

MPLSとGMPLS

～ サービス提供と、その伝達を支える技術～

Internet Week 2006 チュートリアル

第一部:MPLS

松嶋 聡
ソフトバンクテレコム株式会社

2006/12/07

Internet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>

Table of Contents

- MPLSの基礎
- MPLS Traffic-Engineering
- L3VPN (BGP/MPLS-VPN)
- MPLS技術の今後の展望

2006/12/07

Internet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>



MPLSの基礎

2006/12/07

Internet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>



MPLSの基礎 Agenda

- MPLSとは、
- MPLSのパケット転送
- MPLSのシグナリング

2006/12/07

Internet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>

MPLSとは

- **MPLS: Multi Protocol Label Switching**
 - IPネットワーク上で、ラベル(Label)という概念を用いて、パケットを転送する技術
 - ConnectionlessのIPネットワークにパスの概念をもたらし、様々なレイヤ、サービスの統合トランスポートネットワークに変貌させる技術の一つとして注目
 - TrafficEngineering, L3/L2VPN, IPv6, マルチキャスト
- **ラベル転送という一つのスキームですべてを同じに扱うことができる。**

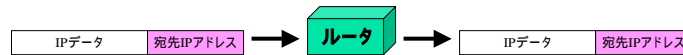
2006/12/07

Internet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>

MPLSとは

- **MPLSになると。**

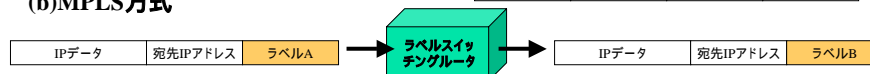
(a)既存IPルーティング方式



宛先IPアドレスに基づきルータが方路選択(パケットルーティング)

ラベルテーブル			
入力インタフェース	ラベル	NextHop	出力時ラベル
:	:	:	:
:	:	:	:

(b)MPLS方式



ラベル番号に基づきラベルスイッチングルータが、方路選択(ラベルスイッチング)

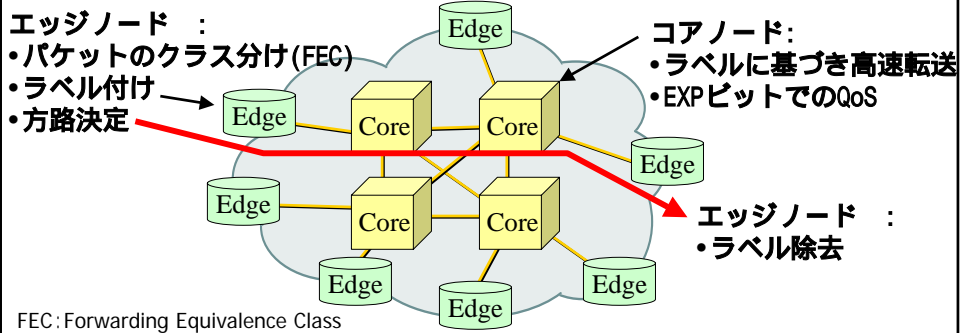
2006/12/07

Internet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>

MPLSとは::アーキテクチャ概要

- MPLSドメイン::一つの管理ドメインに所属し、MPLSが動作する機器で構成されるネットワーク

MPLSドメイン



2006/12/07

Internet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>

MPLSレイヤ位置付け

- Layer2, Layer3双方からマルチプロトコル

Application	レイヤ5以上
TCP/UDP	レイヤ4
IP(v4/v6)	レイヤ3
MPLS	レイヤ2.5
ATM	レイヤ2
FR	
PPP	
Ether他	レイヤ1



- 様々なレイヤ間のサブレイヤとして発展

Application		Application
TCP/UDP		
IP(v4/v6)		
L2		
MPLS/IP		MPLS/IP
L1/L2		L1/L2

2006/12/07

Internet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>



MPLSの歴史と発展

- ATMからの発展
 - VC/VPの概念とIPルーティングの融合
 - IP Switching, CSR (Cell Switching Router), Tag Switching etc
- MPLSの誕生
 - IPネットワーク上でのマルチプロトコル転送技術として誕生
 - 当初は、IPパケットのカプセルリング転送技術
 - 徐々にレイヤ2フレームなどの転送にも応用

2006/12/07

Internet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>



MPLSの歴史と発展

- GMPLS (Generalized MPLS)の展開
 - 光パスなど、IPネットワーク上だけではない、光伝送路へのラベルパス概念の導入
- ネットワークの実用化に伴い、OA&M機能の実装が行われている。

2006/12/07

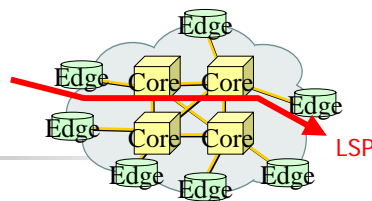
Internet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>

MPLSの パケット転送とシグナリング

2006/12/07

Internet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>

MPLS 用語説明



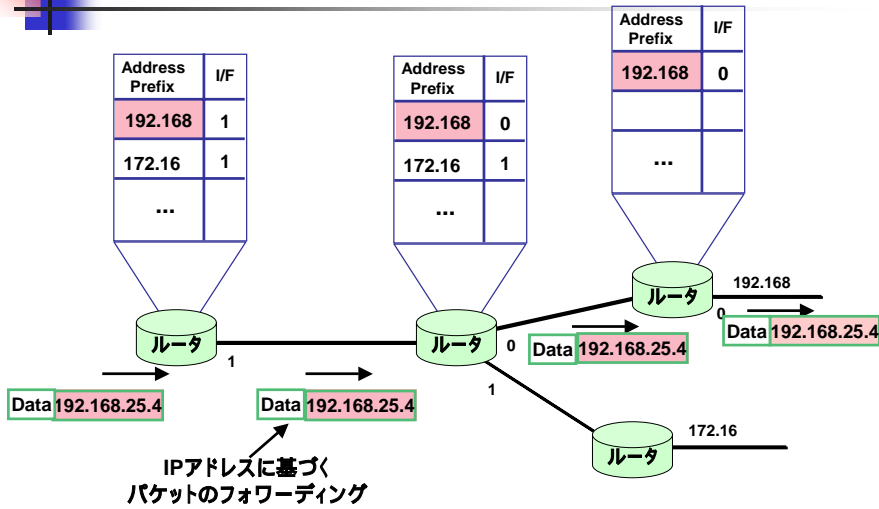
- **LSR (Label Switching Router)** : MPLSドメイン内にありMPLSを解釈できるLayer3装置
 - **Ingress LSR** : MPLSドメイン入り口のエッジLSR
 - **Egress LSR** : MPLSドメイン出口のエッジLSR
- **FEC (Forwarding Equivalence Class)** : 同じ経路、同じ扱いで転送されるIPパケットの集合
 - FEC 1 : 宛先IPアドレス
 - FEC 2 : 宛先IPアドレス + ある特定のTCPポート番号
- **LSP (Label Switched Path)** : FECに対応して形成されるMPLSラベルパス

2006/12/07

Internet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>

MPLSの packets 転送

通常のIPでの転送方式



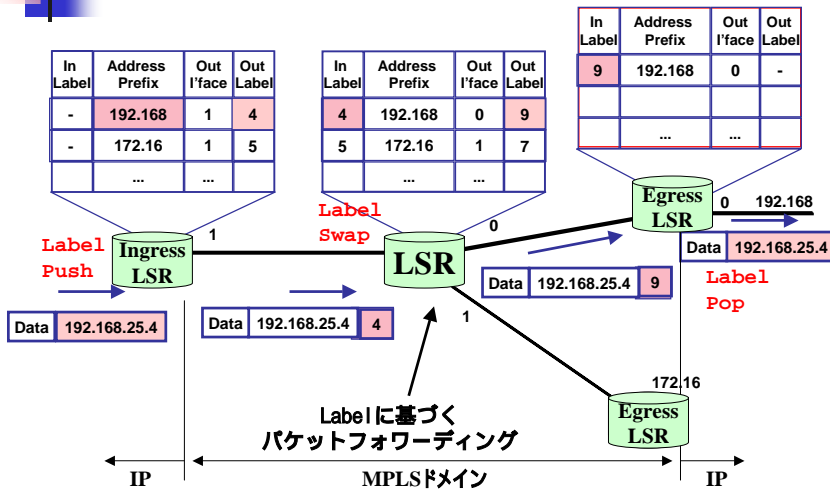
2006/12/07

Internet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>

MPLSの packets 転送

MPLSにおける転送方式

ラベルスイッチング::Push, Swap, Pop

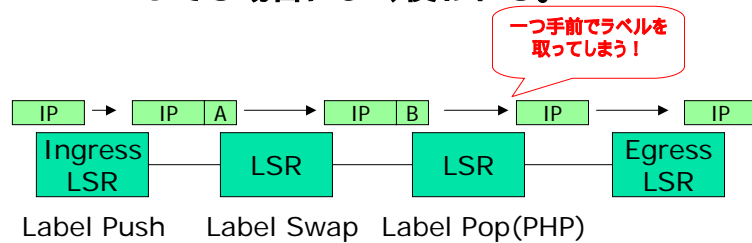


2006/12/07

Internet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>

MPLS のパケット転送

- **PHP(Penultimate Hop Popping)**
- Egressの一つ手前のルータでラベルを除去。
- Egressでラベルが必要なかったり、ラベルをStackしてる場合によく使われる。



