



網統合を再考する

河野 美也 Miya Kohno, (mkohno@juniper.net)

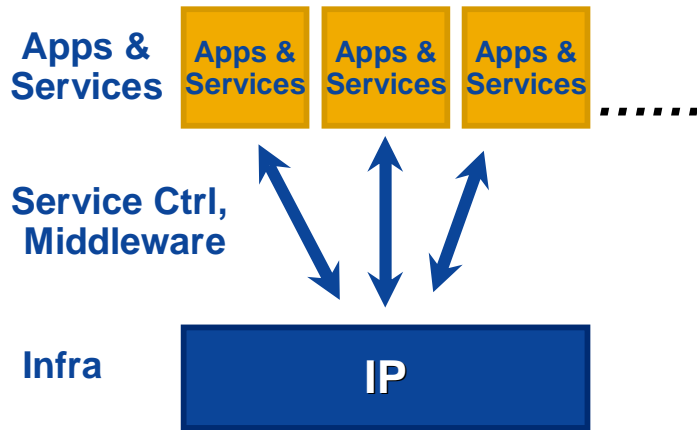
Agenda

- 「網統合」とは一体何か
- 「網統合」における課題の整理
- 統合のための要素技術例
- まとめ

統合の考え方

1.

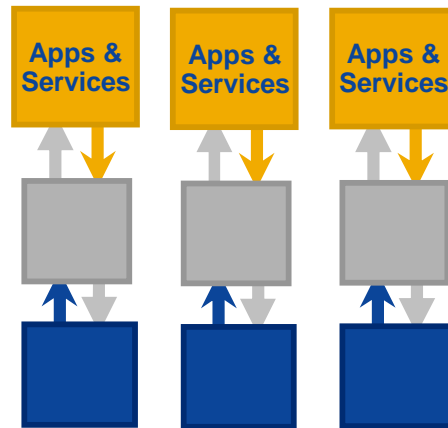
何でも取り込む
(インターネットモデル)



End-to-end
Everything over IP

2.

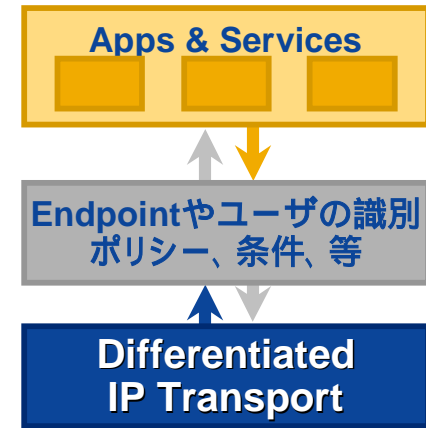
垂直統合
Vertical Integration



Optimization
Closed Architecture

3.

水平統合
Horizontal Integration



Virtualization
Open Architecture

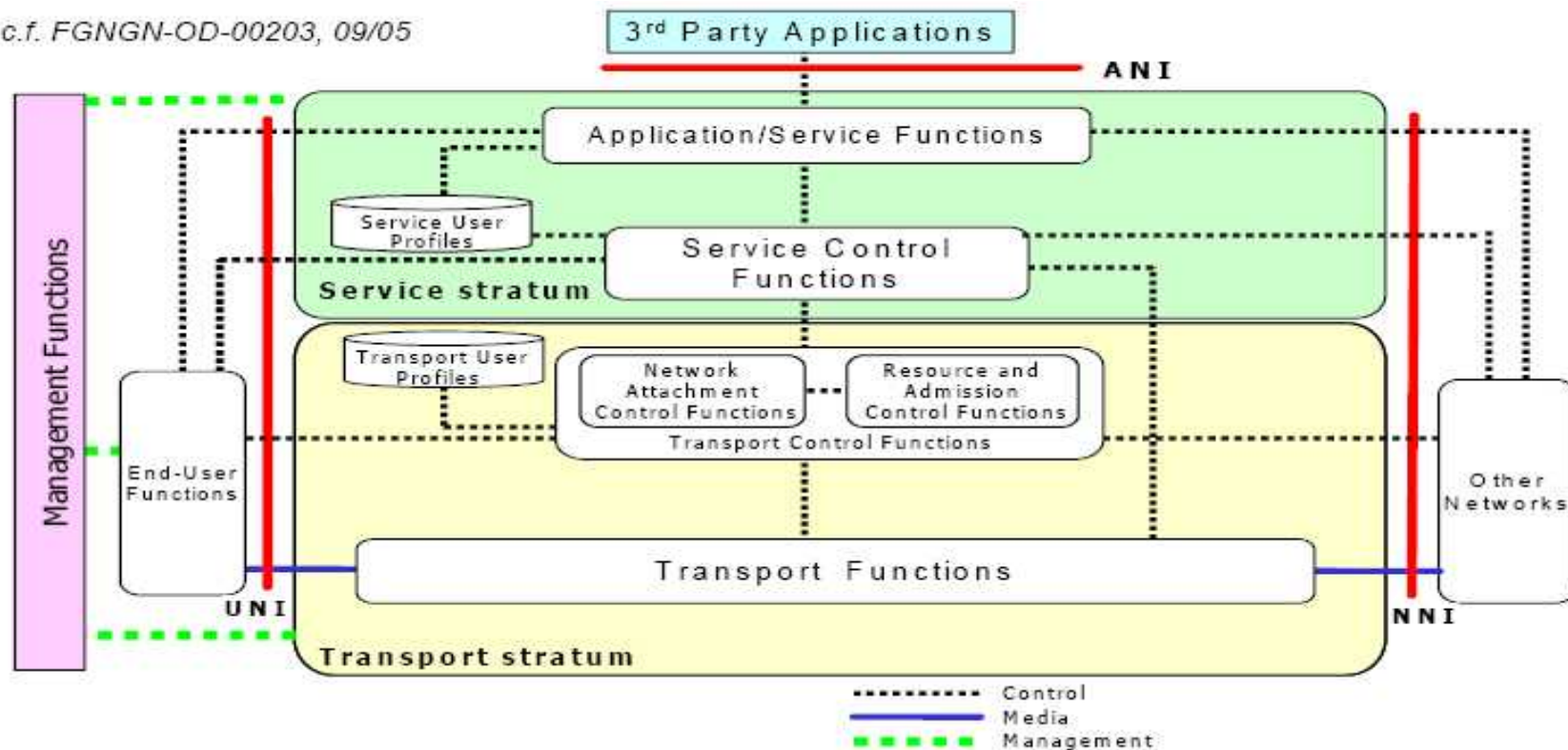
現在の「統合」志向性...

- 「Transport Stratum」
 - マルチサービス、FMC、UNI/NNI/SNI(ANI)(from NGN)
- 「共通インフラ・Platformとしてのネットワーク」
 - 必要に応じて必要なサービスをタイムリーに提供
 - 新たなサービスの協調・融合(Mash-up)、早期展開(from SOA)
- 「複数の異なるネットワークを統合してシンプルに」
- 「運用コスト、機器コストの削減」
(from World-wide SP市場動向)

→ 水平統合/Virtualization...

Transportを切り出す (差別化されたトランスポート)

c.f. FGNGN-OD-00203, 09/05

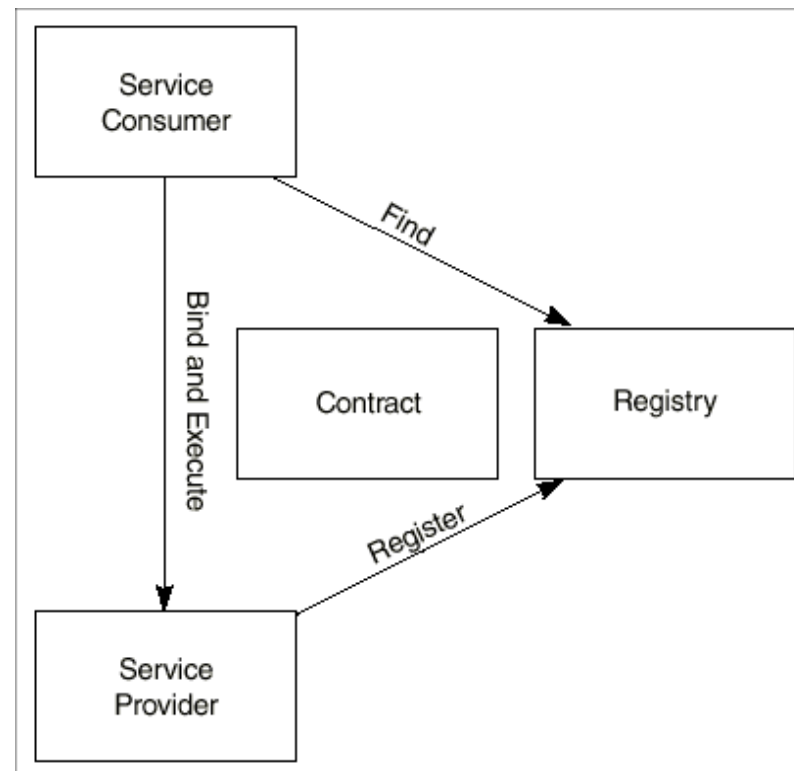


Note: UNI/NNI/ANI are not meant to represent any specific interfaces.

