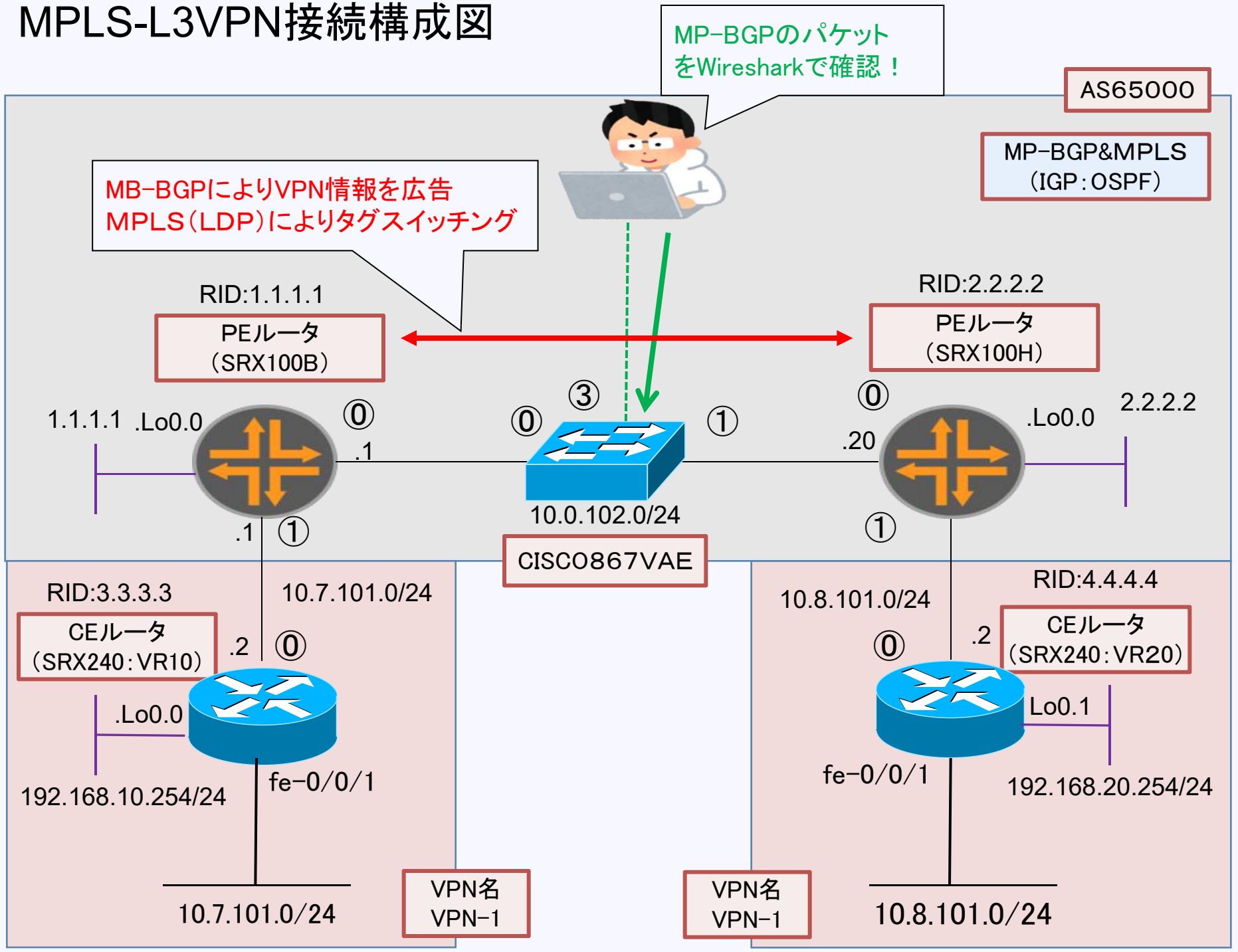
MPLS-L3VPN（Pなし）構成

MPLS-L3VPN接続構成図



MPLS-L3VPNにおけるVPN情報

PEルータ	VPN名	RT/RD	RT: community名	VRFin/out policy名	VPN側 インタ フェース	VPN側の IPアドレス	VPN配下 プロトコル
SRX100B	VPN-1	65000:1	target:65000:1	VRF_import VRF_export	fe- 0/0/1	10.7.101.0/24	OSPF
SRX100H	VPN-1	65000:1	target:65000:1	VRF_import VRF_export	fe- 0/0/1	10.8.101.0/24	OSPF

