MPLS L2/L3
Virtual Private Networks (VPNs)

An MFA Forum Sponsored Tutorial

Dave Christophe
MFA Forum Education WG Chair
Global Programs
Alcatel-Lucent

MPLS VPN Tutorial Agenda

- Introduction to the MFA Forum
- Introduction to MPLS and MPLS VPNs
  - Defining Layer 2 and 3 VPNs
- Layer 3 MPLS VPN
  - Overview
  - BGP Review
  - RFC 4364 (2547bis) Key Characteristics
  - BGP/MPLS VPN Architecture Overview
    - VPN Routing and Forwarding (VRF) Tables
    - Overlapping VPNs
    - VPN Route Distribution
    - VPN Packet Forwarding
    - Scaling L3 VPNs and Route Reflectors

MPLS VPN Tutorial Agenda

- Layer 2 VPNs
  - Overview
  - Encapsulation and Label Stacking
  - Virtual Private Wire Services – VPWS
    - Pt-to-pt Ethernet, Pt-to-pt ATM, Pt-to-pt Frame Relay
  - Virtual Private LAN Services – VPLS
- Introduction to Multi-Service Interworking over MPLS
  - Interworking History and Definition
  - Multi-Service Interworking of Ethernet over MPLS
  - Migration Scenarios and Benefits

Introduction to the MFA Forum

Mission Statement

The MFA Forum is an international, industry-wide, nonprofit association of telecommunications, networking, and other companies focused on advancing the deployment of multi-vendor, multi-service packet-based networks, associated applications, and interworking solutions.

MFA Forum

- Formed in July 2005 by merging the ATM Forum and the MPLS & Frame Relay Alliance
- 38 member companies
- Three primary committees
  - Technical Committee
    - Applications and Deployment Working Group
    - Architecture Working Group
    - ATM Control Signaling Working Group
    - Interoperability Working Group
    - Interworking and Frame Relay Working Group
  - Marketing Awareness and Education Committee
  - Service Provider Council
- MPLS User Group – Enterprises, Carriers

Technical Committee Major Work Items

- MPLS Inter-Carrier Interface
- Packet-Based GMPLS Client to Network Interconnect (CNI)
- Performance Monitoring Across Multi-service Networks
- Layer 2 Service Mediation
- AAL1 and AAL2 Voice Trunking over MPLS
- ATM to PWE3 SPVC Interworking – unmapped mode
- MPLS in Mobile Networks

MFA Forum

- Market Awareness & Education
  - Tutorials

Introduction to MPLS	½ day and full day
MPLS Virtual Private Networks	½ day
MPLS VPN Security	½ day
Traffic Engineering	½ day
GMPLS	½ day
Migrating Legacy Services to MPLS	½ day
MPLS OAM	½ day
Voice over MPLS	½ day
Multi-service Interworking over MPLS	½ day
Multicast in MPLS/VPLS Networks	½ day
New tutorials based upon demand	

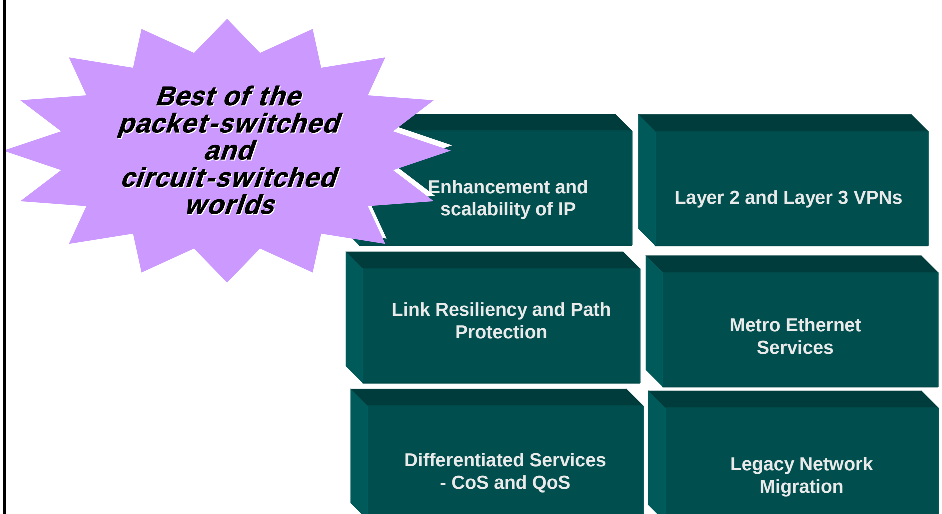
  - Conferences and exhibitions - MFA Forum speaker at almost every MPLS conference globally
  - Website, Newsletter and Public message board
- Next meeting: July 17-19 in San Jose, California
- Please join us!
  - Subscribe to information mail list info@mfaforum.org
  - To join the Forum contact Alexa Morris, Executive Director
    E-Mail: amorris@mfaforum.org Phone: 510 608-5914

Section 1

Introduction to MPLS and MPLS VPNs

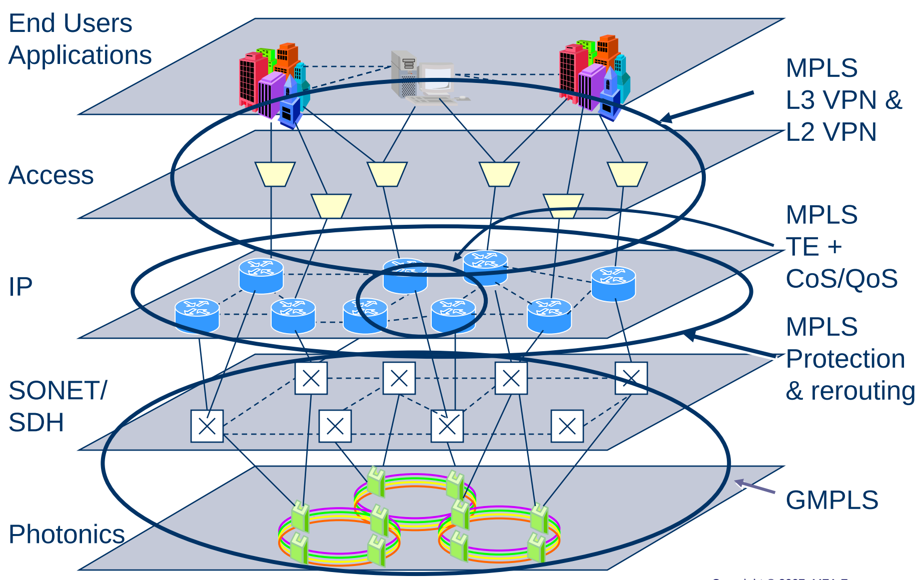
Why MPLS ?

A Common Control Plane



MPLS: Addresses many network needs

MFA FORUM

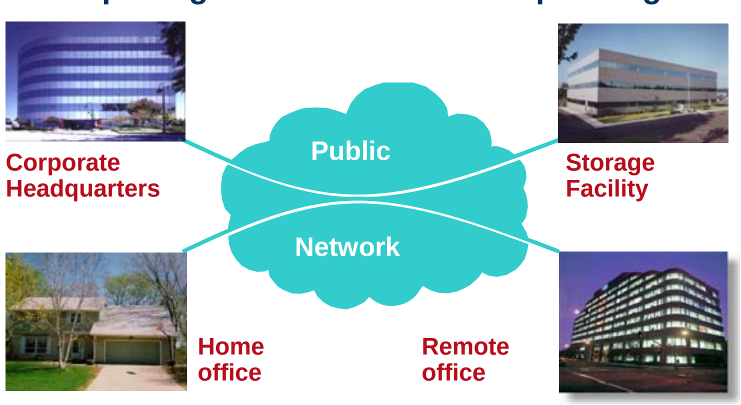


Slide 11

Virtual Private Networks

MFA FORUM

- Provide private line and private LAN connections between multiple sites
- Leverage public network to provide competitive service pricing and reduce service operating cost



Slide 12

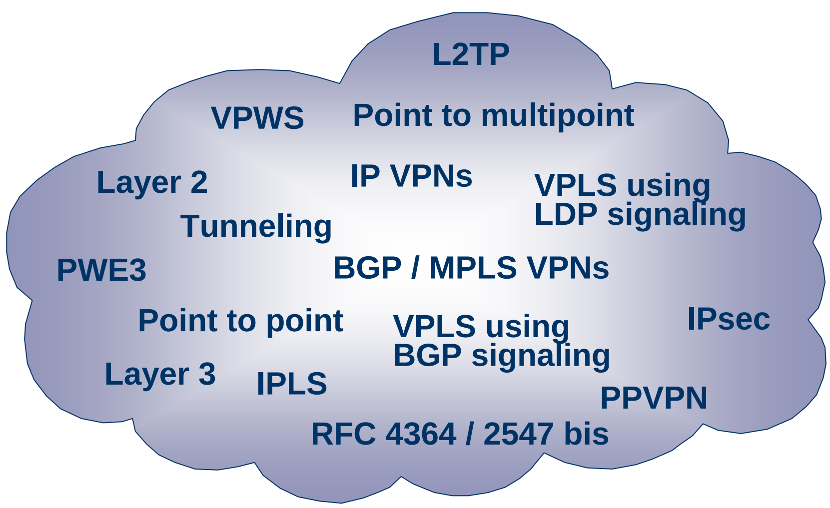
Virtual Private Networks

- VPN (Virtual Private Network) is simply a way of using a public network for private communications, among a set of users and/or sites
- Remote Access: Most common form of VPN is dial-up remote access to corporate database - for example, road warriors connecting from laptops
- Site-to-Site: Connecting two local networks (may be with authentication and encryption) - for example, a Service Provider connecting two sites of the same company over its shared network

Slide 13

MPLS, VPNs, and Standards

Many options



Slide 14

VPNs
Types, Layers, and Implementations

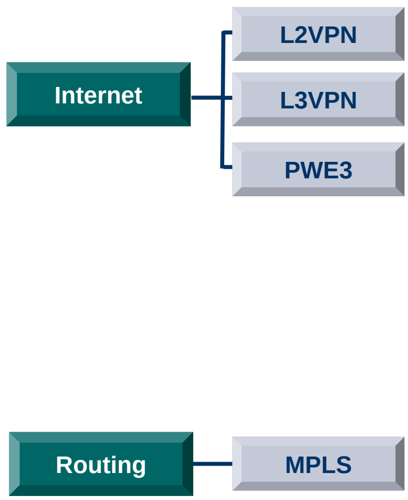
VPN Type	Layer	Implementation
Leased Line	1	TDM/SDH/SONET
Frame Relay	2	DLCI
ATM	2	VC
GRE/UTI/L2TPv3	3	IP Tunnel
Ethernet	2	VLAN / VPWS / VPLS
IP	3	RFC 4364 / VR
IP	3	IPsec

VPNs
How do they compare?

	FR or ATM	IPsec	L3 MPLS	L2 MPLS
Point-to-multipoint	×	×	√	√
Multi-protocol	√	×	×	√
QoS and CoS	√	×	√	√
Low latency	√	×	√	√
Security	√	√	√	√
SLAs	√	×	√	√

MPLS VPNs in the IETF

MFA FORUM



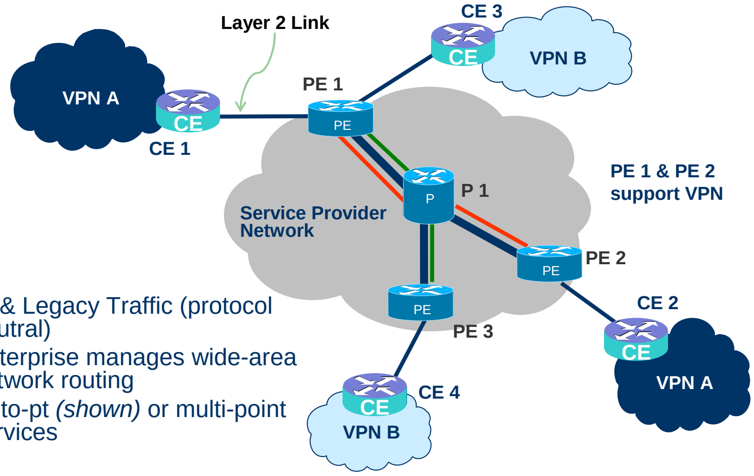
- Layer 2 VPNs
- Layer 3 VPNs
- Pt-to-Pt circuits
- Encapsulations
  - ATM
  - FR
  - Ethernet
  - PPP/HDLC
  - TDM
  - SONET/SDH
- Base Technology

What are Layer 2 and Layer 3 VPNs?