2006/12/07

Internet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>

MPLSのパケット転送

- ◆ **ラベルのスタッキング**
 - ラベルを複数つけてスタッキングすることにより、LSPの**階層化**を可能にする。



2006/12/07

Internet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>

MPLSの packets 転送::まとめ

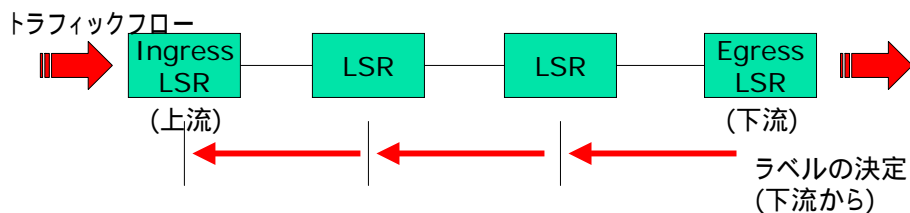
- ラベルの値は個々のLSR内でユニークに決定され、ホップバイホップにラベル値は変わっていく
- ラベルパスは一方向でラベルのみを参照して転送される
(両方向のパスを作るために2本のパスが必要)
- Egressの一つ手前でラベルを取るPHP
- たくさんのラベルをパケットに付けられる
(ラベルスタッキング)

2006/12/07

Internet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>

MPLSのシグナリング

- IngressLSRからEgressLSRまでのラベルパスを決定するためのプロトコル
- ラベルパスの形成には、IPプロトコルを必要とする。
(MPLSは、IPネットワーク上で実現される)
- よく使われるのは、トラフィックフローの下流(宛先)からラベルを順次決定していく方法(DownStream型)



2006/12/07

Internet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>

MPLSのシグナリング

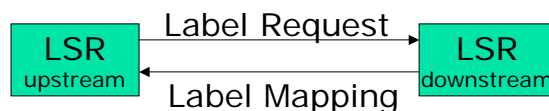
- 経路情報に付加するラベル情報を自動で交換 (トポロジードリブン)
 - LDP (Label Distribution Protocol)
 - BGP-Extension
- 明示的にEnd-to-EndのLSPを張る (コントロールドリブン)
 - RSVP-Extension
- LSPは、これらのシグナリングによって、パケットを運ぶ前にあらかじめ設定される

2006/12/07

Internet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>

MPLSのシグナリング

- 2つの主な考え方
- **Downstream-on-Demand (DoD)**



ラベル要求を受けてからFECに対応したラベルを配布
必要な分だけラベル情報が配布される。

- **Downstream Unsolicited (DU)**

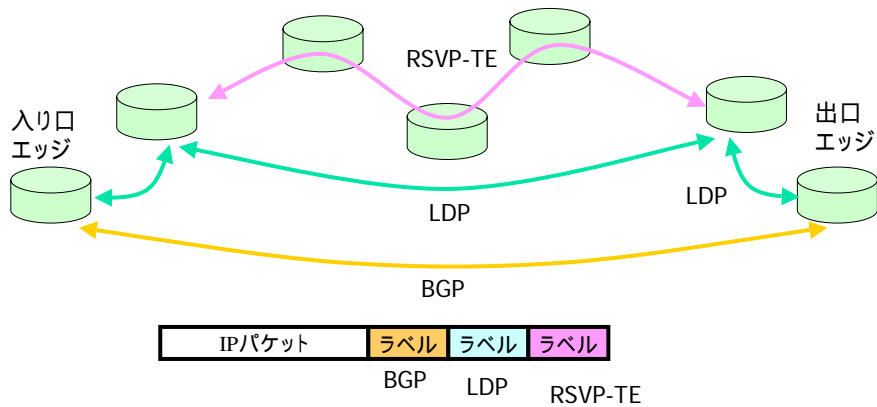


ラベル要求がなくてもFECに対応したラベルを配布
LSPの収束が早い。

2006/12/07

Satoru Matsushima, SOFTBANK TELECOM Corp.>

シグナリングとLSPの関係



2006/12/07

Internet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>

MPLSの基礎 まとめ

- MPLSとは、
 - 特徴、マルチプロトコル。
 - MPLSアーキテクチャ
- パケット転送とシグナリング
 - ラベルスイッチング
 - あらかじめパスを設定するシグナリング

2006/12/07

Internet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>



MPLS Traffic Engineering

2006/12/07

Internet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>



Traffic Engineeringとは何か？

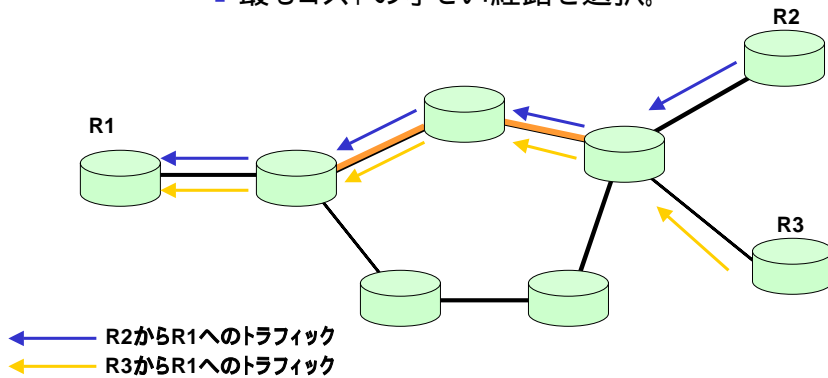
- 広義には...
 - ネットワーク上に流れるトラフィックを効率的に過不足なく処理するために行うネットワーク設計、作業全般。
 - 必要回線容量の見積もり。
 - 回線使用率、トラフィック量の監視。
 - 回線容量の増強、増速作業など。
 - つまりトラフィックの流れから見て、ネットワーク構成を最適化すること。
- 以後、TEと呼びます。

2006/12/07

Internet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>

例題: IPネットワークにおけるTE

- ルータR1へのトラフィックの流れ
 - 最もコストの小さい経路を選択。

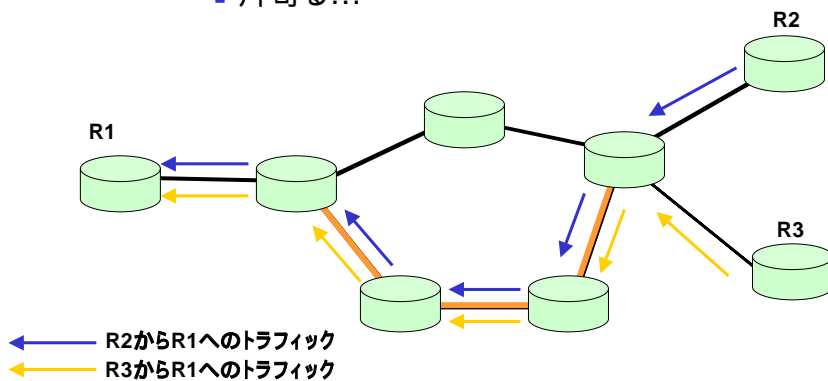


2006/12/07

Internet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>

例題: IPネットワークにおけるTE

- リンクのコスト値を変えてみる。
 - 片寄る...

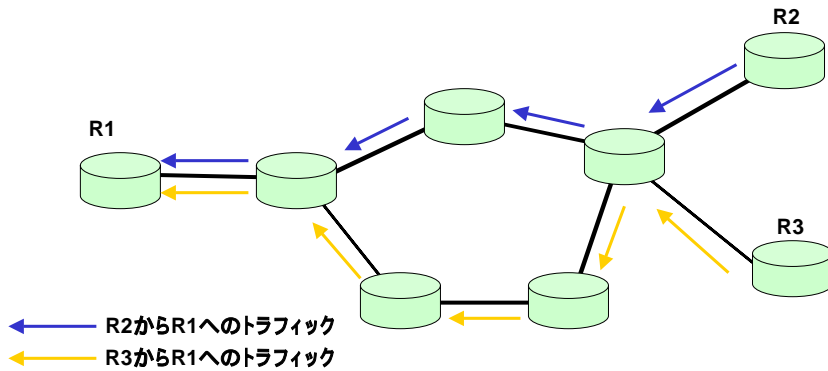


2006/12/07

Internet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>

例題: IPネットワークにおけるTE

- 本当はこうしたかったのに！

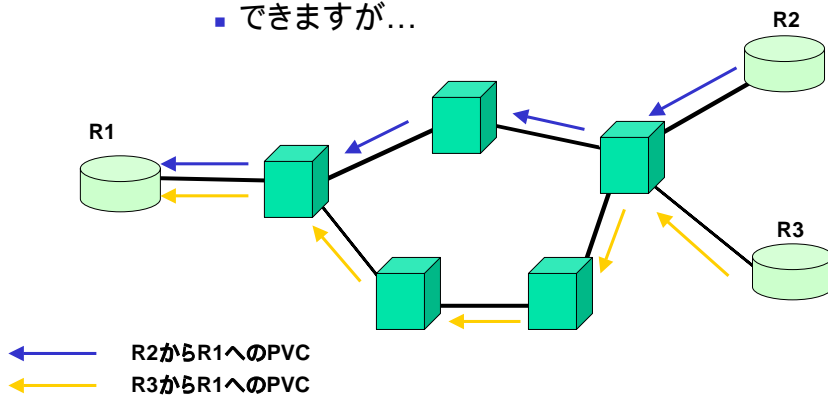


2006/12/07

Internet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>

例題: IPネットワークにおけるTE

- ならばATMやFrame-Relayで...
 - できますが...