Multi-service, support for fixed-mobile convergence,
separation of services and transport, *QoS awareness*, packet transport

Transportを切り出す (Objectとしてのトランスポート)

EmbeddedであったTransportをモジュールとして捉える



- 再利用性
- 可視化
- 高付加価値化

Service Oriented Architecture

http://www.developer.com/java/web/article.php/10935_2207371_1

網統合とは一体何か

- 今我々が「統合」と言っているのはどうやら

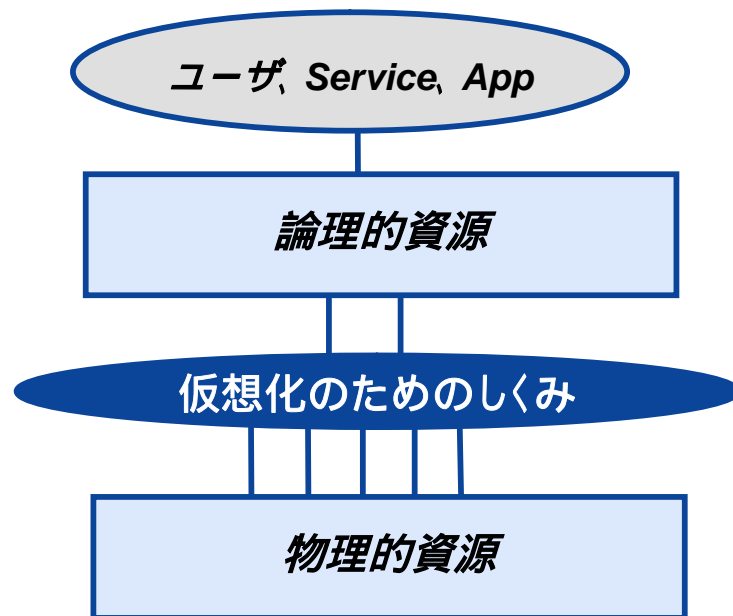
Virtualization

らし

Virtualization

■ 仮想化とは

- 物理的資源は、仮想化のためのしくみにより、論理的資源に、(抽象化 | 隠蔽 | 分割)される。
- ユーザや、サービス・アプリケーションは、論理的資源を利用する。



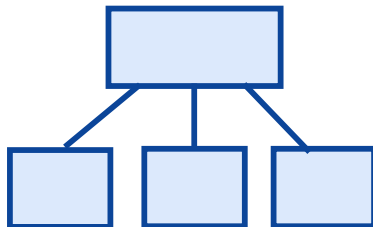
→冗長/Fault Tolerant性を実現する手法、
という側面も持つ。

Virtualization

■ 仮想化の方法

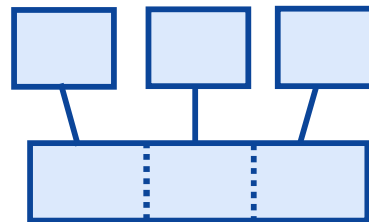
1) Aggregation

- Link bundling
- RE redundancy
- 階層化
CsC, RR, LSP hierarchy...
- ...



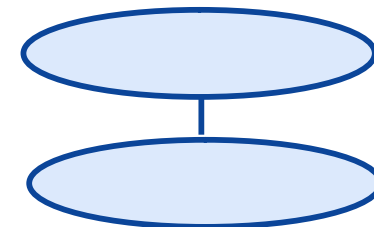
2) Partitioning

- Logical Router
- vlan
- Modularity
- QoS
- Multi-topology
- Confederation
- ...



3) Emulation

- VPN
- VPLS
- PW
- ...



Virtualizationにおける課題

- 「統合」と「分離」という、内在する二律背反をどうするか

Control Plane

↑ - 共通コントロールプレーン

↓ - fate-sharing、リソース競合を避ける

Forwarding Plane

↑ - 共通インフラ、統合トランスポート

↓ - QoS分離、トポロジー分離

Management Plane

↑ - 統合マネジメントシステム、一元管理、集中管理

↓ - 組織主体、サービスによる分離(provisioning, syslog, statistics..)

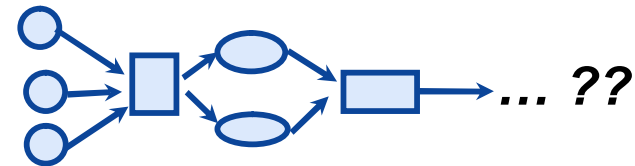
その他

- セキュリティ、責任分解点のためのBoundary
- リソース保護
- Disaster Recovery, Risk Management

Virtualization - 設計指針

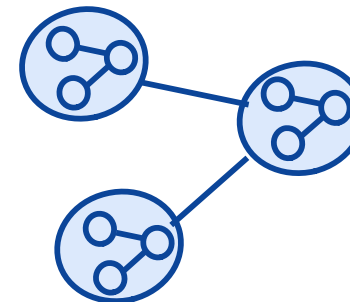
■ 複雑性、オーヴァヘッドを最低限に留める

- 統合・分離を、必要以上には繰り返さない
 - Link Bundling(統合) + QoS(分離) ?!!
 - Logical Router(分離) + RE redundancy(統合)
- Self-similarityが保てればOK(のことが多い)
 - Route Reflector(統合) + Confederation(分離)



■ 拮抗する要素を調整する

- 統合 vs 分離
- 安定性 vs 高速性(高速検出・高速処理)
 - GR/NSR vs Fast Convergence, Route Flap Dampening
- 拡張性 vs きめ細かさ
 - FEC粒度
- 運用性(シンプルさ) vs 多機能
- パーフェクトなエミュレーションは無理かも...



■ 要素技術を充分吟味し選択する

Virtualizationの要素技術例 (1/2)

■ 統合

1) トランスポート統合

- 統計多重によるリソース有効活用
- 共通基盤化によるCAPEX/OPEX削減
- 戦略的企業基盤

2) コントロールプレーン統合

- 運用負荷軽減
- 複雑性の排除
- スケーラビリティ向上

3) コントロールプレーン冗長

- 耐障害性向上
- 網の安定性向上

Virtualizationの要素技術例 (2/2)

