MPLS-VPN

NTTコミュニケーションズ(株)
池尻雄一
<ikejiri@ntt.ocn.ne.jp>

MPLSの特徴

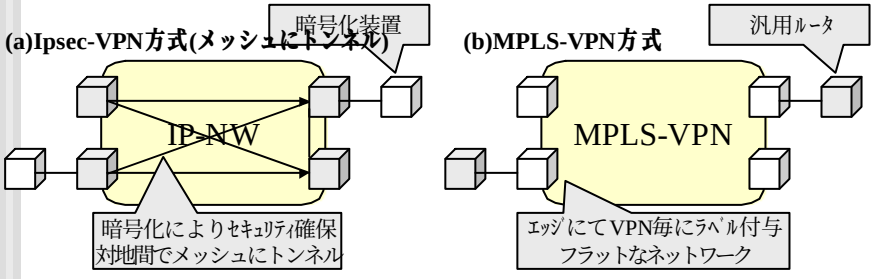
- ラベルパスを使うことによりIPフォワーディングの世界にコネクションの概念を持ち込むことが可能
- **複数のIPアドレスをまとめてひとつのラベルとして表現することができるためフォワーディングテーブルの節約及びカプセル化が可能**
- 最適なラベル値を使い、フォワーディング処理を最適化、高速化可能

MPLS-VPNとは

- MPLSの技術を利用してIP-VPNを実現する技術
- 従来の技術＝ｵｰﾌﾟﾝﾈｯﾄﾜｰｸ上で、IPデータ部を暗号化で実現(IP-Secなど：インターネットVPN)
- MPLS-VPN＝MPLSにより、論理的なｸﾛｰｽﾞﾄﾞﾈｯﾄﾜｰｸを実現(IP-VPN)

MPLS-VPNとは

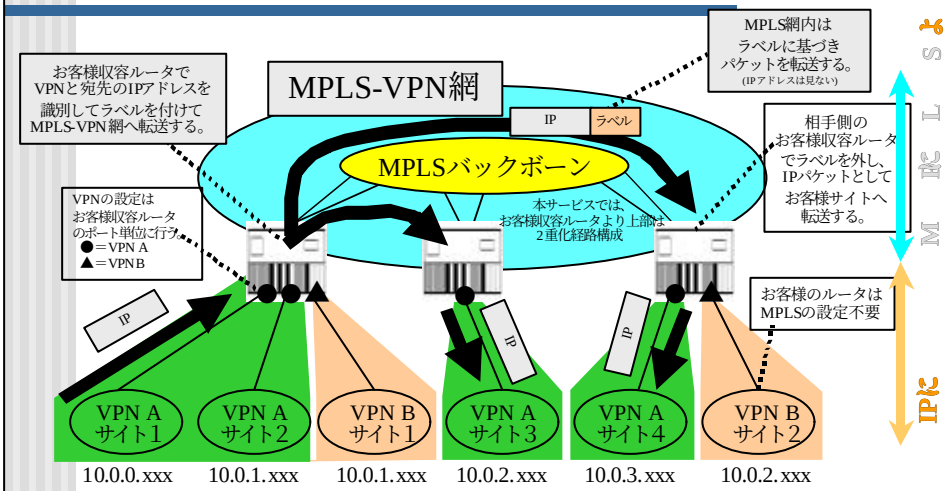
- ルータによる、多様なIFによる提供が可能（ATM～HSDなどの非対称構成も可能）
- 暗号に頼らないセキュリティの確保が可能(FRなどと同等の機能をIPネットワークで実現)
- お客様側への特別な装置が不要



