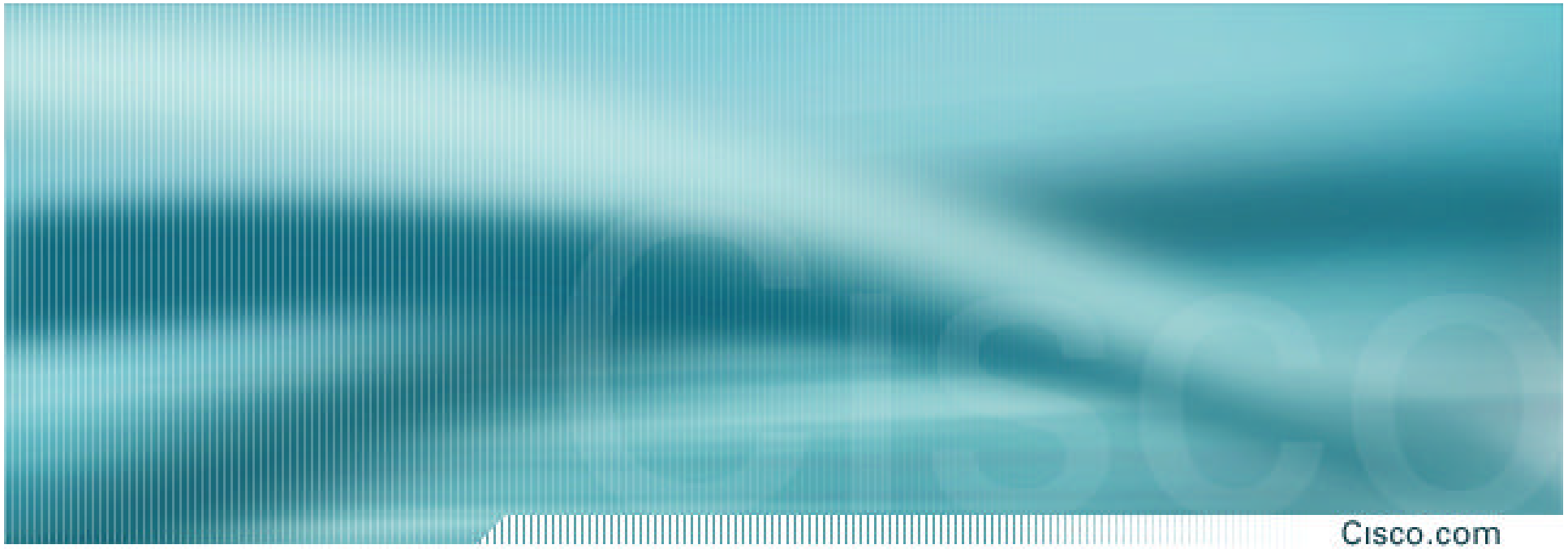


MPLS – VPN´s in der Praxis

Wolfram Maag
Internetworking Consultant

Agenda

- Gründe für MPLS VPN´s
- Einführung in MPLS
- MPLS/VPNs
- Supported Cisco HW

Gründe für MPLS VPNs bei SP´s

- Eine L3 Infrastruktur managen
- Unabhängigkeit von IP Adressen
- Sichere VPN´s ohne Encryption
- AToM-Support
- TE-Support
- Fast Reroute
- Skalierbarkeit
- VRF-Support
- Common Service Areas

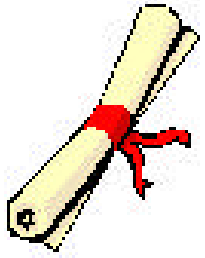
Gründe für MPLS VPN´s im LAN

Cisco.com

- Sehr großer Campus mit sehr vielen Usern (>10.000)
- Verschiedene Firmen teilen einen Campus
- Gemeinsames Netzwerkequipment
- Bedarf nach hoher Verfügbarkeit
- Ein SP für LAN und WAN Services
- Shared services (SAP/R3, Internet, Mail, ….)