■ 分離

4) コントロールプレーン分離

- 組織、運用主管による管理の分離
- サービスの分離
- fate-sharingの回避

5) フォワーディングプレーン分離

- トランスポートを共有しながらも、サービス品質を分ける

■ リソース保護

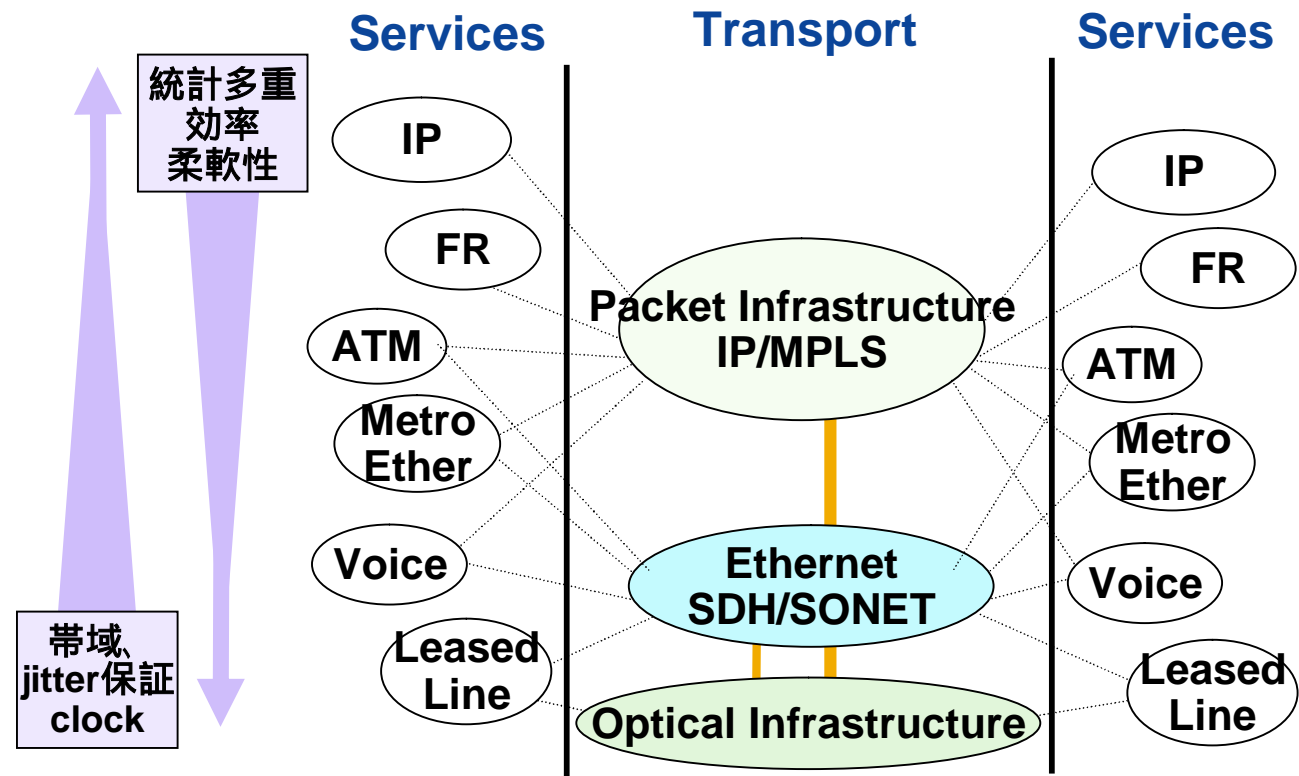
6) コントロールプレーン保護

- 過負荷やリソース不足からコントロールプレーンを保護する

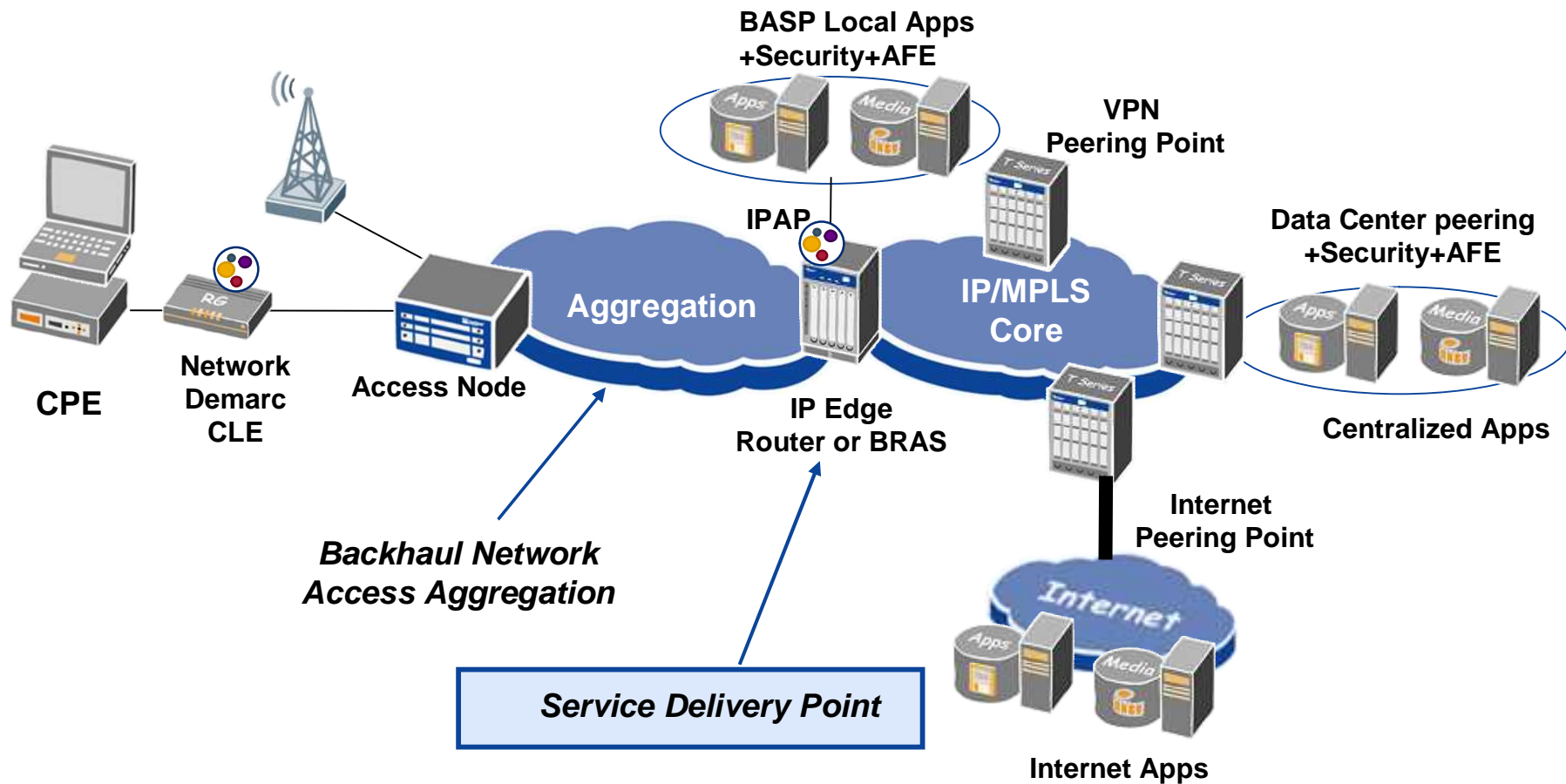
1) トランスポート統合

- IP/MPLS (IETF)
- Ethernet (IEEE, MEF) , SDH/SONET (ITU-T)
- Optical Transport Network (ITU-T, OIF)

- p2p, mp2p
- p2mp, mp2mp

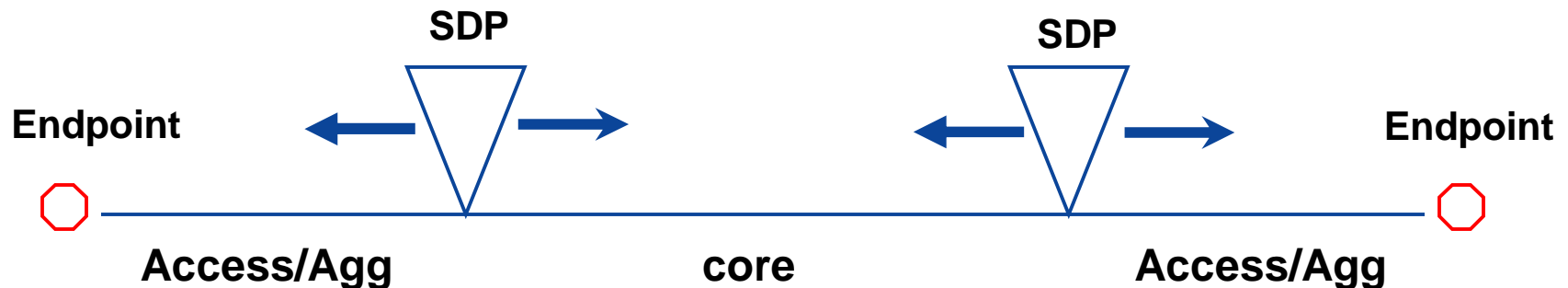


Multi-Service Network Architecture



統合トランスポート - 考慮点

1. どのレイヤで統合するか
2. Service Delivery Point (SDP) をどこにするか
 - どこにどの機能が必要か？
3. Access Aggregationに適用する技術を何にするか



Service Delivery Pointに求められる要件

- 機能要件
 - Multi-service PE (for business use)
 - BRAS (for residential use)
 - Voice GWs
 - Policy Enforcement Point
 - QoSの扱い
 - Security (Filtering, uRPF, etc.)

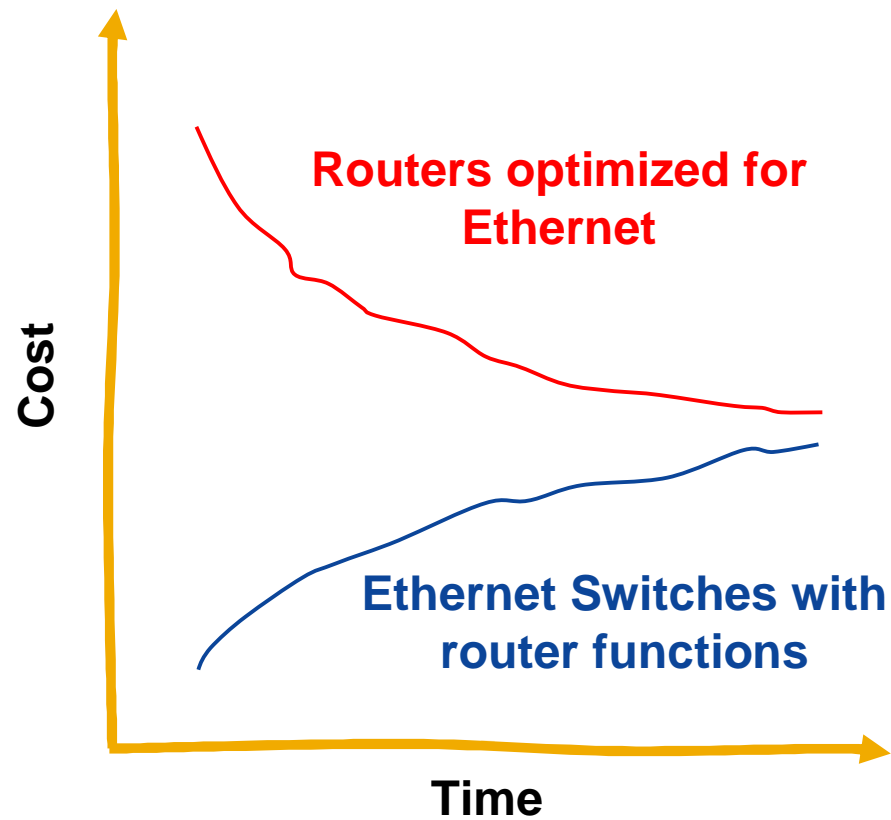
...

