

IP-VPN(BGP MPLS/VPN)

InternetWeek 2002

NTTコミュニケーションズ(株)

池尻雄一 <y.ikejiri@ntt.com>

December 18, 2002

Yuichi Ikejiri @ NTT Communications

IP-VPN

- ◆ MPLSで実現できる代表的なサービスとしてIP-VPNを取り上げます。
- ◆ また、そのVPNの種類としては、L3VPN及びL2VPNがありますが、ここでは、最も普及しているL3VPNを中心に説明します。
- ◆ L2VPNの詳細については、別セッションを参照ください。

December 18, 2002

Yuichi Ikejiri@NTT Communications

IP-VPN Agenda

- ◆ BGP/MPLS-VPNとは
- ◆ BGP/MPLS-VPNの動作概要
- ◆ BGP/MPLS-VPNのラベルパス決定方法
- ◆ BGPにおけるVPN経路情報
- ◆ BGP/MPLS-VPN設定例
- ◆ BGP/MPLS-VPNユーザ構築事例
- ◆ BGP/MPLS-VPNまとめと新技術

December 18, 2002

Yuichi Ikejiri@NTT Communications

BGP/MPLS-VPNとは

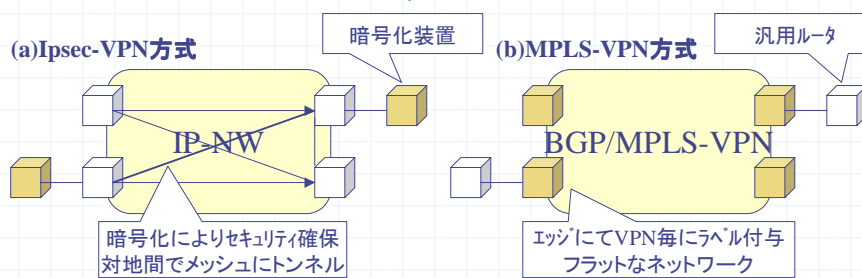
- ◆ RFC2547bisに記されたISPサービスとしてのIP-VPN実現技術
- ◆ インターネットVPN=オープンなネットワーク上で、IPデータ部を暗号化で実現
- ◆ MPLS-VPN=MPLS(ラベルによるカプセルング)により、論理的なクローズドなネットワークを実現
- ◆ 昨今のMPLSを使った他のIP-VPN技術と区別してBGP/MPLS-VPNと呼ばれる。

