0-500>}

説明

スイッチにおける IP-MAC バインディングの状態をポートごとに設定します。ポートがリンクアグリゲーショングループのメンバとして設定されている場合、IP-MAC バインディング機能を有効にすることはできません。バインディングのチェック状態を有効にすると、スイッチは、このポートが受信した IP パケットおよび ARP パケットに対して、IP アドレスおよび MAC アドレスがバインディングエントリに一致するかどうかチェックします。一致しないと、パケットは破棄されます。

スイッチは、本機能に対して ACL モードまたは ARP モードで動作します。ARP モードでは、ARP パケットだけがバインディングのためにチェックされます。ACL モードでは、ARP パケットと IP パケットの両方がバインディングのためにチェックされます。そのため、ACL モードではパケットに対してより厳しいチェックを提供します。

ポートモードを ACL に設定する場合、スイッチはこのポートのエントリに対応する ACL アクセスエントリを作成します。
ポートが ARP モードに変更されると、すべての ACL アクセスエントリが自動的に削除されます。

パラメータ

パラメータ	説明
ports [<portlist> | all]	• <portlist> - 設定するポートまたは範囲を指定します。 • all - スイッチのすべてのポートがアドレスバインディングに設定されます。
state [enable {[strict | loose]} | disable]	アドレスをバインディングしているポートの状態を有効または無効にします。有効にすると、ポートはバインディングのチェックを行います。 • strict - より厳しいコントロール方法を提供します。ユーザがこれを選択すると、すべてのパケットが初期状態でスイッチに防御されます。スイッチは、すべての到来する ARP/IP パケットを比較し、IMPB ホワイトリストとそれらの突き合わせを試みます。IP-MAC のペアがホワイトリストに一致すると、MAC アドレスからのパケットは防御されません。一致しない場合、MAC アドレスは防御されたままとなります。Strict 状態では到来する ARP および IP パケットのチェックに対してより多くのリソースを使用しますが、より高いセキュリティを実施します。初期設定は「strict」が使用されます。 • loose - より緩いコントロール方法を提供します。モードを選択すると、スイッチは初期値ですべてのパケットを転送します。しかし、スイッチは到来する ARP パケットを検証し、スイッチの IMPB ホワイトリストとそれらを比較します。パケットの IP-MAC のペアがホワイトリストに見つけられないと、スイッチは MAC アドレスを防御します。loose 状態を実行する主な利点は、スイッチが入力パケットだけをチェックするため、より少ない CPU リソースの使用だけですむという点です。しかし、それはユニキャスト IP パケットだけを送信するユーザを防御できないため、Strict モードよりも安全性が低くなります。この状況の例は、悪意あるユーザーが (DoS) が彼らの PC の上に静的に ARP テーブルを構成することによって攻撃するサービス妨害を実行しようとする時である。この場合、スイッチは、PC がどんな ARP パケットも送信しないような攻撃から防御することができません。
allow_zeroip [enable | disable]	SIP アドレス 0.0.0.0 を持つ ARP パケットを許容するか否かを指定します。0.0.0.0 がバインディングリストに設定されないと、有効に設定した場合に、この送信元 IP アドレス 0.0.0.0 を持つ ARP パケットは許可されます。 • enable - 送信元 IP がゼロである DHCP パケットを転送できます。 • disable - 標準的なロジックに従って処理します。IP-MAC- ポートバインディングの ACL モードには影響しません。
forward_dhcppkt [enable | disable]	初期設定では、ブロードキャスト DA の DHCP パケットをフラッドします。無効にすると、ブロードキャスト DHCP パケットは特定のポートによって受信され、フォワードされません。本設定は、CPU でトラップした DHCP パケットがソフトウェアで転送される必要があるため、DHCP Snooping が有効に設定されている場合に効果があります。本設定はこの状況における転送の実行をコントロールします。
mode [arp | acl]	• ACL - スイッチはこのポートのエントリに対応する ACL アクセスエントリを作成します。 • ARP - すべての ACL アクセスエントリが自動的に削除されます。ポートの初期モードは「ARP」です。
stop_learning_threshold <0-500>	防御エントリ数がしきい値を超えると、ポートは新しいアドレスの学習を中止します。新しいアドレスを持つパケットは廃棄されます。初期値は 0(制限なし) です。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

ポート 1 にアドレスバインディングを設定します。

```
DGS-3200-10:4#config address_binding ip_mac ports 1 state enable
Command: config address_binding ip_mac ports 1 state enable

Success.

DGS-3200-10:4#show access_profile
Command: show access_profile

Access Profile Table

Total Unused Rule Entries : 200
Total Used Rule Entries   : 0

Access Profile ID: 1                    Type : IP
================================================================================
Owner : IP-MAC-PORT Binding
MASK Option :
Source MAC Source IP MASK
FF-FF-FF-FF-FF-FF 255.255.255.255
----------------- ---------------

Access ID : 1     Mode: Permit     RX Rate(64Kbps) : no_limit
Ports : 1
----------------- ---------------
00-00-00-00-00-01 10.0.0.1
================================================================================
Unused Entries: 199

Access Profile ID: 4                    Type : Ethernet
================================================================================
Owner : IP-MAC-PORT Binding
MASK Option :
Ethernet Type
-------------
Access ID : 1      Mode: Deny
Ports : 1
-------------
0x800
================================================================================
Unused Entries: 199

DGS-3200-10:4#
```

config address_binding ip_mac ipaddress

目的

IP-MAC-Port バインディングエントリを設定します。

構文

config address_binding ip_mac ipaddress <ipaddr> mac_address <macaddr> {ports [portlist | all] mode [acl | arp]}

説明

IP-MAC-Port バインディングエントリを設定します。

パラメータ

パラメータ	説明
<ipaddr>	IP-MAC-Port バインディングを行うデバイスの IP アドレス。
<macaddr>	IP-MAC-Port バインディングを行うデバイスの MAC アドレス。
ports [<portlist> | all]	• <portlist> - アドレスバインディングを設定するポートまたはポート範囲を指定します。 • all - スイッチのすべてのポートがアドレスバインディングに設定されます。
mode [arp | acl]	以下の 2 つのモードのいずれかを選択することによって、IP-MAC-Port バインディング設定のモードを設定します。システムが ARP モードであるなら、ARP モードエントリと ACL モードエントリが有効になります。システムが ACL モードであると、ACL モードエントリだけがアクティブになり、ARP モードエントリは有効になりません。指定されないと、ARP モードが初期値となります。 • arp - 入力した IP と MAC アドレスにより、通常の IP-MAC-Port バインディングエントリを設定します。 • acl - 送信元がここで作成した IP-MAC-Port バインディングエントリであるパケットだけを許可します。異なる IP アドレスを持つそれ以外のパケットは廃棄されます。本モードは、「enable address_binding acl_mode」コマンドで ACL モードを有効にした場合にだけ使用できます。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

スイッチにアドレスバインディングを設定します。

```
DGS-3200-10:4#config address_binding ip_mac ipaddress 10.1.1.1 mac_address 00-00-00-00-00-11
Command: config address_binding ip_mac ipaddress 10.1.1.1 mac_address 00-00-00-00-00-11

Success.

DGS-3200-10:4#
```

delete address_binding

目的

IP-MAC-Port バインディングエントリを削除します。

構文

delete address_binding [ip-mac [ipaddress <ipaddr> mac_address <macaddr> |all] | blocked [all | vlan_name <vlan_name> mac_address <macaddr>]]

説明

IP-MAC-Port バインディングエントリを削除します。2 種類の情報を削除することができます。ACL モードが有効になると、スイッチはそれに対応する ACL アクセスエントリを自動的に削除します。

- ip_mac - デバイスの物理アドレス、および IP アドレスを入力することによって Address Binding エントリを削除することができます。「all」を指定すると、すべての Address Binding エントリを削除します。
- blocked - VLAN 名とデバイスの物理アドレスを入力することによって、Blocked Address Binding エントリ（VLAN 名と MAC アドレス間のバインディング）を削除することができます。「all」を指定すると、すべての Blocked Address Binding エントリを削除します。

パラメータ

パラメータ	説明
<ipaddr>	IP-MAC-Port バインディングを行うデバイスの IP アドレス。
<macaddr>	IP-MAC-Port バインディングを行うデバイスの MAC アドレス。
<vlan_name>	既知の VLAN で特定のデバイスをブロックするために MAC アドレスに割り当てられる VLAN の名前。
all	IP-MAC-Port バインディングとして、すべての IP-MAC-Port バインディングエントリを指定します。Blocked Address Binding エントリとして、ブロックされるすべての VLAN と連結する物理アドレスを指定します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

スイッチの IP-MAC Binding を削除します。

```
DGS-3200-10:4#delete address_binding ip_mac ipaddress 10.1.1.1 mac_address 00-00-00-00-00-11
Command: delete address_binding ip_mac ipaddress 10.1.1.1 mac_address 00-00-00-00-00-11

Success.

DGS-3200-10:4#
```

show address_binding

目的

アドレスバインディングエントリ、ブロックされた MAC エントリ、およびポートの状態を表示します。

構文

show address_binding {[ip_mac [all | ipaddress <ipaddr> mac_address <macaddr>] | blocked [all | vlan_name <vlan_name> mac_address <macaddr>] | ports]}

説明

IP-MAC-Port バインディングエントリを表示します。3 種類の情報を参照することができます。

- ip_mac - デバイスの物理アドレスおよび IP アドレスを入力することによって Address Binding エントリを参照することができます。
- blocked - VLAN 名とデバイスの物理アドレスを入力することによって、Blocked Address Binding エントリ（VLAN 名と MAC アドレス間のバインディング）を参照することができます。
- ports - デバイスにおける有効なポート数。

パラメータ

パラメータ	説明
all	IP-MAC-Port バインディングとして、すべての IP-MAC-Port バインディングエントリを指定します。Blocked Address Binding エントリとして、ブロックされるすべての VLAN と連結する物理アドレスを指定します。
<ipaddr>	IP-MAC-Port バインディングが行われるデバイスの IP アドレス。
<macaddr>	IP-MAC-Port バインディングが行われるデバイスの MAC アドレス。

制限事項

なし。

使用例

アドレスバインディングのグローバルな設定を表示します。

```
DGS-3200-10:4#show address_binding
Command: show address_binding

Trap/Log       : Disabled
DHCP Snoop     : Disabled
ARP Inspection : Disabled

DGS-3200-10:4#
```

アドレスバインディングのグローバルな設定をポートごとに表示します。

```
DGS-3200-10:4#show address_binding ports
Command: show address_binding ports

Port State    Mode Zero      DHCP     Stop Learning
                   IP        Packet   Threshold/Mode
---- -------- ---- --------- -------- --------------
1    Disabled ARP  Not Allow Forward  500/Normal
2    Disabled ARP  Not Allow Forward  500/Normal
3    Disabled ARP  Not Allow Forward  500/Normal
4    Disabled ARP  Not Allow Forward  500/Normal
5    Disabled ARP  Not Allow Forward  500/Normal
6    Disabled ARP  Not Allow Forward  500/Normal
7    Disabled ARP  Not Allow Forward  500/Normal
8    Disabled ARP  Not Allow Forward  500/Normal
9    Disabled ARP  Not Allow Forward  500/Normal
10   Disabled ARP  Not Allow Forward  500/Normal

DGS-3200-10:4#
```

すべての IP-MAC- ポートバインディングエントリのアドレスバインディング設定を表示します。

```
DGS-3200-10:4#show address_binding ip_mac all
Command: show address_binding ip_mac all

IP/MAC Address : 10.1.1.1      /00-00-00-00-00-11
Mode           : Static
Ports          : 1,3,5,7,8

IP/MAC Address : 10.1.1.2      /00-00-00-00-00-12
Mode           : Static
Ports          : 1

IP/MAC Address : 10.1.1.10      /00-00-00-00-00-aa
Mode           : DHCP Snooping
Ports          : 1

Total Entries : 3

DGS-3200-10:4#
```

注意 上記の出力で表示された「mode」パラメータは、IP-MAC- ポートバインディングエントリがマニュアルまたはダイナミックに作成されたかどうかを示すために使用されます。次の項目は、エントリがマニュアルまたはダイナミックに作成されたかどうかを示すのに使用されます。

1. Static : IP-MAC- ポートバインディングエントリが、マニュアルで設定されたことを示しています。
2. DHCP Snooping : IP-MAC- ポートバインディングエントリが、DHCP サーバによってダイナミックに作成されたことを示しています。

enable address_binding trap_log

目的

アドレスバインディングのトラップ / ログを有効にします。

構文

enable address_binding trap_logenable address_binding trap_log

説明

アドレスバインディングモジュールが不正な IP と MAC アドレスを検出するとトラップとログを送信します。

パラメータ

なし。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

アドレスバインディングのトラップ / ログを有効にします。

```
DGS-3200-10:4#enable address_binding trap_log
Command: enable address_binding trap_log

Success.

DGS-3200-10:4#
```

disable address_binding trap_log

目的
　アドレスバインディングのトラップ / ログを無効にします。
構文
　disable address_binding trap_log
説明
　アドレスバインディングのトラップ / ログを無効にします。
パラメータ
　なし。
制限事項
　管理者レベルユーザのみ本コマンドを実行できます。
使用例
　アドレスバインディングのトラップ / ログを無効にします。

```
DGS-3200-10:4#disable address_binding trap_log
Command:disable address_binding trap_log

Success.

DGS-3200-10:4#
```

enable address_binding dhcp_snoop

目的
　アドレスバインディングの Auto モードを有効にします。
構文
　enable address_binding dhcp_snoop
説明
　アドレスバインディングの Auto モードを有効にします。初期値では DHCP Snooping は無効です。

　DHCP Snooping 機能が有効な場合、アドレスバインディングが無効であるすべてのポートがサーバポートとして機能します。つまり、スイッチは、サーバポートを経由して DHCP OFFER と DHCP ACK パケットにより IP アドレスを学習します。

　自動的に学習された IP-MAC バインディングエントリは MAC アドレス学習機能に基づいて特定のソースポートにマップされます。このエントリは、この特定のポートに対して ACL モードのバインディングエントリとして作成されます。各エントリはリースタイムに対応付けられます。リースタイムの期限が切れると、期限切れのエントリはこのポートから削除されます。MAC アドレスが異なるポートに移動したことを DHCP Snooping 機能が学習すると、自動的に学習されたバインディングエントリは 1 つのポートから別のポートに移動されます。

　DHCP Snooping によって学習されたバインディングエントリが、スタティックに設定されたエントリとコンフリクトすると仮定します。これは、バインディング関係が矛盾していることを意味します。例えば、IP A がスタテック設定によって MAC X にバインドされている場合、DHCP Snooping に学習されたバインディングエントリが、MAC Y にバインドされている IP A であるとすると、矛盾となります。DHCP Snooping が学習したエントリがスタティックに設定されたエントリにバインドされる場合、DHCP Snooping が学習したエントリは作成されません。

　DHCP Snooping がバインディングエントリを学習し、同じ IP-MAC をバインディングするペアがスタティックに設定されるというもう一方のコンフリクトケースを仮定します。学習した情報がスタティックに設定したエントリと一致していると、自動的に学習されたエントリは作成されません。エントリが ARP モードでスタティックに設定されると、自動的に学習されたエントリは作成されません。エントリが 1 つのポートにスタティックに設定され、そのエントリが別のポートでも自動的に学習されると、自動的に学習されたエントリは作成されません。
パラメータ
　なし。
制限事項
　管理者レベルユーザのみ本コマンドを実行できます。
使用例
　アドレスバインディングのトラップ / ログを無効にします。

```
DGS-3200-10:4#enable address_binding dhcp_snoop
Command: enable address_binding dhcp_snoop

Success.

DGS-3200-10:4#
```

disable address_binding dhcp_snoop

目的

アドレスバインディングの ACL モードを無効にします。

構文

disable address_binding dhcp_snoop

説明

無効にすると、自動的に学習されたすべてのバインディングエントリが削除されます。

パラメータ

なし。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

アドレスバインディングの Auto モードを無効にします。

```
DGS-3200-10:4#disable address_binding dhcp_snoop
Command: disable address_binding dhcp_snoop

Success.

DGS-3200-10:4#
```

clear address_binding dhcp_snoop

目的

指定ポートで学習したアドレスバインディングエントリをクリアします。

構文

clear address_binding dhcp_snoop binding_entry ports [<portlist> | all]

説明

指定ポートで学習したアドレスバインディングエントリをクリアします。

パラメータ

パラメータ	説明
ports [<portlist> | all]	DHCP Snooping が学習したエントリをクリアするポートのリストを指定します。 • <portlist> - クリアするポートまたはポート範囲を指定します。 • all - スイッチのすべてのポートをクリアします。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

ポート 1-3 のアドレスバインディングエントリをクリアします。

```
DGS-3200-10:4#clear address_binding dhcp_snoop binding_entry ports 1-3
Command: clear address_binding dhcp_snoop binding_entry ports 1-3

Success.

DGS-3200-10:4#
```

show address_binding dhcp_snoop

目的

アドレスバインディングの自動学習データベースを参照します。

構文

show address_binding dhcp_snoop {[max_entry {ports <portlist>} | binding_entry {port <portlist>}]}

説明

自動学習データベースを表示します。

パラメータ

パラメータ	説明
max_entry {ports <portlist>}	DHCP Snooping の最大エントリ情報を表示します。
binding_entry {port <portlist>}	DHCP Snooping のバインディング情報を表示します

制限事項

なし。

使用例

アドレスバインディングにおける DHCP Snooping のステータスを表示します。

```
DGS-3200-10:4#show address_binding dhcp_snoop
Command: show address_binding dhcp_snoop

DHCP_Snoop : Enabled

DGS-3200-10:4#
```

DHCP Snooping のバインディング情報を表示します。

```
DGS-3200-10:4#show address_binding dhcp_snoop binding_entry
Command: show address_binding dhcp_snoop binding_entry

IP Address      MAC Address       Lease Time(secs) Port     Status
--------------- ----------------- ---------------- -------- ---------
10.62.58.35     00-0B-5D-05-34-0B 35964            1        Active
10.33.53.82     00-20-c3-56-b2-ef 2590             2        Inactive

Total Entries : 2

DGS-3200-10:4#
```

注意 「Inactive」は、ポートのリンクダウンのために現在無効であることを示しています。

アドレスバインディングにおける DHCP Snooping のステータスを表示します。

```
DGS-3200-10:4#show address_binding dhcp_snoop max_entry
Command: show address_binding dhcp_snoop max_entry

Port Max Entry
---- ---------
1    10
2    10
3    10
4    no_limit
5    no_limit
6    no_limit
7    no_limit
8    no_limit
9    no_limit
10   no_limit

DGS-3200-10:4#
```

config address_binding dhcp_snoop max_entry

目的

指定ポートが学習できる最大エントリ数を指定します。

構文

config address_binding dhcp_snoop max_entry ports [<portlist> | all] limit [<value 1-10> | no_limit]

説明

指定ポートが学習できる最大エントリ数を指定します。初期設定では 1 ポートあたりの最大エントリは制限なしです。

パラメータ

パラメータ	説明
<portlist> | all	• <portlist> - dhcp-snoop を学習する最大エントリ数を設定するポートまたはポートのリストを指定します。 • all - すべてのポートに指定します。
limit [<value 1-10> | no_limit]	• <value 1-10> - 最大数（1-10）を指定します。 • no_limit - 最大数を指定しません。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

ポート 1-3 に学習する最大エントリ数 10 を設定します。

```
DGS-3200-10:4#config address_binding dhcp_snoop max_entry ports 1-3 limit 10
Command: config address_binding dhcp_snoop max_entry ports 1-3 limit 10

Success.

DGS-3200-10:4#
```

config address_binding recover_learning ports

目的

ポートに対する ARP チェック機能を回復します。

構文

config address_binding recover_learning ports [<portlist> | all]

説明

動作を停止している ARP チェック機能を回復します。

パラメータ

パラメータ	説明
<portlist> | all	• <portlist> - ARP チェック機能を回復するポートのリストを指定します。 • all - すべてのポートに指定します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

ポート 6 および 7 に対する ARP チェック機能を回復します。

```
DGS-3200-10:4#config address_binding recover_learning ports 6-7
Command: config address_binding recover_learning ports 6-7

Success.

DGS-3200-10:4#
```

enable address_binding arp_inspection

目的
　ARP の検証機能を有効にします。
構文
　enable address_binding arp_inspection
説明
　アドレスバインディングの ARP 検証を有効にします。
パラメータ
　なし。
制限事項
　管理者レベルユーザのみ本コマンドを実行できます。
使用例
　アドレスバインディングの ARP 検証を有効にします。

```
DGS-3200-10:4#enable address_binding arp_inspection
Command: enable address_binding arp_inspection

Success.

DGS-3200-10:4#
```

disable address_binding arp_inspection

目的
　アドレスバインディングの ARP 検証を無効にします。
構文
　disable address_binding arp_inspection
説明
　アドレスバインディングの ARP 検証を無効にします。
パラメータ
　なし。
制限事項
　管理者レベルユーザのみ本コマンドを実行できます。
使用例
　アドレスバインディングの ARP 検証を有効にします。

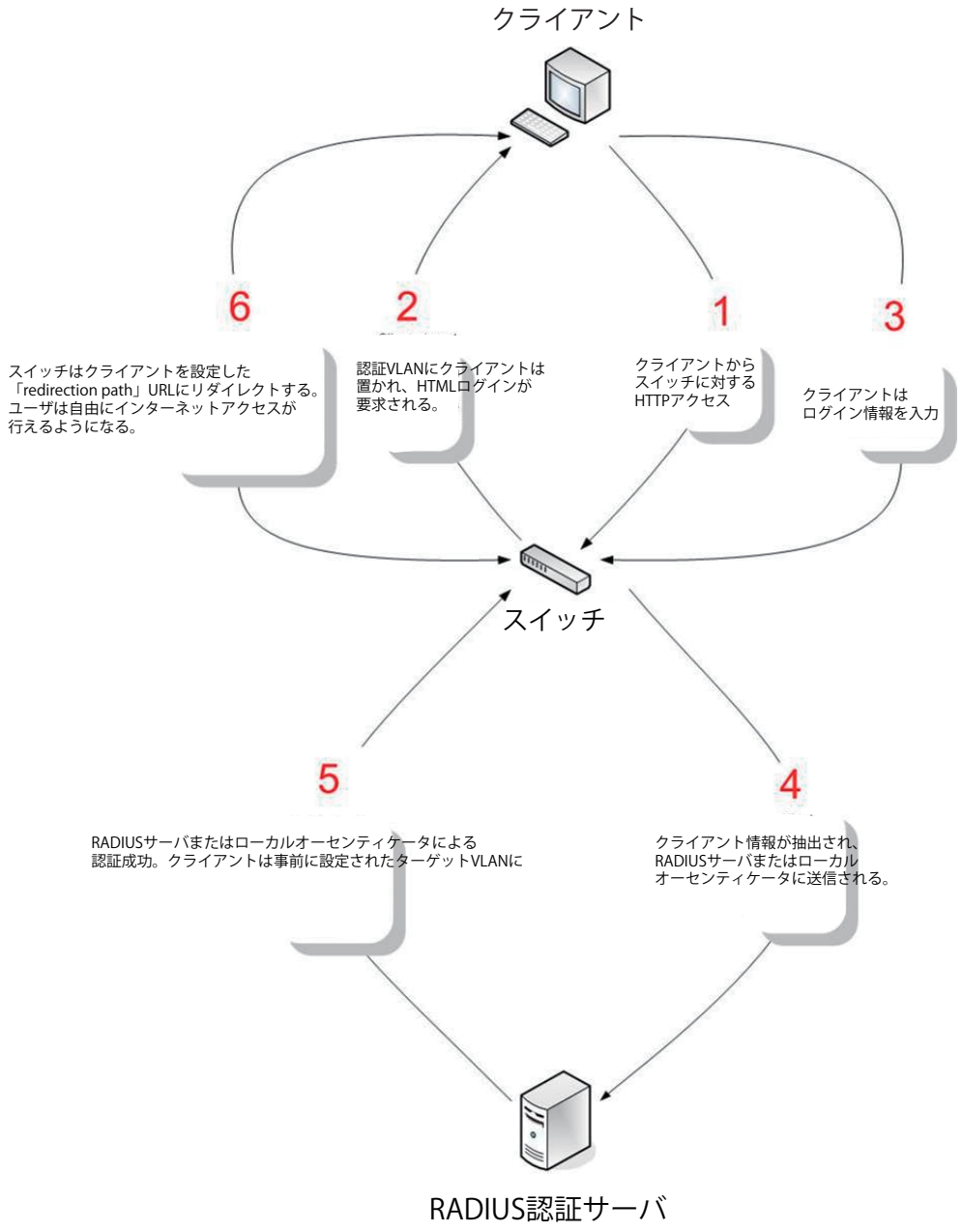
```
DGS-3200-10:4#disable address_binding arp_inspection
Command: disable address_binding arp_inspection

Success.

DGS-3200-10:4#
```

第 47 章　Web 認証コマンド

Web ベースアクセスコントロールとして知られている Web 認証は、先に記述した 802.1X ポートベースのアクセスコントロール方式と並ぶ、もう 1 つのポートベースのアクセスコントロール方式として実装されています。あるユーザがスイッチを経由してネットワークにアクセスを試みる時、そのユーザが接続されているポート上で本機能が有効に設定されていれば、RADIUS サーバ、またはスイッチ上に登録したローカルな認証情報を使用したユーザ認証が行われます。

ユーザが Web へのアクセスを行おうとすると、スイッチからの HTTP パケットの受信が許可される前に、ユーザ名とパスワードの提示を要求されます。クライアントが Web サイトへのアクセスを試みる時、そのポートはユーザが定義する認証 VLAN に割り当てられます。この認証 VLAN 内のすべてのクライアントは、ローカルメソッドにより、または RADIUS サーバを利用した認証を求められます。認証に成功すると、そのユーザはスイッチ上のターゲット VLAN に割り当てられ、インターネットにアクセスする権利を得ます。アクセスを拒否された場合は、ユーザはパケットを受け取ることができず、認証 VLAN へと戻され、再び認証の手順が行われます。
クライアントがあるポートで認証されると、そのポートは事前に設定した VLAN に割り当てられ、そのポート上の他のすべてのクライアントに対しても、特定のリダイレクションパス URL へアクセスするための認証が実行されます。

次の図は、Web ベースのアクセスコントロールを実現させるために、認証に関わる各ノードで行われる基本の 6 つのステップを例示しています。



条件および制限

1. 認証 VLAN の IP インタフェースのサブネットは、クライアントのものと一致している必要があります。この設定が正しく行われないと、オーセンティケータは永遠に認証を拒否します。
2. クライアントが IP アドレス取得のために DHCP を使用している場合、認証 VLAN はクライアントが IP アドレス取得を行えるように、DHCP サーバまたは DHCP リレー機能を持つ必要があります。
3. 本機能で使用する認証 VLAN は、CPU パフォーマンスを向上させ、DNS、UDP、HTTP パケットの処理を行えるように、DNS サーバへアクセスを行うよう設定される必要があります。
4. アクセスプロファイル機能のように、スイッチ上に存在する機能の中には HTTP パケットをフィルタしてしまうものがあります。ターゲット VLAN にフィルタ機能の設定を行う際には、HTTP パケットがスイッチにより拒否されないように、十分に注意してください。
5. リダイレクションパスの設定は、Web ベースのアクセスコントロールを有効にする前に行ってください。そうでない場合は、エラーメッセージが表示され、Web ベースのアクセスコントロールを有効にできません。
6. 認証に RADIUS サーバを使用する場合、Web 認証を有効にする前に、ターゲット VLAN を含む必要な項目を入力して RADIUS サーバの設定を行ってください。

注意 WAC/JWAC 認証では、System インタフェースが Up している必要があります。

コマンドラインインタフェース（CLI）における Web 認証コマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
enable wac	
disable wac	
config wac ports	[[<portlist> | all] {state [enable | disable] | aging_time [infinite | <min 1-1440>] | idle_time [infinite | <min 1-1440>] | block_time [<sec 0-300>]}
config wac method	[local | radius]
config wac auth_failover	[enable | disable]
config wac default_redirpath	<string 128>
config wac clear_default_redirpath	
config wac virtual_ip	<ipaddr>
config wac switch_http_port	<tcp_port_number 1-65535> {[http | https]}
create wac user	<username 15> {[vlan <vlan_name 32> | vlanid <vlanid 1-4094>]}
delete wac	[user <username 15> | all_users]
config wac user	<username 15> [vlan <vlan_name 32> | vlanid <vlanid 1-4094> | clear_vlan]
show wac ports	{<portlist>}
show wac user	
show wac auth_state ports	{<portlist>} {authenticated | authenticating | blocked}
clear wac auth_state	[ports [<portlist> | all] {authenticated | authenticating | blocked} | macaddr <macaddr>]

以下のセクションで各コマンドについて詳しく記述します。

enable wac

目的

Web ベースアクセスコントロール機能を有効にします。

構文

enable wac

説明

WAC ベースアクセスコントロール機能を有効にします。

パラメータ

なし。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

WAC 機能を有効にします。

```
DGS-3200-10:4#enable wac
Command: enable wac

Success.

DGS-3200-10:4#
```

disable wac

目的

WAC ベースアクセスコントロール機能を無効にします。

構文

disable wac

説明

WAC ベースアクセスコントロール機能を無効にします。

パラメータ

なし。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

WAC 機能を無効にします。

```
DGS-3200-10:4#disable wac
Command: disable wac

Success.

DGS-3200-10:4#
```

config wac ports

目的

WAC ポートレベルを設定します。

構文

config wac ports [<portlist> | all] {state [enable | disable] | aging_time [infinite | <min 1-1440>] | idle_time [infinite | <min 1-1440>] | block_time [<sec 0-300>]}

