

L3 inter-domain VPNの現状と展望

KDDI株式会社

熊木 健二

ke-kumaki@kddi.com

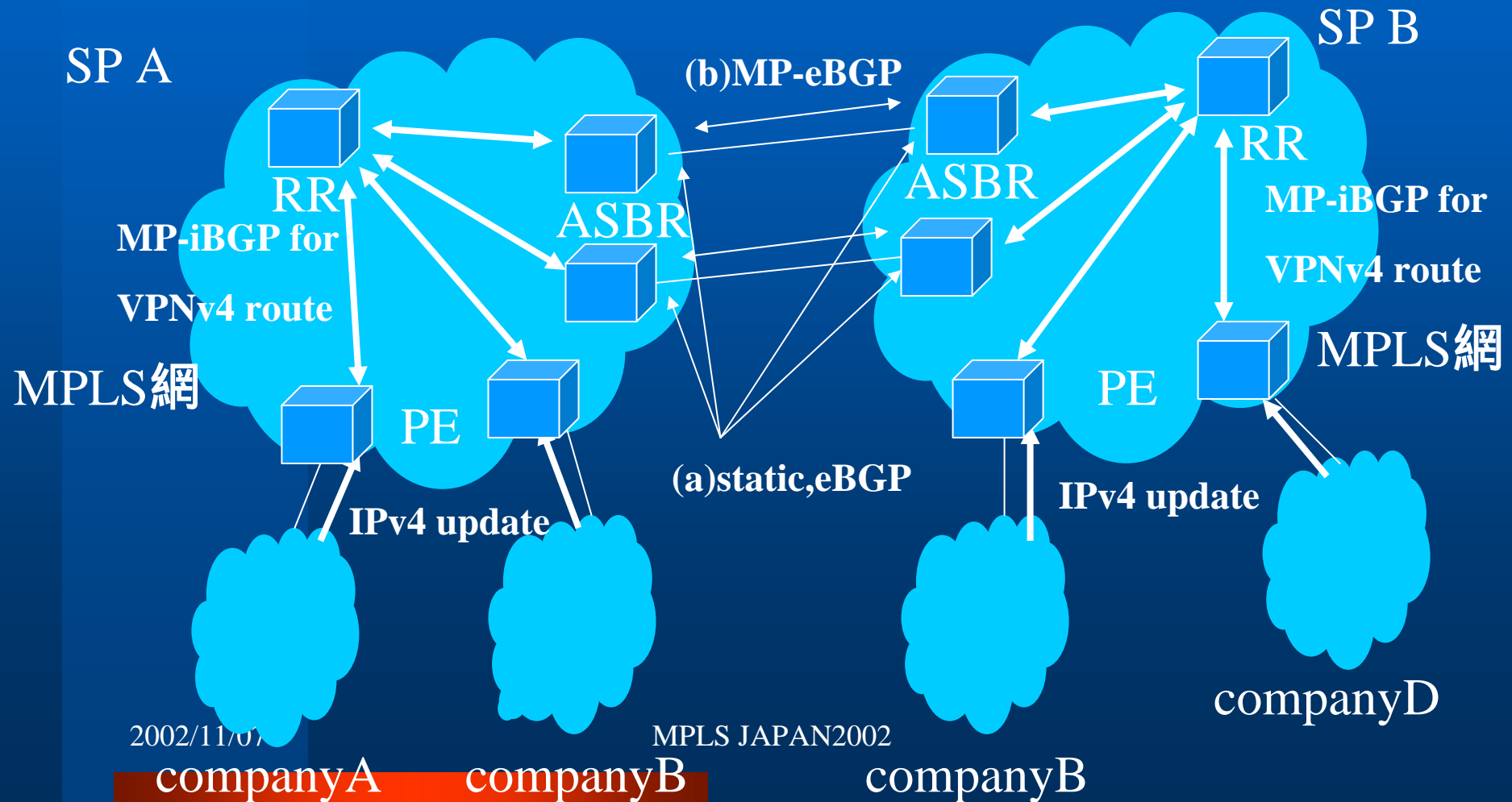
Agenda

- Inter-AS VPNモデル
- End-to-End QoS
- Security
- Scalability
- 現状の問題点
- 今後の展望

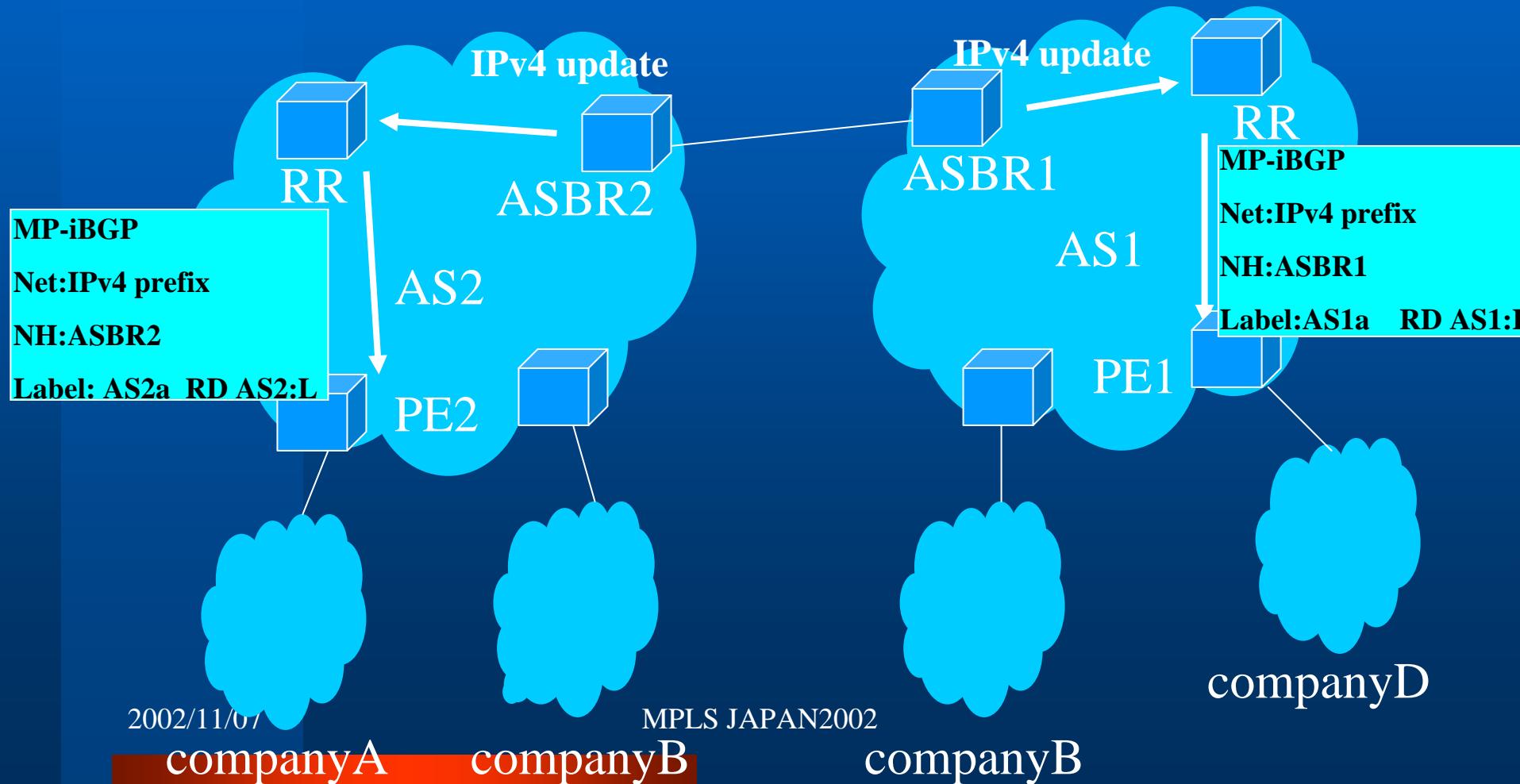
Inter-AS VPNモデル

- 2547bis section10
 - Type(a):vrf-to-vrf approach
 - Type(b):MP-eBGP between ASBRs approach (RFC3107)
 - Type(c):Multihop-eBGP between RRs approach (RFC3107 section6)
- 2547bis section9
 - CsC
- その他にも、、、
 - GRE tunnel

