SG2024/PoE/G

Manual Appendix

(1.3.5 ~ 1.4.4)

Rev.2

20100526JP_01

HANDREAMNET
JAPAN

発行日:2010年5月26日

---------- マニュアルバージョン ----------

1. 2010年4月20日　Rev.1　初版（F/Wバージョン 1.3.5～1.4.4）
   - コマンドの追加・更新
2. 2010年5月26日　Rev.2　二版（初版の改定）
   - コマンドの追加(22～25項目)

目　　次

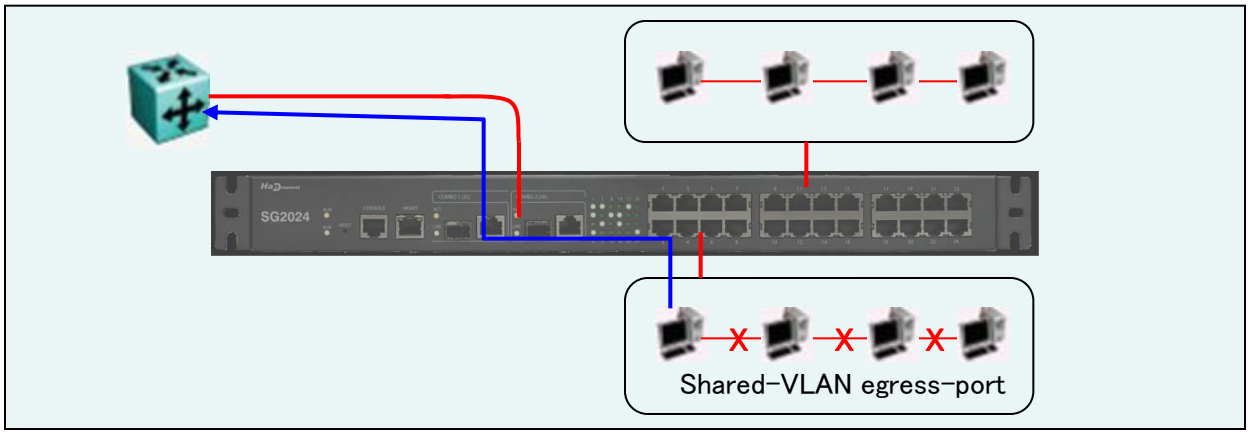
第1章 新機能

1.1 shared-egress port

Shared VLAN egress portで設定されたインタフェースは、Uplink以外のインタフェースから転送されるUnicast、Multicast、Broadcastなど全ての通信が届きません。

この機能は同じNetwork上にいてもセキュリティ上、通信を制限する必要がある場合、使用します。例えば、ホテルで個室別に通信を行わせる場合、またはデータセンターの中で一つのスイッチに接続されていつARP Spoofingの脅威が発生する可能性がある場合。

[図1-1] Shared VLAN egress-port Trafficの流れ



Shared VLAN egress-portを設定するためには、下記のコマンドをご使用ください。

コマンド	モード	機　能
interface range *port-range*	CONFIG	Port Rangeを選択します。
switchport shared-vlan egress-port *IFNAME*	INTERFACE	特定のインタフェイスをegressポートのUplinkとして設定します。

作成されたVLAN及びMember情報を確認するためには、下記のコマンドをご使用ください。

コマンド	モード	機　能
show vlan <2-4094>	TOP	特定のVLAN情報を確認します。
show vlan all bridge 1	TOP	全てのVLAN情報を確認します。
show vlan brief	TOP	全てのVLAN情報を確認します。

Shared VLANを初期化するためには、下記のコマンドをご使用ください。

コマンド	モード	機　能
no switchport shared-vlan egress-port	INTERFACE	設定されたVLAN egress-portを初期化します。

<例題1> Shared VLAN egress-portの設定
fe1-24 : インタフェース間の通信は制限。各、インタフェースはge1との通信のみ、可能

```
SG2024#configure terminal
SG2024(config)#interface range fe
% fe Selected
SG2024(config-if-range)#switchport shared-vlan egress-port ge1
% fe Selected
SG2024(config-if-range)#end
SG2024#show running-config
!
service password-encryption
!
username root password 8 4DBfucrfjXL6o
!
ip domain-lookup
!
spanning-tree mst config
!
maximum-paths 8
bridge 1 protocol rstp vlan-bridge
bridge 1 acquire
mls qos enable
mds enable fe detect
mds uplink ge
!interface fe1
 bridge-group 1
 switchport mode access
 switchport mode access acceptable-frame-type all
 switchport shared-vlan egress-port ge1
!
interface fe2
 bridge-group 1
 switchport mode access
 switchport mode access acceptable-frame-type all
 switchport shared-vlan egress-port ge1
!
--- 以下省略 ---
```

参考	shared egress-portは fe(ge)1-24、po1-6、sa1-6のインタフェースの中で最大2個まで設定することができます。

<例題2> Shared VLAN egress-portの設定
fe1-12 : I Interface間の通信許容 。
fe13-24 : Interface間の通信制限。
　　全てのTrafficはge1 Interfaceを通さなければ通信できないように設定。

```
SG2024(config)#vlan database
SG2024(config-vlan)#vlan 10 bridge 1 state enable
SG2024(config-vlan)#vlan 20 bridge 1 state enable
SG2024(config-vlan)#vlan 30 bridge 1 state enable
SG2024(config-vlan)#shared-vlan 30 block
SG2024(config-vlan)#exit
SG2024(config)#interface range all
% all Selected
SG2024(config-if-range)#switchport mode hybrid
% all Selected
SG2024(config-if-range)#switchport hybrid allowed vlan add 30 egress-tagged disable
% all Selected
SG2024(config-if-range)#exit
SG2024(config)#interface range fe1-12
% fe1-12 Selected
SG2024(config-if-range)#switchport hybrid vlan 10
% fe1-12 Selected
SG2024(config-if-range)#exit
SG2024(config)#interface range fe13-24
% fe13-24 Selected
SG2024(config-if-range)#switchport hybrid vlan 20
% fe13-24 Selected
SG2024(config-if-range)#exit
SG2024(config)#interface range ge
% ge Selected
SG2024(config-if-range)#switchport mode hybrid
% ge Selected
SG2024(config-if-range)#switchport hybrid vlan 30
% ge Selected
SG2024(config-if-range)#switchport hybrid allowed vlan add 10 egress-tagged disable
% ge Selected
SG2024(config-if-range)#switchport hybrid allowed vlan add 20 egress-tagged disable
% ge Selected
SG2024(config-if-range)#exit
SG2024(config)#interface range fe13-24
% fe13-24 Selected
SG2024(config-if-range)#switchport shared-vlan egress-port ge1
% fe13-24 Selected
SG2024(config-if)#end
SG2024#
```

1.2 Voice VLAN

Voice VLAN機能で設定するVoiceトラフィック（特定VLANまたはMAC OUI)の場合、
リアルタイムで転送しなければ、遅延による通話品質の低下、または通信切れに繋がります。
そこでVoice VLANに設定したトラフィックに対して自動的に優先順位を上げて
一般のデータトラフィックより優先的に転送する機能です。

Voice　VLANの設定は該当インタフェースがHybridモードの場合、可能となります。

インタフェースにVoice VLANを設定するとSYSLOGに該当インタフェースのLLDP-MED機能が活性化された内容のイベントが記録されて自動に有効になります。
これでLLDP-MEDのポリシーパケット及びCDPパケットが転送されます。(CDPの場合はは自動に有効になりませんので、必要な場合、別度CDPを有効にします。)

LLDP-MEDパケットはVLAN,タグ,基本優先順位, DSCPオプションなどを含めて転送されて
LLDP-MED パケットの受信設定が有効になったIP電話では自動に設定変更になります。

解除の場合はインタフェースに設定されているVoice VLANとLLDPをそれぞれ別度解除する必要があります。

-vlan VID: Voice VLANに該当するトラフィックは<vlan-id> が付くTagged Frame(CoS5)を転送し、Dataトラフィック(CoS0) はuntagged Frameになっており、VoiceトラフィックがDataトラフィックより優先転送されます。

-untagged :Voiceトラフィックもuntagged Frame (vlan-id4095)として転送されます。

-dot1p :VoiceトラフィックはPriority Tagged Frame (vlan-id 0, CoS5), Dataトラフィックは
untagged Frameに転送されます。

Voice　VLANを設定するためには、下記のコマンドをご使用ください。

コマンド	モード	機　能
switchport voice vlan {*VLANID* | dot1p | untagged}	INTERFACE	InterfaceをVoice VLANメンバーとして設定します。
voice-vlan oui *MAC_OUI* [*Description*]	CONFIG	特定MAC OUIをVoice VLANに設定します。
voice-vlan med {dscp <0-63> | priority <0-7>}	CONFIG	LLDP-MEDを介してVoice VLAN 転送Packetの値を設定します。 (Default : dscp 46, priority 5)

Voice　VLAN情報を確認するためには、下記のコマンドをご使用ください。

コマンド	モード	機　能
show voice-vlan oui	TOP	Voice VLANに指定されたMAC OUIを確認します。

Voice　VLANを初期化するためには、下記のコマンドをご使用ください。

コマンド	モード	機　能
no switchport voice vlan	INTERFACE	InterfaceをVoice VLANメンバーから解除します。
no voice-vlan oui *MAC_OUI*	CONFIG	特定MAC OUIをVoice VLANから解除します。
no voice-vlan med {dscp | priority}	CONFIG	LLDP-MEDを利用した Voice VLAN 転送パケットの値(CoS、LLDP)を初期化します。

 参考	voice vlan設定はインタフェースのhybridモードのみ可能

<예題> Voice VLAN設定

```
SG2024G#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SG2024G(config)#vlan database
SG2024G(config-vlan)#vlan 10 bridge 1 state enable
SG2024G(config-vlan)#exit
SG2024G(config)#voice-vlan oui 00-00-01
SG2024G(config)#
SG2024G(config)#interface range ge1-2
% ge1-2 Selected
SG2024G(config-if-range)#switchport mode hybrid
% ge1-2 Selected
SG2024G(config-if-range)#switchport voice vlan dot1p
% ge1-2 Selected
SG2024G(config-if-range)#end
SG2024G#show voice-vlan oui
================================================================================
 Telephony OUI(s)   Description
--------------------------------------------------------------------------------
 00-00-01-00-00-00
--------------------------------------------------------------------------------
SG2024G#show vlan brief
                                    Bridge Group : 1

VLAN ID    Name             State   Member ports (u)-Untagged, (t)-Tagged
========= ================ ======= ============================================
1          default          ACTIVE  ge3(u) ge4(u) ge5(u) ge6(u) ge7(u) ge8(u)
                                    ge9(u) ge10(u) ge11(u) ge12(u) ge13(u)
                                    ge14(u) ge15(u) ge16(u) ge17(u) ge18(u)
                                    ge19(u) ge20(u) ge21(u) ge22(u) ge23(u)
                                    ge24(u) ge1(u) ge2(u)
10         VLAN0010         ACTIVE

SG2024G#
SG2024G#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SG2024G(config)#interface range ge1-2
% ge1-2 Selected
SG2024G(config-if-range)#switchport voice vlan 10
SG2024G(config-if-range)#end
SG2024G#show vlan brief
                                    Bridge Group : 1

VLAN ID    Name             State   Member ports (u)-Untagged, (t)-Tagged
========= ================ ======= ============================================
1          default          ACTIVE  ge3(u) ge4(u) ge5(u) ge6(u) ge7(u) ge8(u)
                                    ge9(u) ge10(u) ge11(u) ge12(u) ge13(u)
                                    ge14(u) ge15(u) ge16(u) ge17(u) ge18(u)
                                    ge19(u) ge20(u) ge21(u) ge22(u) ge23(u)
                                    ge24(u) ge1(u) ge2(u)
10         VLAN0010         ACTIVE  ge1(t) ge2(t)

SG2024G#
```

1.3 PVSTP

スイッチ間のループを防ぐスパニングツリーはスイッチ同士の物理的LINKに基づいて
一つのツリーで動作を行っています。
この際、物理的なツリー構造である場合、別のVLANトラフィックとしても一つの
物理的なツリーの中で常に一つのLINKはブロック状態になっているので、全てのトラフィックが
ブロック状態のリンクの他に集中されます。
これを改善した方式がVLANごとにスパニングツリーを動作して負荷を分散する仕組みで
PVST(Per VLAN Spanning Tree)と言います。

PVSTはCST(Common Spanning Tree)を使用するデバイスとは互いにSTP BPDUを
処理できないため、併用はできません。
※ CST : 一つのスパニングツリーを使用する方式
PVSTを改善するためのPVSTPはPVCSTで受信したBPDU情報をPVSTに転送する時、VLANごと
に繰り返して転送するかまたはトンネリングで隣接していないPVST間の連結を許可します。

