Layer 2 VPNとPseudo Wire 技術

～ネットワークベースVPN最新動向～

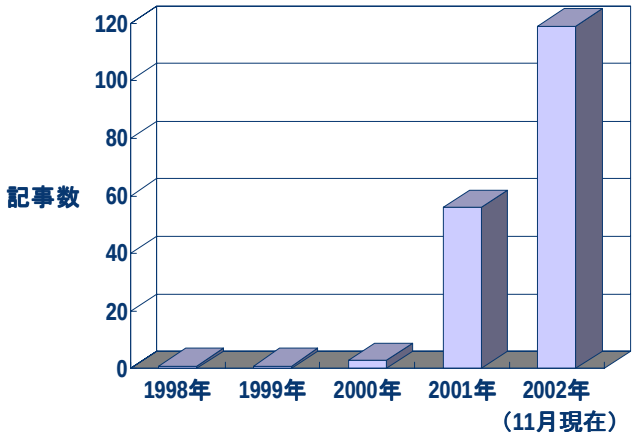
コサインコミュニケーションズ(株)
Technical Director 進藤 資訓
mshindo@cosinecom.com

「IP-VPN」をZDNet Japanで検索

ZDNet Japan で「IP-VPN」を
キーワードに検索
↓
180件のマッチ

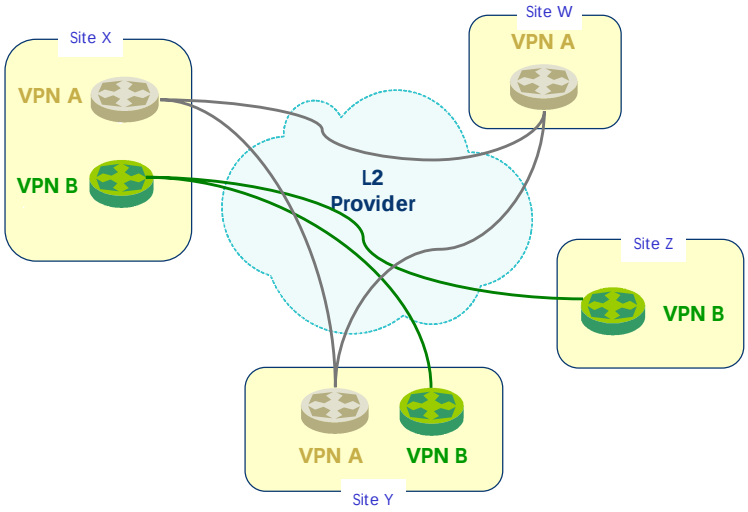
3

2001年は IP-VPN 元年、2002年は成長・定着の年！



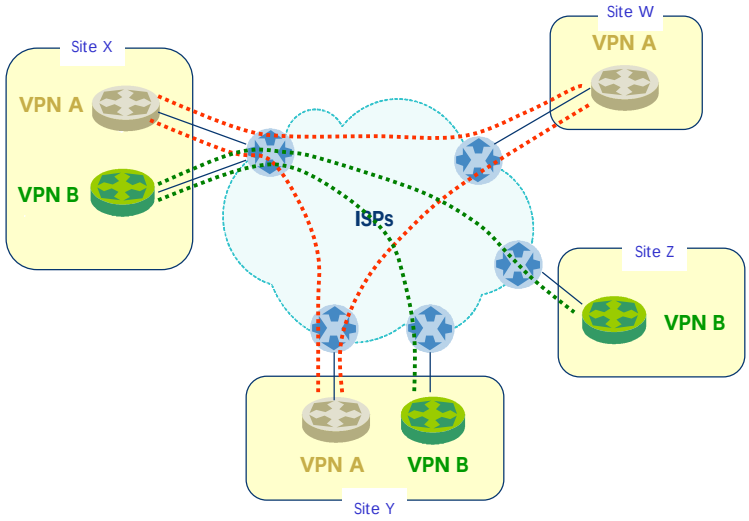
4

VPNの変遷（1）　～(!V)PN時代～



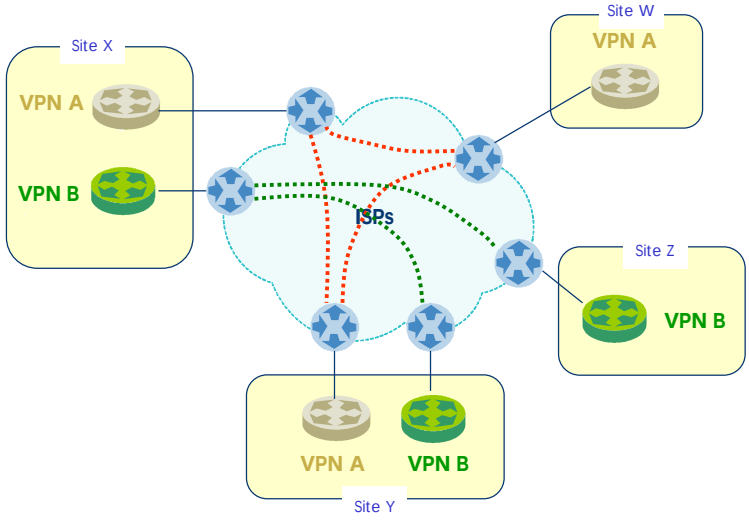
CoSine

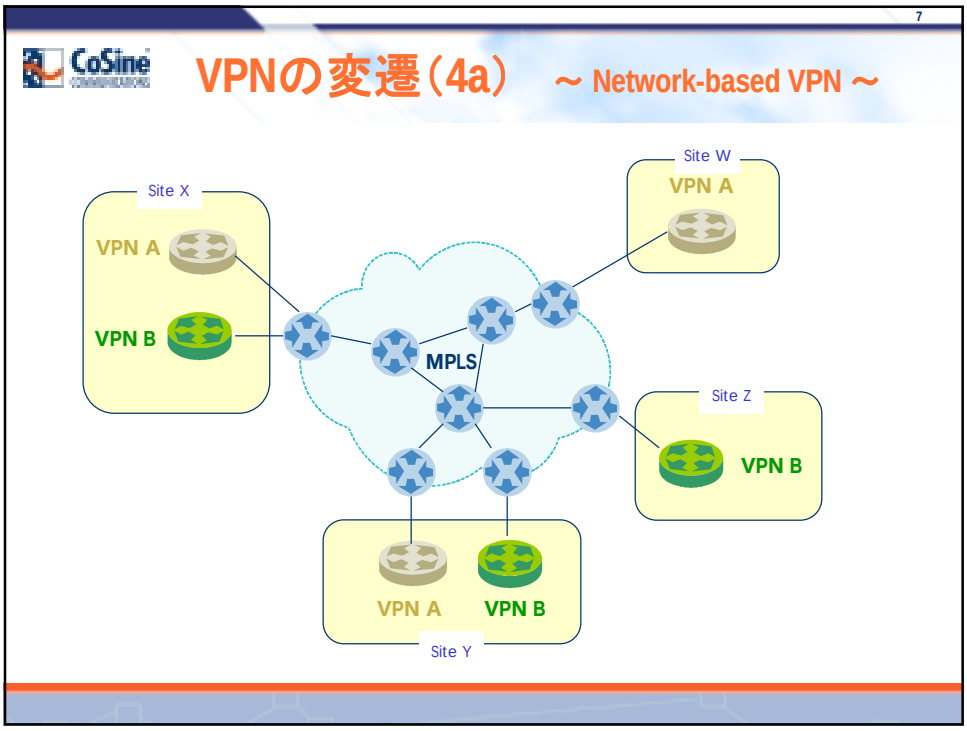
VPNの変遷（2） ～ CPE-based VPN ～

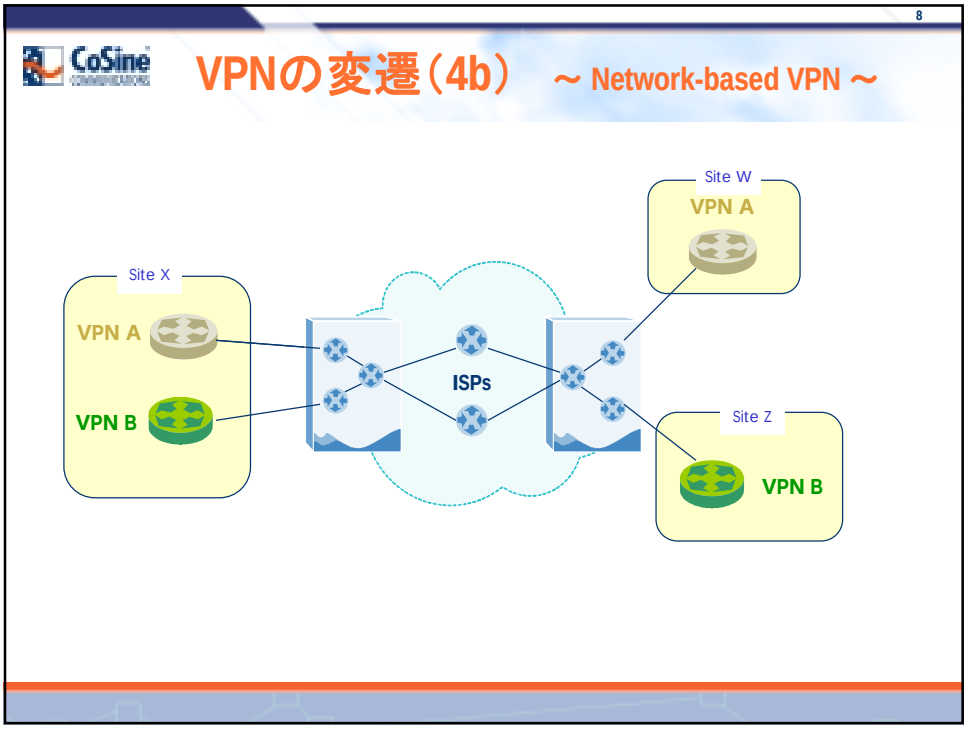


CoSine

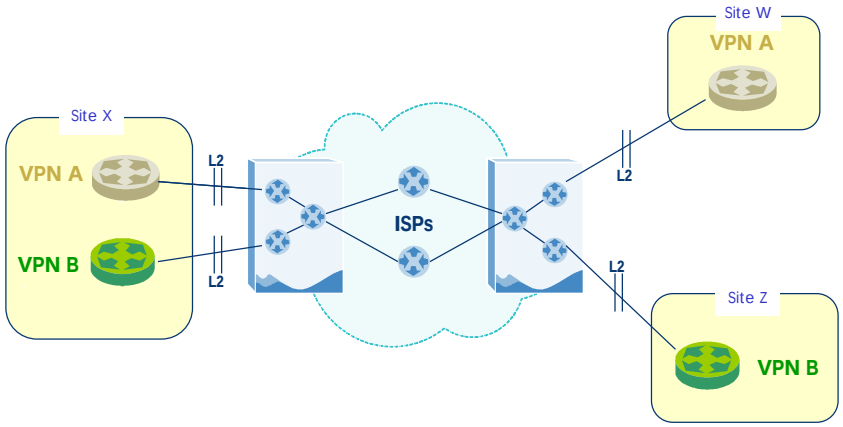
VPNの変遷（3） ～ Managed Router Solution ～




7
CoSine
VPNの変遷（4a）
～ Network-based VPN ～
Site W
VPN A
Site X
VPN A
VPN B
MPLS
Site Z
VPN B
VPN A
VPN B
Site Y


8
CoSine
VPNの変遷（4b）
～ Network-based VPN ～
Site W
VPN A
Site X
VPN A
VPN B
ISPs
Site Z
VPN B

VPNの変遷（4c） ～ Network-based VPN ～



IETF / ITUの活動

- **Network-based VPN (NBVPN)**