December 18, 2002

Yuichi Ikejiri@NTT Communications

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



December 18, 2002

Yuichi Ikejiri@NTT Communications

BGP/MPLS-VPNとは

- ◆ 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

December 18, 2002

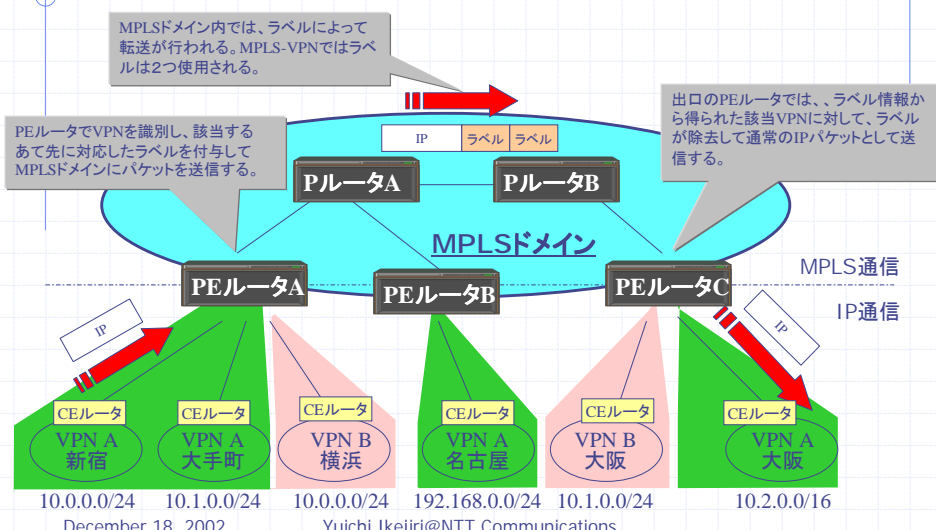
Yuichi Ikejiri@NTT Communications

BGP/MPLS-VPNの動作概要

December 18, 2002

Yuichi Ikejiri @ NTT Communications

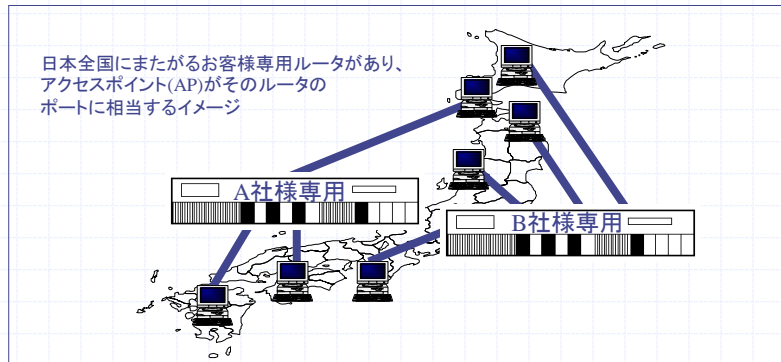
BGP/MPLS-VPN動作概念



December 18, 2002

Yuichi Ikejiri@NTT Communications

BGP/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。

December 18, 2002

Yuichi Ikejiri@NTT Communications

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。

December 18, 2002

Yuichi Ikejiri@NTT Communications

特徴(ISP側)

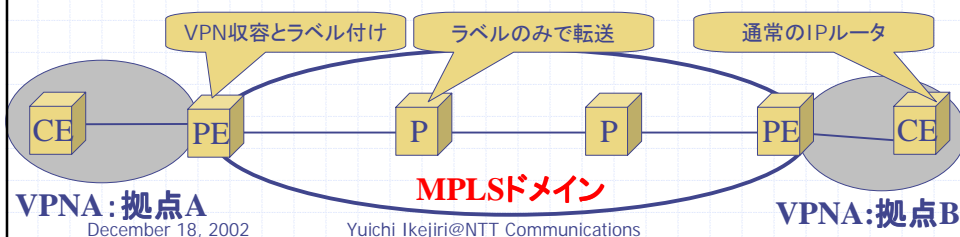
- ◆ 既存のルータによるIPネットワークをそのまま使ってIP-VPNサービスを提供できる。
- ◆ 複数のルーティングプロトコルを使ってお客様を収容できるので柔軟なサービスが提供できる。
- ◆ 複数のVPNを1台のルータに収容できるため効率の良いIP-VPNサービスを提供できる。
- ◆ 異なるVPN間で同じアドレスが使えるためサービスが良い
- ◆ 論理的に分離されたネットワークなのでQoSなどのサービスも実現しやすい。

December 18, 2002

Yuichi Ikejiri@NTT Communications

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)



PEルータのしくみ

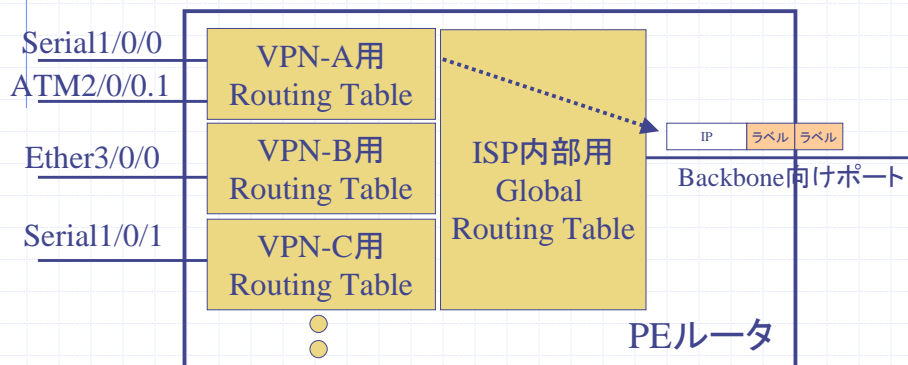
- ◆ 複数のVPNを1台のPEルータに収容するために
 - VRFs:VPN Routing and Forwarding tables
 - VPNごとに異なるルーティングテーブルを持つ
 - 各々CEルータを接続するインタフェースを該当するVRF(VPN)に括りつける
 - VRF同士はルータ内部で分離されており、またバックボーンには、ラベルでカプセルリングしてパケットを送出するので、ATM/FRと同等レベルのセキュリティが確保できる。