◇ RD (Route Distinguisher)
⇒ IPv4アドレスの前に付加してVPNv4プレフィックス(96bit) を形成できる。
⇒ MP-BGPテーブル上において、RDにより同じIPv4アドレスでも区別できる。
⇒ MP-BGPネイバーの対向のPEルータのRD値と同じ値でなくてよい(通常は同じ値にする)

◇ RT (Route Target)
⇒ MP-BGPの拡張コミュニティ属性として、MP-BGPネイバーにアドバタイズされる。
⇒ VRFによるVPNを識別するために使用される。
⇒ MP-BGPネイバーから受信したVPNv4プレフィックスをどのVRFに取り込めばいいのか判断するために使用。
そのために、MP-BGPネイバーとなる対向のPEルータで設定するRT値と整合性を取る必要がある。
⇒ RTには、Export RTとImport RTがある。詳細は以下の通り。

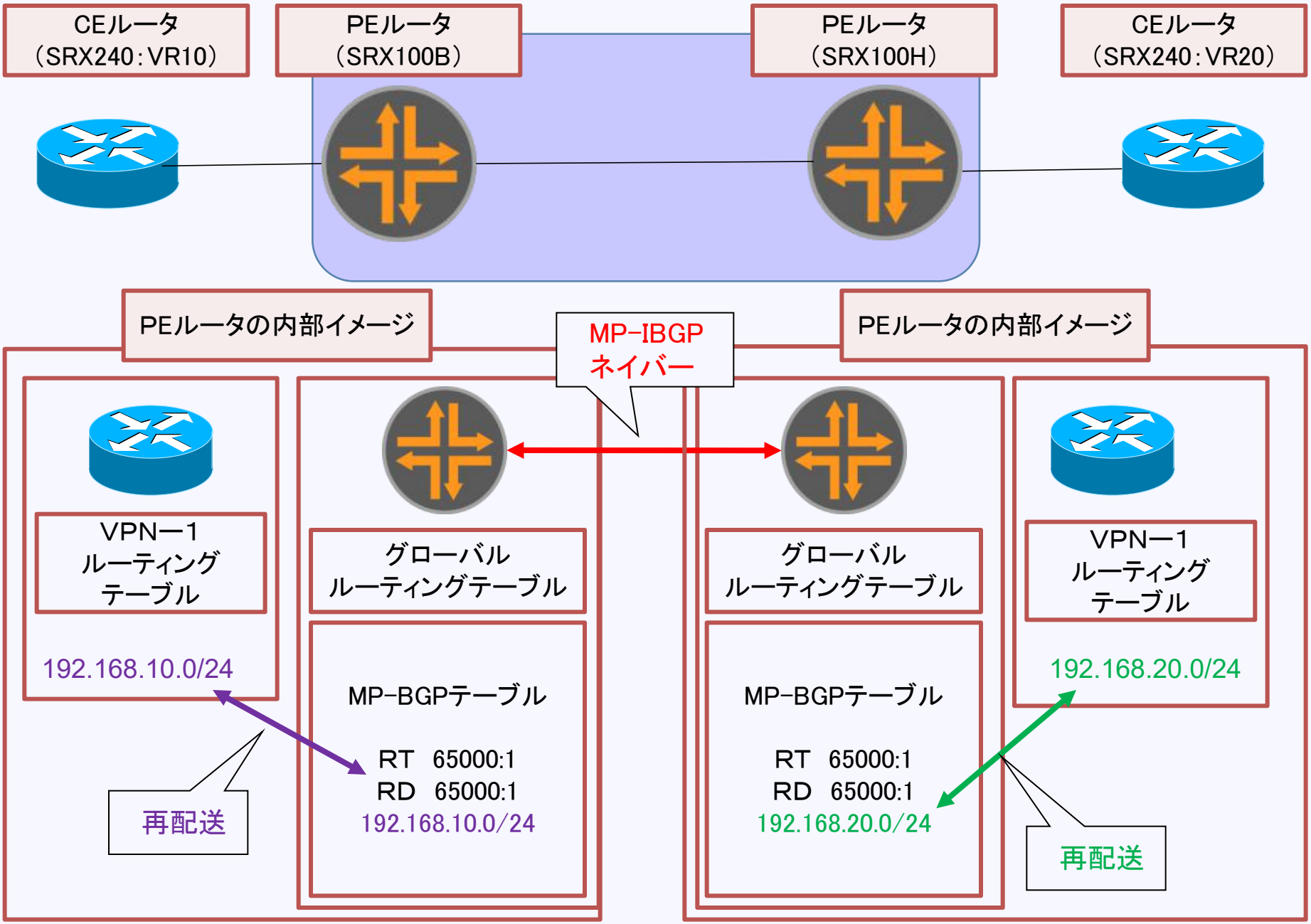
MPLS-L3VPNにおけるVPN情報

2種類のRT（Route Target）についての説明

【Export RT】
- VPNv4プレフィックスを送信する際に付与されるVRFによるVPNの識別子
- １つのVPNv4プレフィックスに対して、複数のRT値を付与することができる。

【Import RT】
- 受信したVPNv4プレフィックスをどのVRFに転送するのかを判断するためのVPN識別子。
- 受信したVPNv4プレフィックスのRT値（対向のMP-BGPネイバーのExport RTで付与された値）を見て、自身のPEルータ上で設定したImport RT値が合致した場合、その経路情報を該当するVRFに取り込む

PEルータの内部イメージ



Junosにおける
MPLS-L3 VPN設定

MPLS-L3VPN事前準備

１　SRX１００のCONFIGをバックアップ及び初期化

```
admin@SRX100H2# load factory-default
```

２　ルートパスワード及び管理者パスワード設定

```
admin@SRX100H2# set system root-authentication plain-text-password
New password:
Retype new password:
root@SRX100H2# set system login user admin class super-user
root@SRX100H2# set system login user admin authentication plain-text-password
New password:
Retype new password:
```

３　セキュリティ周りの設定を削除

```
admin@SRX100H2# delete vlans
admin@SRX100H2# delete protocols
admin@SRX100H2# delete security
admin@SRX100H2# delete interfaces
admin@SRX100H2# set security zones security-zone trust host-inbound-traffic
system-services any-service
admin@SRX100H2# set security zones security-zone trust host-inbound-traffic
protocols all
admin@SRX100H2# set security zones security-zone trust interfaces all
admin@SRX100H2# commit
```

MPLS-L3VPN事前準備

４　MPLSを使用するため、フローベース→パケットベースに変更

```
admin@SRX100H2# set security forwarding-options family mpls mode packet-based
admin@SRX100H2# commit
warning: You have changed mpls flow mode.
You have to reboot the system for your change to take effect.
If you have deployed a cluster, be sure to reboot all nodes.
warning: Inet flow mode has been changed to packet-based mode for mpls mode
modification.
warning: You must reboot the system for your change to take effect.
If you have deployed a cluster, be sure to reboot all nodes.

commit complete
```