MPLS and Security

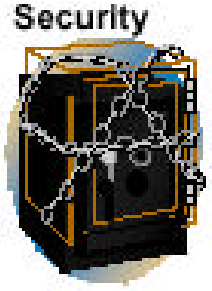
Miercom



Cisco MPLS based VPNs:
Equivalent to the Security of Frame Relay and ATM

Miercom, March 30, 2001

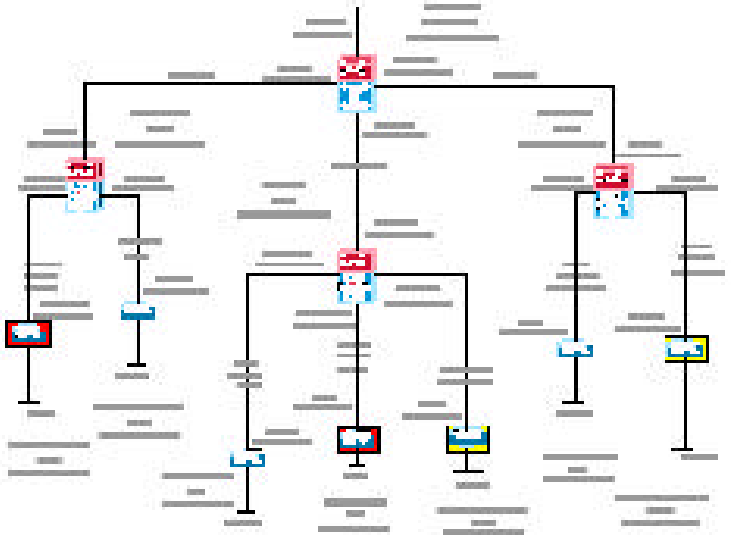
http://www.mier.com/reports/cisco/MPLS-VPNs.pdf



MPLS/VPNs are secure

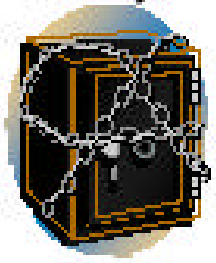
Miercom independent testing confirmed Cisco MPLS VPN is secure:

- Customers network topology is not revealed to the outside world
- Customers can maintain own addressing plans and the freedom to use either public or private address space
- Attackers cannot gain access into VPNs or Service Provider's network
- Impossible for attacker to insert "spoofed" label into a Cisco MPLS network and thus gain access to a VPN or the MPLS core



