MPLS VPN

December 7, 2020

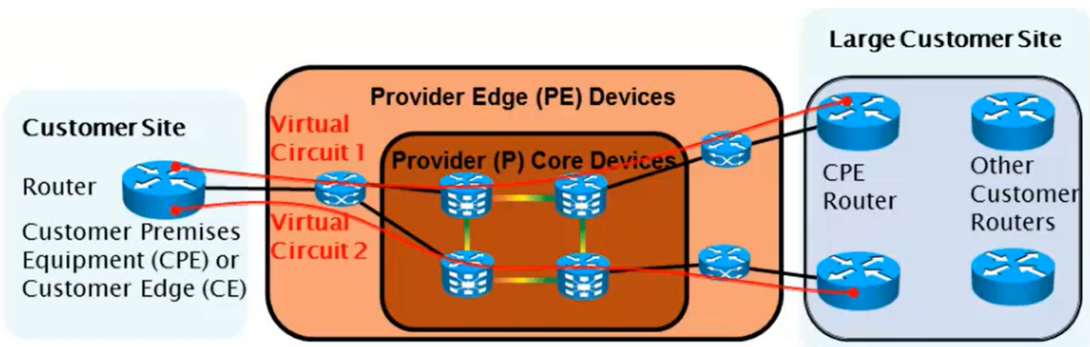
1 VPN basics

1.1 Introduction to Modern WAN Technology

- Traditional router based network used Leased line connections

Advantage	**Disadvantage**
Secure	Expensive
High Throughput	Permenent physical connections
Superior Quality and Reliable	Not-Scalable

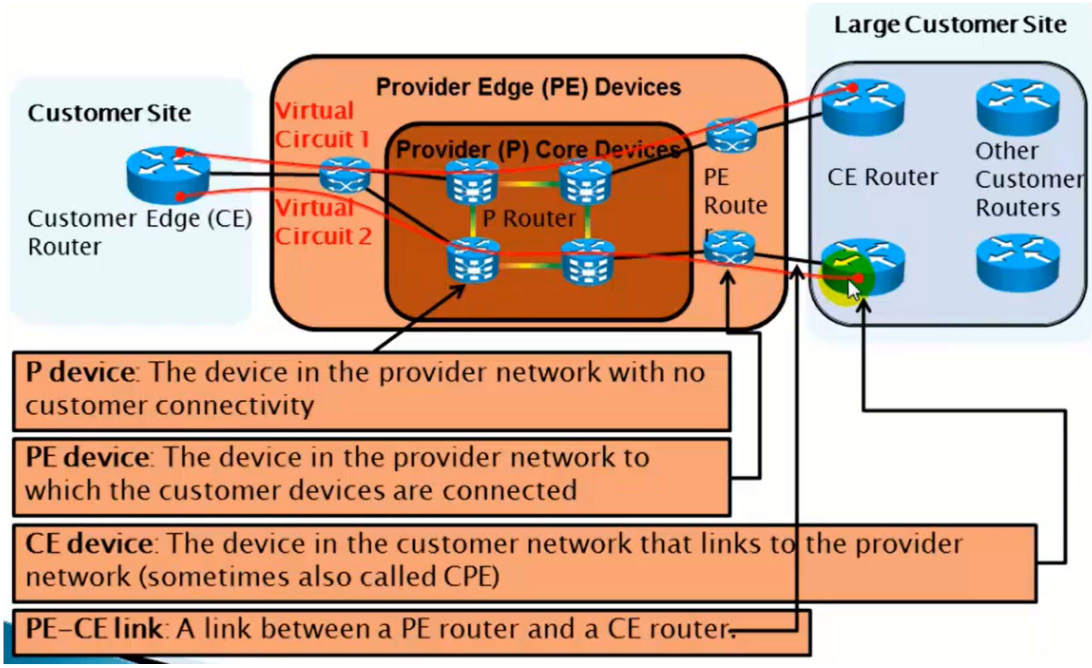
- During 1990s VPNs were introduced that emulates a point-to-point network over a WAN.
- Customers opted for VPN services for reducing their OpEx and to bring flexibility.
- Examples : X.25, Frame-Relay, ATM, GRE, DMVPN, IPSec, MPLS, L2TPv3



- Advantages of VPN

Features	Descriptions
Cost effective	replaces the expensive leased line connections
Scalable	Adding a branch is simple by connecting the CE router to the nearest branch office
Secure	Uses modern Encryption protocol such as IPSec with AES ans HMAC-SHA
Better Performance	Uses fiber based data-plane
Flexible	Does not rely on underlaying protocols
Reliable	something...

