フローモニタリング機能による MPLSトラヒック・マネージメント

ー　xFlowでのMPLSトラフィックモニタリング　ー

小林　淳史 akoba@nttv6.net
NTT情報流通プラットフォーム研究所

概要

- トラフィック・モニタ機能の現状/状況
  - NetFlow, sFlow, IPFIX/PSAMP
- MPLSトラフィック・モニタ機能
  - NetFlow v.9, (sFlow v.5)
- MPLSトラフィックをどうみるか？
  - プロバイダの立場、ユーザの立場
  - トラフィック交流の重要性
  - MPLSトラフィック交流の計測手法
- トラフィック・モニタ機能をサービスに？

目的
xFlowのMPLSトラフィックモニタリングを盛り上げたい

トラフィックモニタ機能の現状

	主な機能	アプリケーション
IF-MIB カウンタ	・リンク単位のトラフィック量計測	・リンク/ルータ単位の負荷状況確認（MRTG ..）
NetFlow	・フローベースのトラフィック配信	・トラフィック動向把握 ・課金（エンド・ユーザ使用量確認） ・トラフィックエンジニアリング ・異常トラフィック検出
sFlow	・フレームの先頭Byte（～256byte）を切り取って、IF-MIB情報とともに配信。	・トラフィック動向把握 ・トラフィックエンジニアリング ・異常トラフィック検出
IPFIX PSAMP	・フローベース/パケットベースのサンプリング抽出 ・サンプリング/フィルタリングによる柔軟な機能	・トラフィック動向把握 ・課金（エンド・ユーザ使用量確認） ・トラフィックエンジニアリング ・異常トラフィック検出 ・QoSモニタリング

トラフィックモニタに関する状況

トラヒックモニタ機能に対する需要.

・DDoS攻撃に代表される異常トラヒックの把握・検出.

・P2Pトラフィック特性の把握

・QoS適用によるトラヒック動向の把握.

・設備設計のためのトラヒック動向の把握.

・NWの大規模化,IPv4/IPv6プロトコルの混在

トラヒックモニタ機能に関する需要が高まる。

今や多くのインターネット・プロバイダでは、フローモニタを実施。

MPLSでは?

・トラフィックモニタの要求は、もっと強い?

・MPLSでも積極活用?

トラフィックモニタ機能（MPLS）

NetFlow v.9のMPLSでは何が配信されるか？（L3VPN）

ID	フィールド名
1	IN_BYTES
2	IN_PKTS
4	PROTOCOL
5	TOS
6	TCP_FLAGS
7	L4_SRC_PORT
8	IPV4_SRC_ADDR
9	SRC_MASK
10	INPUT_SNMP
11	L4_DST_PORT
12	IPV4_DST_ADDR
13	DST_MASK
14	OUTPUT_SNMP
15	IPV4_NEXT_HOP
21	LAST_SWITCHED
22	FIRST_SWITCHED
70	***MPLS_LABEL_1***
71	***MPLS_LABEL_2***
46	***MPLS_TOP_LABEL_TYPE***
47	***MPLS_TOP_LABEL_IP_ADDR***

通常のNetFlow フロー・レコード

MPLS情報

Cisco MPLS-aware NetFlowでは？

-Labelは、上位3つまで配信可能.

-Labelの情報は、Label(20bit), Cos(8bit), S(1bit)を配信。

Label（20bit）	Cos（3bit）	B（1bit）	TTL（8bit）

-TopLabelのアドレス（EdgeRouterのアドレス）とそのTypeを配信.

MPLSのLabelと送信先アドレスの情報が収集可能。

トラフィックモニタ機能の現状(MPLS)

	主な機能	アプリケーション
IF-MIB カウンタ	・リンク単位のトラフィック量計測	・リンク/ルータ単位の負荷状況確認（MRTG ..）
MPLS LSR-MIB カウンタ	・In/Outラベル単位のトラフィック量計測	・トラフィックエンジニアリング 頑張ればTEへの利用も可能
NetFlow	・スタックされたラベル情報が配信. ・ERのアドレス配信.	・トラフィック動向把握 ・トラフィックエンジニアリング ・異常トラフィック検出
sFlow	・フレーム内のラベル情報が配信. ・拡張情報によりERのアドレス配信が可能.	・トラフィック動向把握 ・課金（エンド・ユーザ使用量確認） ・トラフィックエンジニアリング ・異常トラフィック検出

MPLSのトラフィックをどうみるか?