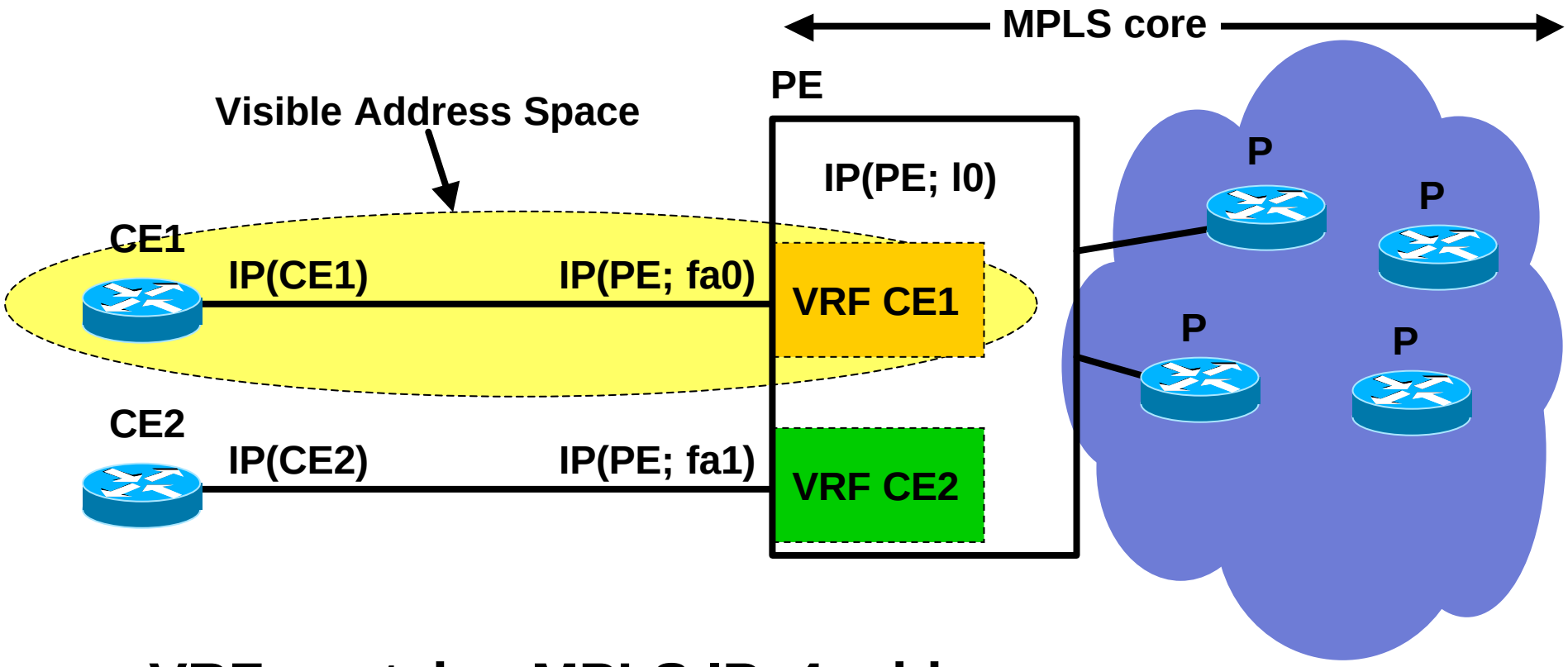
Test Network Topology

Security

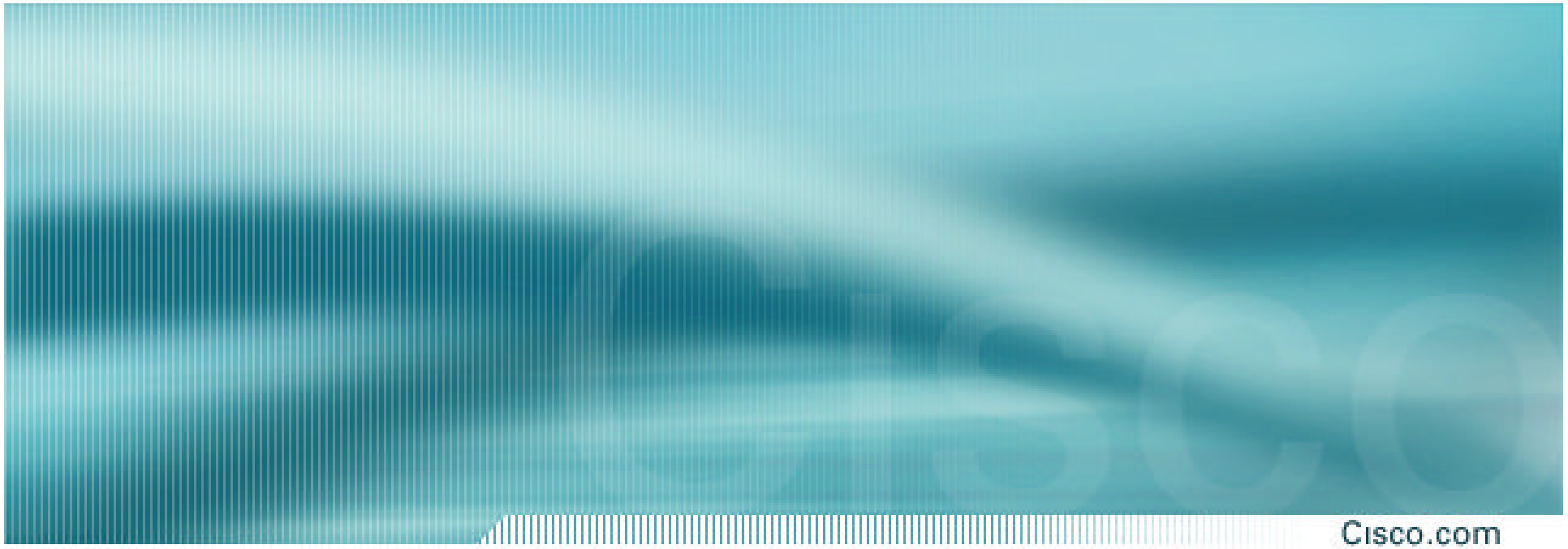


Testbericht unter http://www.mier.com/reports/cisco/MPLS-VPNs.pdf

Hiding of the MPLS Core Structure



- VRF contains MPLS IPv4 addresses
- Only peering Interface (on PE) exposed (-> CE)!
  -> ACL or unnumbered