PVSTPの中でSpanning Tree Protocolに STP BPDUを転送し、PVSTPモードではRSTP BPDUを
転送する方式をPVSTP+ またはPVRSTPと言います。スイッチではPVSTPの設定時、
デフォルトとしてRSTP BPDUを転送しており、PVSTPでサポートしている最大の
スパニングツリーの数は31個になります。

1.3.1 PVSTPモードを設定するためには、下記のコマンドをご使用ください。

コマンド	モード	機　能
bridge 1 protocol pvstp	CONFIG	スイッチをPVSTPモードに選択します。

<例題1> PVSTPモード設定

```
SG2024G(config)#bridge 1 protocol pvstp
SG2024G(config)#end
```

1.3.2 PVSTPを有効に設定するためには、下記のコマンドをご使用ください。

コマンド	モード	機　能
bridge 1 pvstp enable	CONFIG	PVSTPを有効にします。

<例題2> PVSTPを有効設定

```
SG2024G(config)#bridge 1 pvstp enable
SG2024G(config)#end
```

1.3.3 PVSTPでルートスイッチ選定するためには、下記のコマンドをご使用ください。

コマンド	モード	機 能
bridge 1 pvstp vlan *VLANID* priority <0-61440>	CONFIG	PVSTPの特定のVLANの優先順位を変更します。

1.3.3 PVSTPでルートスイッチの優先順位を初期化するためには、下記のコマンドをご使用ください。

コマンド	モード	機 能
no bridge 1 pvstp vlan *VLANID* priority	CONFIG	PVSTPの特定のVLANの優先順位を初期化します。

<例題3> PVSTP優先順位(priority)変更

```
SG2024G(config)#brige 1 pvstp vlan 1 priority 16384
SG2024G(config)#end
SG2024G#show spanning-tree pvstp

VLAN1
  Spanning Tree Enabled protocol PVSTP
  Root Path Cost 0 - Priority 16385 (priority 16384 sys-id-ext 1)
  Root Id 4001001af410010c
    Forward Delay 15 - Hello Time 2 - Max Age 20 - Root Port 0
  Bridge Id 4001001af410010c
    Forward Delay 15 - Hello Time 2 - Max Age 20

Interface  Role       State             Path-cost  Priority   Rcv   Send
---------- ---------- ----------------- ---------- ---------- ----- -----
ge1        Designated Forwarding        19         128        None  RSTP


SG2024G#
```

参考	priorityは4096の倍数を入力

1.3.4 PVSTPでパスコストを設定るためには、下記のコマンドをご使用ください。

コマンド	モード	機　能
bridge-group 1 path-cost <1-200000000>	INTERFACE	該当インタフェースのパスコストを変更します。

1.3.4 PVSTPでパスコストを初期化するためには、下記のコマンドをご使用ください。

コマンド	モード	機　能
no bridge-group 1 path-cost	INTERFACE	該当インタフェースのパスコストを初期化します。

<例題4> パスコスト(path-cost)変更

```
SG2024G(config)#interface ge1
SG2024G(config-if)#bridge-group 1 path-cost 10000
SG2024G(config-if)#end
SG2024G#show spanning-tree pvst pinterface ge1

Vlan       Role       State             Path-cost  Priority
---------- ---------- ----------------- ---------- ----------
VLAN1      Designated Forwarding        10000      128

SG2024G#
```

1.3.5 PVSTPでポートプライオリティを設定るためには、下記のコマンドをご使用ください。

コマンド	モード	機　能
bridge-group 1 priority <0-240>	INTERFACE	該当インタフェースのポートプライオリティを変更します。

1.3.5 PVSTPでポートプライオリティを初期化するためには、下記のコマンドをご使用ください。

コマンド	モード	機　能
no bridge-group 1 priority	INTERFACE	該当インタフェースのポートプライオリティを初期化します。

<例題5> ポートプライオリティ(port-priority)変更

```
SG2024G(config)#interface ge1
SG2024G(config-if)#bridge-group 1 priority 16
SG2024G(config-if)#end
SG2024G#show spanning-tree pvstp interface ge1

Vlan       Role       State             Path-cost  Priority
---------- ---------- ----------------- ---------- ----------
VLAN1      Designated Forwarding        10000      16

SG2024G#
```

参考	port-priorityは16の倍数を入力

1.3.6 PVSTP情報を確認するためには、下記のコマンドをご使用ください。

コマンド	モード	機　能
show spanning-tree pvstp <detail | Interface | summary | vlan>	TOP	PVSTP設定情報を確認します。

1.3.7 PVSTP情報を初期化するためには、下記のコマンドをご使用ください。

コマンド	モード	機　能
no bridge 1 pvstp enable bridge-forward bpdu-flood	CONFIG	PVSTPを無効に設定します。 また、BPDUを受信し、フラッディングします。

<例題6> PVSTP設定
SG2024G-1スイッチ, SG2024G-2スイッチのge23-24を連結後、PVSTP設定
SG2024G-2スイッチのVLAN 5のプライオリティ(priority)を4096に変更

```
================================================================================
                                  SG2024G-1
================================================================================
SG2024G-1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SG2024G-1(config)#vlan database
SG2024G-1(config-vlan)#vlan range 4-5 bridge 1
SG2024G-1(config-vlan)#exit
SG2024G-1(config)#bridge 1 protocol pvstp
SG2024G-1(config)#bridge 1 pvstp enable
SG2024G-1(config)#bridge 1 pvstp vlan 4-5
SG2024G-1(config)#interface range ge23-24
% ge23-24 Selected
SG2024G-1(config-if-range)#switchport mode trunk
% ge23-24 Selected
SG2024G-1(config-if-range)#switchport trunk allowed vlan add 4-5
% ge23-24 Selected
SG2024G-1(config-if-range)#exit
SG2024G-1(config)#interface range ge1-12
% ge1-12 Selected
SG2024G-1(config-if-range)#switchport access vlan 4
% ge1-12 Selected
SG2024G-1(config-if-range)#exit
SG2024G-1(config)#interface range ge13-22
% ge13-22 Selected
SG2024G-1(config-if-range)#switchport access vlan 5
% ge13-22 Selected
SG2024G-1(config-if-range)#end
SG2024G-1#show spanning-tree pvstp summary

portfast bpdu-filter disabled
portfast bpdu-guard disabled
portfast errdisable timeout enabled
portfast errdisable timeout interval 300 sec

Name     Blocking Listening Learning Forwarding STP Active
-------- -------- --------- -------- ---------- ----------
VLAN1    0        0         0        2          2
VLAN4    0        0         0        2          2
VLAN5    1        0         0        1          2
-------- -------- --------- -------- ---------- ----------
3 vlans  1        0         0        5          6

SG2024G-1#
```

```
SG2024G-1#show spanning-tree pvstp

VLAN1
  Spanning Tree Enabled protocol PVSTP
  Root Path Cost 0 - Priority 32769 (priority 32768 sys-id-ext 1)
  Root Id 8001001af4000300
    Forward Delay 15 - Hello Time 2 - Max Age 20 - Root Port 0
  Bridge Id 8001001af4000300
    Forward Delay 15 - Hello Time 2 - Max Age 20

Interface  Role       State             Path-cost  Priority   Rcv   Send
---------- ---------- ----------------- ---------- ---------- ----- -----
ge24       Designated Forwarding        4          128        RSTP  RSTP
ge23       Designated Forwarding        4          128        RSTP  RSTP


VLAN4
  Spanning Tree Enabled protocol PVSTP
  Root Path Cost 0 - Priority 32772 (priority 32768 sys-id-ext 4)
  Root Id 8004001af4000300
    Forward Delay 15 - Hello Time 2 - Max Age 20 - Root Port 0
  Bridge Id 8004001af4000300
    Forward Delay 15 - Hello Time 2 - Max Age 20

Interface  Role       State             Path-cost  Priority   Rcv   Send
---------- ---------- ----------------- ---------- ---------- ----- -----
ge24       Designated Forwarding        4          128        RSTP  RSTP
ge23       Designated Forwarding        4          128        RSTP  RSTP


VLAN5
  Spanning Tree Enabled protocol PVSTP
  Root Path Cost 4 - Priority 32773 (priority 32768 sys-id-ext 5)
  Root Id 1005001af40003aa
    Forward Delay 15 - Hello Time 2 - Max Age 20 - Root Port 5025
  Bridge Id 8005001af4000300
    Forward Delay 15 - Hello Time 2 - Max Age 20

Interface  Role       State             Path-cost  Priority   Rcv   Send
---------- ---------- ----------------- ---------- ---------- ----- -----
ge24       Alternate  Discarding        4          128        RSTP  RSTP
ge23       Rootport   Forwarding        4          128        RSTP  RSTP


SG2024G#
```

```
================================================================================
                                SG2024G-2
================================================================================
SG2024G-2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SG2024G-2(config)#vlan database
SG2024G-2(config-vlan)#vlan range 4-5 bridge 1
SG2024G-2(config-vlan)#exit
SG2024G-2(config)#bridge 1 protocol pvstp
SG2024G-2(config)#bridge 1 pvstp enable
SG2024G-2(config)#bridge 1 pvstp vlan 4-5
SG2024G-2(config)#bridge 1 pvstp vlan 5 priority 4096
SG2024G-2(config)#
SG2024G-2(config)#interface range ge23-24
% ge23-24 Selected
SG2024G-2(config-if-range)#switchport mode trunk
% ge23-24 Selected
SG2024G-2(config-if-range)#switchport trunk allowed vlan add 4-5
% ge23-24 Selected
SG2024G-2(config-if-range)#exit
SG2024G-2(config)#interface range ge1-12
% ge1-12 Selected
SG2024G-2(config-if-range)#switchport access vlan 4
% ge1-12 Selected
SG2024G-2(config-if-range)#exit
SG2024G-2(config)#interface range ge13-22
% ge13-22 Selected
SG2024G-2(config-if-range)#switchport access vlan 5
% ge13-22 Selected
SG2024G-2(config-if-range)#end
SG2024G-2#show spanning-tree pvstp summary

portfast bpdu-filter disabled
portfast bpdu-guard disabled
portfast errdisable timeout enabled
portfast errdisable timeout interval 300 sec

Name     Blocking Listening Learning Forwarding STP Active
-------- -------- --------- -------- ---------- ----------
VLAN1    1        0         0        1          2
VLAN4    1        0         0        1          2
VLAN5    0        0         0        2          2
-------- -------- --------- -------- ---------- ----------
3 vlans  2        0         0        4          6

SG2024G-2#
```

```
SG2024G-2#show spanning-tree pvstp

VLAN1
  Spanning Tree Enabled protocol PVSTP
  Root Path Cost 4 - Priority 32769 (priority 32768 sys-id-ext 1)
  Root Id 8001001af4000300
    Forward Delay 15 - Hello Time 2 - Max Age 20 - Root Port 5025
  Bridge Id 8001001af40003aa
    Forward Delay 15 - Hello Time 2 - Max Age 20

Interface  Role       State            Path-cost  Priority   Rcv   Send
---------- ---------- ---------------- ---------- ---------- ----- -----
ge24       Alternate  Discarding       4          128        RSTP  RSTP
ge23       Rootport   Forwarding       4          128        RSTP  RSTP


VLAN4
  Spanning Tree Enabled protocol PVSTP
  Root Path Cost 4 - Priority 32772 (priority 32768 sys-id-ext 4)
  Root Id 8004001af4000300
    Forward Delay 15 - Hello Time 2 - Max Age 20 - Root Port 5025
  Bridge Id 8004001af40003aa
    Forward Delay 15 - Hello Time 2 - Max Age 20

Interface  Role       State            Path-cost  Priority   Rcv   Send
---------- ---------- ---------------- ---------- ---------- ----- -----
ge24       Alternate  Discarding       4          128        RSTP  RSTP
ge23       Rootport   Forwarding       4          128        RSTP  RSTP


VLAN5
  Spanning Tree Enabled protocol PVSTP
  Root Path Cost 0 - Priority 4101 (priority 4096 sys-id-ext 5)
  Root Id 1005001af40003aa
    Forward Delay 15 - Hello Time 2 - Max Age 20 - Root Port 0
  Bridge Id 1005001af40003aa
    Forward Delay 15 - Hello Time 2 - Max Age 20

Interface  Role       State            Path-cost  Priority   Rcv   Send
---------- ---------- ---------------- ---------- ---------- ----- -----
ge24       Designated Forwarding       4          128        RSTP  RSTP
ge23       Designated Forwarding       4          128        RSTP  RSTP

SG2024G-2#
```

1.4 Port Security

Port Securityは特定MACアドレスをMACテーブルにスタティックで登録する機能です。
この機能は対象インタフェースに接続可能なMACアドレスの数を制限するmax-macs機能が有効になっているインタフェースで設定ができます。