- MPLS Terms



1.2 VPN Models

Overlay Model	Peer-to-peer model
ISP provides virtual P2P links between customer-sites **Layer 2** : FR, ATM, x.25 **Layer 3** : GRE, DMVPN, IPSec, L2TPv3, SSL VPN	ISP participates in the customer routing GET-VPN, MPLS

- **ACL based Shared Routing** : Each PE router was configured with ACL that would prevent any cross-talk betwenn customer routers (More OpEx)
- **Split Routing** : Every customer was given a dedicated PE Routers (More CapEx)
- **MPLS VPN** Solves the problem with **Virtual Routing an Forwarding (VRF)** where the PE maintains virtual routing table for each customer, isolated from eachother, apart from the global routing table.

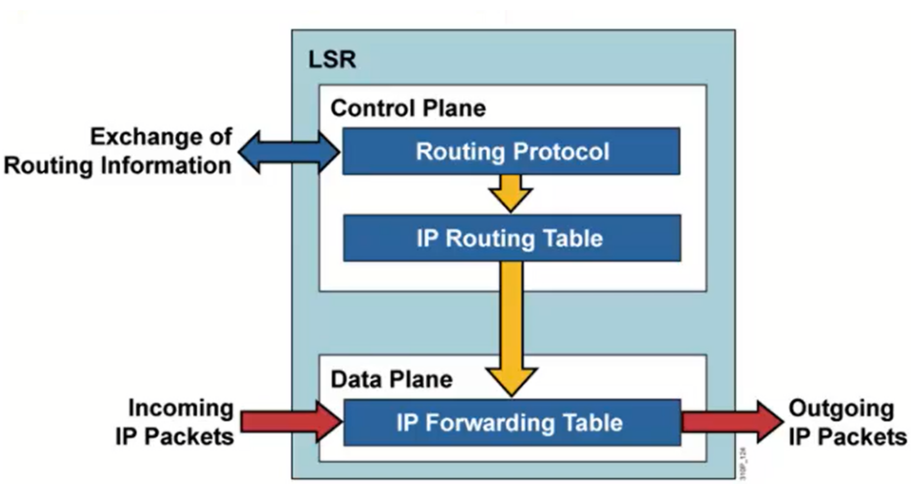
	Advantages	Disadvantages
Overlay	Well known and easy to implement	Optimimal routing requires full-mesh of Virtual Circuits (VC)
	ISP does not participate in cutomer routing	VC to be provissioned manually
	Cusomer and ISP networks are well isolated	Incurs encapsulation overhead
—	—	—

	Advantages	Disadvantages
P2P	Gurantees optimal routing between customers Easier to provision and additional VPN Only Site provisioned, not links between them	ISP must apply filter to the Customer Links ISP is responsible for customer convergence PE routers carry all the routes for all the customer Secure environment must be provided for customers Complex configuration ISP needs detailed IP routing knowledge

1.3 MPLS VPNs

- Forwards packets based on labels instead of IP.
- Combines the best of both Overlay and P2P models.
- The PE router maintans seperate VRF routing tables for each customer (Multi-Tenancy).
- A VPN-V4 peering is eshtablished between PE-PE routers (Similar to a Tunnel).
- The PE router receives a normal IP packet and adds a VPN-Label, the labeled packet will be forwarded to proper destination without seeing the content inside.
- Core ISP routes does not maintain any customer routes : **BGP Free-Core**