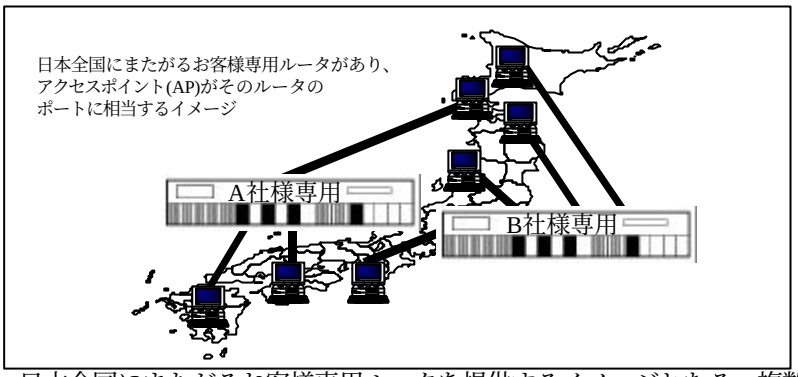
MPLS-VPNとは

- Cisco社を中心としてRFC2547(Informational)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/TDP)、VPN経路情報交換にBGP(mpBGP:RFC2283) 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IP-VPN
- VPNごとに異なるルーティングテーブルを持ちお客様ルータとルーティング情報を交換する。

MPLS-VPN動作概念



MPLS-VPN動作概念



- 日本全国にまたがるお客様専用ルータを提供するイメージとなる。複数のVPNでバックボーンを共用するが、お互いのVPNは論理的に独立している。

MPLS-VPNの特徴(ユーザ側)

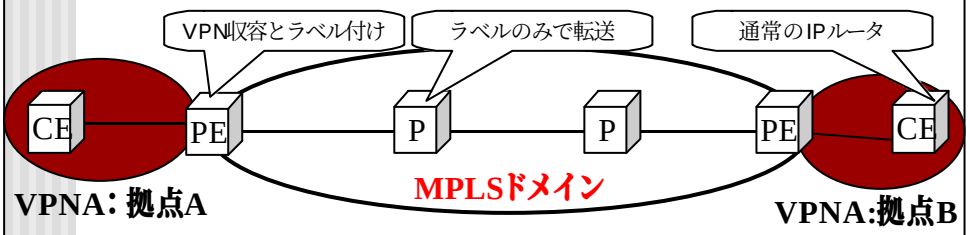
- お客様宅に設置されるルータは通常のルータで良い(MPLSやIP-Sec等の機能はいらない)
- FRやATM等のようなパスの管理が必要ない
- IPアドレスはお客様にて任意に設定可能でありプライベートアドレスを自由に持ちこめる。
- VPN同士の通信は、ルータ内及び網内にて完全に分離されておりFR、ATMと同等のセキュリティが保たれている。

MPLS-VPNの特徴(ISP側)

- IPネットワークの構築で親しんでいるルータ網を使ってIP-VPNサービスを提供できる(Ciscoルータ)。
- 複数のルーティングプロトコルが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
- 閉じたネットワークなのでQoS関係も実現しやすい。

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)

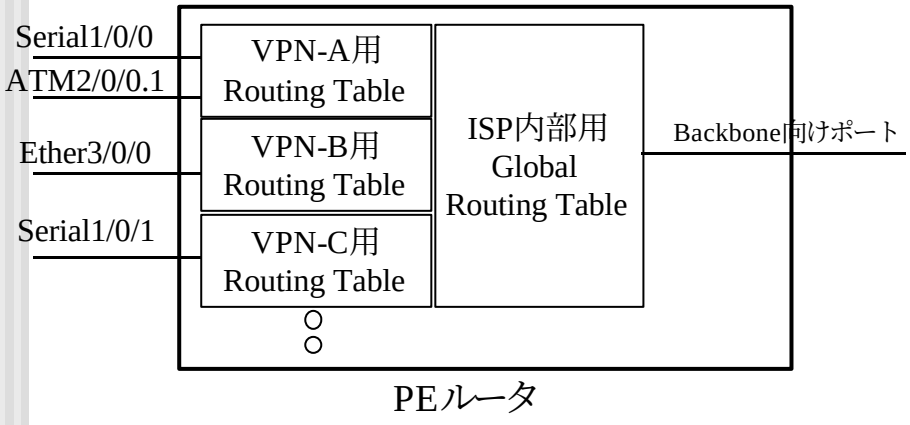


MPLS-VPN PEルータのしくみ

- 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該当するVRF(VPN)に括りつける

MPLS-VPN PEルータのしくみ

- 複数のルーティングテーブルを保持する。



MPLS-VPNラベルフォーマット

- MPLS-VPNラベルフォーマット

PEルータで挿入され、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)

