



10時より開始します

Cisco Community Expert Series Community Live

Catalyst 8000 シリーズルーター - 概要とトラブルシューティング

張 家亮 (Jialiang Zhang)
Technical Consulting Engineer
Dec 6th, 2023



ご参加ありがとうございます



Download the Presentation!

本日の資料はこちらからダウンロードいただけます

<https://community.cisco.com/t5/-/-/ec-p/4946659>

セミナー登録

プレゼンテーション資料

音声ブロードキャストについて

[音声ブロードキャスト (Audio Broadcast)] ウィンドウが自動的に表示され、コンピュータのスピーカーから音声がかかります。

[音声ブロードキャスト (Audio Broadcast)] ウィンドウが表示されない場合は、[通話 (Communicate)] メニューから [音声ブロードキャスト (Audio Broadcast)] を選択します。

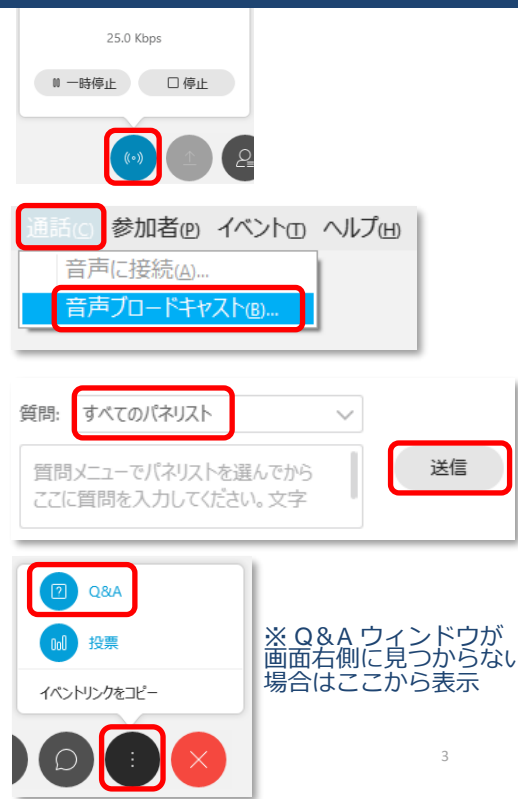
イベントが開始されると自動的に音声がかかります。

音声接続に関する詳細はこちらをご参照ください。

解決しない場合は、Q&A ウィンドウより

[すべてのパネリスト (All Panelists)] 宛にお知らせください。

<https://community.cisco.com/t5/-/-/ta-p/3129991>



ご質問方法

Community Live中のご質問は、
画面右側の Q&A ウィンドウから
すべてのパネリスト (All Panelists)
宛に送信してください



本日のエキスパートご紹介



Download the Presentation!

本日の資料をダウンロードしてお使いください

<https://community.cisco.com/t5/-/-/ec-p/4946659>

張 家亮 (Jialiang Zhang)

シスコシステムズ

グローバル カスタマー エクスペリエンス センター

テクニカル コンサルティング エンジニア



Cisco Community Expert Series Community Live

Catalyst 8000 シリーズルーター - 概要とトラブルシューティング

張 家亮 (Jialiang Zhang)
Technical Consulting Engineer
Dec 6th, 2023



はじめに

- 本セッションは、主に Catalyst 8000 シリーズルーターの Catalyst 8200/8300/8500 (autonomous モード) に基づき解説します
- 本セッションと Cisco.com 上の内容に差分がある場合には Cisco.com 上の内容が優先されます
- 本セッションの内容は 2023 年 12 月 6 日時点の情報となります
- 将来にわたり、情報・仕様等が更新される可能性があります

Agenda

1

Catalyst 8000 製品概要

- Catalyst 8200/8300/8500
- Catalyst 8000 Software

2

Catalyst 8000 トラブルシューティング

- CPU/Memory トラブルシューティング
- Packet トラブルシューティング
- その他トラブルシューティング

3

Catalyst 8000 不具合事例紹介

Catalyst 8000 製品概要

- Catalyst 8200/8300/8500
- Catalyst 8000 Software



投票質問 1

Passcode *

1206

slido

質問 1. Catalyst 8000 シリーズルータに関する知識・経験について以下より1つお選び下さい

- A. サービス環境での運用経験や構築経験があり、障害対応等の経験もある

- B. 検証環境などでの経験はあるが、実運用環境でのオペレーションには携わっていない

- C. トレーニング等で知識はあるが、設定や構築は行ったことがない

- D. 全く知識がない

Catalyst 8000 Edge Platform Family

x86

Headend



Catalyst 8500 Series

C8500-20X6C
C8500-12X4QC
C8500-12X
C8500L-8S4X

x86

Medium-Large
Branch

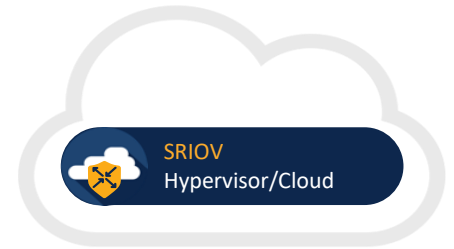


Catalyst 8300 Series

C8300-2N2S-4T2X
C8300-2N2S-6T
C8300-1N1S-4T2X
C8300-1N1S-6T

VNF

Cloud



Catalyst 8000V

x86

Small-Medium
Branch



Catalyst 8200 Series

C8200-1N-4T
C8200L-1N-4T

Autonomous Mode (IOS-XE) / Controller Mode (IOS-XE SD-WAN)

Catalyst 8000 License Subscription

Systems



DNA Subscription



Cisco DNA Premier



Cisco DNA Advantage



Cisco DNA Essentials

[Cisco DNA Software for SD-WAN and Routing Ordering Guide](#)

[Cisco DNA Subscription Software for SD-WAN and Routing FAQ](#)

Catalyst 8200 Series Edge Platforms

ISR4221

ISR4321

ISR4331

* Replacement Product



C8200-1N-4T



C8200L-1N-4T

1N = 1 NIM slot
4T = 4 1G Port
(1 PIM slot)

L = Lite
1N = 1 NIM slot
4T = 4 1G Port
(1 PIM slot)

* ISR4k の [End-of-Sale and End-of-Life Announcement](#) に記載されている Replacement Product になります。

Catalyst 8300 Series Edge Platforms

ISR4351

ISR4431

ISR4451

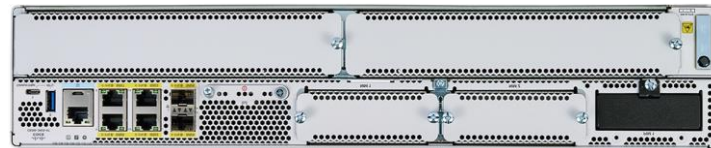
* Replacement Product



C8300-2N2S-4T2X



C8300-1N1S-4T2X



C8300-2N2S-6T



C8300-1N1S-6T




2N = 2 NIM Slot
2S = 2 SM slot
4T = 4 1G Port
2X = 2 SFP+
(1 PIM slot)

1N = 1 NIM Slot
1S = 1 SM slot
4T = 4 1G Port
2X = 2 SFP+
(1 PIM slot)

2N = 2 NIM Slot
2S = 2 SM slot
6T = 6 1G Port
(1 PIM slot)

1N = 1 NIM Slot
1S = 1 SM slot
6T = 6 1G Port
(1 PIM slot)

Catalyst 8200/8300 で利用可能なモジュール

Slot type	Module type	
Pluggable Interface Module (PIM)	LTE	
Service Module (SM) *8300 Only	LAN, WAN, VOICE, DSL, ASYNC	
Network Interface Module (NIM)	LAN, WAN, LTE, VOICE, DSL, ASYNC	

[Cisco Catalyst 8200 Series Edge Platforms Interfaces and Modules](#)

[Cisco Catalyst 8300 Series Edge Platforms Interfaces and Modules](#)

Catalyst 8500 Series Edge Platforms

ASR1001-X

ASR1002-X

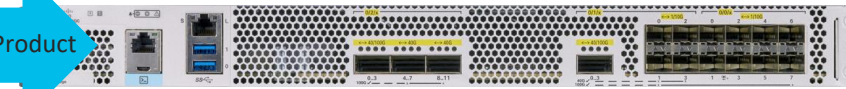
ASR1006

* Replacement Product



C8500-20X6C

6C = 6 QSFP
(6 port 40/100GE)
20X = 20 SFP+



C8500-12X4QC

4QC = 4 QSFP
(2-port 40/100GE +
2-port 40GE)
12X = 12 SFP+



C8500-12X

12X = 12 SFP+



C8500L-8S4X

8S = 8 SFP
4X = 4 SFP+

Catalyst 8200/8300/8500 で利用可能な SFP

- [Cisco Optics-to-Device Compatibility Matrix \(tmgmatrix\)](#) より確認可能

Begin your Search (Type in window)

8500

C8500 in Network Device Product Family

C8500-12X4QC in Network Device Product ID

C8500L-8S4X in Network Device Product ID

C8500-12X in Network Device Product ID

- FORM FACTOR
 - QSFP+ 67
 - QSFP28 50
 - SFP 59
 - SFP+ 106
 - CABLE TYPE
 - Search...
 - Cat5e/6A 6
 - Cat6A/7 1
 - Duplex Fiber 104
 - Parallel Fiber 12
 - +2 more
- TRANSCEIVER PRODUCT ID

C8500

Network Device Product ID	Transceiver Description										Software Release	
	Transceiver Product ID	Data Rate	Form Factor	Max. Reach	Cable Type	Media	Connector Type	Transceiver Type	Case Temp	DOM HW Capable	Minimum	DOM SW
C8500-12X4QC	QSFP-100G-SR4-S	100 Gbps	QSFP28	150m	Parallel Fiber	MMF	MPO-12 (UPC)	Optic	0 to 70C	Y	IOS XE 17.3.2	IOS XE 17.3.2
	QSFP-100G-CWDM4-S	100 Gbps	QSFP28	2km	Duplex Fiber	SMF	LC (UPC)	Optic	0 to 70C	Y	IOS XE 17.3.2	IOS XE 17.3.2
	QSFP-100G-PSM4-S	100 Gbps	QSFP28	500m	Parallel Fiber	SMF	MPO-12 (APC)	Optic	0 to 70C	Y	IOS XE 17.3.2	IOS XE 17.3.2
	QSFP-100G-LR4-S	100 Gbps	QSFP28	10km	Duplex Fiber	SMF	LC (UPC)	Optic	0 to 70C	Y	IOS XE 17.3.2	IOS XE 17.3.2

[tmgmatrix for Catalyst 8200](#)
[tmgmatrix for Catalyst 8300](#)
[tmgmatrix for Catalyst 8500](#)

Catalyst 8200/8300 Performance (1400Bytes)