1.4 Cisco Express Forwarding (CEF)

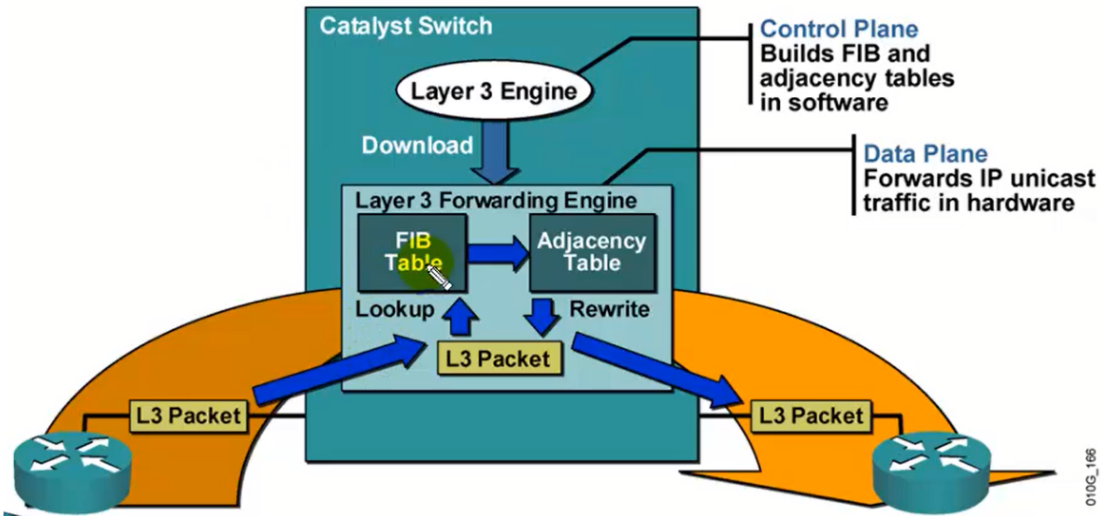


- **Layer 3 switch processing**: When a packet appears to the ingress interface of a router,
  - it sees the destination network IP
  - Performs a Routing table lookup for a next-hop IP address
  - finds the exit interface of the next-hop interface
  - Creates a L2 header, update TTL on IP Header
  - Assemble and send it to the egreee interface

- There are Three Switching modes

Mode	Dription
Process Switching	Requires CPU to be involved with every forwarding decision
Fast Switching	Uses CPU but also caches the most frequently translated informations
CEF	Optimises the process by using dedicated hardware to store pre-computed data

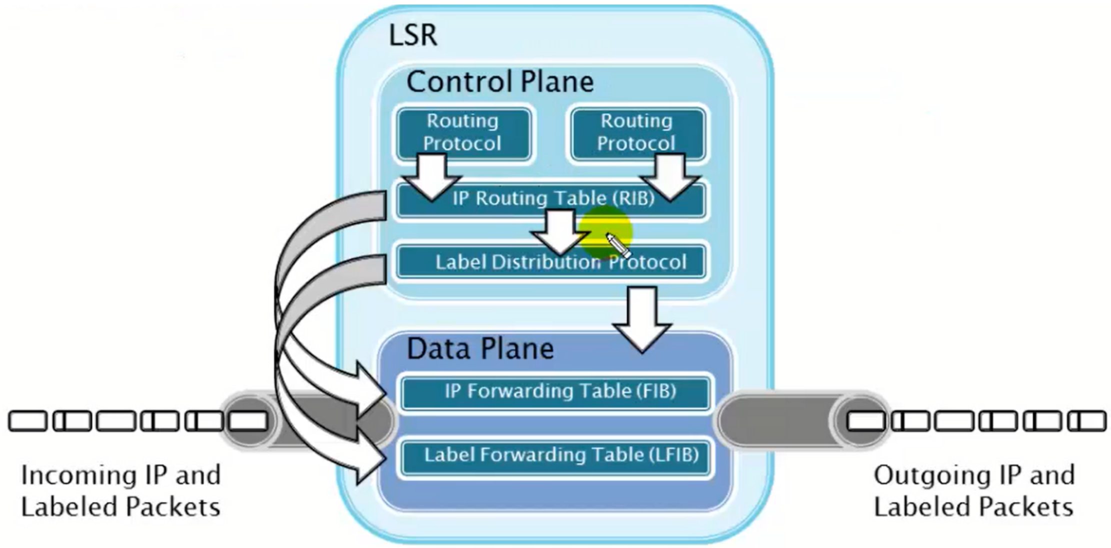
- **CEF in details**
  - L3 routing table (RIB) is downloaded into the hardware (FIB)
  - Lookup is done on the hardwire i.e. in wire-speed
  - The proactive replication of RIB into FIB makes the process optimized.