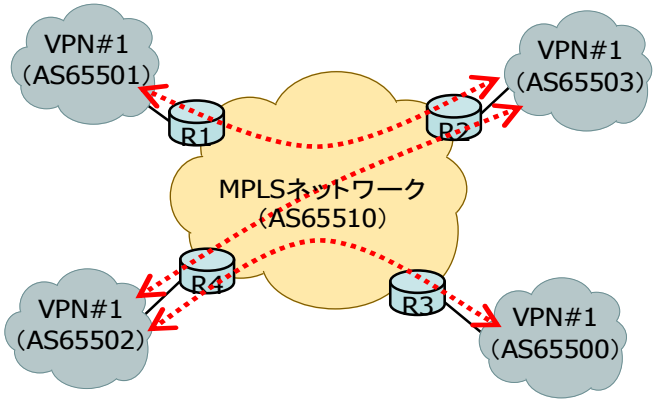
- プロバイダの立場
  - リンクコストが高いPoP間のトラフィック交流量把握.
  - ルータ間のトラフィック交流量をみてNWトポロジーの検討に反映したい.
  - ユーザまたはサービスクラスによってトラフィック量の占める状況を確認.
  - トラフィックトレンドを把握して、QoSポリシーに反映.
  - サイレント故障などによるトラフィックの急激な変動を検知.
  - プロテクションパスにきちんと流れている?

MPLS-LSR-MIBでは、実現が困難であったルータ間・PoP間のトラフィック交流の計測をNetFlowを用いて実現.

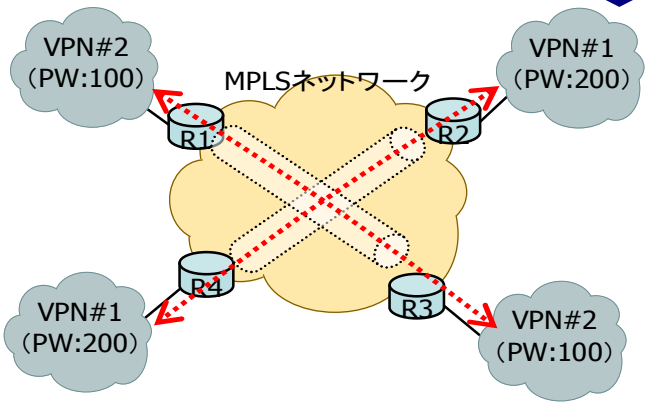
MPLSのトラフィックをどうみるか?

- ユーザの立場
  - フローの中身までは、見てほしくない.
  - フローの中身をユーザ自身で確認する機能を提供.
    - 提供の仕方については、考えないといけない.
    - トラフィックトレンドを分析してコンサルを実施.
  - ユーザトラフィックの地域間交流状況を提供.

ユーザ単位のトラフィック交流を計測



別AS間のトラフィック交流は、ユーザでは、計測できない!?