特徴としてはmax-macコマンドで制限されたMACアドレス数の範囲内で動的なMACアドレスエントリーより優先にstaticとして登録されます。
また、VLAN IDを入力しなかった場合にはPVIDが自動に設定されますが、
PVIDがデフォルトVLAN IDの場合には表示されません。

Port Security機能を使う時に注意点があります。
それはMACテーブルの中で該当ポートのMACアドレス情報を初期化した後、Staticに登録されますので、一度Port Securityで登録されたMACアドレスを使用するマシンは他のインタフェースに繋げた場合、通信ができません。
この場合には、PortSecurityの設定を解除すれば、正常に通信が可能になります。

Port Security 機能はmax-macs設定を解除するとPortSecurityの設定も同時に解除されます。
※ max-macsの数を変更した場合には、もう一度PortSecurityを設定する必要があります。

1.4.1 Port Securityを設定するためには、下記のコマンドをご使用ください。

コマンド	モード	機　能
max-macs <0-8192>　※ 2024,PoE **max-macs <0-32768> ※ 2024G**	INTERFACE	インタフェースに登録可能なMACアドレス数の範囲を制限します。
max-macs mac-address *MAC_Address* [*VLANID*]	INTERFACE	インタフェースにPort Security機能を設定します。

1.4.2 Port Security設定を確認するためには、下記のコマンドをご使用ください。

コマンド	モード	機　能
show max-macs	TOP	インタフェースに設定されているMACアドレス制限情報を表示します。

1.4.3 Port Security設定を初期化するためには、下記のコマンドをご使用ください。

コマンド	モード	機　能
no max-macs	INTERFACE	インタフェースに設定されているMACアドレス制限機能を解除します。
no max-macs mac-address *MAC_Address*	INTERFACE	Port　Security機能を解除します。

〈例題〉Port Security設定

```
SG2024G#show bridge
bridge       VLAN port      mac            fwd timeout
1            1    ge1       0000.0000.000e 1    300
1            1    ge1       0000.0000.0014 1    300
1            1    ge1       0000.0000.0019 1    300
1            1    ge2       0000.1200.0000 1    300
1            1    ge2       0000.1300.0000 1    300
1            1    ge2       0000.1400.0000 1    300
1            1    ge2       0000.1600.0000 1    300
 MAC Count = 7
SG2024G#
SG2024G#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SG2024G(config)#interface ge1
SG2024G(config-if)#max-macs 2
SG2024G(config-if)#max-macs mac-address 0000.0000.0001
SG2024G(config-if)#max-macs mac-address 0000.0000.0002 10
SG2024G(config-if)#end
SG2024G#
SG2024G#show bridge
bridge       VLAN port      mac            fwd timeout
1            1    ge1       0000.0000.0001 1    0
1            10   ge1       0000.0000.0002 1    0
1            1    ge2       0000.1200.0000 1    300
1            1    ge2       0000.1300.0000 1    300
1            1    ge2       0000.1400.0000 1    300
1            1    ge2       0000.1600.0000 1    300
 MAC Count = 6
SG2024G#
SG2024G#show max-macs
ge2     :       2/2       (current/max macs)
SG2024G#
```

 参考	設定されたmax-macsのMACアドレスの数を変更する場合、 Port Security設定が削除になりますので、max-macs数を変更した場合には Port Security機能を改めて設定する必要があります。

1.5 ACL/DHCPとNetBIOS Filter PORTRANGE

ACL, DHCP Filter, NetBIOS Filterはそれぞれ該当インタフェースでひとつずつ設定する機能ですが、ポートレインジを利用して範囲を指定して設定できるようになりました。

※　インタフェースモードでACL, DHCP Filter, NetBIOS Filterを設定する場合にもshow running-configの表示結果はコンフィグモードでポートレインジを利用したコマンドとして設定が保存・表示されます。

1.5.1 ACL、DHCP、NetBIOS　Filter機能を設定するためには、下記のコマンドをご使用ください。

コマンド	モード	機　能
ip acl <acl_no> in PORTRANGE	CONFIG	対象範囲のポートにACLを適用します。
dhcp filter PORTRANGE	CONFIG	対象範囲のポートにDHCPを適用します。
netbios filter PORTRANGE	CONFIG	対象範囲のポートにNetBIOSを適用します。

<例題> ACL/DHCPとNetBIOS Filter PORTRANGE設定

```
SG2024(config)#acl 100 permit ip host 1.1.1.1 any
SG2024(config)#ip acl 100 in fe1-2
SG2024(config)#dhcp filter fe3-4
SG2024(config)#netbios filter fe5-6
SG2024(config)#end
SG2024#show ip acl

Interface  acl
---------  ----------------------------------------
fe1        100
fe2        100
fe3
fe4
fe5
-- 以下省略 --
SG2024#show filter
Port       Netbios Filter  DHCP Filter
==========  ==============  ===========
fe1           -               -
fe2           -               -
fe3           -             Enable
fe4           -             Enable
fe5         Enable            -
fe6         Enable            -
fe7           -               -
-- 以下省略 --
```

1.6 dot1x LOCAL Radius 認証

エンベデッドRADIUSサーバを実装してCLIで簡単にEAPOL認証、WEB基盤認証,
Guest VLANのdot1x認証を利用することができます。

クライアントはMD5-Challenge・PAP (Password authentication protocol)方式で
認証することができます。

エンベデッドRADIUSサーバはlocalhost(127.0.0.1) のリクエストのみ応答します。

エンベデッドRADIUSサーバには最大、512個までユーザー登録ができます。
パスワードは23桁まで入力可能で、セキュリティのために、DES(Data Encryption Standard)を
利用したPrivate Key 基盤暗号化方式を採用しています。

SGシリーズスイッチでリモートRADIUSサーバとエンベデッドRADIUSサーバを
同時に使用することはできません。とちらか一つのRADIUSサーバだけ設定ができます。

ユーザーを追加した場合にRADIUSサーバにユーザー情報が5秒間隔で更新されて
適用される場合があります。

1.6.1 エンベデッドRADIUSサーバ機能を有効にするためには、下記のコマンドをご使用ください。

コマンド	モード	機　能
dot1x embedded enable	CONFIG	エンベデッドRADIUSサーバを有効にします。
dot1x embedded username <USERNAME> password <PASSWORD>	CONFIG	エンベデッドRADIUSサーバにユーザー情報を登録します。

1.6.2 エンベデッドRADIUSサーバ機能を確認するためには、下記のコマンドをご使用ください。

コマンド	モード	機　能
show dot1x [all | brief]	TOP	エンベデッドRADIUSサーバ設定内容と認証状況を確認します。
show running-config | {include | grep} embedded	TOP	エンベデッドRADIUSサーバのユーザー登録内容を確認します。

1.6.2 エンベデッドRADIUSサーバ機能を解除するためには、下記のコマンドをご使用ください。

コマンド	モード	機　能
no dot1x embedded enable	CONFIG	エンベデッドRADIUSサーバを無効にします。
no dot1x embedded username <USERNAME>	CONFIG	エンベデッドRADIUSサーバにユーザー情報を削除します。

<例題> エンベデッドRADIUSサーバ設定
- エンベデッドRADIUSサーバ設定及びユーザー登録後、ge2でtest1アカウントで認証

```
SG2024G#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SG2024G(config)#dot1x system-auth-ctrl
SG2024G(config)#dot1x embedded enable
SG2024G(config)#dot1x embedded username test1 password test1
SG2024G(config)#dot1x embedded username test2 password test2
SG2024G(config)#dot1x embedded username test3 password test3
SG2024G(config)#interface ge1-22
SG2024G(config-if)#dot1x port-control auto
SG2024G(config-if)#dot1x extension multi-user
SG2024G(config-if)#dot1x extension mac-auth-bypass
SG2024G(config-if)#dot1x extension web-auth
SG2024G(config-if)#end
SG2024G#
SG2024G#show dot1x brief
port    instance    port-status    auth      supplicant       supplicant
                                   type        address            name
=================================================================
 ge1     Master     Unauthorized   User
 ge2     Master     Unauthorized   User
 ge2          1       Authorized   User   001f.29a0.7de6    test1
 ge3     Master     Unauthorized   User
 ge4     Master     Unauthorized   User
 ge5     Master     Unauthorized   User
 ge6     Master     Unauthorized   User
 ge7     Master     Unauthorized   User
 ge8     Master     Unauthorized   User
 ge9     Master     Unauthorized   User
ge10     Master     Unauthorized   User
ge11     Master     Unauthorized   User
ge12     Master     Unauthorized   User
ge13     Master     Unauthorized   User
ge14     Master     Unauthorized   User
ge15     Master     Unauthorized   User
ge16     Master     Unauthorized   User
ge17     Master     Unauthorized   User
ge18     Master     Unauthorized   User
ge19     Master     Unauthorized   User
ge20     Master     Unauthorized   User
ge21     Master     Unauthorized   User
ge22     Master     Unauthorized   User
SG2024G#
```


参考

1.リモートRADIUSサーバとエンベデッドRADIUSサーバは同時に有効できません。
2. RADIUSサーバに127.0.0.1のようなlocalhostは追加できません。

1.7 dot1x 追加機能

ポート認証の他にも以下の機能が802.1x認証に追加・改善されました。

1. user-based authentication
 - portごとに多数のユーザー(32個)が同時認証が可能

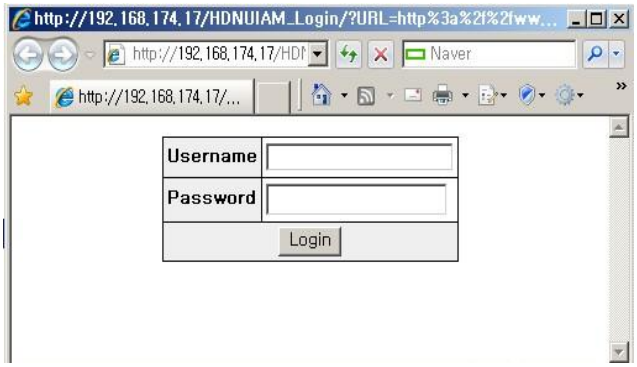
2. MAC Authentication bypass
 - MAC addressを基準として認証
 ※ クライアントから情報を入力できない場合(例:プリンター、IP電話、複合機など)

 - MAC認証はRADIUS Serverに認証対象のMAC Addressを
 User ID、Passwordとして認証作業の前に登録します。
 (MACアドレスは全て小文字でコンマまたはコロン抜きに12桁連続で登録します。)
 例) 0017.4241.5189のMACアドレスの場合に、ユーザー登録方法
 SG2024(config)#embedded radius username 001742415189 password 001742415189

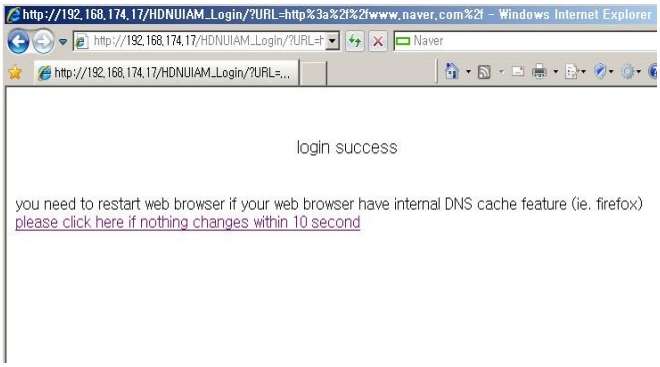
 - 認証方式によって約、1~2分の時間がかかる場合があります。

 - 認証対象ポートでBroadcastが発生しない場合は認証できません。
 ※端末が何らかのトラフィックを発生してSGスイッチが受信する必要があります。

3. WEB-based authentication
 - ユーザーの端末からウェブブラウザーでID, Passwordを入力して認証を行います。
 - DHCP環境のみ使用可能でWEB認証が完了したらexplorerを再起動する必要があります。
 (IP更新のために約、10秒がかかります。)



< 図1 > 認証ウィンドウ



< 図2 > 認証後、DNS Cacheにより
ブラウザを再起動 (IE, FireFoX)

- 端末のDNS Cache問題により即時、WEBの初期画面が現れない場合があります。この場合はIE, Firefoxのブラウザーを終了して暫く待機し起動するとDNS Cacheが削除されます。

4. Guest VLAN基盤の認証
 - User-Based認証とは同時設定ができません。
 - Guest VLANに指定するためにはvlan databaseに該当VLANが生成されている必要があります。

1.7.1 ユーザー基盤認証を有効[無効]にするためには、下記のコマンドをご使用ください。

コマンド	モード	機 能
[no] dot1x extension multi-user	INTERFACE	インタフェースにユーザー基盤認証を有効[無効]にします。
[no] dot1x extension multi-user client-limit <1-32>	INTERFACE	該当インタフェースに認証できるユーザー数を設定します。 ※ デフォルトは32名の認証