Access Aggregationに求められる要件

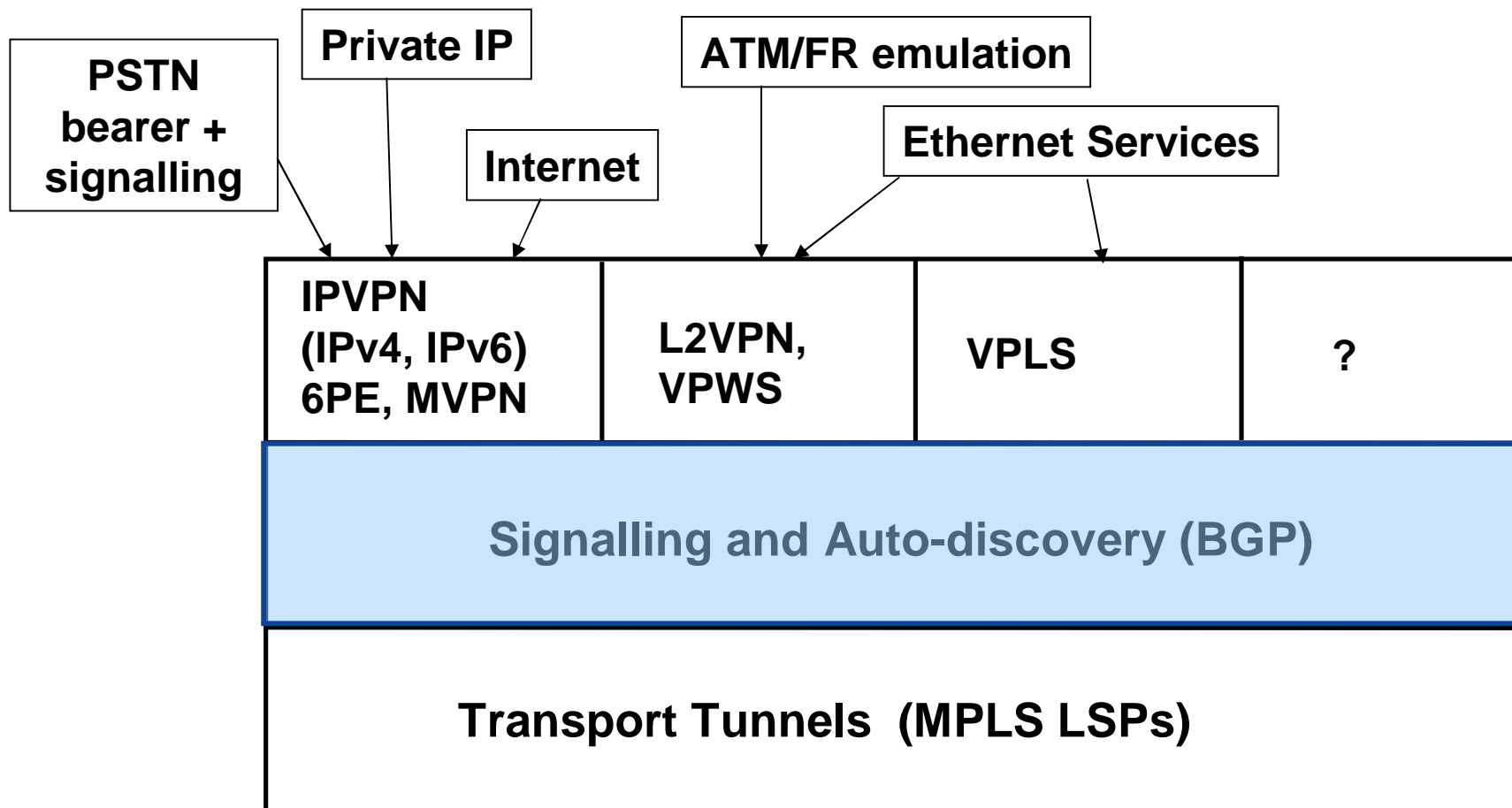
L3機能は必ずしも必要ないが...

- Capacity, Scalability
- Low-Cost
- Multiservice
- p2p, mp2p, p2mp, mp2mp
- Virtualization (aggregation + separation)
- Easy operation
- OAM
- Protection/Resiliency
- QoS

値段が問題?