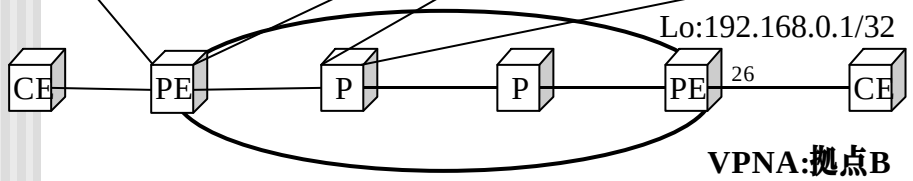
PEルータで挿入され、出口のPEルータに到着するまでは、コアネットワーク内では参照されず値も変わらない。(mpBGPでPEルータ同士で情報交換)

- MPLSラベルスタックを2つ使う
- 各々フォーマットは前述のラベルフォーマット

MPLS-VPN動作概要

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



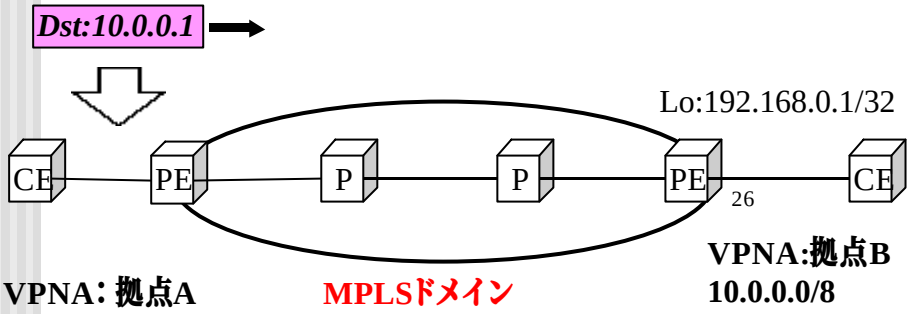
VPNA：拠点A

MPLSドメイン

VPNA:拠点B
10.0.0.0/8

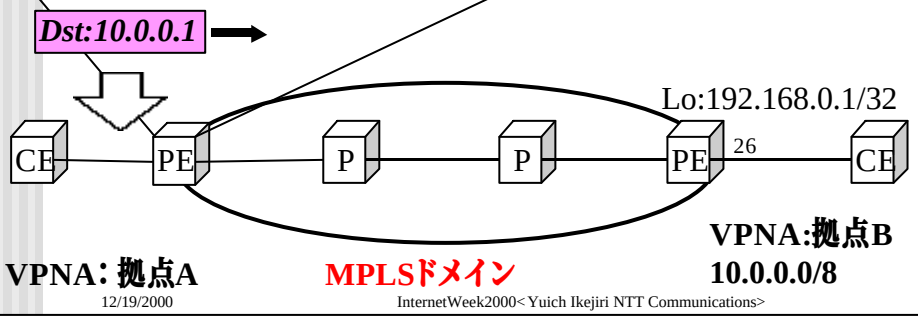
MPLS-VPN動作概要

VPNA；拠点B：10.0.0.1行きパケット到着



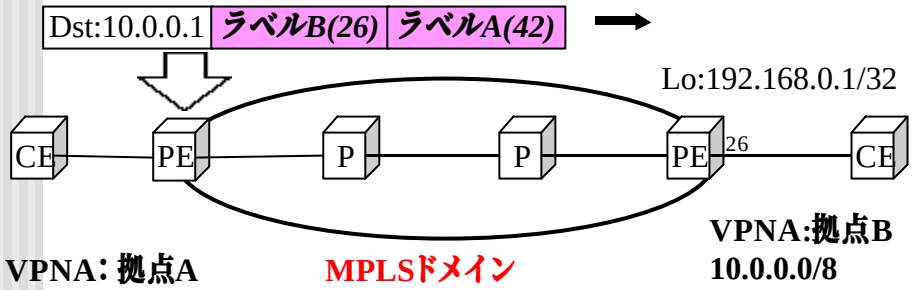
3.4.3 MPLS-VPN動作概要

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

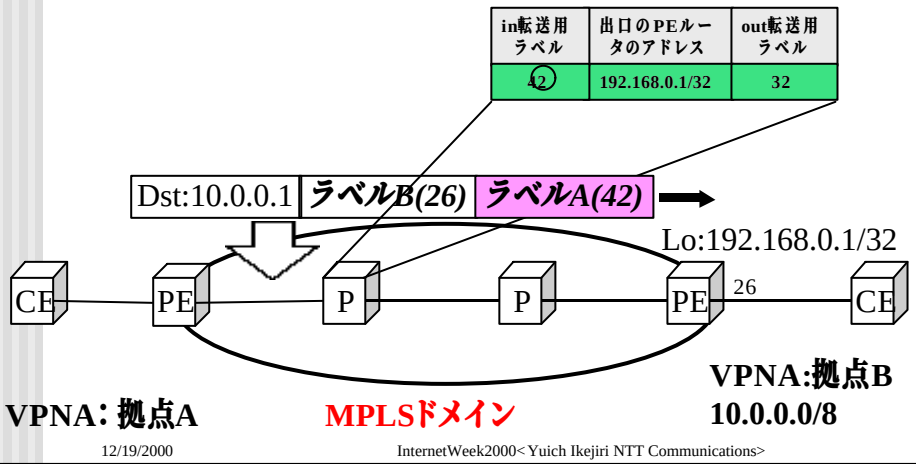


MPLS-VPN動作概要

①(1)VPNA: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。
②出口のPEルータより得たVPNA：10.0.0.0/8に相当するVPN識別用ラベルBを付与する。