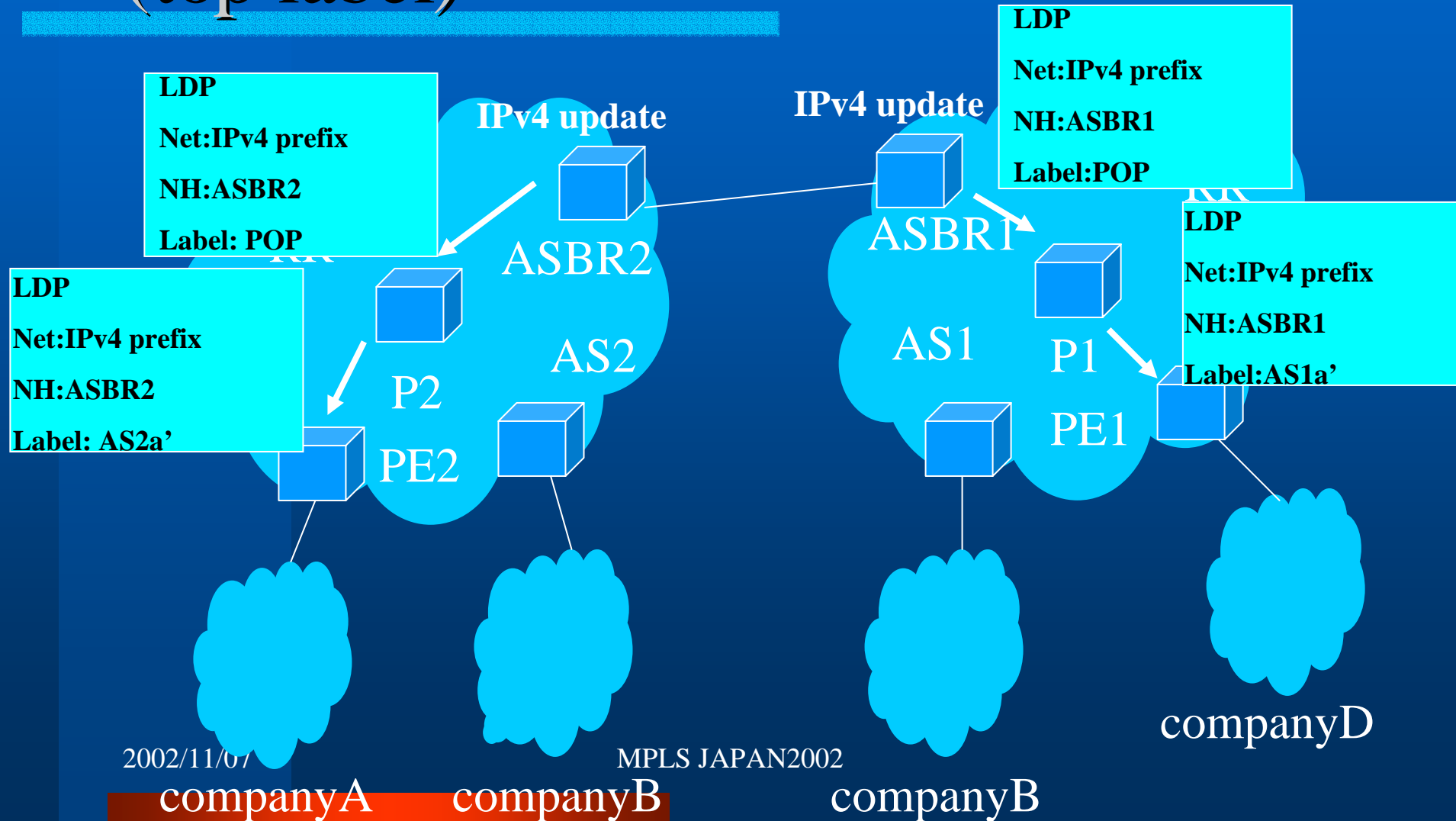
現状でのInter-AS VPN



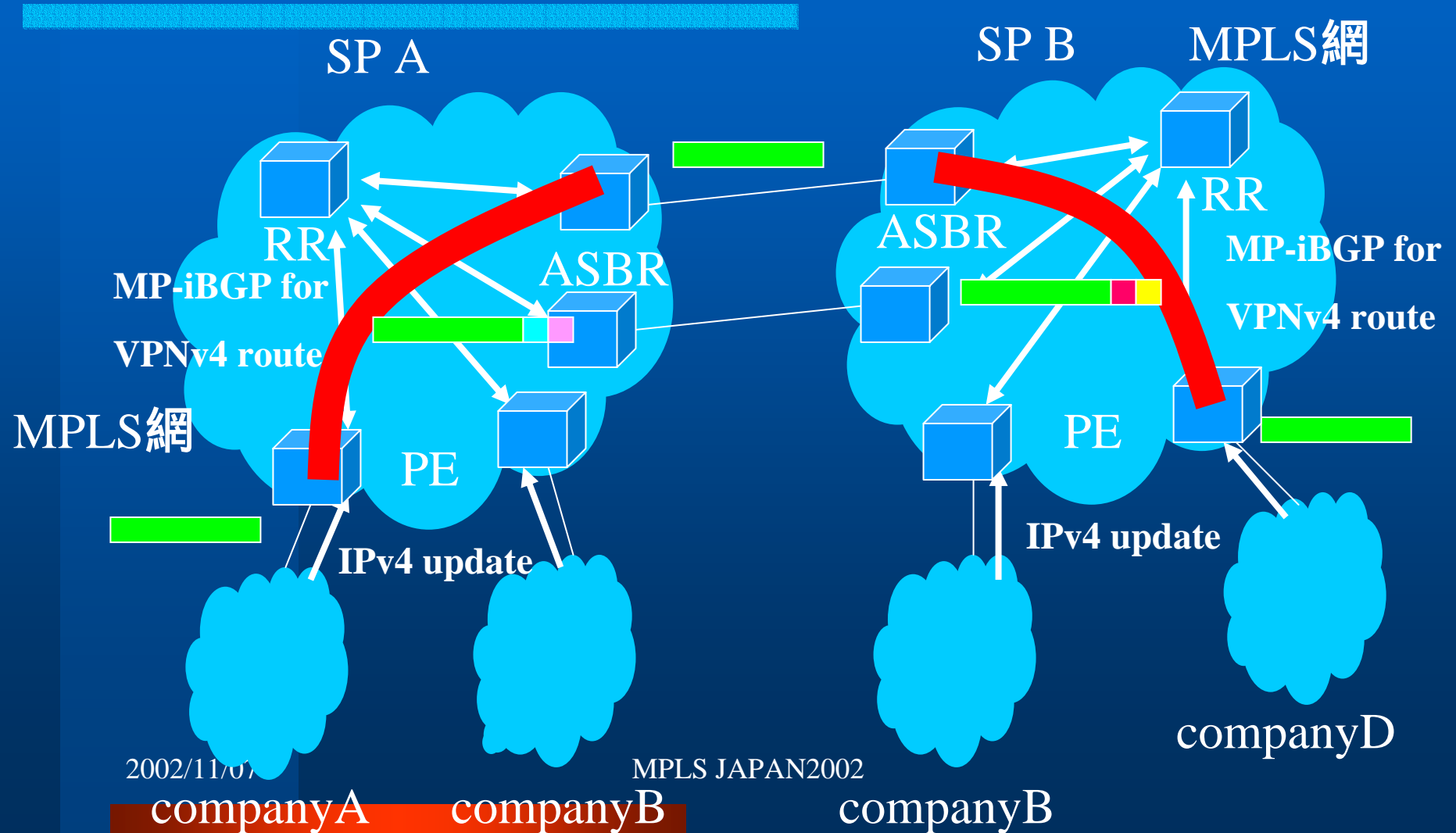
vrf-to-vrf approach – control plane (bottom label)