C8200L-1N-4T

CEF: up to 3.8 Gbps
IPsec: up to 500 Mbps
SD-WAN IPsec: up to 500 Mbps



C8200-1N-4T

CEF: up to 3.8 Gbps
IPsec: up to 1 Gbps
SD-WAN IPsec: up to 1 Gbps



C8300-1N1S-6T

CEF: up to 19.7 Gbps
IPsec: up to 1.9 Gbps
SD-WAN IPsec: up to 1.9 Gbps



C8300-1N1S-4T2X

CEF: up to 19.7 Gbps
IPsec: up to 15.8 Gbps
SD-WAN IPsec: up to 15 Gbps



C8300-2N2S-6T

CEF: up to 19.7 Gbps
IPsec: up to 1.9 Gbps
SD-WAN IPsec: up to 1.9 Gbps



C8300-2N2S-4T2X

CEF: up to 19.7 Gbps
IPsec: up to 18.8 Gbps
SD-WAN IPsec: up to 18 Gbps

Catalyst 8500 Performance (1400Bytes)



C8500L-8S4X

CEF: up to 20 Gbps
IPsec: up to 12 Gbps
SD-WAN IPsec: up to 6.6 Gbps



C8500-12X

CEF: up to 120 Gbps
IPsec: up to 30 Gbps
SD-WAN IPsec: up to 22 Gbps



C8500-12X4QC

CEF: up to 200 Gbps
IPsec: up to 36 Gbps
SD-WAN IPsec: up to 33 Gbps



C8500-20X6C

CEF: up to 500 Gbps
IPsec: up to 150 Gbps
SD-WAN IPsec: up to 100 Gbps

Catalyst 8000 製品概要

- Catalyst 8200/8300/8500
- **Catalyst 8000 Software**



投票質問 2

Passcode *

1206

slido

質問 2. Catalyst 8000 シリーズルータでは以下のどの OS を使っていますか

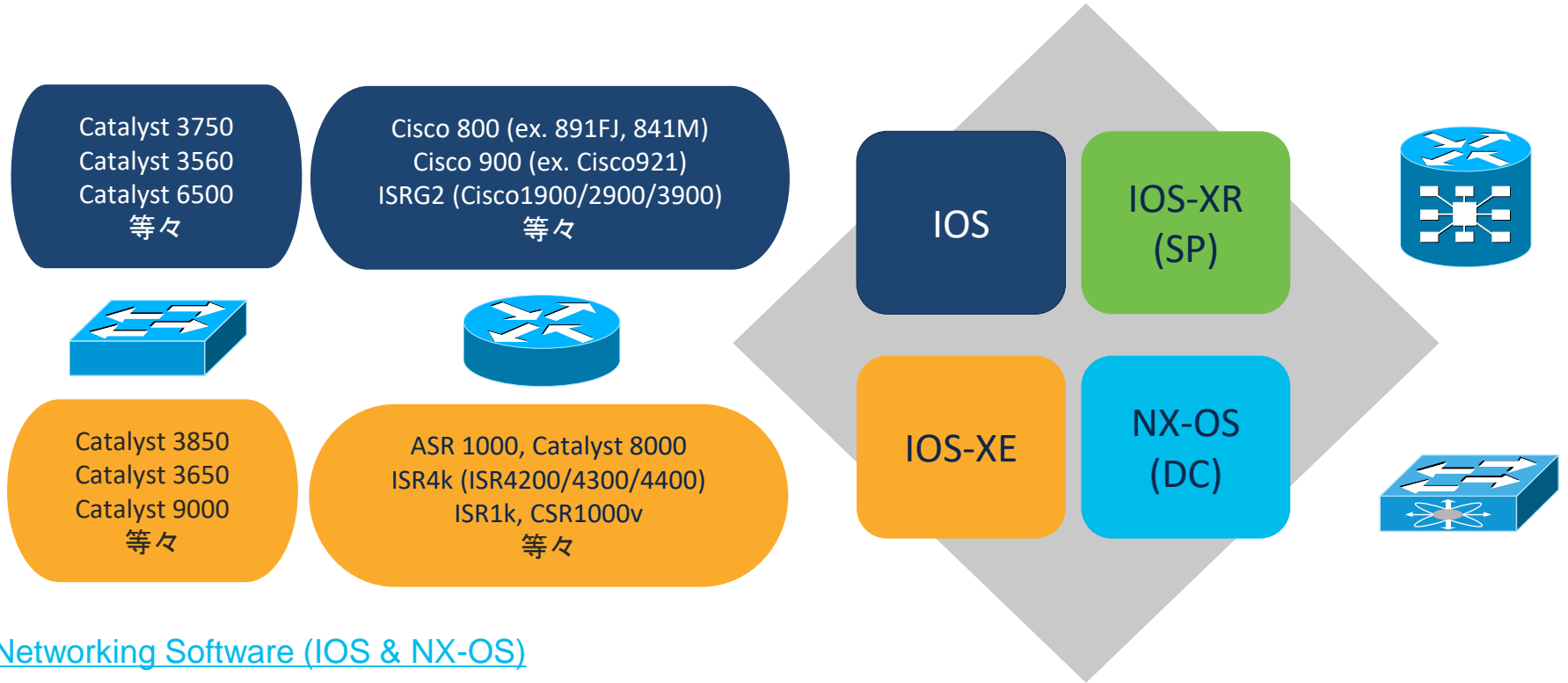
- A.IOS

- B.IOS-XE

- C.IOS-XR

- D.Viptela OS

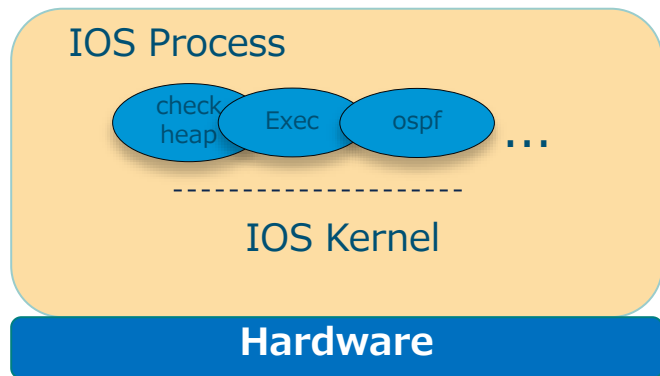
Network Software OS Overview



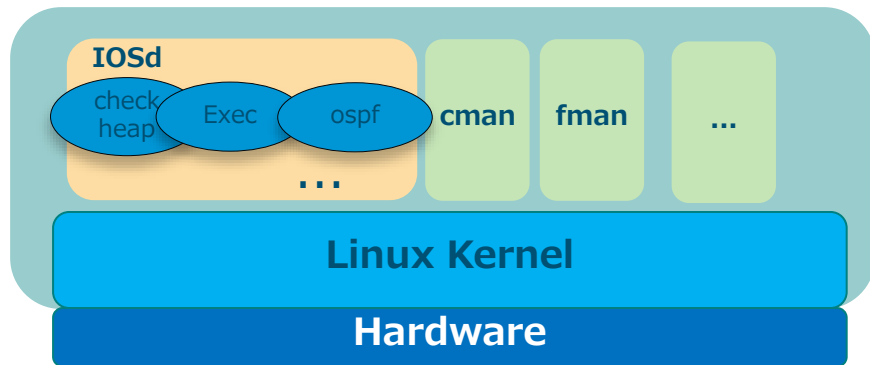
Networking Software (IOS & NX-OS)

IOS vs IOS-XE Software

IOS



IOS-XE



- IOSXE = IOSd + Linux process on Linux Kernel
 - Linux process には MAN が付いているプロセスが多い
- CMAN: Chassis Manager
FMAN: Forwarding Manager
IMAN: Interface Manager

Cisco IOS-XE – Polaris リリース



- Polaris (16.x ~) よりエンタープライズ系のプラットフォームを統一された S/W スタックで管理される
- 各製品分野では (例えば Router と Switch) 新しいバージョンのリリースが前後することがあるが、同じ 17.12.1 でも Switch 系は先にリリースされ 17.12.1 そのままとなる Router 系は後でリリースされ、その場で 17.12.1a となる
- 一緒にリリースされ S/W 名が完全一致の場合もある (17.12.2 など)

Catalyst 8000 における IOS-XE の扱い

- Cisco [Software Download](#) のサイトより

各モデルで現時点利用できる最小バージョン :

Catalyst 8200 --- Bengaluru - 17.4.1a

Catalyst 8200L --- Bengaluru - 17.5.1a

Catalyst 8300 --- Amsterdam - 17.3.2

Catalyst 8500 --- Amsterdam - 17.3.2

Catalyst 8500L --- Bengaluru - 17.4.1a

Catalyst 8000v --- Bengaluru - 17.4.1a

Cisco IOS-XE – Polaris リリース (17.x)

地名(都市)で命名されています

2020 Amsterdam

17.1, 17.2, 17.3 EM

2021 Bengaluru

17.4, 17.5, 17.6 EM

2022 Cupertino

17.7, 17.8, 17.9 EM

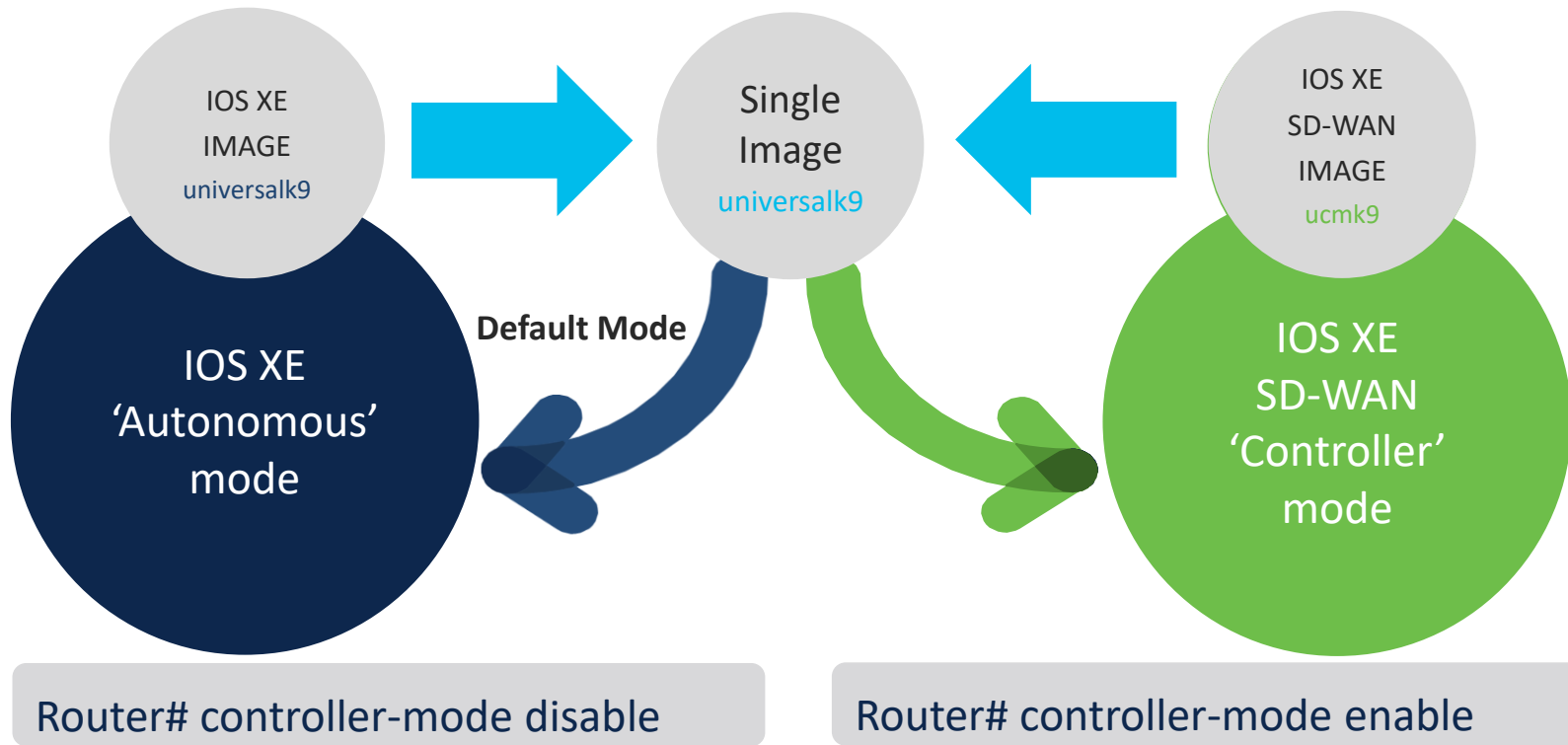
2023 Dublin

17.10, 17.11, 17.12 EM



※ EM : Extended Maintenance release

統合された Universal イメージ (17.2 以降)



