



SDN Japan 2012

API型SDNの例とテクニカルサービス から見たユースケース - Cisco One Platform Kit APIを題材にして -

緒勝 徹 (Toru Okatsu)

tokatsu@cisco.com

TS Technical Leader

Cisco Japan

December 6th

Agenda

- Cisco Open Network Environment 概要
- Cisco One Platform Kit 概要
- テクニカルサービスにおけるOne PKのユースケース
- テクニカルサービスから見たAPI型SDNへの期待

Cisco Open Network Environment

Industry's Most Comprehensive Networking Portfolio

Hardware + Software

Physical + Virtual

Network + Compute

Applications

OPEN NETWORK ENVIRONMENT

Platform APIs

onePK

Virtual Overlays

N1KV
Enhancements
for Open Clouds

Controllers
and Agents

SDN PoC:
SW Controller
OpenFlow on
C3K

www.cisco.com/go/one

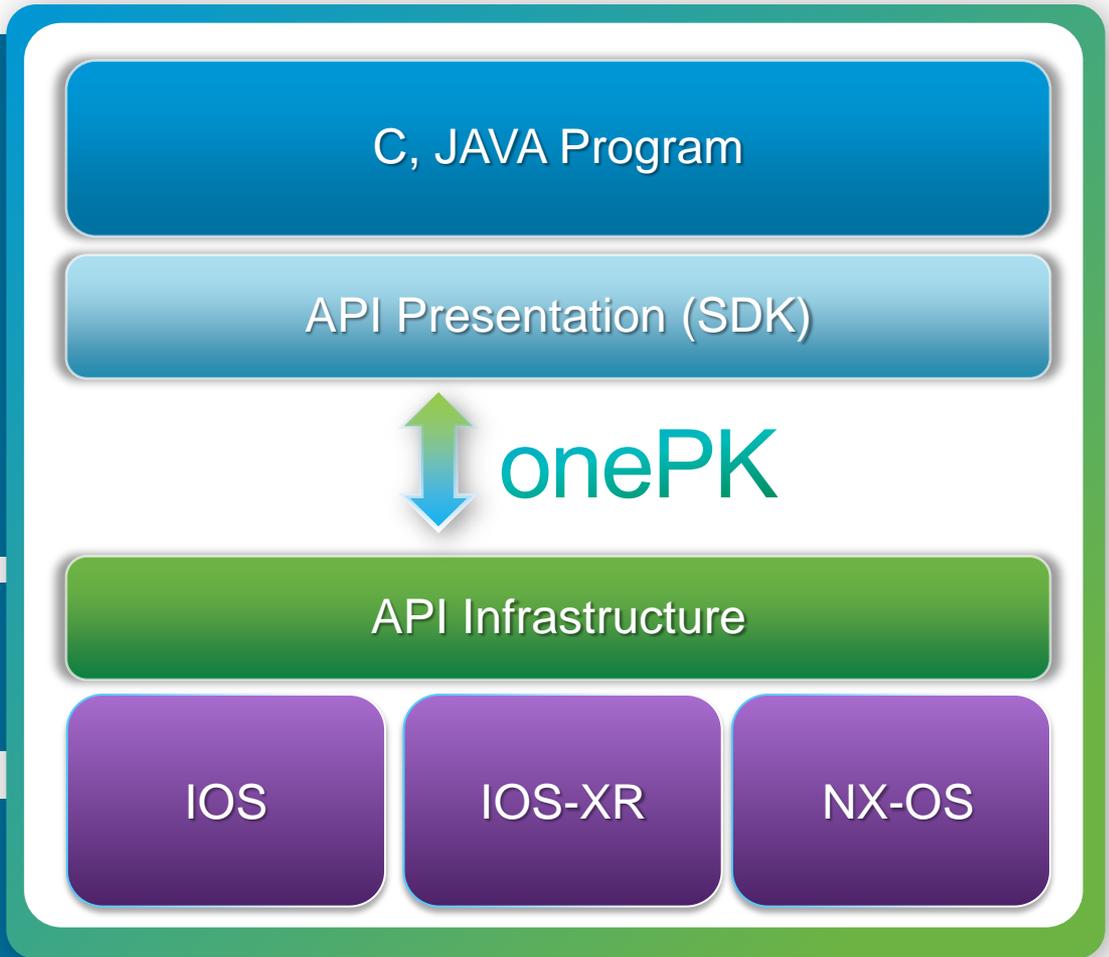
One Platform Kit (onePK)とは

Industry's most Comprehensive Kit
For Network Infrastructure across:

Branch
Campus
Data Center
Service Provider
Cloud

Simplicity, Integration and choice of
protocols and programming languages

Phased availability across multiple
Platforms: ISR G2, ASR, CRS, Catalyst,
Nexus



<http://www.cisco.com/go/onepk>

onePKのBase Service Set

Element

- onePKアプリと機器のセッション管理
- 機器属性の取得と設定
- インターフェース関連のイベントの処理
- CLIの拡張

Utilities

- Syslogのイベント処理
- 機器上のAAA処理の制御とAAA情報の参照

Discovery

- 機器内のサービスの探索
- ネットワークトポロジーの探索

Developer

- onePKのデバッグ機能の操作

Data Path

- データパスの属性の取得と設定
- パケットのコピー、パント、インジェクション

Policy

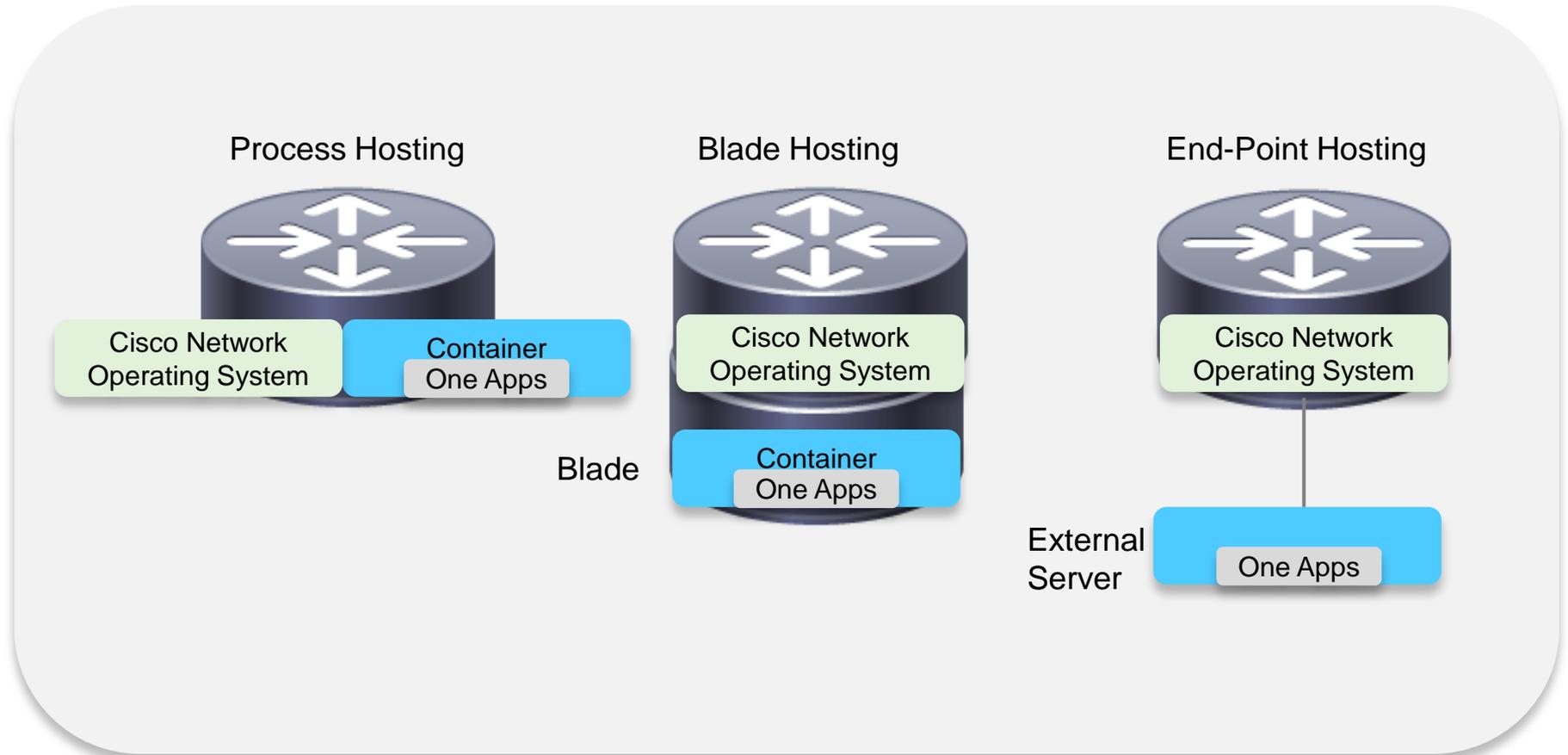
- ACL情報の取得と設定
- QoS情報の取得と設定

Routing

- RIBイベントの処理
- RIB情報の取得
- アプリケーションrouteの追加削除

現在、onePKはBeta段階で、正式リリースまでに機能の追加変更の可能性が 있습니다。

onePK アプリケーションの配置



サポートにおけるonePKのユースケース

データ取得

機器上のイベントをトリガーに障害関連情報を取得するようなアプリケーション

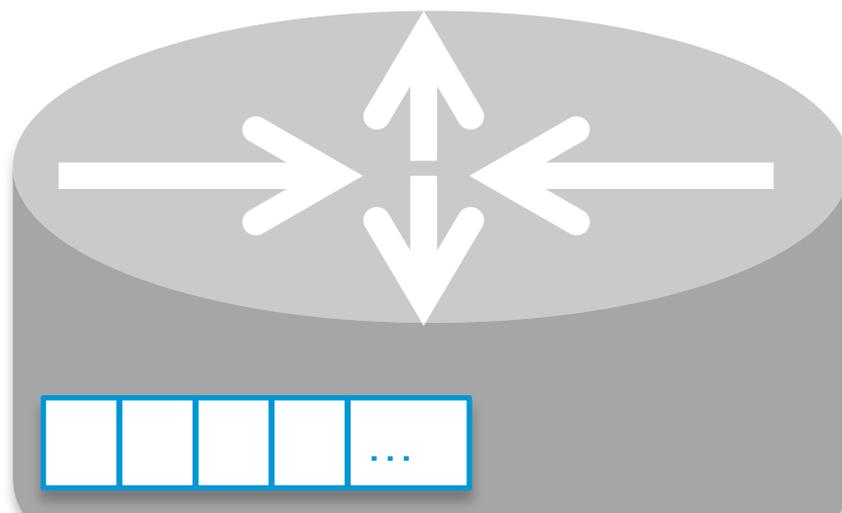
動作確認

パケットを任意の場所から注入して、その到達性を確認するようなアプリケーション



ユースケース その1

- DoS攻撃やウイルスによる異常動作などにより、ルータやスイッチのコントロールプレーンに対する輻輳が引き起こされることがあります。現象が間欠的な場合、それを捉えるには何らかの自動化が効果的です。