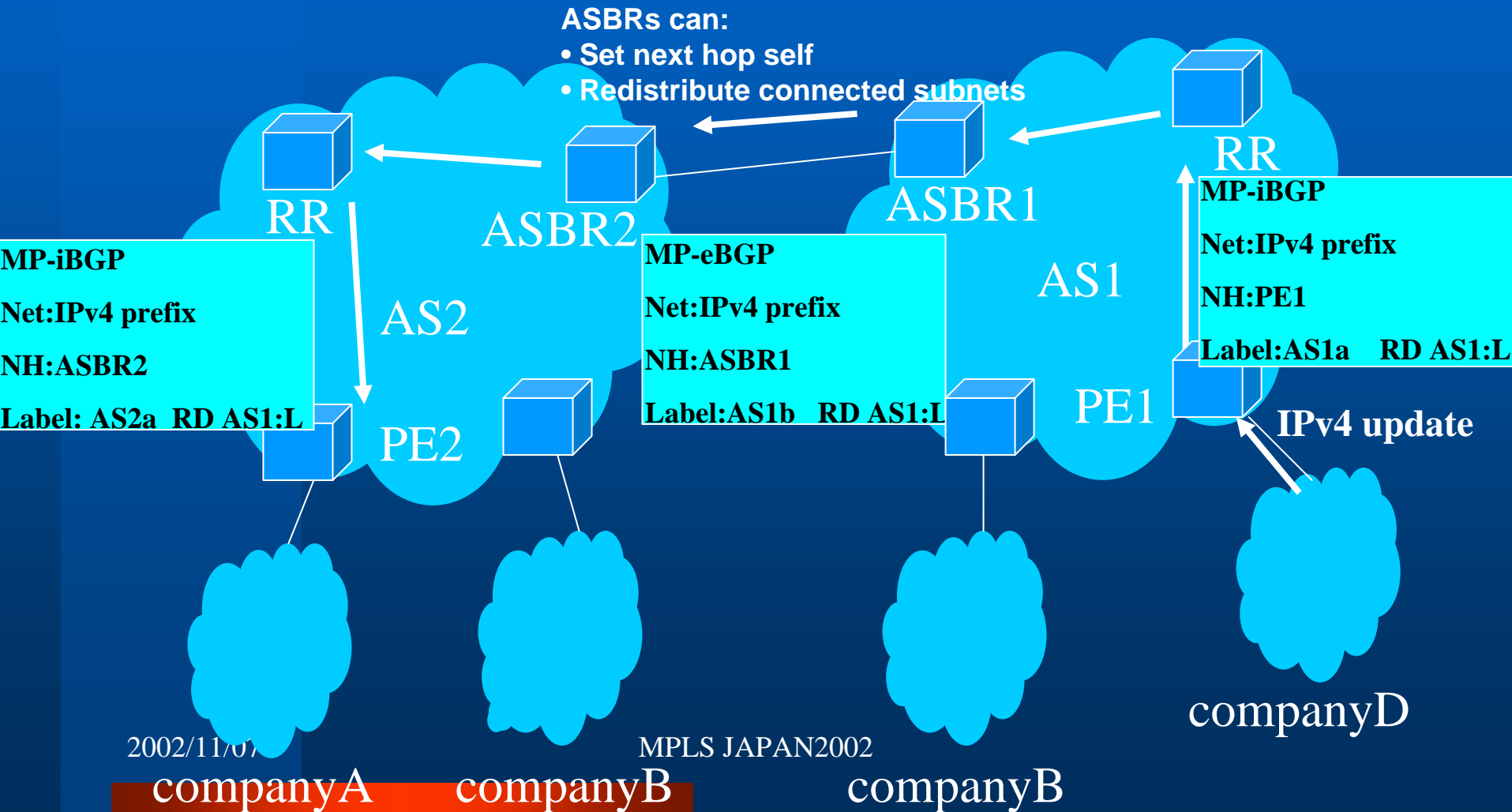
vrf-to-vrf approach – control plane (top label)