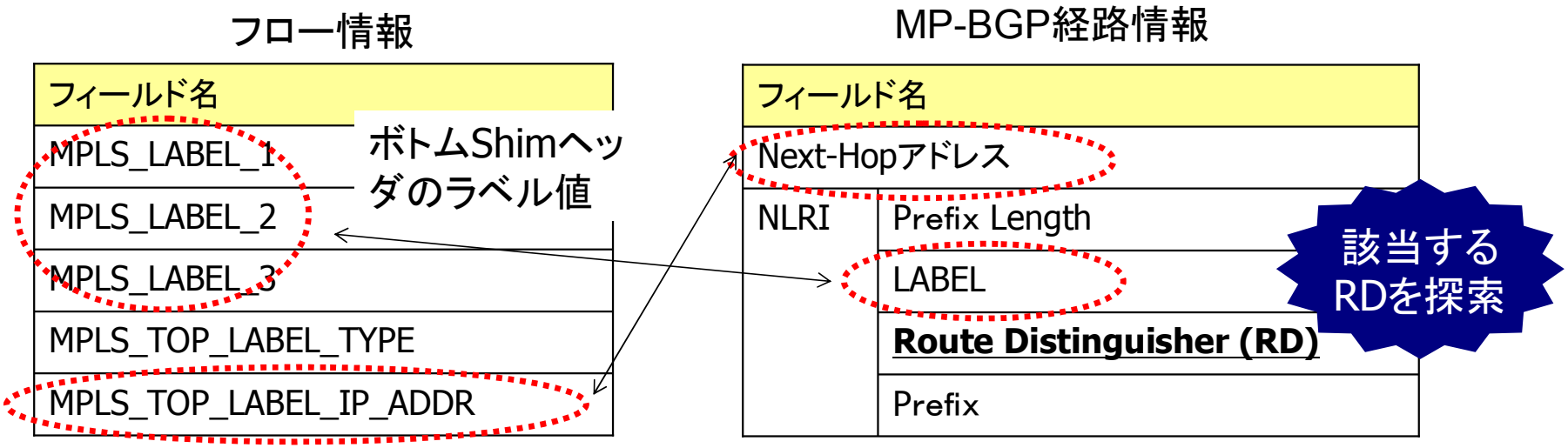
VPN(RD,PW ID)をグループ化して、課金単位に見せることができる。

トラフィック交流測定手法

- ルータ間トラフィック交流
  - 起点情報: NetFlowの配信元ルータ
  - 終点情報: MPLS_TOP_LABEL_IP_ADDR
- PoP間トラフィック交流
  - 各ルータをそれぞれの地域にマッピングしてルータ間トラフィック交流をもとに集計を実施.
- ユーザ識別情報の収集
  - L3VPNの場合: MP-BGPの経路情報を活用
    - VPNラベル→RD
  - L2VPNの場合: PW-MIBの情報を活用
    - VPNラベル→PW ID

ユーザ識別情報の収集（L3VPN）

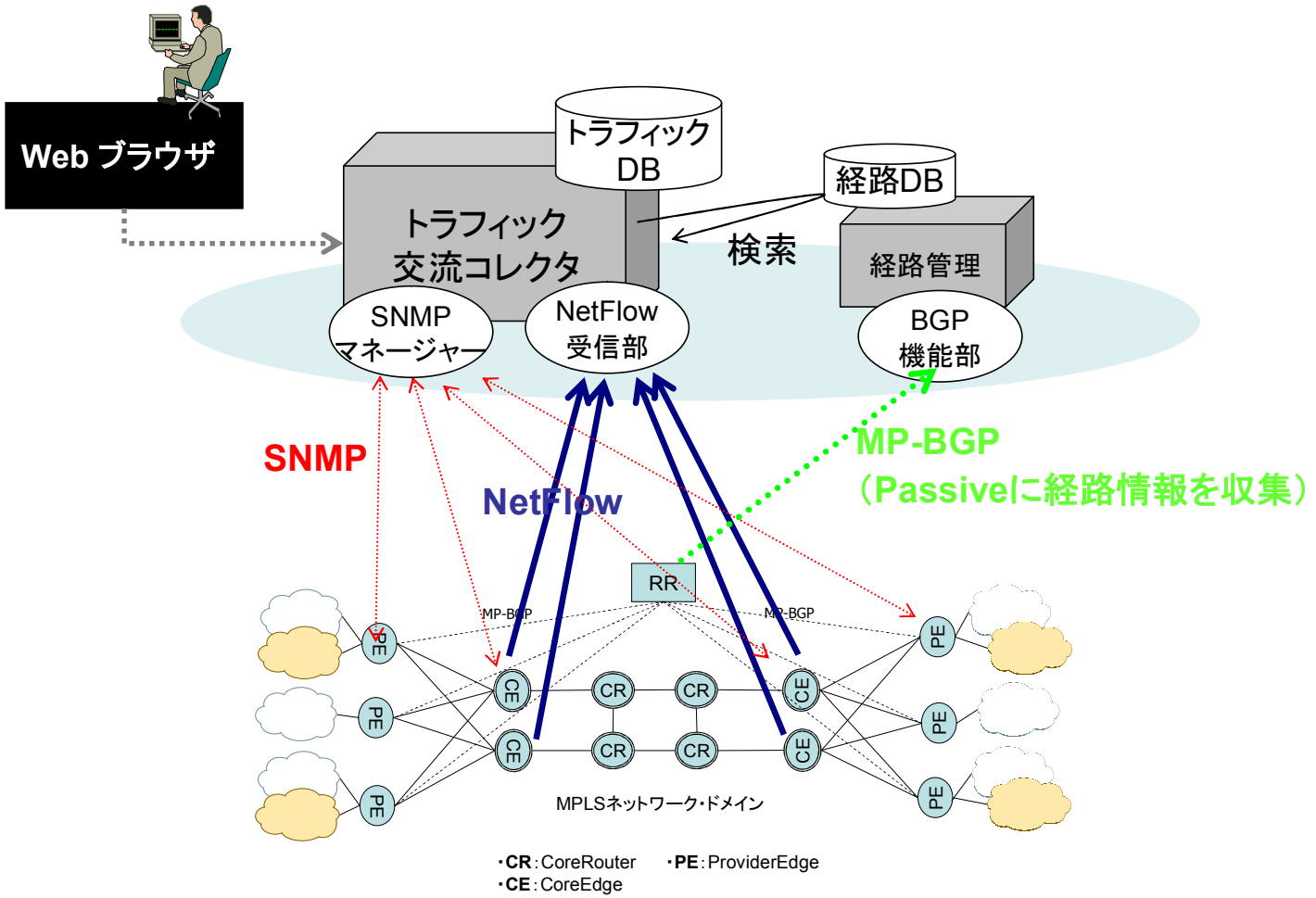
- Bottom Labelのラベル値をもとにMP-BGP情報と突合
  - フロー毎にRDを探索することが可能.
  - MP-BGP情報は、RRとPassive BGP peerにより収集.　or “NetFlow MPLS Label Export（※）”を利用.