Catalyst 8000 トラブル シューティング

- ・ CPU/Memory トラブルシューティング
- ・ Packet トラブルシューティング
- ・ その他トラブルシューティング



投票質問 3

Passcode *

1206

slido

質問 3. CPU/Memory トラブルシューティングで最も使われているコマンドはどれでしょうか

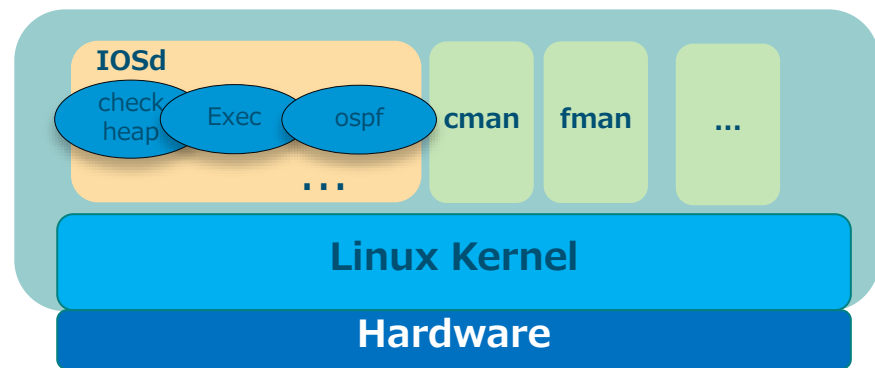
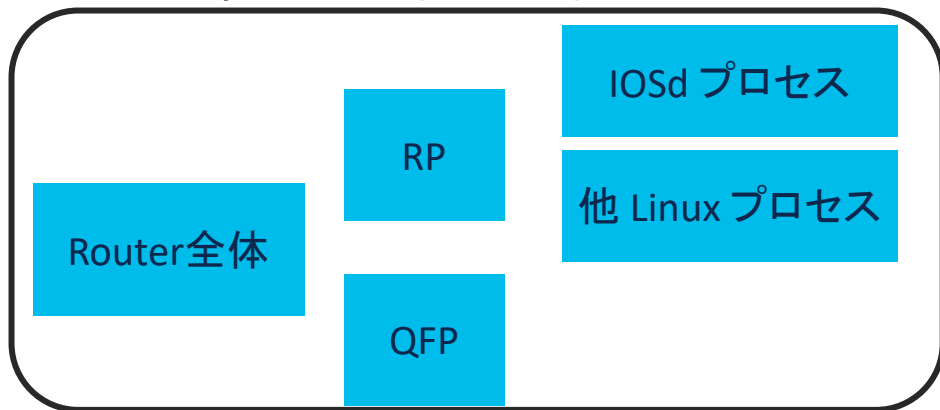
- A. show process cpu/memory
- B. show process cpu/memory platform
- C. show platform resource
- D. show platform software process slot R0 monitor cycles 1

CPU/Memory トラブルシューティングについて

- CPU/Memory はどちらもプロセス特定が一番重要
- IOS-XE の Process 特性を十分に理解する必要がある

IOS: show process cpu/memory による IOS プロセス確認

Catalyst 8000 (IOS-XE): コンポーネント毎に確認



CPU/Memory トラブルシューティングについて

- CPU: 何等かの処理により変化の激しさが特徴

継続的に高い Uti を示している場合、短時間複数回ログ取得が効果的

突発の上昇ですぐ落ち着く場合、後から詳細を追うことができない！

→ 上昇の瞬間、ログ取得を工夫する必要がある

- Devnet も活用しスクリプトで自動化取得を実現しよう

- EEM と エラーメッセージの組み合わせ技もある

[CPU 使用率が上昇した場合に自動的にログを取得する EEM の設定例*](#)

*その例は IOSd のみの監視となります。

CPU/Memory トラブルシューティングについて

- Memory: 問題があってもすぐに表に出ず時間経過により顕著化
短時間複数回ログ取得しても Diff が少ない、もしくはほとんどない!
 - 一> より長い時間間隔で、例えば日単位、もしくは2、3日毎に取得することで長い期間の傾向を少しづつ把握していく

動作保証のためある程度メモリを確保しているプロセスもある

- 一> 安定動作時のログも取り、後から正常性判断に役立つ

各段階に役立つ主要コマンド - RP(CP)



show platform resource
show platform software status control-processor brief

show platform software process slot RP active monitor cycles 1

[CPU]
show process cpu platform sorted
show process cpu platform history
[Memory]
show process memory platform sorted

通常、上記のような IOS-XE 共通のコマンドで確認可能

show platform resource

```
Router#show platform resource
```

```
**State Acronym: H - Healthy, W - Warning, C - Critical
```

Resource	Usage	Max	Warning	Critical	State
RPO (ok, active)					H
Control Processor	10.10%	100%	80%	90%	H
DRAM	2590MB (34%)	7562MB	88%	93%	H
bootflash	5110MB (70%)	7338MB	70%	90%	W
harddisk	797MB (6%)	14534MB	90%	95%	H
ESPO(ok, active)					H
QFP					H
DRAM	23311KB (4%)	524288KB	85%	95%	H
IRAM	207KB (10%)	2048KB	85%	95%	H
CPU Utilization	0.00%	100%	90%	95%	H

<以下省略>

RP/QFP 毎の CPU/Memory 利用状況

Warning/Critical 閾値も確認可能
%PLATFORM-4-ELEMENT_WARNING:
%PLATFORM-3-ELEMENT_CRITICAL:

show platform software status control-processor brief

```
Router#show platform software status control-processor brief
```

Load Average

Slot	Status	1-Min	5-Min	15-Min
RPO	Healthy	1.75	1.69	1.78

RPO 側の CPU Load Average

Memory (kB)

Slot	Status	Total	Used (Pct)	Free (Pct)	Committed (Pct)
RPO	Healthy	7743504	2663356 (34%)	5080148 (66%)	2938152 (38%)

RPO 側の Memory の利用状況

CPU Utilization

Slot	CPU	User	System	Nice	Idle	IRQ	SIRQ	IOwait
RPO	0	2.50	1.60	0.00	88.10	0.00	0.10	7.70
	1	0.00	0.00	0.00	100.00	0.00	0.00	0.00
	2	0.00	0.00	0.00	100.00	0.00	0.00	0.00
	3	0.00	0.00	0.00	100.00	0.00	0.00	0.00
	4	1.90	2.10	0.00	96.00	0.00	0.00	0.00

各 CPU コアの利用状況

<以下省略>

show platform software process slot RP active monitor cycles 1

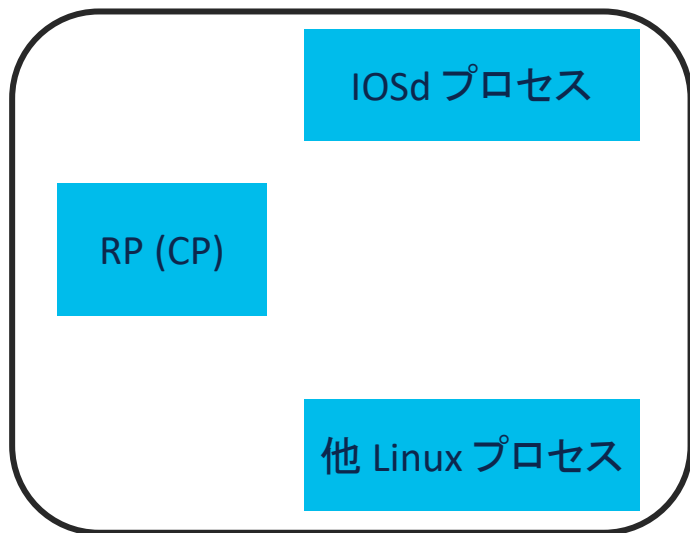
```
Router#show platform software process slot RP active monitor cycles 1
top - 06:54:04 up 4:45, 0 users, load average: 1.68, 1.77, 1.80
Tasks: 399 total, 1 running, 398 sleeping, 0 stopped, 0 zombie
%Cpu(s): 8.8 us, 2.1 sy, 0.0 ni, 89.1 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
MiB Mem : 7562.0 total, 1274.6 free, 2026.6 used, 4260.9 buff/cache
MiB Swap: 0.0 total, 0.0 free, 0.0 used. 5278.8 avail Mem
```

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
20018	root	20	0	2180372	208332	43364	S	143.8	2.7	404:27.04	ucode_pkt+
17105	root	20	0	6120	2036	1364	R	6.2	0.0	0:00.01	top
1	root	20	0	30864	28028	7944	S	0.0	0.4	0:03.41	systemd
2	root	20	0	0	0	0	S	0.0	0.0	0:00.01	kthreadd
3	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	rcu_gp
4	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	rcu_par_gp

<以下省略>

Process 毎の CPU/Memory の利用状況

各段階に役立つ主要コマンド – RP(CP)



[CPU]

```
show process cpu sorted
show process cpu history
show stack <PID>
show interfaces
show ip traffic
show ipv6 traffic
```

[Memory]

```
show process memory sorted
show process memory <PID>
show memory allocating-process totals
show buffers
show buffers leak
show ip traffic
show ipv6 traffic
```

```
show platform software process slot RP active monitor cycles 1
show platform software process list RP active
show platform software process list RP active process-id <PID>
```

通常、上記のような IOS-XE 共通のコマンドで確認可能

show process cpu sorted / show stack <PID>

```
Router#show process cpu sorted
```

```
CPU utilization for five seconds: 0%/0%; one minute: 0%; five minutes: 0%
```

PID	Runtime (ms)	Invoked	uSecs	5Sec	1Min	5Min	TTY	Process
9	22955	11321	2027	0.23%	0.03%	0.00%	0	Check heaps
141	39283	5186575	7	0.07%	0.03%	0.03%	0	SIS Punt Process
215	21685	1308076	16	0.07%	0.02%	0.00%	0	VRRS Main thread
228	23174	2605199	8	0.07%	0.02%	0.01%	0	IP ARP Retry Age
1	1	14	71	0.00%	0.00%	0.00%	0	Chunk Manager