December 18, 2002

Yuichi Ikejiri@NTT Communications

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

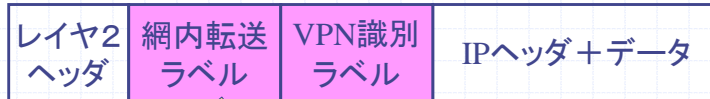


December 18, 2002

Yuichi Ikejiri@NTT Communications

BGP/MPLS-VPN ラベル構成

◆ Shimヘッダ形式



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
- 32bit固定長ラベル×2

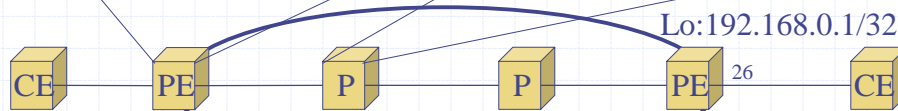
December 18, 2002

Yuichi Ikejiri@NTT Communications

BGP/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

December 18, 2002

MPLSドメイン

Yuichi Ikejiri@NTT Communications

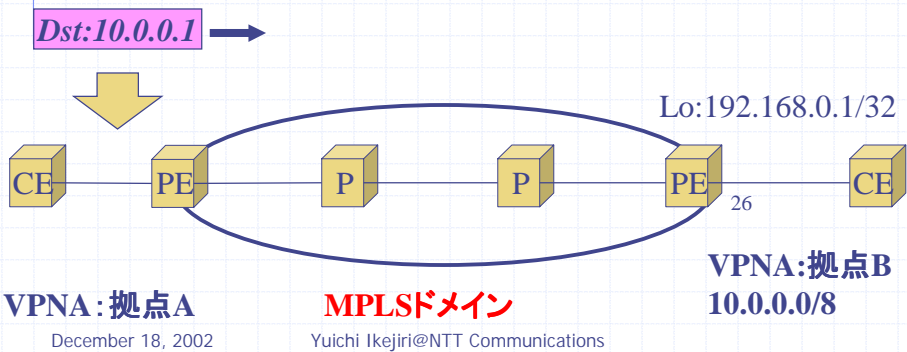
VPNA: 拠点B

10.0.0.0/8

BGP/MPLS-VPN動作概要(cont.)

◆パケット転送(CEルータからのパケット到着)

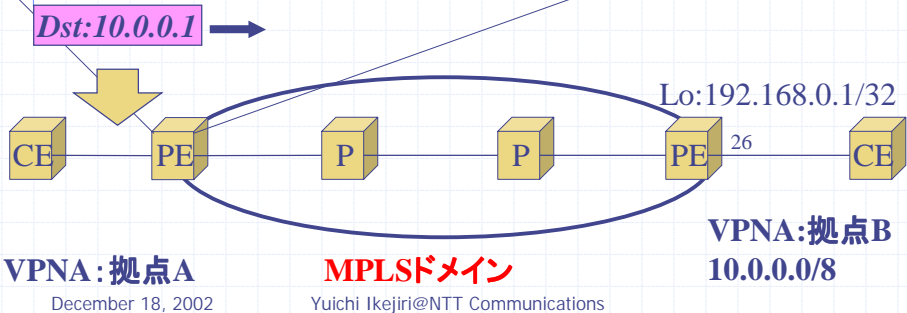
VPNA; 拠点B: 10.0.0.1行きパケット到着



BGP/MPLS-VPN動作概要(cont.)

