CS 540
Computer Networks II

Sandy Wang
chwang_98@yahoo.com

MPLS

Topics

1. Overview
2. LAN Switching
3. IPv4
4. IPv6
5. Tunnels
6. Routing Protocols -- RIP, RIPng
7. Routing Protocols -- OSPF
8. IS-IS
9. Midterm Exam
10. BGP
11. **MPLS**
12. Transport Layer -- TCP/UDP
13. Congestion Control & Quality of Service (QoS)
14. Access Control List (ACL)
15. Final Exam

Reference Books

- **Cisco CCNA Routing and Switching ICND2 200-101 Official Cert Guide, Academic Edition** by Wendel Odom -- July 10, 2013**.** ISBN-13: 978-1587144882
- **The TCP/IP Guide: A Comprehensive, Illustrated Internet Protocols Reference** by Charles M. Kozierok – October 1, 2005. ISBN-13: 978-1593270476
- **Data and Computer Communications (10th Edition) (William Stallings Books on Computer and Data Communications)** by Williams Stallings – September 23, 2013. ISBN-13: 978-0133506488

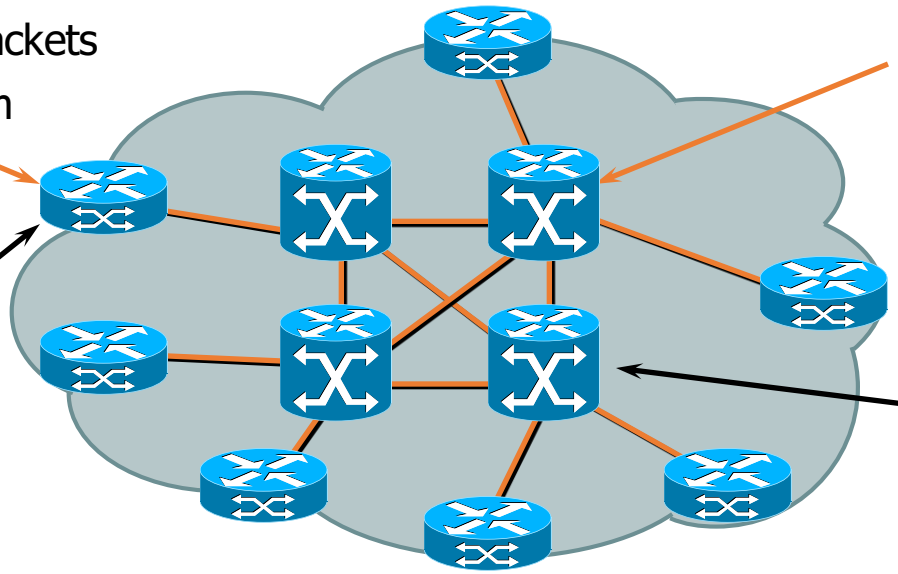
http://class.svuca.edu/~sandy/class/CS540/

Agenda

- Introduction to MPLS
- LDP
- MPLS VPN

MPLS Concept

- At Edge:
  - Classify packets
  - Label them
- In Core:
  - Forward using labels (as opposed to IP addr)
  - Label indicates service class and destination



Edge Label Switch Router

Label Switch Router (LSR)

Label Distribution Protocol (LDP)

Major RFCs

- RFC 3031 -- Multiprotocol Label Switching Architecture
- RFC 5036 -- LDP Specification

MPLS concept

- MPLS: Multi Protocol Label Switching
- Packet forwarding is done based on Labels.
- Labels are assigned when the packet enters into the network.
- Labels are on top of the packet.
- MPLS nodes forward packets/cells based on the label value (not on the IP information).

MPLS concept

- MPLS allows:
  - Packet classification only where the packet enters the network.
  - The packet classification is encoded as a label.
  - In the core, packets are forwarded without having to re-classify them.
    - No further packet analysis
    - Label swapping

Terminology

- LDP – Label Distribution Protocol control protocol for xchang btw 2 MPLS
- LSP – Label-Switched Path
- LSR – Label Switch Router
- LIB -- Label Information Base : database.
- FEC -- Forwarding Equivalence Class
  - A group of IP packets which are forwarded in the same manner

- NHLFE -- Next Hop Label Forwarding Entry

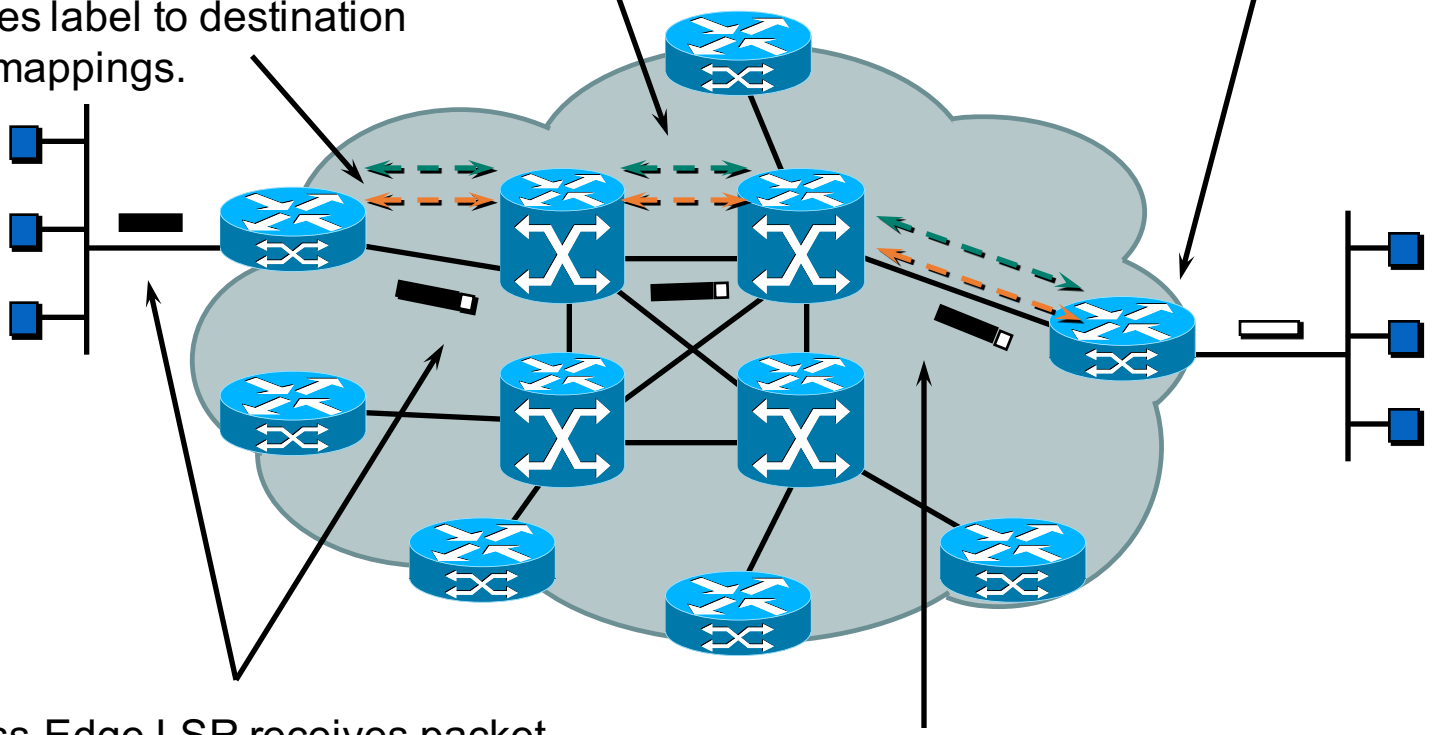
  Contains the forwarding information
  - the packet's next hop
  - the operation to perform on the packet's label stack
    - Swap, push. pop

MPLS Operation

1a. Existing routing protocols (e.g. OSPF, IS-IS) establish reachability to destination networks.

1b. Label Distribution Protocol (LDP) establishes label to destination network mappings.

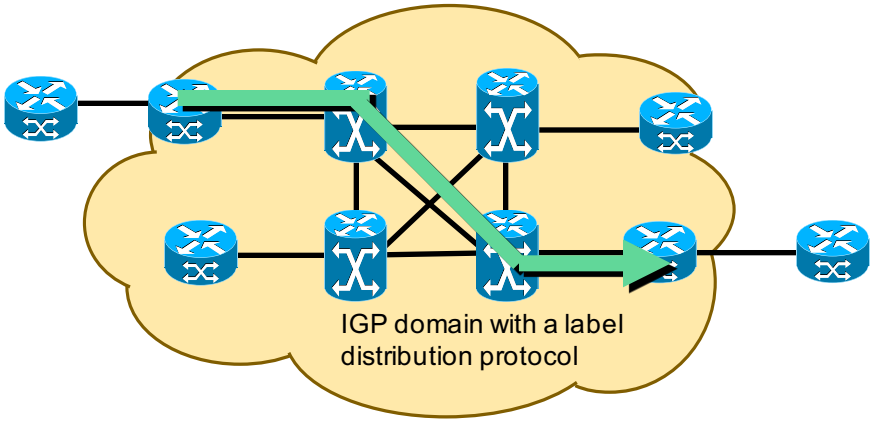
4. Edge LSR at egress removes(POP) label and delivers packet.



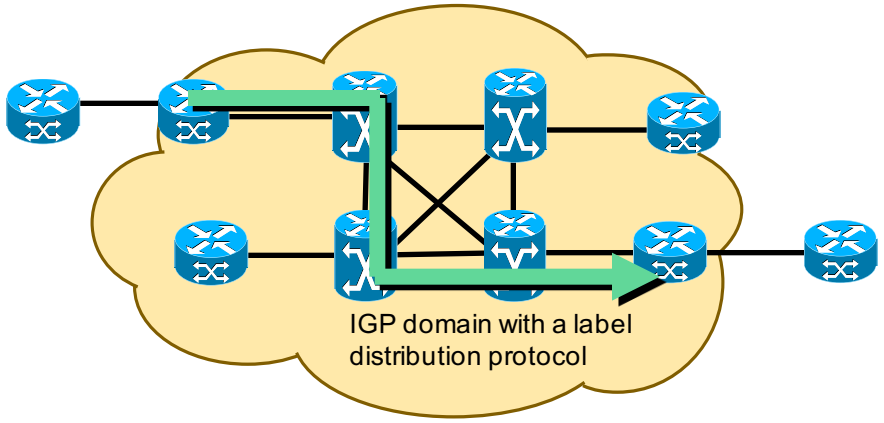
2. Ingress Edge LSR receives packet, performs Layer 3 value-added services, and labels(PUSH) packets.

3. LSR switches packets using label swapping(SWAP) .

Label Switch Path (LSP)



LSP follows IGP shortest path



LSP diverges from IGP shortest path

- LSPs are derived from IGP routing information
- LSPs may diverge from IGP shortest path
- LSPs are unidirectional

  Return traffic takes another LSP

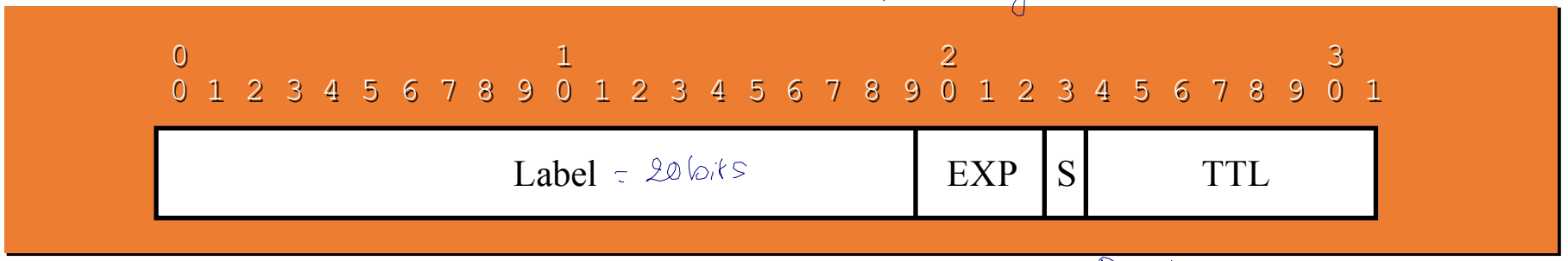
MPLS : 2.5 layer.

Encapsulations

LAN MAC Label Header

Label Header

ethernet header 14 bytes
trailer 4 bytes.
v4 20 bytes
v6 40 bytes
MPLS 4 bytes.



Label = 20 bits

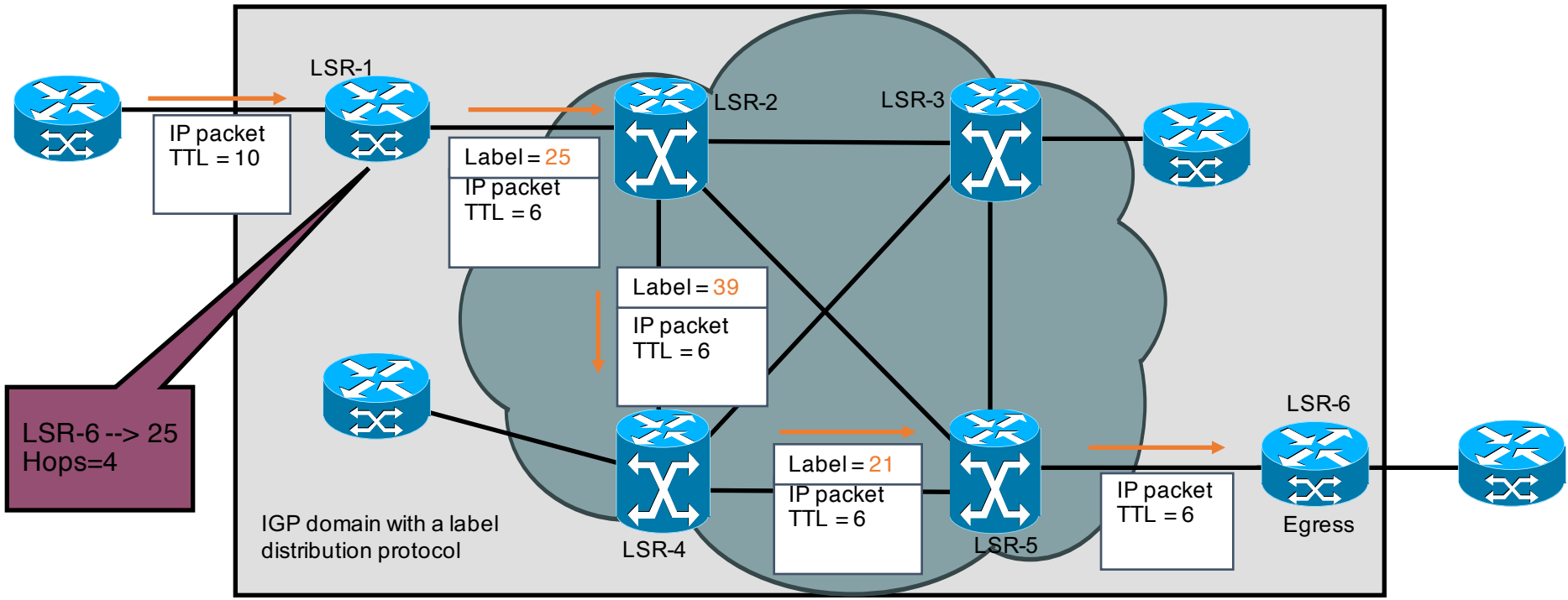
EXP = Class of Service, 3 bits (Priority)

S = Bottom of Stack, 1 bit

TTL = Time to Live, 8 bits

- Header= 4 bytes, Label = 20 bits.
- Can be used over Ethernet, 802.3, or PPP links
- Contains everything needed at forwarding time

Loops and TTL



- TTL is decremented prior to enter the non-TTL capable LSP

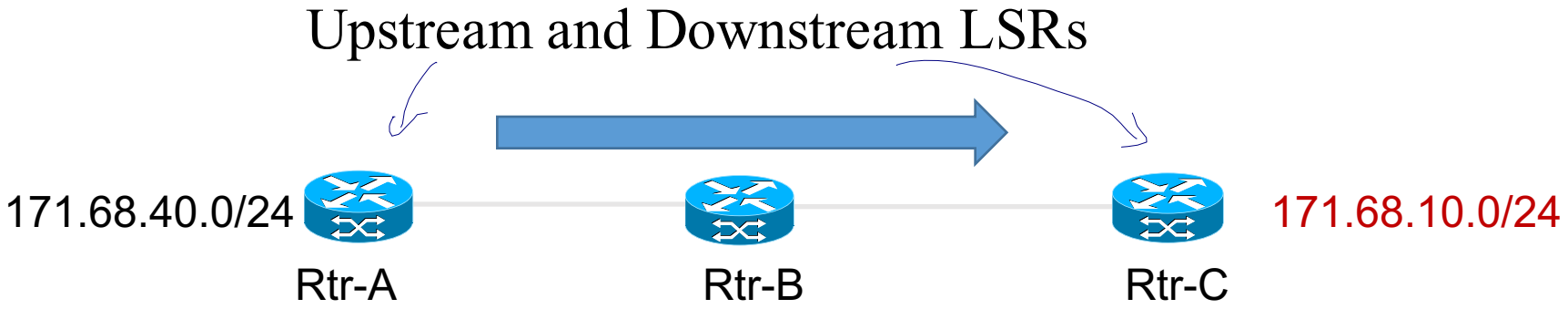
  If TTL is 0 the packet is discarded at the ingress point

- TTL is examined at the LSP exit

Label Assignment and Distribution

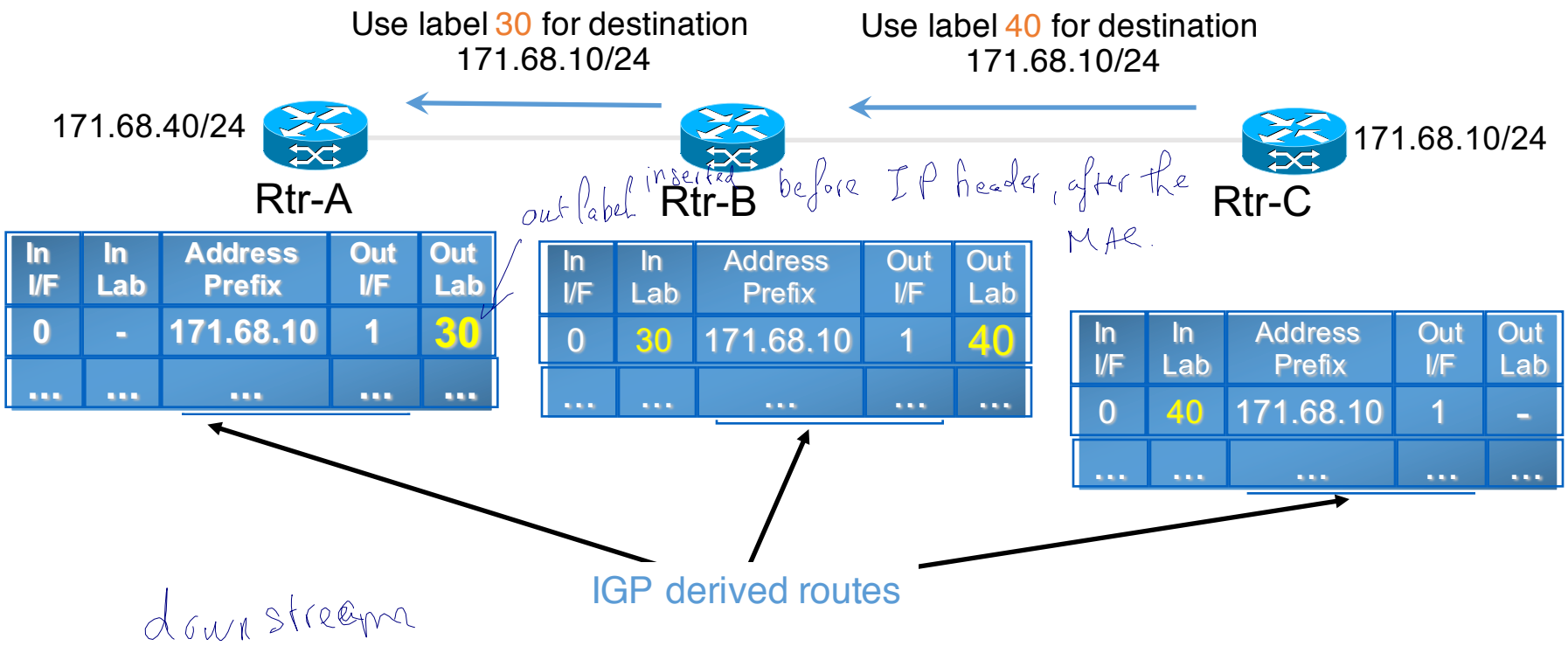
- Labels have link-local significance:
  - Each LSR binds his own label mappings
- Each LSR assign labels to his FECs
- Labels are assigned and exchanged between adjacent LSR

Label Assignment and Distribution



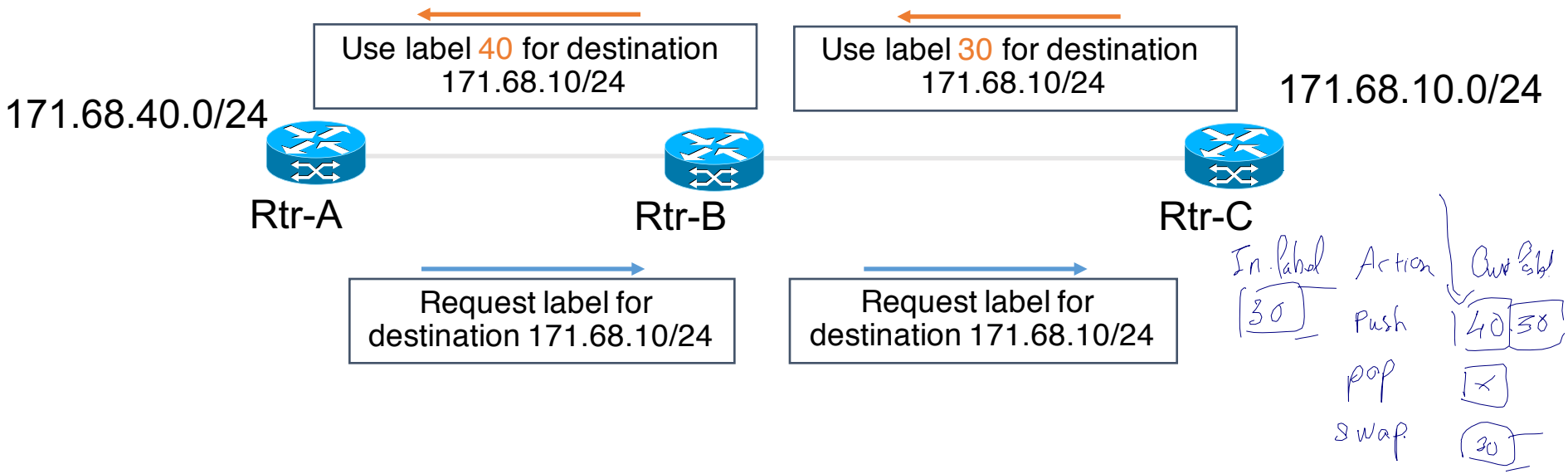
- Rtr-C is the downstream neighbor of Rtr-B for destination 171.68.10.0/24
- Rtr-B is the downstream neighbor of Rtr-A for destination 171.68.10.0/24
- LSRs know their downstream neighbors through the IP routing protocol
  - Next-hop address is the downstream neighbor

Unsolicited Downstream Distribution



- LSRs distribute labels to the upstream neighbors

On-Demand Downstream Distribution



- Upstream LSRs request labels to downstream neighbors
- Downstream LSRs distribute labels upon request

Label Retention Modes

- Label retention mode refers to the way in which an LSR treats label mappings it is not currently using.
- Liberal retention mode
  - LSR retains labels from all neighbors
    - should a topology change occur, the labels to use in the new topology are usually already in place
    - Require more memory and label space
- Conservative retention mode
  - LSR retains labels only from next-hops neighbors
    - Any label mapping received from a peer LSR that is not used in an active NHLFE (Next Hop Label Forwarding Entry) is released
    - Delay in obtaining new labels when a topology change occurs.
    - Free memory and label space

Label Distribution Control Modes

- Independent LSP control

  LSR binds a Label to a FEC independently, whether or not the LSR has received a Label the next-hop for the FEC