  - August 3, 2000 – 48th IETF @ Pittsburgh - NBVPN BOF (Routing Area)
- **Provider Provisioned VPN (PPVPN)**
  - December 14, 2000 – 49th IETF @ San Diego - PPVPN BOF (Routing Area)
  - March 23, 2001 – 50th IETF @ Minneapolis – PPVPN BOF/WG (Sub-IP Area)
  - August 8, 2001 – 51st IETF @ London – PPVPN WG
  - December 12, 2001 – 52nd IETF @ Salt Lake City – PPVPN WG
  - March 21, 2002 – 53rd IETF @ Minneapolis – PPVPN WG
  - Jul 16, 2002 – 54th IETF @ Yokohama – PPVPN WG
  - Nov 20, 2002 – 55th IETF @ Atlanta – PPVPN WG

11

CoSine

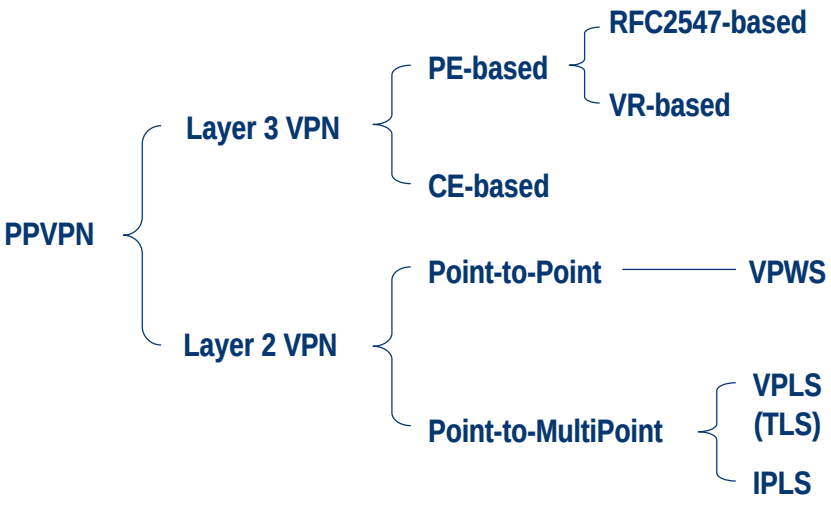
VPNの分類

- ベース
  - CPE-based
  - Network-based
- レイヤー
  - Layer 2
  - Layer 3
- モデル
  - Overlay model
  - Peer model
- Routing 方式
  - Per-VPN 方式
  - Aggregated Routing 方式
- アプリケーション
  - Virtual Leased Lines (VLL)
  - Virtual Private Routed Networks (VPRN)
  - Virtual Private Dial Networks (VPDN)
  - Virtual Private LAN Segments (VPLS)
- その他もろもろ