2) コントロールプレーン統合

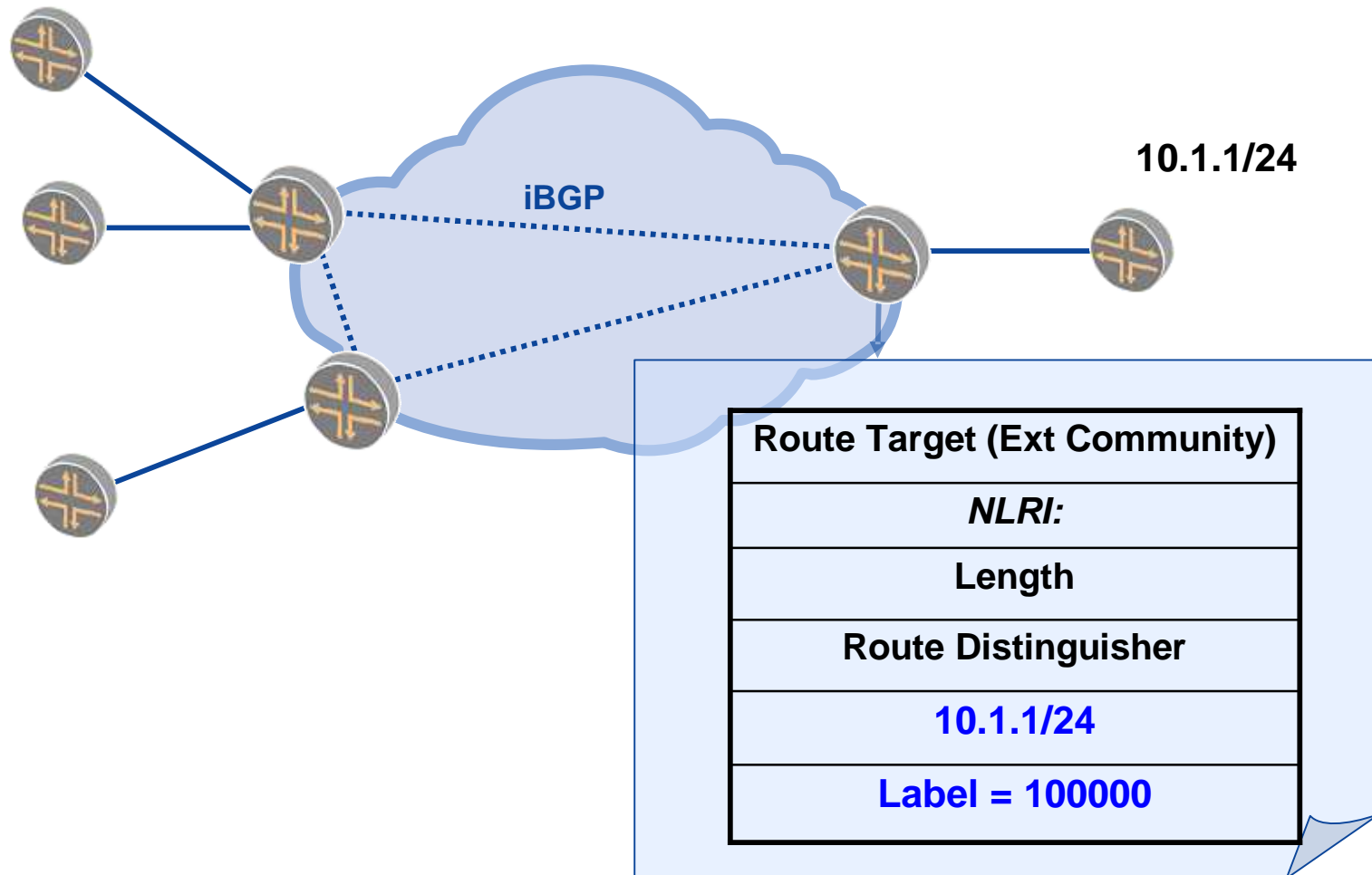


コントロールプレーン統合

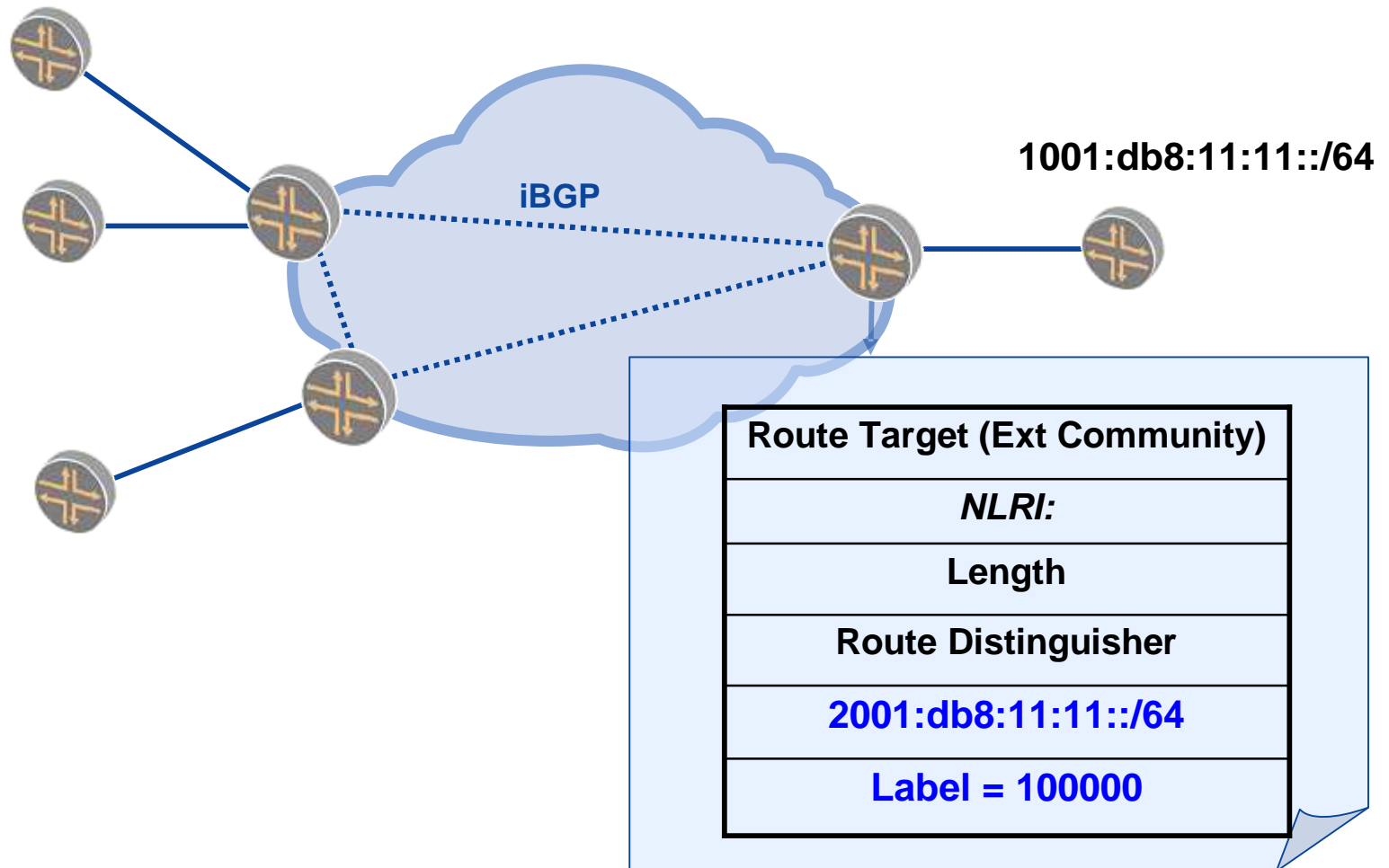
- 共通Control PlaneとしてのBGP

	IP VPN unicast	L2VPN	VPLS	MVPN
広報する Reachability information	IPv4 / IPv6 prefixes	CE-ID	VE-ID	JoinするC-Multicast state (S,G),(*,G)
RDの役割	IP prefixの区別	CE-IDの区別	VE-IDの区別	C-Multicast state (S,G) (*,G) の区別
RTの役割	VPNメンバーシップの制御	同左	同左	同左

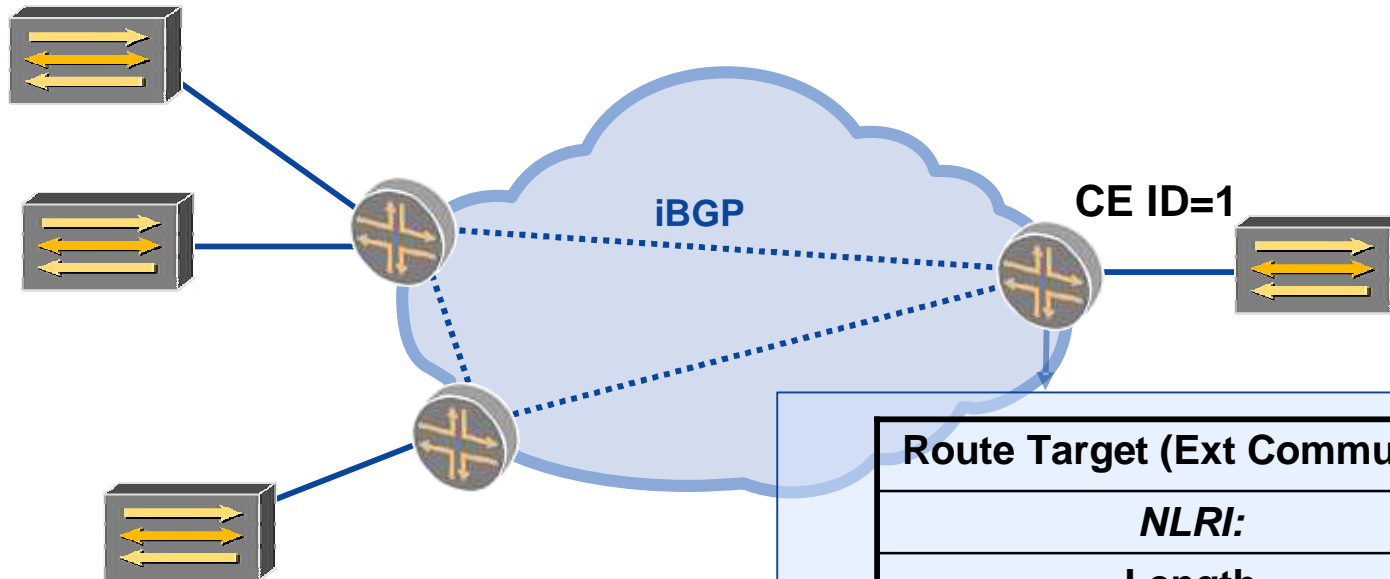
L3VPN (IPv4)



L3VPN (IPv6)



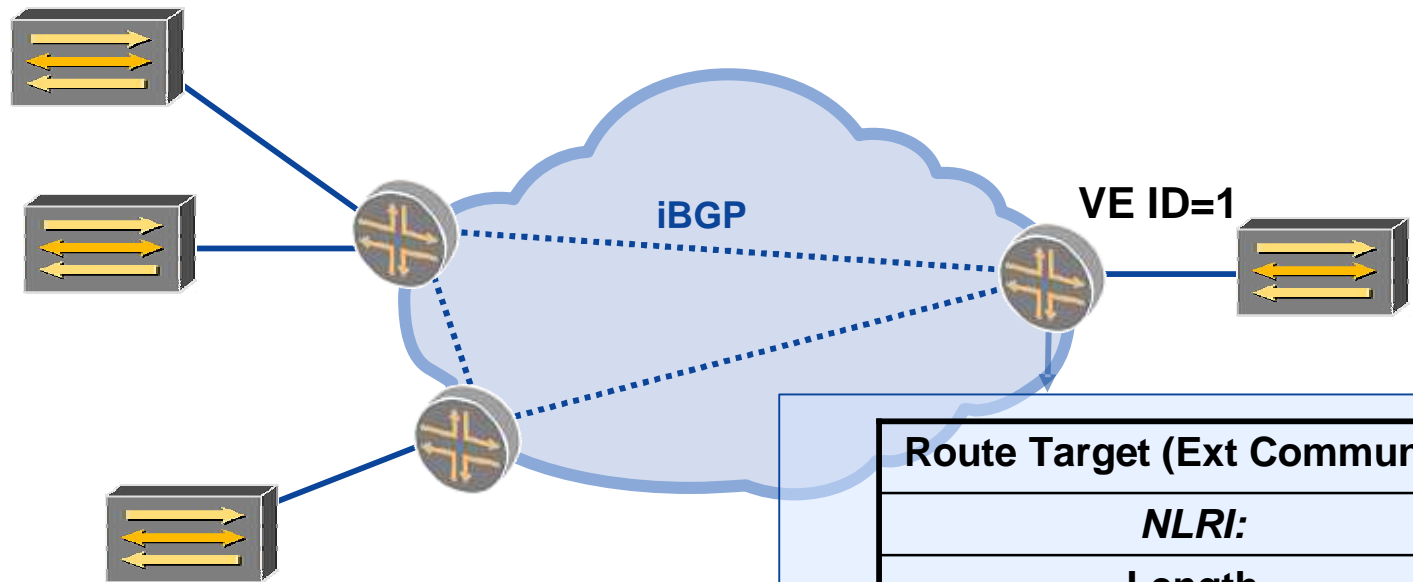
L2VPN



Route Target (Ext Community)
<i>NLRI:</i>
Length
Route Distinguisher
CE ID = 1
Block Offset = 1
Block Size = 8
Label Base = 100000