◆PEルータでのラベルテーブルルックアップ

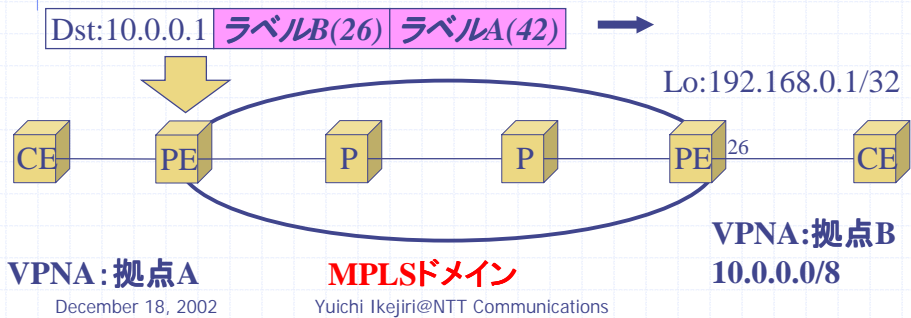
VPN名	Route Dist.	あて先アドレス	VPN識別ラベル	出口のPEルータのアドレス	転送用ラベル
A社	12	10.0.0.0/8	26	192.168.0.1/32	42
A社	12	11.0.0.0/8	989	192.168.0.1/32	42



BGP/MPLS-VPN動作概要(cont.)

◆PEルータでのパケットへのラベル付与

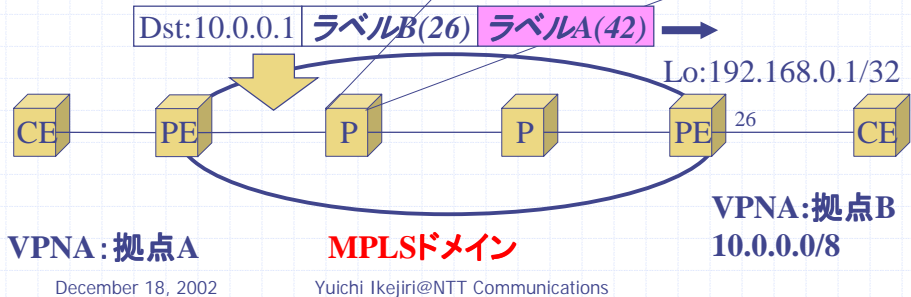
- ① 出口のPEルータより得たVPNA:10.0.0.0/8に相当するVPN識別用ラベルBを付与する。
- ② (1)VPNA:10.0.0.0/8の出口のPEルータをBGP next-hopで知る。
(2) 該当するBGP next-hopに対応した転送用ラベルAを付与する。



BGP/MPLS-VPN動作概要(cont.)

◆Pルータでのラベルテーブルルックアップ

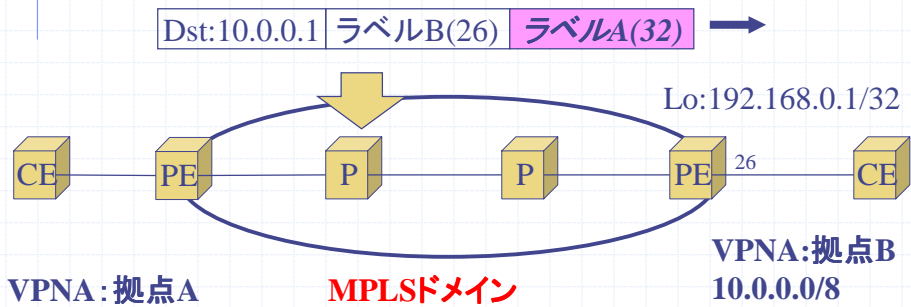
in転送用ラベル	出口のPEルータのアドレス	out転送用ラベル
42	192.168.0.1/32	32



BGP/MPLS-VPN動作概要(cont.)