2006/12/07

Internet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>

ATM/FRをIPトラフィック制御に 用いた時の問題点

- IPネットワークとは別にATM/FRネットワークを用意することになる。
 - ルータ以外のネットワークデバイス。
 - それぞれにおいて運用 / 監視が必要。
高コスト
- IGPへの負荷が高くなる。
 - メッシュによるAdjacency増。
 - 複雑な論理トポロジー。
- 帯域を圧迫するオーバーヘッド
 - ATM Cell Tax.

2006/12/07

Internet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>

IPネットワークにおけるトラフィック 制御の問題点

- リンクのコストやメトリックによるIGPルーティングはトラフィックの流れから見ると、最適ではない。
 - 利用率が非常に高い回線と低い回線が存在。
 - ネットワーク資源を有効活用できず、しかも高利用率回線の増強を常に余儀なくされる。
高コスト!
 - 利用率(トラフィック量)の高い回線が障害になった時のリスクは非常に大きい。
 - 通常そのような回線は高速 / 超高速回線。
 - そのような回線が切れたときのバックアップ容量が十分であることを保証するのは困難。
信頼性、可用性に欠けたネットワーク。

2006/12/07

Internet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>

IPネットワークにおけるトラフィック制御の問題点

- トラフィックの最適化が非常に困難。
 - IGPにトラフィックを最適化する経路変更は行えない。
 - トラフィックフローに対して直接オペレータが介入する手段はほぼ皆無。

明示的にトラフィックの流れを最適化できる
新たなTE手法が必要

MPLSによるTraffic Engineering !

2006/12/07

Internet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>

MPLS-TEのメカニズム

- RSVPによるExplicit (明示的) Routing
- Constraint-based (強制的な)パス選択
 - IGPコストによらず、空いている / 要求条件にマッチパスを検索し、選択する。
 - CSPF(Constrained SPF) or Operatorによる設定。
- IGP(IS-ISやOSPF)を拡張して、ネットワーク資源(リンクの帯域予約情報)やポリシーを運ぶ。
 - 空いている / 要求条件にマッチするパスを選択するために使われる。
- MPLSによるパケットフォワーディング
 - IPアドレスによらないフォワーディングにより、Explicit Routingを実現。

2006/12/07

Internet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>

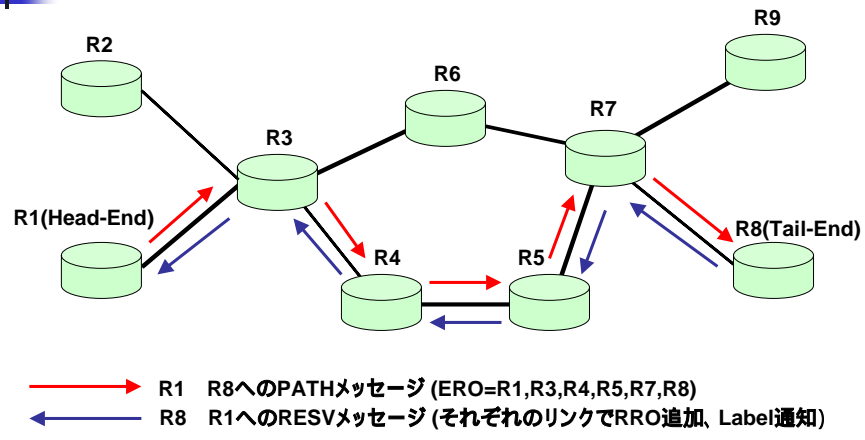
MPLS-TEのためのRSVP

- Pathメッセージ
 - Explicit Route Object (ERO)
 - TEパスを設定するリンクを明示的に連ねる。
 - Label Request Object
 - ラベル割り当て要求
 - Session Attribute Object
 - パスのSetup, Holdプライオリティ,
 - Local repairや予約スタイル(SE)などの要求
- Resvメッセージ
 - Record Route Object (RRO)
 - RSVPメッセージが通過したリンクを記録。(PATHにも)
 - Label Object
 - ラベル割り当て通知

2006/12/07

Internet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>

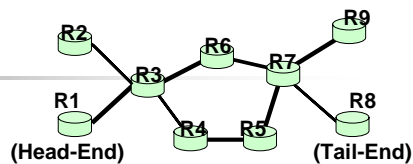
概要:MPLS-TE-LSPセットアップ



2006/12/07

Internet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>

MPLS-TEの基本的な設定(1)



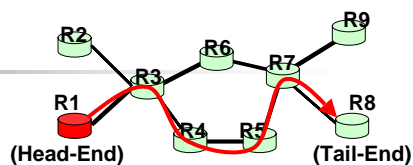
R1からR9まで共通の設定

```
!  
mpls traffic-eng tunnels  
!  
interface POS*/**  
  mpls traffic-eng tunnel  
  mpls traffic-eng administrative-weight 1  
  ip rsvp bandwidth 300  
!  
router ospf 9592  
  mpls traffic-eng router-id Loopback0  
  mpls traffic-eng area 0  
!  
end
```

2006/12/07

Internet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>

MPLS-TEの基本的な設定(2)



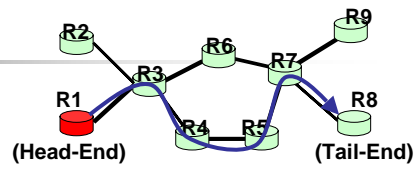
R1(Head-End)からR8(Tail-End)へLSPを設定

```
!  
interface Tunnel 1000  
  description R1->R8  
  ip unnumbered loopback0  
  tunnel destination {R8Router-ID}  
  tunnel mode mpls traffic-eng  
  tunnel mpls traffic-eng path-option 10 explicit t1000  
  tunnel mpls traffic-eng record-route  
!  
ip explicit-path name t1000  
  next-address {R3Router-ID}  
  next-address {R4Router-ID}  
  next-address {R5Router-ID}  
  next-address {R7Router-ID}  
  next-address {R8Router-ID}  
!  
end
```

2006/12/07

Internet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>

MPLS-TEの基本的な設定(3)



R1に設定したLSPにトラフィックを流す

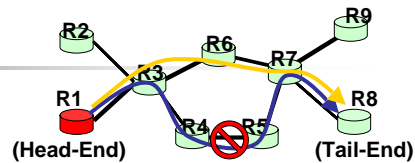
```

!
interface Tunnel 1000
description R1->R8
ip unnumbered loopback0
tunnel destination {R8のRouter-ID}
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng path-option 10 explicit t1000
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng record-route
!
ip explicit-path name t1000
next-address {R3のRouter-ID}
next-address {R4のRouter-ID}
next-address {R5のRouter-ID}
next-address {R7のRouter-ID}
next-address {R8のRouter-ID}
!
end
    
```

2006/12/07

Internet Week 2006 - Satoru Matsushima, SOFTBANK TELECOM Corp. >

MPLS-TEの基本的な設定(4)



LSPを自動的に迂回させるようにしておく

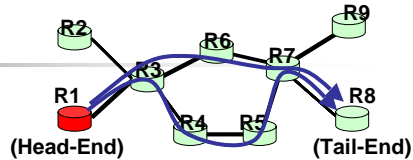
```

!
interface Tunnel 1000
description R1->R8
ip unnumbered loopback0
tunnel destination {R8のRouter-ID}
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng path-option 10 explicit t1000
tunnel mpls traffic-eng path-option 99 dynamic
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng record-route
!
ip explicit-path name t1000
next-address {R3のRouter-ID}
next-address {R4のRouter-ID}
next-address {R5のRouter-ID}
next-address {R7のRouter-ID}
next-address {R8のRouter-ID}
!
end
    
```

2006/12/07

Internet Week 2006 - Satoru Matsushima, SOFTBANK TELECOM Corp. >

MPLS-TEの高度利用(1)