<以下略>

IOSd 全体の利用状況
show process cpu history にて
最大過去72時間確認可能

各プロセスの利用状況

各プロセスのPID

```
Router#show stack 9
Process 9: Check heaps
Tracekey : 1#9f3cd903256c7b1670bada076c5a4c45
```

```
Stack segment 0x7F2401551000 - 0x7F2401556DC0
RSP: 0x7F2401556D10, PC: :555EB14D9000+A8F7560
RSP: 0x7F2401556DB0, PC: :555EB14D9000+92BBA09
```

Stack (PC) は TAC によるデコード可能

show process memory sorted / <PID>

```
Router#show process memory sorted
```

```
Processor Pool Total: 3788048988 Used: 216096264 Free: 3571952724  
reserve P Pool Total: 102404 Used: 88 Free: 102316  
Ismpi_io Pool Total: 6295128 Used: 6294296 Free: 832
```

IOSd 全体の利用状況

PID	TTY	Allocated	Freed	Holding	Getbufs	Retbufs	Process
0	0	290656128	111914240	158597896	0	0	*Init*
91	0	129160480	194840	12942336	0	0	IOSD ipc task
296	0	7780424	294448	5451808	0	0	SNMP MA SA
457	0	11820912	7735240	4127632	849828	0	EEM ED Syslog

各プロセスの利用状況

<以下略>

各プロセスのPID

```
Router#show process memory 91  
Tracekey : 1#9f3cd903256c7b1670bada076c5a4c45  
Process ID: 91  
Process Name: IOSD ipc task  
Total Memory Held: 12942336 bytes
```

PC は TACによるデコード可能

```
Processor memory Holding = 12942336 bytes  
size = 2231488, count = 34, pc = :555EB14D9000+AA37385  
size = 2165856, count = 33, pc = :555EB14D9000+AA37166  
size = 1114792, count = 17, pc = :555EB14D9000+AA2BD37  
<以下略>
```

show platform software process list RP active (process <PID>)

```
Router#show platform software process list RP active
```

Name	Pid	PPid	Group Id	Status	Priority	Size
systemd	1	0	1	S	20	28028
kthreadd	2	0	0	S	20	0
rcu_gp	3	2	0	I	0	0
rcu_par_gp	4	2	0	I	0	0
kworker/0:0-mm_percp	5	2	0	I	20	0

<以下略>

各プロセスの利用状況

各プロセスのPID

```
Router#show platform software process list RP active process-id 1
```

```
Name: systemd
Process id      : 1
Parent process id: 0
Group id       : 1
Status        : S
Session id    : 1
User time     : 143
Kernel time   : 358
Priority      : 20
Virtual bytes : 31604736
Resident pages : 7007
Resident limit : 18446744073709551615
Minor page faults: 28773
Major page faults: 41
```

Linux プロセスの詳細

各段階に役立つ主要コマンド – QFP(DP)

Router全体

QFP (DP)

[CPU]

show platform hardware qfp active datapath utilization

[Memory]

show platform hardware qfp active infrastructure exmem statistics

show platform resource

show platform software status control-processor brief

通常、上記のような IOS-XE 共通のコマンドで確認可能

show platform hardware qfp active datapath utilization

Router#show platform hardware qfp active datapath utilization

CPP 0: Subdev 0	5 secs	1 min	5 min	60 min
Input: Priority (pps)	0	0	0	0
(bps)	0	0	0	0
Non-Priority (pps)	7	5	5	5
(bps)	5928	4328	4288	4288
Total (pps)	7	5	5	5
(bps)	5928	4328	4288	4288
Output: Priority (pps)	0	0	0	0
(bps)	0	0	0	0
Non-Priority (pps)	3	1	1	1
(bps)	17184	8640	8672	8696
Total (pps)	3	1	1	1
(bps)	17184	8640	8672	8696
Processing: Load (pct)	0	0	0	0

QFP側のCPU 利用状況

Crypto/IO				
Crypto: Load (pct)	0	0	0	0
RX: Load (pct)	0	0	0	0
TX: Load (pct)	0	0	0	0
Idle (pct)	99	99	99	99

<以下略>

IPSECに関連するCrypto/IOの利用状況

通常、Load が 95% になるとパケットドロップされる

show platform hardware qfp active infrastructure exmem statistics

```
Router#show platform hardware qfp active infrastructure exmem statistics
QFP exmem statistics
```

```
Type: Name: DRAM, QFP: 0
Total: 536870912
InUse: 23870464
Free: 513000448
Lowest free water mark: 512989184
```

QFP 側メモリ (DRAM) の利用状況
DRAM: QFP で使用するメモリ (FIB, QoS policy など)

```
Type: Name: IRAM, QFP: 0
Total: 2097152
InUse: 211968
Free: 1885184
Lowest free water mark: 1885184
```

QFP 側メモリ (IRAM) の利用状況
IRAM: QFP の命令用メモリ (DRAM がない場合に使用可能)

```
Type: Name: SRAM, QFP: 0
Total: 0
InUse: 0
Free: 0
Lowest free water mark: 0
```

Catalyst 8000 トラブル シューティング

- ・ CPU/Memory トラブルシューティング
- ・ Packet トラブルシューティング
- ・ その他トラブルシューティング



投票質問 4

Passcode *

1206

slido

質問 4. Packet トラブルシューティングで最も使われている方法はどれでしょうか

- A. debug ip packet

- B. show interface/show platform hardware qfp active statistics drop detail

- C. EPC

- D. Packet Trace

Packet トラブルシューティングについて

- Packet トラブルシューティングは以下様々のシナリオで

- パケットドロップ

- パケット処理異常

- 通信遅延

- 通信不可 ...

等があったり、上記シナリオ同士でも関連したりして、一番複雑性があるものかもしれない

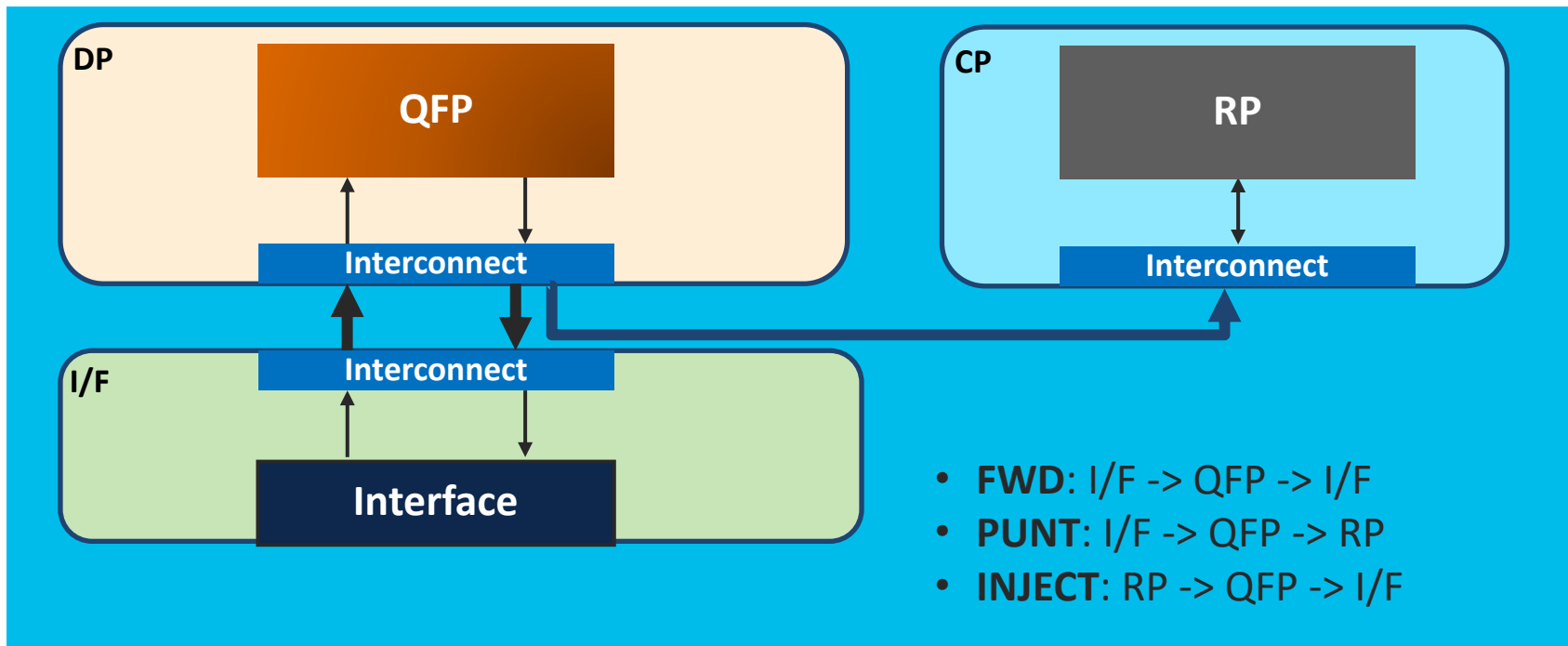
Packet トラブルシューティングについて

- 調査を徹底する場合、共通事項としてパケットがどこから、どこまで、どのように転送されているか理解する必要がある
 - 場合によっては複数分野の製品がかかわっており、TAC 複数チームによる連携調査も想定される
 - * 最初の段階で転送パスが分かる構成図が一番重要
- * 少なくとも以下の要素を含めることが望ましい
- Hostname
 - 物理 interface
 - IP アドレス
 - 転送パス (冗長もある場合それぞれ記載)

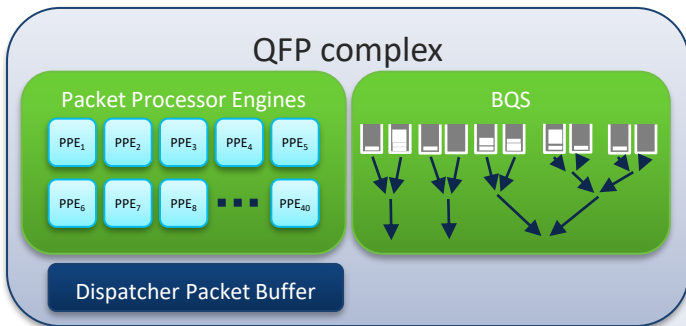
Packet トラブルシューティングについて

- Catalyst 8000 も ASR1k, ISR4k など IOS-XE Router 製品と同じように、RP (Control Plane) と QFP (Data Plane) が分離するデザインを徹底しており、Packet Processing と言えば大きく分けて以下がある
 - Forward: Input ポートで受信した Packet を QFP (Data Plane) で関連処理 (NAT/QoS/ACL/Netflow/IPSec 暗号化・複号等) 後 Output ポートへ転送
 - Punt: Input ポートで受信した Packet を QFP の判断で RP へ転送 (ICMP Request, HSRP/OSPF Hello 等)
 - Inject: RP で生成した Packet を QFP 経由し Output ポートへ転送 (ICMP Reply, HSRP/OSPF Hello 等)