◆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。

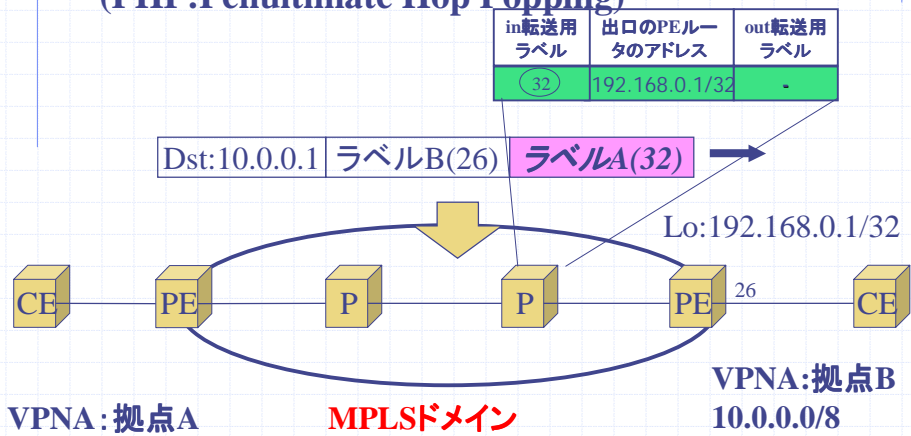


December 18, 2002

Yuichi Ikejiri@NTT Communications

BGP/MPLS-VPN動作概要(cont.)

◆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)



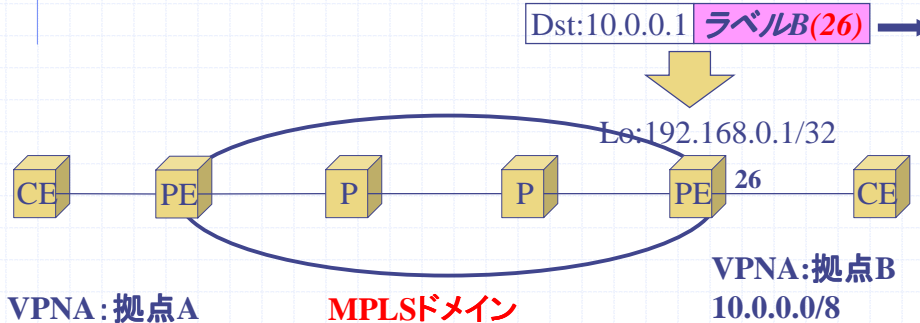
December 18, 2002

Yuichi Ikejiri@NTT Communications

BGP/MPLS-VPN動作概要(cont.)

◆最終PEルータでのラベルテーブルのルックアップ

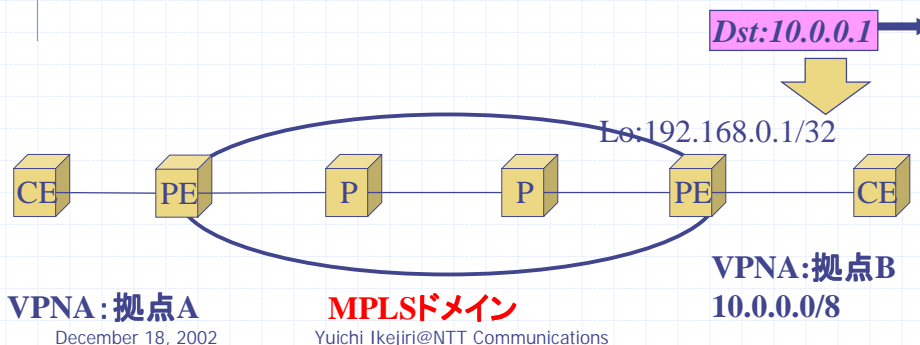
出口のPEルータでは、ラベルBの値を頼りにVPNを識別
& 出カインタフェースを決定しCEルータへパケットを転送



BGP/MPLS-VPN動作概要(cont.)