MFA FORUM

- VPNs based on a Layer 2 (Data Link Layer) technology and managed at that layer are defined as Layer 2 VPNs (MPLS, ATM, Frame Relay)
- VPNs based on tunneling at Layer 3 (Network Layer) are Layer 3 VPNs, (BGP/MPLS, VR, IPSec)

Visually - Layer 2 VPN



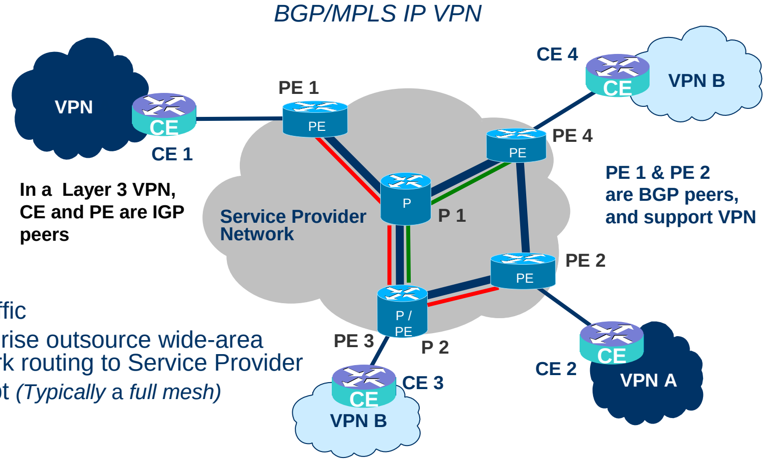
- IP & Legacy Traffic (protocol neutral)
- Enterprise manages wide-area network routing
- Pt-to-pt *(shown)* or multi-point services

CE: Customer Edge device
PE: Provider Edge router
P: Provider router not directly attached to a CE

VPN A (red line)
VPN B (green line)

Visually - Layer 3 VPN

BGP/MPLS IP VPN



In a Layer 3 VPN, CE and PE are IGP peers

- IP Traffic
- Enterprise outsource wide-area network routing to Service Provider
- Pt-to-pt *(Typically a full mesh)*

CE: Customer Edge device
PE: Provider Edge router
P: Provider router not directly attached to a CE

VPN A (red line)
VPN B (green line)

Section 2

Layer 3 MPLS VPN

Slide 21

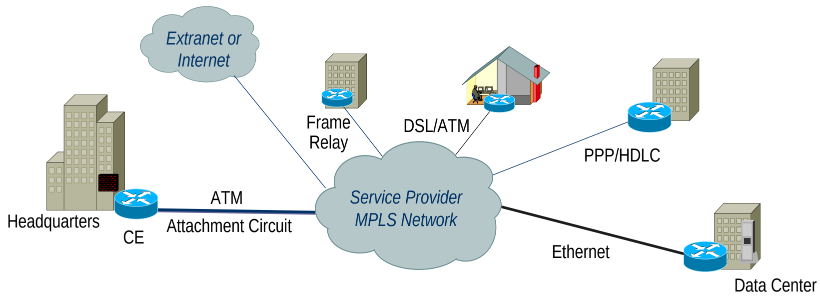
MPLS VPN Tutorial Agenda

Layer 3 MPLS VPN

- Overview
- BGP Review
- RFC 4364 / 2547bis Key Characteristics
- BGP/MPLS VPN Architecture Overview
  - VPN Routing and Forwarding (VRF) Tables
  - Overlapping VPNs
  - VPN Route Distribution
  - VPN Packet Forwarding
  - Scaling L3 VPNs and Route Reflectors

Slide 22

Layer 3 (BGP/MPLS) VPN Overview



- Cost effective full mesh connectivity between sites
- Utilize multiple VPNs at a site with different routes to control access
- Facilitates communications in dynamic organization & business application environments
- Leverages existing access options to preserve investment and effectively support a range of applications

What is BGP?

- BGP is an exterior gateway protocol that allows IP routers to exchange network reachability information
- BGP published as RFC 1105 in 1989, then after several updates as BGP-4 in 1995 with RFC 1771, and now as RFC 4271 (2006)
- Numerous other RFCs and Internet Drafts focus on various aspects and extensions including multi-protocol extensions, extended communities, carrying label information in BGP, etc

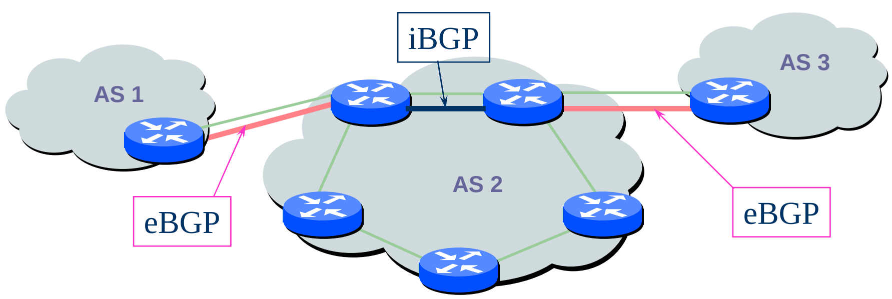
IGP vs. EGP

- Interior Gateway Protocols
  - RIP, OSPF, IS-IS
  - Dynamic, some more than others
  - Define the routing needed to pass data ***within*** a network
- Exterior Gateway Protocol
  - BGP
  - Less Dynamic than IGPs
  - Defines the routing needed to pass data ***between*** networks

Slide 25

Internal Border Gateway Protocol

iBGP - **BGP between border routers in the same AS.**



Provides a consistent view within the AS of the routes exterior to the AS.

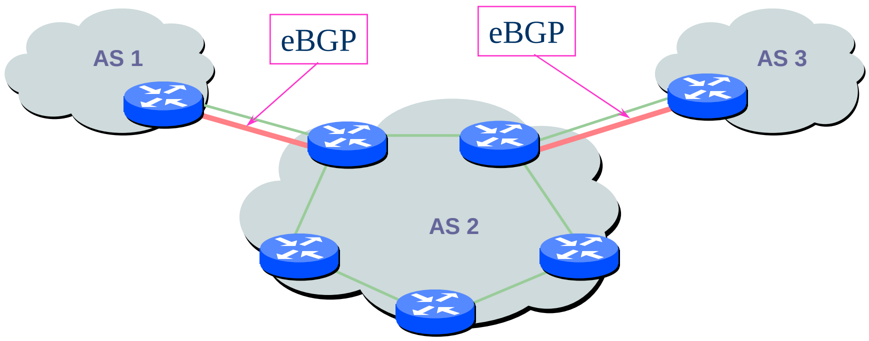
AS: Autonomous System
eBGP: External BGP
iBGP: Internal BGP

Slide 26

External Border Gateway Protocol

MFA FORUM

eBGP - **BGP between border routers in two different AS's.**

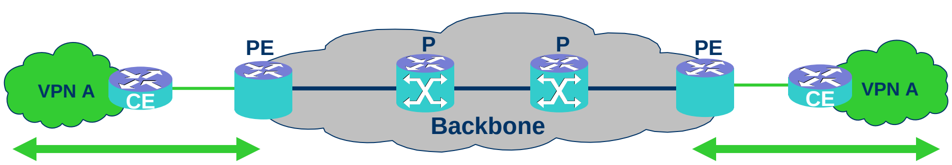


Slide 27

BGP/MPLS IP VPN (RFC 4364)

Key Characteristics

MFA FORUM



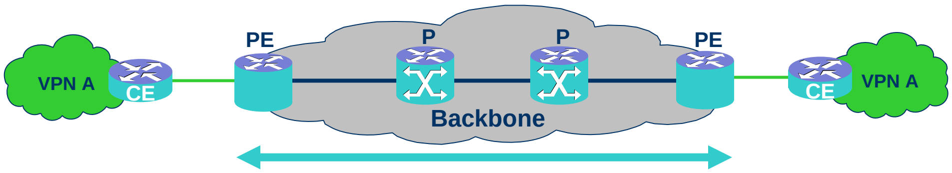
- **Requirements:**
  - **Support for overlapping, private IP address space**
  - **Different customers run different IGPs (i.e. RIP, OSPF, IS-IS)**
- **Solution:**
  - **VPN network layer is terminated at the edge (PE)**
    - **PE routers use plain IP with CE routers**

CE: Customer Edge router
PE: Provider Edge router
P: Provider router not directly attached to a CE

Slide 28

BGP/MPLS IP VPN
Key Characteristics

MFA FORUM

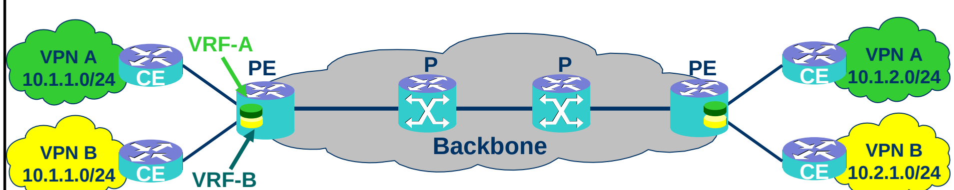


- P routers (LSRs) are in the core of the MPLS cloud
- P and PE (LERs) routers run an IGP and a label distribution protocol
  - Labelled VPN packets are transported over MPLS core
- PE routers are MP-iBGP fully meshed
  - for dissemination of VPN membership and reachability information between PEs

Slide 29

Virtual Routing and Forwarding (VRF) Tables

MFA FORUM

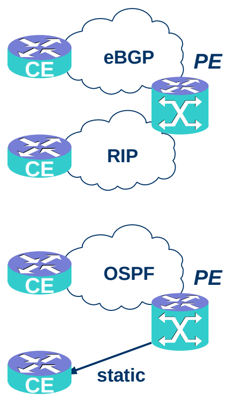


- Each VPN needs a separate <u>Virtual routing and forwarding instance (VRF)</u> in each PE router to
  - Provides VPN isolation
  - Allows overlapping, private IP address space by different organizations

Slide 30

Virtual Routing and Forwarding (VRF) *PE to CE Router Connectivity*

MFA FORUM

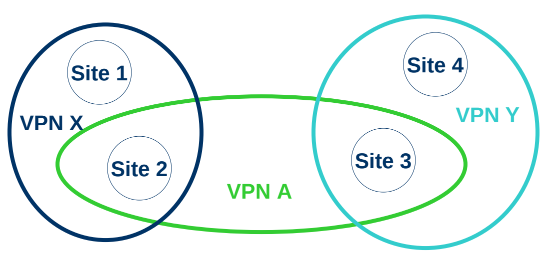


- Protocols used between CE and PE routers to populate VRFs with customer routes
  - BGP-4
    - Useful in stub VPNs and transit VPNs
  - RIPv2
  - OSPF
  - Static routing
    - Particularly useful in stub VPNs
- Note:
  - Customer routes need to be advertised between PE routers
  - Customer routes are not leaked into backbone IGP

Slide 31

Virtual Routing and Forwarding (VRF) *Overlapping VPNs*

MFA FORUM



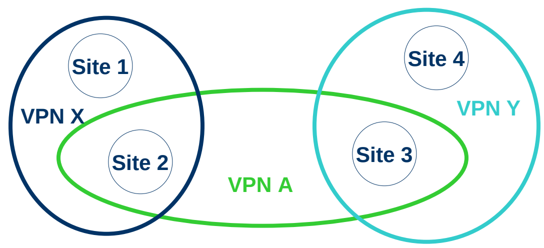
Examples:
- Extranet
- VoIP Gateway

- A VPN is a collection of <u>sites</u> sharing a common routing information (routing table)
- A VPN can be viewed as a community of interest (or Closed User Group)

Slide 32

Virtual Routing and Forwarding (VRF) *Overlapping VPNs (continued)*

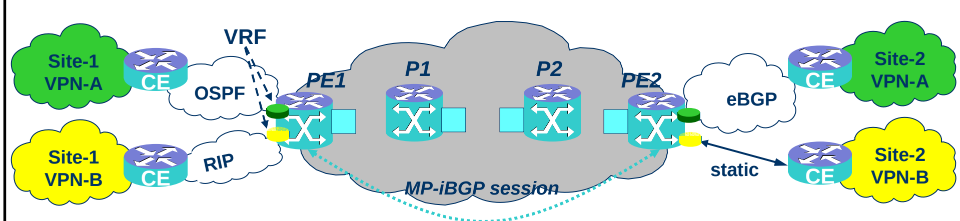
MFA FORUM



- A site can be part of different VPNs
- A site belonging to different VPNs *may* or *may not* be used as a transit point between VPNs
- If two or more VPNs have a common site, address space must be unique among these VPNs

VRFs and Route Distribution

MFA FORUM

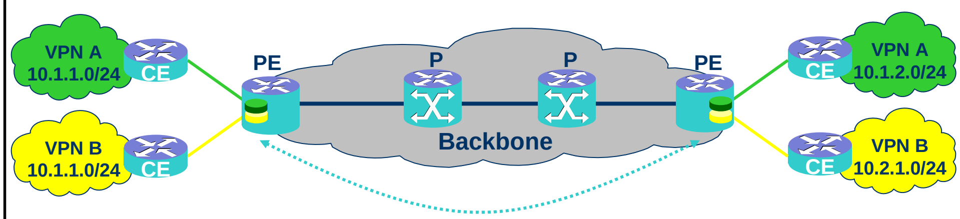


- Multiple VRFs are used on PE routers
- The PE learns customer routes from attached CEs
- Customer routes are distributed to other PEs with MP-BGP
- Different IGPs or eBGP supported between PE and CE peers
- Default forwarding table also exists – public routes