1.7.2 MACアドレス基盤認証を有効[無効]にするためには、下記のコマンドをご使用ください。

コマンド	モード	機 能
[no] dot1x extension mac-auth-bypass	INTERFACE	インタフェースにMACアドレス基盤認証を有効[無効]にします。

1.7.3 guest VLAN機能を有効[無効]にするためには、下記のコマンドをご使用ください。

コマンド	モード	機 能
[no] dot1x extension guest-vlan VLAN_ID	INTERFACE	Guest VLAN機能を有効[無効]にします。

1.7.4 WEB認証機能を有効[無効]にするためには、下記のコマンドをご使用ください。

コマンド	モード	機 能
[no] dot1x extension web-auth	INTERFACE	WEB認証機能を有効[無効]にします。

<例題> dot1x追加認証機能

```
SG2024(config)#dot1x system-auth-ctrl
SG2024(config)#radius-server host 192.168.130.20
SG2024(config)#int fe3
SG2024(config-if)#dot1x port-control auto
SG2024(config-if)#dot1x extension multi-user
SG2024(config-if)#dot1x extension mac-auth-bypass
SG2024(config-if)#dot1x extension web-auth
SG2024(config-if)#end
SG2024#show bridge
bridge       VLAN port      mac            fwd timeout
 MAC Count = 0
SG2024#
SG2024#show dot1x brief
port   instance   port-status   auth     supplicant      supplicant
                               type       address           name
=====================================================================
 fe3    Master    Unauthorized  User
 fe3         1    Unauthorized  User  001a.f40f.0400   001af40f0400
 fe3         2      Authorized  User  0017.4241.5189   hdn70
SG2024#
SG2024#show bridge
bridge       VLAN port      mac            fwd timeout
1            1    fe3       0017.4241.5189 1    300
1            1    fe3       001a.f40f.0400 1    300
 MAC Count = 2
SG2024#


SG2024(config)#int fe3
SG2024(config-if)#no dot1x extension multi-user
SG2024(config-if)#no dot1x extension mac-auth-bypass
SG2024(config-if)#dot1x extension guest-vlan 10
SG2024(config-if)#end
SG2024#show bridge                                          ← 認証前
bridge       VLAN port      mac            fwd timeout
1            1    fe5       001a.f400.0300 1    300
1            10   fe3       0017.4241.5189 1    300
 MAC Count = 2
SG2024#show bridge                                          ← 認証後
bridge       VLAN port      mac            fwd timeout
1            1    fe3       0017.4241.5189 1    300
1            1    fe5       001a.f400.0300 1    300
 MAC Count = 2
SG2024#
```

1.8 Clear MDS ARP-Table

MDSエンジンによりキャッシューされいるARPテーブルをクリアする機能です。
※ ARP Spoofing Detection機能が有効になっている環境

1.8.1 MDSエンジンによりキャッシューされているARPテーブルをクリアにするためには、
下記のコマンドをご使用ください。

コマンド	モード	機　能
clear mds arp-table	TOP	インタフェースにユーザー基盤認証を有効[無効]にします。

<例題>MDS ARPテーブルクリア

```
SG2024(config)#mds arp-spoofing-detect fe
SG2024(config)#end
SG2024#sh mds arp-table

 No  MAC Address     IP Address       GW Port=Lock VLAN tag Static LastSEC
---- --------------  ---------------  -- ----=---- ---- --- ------ -------
   1 001a.f40f.0400  192.168.130.10       25         1                21
   2 001a.f400.0541  192.168.130.20        *         1     Local       8
   3 0017.4241.5189  192.168.130.1    GW   3         1                21
SG2024#
SG2024#clear mds arp-table
SG2024#show mds arp-table

 No  MAC Address     IP Address       GW Port=Lock VLAN tag Static LastSEC
---- --------------  ---------------  -- ----=---- ---- --- ------ -------
SG2024#
```

参考	1. MDS ARPテーブルのAging Timeはデフォルトで3600秒です。

1.9 MDS Extended Permit / Deny

MDSエンジンのポリシーの拡張機能として
プロトコル種類
Source(MAC, IP, Port),
Destination (MAC, IP, Port)

に対してPermit / Denyポリシーを詳細まで設定することができます。

1.9.1 MDSエンジンによる拡張ポリシーを設定するためには、下記のコマンドをご使用ください。

コマンド	モード	機　能
mds extended {deny | permit} {any | icmp | raw | tcp | udp} {any | SMAC} {any | SIP} {any | SPort} {any | DMAC} {any | DIP} {any | DPort} [Comment]	CONFIG	MDSエンジンで許可または遮断する トラフィックの条件を指定します。
clear mds {all | KeyNo.}	TOP	リアルタイム遮断が動作する場合、 強制にMDSポリシーを解除します。

1.9.2 MDSエンジンによる拡張ポリシーを確認するためには、下記のコマンドをご使用ください。

コマンド	モード	機　能
show mds extended	TOP	MDSエンジンで許可または遮断する トラフィック設定のリストを表示します。

1.9.3　MDSエンジンによる拡張ポリシーを削除するためには、下記のコマンドをご使用ください。

コマンド	モード	機　能
no mds extended comment MSG	CONFIG	MDSポリシーをコメントで削除します。 ※ ポリシー登録時にコメントも設定して おく必要があります。
no mds extended {deny | permit} {any | icmp | raw | tcp | udp} {any | SMAC} {any | SIP} {any | SPort} {any | DMAC} {any | DIP} {any | DPort}	CONFIG	リアルタイム遮断が動作する場合、 強制にMDSポリシーを解除します。
no mds extended all	CONFIG	MDSポリシーを全て削除します。

<예제> MDS extended機能

```
SG2024(config)#mds extended permit any any any any 1.1.1.1
SG2024(config)#mds extended permit any any any any 1.1.1.2 test
SG2024(config)#end
SG2024#show mds extended

 MDS extended permit/deny information.
================================================================================
Permit/Deny IP_Protocol Packet    Comment
  Source_MAC      Source_IP       SPort Destination_MAC Destination_IP  DPort
================================================================================
permit      any         0
  any             any                   any             1.1.1.1
--------------------------------------------------------------------------------
permit      any         0         test
  any             any                   any             1.1.1.2
--------------------------------------------------------------------------------
SG2024#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SG2024(config)#no mds extended comment test
SG2024(config)#end
SG2024#sh mds extended

 MDS extended permit/deny information.
================================================================================
Permit/Deny IP_Protocol Packet    Comment
  Source_MAC      Source_IP       SPort Destination_MAC Destination_IP  DPort
================================================================================
permit      any         0
  any             any                   any             1.1.1.1
--------------------------------------------------------------------------------
SG2024#
```

1.10 MDS [Extended] Permit Count

MDS Permit / Extendedポリーシにマッチするパケットがある場合、該当パケットの数をカウントする機能です。
clear count コマンドで特定のACLまたはQoS Policy-mapのカウント値を初期化できます。

1.10.1 MDSエンジンによるポリシーマッチカウントを確認するためには、下記のコマンドをご使用ください。

コマンド	モード	機　能
show mds extended	TOP	MDSエンジンによるポリシーマッチのパケットカウント数を表示します。 [mds permit / mds extended 両方]
show mds permit	TOP	MDSエンジンによるポリシーマッチのパケットカウント数を表示します。 [mds permitのみ]

<例題> MDS extended機能

```
SG2024(config)#mds permit icmp any 1.1.1.1 Ping_Test
SG2024(config)#mds extended permit icmp 0000.0000.00001 1.1.1.10 0000.0000.0002 1.1.1.2
Ping_Test_2
SG2024(config)#
SG2024(config)#end
SG2024#show mds permit
ip prot     source ip/mac  destination ip/mac  dport  count    comment
-------------------------------------------------------------------------------
 icmp                any             1.1.1.1         19900    Ping_Test
SG2024#
SG2024#show mds extended

 MDS extended permit/deny information.
===============================================================================
Permit/Deny IP_Protocol Count     Comment
  Source_MAC      Source_IP       SPort Destination_MAC Destination_IP  DPort
===============================================================================
std permit  icmp        19900     Ping_Test
  any             any                   any             1.1.1.1
-------------------------------------------------------------------------------
permit      icmp        15600     Ping_Test_2
  0000.0000.0000  1.1.1.10              0000.0000.0002  1.1.1.2
-------------------------------------------------------------------------------
SG2024#
```

1.11　MDS arp-spoofing-mac-safe

MDS arp-spoofing検知 / 遮断機能が動作中にある一つのIPに二つのMACが同時に検知された場合、優先順位によりどちらかはarp-spoofingとして通信が遮断されます。

Apple社のノートパーソコンはMicrosoft社のウィンドウ系列のOSに比べ有・無線を同時に有効して使用する機能があります。

これは一つのIPに対して二つ以上のインタフェースが有効になってしまい、同時に複数のMACアドレスがIPと関連付けられているので、arp-spoofingとして検知される現象が発生します。

対策としてはMDSがarp-spoofing 検知/遮断をする前にarp-spoofing対象MAC アドレスにownerのIPが存在するかを確認しOwnerのIPが存在すれば, arp-spoofingとして遮断しIPが存在しなければスキップします。

※　Arp-spoofing-mac-safe機能使用の制約事項
　登録したMACアドレスに対してはIP競合が発生した場合、arp-spoofingの検知ができません。

1.11.1 MACアドレスsafe機能を有効にするためには、下記のコマンドをご使用ください。

コマンド	モード	機　能
mds arp-spoofing-mac-safe {MAC_Addr Wildcard | any | ouiOUI}	CONFIG	ARP Spoofingで遮断するまえ、特定または全体のMACアドレスに対してARPテーブルにオナーのIPが存在するかもう一度チェックを行います。

1.11.2 MACアドレスsafe機能を有効にするためには、下記のコマンドをご使用ください。

コマンド	モード	機　能
show mds arp-spoofing-mac-safe	TOP	ARP spoofing-mac-safeで設定された内容を確認します。

1.11.3 MACアドレスsafe機能を削除するためには、下記のコマンドをご使用ください。

コマンド	モード	機　能
no mds arp-spoofing-mac-safe {MAC_Addr Wildcard | any | ouiOUI}	CONFIG	ARP spoofing-mac-safeで設定された内容を削除します。

<例題> MDS ARP spoofing mac safe機能

```
SG2024(config)#mds arp-spoofing-mac-safe oui 00-17-F2  ← macintosh 有線 MAC アドレス OUI
SG2024(config)#mds arp-spoofing-mac-safe oui 00-19-E3  ← macintosh 無線 MAC アドレス OUI
SG2024(config)#end
SG2024#
```

1.12 DHCP Option-150

SGシリーズスイッチをDHCPサーバとして使用する場合、IPとゲートウェイなどネットワーク情報とTFTPサーバ アドレス(Option-150)を設定してVoIP PhoneなどのデバイスのFirmwareや設定情報などをTFTP サーバから受け取るようにすることができます。

SGシリーズではTFTPサーバの指定は最大5個まで登録できます。

1.12.1 DHCP Option-150機能を有効にするためには、下記のコマンドをご使用ください。

コマンド	モード	機 能
tftp-server IP_Addr	DHCP	TFTPサーバのIPを指定します。

〈例題〉 DHCP Option-150機能

```
SG2024G(config)#interface vlan1.1
SG2024G(config-if)#ip address 172.1.1.254/24
SG2024G(config-if)#exit
SG2024G(config)#ip dhcp server interface vlan1.1
SG2024G(config)#ip dhcp pool pool1
SG2024G(config-dhcp)#network 172.1.1.0/24
SG2024G(config-dhcp)#range 172.1.1.10 172.1.1.100
SG2024G(config-dhcp)#default-router 172.1.1.254
SG2024G(config-dhcp)#lease 0 1 0
SG2024G(config-dhcp)#dns-server 10.10.10.1
SG2024G(config-dhcp)#domain-name test.domain.com
SG2024G(config-dhcp)#tftp-server 172.1.1.252
SG2024G(config-dhcp)#host 0000.1111.2222 static-ip 172.1.1.101
SG2024G(config-dhcp)#end
SG2024G#show ip dhcp
dhcp server/relay enabled
dhcp pool list: pool1
SG2024G#show ip dhcp pool
Pool pool1 :
network: 172.1.1.0/24
address range(s):
add: 172.1.1.10 to 172.1.1.100
lease <days:hours:minutes> <0:1:0>
domain: test.domain.com
dns-server(s): 10.10.10.1
tftp-server(s): 172.1.1.252
default-router(s): 172.1.1.254
host static ip rease config
host entry #1
Mac address : 0000.1111.2222
static ip address : 2.32.3.56
```

1.13　DHCP Snooping

DHCP Snoopingはtrustて設定されたインタフェースからきたDHCP応答情報を許可する機能です。
trustで指定されていない他のインタフェースからDHCP応答（DHCP offer、ack）パケットが
検知される場合、クライアントの転送元のMACアドレスとDHCPパケット内のクライアント
MACアドレスが異なる場合には該当DHCPパケットを遮断します。