12

CoSine

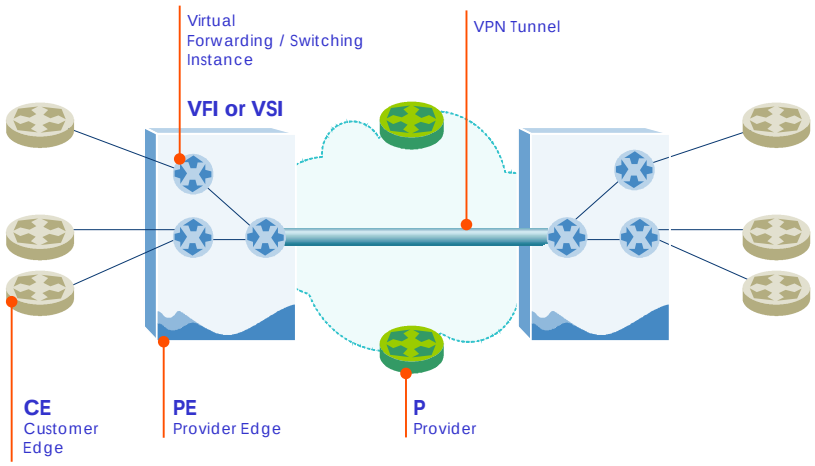
Provider Provisioned VPN の分類



13

CoSine

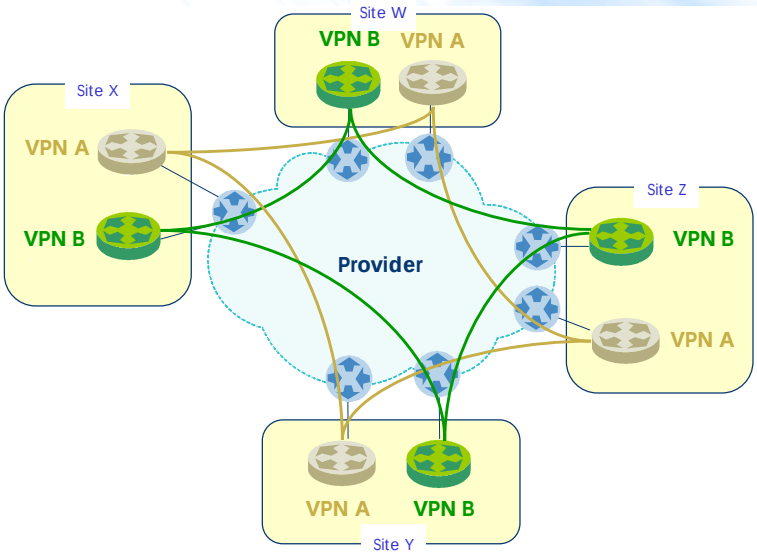
トポロジーと用語（L2 and L3）



14

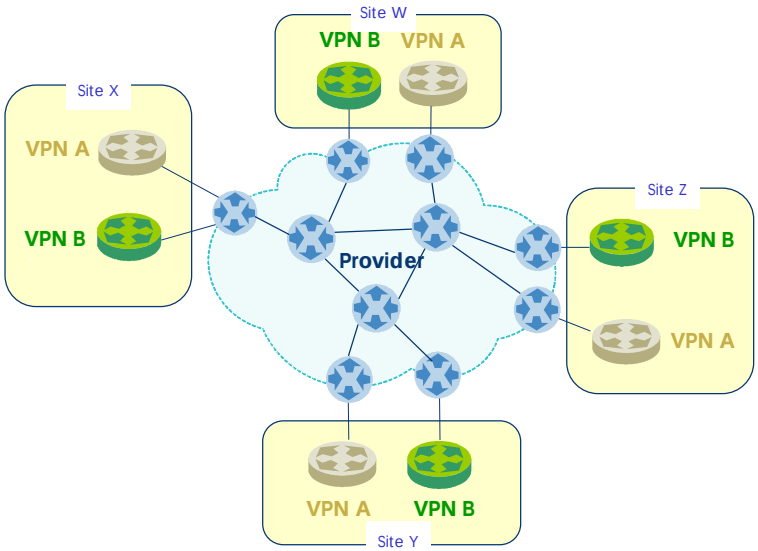
CoSine

Overlayモデル



15

Peerモデル



16

Network-based Layer 3 VPN

- ユーザからみるとルーターに見える
- Overlay model or Peer model
- 利点
  - N^2 問題の回避
  - ルーティングを“サービス”として提供できる
- 欠点
  - カスタマーネットワーク（特にルーティング）に関わる必要がある
  - プロトコルの限定（典型的にはIP only）

17

Network-based Layer 2 VPN

- ユーザからみると（巨大な）スイッチもしくはWireに見える
- 顧客の Layer 3（特にルーティング）に関与しない
- Overlay model
- 利点
  - 管理の分解点が明確
  - 既存のLayer 2ネットワークからの移行がスムーズ
  - 自然なルーティングの分離
  - Layer 3独立（マルチプロトコルのサポート）
  - マルチキャスト
- 欠点
  - N^2問題
  - 単一のLayer 2に縛られる

18

ケーススタディー

- BGP / MPLS VPN (RFC2547)
- L2 MPLS VPN (Martini)
- L2 MPLS VPN (Kompella)
- L2 MPLS VPN (Lasserre - V.Kompella)

19

MPLS/BGP VPN (RFC2547)

- RFC 2547 (Informational)
- draft-ietf-ppvpn-rfc2547bis-03.txt
- Layer 3 Network-based VPN
- Peerモデル
- MPLS (LSP)トンネル
- Aggregated Routing

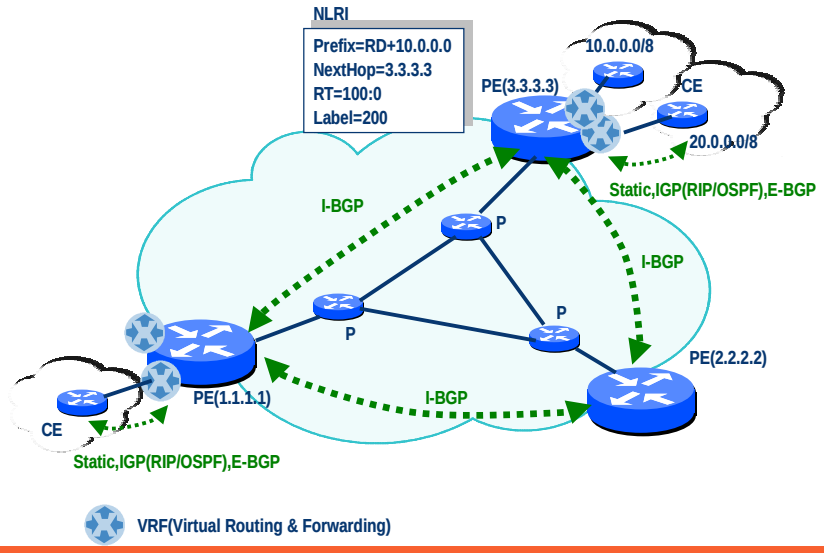
20

基本的な発想

- ルーティング情報の配布制御にBGP を使おう
  - スケールするし
  - Community で Filter するのがいいかも
    - でも、空間が足らないので Extended Community でencodeしよう！
- ルーティング情報を運ぶのにもBGPを使おう！
  - でも、アドレスは一意じゃないな～
    - VPN IP address = Route Distinguisher + IP address
  - そのままじゃ運べないよな～
    - マルチプロトコルなBGPを使おう！
- アドレスの重複はVRFで解決
- そのままじゃパケットを運べないので
  - MPLSを使おう
  - ラベルをスタックさせてスケールさせよう