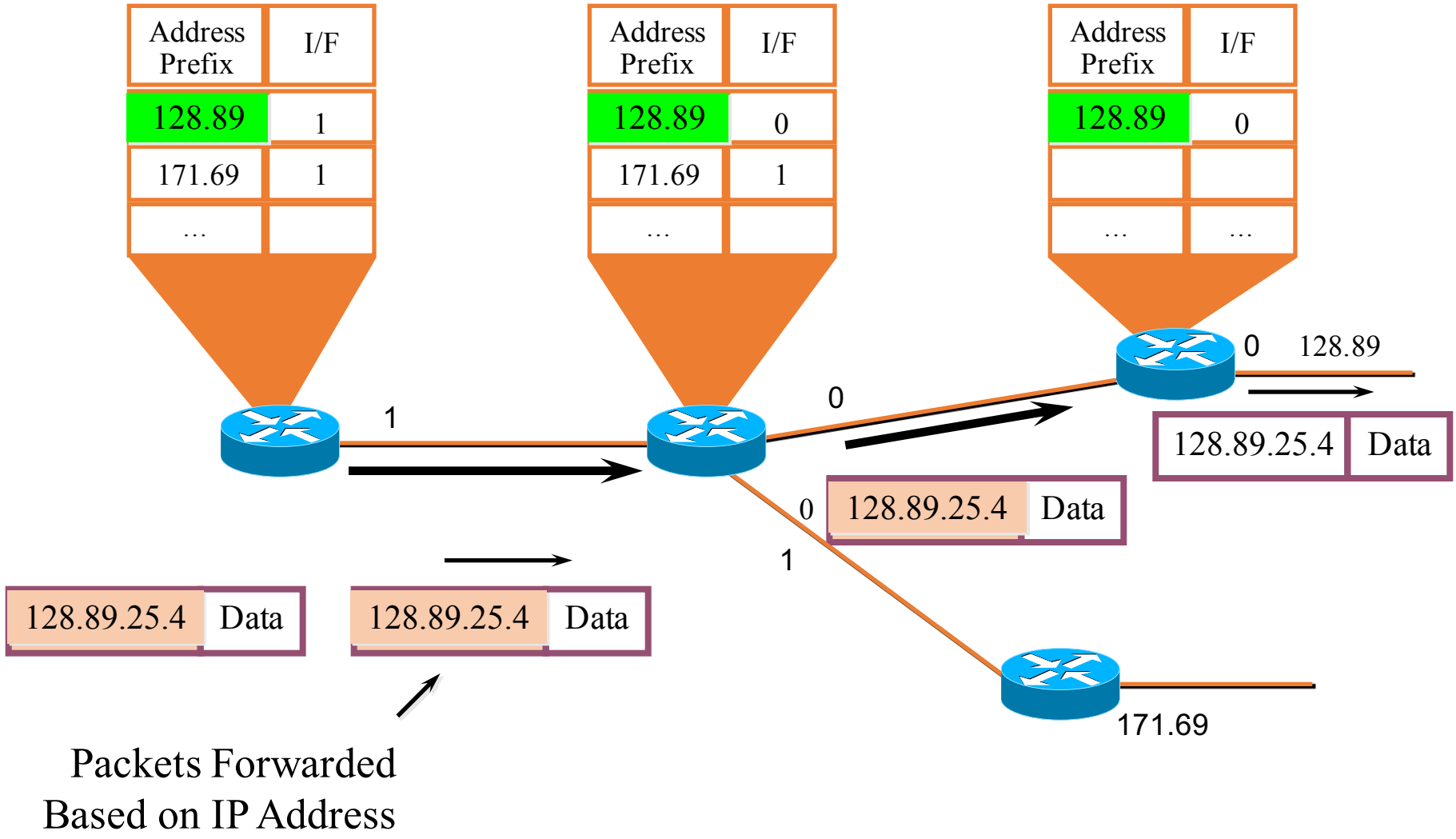
  The LSR then advertises the Label to its neighbor

- Ordered LSP control

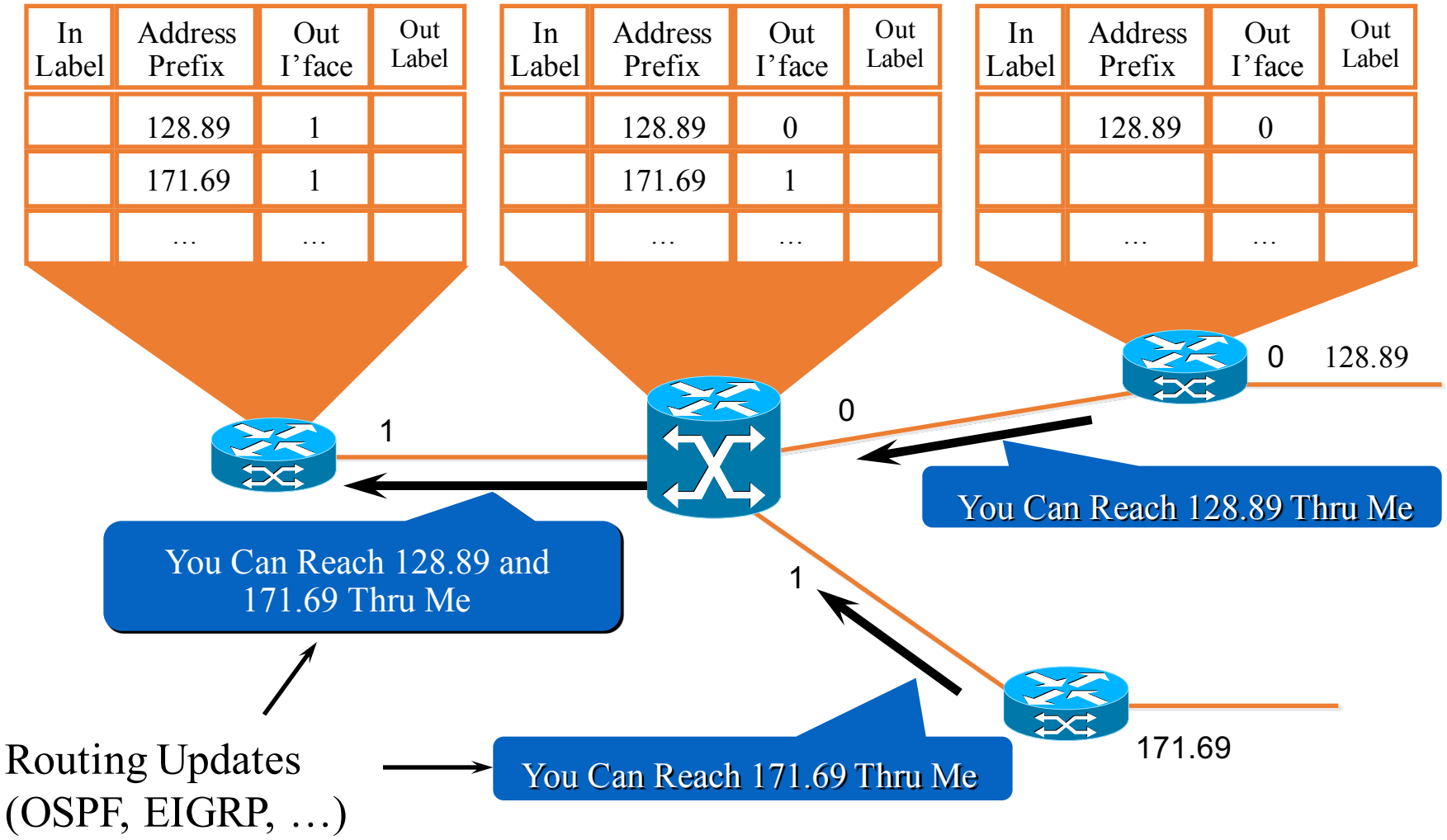
  LSR only binds and advertise a label for a particular FEC if:

  - it is the egress LSR for that FEC or
  - it has already received a label binding from its next-hop

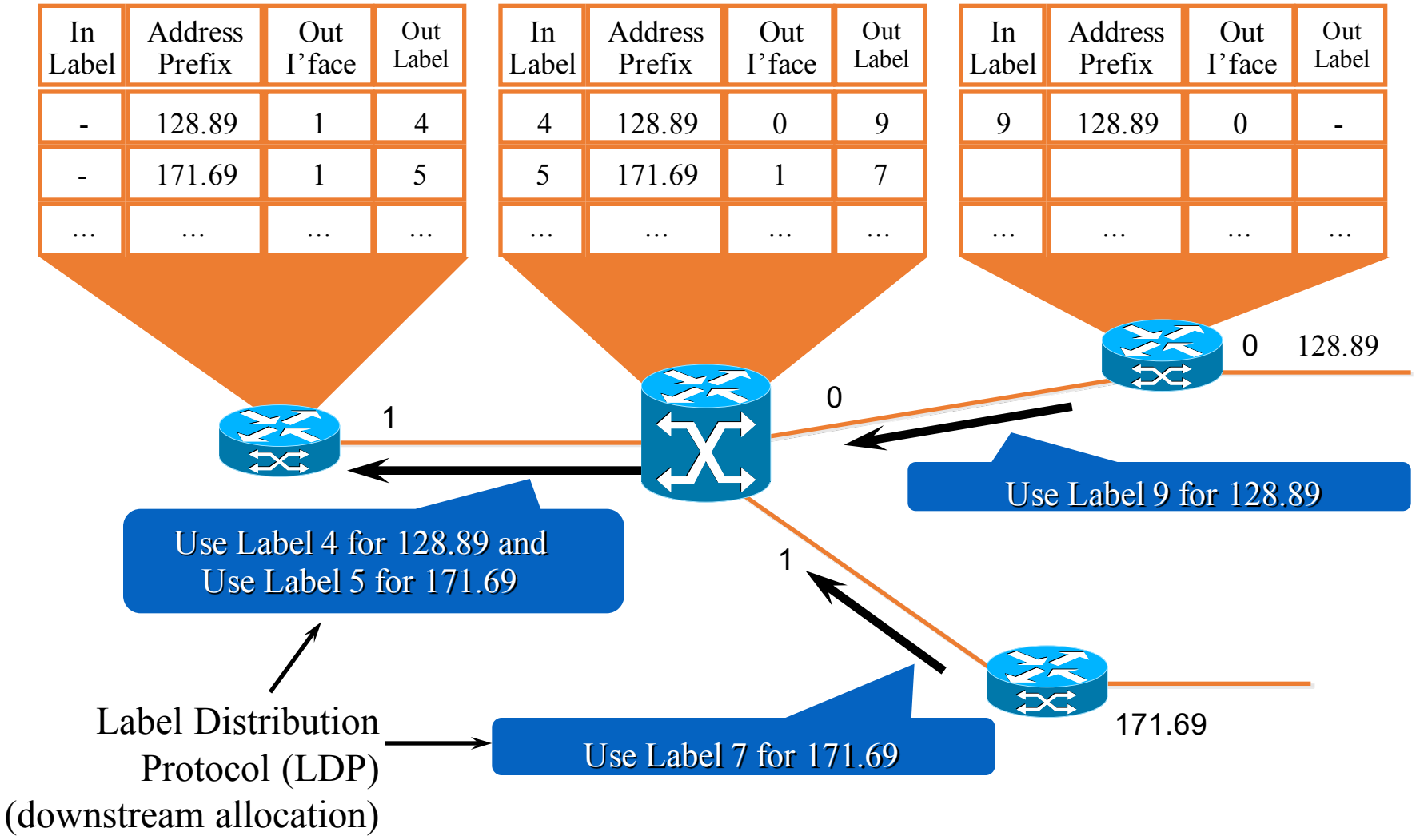
Router Example: Forwarding Packets



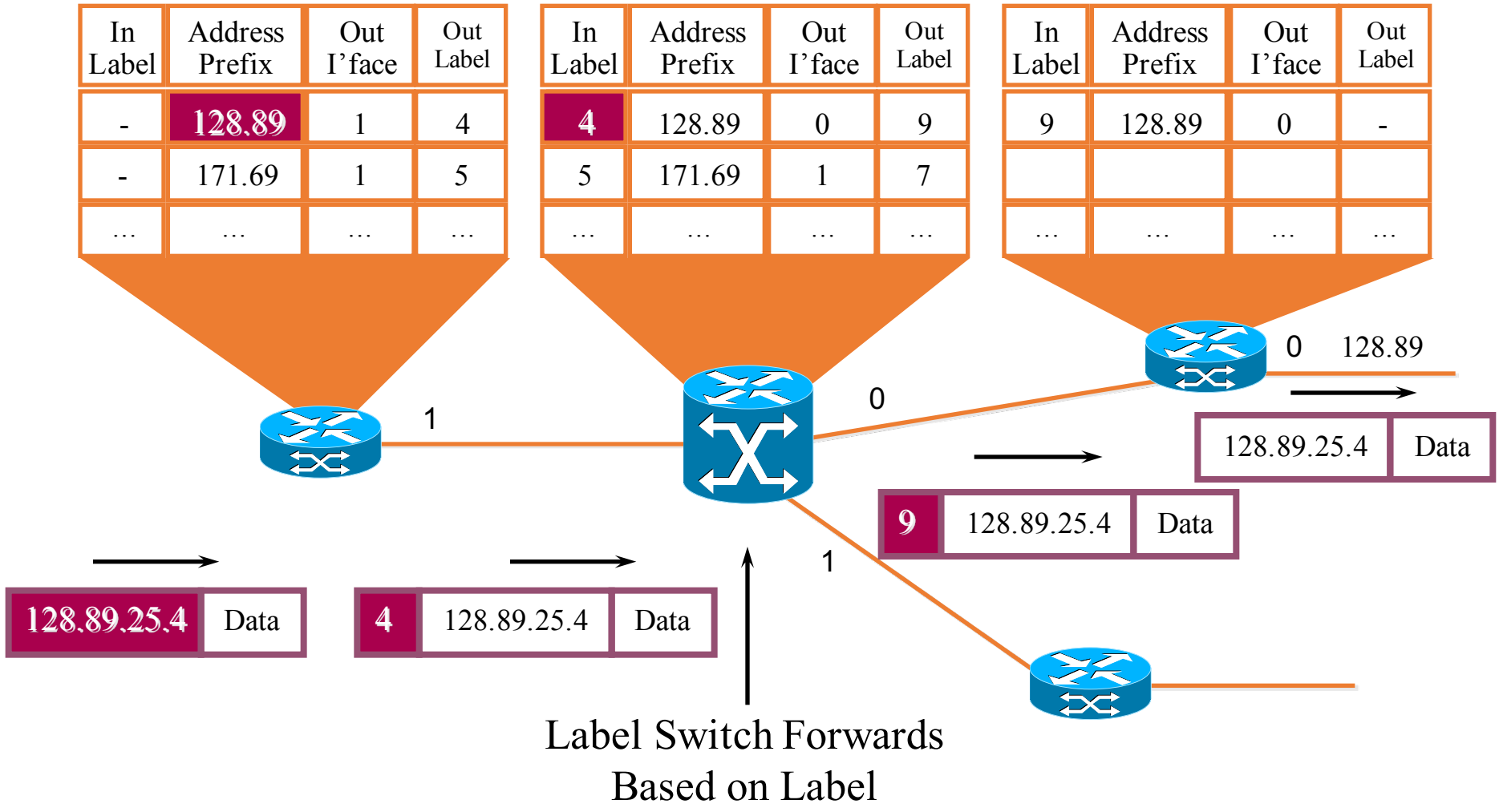
MPLS Example: Routing Information



MPLS Example: Assigning Labels



MPLS Example: Forwarding Packets



Agenda

- Introduction to MPLS
- LDP
- MPLS VPN

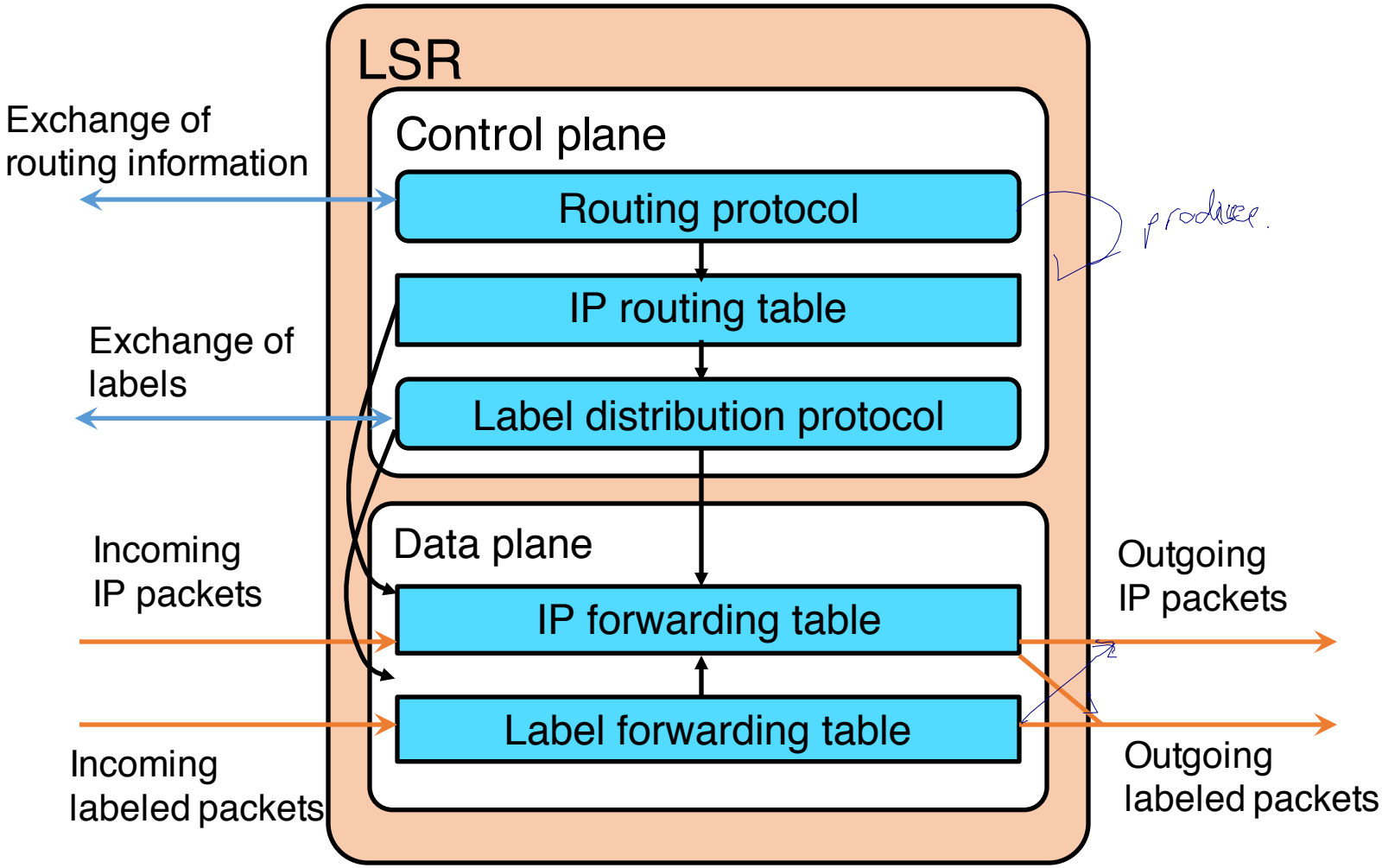
MPLS Unicast IP Routing

- MPLS introduces a new field that is used for forwarding decisions.
- Although labels are locally significant, they have to be advertised to directly reachable peers.
  - One option would be to include this parameter into existing IP routing protocols.
  - The other option is to create a new protocol to exchange labels.
- The second option has been used because there are too many existing IP routing protocols that would have to be modified to carry labels.

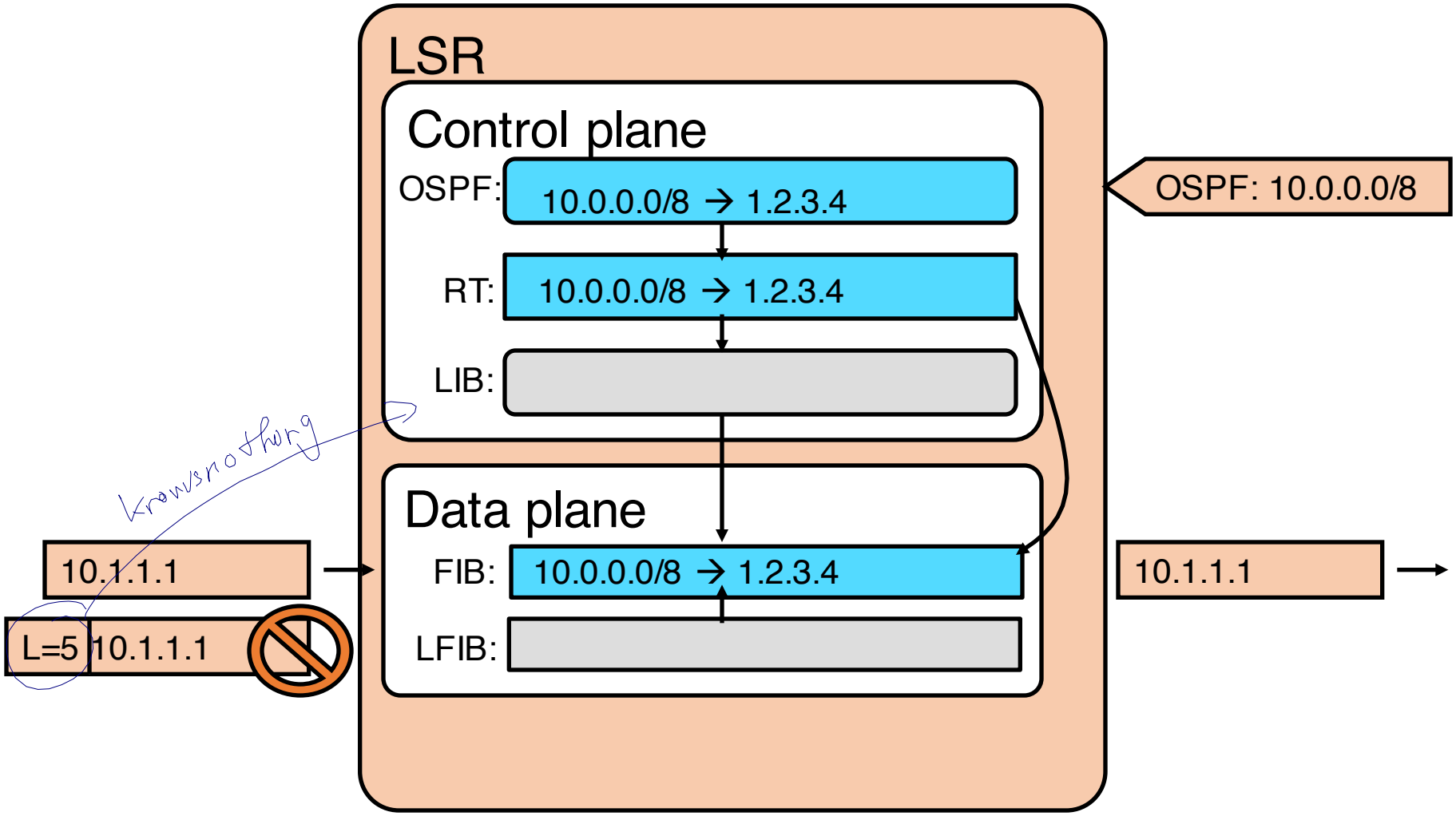
Label Distribution Protocol

- Defined in RFC 3036 and 3037
- Used to distribute labels in a MPLS network
- Forwarding equivalence class
  - How packets are mapped to LSPs (Label Switched Paths)
- Advertise labels per FEC
  - Reach destination a.b.c.d with label x
- Neighbor discovery
  - Basic and extended discovery

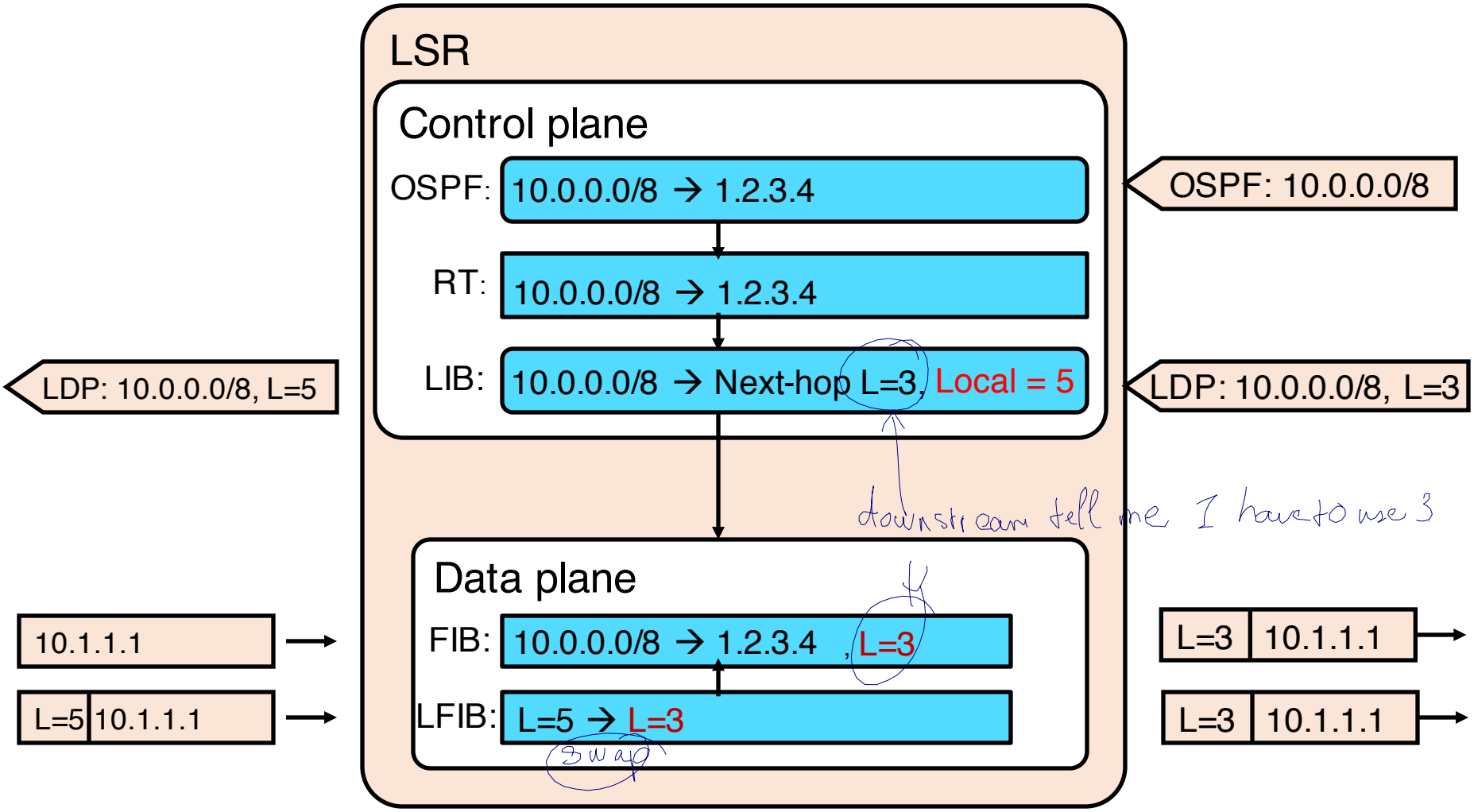
MPLS Unicast IP Routing Architecture



MPLS Unicast IP Routing: Example



MPLS Unicast IP Routing: Example

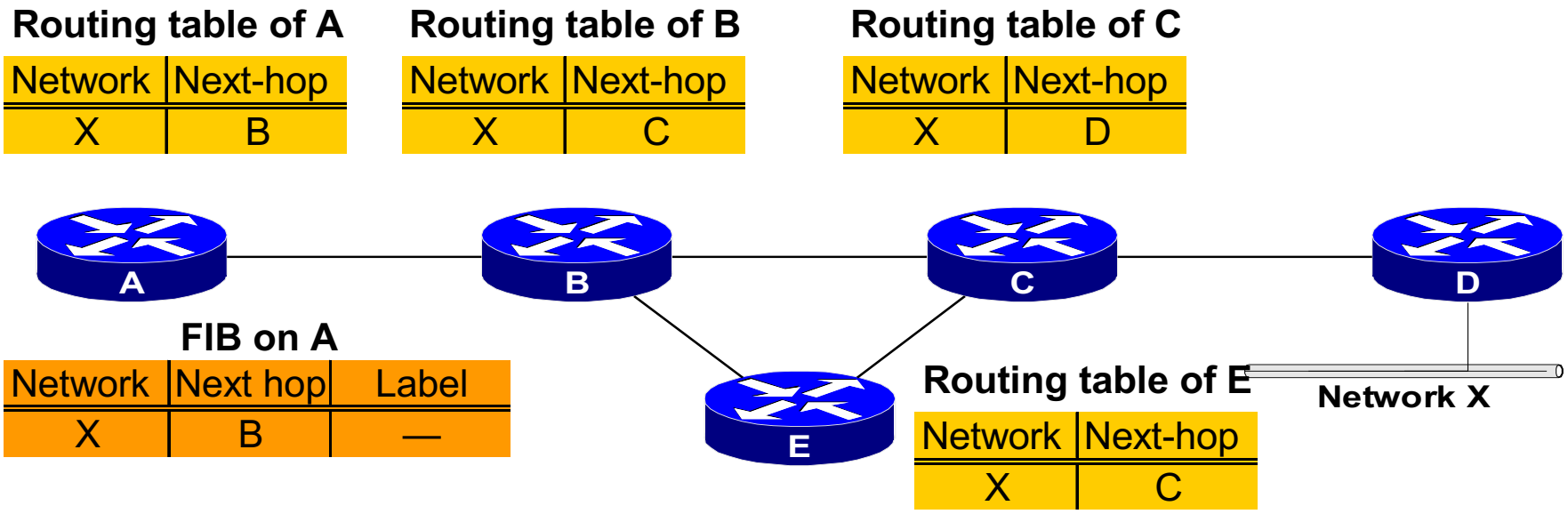


Label Allocation in Packet-Mode MPLS Environment

Label allocation and distribution in packet-mode MPLS environment follows these steps:

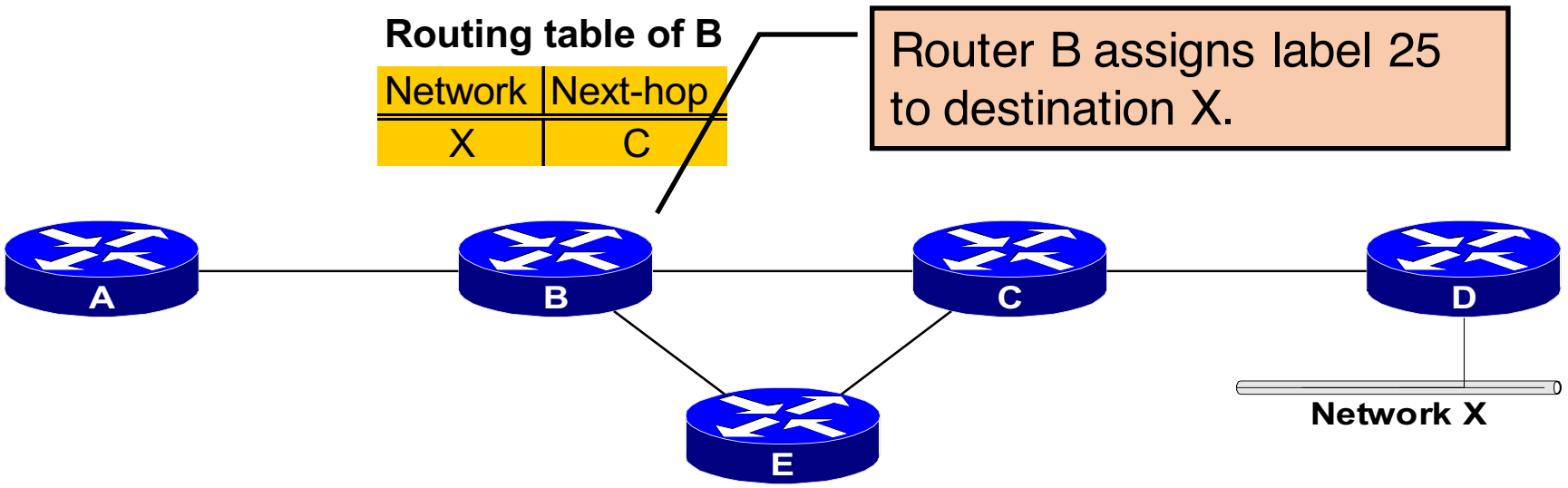
1. IP routing protocols build the IP routing table.
2. Each LSR assigns a label to every destination in the IP routing table independently.
3. LSRs announce their assigned labels to all other LSRs.
4. Every LSR builds its LIB, LFIB data structures based on received labels.

Building the IP Routing Table



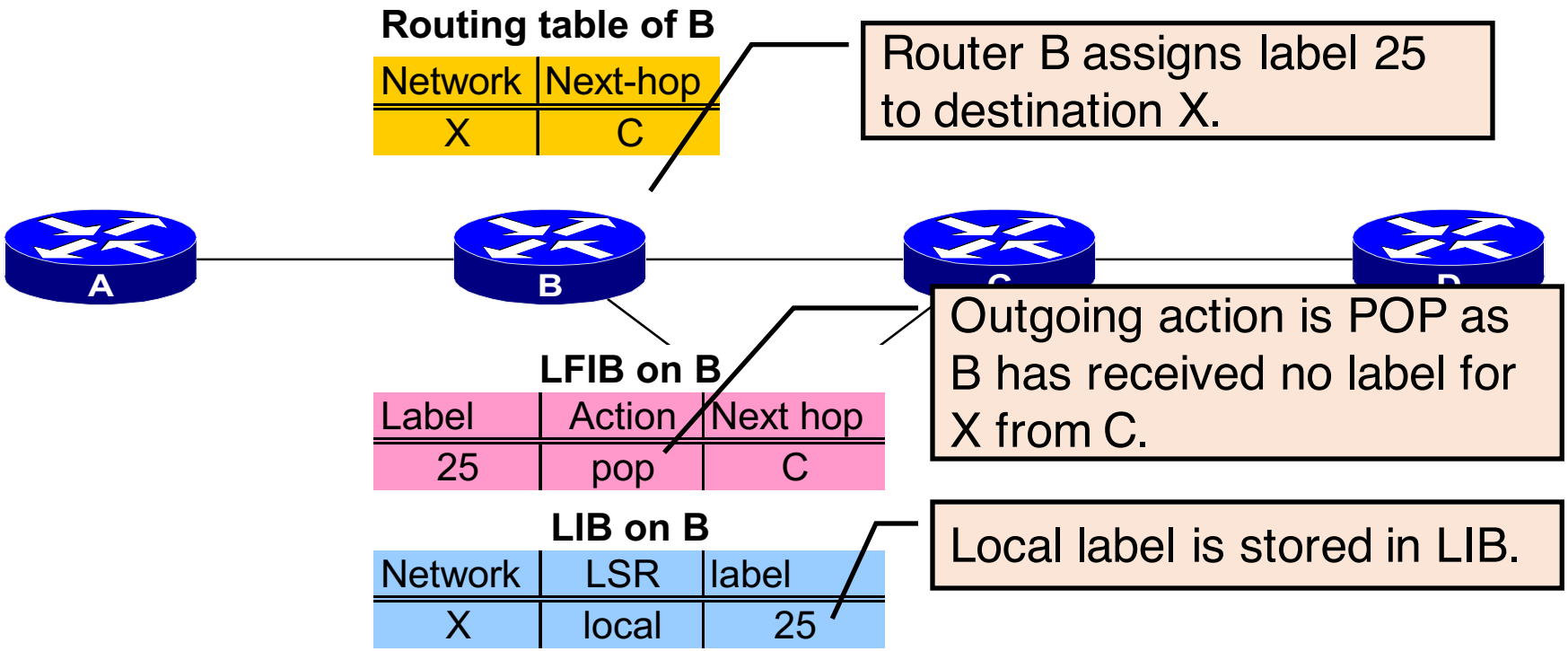
- IP routing protocols are used to build IP routing tables on all LSRs.
- Forwarding tables (FIB) are built based on IP routing tables with no labeling information.

Allocating Labels



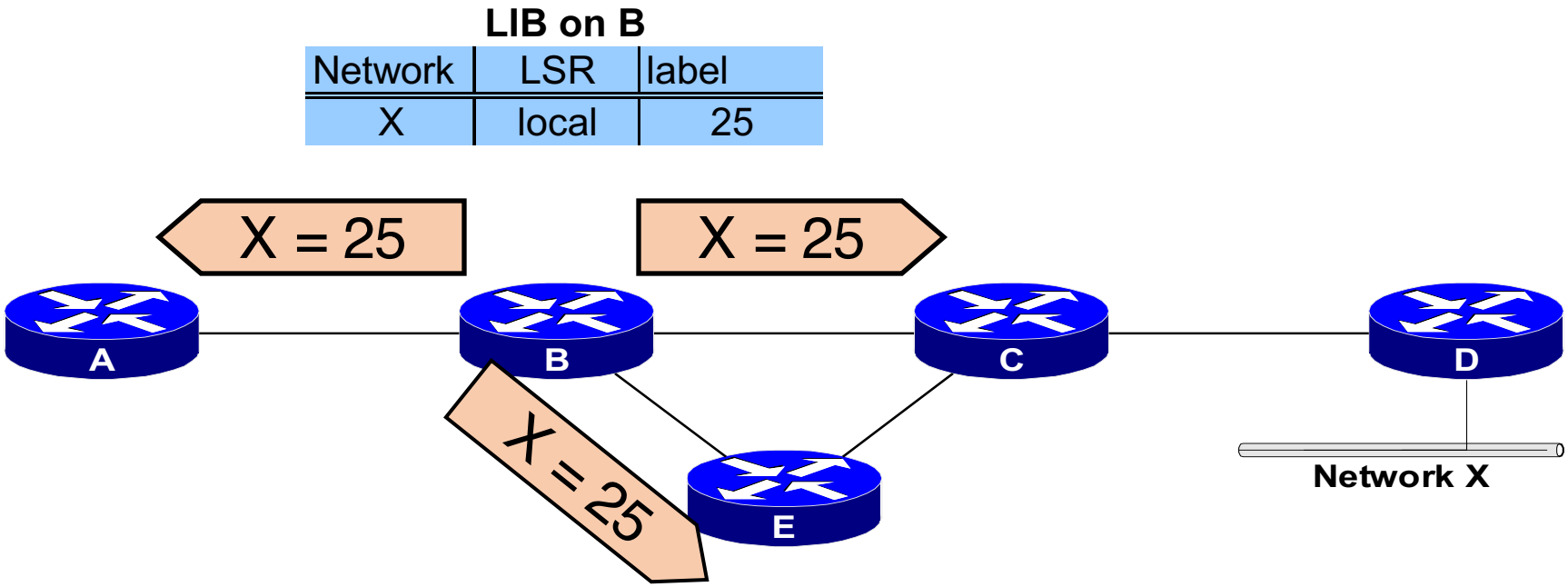
- Every LSR allocates a label for every destination in the IP routing table.
- Labels have local significance.
- Label allocations are asynchronous.

LIB and LFIB Set-up



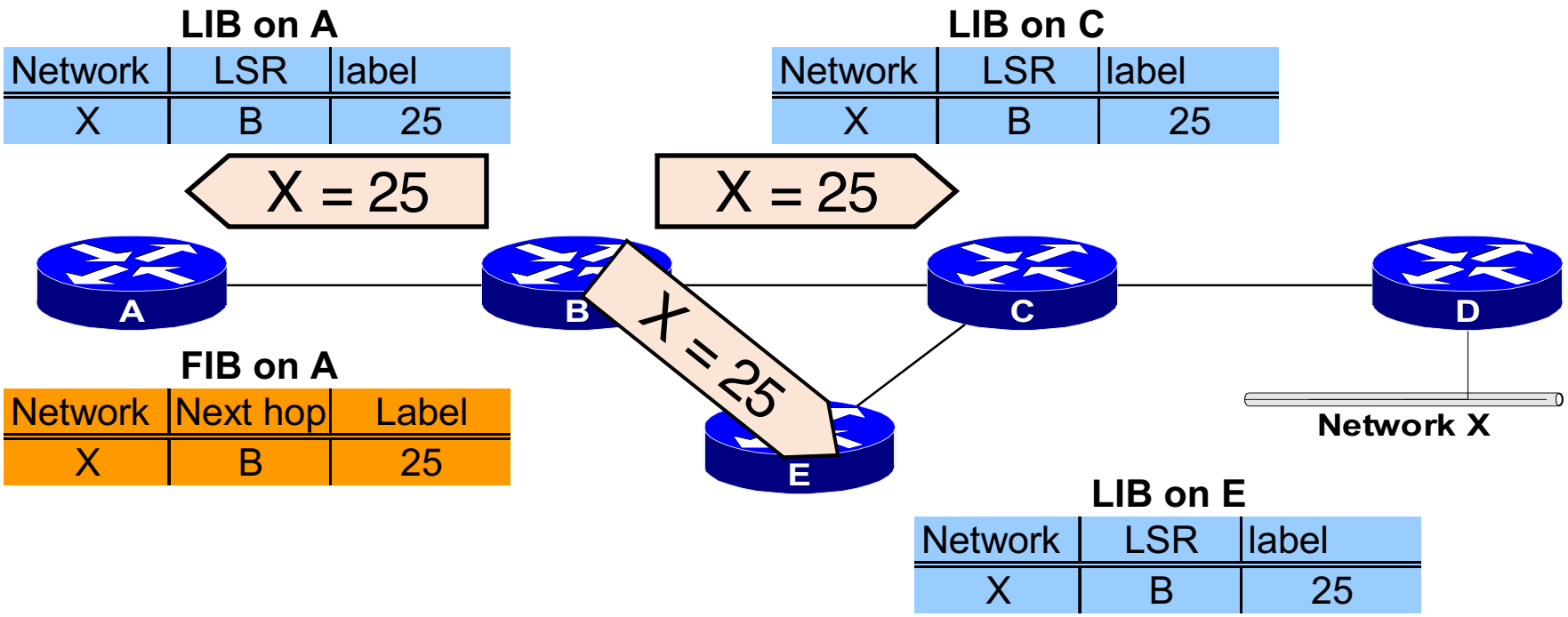
LIB and LFIB structures have to be initialized on the LSR allocating the label.

Label Distribution



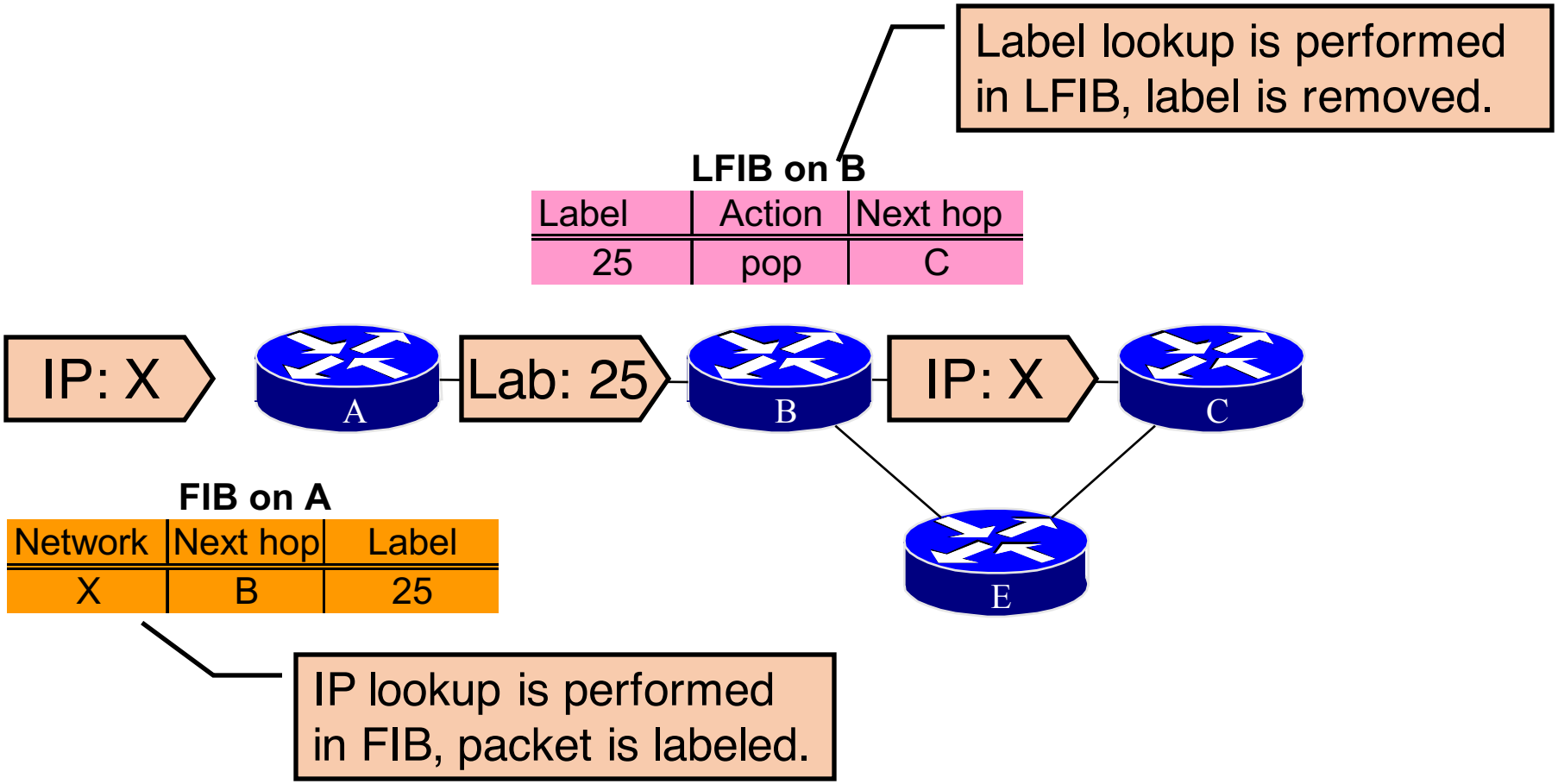
The allocated label is advertised to all neighbor LSRs, regardless of whether the neighbors are upstream or downstream LSRs for the destination.

Receiving Label Advertisement



- Every LSR stores the received label in its LIB.
- Edge LSRs that receive the label from their next-hop also store the label information in the FIB.

Interim Packet Propagation

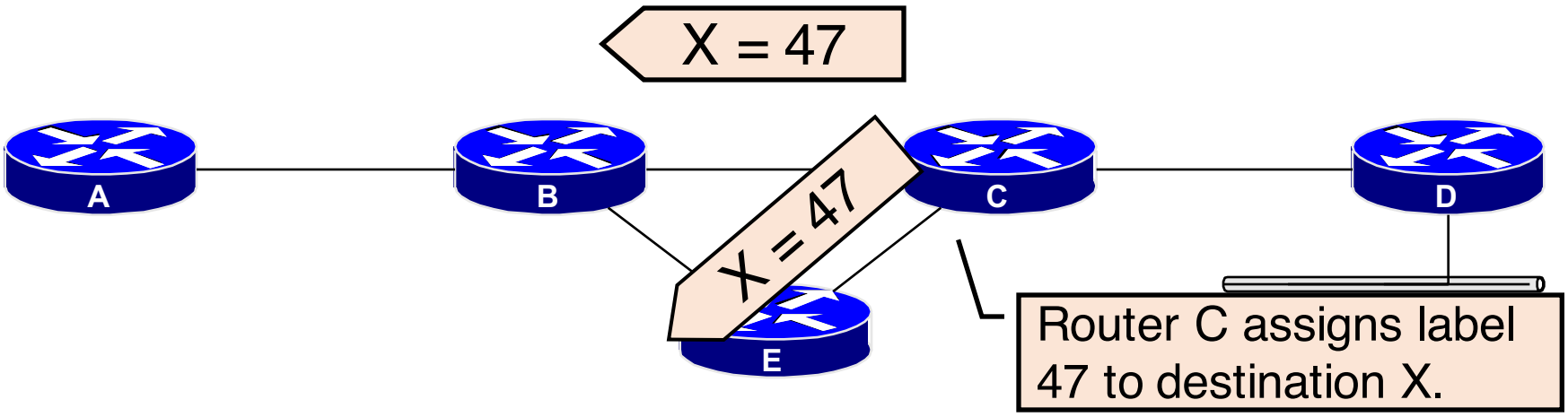


Forwarded IP packets are labeled only on the path segments where the labels have already been assigned.

Further Label Allocation

LIB on C

Network	LSR	label
X	B	25
	local	47

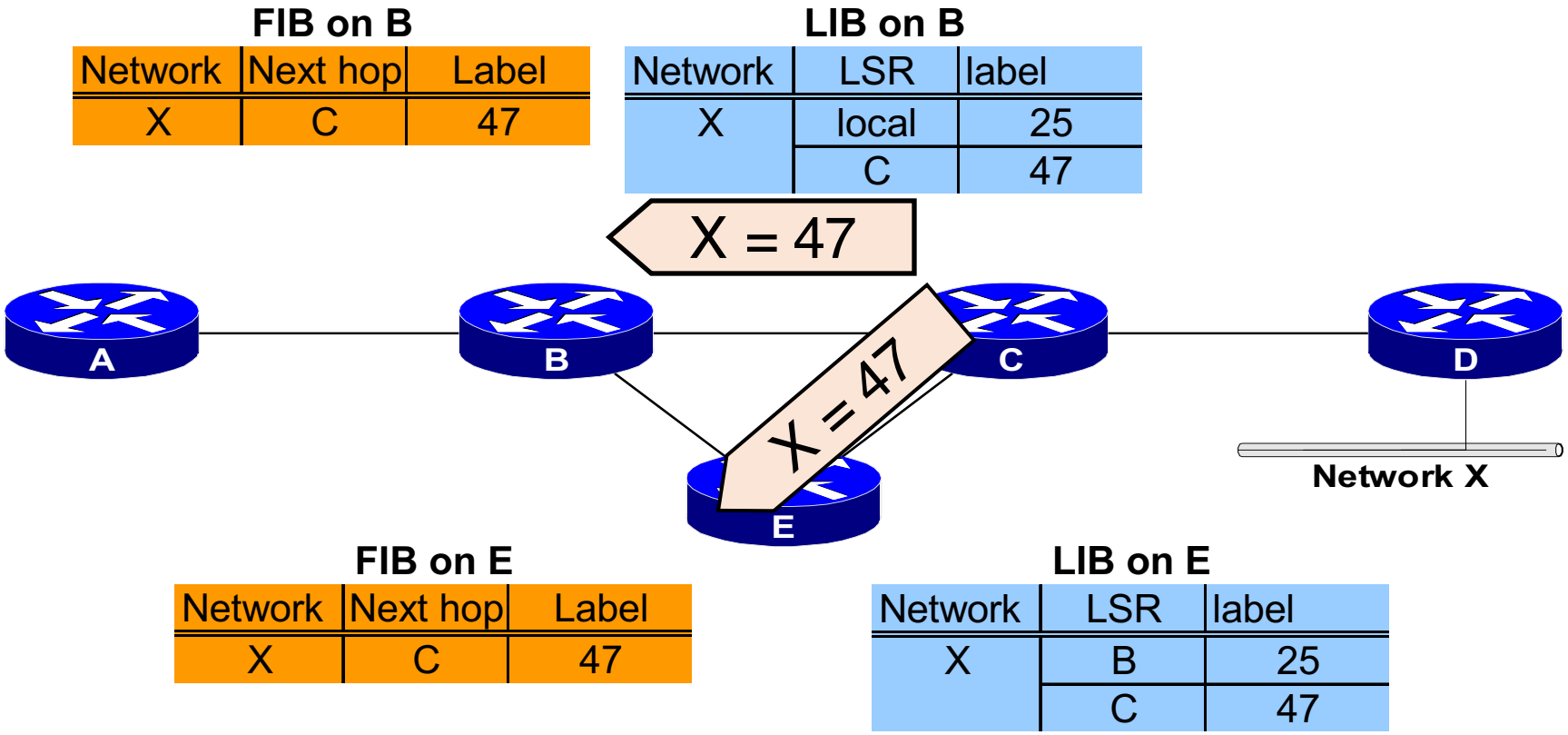


LFIB on C

Label	Action	Next hop
47	pop	D

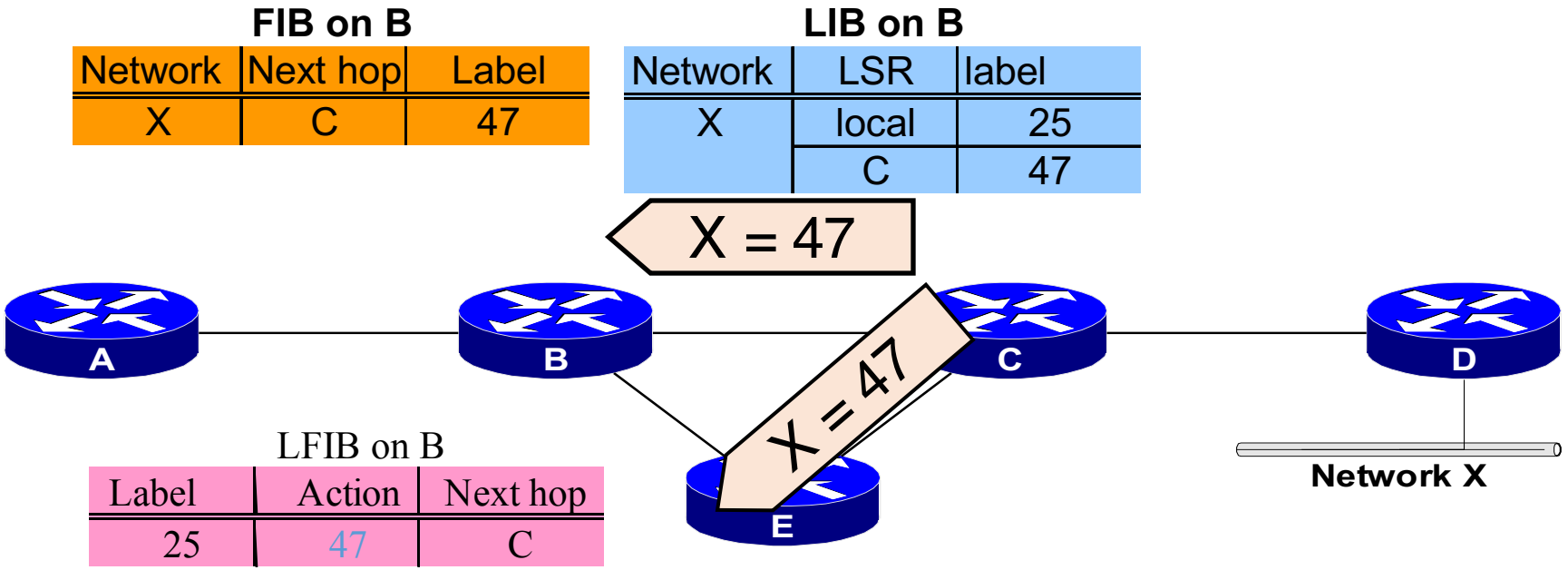
Every LSR will eventually assign a label for every destination.