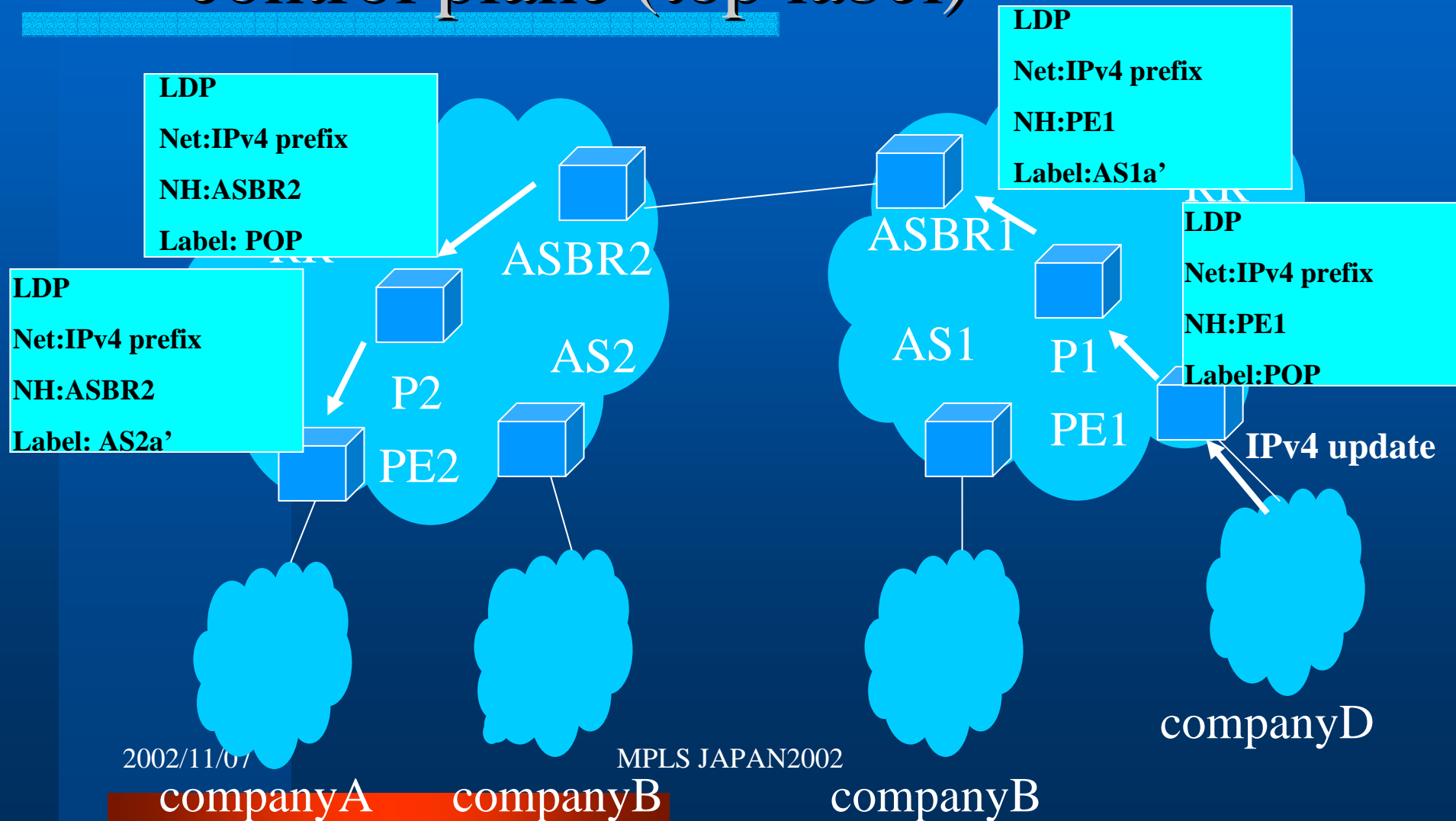
vrf-to-vrf approach-forwarding plane



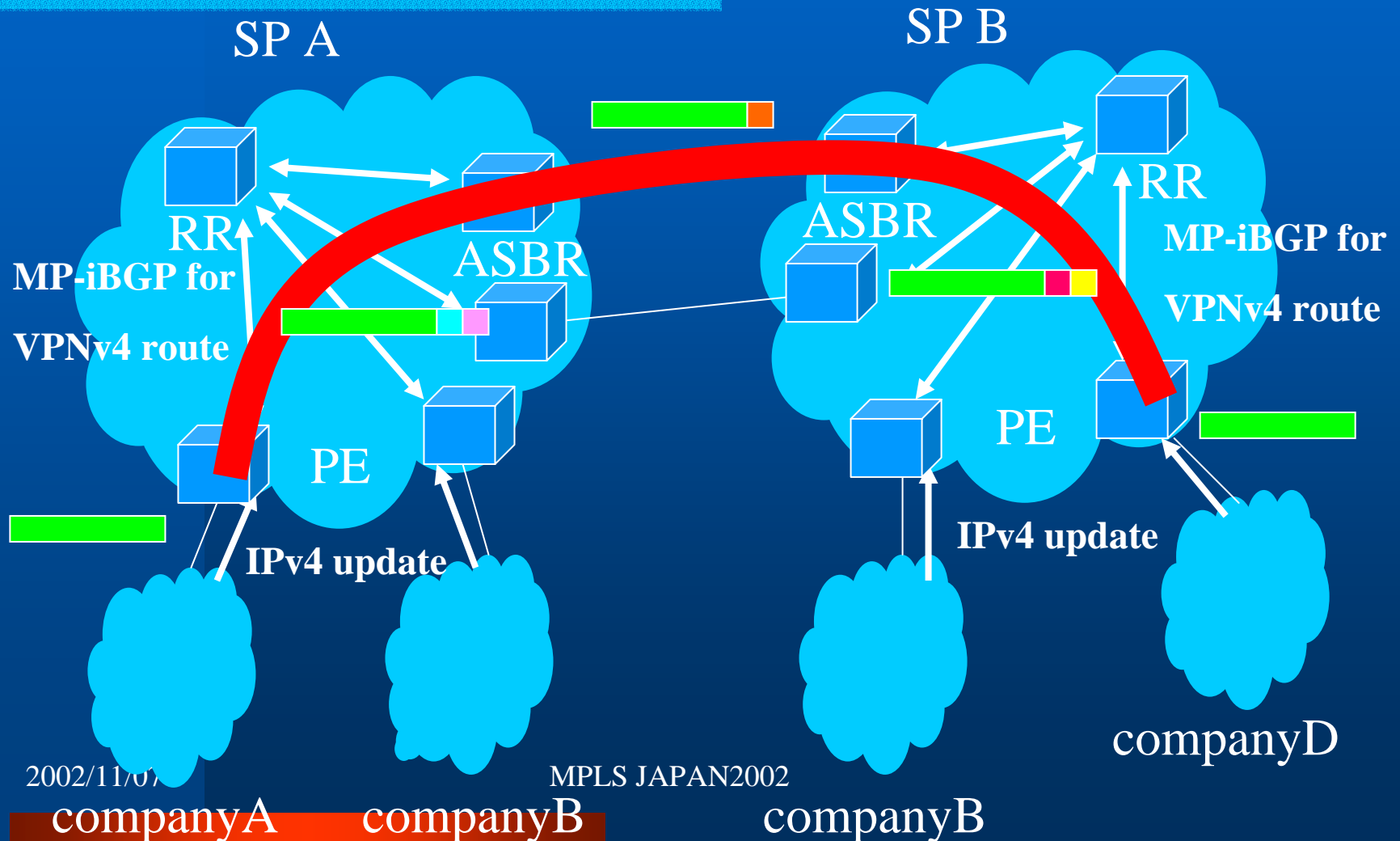
MP-eBGP between ASBRs approach – control plane (bottom label)



MP-eBGP between ASBRs approach – control plane (top label)



MP-eBGP between ASBRs approach – forwarding plane



Multihop-eBGP between RRs approach

- ASBRの保持する経路数及びtraffic量によりtype(c)も必要になる可能性もある
 - IPv4+labelを相手に流す必要がある 必要なIPv4+labelを受け取るためfilterしないといけない
 - BGP peerは相手のネットワークに依存するため場合によっては不安定になる可能性もある
 - Scalabilityはある

End-to-End QoS

- 当初はBEで十分だった。。。
 - End-to-EndでのQoSのrequirementが出てきた
 - ところが。。。
 - SP同士でQoSのpolicyが異なる(特にサービスに直結する)
 - IP precedence base,DSCP base
 - edge,edge+core
- とりあえず方法としては(IP部分、MPLS部分)
 - Type(a):ASBR (marking:rewrite) and/or ingress PE(marking+policing)
 - Type(b):ingress PE(marking+policing) and/or ASBR(marking:rewrite)

End-to-End QoS (Cont.)