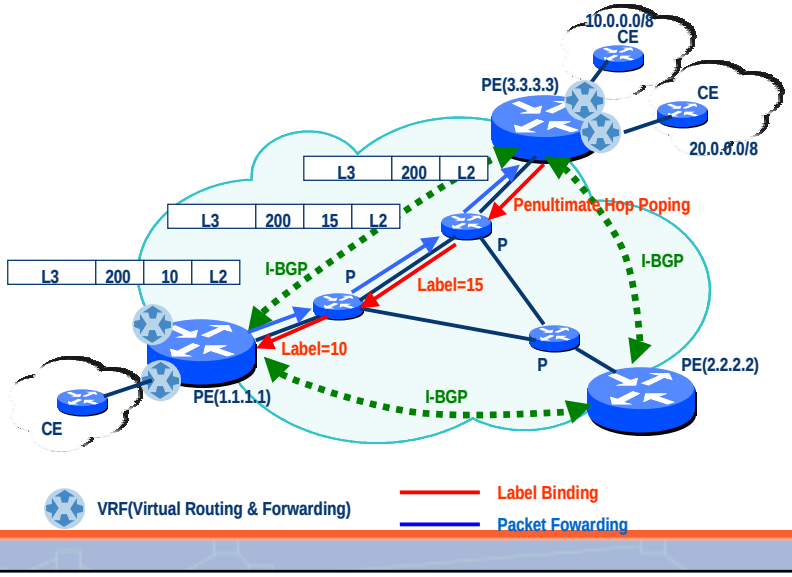
CoSine

RFC2547の動き（1）



CoSine

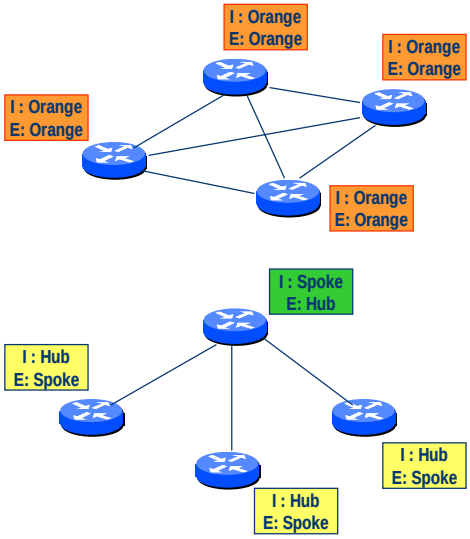
RFC2547の動き（2）



23

Topology Control in RFC2547

- BGPが持つ強力なポリシー機能を活用する
- Route Target（RT）
- Full Mesh
  - すべての PE で
    - Import : “Orange”
    - Export : “Orange”
- Hub & Spoke
  - Hub となる PE で
    - Import : “Spoke”
    - Export : “Hub”
  - Spoke となる PE で
    - Import : “Hub”
    - Export : “Spoke”



24

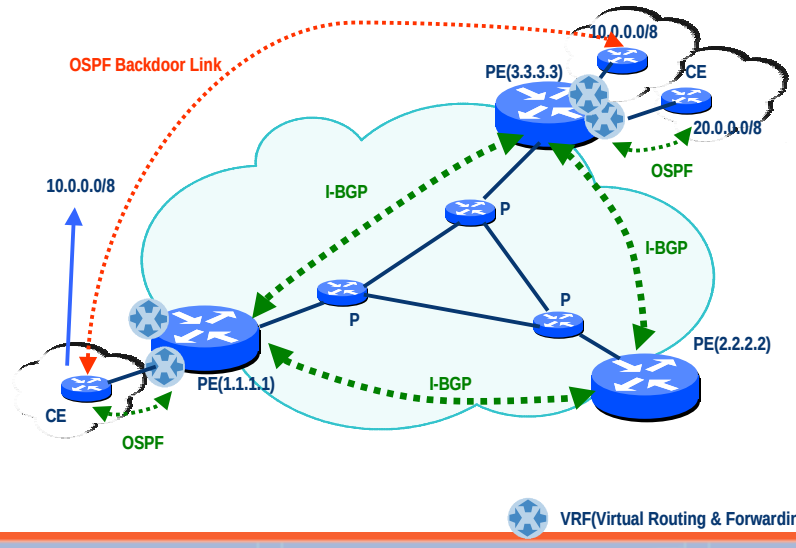
PE – CE routing in RFC2547

- PE (VRF) ～ CE間のルーティングプロトコルは自由に使うことができる
  - BGP-4 / RIP / OSPF / ISIS / Static, etc.
- ただし、
  - ループができやすいRIPなどは事故のもと
  - OSPF / ISIS のような Link State Protocol で、他サイトのルートは AS External なルートになってしまう
- 結局、現実的なのは Static か BGP-4 !!

25

CoSine

OSPF backdoor 問題 in RFC2547



26

CoSine

RFC2547方式の新規性

- どちらかというとBGPを使う点にある！
  - MPLSトンネル（LSP）の必然性無し
- じゃ、別のトンネル方式を使ってもいいんじゃない?
  - 例えば、IPsec や IP/GRE, L2TP 等
- draft-declercq-bgp-ipsec-vpn-01.txt (expired)
- draft-ietf-ppvpn-ipsec-2547-02.txt
- draft-ietf-ppvpn-gre-ip-2547-01.txt

27

CoSine

2547の明と暗

- VPN membership 管理に BGP を使っているのはかなりグー！
  - RTによる Topology Control なんて Beautiful !!
- でも、VPN Routing にまで BGP を使ったのはちょっと・・・。
- Peerモデルってそんなにいいの？
  - Aggregated Routing になるよね
  - CE-PE間ルーティング問題（OSPF Backdoor Link問題）
    - draft-rosen-vpns-ospf-bgp-mpls-05.txt なんてのもあるけどさ
  - 顧客にルーティングを“サービス”する（ルーティングのアウトソース）
    - 言葉を変えると、「顧客からルーティングの自由を奪う」
  - スケールするの？
    - Provisioning的にはすると思う
    - でも、PEがユーザの経路持たなくちゃいけないよね！
    - ユーザーの経路がフラップするかもしれないし
- モデル != 実装

28

CoSine

Layer 3 だけではユーザーの要求を満たせない！

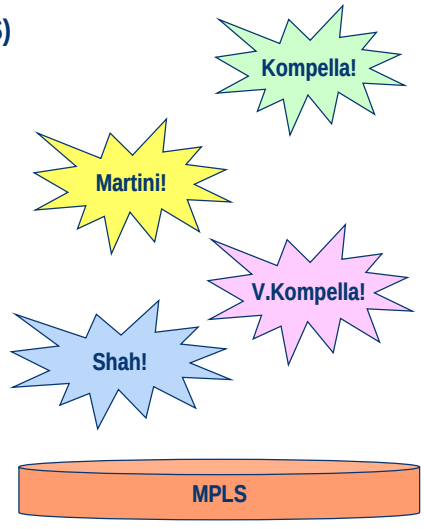
- アクセスラインの多様化と廉価化
  - DSL
  - Optical Ethernet (FTTH)
  - Metro Ethernet Service
- ルーティングの自由
- IPv6 やマルチキャスト
- マルチプトロコル性（IPX、AppleTalk）
- できるだけLayer 2 のセマンティックスを保ちたい
  - In-Order Delivery
  - Non address情報

Layer 2 Network-based VPN

- キャリア・ISP は Layer 3 に関与するのは止めよう！
- Layer 2 Network-based VPN
- Overlay モデル
- ユーザのルーティングには関与しない

Layer 2 VPN

- Virtual Private Wire Service (VPWS)
  - Martini 方式
  - Kompella 方式
- Virtual Private LAN Service (VPLS)
  - Lasserre-V.Kompella 方式
  - Kompella 方式
- IP over LAN Service (IPLS)
  - Shah 方式



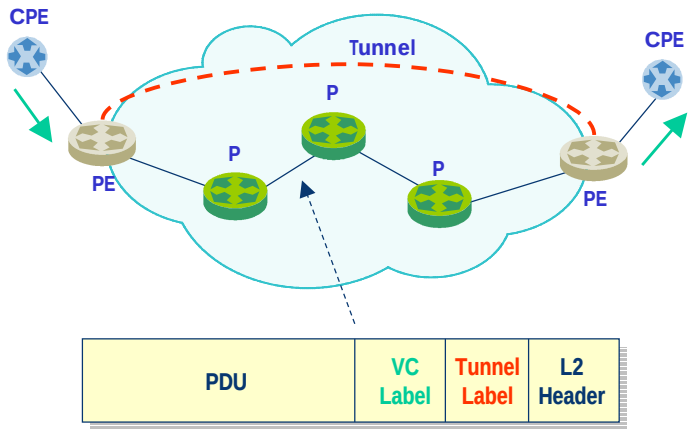
31

Martini 方式

- VPWS の一方式
- MPLS ベース
- Signaling は LDP
  - draft-martini-l2circuit-trans-mpls-10.txt
  - VC Label を配布するための方法を規定
- Encapsulation は Martini 方式
  - draft-martini-{atm,ethernet,frame,ppp-hdlc}-encap-mpls.txt
  - 各種 Layer 2 PDU の Encapsulation 方法を規定