- To verify CEF : `sh ip cef` maps prefix to nexthop and exit interface
- To Disable CEF and move into fast-switching : `no ip cef`

2 MPLS Label Distibution

2.1 MPLS introduction



- In traditional IP routing method, a destination prefix from a IP packet is checked on the Routing table for the next hop and the exit interface. Routing protocols are used to distribute the routing information
- MPLS relies on the traditional IP routing. A customer packet comes to the ISP edge as a normal IP Packet. The ISP Edge **pushes** a label to the packet while it enters the ISP network. Throught the ISP core the labels are **Swapped** by core routers. The exit edge router **Pops** the label and make it a normal IP packet again. It is Called **Multi-protocols** as it runs on any L2 links (ATM, FR, PPP, HDLC etc.), the **Label Switching** is provided by building Lable binding information (LIB, LFIB) in the hardware lavel using CEF.

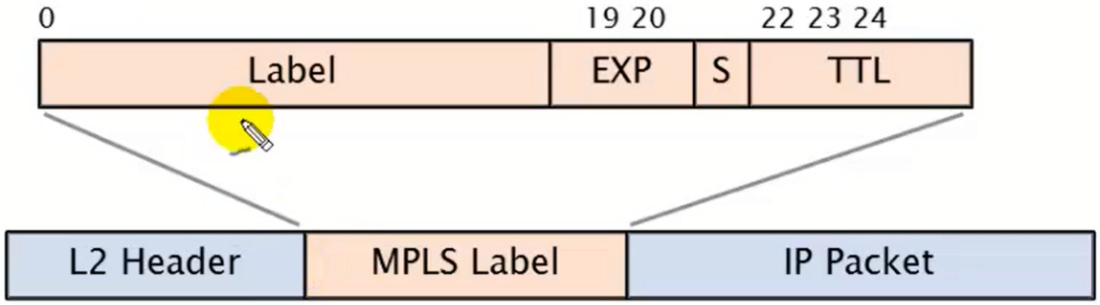
2.1.1 Basic MPLS Terms

- **Core LSR** : Label switched routers are responsible for swapping the label
- **Edge LSR** : Pushes or Pops labels (Ingress LSR and Egress LSR)
- **LSP** : Label switch Path is whre the packets are forwarded based on the labels (not based on IP)

2.1.2 Benifits of MPLS

- MPLS supports multicast routing
- MPLS decreses the overhead on core-routers
- BGP-Free Core : Core routers don't need to maintan any customer routes
- Support Non-IP protocols : as the forwarding process doesn't sees the L3 headers
- Useful for VPN, TE (Traffic Engineering) , QoS, AToM (Any Transport Over MPLS)

2.2 MPLS Labels and Stacks

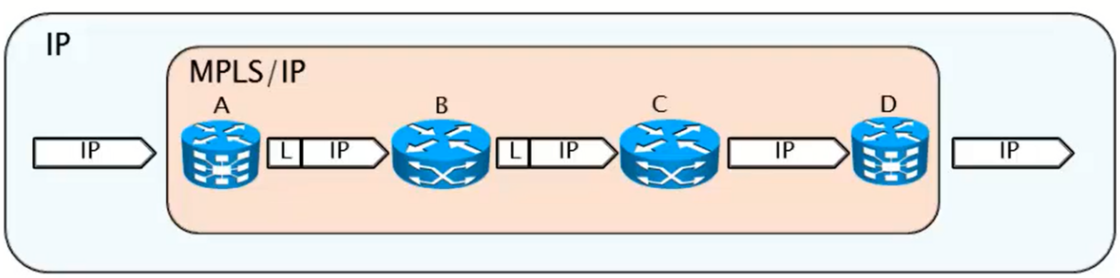


- 32 bits Locally significant.
  - 20 bits : Label
  - 3 bits : Experimental bits, used for QoS marking information
  - 1 bit : Bottom of Stack (BoS) indicates if it is the last label or not.
  - 8 bits : TTL field to prevent loops.
- Labels are distributed by LDP.