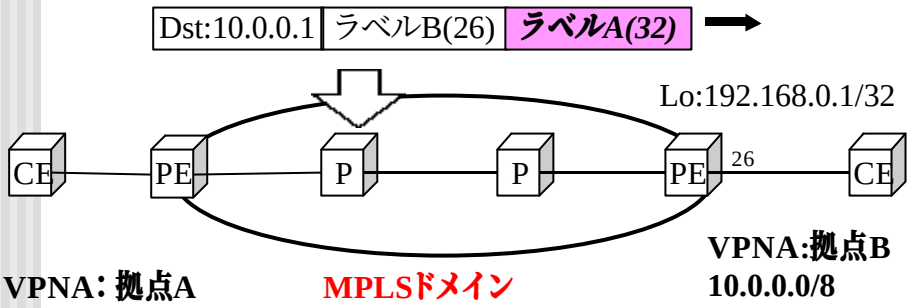


MPLS-VPN動作概要



MPLS-VPN動作概要

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。



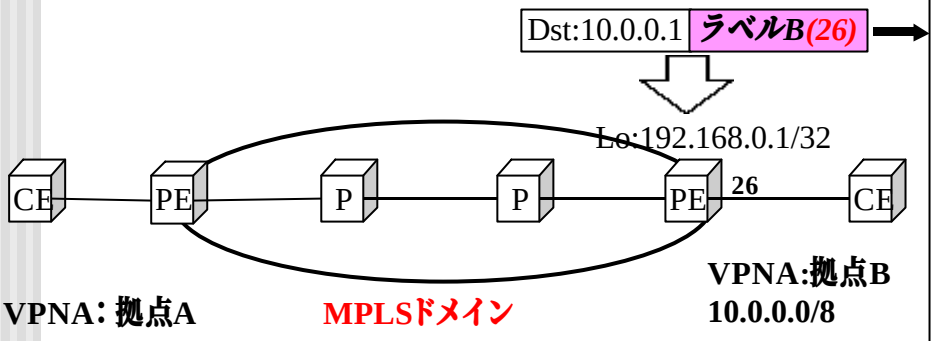
MPLS-VPN動作概要

- 最後のPルータでは転送用のラベルを取ります

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
32	192.168.0.1/32	-

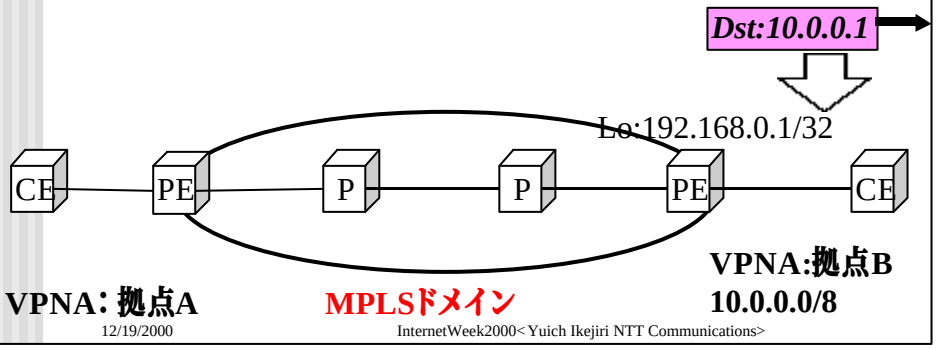
MPLS-VPN動作概要

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