VLANインタフェイスにDHCP Snoopingを有効にすると、該当VLANのDHCPパケットは
CPUが直接転送することになります。

DHCP　Snooping設定が可能なVLANは最大32個でバインディングエントリー数は
最大1024個までサポートします。

もし、バインディングエントリーの最大値を超えた場合には該当DHCPパケット情報は
バインディングテーブルに登録されません。
また、すべてのバインディングエントリーは30秒毎に一度更新されてLease Time情報も
30秒ずつ減少します。

DHCP Snooping Option-82はスイッチとスイッチが連続で繋がっている環境でも動作します。
受信されたDHCPパケットにoption-82情報が無かった場合、
自身の情報をoption-82に挿入しDHCPサーバに転送を行います。
サーバからDHCPパケットを受信した場合はパケットの中のoption-82情報を調べて
スイッチ自身が挿入した情報であれば該当option-82情報を削除します。

DHCP Snoopingの動作は次となります。
1。DHCPサーバが繋がっているインタフェースをDHCP snoopinのTrustインタフェースで
　設定すると他のインタフェースは全てuntrust状態になります。

2。TrustインタフェースからのDHCP Replyだけを認めてuntrustインタフェースからDHCP Reply
　パケットが検知された場合には遮断するか該当インタフェースをダウン指せます。
　※ Disableになったインタフェースは手動で状況を修復する必要があります。

3。SGスイッチは受信されたDHCP Replyパケットの情報に基づいて
　クライアントのMACアドレスサーバから割り当てられたIPアドレス、Lease期間などを
　バインディングエントリーに更新します。

4。クライアントがリクエストもしてない環境でサーバからDHCPReplyが発生した場合、
　もしくはクライアントとサーバの間にソースIPアドレスが異なる場合は
　アラート及び該当インタフェースがダウンされる場合があります。

 参考	1。DHCP Snoopingを設定できるVLANは32個までです。 2。DHCP Snoopingのバインディングテーブルに格納されるエントリー数は 1024個が上限でこれ以上は登録できません。

1.13.1 DHCP Snoopingを設定するためには、下記のコマンドをご使用ください。

コマンド	モード	機　能
ip dhcp snooping	CONFIG	DHCP Snooping機能を有効にします。
ip dhcp snooping vlan *RANGE*	CONFIG	特定VLANにDHCPSnooping機能を活性化します。
ip dhcp snooping information option 82	CONFIG	DHCP SnoopingにOption-82情報を追加します。
ip dhcp snooping trust	INTERFACE	インタフェースをTrustで設定します。 ※他のインタフェースはUntrustモード

1.13.2 DHCP Snoopingを確認するためには、下記のコマンドをご使用ください。

コマンド	モード	機　能
show ip dhcp snooping	TOP	DHCP Snooping情報を確認します。
show ip dhcp snooping { binding | statistics [interface IFNAME]}	TOP	DHCPバインディングテーブル/Counter情報を確認します。

1.13.3 DHCP Snoopingを初期化するためには、下記のコマンドをご使用ください。

コマンド	モード	機　能
no ip dhcp snooping	CONFIG	DHCP Snooping機能を無効にします。
no ip dhcp snooping vlan *RANGE*	CONFIG	特定VLANに設定されているDHCP Snooping機能を解除します。
no ip dhcp snooping information option 82	CONFIG	DHCP Snoopingに追加されたOption-82情報を初期化します。
no ip dhcp snooping trust	INTERFACE	Trustに設定されていたインタフェース情報を初期化します。
clear ip dhcp snooping binding [interface IFNAME| vlan <1-4094>]	CONFIG	DHCP Snooping バインディングエントリーを初期化します。
clear ip dhcp snooping statistics [interface IFNAME]	CONFIG	DHCP Snoopingカウンタを初期化します。

<例題>DHCP Snooping設定
- ip dhcp snooping設定
- DHCPサーバをge1,ge2に繋げた後にge1のみTrustに設定

```
SG2024G(config)#ip dhcp snooping
SG2024G(config)#ip dhcp snooping vlan 1
SG2024G(config)#ip dhcp snooping information option 82
SG2024G(config)#interface ge1
SG2024G(config-if)#ip dhcp snooping trust
SG2024G(config-if)#end
SG2024G#sh ip dhcp snooping statistics interface ge2
DHCP snooping statistic counters for interface ge2
Discover : 0
Discover dropped : 0
Offer : 0
Offer dropped : 8
Request : 0
Request dropped : 0
Ack : 0
Ack dropped : 0
Nack : 0
Nack dropped : 0
Release : 0
Release dropped : 0
Inform : 0
Inform dropped : 0
Decline : 0
Decline dropped : 0
SG2024G#sh ip dhcp snooping statistics interface ge1
DHCP snooping statistic counters for interface ge1
Discover : 0
Discover dropped : 0
Offer : 3
Offer dropped : 0
Request : 0
Request dropped : 0
Ack : 2
Ack dropped : 0
Nack : 0
Nack dropped : 0
Release : 0
Release dropped : 0
Inform : 0
Inform dropped : 0
Decline : 0
Decline dropped : 0
SG2024G#
```

1.14　ACL/QoS Counter

ACL / QoSポリシーにマッチするパケットがある場合、マッチ数を確認する機能です。
設定したACLとQoSがどのぐらい利用されているか確認できます。

clear countコマンドを利用すると指定したACL・ QoS Policy-mapのカウント値を
0に初期化できます。

1.14.1 ACL/QoS Counterを確認するためには、下記のコマンドをご使用ください。

コマンド	モード	機　能
show acl ［Rule_No］	TOP	該当ACLの全体内容とQoSに適用されたパケットマッチカウント値を確認します。
show policy-map	TOP	該当ポリシーマップの設定内容とパケットマッチのカウント値を確認します。

1.14.2 ACL/QoS Counterを初期化するためには、下記のコマンドをご使用ください。

コマンド	モード	機　能
clear count { acl | policy-map }	TOP	ACLまたはポリシーマップでマッチされたカウント値を初期化します。

<例題>ACL/QoS Counter設定
- fe1-2はacl適用でパケットマッチカウント
- fe3-4はQoSポリシー適用でパケットマッチカウント

```
SG2024(config)#acl 100 permit ip host 1.1.1.1 any
SG2024(config)#acl 101 permit ip host 1.1.1.2 any
SG2024(config)#class-map c1
SG2024(config-cmap)#match acl 101
SG2024(config-cmap)#exit
SG2024(config)#policy-map p1
SG2024(config-pmap)#class c1
SG2024(config-pmap-c)#set cos 1
SG2024(config-pmap-c)#exit
SG2024(config-pmap)#exit
SG2024(config)#ip acl 100 in fe1-2
SG2024(config)#int range fe3-4
% fe3-4 Selected
SG2024(config-if-range)#service-policy input p1
% fe3-4 Selected
SG2024(config-if-range)#end
SG2024#show acl

  Extended IP acl: 100
    permit ip host 1.1.1.1 any
      Ports: fe1-2
        Counter: 1000

  Extended IP acl: 101
    permit ip host 1.1.1.2 any

SG2024#show policy-map

  POLICY-MAP-NAME: p1
    State: attached

    CLASS-MAP-NAME: c1
      ACCESS-LIST-NAME: 101
      Set CoS: 1
        Port: fe3
          Count: 1512
        Port: fe4
          Count: 2452
```

1.15　Interface Power-Saving

SGスイッチシリーズはケーブルが未接続されているインタフェース、Link Downされた
インタフェースに対してPower Downさせてスイッチ電力消費を抑えることができます。
Power Downされたインタフェースは通常の電力消費量に比べて70%削減した電力だけ使用します。

インタフェースにケーブルが接続されるか相手のマシンの電源が入ってLink Upになると
自動的にPower Up (auto)させて通信を行い、使用しない状況になるとまた電力を抑えて
効率的な電力管理が可能になってGreen ITを達成しました。

ギガモデルの場合、オートモードに加えて更にスケジュールモード(時間・日付・維持時間・
Interfaceを指定)が別度あり指定時刻に電力を消費しない状況であればLink Downさせて
通常電力消費量に比べて約90%の電力削減ができます。

インタフェースがオートモードではなく、スケジュール設定によってPower Downになった場合には
ケーブルが接続されても相手のマシンに電源が入ってもスケジュールの維持の設定時間内では
Power Downの状態を維持しますが、スケジュールモードの設定時刻以内でも
Power Upしたい場合にはRecovery Intervalを設定すると該当間隔にリンク状況を
チェックして自動的にLink Upすることができます。
※　Recovery Intervalの入力範囲は<60>～<600>秒です。

1.15.1 インタフェースにPower-Savingを設定するためには、下記のコマンドをご使用ください。

コマンド	モード	機　能
power-saving auto PORTRANGE	CONFIG	Power Saving Auto Modeを設定するインタフェースの範囲を設定します。
power-saving Rule_No Day Start_Time Duration PORTRANGE	CONFIG	Power Saving Schedule Modeを設定するインタフェースの範囲を設定します。 ※ ギガモデルのみ
power-saving recovery Interval	CONFIG	Power Saving Schedule Modeを設定時、Link Up Check Intervalを設定します。 ※ ギガモデルのみ

1.15.2 インタフェースのPower-Savingを確認するためには、下記のコマンドをご使用ください。

コマンド	モード	機　能
show power-saving	TOP	インタフェースに適用されている Power Savingの状況を確認します。

1.15.3インタフェースのPower-Savingを初期化するためには、下記のコマンドをご使用ください。

コマンド	モード	機　能
no power-saving auto *PORTRANGE*	CONFIG	Power Saving Auto Mode設定を初期化します。
no power-saving *Rule_No*	CONFIG	Power Saving Schedule設定を初期化します。 ※ギガモデルのみ
no power-saving recovery	CONFIG	Power Saving LinkUp Check Interval設定を初期化します。 ※ギガモデルのみ

参考

Power SavingをScheduleモードで設定してrecover Interval項目を設定しなかった場合にはScheduleに指定された時刻範囲で一度だけでもLink Downされたインタフェースは Power Down状態を維持します。

<例題>インタフェースにPower saving設定
- ge1-4はスケジュールモード設定(毎日 夜7時から12時まで)
  ※ 一分ごとにリンクをチェックし、Link Upの場合、Power Up
- ge5-8はオートモード設定
  ※ Link Upになると自動にPower Up

```
SG2024G(config)#power-saving 10 0 19:00 300 ge1-4
SG2024G(config)#power-saving auto ge5-8
SG2024G(config)#power-saving recovery 60
SG2024G(config)#end
SG2024G#show power-saving

 Recovery Inteval      : 60 sec
-------------------------------------------------------------
 Rule  Days       ApplyTime  Minute     PortRange
-------------------------------------------------------------
 10    AllDay     19:00      300        ge1-4

---------------------------------------
 Port  Static-Power-Down  Auto-Power-Down
---------------------------------------
 ge1   PowerDown          Disable
 ge2   PowerDown          Disable
 ge3   PowerDown          Disable
 ge4   PowerDown          Disable
 ge5   Disable            PowerDown
 ge6   Disable            PowerDown
 ge7   Disable            PowerDown
 ge8   Disable            PowerDown
 ge9   Disable            Disable
 ge10  Disable            Disable
 ge11  Disable            Disable
-- 以下省略 --
```

1.16　N:1*4 Mirror

ポートミラーリングは対象インタフェースを介する全てのトラフィックを指定したインタフェースにコピーしてモニタリングできる機能です。
ポートミラーリングは対象インタフェースを最大4個までひとつのインタフェースでモニタリングできます。但し、対象インタフェースは重複できません。
　例) fe1がfe10にミラーされている場合はfe2がfe1を重複してミラーできません。

1.16.1 ポートミラーリングを設定するためには、下記のコマンドをご使用ください。

コマンド	モード	機　能
mirror interface PORTRANGE direction {both | receive | transmit}	INTERFACE	モニタリングするインタフェース範囲及びパケット転送方向を指定します。

1.16.2　ポートミラーリングを確認するためには、下記のコマンドをご使用ください。

コマンド	モード	機　能
show mirror	TOP	ポートミラーリングの設定状況を確認します。
show running-config interface IFNAME	TOP	インタフェースに設定されているミラーリングの状況を確認します。

1.16.3　ポートミラーリングを初期化するためには、下記のコマンドをご使用ください。

コマンド	モード	機　能
no mirror interface PORTRANGE [direction {receive | transmit}]	INTERFACE	ポートミラーリング設定を解除します。

<例題>ポートミラーリング設定

```
SG2024G(config)#interface ge9
SG2024G(config-if)#mirror interface ge1 direction both
SG2024G(config-if)#end
SG2024G#show running-config interface ge9
!
interface ge9
mirror interface ge1 direction both
bridge-group 1
switchport mode access
switchport mode access acceptable-frame-type all
!
SG2024G#
```