2.2.1 MPLS Lable stack

- Usually one one label is assigned to a packet, but multipe lables in a label stack are supprted.
- this is cenarios may produce more than one label.
  - **MPLS VPN (Two lables)** : top label points to the egress router and the second label indentifies the VPN.
  - **MPLS TE (Two or more lables)**: TE uses RSVP instead of LDP. The top label points to the endpoint of the traffic engineering tunnel and the second label points to the destination
  - MPLS VPNS combined with MPLS TE.

2.3 Sharing of the Label Information

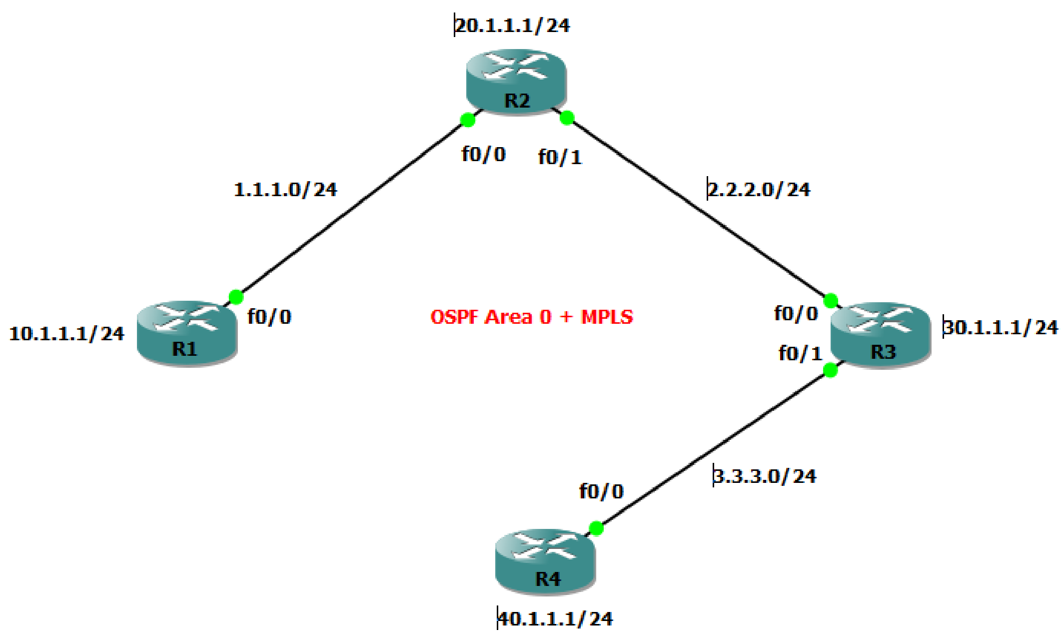


- MPLS does not share the label iformation automatically, it needs a distribution protocol using the IGP in the ISP core. The following protols are majorly used to do so.

Protocols	Descriptons

Protocols	Descriptons
TDP	Cisco Prop Obsolete TCP port 711
LDP	Standard Default on cisco UDP port 646
RSVP	used for MPLS TE Labels

2.4 Configuring LDP in ISP Core



2.4.1 Base Config

```
!r1
conf t
    int f0/0
        ip add 1.1.1.1 255.255.255.0
        no sh
    int l0
        ip add 10.1.1.1 255.255.255.0
    router os 1
        pass def
        net 0.0.0.0 0.0.0.0 a 0
        no pass f0/0
end
```

```
!r2
conf t
    int f0/0
        ip add 1.1.1.2 255.255.255.0
        no sh
    int f0/1
        ip add 2.2.2.2 255.255.255.0
        no sh
    int l0
        ip add 20.1.1.1 255.255.255.0
    router os 1
        pass def
        net 0.0.0.0 0.0.0.0 a 0
        no pass f0/0
        no pass f0/1
end

!r3
conf t
    int f0/0
        ip add 2.2.2.3 255.255.255.0
        no sh
    int f0/1
        ip add 3.3.3.3 255.255.255.0
        no sh
    int l0
        ip add 30.1.1.1 255.255.255.0
    router os 1
        pass def
        net 0.0.0.0 0.0.0.0 a 0
        no pass f0/0
        no pass f0/1
end

!r1
conf t
    int f0/0
        ip add 3.3.3.4 255.255.255.0
        no sh
    int l0
        ip add 40.1.1.1 255.255.255.0
    router os 1
        pass def
        net 0.0.0.0 0.0.0.0 a 0
        no pass f0/0
end
```