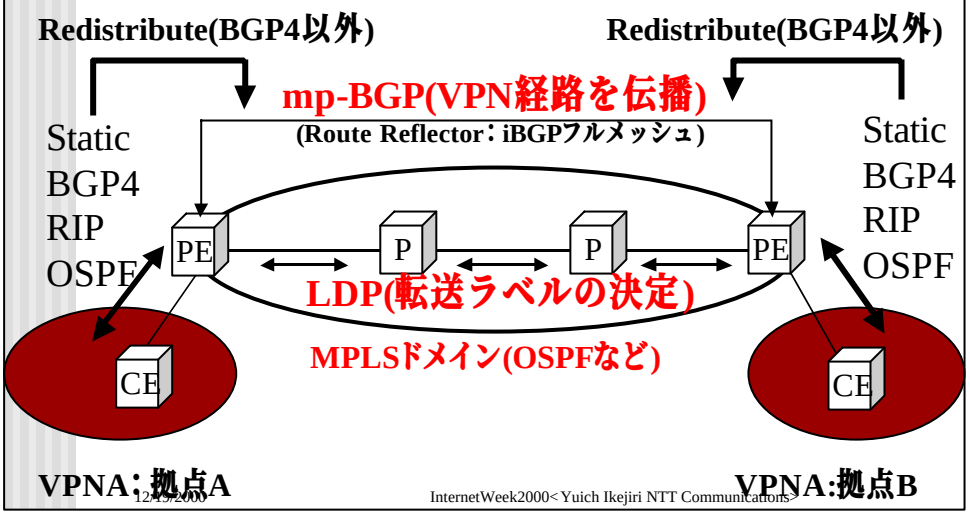


MPLS-VPN動作概要

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

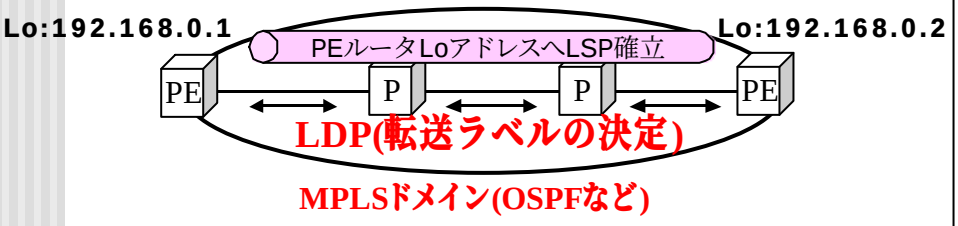


MPLS-VPNプロトコル構成



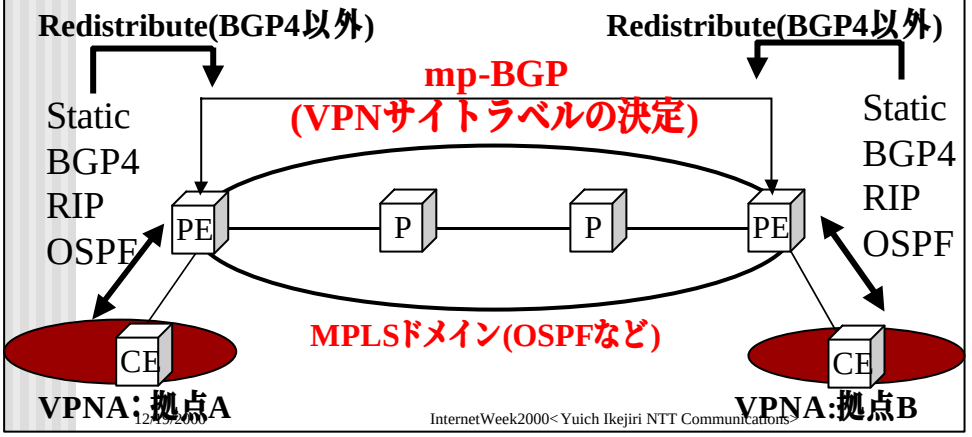
MPLS-VPNラベル決定方法

- 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
- 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