VRF: VPN Routing and Forwarding Table

VPN Route Distribution
Route Targets

MFA FORUM

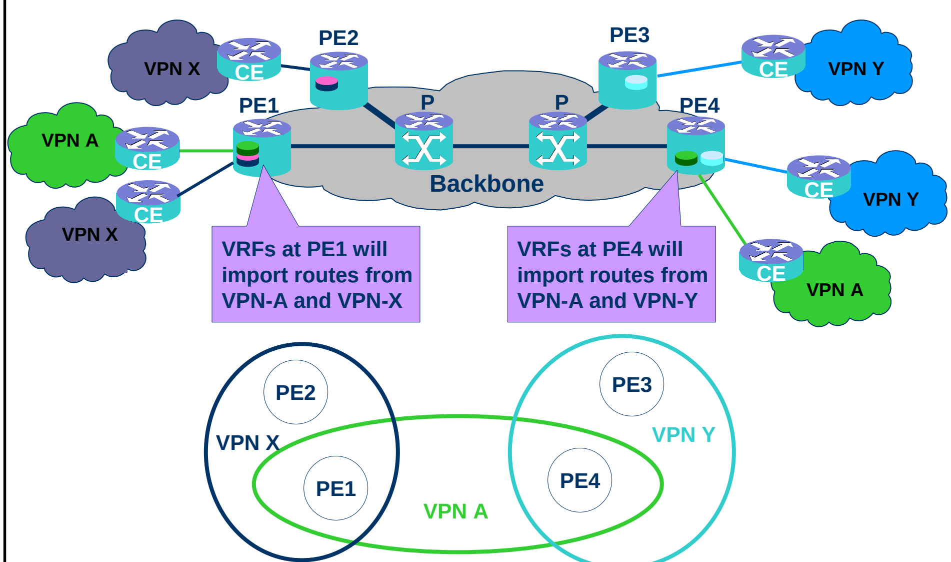


Route Target attributes:

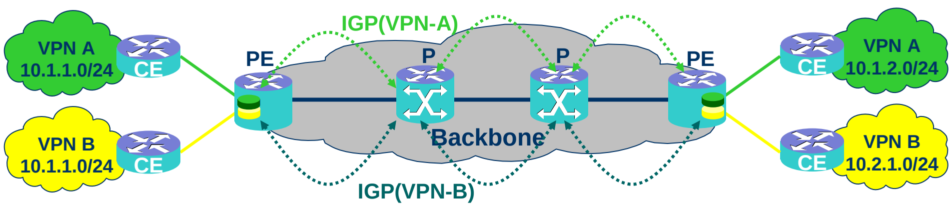
- **"Export" Route Target**: Every VPN route is tagged with one or more route targets when it is exported from a VRF (to be offered to other VRFs)
- **"Import" Route Target**: A set of routes targets can be associated with a VRF, and all routes tagged with at least one of those route targets will be inserted into the VRF

VPN Route Distribution
Route Targets

MFA FORUM



VPN Route Distribution

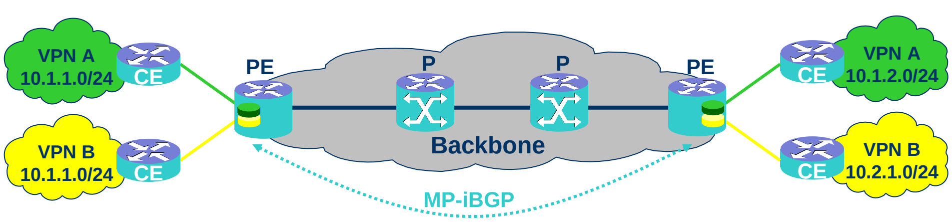


How will the PE routers exchange information about VPN customers and VPN routes between themselves?

Option #1: PE routers run a different routing algorithm for each VPN

- Scalability problems in networks with a large number of VPNs
- Difficult to support overlapping VPNs

VPN Route Distribution



How will the PE routers exchange information about VPN customers and VPN routes between themselves?

Option #2: BGP/MPLS IP VPN - PE routers run a single routing protocol to exchange all VPN routes

- Problem: Non-unique IP addresses of VPN customers. BGP always propagates one route per destination not allowing address overlap.

VPN Route Distribution
VPN-IPv4 Addresses

MFA FORUM

- **VPN-IPv4 Address**
  - **VPN-IPv4 is a globally unique, 96bit routing prefix**

Route Distinguisher (RD)	IPv4 Address
64 bits Creates a VPN-IPv4 address that is globally unique, RD is configured in the PE for each VRF, RD may or may not be related to a site or a VPN	32 bits IP subnets advertised by the CE routers to the PE routers

Slide 39

VPN Route Distribution
VPN-IPv4 Addresses

MFA FORUM

Route Distinguisher format

00	00	ASN	nn

- **ASN:nn**
  - **Autonomous System Number (ASN) assigned by Internet Assigned Number Authority (IANA)**

00	01	IP address	nn

- **IP-address:nn**
  - **Use only if the MPLS/VPN network uses a private AS number**

00	02	BGP-AS4	nn

- **BGP-AS4:nn**
  - **4-byte Autonomous System Number (BGP-AS4)**

nn: assigned number administered by Enterprise

Slide 40

VPN Route Distribution
BGP with Multiprotocol Extensions

MFA FORUM

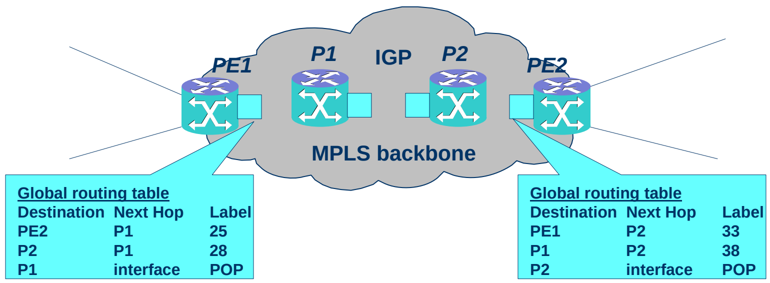
- *How are 96-bit VPN-IPv4 routes exchanged between PE routers?*
- BGP with Multiprotocol Extensions (MP-BGP) was designed to carry such routing information between peer routers (PE)
  - Propagates VPN-IPv4 addresses
  - Carries additional BGP route attributes (e.g. route target) called extended communities

VPN Route Distribution
BGP with Multiprotocol Extensions

MFA FORUM

- A BGP route is described by:
  - Standard BGP Communities attributes (e.g. Local Preference, MED, Next-hop, AS_PATH, Standard Community, etc.)
  - Extended BGP Communities attributes
- Extended Communities
  - Route Target (RT)
    - Identifies the set of sites the route has to be advertised to
  - Route Origin (RO)/Site of Origin
    - Identifies the originating site
    - Prevents routing loops with multi-homed customer sites

IGP Label Distribution



Global routing table (PE1)

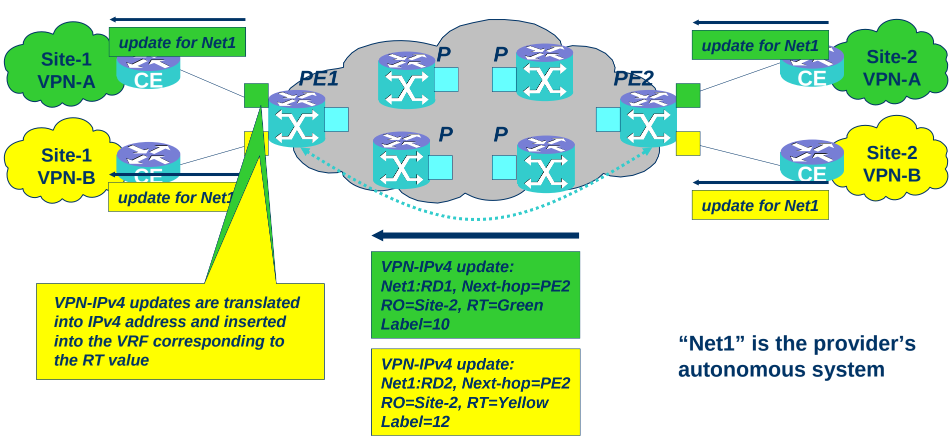
Destination	Next Hop	Label
PE2	P1	25
P2	P1	28
P1	interface	POP

Global routing table (PE2)

Destination	Next Hop	Label
PE1	P2	33
P1	P2	38
P2	interface	POP

- All routers (P and PE) run an IGP and a label distribution protocol
- Each P and PE router has routes for the backbone nodes and a label is associated to each route
- MPLS forwarding is used within the backbone

MP-BGP Route Distribution

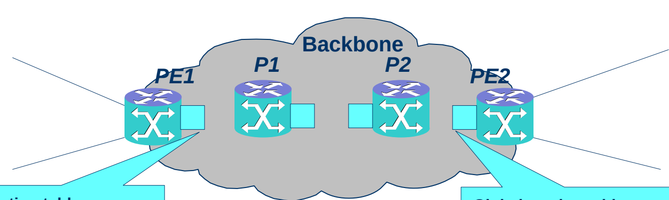


MP-BGP Route Distribution
Summary

- VPN Routing and Forwarding (VRF) Table
  - Multiple routing tables (VRFs) are used on PEs
    - VPNs are isolated
- Customer addresses can overlap
  - Need for unique VPN route prefix
  - PE routers use MP-BGP to distribute VPN routes to each other
  - For security and scalability, MP-BGP only propagates information about a VPN to other routers that have interfaces with the same Route Target value
- BGP-MPLS VPN extensions for IPv6 (RFC 4659)

MP-BGP: BGP with Multiprotocol Extensions

VPN Packet Forwarding



Global routing table (PE1)

Destination	Next Hop	Label
PE2	P1	25
P2	P1	28
P1	interface	POP

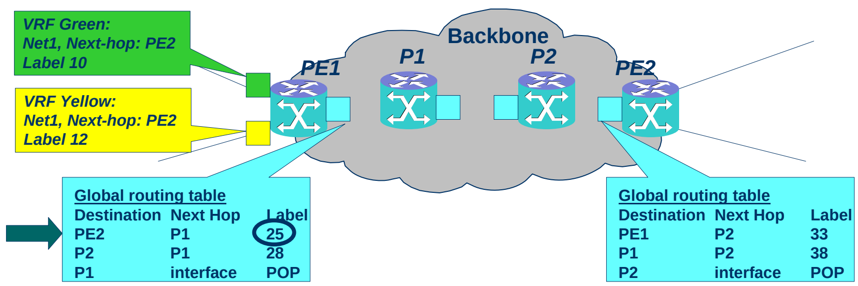
Global routing table (PE2)

Destination	Next Hop	Label
PE1	P2	33
P1	P2	38
P2	interface	POP

PE-to-PE connectivity via LSPs
- All routers (P and PE) run an IGP and a label distribution protocol
- Each P and PE router has routes for the backbone nodes and a label is associated to each route
- MPLS forwarding is used within the backbone

VPN Packet Forwarding
Label Stacking

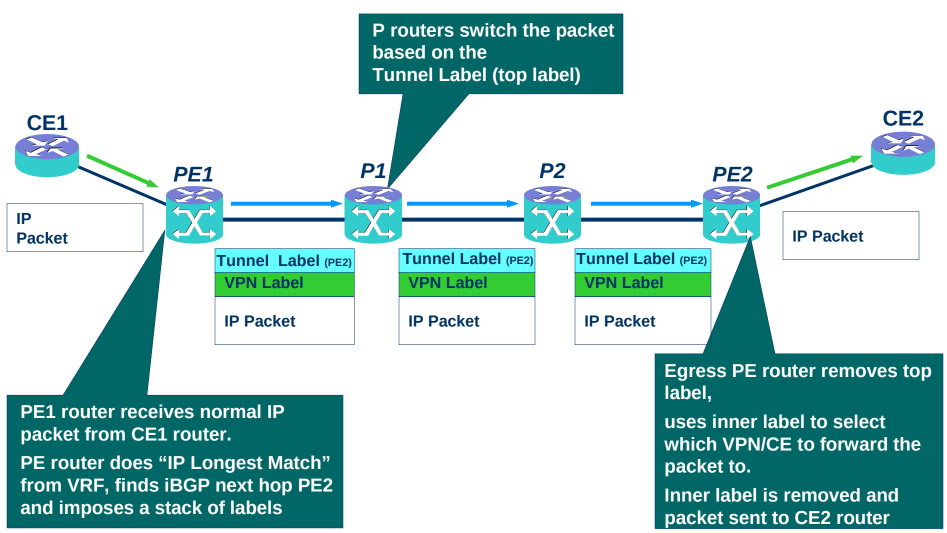
MFA FORUM



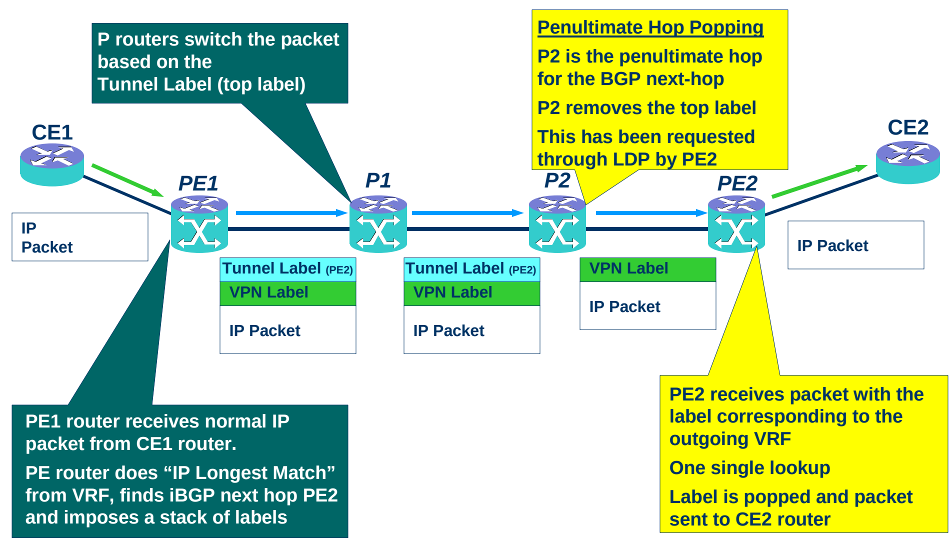
- **Ingress PE router uses two-level label stack**
  - VPN label **(inner label) assigned by the egress PE router**
  - Tunnel (IGP) label **(top label) identifying the PE router**
- **Label stack is attached in front of the IP packet that belongs to a VPN**
- **The MPLS packet is forwarded across the P routers in the backbone network**