- 結局のところサービスとサービスのmappingをするしかない
 - どうやるの。。。 (サービスの均一性)
 - Edge機能のQoSのmapping (IP Precedence, DSCP)
 - Core機能のQoSのmapping (Cos)
- シームレスなサービスは無理なの？
 - あくまで擬似的 (QoSの粒度の違いなど)
 - ユーザの要求にもよる
 - でもなんとか。。。

Security

- もちろん信頼できる相手とのpeeringである
 - ext-communityのfiltering(in,out)
 - 必要な経路以外はadvertise, receiveしない
 - IPv4+labelのfiltering
 - 場合によってはLDP/BGP sessionでMD5 authenticationを用いる

Scalability

- RRからは必要なRTだけを受け取る
 - RRのフル経路は必要ない
- ASBRからは必要なRTだけを広報する
- 相互接続先ASBRからは必要なRTだけを受け取る

現状の問題点

- Traffic control
 - 1つもしくは複数のASをまたいでのシームレスなtraffic制御(specific route等)ができない
- Protection
 - 1つもしくは複数のASをまたいでの高速なprotectionができない(link/node protection)
- End-to-End QoS
 - シームレスなEnd-to-EndでのQoSは提供できない
 - 帯域保証ができない

現状の問題点 (Cont.)

結局のところ現状の問題を克服できるのは1 domainのRSVP-TEを拡張すること
(top labelの部分)

Diffserv aware inter-AS TE

今後の展望

- draft-zhang-mpls-interas-te-req-00.txt

(55th IETF @Atlanta)

Raymond Zhang(Infonet Services Corporation)

Kenji Kumaki(KDDI Corporation)

JP Vasseur(Cisco Systems, Inc)

Paul Mabey(Qwest Communications)

Nadim Constantine(Infonet Services Corporation)

– このdraftはあくまでinter-AS TEについての記述

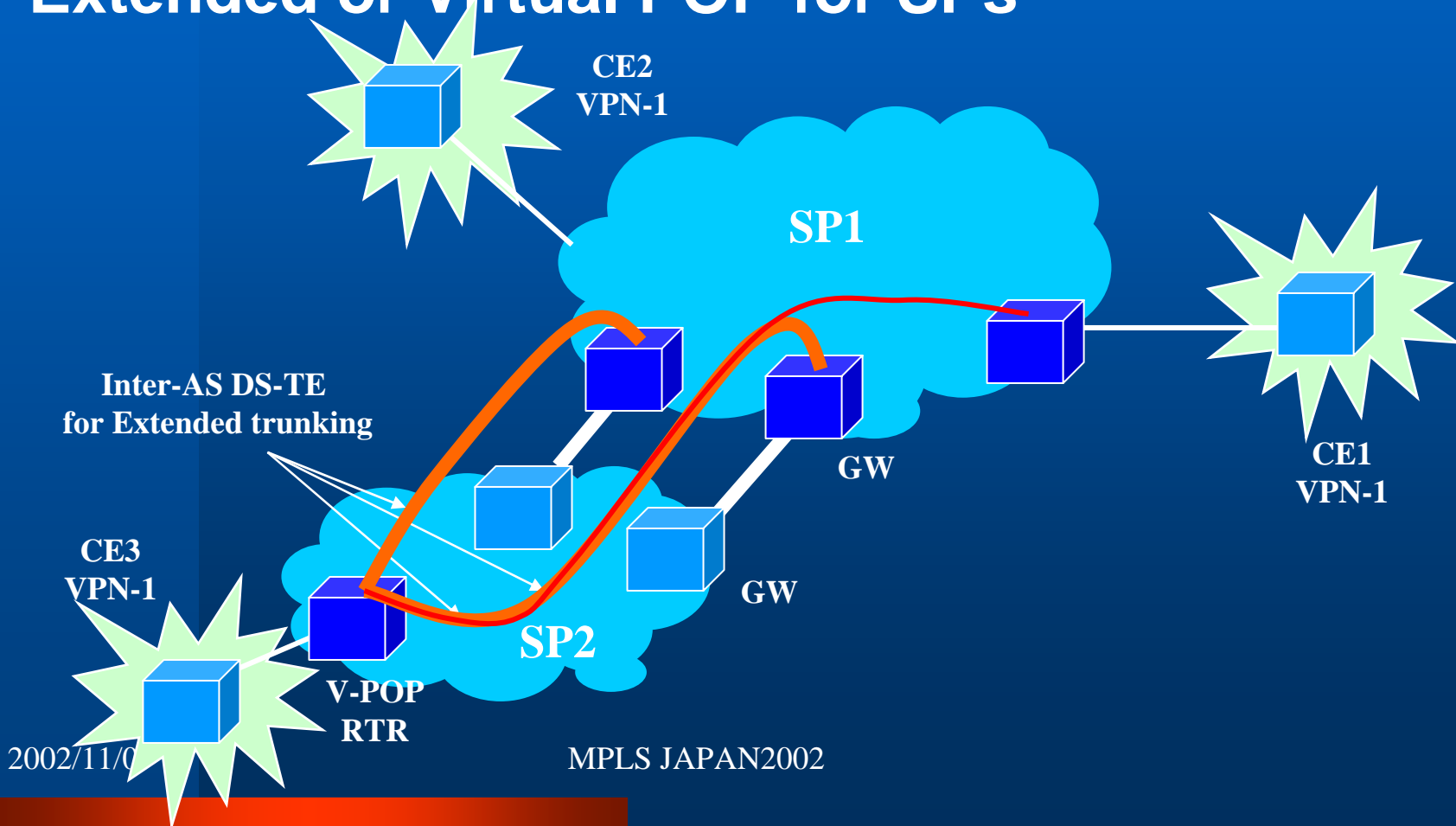
– draftの一部のシナリオをinter-AS VPNに適用する

シナリオ(1)

- 相互接続先のPoPにVPN userが多数ある
- 相互接続先のPoPを利用してPEを置く
- PEは相互接続先のIGP,BGP domainに属さない
- シームレスさを保証するために相互接続先のPEから接続元ASBRまではinter-AS TE trunk(s)のLSPを張る
- End-to-End Diffserv pathを張るために、SPはDiffserv PHBをサポートする

シナリオ(1) (Cont.)