Receiving Label Advertisement



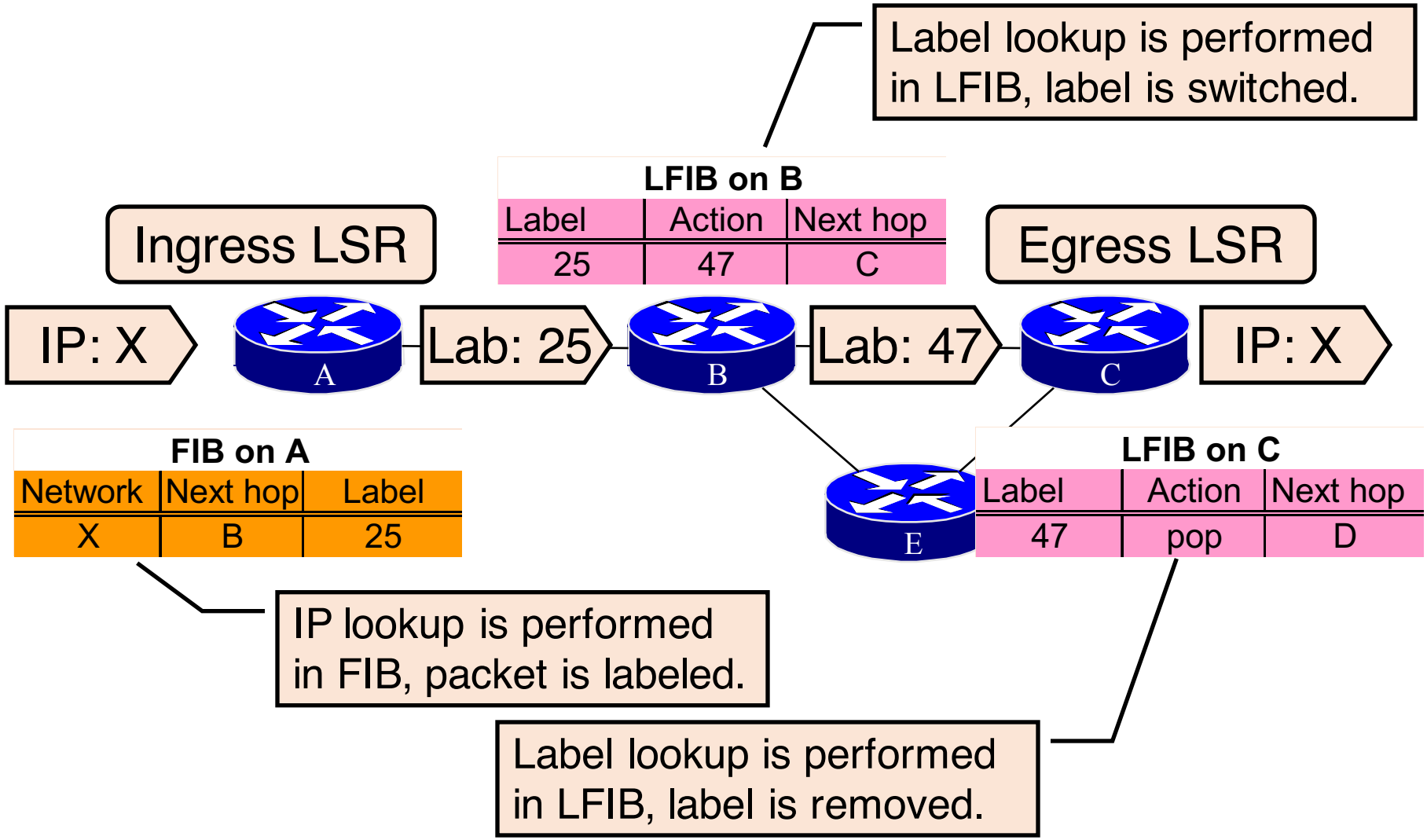
- Every LSR stores received information in its LIB.
- LSRs that receive their label from their next-hop LSR will also populate the IP forwarding table (FIB).

Populating LFIB



- Router B has already assigned label to X and created an entry in LFIB.
- Outgoing label is inserted in LFIB after the label is received from the next-hop LSR.

Packet Propagation Across MPLS Network



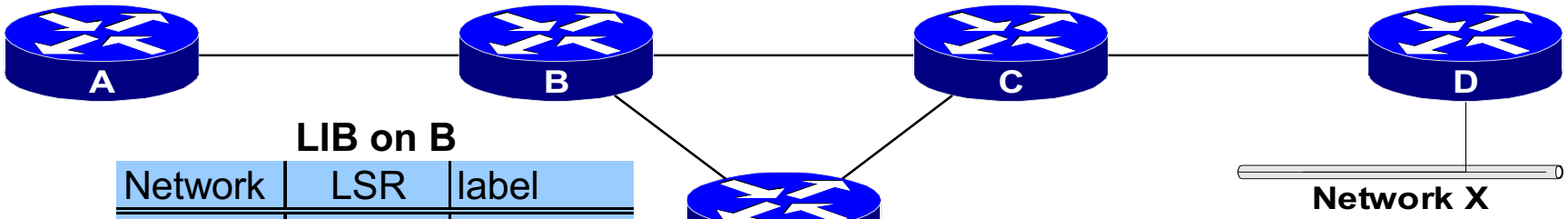
Convergence in Packet-mode MPLS Steady State Description

Routing table of B

Network	Next-hop
X	C

FIB on B

Network	Next hop	Label
X	C	47



LIB on B

Network	LSR	label
X	local	25
	C	47
	E	75

LFIB on B

Label	Action	Next hop
25	47	C

- After the LSRs have exchanged the labels, LIB, LFIB and FIB data structures are completely populated.

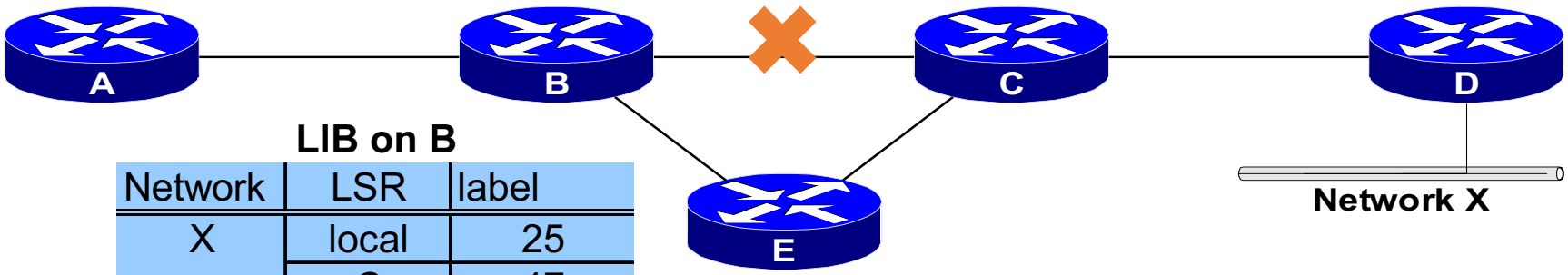
Link Failure Actions

Routing table of B

Network	Next-hop
~~X~~	~~C~~

FIB on B

Network	Next hop	Label
X	~~C~~	~~47~~



LIB on B

Network	LSR	label
X	local	25
	~~C~~	~~47~~
	E	75

LFIB on B

Label	Action	Next hop
25	~~47~~	~~C~~

- Routing protocol neighbors and LDP neighbors are lost after a link failure.
- Entries are removed from various data structures.

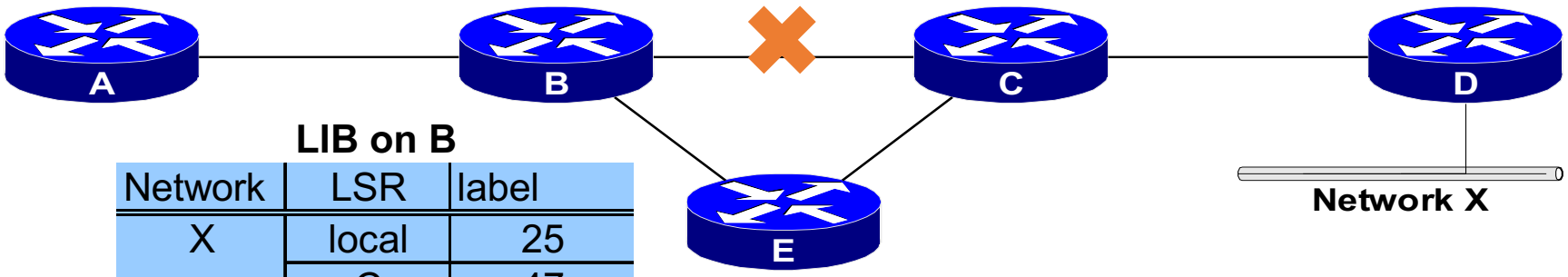
Routing Protocol Convergence

Routing table of B

Network	Next-hop
X	E

FIB on B

Network	Next hop	Label
X	E	—



LIB on B

Network	LSR	label
X	local	25
	~~C~~	~~47~~
	E	75

LFIB on B

Label	Action	Next hop
25	~~47~~	~~C~~

- Routing protocols rebuild the IP routing table and the IP forwarding table.

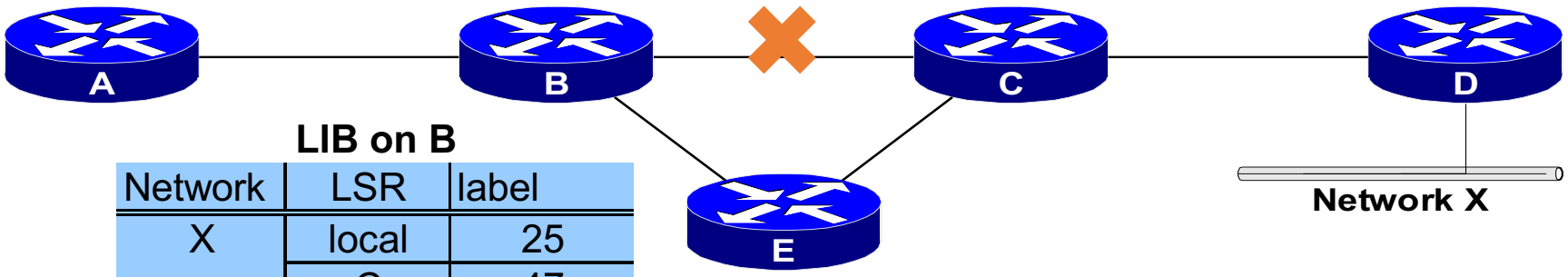
MPLS Convergence

Routing table of B

Network	Next-hop
X	E

FIB on B

Network	Next hop	Label
X	E	75



LIB on B

Network	LSR	label
X	local	25
	~~C~~	~~47~~
	E	75

LFIB on B

Label	Action	Next hop
25	75	E

- LFIB and labeling information in FIB are rebuilt immediately after the routing protocol convergence, based on labels stored in LIB.

MPLS Convergence After a Link Failure

- MPLS convergence in packet-mode MPLS does not impact the overall convergence time.
- MPLS convergence occurs immediately after the routing protocol convergence, based on labels already stored in LIB.

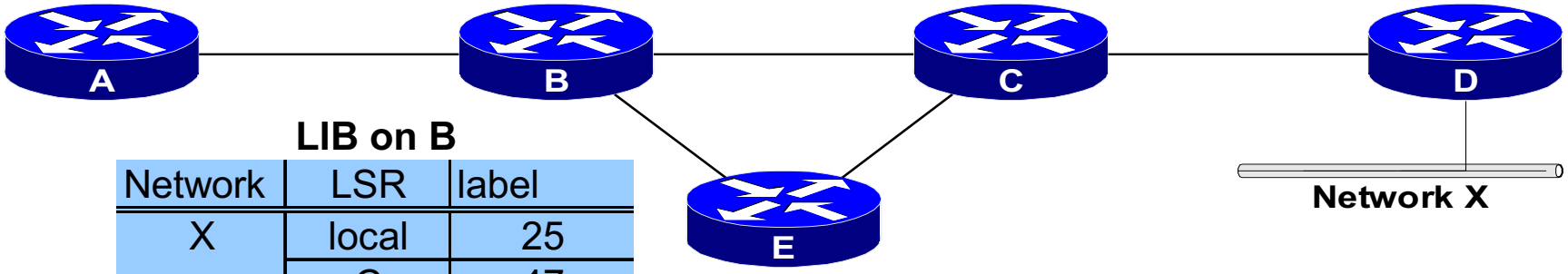
Link Recovery Actions

Routing table of B

Network	Next-hop
X	E

FIB on B

Network	Next hop	Label
X	E	75



LIB on B

Network	LSR	label
X	local	25
	~~C~~	~~47~~
	E	75

LFIB on B

Label	Action	Next hop
25	75	E

- Routing protocol neighbors are discovered after link recovery.

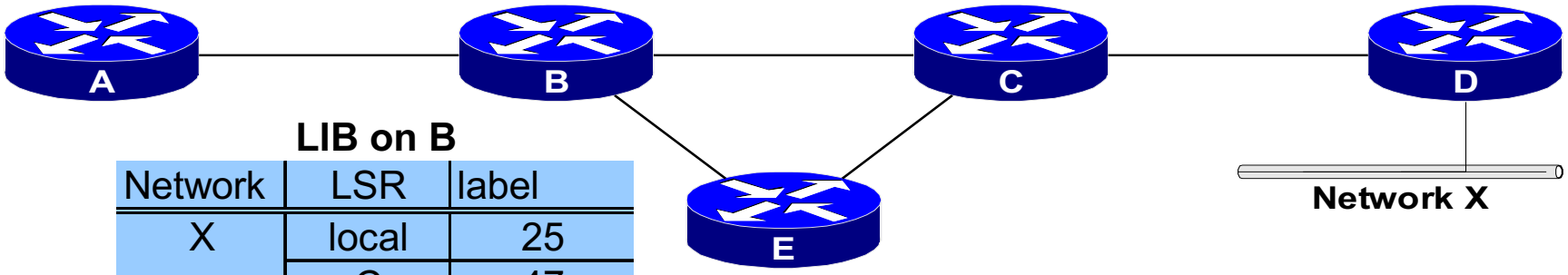
IP Routing Convergence After Link Recovery

Routing table of B

Network	Next-hop
X	C

FIB on B

Network	Next hop	Label
X	C	—



LIB on B

Network	LSR	label
X	local	25
	~~C~~	~~47~~
	E	75

LFIB on B

Label	Action	Next hop
25	pop	C

- IP routing protocols rebuild the IP routing table.
- FIB and LFIB are also rebuilt, but the label information might be lacking.

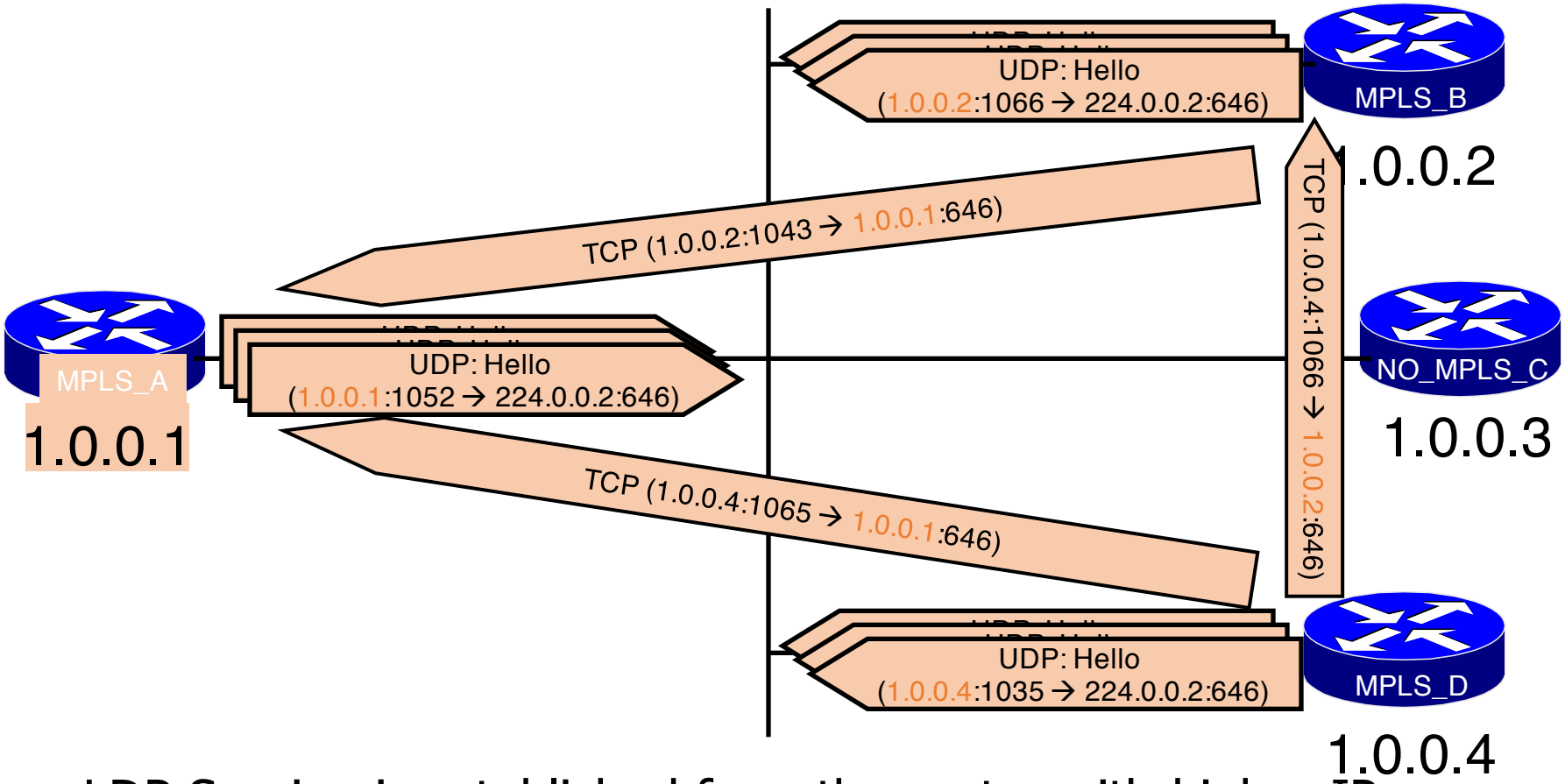
MPLS Convergence After a Link Recovery

- Routing protocol convergence optimizes the forwarding path after a link recovery.
- LIB might not contain the label from the new next-hop by the time the IP convergence is complete.
- End-to-end MPLS connectivity might be intermittently broken after link recovery.
- Use MPLS Traffic Engineering for make-before-break recovery.

LDP Session Establishment

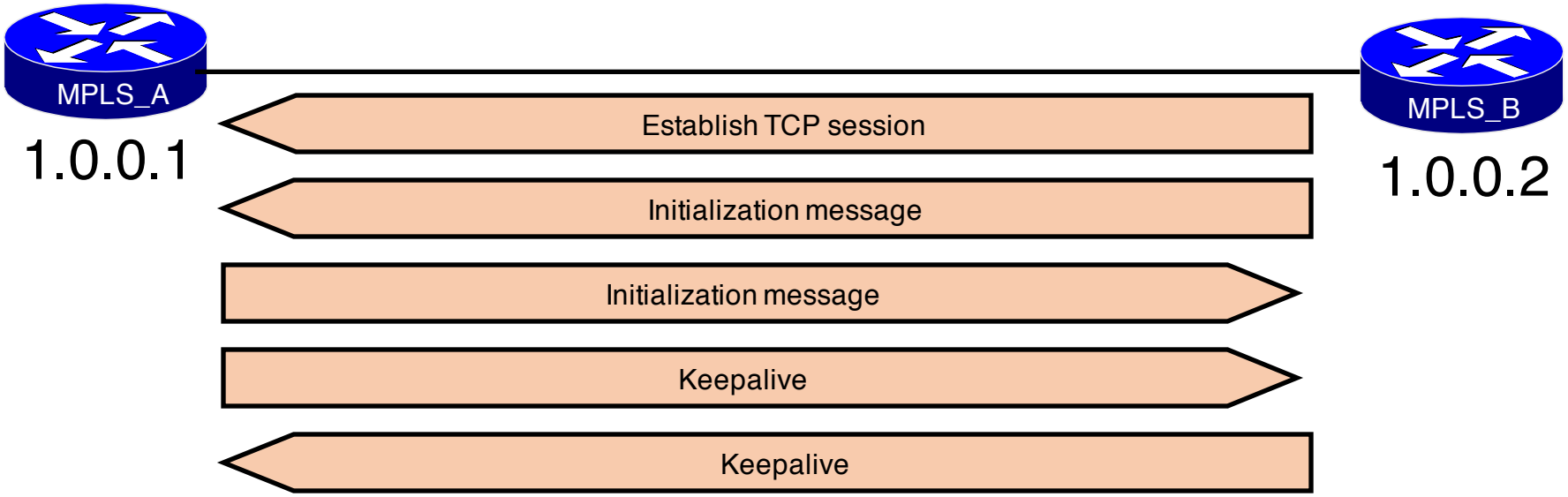
- LDP -- establish a session
  - Hello messages are periodically sent on all interfaces enabled for MPLS.
  - If there is another router on that interface it will respond by trying to establish a session with the source of the hello messages.
- UDP is used for hello messages. It is targeted at "all routers on this subnet" multicast address (224.0.0.2).
- TCP is used to establish the session.
- Both TCP and UDP use well-known LDP port number 646.

LDP Neighbor Discovery



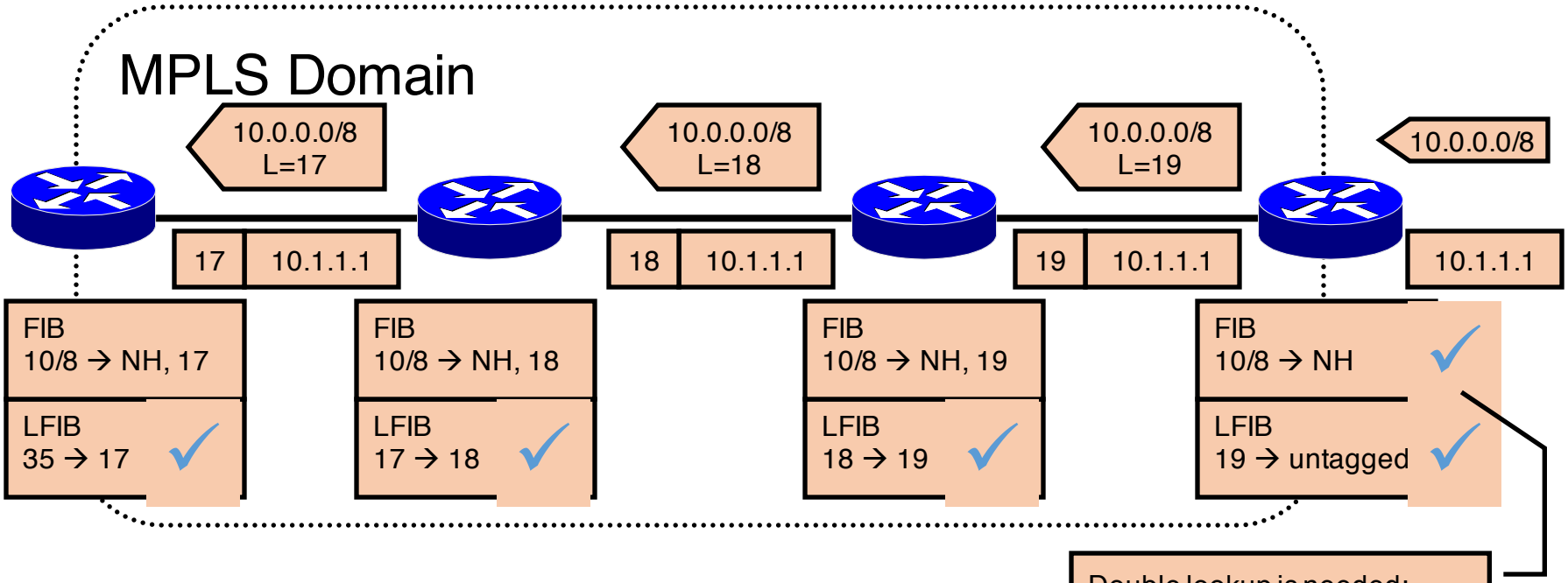
- LDP Session is established from the router with higher IP address.