参考	ポートミラーリング機能を長時間使用するとCPUに負荷が掛かってしまい、パケットの処理に遅延が発生しますので、パフォーマンスが低下する場合があります。 データ分析が終了するとミラーリング設定を解除してください。

1.17　CDP

CDP (Cisco Discovery Protocol)はData　Layerで隣接したCiscoデバイス及び情報を確認するために、使用されるCisco独自のプロトコルです。

CDPはハードウェアタイプとソフトウェアバージョン、Ciscoデバイスが使用しているインタフェースなどの情報のやり取りを行います。

SGスイッチシリーズではCDPの情報を転送時、Ciscoデバイスに影響を及ぼさないよう、最小限の情報(1。バージョン、2。デバイスID,、ポートID、Capabilities、ソフトウェアバージョン,フラットフォーム）だけを転送しています。因みにCDP情報の修正はできません。

Voice-vlanを設定した場合にはVoIP VLAN Reply Fieldを追加し、CDP情報を転送してCisco IP Phoneの設定を自動に変更します。

CDPが有効になっていない場合に、SGスイッチがCDPパケットを受信するとCPUにコピーされずに、フラッディングされます。

1.17.1 CDPを設定するためには、下記のコマンドをご使用ください。

コマンド	モード	機　能
cdp enable	CONFIG	CDPを有効にします。
cdp port {receive | transmit | both} ***PORTRANGE***	CONFIG	CDPパケットを転送するインタフェースを指定します。

1.17.2　CDPを確認するためには、下記のコマンドをご使用ください。

コマンド	モード	機　能
show cdp neighbor [*IFNAME* | detail]	TOP	隣接したCDPサポートのデバイス情報を確認します。

1.17.3インタフェースのPower-Savingを初期化するためには、下記のコマンドをご使用ください。

コマンド	モード	機　能
no cdp enable	CONFIG	CDPを無効にします。
no cdp port {both | receive | transmit} *PORTRANGE*	CONFIG	CDPを有効にしたインタフェースを初期化します。

<예제> CDP설정

```
SG2024G#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SG2024G(config)#cdp enable
SG2024G(config)#cdp port both ge2
SG2024G(config)#end
SG2024G#
SG2024G#show cdp neighbor

 CDP Neighbor Devices Information

 Port       | DeviceID               PortID                 Platform
------------+------------------------ ---------------------- ----------------------
 ge2        | SG2024                 ge2                    SG2024 #7682 Fri Ma

SG2024G#
SG2024G#show cdp neighbor detail
Port = ge2
 CDP Ver         : 2
 TTL             : 180 second
 Device ID       : SG2024
 Port ID         : ge2
 Capabilities    : Switch IGMPcapable
 ISO Version     : SG-1.4.4
 PLATFORM        : SG2024 #7682 Fri Mar 12 09:55:26 KST 2010

SG2024G#
```

1.18　SFF-8472:SFPチェック及びモニターリング

アップリンク　インタフェースではSFPタイプと10/100/1000Base-TのCOMBOタイプを
使用することができます。

SFPモジュールを取り付けた場合、SFPモジュールの情報及び現在、
動作中のインタフェースタイプを確認することができます。

さらにSFF-8472規格をサポートしているSFPモジュールを取り付けた場合には
SFF-8472(Tx/Rx Power, Voltags, Bias current, Temperatureなど)情報を確認することができます。.

また、SFF-8472サポートSFPでAlarmまたはWarningが発生した場合には
Syslogにイベントを記録し、SNMPトラップが設定されている場合は
SNMPトラップサーバにSFP関連イベントを転送します。

1.18.1　SFP-8472を確認するためには、下記のコマンドをご使用ください。

コマンド	モード	機　能
show system sfp SFP_No	TOP	SFPモジュールの情報を確認します。
show interface media [IFNAME]	TOP	動作中のインタフェースのタイプを 確認します。

 参考	SFPのポート指定は以下となります。 SG2024/PoE : <1-2> SG2024G : <21-24> SG2048G : <45-48>

<例題1> Comboポートの情報確認
　- ge21にSFPモジュール取り付け. 10/100/1000Base-Tで通信

```
SG2024G#show system sfp 21
Identifier    : SFP transceiver
Connector     : LC
Transceiver   :
         Gigabit Ethernet Compliance Codes:
         Fibre Channel link length:
           intermediate distance (I)
         Fibre Channel transmitter technology:
           Shortwave laser w/o OFC (SN)
         Fibre Channel transmission media:
           Multi-mode, 62.5m (M6)
           Multi-mode, 50m (M5)
         Fibre Channel Speed:
           100 MBytes/Sec
Encoding      : Manchester
BR. Norminal  : 1300MBits/sec
BR. MAX       : 0%
BR. MIN       : 0%
Length        :
   Link length supported for   50/125mm fiber, 550m
Vendor Name   : HG GENUINE
Vendor OUI    : 0
Vendor PN     : MXP-248S-550M
Vendor Rev    :
Vendor SN     :         01888511
Date code     : 2007.05.16
Options       :
   TX_DISABLE implemented
   TX_FAULT implemented
   loss of signal implemented.
SG2024G#
SG2024G#show interface media ge21
 Interface:  ge21  Active medium: Copper
SG2024G#
```

参考	Comboポートの場合、モデルによって優先順位が異なります。 SG2024/PoE :　Fiber　優先 SG2024G/48G: Copper 優先

<例題2> SFF-8472規格サポートのComboポートの情報確認
- ge21にSFPモジュール取り付け. 10/100/1000Base-Tで通信

```
SG2024G#show system sfp 21
Identifier    : SFP transceiver
Connector     : LC
Transceiver   :
         Gigabit Ethernet Compliance Codes:
         Fibre Channel link length:
           intermediate distance (I)
         Fibre Channel transmitter technology:
           Shortwave laser w/o OFC (SN)
         Fibre Channel transmission media:
           Multi-mode, 62.5m (M6)
           Multi-mode, 50m (M5)
         Fibre Channel Speed:
           100 MBytes/Sec
Encoding      : Manchester
BR. Norminal  : 1300MBits/sec
BR. MAX       : 0%
BR. MIN       : 0%
Length        :
   Link length supported for   50/125mm fiber, 550m
   Link length supported for 62.5/125mm fiber, 270m
Vendor Name   : FIBERXON INC.
Vendor OUI    : 0
Vendor PN     : FTM-8112C-SLG
Vendor Rev    : 10
Vendor SN     : 14W220091368308
Date code     : 2009.03.29
Options       :
   TX_DISABLE implemented
   TX_FAULT implemented
   loss of signal implemented.
SFF-8472 Info :
  Temperature : 28.96 C
  Vcc         : 3.26 V
  Bias        : 3 mA
  TX Power    : 0.4 dBm
  RX Power    : -inf dBm
  Alarm       : RX Power Low Alarm
  Warining    : RX Power Low Warining

SG2024G#
SG2024G#show interface media ge21
 Interface:  ge21  Active medium: Fiber
SG2024G#
```

1.19 sFlow

sFlowはRFC3176で標準化されており、ネットワークデバイスでトラフィックを高速にキャプチャーして分析するために使われるプロトコルです。
sFlowはリアルタイムパケットサンプリング方式を採用しているので、L2からL7トラフィックに対してネットワークのパフォーマンス低下無しにモニタリングできます。
sFlowエージェントはインタフェースから処理されるパケットを分析した情報をトラフィック収集サーバ(Collector)に転送する方式で動作します。
sFlow統計機能を利用して下位ネットワーク及び隣接したネットワークの流れの特性またはインタフェース単位MIB情報収集のイベントをモニタリングします。
このために各、インタフェースにリアルタイムパケットカウンタの周期を設定しなければなりません。
そしてパケットを抽出する頻度をサンプリング比率(sample-rate)と言います。

1.19.1 sFlowを設定するためには、下記のコマンドをご使用ください。

コマンド	モード	機　能
sflow agent *IP_Address*	CONFIG	AgentIPアドレスを設定します。 (デフォルト:127.0.0.1)
sflow {both | egress | ingress} *Port_Range*	CONFIG	パケットを分析するためのインタフェースを設定します。
sflow collector *IP_Address* [*Port_No*]	CONFIG	Collector IPアドレス及びサービスポートを設定します。(デフォルトポート:6343)
sflow sample-rate <5000-1048576>	CONFIG	パケットを抽出するサンプリング比率を設定します。 (デフォルト:1 out of 10000 パケット)

1.19.2 sFlowを確認するためには、下記のコマンドをご使用ください。

コマンド	モード	機　能
show sflow config	TOP	sFlow 設定状態を確認します。

1.19.3 sFlowを初期化するためには、下記のコマンドをご使用ください。

コマンド	モード	機　能
no sflow agent	CONFIG	AgentIPアドレスを削除します。
no sflow {both | egress | ingress} *Port_Range*	CONFIG	パケットを分析するインタフェースを削除します。
no sflow collector	CONFIG	Collector IPアドレスを削除します。
no sflow sample-rate	CONFIG	パケットを抽出するサンプリング比率を削除します。

<例題1> スイッチ(IP 192.168.0.1)からge1～ge10のインタフェースのIngress / Egressトラフィックに対してパケット5000個当たりに一つをサンプリングしてトラフィック収集サーバ(IP 192.168.0.100)に転送するように設定

```
SG2024G#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SG2024G(config)#sflow agent 192.168.0.1
SG2024G(config)#
SG2024G(config)#sflow both ge1-10
SG2024G(config)#
SG2024G(config)#sflow collector 192.168.0.100
SG2024G(config)#
SG2024G(config)#sflow sample-rate 5000
SG2024G(config)#end
SG2024G#
SG2024G#show sflow config
 - sFlow Agent Address     : 192.168.0.1
 - sFlow Collector Address : 192.168.0.100
 - sFlow Collector Port    : 6343
-----------------------------------------------------
 Interface Ingress   Rate          Egress    Rate
=====================================================
 ge1       Enable    5000          Enable    5000
 ge2       Enable    5000          Enable    5000
 ge3       Enable    5000          Enable    5000
 ge4       Enable    5000          Enable    5000
 ge5       Enable    5000          Enable    5000
 ge6       Enable    5000          Enable    5000
 ge7       Enable    5000          Enable    5000
 ge8       Enable    5000          Enable    5000
 ge9       Enable    5000          Enable    5000
 ge10      Enable    5000          Enable    5000
 ge11
 ge12
-- 以下省略 --
SG2024G#
```

参考	sFlowエージェント及びCollector IPアドレスは一つのみ指定ができます。 重複して設定した場合には最後のIPアドレスが設定されます。

1.20 RMON (GROUP 1,2,3,9)

RMON (Remote Monitoring)はリモートにある通信網を管理できるように設計されたSNMPの拡張機能でRFC1757に定義されたMIBの一部として定義されています。
標準SNMP転送構造とコマンドを利用して特定インタフェースを介する分散されたLAN環境の全てのトラフィックを収集しリモートでチェックし確認する機能です。
SNMPはSNMPエージェントデバイスだけの情報を取得できますが、RMONはデバイスを含めてセグメント全体から発生する情報を把握することができるので、より効率的にネットワークを管理することができます。

RMONの種類はLayer2レベルでトラフィック内容を分析するRMONバージョン1とLayer2から7まですべてのLayerに対してトラフィック分析情報を提供してくれるバージョン2があります。

SGスイッチシリーズはRMONバージョン1をサポートしています。
その上、RFC1757に定義されているStatistics、History、 Alarm、Host、Host Enable N、Matrix、Filter、Packet capture、Eventの九つの情報の中でStatistics、History、Alarm、Eventの四つMIBグループをサポートします。
RMONはインタフェースの全てのトラフィックを分析するため、CPUに負荷がかかる可能性がありますので、設定の際には注意する必要があります。

RMON Statistics(OID 1.3.6.1.2.1.16.1)はデバイスが測定した各種、ネットワーク統計に関連のオブジェクトを含めてネットワークのトラフィック量、平均パケットサイズ、ブロードキャストの回数、発生したエラー数、一定のサイズを持つパケットの数を測定して報告します。
 - Owner : 所有者に対する情報を登録します。

1.20.1 RMON Statsを設定するためには、下記のコマンドをご使用ください。

コマンド	モード	機　能
rmon collection stats <1-65535> [owner *WORD*]	INTERFACE	RMON Statisticを設定します。

1.20.2 RMON Statsを確認するためには、下記のコマンドをご使用ください。

コマンド	モード	機　能
show rmon statistics	TOP	RMON Statistic設定を確認します。

1.20.3 RMON Statsを初期化するためには、下記のコマンドをご使用ください。

コマンド	モード	機　能
no rmon collection stats <1-65535>	INTERFACE	RMON Statistic設定を削除します。