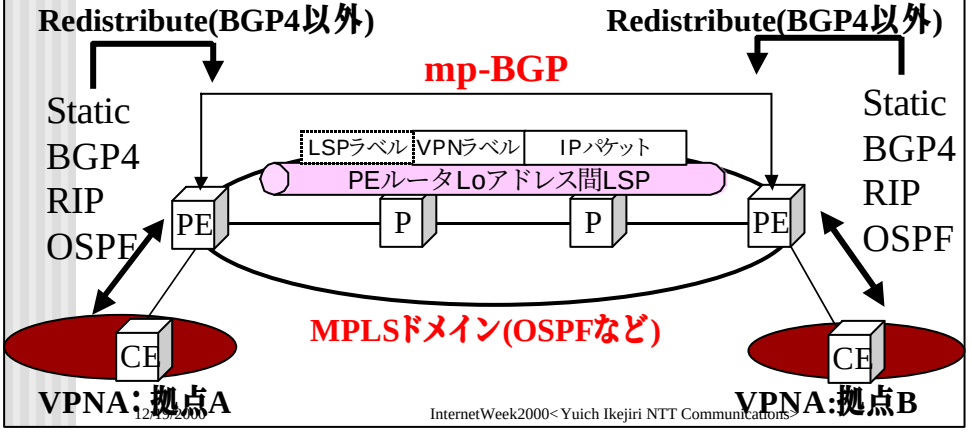
MPLS-VPNラベル決定方法

- 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



MPLS-VPNラベル決定方法

- 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

- IPv6やマルチキャストと同じように RFC2283 Multiprotocol extensions for BGP-4を使用
- MP_REACH_NLRI(Type Code 14)
- MP_UNREACH_NLRI(Type Code 15)
- AFI=1 & SAFI =128
- MPLS-labeled VPN-IPv4 address

BGPにおけるVPN経路

- 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)
    ＝RD(8byte)＋IPv4(4byte)

BGPにおけるVPN経路

- **mp-BGPにおける経路扱い**
  - **RD(8byte)のFormat**

Type 2byte	Value 6byte

  - **ISP間の識別も可能なValue Field Format**

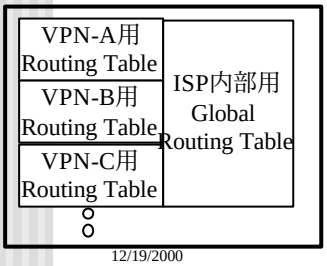
Type 0 = ASN(2-byte):任意の番号(4-byte)
例→9598:1
Type 1 = IP address(4-byte):任意の番号(2-byte)
例：192.168.0.1:1

Extended Community

- Extended Community Attribute(Type Code 16)が新たに定義
- その中の一つがRoute Target(RT)
- VRFには必ず一つ以上のRTが付与される
- Export Targets:CEからの経路の付与
- Import Targets:他PEからの経路選択に使用
- VPN間通信、AS間通信の実現

Extended Community

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



BGPテーブル

RD:9598:1(VPN-A)
10.0.0.0/24 RT:9598:1(Export)
10.0.1.0/24 RT:9598:1(Export)
RD:9598:2(VPN-B)
10.0.0.0/24 RT:9598:2(Export)
10.0.1.0/24 RT:9598:2(Export)
RD:9598:3(VPN-C)
10.0.0.0/8 RT:9598:3(Export)
•
•
•

MPLS-VPN PEルータConfig例

- VPNの定義

```
ip vrf VPN-TEST
 rd 9598:1
 route-target import 9598:1
 route-target export 9598:1
```

- インタフェースのVPNへ括り付け

```
Interface Serial1/0/0
 ip vrf forwarding VPN-TEST
 ip address 10.0.0.1 255.255.255.252
```