入インターフェースのキューが長くなってきたら中身を確認

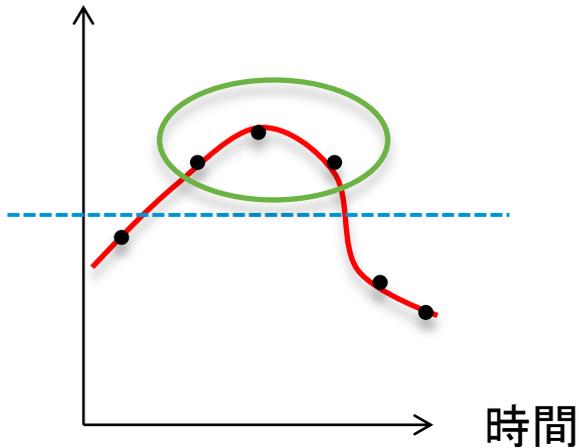
インターフェース統計情報イベントの利用

- Interface Service Setの中に、インタフェースの統計情報を監視して、閾値を越えると、アプリケーションにイベントを通知するAPIがあります。
- Vty Service Setの中に、任意のshow コマンドの結果を取得する機能があります。
- 上記の二つを組み合わせて、入力インタフェースに過剰にパケットが来て、ドロップが増えた時にバッファの内容を取得するプログラムを作成してみました。

InterfaceStatisticsFilterの仕様

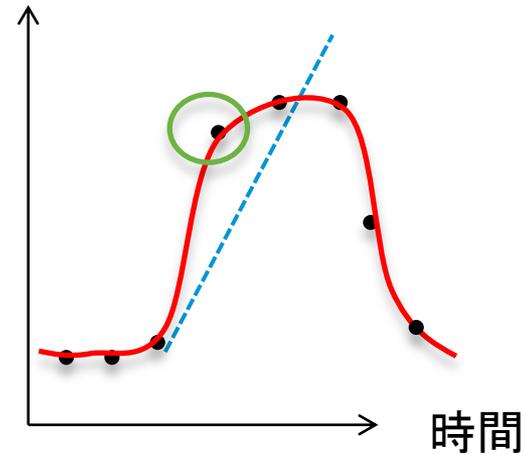
- show interfacesで取得できる統計情報が対象になります。
- イベントの発生のはり方は二通りあります。