<例題1> RMON Stats設定及び確認

```
SG2024G#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SG2024G(config)#
SG2024G(config)#interface ge1
SG2024G(config-if)#rmon collection stats 1
SG2024G(config-if)#end
SG2024G#
SG2024G#show rmon statistics
 ==============================
    etherStatsIndex : 1
    etherStatsDataSource : 5001
    etherStatsDropEvents : 0
    etherStatsOctets : 545,461,731
    etherStatsPkts : 8,522,273
    etherStatsBroadcastPkts : 8,521,522
    etherStatsMulticastPkts : 20,366
    etherStatsCRCAlignErrors : 0
    etherStatsUndersizePkts : 0
    etherStatsOversizePkts : 0
    etherStatsFragments : 0
    etherStatsJabbers : 0
    etherStatsCollisions : 0
    etherStatsPkts64Octets : 17,125,238
    etherStatsPkts65to127Octets : 893
    etherStatsPkts128to255Octets : 533
    etherStatsPkts256to511Octets : 160
    etherStatsPkts521to1023Octets : 1
    etherStatsPkts1024to1518Octets : 0
    etherStatsOwner :
    etherStatsStatus : 1

SG2024G#
```

参考	RMON Statsは一つのインタフェースに重複して設定できません。 指定したStats Indexを他のインタフェースに重複して設定した場合、 最後に登録したインタフェースがRMON Statsと設定されます。

1.21 IPv6 サポート

Management IPとして IPv4とIPv6のStatic設定が可能となりました。

1.21.1 IPv6を設定するためには、下記のコマンドをご使用ください。

コマンド	モード	機 能
ipv6 address ADDRESS [anycast]	INTERFACE	IPv6を設定します。

1.21.2 IPv6を確認するためには、下記のコマンドをご使用ください。

コマンド	モード	機 能
show running-config interaface *IFNAME*	TOP	インタフェースに設定されている マネージメントIPを確認します。

1.21.2 IPv6を削除するためには、下記のコマンドをご使用ください。

コマンド	モード	機 能
no ipv6 address ADDRESS	TOP	インタフェースに設定されている IPv6を削除します。

〈例題〉 Management IPv6設定

```
SG2024(config)#int vlan1.1
SG2024(config-if)#ipv6 address 3ffe:506::20/48
SG2024(config-if)#end
SG2024#show running-config interface vlan1.1
!
interface vlan1.1
 ip address 192.168.130.20/24
 ipv6 address fe80::21a:f4ff:fe00:541/64
 ipv6 address 3ffe:506::20/48
!
SG2024#
```

1.22 REMOTE SYSLOG設定

REMOTE SYSLOG機能はデフォルトでスイッチに格納されるSYSLOG情報を別途SYSLOGサーバに転送できる機能です。

SYSLOGプロセスが走っているサーバのIPを指定するとスイッチから発生する警報やイベントメッセージをリアルタイムで受信することができます。

例えば、SYSLOGのレベルを緊急(emergencies)・facility(kern)を指定してスイッチの各々のSYSLOGの管理を行うことができます。

1.22.1 REMOTE SYSLOGを設定するためには、下記のコマンドをご使用ください。

コマンド	モード	機　能
log trap {alerts | critical | debugging | emergencies | errors | informational | notifications | warnings}	CONFIG	SYSLOGレベルを設定します。
log syslog remote *ip-address*	CONFIG	リモートSYSLOGサーバを指定します。
log syslog facility {auth | authpriv | cron | daemon | ftp | kern | local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7 | lpr | mail | news | syslog | user | uucp}	CONFIG	SYSLOGのFacility キーワードを設定します。 ※ デフォルト：local7

1.22.2 REMOTE SYSLOG設定を確認するためには、下記のコマンドをご使用ください。

コマンド	モード	機　能
show log syslog {config | remote}	TOP	SYSLOG設定情報を確認します。

1.22.3 REMOTE SYSLOG設定を初期化するためには、下記のコマンドをご使用ください。

コマンド	モード	機　能
no log trap	CONFIG	SYSLOGレベルを初期化します。
no log syslog remote *ip-address*	CONFIG	リモートSYSLOGサーバを解除します。
no log syslog facility	CONFIG	SYSLOGのFacility キーワードを初期化します。

<예제> 이벤트 발생시, remote syslog 서버(IP주소:192.168.100.1)에 전송하도록 설정

```
SG2024G#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SG2024G(config)#log syslog remote 192.168.100.1
SG2024G(config)#log syslog facility local7
SG2024G(config)#exit
SG2024G#
SG2024G#show log syslog config
------------------------------
      syslog configuartion
------------------------------
     trap level : informational
record priority : No
------------------------------

SG2024G#
SG2024G#show running-config | include remote
log syslog remote 192.168.100.1
SG2024G#
```

참照

1. remote Syslog서버는 최대10개까지 설정할 수 있습니다.
2. The syslog source facilities

auth	Login Authentication Messages
authpriv	Security/Authorization Messages
cron	Clock Daemon Messages
daemon	System Daemons Messages
ftp	FTP Daemon Messages
kern	The Kernel Messages
local0 through local7	As Defined Locally
lpr	The Line Printer Subsystem Messages
mail	Mail System Messages
news	Network News Subsystem Messages
syslog	Messages Generated Internally by Syslogd
user	User-Level Messages
uucp	The UUCP Subsystem Messages

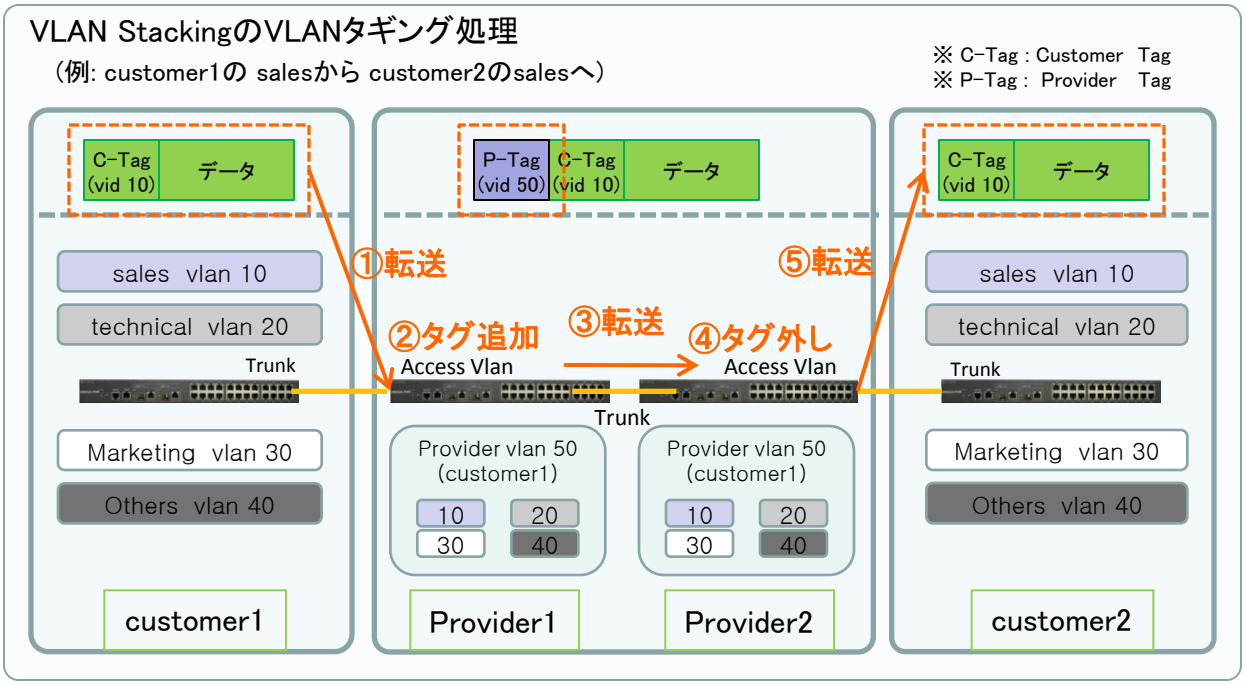
1.23 VLAN Stacking (QinQ)設定

VLAN StackingはVLANネットワーク間の通信を共通する一つのVLANによってグループ化する機能であり、IEEE 802.1ad に規約されています。

また、802.1QタグVLANにもう一つのVLAN ID (タグ)を付けて転送する方式で複数のVLANをグループ化することができます。
これはIEEE 802.1Q Tagged VLANの 生成可能範囲(1～4096)よりVLANを拡張できる効果があり、VLANの構成・変更作業をスムーズに行うことができます。

VLAN StackingはドキュメントまたはベンダーによってQinQ, Provider BridgeまたはDouble Q-Tagとも呼ばれています。

VLAN Stacking環境ではスイッチをProvider側とcustomer側に分類します。



Customer1からCustomer2へ通信する方法は構成図と以下の通りになります。

① Customer1(sales vlan 10)からProvider1へデータが転送されます。

② Provider1はCustomer1から受信したデータにもう一つのタグ(Provider Tag VLAN 50)を付けます。

③ 項目②のデータをProvider2に転送します。

④ Provider2はProvider1から転送されてきたデータの中でタグ(Provider Tag VLAN 50)を外します。

⑤ Provider2は項目④のデータをcustomer2に転送します。

1.23.1 VLAN Stackingを設定するためには、下記のコマンドをご使用ください。

コマンド	モード	機 能
Interface range *PORTRANGE*	CONFIG	インタフェースの範囲を設定します。
switchport mode trunk	INTERFACE	インタフェースをtrunkモードに設定します。
switchport trunk allowed vlan {add | remove} *VLANRANGE*	INTERFACE	インタフェースにVLANを設定します。
switchport vlan-stacking {customer-edge-port | provider-port}	INTERFACE	VLAN Stackingの種類を設定します。

1.23.2 VLAN Stacking設定を確認するためには、下記のコマンドをご使用ください。

コマンド	モード	機 能
show vlan {*VID* | brief}	TOP	VLAN情報及びメンバーを確認します。

1.23.3 VLAN Stacking設定を初期化するためには、下記のコマンドをご使用ください。

コマンド	モード	機 能
switchport mode access	INTERFACE	インタフェースをACCESSモードに設定します。
no switchport trunk	INTERFACE	インタフェースをtrunkモードからACCESSモードに設定します。 ※ VLAN IDはデフォルトVLAN IDが設定されます。
no switchport vlan-stacking	INTERFACE	VLAN Stackingの種類設定を初期化します。

参照

1. ProviderとCustomer Switchは同じVLANを使っても通信はできません。ProviderとCustomer Switchが通信するためにはVLAN Stackingで構成されるVLAN以外に別途VLANを設定する必要があります。
2. Provider SwitchはCustomer Switchと接続しているインタフェースをAccessモードでCustomer SwitchはTrunkモードに設定する必要があります。

<例題> VLAN Stacking設定
- Customer1 : vlan10(ge1-10, sales), vlan20(ge11-15, technical),
  vlan30(ge16-18, Marketing), vlan40(ge19-20, Others),
  ge24 - Provider1と接続(trunk)
- Provider1 : ge2 customer1と接続(Customer1 vlanの代表VID設定)
  ge1 Provider2と接続(VLAN StackingのためのTrunk VID設定)
- Provider2 : ge2 customer2と接続(Customer1 vlanの代表VID設定)
  ge1 Provider1と接続 (VLAN StackingのためのTrunk VID設定)
- Customer2 : vlan10(ge1-10, sales), vlan20(ge11-15, technical),
  vlan30(ge16-18, Marketing), vlan40(ge19-20, Others),
  ge24 - Provider2と接続(trunk)

```
================================================================================
                                Customer1設定
================================================================================

Customer1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Customer1(config)#vlan database
Customer1(config-vlan)#vlan range 10,20,30,40,50 bridge 1
Customer1(config-vlan)#exit
Customer1(config)#interface vlan1.50
Customer1(config-if)#ip address 192.168.50.2/24
Customer1(config-if)#exit
Customer1(config)#interface ge24
Customer1(config-if)#switchport mode trunk
Customer1(config-if)#switchport trunk allowed vlan add 10,20,30,40,50
Customer1(config-if)#exit
Customer1(config)#interface range ge1-10
% ge1-10 Selected
Customer1(config-if-range)#switchport access vlan 10
% ge1-10 Selected
Customer1(config-if-range)#exit
Customer1(config)#interface range ge11-15
% ge11-15 Selected
Customer1(config-if-range)#switchport access vlan 20
% ge11-15 Selected
Customer1(config-if-range)#exit
Customer1(config)#interface range ge16-18
% ge16-18 Selected
Customer1(config-if-range)#switchport access vlan 30
% ge16-18 Selected
Customer1(config-if-range)#exit
Customer1(config)#interface range ge19-20
% ge19-20 Selected
Customer1(config-if-range)#switchport access vlan 40
% ge19-20 Selected
Customer1(config-if-range)#exit
Customer1(config)#exit
Customer1#
```

```
Customer1#show vlan brief
                                    Bridge Group : 1

VLAN ID    Name             State   Member ports (u)-Untagged, (t)-Tagged
========= ================ ======= ============================================
1          default          ACTIVE  ge21(u) ge22(u) ge23(u) ge24(u)
10         VLAN0010         ACTIVE  ge24(t) ge1(u) ge2(u) ge3(u) ge4(u) ge5(u)
                                    ge6(u) ge7(u) ge8(u) ge9(u) ge10(u)
20         VLAN0020         ACTIVE  ge24(t) ge11(u) ge12(u) ge13(u) ge14(u)
                                    ge15(u)
30         VLAN0030         ACTIVE  ge24(t) ge16(u) ge17(u) ge18(u)
40         VLAN0040         ACTIVE  ge24(t) ge19(u) ge20(u)
50         VLAN0050         ACTIVE  ge24(t)

Customer1#
```