VPN Packet Forwarding
Label Stacking

MFA FORUM



VPN Packet Forwarding
Penultimate Hop Popping



Slide 49

Core Routers (P Routers)

- **Not involved in MP-BGP**
- **Does not make routing decision based on VPN addresses**
- **Forwards packet based on the top label value**

- **P routers do not need to carry VPN routing information or Internet routing information, thus providing better network scalability**

Slide 50

Scaling BGP/MPLS VPNs

- Scalability of BGP/MPLS VPNs
  - Expanding the MPLS core network
    - Without impact on the VPN services, e.g. adding P routers (LSRs), new or faster links
  - Label stacking
    - Allows reducing the number of LSPs in the network core and avoiding LSP exhaustion
  - VPN Route Distribution
    - Route Reflectors

Scaling BGP/MPLS VPNs
Route Reflectors

- BGP Route Reflectors
  - Existing BGP technique, can be used to scale VPN route distribution
    - PEs don't need full mesh of BGP connections, only connect to RRs
    - By using multiple RRs, no one box needs to have all VPN routes
  - Each edge router needs only the information for the VPNs it supports
    - directly connected VPNs

RR: Route Reflector

Section 3

Layer 2 VPNs

Slide 53

MPLS VPN Tutorial Agenda

Layer 2 VPNs

- Overview
- Encapsulation and Label Stacking
- Virtual Private Wire Services – VPWS
  - Pt-to-pt Ethernet, Pt-to-pt ATM, Pt-to-pt Frame Relay
- Virtual Private LAN Services – VPLS

Slide 54

MPLS L2 VPN Market Drivers

What can we conclude?

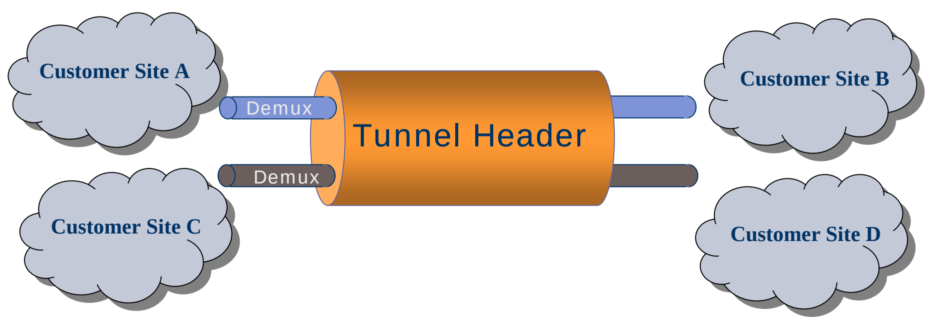
- Layer 3 IP is not the only traffic
  - Still a lot of legacy SNA, IPX, etc
  - Large enterprises have legacy protocols
- Layer 3 IP VPNs are not the whole answer
  - IP VPNs cannot handle legacy traffic
- Layer 2 legacy traffic widely deployed

Need for Layer 2 and Layer 3 VPNs to support the broad range of applications

MPLS Layer 2 VPNs

- Point-to-point Layer 2 solutions
  - Virtual Private Wire Services - **VPWS**
  - Similar to ATM / FR services, uses tunnels and connections (LSPs)
  - Customer gets connectivity only from provider
  - Ongoing work to encapsulate Ethernet, ATM, FR, TDM, SONET, etc
- Multi-point Layer 2 solutions
  - Virtual Private LAN Services - **VPLS**
  - Virtual Private LAN Services aka Transparent LAN Service (TLS)
  - Ethernet Metro VLANs / TLS over MPLS
  - Independent of underlying core transport
  - Ethernet encapsulation for transport over MPLS (RFC 4448)
  - Two approaches to signaling (RFC 4761 & RFC 4762)

MPLS Point-to-Point Service



- Tunnel Label determines path through network
- VC Label identifies VLAN, VPN, or connection at the end point

MPLS Point-to-Point Services
Label Stacking

Tunnel Header	PW Header	VC Encaps Information	Layer 2 payload
1	2	3	

- Three Layers of Encapsulation
  1) Tunnel Header: Contains information needed to transport the PDU across the IP or MPLS network
  2) Pseudo wire Header (PW): Used to distinguish individual emulated VCs within a single tunnel
  3) Emulated VC Encapsulation: Contains the information about the enclosed PDU (known as Control Word)
- Tunnel Header determines path through network
- Pseudo wire Header identifies VLAN, VPN, or connection at the end point
- All services look like a Virtual Circuit to MPLS network

Encaps Information Field

bits 0-3	4-7	8-9	10-15	16-31
Reserved	Flags	FRG	Length	Sequence Number

FRG: Fragmentation

Generic Control Word

- Layer 2 header fields may be discarded at ingress
- Control word carries "flag" bits depending on encapsulation
  - (FR: FECN, BECN, C/R, DE, ATM: CLP, EFCI, C/R, etc)
- Length required when padding small frames on links which have a minimum frame size
- Sequence number is optional. It is used to detect out of order delivery of frames.

bits 0-3	4-7	8-15	16-31
Reserved	Version	Reserved	Channel Type

Control Word for PW Associated Channel

RFC 4385

LDP - Label Mapping Message

Label Mapping	Message Length
Message ID	
FEC TLV	
Label TLV	
Label Request Message ID TLV	
LSPID TLV (optional)	
Traffic TLV (optional)	

New VC FEC Element Defined

VC TLV	C	VC Type	VC Info Length
Group ID			
VC ID			
Interface Parameters			

- **Virtual Circuit FEC Element**
  - **C - Control Word present**
  - **VC Type - FR, ATM, Ethernet, HDLC, PPP, ATM cell**
  - **VC Info Length - length of VCID field**
  - **Group ID - user configured - group of VCs representing port or tunnel index**
  - **VC ID - used with VC type to identify unique VC**
  - **Interface Parameters - Specific I/O parameters**

Layer 2 Encapsulation
PWE3 Work

- **RFC 3916: Requirements for PWE3**
  - **"This document describes base requirements for the Pseudo-Wire Emulation Edge to Edge Working Group (PWE3 WG). It provides guidelines for other working group documents that will define mechanisms for providing pseudo-wire emulation of Ethernet, ATM, Frame Relay. "**
- **RFC 3985: PWE3 Architecture**
  - **"This document describes an architecture for Pseudo Wire Emulation Edge-to-Edge (PWE3). It discusses the emulation of services (such as Frame Relay, ATM, Ethernet TDM and SONET/SDH) over packet switched networks (PSNs) using IP or MPLS. It presents the architectural framework for pseudo wires (PWs), defines terminology, specifies the various protocol elements and their functions."**

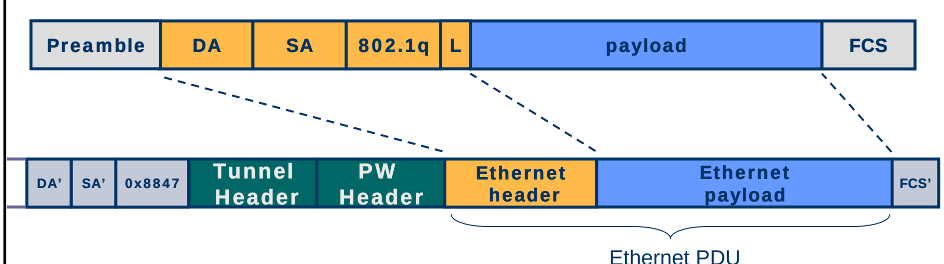
Layer 2 Encapsulation *PWE3*
PWE3 Work

- **ATM AAL5 and ATM cell**
  - **RFC 4717**
- **Frame Relay**
  - **RFC 4619**
- **Ethernet / 802.1q VLAN**
  - **RFC 4448**
- **PPP/HDLC**
  - **RFC 4618**
- **TDM**
  - **RFC 4553**
- **Pseudo wire Set-up and Maintenance using LDP**
  - **RFC 4447**

Slide 63

Ethernet Encapsulation for Transport over MPLS

Original Ethernet frame



Encapsulated Ethernet over MPLS <u>over Ethernet Transport</u>

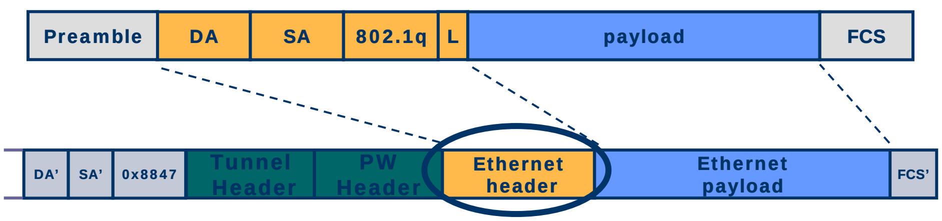
- **Ingress device strips the Ethernet preamble and FCS**
- **Raw or Tagged mode**
- **Optional Control Word** | 0000 | Reserved | Sequence # |
- **New MPLS Ethernet header (type 0x8847) and new FCS is added to MPLS Ethernet packet**

RFC 4448

Slide 64

Ethernet Encapsulation for Transport over MPLS

MFA FORUM



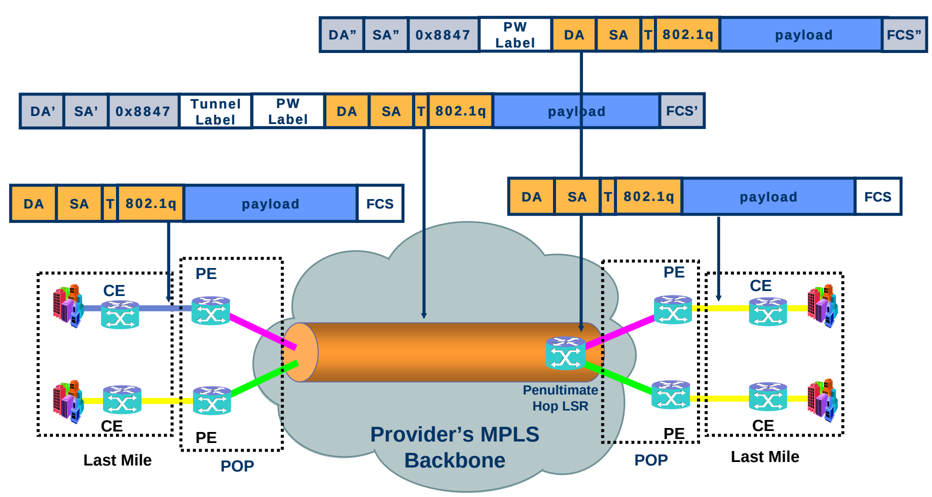
- VC Encaps field is normally 32 bits
- Ethernet VC Encaps fields:
  - DA and SA at 6 bytes each
  - Length at 2 bytes
  - 802.1q VLAN at 4 bytes
  - Total of 18 bytes (144 bits vs. 32 bits)

RFC 4448

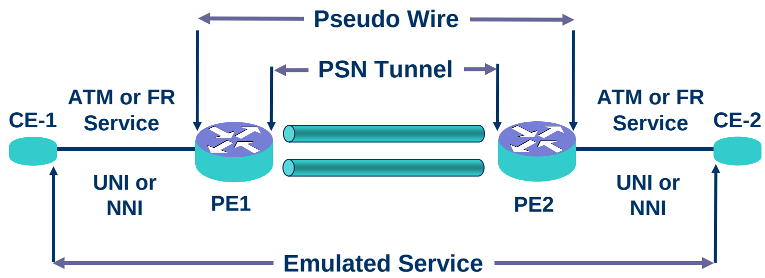
Life of a Frame

Ethernet over Ethernet MPLS

MFA FORUM



ATM and Frame Relay Service Transport over MPLS - *Reference Model*



PE = Provider Edge
CE = Customer Edge

Requirements for Pseudo Wire Emulation Edge-to Edge (PWE3)