説明

Web 認証を設定します。

パラメータ

パラメータ	説明
ports [<portlist> | all]	Web 認証ポートとして有効になるポートおよびポート範囲を指定します。「all」はすべてのポートを指定します。
state [enable | disable]	Web 認証機能を「enable」（有効）または「disable」（無効）にします。
aging_time [infinite | <min 1-1440>]	認証ホストが認証状態を保つ時間を指定します。「infinite」を指定すると、ポート上の認証ホストはエージングされません。初期値は 1440 分（24 時間）です。
idle_time [infinite | <min 1-1440>]	指定期間にトラフィックがない場合、認証ホストは未認証状態に移行します。「infinite」を指定すると、ホストはアイドル状態となり、認証状態から削除されません。初期値は「infinite」です。
block_time [<sec 0-300>]	認証を通過することに失敗した場合にホストが再認証前にブロックされる時間を指定します。初期値は 60（秒）です。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

WAC ポートの状態を指定します。

```
DGS-3200-10:4#config wac ports 1-8 state enable
Command: config wac ports 1-8 state enable

Success.

DGS-3200-10:4#
```

エージングタイムを設定します。

```
DGS-3200-10:4#config wac ports 1 aging_time 10
Command: config wac ports 1 aging_time 10

Success.

DGS-3200-10:4#
```

config wac method

目的

Web 認証のグローバルなパラメータを設定します。

構文

config wac method [local | radius]

説明

Web 認証のグローバルなパラメータを設定します。

パラメータ

パラメータ	説明
[local | radius]	認証方式を指定します。 • local - 認証はローカルデータベース経由で行われます。 • radius - 認証は RADIUS サーバ経由で行われます。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

認証方式を設定します。

```
DGS-3200-10:4#config wac method radius
Command: config wac method radius

Success.

DGS-3200-10:4#
```

config wac auth_failover

目的

WAC 認証フェイルオーバを設定します。

構文

config wac auth_failover [enable | disable]

説明

WAC 認証フェイルオーバを設定します。初期値では認証フェイルオーバは無効です。RADIUS サーバに到達しないと、認証エラーとなります。
認証フェイルオーバが有効な場合には RADIUS サーバ認証は未反応でありローカルデータベースが認証のために使用されます。

パラメータ

パラメータ	説明
[enable | disable]	• enable - プロトコル認証フェイルオーバを有効にします。 • disable - プロトコル認証フェイルオーバを無効にします。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

WAC 認証フェイルオーバを設定します。

```
DGS-3200-10:4#config wac auth_failover enable
Command: config wac auth_failover enable

Success.

DGS-3200-10:4#
```

config wac default_redirpath

目的

WAC のリダイレクト先の初期値を設定します。

構文

config wac default_redirpath <string 128>

説明

WAC のリダイレクト先の初期値を設定します。ダイレクト先の初期値が設定されると、認証完了後にクライアントはこのパスにリダイレクトされます。文字列がクリアされると、認証完了後にクライアントは別の URL にはリダイレクトされません。

パラメータ

パラメータ	説明
<string 128>	認証完了後にクライアントがリダイレクトされる URL を指定します。初期値では、リダイレクトされるパスはありません。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

WAC のリダイレクト先の初期値を設定します。

```
DGS-3200-10:4#config wac default_redirpath http://www.dlink.com
Command: config wac default_redirpath http://www.dlink.com

Success.

DGS-3200-10:4#
```

config wac clear_default_redirpath

目的

WAC のリダイレクト先の初期値をクリアします。

構文

config wac clear_default_redirpath

説明

WAC のリダイレクト先の初期値をクリアします。文字列がクリアされると、認証完了後にクライアントは別の URL にはリダイレクトされません。

パラメータ

なし。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

WAC のリダイレクト先の初期値をクリアします。

```
DGS-3200-10:4#config wac clear_default_redirpath
Command: config wac clear_default_redirpath

Success.

DGS-3200-10:4#
```

config wac virtual_ip

目的

未認証ホストからの認証リクエストを許可するのに使用する WAC バーチャル IP アドレスを設定します。

構文

config wac virtual_ip <ipaddr>

説明

未認証ホストからの認証リクエストを許可するのに使用する WAC バーチャル IP アドレスを設定します。バーチャル IP が指定されると、バーチャル IP に送信された TCP パケットは応答を受け取ります。バーチャル IP が有効にされると、バーチャル IP または物理 IP インタフェースの IP アドレスに送信された TCP パケットは共に応答を受け取ります。バーチャル IP に 0.0.0.0 が設定されている場合、バーチャル IP は無効となります。初期値では、バーチャル IP は 0.0.0.0 です。本バーチャル IP は、どの ARP リクエストまたは ICMP パケットにも応答しません。本機能を適切に動作させるためには、バーチャル IP は既存の IP アドレスにしないでください。さらに、既存のサブネットに位置することもできません。

パラメータ

パラメータ	説明
<ipaddr>	バーチャル IP の IP アドレスを指定します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

未認証ホストからの認証リクエストを許可するのに使用する WAC バーチャル IP アドレスを設定します。

```
DGS-3200-10:4#config wac virtual_ip 1.1.1.1
Command: config wac virtual_ip 1.1.1.1

Success.

DGS-3200-10:4#
```

config wac switch_http_port

目的

WAC スイッチがリッスンする TCP ポートを指定します。

構文

config wac switch_http_port <tcp_port_number 1-65535> {[http | https]}

説明

WAC スイッチがリッスンする TCP ポートを指定します。HTTP または HTTPS に対する TCP ポートは、認証処理のために CPU にトラップされる HTTP または HTTPS パケットを識別するためやログインページにアクセスするために使用されます。指定しない場合、HTTP に対するポート番号の初期値は 80、HTTPS に対するポート番号の初期値は 443 となります。プロトコルを指定しないと、HTTP になります。

パラメータ

パラメータ	説明
<tcp_port_number 1-65535>	WAC スイッチがリッスンし、認証プロセスを終了するために使用する TCP ポート。
[http | https]	• http - WAC はこの TCP ポート上で HTTP プロトコルを動作させます。 • https - WAC はこの TCP ポート上で HTTPS プロトコルを動作させます。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。HTTP ポートは TCP ポート 443、HTTPS は TCP ポート 80 で動作することはできません。

使用例

WAC スイッチがリッスンする TCP ポートを指定します。

```
DGS-3200-10:4#config wac switch_http_port 8888 http
Command: config wac switch_http_port 8888 http

Success.

DGS-3200-10:4#
```

create wac user

目的

Web ベースアクセスコントロールにユーザアカウントを作成します。

構文

create wac user <username 15> {[vlan <vlan_name 32> | vlanid <vlanid 1-4094>]}

説明

Web ベースアクセスコントロールにユーザアカウントを作成します。このユーザアカウントはログインユーザアカウントとは無関係です。VLAN が指定されないと、ユーザは認証後に VLAN を割り当てることができません。

パラメータ

パラメータ	説明
<username 15>	Web ベースアクセスコントロールのユーザアカウントを指定します。
vlan <vlan_name 32>	作成済みの VLAN から、上記ユーザが認証に成功した際に割り当てる VLAN 名を指定します。
vlanid <vlanid 1-4094>	作成済みの VLAN から、上記ユーザが認証に成功した際に割り当てる VLAN ID を指定します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

WAC アカウントを作成します。

```
DGS-3200-10:4#create wac user duhon vlan 123
Command: create wac user duhon vlan 123

Enter a case-sensitive new password:****
Enter the new password again for confirmation:****
Success.

DGS-3200-10:4#
```

delete wac user

目的

Web ベースアクセスコントロールのユーザアカウントを削除します。

構文

delete wac [user <username 15> | all users]

説明

アカウントを削除します。

パラメータ

パラメータ	説明
user <username 15>	Web ベースアクセスコントロールのユーザアカウント。
all users	本オプションを選択すると、現在の WAC ユーザをすべて削除します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

WAC アカウントを削除します。

```
DGS-3200-10:4#delete wac user duhon
Command: delete wac user duhon

Success.

DGS-3200-10:4#
```

config wac user

目的

ユーザアカウントの VLAN を設定します。

構文

config wac user <username 15> [vlan <vlan_name 32> | vlanid <vlanid 1-4094> | clear_vlan]

説明

ユーザアカウントの VLAN を設定します。

パラメータ

パラメータ	説明
<username 15>	VID を変更するユーザアカウント名。
vlan <vlan_name 32>	認証 VLAN 名。
vlanid <vlanid 1-4094>	認証 VLAN ID。
clear_vlan	指定 VLAN をクリアします。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

ユーザアカウントの VLAN を設定します。

```
DGS-3200-10:4#config wac user duhon vlan default
Command: config wac user duhon vlan default

Enter a old password:***
Enter a case-sensitive new password:*****
Enter the new password again for confirmation:*****

Success.

DGS-3200-10:4#
```

show wac ports

目的

Web 認証のポートレベル設定を表示します。

構文

show wac ports {<portlist>}

説明

Web 認証のポートレベル設定を表示します。

パラメータ

パラメータ	説明
{<portlist>}	ステータスを表示するするポートまたはメンバポートの範囲。

制限事項

なし。

使用例

ポート 1-3 の Web 認証設定を表示します。

```
DGS-3200-10:4#show wac ports 1-3
Command: show wac ports 1-3

Port    State    Aging Time    Idle Time  Block Time
                 (Minutes)     (Minutes)  (Seconds)
------- -------- ------------ ---------- -----------
1       Disabled 1440         Infinite   60
2       Disabled 1440         Infinite   60
3       Disabled 1440         Infinite   60

DGS-3200-10:4#
```

show wac user

目的

Web 認証ユーザアカウントを表示します。

構文

show wac user

説明

Web 認証ユーザアカウントを表示します。

パラメータ

なし。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

Web 認証ユーザアカウントを表示します。

```
DGS-3200-10:4#show wac user
Command: show wac user

Username  Password   VLAN ID
--------- ---------- ----------
123       abcde      1000

Total Entries : 1

DGS-3200-10:4#
```

show wac auth_state

目的

ポートの認証状態を表示します。

構文

show wac auth_state ports {<portlist>} {authenticated | authenticating | blocked }

説明

ポートの認証状態を表示します。

パラメータ

パラメータ	説明
ports {<portlist>}	WAC 状態を表示するポートのリストを指定します。
authenticated | authenticating | blocked	• authenticated - ポートに対して認証済みユーザのすべてを表示します。 • authenticating - ポートに対して認証中ユーザのすべてを表示します。 • blocked - ポートに対してブロックされたユーザのすべてを表示します。

制限事項

なし。

使用例

ポート 13 のポート認証状態を表示します。

```
DGS-3200-10:4#show wac auth_state ports 13
Command: show wac auth_state ports 13

                              Aging      Idle     Block
Port Hosts               VID   Time      Time     Time  Status
---- ------------------- ---- --------- --------- ------ ----------------
13   00-05-5D-0B-AD-A5   -    15 Sec    -         -      Authenticating
13   00-05-5D-0F-FB-35   -    15 Sec    -         -      Authenticating
13   00-05-5D-0F-FB-8D   1    1440      Infinite  -      Authenticated
13   00-05-5D-A5-5B-42   1    20 Sec    -         -      Authenticating
13   00-0D-61-95-AB-B7   -    1 Sec     -         -      Authenticating
13   00-0D-61-E7-95-0F   -    1 Sec     -         -      Authenticating
13   00-0F-EA-13-4F-4A   1    1 Sec     -         -      Authenticating
13   00-1A-4D-30-31-50   1    15 Sec    -         -      Authenticating

Total Authenticating Hosts :7
Total Authenticated Hosts :1
Total Blocked Hosts :0

DGS-3200-10:4#
```

clear wac auth_state

目的

ポートの WAC 認証状態をクリアします。

構文

clear wac auth_state [ports [<portlist> | all] {authenticated | authenticating | blocked} | macaddr <macaddr>]

説明

ポートの WAC 認証状態をクリアします。ポートは未認証状態に戻ります。ポートに関連しているすべてのタイマがリセットされます。

パラメータ

パラメータ	説明
ports [all | <portlist>]	WAC 状態をクリアするポートのリストを指定します。「all」を指定すると、すべてのポートの認証ステータスをクリアします。
authenticated | authenticating | blocked	• authenticated - ポートに対して認証済みユーザのすべてをクリアします。 • authenticating - ポートに対して認証中のユーザのすべてをクリアします。 • blocked - ポートに対してブロックされたユーザのすべてをクリアします。
macaddr <macaddr>	指定ユーザをクリアします。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

ポート 1-5 の WAC 状態をクリアします。

```
DGS-3200-10:4#clear wac auth_state ports 1-5
Command: clear wac auth_state ports 1-5

Success.

DGS-3200-10:4#
```

第 48 章　MAC アドレス認証コマンド

MAC アドレス認証機能は、ローカルまたはリモートの RADIUS サーバに MAC アドレスリストの設定を可能にし、スイッチによる認証と認証ユーザが位置するターゲット VLAN のスイッチ設定に基づいてアクセス権を付与します。

スイッチは、ARP パケットまたは DHCP パケットの受信を通してデバイスの MAC アドレスを学習し、認証リストとそれらを照合します。クライアントが DHCP 設定をしておらず、スタティックモードにも IP 設定がない場合、MAC アドレスは検出されないため、クライアントは認証されません。認証を待つポートと MAC アドレスは、スイッチ管理者が制限された権利と特権を割り当てることができるゲスト VLAN に置かれます。

スイッチのローカル認証のためには、以下の「MAC-Based Access Control Local Database Settings」画面を使用して、このメカニズムを通じて認証される MAC アドレスリストを入力する必要があります。ユーザは最大 1024 個の MAC アドレスをローカルにスイッチに入力できますが、MAC アドレス認証が有効な物理ポートに対して認証される MAC アドレスは 16 個です。
MAC アドレスがローカル側のスイッチに認証されると、その MAC アドレスがあり、権利と特権がスイッチの管理者に設定されているポートは、設定済みのターゲット VLAN に置かれます。ゲスト VLAN が無効であると、ターゲット VLAN は無視されます。ターゲット VLAN の VLAN 名をスイッチが検出できない場合、スイッチはその MAC アドレスを含むポートを送信元の VLAN に返します。MAC アドレスが検出されず、ポートがゲスト VLAN にある場合、そのゲスト VLAN に残ります。ポートがゲスト VLAN にない場合、この MAC アドレスはスイッチにブロックされます。

リモート RADIUS サーバ認証のためには、ユーザは、はじめにスイッチに認証されている MAC アドレスと対応するターゲット VLAN のリストを持つ RADIUS サーバを設定する必要があります。MAC アドレスが ARP または DHCP パケットを通じてスイッチに検出されると、スイッチは、RADIUS Access Request パケットを使用して、可能性のある MAC アドレスを持つリモート RADIUS サーバにクエリを送信します。ゲスト VLAN が有効であると、MAC アドレスとポートがタグなしとしてターゲット VLAN に追加されますが、PVID は変更されません。ターゲット VLAN が不正または「VLAN Static Table」に存在しない場合、MAC アドレスはオリジナルの VLAN に戻ります。オリジナルの VLAN が存在しないと、デフォルト VLAN におかれます。ゲスト VLAN が無効であると、RADIUS サーバによって割り当てられたターゲット VLAN が無視されます。MAC アドレスが検出されず、ポートがゲスト VLAN にある場合、対応する権利を持つゲスト VLAN にとどまります。ポートがゲスト VLAN にない場合、この MAC アドレスはスイッチにブロックされます。

MAC アドレス認証に関する注意

MAC アドレス認証に関するいくつかの制限と規則があります。

1. 本機能がポートに有効になると、スイッチはそのポートの FDB をクリアします。

2. ポートが、ゲスト VLAN ではない VLAN で MAC アドレスをクリアする権利を認められている場合、そのポート上の他の MAC アドレスは、アクセスのために認証されている必要があり、そうでない場合、スイッチにブロックされます。

3. ポートは、ゲスト VLAN ではない VLAN の物理ポートごとに最大 200 個の認証 MAC アドレスを受け入れます。既に最大数の認証済み MAC アドレスを持つポートに対して認証を試みても、他の MAC アドレスはブロックされます。

4. リンクアグリゲーション、ポートセキュリティ、または GVRP 認証が有効なポートを MAC アドレス認証用に有効にすることはできません。

コマンドラインインタフェース（CLI）における MAC アドレス認証コマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
enable mac_based_access_control	
disable mac_based_access_control	
config mac_based_access_control password	<passwd 16>
config mac_based_access_control method	[local | radius]
config mac_based_access_control auth_failover	[enable | disable]
config mac_based_access_control guest_vlan ports	<portlist>
config mac_based_access_control ports	[<portlist> | all] {state [enable | disable] | mode [port_based | host_based] | aging_time [infinite | <min 1-1440>] | hold_time [infinite | <sec 1-300>]}
create mac_based_access_control	[guest_vlan <vlan_name 32> | guest_vlanid <vlanid 1-4094>]
delete mac_based_access_control	[guest_vlan <vlan_name 32> | guest_vlanid < vlanid 1-4094>]
clear mac_based_access_control auth_mac	[ports [all | portlist] | mac_addr <macaddr>]
create mac_based_access_control_local	mac<macaddr> {[vlan <vlan_name 32> | vlanid <vlanid 1-4094>]}
config mac_based_access_control_local	mac <macaddr> [vlan <vlan_name 32> | vlanid <vlanid 1-4094>| clear_vlan]
delete mac_based_access_control_local	[mac <macaddr> | vlan <vlan_name 32> | vlanid <vlanid 1-4094>]
show mac_based_access_control	{ports [<portlist> | all]}
show mac_based_access_control auth_mac	{ports <portlist>}
show mac_based_access_control_local	{[mac<macaddr> | vlan <vlan_name 32> | vlanid <1-4094>]}
config mac_based_access_control trap	[enable | disable]

以下のセクションで各コマンドについて詳しく記述します。

enable mac_based_access_control

目的
　MAC アドレス認証を有効にします。
構文
　enable mac_based_access_control
説明
　MAC アドレス認証を有効にします。
パラメータ
　なし。
制限事項
　管理者レベルユーザのみ本コマンドを実行できます。
使用例
　MAC アドレス認証を有効にします。

```
DGS-3200-10:4#enable mac_based_access_control
Command: enable mac_based_access_control

Success.

DGS-3200-10:4#
```

disable mac_based_access_control

目的
　MAC アドレス認証を無効にします。
構文
　disable mac_based_access_control
説明
　MAC アドレス認証を無効にします。
パラメータ
　なし。
制限事項
　管理者レベルユーザのみ本コマンドを実行できます。
使用例
　MAC アドレス認証を無効にします。

```
DGS-3200-10:4#disable mac_based_access_control
Command: disable mac_based_access_control

Success.

DGS-3200-10:4#
```

config mac_based_access_control password

目的

MAC アドレス認証のパスワードを設定します。

構文

config mac_based_access_control password <passwd 16>

説明

RADIUS サーバ経由の認証に使用されるパスワードを設定します。

パラメータ

パラメータ	説明
<passwd 16>	RADIUS モードでは、スイッチは RADIUS サーバとの通信にパスワードを使用します。キーは 16 文字以内で指定します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

RADIUS サーバ経由の認証に使用されるパスワードに「rosebud」を設定します。

```
DGS-3200-10:4#config mac_based_access_control password rosebud
Command: config mac_based_access_control password rosebud

Success.

DGS-3200-10:4#
```

config mac_based_access_control method

目的

MAC アドレス認証方式を設定します。

構文

config mac_based_access_control method [local | radius]

説明

ローカルデータベースまたは RADIUS サーバ経由の認証に使用されます。

パラメータ

パラメータ	説明
[local | radius]	認証方式を指定します。認証タイプは以下の通りです。 • local - MACアドレス認証のオーセンティケータとしてローカルに設定されたMACアドレスデータベースを利用します。 • radius - MAC アドレス認証のオーセンティケータとしてリモート RADIUS サーバを利用します。MAC リストははじめに RADIUS サーバに設定されている必要があり、サーバの設定もスイッチに設定されている必要があることにご注意ください。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

MAC アドレス認証方式を「local」に設定します。

```
DGS-3200-10:4#config mac_based_access_control method local
Command: config mac_based_access_control method local

Success.

DGS-3200-10:4#
```

config mac_based_access_control auth_failover

目的

MAC アドレス認証の認証フェイルオーバを設定します。

構文

config mac_based_access_control auth_failover [enable | disable]

説明

MAC アドレス認証の認証フェイルオーバを設定します。RADIUS サーバに到達しないと、認証エラーとなります。認証フェイルオーバが有効な場合には、RADIUS サーバ認証には到達せずローカルデータベースが認証のために使用されます。初期値ではステータスは無効です。

パラメータ

パラメータ	説明
[enable | disable]	プロトコル認証フェイルオーバを有効または無効にします。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

MAC アドレス認証の認証フェイルオーバを設定します。

```
DGS-3200-10:4#config mac_based_access_control aut_failover enable
Command: config mac_based_access_control aut_failover enable

Success.

DGS-3200-10:4#
```

config mac_based_access_control guest_vlan

目的

MAC アドレス認証のゲスト VLAN メンバシップを設定します。

構文

config mac_based_access_control guest_vlan ports <portlist>

説明

指定ポートをゲスト VLAN モードに設定します。ポートリストに含まれないポートは、ゲスト VLAN ではないモードになります。ゲスト VLAN モードの操作に関する詳細情報については、MAC ベースのアクセスコントロールポートコマンドの設定に関する説明を参照してください。

パラメータ

パラメータ	説明
ports <portlist>	ゲスト VLAN がポートに設定されると、ポートは RADIUS サーバから割り当てられた VLAN に基づいて VLAN の割り当てをします。ゲスト VLAN が設定されないと、ポートは VLAN の割り当てをしません。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

ポート 1-8 に MAC アドレス認証のゲスト VLAN メンバシップを設定します。

```
DGS-3200-10:4#config mac_based_access_control guest_vlan ports 1-8
Command: config mac_based_access_control guest_vlan ports 1-8

Success.

DGS-3200-10:4#
```

config mac_based_access_control ports

目的

MAC アドレス認証にパラメータを設定します。

MAC-AC 機能がポートに対して有効であり、このポートへのゲスト VLAN 機能は無効である場合、このポートに割り付けられているユーザのトラフィックは、認証を通過しない限り転送されません。認証を通過しないユーザは、スイッチによりサービスを提供されません。ユーザが認証を通過すると、ユーザは元の VLAN 設定のもとで操作されたトラフィックを転送することができます。MAC-AC 機能がポートに対して有効であり、このポートへのゲスト VLAN 機能が有効である場合、ポートは認証処理を開始する前に元の VLAN メンバから移動し、ゲスト VLAN のメンバポートになります。認証後に有効な VLAN が RADIUS サーバによって割り当てられると、このポートは、次に、ゲスト VLAN から削除されて、割り当てられた VLAN のメンバポートになります。

ゲスト VLAN モードには考慮すべき 2 つの状態があります。
- デバイスがポートベース VLAN クラシフィケーションだけをサポートしていると、ポートが認証 VLAN に移動した場合、続くユーザは再度認証されません。それらは現在の認証 VLAN で動作します。
- デバイスが、MAC ベース VLAN クラシフィケーションをサポートしていると、各ユーザは、個別に認証されて、自身の VLAN を持つことができます。

ゲスト VLAN モードのために、MAC アドレスが認証されているが、VLAN 情報が全く RADIUS サーバから割り当てられないか、または RADIUS サーバによって割り当てられた VLAN が無効である場合 (例えば、割り当てられた VLAN は存在しない)、このポート /MAC はゲスト VLAN のメンバポートから削除されて、元の VLAN のメンバポートになります。

構文

config mac_based_access_control ports [<portlist> | all] {state [enable | disable] | mode [port_based | host_based] | aging_time [infinite | <min 1-1440>] | hold_time [infinite | <sec 1-300>] }

説明

スイッチの MAC アドレス認証機能にパラメータを設定します。

パラメータ

パラメータ	説明
ports [<portlist> | all]	MAC アドレス認証機能を有効または無効にするポート範囲を設定します。
state [enable | disable]	MAC AC 機能を有効または無効にします。
mode [port_based | host_based]	ポートベースまたはホストベースのいずれかを指定します。 • port_based - ポートに接続するすべてのユーザがはじめの認証結果を共有することを意味します。 • host_based - 各ユーザがそれ自身の認証結果を持つことができることを意味します。 スイッチが MAC ベースの VLAN をサポートしていないと、スイッチは、ゲスト VLAN モードであるポートに host_based オプションを許可しません。
aging_time [infinite | <min 1-1440>]	認証ホストが認証状態を保つ時間。aging_time がタイムアウトになると、ホストは未認証状態に戻ります。
hold_time [infinite | <sec 1-300>]	ホストが認証通過に失敗した場合に認証を開始できない時間。ユーザがエントリ状態を手動でクリアしない限り、次の認証はこの時間内に開始しません。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

ポート 1-8 のポートステータスを有効にします。

```
DGS-3200-10:4#config mac_based_access_control ports 1-8 state enable
Command: config mac_based_access_control ports 1-8 state enable

Success.

DGS-3200-10:4#
```

create mac_based_access_control guest_vlan

目的

MAC アドレス認証のためにゲスト VLAN を作成します。

構文

create mac_based_access_control [guest_vlan <vlan_name 32> | guest_vlanid <1-4094>]

説明

MAC アドレス認証のためにゲスト VLAN を作成します。

パラメータ

パラメータ	説明
guest_vlan <vlan_name 32>	MAC アドレスが認証されると、ポートはこの VLAN に割り当てられます。
guest_vlanid <1-4094>	MAC アドレスが認証されると、ポートはこの VLAN ID に割り当てられます。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

MAC アドレス認証のためにゲスト VLAN を作成します。

```
DGS-3200-10:4#create mac_based_access_control guest_vlanid 2
Command: create mac_based_access_control guest_vlanid 2

Success.

DGS-3200-10:4#
```

delete mac_based_access_control guest_vlan

目的

ゲスト VLAN の割り当てを解除します。

構文

delete mac_based_access_control [guest_vlan <vlan_name 32> | guest_vlanid <1-4094>]

説明

ゲスト VLAN の割り当てを解除します。ゲスト VLAN が割り当てを解除されると、ゲスト VLAN 機能は無効になります。

パラメータ

パラメータ	説明
guest_vlan <vlan_name 32>	指定した VLAN 名を持つデータベースを削除します。
guest_vlanid <1-4094>	指定した VLAN ID を持つデータベースを削除します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

ゲスト VLAN の割り当てを解除します。

```
DGS-3200-10:4#delete mac_based_access_control guest_vlan Guest_VLAN
Command: config mac_based_access_control guest_vlan Guest_VLAN

Success.

DGS-3200-10:4#
```

clear mac_based_access_control auth_mac

目的

ユーザの現在の認証状態をリセットします。再認証は、再度ユーザトラフィックの受信した後に開始します。

構文

clear mac_based_access_control auth_mac [ports [all | portlist] | mac_addr <macaddr>]

説明

ユーザまたはポートの認証状態をクリアします。ポートまたはユーザは未認証状態に戻ります。ポートまたはユーザに関連しているすべてのタイマがリセットされます。

パラメータ

パラメータ	説明
ports [all | portlist]	MAC を削除するポート範囲を指定します。「all」を指定するとすべてのポートを削除します。
mac_addr <macaddr>	この MAC アドレスを持つホストを削除します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

MAC アドレス認証により処理した MAC をクリアします。

```
DGS-3200-10:4#clear mac_based_access_control auth_mac ports all
Command: clear mac_based_access_control_ports auth_mac ports all

Success.

DGS-3200-10:4#
```

create mac_based_access_control_local

目的

ローカルデータベースエントリを作成します。

構文

create mac_based_access_control_local mac <macaddr> {[vlan < vlan_name 32> | vlanid <1-4094>]}

説明

ローカルデータベースエントリを作成します。

パラメータ

パラメータ	説明
mac<macaddr>	ローカルモードでアクセスが許可される MAC アドレス。
vlan < vlan_name 32> | vlanid <1-4094>	MAC アドレスが認証されると、ポートはこの VLAN または VLAN ID に割り当てられます。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

ローカルデータベースエントリを作成します。

```
DGS-3200-10:4#create mac_based_access_control_local mac 00-00-00-00-00-01 vlan default
Command: create mac_based_access_control_local mac 00-00-00-00-00-01 vlan default

Success.

DGS-3200-10:4#
```

config mac_based_access_control_local

目的

ローカルデータベースエントリを設定します。

構文

config mac_based_access_control_local mac <macaddr> [vlan <vlan_name 32> | vlanid <1-4094> | clear_vlan]

説明

データベースエントリを編集します。

パラメータ

パラメータ	説明
mac <macaddr>	ローカルモードでアクセスが許可される MAC アドレス。
vlan < vlan_name 32> | vlanid <1-4094> | clear_vlan	• vlan - MAC アドレスが認証されると、ポートはこの VLAN に割り当てられます。 • vlanid - MAC アドレスが認証されると、ポートはこの VLAN ID に割り当てられます。 • clear_vlan - 指定 VLAN をクリアするために選択します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

MAC アドレス認証のローカルデータベースエントリを設定します。

```
DGS-3200-10:4#config mac_based_access_control_local mac 00-00-00-00-00-01 vlan default
Command: config mac_based_access_control_local mac 00-00-00-00-00-01 vlan default

Success.

DGS-3200-10:4#
```

delete mac_based_access_control_local

目的

ローカルデータベースエントリを削除します。

構文

delete mac_based_access_control_local [mac <macaddr> | vlan <vlan_name 32> | vlanid <1-4094>]

説明

ローカルデータベースエントリを削除します。

パラメータ

パラメータ	説明
mac <macaddr>	この MAC アドレスでデータベースを削除します。
vlan < vlan_name 32>	この VLAN 名でデータベースを削除します。
vlanid <1-4094>	この VLAN ID でデータベースを削除します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

MAC アドレスで MAC アドレス認証のローカルデータベースエントリを削除します。

```
DGS-3200-10:4#delete mac_based_access_control_local mac 00-00-00-00-00-01
Command: delete mac_based_access_control_local mac 00-00-00-00-00-01

Success.

DGS-3200-10:4#
```