LSPを異なる経路で複数設定し、任意の割合でロードバランスさせる(例: 2:3)

```

!
interface Tunnel 1000
description R1->R8
ip unnumbered loopback0
tunnel destination {R8のRouter-ID}
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng path-option 10
tunnel mpls traffic-eng load-share 2
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng record-route
!
ip explicit-path name t1000
next-address {R3のRouter-ID}
next-address {R4のRouter-ID}
next-address {R5のRouter-ID}
next-address {R7のRouter-ID}
next-address {R8のRouter-ID}
!
end
    
```

```

!
interface Tunnel 1001
description R1->R8
ip unnumbered loopback0
tunnel destination {R8のRouter-ID}
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng path-option 10 explicit t1001
tunnel mpls traffic-eng load-share 3
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng record-route
!
ip explicit-path name t1001
next-address {R3のRouter-ID}
next-address {R6のRouter-ID}
next-address {R7のRouter-ID}
next-address {R8のRouter-ID}
!
end
    
```

2006/12/07

Internet Week2006

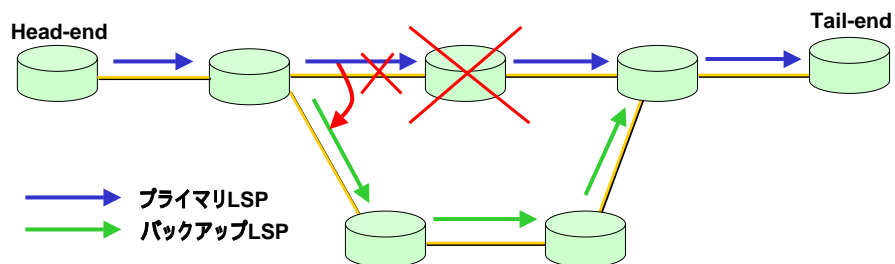
end

MPLS-TEの高度利用(2)



Fast-Reroute

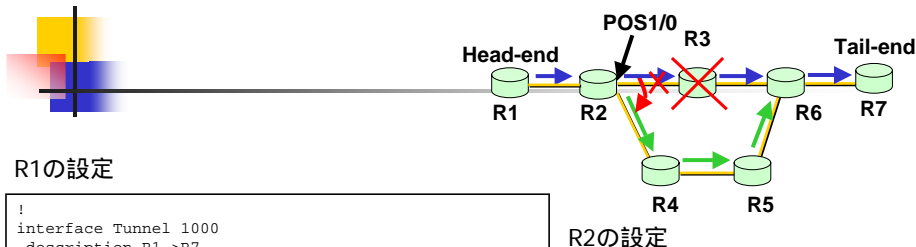
- 障害となったリンクまたはノードに隣接し、トラフィックの上流となっているノードによってLSPが高速迂回される。(数msec~数10msec)
- プライマリLSPのためのバックアップLSPが事前に設定される。



2006/12/07

Internet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>

Fast-Reroute の設定



R1の設定

```
!
interface Tunnel 1000
description R1->R7
ip unnumbered loopback0
tunnel destination {R7のRouter-ID}
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng path-option 10
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng record-route
tunnel mpls traffic-eng fast-reroute
!
ip explicit-path name t1000
next-address {R2のRouter-ID}
next-address {R3のRouter-ID}
next-address {R6のRouter-ID}
next-address {R7のRouter-ID}
!
end
```

R2の設定

```
!
interface Tunnel 2000
description R2->R6
ip unnumbered loopback0
tunnel destination {R6のRouter-ID}
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng path-option 10 explicit t2000
tunnel mpls traffic-eng record-route
!
ip explicit-path name t2000
next-address {R4のRouter-ID}
next-address {R5のRouter-ID}
next-address {R6のRouter-ID}
!
interface POS1/0
mpls traffic-eng backup-path Tunnel2000
!
end
```

2006/12/07

Internet Week2006

MPLS-TE:まとめ

- TEとは、トラフィックの流れから見てネットワーク構成を最適化すること。
- MPLS-TEでは以下によりTEを実現。
 - IGP(IS-IS/OSPF)拡張などによる強制的パス選択
 - RSVPによる明示的パス設定
 - MPLSによるパケットフォワーディング
- Fast-Rerouteや明示的なロードバランスなど新たなメリットを生み出す

2006/12/07

Internet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>



L3VPN (BGP/MPLS VPN)

2006/12/07

Internet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>



BGP/MPLS VPNとは

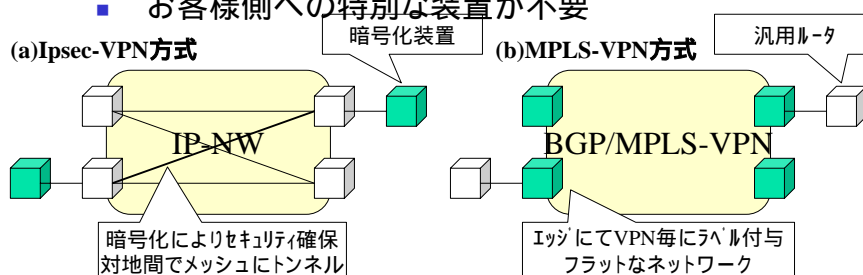
- MPLSの技術を利用してIP-VPNを実現する技術
- インターネットVPN技術 = オープンなネットワーク上で、IPデータ部を暗号化で実現(IP-Secなど)
- MPLS-VPN = MPLS(ラベルによるカプセリング)により、論理的なクローズドなネットワークを実現(IP-VPN)
- 昨今のMPLSを使った他のIP-VPN技術と区別してBGP/MPLS VPNと呼ばれる。

2006/12/07

Internet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>

BGP/MPLS VPNとは

- ルータによる、多様なIFによる提供が可能(ATM～HSDなどの非対称構成も可能)
- 暗号に頼らないセキュリティの確保が可能(FRなどと同等の機能をIPネットワークで実現)
- お客様側への特別な装置が不要



2006/12/07

Internet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>

BGP/MPLS VPNとは

- RFC2547bisに記されたISPサービスとしてのIP-VPN実現技術
- 網内パケット転送にMPLS(LDP/RSVP)、VPN経路情報交換にBGP(mpBGP:RFC2858,RFC3107)を使用
- ルーティングプロトコルがエッジで終端されるPeerモデルのLayer3 IP-VPN
- VPNごとに異なるルーティングテーブルを持ちユーザルータとルーティング情報を交換する。
- Layer3ルーティングのISPへのアウトソーシング

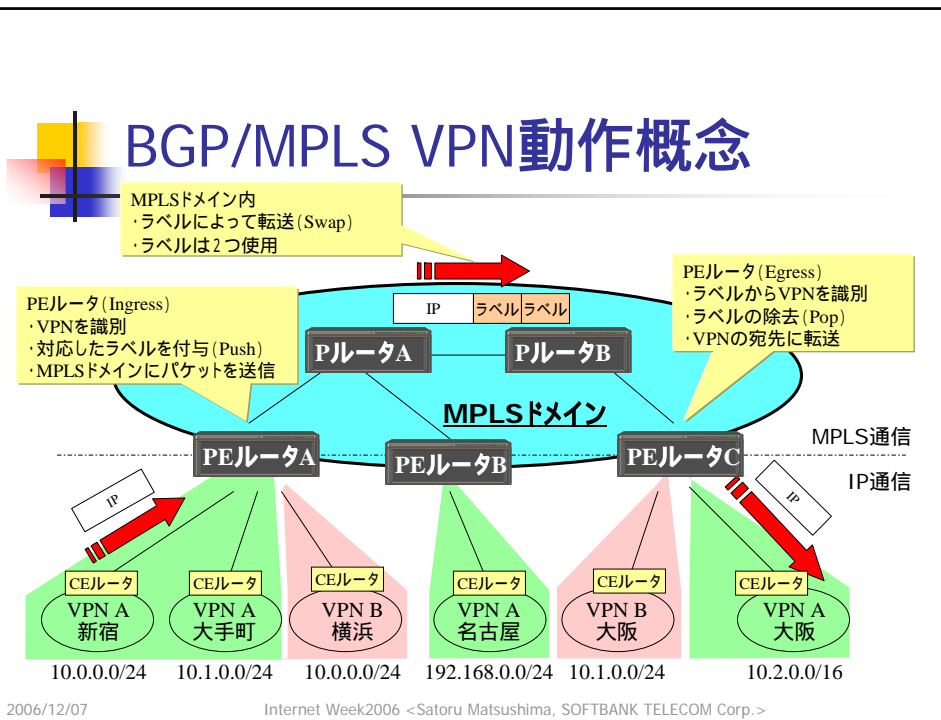
2006/12/07

Internet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>

BGP/MPLS VPNの動作概要

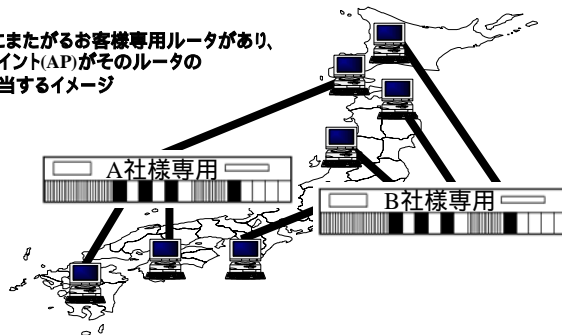
2006/12/07

Internet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>



BGP/MPLS VPN動作概念

日本全国にまたがるお客様専用ルータがあり、
アクセスポイント(AP)がそのルータの
ポートに相当するイメージ



- バックボーンを共用するがVPNは論理的に独立しており、
お客様専用ルータを提供するイメージとなる。

2006/12/07

Internet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>

特徴(ユーザ側)