MPLS-VPN PEルータConfig例

- mpBGP部分の設定(CEルータStatic)：抜粋

```
router bgp 9598
 no bgp default ipv4-unicast
 neighbor 192.168.0.1 remote-as 9598 →他PEルータ向けPeer
!
 address-family ipv4 vrf VPN-TEST       →VPN用設定
 redistribute static
 no auto-summary
 no synchronization
 exit-address-family
!
 address-family vpnv4                   →route-target情報用
 neighbor 192.168.0.1 send-community extended
!
```


MPLS-VPN PEルータConfig例

- VPN用Static設定

```
ip route vrf VPN-TEST 10.0.0.0 255.0.0.0 Serial1/0/0 10.0.0.2
ip route vrf OTHER-VPN 10.0.0.0 255.0.0.0 Serial1/1/0 10.0.0.2
```

- VPNが異なれば同じアドレスでも設定可

MPLS-VPN技術の実際

- MPLS-VPNの枠組みはわかるが、細かい部分の規定がない(Informational)。
- バックボーンは軽くなったが、エッジルータはVPNをハンドルするため負荷がかかる傾向
- 経路数が莫大に増える可能性
  - 1VPN*1000経路×200VPN=20万経路！
  - リフレクタを分ける、PEルータ収容を分ける、BGP Peer構成を分ける等のスケーラビリティ対応要
- iBGPしか実装がない

MPLS-VPN関連新機能

- MPLS-VPN事業者間接続
  - Inter-mpls-vpn機能を使ったMPLS-VPNのeBGPによる事業者間接続
- Carrier's Carrier機能
  - ISPのバックボーンをMPLS-VPNを使って作る機能
  - 既存のIPネットワークをMPLS-VPNの統一プラットフォーム上に実現できる。
- MPLS-VPNとTraffic Engineeringとの組合せ
  - 特定のVPNに対してTEの機能を適用して、Qos(Diffserve)やFRR等の機能を提供

MPLS標準化動向

- MPLSの標準化の主な動き
- まだいずれも標準化作業途中
  - MPLSの基本動作概念
  - MPLSのラベルフォーマット
  - MPLSのラベル決定のためのプロトコル
  - MPLSを使って特定の経路情報やQoSを持った特定のラベルパスとはるためのシグナリング方式 (Traffic Engineeringなど)
  - MPLSを使ったIP-VPN実現方式

MPLS標準化動向

- MPLSの基本動作概念
  - draft-ietf-mpls-arch-07.txtとしてIETFにて標準化進行中
- MPLSのラベルフォーマット
  - draft-ietf-mpls-label-encaps-08.txtとしてIETFにて標準化進行中

いずれも各社実装などが行われつつある状況

MPLS標準化動向

- MPLSラベル決定のためのプロトコル
  - もともとCisco社独自のTDP(Tag Distribution Protocol)等が存在していた。
  - 現在では、LDP(Label Distribution Protocol)として標準化がほぼ終了している。
    draft-ietf-mpls-ldp-11.txt

MPLS標準化動向

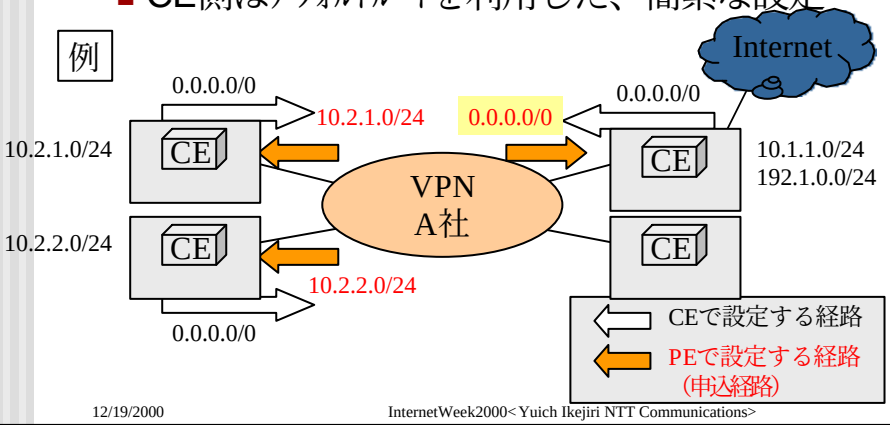
- MPLSを使って特定の経路情報やQoSを持った特定のラベルパスとはるためのシグナリング方式(Traffic Engineeringなど)
  - RSVP-Extension方式
    draft-ietf-mpls-rsvp-lsp-tunnel-05.txt
  - CR(Constraint-Routing)-LDP方式
    draft-ietf-mpls-cr-ldp-04.txt
  - 機能的にはほぼ同じであるが、上記２つの方式が標準化に向けて作業中
  - 実装が使われているのはRSVP-Extension