５　再起動

```
admin@SRX100H2>request system reboot
```

MPLS-L3VPN設定手順及び確認

１　バックボーン（PE間）の設定
　　設定器材：PEルータ（SRX100B、SRX100H）
　　IPアドレス及びIGP（OSPF）設定、BGP設定
　　→　OSPFネイバー及経路広告確認、BGPピアーの確認
２　PE配下（PE～CE間）の設定
　　設定器材：PEルータ（SRX100B、SRX100H）
　　CEルータ（SRX240）
　　IPアドレス設定及びOSPF設定
　　→　OSPFネイバー及び経路広告確認
３　ルートターゲット及びルーティングインスタンスの設定
　　設定器材：PEルータ（SRX100B、SRX100H）
　　ルーティングインスタンス：
　　VPN毎のVRFテーブルを作成するため
　　ルートターゲット：
　　エクスポートポリシー：各ルートにどのようにターゲットが関連付けるか定義
　　インポートポリシー　：どのルートがVRFに追加されるかを定義
４　MPLS設定及びLDP設定
　　設定器材：PEルータ（SRX100B、SRX100H）
　　タグスイッチングで必要なMPLS及びタグ配布プロトコル（LDP）を有効化
５　各種確認
　　LDPネイバーの確認、経路情報の確認、PCAPの取得

MP-BGPパケットの観察

MP−BGPパケットの観察

○MG-BGPについて

BGP では伝達できるルート情報は IPv4 unicast のみでしたが、
MP-BGP (MultiProtocol-BGP)では、IPv4 unicast 以外の色々なプロトコルのアドレスが伝達できるように拡張されました。（BGP4+ とも呼ばれています）

MP-BGP は、BGP と異なるプロトコルを作るのではなく、BGP の Path Attribute を増やすことで実現しました。（下位互換性あり）

【拡張されたPath　Arrtibuteの例】

Multiprotocol Reachable NLRI (Type14)

形式：[Address Family Information, Next Hop Information, NLRI]

Multiprotocol Unreachable NLRI (Type 15)

形式：[Address Family Information, Unfeasible Routes Length, Withdrawn Routes]

Extended Communities (type 16)

形式：[Type high, Type low, Value]

（Route-Targetの場合、Type high=Ox00, Type low=Ox02となります）

(参考）

http://www.iana.org/assignments/address-family-numbers/address-family-numbers.xhtml

MP−BGPパケットの観察

○MG-BGPにおけるAddress-Familyについて
Address Familyとは、RFC2453 と RFC2858 により IANA で規定された、
プロトコルと AFI の対応付けのことです。

Address Family Information は [AFI, SAFI(Sub-AFI)] で構成さます。

AFIとは、Address Family Identifier の略で、伝達するプロトコルのアドレスを識別する情報のことです。
AFI = 1 ⇒ IPv4
AFI = 2 ⇒ IPv6

SAFI (Sub-AFI)とは、AFI で識別されたプロトコルの詳細識別のことです。
Sub-AFI = 1 (SAFI=1) ⇒ Unicast
Sub-AFI = 2 (SAFI=2) ⇒ Multicast
Sub-AFI = 4 (SAFI=4) ⇒ NLRI with MPLS Labels
Sub-AFI = 128 (SAFI=128) ⇒ MPLS-labeled VPN address

https://www.iana.org/assignments/safi-namespace/safi-namespace.xhtml

WiresharkによるMP-BGPの確認

取得したPCAPでは以下を観察できました！
【今回は送信元：1.1.1.1（SRX100B）、宛先：2.2.2.2（SRX100H）
のBGP Updateに注目！】

