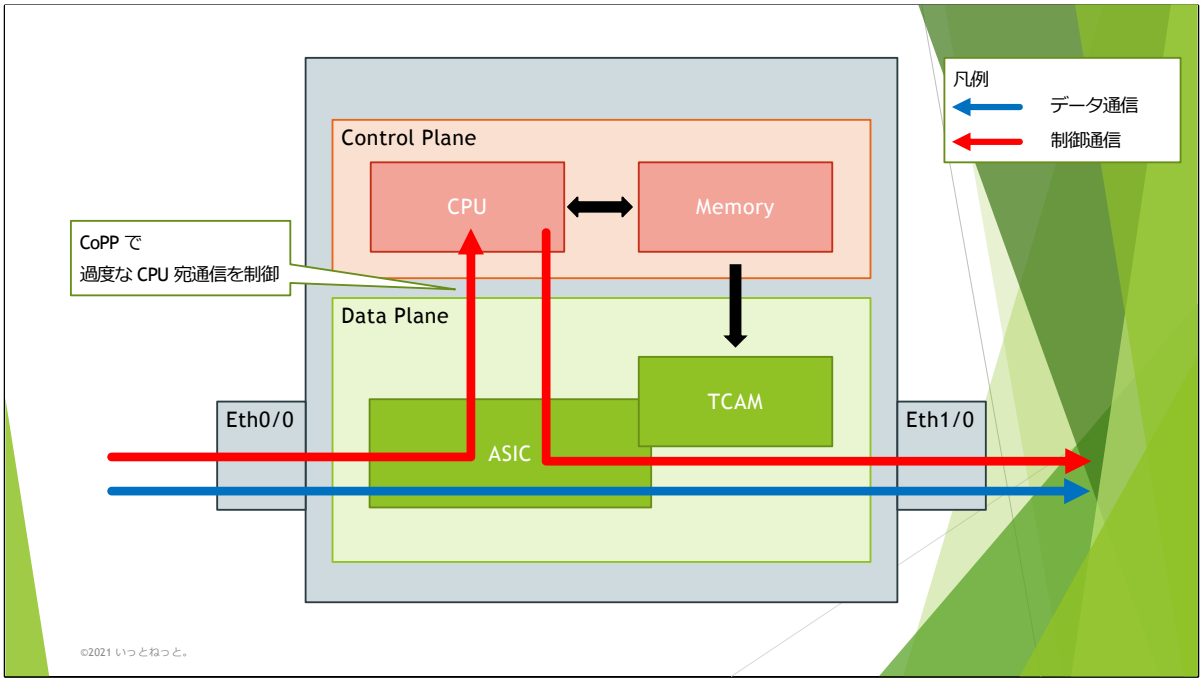
# CoPP の概要と設定

# Agenda

- CoPP の概要
- CoPP の設定

# CoPP の概要




CoPP (Control Plane Policing) とは、ネットワーク機器に過度な CPU 負荷がかかることを防ぐ機能である。

スライドではネットワーク機器の構成を簡単に図示している。
一般的に自身を通過するデータ通信は Data Plane で処理され、自身宛てや制御通信 (例えば OSPF Hello packet) は CPU で処理される。

そのため、 Control plane で処理されるパケットが大量に送りつけられると、ネットワーク機器の CPU 使用率が高騰してしまう恐れがある。

CoPP を用いると、以下のような制御が可能となり、過度な CPU 負荷を防ぐことができる。
・特定の通信が規定流量を超過した際に破棄する
・特定の通信を破棄する
…など

※現在の ネットワーク機器では、 セキュリティの観点から default で CoPP が設定されている製品も存在する。

# CoPP の設定

```
Step1, 疎通確認
RT1#ping 192.168.12.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.12.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/5/6 ms
---------------------------------------------------------------------------
RT1#ping 192.168.23.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.23.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/6 ms
```

```
Step2, ACLs を設定
RT2(config)#ip access-list extended ICMP
RT2(config-ext-nacl)#permit icmp any any
```

```
Step3, Class-map を設定
RT2(config)#class-map ICMP_CLASS
RT2(config-cmap)#match access-group name ICMP
```

```
Step4, Policy-map を設定
RT2(config)#policy-map CoPP
RT2(config-pmap)#class ICMP_CLASS
RT2(config-pmap-c)#drop
RT2(config-pmap-c)#exit
RT2(config-pmap)#exit
```

```
Step5, CoPP を設定
RT2(config)#control-plane
RT2(config-cp)#service-policy input CoPP
```


この例では、CoPP を用いて RT2 に着信する ICMP packet を破棄する。

まず、 RT1 から以下に対して問題なく疎通できることを確認している。
・RT2 (192.168.12.1)
・RT3 (192.168.23.3)

続いて CoPP を設定していくが、 CoPP は以下3つの STEP で設定していく。
(1) ACL の定義
(2) Class-map の定義
(3) Policy-map の定義

はじめに ICMP を対象とする ACL 「ICMP」 を定義する。
今回は通信を破棄するためのものだが、この ACL は ICMP を match させるものなので “permit” で記載する。

次に Class-map 「ICMP_CLASS」 を定義し、先ほど設定した ACL を紐づける。
これにより、 ICMP をこの class-map に分類させる。

続いてPolicy-map 「CoPP」 を定義し、 「ICMP_CLASS」 に分類された通信を破棄するように “drop” を定義する。

最後に 「CoPP」 を control-plane に紐づけることで、 CoPP を動作させる。

```
Step6, 疎通確認
RT1#ping 192.168.12.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.12.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
---------------------------------------------------------------------------
RT1#
RT1#ping 192.168.23.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.23.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/5/6 ms
```

```
Step7, 動作確認
RT2#show policy-map control-plane input
 Control Plane

  Service-policy input: CoPP

    Class-map: ICMP_CLASS (match-all)
      5 packets, 570 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: access-group name ICMP
      drop

    Class-map: class-default (match-any)
      2 packets, 738 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: any
```


その後、再度疎通確認を実施すると、 RT2 宛の ICMP が破棄されていることがわかる。
RT3 宛のような RT2 を経由する通信は CoPP の対象とならない。

また、 CoPP の動作状況を確認すると、 ICMP_CLASS に分類された通信が破棄されていることが数値としても確認できた。

※1
Policy-map では default で 「class-default」 が定義されており、どの Class-map にも分類されなかった通信は 「class-default」 として処理される。