LDP Session Negotiation



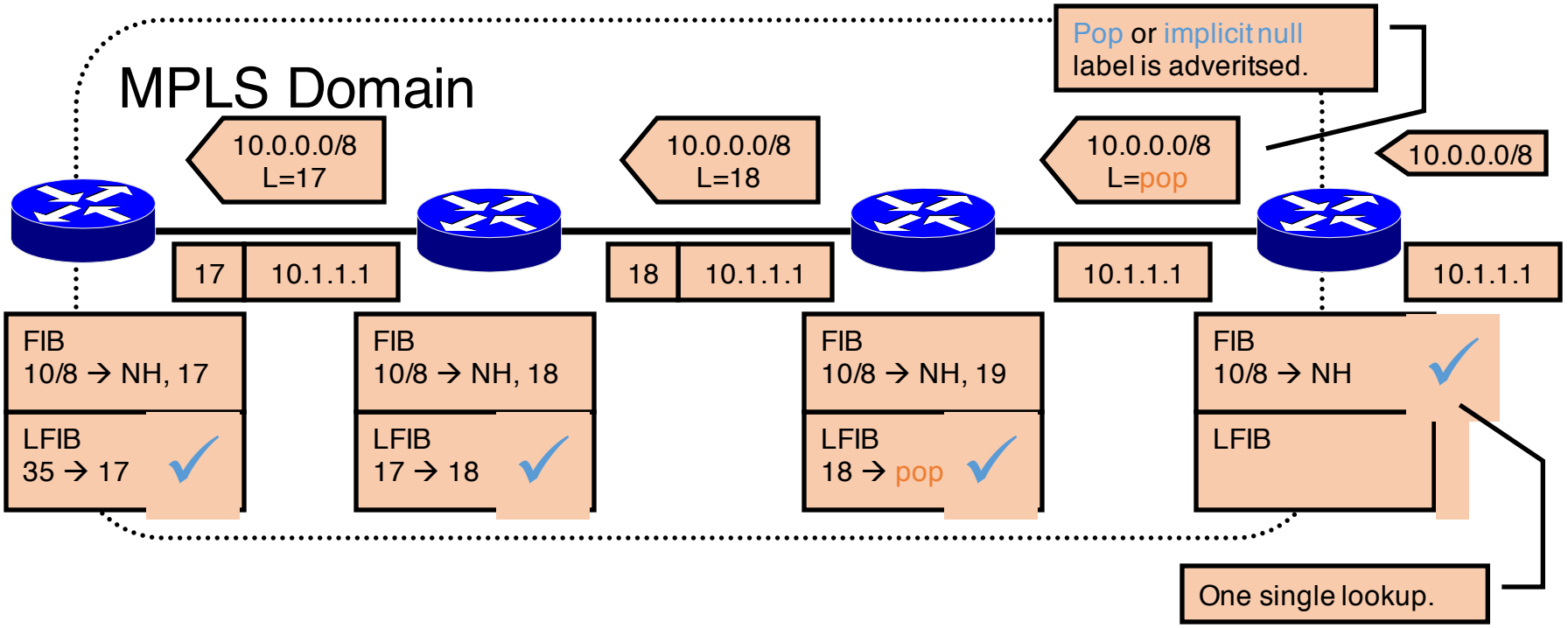
- Peers first exchange initialization messages.
- The session is ready to exchange label mappings after receiving the first keepalive.

Double Lookup Scenario



- Double lookup is not an optimal way of forwarding labeled packets.
- A label can be removed one hop earlier.

Penultimate Hop Popping



- A label is removed on the router before the last hop within an MPLS domain.

Penultimate Hop Popping

- Penultimate hop popping optimizes MPLS performace (one less LFIB lookup).
- Pop or implicit null label uses value 3 when being advertised to a neighbor.
- Reserved Label values:
  - **0: explicit NULL.** Can be used in signaling protocols as well as label headers.
  - **3: implicit NULL**. Used in signaling protocols only. It should never appear in the label stack. Its use in a signaling protocol indicates that the upstream router should perform penultimate hop popping (PHP; remove the top label on the stack).

LDP Messages

- Discovery messages
  - Used to discover and maintain the presence of new peers
  - Hello packets (UDP) sent to all-routers multicast address
  - Once neighbor is discovered, the LDP session is established over TCP

LDP Messages

- Session messages
  - Establish, maintain and terminate LDP sessions
- Advertisement messages
  - Create, modify, delete label mappings
- Notification messages
  - Error signalling

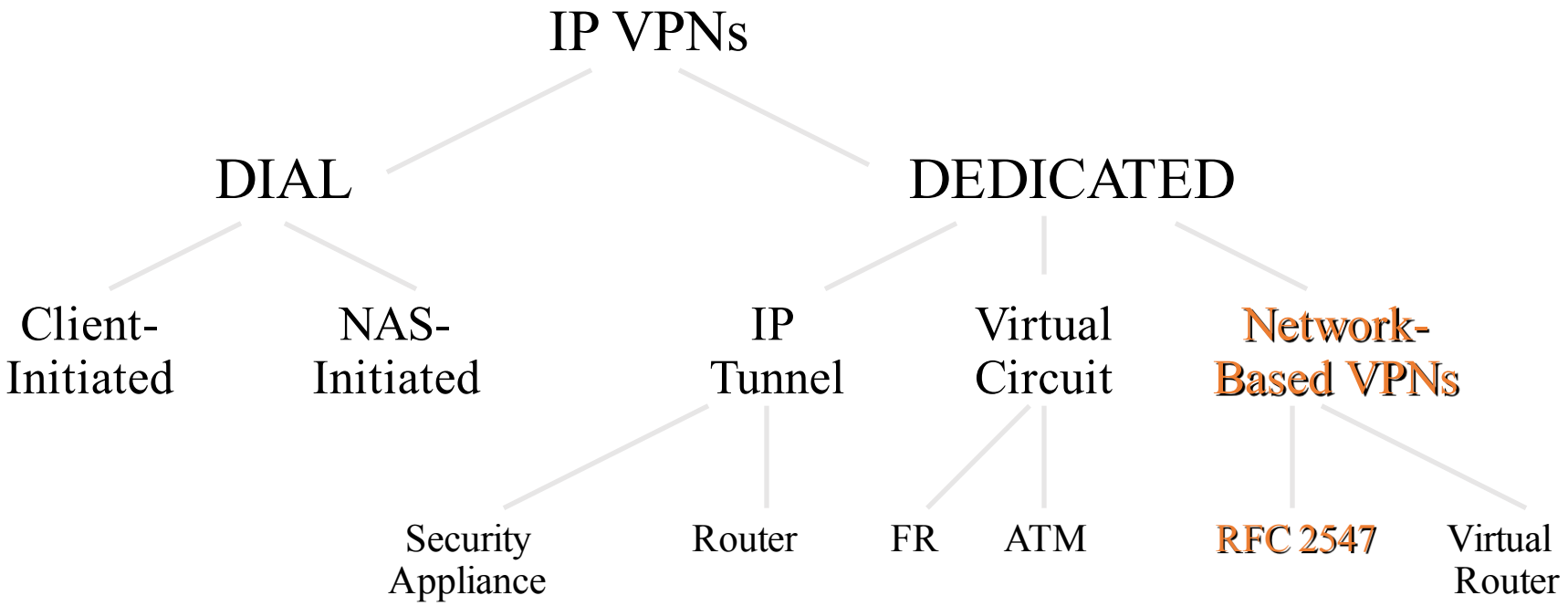
Agenda

- Introduction to MPLS
- LDP
- MPLS VPN

What Is a VPN?

- Virtual Private Network – Provide a private network over a shared infrastructure
- Interconnect geographically separate sites, with the same privacy and guarantees as a private network

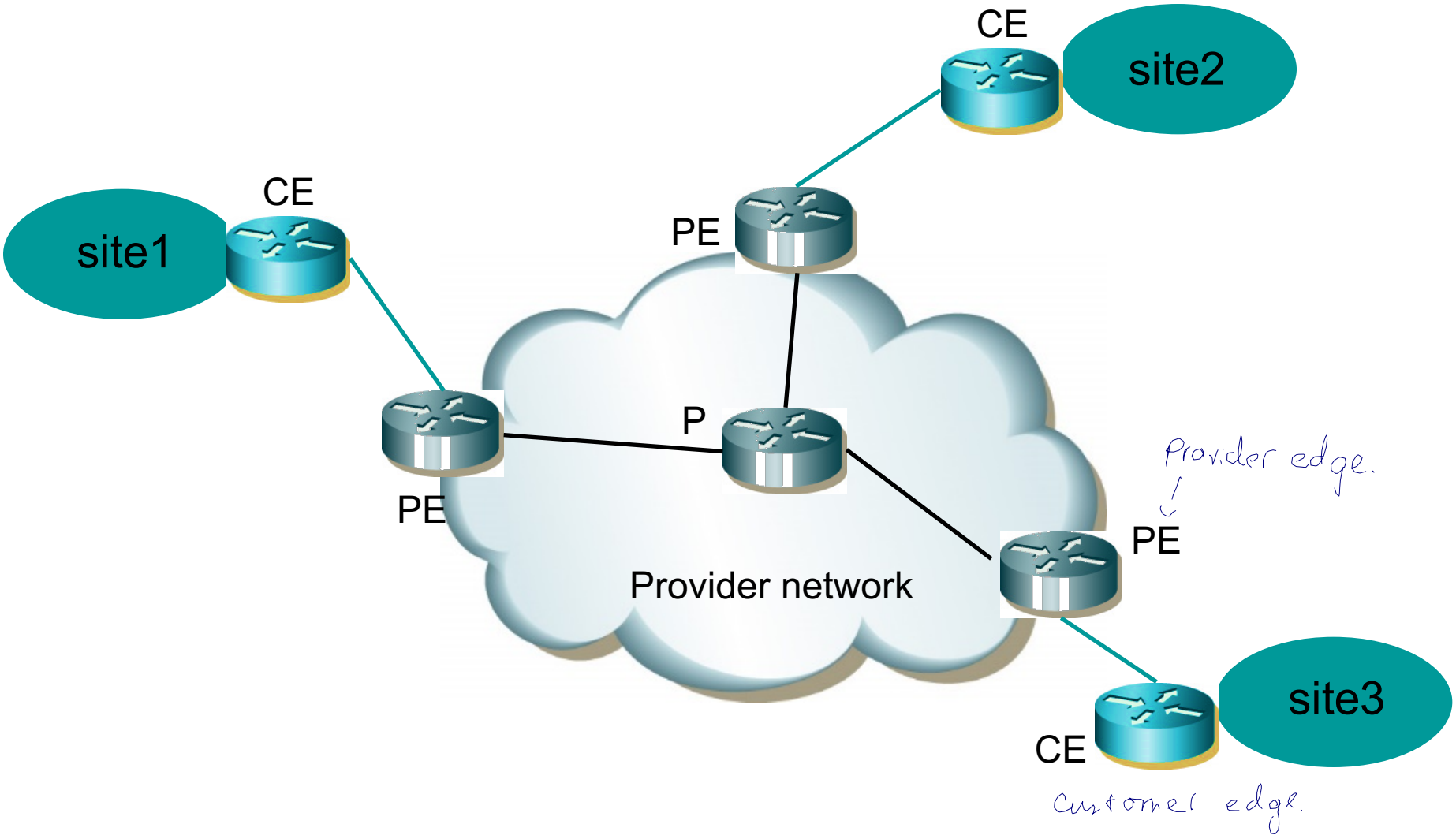
IP VPN Taxonomy



MPLS-VPN Terminology

- Provider Network (P-Network)
  - The backbone under control of a Service Provider
- Customer Network (C-Network)
  - Network under customer control
- CE router
  - Customer Edge router. Part of the C-network and interfaces to a PE router
- Site -- Set of (sub)networks part of the C-network and co-located
  - A site is connected to the VPN backbone through one or more PE/CE links
- PE router -- Provider Edge router.
  - Part of the P-Network and interfaces to CE routers
- P router -- Provider (core) router, without knowledge of VPN

Site 1, 2, 3 ∈ 1 company.



Goals

- Inter-site connectivity
- Privacy – Don’t allow traffic from one VPN to be seen in another VPN
- Independent addressing – Private addresses in each VPN

BGP – MPLS VPNs

- Separation of forwarding
- Distribution of routing information
- New address type
- Forwarding with MPLS

Separation of Forwarding

- Goal – control connectivity and ensure privacy by segregating the forwarding information
- PE router connected to CEs from several VPNs
- With a single forwarding table, it is possible to forward packets from one VPN to another

Multiple Forwarding Tables

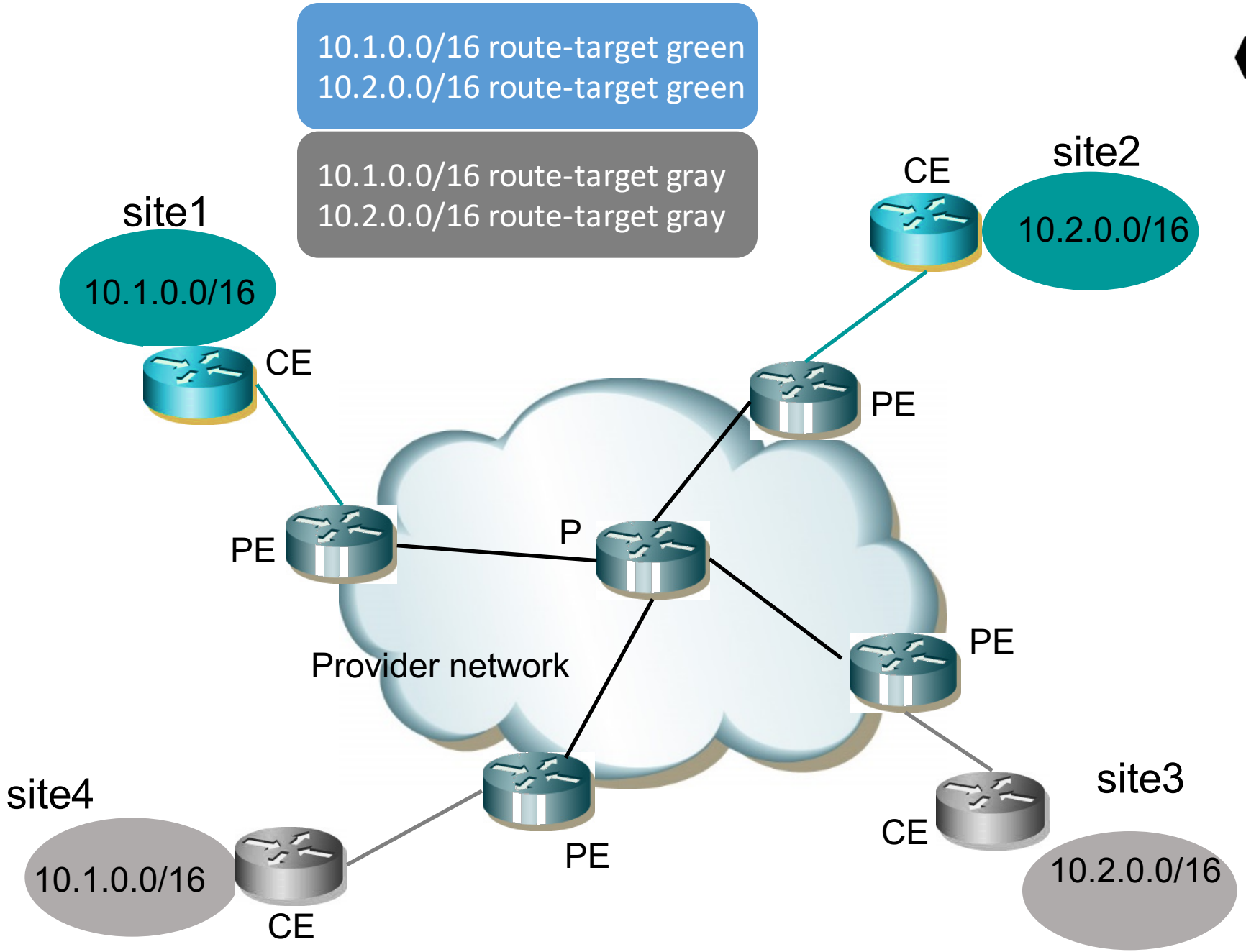
- Multiple forwarding tables – each table associated with a site
- Packets from the customer are identified based on the incoming port, which identifies the forwarding table
- Contents – routes received from the CE and routes received from remote PEs with constrained routing
- Called VPN routing and forwarding Table -- VRF

Constrained Distribution of Routing Information

The Idea:

- CE advertised routes to the local PE via some routing protocol
- The local PE marks these routes with an extended community and advertise them in BGP
- The routes are distributed to all remote PEs by BGP
- Remote PE receives BGP routes, filters them based on the community and advertises them to the CE

➔ **The need for unique addresses**


10.1.0.0/16 route-target green
10.2.0.0/16 route-target green
10.1.0.0/16 route-target gray
10.2.0.0/16 route-target gray
site1
10.1.0.0/16
CE
site2
CE
10.2.0.0/16
PE
PE
P
Provider network
PE
PE
site4
10.1.0.0/16
CE
PE
CE
site3
10.2.0.0/16

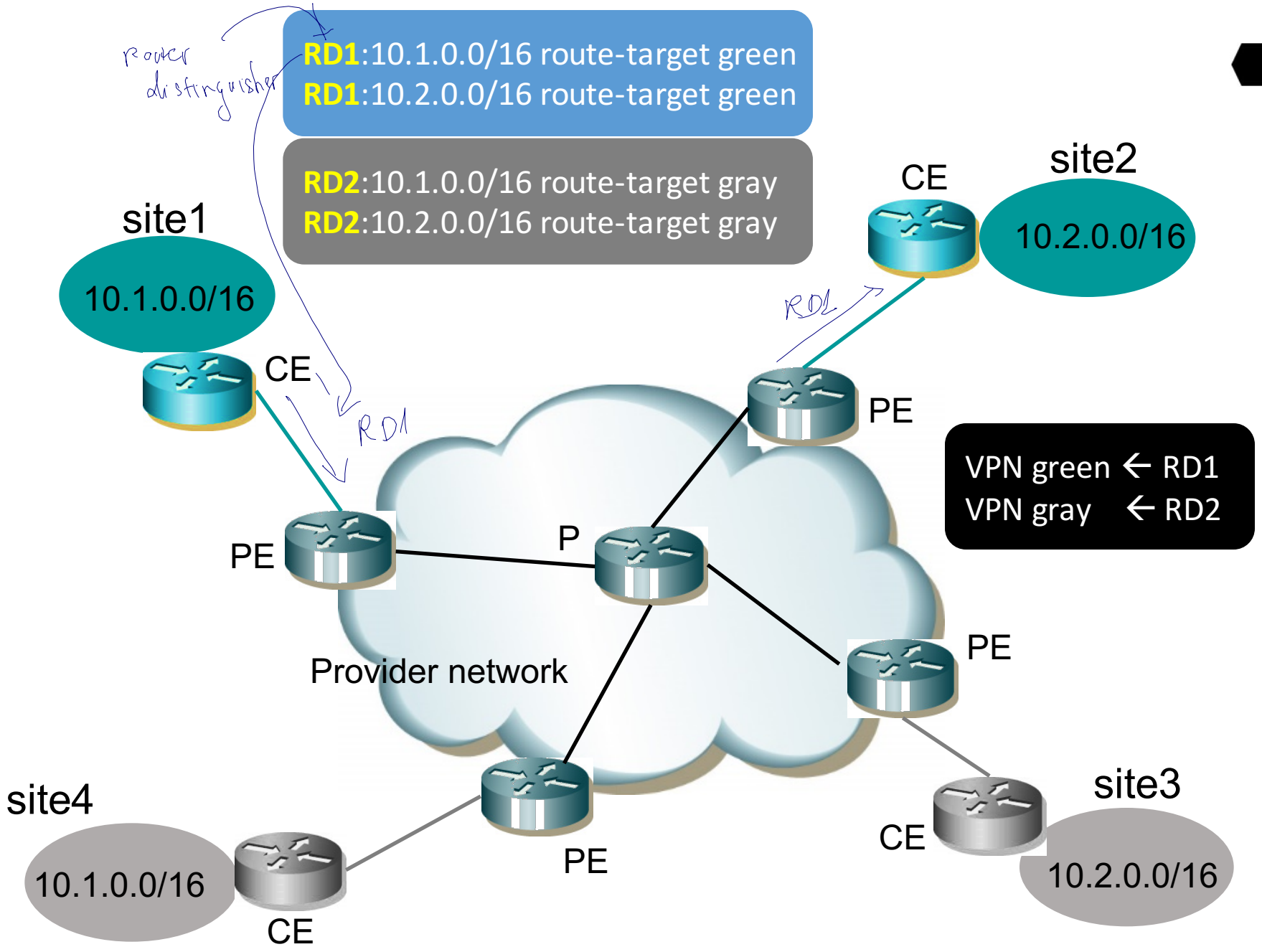
Overlapping address space and VPN-IP addresses

Goal

- Turn non-unique addresses into unique addresses
- An 8-byte unique identifier called the route distinguisher concatenated with IP addresses
- Route Distinguisher Format

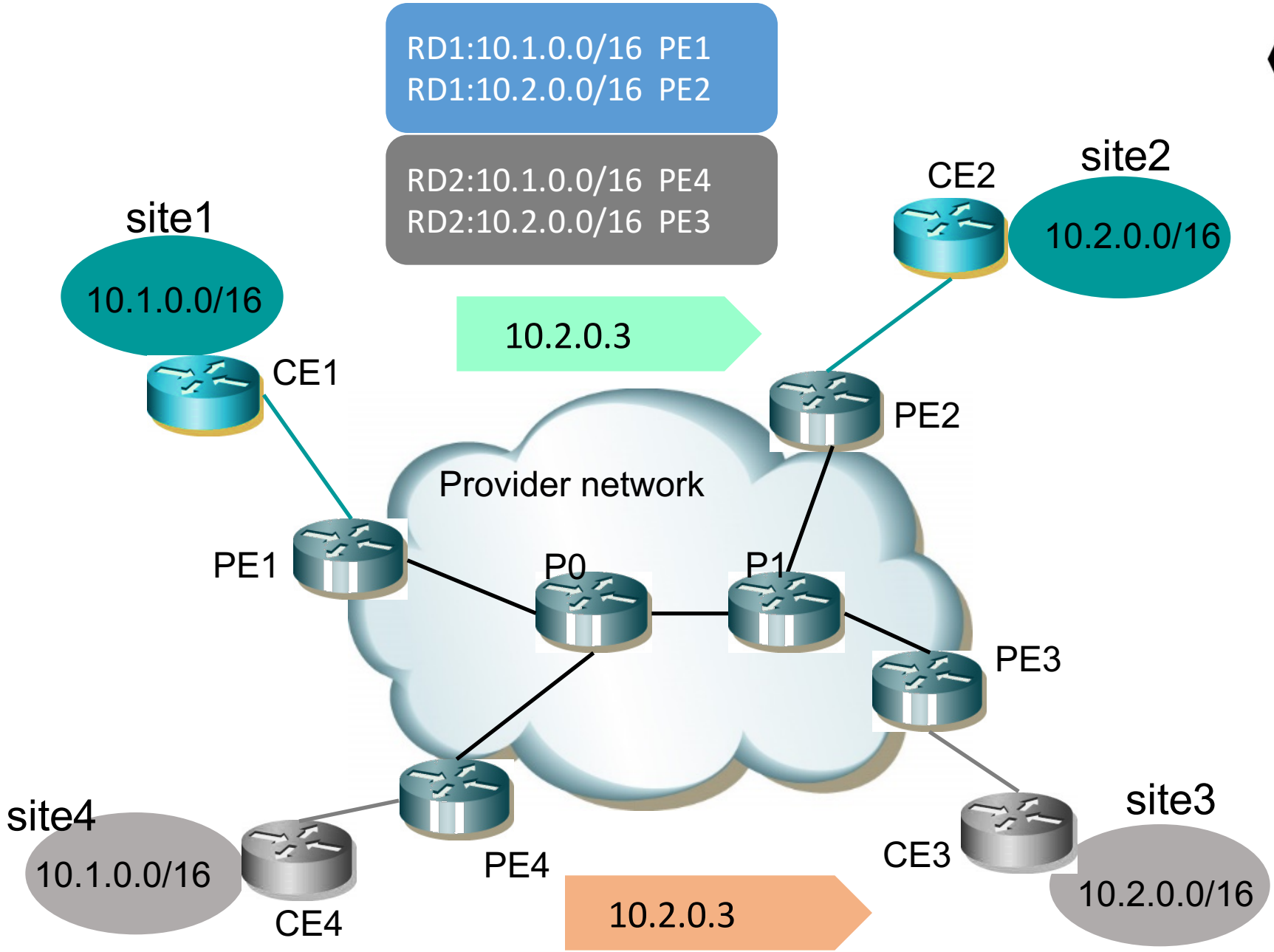
VPN-IP addresses

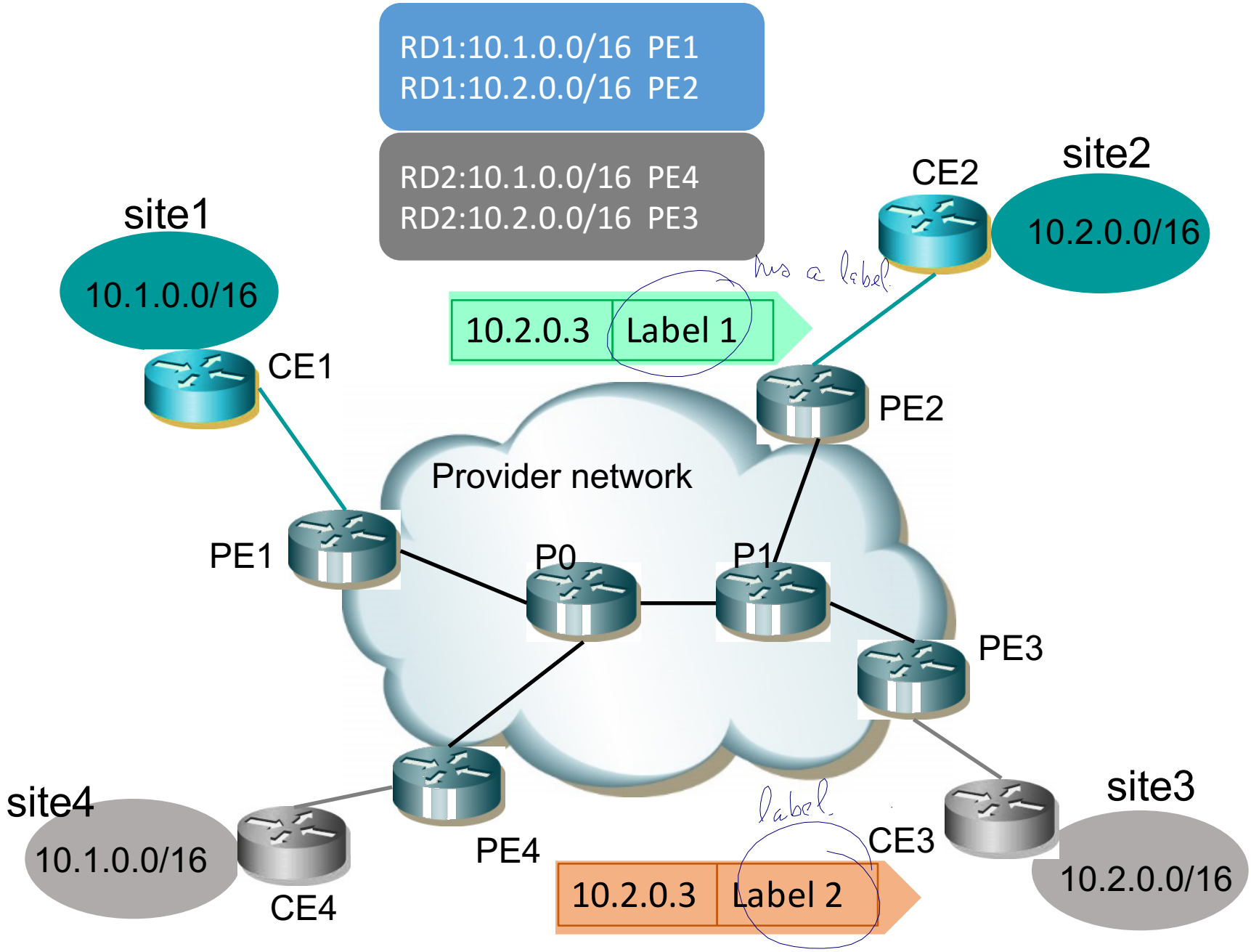
- Used only in the provider’s network
- Used only in the control plane
- The translation happens on the PE


router distinguisher
RD1:10.1.0.0/16 route-target green
RD1:10.2.0.0/16 route-target green
RD2:10.1.0.0/16 route-target gray
RD2:10.2.0.0/16 route-target gray
site1
10.1.0.0/16
CE
RD1
site2
CE
10.2.0.0/16
RD1
PE
VPN green ← RD1
VPN gray ← RD2
PE
P
Provider network
PE
site4
10.1.0.0/16
CE
PE
CE
site3
10.2.0.0/16