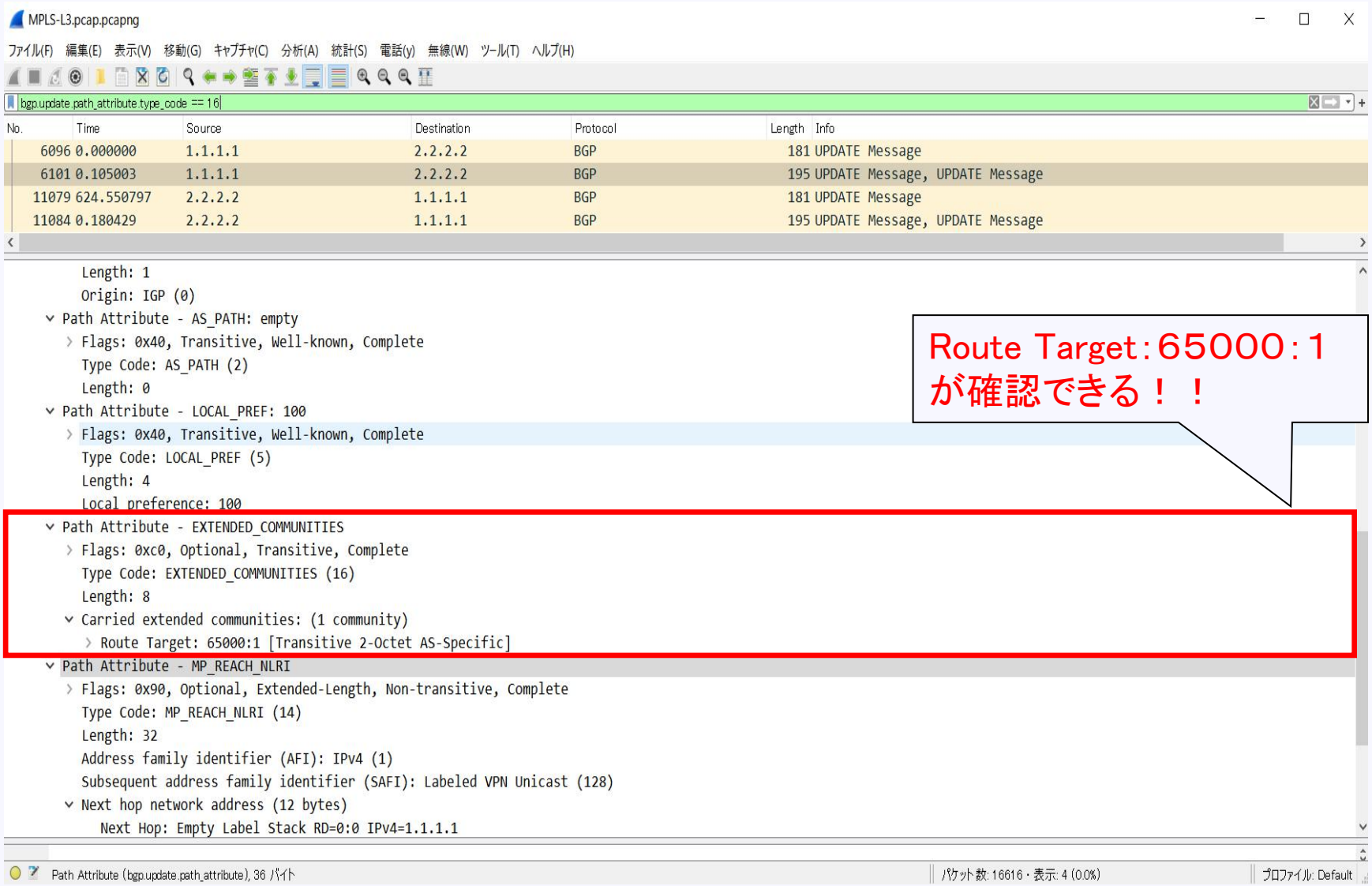
○ RT（Route Target）の確認
表示フィルタ：”bgp.update.path_attribute.type_code == 16”
→ Path Attribute - EXTENED__COMMUNITIES
Carried Extened communities
Route Target: 65000:1
が確認できる！

○ RD(Route Distinguisher)の確認
表示フィルタ：”bgp.update.path_attribute.type_code == 14”
→ Path Attribute - MP_REACH__NLRI
Subusequest address family identifier(SAFI): Labeled VPN unicast(128)
Network layer reachability information (15bytes)
Route Distinguisher : 65000:1
MP Reach NLRI IPv4 prefix: 10.7.101.0
が確認できる！

WiresharkによるMP-BGPの確認

○　RT（Route Target）の確認

”bgp.update.path_attribute.type_code == 16”