32

Tunnel Label vs VC Label



CoSine

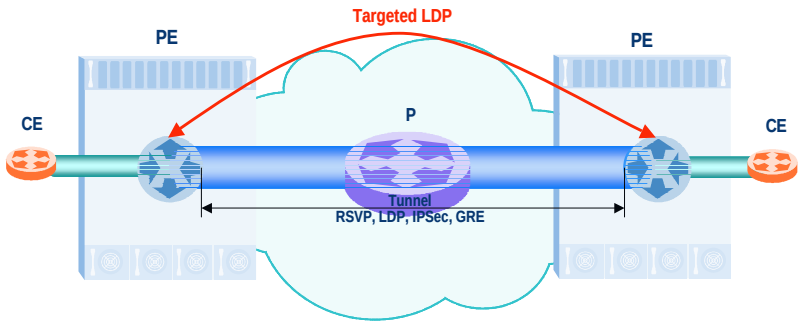
Martini シグナリング

- Point to Point 型
- LDPを利用する
  - Downstream Unsolicited Mode
  - Extended Discovery (Targeted HELLO)
  - VC FEC in Label Mapping Message

VC tlv	C	VC Type	VC info Length
Group ID			
VC ID			
Interface parameters : :			

CoSine

Targeted LDP



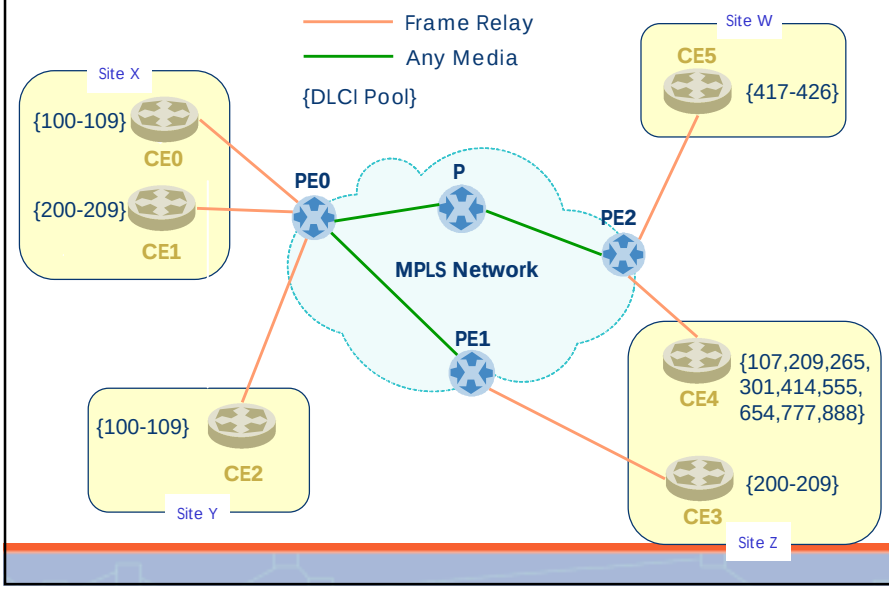
35

Kompella方式

- VPWS の一方式
- MPLS ベース
- Signaling は BGP
  - draft-kompella-ppvpn-l2vpn-02.txt
- Encapsulation は Martini ベース
- N^2 問題の軽減
  - Over Provisioning でProvisioningの負荷を軽減（半自動 Provisioning）
  - Layer 2 ID (DLCI, VPI/VCI) および Label は cheap である、という前提

36

Topology



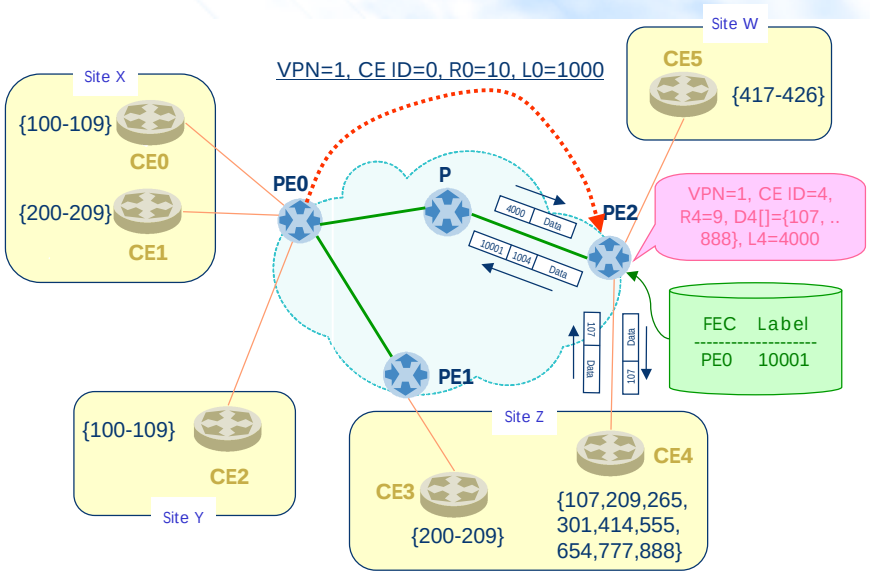
CoSine

設定

- VPN ID
- CE ID
- Range
- Label Base

CoSine

PE Advertisement



39

ポイント

- CE_a→CE_bなパケットを送る際にPE_kがinner labelとして割り当てたlabelは、PE_lがCE_a→CE_bなパケットを受け取る際のincomingなlabelとして割り当てたものと必ず等しくなる
- Layer2 ID（DLCI, VPI/VCI, etc.）とMPLS LabelのOver provisioningにより、CEの追加が発生しても、変更は局所的で済む（full mesh時でも）

40

Kompella シグナリング

- **Point-to-Multipoint 型**
  - リフレクターが使える！
- **BGP を使う**
  - Multiprotocol BGP
  - L2-VPNのためのAFIおよびSAFIを新たに導入
  - L2-VPNのためのNLRIを規定
  - Extended Community

41

CoSine

BGP NLRI for L2-VPN

Length (2 octets)
Route Distinguisher (8 octets)
CE ID (2 octets)
Label-block Offset (2 octets)
Label-base (3 octets)
Variable TLVs (0 to N octets) ….