Catalyst 8000 共通のパケットパス

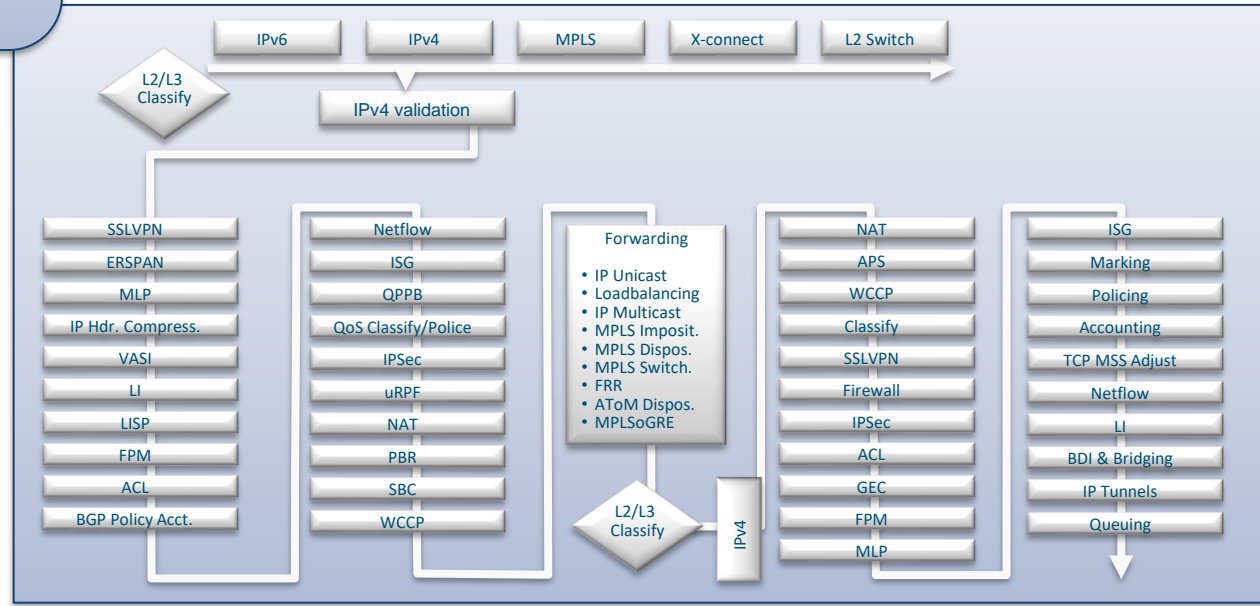


QFP (Quantum Flow Processor) と PPE, BQS, FIA

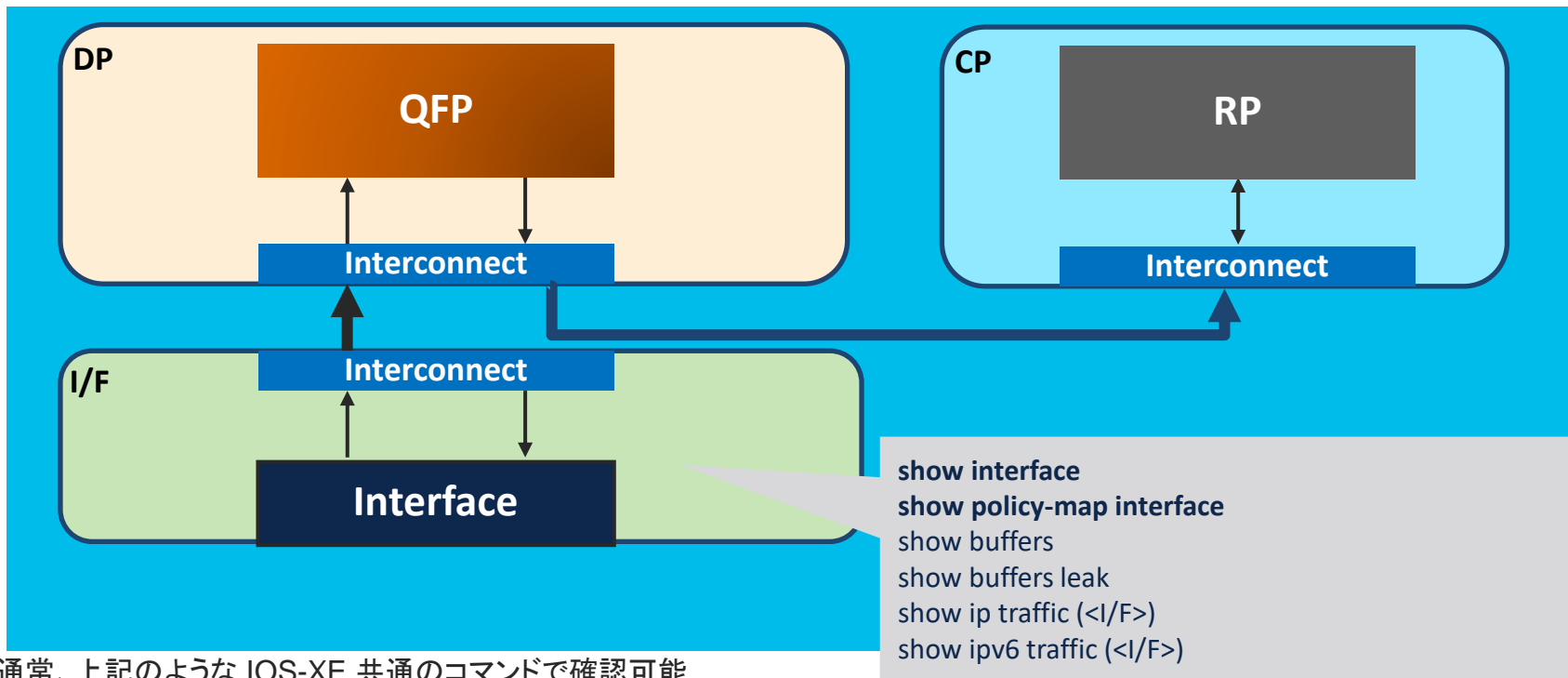


- PPE: Packet Processor Engines
- BQS: QoSの処理を担う

- FIA:
Feature Invocation Array
様々な機能を順番に処理する



各段階に役立つ主要コマンド - I/F



通常、上記のような IOS-XE 共通のコマンドで確認可能

show interfaces

```
Router#show interfaces GigabitEthernet 0/0/1
GigabitEthernet0/0/1 is up, line protocol is up
Hardware is 4x1G-2xSFP+, address is ecc0.18f2.7b21 (bia ecc0.18f2.7b21)
MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive not supported
Full Duplex, 1000Mbps, link type is auto, media type is RJ45
output flow-control is on, input flow-control is on
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:11, output 00:00:16, output hang never
Last clearing of "show interface" counters never
```

```
Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
```

```
Queueing strategy: fifo
```

```
Output queue: 0/40 (size/max)
```

```
5 minute input rate 0 bits/sec, 0 packets/sec
```

```
5 minute output rate 0 bits/sec, 0 packets/sec
```

```
11 packets input, 4460 bytes, 0 no buffer
```

```
Received 1 broadcasts (0 IP multicasts)
```

```
0 runs, 0 giants, 0 throttles
```

```
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored,
```

```
0 watchdog, 10 multicast, 0 pause input
```

```
9 packets output, 3681 bytes, 0 underruns
```

```
Output 0 broadcasts (0 IP multicasts)
```

```
0 output errors, 0 collisions, 1 interface resets
```

```
0 unknown protocol drops
```

```
0 babbles, 0 late collision, 0 deferred
```

```
0 lost carrier, 0 no carrier, 0 pause output
```

```
0 output buffer failures, 0 output buffers swapped out
```

Input queue :

size : Input queue に格納されているパケットの数

max queue : の最大サイズ

drops : 破棄されたパケット数

flushes : SPDにより破棄されたパケット数

Total output drops : 送信出来なかったパケット数

5 minute input/output rate : 5分間平均の送受信bps, 送受信pps
load-interval <sec> により30秒以上で30の倍数で指定可能

runs : 最小パケットサイズより小さいために破棄されたパケット数

giants : 最大パケットサイズより大きいために破棄されたパケット数

throttles : バッファやCPUのリソースが不足した際にカウントされる

input errors : CRC, frame, overrun, ignored のエラーカウンターの合計

CRC : CRC(Cyclic Redundancy Check) error が検出されたことを示す。ケーブル不良、対向のポート不良、自身のポート不良など基本的には Hardware の問題によってカウントされる。

frame : CRC error やオクテットの数に誤りがあるパケットを受信した場合にカウント。

overrun : ルータの処理能力を超え interface バッファにパケットを渡せない場合
ignored : 新しいパケットを受け入れる空きバッファがないときにカウント

output errors : パケットを送信する際にエラーが発生した場合にカウント

collisions : パケットを送信する際にコリジョンが発生し、再送された場合にカウント

show policy-map interface

```
Router#show policy-map interface GigabitEthernet0/0/1
GigabitEthernet0/0/1
```

```
Service-policy output: PARENT
```

```
Class-map: class-default (match-any)
```

```
15 packets, 862 bytes
```

```
5 minute offered rate 1000 bps, drop rate 0000 bps
```

```
Match: any
```

```
Queueing
```

```
queue limit 416 packets
```

```
(queue depth/total drops/no-buffer drops) 0/0/0
```

```
(pkts output/bytes output) 15/862
```

```
shape (average) cir 1000000000, bc 400000, be 400000
```

```
target shape rate 100000000
```

```
Service-policy : CHILD
```

```
queue stats for all priority classes:
```

```
Queueing
```

```
queue limit 512 packets
```

```
(queue depth/total drops/no-buffer drops) 0/0/0
```

```
(pkts output/bytes output) 0/0
```

```
Class-map: C1 (match-all)
```

```
0 packets, 0 bytes
```

```
5 minute offered rate 0000 bps, drop rate 0000 bps
```