Provider1設定

```
Provider1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Provider1(config)#vlan database
Provider1(config-vlan)#vlan 50 bridge 1
Provider1(config-vlan)#exit
Provider1(config)#interface vlan1.50
Provider1(config-if)#ip address 192.168.50.3/24
Provider1(config-if)#exit
Provider1(config)#interface ge2
Provider1(config-if)#switchport access vlan 50
Provider1(config-if)#switchport vlan-stacking customer-edge-port
Provider1(config-if)#exit
Provider1(config)#interface ge1
Provider1(config-if)#switchport mode trunk
Provider1(config-if)#switchport trunk allowed vlan add 50
Provider1(config-if)#switchport vlan-stacking provider-port
Provider1(config-if)#end
Provider1#show vlan brief
                                    Bridge Group : 1

VLAN ID    Name             State   Member ports (u)-Untagged, (t)-Tagged
========= ================ ======= ============================================
1          default          ACTIVE  ge3(u) ge4(u) ge5(u) ge6(u) ge7(u) ge8(u)
                                    ge9(u) ge10(u) ge11(u) ge12(u) ge13(u)
                                    ge14(u) ge15(u) ge16(u) ge17(u) ge18(u)
                                    ge19(u) ge20(u) ge21(u) ge22(u) ge23(u)
                                    ge24(u) ge1(u)
50         VLAN0050         ACTIVE  ge2(u) ge1(t)

Provider1#
```

Customer1の代表VID

Customer1と接続

Provider2 Stacking VID

Provider2と接続

```
================================================================================
                                Provicer2設定
================================================================================

Provider2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Provider2(config)#vlan database
Provider2(config-vlan)#vlan 50 bridge 1
Provider2(config-vlan)#exit
Provider2(config)#interface vlan1.50
Provider2(config-if)#ip address 192.168.50.4/24
Provider2(config-if)#exit
Provider2(config)#interface ge2
Provider2(config-if)#switchport access vlan 50 ──→ Customer2の代表VID
Provider2(config-if)#switchport vlan-stacking customer-edge-port
Provider2(config-if)#exit                          ──→ Customer2と接続
Provider2(config)#interface ge1
Provider2(config-if)#switchport mode trunk
Provider2(config-if)#switchport trunk allowed vlan add 50 ──→ Provider1 Stacking VID
Provider2(config-if)#switchport vlan-stacking provider-port ──→ Provider1と接続
Provider2(config-if)#end
Provider2#show vlan brief
                                  Bridge Group : 1

VLAN ID    Name            State   Member ports (u)-Untagged, (t)-Tagged
========= ================ ======= ========================================
1          default          ACTIVE  ge3(u) ge4(u) ge5(u) ge6(u) ge7(u) ge8(u)
                                    ge9(u) ge10(u) ge11(u) ge12(u) ge13(u)
                                    ge14(u) ge15(u) ge16(u) ge17(u) ge18(u)
                                    ge19(u) ge20(u) ge21(u) ge22(u) ge23(u)
                                    ge24(u) ge1(u)
50         VLAN0050         ACTIVE  ge2(u) ge1(t)

Provider2#

================================================================================
                                Customer2設定
================================================================================
Customer2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Customer2(config)#vlan database
Customer2(config-vlan)#vlan range 10,20,30,40,50 bridge 1
Customer2(config-vlan)#exit
Customer2(config)#interface vlan1.50
Customer2(config-if)#ip address 192.168.50.5/24
Customer2(config-if)#exit
Customer2(config)#interface ge24
Customer2(config-if)#switchport mode trunk
Customer2(config-if)#switchport trunk allowed vlan ad 10,20,30,40,50
Customer2(config-if)#exit
```

```
Customer2(config)#interface rang ge1-10
% ge1-10 Selected
Customer2(config-if-range)#switchport access vlan 10
% ge1-10 Selected
Customer2(config-if-range)#exit
Customer2(config)#interface range ge11-15
% ge11-15 Selected
Customer2(config-if-range)#switchport access vlan 20
% ge11-15 Selected
Customer2(config-if-range)#exit
Customer2(config)#interface range ge16-18
% ge16-18 Selected
Customer2(config-if-range)#switchport access vlan 30
% ge16-18 Selected
Customer2(config-if-range)#exit
Customer2(config)#interface range ge19-20
% ge19-20 Selected
Customer2(config-if-range)#switchport access vlan 40
% ge19-20 Selected
Customer2(config-if-range)#end
Customer2#show vlan brief
                                  Bridge Group : 1

VLAN ID    Name             State   Member ports (u)-Untagged, (t)-Tagged
========= ================ ======= ============================================
1         default          ACTIVE  ge21(u) ge22(u) ge23(u) ge24(u)
10        VLAN0010         ACTIVE  ge24(t) ge1(u) ge2(u) ge3(u) ge4(u) ge5(u)
                                   ge6(u) ge7(u) ge8(u) ge9(u) ge10(u)
20        VLAN0020         ACTIVE  ge24(t) ge11(u) ge12(u) ge13(u) ge14(u)
                                   ge15(u)
30        VLAN0030         ACTIVE  ge24(t) ge16(u) ge17(u) ge18(u)
40        VLAN0040         ACTIVE  ge24(t) ge19(u) ge20(u)
50        VLAN0050         ACTIVE  ge24(t)

Customer2#
```

1.24 port-security

port security はスイッチのインタフェースに接続可能なMACアドレスの数を制限し、設定したMACアドレスのみネットワークを使用可能にする機能です。port securityが適用されたインタフェースではmax-macsに制限された登録範囲以内であれば、設定したMACアドレスが他のMACアドレスより優先登録されます。

スイッチはインタフェースにport securityを設定した場合、転送されてきたMACアドレスをMACアドレステーブルに固定で登録します。これにより登録されているMACアドレスが他のインタフェースによって使用できないため、セキュリティを向上させることができます。

port security を設定するためにはmax-macsを優先的に設定します。また、VLAN IDを入力しなかった場合はPVID値が設定されます。
但し、Default VLANの場合には表示されません。

設定解除はmax-macs設定とport security機能が両方適用されている場合、max-macs 機能を解除すると、port security機能は自動的に解除されます。

1.24.1 Port securityを設定するためには、下記のコマンドをご使用ください。

コマンド	モード	機　能
max-macs <0-8192> | <0-32768>	INTERFACE	インタフェース別登録可能なMACアドレスの数を設定します。 ※ SG2024、SG2024PoEは <0-8192> ※ SG2024G/48Gは <0-32768>
max-macs mac-address ***MAC_Address*** **[*VLANID*]**	INTERFACE	インタフェイスにport securityを設定します。

1.24.2 Port securityを確認するためには、下記のコマンドをご使用ください。

コマンド	モード	機　能
show max-macs	TOP	MACアドレス制限設定を確認します。

1.24.3 Port securityを初期化するためには、下記のコマンドをご使用ください。

コマンド	モード	機　能
no max-macs	INTERFACE	インタフェース別MACアドレス制限を解除します。
no max-macs mac-address ***MAC_Address***	INTERFACE	port securityを解除します。

〈例題〉Port Security設定

```
SG2024G#show bridge
bridge       VLAN port      mac            fwd timeout
1            1    ge1       0000.0000.000e 1    300
1            1    ge1       0000.0000.0014 1    300
1            1    ge1       0000.0000.0019 1    300
1            1    ge2       0000.1200.0000 1    300
1            1    ge2       0000.1300.0000 1    300
1            1    ge2       0000.1400.0000 1    300
1            1    ge2       0000.1600.0000 1    300
 MAC Count = 7
SG2024G#
SG2024G#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SG2024G(config)#interface ge1
SG2024G(config-if)#max-macs 2
SG2024G(config-if)#max-macs mac-address 0000.0000.0001
SG2024G(config-if)#max-macs mac-address 0000.0000.0002 10
SG2024G(config-if)#end
SG2024G#
SG2024G#show bridge
bridge       VLAN port      mac            fwd timeout
1            1    ge1       0000.0000.0001 1    0
1            10   ge1       0000.0000.0002 1    0
1            1    ge2       0000.1200.0000 1    300
1            1    ge2       0000.1300.0000 1    300
1            1    ge2       0000.1400.0000 1    300
1            1    ge2       0000.1600.0000 1    300
 MAC Count = 6
SG2024G#
SG2024G#show max-macs
ge2     :       2/2       (current/max macs)
SG2024G#
```

 参照	max-macs数を変更した場合、Port Securityの設定内容も解除されますので、Port Security機能も改めて設定する必要があります。

1.25 MLS (Multi-Layer Switch) DoS機能

MLS (Multi-Layer Switch) DoS機能は、スイッチングファブリックからパケットヘッダーを分析し、該当するトラフィックを遮断します。

MLS DoSで遮断が可能なトラフィックは以下の通りです。

- icmpfragments : ICMP Fragmentedであれば遮断
- macsaequalmacda : 送信元MACアドレスと宛先MACアドレスと同じであれば遮断
- sipequaldip : 送信元IPアドレスと宛先IPアドレスが同じであれば遮断
- tcpflagsfup : TCPのFIN、URG、PSHフラグが設定されていてシーケンス番号が0であれば遮断
- tcpflagssf : TCPのSYN、FINフラグが同時に有効に設定されていると遮断
- tcpportsequal : TCPの送信元と宛先のポート番号が同じであれば遮断
- udpportsequal : UDPの送信元と宛先が同じであれば遮断

遮断パターンに当てはまるパケットはスイッチングファブリックから遮断されてしまうため、別途遮断ログを残しません。

1.25.1 MLS DoS機能を設定するためには、下記のコマンドをご使用ください。

コマンド	モード	機　能
mls dos	CONFIG	mls dos機能を有効にします。
mls dos-option {icmpfragments | macsaequalmacda | sipequaldip | tcpflagsfup | tcpflagssf | tcpportsequal | udpportsequal}	CONFIG	mls dos機能で遮断する項目を設定します。

1.25.2 MLS DoS機能の設定内容を確認するためには、下記のコマンドをご使用ください。

コマンド	モード	機　能
show running-config | include mls	TOP	mls dos機能の設定情報を確認します。

1.25.3 MLS DoS機能の設定内容を初期化するためには、下記のコマンドをご使用ください。

コマンド	モード	機　能
no mls dos	CONFIG	mls dos機能を無効にします。
no mls dos-option {icmpfragments | macsaequalmacda | sipequaldip | tcpflagsfup | tcpflagssf | tcpportsequal | udpportsequal}	CONFIG	mls dos機能で遮断する項目の設定を解除します。

〈例題〉 mls dos設定

```
SG2024G#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SG2024G(config)#mls dos-option icmpfragments
SG2024G(config)#mls dos-option macsaequalmacda
SG2024G(config)#mls dos-option sipequaldip
SG2024G(config)#mls dos-option tcpflagsfup
SG2024G(config)#mls dos-option tcpflagssf
SG2024G(config)#mls dos-option tcpportsequal
SG2024G(config)#mls dos-option udpportsequal
SG2024G(config)#mls dos
SG2024G(config)#
SG2024G(config)#show running-config | include mls
mls qos enable
 mls dos
 mls dos-option sipequaldip
 mls dos-option macsaequalmacda
 mls dos-option icmpfragments
 mls dos-option udpportsequal
 mls dos-option tcpportsequal
 mls dos-option tcpflagssf
 mls dos-option tcpflagsfup
SG2024G(config)#
```

 注意	1. mls dos機能を有効にする場合、遮断されるトラフィックのログは記録されないため、遮断されたパケットに対して はモニタリングできる方法はありません。 2. スイッチが起動しているネットワーク上で遮断パターンに当てはまるパケットを送受信するアプリケーションを使用する場合、障害が発生するため、mls dos機能を設定する際に設定内容をもう一度確認する必要があります。