* L3VPNとの違いは、相手CEにより使用するLabelが異なるところ。

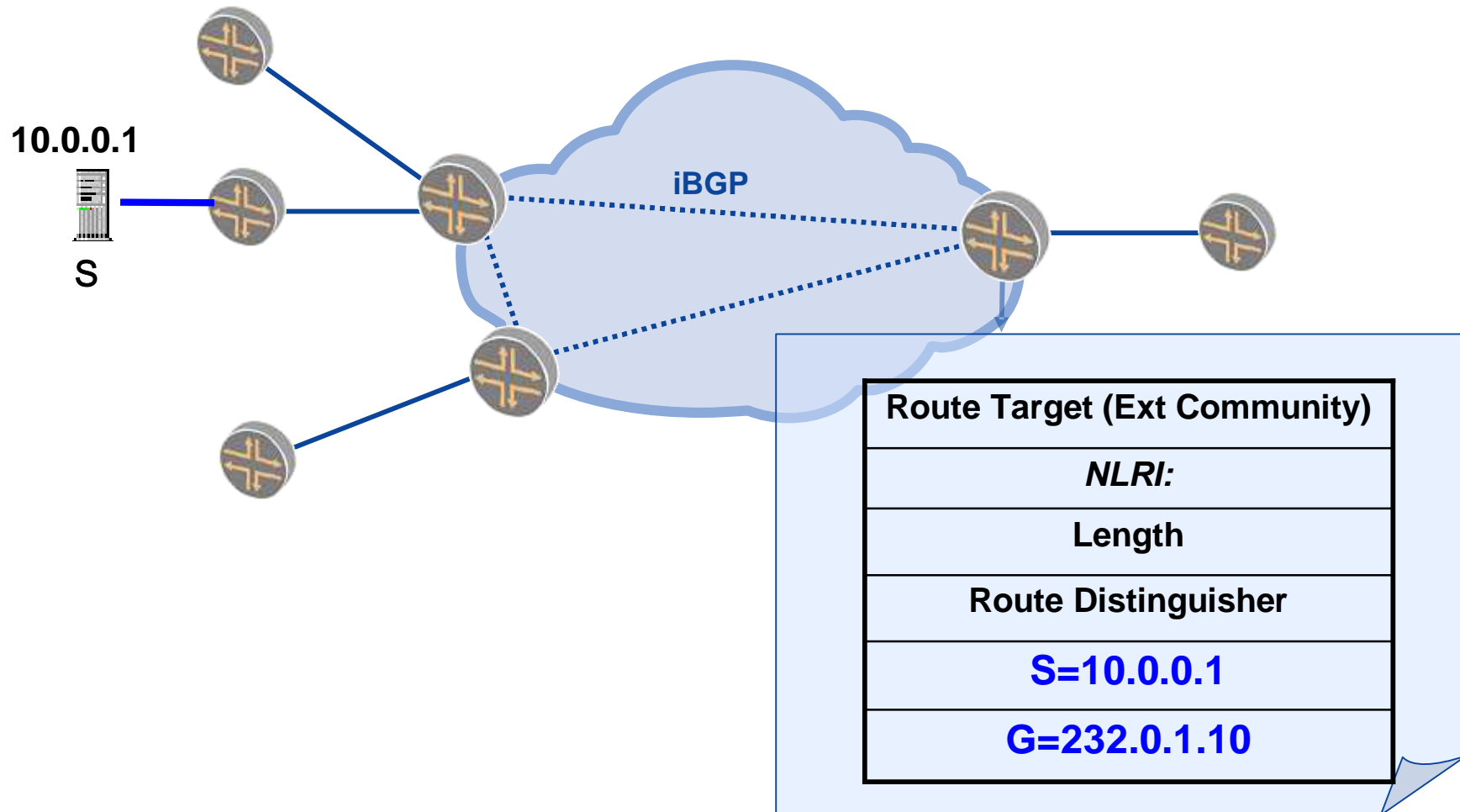
VPLS



Route Target (Ext Community)
<i>NLRI:</i>
Length
Route Distinguisher
VE ID = 1
VE Block Offset = 1
VE Block Size = 8
Label Base = 100000

* L3VPNとの違いは、L2VPN同様、相手CEにより使用するLabelが異なるところ。

MVPN



コントロールプレーン統合

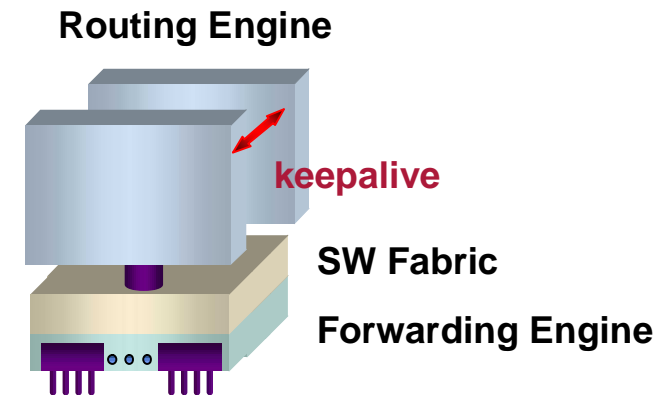
-共通Control PlaneとしてBGPを使うことのメリット

- MP-BGP + Capability negotiationによる機能・サービスの取捨選択
 - Route ReflectorによるScalability向上
 - Route Target Ext Communityによる柔軟なReachability制御
 - Inter-AS対応
 - Auto Discovery
 - Multihome (+BGP path selection)による冗長化と切り替え
- 【 PE-PE full-mesh T-LDP sessionやPE-PE full-mesh PIM は
要りません 😊 】

3) コントロールプレーン冗長

■ コントロールプレーン冗長の必要性

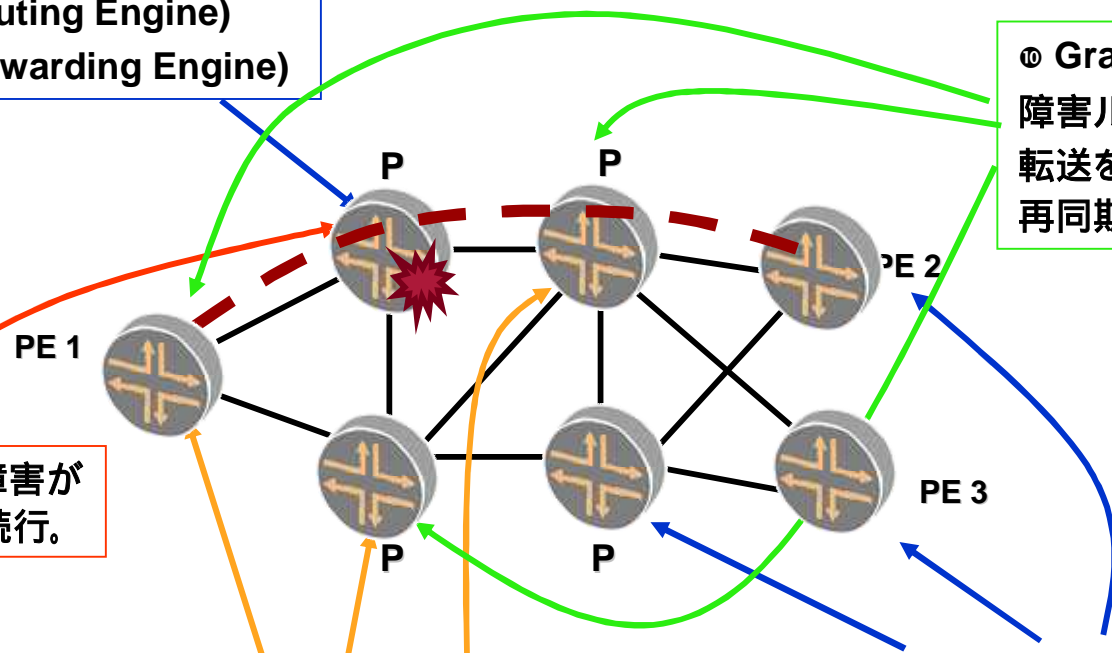
- コントロールプレーン断は起こりえる
 - 計画停止
ソフトウェアのアップグレード、保守
 - 無計画停止
異常事象、バグ
- 起こった場合の影響が予想以上に大きくなる可能性がある
 - ルーティング収束
 - Oscillation
 - Cascade Failure



Graceful Restart / NSR

Control PlaneとData Planeは独立

- ⑩ RE (Routing Engine)
- ⑩ FE (Forwarding Engine)



Control Planeに障害が
起こっても転送は続行。

⑩ Graceful Restartの場合、
障害ルータが復帰すると
転送を続行しながら、状態の
再同期を取る。

⑩ Graceful Restartの場合、Neighborは
helperとして動作する。但し、他のノードに
障害が起こったことを伝播しない。

⑩ NSRの場合、Neighborも障害を関知し
ない。

他のノードは、障害を関知しない。

→ 障害は局所に留まる
→ 安定

4) コントロールプレーン分離

■ Logical Router (LR)によるコントロールプレーン分離

● 分離

- Management Plane
- Control Plane
- 各LRで動作させるSoftware Instance

● 共用

- Master Management Plane
- ハードウェア資源 (Software Logical Routerの場合)
 - Uplink回線
 - CPU, memory
 - ... with some partitions

Service Separation

セキュリティ境界

fate sharingの回避

Software Logical Routerがサポートする機能

ルーティングインスタンスの分離

IS-IS, OSPF, RIP, RIPng
BGP
Routing instances
IP Multicast
IPv6 support
Routing policies