Forward VPN packets in Provider Network

- VPN-IP addresses do not appear in IP header
- Need a way to forward traffic with overlapping addresses in the provider network

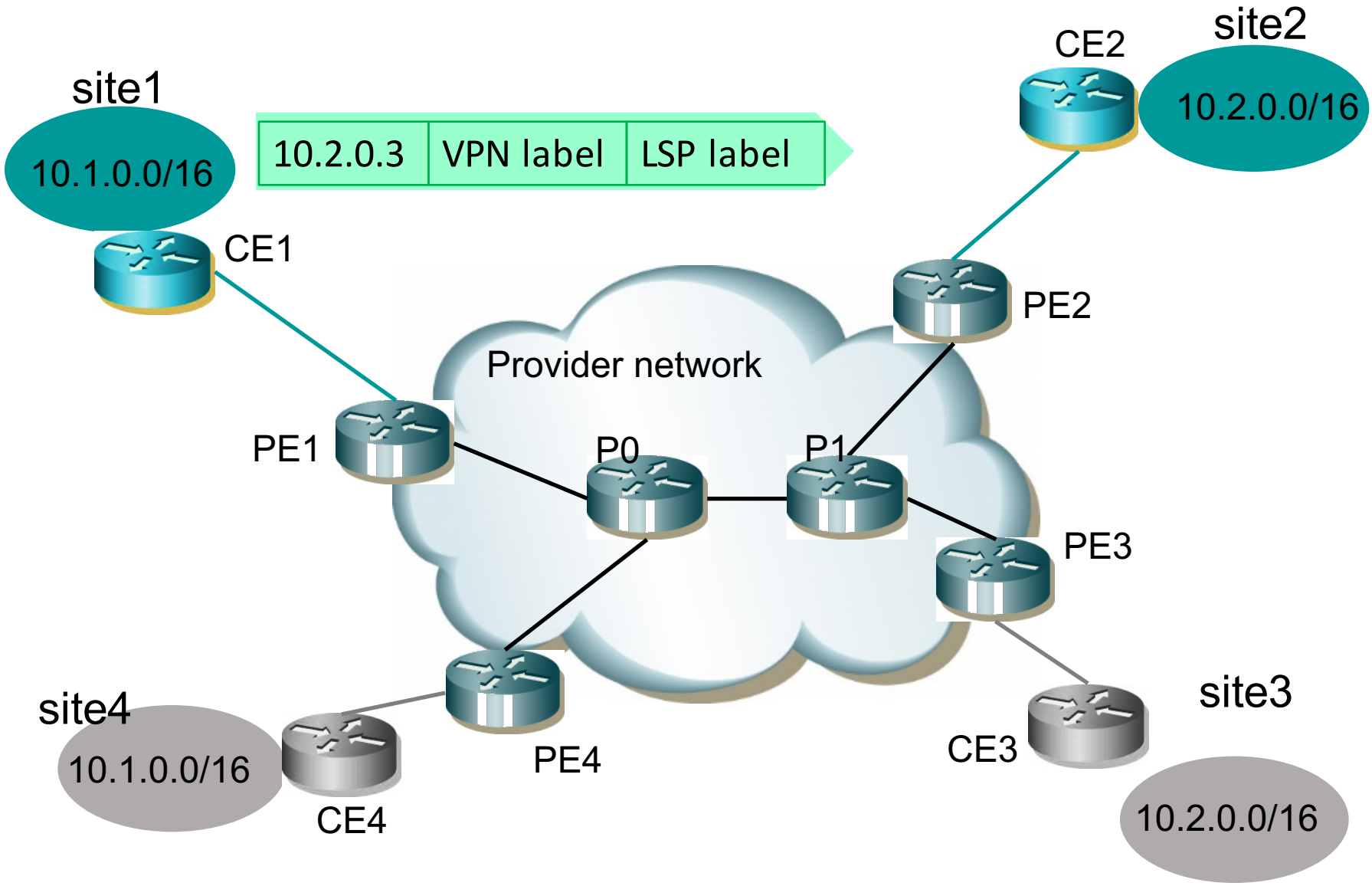

RD1:10.1.0.0/16 PE1
RD1:10.2.0.0/16 PE2
RD2:10.1.0.0/16 PE4
RD2:10.2.0.0/16 PE3
site1
10.1.0.0/16
CE1
CE2
site2
10.2.0.0/16
10.2.0.3
PE2
Provider network
PE1
P0
P1
PE3
site4
10.1.0.0/16
CE4
PE4
CE3
site3
10.2.0.0/16
10.2.0.3


RD1:10.1.0.0/16 PE1
RD1:10.2.0.0/16 PE2
RD2:10.1.0.0/16 PE4
RD2:10.2.0.0/16 PE3
site1
10.1.0.0/16
CE1
CE2
site2
10.2.0.0/16
has a label
10.2.0.3 Label 1
PE2
Provider network
PE1
P0
P1
PE3
site4
10.1.0.0/16
CE4
PE4
label
CE3
site3
10.2.0.0/16
10.2.0.3 Label 2

VPN Labels

The Idea:

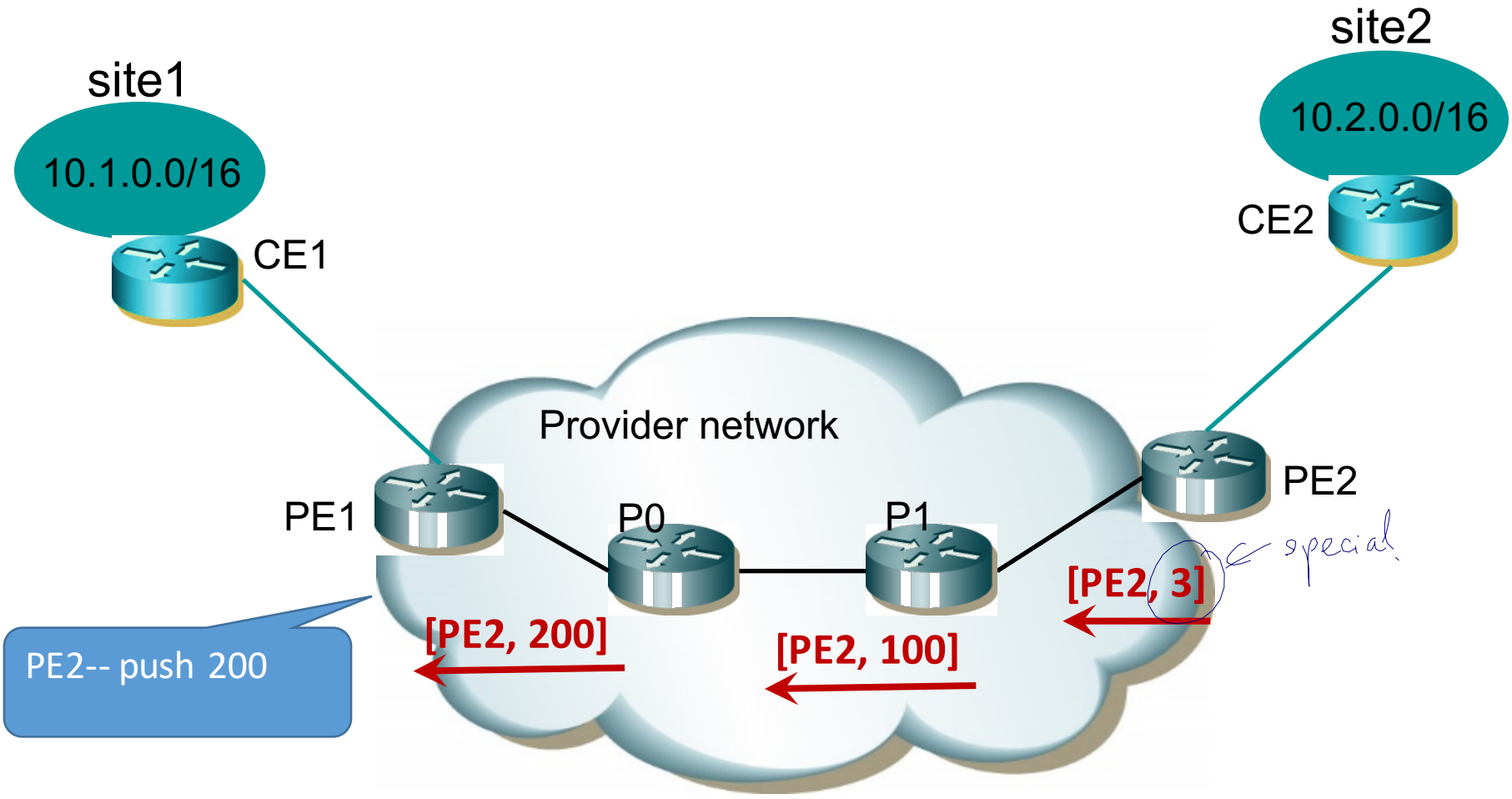
- Use a label to identify the next hop at the remote PE. Also called VPN label
- The label is distributed by BGP, along with the VPN-IP address
- Traffic will carry two labels – the VPN label and the LSP label
- The remote PE makes the forwarding decision based on the VPN label


site1
10.1.0.0/16
10.2.0.3
VPN label
LSP label
CE1
CE2
site2
10.2.0.0/16
PE2
Provider network
PE1
P0
P1
PE3
site4
10.1.0.0/16
CE4
PE4
CE3
site3
10.2.0.0/16

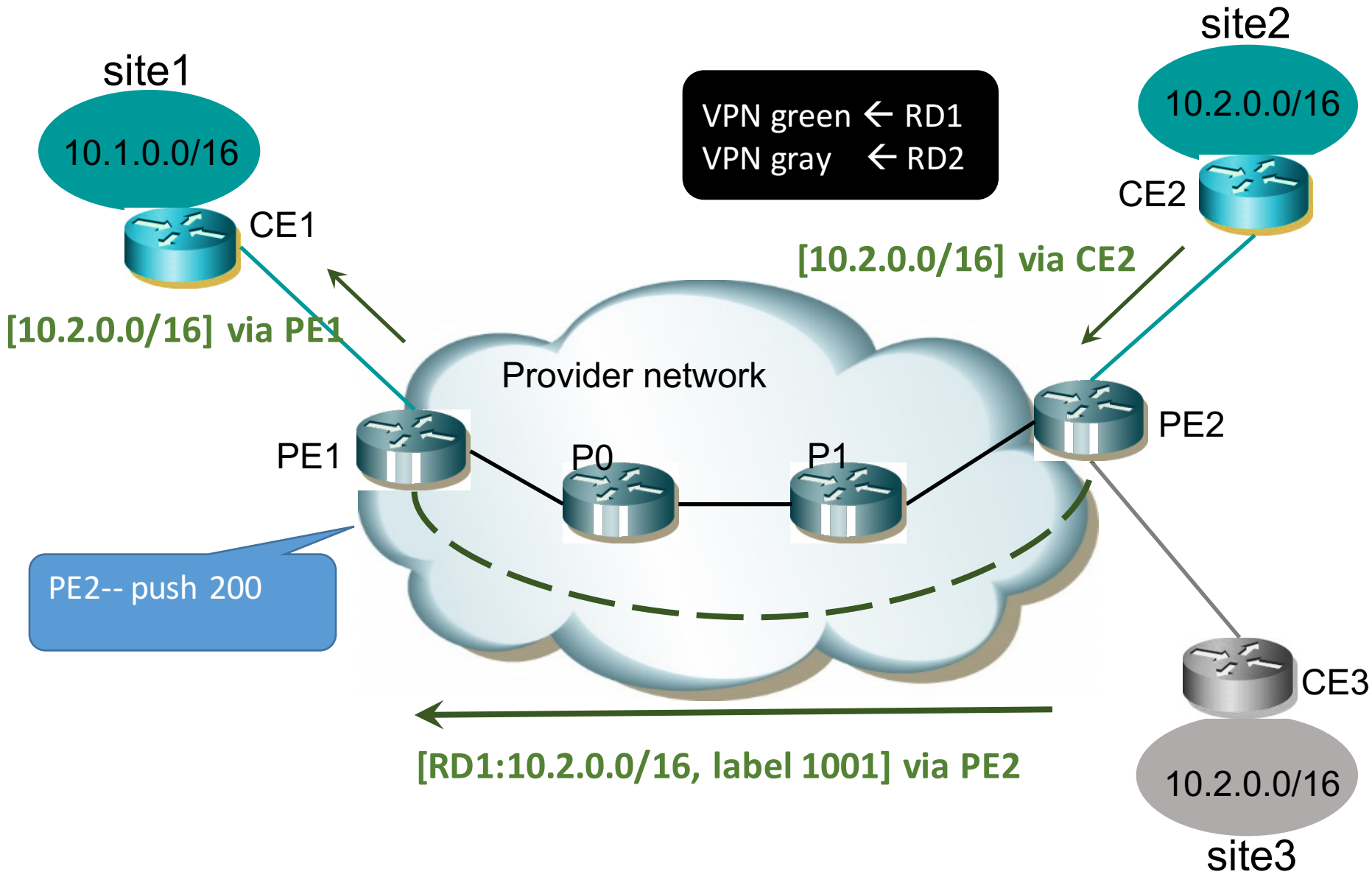
VPN Model -- Summary

- P routers do not maintain VPN routes. Only maintain routes to other P and PE routers
- PE routers maintain VPN routes, but only for VPNs that have sites attached to them
- VPNs can have overlapping address spaces

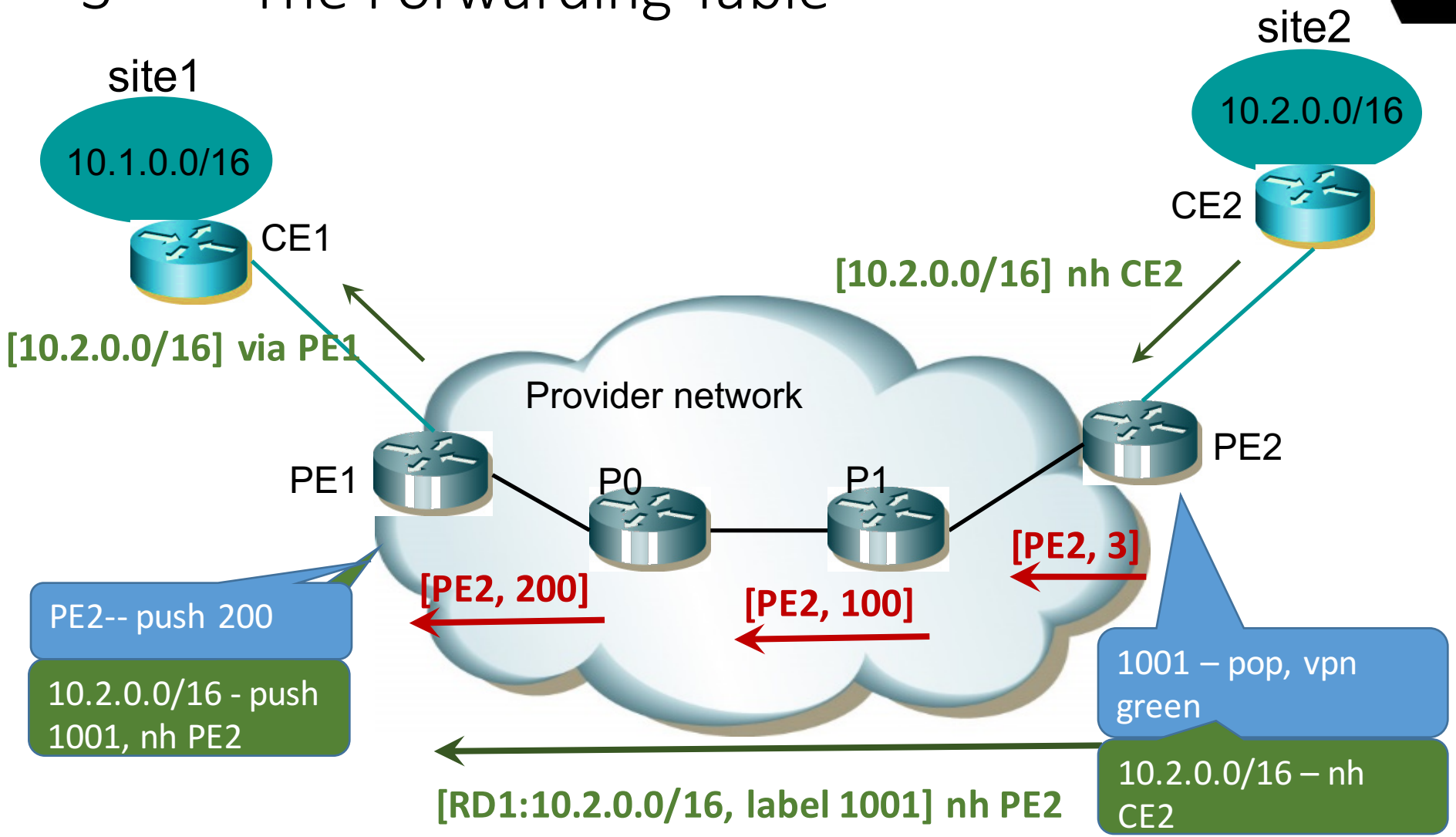
1st – LSP Setup



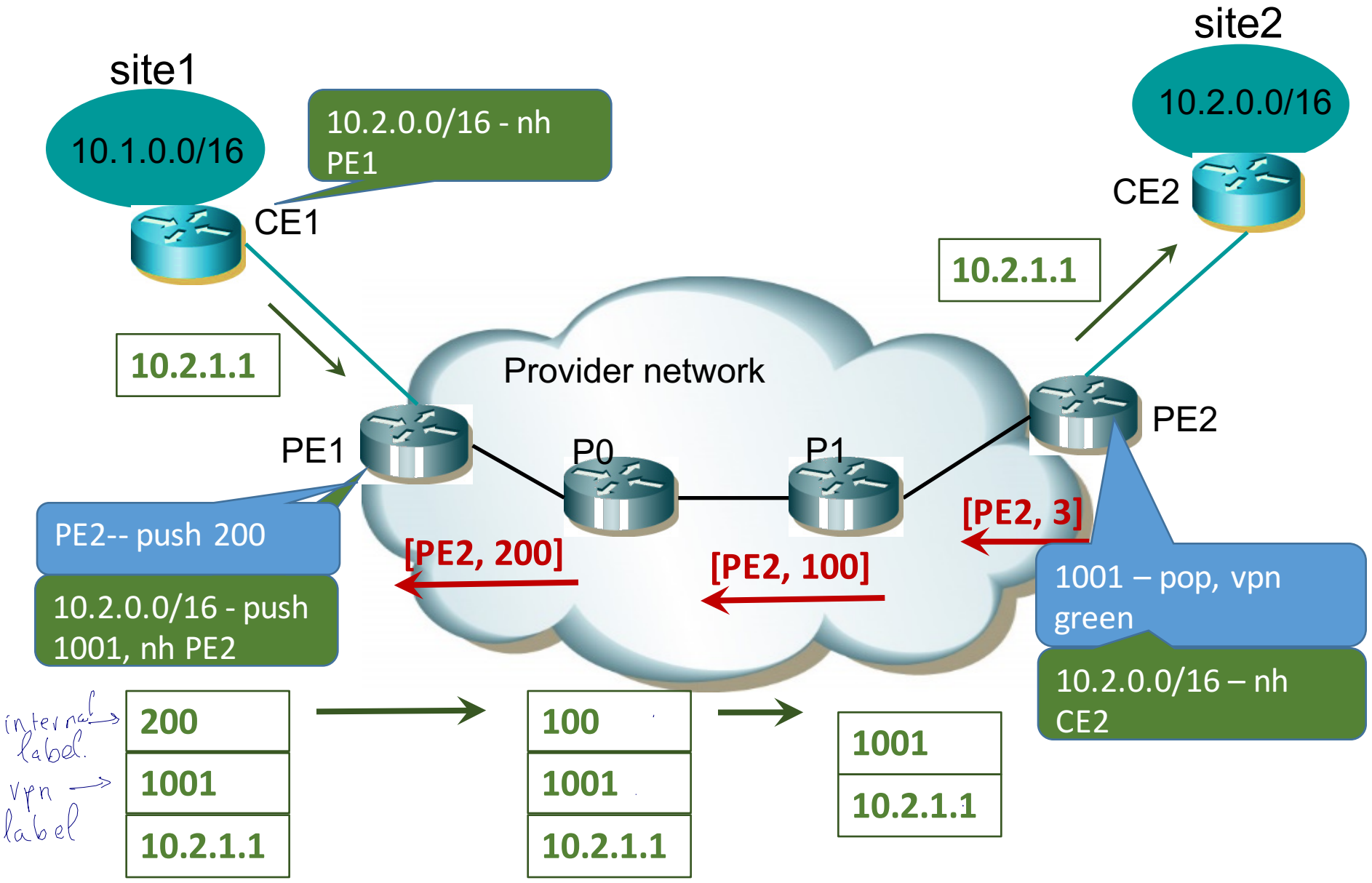
2nd – Route Distribution



3rd – The Forwarding Table



4th – Forwarding Traffic



Route Distinguisher

- Distinguish one set of routes (one VRF) from another. It is a unique number prepended to each route within a VRF to identify it as belonging to that particular VRF. An RD is carried along with a route via MP-BGP when exchanging VPN routes with other PE routers.
- An RD is 64 bits in length comprising three fields:
  - type (two bytes), administrator, and value.