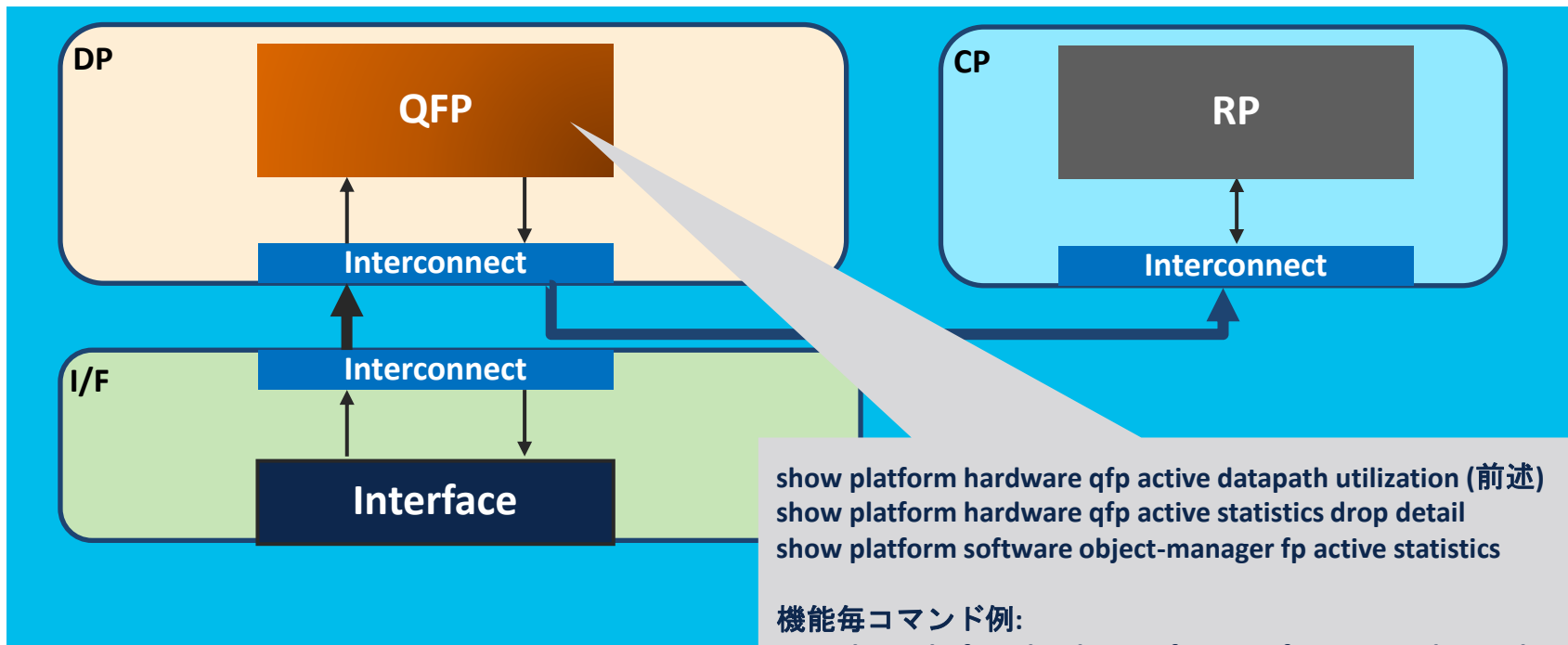
```
Match: access-group 1
```

```
Priority: 10 kbps, burst bytes 1500, b/w exceed drops: 0
```

- 親ポリシーと子ポリシーそれぞれドロップカウント、並びに offered rate/drop rate を確認可能
- offered rate/drop rate の精度は前述の load-interval <sec> により 最小 30 秒に設定可能

<以下略>

各段階に役立つ主要コマンド - QFP(DP)



通常、上記のような IOS-XE 共通のコマンドで確認可能

`show platform hardware qfp active datapath utilization (前述)`
`show platform hardware qfp active statistics drop detail`
`show platform software object-manager fp active statistics`

機能毎コマンド例:

`NAT: show platform hardware qfp active feature nat datapath stat`
`IPSEC: show platform hardware qfp active feature ipsec datapath drop`
`FW: show platform hardware qfp active feature firewall drop`

show platform hardware qfp active statistics drop detail

```
Router#show platform hardware qfp active statistics drop detail
Last clearing of QFP drops statistics : never
```

ID	Global Drop Stats	Packets	Octets
33	Ipv6NoRoute	69	3864
206	PuntPerCausePolicerDrops	222999	50228489
216	UnconfiguredIpv6Fia	783624	67325836
23	TailDrop	5185356	176302473

TailDrop は一番シンプルかもしれないが、QoS でなければスループット制限になる “show interfaces” の “Total output drops” もカウントされる

QFP の PPE でドロップした原因並びにその ID を確認可能
ID は後述にもあるが関連コマンドは以下
show platform packet-trace code drop

QFP の PPE でドロップされたパケット数および Octets 数を確認可能

show platform software object-manager fp active statistics

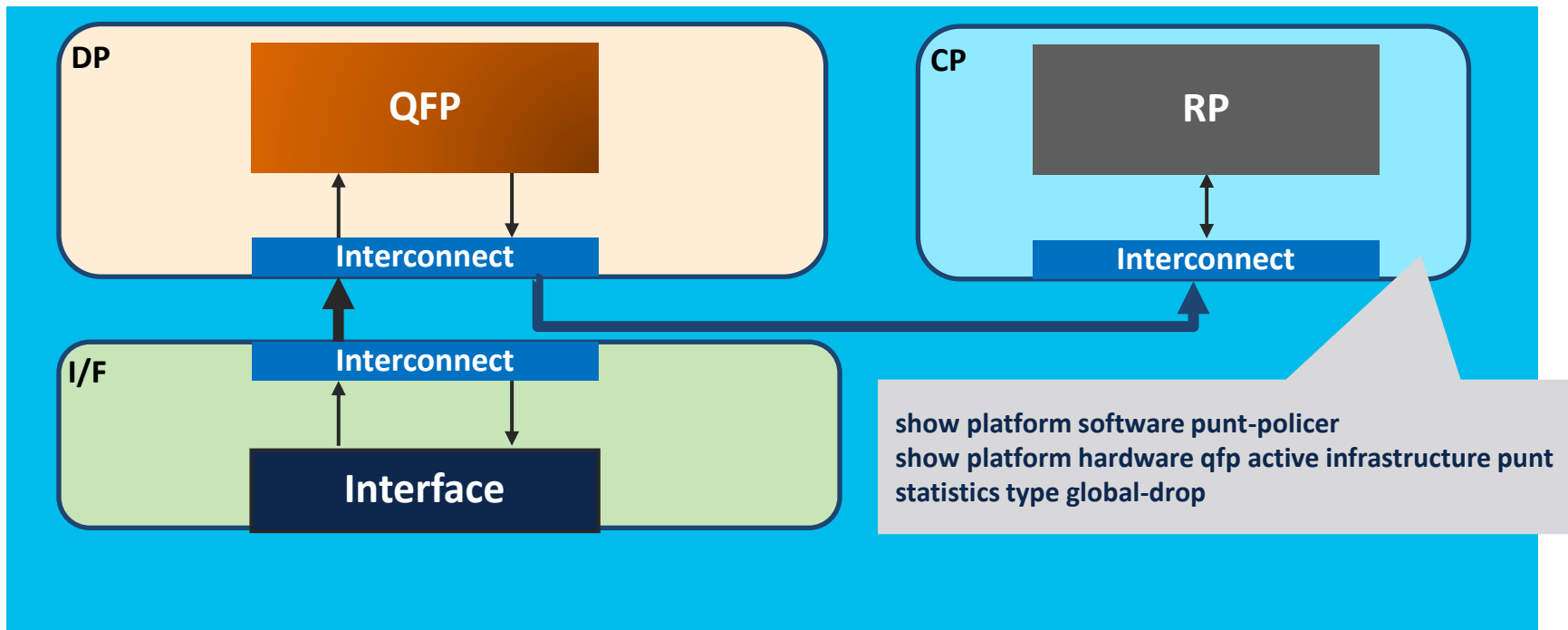
```
Router#show platform software object-manager fp active statistics
Forwarding Manager Asynchronous Object Manager Statistics
```

```
Object update: Pending-issue: 0, Pending-acknowledgement: 0
Batch begin:   Pending-issue: 0, Pending-acknowledgement: 0
Batch end:     Pending-issue: 0, Pending-acknowledgement: 0
Command:      Pending-acknowledgement: 0
Total-objects: 90
Stale-objects: 0
Resolve-objects: 0
Childless-delete-objects: 0
Backplane-objects: 0
Error-objects: 0
Number of bundles: 0
Paused-types: 3
```

Control Plane から Data Plane へのプログラミングの Issue
がないか確認可能

Pending-issue: 0, Pending-acknowledgement: 0 が正常状態

各段階に役立つ主要コマンド - RP(CP)



通常、上記のような IOS-XE 共通のコマンドで確認可能

show platform software punt-policer

```
Router#show platform software punt-policer
```

```
Per Punt-Cause Policer Configuration and Packet Counters
```

Punt Cause	Description	Config Rate (pps)		Conform Packets		Dropped Packets		Config Burst (pkts)		Config Alert	
		Normal	High	Normal	High	Normal	High	Normal	High	Normal	High
2	IPv4 Options	1764	1323	0	0	0	0	1764	1323	Off	Off
3	Layer2 control and legacy	17640	4410	58733	0	0	0	17640	4410	Off	Off
4	PPP Control	2000	1000	0	0	0	0	2000	1000	Off	Off
5	CLNS IS-IS Control	17640	4410	0	0	0	0	17640	4410	Off	Off
6	HDLC keepalives	2000	1000	0	0	0	0	2000	1000	Off	Off
7	ARP request or response	2000	1000	0	73584	0	125635	2000	1000	Off	Off
8	Reverse ARP request or repso	2000	1000	0	0	0	0	2000	1000	Off	Off
9	Frame-relay LMI Control	2000	1000	0	0	0	0	2000	1000	Off	Off
10	Incomplete adjacency	2000	1000	0	0	0	0	2000	1000	Off	Off
11	For-us data	17640	2205	184	0	0	0	17640	2205	Off	Off

Punt Policer の Rate, Conform Packets, Dropped Packets 数等を各 Punt Cause で確認可能。
Punt Cause ID は後述にもあるが関連コマンドは以下
show platform packet-trace code punt

Punt Policer によるドロップの場合、右の
PuntPerIntfPolicerDrops としてもカウントされる

```
Router#show platform hardware qfp active statistics drop detail
```

ID	Global Drop Stats	Packets	Octets
206	PuntPerIntfPolicerDrops	257	274166

show platform hardware qfp active infrastructure punt statistics type global-drop

```
Router#show platform hardware qfp active infrastructure punt statistics type global-drop  
Global Drop Statistics
```

```
Number of global drop counters = 22
```

Counter ID	Drop Counter Name	Packets
000	INVALID_COUNTER_SELECTED	0
001	INIT_PUNT_INVALID_PUNT_MODE	0
002	INIT_PUNT_INVALID_PUNT_CAUSE	0
003	INIT_PUNT_INVALID_INJECT_CAUSE	0
004	INIT_PUNT_MISSING_FEATURE_HDR_CALLBACK	0
005	INIT_PUNT_EXT_PATH_VECTOR_REQUIRED	0
006	INIT_PUNT_EXT_PATH_VECTOR_NOT_SUPPORTED	0
007	INIT_INJ_INVALID_INJECT_CAUSE	0
008	INIT_INJ_MISSING_FEATURE_HDR_CALLBACK	0
009	PUNT_INVALID_PUNT_CAUSE	0
010	PUNT_INVALID_COMMON_HDR_VERSION	0
011	PUNT_INVALID_PLATFORM_HDR_VERSION	0
012	PUNT_PATH_NOT_INITIALIZED	0
013	PUNT_GPM_ALLOC_FAILURE	0
014	PUNT_TRANSITION_FAILURE	0
015	PUNT_DELAYED_PUNT_PKT_SB_NOT_IN_USE	0
016	PUNT_CAUSE_GLOBAL_POLICER	0
017	INJ_INVALID_INJECT_CAUSE	0
018	INJ_INVALID_COMMON_HDR_VERSION	0
019	INJ_INVALID_PLATFORM_HDR_VERSION	0
020	INJ_INVALID_PAL_HDR_FORMAT	0
021	PUNT_GPM_TX_LEN_EXCEED	0

22 個のタイプとして分けられているが、
Global Punt Policer によるドロップが確認可能

パケットキャプチャの方法

- 前述のカウンタを見ても問題特定ができず、または更に詳細な動作を確認する必要がある場合、パケットキャプチャの出番になる
- Debug ip packet: IOS-XE の場合 RP 処理のパケットのみキャプチャされるため不向き
- EPC: パケットをキャプチャし DRAM のバッファに保存されるが、後で bootflash などでエクスポート可能
- Packet Trace: パケットをキャプチャして QFP でのどのように転送処理をしているかトレース可能

EPC (Embedded Packet Capture) の実施方法

[設定]

monitor capture CAP interface GigabitEthernet 0/0/1 both <<<< I/F指定可能

monitor capture CAP control-plane both <<<< CPも指定可能

monitor capture CAP match ipv4 any any <<<< フィルタも指定可能

[キャプチャ開始] monitor capture CAP start

[キャプチャ停止] monitor capture CAP stop

[show コマンド]

show monitor capture

show monitor capture CAP buffer brief

show monitor capture CAP buffer detailed

[エクスポート]

monitor capture CAP export bootflash:CAP.pcap

同じ EPC でも IOS-XE と IOS の方法が異なる

[IOS-XE : EPC\(Embedded Packet Capture\)を使用したパケットキャプチャ方法](#)

EPC (Embedded Packet Capture) の実施方法

[その他注意事項]

- キャプチャ実行はルータに負荷がかかるため注意が必要
- キャプチャ対象となるパケットは IPv4/IPv6 となり、CDP, ARP, PPP などはキャプチャ不可
- キャプチャ対象の I/F は以下の通り確認可能

Router#monitor capture cap interface ?