インタフェース共有

- all types
- sub-interface level

論理インタフェース

Frame relay
VLAN
CCC
VPLS

SLRにおけるHA機能

stability
Aggregate i/f
APS, VRRP
Fast re-route
BFD **New**
Graceful restart

SLRにおける VPNサポート

Layer 2 VPNs
Layer 3 VPNs
VPLS **New**
CCC

SLRにおける MPLSサポート

RSVP
LDP
DiffServ TE

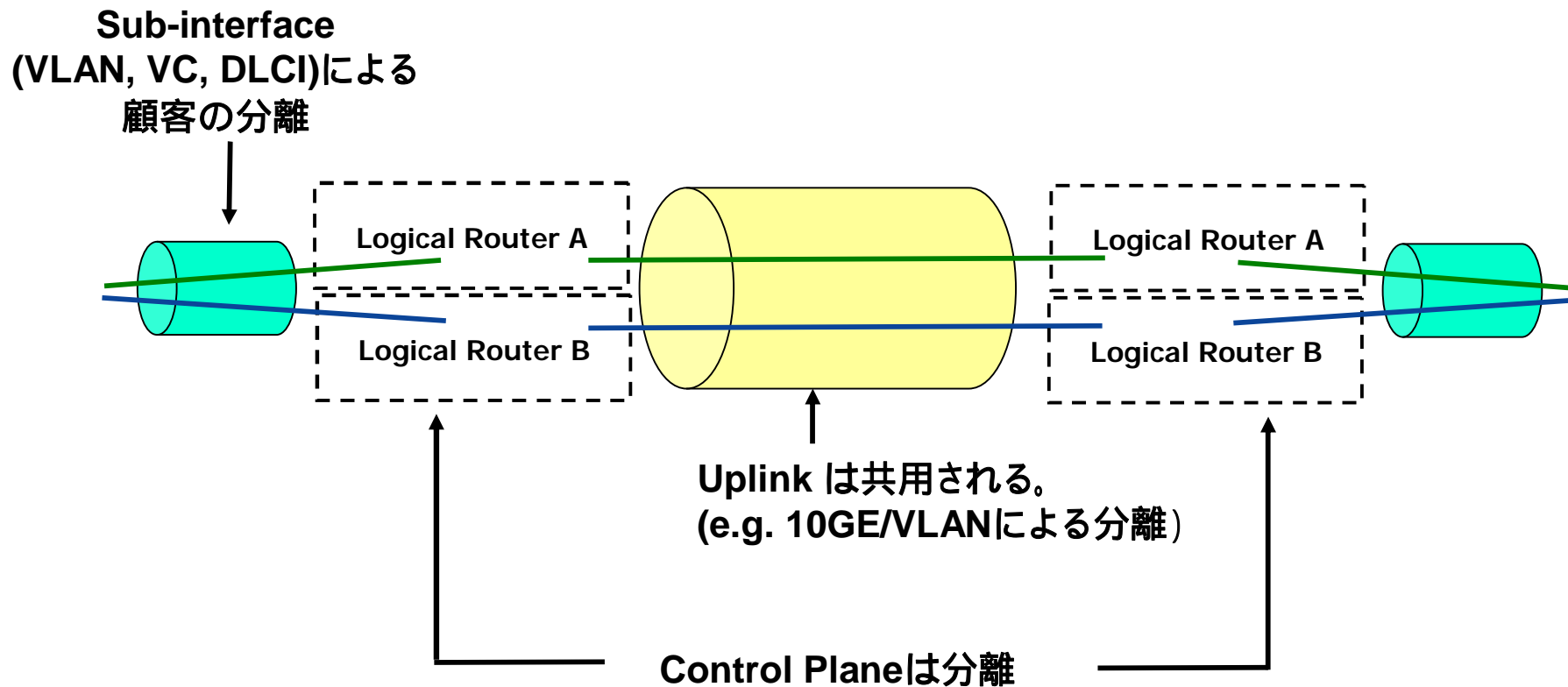
管理ドメインの分離

SNMP per LR **New**
LR login class **New**

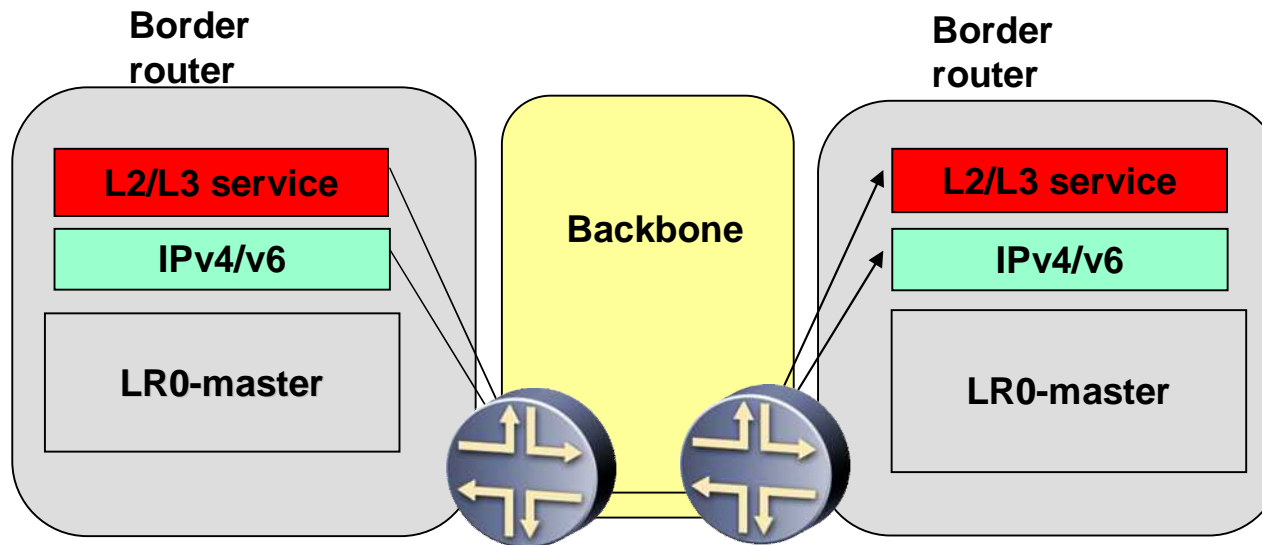
LR Masterにてサポートされる 機能

GMPLS
Class-of-service
Forwarding options
NSR, ISSU

Logical RouterによるUplinkの共有



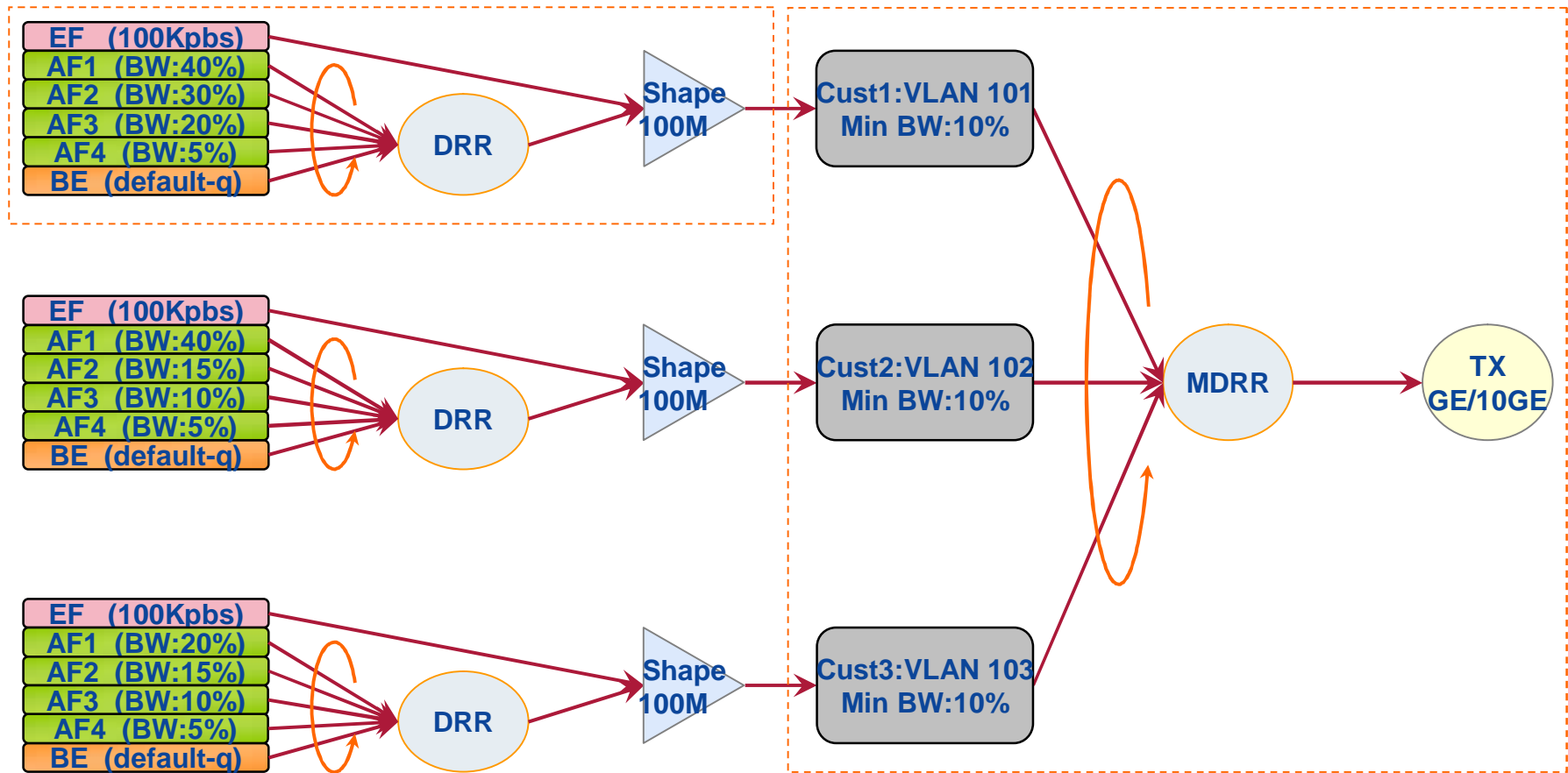
Logical Routerによるサービス分離例



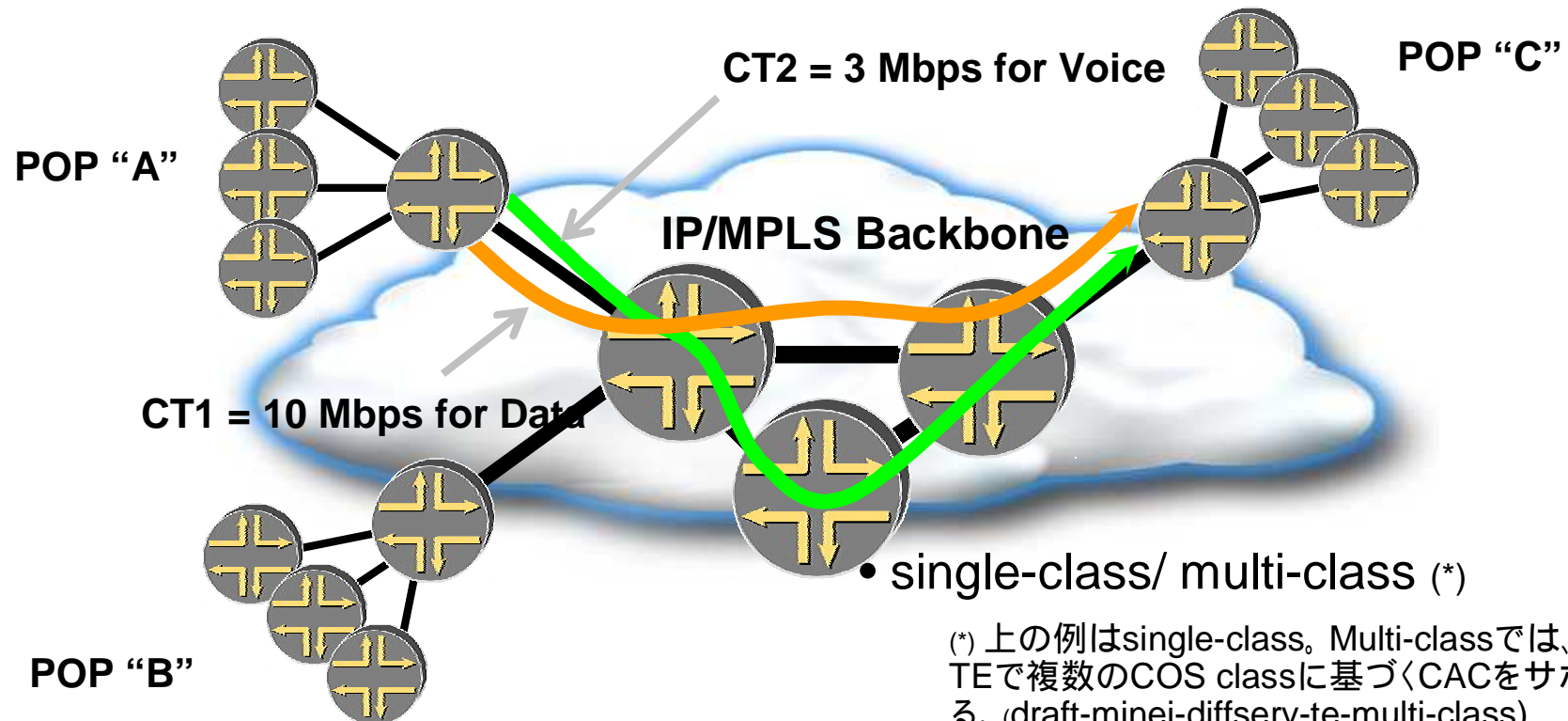
5) フォワーディングプレーン分離

- Diffserv Queueによる分離
- TE, DS-TEによるCSPFとCAC
- MTR (Multi Topology Routing)

Diffserv Queueによる分離



TE, DS-TEによるCSPFとCAC

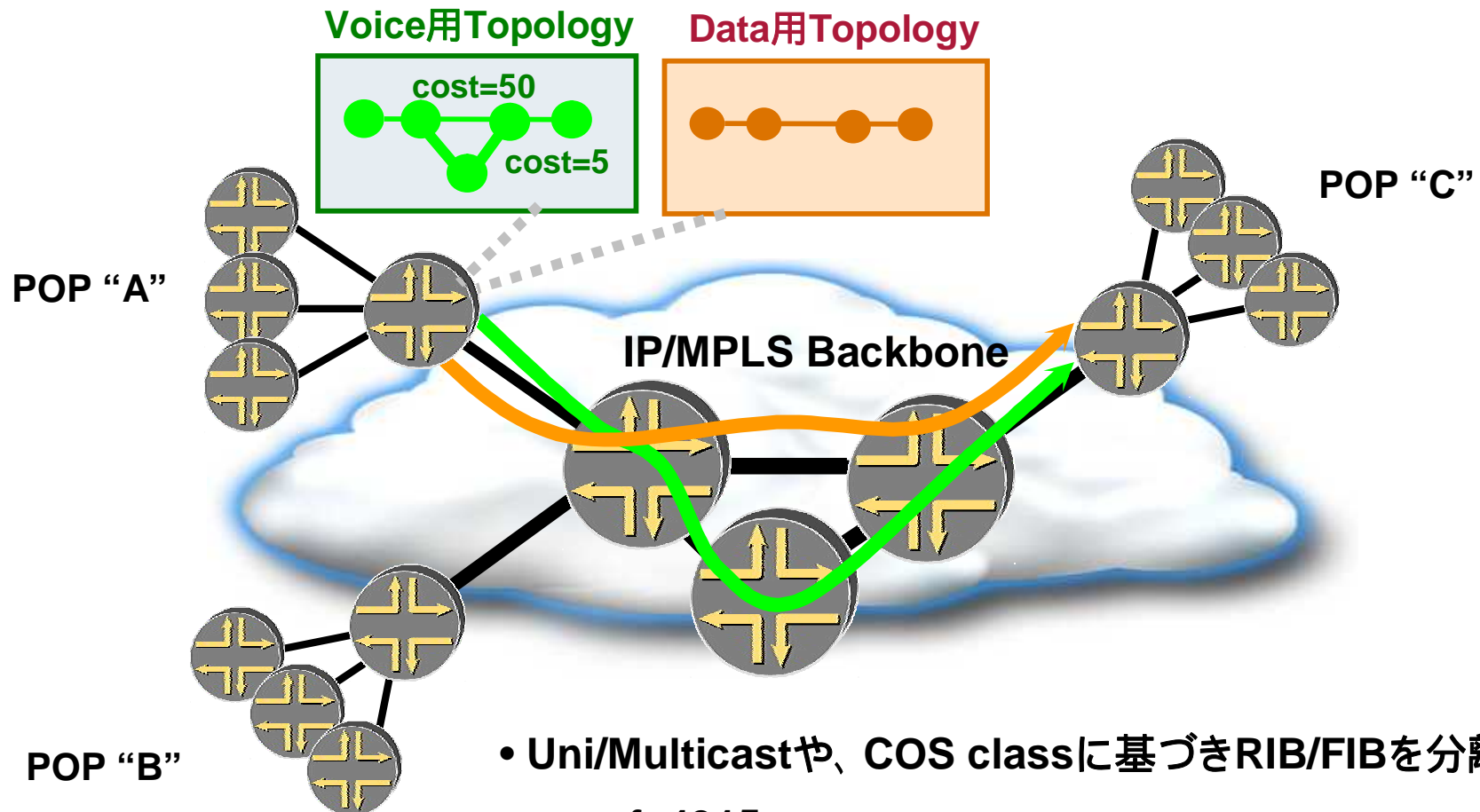