- お客様宅に設置されるルータは通常のルータで
良い(MPLSやIP-Sec等の機能はいらぬ)
- FRやATM等のようなパスの管理が必要ない
- IPアドレスはお客様にて任意に設定可能であり
IPv4プライベートアドレスを自由に持ちこめる。
- VPN同士の通信は、ルータ内及び網内にて完全
に分離されておりFR、ATMと同等のセキュリティ
が保たれている。

2006/12/07

Internet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>

特徴 (ISP側)

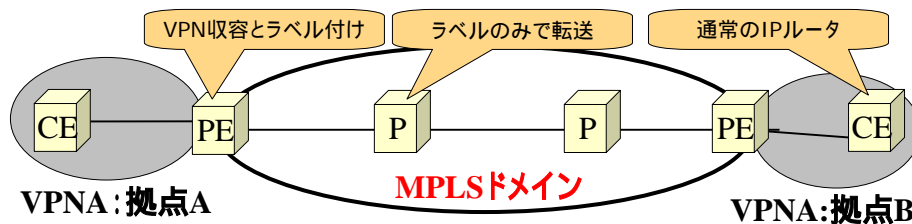
- 既存のルータによるIPネットワークをそのまま使ってIP-VPNサービスを提供できる。
- 複数のルーティングプロトコルを使ってお客様を収容できるので柔軟なサービスが提供できる。
- 複数のVPNを1台のルータに収容できるため効率の良いIP-VPNサービスを提供できる。
- 異なるVPN間で同じアドレスが使えるためサービス性が良い
- 論理的に分離されたネットワークなのでQoSなどのサービスも実現しやすい。

2006/12/07

Internet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>

BGP/MPLS VPN構成ルータ

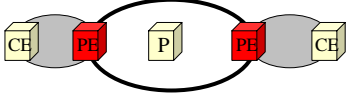
- PEルータ: Provider Edge Router (お客様を収容するルータ、MPLSエッジルータ)
- Pルータ: Provider Router (MPLSコアルータ)
- CEルータ: Customer Edge Router (PEルータにつながるお客様ルータ)



2006/12/07

Internet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>

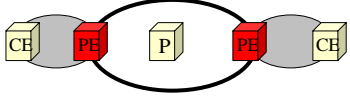
PEルータのしくみ



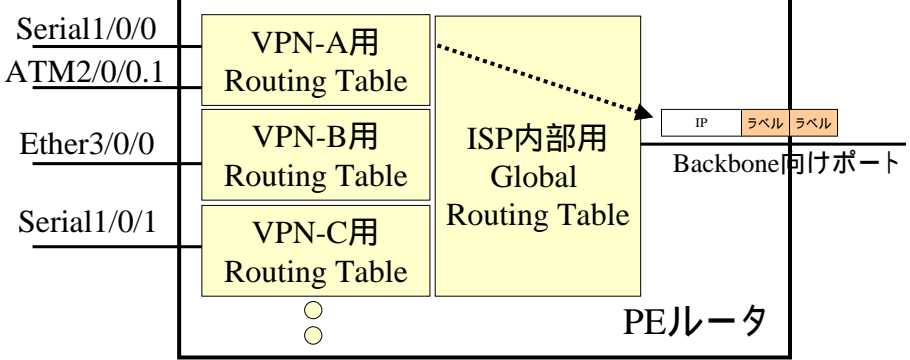
- 複数のVPNを1台のPEルータに収容するために
 - VRFs:VPN Routing and Forwarding tables
 - VPNごとに異なるルーティングテーブルを持つ
 - 各々CEルータを接続するインタフェースを該当するVRF(VPN)に括りつける
 - VRF同士はルータ内部で分離されており、またバックボーンには、ラベルでカプセルリングしてパケットを送出するので、ATM/FRと同等レベルのセキュリティが確保できる。

2006/12/07 Internet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>

PEルータのしくみ



- VPNごとにルーティングテーブルを保持する。
- 一部の実装では、VR(Virtual Router)の場合も



Serial1/0/0
ATM2/0/0.1
Ether3/0/0
Serial1/0/1

VPN-A用 Routing Table
VPN-B用 Routing Table
VPN-C用 Routing Table

ISP内部用 Global Routing Table

IP ラベル ラベル

Backbone向けポート

PEルータ

2006/12/07 Internet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>

BGP/MPLS-VPN のパケット転送

2006/12/07

Internet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>

BGP/MPLS VPN のパケット転送 - MPLS Label -

レイヤ2 ヘッダ	網内転送 ラベル	VPN識別 ラベル	IPヘッダ + データ
-------------	-------------	--------------	-------------

PEルータで付与され、出口のPEルータを目指してPルータをホップするたびにラベルの値は変わっていく
(LDPでhop by hopに決定)

PEルータで付与され、出口のPEルータに到着するまでは、コアネットワーク内では参照されず値も変わらない。
(mp-BGPでPEルータ同士で情報交換)

- MPLSラベルをスタックして2つ使う
- 32bit固定長ラベル×2

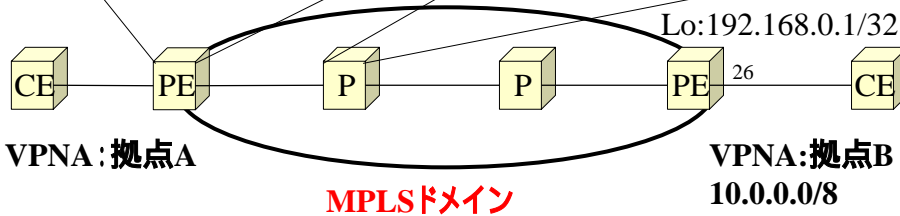
2006/12/07

Internet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>

BGP/MPLS VPN のパケット転送 - 転送テーブル -

VPN名	Route Dist.	あて先アドレス	VPN識別ラベル	出口のPEルータのアドレス	転送用ラベル
A社	12	10.0.0.0/8	26	192.168.0.1/32	42
A社	12	11.0.0.0/8	989	192.168.0.1/32	42

in転送用ラベル	出口のPEルータのアドレス	out転送用ラベル
42	192.168.0.1/32	32



2006/12/07

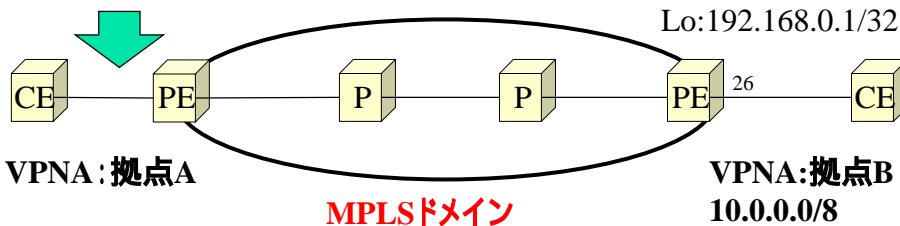
Internet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>

BGP/MPLS VPN のパケット転送

- パケット転送(CEルータからのパケット到着)

VPNA; 拠点B: 10.0.0.1行きパケット到着

Dst:10.0.0.1 →



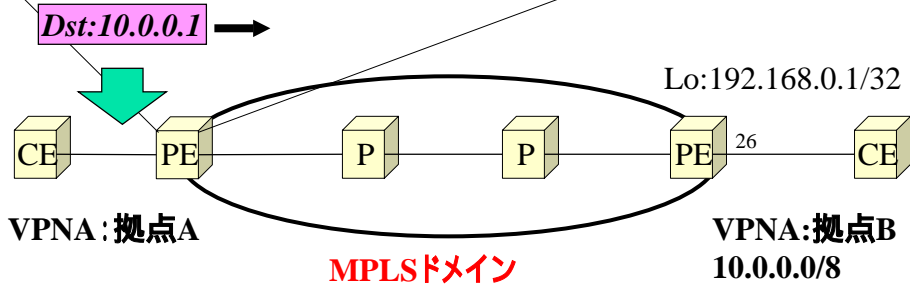
2006/12/07

Internet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>

BGP/MPLS VPN のパケット転送

PEルータでのラベルテーブル検索

VPN名	Route Dist.	あて先アドレス	VPN識別ラベル	出口のPEルータのアドレス	転送用ラベル
A社	12	10.0.0.0/8	26	192.168.0.1/32	42
A社	12	11.0.0.0/8	989	192.168.0.1/32	42