（※） http://www.cisco.com/en/US/products/ps6566/products_feature_guide09186a00805f236a.html

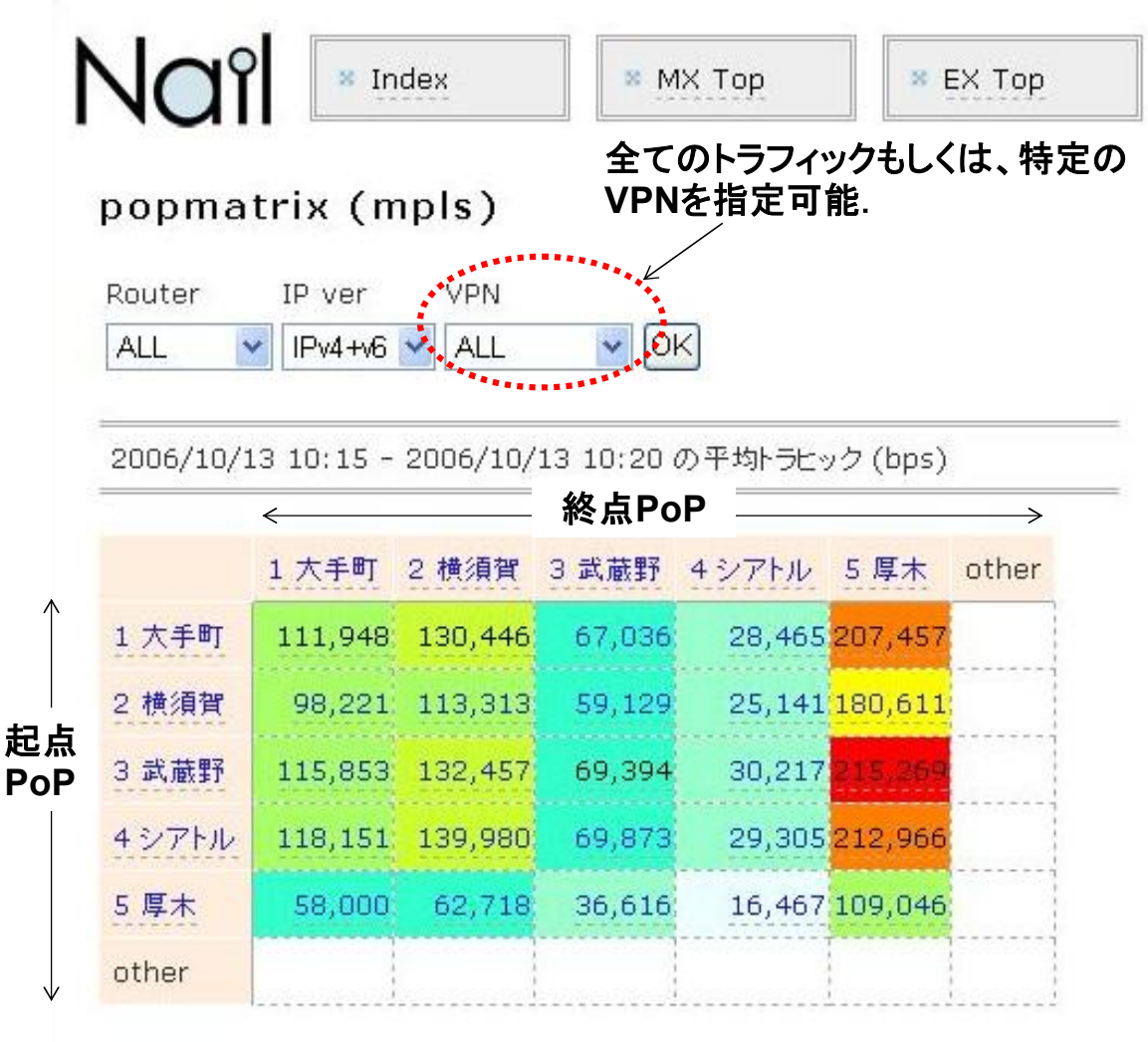