カウンタ値
or レート



ある一定値を越えている間はイベントが発生し続ける

カウンタ値
or レート



前回のカウンタの確認時から一定数以上増加したらイベントが発生する

インターネットフェース監視プログラムの動作

ネットワーク機器

メインプログラム

イベントハンドラ

- 監視対象のインタフェース、カウンタ
- 監視間隔
- イベントの発生方法

- イベント監視用のハンドラの起動

- カウンタの監視

監視間隔

ドロップ増加

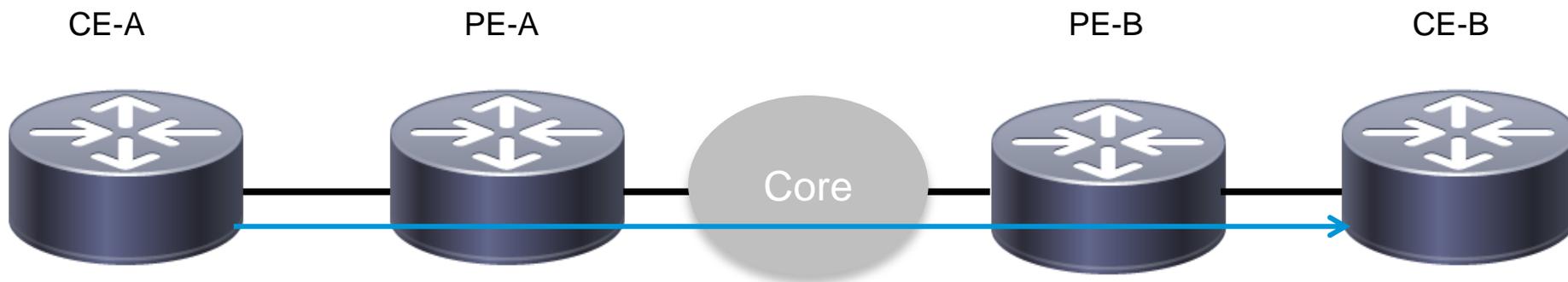
- 対象インタフェース名とカウンタ増分の通知

- show buffer input-interfaceによる対象バッファの取得

- 対象インタフェースバッファの内容

ユースケース その2

- QoSやACLの動作確認や障害解析でユーザトラフィックを流したい場合があります。

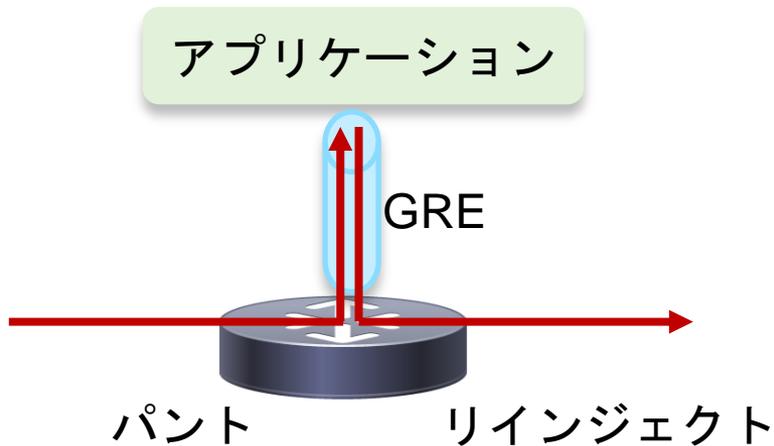
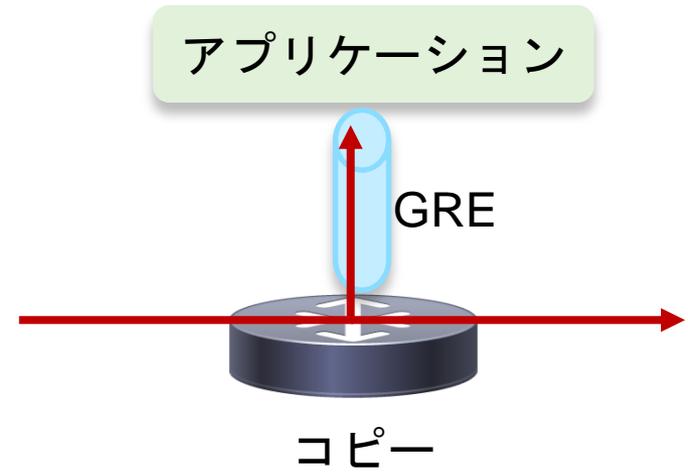
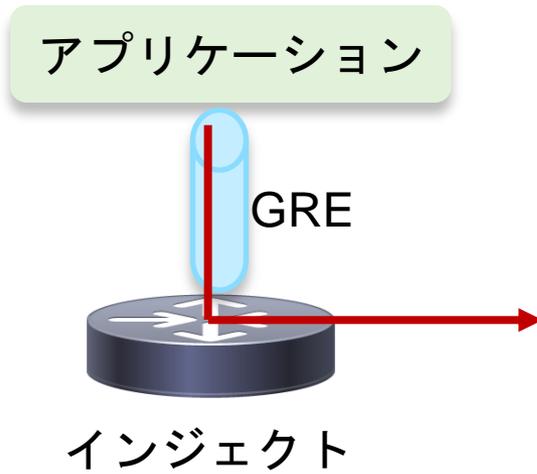