- single-class/ multi-class (*)

(*) 上の例はsingle-class。Multi-classでは、一つのTEで複数のCOS classに基づくCACをサポートする。(draft-minei-diffserv-te-multi-class)

- RDM/ MAM/ extended MAM
- Policer on/off

MTR (Multi Topology Routing)



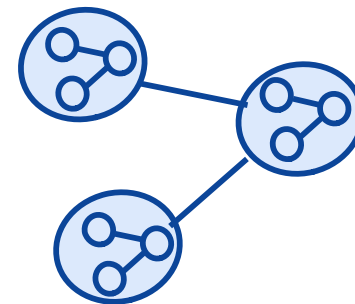
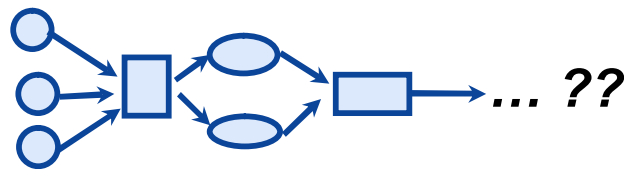
- Uni/Multicastや、COS classに基づきRIB/FIBを分離する。
- rfc4915
- draft-ietf-isis-wg-multi-topology-11
- ...

6) リソース保護

- コントロールプレーンによるリソース保護
 - エッジルータのメモリ保護
 - L3VPN – per-VRF prefix-limit
 - Internet – per eBGP peer prefix-limit
 - VPLS – per VPLS Forwarding Table Max MAC addresses
 - エッジルータのCPU保護
 - Control Plane Rate Limiting – per (sub) interface

まとめ – Virtualized Networkの設計指針

- 「網統合」の目的を明確にする。
 - 利用する技術を慎重に吟味する。
{Control plane|Forwarding Plane} x {集約|分離|保護}
 - 必要以上に「統合」「分離」を繰り返さない。
 - 二律背反、拮抗を調整する。



Thank you !