Pre-Requisete : CEF must be runing on the routers to enable LDP

```
R1#sh ip cef 20.1.1.0 255.255.255.0
20.1.1.0/24, version 23, epoch 0, cached adjacency 1.1.1.2
0 packets, 0 bytes
  via 1.1.1.2, FastEthernet0/0, 0 dependencies
    next hop 1.1.1.2, FastEthernet0/0
    valid cached adjacency

R1#sh ip cef 30.1.1.0 255.255.255.0
30.1.1.0/24, version 24, epoch 0, cached adjacency 1.1.1.2
0 packets, 0 bytes
  via 1.1.1.2, FastEthernet0/0, 0 dependencies
    next hop 1.1.1.2, FastEthernet0/0
    valid cached adjacency

R1#sh ip cef 40.1.1.0 255.255.255.0
40.1.1.0/24, version 25, epoch 0, cached adjacency 1.1.1.2
0 packets, 0 bytes
  via 1.1.1.2, FastEthernet0/0, 0 dependencies
    next hop 1.1.1.2, FastEthernet0/0
    valid cached adjacency
```

2.4.2 Activating LDP

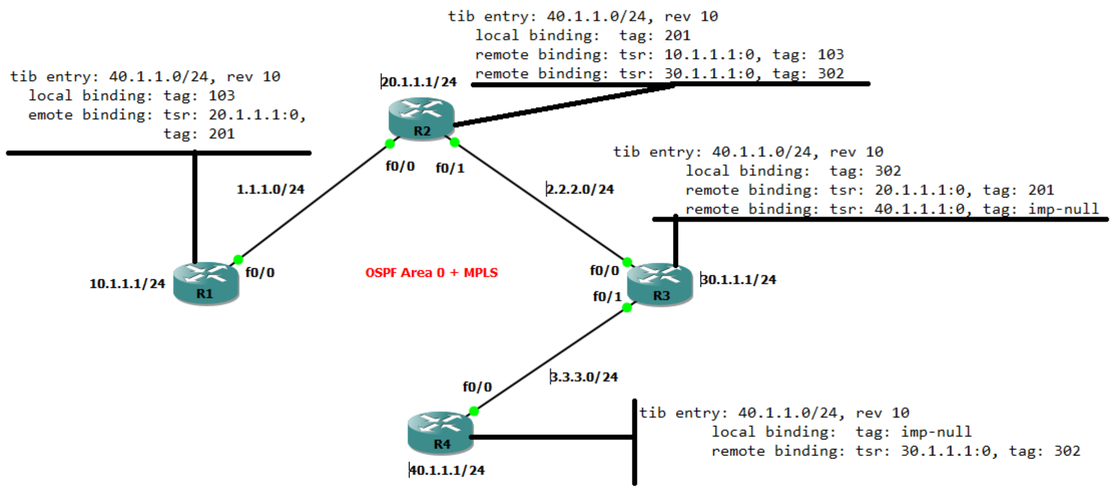
```
!r1
conf t
    mpls label protocol ldp  ! optional
    mpls label range 100 199
    mpls ldp router-id loop0 ! optional but RID must be reachable

    int f0/0
        mpls ip    ! activate ldp on the interface
end

!verification
sh mpls ldp nei    ! shows ldp neighburs
sh mpls ldp int    ! shows ldp enabled interfaces
sh mpls ldp binding A.B.C.D CIDR       ! shows local binding
sh mpls forwarding-table               ! shows LFIB
trace 40.1.1.1     ! shows the LSP
```

2.5 LDP Forwarding process

- IGP builds routing table (FIB using CEF)
- LSR assigns a local label for each route learnt
- LSR Share the label with nighbours using LDP
- Based on the collected information, LSR builds their LFIB.