VLAN で MAC アドレス認証のローカルデータベースエントリを削除します。

```
DGS-3200-10:4#delete mac_based_access_control_local vlan default
Command: delete mac_based_access_control_local vlan default

Success.

DGS-3200-10:4#
```

show mac_based_access_control

目的

MAC アドレス認証設定を表示します。

構文

show mac_based_access_control {ports [<portlist> | all]}

説明

MAC アドレス認証設定を表示します。

パラメータ

パラメータ	説明
ports <portlist> | all	参照するポート。「all」はすべてのポートを表示します。

制限事項

なし。

使用例

MAC アドレス認証設定を表示します。

```
DGS-3200-10:4#show mac_based_access_control
Command: show mac_based_access_control

MAC Based Access Control
-----------------------------------
State                    : Disabled
Trap                     : Enabled
Method                   : Local
Authentication Failover  : Disabled
Password                 : default
Guest VLAN               :
Guest VLAN VID           :
Guest VLAN Member Ports  :

DGS-3200-10:4#
```

ポート 1-4 の MAC アドレス認証設定を表示します。

```
DGS-3200-10:4#show mac_based_access_control ports 1-4
Command: show mac_based_access_control ports 1-4

Port   State    Aging Time Hold Time Auth Mode
                (mins)     (secs)
------ -------- ---------- --------- -----------
1      Disabled 100        100       Port_based
2      Disabled 100        200       Host_based
3      Disabled 50         300       Port_based
4      Disabled 200        100       Host_based

DGS-3200-10:4#
```

show mac_based_access_control auth_mac

目的

MAC アドレス認証における認証 MAC アドレスを表示します。

構文

show mac_based_access_control auth_mac {ports <portlist>}

説明

ポートまたはすべてのポート上の MAC アドレス認証の認証を表示します。

パラメータ

パラメータ	説明
ports <portlist>	参照するポート。

制限事項

なし。

使用例

MAC アドレス認証における認証 MAC アドレスを参照します。

```
DGS-3200-10:4#show mac_based_access_control auth_mac
Command: show mac_based_access_control auth_mac

Port Number : 1
Index  MAC Address         Auth State      VLAN Name    VID
-----  -----------------   --------------  -----------  -----------
1      00-00-01-02-03-A2   Authenticating  vlan0        100
2      00-03-09-18-10-01   Authenticating  vlan0        100
3      00-05-5D-ED-84-EA   Authenticating  vlan0        100
4      00-0D-0B-4E-A0-F7   Authenticating  vlan0        100
5      00-0D-60-8F-49-38   Authenticating  vlan0        100
6      00-0E-A6-8E-C1-B7   Authenticating  vlan0        100
7      00-10-4B-69-F4-AD   Authenticating  vlan0        100
8      00-11-D8-DA-CE-0B   Authenticating  vlan0        100
```

show mac_based_access_control_local

目的

MAC アドレス認証のローカルデータベースを表示します。

構文

show mac_based_access_control_local {[mac<macaddr> | vlan <vlan_name 32> | vlanid <1-4094>]}

説明

MAC アドレス認証のローカルデータベースを表示します。

パラメータ

パラメータ	説明
mac <macaddr>	指定 MAC アドレスによる MAC アドレス認証のローカルデータベースを表示します。
vlan <vlan_name 32>	VLAN ごとに MAC アドレス認証のローカルデータベースエントリを表示します。
vlanid <1-4094>	VLAN ID ごとに MAC アドレス認証のローカルデータベースエントリを表示します。

制限事項

なし。

使用例

MAC アドレス認証のローカルデータベースを表示します。

```
DGS-3200-10:4#show mac_based_access_control_local
Command: show mac_based_access_control_local

MAC Address         VLAN Name             VID
-----------------   -------------------   -------------
00-00-00-00-00-01   default                1
00-00-00-00-00-02   123                   10
00-00-00-00-00-03   123                   10
00-00-00-00-00-04   default                1

Total Entries:4

DGS-3200-10:4#
```

MAC アドレスごとに MAC アドレス認証のローカルデータベースエントリを参照します。

```
DGS-3200-10:4#show mac_based_access_control_local mac 00-00-00-00-00-01
Command: show mac_based_access_control_local mac 00-00-00-00-00-01

MAC Address         VLAN Name          VID
-----------------   ----------------   ----------------
00-00-00-00-00-01   default            1

Total Entries:1

DGS-3200-10:4#
```

VLAN ごとに MAC アドレス認証のローカルデータベースエントリを参照します。

```
DGS-3200-10:4#show mac_based_access_control_local vlan default
Command: show mac_based_access_control_local vlan default

MAC Address         VLAN Name          VID
-----------------   ----------------   ----------------
00-00-00-00-00-01   default            1
00-00-00-00-00-04   default            1

Total Entries:2

DGS-3200-10:4#
```

config mac_based_access_control trap

目的

トラップ状態を設定します。

構文

config mac_based_access_control trap [enable | disable]

説明

トラップコントロールのグローバル状態を設定します。

パラメータ

パラメータ	説明
trap [enable | disable]	トラップの状態を有効または無効にします。 • enable - 送信される MBA トラップを許可します。 • disable - 送信される MBA トラップを許可しません。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

トラップコントロールのグローバル状態を設定します。

```
DGS-3200-10:4#config mac_based_access_control trap enable
Command: config mac_based_access_control trap enable

Success.

DGS-3200-10:4#
```

第 49 章　JWAC コマンド

JWAC は、スイッチの拡張 Web ベースのアクセスコントロールです。JWAC と Web 認証が相互に排他的な機能であり、それらを同時に使用することができませんのでご注意ください。

JWAC 機能を利用して、①ユーザ ID の Web ブラウザでの認証、②検疫サーバとの連携による PC 検疫を実行することができます。（連携可能な検疫サーバに関しては、本製品のデータシートをご参照ください。）

①の Web 認証では、1 ポートに複数ユーザを接続した状態で Web 認証が可能となり、MAC based VLAN と併用することで、RADIUS サーバから動的に VLAN-ID を割り当てることが可能となります。
②の検疫では、ユーザは 2 つの認証ステップを通過する必要があります。最初のステップは、検疫サーバで検疫を行い、2 番目のステップでユーザ認証が行われます。

RADIUS サーバは、802.1X コマンドセットによって定義されたサーバ設定を共有します。

注意　WAC/JWAC 認証では、System インタフェースが Up している必要があります。

コマンドラインインタフェース（CLI）における JWAC コマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
enable jwac	
disable jwac	
enable jwac redirect	
disable jwac redirect	
enable jwac forcible_logout	
disable jwac forcible_logout	
enable jwac udp_filtering	
disable jwac udp_filtering	
enable jwac quarantine_server_monitor	
disable jwac quarantine_server_monitor	
config jwac quarantine_server_error_timeout	<sec 5-300>
config jwac redirect	{destination [quarantine_server | jwac_login_page] | delay_time <value 0-10>}
config jwac virtual_ip	<ipaddr>
config jwac quarantine_server_url	<string 128>
config jwac clear_quarantine_server_url	
config jwac update_server	[add | delete] ipaddress <network_address>
config jwac switch_http_port	<tcp_port_number 1-65535>{[http | https]}
config jwac ports	[<portlist>| all] {state [enable | disable] | mode [host_based | port_based] | max_authenticating_host <value 0-10> | aging_time [infinite | <min 1-1440>] | idle_time [infinite | <min 1-1440>] | block_time [<sec 0-300>]}
config jwac radius_protocol	[local | pap | chap | ms_chap | ms_chapv2 | eap_md5]
create jwac user	<username 15> {vlan <vlanid 1-4094>}
config jwac user	<username 15> {vlan <vlanid 1-4094>}
delete jwac	[user <username 16> | all_users]
show jwac user	
delete jwac host	[ports [all | <portlist>] {authenticated | authenticating | blocked} | <macaddr>]
show jwac	
show jwac host	{ports [all | <portlist>]} {authenticated | authenticating | blocked}
show jwac ports	[all | <portlist>]
config jwac authenticate_page	[japanese | english]
config jwac page_element	[japanese | english] [default | {page_title <mutiword 128> | login_window_title <mutiword 32> | user_name <mutiword 16> | password <mutiword 16> | logout_window_title <mutiword 32>}]
show jwac customize_page element	
config jwac auth_failover	[enable | disable]

以下のセクションで各コマンドについて詳しく記述します。

enable/disable jwac

目的

JWAC 機能を有効または無効にします。

構文

enable jwac

disable jwac

説明

JWAC 機能を使用して、ユーザは 2 段階の認証を通過する必要があります。最初のステップは、検疫サーバで検疫を行い、2 番目のステップでユーザ認証が行われます。2 番目のステップは、ホストが認証を通過した後にポートの VLAN メンバシップ変更がないという点を除き、WAC に似ています。RADIUS サーバは、802.1X コマンドセットによって定義されたサーバ設定を共有します。JWAC と Web 認証は相互に排他的な機能であり、それらを同時に使用することができませんのでご注意ください。

「enable jwac」を実行する前に、「config jwac virtual_ip」でバーチャル IP アドレスを設定してください。

パラメータ

なし。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

WAC 機能を有効にします。

```
DGS-3200-10:4#enable jwac
Command: enable jwac

Success.

DGS-3200-10:4#
```

WAC 機能を無効にします。

```
DGS-3200-10:4#disable jwac
Command: disable jwac

Success.

DGS-3200-10:4#
```

enable/disable jwac redirect

目的

JWAC リダイレクト機能を有効または無効にします。

構文

enable jwac redirect

disable jwac redirect

説明

リダイレクト検疫サーバが有効な場合、ランダムな URL にアクセスしようとすると、未認証ホストは検疫サーバにリダイレクトされます。リダイレクト先に JWAC Login Page を指定した場合、未認証ホストは、スイッチの JWAC Login Page にリダイレクトされます。

リダイレクトが無効な場合、未認証ユーザは検疫サーバへのアクセスと未認証ホストからの JWAC Login Page だけが許可され、他のすべての Web アクセスは拒否されます。

パラメータ

なし。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。Quarantine Server（検疫サーバ）へのリダイレクトを有効にする場合、はじめに検疫サーバを設定する必要があります。

使用例

JWAC リダイレクト機能を有効にします。

```
DGS-3200-10:4#enable jwac redirect
Command: enable jwac redirect

Success.

DGS-3200-10:4#
```

JWAC リダイレクト機能を無効にします。

```
DGS-3200-10:4#disable jwac redirect
Command: disable jwac redirect

Success.

DGS-3200-10:4#
```

enable/disable jwac forcible_logout

目的

JWAC の強制ログアウト機能を有効または無効にします。

構文

enable jwac forcible_logout

disable jwac forcible_logout

説明

JWAC Forcible Logout 機能が有効の場合、認証ホストから JWAC スイッチに TTL=1 を持つ ping パケットはログアウトリクエストと見なされ、ホストは未認証状態に戻ります。

パラメータ

なし。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

JWAC の強制ログアウト機能を有効にします。

```
DGS-3200-10:4#enable jwac forcible_logout
Command: enable jwac forcible_logout

Success.

DGS-3200-10:4#
```

JWAC の強制ログアウト機能を無効にします。

```
DGS-3200-10:4#disable jwac forcible_logout
Command: disable jwac forcible_logout

Success.

DGS-3200-10:4#
```

enable/disable jwac udp_filtering

目的

JWAC UDP フィルタリング機能を有効または無効にします。

構文

enable jwac udp_filtering

disable jwac udp_filtering

説明

JWAC UDP フィルタリング機能を有効にすると、DHCP と DNS を除く未認証ホストからの UDP と ICMP パケットは破棄されます。

パラメータ

なし。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

JWAC UDP フィルタリング機能を有効にします。

```
DGS-3200-10:4#enable jwac udp_filtering
Command: enable jwac udp_filtering

Success.

DGS-3200-10:4#
```

JWAC UDP フィルタリング機能を無効にします。

```
DGS-3200-10:4#disable jwac udp_filtering
Command: disable jwac udp_filtering

Success.

DGS-3200-10:4#
```

enable/disable jwac quarantine_server_monitor

目的

JWAC Quarantine Server モニタを有効または無効にします。

構文

enable jwac quarantine_server_monitor
disable jwac quarantine_server_monitor

説明

JWAC Quarantine Server モニタを有効または無効にします。JWAC Quarantine Server モニタ機能が有効な場合、JWAC スイッチは、サーバが問題ないことを保証するためにQuarantine Serverをモニタします。スイッチがQuarantine Serverを検出しないと、リダイレクトが有効で、「Redirect Destination」が「Quarantine Server」に設定されている場合、強制的にJWAC Login Pageに未認証のすべてのHTTPアクセスをリダイレクトします。

パラメータ

なし。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

JWAC Quarantine Server モニタを有効にします。

```
DGS-3200-10:4#enable jwac quarantine_server_monitor
Command: enable jwac quarantine_server_monitor

Success.

DGS-3200-10:4#
```

JWAC Quarantine Server モニタを無効にします。

```
DGS-3200-10:4#disable jwac quarantine_server_monitor
Command: disable jwac quarantine_server_monitor

Success.

DGS-3200-10:4#
```

config jwac quarantine_server_error_timeout

目的

Quarantine Server のエラータイムアウトを設定します。

構文

config jwac quarantine_server_error_timeout <sec 5-300>

説明

Quarantine Server のエラータイムアウトを設定します。
Quarantine Server モニタが有効な場合、JWAC スイッチは、定期的に検疫が問題なく動作するかどうかをチェックします。スイッチが設定された時間に Quarantine Server から応答を受信しないと、スイッチは適切に動作していないと見なします。

パラメータ

パラメータ	説明
<sec 5-300>	エラータイムアウト間隔を指定します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

Quarantine Server のエラータイムアウトを設定します。

```
DGS-3200-10:4#config jwac quarantine_server_error_timeout 60
Command: config jwac quarantine_server_error_timeout 60

Success.

DGS-3200-10:4#
```

config jwac redirect

目的

リダイレクト先の設定および未認証ホストが Quarantine Server または JWAC Login Page にリダイレクトされる場合の遅延時間を指定します。

構文

config jwac redirect {destination [quarantine_server | jwac_login_page] | delay_time <value 0-10>}

説明

リダイレクト先の設定および未認証ホストが Quarantine Server または JWAC Login Page にリダイレクトされる場合の遅延時間を指定します。遅延時間の単位は秒です。0 はリダイレクトの遅延がないことを示します。

パラメータ

パラメータ	説明
destination [quarantine_server | jwac_login_page]	未認証ホストがリダイレクト Quarantine Server または JWAC Login Page のいずれかにリダイレクトされるかを指定します。
delay_time <value 0-10>	未認証ホストがリダイレクトされる場合の遅延時間を指定します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

リダイレクト先の設定および未認証ホストが Quarantine Server または JWAC Login Page にリダイレクトされる場合の遅延時間を指定します。

```
DGS-3200-10:4#config jwac redirect destination jwac_login_page delay_time 5
Command: config jwac redirect destination jwac_login_page delay_time 5

Success.

DGS-3200-10:4#
```

config jwac virtual_ip

目的

未認証ホストから認証リクエストを受け入れるために使用する JWAC バーチャル IP アドレスを指定します。

構文

config jwac virtual_ip <ipaddr>

説明

未認証ホストから認証リクエストを受け入れるために使用する JWAC バーチャル IP アドレスを指定します。この IP に送信されたリクエストだけが正しい応答を取得します。

この IP は、ARP リクエストまたは ICMP パケットには応答しません。

パラメータ

パラメータ	説明
<ipaddr>	バーチャル IP の IP アドレスを指定します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

未認証ホストから認証リクエストを受け入れるために JWAC バーチャル IP アドレスに 1.1.1.1 を指定します。

```
DGS-3200-10:4#config jwac virtual_ip 1.1.1.1
Command: config jwac virtual_ip 1.1.1.1

Success.

DGS-3200-10:4#
```

config jwac quarantine_server_url

目的

JWAC Quarantine サーバの URL を指定します。

構文

config jwac quarantine_server_url <string 128>

説明

JWAC Quarantine サーバの URL を指定します。リダイレクトが有効で、未認証ホストが HTTP リクエストパケットをランダムな Web サーバに送信する場合、「Redirect Destination」が「Quarantine Server」であると、スイッチは、この HTTP パケットを処理し、設定された URL を持つ Quarantine Server へのアクセスを許可するためにホストにメッセージを送り返します。コンピュータが指定 URL に接続している場合、Quarantine Server は、ユーザ名とパスワードの入力し、認証を行います。

パラメータ

パラメータ	説明
<string 128>	JWAC Quarantine サーバの URL を指定します

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

JWAC Quarantine サーバの URL を指定します。

```
DGS-3200-10:4#config jwac quarantine_server_url http://10.90.90.88/authpage.html
Command: config jwac quarantine_server_url http://10.90.90.88/authpage.html

Success.

DGS-3200-10:4#
```

config jwac clear_quarantine_server_url

目的

Quarantine Server 設定をクリアします。

構文

config jwac clear_quarantine_server_url

説明

Quarantine Server 設定をクリアします。

パラメータ

なし。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。JWAC が有効でリダイレクトの宛先が Quarantine Server である場合、Quarantine Server をクリアすることはできません。

使用例

Quarantine Server 設定をクリアします。

```
DGS-3200-10:4#config jwac clear_quarantine_server_url
Command: config jwac clear_quarantine_server_url

Success.

DGS-3200-10:4#
```

config jwac update_server

目的

JWAC 認証を完了するために、PC が接続するサーバを設定します。

構文

config jwac update_server [add | delete] ipaddress <network_address>

説明

未認証クライアントホストからのトラフィックが JWAC スイッチによってブロックされないサーバのネットワークアドレスを追加または削除することができます。クライアントが認証を通過する前にアクティブ X が認証を完了するようにアクセスする必要があるすべてのサーバは、その IP アドレスを持つスイッチに追加されるべきです。例えば、クライアントは update.microsoft.com またはアンチウィルスソフトウェアの会社にアクセスし、クライアントの OS やアンチウィルスソフトウェアが最新であるかどうかをチェックする必要があります。そのため、update.microsoft.com およびアンチウィルスソフトウェアの会社の IP アドレスをスイッチに追加する必要があります。

パラメータ

パラメータ	説明
[add | delete]	• add - トラフィックがブロックされないネットワークアドレスを追加します。5 つまでのネットワークアドレスを追加することができます。 • delete - トラフィックがブロックされないネットワークアドレスを削除します。
ipaddress <network_address>	追加または削除するネットワークアドレスを指定します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

JWAC 認証を完了するために PC が接続する必要があるサーバを設定します。

```
DGS-3200-10:4#config jwac update_server add ipaddress 10.90.90.109/24
Command: config jwac update_server add ipaddress 10.90.90.109/24

 Warning:the real added update server is 10.90.90.0/24

Success.

DGS-3200-10:4#
```

config jwac switch_http_port

目的

JWAC スイッチがリッスンする TCP ポートを指定します。

構文

config jwac switch_http_port <tcp_port_number 1-65535>{[http | https]}

説明

JWAC スイッチがリッスンする TCP ポートを指定します。このポートは認証プロセスの 2 つ目のステップで使用されます。PC ユーザはスイッチのページに接続し、ユーザ名とパスワードを入力します。指定しないと、ポート番号の初期値は 80 となります。プロトコルを指定しないと、HTTP になります。

パラメータ

パラメータ	説明
<tcp_port_number 1-65535>	JWAC スイッチがリッスンし、認証プロセスを終了するために使用する TCP ポート。
[http | https]	• http - JWAC はこの TCP ポート上に HTTP を動作させます。 • https - JWAC はこの TCP ポート上に HTTPS を動作させます。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。HTTP ポートは TCP ポート 443 で動作し、HTTPS は TCP ポート 80 で動作することはできません。

使用例

JWAC スイッチがリッスンする TCP ポートを指定します。

```
DGS-3200-10:4#config jwac switch_http_port 8888 http
Command: config jwac switch_http_port 8888 http

Success.

DGS-3200-10:4#
```

config jwac ports

目的

JWAC のポートステータスを設定します。

構文

config jwac port [<portlist> | all] {state [enable | disable] | mode [host_based | port_based] | max_authenticating_host <value 0-10> | aging_time [infinite | <min 1-1440>] | idle_time [infinite | <min 1-1440>] | block_time [<sec 0-300>]}

説明

JWAC のポートステータスを設定します。max_authenticating_host の初期値は 10 です。aging_time の初期値は 1440（分）です。idle_time の初期値は infinite です。block_time の初期値は 0（秒）です。

パラメータ

パラメータ	説明
<portlist> | all	JWAC ステータスを設定するポート範囲。「all」を指定すると、すべてのスイッチポートの JWAC ステータスが設定されます。
state [enable | disable]	JWAC のポートステータスを指定します。
mode [host_based | port_based]	「host_based」または「port_based」を指定します。
max_authenticating_host <value 0-10>	同時に各ポートに許可されるホストの認証処理の試みの最大数を指定します。
aging_time [infinite | <min 1-1440>]	認証ホストが認証状態を保つ時間を指定します。「infinite」を指定すると、認証ホストはポートにエージングを行いません。
idle_time [infinite | <min 1-1440>]	本設定時間にトラフィックがない場合、ホストは未認証状態に戻ります。「infinite」を指定すると、ポート上の認証ホストのアイドル状態がチェックされません。
block_time [<sec 0-300>]	認証を通過することに失敗した場合にホストがブロックされる時間を指定します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

JWAC のポートステータスを設定します。

```
DGS-3200-10:4#config jwac port 1-9 state enable
Command: config jwac port 1-9 state enable

Success.

DGS-3200-10:4#
```

config jwac radius_protocol

目的

JWAC によって使用される RADIUS プロトコルを設定します。

構文

config jwac radius_protocol [local | pap | chap | ms_chap | ms_chapv2 | eap_md5]

説明

JWAC に使用される RADIUS プロトコルを指定し、RADIUS 認証を完了します。

パラメータ

パラメータ	説明
local	JWAC スイッチは、ローカルユーザデータベースを使用して認証を完了します。
pap	JWAC スイッチは、ローカルユーザデータベースを使用して認証を完了します。
chap	JWAC スイッチは、CHAP を使用して RADIUS サーバと通信します。
ms_chap	JWAC スイッチは、MS-CHAP を使用して RADIUS サーバと通信します。
ms_chapv2	JWAC スイッチは、MS-CHAPv2 を使用して RADIUS サーバと通信します。
eap_md5	JWAC スイッチは、EAP MD5 を使用して RADIUS サーバと通信します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。JWAC は 802.1X とともに他の RADIUS 設定を共有します。このコマンドを使用して RADIUS プロトコルを設定する場合、追加される RADIUS サーバがそのプロトコルをサポートしていることを確認する必要があります。

使用例

JWAC に使用される RADIUS プロトコルを指定し、RADIUS 認証を完了します。

```
DGS-3200-10:4#config jwac radius_protocol ms_chapv2
Command: config jwac radius_protocol ms_chapv2

Success.

DGS-3200-10:4#
```

create jwac user

目的

ローカルデータベースに JWAC ユーザを作成します。

構文

create jwac user <username 15> {vlan <vlanid 1-4094>}

説明

ローカルデータベースに JWAC ユーザを作成します。JWAC RADIUS プロトコルの設定時に「local」を選択すると、ローカルデータベースが使用されます。

パラメータ

パラメータ	説明
<username 15>	作成するユーザ名。
<vlanid 1-4094>	認証を通過するためにこのユーザアカウントを使用する認証ホストのターゲット VLAN ID。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

ローカルデータベースに JWAC ユーザを作成します。

```
DGS-3200-10:4#create jwac user 112233
Command: create jwac user 112233

Enter a case-sensitive new password:***
Enter the new password again for confirmation:***

Success.

DGS-3200-10:4#
```

config jwac user

目的

ローカルデータベースに JWAC ユーザを作成します。

構文

config jwac user <username 15> {vlan <vlanid 1-4094>}

説明

ローカルデータベースの JWAC ユーザを更新します。JWAC RADIUS プロトコルの設定時に「local」を選択すると、ローカルデータベースが使用されます。

パラメータ

パラメータ	説明
<username 15>	作成するユーザ名。
<vlanid 1-4094>	認証を通過するために、このユーザアカウントを使用する認証ホストのターゲット VLAN ID。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

ローカルデータベースに JWAC ユーザを作成します。

```
DGS-3200-10:4#config jwac user 112233 vlan vlan2
Command: config jwac user 112233 vlan vlan2

Enter a old password ******
Enter a case-sensitive new password:***
Enter the new password again for confirmation:***
Success.

DGS-3200-10:4#
```

delete jwac user

目的

ローカルデータベースの JWAC ユーザを削除します。

構文

delete jwac [user <username 15> | all_users]

説明

ローカルデータベースの JWAC ユーザを削除します。

パラメータ

パラメータ	説明
<username 15>	削除するユーザ名。
all_users	ローカルデータベース内のすべてのユーザアカウントが削除されます。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

ローカルデータベースから JWAC ユーザを削除します。

```
DGS-3200-10:4#delete jwac user 112233
Command: delete jwac user 112233

Success.

DGS-3200-10:4#
```

show jwac user

目的

ローカルデータベースの JWAC ユーザを参照します。

構文

show jwac user

説明

ローカルデータベースの JWAC ユーザを参照します。

パラメータ

なし。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

ローカルデータベースの JWAC ユーザを参照します。

```
DGS-3200-10:4#show jwac user
Command: show jwac user

 Current Accounts:
 Username     Target VID  Password
 -----------  ----------  ----------------
   1              -         1

Total Entries:1

DGS-3200-10:4#
```

delete jwac host

目的

JWAC が有効なポート上のホストを削除します。

構文

delete jwac host [ports [all | <portlist>] {authenticated | authenticating | blocked} | <macaddr>]

説明

JWAC ホストを削除します。

パラメータ

パラメータ	説明
ports [all | <portlist>]	ホストを削除するポート範囲を指定します。
authenticated | authenticating | blocked	削除するホストのステータスを指定します。authenticated（認証済み）、authenticating（認証中）または blocked（ブロック済み）。
<macaddr>	この MAC アドレスを持つホストを削除します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

認証ステータスが「blocked」のホストを削除します。

```
DGS-3200-10:4#delete jwac host ports all blocked
Command: delete jwac host ports all blocked

Success.

DGS-3200-10:4#
```

show jwac

目的

JWAC 設定を表示します。

構文

show jwac

説明

JWAC 設定を表示します。

パラメータ

なし。

制限事項

なし。

使用例

JWAC 設定を表示します。

```
DGS-3200-10:4#show jwac
Command: show jwac

 State                : Enabled
 Enabled Ports        : 1,9
 Virtual IP           : 1.1.1.1
 Switch HTTP Port     : 21212 (HTTP)
 UDP Filtering        : Enabled
 Forcible Logout      : Enabled
 Redirect State       : Enabled
 Redirect Delay Time  : 3 Seconds
 Redirect Destination : Quarantine Server
 Quarantine Server    : http://172.18.212.147/pcinventory
 Q-Server Monitor     : Enabled (Running)
 Q-Srv Error Timeout  : 5 Seconds
 RADIUS Auth-Protocol : PAP
 Update Server        : 172.18.202.1/32
                        172.18.202.0/24
                        10.1.1.0/24

DGS-3200-10:4#
```

show jwac host

目的

JWAC クライアントホスト情報を表示します。

構文

show jwac host {ports [all | <portlist>]} {authenticated | authenticating | blocked}

説明

JWAC クライアントホスト情報を表示します。

パラメータ

パラメータ	説明
ports [all | <portlist>]	クライアントホストの情報を表示するポート範囲。
authenticated | authenticating | blocked	• authenticated - 認証済みクライアントホストだけを表示します。 • authenticating - 認証処理中のクライアントホストだけを表示します。 • blocked - 認証エラーのために一時的にブロックされているクライアントホストだけを表示します。

制限事項

なし。

使用例

JWAC クライアントホスト情報を表示します。

```
DGS-3200-10:4#show jwac host ports 3
Command: show jwac host ports 3

                                Remaining
Hosts                Port VID  AgeTime/IdleTime   Authentication State
                               or BlockingTime
-----------------    ---- ---  ----------------   --------------------
00-00-00-00-00-01    3    5    98   Min/Infinite  Authenticated
00-00-00-00-00-02    3    99   Infinite/Infinite  Authenticating
00-00-00-00-00-03    2    44       30 Sec         Blocked

Total Authenticating Hosts :1
Total Authenticated Hosts  :1
Total Blocked Hosts        :1

DGS-3200-10:4#
```

show jwac ports

目的

JWAC のポート設定を表示します。

構文

show jwac ports [all | <portlist>]

説明

JWAC のポート設定を表示します。

パラメータ

パラメータ	説明
ports [all | <portlist>]	JWAC 設定を表示するポート範囲を指定します。「all」を指定すると、JWAC の全ポートの設定を表示します。

制限事項

なし。

使用例

JWAC 設定を表示します。

```
DGS-3200-10:4#show jwac ports 1-4
Command: show jwac ports 1-4

Port  State          Max          Aging Time Idle Time Block Time
               Authenticating  (Minutes)  (Minutes) (Seconds)
                    Host
----- -------- --------------- ---------- --------- ----------
1     Enabled       10          Infinite   20        10
2     Disabled      50          60         10        2
3     Enabled       50          1440       Infinite 2
4     Enabled       0           600        30        5

DGS-3200-10:4#
```

config jwac authenticate_page

目的

JWAC 認証ページをカスタマイズします。

構文

config jwac authenticate_page [japanese | english]

説明

JWAC 認証ページをカスタマイズします。

パラメータ

パラメータ	説明
japanese | english	• japanese - 日本語のページに変更します。 • english - 英語のページに変更します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