Slide 67

ATM AAL5 Encapsulation for Transport over MPLS

4 octets	4 octets	4 octets	
Tunnel Header	PW Header	Control word	AAL5 CPCS-PDU

bits	4	1	1	1	1	8	16
	Rsvd	T	E	C	U	Length	Sequence Number*

ATM Control Word

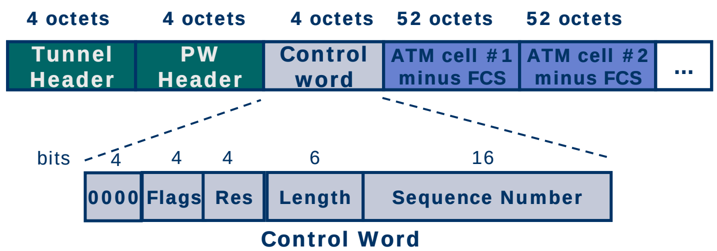
* optional

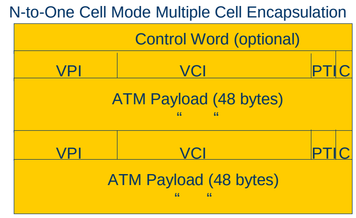
- **2 modes:**
  - **PDU Frame Mode – encapsulates PDU payload, pad and trailer**
  - **SDU Frame Mode – encapsulates PDU payload** *(shown above)*
- **Ingress reassembles AAL5 frames**
- **SDU Frame mode required control word includes:**
  - **T = Transport type bit identifies whether packet contains an AAL5 payload or ATM admin cell**
  - **E = EFCI bit - Explicit Forward Congestion Indication**
  - **L = CLP bit - Cell Loss Priority**
  - **U = Command / Response bit**

RFC 4717

Slide 68

ATM Cell Mode Encapsulation for Transport over MPLS

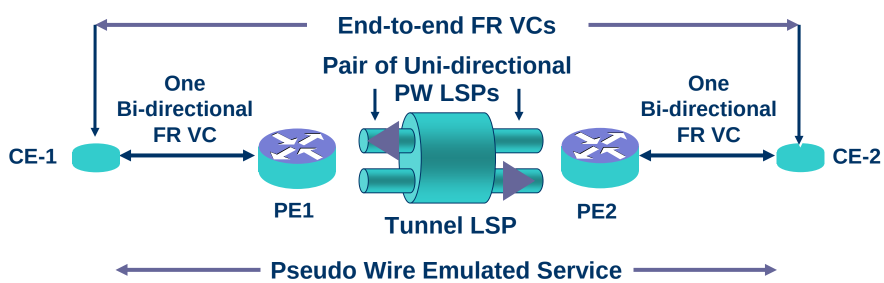




- **2 modes:**
  - **One-to-One Cell Mode - maps one ATM VCC (or VPC) to one PW**
  - **N-to-One Cell Mode - maps one or more ATM VCCs (or VPCs) to one PW** *(shown above);* **only required mode for ATM support**
- **Ingress performs no reassembly**
- **Control word is <u>optional</u>: If used, Flag and Length bits are not used**

RFC 4717

Frame Relay Encapsulation for Transport over MPLS

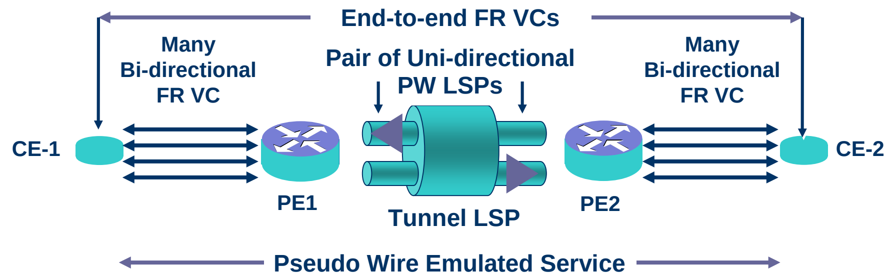


- **Frame Relay (FR) Transport Service application**
- **Two Mapping modes:**
  - **One-to-one mapping: One FR VC mapped to a pair of unidirectional PWs** *(shown above)*
  - **Many-to-one or port mode mapping: Many FR VCs mapped to a pair of Unidirectional PWs**

RFC 4619

Frame Relay Encapsulation for Transport over MPLS

MFA FORUM

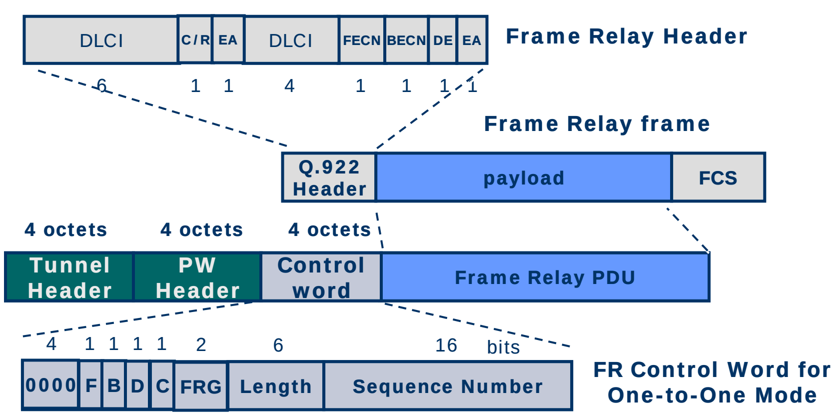


- **Two Mapping modes:**
  - One-to-One Mapping: One FR VC mapped to a pair of unidirectional PWs
  - **Many-to-One or Port Mode Mapping: Many FR VCs mapped to a pair of Unidirectional PWs** *(shown above)*

RFC 4619

Frame Relay Encapsulation for Transport over MPLS

MFA FORUM



- F = FECN (Forward Explicit Congestion Notification)
- B = BECN (Backward Explicit Congestion Notification)
- D = DE (Discard Eligibility Indicator)
- C = C/R (Command / Response Field)

RFC 4619

MPLS VPN Tutorial Agenda

MFA FORUM

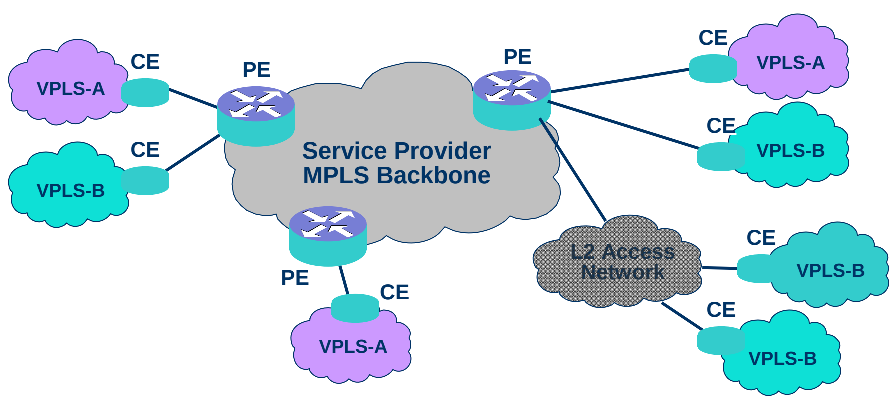
Layer 2 VPNs

- Overview
- Encapsulation and Label Stacking
- Virtual Private Wire Services – VPWS
  - Pt-to-pt Ethernet, Pt-to-pt ATM, Pt-to-pt Frame Relay
- Virtual Private LAN Services – VPLS

MPLS VPLS

Reference Model

MFA FORUM



Creates an emulated Ethernet LAN Segment across a wide-area network for a set of users

RFC 4464, RFC 4026

Virtual Private LAN Services

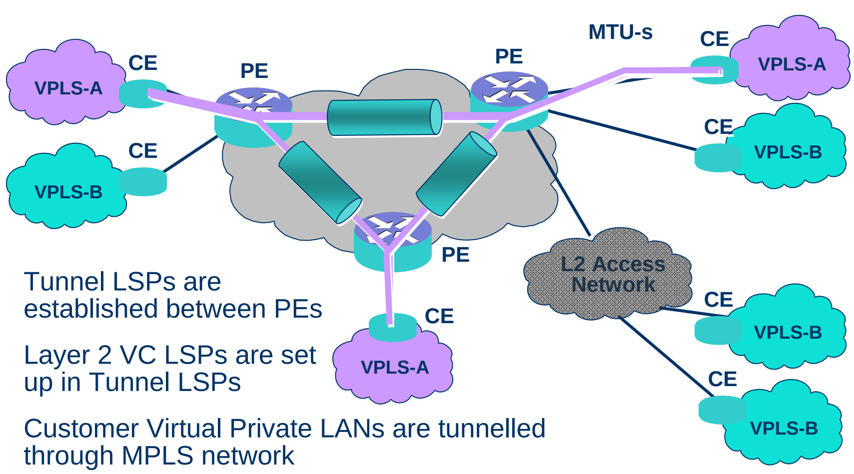
- Defines an Ethernet (IEEE 802.1D) learning bridge model over MPLS Ethernet PWs
- Defines the PE function for an MPLS VPLS network
- Creates a layer 2 broadcast domain for a closed group of users
- MAC address learning and aging on a per LSP basis
- Packet replication across LSPs for multicast, broadcast, and unknown unicast traffic
- Hierarchical VPLS for scalability

Slide 75

MPLS VPLS

Reference Model

Emulates LAN Segment across a wide-area network

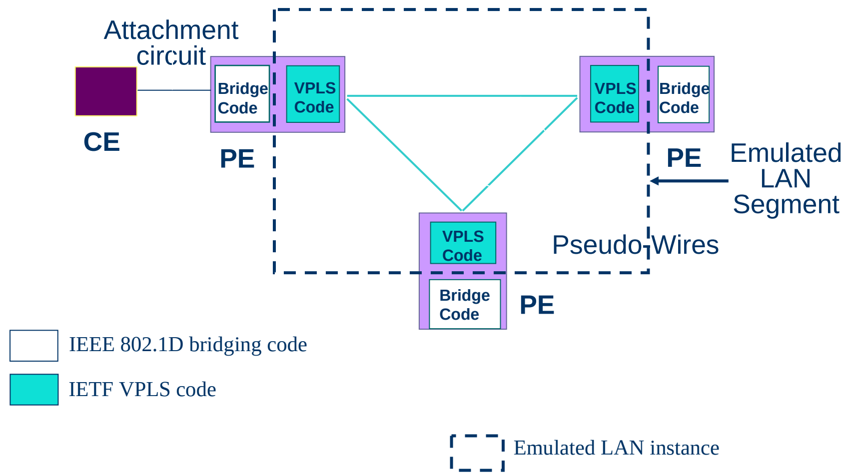


- Tunnel LSPs are established between PEs
- Layer 2 VC LSPs are set up in Tunnel LSPs
- Customer Virtual Private LANs are tunnelled through MPLS network
- Core MPLS network acts as a LAN switch

Slide 76

VPLS Internal PE Architecture

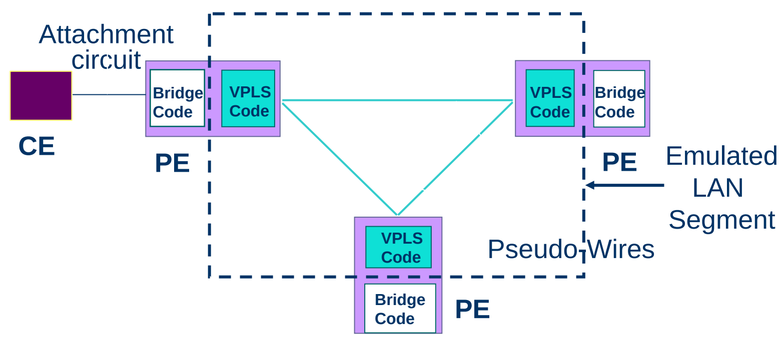
MFA FORUM



Slide 77

PE Bridging Code

MFA FORUM



Standard IEEE 802.1D Bridging code

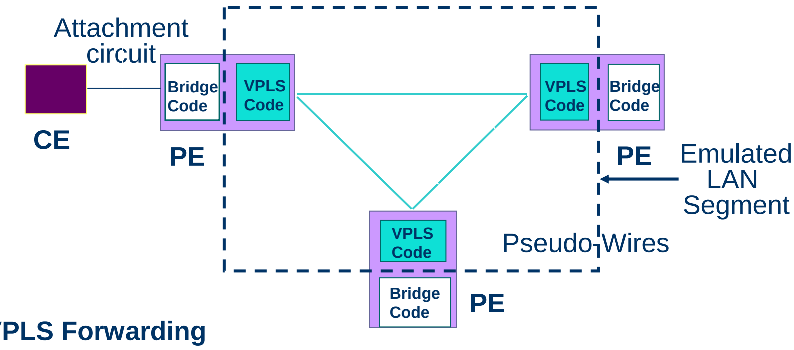
- **Used to interface with CE facing ports**
- **Learn MAC addresses and aging**
- **Might run STP with CEs**
- **Used to interface with VPLS**
- **Might run STP between PEs**

IEEE 802.1D bridging code

IETF VPLS code

Slide 78

PE VPLS Code



VPLS Forwarding

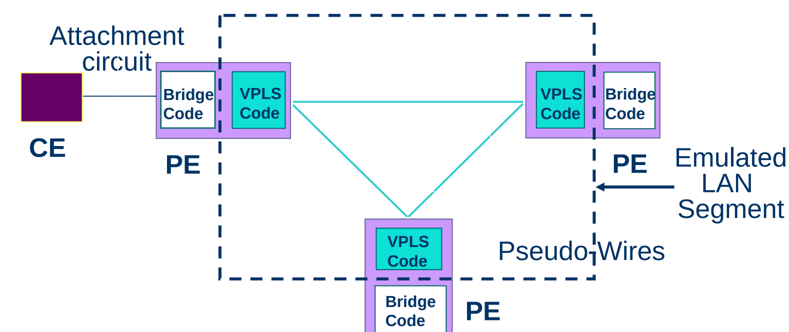
- **Learns MAC addresses per pseudo-wire (VC LSP)**
- **Forwarding based on MAC addresses**
- **Replicates multicast & broadcast frames**
- **Floods unknown frames**
- **Split-horizon for loop prevention**