CE-AとCE-Bの間のトラフィック生成には
CE-Aの管理者権限が必要

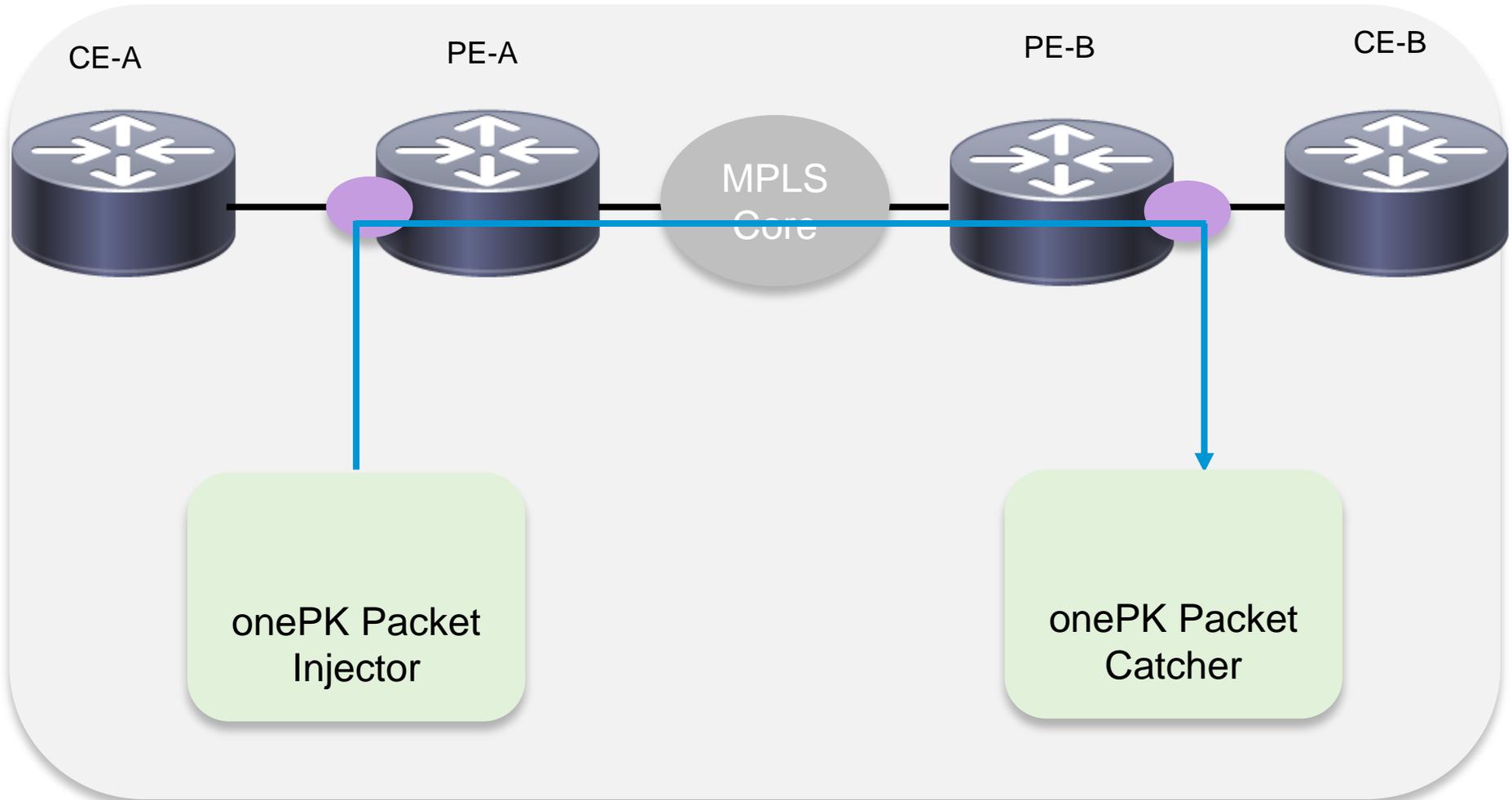
DPSS (Data Path Service Set)の利用

- DPSSはネットワーク機器からパケットを横取りしたり、ネットワーク機器にパケットを注入したりできます。
- これを利用して、あたかもユーザのネットワーク機器からコアのネットワークにパケットが到達したかのように見せかけることができるパケット送信プログラムを作成してみました。