42

CoSine

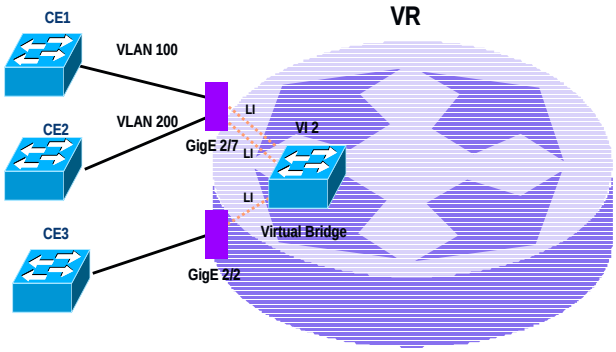
Martini (transport) vs (K.) Kompella

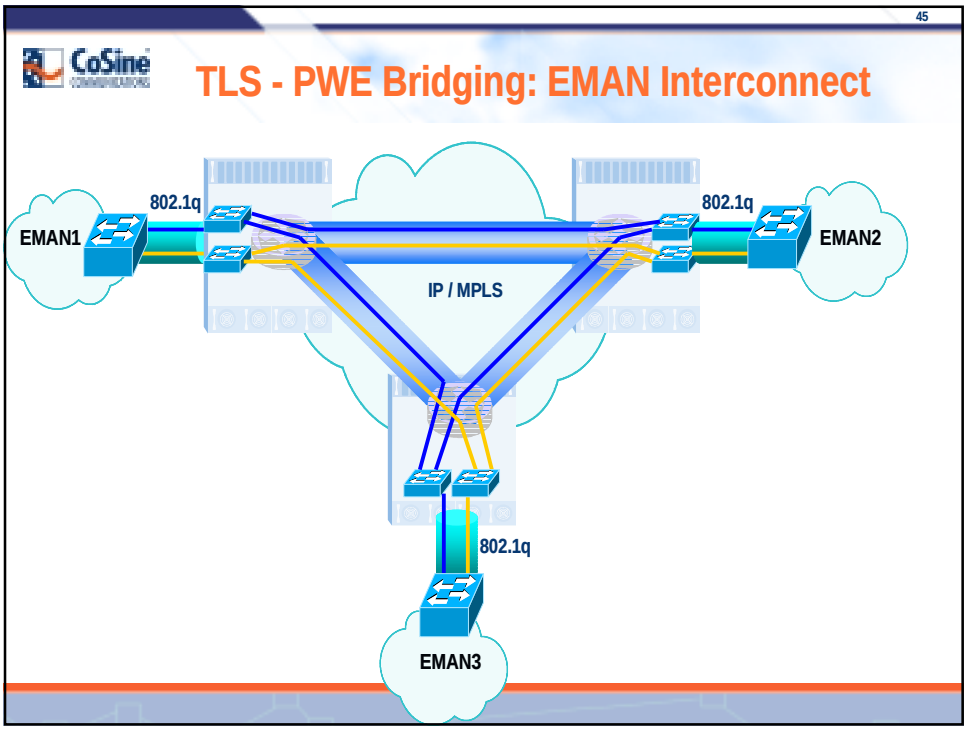
- **Point-to-Point Circuit を作る（Martini）なのか、VPN を作る（Kompella）なのかの違い？**
  - Full mesh はあまり必要がない？
- **Label Distribution Protocol として LDP を使う（Martini）か、BGP を使う（Komplla）かの違い？**
  - Auto Discovery は便利だよね
  - スケーラビリティーは？
  - 2547でBGPしてるなら、そのまま使えば？
- **現時点での実装の数は Martini のほうが多いが、なぜ？**
  - BGPの実装は難しいから？
  - パワーゲーム？？☺

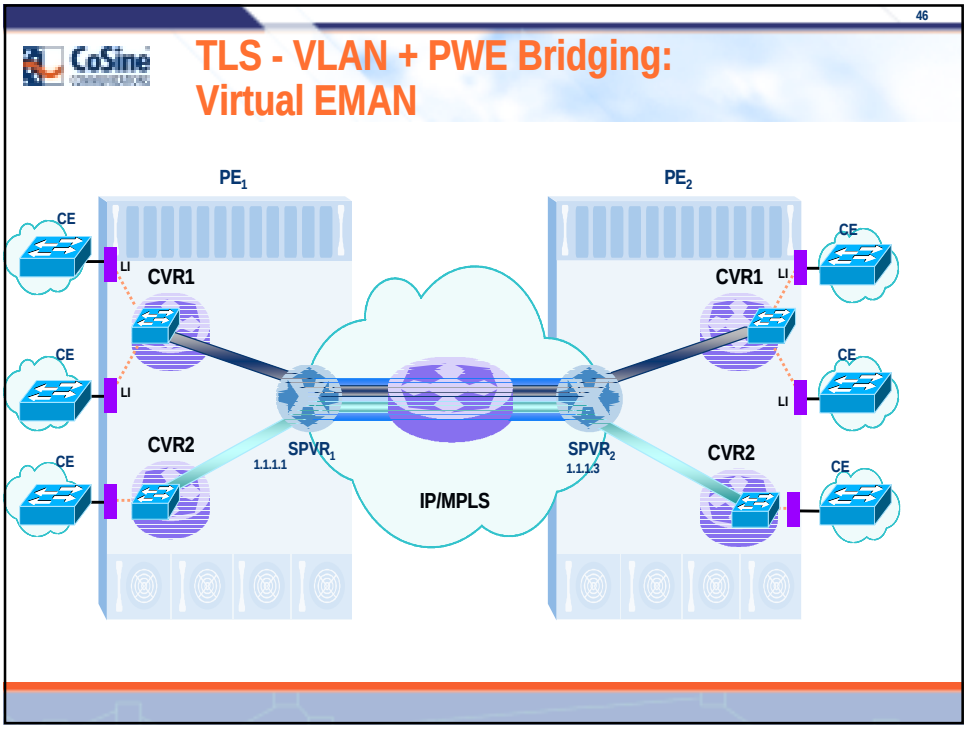
Lasserre-V.Kompella方式

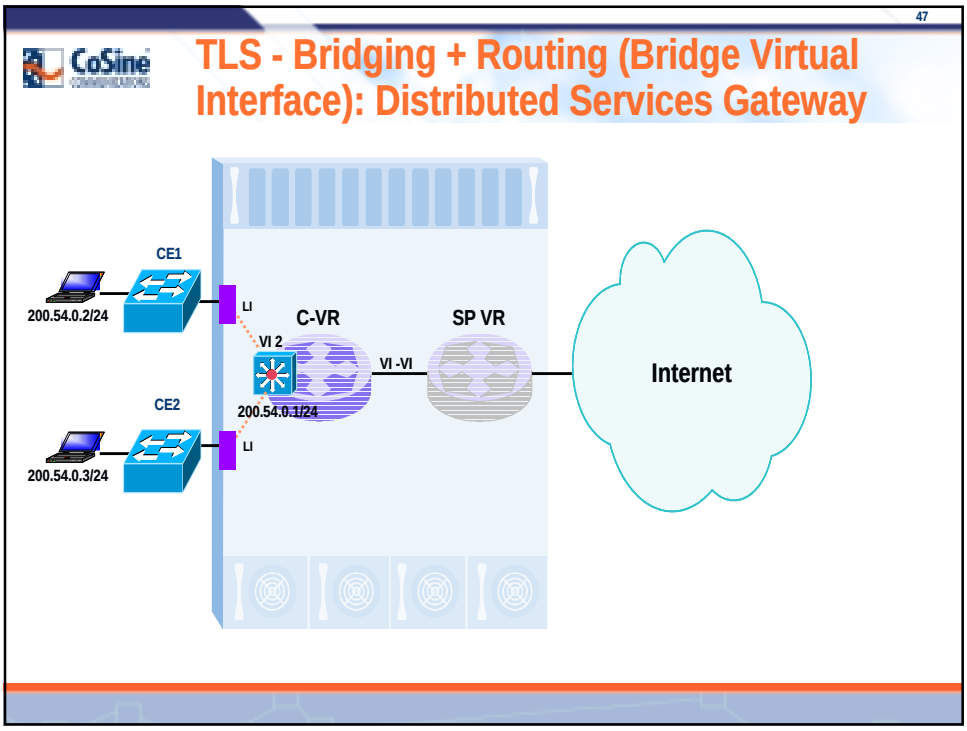
- VPLS の一方式
- MPLS ベース
- Signaling は LDP
  - Martini Signaling の拡張
  - draft-lasserre-vkompella-ppvpn-vpls-02.txt
- Encapsulation は Martini ベース
- Virtual Bridging (802.1D) による実現