MPLS トラフィック交流コレクタの作成

- システム概要図　　どうみせるのかの可視化も重要。



MPLS トラフィック交流コレクタの作成

- PoP間トラフィック交流

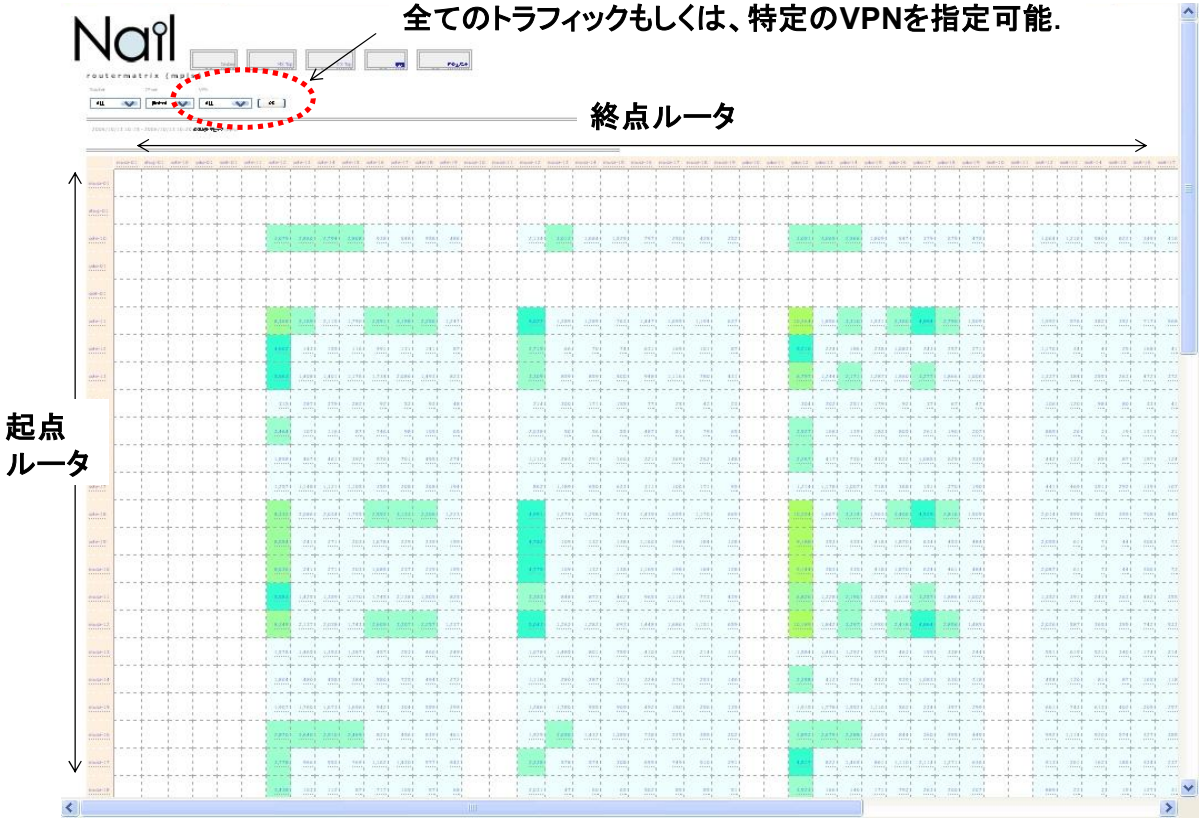


・リアルタイムにトラフィック状況を更新.

