

SDMテンプレートの確認

```
Switch#show sdm prefer
```

The current template is "desktop default" template.

The selected template optimizes the resources in the switch to support this level of features for 8 routed interfaces and 1024 VLANs.

number of unicast mac addresses:	6K
number of IPv4 IGMP groups + multicast routes:	1K
number of IPv4 unicast routes:	8K
number of directly-connected IPv4 hosts:	6K
number of indirect IPv4 routes:	2K
number of IPv4 policy based routing aces:	0
number of IPv4/MAC qos aces:	0.5K
number of IPv4/MAC security aces:	0.875k

この例ではdesktop defaultが使用されている

SDMテンプレートの変更

```
Switch(config)#sdm prefer ?
```

access	Access bias
default	Default bias
dual-ipv4-and-ipv6	Support both IPv4 and IPv6
indirect-ipv4-and-ipv6-routing	Supports more V4 and V6 Indirect Routes
lanbase-routing	Supports both IPv4 and IPv6 Static Routing
routing	Unicast bias
vlan	VLAN bias

SDMテンプレートの変更を適用するためには、設定後に再起動が必要

問題が常時発生していない場合

```
Switch(config)#process cpu threshold type ?  
  interrupt  interrupt level utilization  
  process    process level utilization  
  total      total cpu utilization
```

```
Switch(config)#process cpu threshold type total rising 70 interval 15
```

CPU使用率がある一定の値を越えたら、ロギングを行う様に設定できる
使用率は合計/Process Level/Interrupt Levelを指定できる

```
%SYS-1-CPURISINGTHRESHOLD:Threshold: Process CPU Utilization(Total/Intr): 9%/0%, Top 3  
processes(Pid/Util): 214/3%, 153/0%, 159/0%
```

問題が常時発生していない場合

```
event manager applet DETECT_CPU
event syslog pattern "SYS-1-CPURISINGTHRESHOLD"
action 1 cli command "enable"
action 2 cli command "show proc cpu sort | append slot0:cpu_sorted"
action 3 cli command "show proc cpu history | append slot0:cpu_his"
action 4 cli command "show platform health | append slot0:cpu_health"
action 6 cli command "show log | append slot0:cpu_log"
```

EEMを使用し、SYS-1-CPURISINGTHRESHOLD のロギングをトリガとして、コマンドを実行させる

この例では、show process cpu sorted, show process history, show platform health, show logを実行し、その出力をslot0:に保存

CPU使用率が一時的に上昇する場合でも、必要なログが取得できる

Catalyst4500 COPP

- Catalyst4500シリーズスイッチでは、Control Plane Policing (COPP)という機能が使用できる
- COPPは、CPUが受信するパケットをPolicingし、CPUが大量のパケットを受信してリソースを消費する事を防ぐ
- Catalyst4500シリーズスイッチでのCOPPは、SupervisorのH/Wで行われる
- あらかじめ定義されているclassを使用して設定する事も、ACLとclassを新たに定義して設定する事もできる

Catalyst4500 COPP

```
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#qos
Switch(config)#macro global apply system-cpp
Switch(config)#policy-map system-cpp-policy
Switch(config-pmap)#class system-cpp-cdp
Switch(config-pmap-c)#police 32000 1000 conform-action transmit exceed-action drop
```

QOSをEnableにし、macro global apply system-cppを設定する
system-cpp-policyというpolicy mapを必ず使用する

この例では、あらかじめ定義されているclass system-cpp-cdpを使用して
CDPパケットをpolicingの対象としている

Catalyst4500 COPP

```
Switch#show policy-map system-cpp-policy
-----SNIP-----
Policy Map system-cpp-policy
  Class system-cpp-dot1x
  Class system-cpp-bpdu-range
  Class system-cpp-cdp
  police cir 32000 bc 1000
    conform-action transmit
    exceed-action drop
  Class system-cpp-sstp
  Class system-cpp-ospf
  Class system-cpp-igmp
  Class system-cpp-pim
  Class system-cpp-all-systems-on-subnet
  Class system-cpp-all-routers-on-subnet
  Class system-cpp-ripv2
  Class system-cpp-hsrpv2
  Class system-cpp-ip-mcast-linklocal
  Class system-cpp-dhcp-cs
  Class system-cpp-dhcp-sc
  Class system-cpp-dhcp-ss
  Class class-default
```