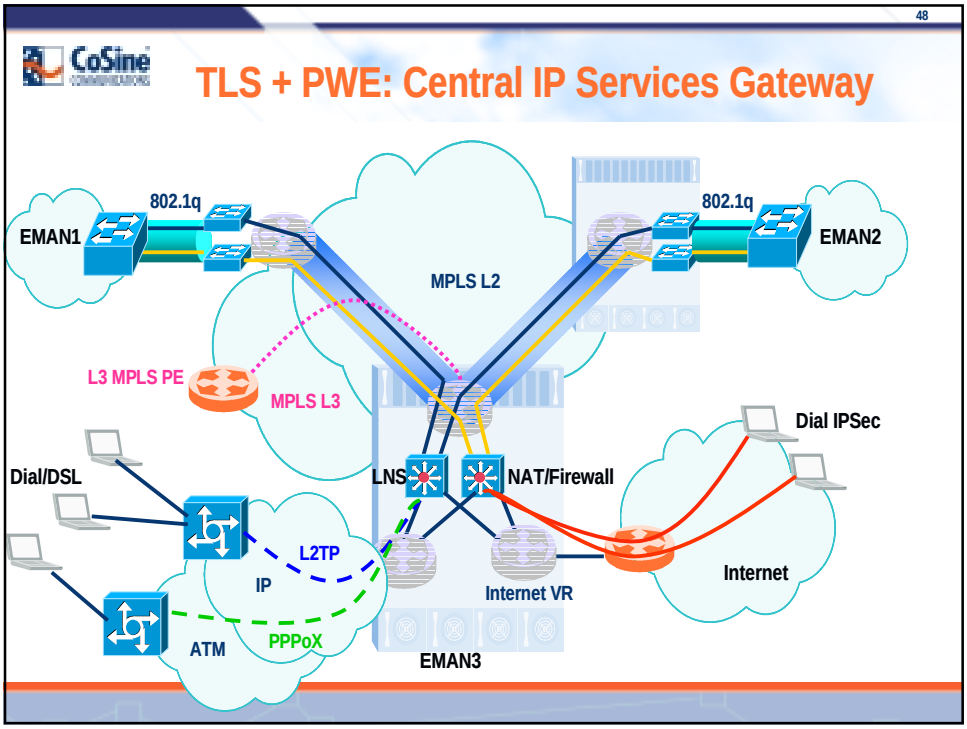
Virtual Bridge: Local Bridging




45
CoSine
TLS - PWE Bridging: EMAN Interconnect
802.1q
802.1q
EMAN1
EMAN2
IP / MPLS
802.1q
EMAN3


46
CoSine
TLS - VLAN + PWE Bridging:
Virtual EMAN
PE1
PE2
CE
CE
CE
CE
CE
CE
LI
LI
LI
LI
CVR1
CVR1
CVR2
CVR2
SPVR1
1.1.1.1
SPVR2
1.1.1.3
IP/MPLS


47
CoSine
TLS - Bridging + Routing (Bridge Virtual Interface): Distributed Services Gateway
CE1
200.54.0.2/24
LI
C-VR
SP VR
VI 2
VI -VI
Internet
200.54.0.1/24
CE2
200.54.0.3/24
LI


48
CoSine
TLS + PWE: Central IP Services Gateway
802.1q
EMAN1
802.1q
EMAN2
MPLS L2
L3 MPLS PE
MPLS L3
Dial IPSec
Dial/DSL
LNS
NAT/Firewall
L2TP
IP
Internet
Internet VR
ATM
PPPoX
EMAN3

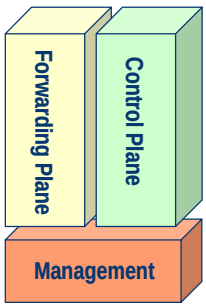
別に MPLS じゃなくても・・・

- 要は PE 間を結ぶ Wire があればいいんでしょ！
- じゃ、作りましょ！

Pseudo Wire Emulation Edge to Edge (PWE3)

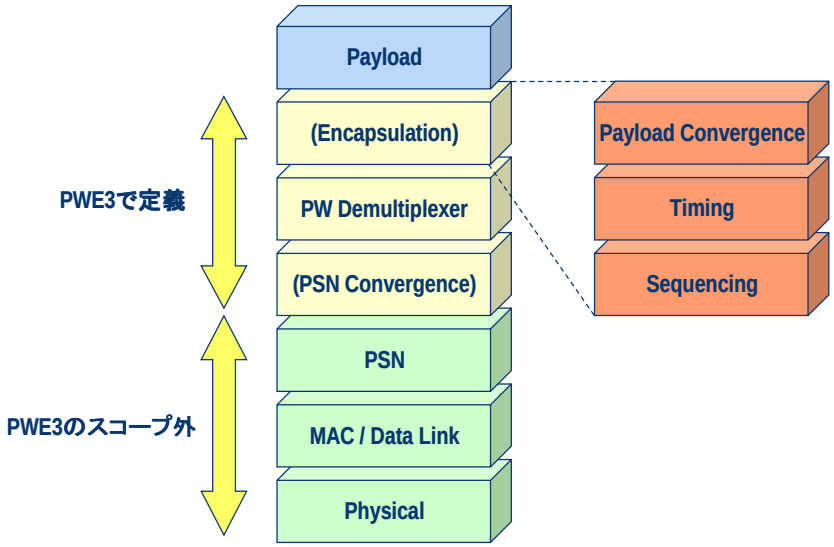
Scope of PWE3

- **Forwarding Plane**
  - 各種サービスのEncapsulation
  - フレームの順序性の保証
  - Segmentation & Reassembly
- **Control Plane**
  - PWの確立と解除のためのシグナリング
  - Status Monitoring & Notification
  - Keepalive
  - クロックの回復
- **Management**
  - MIB
  - Traceroute



CoSine

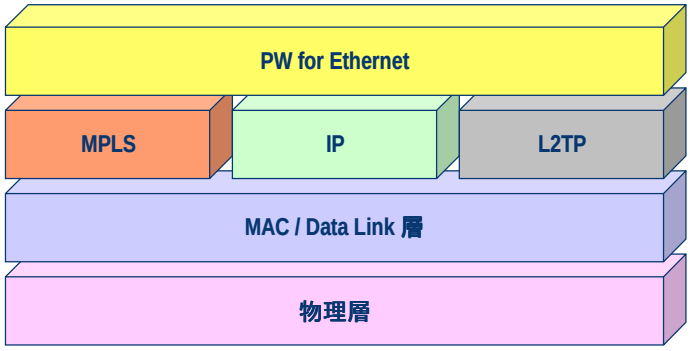
PWE3 Layering



CoSine

PWE3 for Ethernet

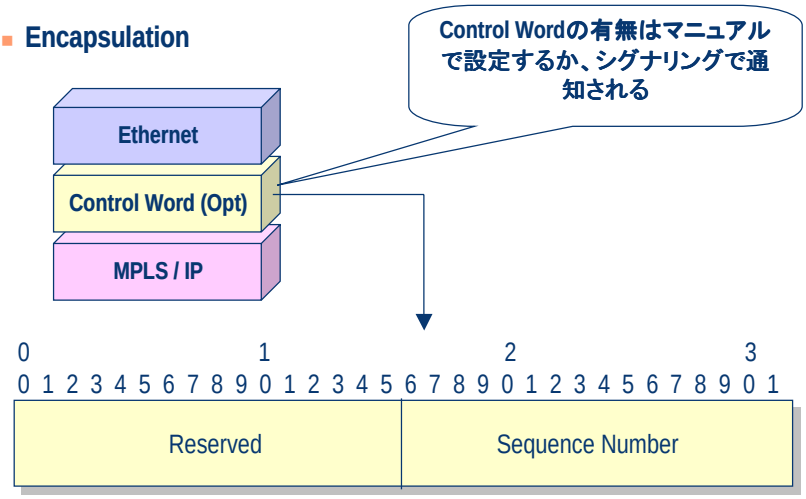
- draft-ietf-pwe3-ethernet-encap-01.txt (for MPLS and IP)
- draft-ietf-l2tpext-pwe3-ethernet-00.txt (for L2TP)