・2次元上に表現し、NWの交流状況を俯瞰的に可視化.

MPLS トラフィック交流コレクタの作成

- ルータ間トラフィック交流



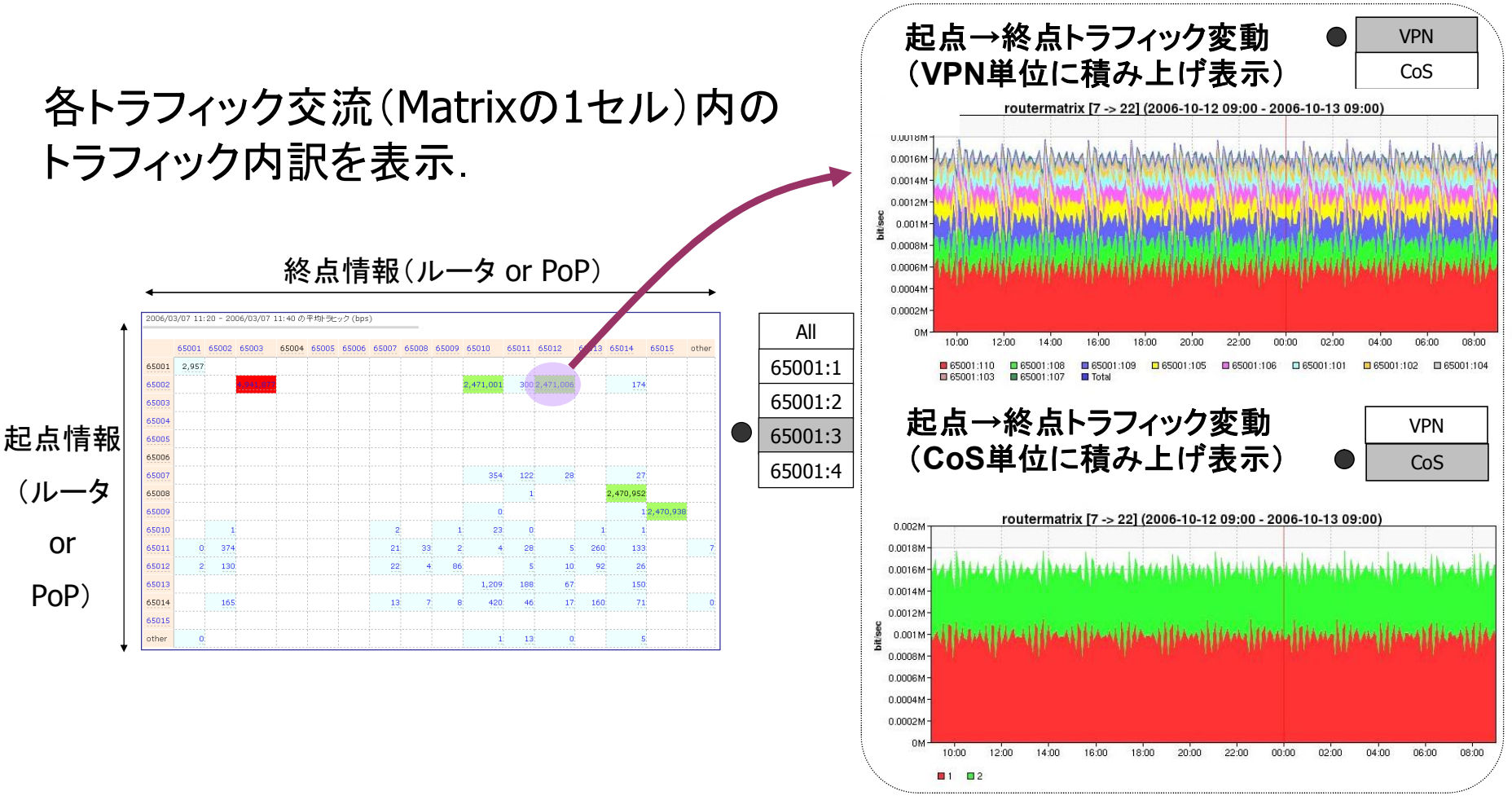
・リアルタイムにトラフィック状況を更新.