認証ページをカスタマイズします。

```
DGS-3200-10:4#config jwac authenticate_page japanese
Command: config jwac authenticate_page japanese

Success.

DGS-3200-10:4#
```

config jwac page_element

目的

JWAC 認証ページをカスタマイズします。

構文

config jwac page_element [japanese | english] [default | {page_title <mutiword 128> | login_window_title <mutiword 32> | user_name <mutiword 16> | password <mutiword 16> | logout_window_title <mutiword 32>}]

説明

JWAC 認証ページをカスタマイズします。

パラメータ

パラメータ	説明
japanese | english	• japanese - 日本語のページに変更します。 • english - 英語のページに変更します。
default	ページエレメントを初期値にリセットします。
page_title<mutiword 128>	認証ページのタイトル。
login_window_title<mutiword 32>	認証ページのログイン画面のタイトル。
user_name <mutiword 16>	認証ページのユーザ名のタイトル。
password <mutiword 16>	認証ページのパスワードのタイトル。
logout_window_title <mutiword 32>	認証ページのログアウト画面のタイトル。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

認証ページをカスタマイズします。

```
DGS-3200-10:4#config jwac page_element japanese page_title " ディーリンクジャパン株
式会社 " login_window_title "JWAC 画面 " user_name " ユーザ名 " password " パスワード "
logout_window_title " ログアウト "
Command: config jwac page_element japanese page_title " ディーリンクジャパン株式
会社 " login_window_title "JWAC 画面 " user_name " ユーザ名 " password " パスワード "
logout_window_title " ログアウト "

Success.

DGS-3200-10:4#
```

show jwac customize_page element

目的

カスタマイズした認証ページのエレメントを参照します。

構文

show jwac customize_page element

説明

カスタマイズした認証ページのエレメントを参照します。

パラメータ

なし。

制限事項

なし。

使用例

認証ページの初期値を表示します。

```
DGS-3200-10:4#show jwac customize_page element
Command: show jwac customize_page element

Current Page :English
Customization page element mapping
-------------------------------------
English page mapping:

Page title mapping to            :D-Link Corp.
Login window title mapping to    :Authentication Login
User name mapping to             :User Name
Password mapping to              :Password
Login out window title mapping to:Logout from the network

Japanese page mapping:

Page title mapping to            :
Login window title mapping to    : 社内 LAN 認証ログイン
User name mapping to             : ユーザ ID
Password mapping to              : パスワード
Login out window title mapping to: 社内 LAN 認証ログアウト

DGS-3200-10:4#
```

config jwac auth_failover

目的

JWAC 認証フェイルオーバを設定します。

構文

config jwac auth_failover [enable | disable]

説明

JWAC 認証フェイルオーバを設定します。RADIUS サーバに到達しないと認証エラーとなります。また、認証フェイルオーバが有効な場合には、RADIUS サーバ認証には到達せずローカルデータベースが認証のために使用されます。初期値ではステータスは無効です。

パラメータ

パラメータ	説明
enable | disable	• enable - プロトコル認証フェイルオーバを有効にします。 • disable - プロトコル認証フェイルオーバを無効にします。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

JWAC 認証フェイルオーバを設定します。

```
DGS-3200-10:4#config jwac auth_failover enable
Command: config jwac auth_failover enable

Success.

DGS-3200-10:4#
```

第 50 章　マルチプル認証コマンド

本スイッチは、802.1X、MAC ベースアクセスコントロール（MBAC）、Web ベースアクセスコントロール（WAC）、JWAC、および IP-MAC- ポートバインディング（IMPB）を含むマルチプル認証方式をサポートしています。マルチプル認証機能では、異なる認証方式を実行している複数のクライアントが同じスイッチポートを使用してネットワークに接続することができます。

コマンドラインインタフェース（CLI）におけるマルチプル認証コマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
create authentication guest_vlan	[vlan <vlan_name 32> | vlanid <vlanid 1-4094>]
delete authentication guest_vlan	[vlan <vlan_name 32> | vlanid <vlanid 1-4094>]
config authentication guest_vlan	[vlan <vlan_name 32> | vlanid <vlanid 1-4094>] [add | delete] ports [<portlist> | all]
config authentication ports	[<portlist> | all] {auth_mode [port_based | host_based] | multi_authen_methods [none | any | dot1x_impb | impb_jwac | impb_wac]}
show authentication guest_vlan	
show authentication ports	{<portlist>}
enable authorization network	
disable authorization network	
show authorization	

以下のセクションで各コマンドについて詳しく記述します。

create authentication guest_vlan

目的

スタティック VLAN をゲスト VLAN として設定します。

構文

create authentication guest_vlan [vlan <vlan_name 32> | vlanid <vlanid 1-4094>]

説明

スタティック VLAN をゲスト VLAN として設定します。ゲスト VLAN になるように割り当てられる VLAN をあらかじめ作成する必要があります。ゲスト VLAN になるように割り当てられた VLAN を削除することはできません。本コマンドの詳しい説明については、「config authentication guest_vlan ports」を参照してください。

パラメータ

パラメータ	説明
vlan <vlan_name 32>	VLAN 名によりゲスト VLAN を指定します。
vlanid <vlanid 1-4094>	VLAN ID によりゲスト VLAN を指定します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

スタティック VLAN をゲスト VLAN として設定します。

```
DGS-3200-10:4#create authentication guest_vlan vlan guestVLAN
Command: create authentication guest_vlan vlan guestVLAN

Success.

DGS-3200-10:4#
```

delete authentication guest_vlan

目的

ゲスト VLAN を削除します。

構文

delete authentication guest_vlan [vlan <vlan_name 32> | vlanid <vlanid 1-4094>]

説明

ゲスト VLAN 設定を削除します。スタティック VLAN は削除されません。ゲスト VLAN を削除後、ゲスト VLAN として有効であったすべてのポートはオリジナルの VLAN に移行します。本コマンドの詳しい説明については、「config authentication guest_vlan ports」を参照してください。

パラメータ

パラメータ	説明
vlan <vlan_name 32>	VLAN ID によりゲスト VLAN を指定します。
vlanid <vlanid 1-4094>	ゲスト VLAN を削除します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

ゲスト VLAN 設定を削除します。

```
DGS-3200-10:4#delete authentication guest_vlan vlan guestVLAN
Command: delete authentication guest_vlan vlan guestVLAN

Success.

DGS-3200-10:4#
```

config authentication guest_vlan ports

目的

セキュリティポートを指定のゲスト VLAN メンバとして設定します。

構文

config authentication guest_vlan [vlan <vlan_name 32> | vlanid <vlanid 1-4094>] [add | delete] ports [<portlist> | all]

説明

ゲスト VLAN へのポートの割り当ておよびポートの削除を行います。

パラメータ

パラメータ	説明
vlan <vlan_name 32> | vlanid <vlanid 1-4094>	• vlan_name - ゲスト VLAN として指定の VLAN 名を割り当てます。 • vlanid - ゲスト VLAN として指定の VLAN ID を割り当てます。 VLAN は既存のスタティック VLAN である必要があります。
add | delete	• add - ゲスト VLAN にポートリストを追加します。 • delete - ゲスト VLAN からポートリストを削除します。
<portlist> | all	構成するポートを指定します。「all」を指定すると全ポートが対象となります。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

ゲスト VLAN「gv」に対してすべてのポートに認証設定をします。

```
DGS-3200-10:4#config authentication guest_vlan vlan gv add ports all
Command: config authentication guest_vlan vlan gv add ports all

Success.

DGS-3200-10:4#
```

config authentication ports

目的

セキュリティポートを設定します。

構文

config authentication ports [<portlist> | all] {auth_mode [port_based | host_based] | multi_authen_methods [none | any | dot1x_impb | impb_jwac | impb_wac]}

説明

ポートに認証モードおよび認証方式を設定します。

パラメータ

パラメータ	説明
<portlist> | all	設定するポートを指定します。
auth_mode [port_based | host_based]	• port-based - 割り当てされているホストの一つが認証を通過すると、同じポート上のすべてのホストがネットワークへアクセスを許可されます。ユーザが認証に失敗すると、このポートは次の認証の試みを継続します。 • host-based - すべてのユーザが個別に認証されます。
multi_authen_methods [none | any | dot1x_impb | impb_jwac | impb_wac]	マルチプル認証の方式を指定します。 • none - マルチプル認証を無効にします。 • any - 認証方式（802.1X、MBAC、および JWAC/WAC）のいずれかを通過すれば、認証となります。 • dot1x_impb - Dot1x が最初に検証され、次に IMPB が検証されます。両方の認証が通過のために必要です。 • impb_jwac - IMPB が最初に検証され、JWAC が検証されます。両方の認証が通過のために必要です。 • impb_wac - IMPB が最初に検証され、次に WAC が検証されます。両方の認証が通過のために必要です。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

全ポートの認証モードをホストベースに設定します。

```
DGS-3200-10:4#config authentication ports all auth_mode host_based
Command: config authentication ports all auth_mode host_based

Success.

DGS-3200-10:4#
```

全ポートのマルチプル認証モードを「any」に設定します。

```
DGS-3200-10:4#config authentication ports all multi_authen_methods any
Command: config authentication ports all multi_authen_methods any

Success.

DGS-3200-10:4#
```

show authentication guest_vlan

目的
　ゲスト VLAN 設定を参照します。
構文
　show authentication guest_vlan
説明
　ゲスト VLAN 情報を表示します。
パラメータ
　なし。
制限事項
　なし。
使用例
　ゲスト VLAN 情報を表示します。

```
DGS-3200-10:4#show authentication guest_vlan
Command: show authentication guest_vlan

Guest VLAN VID         : 10
Guest VLAN Member Ports: 1-10

DGS-3200-10:4#
```

show authentication ports

目的
　ポートの認証設定を表示します。
構文
　show authentication ports {<portlist>}
説明
　ポートの認証方式および認証モード設定を表示します。
パラメータ

パラメータ	説明
<portlist>	指定したポートのマルチプル認証設定を表示します。

制限事項
　管理者レベルユーザのみ本コマンドを実行できます。
使用例
　すべてのポートの認証設定を表示します。

```
DGS-3200-10:4#show authentication ports
Command: show authentication ports

Port Methods         Authorized Mode
---- --------------- -------------------
1    None            Host_based
2    Any             Host_based
3    802.1X_IMPB     Host_based
4    None            Host_based
5    None            Host_based
6    IMPB_JWAC       Host_based
7    None            Host_based
8    None            Host_based
9    802.1X_IMPB     Host_based
10   None            Host_based

DGS-3200-10:4#
```

enable authorization

目的

許可を有効にします。

構文

enable authorization network

説明

ネットワークにおける許可を有効にします。ネットワークにおける許可を有効にすると、RADUIS サーバに割り当てられる許可データを受け取り、有効となります。初期値ではネットワークへの許可は有効です。

パラメータ

なし。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

ネットワークにおける許可を有効にします。

```
DGS-3200-10:4#enable authorization network
Command: enable authorization network

Success.

DGS-3200-10:4#
```

disable authorization

目的

許可を無効にします。

構文

disable authorization network

説明

ネットワークにおける許可を無効にします。初期値ではネットワークへの許可は有効です。

パラメータ

なし。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

ネットワークにおける許可を無効にします。

```
DGS-3200-10:4#disable authorization network
Command: disable authorization network

Success.

DGS-3200-10:4#
```

show authorization

目的

許可の状態を表示します。

構文

show authorization

説明

許可状の態を表示します。

パラメータ

なし。

制限事項

なし。

使用例

許可の状態を表示します。

```
DGS-3200-10:4#show authorization
Command: show authorization

Authorization for Network: Enabled

DGS-3200-10:4#
```

第 51 章　フィルタコマンド

不正な DHCP サーバへの接続を拒否する DHCP サーバスクリーニング機能をサポートしています。DHCP サーバフィルタ機能が有効の場合、指定されたポートからのすべての DHCP サーバパケットはフィルタリングされます。本機能では、ユーザはすべての DHCP サーバパケットを制限できるだけでなく、指定したどの DHCP クライアントからの DHCP サーバパケットも受信することが可能になります。

コマンドラインインタフェース（CLI）におけるフィルタコマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
config filter dhcp_server	[add permit server_ip <ipaddr> {client_mac <macaddr>} ports [<portlist> | all] | delete permit server_ip <ipaddr> {client_mac <macaddr>} ports [<portlist> | all] | ports [<portlist> | all] state [enable | disable]]
config filter dhcp_server trap_log	[enable | disable]
config filter dhcp_server illegal_server_log_suppress_duration	[1min | 5min | 30min]
show filter dhcp_server	

以下のセクションで各コマンドについて詳しく記述します。

config filter dhcp_server

目的

DHCP サーバパケットのフィルタリング機能を設定します。また、DHCP サーバまたはクライアントバインディングエントリの追加または削除をします。

構文

config filter dhcp_server [add permit server_ip <ipaddr> {client_mac <macaddr>} ports [<portlist> | all] | delete permit server_ip <ipaddr> {client_mac <macaddr>} ports [<portlist> | all] | ports [<portlist> | all] state [enable | disable]]

説明

本コマンドには、次の 2 つの目的があります。

- 指定ポートにおける全 DHCP サーバパケットのフィルタ。
- 定義済みのサーバの IP アドレスおよびクライアントの MAC アドレスを持つ DHCP サーバのパケットの許可。

本機能により DHCP サーバを制限して特定の DHCP クライアントにサービスを提供することができます。一方がプライベート IP アドレスを提供し、もう一方がパブリック IP アドレスを提供するという 2 つの DHCP サーバがネットワークに存在している場合に便利です。フィルタを有効にすると、1 つのアクセスプロファイルが作成され、1 ポートあたり 1 つのアクセスルール (UDP ポート =67) が作成されます。このファイルにおけるフィルタコマンドは同じアクセスプロファイルを共有します。

パラメータ

パラメータ	説明
add permit server_ip <ipaddr>	フィルタする DHCP サーバの IP アドレスを追加します。
client_mac <macaddr>	DHCP クライアントの MAC アドレス。
ports [<portlist> | all]	DHCP サーバのポート番号。
delete permit server_ip <ipaddr>	フィルタから除外する DHCP サーバの IP アドレスを削除します。
state [enable | disable]	DHCP サーバ機能を「Enable」(有効) または「Disable」(無効) にします。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

スイッチのデータベースにある DHCP サーバ / クライアントフィルタリストからエントリを追加または削除します。

```
DGS-3200-10:4#config filter dhcp_server add permit server ip 10.1.1.1 client_
mac 00-00-00-00-00-01 ports 1-10
Command: config filter dhcp_server add permit server_ip 10.1.1.1 client_mac 00-
00-00-00-00-01 ports 1-10

Success.

DGS-3200-10:4#
```

DHCP サーバのフィルタ機能を設定します。

```
DGS-3200-10:4#config filter dhcp_server ports 1-10 state enable
Command: config filter dhcp_server ports 1-10 state enable

Success.

DGS-3200-10:4#
```

config filter dhcp_server trap_log

目的

DHCP サーバフィルタに関連するトラップまたはログを有効または無効にします。

構文

config filter dhcp_server trap_log [enable | disable]

説明

DHCP サー名フィルタに関連するトラップまたはログを有効または無効にします。

パラメータ

パラメータ	説明
[enable | disable]	DHCP サーバフィルタイベントに対するログおよびトラップを有効または無効にします。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

DHCP サーバフィルタイベントに対するログおよびトラップを無効にします。

```
DGS-3200-10:4#config filter dhcp_server trap_log disable
Command: config filter dhcp_server trap_log disable

Success.

DGS-3200-10:4#
```

config filter dhcp_server illegal_server_log_suppress_duration

目的

不正なサーバログの抑止時間を設定します。

構文

config filter dhcp_server illegal_server_log_suppress_duration [1min | 5min | 30min]

説明

不正な DHCP パケットを送り続けている DHCP サーバのログ取得を抑止します。検出された同じ不正な DHCP サーバの IP アドレスをログ取得を停止する未許可期間にトラップ送信先に一度だけ送信します。

パラメータ

パラメータ	説明
1min | 5min | 30min	ログ / トラップを抑止する時間を指定します。1、5 または 30（分）。初期値は 5（分）です。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

不正なサーバログの抑止時間を設定します。

```
DGS-3200-10:4#config filter dhcp_server illegal_server_log_suppress_duration
30min
Command: config filter dhcp_server illegal_server_log_suppress_duration 30min

Success.

DGS-3200-10:4#
```

show filter dhcp_server

目的

スイッチに作成した DHCP サーバ / クライアントフィルタリストを表示します。

構文

show filter dhcp_server

説明

スイッチに作成した DHCP サーバ / クライアントフィルタリストを表示します。

パラメータ

なし。

制限事項

なし。

使用例

スイッチに作成した DHCP サーバ / クライアントフィルタリストを表示します。

```
DGS-3200-10:4#show filter dhcp_server
Command: show filter dhcp_server

Filter DHCP Server Trap_Log State    : Disabled
Enabled Ports                        :
Illegal Server Log Suppress Duration : 5 minutes

Filter DHCP Server/Client Table
Server IP Address Client MAC address  Port
----------------- ------------------- ---------------
10.1.1.1          00-00-00-00-00-01   1-10

Total Entries: 1

DGS-3200-10:4#
```

第 52 章　ARP Spoofing 防御コマンド

以下のセキュリティ機能を使用して、スイッチにアクセスしようとするハッカーや権限のない第三者による ARP Spoofing を防御します。

コマンドラインインタフェース（CLI）における ARP Spoofing 防御コマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
config arp_spoofing_prevention	[add gateway_ip <ipaddr> gateway_mac <macaddr> ports [<portlist> | all] | delete gateway_ip <ipaddr>]
show arp_spoofing_prevention	

以下のセクションで各コマンドについて詳しく記述します。

config arp_spoofing_prevention

目的

ARP Spoofing 攻撃の防御を設定します。

構文

config arp_spoofing_prevention [add gateway_ip <ipaddr> gateway_mac <macaddr> ports [<portlist> | all] | delete gateway_ip <ipaddr>]

説明

ARP Spoofing 攻撃の防御を設定します。

パラメータ

パラメータ	説明
add gateway_ip <ipaddr>	追加するゲートウェイ IP を指定します。
gateway_mac <macaddr>	設定するポート範囲を指定します。
ports [<portlist> | all]	• <portlist> - 設定するポート範囲を指定します。 • all - すべてのポートを設定します。
delete gateway_ip <ipaddr>	削除するゲートウェイ IP を指定します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

ARP Spoofing 攻撃の防御を設定します。

```
DGS-3200-10:4#config arp_spoofing_prevention add gateway_ip 10.254.254.254
gateway_mac 00-00-00-11-11-11 ports 1-2
Command: config arp_spoofing_prevention add gateway_ip 10.254.254.254 gateway_mac
00-00-00-11-11-11 ports 1-2

Success.

DGS-3200-10:4#
```

show arp_spoofing_prevention

目的

ARP Spoofing 防御エントリを表示します。

構文

show arp_spoofing_prevention

説明

ARP Spoofing 防御エントリを表示します。

パラメータ

なし。

制限事項

なし。

使用例

ARP Spoofing 防御エントリを表示します。

```
DGS-3200-10:4#show arp_spoofing_prevention
Command: show arp_spoofing_prevention

ARP Spoofing Prevention Table
Gateway IP Address  Gateway MAC Address   Port
------------------  --------------------  ----------------------
10.254.254.254      00-00-00-11-11-11     1-2

Total Entries: 1

DGS-3200-10:4#
```

第 53 章　CPU フィルタコマンド

チップセットの制限やスイッチのセキュリティの必要性などから、本スイッチは、CPU インタフェースフィルタリング機能を持っています。この追加機能によって CPU インタフェース向けのパケットアクセスルールリストの作成が可能になり、動作時のセキュリティが高くなります。

コマンドラインインタフェース（CLI）における CPU フィルタコマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
config cpu_filter l3_control_pkt	<portlist> [{dvmrp | pim | igmp_query | ospf | rip | vrrp} | all] state [enable | disable]
show cpu_filter l3_control_pkt	{<portlist>}

以下のセクションで各コマンドについて詳しく記述します。

config cpu_filter l3_control_pkt

目的

指定ポートから CPU に送信される L3 コントロールパケットを破棄します。

構文

config cpu_filter l3_control_pkt <portlist> [{dvmrp | pim | igmp_query | ospf | rip | vrrp} | all] state [enable | disable]

説明

指定ポートから CPU に送信される L3 コントロールパケットを破棄します。

パラメータ

パラメータ	説明
<portlist>	コントロールパケットをフィルタするポートリストを指定します。
[{dvmrp | pim | igmp_query | ospf | rip | vrrp} | all]	フィルタするプロトコルを指定します。「all」を指定すると、すべての L3 コントロールパケットをフィルタします。
state [enable | disable]	フィルタリング機能を「enable」（有効）または「disable」（無効）にします。初期値では無効に設定されています。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

ポート 1-10 の DVMRP と OSPF をフィルタします。

```
DGS-3200-10:4#config filter l3_control_pkt 1-10 dvmrp ospf state enable
Command: config filter filter l3_control_pkt 1-10 dvmrp ospf state enable

Success.

DGS-3200-10:4#
```

show cpu_filter l3_control_pkt

目的

L3 コントロールパケットのフィルタ設定を表示します。

構文

show cpu_filter l3_control_pkt {<portlist>}

説明

L3 コントロールパケットのフィルタ設定を表示します。

パラメータ

パラメータ	説明
<portlist>	コントロールパケットのフィルタ設定を表示するポートリストを指定します。

制限事項

なし。

使用例

ポート 1-2 のフィルタ設定を表示します。

```
DGS-3200-10:4#show cpu_filter l3_control_pkt 1-2
Command: show cpu_filter l3_control_pkt 1-2

Port IGMP-Query DVMRP   PIM     OSPF    RIP     VRRP
---- ---------- ------- ------- ------- ------- -------
1    Disable    Disable Disable Disable Disable Disable
2    Disable    Disable Disable Disable Disable Disable

DGS-3200-10:4#
```

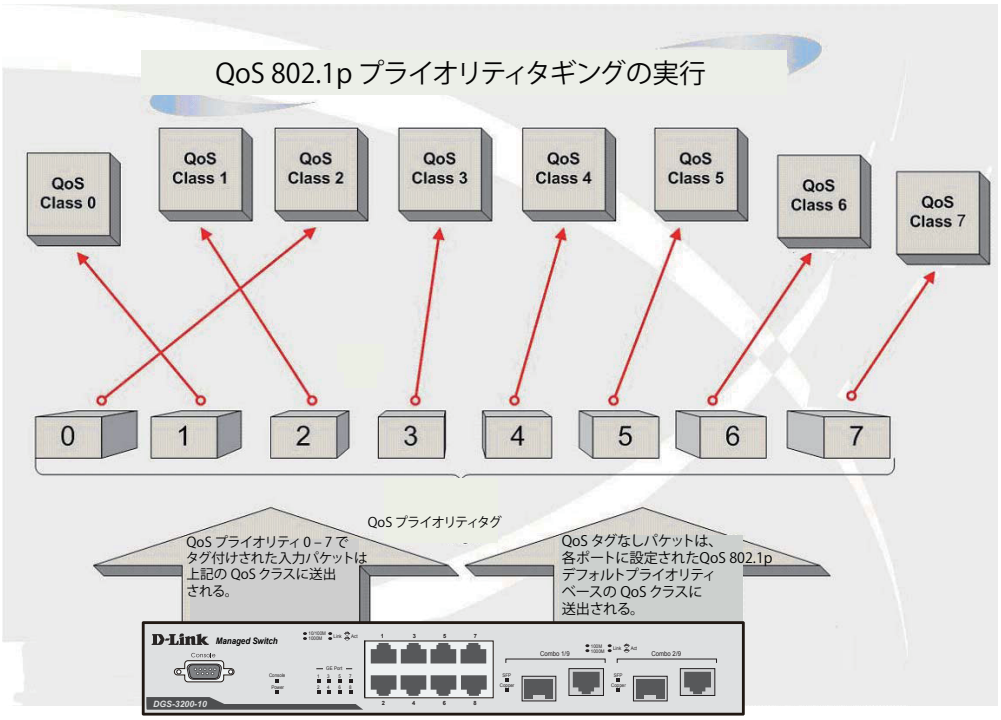
第 54 章　QoS コマンド

本シリーズは、802.1p キューイング QoS（Quality of Service）をサポートしています。QoS メニューを使用し、本スイッチにセキュリティ機能を設定することができます。
本スイッチは TACACS、セキュリティ IP、SSL、SSH、SNMP などの機能をサポートしています。

次に QoS の機能と、802.1p プライオリティキューイングを利用するメリットについて説明します。

QoS の長所

QoS は IEEE 802.1p 標準で規定される技術で、ネットワーク管理者に、VoIP（Voice-over Internet Protocol）、Web 閲覧用アプリケーション、ファイルサーバアプリケーション、またはビデオ会議などの広帯域を必要とする、または高い優先順位を持つ重要なサービスのために、帯域を予約する方法を提供します。より大きい帯域を作成可能なだけではなく他の重要度の低いトラフィックを制限することで、ネットワークが必要以上の帯域を使用しないようにします。スイッチは各物理ポートで受信した様々なアプリケーションからのパケットをプライオリティに基づき独立したハードウェアキューに振り分けます。
以下の図に、802.1p プライオリティキューイングがどのように本スイッチに実装されているかを示しています。



スイッチ上での QoS マッピングの例

上の図は本スイッチのプライオリティの初期設定です。クラス 7 はスイッチ上の 7 つのプライオリティキューのなかで、最も高い優先権を持っています。QoS を実行するためには、ユーザはスイッチに対し、パケットのヘッダに適切な識別タグが含まれているかを確認するように指示する必要があります。そして、ユーザはそれらのタグ付きパケットをスイッチ上の指定されたキューに送り、優先順序に従って送出するようにします。

例えば、遠隔地に設置した 2 台のコンピュータ間でビデオ会議を行うとします。管理者は Access Profile コマンドを使用して、送信するビデオパケットにプライオリティタグを付加します。次に受信側ではスイッチにそのタグの確認するよう指示を行い、タグ付きパケットを受信したら、それをスイッチのクラスキューに関連付けを行うようにします。また、管理者はこのキューに優先順位を与え、他のパケットが送出されるよりも前に送信されるように設定を行います。この結果、このサービス用のパケットは、できるだけ早く送信され、キューが最優先されることにより、中断されることなくパケットを受け取ることができるため、このビデオ会議用に帯域を最適化することが可能になります。

QoS について

本スイッチは、802.1p プライオリティキューをサポートしており、8 個のプライオリティキューがあります。プライオリティキューには、最高レベルの 7 番キューから最低レベルの 0 番キューまでがあります。IEEE 802.1p（p0 から p7）に規定される 8 つのプライオリティタグはスイッチのプライオリティタグと以下のように関連付けされます。

- プライオリティ 0 は、スイッチの Q2 キューに割り当てられます。
- プライオリティ 1 は、スイッチの Q0 キューに割り当てられます。
- プライオリティ 2 は、スイッチの Q1 キューに割り当てられます。
- プライオリティ 3 は、スイッチの Q3 キューに割り当てられます。
- プライオリティ 4 は、スイッチの Q4 キューに割り当てられます。
- プライオリティ 5 は、スイッチの Q5 キューに割り当てられます。
- プライオリティ 6 は、スイッチの Q6 キューに割り当てられます。
- プライオリティ 7 は、スイッチの Q7 キューに割り当てられます。

Strict（絶対優先）のプライオリティベースのスケジューリングでは、優先度の高いキューに属するパケットから送信されます。優先度の高いキューが複数ある場合は、プライオリティタグに従って送信されます。高プライオリティのキューが空である時にだけプライオリティの低いパケットは送信されます。

重み付けラウンドロビンキューイングでは、各プライオリティキューから送信されるパケットの数は、指定された重み付けによって決定されます。A から H までの 8 つある CoS（Class of Service）キューに、8 から 1 までの重み付けを設定したとすると、パケットは以下の順に送信されます。A1, B1, C1, D1, E1, F1, G1, H1, A2, B2, C2, D2, E2, F2, G2, A3, B3, C3, D3, E3, F3, A4, B4, C4, D4, E4, A5, B5, C5, D5, A6, B6, C6, A7, B7, A8, A1, B1, C1, D1, E1, F1, G1, H1
重み付けラウンドロビンキューイングでは、各 CoS キューが同じ重み付けを持つならば、各 CoS キューのパケット送信の機会はラウンドロビンキューイングのように、全く同じになります。また、ある CoS の重み付けとして 0 を設定すると、その CoS から送信するパケットがなくなるまでパケットを処理します。0 以外の値を持つ他の CoS キューでは、重み付けラウンドロビンの規則により、重みに従って送信を行います。

本スイッチは、スイッチ上の各ポートに 7 つのプライオリティキュー（と 7 つの CoS）を持っています。

注意 本スイッチは内部的にはポートに対して 8 つのサービスクラスを持っています。そのうちひとつは最初からスイッチが使用するように予約されていて変更できません。以下のサービスクラスに関する説明はすべて管理者が使用および変更できる 7 つのサービスクラスについて行っています。

コマンドラインインタフェース（CLI）における QoS コマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
config bandwidth_control	[<portlist> | all] {rx_rate [no_limit | <value 64-1024000>] | tx_rate [no_limit | <value 64-1024000>]}
show bandwidth_control	{<portlist>}
config scheduling	<class_id 0-7> max_packet <value 0-255>
config scheduling_mechanism	[strict | weight_fair]
show scheduling	
show scheduling_mechanism	
config 802.1p user_priority	<priority 0-7> <class_id 0-7>
show 802.1p user_priority	
config 802.1p default_priority	[<portlist> | all] <priority 0-7>
show 802.1p default_priority	{<portlist>}

以下のセクションで各コマンドについて詳しく記述します。

config bandwidth_control

目的
　ポートベースで帯域幅制御を設定します。
構文
　config bandwidth_control [<portlist> | all] {rx_rate [no_limit | <value 64-1024000>] | tx_rate [no_limit | <value 64-1024000>]}
説明
　ポートベースで帯域幅制御を設定します。
パラメータ