- Extended or Virtual POP for SPs

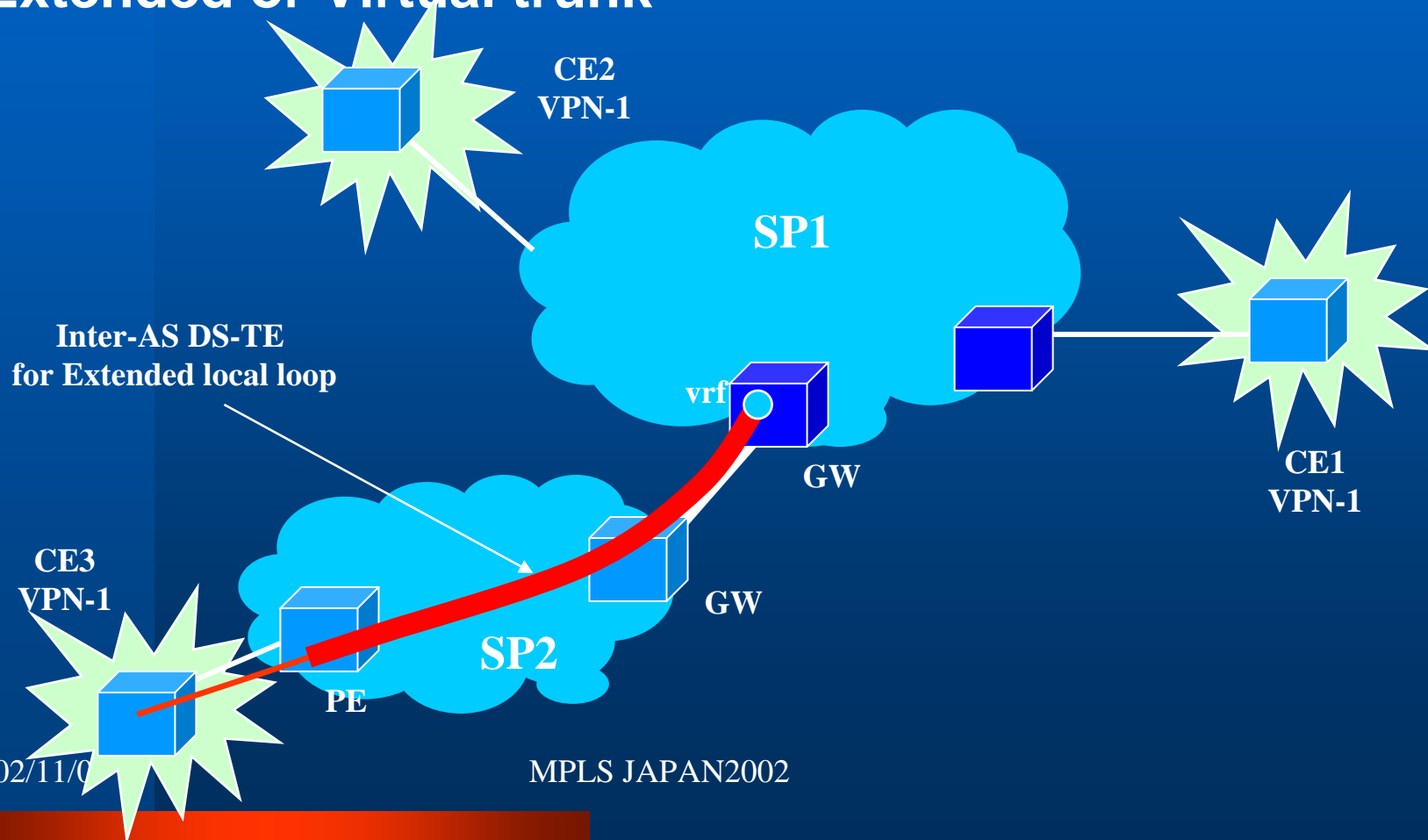


シナリオ(2)

- 相互接続先のPoP先にVPN userが少数
- ASBRからは相互接続先CEにdirectに inter-AS TE LSPを張る
 - ASBRの足はvrfとする
- 複数のCEへLSPを張る場合にはPEで LSPの階層化を行ってもよい
- LSPの帯域は保証される

シナリオ(2) (Cont.)