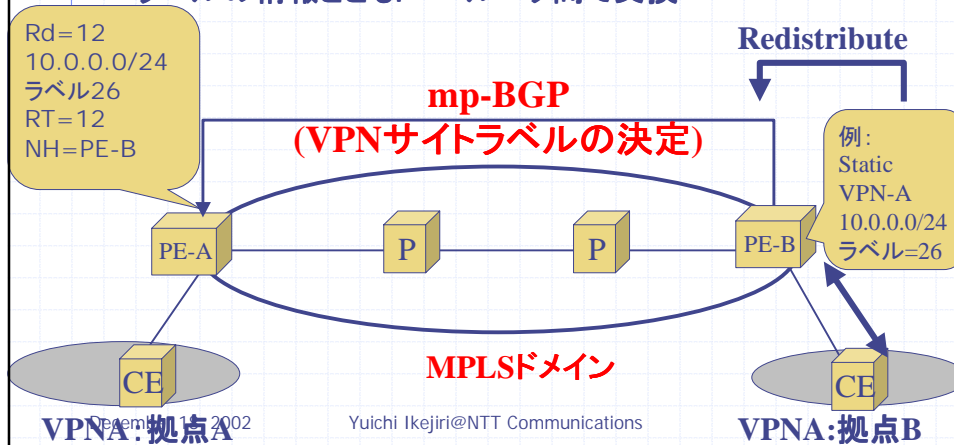
◆目的のCEルータへ到着

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



BGP/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



BGPにおけるVPN経路情報

December 18, 2002

Yuichi Ikejiri @ NTT Communications

BGPにおけるVPN経路

- ◆RFC2858 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
- ◆ラベル情報は、RFC3107に従って Encoding

December 18, 2002

Yuichi Ikejiri@NTT Communications

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)



December 18, 2002

Yuichi Ikejiri@NTT Communications

BGPにおけるVPN経路

◆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 : 9598:1

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

例 : 192.168.0.1:1

December 18, 2002

Yuichi Ikejiri@NTT Communications

Extended Community

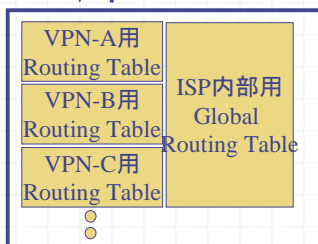
- ◆ Extended Community Attribute(Type Code 16)が新たに定義
- ◆ その中の一つがRoute Target(RT)
- ◆ VRFよりBGPにアナウンスされる経路には、必ず一つ以上のRTを付与する(Export Targets)
- ◆ リモートPEからの経路をローカルVRFに落とし込む際の選択に使用(Import Targets)
- ◆ VPN間通信、AS間通信の実現

December 18, 2002

Yuichi Ikejiri@NTT Communications

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)



テーブルに
のせる際に
付与
(Export)

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)
  .
  .
  .
```

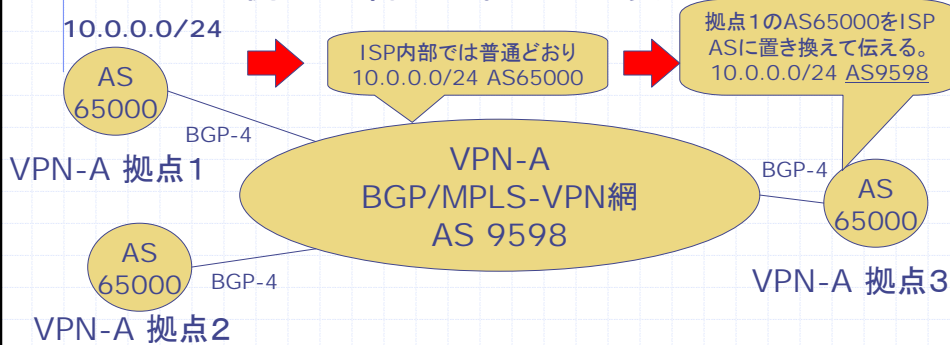
December 18, 2002

Yuichi Ikejiri@NTT Communications

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



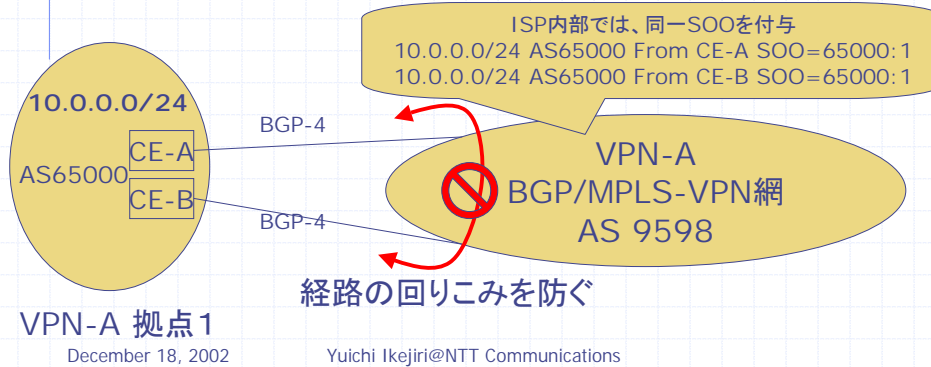
December 18, 2002

Yuichi Ikejiri@NTT Communications

SOO(Site Of Origin)

◆ AS Overrideと併用され冗長構成拠点の同一AS間のループを防ぐ

◆ RTと同じExtend Communityの一つ



BGP/MPLS-VPN設定例

December 18, 2002

Yuichi Ikejiri @ NTT Communications

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
```