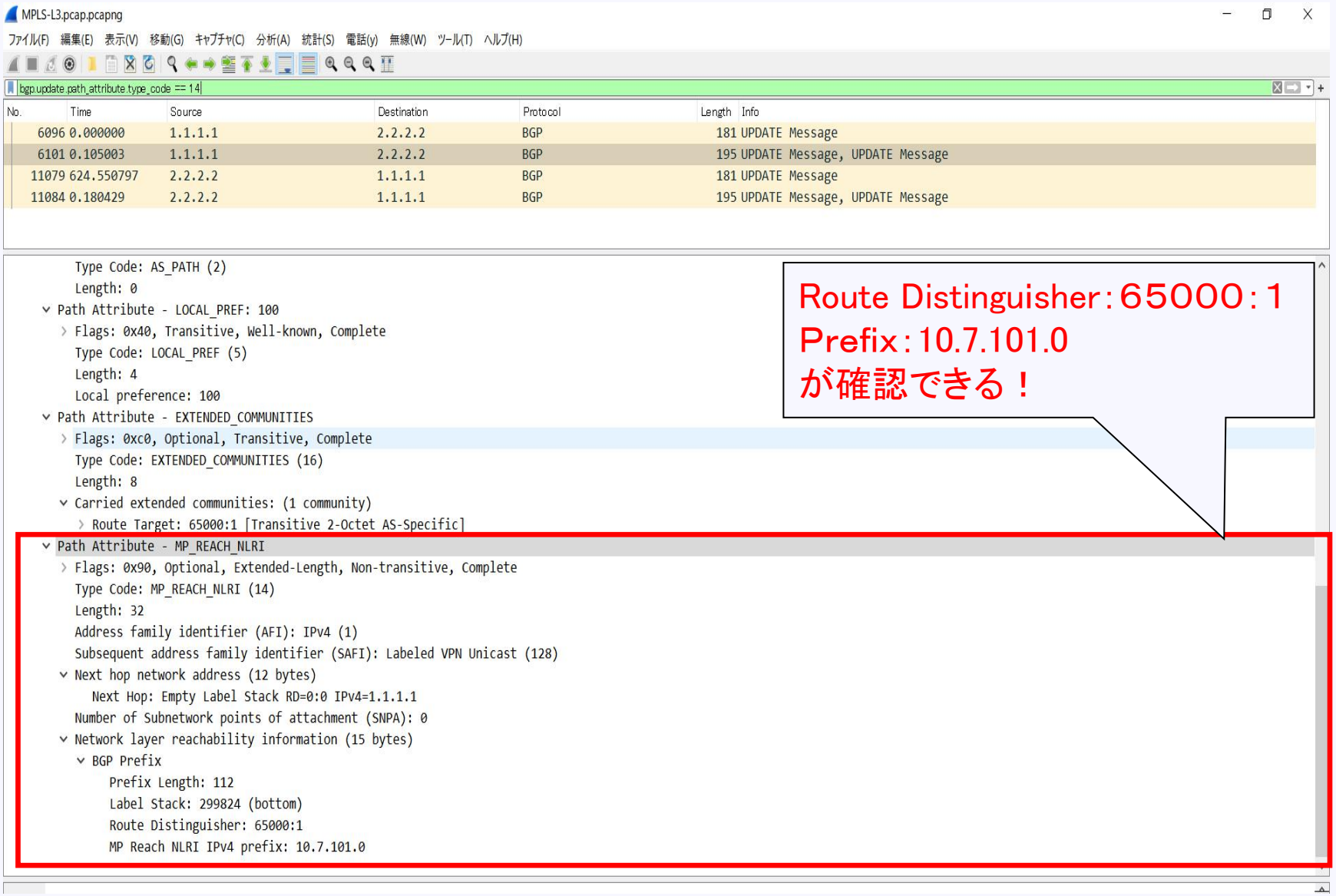


Route Target：65000：1
が確認できる！！

WiresharkによるMP-BGPの確認

○ RD(Route Distinguisher)の確認

”bgp.update.path_attribute.type_code == 14”



〇MPLS-VPNとは？？
https://www.infraexpert.com/study/mpls6.htm

SEの指標

【MP-BGP】のType(NLRI, AFI/SAFIやRoute-Target)の仕組みとシーケンス, パケットキャプチャ
https://milestone-of-se.nesuke.com/nw-advanced/mpls-vpn/detail-of-mp-bgp/