Catalyst6500 Rate Limiter

```
Switch(config)# mls rate-limit ?
  all          Rate Limiting for both Unicast and Multicast packets
  layer2       layer2 protocol cases
  multicast    Rate limiting for Multicast packets
  unicast      Rate limiting for Unicast packets
Switch(config)# mls rate-limit unicast ?
  acl  ACL BRIDGE results
  cef  CEF cases
  ip   IP packets
Switch(config)# mls rate-limit unicast ip icmp ?
  redirect    packets requiring ICMP redirect (same VLAN)
  unreachable packets requiring ICMP unreachable message
Switch(config)# mls rate-limit unicast ip icmp redirect ?
  <0-0>       no packets up to the RP
  <10-1000000> packets per second
Switch(config)# mls rate-limit unicast ip icmp redirect 1000
```

PFCやDFCでH/W処理される

COPPと重複した場合には、Rate limiterが優先

Catalyst 6500 Rate Limiter

```
BROWBRO#show mls rate-limit
```

```
Sharing Codes: S - static, D - dynamic
```

```
Codes dynamic sharing: H - owner (head) of the group, g - guest of the group
```

Rate Limiter Type	Status	Packets/s	Burst	Sharing
MCAST NON RPF	Off	-	-	-
MCAST DFLT ADJ	On	100000	100	Not sharing
MCAST DIRECT CON	Off	-	-	-
ACL BRIDGED IN	Off	-	-	-
ACL BRIDGED OUT	Off	-	-	-
IP FEATURES	Off	-	-	-
ACL VACL LOG	On	2000	1	Not sharing
MAC PBF IN	Off	-	-	-
CEF RECEIVE	Off	-	-	-
CEF GLEAN	Off	-	-	-
MCAST PARTIAL SC	On	100000	100	Not sharing
IP RPF FAILURE	On	100	10	Group:0 S
TTL FAILURE	Off	-	-	-
ICMP UNREAC. NO-ROUTE	On	100	10	Group:0 S
ICMP UNREAC. ACL-DROP	On	100	10	Group:0 S
ICMP REDIRECT	On	1000	10	Not sharing

Catalyst6500 COPP

クラスを定義する

```
cat6500(config)# class-map <traffic_class_name>
```

```
cat6500(config-cmap)# match <access-group>
```

ポリシーを定義する

```
cat6500(config-pmap)# policy-map<service_policy_name>
```

```
cat6500(config-pmap)# class <traffic_class_name>
```

```
cat6500(config-pmap)# police <rate> conform-action transmit  
exceed-action drop
```

適用先にcontrol-planeを指定する

```
cat6500(config)# control-plane
```

```
cat6500(config-cp)#
```

ポリシーを適用する

```
cat6500(config-cp)# service-policy input <service_policy_name>
```

PFCやDFCでH/W処理される

MQCのCLIで設定

Policy Mapの適用先はcontrol-plane

Rate limiterと重複した場合には、Rate limiterが優先

Catalyst6500 COPP

```
! Define telnet class
class-map telnet-class
  match access-group 140

! Define ACL to select necessary telnet traffic

! Allow 3.3.3.3 trusted host traffic
access-list 140 deny tcp host 3.3.3.3 any eq telnet
! Allow 4.4.4.4 trusted host traffic
access-list 140 deny tcp host 4.4.4.4 any eq telnet
! All other inbound telnet traffic will be policed
access-list 140 permit tcp any any eq telnet

! Define policy
policy-map control-plane-policy
class telnet-class
! Police telnet class to 80kbps, drop excess
  police 80000

! Attach the policy
control-plane
  service-policy input control-plane-policy
```

Catalyst 6500 COPP

```
Switch# sh policy-map control-plane
Control Plane Interface
  Service policy cpp-test
Hardware Counters:
class-map: cpp-class1 (match-all)
  Match: access-group 111
  police :
    96000 bps 3000 limit 3000 extended limit
Earl in slot 6 :
  0 bytes
  5 minute offered rate 0 bps
  aggregate-forwarded 0 bytes action: transmit
  exceeded 0 bytes action: drop
  aggregate forward 0 bps exceed 0 bps
Software Counters:
Class-map: cpp-class1 (match-all) 0 packets, 0 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match: access-group 111
  police:
    100000 bps, 3125 limit, 3125 extended limit
    conformed 0 packets, 0 bytes; action: transmit
    exceeded 0 packets, 0 bytes; action: drop
    conformed 0 bps, exceed 0 bps, violate 0 bps
```

Catalyst 6500 COPP

- DFC搭載モジュールが存在する場合、DFCでCOPPが行われる
- ある特定のトラフィックにXというレートが設定されていた場合、各モジュールのDFCは、そのトラフィックを受信した場合、Xというレートに制限する
- DFC搭載モジュールが3枚あった場合、あるトラフィックはモジュールの数だけ、つまりXの3倍CPUへ送信される可能性がある
- Supervisorで $(N-1)X$ のトラフィックをDropし調節、この際S/W処理が発生する