IEEE 802.1D bridging code

IETF VPLS code

Slide 79

PE VPLS Code



- **VPLS Signaling**
  - **Establishes pseudo-wires per VPLS between relevant PEs**
  - **Two signaling protocol options:**
    - **LDP – RFC 4762**
    - **BGP – RFC 4761**
- **VPLS Discovery (Manual, LDP, BGP, DNS)**

IEEE 802.1D bridging code

IETF VPLS code

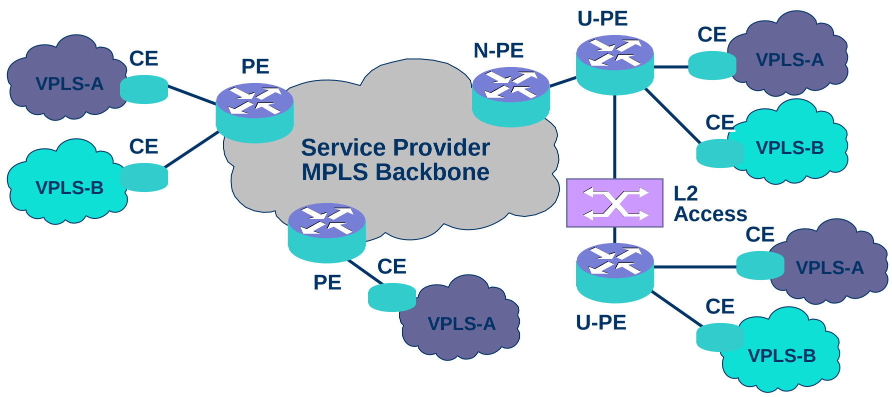
Slide 80

MPLS VPLS

Reference Model – Distributed PE Functions

MFA FORUM

Distributed PE functions
N-PE = PE closer to core network
U-PE = PE closer to user/customer



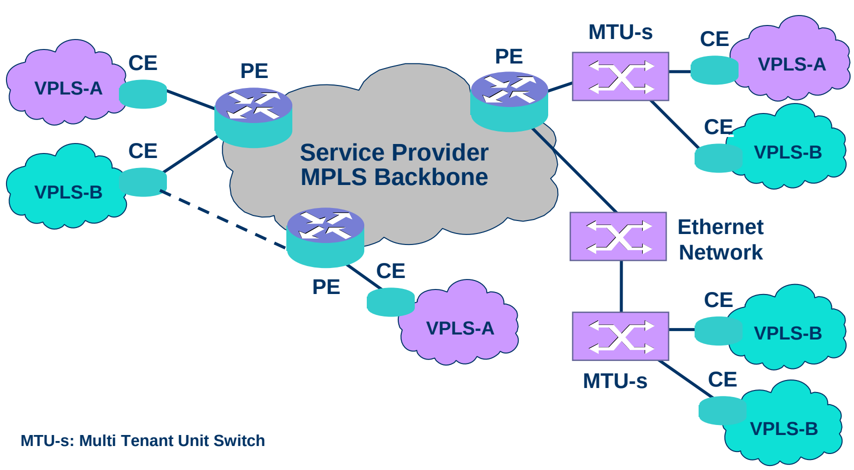
RFC 4464, RFC 4026

Slide 81

MPLS VPLS

Reference Model

MFA FORUM



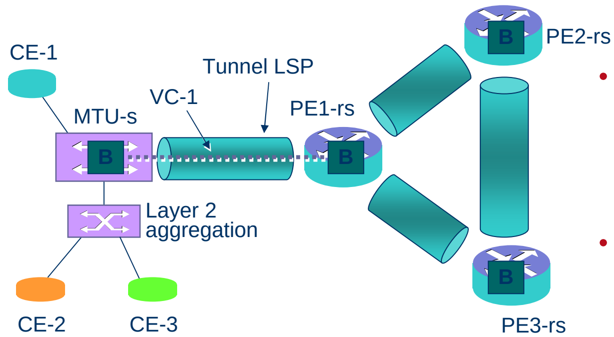
MTU-s: Multi Tenant Unit Switch

RFC 4762

Slide 82

Virtual Private LAN Services

RFC 4762



- Reduces signaling and packet replication to allow large scale deployment of VPLS
- Uses VC / LSPs between edge MTU and VPLS aware PE devices

VC-1 = Single pt-to-pt Tunnel LSP

MTU-s = Bridging Capable MTU (Multi Tenant Unit)

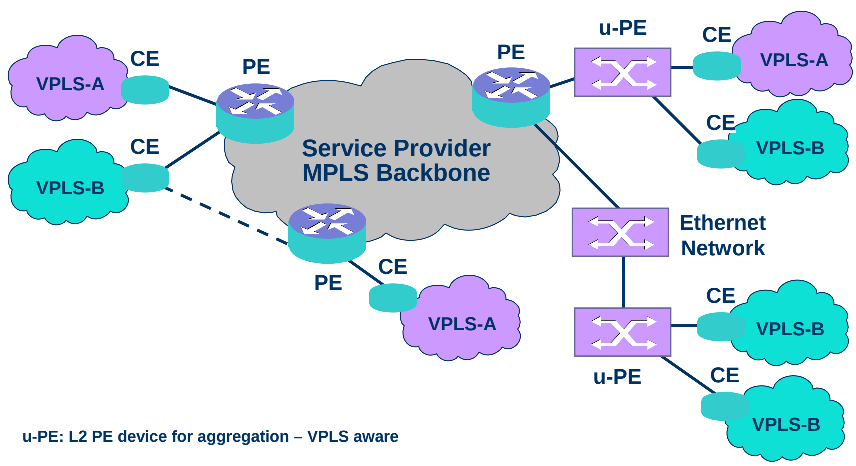
PE-rs = VPLS Capable PE

B = Virtual VPLS (Bridge) Instance

Slide 83

MPLS VPLS

Reference Model



u-PE: L2 PE device for aggregation – VPLS aware

RFC 4761

Slide 84

VPLS Scalability

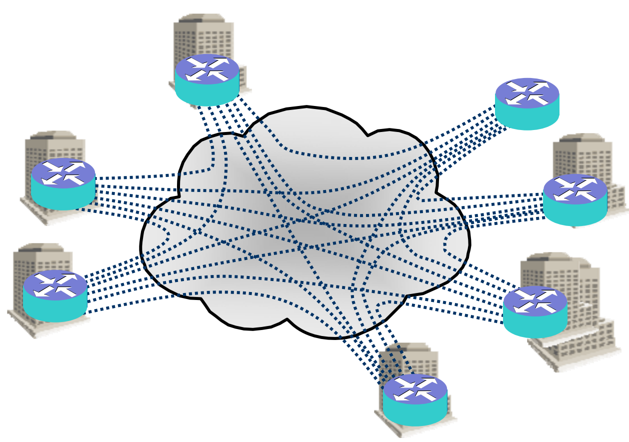
Parameters

- Number of MAC Addresses
- Number of replications
- Number of LSPs
- Number of VPLS instances
- Number of LDP peers
- Number of PEs

VPLS Scalability

Signaling Overhead – Flat Topology

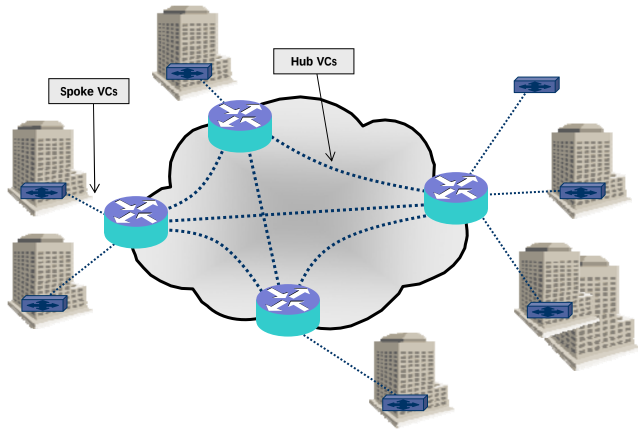
- **Architecture has a direct impact on the Signaling Overhead (control plane)**



VPLS Scalability

Signaling Overhead – Hierarchical Topology

- Architecture has a direct impact on the Signaling Overhead (control plane)

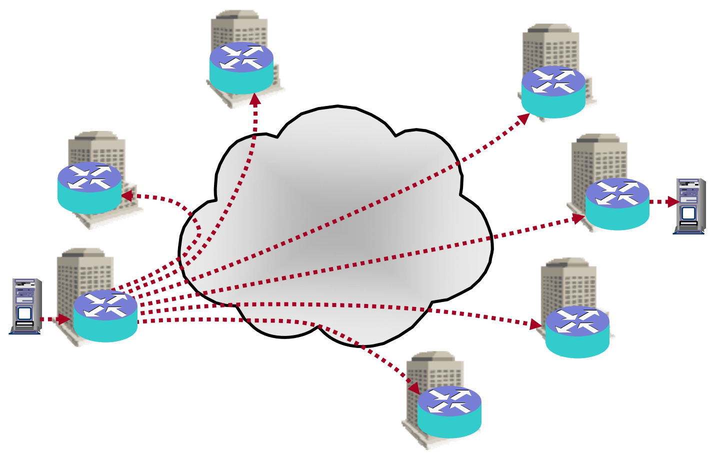


Slide 87

VPLS Scalability

Replication Overhead – Flat Topology

- Architecture has a direct impact on Replication Overhead (forwarding plane)

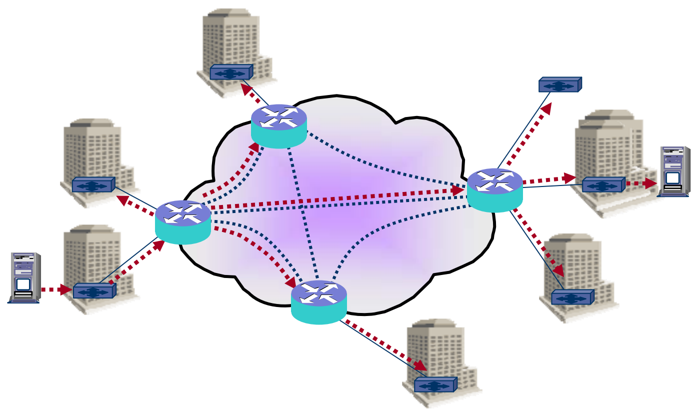


Slide 88

VPLS Scalability

Replication Overhead – Hierarchical Topology

- Architecture has a direct impact on Replication Overhead (forwarding plane)

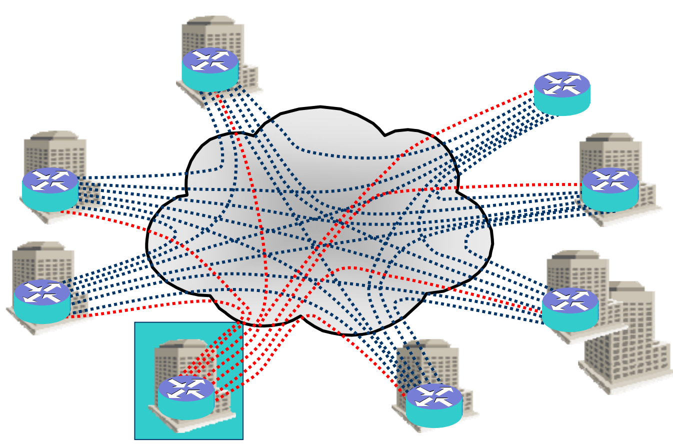


Slide 89

VPLS Scalability

Adding a New Site – Flat Topology

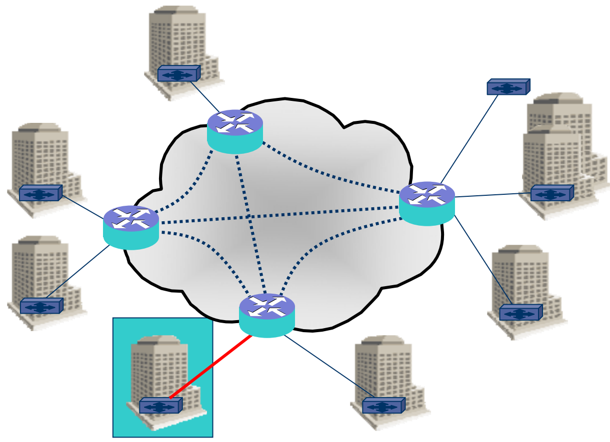
- Architecture affects Provisioning & Signaling between all nodes