GigabitEthernet	GigabitEthernet IEEE 802.3z
Multilink	Multilink-group interface
Port-channel	Ethernet Channel of interfaces
Serial	Serial
TenGigabitEthernet	Ten Gigabit Ethernet
Tunnel	Tunnel interface
Vlan	Catalyst Vlans
range	interface range command

- キャプチャバッファは以下から指定可能

Router#monitor capture CAP buffer size ?

<1-100> Total size of file(s) in MB

Packet Trace の実施方法

[設定]

```
debug platform packet-trace packet 8192 fia-trace <<<<< 8192 パケットという制限には要注意  
debug platform condition interface GigabitEthernet 0/0/1 both <<<< I/F指定可能、ほぼ全 I/F 種類  
debug platform condition interface internal-RP both <<<< CPも指定可能  
debug platform packet-trace copy packet both size 2048  
debug platform packet-trace statistics
```

[キャプチャ開始] debug platform condition start

[キャプチャ停止] debug platform condition stop

[show コマンド]

```
show platform packet-trace configuration  
show platform packet-trace statistics  
show platform packet-trace summary  
show platform packet-trace packet all decode  
(show platform packet-trace packet <Pkt No.> decode)
```

詳細は下記 Community URL をご参照ください

[IOS-XE: Packet Trace 機能の紹介](#)

Packet Trace の実施方法

[フィルタ方法]

```
debug platform condition interface Interface [ ipv4 A.B.C.D/nn | ipv6 X:X:X:X::X/0-128 ] { ingress | egress | both }
```

```
debug platform packet-trace drop [ code code-num ]
```

```
debug platform packet-trace punt [ code code-num ]
```

```
debug platform packet-trace inject [ code code-num ]
```

* 8192 の制限並びに QFP メモリ使用されるため、場合によってフィルタが必要

[drop/punt/inject コードの確認コマンド]

```
show platform packet-trace code drop
```

```
show platform packet-trace code punt
```

```
show platform packet-trace code inject
```

詳細は下記 Community URL をご参照ください

[IOS-XE: Packet Trace 機能の紹介](#)

Packet Trace 出力の確認例

```
Router#show platform packet-trace summary
```

Pkt	Input	Output	State	Reason
0	internal0/0/rp:0	internal0/0/rp:0	PUNT	21 (RP<->QFP keepalive)
1	Gi0/0/0	internal0/0/rp:0	PUNT	3 (Layer2 control and legacy)
2	internal0/0/rp:0	internal0/0/rp:0	PUNT	21 (RP<->QFP keepalive)
3	internal0/0/rp:0	internal0/0/rp:0	PUNT	21 (RP<->QFP keepalive)
4	internal0/0/rp:0	internal0/0/rp:0	PUNT	21 (RP<->QFP keepalive)
5	Gi0/0/0	internal0/0/rp:0	PUNT	3 (Layer2 control and legacy)
6	internal0/0/rp:0	internal0/0/rp:0	PUNT	21 (RP<->QFP keepalive)
7	internal0/0/rp:0	internal0/0/rp:0	PUNT	21 (RP<->QFP keepalive)
8	Gi0/0/0	internal0/0/rp:0	PUNT	3 (Layer2 control and legacy)
9	Gi0/0/1	Gi0/0/0	FWD	
10	Gi0/0/0	Gi0/0/1	FWD	
11	Gi0/0/1	Gi0/0/0	FWD	
12	Gi0/0/0	Gi0/0/1	FWD	
13	Gi0/0/1	Gi0/0/0	FWD	
14	Gi0/0/0	Gi0/0/1	FWD	
15	Gi0/0/1	Gi0/0/0	FWD	
16	Gi0/0/0	Gi0/0/1	FWD	
17	Gi0/0/1	Gi0/0/0	FWD	
18	Gi0/0/0	Gi0/0/1	FWD	
19	internal0/0/rp:0	internal0/0/rp:0	PUNT	21 (RP<->QFP keepalive)
20	internal0/0/rp:0	internal0/0/rp:0	PUNT	21 (RP<->QFP keepalive)
21	internal0/0/rp:0	internal0/0/rp:0	PUNT	21 (RP<->QFP keepalive)

Packet Trace 出力の確認例 – NAT 対象のパケット

```
#show platform hardware qfp active interface if-name G0/0/0  
--> 右の出力と関連しI/F 側の処理順序を確認可能
```

```
Protocol 1 - ipv4_output
```

```
FIA handle - CP:0x55a900fda5a8 DP:0x20ba2980
```

```
CBUG_OUTPUT_FIA
```

```
IPV4_OUTPUT_VFR
```

```
IPV4_NAT_OUTPUT_FIA
```

```
IPV4_OUTPUT_THREAT_DEFENSE
```

```
IPV4_VFR_REFRAG (M)
```

```
DEBUG_COND_APPLICATION_OUT_CLR_TXT
```

```
IPV4_OUTPUT_L2_REWRITE (M)
```

```
DEBUG_COND_MAC_EGRESS
```

```
DEBUG_COND_APPLICATION_OUT
```

```
IPV4_OUTPUT_FRAG (M)
```

```
IPV4_OUTPUT_DROP_POLICY (M)
```

```
DEBUG_COND_OUTPUT_PKT
```

```
MARMOT_SPA_D_TRANSMIT_PKT
```

```
DEF_IF_DROP_FIA (M)
```

```
Router #show platform packet-trace packet 0 decode
```

```
Packet: 0 CBUG ID: 22
```

```
Summary
```

```
Input : GigabitEthernet0/0/1
```

```
Output : GigabitEthernet0/0/0
```

```
State : FWD
```

```
Timestamp
```

```
Start : 354187806473370 ns (01/14/2022 20:55:50.450216 UTC)
```

```
Stop : 354187806854734 ns (01/14/2022 20:55:50.450598 UTC)
```

```
<snip>
```

```
Feature: IPV4_OUTPUT_VFR
```

```
Entry : Output - 0x70014890
```

```
Input : GigabitEthernet0/0/1
```

```
Output : GigabitEthernet0/0/0
```

```
Lapsed time : 1088 ns
```

```
Feature: NAT
```

```
Direction : IN to OUT
```

```
Action : Translate Source
```

```
Steps : SESS-CR
```

```
Match id : 3
```

```
Old Address : 192.168.1.2
```

```
New Address : 172.16.1.10
```

```
Feature: IPV4_NAT_OUTPUT_FIA
```

```
Entry : Output - 0x700148b8
```

```
Input : GigabitEthernet0/0/1
```

```
Output : GigabitEthernet0/0/0
```

```
Lapsed time : 288149 ns
```

Packet Trace 出力の確認例 - NAT 対象外のパケット

```
#show platform hardware qfp active interface if-name G0/0/0  
--> 右の出力と関連し I/F 側の処理順序を確認可能
```

```
Protocol 1 - ipv4_output  
FIA handle - CP:0x55a900fda5a8 DP:0x20ba2980  
CBUG_OUTPUT_FIA  
IPV4_OUTPUT_VFR  
IPV4_NAT_OUTPUT_FIA  
IPV4_OUTPUT_THREAT_DEFENSE  
IPV4_VFR_REFRAG (M)  
DEBUG_COND_APPLICATION_OUT_CLR_TXT  
IPV4_OUTPUT_L2_REWRITE (M)  
DEBUG_COND_MAC_EGRESS  
DEBUG_COND_APPLICATION_OUT  
IPV4_OUTPUT_FRAG (M)  
IPV4_OUTPUT_DROP_POLICY (M)  
DEBUG_COND_OUTPUT_PKT  
MARMOT_SPA_D_TRANSMIT_PKT  
DEF_IF_DROP_FIA (M)
```

```
Feature: CBUG_OUTPUT_FIA  
Entry : Output - 0x7001457c  
Input : GigabitEthernet0/0/1  
Output : GigabitEthernet0/0/0  
Lapsed time : 85 ns  
Feature: IPV4_OUTPUT_VFR  
Entry : Output - 0x70014890  
Input : GigabitEthernet0/0/1  
Output : GigabitEthernet0/0/0  
Lapsed time : 85 ns  
Feature: NAT  
Direction : IN to OUT  
Action : FWD  
FWD-POINT : LOOKUP_FAIL <<< !!!! NAT されていない !!!!  
VRF : 0  
Feature: IPV4_NAT_OUTPUT_FIA  
Entry : Output - 0x700148b8  
Input : GigabitEthernet0/0/1  
Output : GigabitEthernet0/0/0  
Lapsed time : 67893 ns  
Feature: IPV4_OUTPUT_THREAT_DEFENSE  
Entry : Output - 0x70014b70  
Input : GigabitEthernet0/0/1  
Output : GigabitEthernet0/0/0  
Lapsed time : 2901 ns  
Feature: IPV4_VFR_REFRAG  
Entry : Output - 0x700148c0  
Input : GigabitEthernet0/0/1  
Output : GigabitEthernet0/0/0  
Lapsed time : 42 ns  
Feature: DEBUG_COND_APPLICATION_OUT_CLR_TXT  
Entry : Output - 0x7001458c  
Input : GigabitEthernet0/0/1  
Output : GigabitEthernet0/0/0  
Lapsed time : 64 ns
```

```
Feature: IPV4_OUTPUT_L2_REWRITE  
Entry : Output - 0x7000c1cc  
Input : GigabitEthernet0/0/1  
Output : GigabitEthernet0/0/0  
Lapsed time : 544 ns  
Feature: DEBUG_COND_MAC_EGRESS  
Entry : Output - 0x70014584  
Input : GigabitEthernet0/0/1  
Output : GigabitEthernet0/0/0  
Lapsed time : 928 ns  
Feature: DEBUG_COND_APPLICATION_OUT  
Entry : Output - 0x70014588  
Input : GigabitEthernet0/0/1  
Output : GigabitEthernet0/0/0  
Lapsed time : 53 ns  
Feature: IPV4_OUTPUT_FRAG  
Entry : Output - 0x70014c14  
Input : GigabitEthernet0/0/1  
Output : GigabitEthernet0/0/0  
Lapsed time : 42 ns  
Feature: IPV4_OUTPUT_DROP_POLICY  
Entry : Output - 0x70014ca4  
Input : GigabitEthernet0/0/1  
Output : GigabitEthernet0/0/0  
Lapsed time : 3168 ns  
Feature: DEBUG_COND_OUTPUT_PKT  
Entry : Output - 0x70014580  
Input : GigabitEthernet0/0/1  
Output : GigabitEthernet0/0/0  
Lapsed time : 490 ns  
Feature: MARMOT_SPA_D_TRANSMIT_PKT  
Entry : Output - 0x70014720  
Input : GigabitEthernet0/0/1  
Output : GigabitEthernet0/0/0  
Lapsed time : 10762 ns
```