2006/12/07

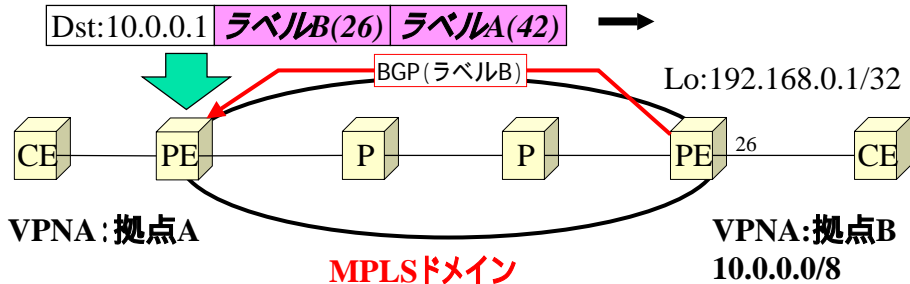
Internet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>

BGP/MPLS VPN のパケット転送

PEルータでのパケットへのラベル付与

出口のPEルータより得たVPN A: 10.0.0.0/8に相当するVPN識別用ラベルBを付与する。

- (1) VPN A: 10.0.0.0/8の出口のPEルータをBGP next-hopで知る。
- (2) 該当するBGP next-hopに対応した転送用ラベルAを付与する。

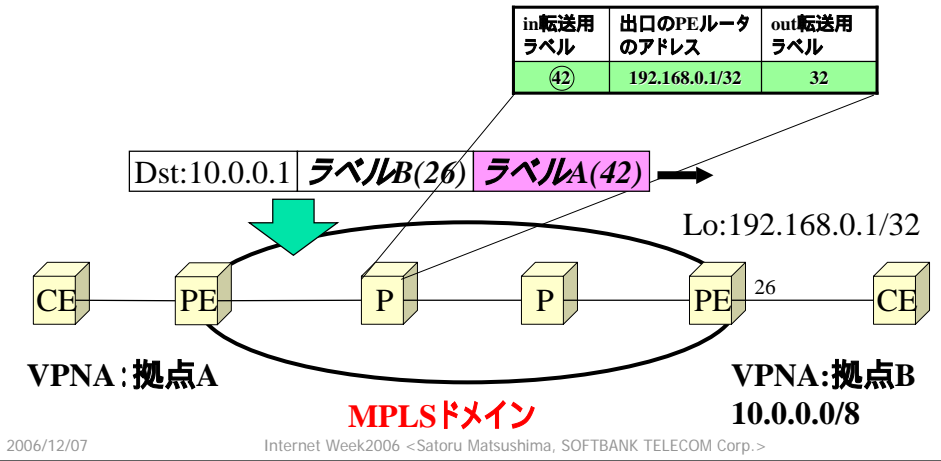


2006/12/07

Internet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>

BGP/MPLS VPN のパケット転送

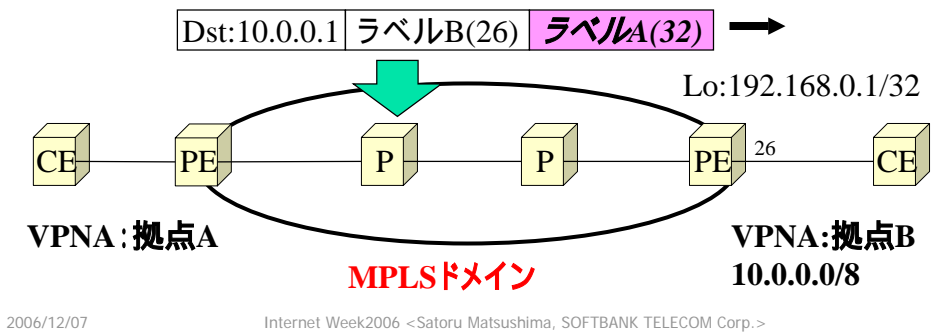
■ Pルータでのラベルテーブルルックアップ



BGP/MPLS VPN のパケット転送

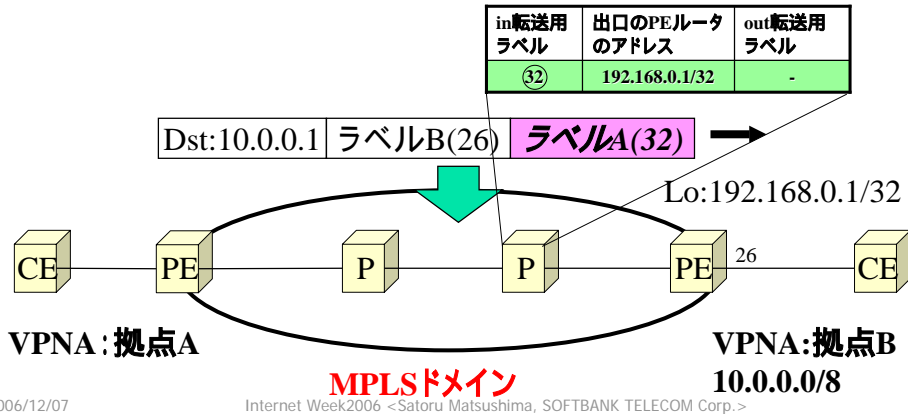
■ Pルータでのラベルスワップ

バックボーン内のPルータでは、転送用ラベルAだけを参照値はホップバイホップで変わります。



BGP/MPLS VPN のパケット転送

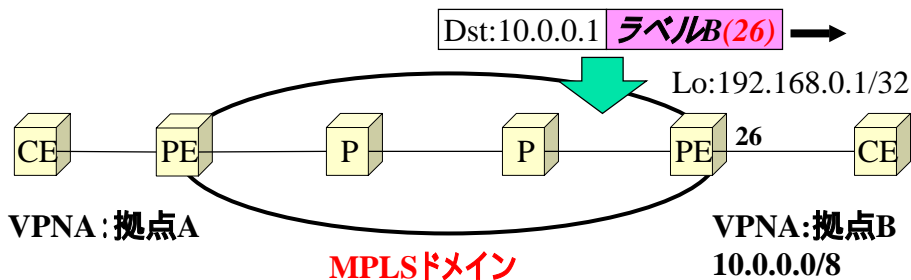
- 最後のPルータでは転送用のラベルを取ります (PHP:Penultimate Hop Popping)



BGP/MPLS VPN のパケット転送

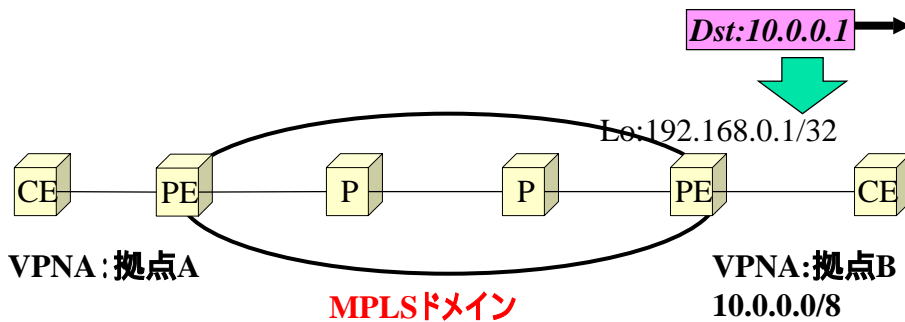
- 最終PEルータでのラベルテーブルのルックアップ

出口のPEルータでは、ラベルBの値を頼りにVPNを識別 & 出力インタフェースを決定しCEルータへパケットを転送



BGP/MPLS VPN のパケット転送

- 目的のCEルータへ到着
ラベルがはずされ通常のIPパケットとして
CEルータに到着する



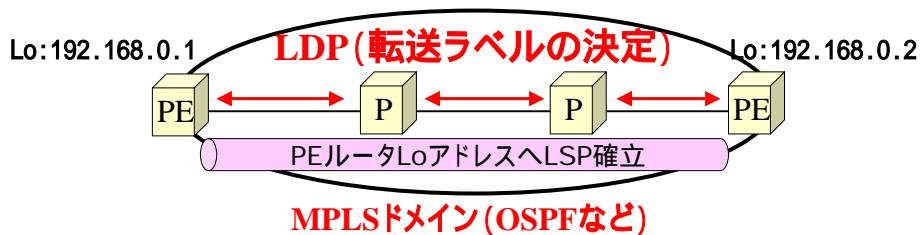
2006/12/07

Internet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>

BGP/MPLS VPN のLSP設定

- PE-PE間 -

- PEルータ・Pルータ間でOSPFにて経路のやり取りをし、その経路情報にラベル情報を対応(LDP)
- 特にPEルータのLoopbackアドレスが最終的にVPNの出口を示すので重要