Slide 90

VPLS Scalability
Adding a New Site – Hierarchical Topology

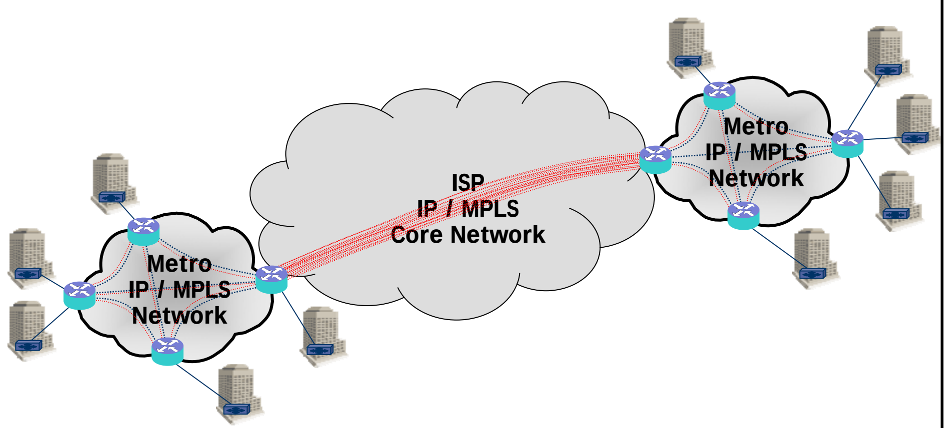
- Architecture affects Provisioning & Signaling between all nodes



Slide 91

VPLS Scalability
Inter-Metro Service

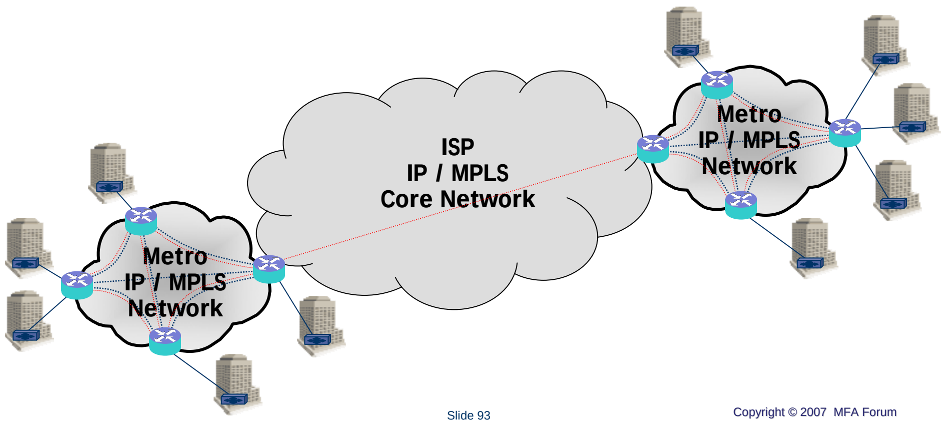
- Architecture has a direct impact on ability to offer Inter-Metro Service



Slide 92

VPLS Scalability
Inter-Metro Service

- Architecture has a direct impact on ability to offer Inter-Metro Service



VPLS Scalability
FIB Size

- VPLS FIB size depends on the type of Service Offering:
  - Multi-protocol Inter-connect service
    - Mimics the DSL Tariff Model
    - Customers are charged per site per block of MAC addresses
  - Router Inter-connect
    - One MAC address per site
- Same Network Design principles apply for
  - MAC FIB Size of VPLS Service and,
  - Route Table Size of Virtual Private Routed Network (VPRN) Service

FIB: Forwarding Information Base

IETF Layer 2 VPNs

RFC 4665

- Service requirements for L2 VPNs
  - Virtual Private Wire Services (VPWS) - point-to-point VPNs
  - Virtual Private LAN services (VPLS) - multipoint-to-multipoint VPNs
  - Service Provider and Enterprise Views’
- Checklist of requirements to help evaluate how an approach satisfies specific requirements
- Service Level Specification (SLS)

Slide 95

Section 4

Introduction to Multi-Service Interworking

Slide 96

MPLS VPN Tutorial Agenda

MFA FORUM

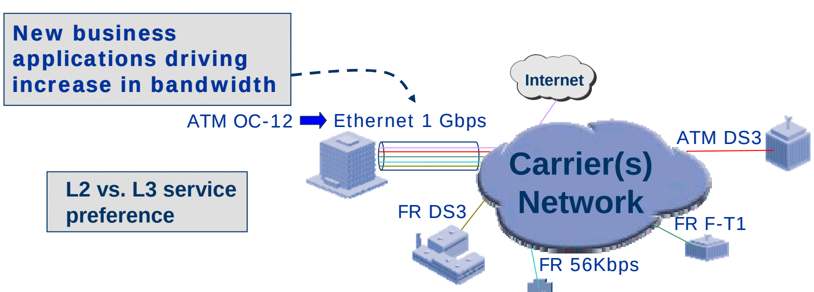
Introduction to Multi-Service Interworking over MPLS

- Interworking History and Definition
- Multi-Service Interworking of Ethernet over MPLS
- Migration Scenarios and Benefits

Slide 97

Why Interwork?

MFA FORUM

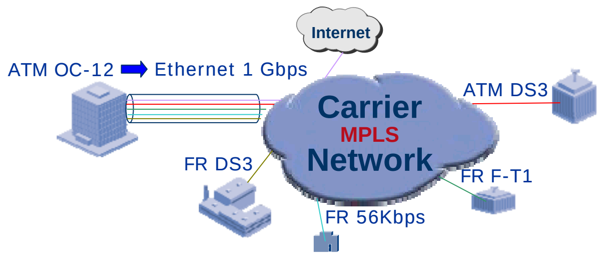


Enterprise perspective:

- Many have an embedded Frame Relay and/or ATM network
- Need to cost effectively scale bandwidth at select sites to support new business applications
- Maintain a network with mixture of services, bandwidths to match application needs at specific sites
- Reduce cost, time and risk to address emerging needs

Slide 98

Why Interwork?



Carrier Perspective:

- Want a common edge infrastructure to support and "Interwork" with legacy and new services
- Support all legacy transport technologies and services
- Planning to converge on an IP / MPLS core
- Want to seamlessly introduce Metro Ethernet services and IP VPNs

Interworking

History

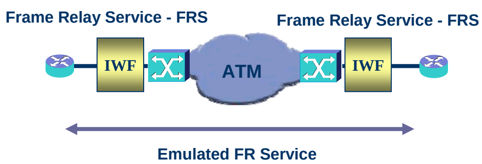
- The Frame Relay Forum defined the <u>Network Interworking</u> function between Frame Relay and ATM in the <u>FRF.5</u> document finalized in 1994
- The Frame Relay Forum defined the <u>Service interworking</u> function between Frame Relay and ATM in the <u>FRF.8.2</u> document finalized in 2004
- Why define FR and ATM interworking?
  - ATM cores with FR/ATM access services deployed
  - ATM and Frame Relay circuits are point-to-point
  - Both data links have services that are somewhat similar (ie. FR to AAL5) in nature even though the signaling is different

Interworking Function - IWF

Network vs Service IWF

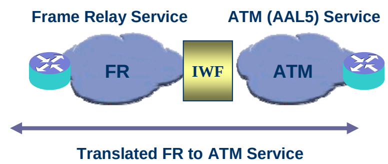
MFA FORUM

Network Interworking



- Network Interworking is used when one protocol is "tunneled" across another "intermediary" network / protocol
- The Network Interworking (IWF) function "terminates" and "encapsulates" the protocol over a Pt-to-Pt connection
- Service at end points ***has to be*** the same

Service Interworking



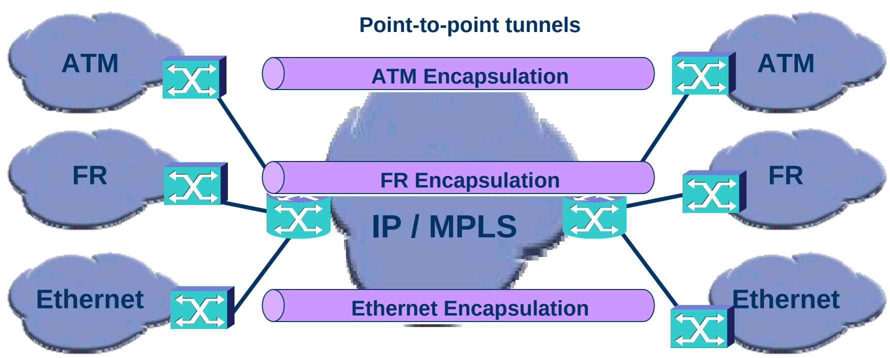
- Service Interworking is required to "translate" one protocol to another protocol – used between two unlike protocols
- The Service Interworking function "translates" the control information transparently by an interworking function (IWF)
- Services at the end points ***are not*** the same

Slide 101

MPLS Network Interworking

IETF PWE3 Pt-to-Pt Encapsulation

MFA FORUM

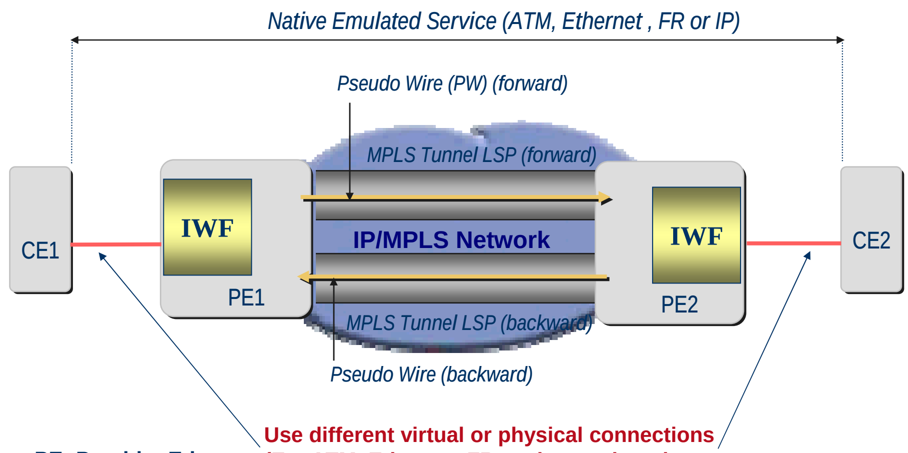


Service has to be pt-to-pt between like services: ATM to ATM, FR to FR, Ethernet to Ethernet, etc

Slide 102

MPLS Multi-Service Interworking

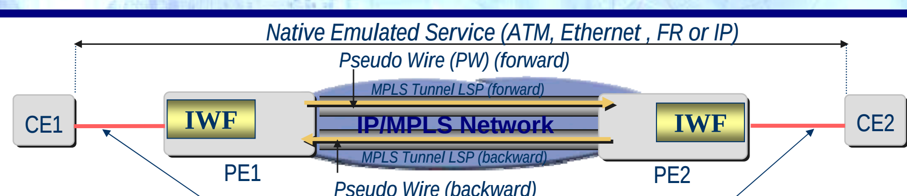
Reference Model



Use different virtual or physical connections
(Ex: ATM, Ethernet, FR, etc) at each end
Attachment Circuit (AC)

PE: Provider Edge
CE: Customer Edge
IWF: Interworking Function
Multi-Service: Services are ATM, Ethernet, FR and IP

Multi-Service Interworking

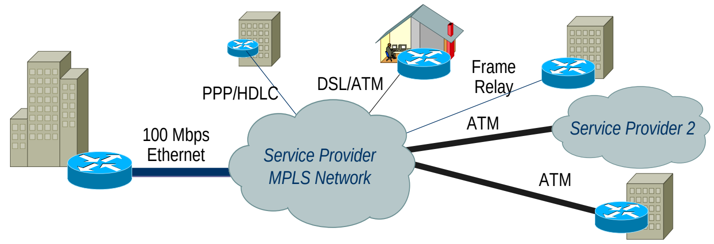


Use different virtual or physical connections
(Ex: ATM, Ethernet, FR, etc) at each end
Attachment Circuit (AC)

- Multi-Service Interworking of Ethernet over MPLS
- Multi-Service Interworking of IP over MPLS
  - MFA Forum Multi-Service Interworking – IP over MPLS Implementation Agreement 16.0
- Frame Relay and ATM Service Interworking over MPLS
  - MFA Forum Multi-Service Interworking – Frame Relay and ATM Service Interworking over MPLS Implementation Agreement 15.0
- Fault Management for Multi-Service Interworking
  - MFA Forum Fault Management for Multi-Service Interworking over MPLS Implementation Agreement 13.0