Packet Trace 出力の確認例 – ハッシュとサマリ

```
Packet Copy In
a09351d3 1801700f 6a7f0b81 08004500 0064003c 0000ff01 4ca2c0a8 0101ac10
01010800 f6ff000c 00000000 0000154e 71f0abcd abcdabcdn abcdabcdn abcdabcdn
abcdabcdn abcdabcdn abcdabcdn abcdabcdn abcdabcdn abcdabcdn abcdabcdn abcdabcdn
abcdabcdn abcdabcdn abcdabcdn abcdabcdn abcd
```

ARPA

Destination MAC : a093.51d3.1801

Source MAC : 700f.6a7f.0b81

Type : 0x0800 (IPV4)

IPv4

Version : 4

Header Length : 5

ToS : 0x00

Total Length : 100

Identifier : 0x003c

IP Flags : 0x0

Frag Offset : 0

TTL : 255

Protocol : 1 (ICMP)

Header Checksum : 0x4ca2

Source Address : 192.168.1.1

Destination Address : 172.16.1.1

ICMP

Type : 8 (Echo)

Code : 0 (No Code)

Checksum : 0xf6ff

Identifier : 0x000c

Sequence : 0x0000

```
Packet Copy Out
0072783e f1f6a093 51d31802 08004500 0064003c 0000fe01 4da2c0a8 0101ac10
01010800 f6ff000c 00000000 0000154e 71f0abcd abcdabcdn abcdabcdn abcdabcdn
abcdabcdn abcdabcdn abcdabcdn abcdabcdn abcdabcdn abcdabcdn abcdabcdn abcdabcdn
abcdabcdn abcdabcdn abcdabcdn abcdabcdn abcd
```

ARPA

Destination MAC : 0072.783e.f1f6

Source MAC : a093.51d3.1802

Type : 0x0800 (IPV4)

IPv4

Version : 4

Header Length : 5

ToS : 0x00

Total Length : 100

Identifier : 0x003c

IP Flags : 0x0

Frag Offset : 0

TTL : 254

Protocol : 1 (ICMP)

Header Checksum : 0x4da2

Source Address : 192.168.1.1

Destination Address : 172.16.1.1

ICMP

Type : 8 (Echo)

Code : 0 (No Code)

Checksum : 0xf6ff

Identifier : 0x000c

Sequence : 0x0000

Packet Trace に関連するコマンド

[punt/drop/inject コード関連]

```
show platform packet-trace code drop  
show platform packet-trace code punt  
show platform packet-trace code inject
```

[パケットドロップ関連]

```
show platform hardware qfp active statistics drop detail (drop code 連動カウンタ)  
show platform software punt-policer (punt code 連動カウンタ)
```

[I/F 単位での QFP 処理関連]

```
show platform hardware qfp active interface if-name <I/F>
```

Catalyst 8000 トラブル シューティング

- ・ CPU/Memory トラブルシューティング
- ・ Packet トラブルシューティング
- ・ その他トラブルシューティング



予期せぬ再起動のトラブルシューティングについて

- 予期せぬ再起動は下記のポイントから調査を行う
 - 再起動するたびにロギングバッファがクリアされるため、事象発生時、syslog サーバのログがあったほうがよい
 - Last reload reason は show ver に表示されるので確認しておく
 - 予期せぬ再起動のトリガーがあるか確認しておく

例: 何等かのコマンド実行、何等かのトラフィック受信、何等かの作業により I/F またはプロトコルの状態遷移等

予期せぬ再起動のトラブルシューティングについて

- ほとんどの場合 Crashinfo/Core ファイルも自動的に生成するので、以下のディレクトリに関連ファイルがあるか確認を行い、ある場合回収しておく

[Crashinfo]

bootflash:

harddisk: (harddisk をもつ機種は通常そのパスに生成される)

[Core]

bootflash:/core/

harddisk:/core/ (harddisk をもつ機種は通常そのパスに生成される)

system shell login について

- ・ 複雑なトラブルシューティングの場合、TAC より system shell login でのログ取得を提案をすることがあるが、基本的な流れは以下の通り

- (1) 下記コマンドを実施頂き、public key のリクエスト実施
`#request consent-token generate-challenge shell-access auth-timeout 1800`
- (2) 長い文字列の public key が表示され、直ちにメールで弊社にご提供頂く
- (3) 弊社より認証コードを発行して、メールで送付する
- (4) 受信できましたら、直ちに下記コマンドを実行して、認証コードを投入する
`Router#request consent-token accept-response shell-access <認証コード>`
(チャレンジ生成からレスポンス入力まで30分以内であることをご注意ください)

*カーソル点滅が 5 秒以上続く場合、もう一度 [Enter] を押す
認証成功しましたら、successというようなログが出る

- (5) 下記コマンドを実行する
`Router#request platform software system shell r0`

- (6) 以下のメッセージが表示されましたら、[y] を入力する
Activity within this shell can jeopardize the functioning of the system.
Are you sure you want to continue? [y/n] y

詳細は下記 Community URL もご参照ください

[IOS-XE/XE SD-WAN: system shell login について](#)

多彩な show tech も活用可能

- IOS-XE 17.x では show tech の後にキーワードを付けることで特定機能に対するトラブルシューティングコマンドが一括取得可能
- 以下に例をいくつか記載したが、TAC から案内する場合があります

show tech-support license

show tech-support aaa

show tech-support routing

show tech-support cef

show tech-support nat

show tech-support diagnostic

show tech-support ospf

show tech-support install

show tech-support bgp

show tech-support memory 等々

※ コマンドや出力量にも関係するが、show tech 取得時に show tech XXX | redirect XXX.txt により負荷軽減可能

Catalyst 8000 不具合事例紹介



C8300 HSRP received unexpected active hello packet when interface recovered

<事象>

元ActiveルータのHSRP I/FがDownの状態から復旧する際、preempt delayの時間を設定しているにも関わらず、I/FがUp状態になるとともにHSRP Hello パケットを対向側デバイスへ送信することでHSRPのFlapが発生する

<発生条件>

ルータ側ではRJ45ポートを使用している場合、該当ポートのケーブル抜き差し、または対向側ポートのshut/no shut

<暫定回避策>

SFP ポートを使用する

またはルータ側のI/Fのshut/no shut

<修正バージョン>

17.12.2以降

CSCwa38451

Packets loss happens on C8300/C8500L when inserting SFP into or no shut other IF with a SFP

<事象>

SFPポートをno shut、またはno shut状態のポートにSFPを挿入すると、
その他のI/Fにてoverrunカウンターが上昇し、パケットドロップが発生する

<暫定回避策>

なし

<修正バージョン>

17.6.3以降、17.7.2以降、17.8.1a以降

CSCwd84391

C8500L incorrectly drops ip fragments due to reassembly timeout despite fix for CSCwb74917

<事象>

フラグメントパケットがVFRにより処理される場合、reassembly timeout intervalに達していないに関わらず、reassembly timeoutによって誤ってドロップされる

<発生条件>

C8500L 機器のuptimeが7週～8週以上

<暫定回避策>

機器のuptimeが7週～8週になる前に機器を一度手動でリロードする

<修正バージョン>

17.6.6以降、17.9.3以降、17.11.1以降、17.12.1以降

Reference



Reference

- [Cisco Catalyst 8200 Series Edge Platforms Data Sheet](#)
- [Cisco Catalyst 8300 Series Edge Platforms Data Sheet](#)
- [Cisco Catalyst 8500 Series Edge Platforms Data Sheet](#)
- [Cisco Catalyst 8200 Series Edge Platforms Interfaces and Modules](#)
- [Cisco Catalyst 8300 Series Edge Platforms Interfaces and Modules](#)
- [Cisco Optics-to-Device Compatibility Matrix](#)

Reference

- [Networking Software \(IOS & NX-OS\)](#)
- [IOS-XE Polaris について](#)
- [IOS-XE : EPC\(Embedded Packet Capture\)を使用したパケットキャプチャ方法](#)
- [IOS-XE: Packet Trace 機能の紹介](#)
- [IOS-XE/XE SD-WAN: system shell login について](#)
- [CPU 使用率が上昇した場合に自動的にログを取得する EEM の設定例*](#)

*その例は IOSd のみの監視となります。

Thank You



5 mins Break

まもなく Q&A セッションを開始します。ご参加される方は
少々お待ちください。

Q&A

画面右側の Q&A ウィンドウから、
すべてのパネリスト (All Panelists) 宛
に送信してください。



次回の オンラインセミナー予定



Wireless TAC Time

- 今すぐ現場に効く Tips 紹介 -

2023年12月20日(水) 10:00 - 11:30 (予定)

大崎 秀行 (Hideyuki Osaki)

シスコシステムズ

グローバル カスタマー エクスペリエンス センター

テクニカル リーダー

登録受付中

<https://community.cisco.com/t5/e-/-/ev-p/4954843>



書籍ネットワークエンジニアの教科書 紹介



弊社TAC監修の書籍が改訂3版として出版！



各製品担当のエキスパートエンジニアが
わかりやすい言葉で各テクノロジーを解説！！



ネットワーク初心者に最適な入門書として是非！！！！

好評発売中



書籍情報

タイトル: [改訂3版 ネットワークエンジニアの教科書](#)

ISBNコード: 978-4-86354-414-7

本のサイズ: A5判、ソフトカバー

総ページ数: 304ページ

出版方法: 電子書籍および書籍

出版社: シーアンドアール研究所

ご参加いただいた方へ 書籍プレゼントのお知らせ

セッション後のアンケートに回答くださった方から抽選で1名様へ書籍「ネットワークエンジニアの教科書」を差し上げます！

終了後、ブラウザに表示されるアンケートにご回答ください。フリーコメントもお願いします。

当選通知は近日中、メールにてご連絡差し上げます。

書籍プレゼント Wチャンスのお知らせ



インタビュー記事に「いいね！」をして抽選に参加しませんか？
日本のコミュニティで初！シスコ認定 VIP の記事をご覧ください

対象記事はこちら：[シスコ VIP の 高井 史裕 さんにお話を伺いました！](#)

アンケートを見逃してしまった方や抽選にもれた方も大丈夫！ぜひ記事へアクセスしていいね！をクリックするか、またはコメントを投稿してください。



ご参加ありがとうございました。

Community Liveと Cisco Communityの
各アンケートにも ぜひ ご協力ください。