パラメータ	説明
all | <portlist>	表示するポートまたは範囲を指定します。「all」はすべてのポートを指定します。
rx_rate	以下のパラメータは、上で指定したポートにおいてパケットの受信が可能な速度を指定します。 • no_limit - 指定ポートが受信するパケットの速度を制限しません。 • <value 64-1024000> - 受信パケットの制限値（Kbps）を指定します。指定した帯域幅の制限値と等しいのは可能ですが、超えることはできません。この正確な論理的制限値またはトークン値によってハードウェアが決定されます。トークン値は常にプロジェクトに使用されるチップに対して帯域インクリメントの倍数となります（すなわち、32Kbit、64Kbit、128Kbit など）。帯域幅制限値を整数で入力する場合、CPU によって認識される実際の制限値であるこのトークン値が表示されます。 **注意** 1 Kbit = 1000 bit、1 Gigabit = 1000*1000 Kbit
tx_rate	以下のパラメータは、上で指定したポートにおいてパケットの送信が可能な速度を指定します。 • no_limit - 指定ポートが送信するパケットの速度を制限しません。 • <value 64-1024000> - 送信パケットの制限値（Kbps）を指定します。指定した帯域幅の制限値と等しいのは可能ですが、超えることはできません。この正確な論理的制限値またはトークン値によってハードウェアが決定されます。トークン値は常にプロジェクトに使用されるチップに対して帯域インクリメントの倍数となります（すなわち、32Kbit、64Kbit、128Kbit など）。帯域幅制限値を整数で入力する場合、CPU によって認識される実際の制限値であるこのトークン値が表示されます。 **注意** 1 Kbit = 1000 bit、1 Gigabit = 1000*1000 Kbit

制限事項
　管理者レベルユーザのみ本コマンドを実行できます。

使用例

帯域幅制御を設定します。

```
DGS-3200-10:4#config bandwidth_control 1-10 tx_rate 1024
Command: config bandwidth_control 1-10 tx_rate 1024

Success.

DGS-3200-10:4#
```

応答メッセージ

1. 「Success.」
   64 の倍数を入力し、設定が成功した場合に表示されます。

2. 「Fail !Trunk member port（ポート番号）can not be configured because the master is not contained in the portlist.」
   設定ポートリストにマスタポートではなくトランクポートが含まれます。

3. 「Success, The setting value is not a multiple of 64, closest value %d is chosen.」
   64 の倍数でない数値を入力した場合に表示されます。そうでないと、帯域インクリメントはチップに使用されます。トークン値は有効な制限になります。トークン値は、指定した制限値を超えないで、チップに使用される帯域インクリメントの倍数に最も近い値が設定されます。（すなわち、32Kbit、64Kbit、128Kbit など）。例えば、制限値に 130 を入力すると、トークン値は 128 になります。

show bandwidth_control

目的

帯域幅制御テーブルを表示します。

構文

show bandwidth_control {<portlist>}

説明

スイッチの現在の帯域幅制御設定をポートベースで表示します。

パラメータ

パラメータ	説明
<portlist>	表示するポートまたは範囲を指定します。パラメータが指定されないと、システムはすべてのポート帯域設定を表示します。

制限事項

なし。

使用例

帯域幅制御設定を表示します。

```
DGS-3200-10:4#show bandwidth_control 1-10
Command: show bandwidth_control 1-10

Bandwidth Control Table

Port    RX Rate      TX_Rate     Effective RX   Effective TX
       (kbit/sec)   (kbit/sec)   (kbit/sec)     (kbit/sec)
----   ----------   ----------   ------------   ------------
1       1024         1024         1024           1024
2       1024         1024         1024           1024
3       1024         1024         1024           1024
4       1024         1024         1024           1024
5       1024         1024         1024           1024
6       no_limit     no_limit     no_limit       no_limit
7       no_limit     no_limit     no_limit       no_limit
8       no_limit     no_limit     no_limit       no_limit
9       no_limit     no_limit     no_limit       no_limit
10      no_limit     no_limit     no_limit       no_limit

DGS-3200-10:4#
```

config scheduling

目的

weight_fair メカニズムに指定されるクラスのパケットの割合を設定します。

構文

config scheduling <class_id 0-7> max_packet <value 0-255>

説明

weight_fair メカニズムに指定されるクラスのパケットの割合を設定します。スイッチには (n+1) 個のハードウェアプライオリティキューがあります。これらの (n+1) 個のキューの 1 つに入力パケットをマップする必要があります。優先順位が次のキューからパケット送信を行う前に送信を許可される各ハードウェアプライオリティキューのパケットの最大数を設定します。

パラメータ

パラメータ	説明
<class_id 0-7>	8 つのハードウェアプライオリティキューのどれに適用されるかを指定します。8 つのハードウェアプライオリティキューは、最も低い優先度である 0 キューを持つ 0 から 7 の番号によって識別されます。
max_packet <value 0-255>	優先順位が次のキューがパケット送信を行う前に送信される、上で指定したハードウェアプライオリティキューのパケットの最大数を指定します。0 から 255 の間の値を指定します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

各 CoS キューにトラフィックスケジューリングメカニズムを設定します。

```
DGS-3200-10:4#config scheduling 0 max_packet 34
Command: config scheduling 0 max_packet 34

Success.

DGS-3200-10:4#
```

config scheduling_mechanism

目的

CoS 機能にスケジューリングメカニズムを設定します。

構文

config scheduling_mechanism [strict | weight_fair]

説明

プライオリティキューでスイッチがパケットを処理する方法を指定します。

パラメータ

パラメータ	説明
strict	上位の CoS キューからトラフィックを処理します。上位キューの送信が完了するまで下位キューからはパケットは送信されません。
weight_fair	プライオリティ CoS で送信されたパケットを重み付けされたラウンドロビン（WRR）アルゴリズムによって処理します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

各 CoS キューにトラフィック・スケジューリングメカニズムを設定します。

```
DGS-3200-10:4#config scheduling_mechanism strict
Command: config scheduling_mechanism strict

Success.

DGS-3200-10:4#
```

show scheduling

目的

スイッチに設定されている現在のトラフィックスケジューリングを表示します。

構文

show scheduling

説明

スイッチに使用中の現在のトラフィックスケジューリングを表示します。

パラメータ

なし。

制限事項

なし。

使用例

各 CoS キューの現在のトラフィックスケジューリングメカニズムを表示します。

```
DGS-3200-10:4#show scheduling
Command: show scheduling

QOS Output Scheduling

Class ID  MAX. Packets
--------  ------------
Class-0   1
Class-1   2
Class-2   3
Class-3   4
Class-4   5
Class-5   6
Class-6   7
Class-7   8

DGS-3200-10:4#
```

show scheduling_mechanism

目的

スイッチで使用中の現在のトラフィックスケジューリングメカニズムを表示します。

構文

show scheduling_mechanism

説明

スイッチで使用中の現在のトラフィックスケジューリングメカニズムを表示します。

パラメータ

なし。

制限事項

なし。

使用例

スケジューリングメカニズムを表示します。

```
DGS-3200-10:4#show scheduling_mechanism
Command: show scheduling_mechanism

QOS Scheduling_mechanism
Class ID  Mechanism
--------  ------------
Class-0   Strict
Class-1   Strict
Class-2   Strict
Class-3   Strict
Class-4   Strict
Class-5   Strict
Class-6   Strict
Class-7   strict

DGS-3200-10:4#
```

config 802.1p user_priority

目的

スイッチで利用可能な 8 つのハードウェアキューの 1 つに入力パケットの 802.1p ユーザプライオリティをマップします。

構文

config 802.1p user_priority <priority 0-7> <class_id 0-7>

説明

スイッチで利用可能な 8 つのハードウェアキューの 1 つに入力パケットの 802.1p ユーザプライオリティに基づいて入力パケットをマップする方法を設定します。スイッチの初期値では、続いて到来する 802.1p ユーザプライオリティ値を 8 つのハードウェアプライオリティキューにマップします。

パラメータ

パラメータ	説明
<priority 0-7>	<class_id 0-6>（ハードウェアキューの番号）に連携させる 802.1p ユーザプライオリティ。
<class_id 0-7>	スイッチのハードウェアプライオリティキューの番号。本スイッチには、8 個のプライオリティキューがあります。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

スイッチに 802.1 ユーザプライオリティを設定します。

```
DGS-3200-10:4#config 802.1p user_priority 1 3
Command: config 802.1p user_priority 1 3

Success.

DGS-3200-10:4#
```

show 802.1p user_priority

目的

入力パケットの 802.1p ユーザプライオリティ値とスイッチの 7 つのハードウェアプライオリティキューとの現在のマッピングを表示します。

構文

show 802.1p user_priority

説明

入力パケットの 802.1p ユーザプライオリティ値とスイッチの 7 つのハードウェアプライオリティキューとの現在のマッピングを表示します。

パラメータ

なし。

制限事項

なし。

使用例

802.1p ユーザプライオリティを表示します。

```
DGS-3200-10:4#show 802.1p user_priority
Command: show 802.1p user_priority

QOS Class of Traffic

Priority-0  ->  <Class-2>
Priority-1  ->  <Class-0>
Priority-2  ->  <Class-1>
Priority-3  ->  <Class-3>
Priority-4  ->  <Class-4>
Priority-5  ->  <Class-5>
Priority-6  ->  <Class-6>
Priority-7  ->  <Class-7>

DGS-3200-10:4#
```

config 802.1p default_priority

目的

スイッチの 802.1p デフォルトプライオリティ設定を指定します。タグなしパケットをスイッチが受信すると、本コマンドで設定したプライオリティは、パケットのプライオリティフィールドに記載されます。

構文

config 802.1p default_priority [<portlist> | all] <priority 0-7>

説明

スイッチが受信したタグなしパケットのデフォルトプライオリティ処理に関する指定をします。本コマンドで入力されたプライオリティ値は、パケットが 7 つのハードウェアプライオリティキューのうちのどれに送信されるかを決定するために使用されます。

パラメータ

パラメータ	説明
<portlist> | all	デフォルトプライオリティが設定されるポート範囲を指定します。「all」はスイッチのすべてのポートに適用します。
<priority 0-7>	スイッチまたはスイッチのポート範囲が受信したタグなしパケットに割り当てるプライオリティ値。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

スイッチに 802.1p デフォルトプライオリティを設定します。

```
DGS-3200-10:4#config 802.1p default_priority all 5
Command: config 802.1p default_priority all 5

Success.

DGS-3200-10:4#
```

show 802.1p default_priority

目的

スイッチの現在のデフォルトプライオリティ設定を表示します。

構文

show 802.1p default_priority {<portlist>}

説明

スイッチの現在のデフォルトプライオリティ設定を表示します。

パラメータ

パラメータ	説明
<portlist>	表示するポートまたは範囲を指定します。パラメータが指定されないと、システムはすべてのデフォルトプライオリティ設定を表示します。

制限事項

なし。

使用例

スイッチの現在の 802.1p デフォルトプライオリティ設定を表示します。

```
DGS-3200-10:4#show 802.1p default_priority
Command: show 802.1p default_priority

Port     Priority     Effective Priority
-------  -----------  ------------------
1        0            0
2        0            0
3        0            0
4        0            0
5        0            0
6        0            0
7        0            0
8        0            0
9        0            0
10       0            0

DGS-3200-10:4#
```

第 55 章　DHCP リレーコマンド

DHCP/BOOTP メッセージが中継される最大のホップ（ルータの）数と DHCP/BOOTP 情報をスイッチに中継するための DHCP/BOOTP サーバの登録を行います。

コマンドラインインタフェース（CLI）における DHCP リレーコマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
config dhcp_relay	{hops <value 1-16> | time <sec 0-65535>}
config dhcp_relay add	ipif <ipif_name 12> <ipaddr>
config dhcp_relay delete	ipif <ipif_name 12> <ipaddr>
config dhcp_relay option_82	{state [enable | disable] | check [enable | disable] | policy [replace | drop|keep]}
enable dhcp_relay	
disable dhcp_relay	
show dhcp_relay	{ipif <ipif_name 12>}

注意

1. DHCP リレーコマンドは BOOTP リレーコマンドで定義したすべてのコマンドを含んでいます。この DHCP リレーコマンドがご使用のシステムでサポートされている場合、BOOTP リレーコマンドを無視することができます。
2. DHCP リレーをサポートするシステムは、コンフィグレーションファイル内に BOOTP リレーコマンドを許可しますが、コンソール画面からは入力できません。また、コンフィグレーションファイルからの BOOTP リレーコマンド設定は、「save」コマンドが実行される場合、DHCP リレーコマンドとして保存されます。

以下のセクションで各コマンドについて詳しく記述します。

config dhcp_relay

目的

スイッチの DHCP リレー機能を設定します。

構文

config dhcp_relay {hops <value 1-16> | time <sec 0-65535>}

説明

DHCP リレー機能を設定します。

パラメータ

パラメータ	説明
hops <value 1-16>	DHCP パケットが越えることができるリレーエージェントの最大ホップ数を指定します。範囲は、1-16 です。初期値は 4 です。
time <sec 0-65535>	スイッチが DHCP リクエストをリレーしなければならない最小の時間（秒）。この時間を経過すると、スイッチは DHCP パケットを破棄します。範囲は 0-65535（秒）です。初期値は 0（秒）です。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

DHCP リレーを設定します。

```
DGS-3200-10:4#config dhcp_relay hops 4 time 2
Command: config dhcp_relay hops 4 time 2

Success.

DGS-3200-10:4#
```

config dhcp_relay add

目的

スイッチの DHCP リレーテーブルに送信先 IP アドレスを追加します。

構文

config dhcp_relay add ipif <ipif_name 12> <ipaddr>

説明

DHCP リレーパケットを転送（リレー）する送信先として IP アドレスを追加します。

パラメータ

パラメータ	説明
<ipif_name 12>	DHCP リレーを有効にする IP インタフェース名。本製品では「System」です。
<ipaddr>	DHCP サーバの IP アドレス。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

DHCP/BOOTP リレーテーブルに送信先 IP アドレスを追加します。

```
DGS-3200-10:4#config dhcp_relay add ipif System 10.43.21.12
Command: config dhcp_relay add ipif System 10.43.21.12

Success.

DGS-3200-10:4#
```

config dhcp_relay delete

目的

スイッチの DHCP/BOOTP リレーテーブルから送信先 IP アドレスを削除します。

構文

config dhcp_relay delete ipif <ipif_name 12> <ipaddr>

説明

スイッチの DHCP/BOOTP リレーテーブルから送信先 IP アドレスを削除します。

パラメータ

パラメータ	説明
<ipif_name 12>	以下の IP アドレスを含む IP インタフェース名。本製品では「System」です。
<ipaddr>	DHCP サーバの IP アドレス。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

DHCP/BOOTP リレーテーブルから送信先 IP アドレスを削除します。

```
DGS-3200-10:4#config dhcp_relay delete ipif System 10.43.21.12
Command: config dhcp_relay delete ipif System 10.43.21.12

Success.

DGS-3200-10:4#
```

config dhcp_relay option_82

目的

スイッチの DHCP リレーエージェント Information Option 82 の状態を設定します。

構文

config dhcp_relay option_82 {state [enable | disable] | check [enable | disable] | policy [replace | drop | keep]}

説明

スイッチの DHCP リレーエージェント Information Option 82 の設定を行う際に使用します。Circuit ID サブオプションおよび Remote ID サブオプションのフォーマットは以下の通りです。

注意 スタンドアロンスイッチの場合、サーキット ID のサブオプションのモジュールフィールドは常に 0 です。

サーキット ID のサブオプションフォーマット

1.	2.	3.	4.	5.	6.	7.
1	6	0	4	VLAN	モジュール	ポート
1 バイト	1 バイト	1 バイト	1 バイト	2 バイト	1 バイト	1 バイト

1. サブオプションタイプ
2. サブオプションタイプ長
3. Circuit ID タイプ
4. Circuit ID 長
5. VLAN : DHCP クライアントパケットを受信した VLAN
6. モジュール : スタンドアロンスイッチの場合は常に 0。スタッカブルスイッチの場合は Unit ID。
7. ポート : DHCP クライアントパケットを受信したポート番号。ポート番号は 1 から始まります。

リモート ID のサブオプションフォーマット

1.	2.	3.	4.	5.
2	8	0	6	MAC アドレス
1 バイト	1 バイト	1 バイト	1 バイト	6 バイト

1. サブオプションタイプ
2. サブオプション長
3. Remote ID タイプ
4. Remote ID 長
5. MAC アドレス : スイッチのシステム MAC アドレス

パラメータ

パラメータ	説明
state [enable | disable]	• enable - リレーエージェントは DHCP サーバとクライアント間で交わすメッセージに DHCP Relay Information（Option 82 フィールド）を挿入 / 削除します。リレーエージェントが DHCP リクエストを受信すると、Option 82 情報と（設定があれば）リレーエージェントの IP アドレスをパケットに付加します。Option 82 情報が付加されたパケットは DHCP サーバに送信されます。Option 82 をサポートする DHCP サーバがパケットを受信すると、そのサーバは remote ID、circuit ID、またはそれらの両方を使用して IP アドレスを割り当て、単一の remote ID または circuit ID に割り当て可能な IP アドレス制限などのポリシーを適用します。DHCP サーバは Option-82 フィールドの値を DHCP Reply にそのまま残します。DHCP サーバは、スイッチが DHCP request を中継していた場合はユニキャストで応答します。スイッチは remote ID や circuit ID フィールドを調べて、本来の Option-82 情報が挿入されていたかを確認します。スイッチは Option-82 フィールドを削除後、そのパケットを DHCP クライアントに接続しているスイッチポートに転送します。 • disable - リレーエージェントは DHCP サーバとクライアント間で交換するメッセージに DHCP Relay Information（Option 82 フィールド）の挿入 / 削除を行いません。また、以下の Option 82 の Check と Policy のフィールドは無効になります。（初期値）
check [enable | disable]	• enable - 本フィールドを有効にすると、リレーエージェントはパケットの Option 82 フィールドの妥当性のチェックを行います。スイッチが DHCP クライアントから Option 82 フィールドを含むパケットを受信すると、スイッチはこれらのパケットは不正だとしてパケットを廃棄します。リレーエージェントは DHCP サーバから受信したパケットから不正なメッセージを削除します。 • disable - 本フィールドを無効にすると、リレーエージェントはパケットの Option 82 フィールドの妥当性のチェックを行いません。（初期値）
policy [replace | drop | keep]	• replace - DHCP クライアントから受信したパケットの既存のリレー情報をスイッチの DHCP リレー情報に置き換えます。（初期値） • drop - DHCP クライアントから受信したパケットに既にリレー情報があった場合はそのパケットを削除します。 • keep - DHCP クライアントから受信したパケットの既存のリレー情報を保持します。

注意 「check」オプションが無効の場合にのみ再転送ポリシーはアクティブとなります。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

DHCP Relay Agent Information Option 82 State を設定します。

```
DGS-3200-10:4#config dhcp_relay option_82 state enable
Command: config dhcp_relay option_82 state enable

Success.

DGS-3200-10:4#
```

DHCP Relay Agent Information Option 82 Check を設定します。

```
DGS-3200-10:4#config dhcp_relay option_82 check enable
Command: config dhcp_relay option_82 check enable

Success.

DGS-3200-10:4#
```

DHCP Relay Agent Information Option 82 Policy を設定します。

```
DGS-3200-10:4#config dhcp_relay option_82 policy replace
Command: config dhcp_relay option_82 policy replace

Success.

DGS-3200-10:4#
```

enable dhcp_relay

目的

スイッチの DHCP/BOOTP リレーを有効にします。

構文

enable dhcp_relay

説明

スイッチの DHCP/BOOTP リレーを有効にします。

パラメータ

なし。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

DHCP リレーを有効にします。

```
DGS-3200-10:4#enable dhcp_relay
Command: enable dhcp_relay

Success.

DGS-3200-10:4#
```

disable dhcp_relay

目的

スイッチの DHCP リレー機能を無効にします。

構文

disable dhcp_relay

説明

スイッチの DHCP リレー機能を無効にします。

パラメータ

なし。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

DHCP リレーを無効にします。

```
DGS-3200-10:4#disable dhcp_relay
Command: disable dhcp_relay

Success.

DGS-3200-10:4#
```

show dhcp_relay

目的

現在の DHCP/BOOTP リレー設定を表示します。

構文

show dhcp_relay {ipif <ipif_name 12>}

説明

現在の DHCP リレー設定を表示するか、または IP インタフェース名が指定されると、その IP インタフェースの DHCP リレー設定を表示します。

パラメータ

パラメータ	説明
ipif <ipif_name 12>	現在の DHCP リレー設定を表示する IP インタフェース名。本製品では「System」です。パラメータが指定されないと、システムはすべての DHCP リレー設定を表示します。

制限事項

なし。

使用例

DHCP リレー設定を表示します。

```
DGS-3200-10:4#show dhcp_relay ipif System
Command: show dhcp_relay ipif System

DHCP/Boop Relay Status         : Disabled
DHCP/Boop Hops Count Limit     : 4
DHCP/Boop Relay Time Threshold : 0
DHCP Relay Agent Information Option 82 State  : Disabled
DHCP Relay Agent Information Option 82 Check  : Disabled
DHCP Relay Agent Information Option 82 Policy : Replace

Interface     Server 1        Server 2         Server 3        Server 4
------------- --------------- ---------------- --------------- --------------
System        10.48.74.122    10.23.12.34      10.12.34.12     10.48.75.121

DGS-3200-10:4#
```

第 56 章　DHCP ローカルリレー設定コマンド

コマンドラインインタフェース（CLI）における DHCP ローカルリレーコマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
config dhcp_local _relay	vlan <vlan_name 32> state [enable | disable]
enable dhcp_local_relay	
disable dhcp_local_relay	
show dhcp_local_relay	

以下のセクションで各コマンドについて詳しく記述します。

config dhcp_local_relay vlan

目的

指定の VLAN に対して DHCP ローカルリレー機能を有効または無効にします。

構文

config dhcp_local_relay vlan <vlan_name 32> state [enable | disable]

説明

指定の VLAN への DHCP ローカルリレー機能を有効または無効にします。VLAN への DHCP ローカルリレー機能を有効にした場合、DHCP パケットは送信元 MAC アドレスおよびゲートウェイアドレスを変更することなくブロードキャストでリレーされます。DHCP オプション 82 は自動的に追加されます。

パラメータ

パラメータ	説明
<vlan_name 32>	DHCP ローカルリレー機能を有効にする VLAN 名。
state [enable | disable]	指定の VLAN への DHCP ローカルリレーを有効または無効にします。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

デフォルト VLAN への DHCP ローカルリレーを有効にします。

```
DGS-3200-10:4#config dhcp_local_relay vlan default state enable
Command: config dhcp_local_relay vlan default state enable

Success.

DGS-3200-10:4#
```

enable dhcp_local_relay

目的

スイッチの DHCP ローカルリレー機能を有効にします。

構文

enable dhcp_local_relay

説明

スイッチの DHCP ローカルリレー機能を有効にします。

パラメータ

なし。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

SNTP 設定情報を表示します。

```
DGS-3200-10:4#enable dhcp_local_relay
Command: enable dhcp_local_relay

Success.

DGS-3200-10:4#
```

disable dhcp_local_relay

目的
　スイッチの DHCP ローカルリレー機能を無効にします。
構文
　disable dhcp_local_relay
説明
　スイッチの DHCP ローカルリレー機能をグローバルに無効にします。
パラメータ
　なし。
制限事項
　管理者レベルユーザのみ本コマンドを実行できます。
使用例
　スイッチの DHCP ローカルリレー機能を無効にします。

```
DGS-3200-10:4#disable dhcp_local_relay
Command: disable dhcp_local_relay

Success.

DGS-3200-10:4#
```

show dhcp_local_relay

目的
　現在の DHCP ローカルリレー設定を表示します。
構文
　show dhcp_local_relay
説明
　現在の DHCP ローカルリレー設定を表示します。
パラメータ
　なし。
制限事項
　なし。
使用例
　現在の DHCP ローカルリレー設定を表示します。

```
DGS-3200-10:4# show dhcp_local_relay
Command: show dhcp_local_relay

DHCP/BOOTP Local Relay Status    : Disabled
DHCP/BOOTP Local Relay VID List  : 1,3-4

DGS-3200-10:4#
```

第 57 章　IPv6 Neighbor 検出コマンド

以下のコマンドは、スイッチの IPv6 Neighbor を検出し、これらの Neighbor デバイスに関する動作中のデータベースを保持するために使用されます。

コマンドラインインタフェース（CLI）における IPv6 Neighbor 検出コマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
create ipv6 neighbor_cache ipif	<ipif_name 12> <ipv6addr> <macaddr>
delete ipv6 neighbor_cache ipif	[<ipif_name 12> | all] [<ipv6addr> | static | dynamic | all]
show ipv6 neighbor_cache ipif	[<ipif_name 12> | all] [ipv6address <ipv6addr> | static | dynamic | all]
config ipv6 nd ns ipif	<ipif_name 12> retrans_time <unit 0-4294967295>
show ipv6 nd ipif	{<ipif_name 12>}

以下のセクションで各コマンドについて詳しく記述します。

create ipv6 neighbor_cache ipif

目的

スタティックな IPv6 Neighbor を追加します。

構文

create ipv6 neighbor_cache ipif<ipif_name 12> <ipv6addr> <macaddr>

説明

スイッチに作成した IPv6 インタフェースにスタティックな IPv6 Neighbor を追加します。

パラメータ

パラメータ	説明
<ipif_name 12>	「create ipif」コマンドを使用して設定した IPv6 インタフェース名を入力します。
<ipv6addr>	Neighbor デバイスの IPv6 アドレスを入力し、本コマンドで作成した IP インタフェースの IPv6 Neighbor として追加します。
<macaddr>	Neighbor デバイスの MAC アドレスを入力し、本コマンドで作成した IP インタフェースの IPv6 Neighbor として追加します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

スタティックな IPv6 Neighbor を作成します。

```
DGS-3200-10:4#create ipv6 neighbor_cache ipif System 3ffc::1 00:01:02:03:04:05
Command: create ipv6 neighbor_cache ipif System 3FFC::1 00-01-02-03-04-05

Success.

DGS-3200-10:4#
```

delete ipv6 neighbor_cache ipif

目的

スタティックな IPv6 Neighbor を削除します。

構文

delete ipv6 neighbor_cache ipif [<ipif_name 12> | all] [<ipv6addr> | static | dynamic | all]

説明

本 ipif（IP インタフェース）でアドレスキャッシュまたはすべてのアドレスキャッシュエントリから Neighbor キャッシュエントリまたはスタティック Neighbor キャッシュエントリを削除します。スタティックとダイナミック両方のエントリを削除することができます。

パラメータ

パラメータ	説明
<ipif_name 12> | all	• <ipif_name 12> -「create ipif」コマンドを使用して作成した IPv6 インタフェース名を入力します。 • all - スイッチのすべての IPv6 Neighbor を表します。
<ipv6addr>	Neighbor デバイスの IPv6 アドレスを入力し、本コマンドを入力して作成した IP インタフェースの IPv6 Neighbor を削除します。
static | dynamic | all	• static - 以前に登録した IP インタフェースの IPv6 Neighbor からスタティックに設定された Neighbor デバイスを削除します。 • dynamic - 以前に登録した IP インタフェースの IPv6 Neighbor からダイナミックに設定された Neighbor デバイスを削除します。 • all - スイッチのすべての IPv6 Neighbor を削除します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

スタティックな IPv6 Neighbor を削除します。

```
DGS-3200-10:4#delete ipv6 neighbor_cache ipif System 3ffc::1
Command: delete ipv6 neighbor_cache ipif System 3FFC::1

Success.

DGS-3200-10:4#
```

show ipv6 neighbor_cache ipif

目的

スイッチの IPv6 インタフェースの Neighbor キャッシュを参照します。

構文

show ipv6 neighbor_cache ipif [<ipif_name 12> | all] [ipv6address <ipv6addr> | static | dynamic | all]

説明

スイッチの現在の IPv6 インタフェースにおける IPv6 Neighbor を表示します。Neighbor キャッシュを参照するためには、IP インタフェース、IPv6 アドレスまたはスタティックに入力された IPv6 アドレスを指定します。

パラメータ

パラメータ	説明
<ipif_name 12> | all	• <ipif_name 12> - IPv6 Neighbor を参照する IP インタフェースを入力します。これは本インタフェースのすべての IPv6 Neighbor を表示します。 • all - スイッチに作成したすべての IPv6 インタフェースを表します。
ipv6address <ipv6addr>	情報を参照する Neighbor の IPv6 アドレスを入力します。
static | dynamic | all	• static - スイッチに登録済みのすべてのスタティック IPv6 Neighbor を参照します。 • dynamic - 以前に登録した IP インタフェースの IPv6 Neighbor からダイナミックに設定された Neighbor デバイスを参照します。 • all - 以前に登録した IP インタフェースの IPv6 Neighbor から設定されたすべての Neighbor デバイスを参照します。

制限事項

なし。

使用例

設定した IP インタフェースの IPv6 Neighbor を表示します。

```
DGS-3200-10:4#show ipv6 neighbor_cache ipif System all
Command: show ipv6 neighbor_cache ipif System all

Neighbor                  Link Layer Address  Interface  State
------------------------  ------------------  ---------  ------
FE80::20B:6AFF:FECF:7EC6  00-0B-6A-CF-7E-C6   System      T

Total Entries:1

State:
(I)means Incomplete state. (R)means Reachable state.
(S)means Stale state.      (D)means Delay state.
(P)means Probe state.      (T)means Static state.

DGS-3200-10:4#
```

config ipv6 nd ns ipif

目的

スイッチから送信される Router Solicitation メッセージのパラメータを設定します。

構文

config ipv6 nd ns ipif <ipif_name 12> retrans_time <unit 0-4294967295>

説明

スイッチから送信される Router Solicitation メッセージのパラメータを設定します。これらのメッセージは、スイッチの IPv6 Neighbor を検出するのに使用されます。