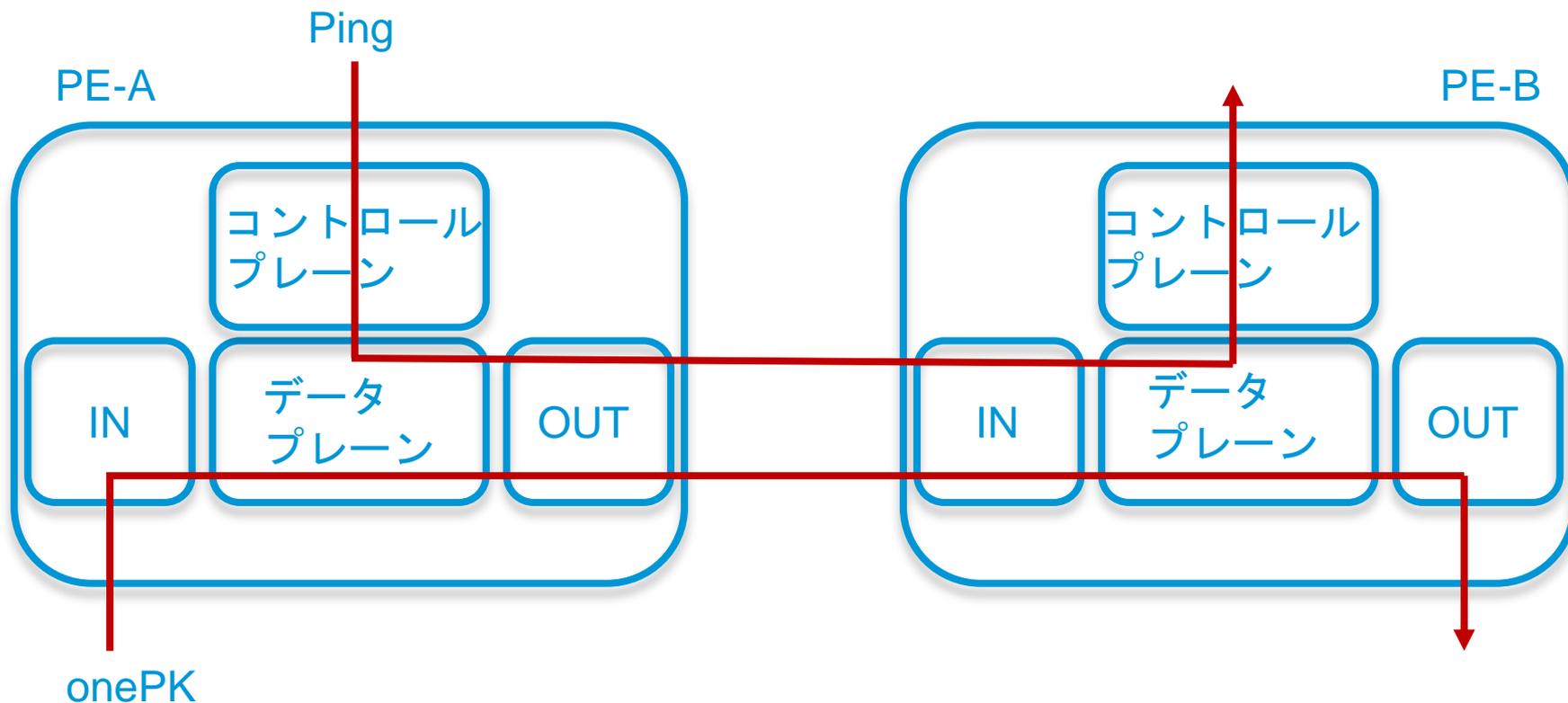
DPSS によるパケットの操作



DPSSを利用したL3 VPN Pathのチェック



PE上のPingとの違い



- 任意の packets が使用できます。
- ユーザネットワーク側のインタフェースのQoSなども適用されます。
- データプレーンのみで packets が転送されます。

テクニカルサービスからのAPI型SDNに対する期待

- データフォーマットが規定されることは歓迎できます。特に状態や状態遷移に関する情報がアプリケーションで扱いやすい形で取り出せると、アプリケーションが作りやすくなります。
- イベントが迅速に検出できるのは、API型の利点です。捕捉できるイベントの種類が増えると応用範囲も広がります。
- フォワーディングやルーティングだけでなく、ネットワークサービスやマネージメントなどの多様な機能に、APIであれば対応できると期待しています。



Thank you.