・2次元上に表現し、NWの交流状況を俯瞰的に可視化.

MPLS トラフィック交流コレクタの作成

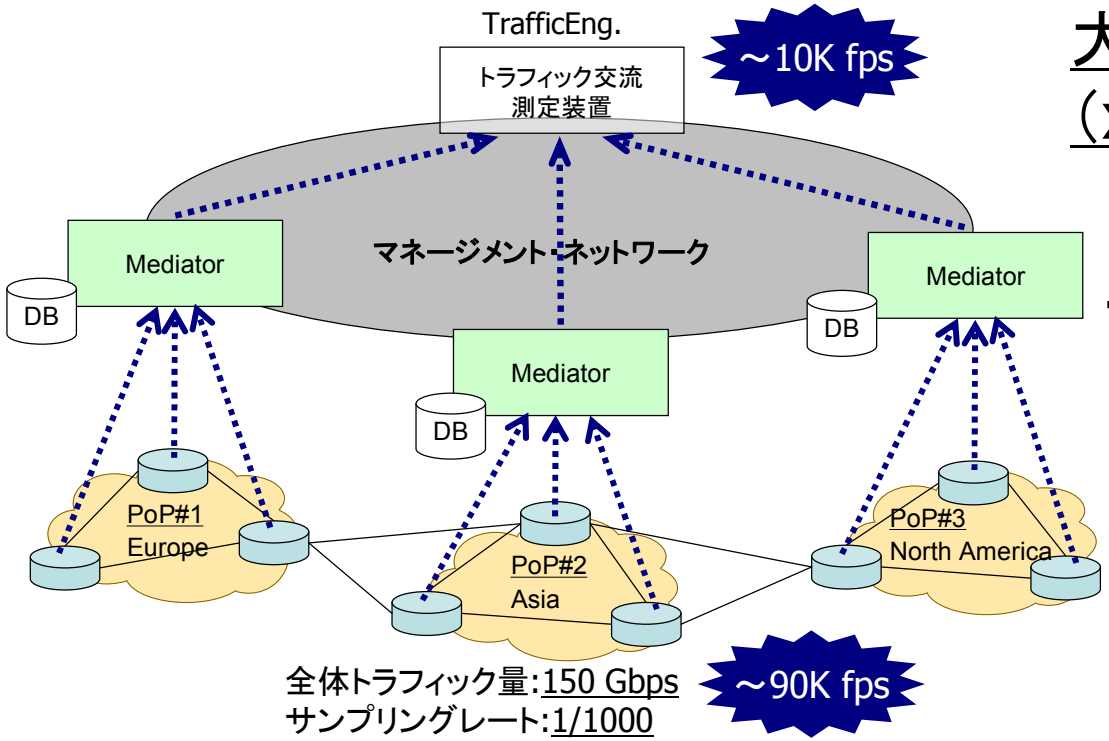
- VPN単位,CoS単位のトラフィック変動を図示.

各トラフィック交流（Matrixの1セル）内の
トラフィック内訳を表示.