- Extended or Virtual trunk

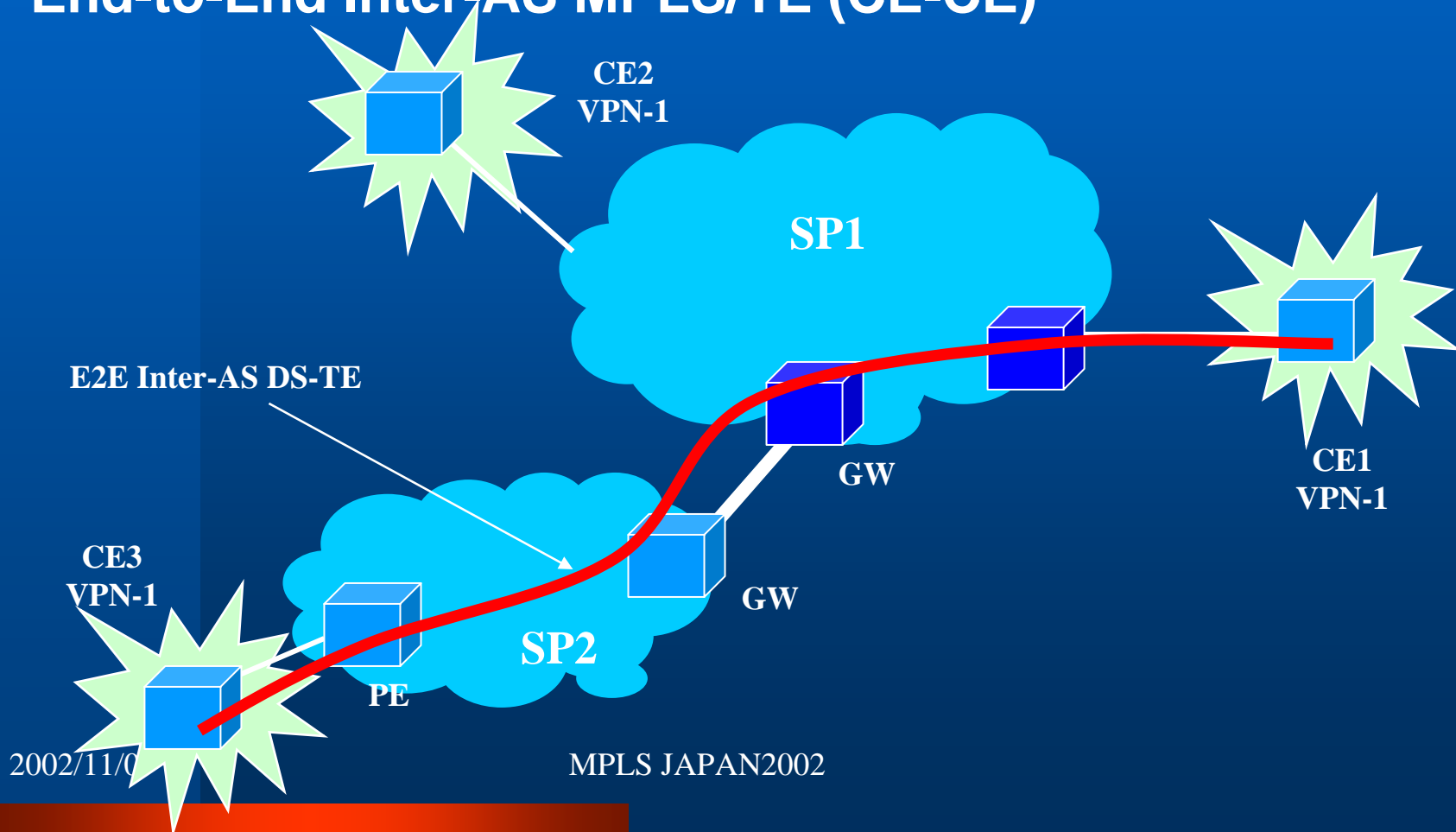


シナリオ(3)

- End-to-Endで帯域保証
 - CE-CE間でEF trafficを通す
- CE-CE間でInter-AS TE LSPを張る

シナリオ(3) (Cont.)

- End-to-End Inter-AS MPLS/TE (CE-CE)



シナリオに対する要求

- Inter-AS TEのサポート
 - ASBRを越えてシームレスにend-to-endでLSPが張れる (RSVP signaling)
- Inter-AS DS-TEのサポート
 - draft-ietf-tewg-diff-te-reqts-06 section4.1を満たす必要がある
- LSPの階層化
 - シナリオ(1)(2)(3)のように1つのASBRから複数のinter-AS TE LSPを張る場合にはscalabilityの問題から階層化できることが望ましい

シナリオに対する要求(Cont.)

- 最適化

- Inter-AS pathは異なるIGP metricを持ついくつかのASをまたぐためIGP metricの正規化をする必要がある

- 異なる経路のinter-AS TE LSPのサポート

- LSR間で複数のLSPを張ることが望ましい(特にシナリオ2の場合)
 - Link/SRLG/Node diversely routed inter-AS TE LSPをセットアップできること

シナリオに対する要求(Cont.)

- **Fast Recovery**

- Inter-AS link障害時に高速にlocal protectionができること
 - Link/Node protection (Detour LSP, Bypass LSP)

- **Protocol Signaling and Path Computations**

- Inter-AS TE tunnel pathは(intra-AS segment in AS x, inter-AS segment across inter-AS link, intra-AS segment in AS y)からなる
- ASBRのselectionはmanualとauto-discovery
 - Auto-discoveryではIGPのextensionが必要

シナリオに対する要求(Cont.)

– LSPのset up

- manual: マニュアルでhopを指定(全て/一部)
- automatic: IGP Extension(例えばdraft-vasseur-mpls-ospf-te-cap-00.txt)を使用したPCS(Path Computation Server)のdiscovery mechanism、PCSにinter-AS TE LSPを計算する要求をするためにsignaling protocolの拡張が必要
- RFC3107を使用してLSPを張ることも可能だがlabeled IP prefixを他ASに広報する必要がある

シナリオに対する要求(Cont.)

- 機密性

- 他ASの詳細なhop-listを知らなくても他ASのASBRからそのASの最適なTE LSPを知ることができること

- TrafficをInter-AS TE tunnelにmapping

- 特定のvrfにTE LSPをmappingできること
(シナリオ(2))

シナリオに対する要求(Cont.)

- Policy control

- 異なるSP間ではpolicyが異なる (policy serverでも可)

- FRRをサポートする？
- DS-TE bitの書き換え、TE metrics等
- RSVP path attribute(affinities,preemption priorities)の書き換え
- Bandwidth controlをサポートするか

- LSPの運用保守

- lsp ping,tunnel trace,MPLS TTL...

評価基準

- Scalability

- IGP (IGP flooding frequency, link state database size, SPF....等の影響)
- BGP (BGPで追加で運ぶ情報の影響)
- RSVP message flooding (RSVP message, LSPの数の影響)

0 0 0

評価基準 (Cont.)

- Performance

- TE LSP setup time

- Inter-AS TE LSPの最適化指数

0 0 0

Security

- Inter-AS signaling requestを authenticate/allow/denyできるようなモデルが必要

Thank you

ke-kumaki@kddi.com