- Routers will local prefix uses label ID = 3 called Implecit Null.
- **TIB**: Tag Information Base, **TSR**: Tag Switch Router

The following figure depicts the LIB of the 4 LSRs with respect to 40.1.1.0/24 prefix using **`sh mpls ldp binfing 40.1.1.0 24`** command.



The following list presents the complete LFIB desciption of all the routers. Using **`sh mpls forwarding-table`** command

LFIB of Router R1

Local tag	Outgoing tag or VC	Prefix or Tunnel Id	Bytes tag switched	Outgoing interface	Next Hop
100	Pop tag	2.2.2.0/24	0	Fa0/0	1.1.1.2
101	200	3.3.3.0/24	0	Fa0/0	1.1.1.2
102	Pop tag	20.1.1.0/24	0	Fa0/0	1.1.1.2
103	201	40.1.1.0/24	0	Fa0/0	1.1.1.2
104	203	30.1.1.0/24	0	Fa0/0	1.1.1.2

LFIB of Router R2

Local tag	Outgoing tag or VC	Prefix or Tunnel Id	Bytes tag switched	Outgoing interface	Next Hop
200	Pop tag	3.3.3.0/24	0	Fa0/1	2.2.2.3
201	302	40.1.1.0/24	1200	Fa0/1	2.2.2.3
202	Pop tag	10.1.1.0/24	0	Fa0/0	1.1.1.1
203	Pop tag	30.1.1.0/24	0	Fa0/1	2.2.2.3

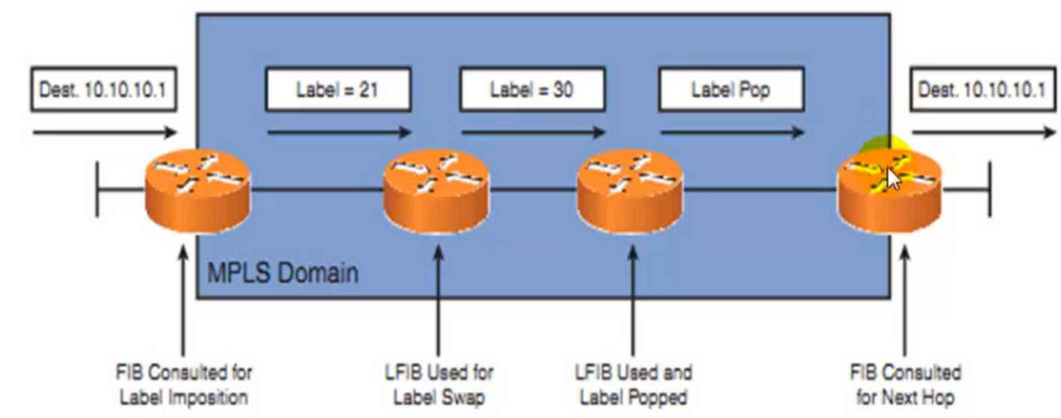
LFIB of Router R3

Local tag	Outgoing tag or VC	Prefix or Tunnel Id	Bytes tag switched	Outgoing interface	Next Hop
300	Pop tag	1.1.1.0/24	1302	Fa0/0	2.2.2.2
301	Pop tag	20.1.1.0/24	0	Fa0/0	2.2.2.2
302	Pop tag	40.1.1.0/24	1260	Fa0/1	3.3.3.4
303	202	10.1.1.0/24	0	Fa0/0	2.2.2.2

LFIB of Router 4

Local tag	Outgoing tag or VC	Prefix or Tunnel Id	Bytes tag switched	Outgoing interface	Next Hop
400	300	1.1.1.0/24	0	Fa0/0	3.3.3.3
401	Pop tag	2.2.2.0/24	0	Fa0/0	3.3.3.3
402	301	20.1.1.0/24	0	Fa0/0	3.3.3.3
403	303	10.1.1.0/24	0	Fa0/0	3.3.3.3
404	Pop tag	30.1.1.0/24	0	Fa0/0	3.3.3.3