December 18, 2002

Yuichi Ikejiri@NTT Communications

PEルータConfig例(Cont.)

◆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
```

December 18, 2002

Yuichi Ikejiri@NTT Communications

PEルータConfig例(Cont.)

◆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

December 18, 2002

Yuichi Ikejiri@NTT Communications

BGP/MPLS-VPNユーザ構築例

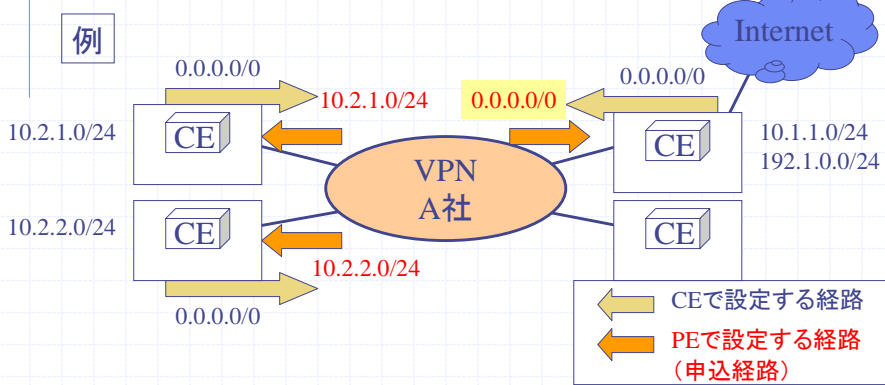
December 18, 2002

Yuichi Ikejiri @ NTT Communications

MPLS-VPNユーザ構築例

◆Staticの考え方・・・主に拠点向き

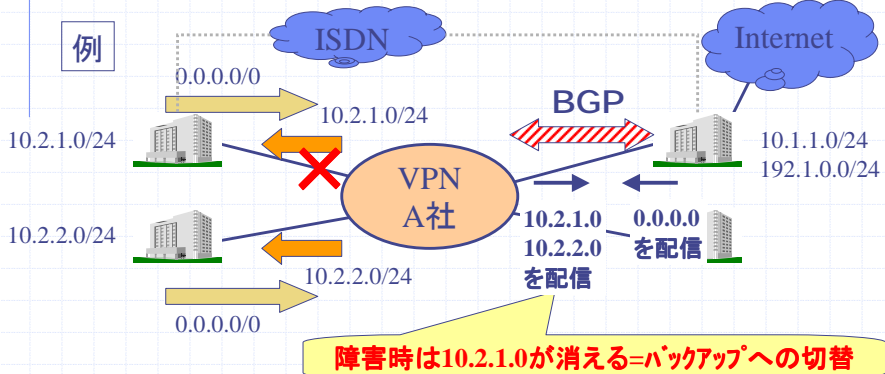
- CE側はデフォルトルートを利用した、簡素な設定



MPLS-VPNユーザ構築例

◆BGPの考え方・・・主にセンタ向き

- 動的ルーチングを生かしたバックアップ構成の実現



BGP/MPLS-VPNまとめ (実際と新技術)

December 18, 2002

Yuichi Ikejiri @ NTT Communications

BGP/MPLS-VPN技術の実際



December 18, 2002

Yuichi Ikejiri@NTT Communications