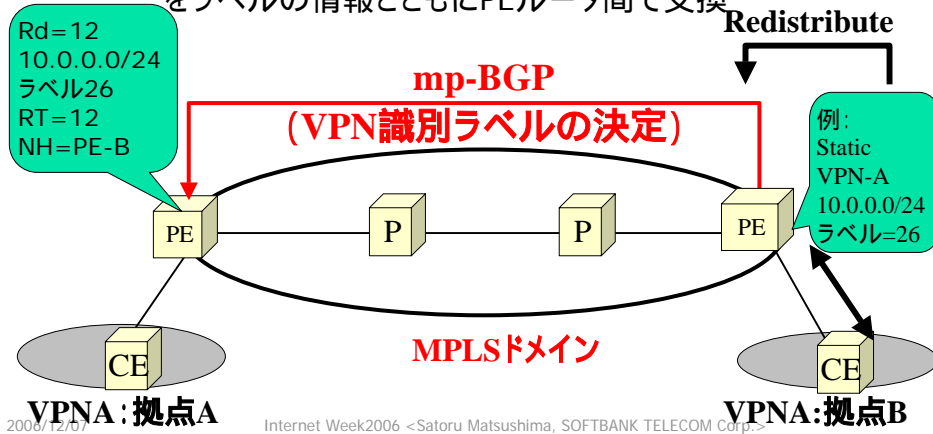
2006/12/07

Internet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>

BGP/MPLS VPNのLSP設定

- VPNラベルの配布 -

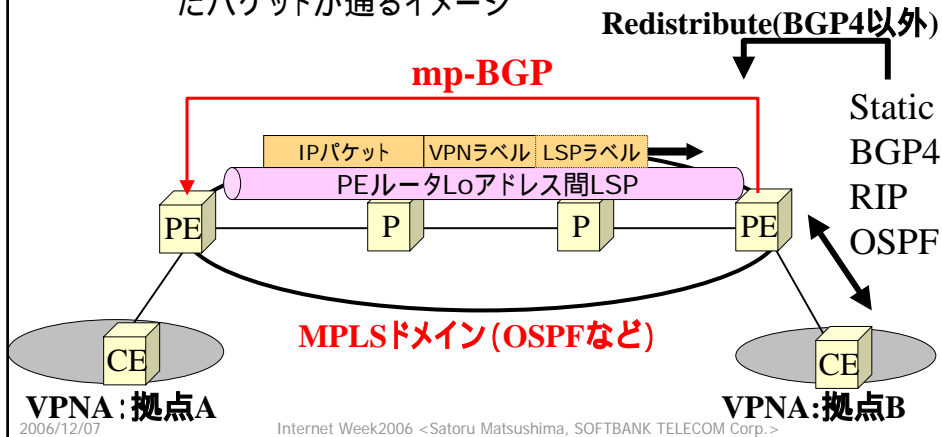
- PE-CE間のルーティングプロトコルで得たVPN経路情報をラベルの情報とともにPEルータ間で交換



BGP/MPLS VPN のLSP設定

- VPN経路とLSP -

- PEルータ間のLSPをVPN識別用ラベルでカプセル化されたパケットが通るイメージ





BGPにおけるVPN経路情報

2006/12/07

Internet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>



BGPにおけるVPN経路

- VPN間でアドレス空間が重なる可能性を排除する
 - VPNv4アドレス

- 経路情報が、どのVPNに属するかを識別
 - 拡張コミュニティ属性
(Route Target community attribute)

2006/12/07

Internet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>

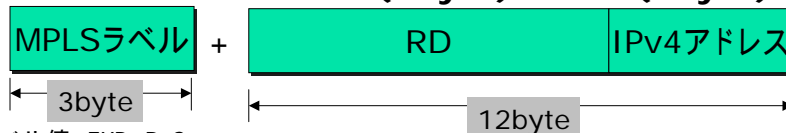
BGPにおけるVPN経路

- VPNv4アドレス -

■ mp-BGPにおける経路扱い

- VPN-IPv4 Address Family
- 通常のIPv4アドレスに8byteの識別子Route Distinguisher (RD)を付与し、12byteのアドレス空間に拡大
- VPN-IPv4 Address(12byte)

$$= \text{RD}(8\text{byte}) + \text{IPv4}(4\text{byte})$$



2006/12/07 ラベル値+EXP+BoS rnet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>

BGPにおけるVPN経路

- VPNv4アドレス -

■ mp-BGPにおける経路扱い

- RD(8byte)のFormat

Type	Value
2byte	6byte

- ISP間の識別も可能なValue Field Format

Type 0 = ASN(2-byte):任意の番号(4-byte)

例 : 9592:1

Type 1 = IP address(4-byte):任意の番号(2-byte)

例 : 192.168.0.1:1

2006/12/07

Internet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>

BGPにおけるVPN経路

- VPNの識別 -

- Route Target (RT)
 - RDはNLRIに付与し、アドレスをユニークに保つ
 - RTはNLRIが、どのVPNの経路かを識別
- VRFよりBGPにアナウンスされる経路には、必ず一つ以上のRTを付与する (Export)
- リモートPEからの経路をローカルVRFに落とし込む際の選択に使用 (Import)

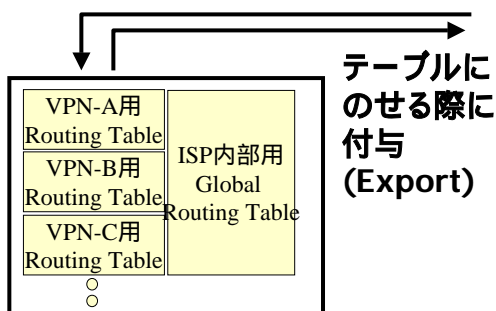
2006/12/07

Internet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>

BGPにおけるVPN経路

- VPNの識別 -

RTをもとにVPNv4-prefixを
どのVPNのRouting Tableに
突っ込むかを選択(Import)



BGPテーブル

```
RD:9592:1(VPN-A)
 10.0.0.0/24 RT:9592:1
 10.0.1.0/24 RT:9592:1
RD:9592:2(VPN-B)
 10.0.0.0/24 RT:9592:2
 10.0.1.0/24 RT:9592:2
RD:9592:3(VPN-C)
 10.0.0.0/8 RT:9592:3
.
.
.
```

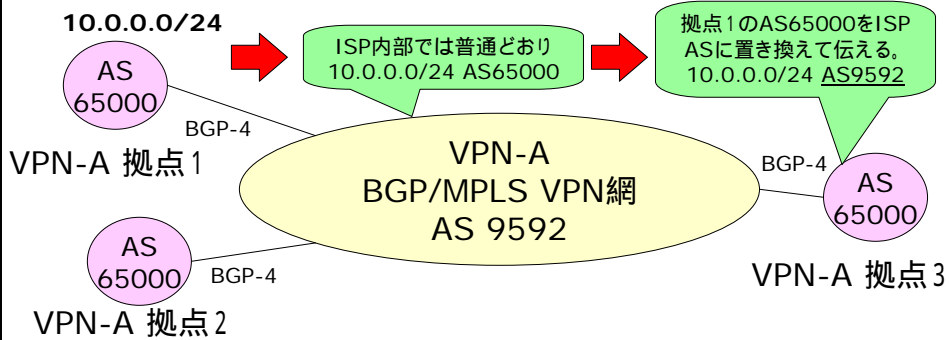
2006/12/07

Internet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>

BGP/MPLS-VPN の経路制御

- AS Override -

- 同一VPN内で複数の拠点で同一のAS番号を用いて PE-CE間を接続するための技術
- ユーザ側でAS番号の管理が不要



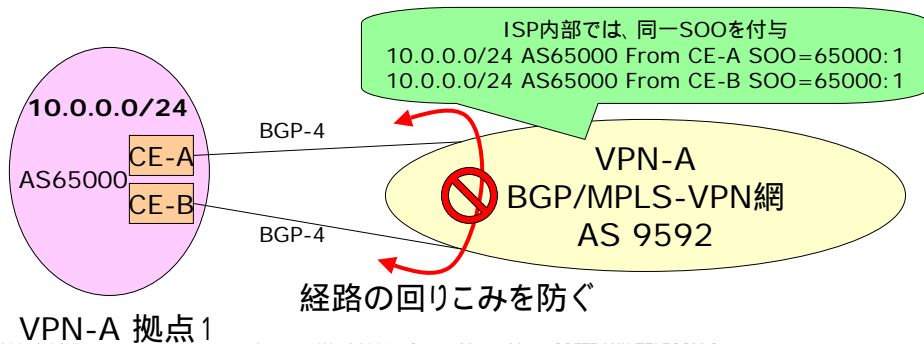
2006/12/07

Internet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>

BGP/MPLS-VPNの経路制御

- SOO (Site Of Origin) -

- AS OverrideするとAS-PATHでループを防げない
- AS-PATHの代わりに同一AS間のループを防ぐもの
- RTと同じExtend Communityの一つ