パラメータ

パラメータ	説明
<ipif_name 12>	Router Solicitation を送信する IPv6 インタフェース名を入力します。
retrans_time <unit 0-4294967295>	ローカルネットワークに Neighbor Solicitation パケットを再送する間隔（m 秒）を設定します。「config ipv6 nd ra」コマンドにおいても同じ「ra retrans_time」値を持っています。一方を設定した場合、もう一方も変更します。0-4294967295（m 秒）の範囲から指定します。低い数字を指定すると、非常に速い間隔となるため、お勧めしません。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

IPv6 Neighbor Detection（ND）Neighbor Solicitation メッセージを設定します。

```
DGS-3200-10:4#config ipv6 nd ns ipif System retrans_time 400
Command: config ipv6 nd ns ipif System retrans_time 400

Success.

DGS-3200-10:4#
```

show ipv6 nd

目的

スイッチの Neighbor Detection に関する情報を表示します。

構文

show ipv6 nd {ipif <ipif_name 12>}

説明

スイッチの IPv6 Neighbor Detection に関する設定情報を表示します。情報を参照する IP インタフェースを指定することもできます。

パラメータ

パラメータ	説明
<ipif_name 12>	本情報を参照するために、IPv6 Neighbor の IP インタフェース名を入力します。本パラメータを省略すると、現在スイッチに設定されている Neighbor Detection に関する全情報が表示されます。

制限事項

なし。

使用例

IPv6 の Neighbor Detection パラメータを表示します。

```
DGS-3200-10:4#show ipv6 nd ipif System
Command: show ipv6 nd ipif System

Interface Name     : System
NS Retransmit Time : 0 (ms)

DGS-3200-10:4
```

第 58 章　アクセスコントロールリスト（ACL）コマンド

アクセスプロファイルを作成すると、各パケットヘッダの中の情報に従い、スイッチがパケット送信を決定するための基準を設定できるようになります。VLAN ごとにこれらの基準を指定できます。

アクセスプロファイルの作成は 2 段階に分かれます。最初に「create access_profile」コマンドを使用してアクセスプロファイルを作成します。例えば、サブネット 10.42.73.0 ～ 10.42.73.255 に対して全トラフィックを制限したい場合、はじめにスイッチに対して各フレームの関連フィールドすべてを調査するアクセスプロファイルを作成します。

上記はスイッチが受信した各フレームの IP フィールドを調査するアクセスプロファイルの例です。スイッチが検出した各送信元 IP アドレスを論理和により source_ip_mask と照合します。profile_id パラメータを使用してアクセスプロファイルに識別番号（ここでは 1）を設定します。スイッチは deny パラメータを使用して規準に合うフレームを廃棄します。（ここでは、次のステップで指定する IP アドレスと ip_source_mask 照合の論理和）。スイッチのアクセスプロファイルの初期値はトラフィックフローを permit（許可）しています。トラフィックを制限するためには、deny パラメータを使用する必要があります。

アクセスプロファイルの作成後、スイッチがある特定フレームの送信、または廃棄を決定するために基準を追加する必要があります。ここでは、10.42.73.0 と 10.42.73.255 間の IP ソースアドレスを持つすべてのパケットを廃棄するものとします。

```
config access_profile profile_id 1 add access_id 1 ip source_ip 10.42.73.1 port 1 deny
```

ここではアクセスプロファイルの作成時に指定した profile_id 1 を使用しています。「add」パラメータはアクセスプロファイルと関連付けられるルールリストに従う基準をスイッチに追加します。アクセスプロファイルに登録した各ルールに、ルールを識別し、ルールリスト内にプライオリティを設定する access_id を割り当てることができます。数字の小さい access_id ほど高いプライオリティになります。アクセスプロファイルに登録したルール内に矛盾がある場合、最も高いプライオリティ（最も低い access_id）のルールが優先されます。

ip パラメータはこの新しいルールが各フレームヘッダ内の IP アドレスに適用されるようにします。source_ip はこのルールを各フレームヘッダの送信元 IP アドレスに適用するようにスイッチに指示します。最後に、IP アドレス 10.42.73.1 は source_ip_mask 255.255.255.0 に統合し、10.42.73.0 と 10.42.73.255 の間の送信元 IP アドレスに IP アドレス 10.42.73.0 を与えます。

本スイッチは、最大 200 個のアクセスプロファイルとルールをサポートしています。

コマンドラインインタフェース（CLI）におけるアクセスコントロールリストとそのパラメータは以下の通りです。

コマンド	パラメータ
create access_profile	profile_id <value 1-200> [ethernet {vlan | source_mac <macmask 000000000000-ffffffffffff> | destination_mac <macmask 000000000000-ffffffffffff> | 802.1p | ethernet_type } | ip {vlan source_ip_mask <netmask> | destination_ip_mask <netmask> | dscp | [icmp {type | code} | igmp {type } | tcp {src_port_mask <hex 0x0-0xffff> | dst_port_mask(<hex 0x0-0xffff> | flag_mask [all | {urg | ack | psh | rst | syn | fin}]} | udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | protocol_id_mask <hex 0x0-0xff> {user_define_mask <hex 0x0-0xffffffff>}]} | packet_content_mask {offset_chunk_1 <value 0-31> <hex 0x0-0xffffffff> offset_chunk_2 <value 0-31> <hex 0x0-0xffffffff> offset_chunk_3 <value 0-31> <hex 0x0-0xffffffff> offset_chunk_4 <value 0-31> <hex 0x0-0xffffffff>} | ipv6 {class | flowlabel | source_ipv6_mask <ipv6mask> | destination_ipv6_mask <ipv6mask>}]
delete access_profile	{profile_id <value 1-200> | all}

コマンド	パラメータ
config access_profile	profile_id <value 1-200> [add access_id [auto_assign | <value 1-200>] [ethernet {vlan <vlan_name 32> | source_mac <macaddr 000000000000-ffffffffffff> | destination_mac <macaddr 000000000000-ffffffffffff> | 802.1p <value 0-7> | ethernet_type <hex 0x0-0xffff>} | ip {vlan <vlan_name 32> | source_ip <ipaddr> | destination_ip <ipaddr> | dscp <value 0-63> | [icmp {type <value 0-255> | code <value 0-255>} | igmp {type <value 0-255>} | tcp {src_port <value 0-65535> | dst_port <value 0-65535> | urg | ack | psh | rst | syn | fin} | udp {src_port <value 0-65535> | dst_port <value 0-65535>} | protocol_id <value 0 - 255> {user_define<hex 0x0-0xffffffff>}]} | packet_content_mask {offset_chunk_1 <hex 0x0-0xffffffff> offset_chunk_2 <hex 0x0-0xffffffff> offset_chunk_3 <hex 0x0-0xffffffff> offset_chunk_4 <hex 0x0-0xffffffff>} | ipv6 {class <value 0-255> | flowlabel <hex 0x0-0xfffff> | source_ipv6 <ipv6addr> | destination_ipv6 <ipv6addr>}] port [<portlist> | all] [permit {priority <value 0-7> {replace_priority} | replace_dscp <value 0-63> | rx_rate [no_limit | <value 1-15625> | counter [enable | disable]} | mirror | deny] {time_range <range_name 32>} |delete access_id <value 1-200>]
show access_profile	{profile_id <value 1-200>}
config time_range	<range_name 32> [hours start_time <time hh:mm:ss> end_time <time hh:mm:ss> weekdays <daylist> | delete]
show time_range	
create cpu access_profile	profile_id <value 1-5> [ethernet {vlan | source_mac <macmask 000000000000-ffffffffffff> | destination_mac <macmask 000000000000-ffffffffffff> | 802.1p | ethernet_type} | ip {vlan | source_ip_mask <netmask> | destination_ip_mask <netmask> | dscp | [icmp {type | code} | igmp {type} | tcp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff> | flag_mask [all | {urg | ack | psh | rst | syn | fin}]} | udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | protocol_id_mask <hex 0x0-0xff> {user_define_mask <hex 0x0-0xffffffff>}]} | packet_content_mask {offset_0-15 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_16-31 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_32-47 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_48-63 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_64-79 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff>} | ipv6 {class | flowlabel | source_ipv6_mask <ipv6mask> | destination_ipv6_mask <ipv6mask>}]
delete cpu access_profile	[profile_id <value 1-5> | all]

コマンド	パラメータ
config cpu access_profile	profile_id <value 1-5> [add access_id <value 1-100> [ethernet {vlan <vlan_name 32> | source_mac <macaddr 000000000000-ffffffffffff> | destination_mac <macaddr 000000000000-ffffffffffff> | 802.1p <value 0-7> | ethernet_type <hex 0x0-0xffff>} | ip {vlan <vlan_name 32> | source_ip <ipaddr> | destination_ip <ipaddr> | dscp <value 0-63> | [Icmp {type <value 0-255> | code <value 0-255>} | igmp {type <value 0-255>} | tcp{src_port <value 0-65535> | dst_port <value 0-65535> | urg | ack | psh | rst | syn | fin} | udp {src_port <value 0-65535> | dst_port <value 0-65535>} | protocol_id <value 0-255> {user_define <hex 0x0-0xffffffff>}]} | packet_content {offset_0-15 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_16-31 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff>| offset_32-47 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff>| offset_48-63 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff>| offset_64-79 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> } | ipv6 {class <value 0-255> | flowlabel <hex 0x0-0xfffff> | source_ipv6 <ipv6addr> | destination_ipv6 <ipv6addr>}] port [<portlist> | all] [permit | deny] {time_range <range_name 32>} | delete access_id <value 1-100>]
show cpu access_profile	{profile_id <value 1-5>}
enable cpu_interface_filtering	
disable cpu_interface_filtering	

以下のセクションで各コマンドについて詳しく記述します。

create access_profile

目的

本コマンドを使用し、パケットヘッダのイーサネット、IP、IPv6 部分を調査するアクセスプロファイルを作成します。入力するマスクはスイッチが指定したフレームのヘッダフィールドに検出した値に合わせることができます。ルールに対する具体的な値は「config access_profile」コマンドを使用します。

構文

```
create access_profile profile_id <value 1-200>
    [ ethernet
        {vlan | source_mac <macmask 000000000000-ffffffffffff> |
        destination_mac <macmask 000000000000-ffffffffffff> |
        802.1p | ethernet_type }(1)"
    | ip
        {vlan | source_ip_mask <netmask> |  destination_ip_mask <netmask> | dscp |
          [icmp {type | code } | igmp {type} |
        tcp  {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff> |
             flag_mask [all | {urg | ack | psh | rst | syn | fin}]} |
        udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} |
        protocol_id_mask <hex 0x0-0xff> {user_define_mask <hex 0x0-0xffffffff>}]}
    | packet_content_mask
        {offset_chunk_1 <value 0-31> <hex 0x0-0xffffffff>
        offset_chunk_2 <value 0-31> <hex 0x0-0xffffffff>
        offset_chunk_3 <value 0-31> <hex 0x0-0xffffffff>
        offset_chunk_4 <value 0-31> <hex 0x0-0xffffffff>}
    | ipv6
       {class | flowlabel | source_ipv6_mask<ipv6mask> | destination_ipv6_mask <ipv6mask>}
    ]
```

説明

このコマンドはパケットヘッダ内のイーサネット、IP、IPv6 部分を調査してスイッチに許可、または拒否されるパケットのプロファイルを作成します。パケットヘッダのイーサネット部分に関連するルールに設定する特定の値は以下に記載されているように「config access_profile」コマンドで定義します。

参照 設定例とより詳しい説明は、359 ページの「付録 A パケットコンテンツ ACL を使用した ARP スプーフィング攻撃の軽減」を参照してください。

パラメータ

パラメータ	説明
profile_id <value 1-200>	このコマンドで作成されるプロファイルを識別するインデックス番号を 1 から 200 で指定します。
ethernet	以下のようにスイッチは各パケットヘッダのレイヤ 2 部分を調査します。 • vlan - 各パケットヘッダの VLAN 部分を調査します。 • source_mac<macmask> - 送信元 MAC アドレスの MAC アドレスマスクを指定します。このマスクは 16 進数（000000000000-FFFFFFFFFFFF）で指定します。 • destination_mac<macmask> - 送信先 MAC アドレスの MAC アドレスマスクを 16 進数（000000000000-FFFFFFFFFFFF）で指定します。 • 802.1p - フレームヘッダの 802.1p プライオリティ値を調査します。 • ethernet_type - 各フレームヘッダのイーサネットタイプ値を調査します。
ip	以下のパラメータで各パケットの IP フィールドを調査します。 • source_ip_mask<netmask> - 送信元 IP アドレスの IP アドレスマスクを指定します。 • destination_ip_mask<netmask> - 送信先 IP アドレスの IP アドレスマスクを指定します。 • icmp - 各フレームヘッダ内の Internet Control Message Protocol（ICMP）フィールドを調査します。 - type - ICMP パケットタイプを指定します。 - code - ICMP コードを指定します。 • igmp - 各フレームヘッダ内の IGMP フィールドを調査します。 - type - IGMP パケットタイプを指定します。 • tcp - 各フレームの Transport Control Protocol（TCP）フィールドを調査します。 - src_port_mask <hex 0x0-0xffff> - 送信元ポートの TCP ポートマスクを指定します。 - dst_port_mask <hex 0x0-0xffff> - 送信先ポートに TCP ポートマスクを指定します。 - flag_mask[all|{urg|ack|psh|rst|syn|fin}]- 対応する flag_mask パラメータを入力します。すべての入力パケットは送信基準として TCP ポート番号を持っており、これらの番号はパケットをどうするかを決定するパケットの一部分に関連する flag bit を持っています。パケット内の特定の flag bit を調査して、パケットを拒否します。次のパラメータから選択できます。all、urg（urgent）、ack（acknowledgement）、psh（push）、rst（reset）、syn（synchronize）、および fin（finish）。 • udp - 各フレームの Universal Datagram Protocol（UDP）フィールドを調査します。 - src_port_mask <hex 0x0-0xffff> - 送信元ポートに UDP ポートマスクを指定します。 - dst_port_mask <hex 0x0-0xffff> - 送信先ポートに UDP ポートマスクを指定します。 • protocol_id_mask - 各フレームのプロトコル ID フィールドを調査します。 - <hex 0x0-0xff>- パケットヘッダ内で検出されるプロトコルを識別する値を 16 進数で指定します。 - user_define <hex 0x0-0xffffffff> - パケットヘッダ内で検出されるユーザ定義のプロトコルを識別する値を 16 進数で指定します。
packet_content_mask	オフセットフィールドは、各ブロックが 4 バイトを表す 4 つの「chunk」に分割されるパケットヘッダを調査するために使用されます。指定されるパケットヘッダブロック内の値は、「mask」フィールドに 16 進数形式で「マスク」フィールドに記載します。 • offset_chunk_1 <value 0-31> <hex 0x0-0xffffffff> • offset_chunk_2 <value 0-31> <hex 0x0-0xffffffff> • offset_chunk_3 <value 0-31> <hex 0x0-0xffffffff> • offset_chunk_4 <value 0-31> <hex 0x0-0xffffffff> 以下のテーブルは、各ブロック内のバイトを指定するための資料です。 chunk0 chunk1 chunk2 …… chunk29 chunk30 chunk31 ====== ====== ====== ======= ======= ====== b126 b2 b6 b114 b118 b122 b127 b3 b7 b115 b119 b123 b1 b4 b8 b116 b120 b124 b0 b5 b9 b117 b121 b125 例 : offset_chunk_1 0 0xffffffff は、オフセット 126,127,0,1 に一致し、offset_chunk_1 0 0x0000ffff は、オフセット 0,1 に一致します。 注意 1 つのパケットコンテンツマスクだけが作成できます。

パラメータ	説明
ipv6	スイッチは IPv6 の「config access_profile」コマンドで設定したルールに基づき、送信または廃棄するために IPv6 パケットを調査します。IPv6 パケットは以下のパラメータによって識別されます。 • class - このパラメータを入力すると、スイッチは IPv6 ヘッダの class フィールドを調査します。本フィールドは IPv4 における「Type of Service（ToS）」、「Precedence bits」フィールドのようなパケットヘッダの一部です。 • flowlabel - このパラメータを入力すると、スイッチは IPv6 ヘッダの flow label フィールドを調査します。本フィールドは送信元で順番につけられる QoS やリアルタイムサービスパケットのためのデフォルトではないフィールドです。 • source_ipv6_mask<ipv6mask> - 送信元の IPv6 アドレスの IP アドレスマスクを指定します。 • destination_ipv6_mask<ipv6mask> - 送信先の IPv6 アドレスの IP アドレスマスクを指定します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。200 個のプロファイルをサポートしています。

使用例

アクセスリストルールを作成します。

```
DGS-3200-10:4#create access_profile profile_id 100 ethernet vlan source_mac FF-FF-FF-FF-FF-FF
destination_mac 00-00-00-FF-FF-FF 802.1p ethernet_type
Command: create access_profile profile_id 100 ethernet vlan source_mac FF-FF-FF-FF-FF-FF
destination_mac 00-00-00-FF-FF-FF 802.1p ethernet_type

Success.

DGS-3200-10:4#create access_profile profile_id 101 ip vlan source_ip_mask 255.255.255.255
destination_ip_mask 255.255.255.0 dscp icmp
Command: create access_profile profile_id 101 ip vlan source_ip_mask 255.255.255.255
destination_ip_mask 255.255.255.0 dscp icmp

Success.

DGS-3200-10:4#
```

delete access_profile

目的

作成したアクセスプロファイルを削除します。

構文

delete access_profile {profile_id <value 1-200> | all}

説明

スイッチに作成済みのアクセスプロファイルを削除するために使用されます。

パラメータ

パラメータ	説明
profile_id <value 1-200>	本コマンドで削除するアクセスプロファイルを識別する番号を 1 から 200 で指定します。この値はアクセスプロファイルが「create access_profile」コマンドで作成される時に割り当てられます。
all	IP-MAC バインディングコマンドを使用して自動的に作成したものを除き、スイッチに現在設定されているすべての IP プロファイルを削除します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。スイッチは 200 個のアクセスエントリをサポートしています。ACL モジュールによって作成されるプロファイルを削除します。

使用例

プロファイル ID 10 を持つアクセスプロファイルを削除します。

```
DGS-3200-10:4#delete access_profile profile_id 10
Command: delete access_profile profile_id 10

Success.

DGS-3200-10:4#
```

config access_profile

目的

本コマンドを使用し、スイッチにアクセスプロファイルを設定し、スイッチに使用されるルールに受信パケットを送信するか、廃棄するかを決めるために使用する値を定義します。「create access_profile」コマンドを使用して入力したマスク値は論理和を使用し、指定したフレームのヘッダフィールド内にスイッチが検出した値と統合します。

構文

```
config access_profile profile_id <value 1-200>
    [add access_id [auto_assign | <value 1-200>]
    [ethernet
      {vlan <vlan_name 32> | source_mac <macaddr 000000000000-ffffffffffff> |
      destination_mac <macaddr 000000000000-ffffffffffff> |
      802.1p <value 0-7> | ethernet_type <hex 0x0-0xffff>}
     port [<portlist> | all]
     [permit {priority <value 0-7> | rx_rate [no_limit | <value 1-156249>]} | mirror | deny]
    | ip
      {vlan <vlan_name 32> | source_ip <ipaddr> | destination_ip <ipaddr> | dscp <value 0-63> |
       [icmp {type <value 0-255> | code <value 0-255>} | igmp {type <value 0-255>} |
        tcp {src_port <value 0-65535> | dst_port <value 0-65535> |
        urg | ack | psh | rst | syn | fin} |
        udp {src_port <value 0-65535> | dst_port <value 0-65535>} |
        protocol_id <value 0 - 255>  {user_define<hex 0x0-0xffffffff>}]}
    | packet_content_mask
       {offset_chunk_1 <value 0-31> <hex 0x0-0xffffffff>
       offset_chunk_2 <value 0-31> <hex 0x0-0xffffffff>
       offset_chunk_3 <value 0-31> <hex 0x0-0xffffffff>
       offset_chunk_4 <value 0-31> <hex 0x0-0xffffffff>}
    | ipv6
       {class <value 0-255> | flowlabel <hex 0x0-0xfffff> |
       source_ipv6 <ipv6addr> | destination_ipv6 <ipv6addr>}
       port [<portlist> | all]
       [permit {priority <value 0-7> | rx_rate [no_limit | <value 1-15625>] | counter [enable | disable]}
       | mirror | deny]]
       {time_range <range_name 32>}
       | delete access_id <value 1-200>]
```

説明

本コマンドを使用し、各パケットヘッダのイーサネット、ip、ipv6 部分を元にパケットの廃棄または転送のいずれかを行うためにスイッチが使用するルールを定義します。

パラメータ

パラメータ	説明
profile_id <value 1-200>	本コマンドで設定したアクセスプロファイルを識別する番号を 1 から 200 で指定します。この値はアクセスプロファイルが「create access_profile」コマンドで作成される時に割り当てられます。低いプロファイル ID ほどプライオリティが高くなります。
add access_id <value 1-200>	上で指定したアクセスプロファイルにルールを追加します。値は追加ルールの相対的なプライオリティを示します。最大 200 種類のルールをアクセスプロファイルに設定できます。 • auto_assign - 設定するルールに自動的に 1-200 の数字を割り当てます。
ethernet	以下のパラメータに基づきパケットを廃棄するか、送信するかを決定するために各パケットのレイヤ 2 部分をスイッチが調査します。 • vlan<vlan_name 32> - 既に作成しているこの VLAN だけにアクセスプロファイルを適用します。 • source_mac<macaddr> - 送信元 MAC アドレスを持つパケットだけにアクセスプロファイルを適用します。MAC アドレスエントリは 16 進数（000000000000-FFFFFFFFFFFF）で指定します • destination_mac<macaddr> - 送信先 MAC アドレスを持つパケットだけにアクセスプロファイルを適用します。MAC アドレスエントリは 16 進数（000000000000-FFFFFFFFFFFF）で指定します • 802.1p<value 0-7> - 802.1p プライオリティ値を持つパケットだけにアクセスプロファイルを適用します。 • ethernet_type<hex 0x0-0xffff> - パケットヘッダ内に 16 進数の 802.1Q イーサネットタイプを持つパケットだけにアクセスプロファイルを適用します。

パラメータ	説明
ip	以下のパラメータで各パケットの IP フィールドを調査します。 • vlan <vlan_name 32> - 既に作成しているこの VLAN だけにアクセスプロファイルを適用します。 • source_ip_mask <netmask> - 送信元 IP アドレスの IP アドレスマスクを指定します。 • dscp <value 0-63> - DSCP の値（0-63）を指定します。 • destination_ip_mask <netmask> - 送信先 IP アドレスの IP アドレスマスクを指定します。 • icmp - 各フレームヘッダ内の Internet Control Message Protocol（ICMP）フィールドを調査します。 • tcp - 各フレームの Transport Control Protocol（TCP）フィールドを調査します。 - src_port_mask <hex 0x0-0xffff> - 送信元ポートの TCP ポートマスクを指定します。 - dst_port_mask <hex 0x0-0xffff> - 送信先ポートに TCP ポートマスクを指定します。 • flag_mask [all | {urg | ack | psh | rst | syn | fin}] - 対応する flag_mask パラメータを入力します。すべての入力パケットは送信基準として TCP ポート番号を持っており、これらの番号はパケットをどうするかを決定するパケットの一部分に関連する flag bit を持っています。パケット内の特定の flag bit を調査して、パケットを拒否します。次のパラメータから選択できます。all、urg（urgent）、ack（acknowledgement）、psh（push）、rst（reset）、syn（synchronize）、および fin（finish）。 • udp - 各フレームの Universal Datagram Protocol（UDP）フィールドを調査します。 - src_port_mask<hex 0x0-0xffff> - 送信元ポートに UDP ポートマスクを指定します。 - dst_port_mask<hex 0x0-0xffff> - 送信先ポートに UDP ポートマスクを指定します。 • protocol_id_mask - 各フレームのプロトコル ID フィールドを調査します。 - <hex 0x0-0xff>- パケットヘッダ内で検出されるプロトコルを識別する値を 16 進数で指定します。 - user_define <hex 0x0-0xffffffff>- パケットヘッダ内で検出されるユーザ定義のプロトコルを識別する値を 16 進数で指定します。
packet_content_mask	オフセットフィールドは、各ブロックが 4 バイトを表す 4 つの「chunk」に分割されるパケットヘッダを調査するために使用されます。指定されるパケットヘッダブロック内の値は、「mask」フィールドに 16 進数形式で「マスク」フィールドに記載します。 • offset_chunk_1 <value 0-31> <hex 0x0-0xffffffff> • offset_chunk_2 <value 0-31> <hex 0x0-0xffffffff> • offset_chunk_3 <value 0-31> <hex 0x0-0xffffffff> • offset_chunk_4 <value 0-31> <hex 0x0-0xffffffff> 以下のテーブルは、各ブロック内のバイトを指定するための資料です。 chunk0 chunk1 chunk2 …… chunk29 chunk30 chunk31 ====== ====== ====== ======= ======= ======= b126 b2 b6 b114 b118 b122 b127 b3 b7 b115 b119 b123 b1 b4 b8 b116 b120 b124 b0 b5 b9 b117 b121 b125 例 : offset_chunk_1 0 0xffffffff は、オフセット 126,127,0,1 に一致し、offset_chunk_1 0 0x0000ffff は、オフセット 0,1 に一致します。 **注意** 1 つのパケットコンテンツマスクだけが作成できます。
ipv6	スイッチは IPv6 の config access_profile コマンドで設定したルールに基づき、送信または廃棄するために IPv6 パケットを調査します。IPv6 パケットは以下のパラメータによって識別されます。 • class - このパラメータを入力すると、スイッチは IPv6 ヘッダの class フィールドを調査します。本フィールドは IPv4 における「Type of Service（ToS）」、「Precedence bits」フィールドのようなパケットヘッダの一部です。 • flowlabel - このパラメータを入力すると、スイッチは IPv6 ヘッダの flow label フィールドを調査します。本フィールドは送信元で順番につけられる QoS やリアルタイムサービスパケットのためのデフォルトではないフィールドです。 • source_ipv6_mask <ipv6mask> - 送信元の IPv6 アドレスの IP アドレスマスクを指定します。 • destination_ipv6_mask <ipv6mask> - 送信先の IPv6 アドレスの IP アドレスマスクを指定します。
port<portlist> | all	イーサネットのアクセスプロファイルをスイッチの各ポートに定義します。
permit	スイッチによる送信を許可するアクセスプロファイルに適合するパケットを指定します。 • priority <value 0-7> - スイッチに既に設定している 802.1p デフォルトプライオリティを書き換えたい場合に、このパラメータを指定します。パケットが送信される CoS キューを決定するためにこのパラメータを使用します。本フィールドを選択すると、スイッチが受信したパケットの中の、本プライオリティに一致するパケットは、既に指定した CoS キューに送られます。 • {replace_priority} - 指定した CoS キューにパケットを送信する前に、このコマンドで既に指定している基準に適合するパケットの 802.1p デフォルトプライオリティをプライオリティフィールドに入力した値に書き換えたい場合に、このパラメータを入力します。指定しない場合は、パケットは送出される前に、入力用の 802.1p ユーザプライオリティを元の値に書き換えられます。
rx_rate [no_limit | <value 1-15625>]	設定したプロファイルの Rx 帯域を制限するために使用します。このレートは次の式を使用します。1value=64kbit/sec。（例 :Rx rate に 10 を選択すると、Ingress レートは 640kbit/sec となります。）1-15625 の範囲で値を指定するか、または「no_limit」を指定します。初期値は「no_limit」です。

パラメータ	説明
counter [enable | disable]	カウンタ機能を有効または無効にします。カウンタ機能は、アクセスルールに一致するパケット数を記録するために使用されます。例えば、送信元 MAC アドレス 00-00-00-00-00-01 がスイッチへのアクセスを許可するイーサネット ACL を作成し、スイッチが送信元 MAC アドレス 00-00-00-00-00-01 を持つ 1000 個のパケットを受信した場合、カウンタ値は 1000 となり、ACL が 1000 個のパケットを照合したことを示します。本機能はオプションです。初期値では無効に設定されています。
mirror	アクセスプロファイルを設定済みのポートにミラーリングします。ポートミラーリングが有効でターゲットポートに設定されている必要があります。
deny	アクセスプロファイルに適合しないパケットはスイッチによって送信することを許可されず破棄されます。
{time_range <range_name 32>}	本パラメータを選択し、「config time_range」コマンドを使用して設定したタイムレンジ設定名を入力します。このアクセスルールがスイッチで有効または無効にされる場合の実行回数を設定します。
delete access_id <value 1-200>	イーサネットプロファイルから指定ルールを削除します。最大 200 個のルールがイーサネットプロファイルに指定できます。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

イーサネットプロファイルにルールを指定します。

```
DGS-3200-10:4#config access_profile profile_id 101 add access_id 1 ip vlan default source_ip
20.2.2.3 destination_ip 10.1.1.252 dscp 3 icmp port 1 permit
Command: config access_profile profile_id 101 add access_id 1 ip vlan default source_ip 20.2.2.3
destination_ip 10.1.1.252 dscp 3 icmp port 1 permit

Mirror function must be enabled and mirror port must be configured.
Success.

DGS-3200-10:4#
```

show access_profile

目的

スイッチに現在設定されているアクセスプロファイルを表示します。

構文

show access_profile {profile_id <value 1-200>}

説明

現在設定されているアクセスプロファイルを表示します。

パラメータ

パラメータ	説明
profile_id <value 1-200>	本コマンドで参照するアクセスプロファイルを識別する番号を 1 から 200 で指定します。この値はアクセスプロファイルが「create access_profile」コマンドで作成される時に割り当てられます。