ルータの性能/コレクタの性能

- ルータの性能は、日々向上. ~30k fps
- コレクタに必要とされるものは?
  - フローを保存、集約後、再配信するMeidatorを提案.



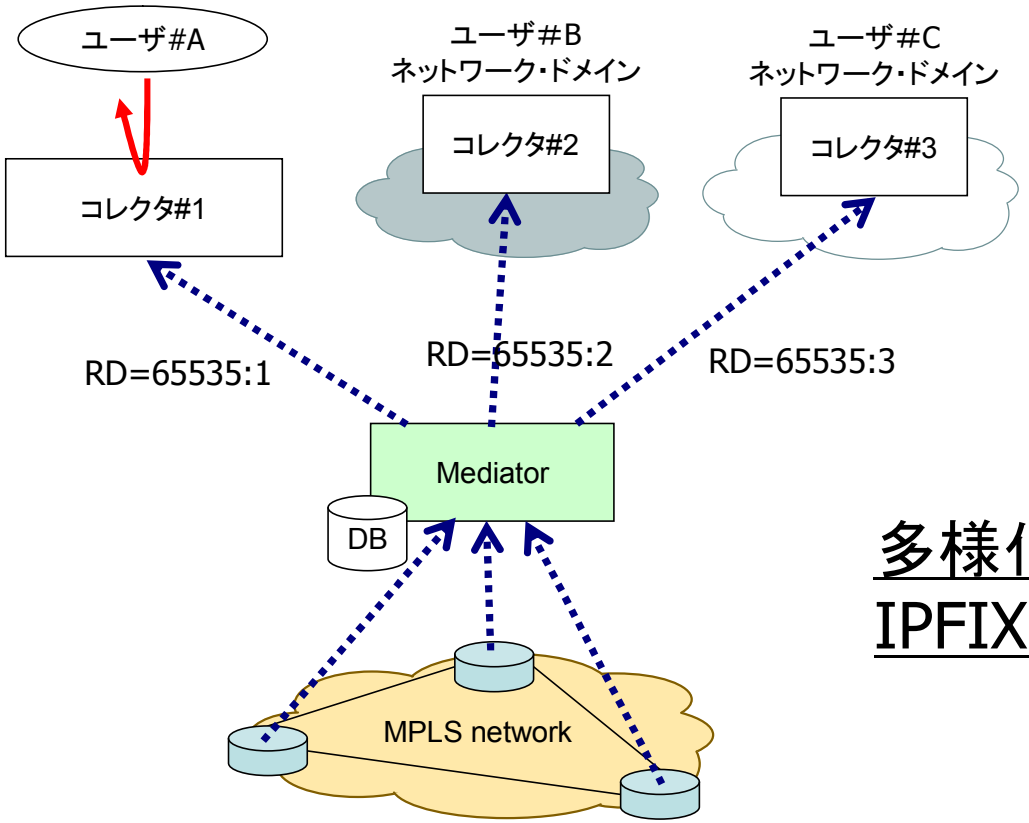
大規模NWでのIPFIX（xFlow）の適応性

・Label毎の集約.

draft-kobayashi-ipfix-mediator-01.txt

ユーザへの提供

- ユーザへのトラフィック提供のシナリオ
  - RD（VPN単位）にトラフィックを分散配置.
  - 場合によっては、そのままユーザNWドメインまで配信する.



多様化したNWでの
IPFIX（xFlow）の適応性

今後、議論していきたいこと

- MPLS　フローモニタリングの有効性
  - プロバイダの立場（実際にもう利用してる!?）
  - ユーザの立場(できるなら提供してほしい!?)
    - フローの情報はどう扱う?
- トラフィック交流
  - 計測手法・Tips.
    - NetFlowとMPLS MIBの連携．ifTypeに注意。
    - Template数＝stackの数×IPv4,v6×L2/L3
    - どこをenableにすると最適か?
    - LDP,RSVP,プロテクションパスとNetFlow親和性?
  - 小さいVPNトラフィックは、埋もれてしまう?

ご清聴ありがとうございました.

謝辞　本稿は，総務省委託研究「次世代バックボーンに関する研究開発」による成果である.