MPLS標準化動向

- MPLSを使ったIP-VPN実現方式
  - Cisco社のMPLS-VPNやNortel社のVR(Virtual Router)とCR-LDPを組合せた方式などいくつか存在しているが、まだメーカ独自方式
  - RFC2547(Informational:MPLS-VPN)
  - RFC2764(Informational:VR方式) など
  - 7月のIETFにてNetwork Based VPNsのBOFが開催され、今後WGとして標準化作業に向けて動き出したところ。

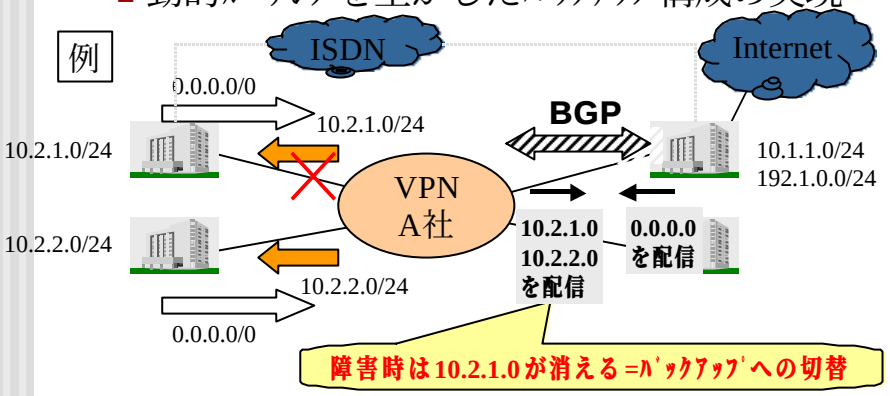
MPLS-VPNユーザ構築例

- Staticの考え方・・・主に拠点向き
  - CE側はﾃﾞﾌｫﾙﾄﾙｰﾄを利用した、簡素な設定



MPLS-VPNユーザ構築例

- BGPの考え方・・・主にｾﾝﾀ向き
  - 動的ﾙｰﾁﾝｸﾞを生かしたﾊﾞｯｸｱｯﾌﾟ構成の実現



参考：IP-VPN方式の特徴比較

VPN分類	Internet VPN		IP-VPN	
VPN方式	IP Sec	L2TP	MPLS-VPN	L2+VR
方式概要	IPパケットの暗号化によるトンネリング	PPPフレームのIPによるトンネリング	ラベルによるIPパケットのカプセリング	FR+レイヤ３終端装置
お客様ルータに必要とされる機能	IP Sec終端機能を持ったルータ/PC	通常のPPPが機能するルータ/PC	通常のルータ	通常のルータ
提供形態	お客様自身によるVPN構築（プロバイダ提供型もあり）	プロバイダとお客様との組合せによるVPN	プロバイダ提供VPN	プロバイダ提供VPN
閉域性	△（インターネット利用）	△（インターネット利用）	○	○
暗号化	あり	なし	なし	なし
帯域確保	△（IPネットワーク）	△（IPネットワーク）	△（IPネットワーク）	○（FRのCIR等）
遅延時間	△（ 装置に依存する部分有り ）	○	○	△（FR網内輻輳時等）
アクセスライン	HSD/DA/FR/ATM/Dup	HSD/DA/Dup	HSD/DA/FR/ATM/(Dup)	FR/CRが中心
お客様側での運用性	△（トンネル構成管理）	△（セッション数管理等）	○（トンネル管理不要）	○（PVC管理不要）
適合する用途	拠点数の少ないLAN間接続	リモートアクセスの方式としては簡易	数100拠点規模の大規模拠点間接続VPN	数100拠点規模の大規模拠点間接続VPN