制限事項

なし。

使用例

スイッチに現在設定されているすべてのアクセスプロファイルを表示します。

```
DGS-3200-10:4#show access_profile
Command: show access_profile

Access Profile Table
================================================================================
Access Profile ID : 100
Type     : Ethernet Frame Filter
Ports    : 1, 3, 5, 7
Time_range: range_name
Masks    : VLAN             Source MAC        Destination MAC   802.1p Ethernet
           ---------------- ----------------- ----------------- ------ --------
           default          00-00-00-00-00-01 00-00-00-00-00-02
           vlan1
ID Mode
-- ------  ---------------- ----------------- ----------------- ------ --------
1  Permit  default          00-00-00-00-00-00 00-00-00-00-00-00 0      0x800
2  Deny    default          00-00-00-00-00-00 00-00-00-00-00-00 5      0x800
================================================================================
Access Profile ID : 101
Type     : IP Frame Filter
Ports    : 2, 4-8
Time_range: range_name

Masks    : VLAN             Source IP MASK  Dest. IP MASK   DSCP ICMP TYPE CODE
           ---------------- --------------- --------------- ---- --------- ----
                            111.111.111.111 111.111.111.111
ID Mode
-- ------  ---------------- --------------- --------------- ---- --------- ----
1  Permit  default          0.0.0.0         0.0.0.0        1    5         7
================================================================================
Access Profile ID : 102
Type    : IP Frame Filter - IGMP
Ports   : 2, 4-8
Time_range: range_name
Masks   : VLAN             Source IP_Addr  Dest. IP_Addr_  DSCP TYPE
          ---------------- --------------- --------------- ---- ----
                           111.111.111.111 111.111.111.111
ID Mode
-- ------ ---------------- --------------- --------------- ---- ----
1  Permit  default          0.0.0.0         0.0.0.0         1   7
================================================================================
Access Profile ID : 103
Type    : IP Frame Filter - TCP
Ports   : 2, 4-8
Time_range: range_name
Masks   : VLAN             Source IP Addr  Dest. IP Addr   DSCP Src.P Dst.P Flg
          ---------------- --------------- --------------- ---- ----- ----- ---
                           111.111.111.111 111.111.111.111      FFFF  FFFF  FF
ID Mode
-- ------ ---------------- --------------- --------------- ---- ----- ----- ---
1  Permit default          0.0.0.0         0.0.0.0                          FF
================================================================================
Access Profile ID : 104
Type    : IP Frame Filter - UDP
Ports   : 2, 4-8
Time_range: range_name
Masks   : VLAN             Source IP Addr  Dest. IP Addr   DSCP Src.P Dst.P Flg
          ---------------- --------------- --------------- ---- ----- ----- ---
                           111.111.111.111 111.111.111.111      FFFF  FFFF  FF
ID Mode
-- ------ ---------------- --------------- --------------- ---- ----- ----- ---
1  Permit default          0.0.0.0         0.0.0.0                          FF
```

```
================================================================================
Access Profile ID : 105
Type    : IP Frame Filter - User defined
Ports   : 2, 4-8
Time_range: range_name
Masks   : VLAN             Source IP Addr  Dest. IP Addr   DSCP_Prot  Payload
          ---------------- --------------- --------------- ---- ----- --------
                                                                      FFFFFFFF
                                                                      FFFFFFFF
                                                                      FFFFFFFF
                                                                      FFFFFFFF
                                                                      FFFFFFFF
ID Mode
-- ------ ---------------- --------------- --------------- ---- ----- --------
1  Permit                                                21        FFFFFFFF
                                                                      FFFFFFFF
                                                                      FFFFFFFF
                                                                      FFFFFFFF
                                                                      FFFFFFFF
Total Entries : 7

DGS-3200-10:4#
```

config time_range

目的

アクセスプロファイルルールが有効となる時間の範囲を設定します。

構文

config time_range <range_name 32> [hours start_time <time hh:mm:ss> end_time <time hh:mm:ss> weekdays <daylist> | delete]

説明

曜日、時間範囲を指定することによってスイッチの機能が時間範囲内で動作するように指定します。指定される時間の範囲は SNTP 時間または設定時間に基づいています。この時間が有効でない場合、タイムレンジは有効になりません。

パラメータ

パラメータ	説明
<range_name 32>	タイムレンジを識別するために使用する名前を半角英数字 32 文字以内で入力します。このレンジ名はアクセスプロファイルテーブルで使用され、このタイムレンジで有効であるアクセスプロファイルと関連するルールを識別します。
hours	タイムレンジが設定する時間を以下のパラメータで設定します。 • start time <time hh:mm:ss> - 開始時刻を時間、分、秒（24 時形式）で指定します。 • end time <time hh:mm:ss> - 終了時刻を時間、分、秒（24 時形式）で指定します。 例 :19:00:00 は午後 7 時を意味します。開始時刻は終了時刻よりも早くします。
weekdays	タイムレンジを設定するために、曜日を決定します。 • <daylist> - 曜日を 3 文字形式で指定します。（mon、tue、wed など）「-」（ダッシュ）を使用して区切ることで曜日の範囲を指定します。例 : mon-fri は月曜日から金曜日を意味します。「,」（カンマ）を使用して区切ることで曜日を指定します。スペースは使用できません。例 : mon,tue,fri はそれぞれ月曜日、火曜日、金曜日を意味します。
delete	設定したタイムレンジを削除します。タイムレンジプロファイルが ACL エントリに関連付けられている場合、このタイムレンジプロファイルの削除はエラーになります。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

月曜日から金曜日の午前 6 時 30 分から午後 9 時 40 分にタイムレンジを設定します。

```
DGS-3200-10:4#config time_range testdaily hours start_time 12:00:00 end_time 20:00:00 weekdays
mon, fri
Command: config time_range testdaily hours start_time 12:00:00 end_time 20:00:00 weekdays mon,
fri

Success.

DGS-3200-10:4#
```

show time_range

目的

スイッチのタイムレンジの現在の設定を表示します。

構文

show time_range

説明

スイッチの現在のタイムレンジを表示します。

パラメータ

なし。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

現在のタイムレンジを参照します。

```
DGS-3200-10:4#show time_range
Command: show time_range

Time Range information
-------------------------------------------------------------
Range Name    :  test
Weekdays      :  Sun,Tue
Start Time    :  11:00:00
End Time      :  12:00:00
Associated ACL Entries: 2-10, 3-8

DGS-3200-10:4#
```

create cpu access_profile

目的

CPU インタフェースフィルタリングのアクセスプロファイルを特別に作成し、スイッチが調査する入力フレームのヘッダの一部を定義します。マスクを入力し、特定のヘッダフィールド内に検出した値と統合されます。ルールに対する具体的な値は「config cpu access_profile」コマンドを使用して指定します。

構文

```
create cpu access_profile profile_id <value 1-5>
    [ethernet
      {vlan | source_mac <macmask 000000000000-ffffffffffff> |
       destination_mac <macmask 000000000000-ffffffffffff> | 802.1p | ethernet_type}
    | ip
      {vlan | source_ip_mask <netmask> | destination_ip_mask <netmask> |
       dscp | [icmp {type | code} | igmp {type} |
       tcp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff> |
         flag_mask [all | {urg | ack | psh | rst | syn | fin}] } |
       udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} |
       protocol_id_mask <hex 0x0-0xff> {user_define_mask <hex 0x0-0xffffffff>}]}
    | packet_content_mask
       {offset_0-15 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> |
        offset_16-31 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> |
        offset_32-47 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> |
        offset_48-63 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> |
        offset_64-79 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff>}
    | ipv6
       {class | flowlabel | source_ipv6_mask <ipv6mask> | destination_ipv6_mask <ipv6mask>}
    ]
```

説明

CPU Interface Filtering だけに使用するアクセスプロファイルを作成します。マスクを入力し、特定のヘッダフィールド内に検出した値と統合されます。ルールに対する具体的な値は下の config cpu access_profile コマンドを使用して指定します。

パラメータ

パラメータ	説明
profile_id <value 1-5>	アクセスプロファイルを識別する番号を 1 から 5 で指定します。

パラメータ	説明
ethernet	各パケットヘッダのレイヤ 2 部分を調査します。 • vlan - 各パケットヘッダの VLAN 部分を調査します。 • source_mac <macaddr 000000000000-ffffffffffff> - 送信元 MAC アドレスマスクを調査します。MAC アドレスエントリは 16 進数（000000000000-FFFFFFFFFFFF）で指定します。 • destination_mac <macaddr 000000000000-ffffffffffff> - 送信先 MAC アドレスマスクを調査します。MAC アドレスエントリは 16 進数（000000000000-FFFFFFFFFFFF）で指定します。 • 802.1p - フレームヘッダの 802.1p プライオリティ値を調査します。 • ethernet_type - 各フレームヘッダのイーサネットタイプ値を調査します。
ip	各フレームヘッダの IP アドレスを調査します。 • vlan - VLAN マスクを指定します。 • source_ip_mask <netmask> - 送信元 IP アドレスの IP アドレスマスクを指定します。 • destination_ip_mask<netmask> - 送信先 IP アドレスの IP アドレスマスクを指定します。 • dscp - 各フレームヘッダ内の DiffServ Code Point（DSCP）フィールドを調査します。 • icmp- 各フレームヘッダ内の Internet Control Message Protocol（ICMP）フィールドを調査します。 - type - 各フレームの ICMP Type フィールドを調査します。 - code - 各フレームの ICMP Code フィールドを調査します。 • igmp - 各フレームの Internet Group Management Protocol（IGMP）フィールドを調査します。 • tcp - 各フレームの Transport Control Protocol（TCP）フィールドを調査します。 - src_port_mask <hex 0x0-0xffff> - 送信元ポートの TCP ポートマスクを指定します。 - flag_mask [all | {urg | ack | psh | rst | syn | fin}] - 対応する flag_mask パラメータを入力します。すべての入力パケットは基準を送信するような TCP ポート番号を持っており、これらの番号はパケットをどうするかを決定するパケットの一部分に関連する flag bit を持っています。パケット内の特定の flag bit を調査して、パケットを拒否します。次のパラメータから選択できます。all、urg（urgent）、ack（acknowledgement）、psh（push）、rst（reset）、syn（synchronize）、および fin（finish）。 • udp- 各フレームの Universal Datagram Protocol（UDP）フィールドを調査します。 - src_port_mask <hex 0x0-0xffff> - 送信元ポートに UDP ポートマスクを指定します。 - dst_port_mask <hex 0x0-0xffff> - 送信先ポートに UDP ポートマスクを指定します。 • protocol_id_mask <hex 0x0-0xffffffff> - 各フレームのプロトコル ID フィールドを調査します。16 進数で指定します。 - user_define_mask <hex 0x0-0xff>IP プロトコル IP と IP ヘッダの後のマスクオプションにルールを適用します。
packet_content_mask	以下の指定したオフセット値で始まるパケットヘッダをマスクします。 • offset_0-15 - 16 進数でパケットの 0 バイト目から 15 バイト目までのマスクを指定します。 • offset_16-31 - 16 進数でパケットの 16 バイト目から 31 バイト目までのマスクを指定します。 • offset_32-47 - 16 進数でパケットの 32 バイト目から 47 バイト目までのマスクを指定します。 • offset_48-63 - 16 進数でパケットの 48 バイト目から 63 バイト目までのマスクを指定します。 • offset_64-79 - 16 進数でパケットの 64 バイト目から 79 バイト目までのマスクを指定します。
ipv6	• class - IPv6 クラスマスクを指定します。 • flowlabel - IPv6 送信元 IP マスクを指定します。 • source_ipv6_mask - IPv6 送信元 IP マスクを指定します。 • destination_ipv6_mask - IPv6 送信先 IP マスクを指定します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。スイッチは、5 個の CPU プロファイルをサポートしています。

使用例

CPU アクセスプロファイルを作成します。

```
DGS-3200-10:4#create cpu access_profile profile_id 1 ethernet vlan
Command: create cpu access_profile profile_id 1 ethernet vlan

Success.

DGS-3200-10:4#create cpu access_profile profile_id 2 ip source_ip_mask 255.255.255.255
Command: create cpu access_profile profile_id 2 ip source_ip_mask 255.255.255.255

Success.

DGS-3200-10:4#
```

delete cpu access_profile

目的

アクセスプロファイル、または CPU アクセスプロファイルを削除します。

構文

delete cpu access_profile [profile_id <value 1-5> | all]

説明

作成済みの CPU アクセスプロファイルを削除するために使用されます。

パラメータ

パラメータ	説明
profile_id <value 1-5>	削除する CPU アクセスプロファイルを識別する番号を 1 から 5 で指定します。
all	現在スイッチに設定されているすべて CPU アクセスプロファイルを削除します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。スイッチは、5 個のアクセスエントリをサポートしています。CPU ACL モジュールによって作成されるプロファイルを削除するだけです。

使用例

プロファイル 1 を持つ CPU アクセスプロファイルを削除します。

```
DGS-3200-10:4#delete cpu access_profile profile_id 3
Command: delete cpu access_profile profile_id 3

Success.

DGS-3200-10:4#
```

config cpu access_profile

目的

CPU インタフェースフィルタリングに使用する CPU アクセスプロファイルを設定し、受信パケットを送信するか、廃棄するかを決めるためにスイッチに使用される特定の値を定義します。「create cpu access_profile」コマンドを使用して入力したマスク値は、論理和を使用して特定のフレームヘッダフィールド内にスイッチが検出した値と統合します。ルールに対する具体的な値は下の「config cpu access_profile」コマンドを使用して指定します。

構文

```
config cpu access_profile profile_id <value 1-5>
      [add access_id <value 1-100>
       [ethernet
          {vlan <vlan_name 32> | source_mac <macaddr 000000000000-ffffffffffff> |
          destination_mac <macaddr 000000000000-ffffffffffff> |
          802.1p <value 0-7> | ethernet_type <hex 0x0-0xffff>}
        | ip
          {vlan <vlan_name 32> | source_ip <ipaddr> | destination_ip <ipaddr> | dscp <value 0-63> |
          [
            icmp {type <value 0-255> | code <value 0-255>} |
            igmp {type <value 0-255>} |
            tcp {src_port <value 0-65535> | dst_port <value 0-65535> |
           urg | ack | psh | rst | syn | fin} |
            udp {src_port <value 0-65535> | dst_port <value 0-65535>} |
            protocol_id <value 0 - 255> {user_define <hex 0x0-0xffffffff>}
          ]}
        | packet_content
          {offset_0-15 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff>|
           offset_16-31 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff>|
           offset_32-47 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff>|
           offset_48-63 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff>|
           offset_64-79 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff>
          }(1)
        | ipv6
          {class <value 0-255> | flowlabel <hex 0x0-0xfffff> |
           source_ipv6 <ipv6addr> | destination_ipv6 <ipv6addr>}
      ]
      port [<portlist> | all] [ permit | deny] {time_range <range_name 32>}
      | delete access_id <value 1-100>
     ]
```

説明

CPU インタフェースフィルタリングのために CPU アクセスプロファイルを設定し、「create cpu access_profile」コマンドを使用して入力したマスク値と論理和を使用して統合する値を入力します。

パラメータ

パラメータ	説明
profile_id <value 1-5>	本コマンドで設定するアクセスプロファイルを識別する番号を 1 から 5 で指定します。この値はアクセスプロファイルが「create access_profile」コマンドで作成される時に割り当てられます。プロファイル ID はプロファイルに相対的なプロパティを設定し、このコマンドで作成したアクセスプロファイルを識別するインデックス番号を指定します。プライオリティは別のプロファイルとの比較で設定されます。低いプロファイル ID ほどプライオリティが高くなります。 • add access_id <value 1-100> - 上で指定したアクセスプロファイルにルールを追加します。値は作成したルールにインデックスをつけるために使用されます。
ethernet	スイッチが各パケットのレイヤ 2 部分だけを調査します。 • vlan <vlan_name 32> - アクセスプロファイルをこの VLAN にだけ適用します。 • source_mac <macaddr 000000000000-ffffffffffff> - アクセスプロファイルをこの送信元 MAC アドレスに適用します。 • destination_mac <macaddr 000000000000-ffffffffffff> - アクセスプロファイルをこの送信先 MAC アドレスにだけ適用します。 • ethernet_type <hex 0x0-0xffff> - パケットヘッダ内に 16 進数の 802.1Q イーサネットタイプを持つパケットだけにアクセスプロファイルを適用します。
ip	各パケットの IP フィールドを調査します。 • vlan <vlan_name 32> - この VLAN だけにアクセスプロファイルを適用します。 • source_ip <ipaddr> - アクセスプロファイルをこの送信元 IP アドレスを持つパケットにだけ適用します。 • destination_ip <ipaddr> - アクセスプロファイルをこの送信先 IP アドレスを持つパケットにだけ適用します。 • dscp <value 0-63> - アクセスプロファイルを IP パケットヘッダの Type-of-Service（DiffServ code point、DSCP）フィールド内のこの値を持つパケットにだけ適用します。 • icmp - 各パケット内の Internet Control Message Protocol（ICMP）フィールドを調査する場合に指定します。 - type<value 0-255> - アクセスプロファイルを ICMP Type 値に適用します。 - code<value 0-255> - アクセスプロファイルを ICMP Code に適用します。 • igmp - 各パケットの Internet Group Management Protocol（IGMP）フィールドを調査します。 - type <value 0-255> - アクセスプロファイルをこの IGMP type 値を持つパケットに適用します。 • tcp - 各パケットの Transmission Control Protocol（TCP）フィールドを調査します。 - src_port<value 0-65535> - アクセスプロファイルを TCP ヘッダにこの TCP 送信元ポートを持つパケットにだけ適用します。 - dst_port<value 0-65535> - アクセスプロファイルを TCP ヘッダにこの TCP 送信先ポートを持つパケットにだけ適用します。 • udp - 各パケットの Transmission Control Protocol（TCP）フィールドを調査します。 - src_port <value 0-65535> - アクセスプロファイルはヘッダ内にこの UDP 送信元ポートを持つパケットにだけ適用します。 - dst_port <value 0-65535> - アクセスプロファイルはヘッダ内にこの UDP 送信先ポートを持つパケットにだけ適用します。 • protocol_id <value 0-255> - 各パケットのプロトコルフィールドを調査します。このフィールドがここで入力された値を含む場合、以下のルールを適用します。 - user_define_mask <hex 0x0-0xffffffff> - IP プロトコル IP と IP ヘッダの後のマスクオプションにルールを適用します。
packet_content_mask	以下のオフセット値で始まるパケットヘッダをマスクします : • offset_0-15 - 16 進数でパケットの 0 バイト目から 15 バイト目までのマスクを指定します。 • offset_16-31 - 16 進数でパケットの 16 バイト目から 31 バイト目までのマスクを指定します。 • offset_32-47 - 16 進数でパケットの 32 バイト目から 47 バイト目までのマスクを指定します。 • offset_48-63 - 16 進数でパケットの 48 バイト目から 63 バイト目までのマスクを指定します。 • offset_64-79 - 16 進数でパケットの 64 バイト目から 79 バイト目までのマスクを指定します。
ipv6	• class - IPv6 クラスマスクを指定します。 • flowlabel - IPv6 送信元 IP マスクを指定します。 • destination_ipv6_mask - IPv6 送信元 IP マスクを指定します。
<portlist | all>	このアクセスプロファイルを適用するポートを入力します。
permit|mirror|deny	• permit - このコマンドで設定した基準に適合するパケット CPU へのエントリを許可します。 • mirror - アクセスプロファイルを設定済みのポートにミラーリングします。ポートミラーリングが有効でターゲットポートに設定されている必要があります。 • deny - このコマンドで設定した基準に適合するパケット CPU へのエントリを拒否します。
{time_range <range_name 32>}	本パラメータを選択し、「config time_range」コマンドを使用して設定したタイムレンジ設定名を入力します。このアクセスルールがスイッチで有効または無効にされる場合の実行回数を設定します。
delete access_id <value 1-100>	作成済みの指定プロファイル ID のアクセスルールを削除します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

CPU アクセスリストエントリを設定します。

```
DGS-3200-10:4#config cpu access_profile profile_id 1 add access_id 1 ethernet vlan default port
1-3 deny
Command: config cpu access_profile profile_id 1 add access_id 1 ethernet vlan default port 1-3
deny

Success.

DGS-3200-10:4#
```

show cpu access_profile

目的

スイッチに設定されている現在の CPU アクセスプロファイルエントリを参照します。

構文

show cpu access_profile {profile_id <value 1-5>}

説明

スイッチに設定されている現在の CPU アクセスプロファイルエントリを表示します。

パラメータ

パラメータ	説明
profile_id<value 1-5>	削除するCPUアクセスプロファイルを識別する番号を1から5で指定します。この値はアクセスプロファイルが「create cpu access_profile」コマンドで作成される時に割り当てられます。

制限事項

なし。

使用例

スイッチに設定されている CPU フィルタリングリストを表示します。

```
DGS-3200-10:4#show cpu access_profile
Command: show cpu access_profile

CPU Interface Filtering State: Enabled

CPU Interface Access Profile Table

Total Unused Rule Entries:498
Total Used Rule Entries  :2

Access Profile ID: 1                                    Type : Ethernet
================================================================================
MASK Option :
VLAN         Source MAC
             FF-FF-FF-FF-FF-FF
-----------  -----------------

Access ID : 1              Mode: Deny
Ports     : 3
-----------  -----------------
default      00-01-02-03-04-05
================================================================================
Unused Entries: 99

Access Profile ID: 2                                    Type : IP
================================================================================
MASK Option :
Source IP MASK  TCP
255.255.255.255
--------------- -----------------

Access ID : 1              Mode: Deny
Ports     : 7
--------------- -----------------
1.1.1.1
================================================================================
Unused Entries: 99

DGS-3200-10:4#
```

enable/disable cpu_interface_filtering

目的

CPU インタフェースフィルタリングを有効または無効にします。

構文

enable cpu_interface_filtering

disable cpu_interface_filtering

説明

「enable cpu_interface_filtering」コマンドは CPU インタフェースフィルタリングを有効に、「disable cpu_interface_filtering」コマンドは無効にします。

パラメータ

なし

制限事項

なし。

使用例

CPU インタフェースフィルタリングを有効にします

```
DGS-3200-10:4#enable cpu_interface_filtering
Command: enable cpu_interface_filtering

Success.

DGS-3200-10:4#
```

CPU インタフェースフィルタリングを無効にします。

```
DGS-3200-10:4#disable cpu_interface_filtering
Command: disable cpu_interface_filtering

Success.

DGS-3200-10:4#
```

第 59 章　トラフィックコントロールコマンド

コンピュータネットワーク上にはマルチキャストパケットやブロードキャストパケットなどのパケットが正常な状態でも絶えずあふれています。このトラフィックはネットワーク上の端末の不良や、故障したネットワークカードなどのように誤動作しているデバイスによって増加することもあります。そのため、スイッチのスループットに関する問題が発生し、その結果、ネットワークの全体的なパフォーマンスにも影響する可能性があります。このパケットストームを調整するために、本スイッチは状況を監視し、制御します。

パケットストームを監視し、ユーザが指定したしきい値を基にパケットがネットワークにあふれているどうか判断します。パケットストームが検出されると本スイッチはパケットストームが緩和されるまで受信したパケットを破棄します。この方法を使用するためには、「action」フィールドの「Drop」オプションを設定します。スイッチのチップカウンタを監視することによりスイッチに入力するパケットのスキャンとモニタを行います。

スイッチのチップカウンタにはブロードキャストとマルチキャストパケット用のカウンタのみ存在するため、この方法はブロードキャストストームとマルチキャストストームに対してのみ有効です。ストームが検出されると（以下で設定するパケット数のしきい値を超過すると）、スイッチは STP BPDU パケットを除くすべてのトラフィックの入力に対して、「countdown」フィールドで指定した時間、ポートをシャットダウンします。本時間経過後もパケットストームが続くようであれば、そのポートは「Shutdown Forever」（永久シャットダウン）モードに遷移し、トラップレシーバに送信する警告メッセージを生成します。一度「Shutdown Forever」モードに入ると、本ポートを通常の状態に戻すには、無効になっているポートを手動で有効状態に戻すしか方法はありません。このようなストームコントロール機能を利用するためには、「action」フィールドで「shutdown」オプションを選択してください。

コマンドラインインタフェース（CLI）におけるトラフィックコントロールコマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
config traffic control	[<portlist> | all] {broadcast [enable | disable] | multicast [enable | disable] | unicast [enable | disable] | action [drop | shutdown] | threshold <value 512-1024000> | countdown [<value 0> | value 5-30>] | time_interval <value 5-30>}
config traffic trap	[none | storm_occurred | storm_cleared | both]
show traffic control	{<portlist>}

以下のセクションで各コマンドについて詳しく記述します。

config traffic control

目的

ブロードキャスト / マルチキャスト / ユニキャストトラフィックコントロールコマンドを設定します。ハードウェアストームコントロールに加え、ソフトウェアメカニズムがトラフィックレートのモニタをします。トラフィックレートが高過ぎると、このポートをシャットダウンします。

構文

config traffic control [<portlist> | all] {broadcast [enable | disable] | multicast [enable | disable] | unicast [enable | disable] | action [drop | shutdown] | threshold <value 512-1024000> | countdown [<value 0> | <value 5-30>] | time_interval <value 5-30> }

説明

ブロードキャスト / マルチキャスト / ユニキャストトラフィックコントロールコマンドを設定します。ブロードキャストストームコントロールコマンドでは、H/W ストームコントロールメカニズムだけが提供されますが、これらのトラフィックコントロールは H/W、S/W メカニズムを含み、シャットダウン、リカバリおよびトラップ通知機能を提供します。

パラメータ

パラメータ	説明
<portlist>	トラフィックコントロールを設定するポートまたは範囲を指定します。
all	すべてのポートにトラフィックコントロールを設定します。
broadcast [enable | disable]	ブロードキャストストームコントロールを「enable」（有効）または「disable」（無効）にします。
multicast [enable | disable]	マルチキャストストームコントロールを「enable」（有効）または「disable」（無効）にします。
unicast [enable | disable]	未知のユニキャストトラフィックコントロールを「enable」（有効）または「disable」（無効）にします。（「drop」アクションのみサポートします。）
action	トラフィックコントロールがスイッチに検出された場合に行うアクションを設定します。2 つのタイプを選択できます。 • drop - スイッチのハードウェアによるトラフィックコントロールを行います。選択すると、スイッチのハードウェアが指定したしきい値に基づくパケットストームの検知を行い、パケットストームが発生すると、状態が改善するまでパケットの廃棄を行います。 • shutdown - スイッチのソフトウェアによるトラフィックコントロールにより、トラフィックストームの発生を検知します。ストームが検出されると、スイッチはスパニングツリーの保持に必要である STP BPDU パケットを除くすべてのトラフィックの入力に対して、ポートをシャットダウンします。カウントタイマ経過後もパケットストームが続くようであれば、そのポートは「Shutdown Forever」（永久シャットダウン）モードに遷移します。一度「Shutdown Forever」モードに入ると、「config traffic control_recover」コマンドを使用して無効になっているポートを手動で有効状態に戻すまで、使用することはできません。本オプションを選択する際は、スイッチのチップからパケットカウントを受け取ってパケットストームの発生を検知するために必要な threshold（しきい値）、countdown（カウントダウン値）および time_interval（間隔）の設定も必要となります。

パラメータ	説明
threshold <value 512-1024000>	指定されたトラフィックコントロールが起動するしきい値の上限。ストームトラフィックコントロール測定のトリガーとなるスイッチが受信するブロードキャスト / マルチキャスト /dlf（Kbps）の値です。
countdown [<value 0> | <value 5-30>]	トラフィックストームが発生中のポートをシャットダウンするまでスイッチが待機する時間（分）を表します。本パラメータは、「action」フィールドで「shutdown」を指定し、ハードウェアによるトラフィックコントロールを行わない場合に有効です。 • 0 - 初期値は 0 で、ポートはシャットダウンされることはありません。 • 5-30 - シャットダウンするまでにスイッチが待機する時間（分）を 5-30 で指定します。「countdown」タイマ経過後もパケットストームが続くようであれば、そのポートは「Shutdown Forever」（永久シャットダウン）モードに遷移し、無効になっているポートを手動で有効状態に戻すまで使用することはできません。
time_interval <secs 5-30>	スイッチのチップからトラフィックコントロール機能に送信する、マルチキャストブロードキャストパケットカウントの送信間隔。このパケットカウントにより、いつ入力パケットがしきい値を超過したかが検出されます。 値の範囲は 5-30 です。本パラメータはアクションに「drop」（パケットの破棄）を選択している場合には関係ありません。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

トラフィックコントロールを設定し、ブロードキャストストームコントロールシステムを有効にします。

```
DGS-3200-10:4#config traffic control 1-10 broadcast enable action shutdown
threshold 512 time_interval 10
Command: config traffic control 1-10 broadcast enable action shutdown threshold
512 time_interval 10

Success.

DGS-3200-10:4#
```

config traffic trap

目的

トラフィックコントロールにトラップを設定します。

構文

config traffic trap [none | storm_occurred | storm_cleared | both]

説明

トラフィックストームイベントが S/W トラフィックストームコントロールメカニズムによって検出された場合、トラフィックストームコントロール通知を生成するかどうかを設定します。

注意 トラフィックコントロールトラップは、コントロールアクションが「shutdown」に設定されている場合にだけアクティブになります。コントロールアクションが「drop」の場合、ストームイベントが検出されてもトラップは発行されません。

パラメータ

パラメータ	説明
none	トラフィックコントロールメカニズムの動作に関わらず、ストームトラップメッセージを送信しません。
storm_occurred	ストームトラップ発生時にストームトラップメッセージを送信します。
storm_cleared	ストームトラップがクリアされる場合、スイッチはストームトラップメッセージを送信します。
both	ストームトラップ発生時がクリアされる場合、スイッチがストームトラップメッセージを送信します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