Multi-Service Interworking - Ethernet over MPLS

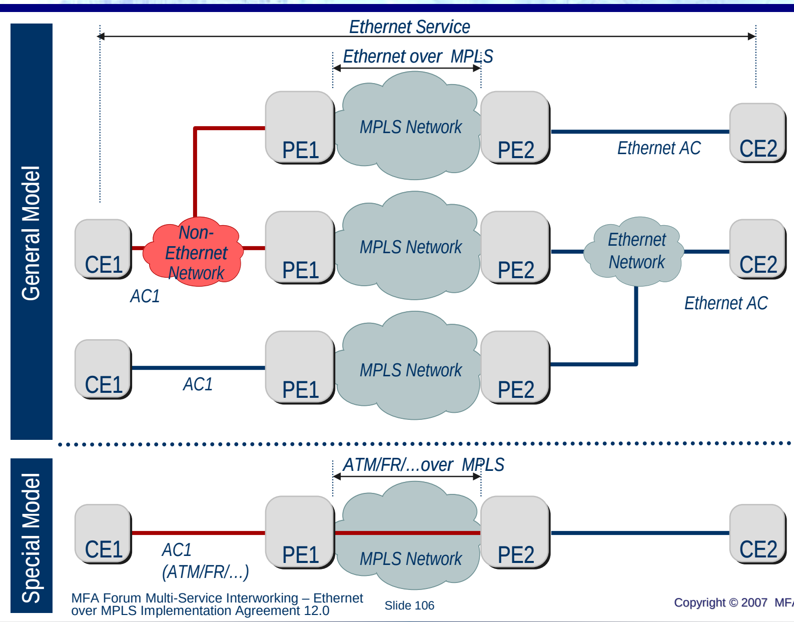
MFA FORUM



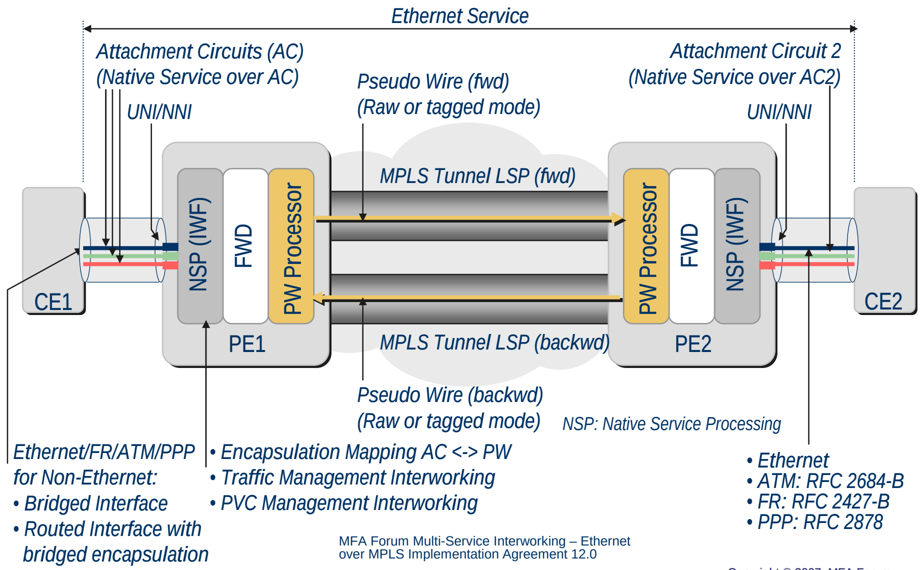
- **Ubiquitous Ethernet-Service offering** requires that different UNI/NNIs are supported – Ethernet as well as ATM, FR, PPP, …
  - SPs expand their existing Ethernet UNI/NNI offering
- **Characteristics**
  - Native Service: Ethernet
  - Consistent service definitions across technology boundaries
  - Point-to-Point and Multipoint
  - Independence from CE protocol processing (address resolution, L3-protocols,…)

Models for Ethernet Interworking

MFA FORUM



Interworking Reference Model



MFA Forum Multi-Service Interworking – Ethernet over MPLS Implementation Agreement 12.0

Slide 107

Multi-Service Interworking of Ethernet over MPLS - Observations

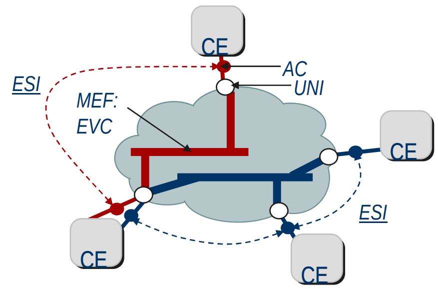
- Interworking is a local function to the PE
  - PE only needs to implement procedures for those interfaces it supports (e.g. PE with ATM: RFC2684 bridged only)
  - PE only needs to support PW of type Ethernet – irrespective of the other end. Set of translations limited to (to/from) Ethernet
  - AC configuration local to the PE
  - AC termination on PE supports VPLS (and VPWS) – MAC-addresses are visible to the PE
- CPE uses bridged encapsulation (native Service is Ethernet)
  - Implicit support for any L3 Network protocol
  - ARP resolution done by both end CPEs – no handling of protocol specific address resolution required
  - Integrated Routing and Bridging for Frame-Relay AC, IRB/Routed Bridge Encapsulation for ATM AC
  - Required configuration changes for CE devices that have routed interfaces
- Consider hidden complexities, e.g. IP-routing protocols behave differently over broadcast & non-broadcast media

Slide 108

Ethernet Service Instance (ESI)

MFA FORUM

- Ethernet Service Instance
  - "Association of two or more AC over which an Ethernet Service is offered to a given customer"
- Corresponding concepts
  - ESI can correspond to VPLS/VPWS (IETF L2VPN WG), S-VLAN (IEEE 802.1ad)
  - Note: MEF EVC associates a set of UNI, while ESI associates a set of AC
- Multiple Mappings options at individual AC to the corresponding Service Instance



Mapping at an AC (per ESI)	Ethernet Interface	ATM/ FR VC	PPP/HDLC Interface
Port based (untagged only)	✓	✓	✓
Port based (tagged & untagged)	✓	✓	✓
VLAN mapping	✓	NS	NS
VLAN bundling	✓	NS	NS

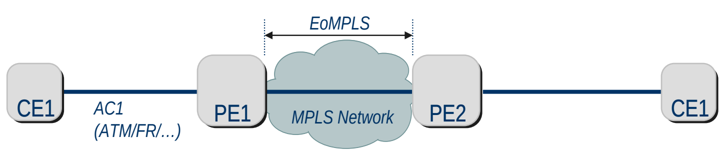
NS: Not specified in this version

MFA Forum Multi-Service Interworking – Ethernet over MPLS Implementation Agreement 12.0

Slide 109

Ethernet Service Interworking Encapsulation Formats

MFA FORUM



Native Ethernet		**Native Ethernet**
Ethernet VLAN		**Ethernet VLAN**
Bridged Ethernet over ATM (RFC 2684-B)		**Bridged Ethernet over ATM (RFC 2684-B)**
Bridged Ethernet over FR (RFC 2427-B)		**Bridged Ethernet over FR (RFC 2427-B)**
Bridged Ethernet over HDLC/PPP (RFC 2878)		**Bridged Ethernet over HDLC/PPP (RFC 2878)**

MFA Forum Multi-Service Interworking – Ethernet over MPLS Implementation Agreement 12.0

Slide 110

Multi-Service Interworking of Ethernet over MPLS Summary

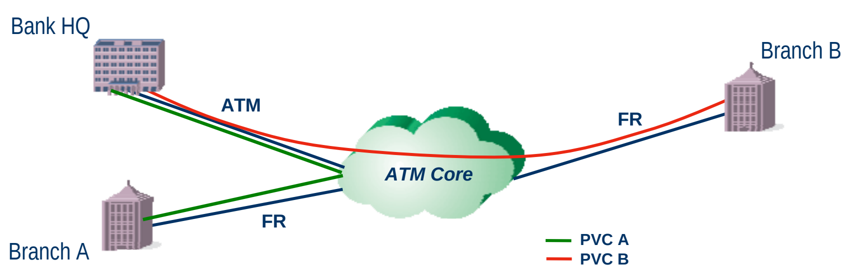
MFA FORUM

- **Layer 2 Service Interworking is critically important to Ethernet WAN services**
  - **Limited Ethernet footprint**
  - **Leverages installed base of ATM/Frame Relay, and HDLC copper based circuits**
- **General Interworking Model**
  - **Concept of Ethernet Service Instance**
  - **Local Termination of the AC – keep complexities low**
- **Standards Evolution to support comprehensive service interworking**
  - **Ethernet OAM standards work (ITU, IEEE)**

Slide 111

Enterprise Network Today

MFA FORUM

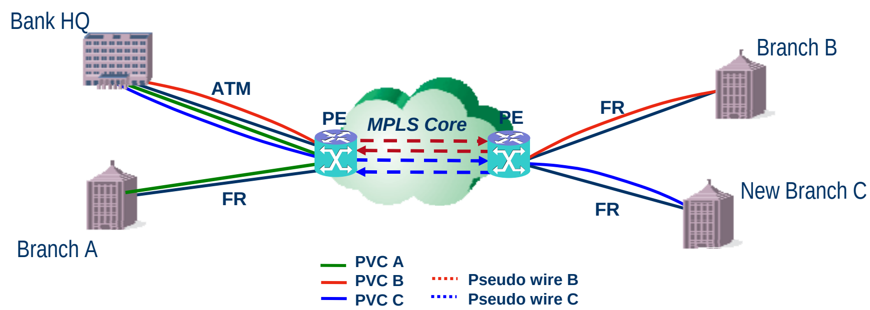


FRF.8.2 Service interworking is a key enabler

- Connecting branch offices with low-speed FR access to the Headquarter with a high-speed ATM connection

Slide 112

Network Migration Scenario 1:
- ATM/FR Interworking over MPLS

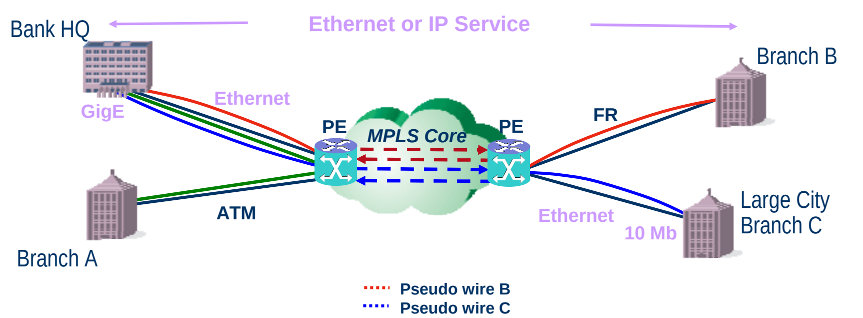


Enables graceful traffic migration from ATM to MPLS core

- Preserves existing ATM and FR service SLAs and revenues
- Transparent to Enterprise
- Enables service provider MPLS network investment for new FR/ATM endpoints

Slide 113

Network Migration Scenario 2:
- Ethernet or IP Interworking over MPLS



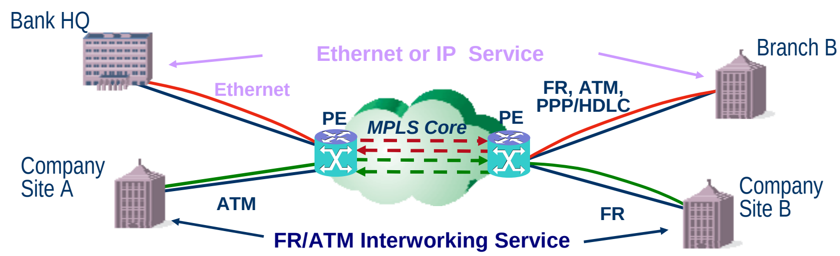
Introduce Ethernet connectivity to existing ATM/FR infrastructure

- Cost effectively scale bandwidth at select sites to support new business applications
- Graceful migration of legacy ATM/FR service to Ethernet services
- Ethernet and IP pt-pt *(shown)* and multipoint (Ethernet only) VPN services

Slide 114

Benefits of Multi-Service Interworking over MPLS

MFA FORUM



Carrier Benefits

- Increases addressable market
- Lowers capital expenses
- Increases flexibility
- Preserves revenues from legacy services

Enterprise Benefits

- Cost effectively scale bandwidth to support new applications
- Flexible support for sites with different access technologies
- Seamless integration of new sites on to network

Enables a smooth, cost effective evolution for both Enterprises and Carriers to new services

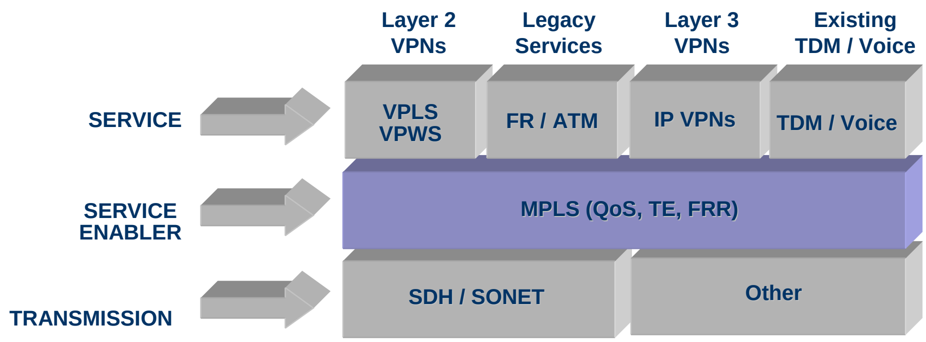
MFA FORUM

Summary

MPLS VPNs Summary

- **Layer 2 and Layer 3 VPNs each address specific needs** (traffic types, business applications, CPE investment, level of Service Provider participation in routing, etc)
- **Both are standards based and widely deployed**
- **Solutions today include a combination of Layer 2 and Layer 3 VPNs**

MPLS as a Service Enabler



VPLS = Virtual Private LAN Services
VPWS = Virtual Private Wire Services
L3 IP VPN = BGP/MPLS VPN RFC4364

For More Information. . .

- http://www.mfaforum.org
- http://www.ietf.org
- http://www.itu.int
- http://www.mplsrc.com

For questions, utilize the MFA Forum Message Board

Website: http://www.mfaforum.org/board/

***Thank you* for attending the**

MPLS L2/L3
Virtual Private Networks Tutorial