Type 0	ASN (2 bytes)	Value (4 bytes)

Type 1	IP (4 bytes)	Value (2 bytes)

Type 2	ASN (4 bytes)	Value (2 bytes)

Route Target

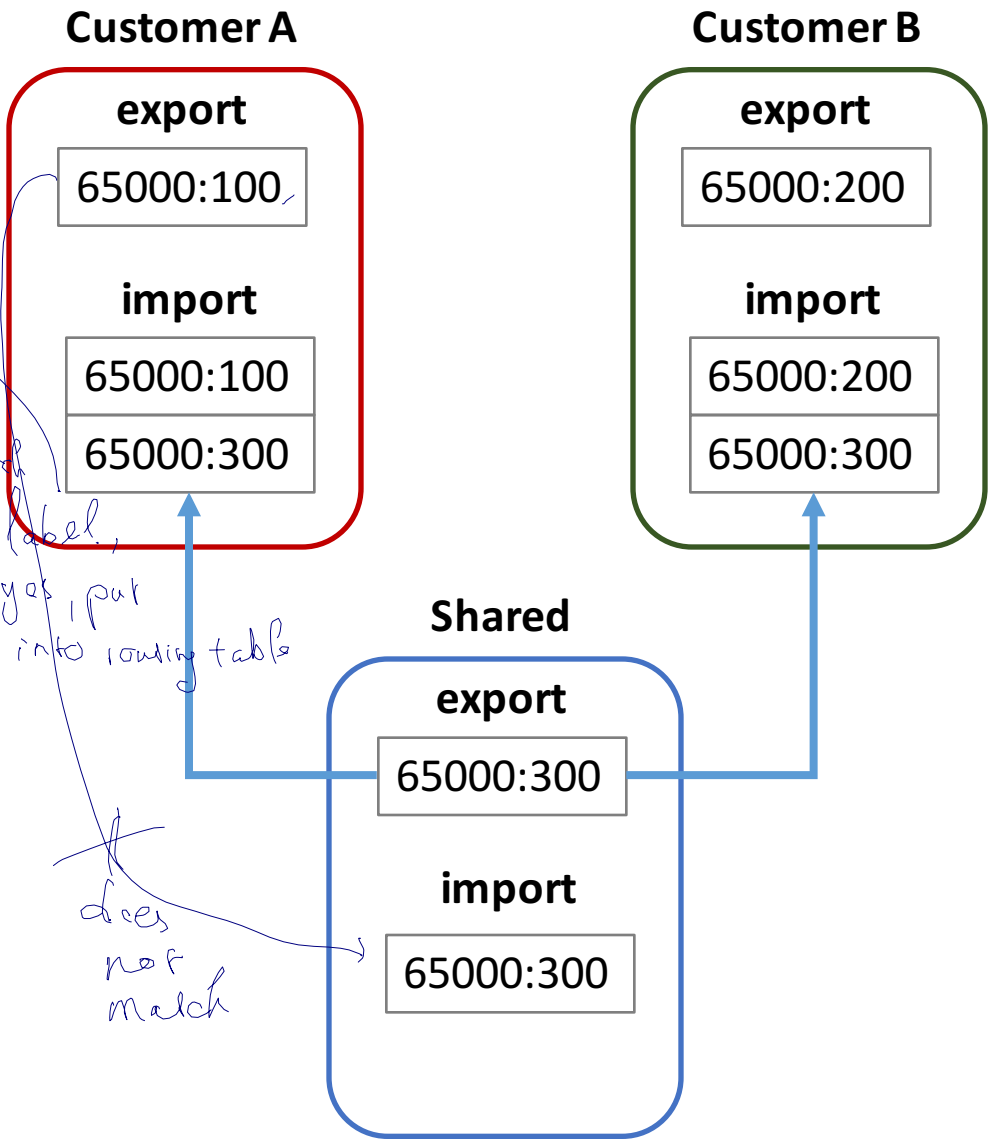
- A BGP extended community attribute used control route distribution among VRFs. Route targets are applied to a VRF to control the import and export of routes among it and other VRFs.
- Route-target Export:
- Route-target Import:

```
ip vrf Customer_A
 rd 65000:100
 route-target export 65000:100
 route-target import 65000:100
```

BGP update:
Extended community:
    Route-taget 65000:100
Prefix 10.2.0.0/16
Route Distinguisher: 65000:100

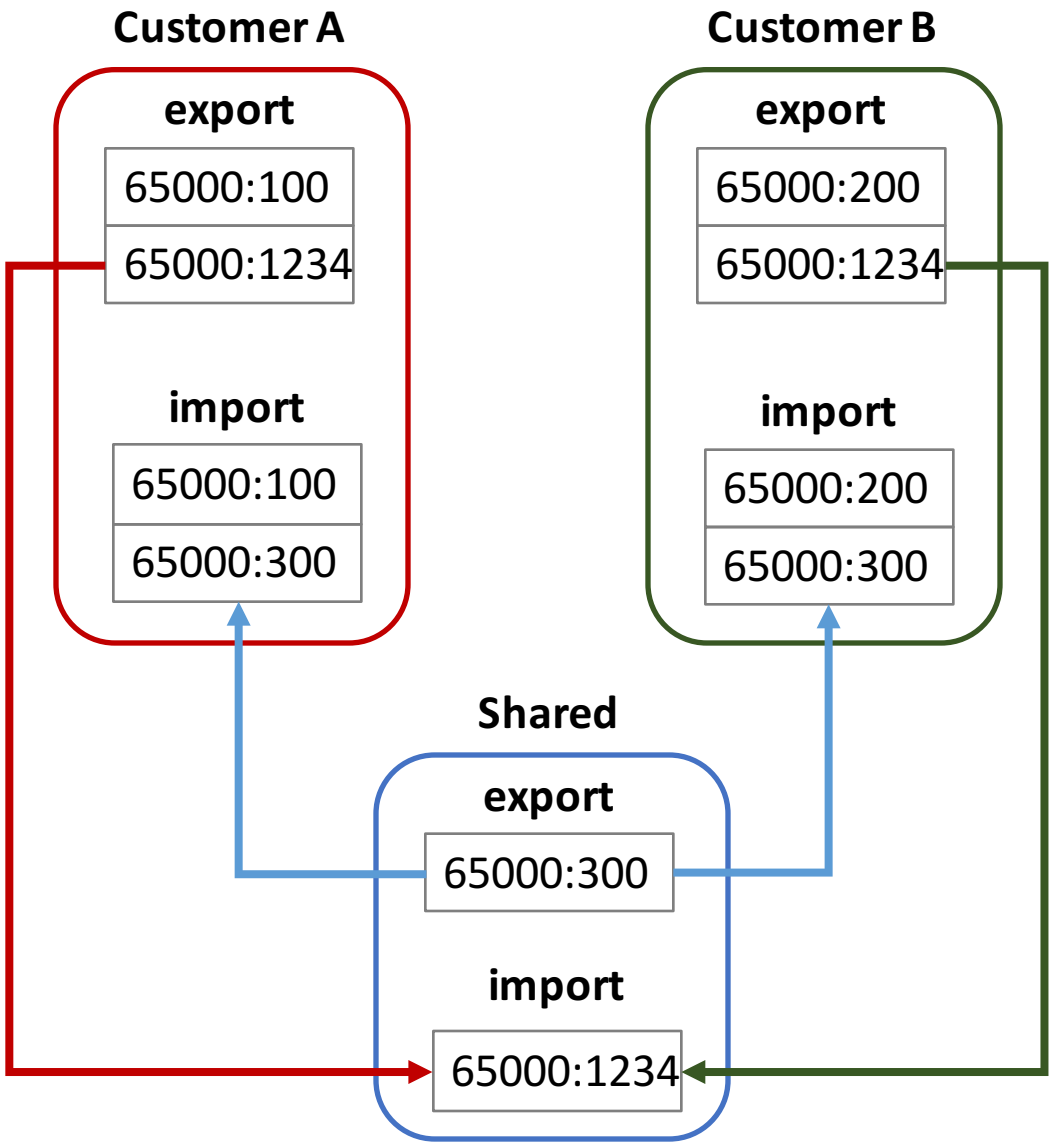
Route-Target Example 1

```
ip vrf Customer_A
 rd 65000:100
 route-target export 65000:100
 route-target import 65000:100
 route-target import 65000:300
!
ip vrf Customer_B
 rd 65000:200
 route-target export 65000:200
 route-target import 65000:200
 route-target import 65000:300
!
ip vrf Shared
 rd 65000:300
 route-target export 65000:300
 route-target import 65000:300
```

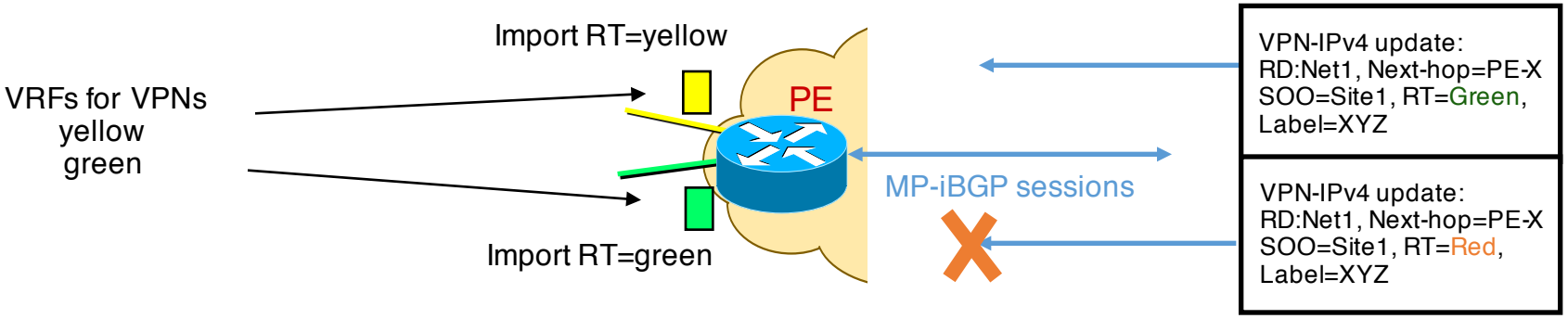


Route-Target Example 2

```
ip vrf Customer_A
 rd 65000:100
 route-target export 65000:100
 route-target export 65000:1234
 route-target import 65000:100
 route-target import 65000:300
!
ip vrf Customer_B
 rd 65000:200
 route-target export 65000:200
 route-target export 65000:1234
 route-target import 65000:200
 route-target import 65000:300
!
ip vrf Shared
 rd 65000:300
 route-target export 65000:300
 route-target import 65000:1234
```



MPLS-VPN Scaling
BGP updates filtering



Each VRF has an *import* and *export* policy configured

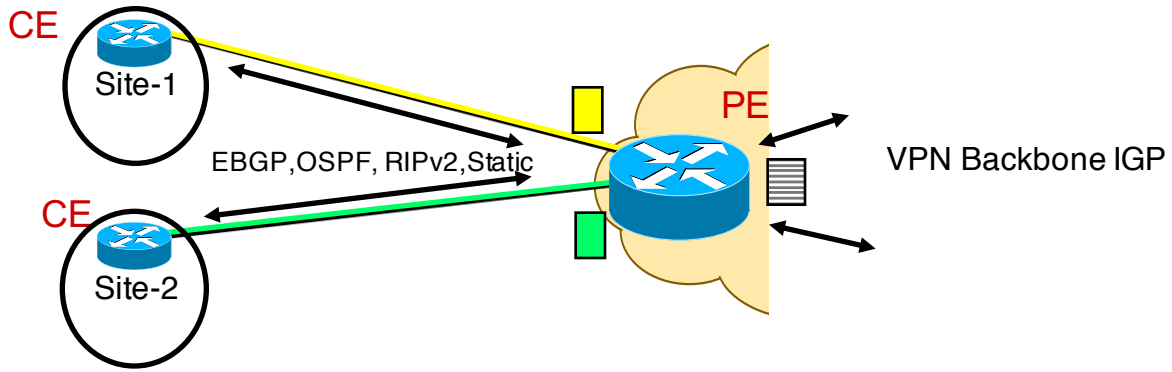
Policies use *route-target* attribute (extended community)

PE receives MP-iBGP updates for VPN-IPv4 routes

If route-target is equal to any of the import values configured in the PE, the update is accepted

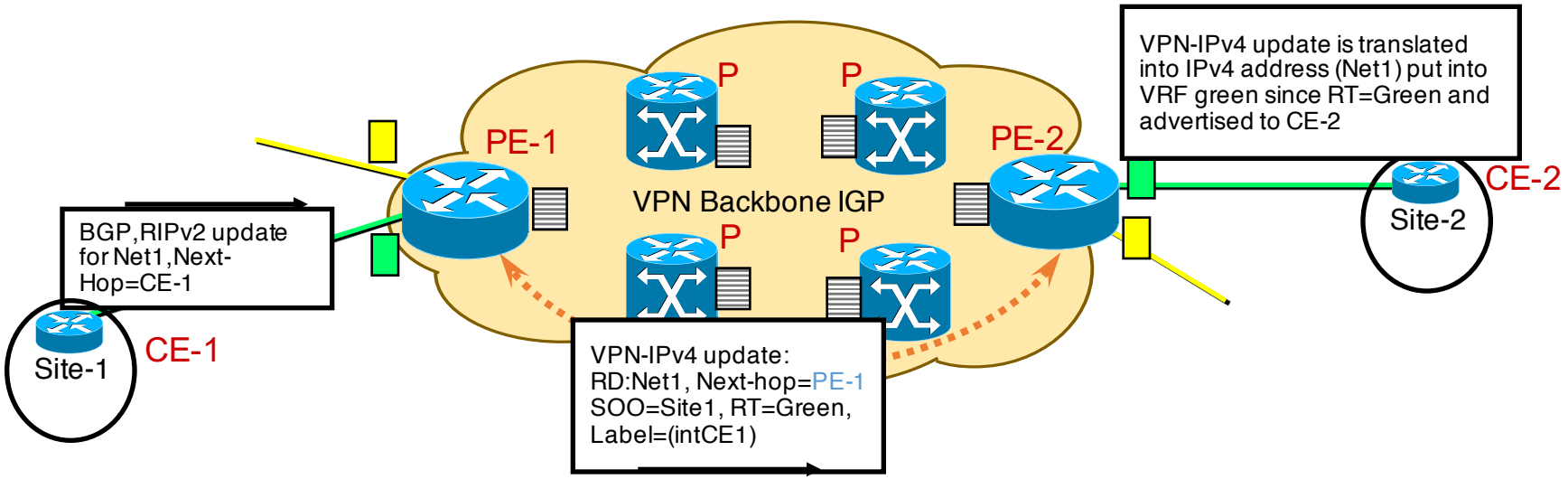
Otherwise it is silently discarded

MPLS VPN Connection Model



- The routes the PE receives from CE routers are installed in the appropriate VRF
- The routes the PE receives through the backbone IGP are installed in the global routing table
- By using separate VRFs, addresses need NOT to be unique among VPNs

MPLS VPN Connection Model

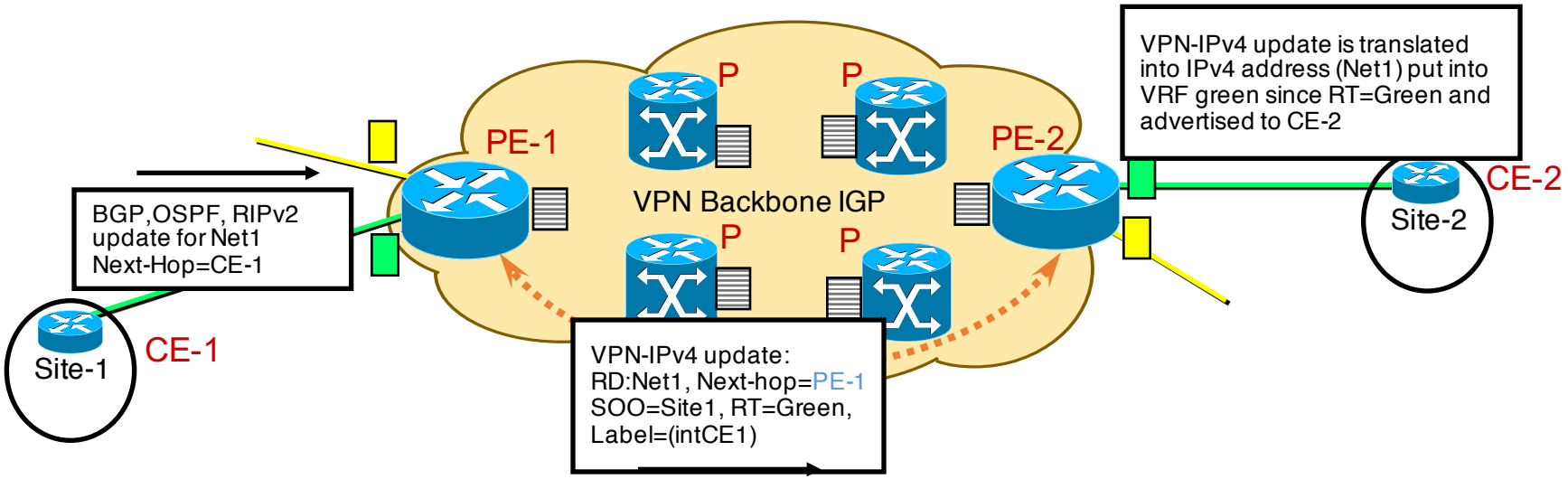


PE routers receive IPv4 updates (EBGP, RIPv2, Static…)

PE routers translate into VPN-IPv4

- Assign a SOO and RT based on configuration
- Re-write Next-Hop attribute
- Assign a label based on VRF and/or interface
- Send MP-iBGP update to all PE neighbors

MPLS VPN Connection Model

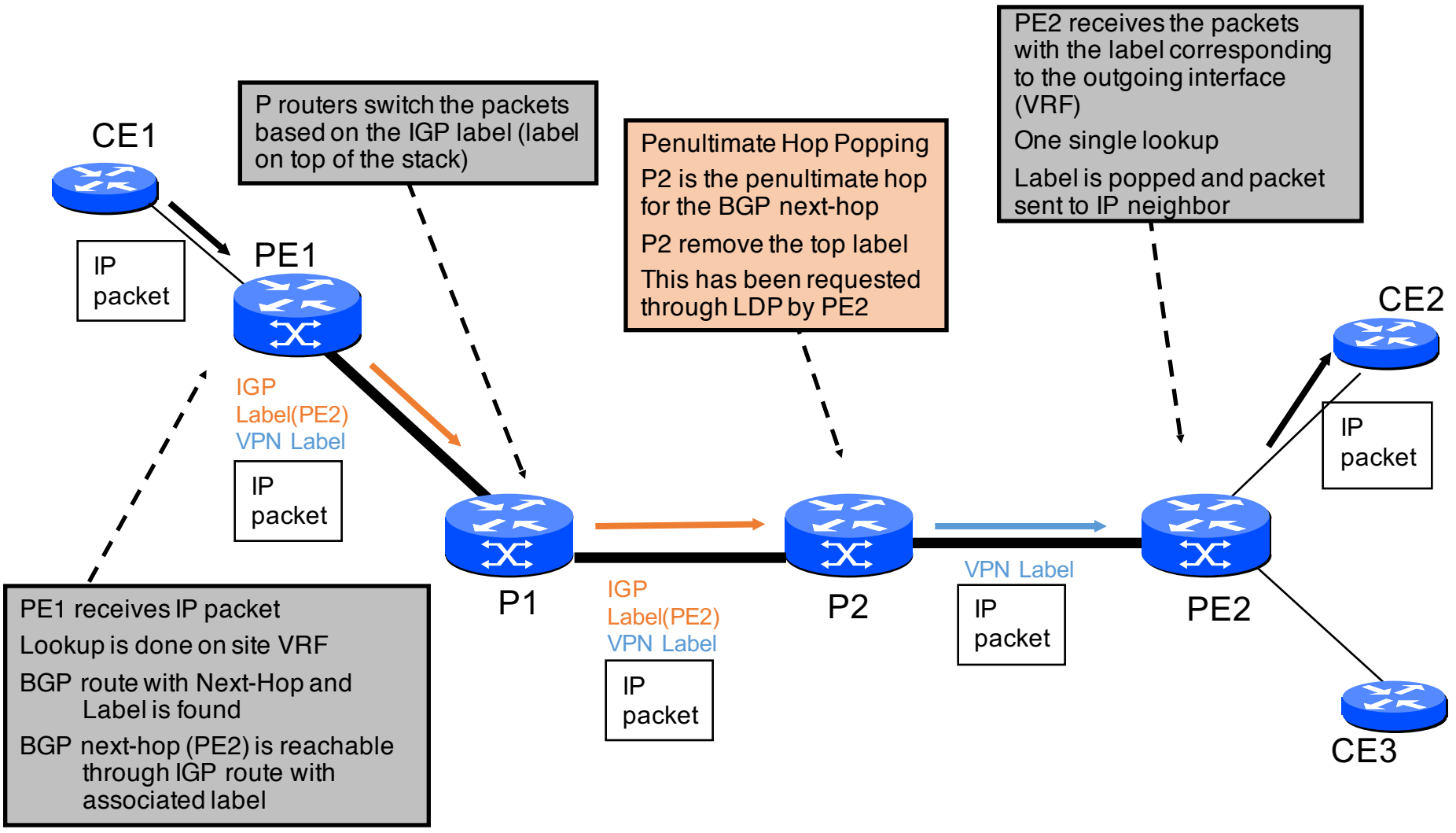


Receiving PEs translate to IPv4

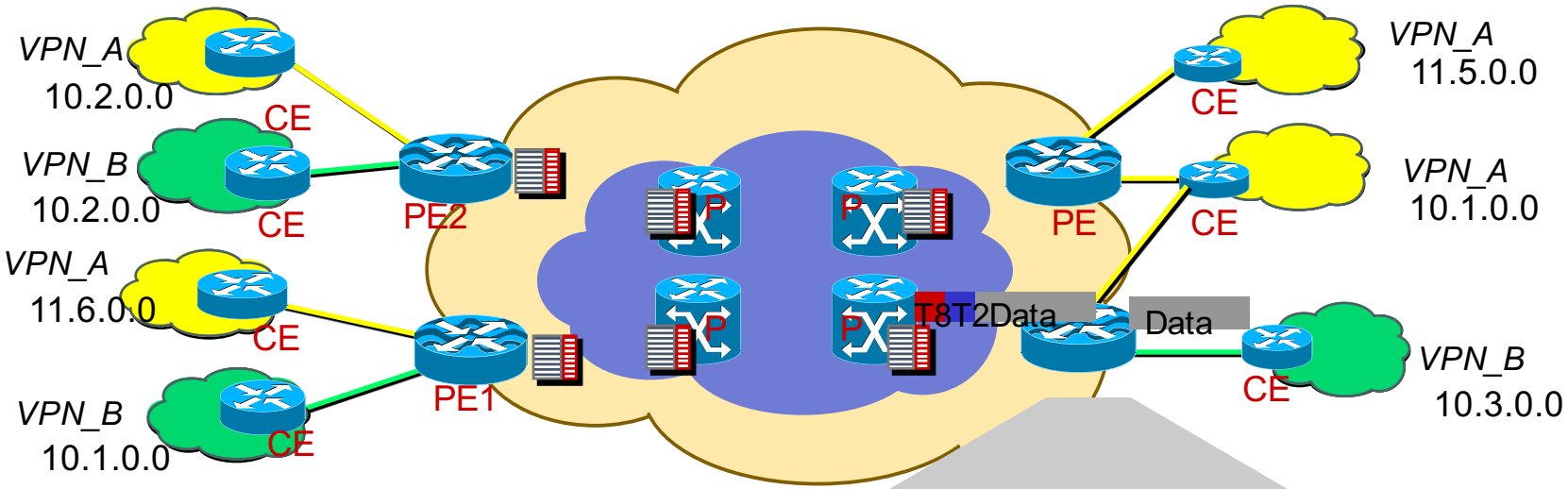
Insert the route into the VRF identified by the RT attribute (based on PE configuration)

The label associated to the VPN-IPv4 address will be set on packet forwarded towards the destination

MPLS Forwarding
Penultimate Hop Popping



Packet Forwarding Example 1

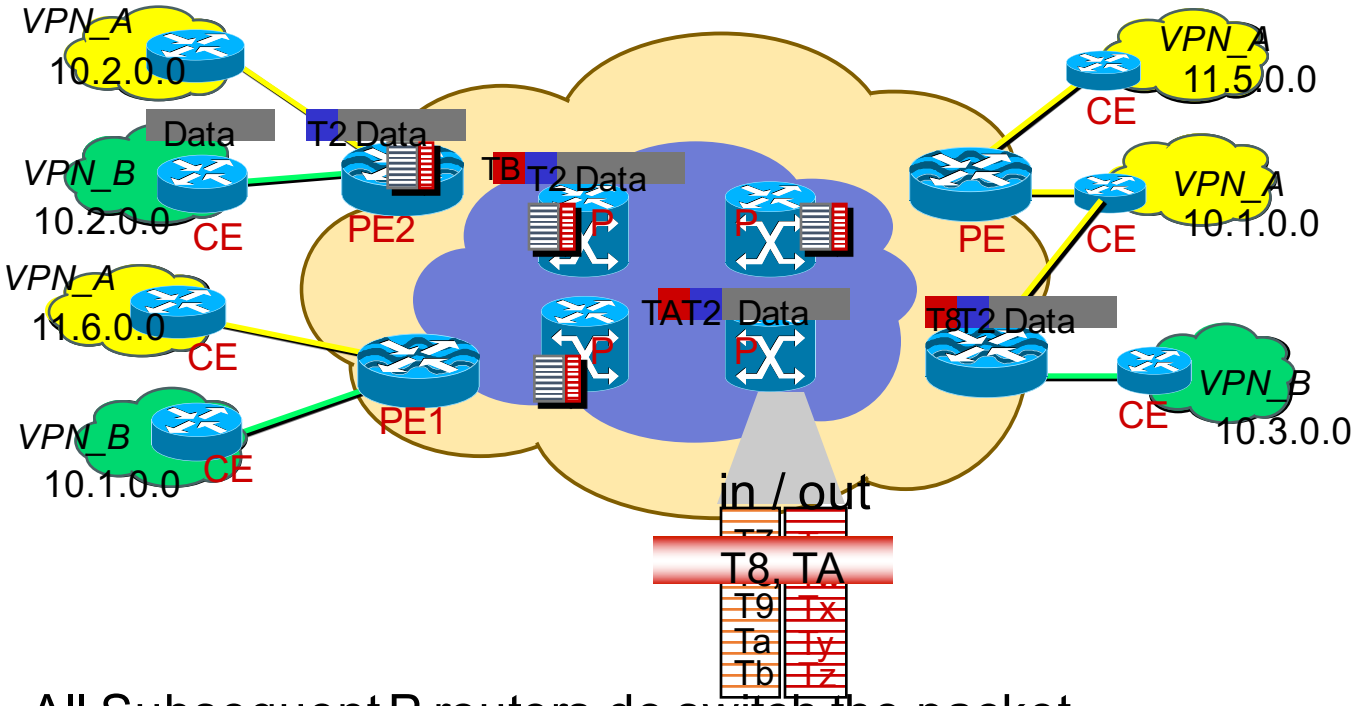


- Ingress PE receives normal IP Packets from CE router
- PE router does "IP Longest Match" from VPN_B FIB , find iBGP next hop PE2 and impose a stack of labels: exterior Label T2 + Interior Label T8

<RD_B,10.1> , iBGP next hop PE1	T1	T7
<RD_B,10.2> , iBGP next hop PE2	T2	T8
<RD_B,10.3> , iBGP next hop PE3	T3	T9
<RD_A,11.6> , iBGP next hop PE1	T4	T7
<RD_A,10.1> , iBGP next hop PE4	T5	TB
<RD_A,10.4> , iBGP next hop PE4	T6	TB
<RD_A,10.2> , iBGP next hop PE2	T7	T8

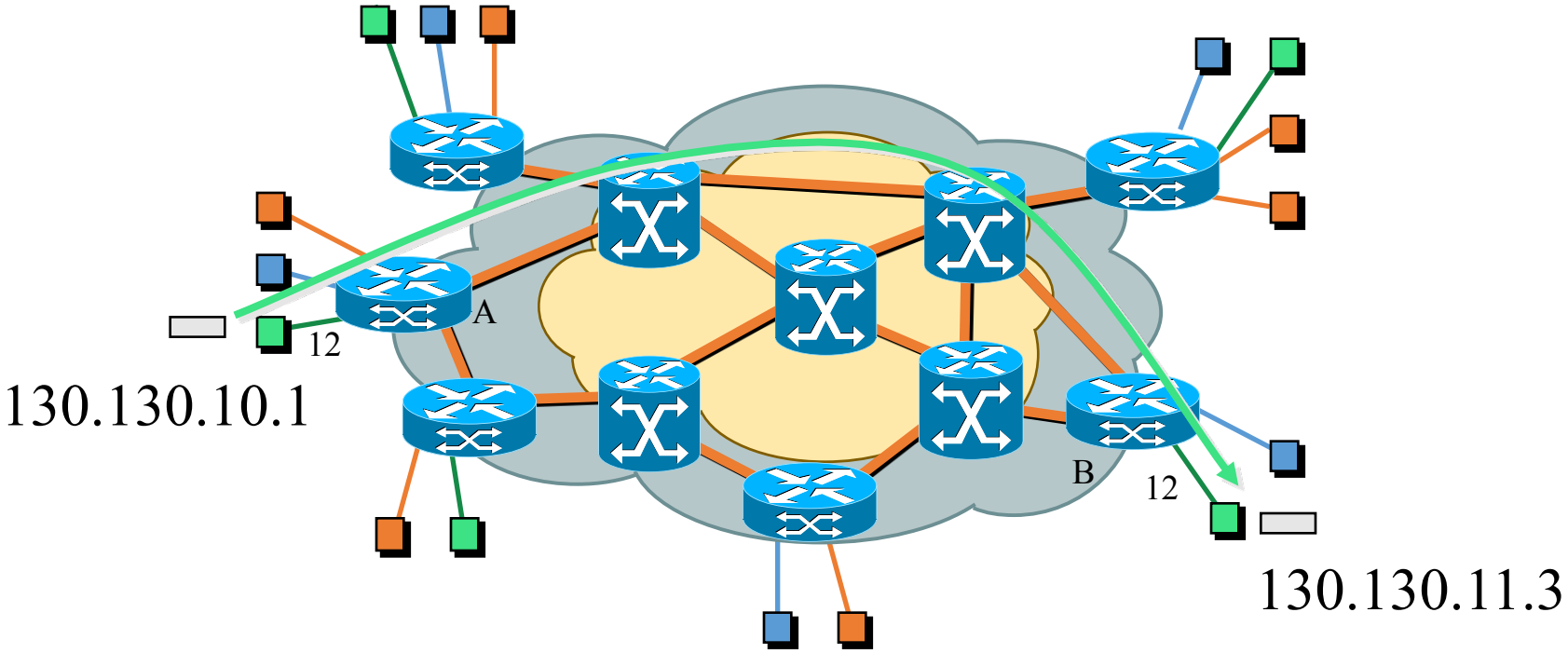
<RD_B,10.2> , iBGP NH= PE2 , T2 T8

Packet Forwarding Example 1 (cont.)