トラフィックコントロールを設定し、ブロードキャストトラフィックコントロールを有効にします。

```
DGS-3200-10:4#config traffic trap both
Command: config traffic trap both

Success.

DGS-3200-10:4#
```

show traffic control

目的

トラフィックコントロール設定を表示します。

構文

show traffic control {<portlist>}

説明

スイッチの現在のトラフィックコントロール設定を表示します。

パラメータ

パラメータ	説明
<portlist>	表示するポートまたはポート範囲を指定します。指定しないと、すべてのポートを表示します。

制限事項

なし。

使用例

トラフィックコントロール設定を表示します。

```
DGS-3200-10:4#show traffic control
Command: show traffic control

Traffic Storm Control Trap :[None]

Port Thres Broadcast Multicast Unicast  Action Count Time      Shutdown
     hold  Storm     Storm     Storm            down  Interval   Forever
---- ----- -------- ---------- -------- ----   ----- --------  ------------
1    512   Disabled Disabled   Disabled drop   0     5
2    512   Disabled Disabled   Disabled drop   0     5
3    512   Disabled Disabled   Disabled drop   0     5
4    512   Disabled Disabled   Disabled drop   0     5
5    512   Disabled Disabled   Disabled drop   0     5
6    512   Disabled Disabled   Disabled drop   0     5
7    512   Disabled Disabled   Disabled drop   0     5
8    512   Disabled Disabled   Disabled drop   0     5
9    512   Disabled Disabled   Disabled drop   0     5
10   512   Disabled Disabled   Disabled drop   0     5

DGS-3200-10:4#
```

付録 A パケットコンテンツ ACL を使用した ARP スプーフィング攻撃の軽減

ARP を動作させる方法

ARP（Address Resolution Protocol）は、IP アドレスだけがわかっている場合にホストのハードウェアアドレス（MAC アドレス）を検索するための標準的な方法です。しかし、クラッカーが ARP パケット内の IP および MAC 情報を偽造して LAN への攻撃（ARP スプーフィングとして、知られている）を行うために、このプロトコルは被害を受けやすいと言えます。ここでは ARP プロトコル、ARP スプーフィング攻撃、および D-Link スイッチが提供する ARP スプーフィング攻撃を防御する対策について紹介します。

ARP 処理中に、PC-A は、はじめに、PC-B の MAC アドレスを問い合わせする ARP リクエストを発行します。そのネットワーク構造は図 A-1 の通りです。

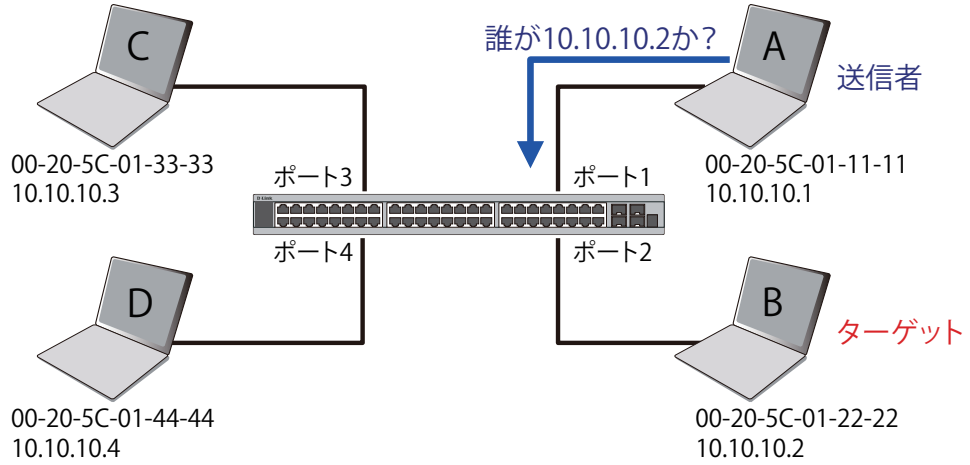


図 A-1

その間、PC-A の MAC アドレスは「送信側 H/W アドレス」に書かれ、その IP アドレスは ARP ペイロードの「送信側プロトコルアドレス」に書かれます。PC-B の MAC アドレスが未知である場合、「ターゲット H/W アドレス」は「00-00-00-00-00-00」であり、PC-B の IP アドレスは表 A-1 に示された「ターゲットプロトコルアドレス」に書かれます。

表 A-1　ARP ペイロード

H/W タイプ	プロトコルタイプ	H/W アドレス長	プロトコルアドレス長	操作	送信側 H/W アドレス	送信側プロトコルアドレス	ターゲット H/W アドレス	ターゲットプロトコルアドレス
				ARP request	*00-20-5C-01-11-11*	*10.10.10.1*	*00-00-00-00-00-00*	*10.10.10.2*

ARP リクエストはイーサネットフレームにカプセル化されて送信されます。表 A-2 の通り、イーサネットフレーム内の「送信元アドレス」は、PC-A の MAC アドレスとなります。ARP リクエストは、ブロードキャスト経由で送信されるため、イーサネットのブロードキャスト（FF-FF-FF-FF-FF-FF）のフォーマットには「宛先アドレス」があります。

表 A-2　イーサネットフレームフォーマット

宛先アドレス	送信元アドレス	Ether-type	ARP	FCS
FF-FF-FF-FF-FF-FF	*00-20-5C-01-11-11*			

スイッチがフレームを受信すると、イーサネットフレームヘッダの「送信元アドレス」をチェックします。アドレスがフォワーディングテーブルにないと、スイッチは学習して PC-A の MAC アドレスと関連ポートをフォワーディングテーブルに追加します。

フォワーディングテーブル	
ポート 1	*00-20-5C-01-11-11*

さらに、スイッチがブロードキャストされた ARP リクエストを受信すると、送信元ポート（図 A-2 ではポート 1）を除くすべてのポートにフレームをフラッドします。

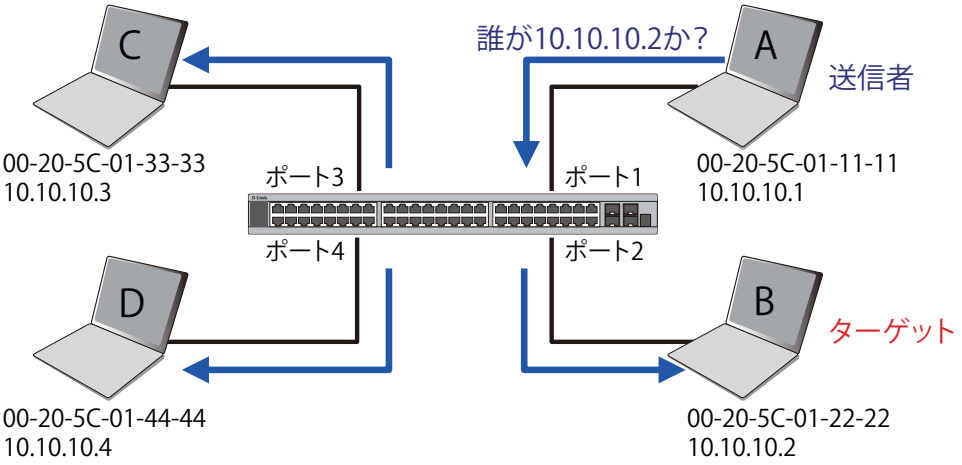


図 A-2

スイッチが ARP リクエストのフレームをネットワークにフラッドする場合、すべての PC が、フレームを受信し、検証を行いますが、PC-B だけが宛先 IP に一致するためにクエリに応答します（図 A-3 参照）。

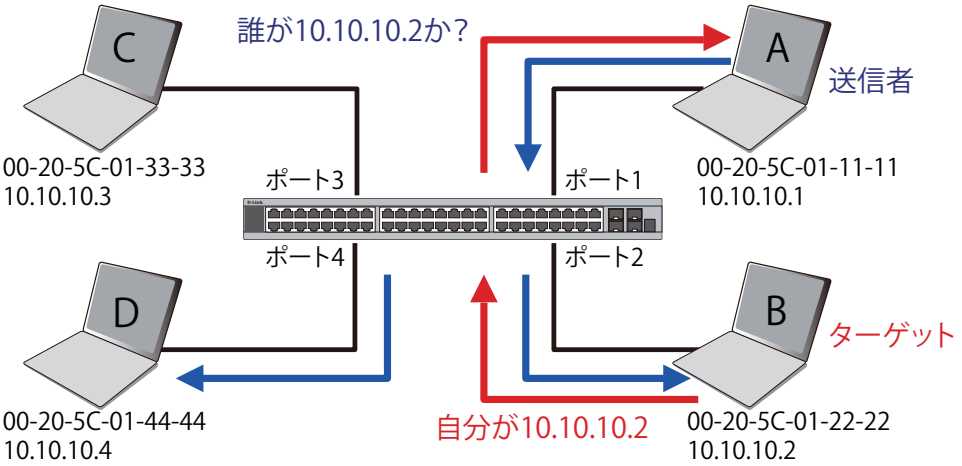


図 A-3

PC-B が ARP リクエストに応答すると、その MAC アドレスは表 A-3 に示されている ARP ペイロード内の「ターゲット H/W アドレス」に書かれます。ARP リプライは、次に、再びイーサネットフレームにカプセル化されて、送信側に返送されます。ARP リプライはユニキャスト通信の形式です。

表 A-3　ARP ペイロード

H/W タイプ	プロトコルタイプ	H/W アドレス長	プロトコルアドレス長	操作	送信側 H/W アドレス	送信側プロトコルアドレス	ターゲット H/W アドレス	ターゲットプロトコルアドレス
				ARP reply	00-20-5C-01-11-11	10.10.10.1	00-00-00-00-00-00	10.10.10.2

PC-B がクエリに応答する場合、イーサネットフレーム内の「宛先アドレス」は、PC-A の MAC アドレスに変更されます。「送信元アドレス」は PC-B の MAC アドレスに変更されます（表 A-4 参照）。

表 A-4　イーサネットフレームフォーマット

宛先アドレス	送信元アドレス	Ether-type	ARP	FCS
00-20-5C-01-11-11	00-20-5C-01-22-22			

スイッチは、また、イーサネットフレームの「送信元アドレス」を調べて、フォワーディングテーブルにはアドレスがないことを見つけます。スイッチは PC の MAC アドレスを学習してフォワーディングテーブルを更新します。

フォワーディングテーブル	
ポート 1	00-20-5C-01-11-11
ポート 2	00-20-5C-01-22-22

ARP スプーフィングがネットワークを攻撃する方法

また、ARP を汚染することで知られている ARP スプーフィングは、イーサネットネットワークを攻撃する方法で、DoS（Denial of Service）として知られているように、攻撃者は LAN 上のデータフレームをかぎつけて、トラフィックを編集、またはトラフィックを停止させてしまう可能性があります。ARP スプーフィングの原則は、偽造または改ざんした ARP メッセージをイーサネットネットワークに送信することです。一般的に、目的は、デフォルトゲートウェイなどの別のノードの IP アドレスに攻撃者の MAC アドレスかでたらめの MAC アドレスを割り当ててしまうことです。その IP アドレスに向かう予定だったトラフィックが、攻撃者に指定されたノードに誤ってリダイレクトされてます。

IP スプーフィング攻撃は、ホストが自身の IP アドレスを解決するため ARP リクエストを送信する場合に発生する Gratuitous ARP によって引き起こされます。図 A-4 は、LAN のハッカーによる ARP スプーフィング攻撃の開始を示しています。

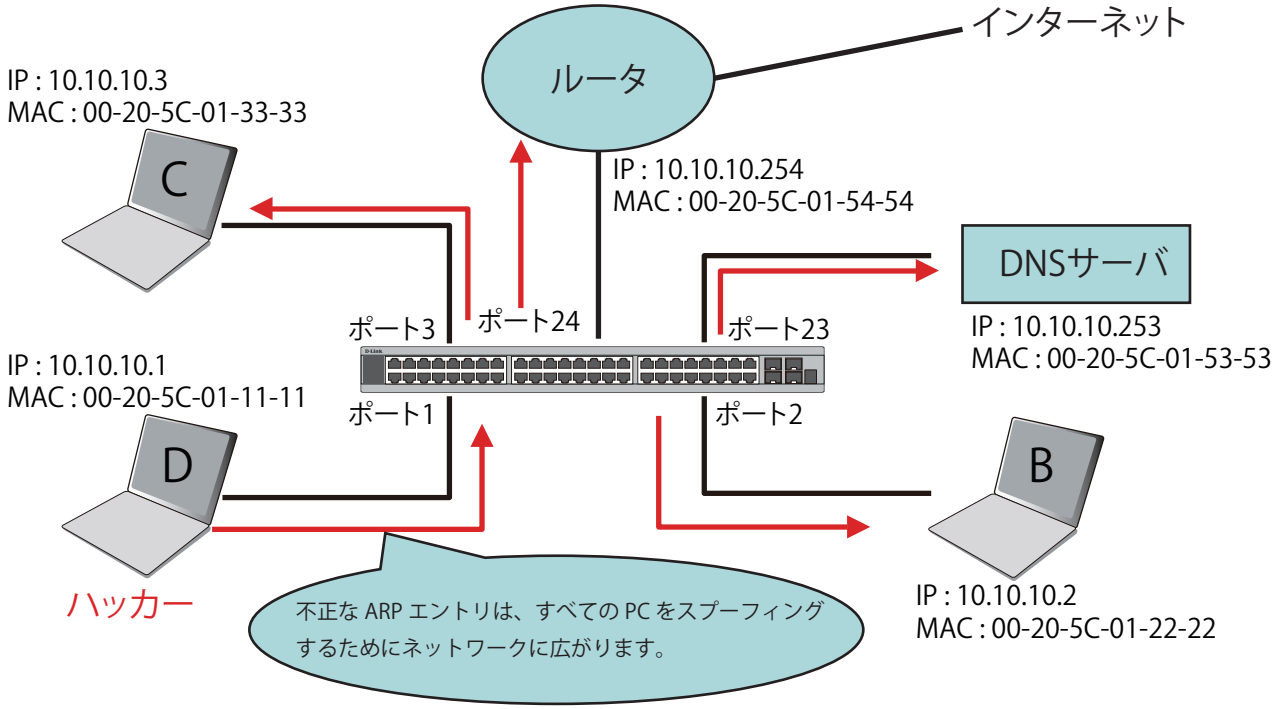


図 A-4

Gratuitous ARP パケットでは、「送信側プロトコルアドレス」と「ターゲットプロトコルアドレス」は同じ送信元 IP アドレスとなります。「送信側 H/W アドレス」と「ターゲット H/W アドレス」は同じ送信元 MAC アドレスとなります。宛先の MAC アドレスは、イーサネットブロードキャストアドレス（FF-FF-FF-FF-FF-FF）となります。ネットワーク内のすべてのノードは、送信側の MAC アドレスおよび IP アドレスに従って、直ちに自身の ARP テーブルを更新します。Gratuitous ARP の書式は以下の表の通りです。

表 A-5　Gratuitous ARP

イーサネットヘッダ			Gratuitous ARP								
宛先アドレス	送信元アドレス	イーサネットタイプ	H/W タイプ	プロトコルタイプ	H/W アドレス長	プロトコルアドレス長	操作	送信元 H/W アドレス	送信元プロトコルアドレス	ターゲット H/W アドレス	ターゲットプロトコルアドレス
6 バイト	6 バイト	2 バイト	2 バイト	2 バイト	1 バイト	1 バイト	2 バイト	6 バイト	4 バイト	6 バイト	4 バイト
FF-FF-FF-FF-FF-FF	*00-20-5C-01-11-11*	806					*ARP reply*	*00-20-5C-01-11-11*	*10.10.10.254*	*00-20-5C-01-11-11*	*10.10.10.254*

一般的な DoS 攻撃は、実在しない MAC アドレスやあらゆる指定 MAC アドレスをネットワークのデフォルトゲートウェイの IP アドレスに関連させることで行われます。悪意がある攻撃者は、一つの Gratuitous ARP をゲートウェイであると言っているネットワークに対してブロードキャストする必要があるだけであり、これによりすべてのネットワーク操作は、インターネットへの全パケットが間違ったノードに向けられるためにダウンさせられてしまいます。
同様に、攻撃者は、実際のデフォルトゲートウェイにトラフィックを転送する（パッシブスニッフィング）か、またはそれを転送する前にデータを更新する（man-in-the-middle 攻撃）を選択することが可能です。ハッカーは PC をだまし、犠牲者であるルータをだまします。図 A-5 で参照されるように、すべてのトラフィックはハッカーにスニッフィングされますが、ユーザはそれを発見できません。

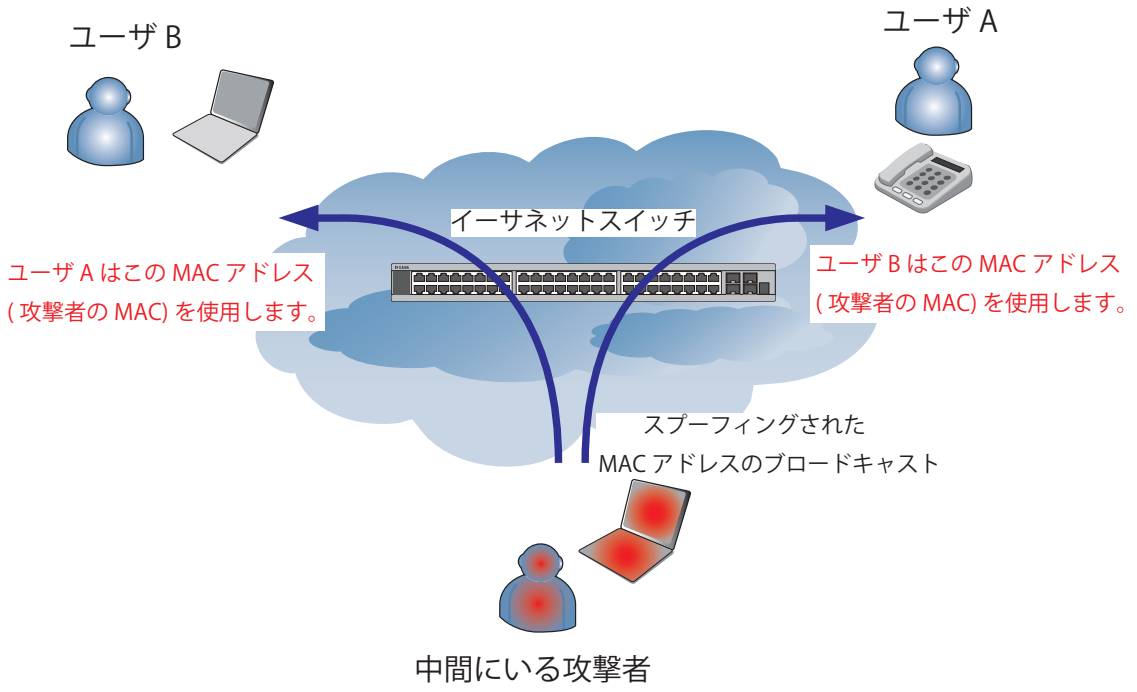


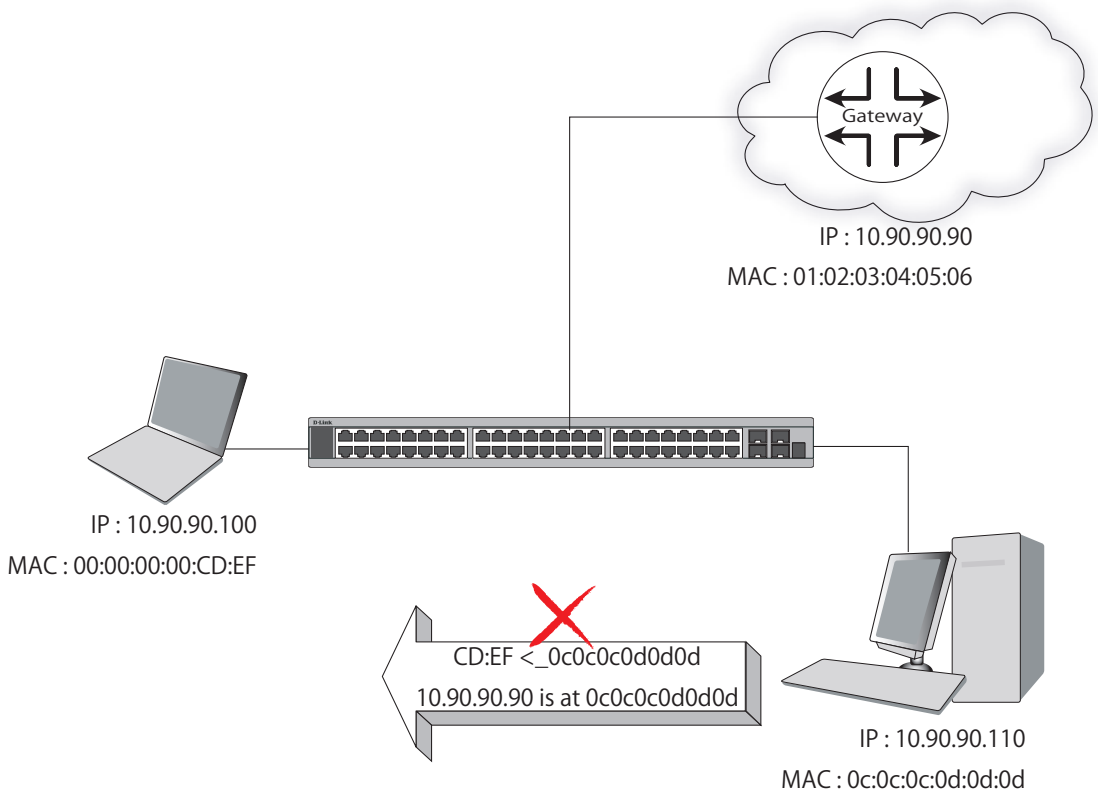
図 A-5

パケットコンテンツ ACL 経由で ARP スプーフィング攻撃を防止する

D-Link マネージドスイッチは、独自のパケットコンテンツ ACL 経由で ARP スプーフィングが引き起こした一般的な DoS を効果的に軽減することができます。基本的な ACL は、パケットタイプ、VLAN ID、送信元および送信先 MAC 情報に基づいて ARP パケットをフィルタするだけであるため、より詳細な ARP パケットの検証が必要となります。

ARP スプーフィング攻撃を防ぐために、スイッチでパケットコンテンツ ACL を使用し、偽造されたゲートウェイの MAC と IP バインディングを含む不正な ARP パケットを防御します。

トポロジの例題



設定

設定のロジックは以下の通りです。

1. ARP がイーサネットにおける送信元 MAC アドレスに一致する場合にだけ、ARP プロトコルの送信者の MAC アドレスと送信者の IP アドレスはスイッチを通過することができます。（この例では、ゲートウェイの ARP です。）
2. スイッチはゲートウェイの IP アドレスから来ていると言う他のすべての ARP パケットを拒否します。

スイッチのパケットコンテンツ ACL の設計により、ユーザはどんなオフセットチャンクも検証することができます。オフセットチャンクは 16 進数形式の 4 バイトのブロックであり、イーサネットフレーム内の各項目に一致させるために利用されます。各プロファイルは、最大 4 つのオフセットチャンクを持つことができます。その上、パケットコンテンツ ACL に 1 個のプロファイルだけがスイッチごとサポートされます。つまり、最大 16 バイトのオフセットチャンクが各プロファイルとスイッチに適用されます。そのため、有効なオフセットチャンクの計画と設定が必要とされます。

表 A-6 で、Offset_Chunk0 が 127 バイト目から開始し、128 バイト目で終了することにご注意ください。されに、オフセットチャンクが 0 ではなく、1 から抽出されることがわかります。

表 A-6　チャンクとパケットオフセット

Offset Chunk	Offset Chunk0	Offset Chunk1	Offset Chunk2	Offset Chunk3	Offset Chunk4	Offset Chunk5	Offset Chunk6	Offset Chunk7	Offset Chunk8	Offset Chunk9	Offset Chunk10	Offset Chunk11	Offset Chunk12	Offset Chunk13	Offset Chunk14	Offset Chunk15
バイト	127	3	7	11	15	19	23	27	31	35	39	43	47	51	55	59
バイト	128	4	8	12	16	20	24	28	32	36	40	44	48	52	56	60
バイト	1	5	9	13	17	21	25	29	33	37	41	45	49	53	57	61
バイト	2	6	10	14	18	22	26	30	34	38	42	46	50	54	58	62

Offset Chunk	Offset Chunk15	Offset Chunk16	Offset Chunk17	Offset Chunk18	Offset Chunk19	Offset Chunk20	Offset Chunk21	Offset Chunk22	Offset Chunk23	Offset Chunk24	Offset Chunk25	Offset Chunk26	Offset Chunk27	Offset Chunk28	Offset Chunk29	Offset Chunk30
バイト	63	67	71	75	79	83	87	91	95	99	103	107	111	115	119	123
バイト	64	68	72	76	80	84	88	92	96	100	104	108	112	116	120	124
バイト	65	69	73	77	81	85	89	93	97	101	105	109	113	117	121	125
バイト	66	70	74	78	82	86	90	94	98	102	106	110	114	118	122	126

以下の表は、パケットオフセットの計算のためのパターンであるイーサネットフレームに含まれる完全な ARP パケットを示しています。

表 A-7　イーサネットフレームに含まれる完全な ARP パケット

イーサネットヘッダ			ARP								
宛先アドレス	送信元アドレス	イーサネットタイプ	H/W タイプ	プロトコルタイプ	H/W アドレス長	プロトコルアドレス長	操作	送信元 H/W アドレス	送信元プロトコルアドレス	ターゲット H/W アドレス	ターゲットプロトコルアドレス
6 バイト	6 バイト	2 バイト	2 バイト	2 バイト	1 バイト	1 バイト	2 バイト	6 バイト	4 バイト	6 バイト	4 バイト
01 02 03 04 05 06	0806								0a5a5a5a (10.90.90.90)		

	コマンド	記述
手順 1	create access_profile profile_id 1 ethernet source_mac FF-FF-FF-FF-FF-FF ethernet_type	• 「イーサネットタイプ」と「送信元 MAC アドレス」を一致させるアクセスプロファイル 1 を作成します。
手順 2	config access_profile profile_id 1 add access_id1 ethernet source_mac 01-02-03-04-04-06 ethernet_type 0x806 port 1-27 permit	• アクセスプロファイル 1 を設定します。 • ゲートウェイの ARP パケットがイーサネットフレームに正しい「送信元 MAC」を持っている場合だけスイッチを通過できます。
手順 3	create access_profile profile_id 2 packet_content_mask offset_chunk_1 3 0x0000FFFF ↑ イーサネットタイプ（1 バイト）: ARP offset_chunk_2 7 0x0000FFFF ↑ Sdr IP（始め 2 バイト） offset_chunk_3 8 0x0000FFFF ↑ Sdr IP（最後 2 バイト）	• アクセスプロファイル 2 を作成します。 • ２つ目のチャンクは Chunk7 から開始します。 :「イーサネットタイプ」のマスク（表 A-6 : 13/14 バイト目の青色部分） • 1 つ目のチャンクは Chunk3 から開始します。 : ARP パケットの「Sender IP」（始め 2 バイト）のマスク（表 A-6 : 29/30 バイト目の緑色部分） • 1 つ目のチャンクは Chunk8 から開始します。 : ARP パケットの「Sender IP」（最後 2 バイト）のマスク（表 A-6 : 31/32 バイト目の茶色部分）
手順 4	config access_profile profile_id 2 add access_id 1 packet_content offset_chunk_1 0x00000806 ↑ イーサネットタイプ（1 バイト）: ARP offset_chunk_2 0x00000A5A ↑ Sdr IP（始め 2 バイト）: 10.90 offset_chunk_3 0x5A5A0000 ↑ Sdr IP（最後 2 バイト）: 90.90 port 1-27 deny	• アクセスプロファイル 2 を設定します。 • 「Sender IP」がゲートウェイの IP であると言う残りの ARP パケットは廃棄されます。
手順 5	save	• 設定を保存します。

付録 B パスワードリカバリ手順

ここでは、弊社スイッチのパスワードのリセットについて記述します。ネットワークにアクセスを試みるすべてのユーザに認証は必要で重要です。権限のあるユーザを受け入れるために使用する基本的な認証方法は、ローカルログイン時にユーザ名とパスワードを利用するこうとです。時々パスワードが忘れられたり、壊れたりするため、ネットワーク管理者は、これらのパスワードをリセットする必要があります。ここでは、パスワードリカバリ機能は、そのような場合にネットワーク管理者を助けるものです。以下の手順で、容易にパスワードを回復するパスワードリカバリ機能の使用方法を説明します。

これらの手順を終了するとパスワードはリセットされます。

1. セキュリティの理由のため、パスワードリカバリ機能は物理的にデバイスにアクセスすることが必要です。そのため、デバイスのコンソールポートへの直接接続を行っている場合だけ、本機能を適用することが可能です。ユーザは端末エミュレーションソフトを使用して、スイッチのコンソールポートに端末または PC を接続する必要があります。

2. 電源をオンにします。runtime image が 100% までロードされた後に、「Password Recovery Mode」に入るために、2 秒以内に、ホットキー「 ^ 」（シフト +6）を押します。「Password Recovery Mode」に一度入ると、スイッチのすべてのポートが無効になります。

```
Boot Procedure                                                    V1.00.B012
--------------------------------------------------------------------------------
Power On Self Test ..................................... 100%
MAC Address : 00-19-5B-EC-32-15
H/W Version : A2

Please wait, loading V1.50.B019 Runtime image.............. 00%
The switch is now entering Password Recovery Mode:_
```

```
The switch is currently in Password Recovery Mode.
>
```

3. 「Password Recovery Mode」では、以下のコマンドのみ使用できます。

コマンド	説明
reset config	リセットし、全設定を工場出荷時設定に戻します。
reboot	「Password Recovery Mode」を終了し、スイッチを再起動します。現在の設定を保存するように確認メッセージが表示されます。
reset account	作成済みのアカウントのすべてを削除します。
reset password	指定ユーザのパスワードをリセットします。
{<username>}	ユーザ名を指定しないと、すべてのユーザのパスワードがリセットされます。
show account	設定済みのすべてのアカウントを表示します。