2.6 Penultimate Hop Popping (PHP)



- A built-in feature to **optimize** the MPLS performance
- PHP removes the requirement for a **double lookup** to be performed on an egress PE. Without PHP, when a labeled packet appears on its egress LSR, the LSR first looks up the LFIB and finds the prefix is local. Then, it needs to lookup its FIB to find its exit interface. Therefore, two lookups.
- Egress router assigns **imp-null** (Label 3) to all its local prefixes and advertises to its LDP neighbours. The Penultimate (Second to Last) router pops the label and send the packet to the egress router as a normal IP packet.
- The PHP router put a **pop-tag** label at its LFIB for the prefixes it received **imp-null**.

```
R3#sh mpls forwarding-table 40.1.1.0 24
Local  Outgoing    Prefix            Bytes tag  Outgoing   Next Hop
tag    tag or VC   or Tunnel Id      switched   interface
302    Pop tag     40.1.1.0/24       1260       Fa0/1      3.3.3.4
```

- To disable PHP, use the **`mpls ldp explicit-null`** command. The Egress router sends a **label=0** instead of 3. It is recommanded when using **MPLS QoS** , if the last router doesn't receive labeled packet then, the end-to-end Marking will not be guranteed.

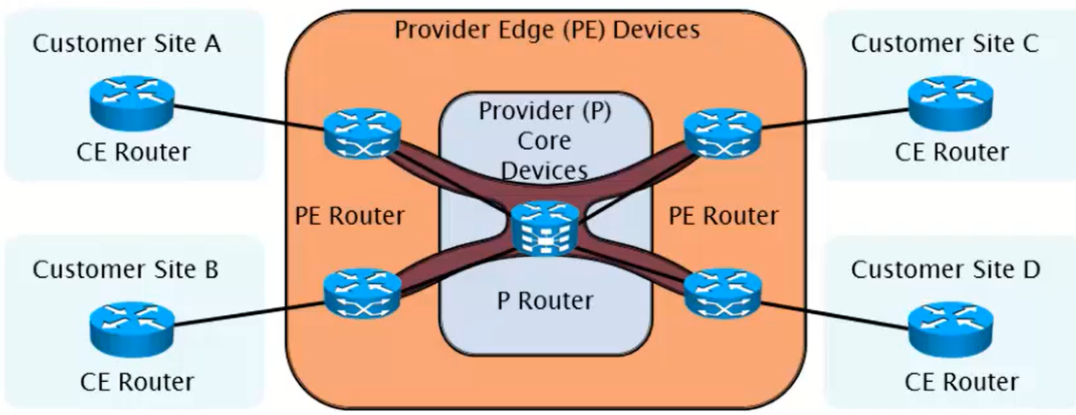
2.7 LDP Troubleshoting

2.7.1 Possible issues

- `mpls ip` command is not enabled in the interface
- Protocol mismatch (LDP/TDP) global or at local interface level
- Higher loopback IP is taken as RID which is not advertised by IGP
- Authentication mismatch
- Port 646 is filterred

3 MPLS VPN

3.1 Introduction to MPLS VPN



- Packet forwarding takes place based on labels instead of the IP
- Combines the best of both overlay and peer-to-peer model
- Customer advertises its routes to the PE router.
- PE maintains customer routes into seperate routing table
- a VPN-v4 peering must be established between PE-PE (e.g. a GRE Tunnel)
- When Customer routes enters the ISP core, The PE **Pushes** a label on the packet.
- ISP core routers (P) only swaps the label and forwards the labels based on the labels only. As a result the P routes don't need to maintain any customer routes, hence achiecing a **BGP Free Core**.

3.2 Steps to Configure MPLS L3 VPN

- **Step 1**: Configure IGP inside ISP core (mostly OSPF or IS-IS protocols are preferred)
- **Step 2**: Configure MPLS LDP inside the SP Core
- **Step 3**: Create VRF, and assign RD, RT
- **Step 4**: Configure VPNv4 peering between both PE routers
- **Step 5**: Configure Routing between PE and CE (Static/Default, IGP, BGP)
- **Step 6**: Configure Redistribution on PE Routers

```
[ ]:
```