2006/12/07

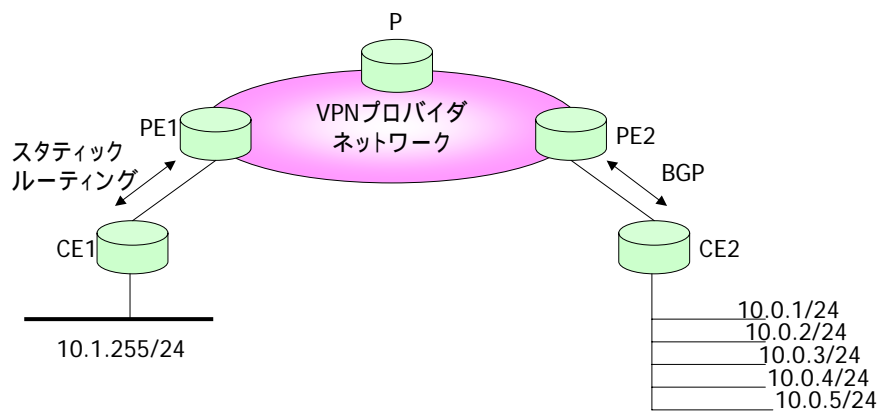
Internet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>

BGP/MPLS-VPN の設定例

2006/12/07

Internet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>

BGP/MPLS-VPN 基本的な設定例

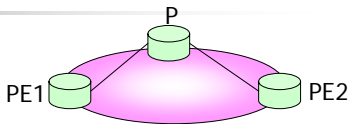


2006/12/07

Internet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>

基本的な設定例

- PE, Pルータ はじめの設定 -



```

PE1の設定
!
interface loopback 0
ip address 1.1.1.1/30
!
interface POS1/0
description PE1<->P
ip address 1.0.0.1/30
mpls ip
!
router bgp 9592
neighbor 1.1.1.2 remote-as 9592
neighbor 1.1.1.2 update-source lo0
!
address-family vpnv4
neighbor 1.1.1.2 activate
neighbor 1.1.1.2 send-community both
!
end
2006/12/07

```

```

Pの設定
!
interface POS1/0
ip address 1.0.0.2/30
mpls ip
!
interface POS2/0
ip address 2.0.0.2/30
mpls ip
!
end
Internet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>

```

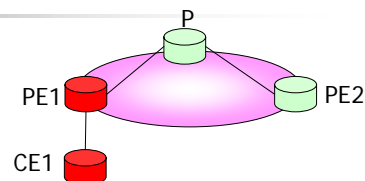
```

PE2の設定
!
interface loopback 0
ip address 1.1.1.2/30
!
interface POS1/0
description PE2<->P
ip address 2.0.0.1/30
mpls ip
!
router bgp 9592
neighbor 1.1.1.1 remote-as 9592
neighbor 1.1.1.1 update-source lo0
!
address-family vpnv4
neighbor 1.1.1.1 activate
neighbor 1.1.1.1 send-community both
!
end
SOFTBANK TELECOM Corp. >

```

基本的な設定例

- VPNの設定 (PE-CE間Static) -



```

PE1の設定
!
ip vrf VPN1
rd 9592:1
route-target export 9592:1
route-target import 9592:1
!
interface fastethernet1/0
description CE1
ip vrf forwarding VPN1
ip address 10.255.255.1/30
!
router bgp 9592
address-family ipv4 vrf VPN1
redistribute static
!
ip route vrf VPN1 10.1.255.24 10.255.255.2
!
end
2006/12/07

```

```

CE1の設定
!
interface fastethernet0/0
description PE1
ip address 10.255.255.2/30
!
interface fastethernet1/0
ip address 10.1.255.1/24
!
ip route 0.0.0.0 0.0.0.0 10.255.255.1
!
end
Internet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>

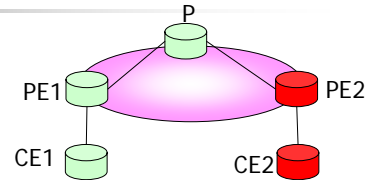
```

基本的な設定例

- VPNの設定 (PE-CE間BGP) -

PE2の設定

```
!
ip vrf VPN1
rd 9592:1
route-target export 9592:1
route-target import 9592:1
!
interface fastethernet1/0
description CE2
ip vrf forwarding VPN1
ip address 10.255.254.1/30
!
router bgp 9592
address-family ipv4 vrf VPN1
neighbor 10.255.254.2 remote-as 65000
neighbor 10.255.254.2 as-override
!
end
```



CE2の設定

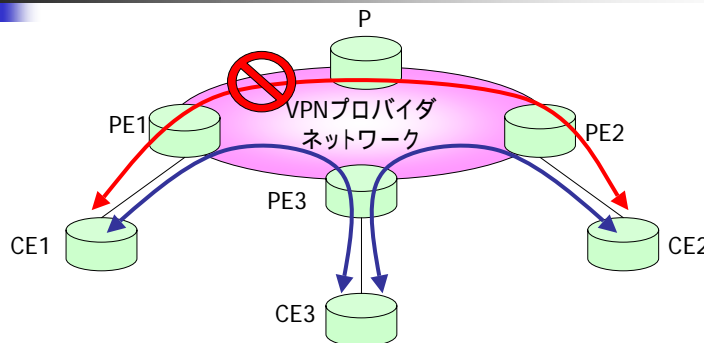
```
!
interface fastethernet0/0
description PE2
ip address 10.255.254.2/30
!
interface ethernet 1/0
ip address 10.0.1.1/24
!
interface ethernet */*
ip address x.x.x.x
!
router bgp 65000
neighbor 10.255.254.1 remote-as 9592
redistribute connected
!
end
```

2006/12/07

Internet Week2006 <Satou Toshima, SOFTBANK TELECOM Corp.>

BGP/MPLS-VPN

応用的な設定例: Hub&Spoke



以下のような条件を満たすVPNを構成する必要があるとき、Hub&Spokeが有効

- ・CE1のVPNサイトと、CE2のVPNサイトは直接通信できない。
- ・CE1のVPNサイトと、CE2のVPNサイトは、CE3のVPNサイトと通信させる。

例: 異なる企業で、システムを安全に共有するためのセキュリティ確保, など。

2006/12/07

Internet Week2006 <Satou Toshima, SOFTBANK TELECOM Corp.>

応用的な設定例 Hub & Spoke VPN

PE3の設定

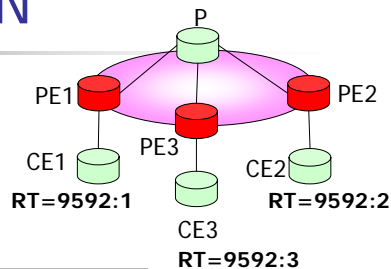
```
!
ip vrf VPN3
rd 9592:1
route-target export 9592:3
route-target import 9592:1
route-target import 9592:2
!
interface fastethernet1/0
description CE3
ip vrf forwarding VPN3
ip address 10.255.253.1/30
!
router bgp 9592
address-family ipv4 vrf VPN3
neighbor 10.255.253.2 remote-as 65000
neighbor 10.255.253.2 as-override
!
end
```

PE1の設定

```
!
ip vrf VPN1
rd 9592:1
route-target export 9592:1
route-target import 9592:3
!
end
```

PE2の設定

```
!
ip vrf VPN2
rd 9592:1
route-target export 9592:2
route-target import 9592:3
!
end
```



2006/12/07

Internet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>

L3VPN(BGP/MPLS) まとめ

- MPLSでVPNを実現するために
 - ラベルによるVPN識別とパケット転送
 - BGPの拡張により、VPN経路情報の識別とラベル情報を配布
 - VRFにより、VPN経路情報を仮想化
- VPN経路情報の制御方法を工夫することでセキュリティ要件に合ったVPNを構築可能
 - Hub & Spoke VPN など

2006/12/07

Internet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>



MPLS技術の今後の展望

2006/12/07

Internet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>



MPLS技術の今後の展望

- パケットネットワークであらゆる形態の通信をサポートする拡張
 - レガシー系インタフェースをエミュレート
 - ATM/FR, TDM, Ethernet, いわゆるL2VPN
 - マルチキャストの転送
 - ポイント・ツー・マルチポイント LSP, マルチキャストVPN
- より高信頼・より最適化をサポートする拡張
 - インタードメインでのトラフィックエンジニアリング
 - VPN上でのトラフィックエンジニアリング
- MPLSは、パケットネットワークでの様々なサービス実現、高信頼化のための基盤技術として期待されている

2006/12/07

Internet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>



Q&A

MPLSとGMPLS
～ サービス提供と、その伝達を支える技術～

第一部:MPLS

2006/12/07

Internet Week2006 <Satoru Matsushima, SOFTBANK TELECOM Corp.>