53

PWE3 for Ethernet over MPLS / IP

- Encapsulation



54

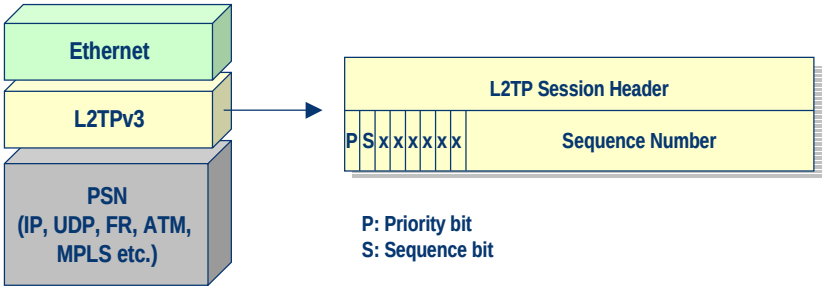
PSNシグナリングとしてのL2TP

- L2TPv3
  - draft-ietf-l2tpext-l2tp-base-04.txt
- L2TPv2 vs L2TPv3
  - 相互運用や実装経験から得られた不明確な点の明確化
  - PPPからの独立
  - Session ID と Tunnel ID の 32bit 化
  - Pseudo Wire 対応
    - Pseudo Wire Type (ICRQ, OCRQ)
    - Pseudo Wire Capabilities List (SCCRQ, SCCRP)
    - Pseudo Wire Control Encapsulation (ICRQ, ICRP, ICCN, OCRQ, OCRP, OCCN)

55

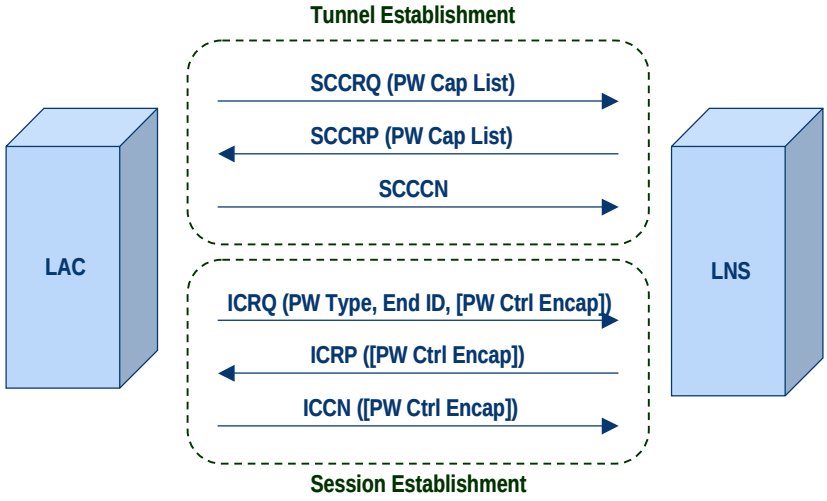
PWE3 for Ethernet over L2TP

- Pseudo Wire Type = “Ethernet port” or “Ethernet VLAN”
- End Identifier AVP を PW ID として使う
- Pseudo Wire Control Encapsulation



56

PW establishment by L2TP



57

CoSine

その他のPW Type

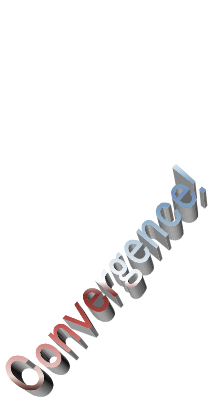
- SONET / SDH
  - draft-ietf-pwe3-sonet-00.txt
- TDM Circuit
  - draft-ietf-pwe3-sonet-vt-00.txt
- ATM (cell & frame)
  - draft-ietf-pwe3-atm-encap-00.txt
- Frame Relay
  - draft-ietf-pwe3-frame-relay-01.txt

58

CoSine

PWのメリット

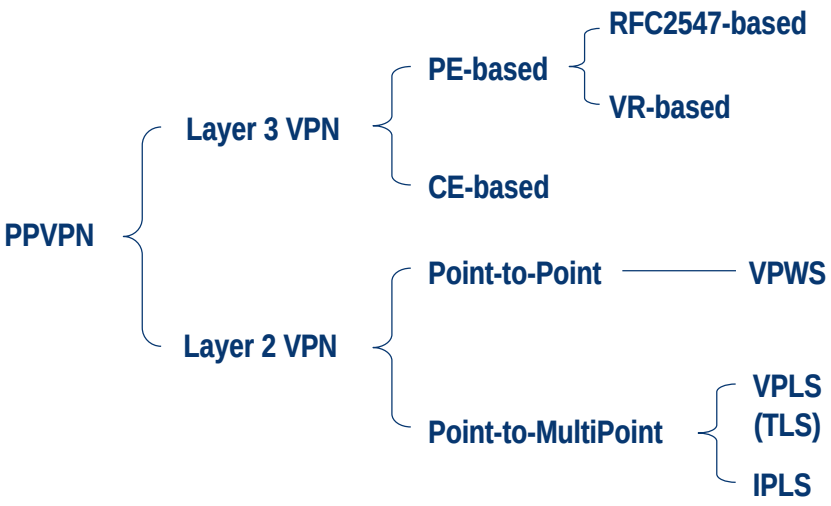
- コンバージェンス!!
- 「安い」ネットワーク
- L2 VPN の加速化



59

CoSine

おさらい



60

CoSine

まとめ

- IP-VPN != RFC2547
  - Non-MPLS 2547-based VPN
  - L2-based VPN
  - …
- VPN の Building Block は十分（過ぎるくらい）出揃った
- 基本的にユーザーは「わがまま」
  - 安く
  - 自由に
  - スケールして
  - なんでもできる
- サービスプロバイダはこのわがままに応えなければ生き残れない！

61

参考資料 (1)

- RFC 2547 (BGP/MPLS VPN)
- RFC 2661 (L2TP)
- RFC 2764 (IP VPN Framework)
- RFC 3036 (LDP)
- draft-ietf-ppvpn-rfc2547bis-03.txt
- draft-declercq-bgp-ipsec-vpn-01.txt (expired)
- draft-ietf-ppvpn-ipsec-2547-02.txt
- draft-ietf-ppvpn-gre-ip-2547-01.txt
- draft-rosen-vpns-ospf-bgp-mpls-05.txt
- draft-martini-l2circuit-trans-mpls-10.txt
- draft-martini-{atm,ethernet,frame,ppp-hdlc}-encap-mpls-nn.txt

62

参考資料 (2)

- draft-kompella-ppvpn-l2vpn-02.txt
- draft-lasserre-vkompella-ppvpn-vpls-02.txt
- draft-ietf-pwe3-ethernet-encap-01.txt
- draft-ietf-l2tpext-pwe3-ethernet-00.txt
- draft-ietf-l2tpext-l2tp-base-04.txt
- draft-ietf-pwe3-sonet-00.txt
- draft-ietf-pwe3-sonet-vt-00.txt
- draft-ietf-pwe3-atm-encap-00.txt
- draft-ietf-pwe3-frame-relay-01.txt