- All Subsequent P routers do switch the packet Solely on Interior Label
- Egress PE router, removes Interior Label
- Egress PE uses Exterior Label to select which VPN/CE to forward the packet to.
- Exterior Label is removed and packet routed to CE router

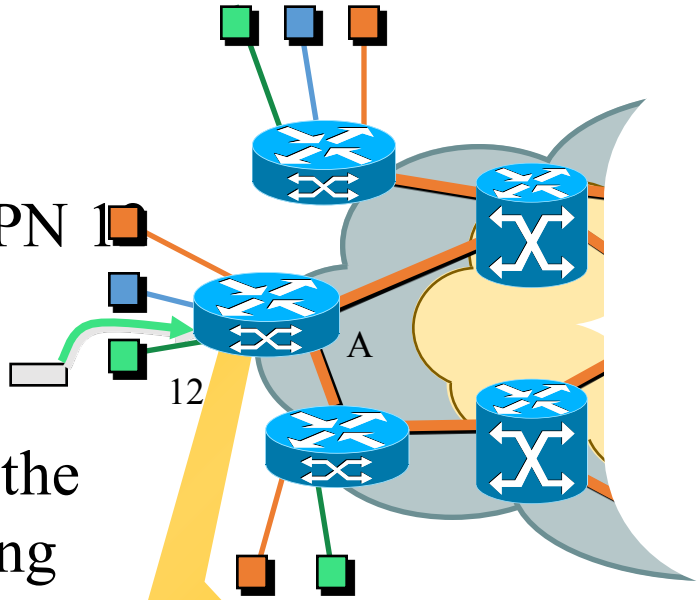
Packet Forwarding Example 2



- In VPN 12, host 130.130.10.1 sends a packet with destination 130.130.11.3
- Customer sites are attached to Provider Edge (PE) routers A & B.

Packet Forwarding Example 2 (cont.)

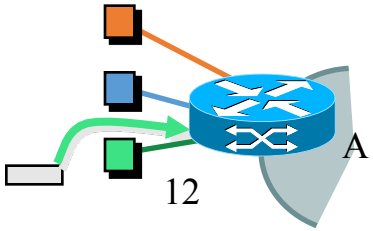
1. Packet arrives on VPN 12 link on PE router A.



2. PE router A selects the correct VPN forwarding table based on the links' VPN ID (12).

VPN-ID	VPN Site Address	VPN Site Label	Provider Edge Router Address	PE Label
12	130.130.10.0/24	26	172.68.1.11/32	42
12	130.130.11.0/24	989	172.68.1.2/32	101
…	…	…	…	…

Packet Forwarding Example 2 (cont.)



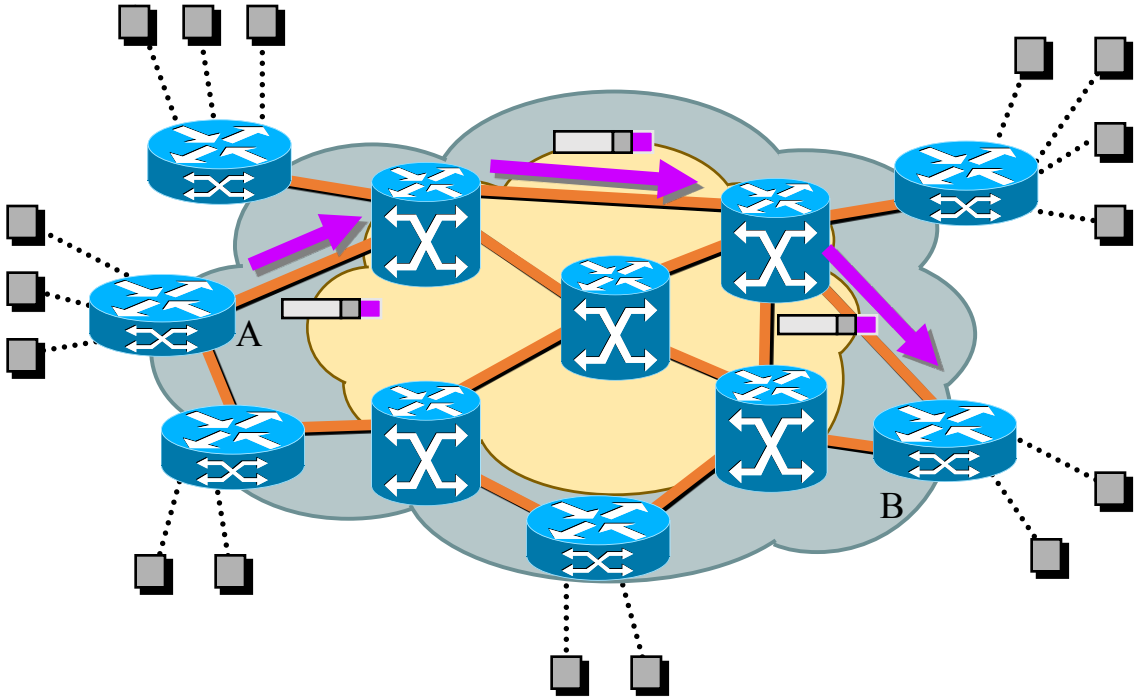
VPN-ID	VPN Site Address	VPN Site Label	Provider Edge Router Address	PE Label
12	130.130.10.0/24	26	172.68.1.11/32	42
12	130.130.11.0/24	989	172.68.1.2/32	101
…	…	…	…	…

101	989	130.130.11.3	Rest of IP packet

3. PE router A matches the incoming packet's destination address with VPN 12's forwarding table.

4. PE router A adds two labels to the packet: one identifying the destination PE, and one identifying the destination VPN site.

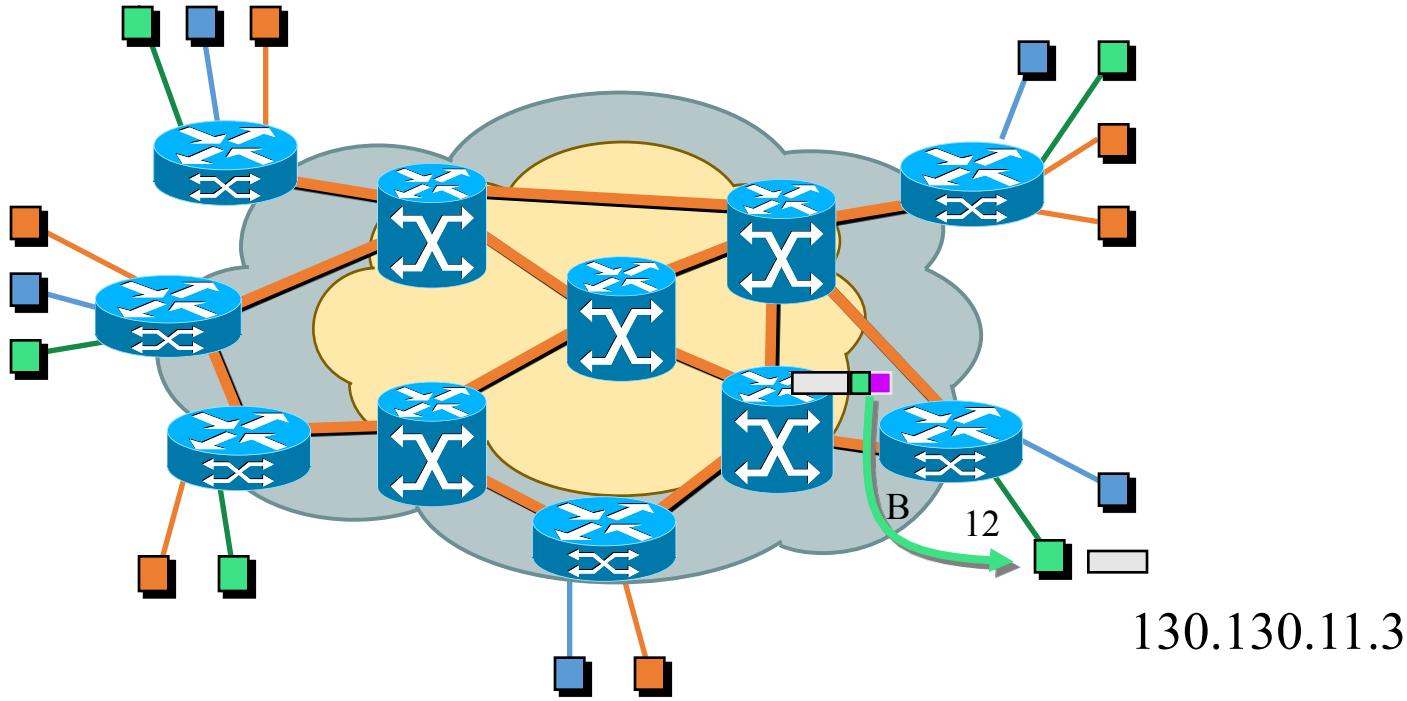
Packet Forwarding Example 2 (cont.)



5. Packet is label-switched from PE router A to PE B based on the top label, using normal MPLS.

The network core knows nothing about VPNs and sites: it only knows how to get packets from A to B using MPLS.

Packet Forwarding Example 2 (cont.)



6. PE router B identifies the correct site in VPN 12 from the inner label.

7. PE router B removes the labels and forwards the IP packet to the correct VPN 12 site.

MPLS VPN - Configuration

- VPN knowledge is on PE routers
- PE router have to be configured for
  - VRF and Route Distinguisher
  - VRF import/export policies (based on Route-target)
  - Routing protocol used with CEs
  - MP-BGP between PE routers
  - BGP for Internet routers
    - With other PE routers
    - With CE routers

MPLS VPN - Configuration
VRF and Route Distinguisher

- RD is configured on PE routers (for each VRF)
- VRFs are associated to RDs in each PE
- Common (good) practice is to use the same RD for the same VPN in all PEs

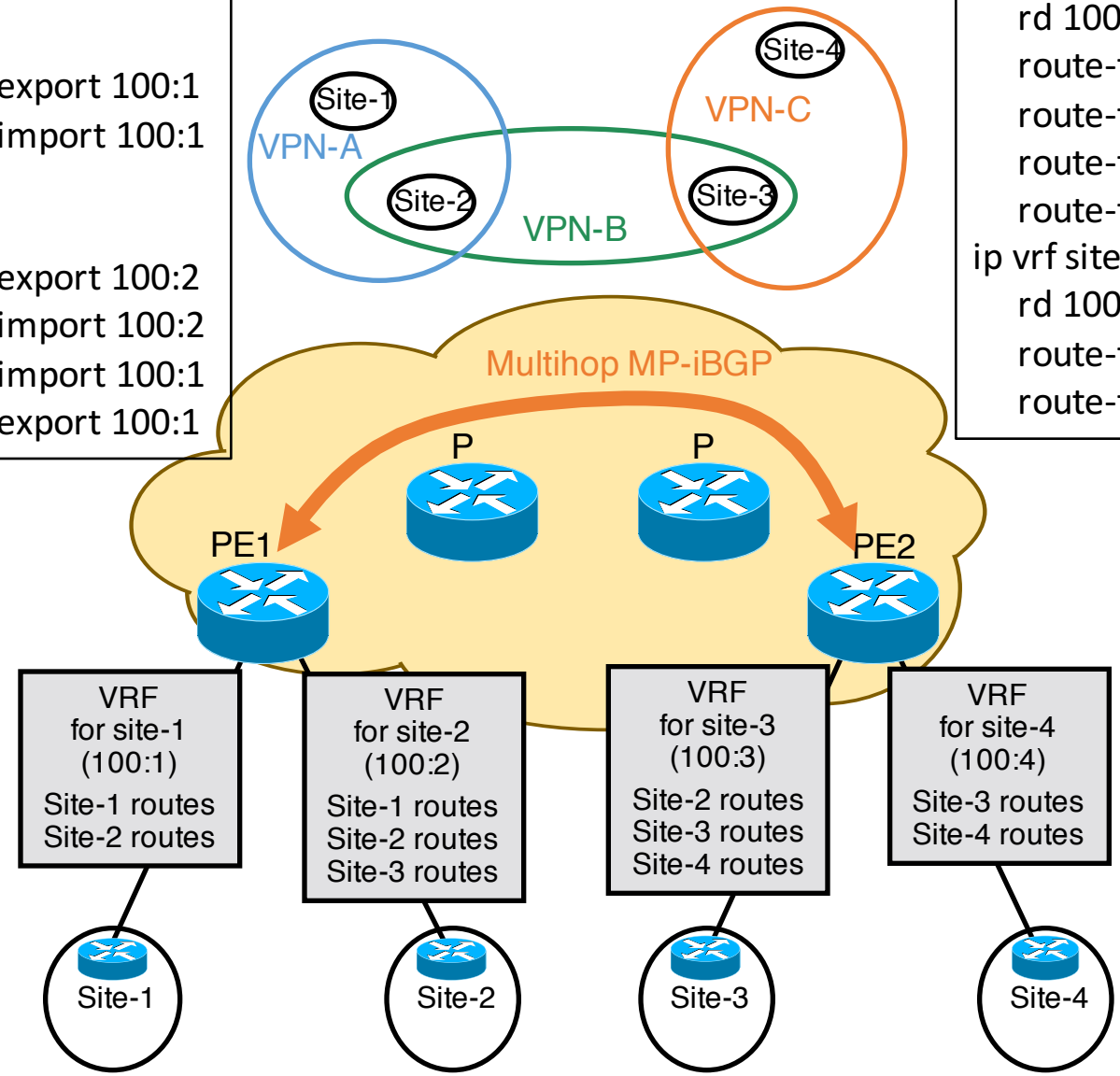
  But not mandatory
- VRF configuration command

```
ip vrf <vrf-symbolic-name>
 rd <route-distinguisher-value>
 route-target import <community>
 route-target export <community>
```

CLI - VRF configuration

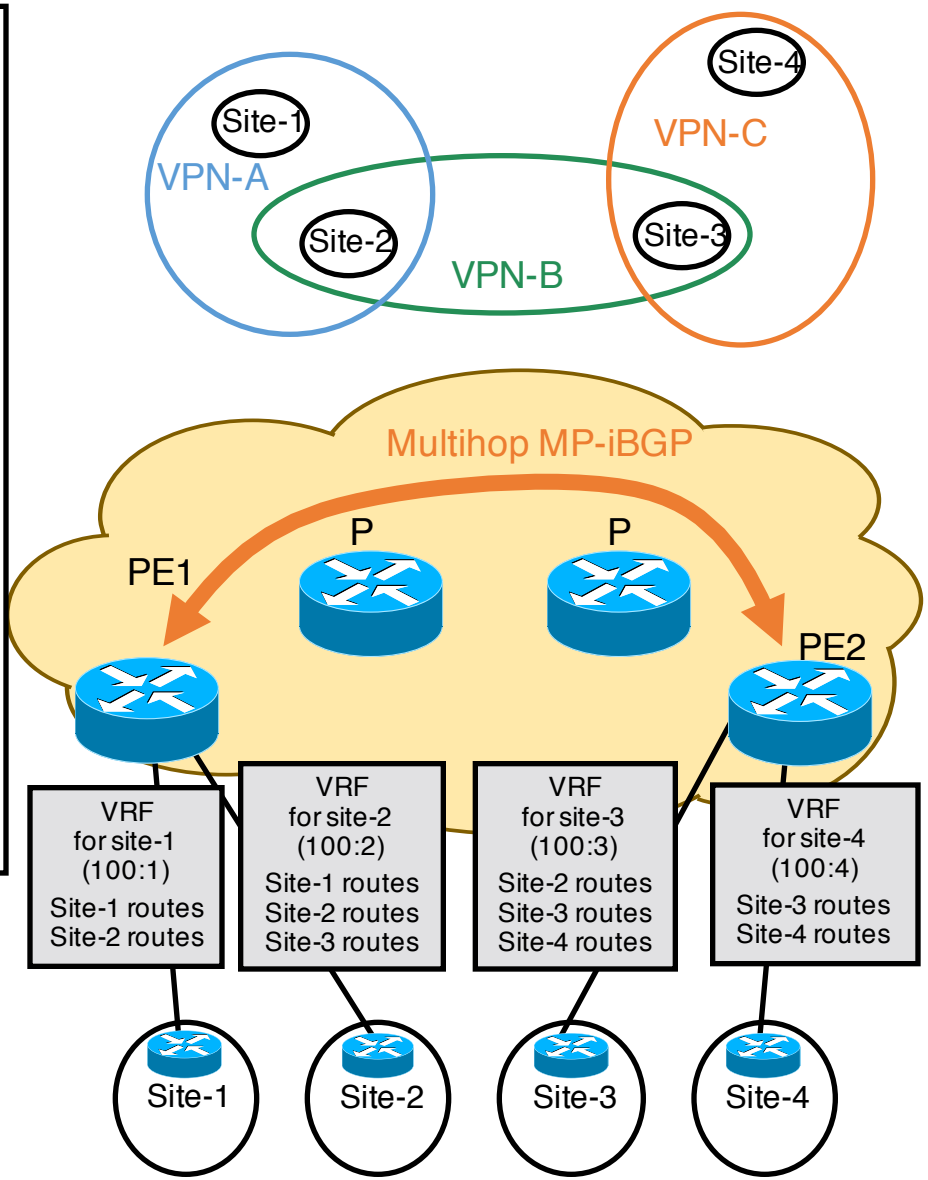
```
ip vrf site1
    rd 100:1
    route-target export 100:1
    route-target import 100:1
ip vrf site2
    rd 100:2
    route-target export 100:2
    route-target import 100:2
    route-target import 100:1
    route-target export 100:1
```

```
ip vrf site3
    rd 100:3
    route-target export 100:2
    route-target import 100:2
    route-target import 100:3
    route-target export  100:3
ip vrf site-4
    rd 100:4
    route-target export 100:3
    route-target import 100:3
```



MPLS VPN - Configuration
PE/CE routing protocols

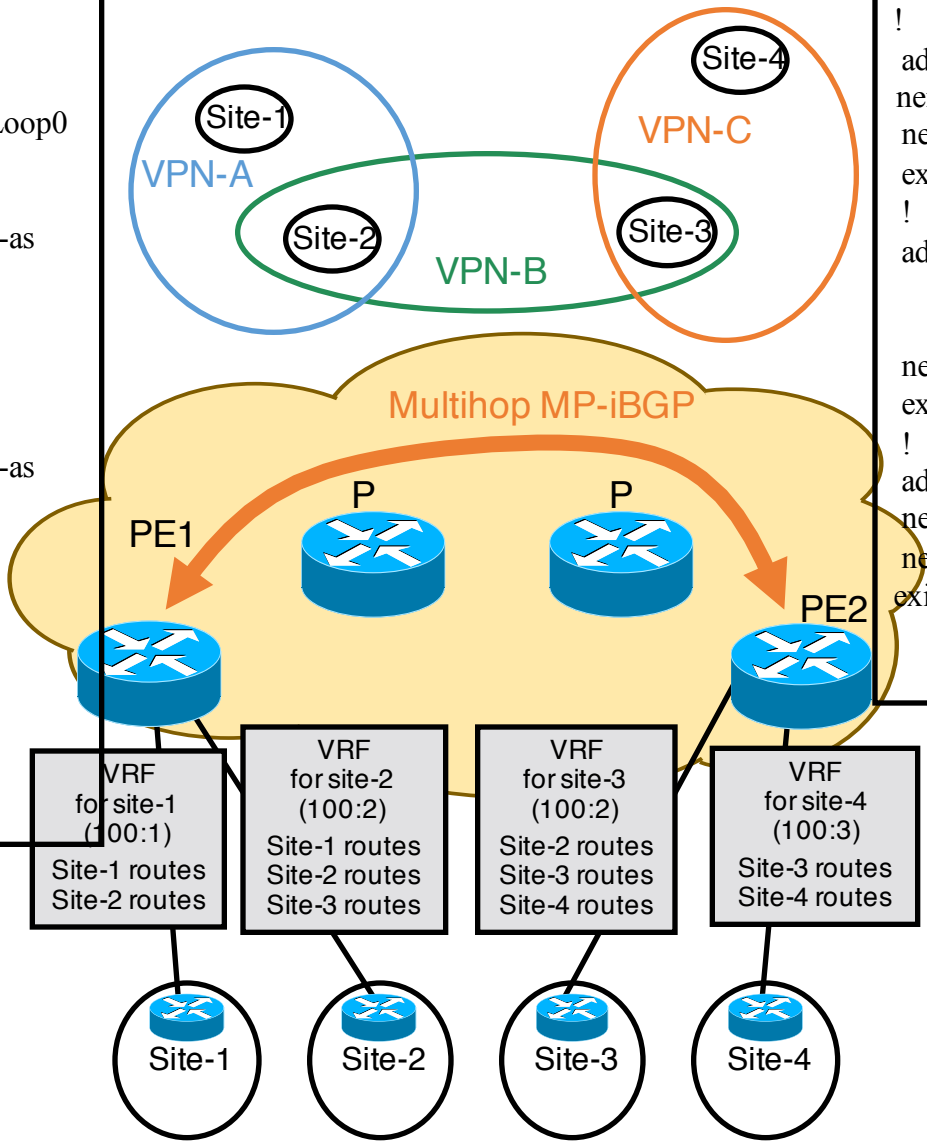
```
ip vrf site1
    rd 100:1
    route-target export 100:12
    route-target import 100:12
ip vrf site2
    rd 100:2
    route-target export 100:12
    route-target import 100:12
    route-target import 100:23
    route-target export 100:23
!
interface Serial3/6
 ip vrf forwarding site1
 ip address 192.168.61.6
255.255.255.0
 encapsulation ppp
!
interface Serial3/7
 ip vrf forwarding site2
 ip address 192.168.62.6
255.255.255.0
 encapsulation ppp
```




```
ip vrf site3
    rd 100:3
    route-target export 100:23
    route-target import 100:23
    route-target import 100:34
    route-target export 100:34
ip vrf site-4
    rd 100:4
    route-target export 100:34
    route-target import 100:34
!
interface Serial4/6
 ip vrf forwarding site3
 ip address 192.168.73.7
255.255.255.0
 encapsulation ppp
!
interface Serial4/7
 ip vrf forwarding site4
 ip address 192.168.74.7
255.255.255.0
 encapsulation ppp
```

MPLS VPN - Configuration
PE/CE routing protocols

```
router bgp 100
no bgp default ipv4-unicast
 neighbor 7.7.7.7 remote-as 100
 neighbor 7.7.7.7 update-source Loop0
!
 address-family ipv4 vrf site2
    neighbor 192.168.62.2 remote-as
                    65502
 neighbor 192.168.62.2 activate
 exit-address-family
 !
 address-family ipv4 vrf site1
    neighbor 192.168.61.1 remote-as
                    65501
 neighbor 192.168.61.1 activate
 exit-address-family
 !
 address-family vpnv4
 neighbor 7.7.7.7 activate
 neighbor 7.7.7.7 next-hop-self
exit-address-family
```




```
router bgp 100
no bgp default ipv4-unicast
 neighbor 6.6.6.6 remote-as 100
 neighbor 6.6.6.6 update-source Loop0
!
 address-family ipv4 vrf site4
neighbor 192.168.74.4 remote-as 65504
 neighbor 192.168.74.4 activate
 exit-address-family
 !
 address-family ipv4 vrf site3
     neighbor 192.168.73.3 remote-as
                    65503
 neighbor 192.168.73.3 activate
 exit-address-family
 !
 address-family vpnv4
 neighbor 6.6.6.6 activate
 neighbor 6.6.6.6 next-hop-self
exit-address-family
```