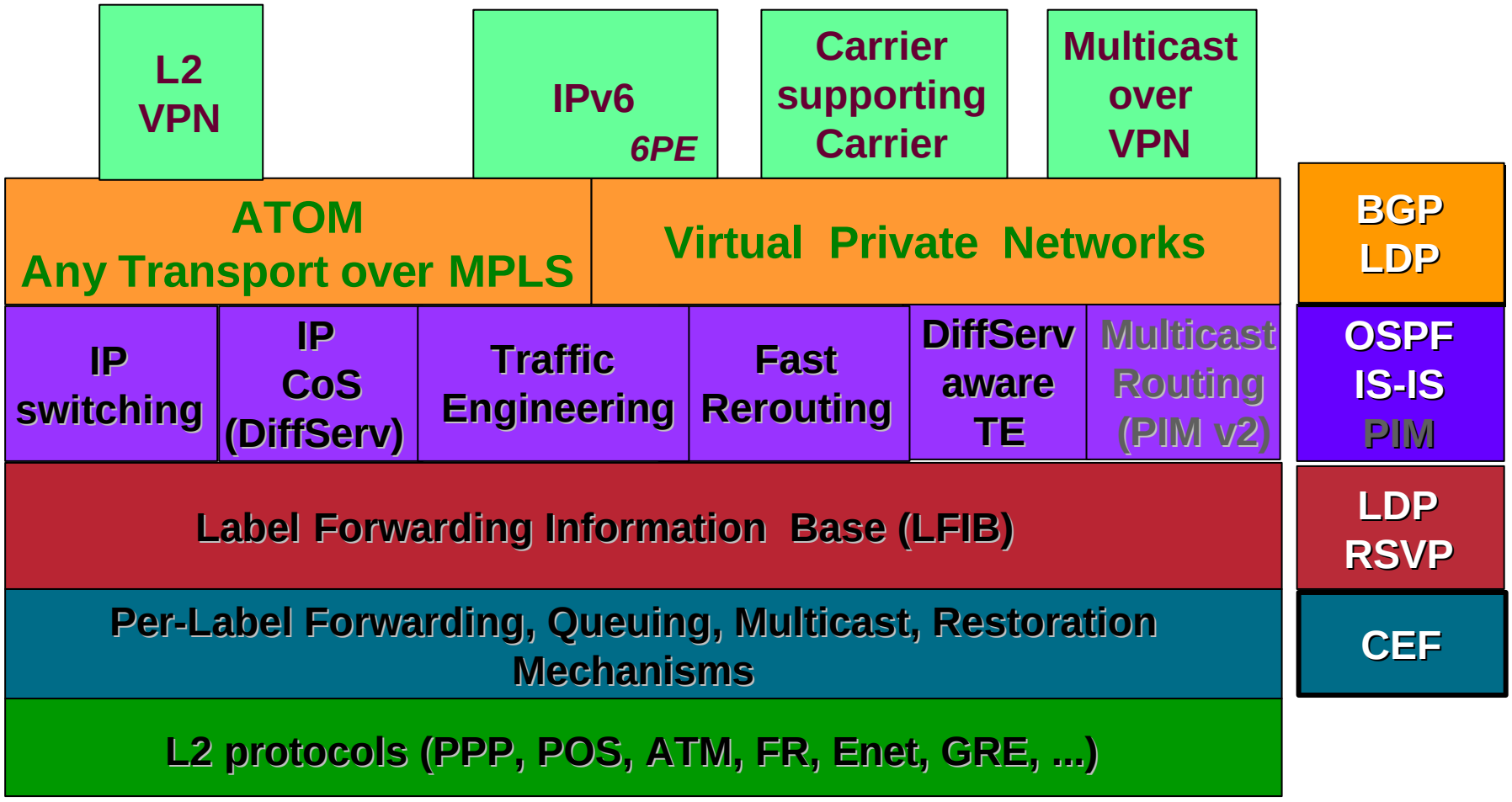
History and Basic Functions

Standardization

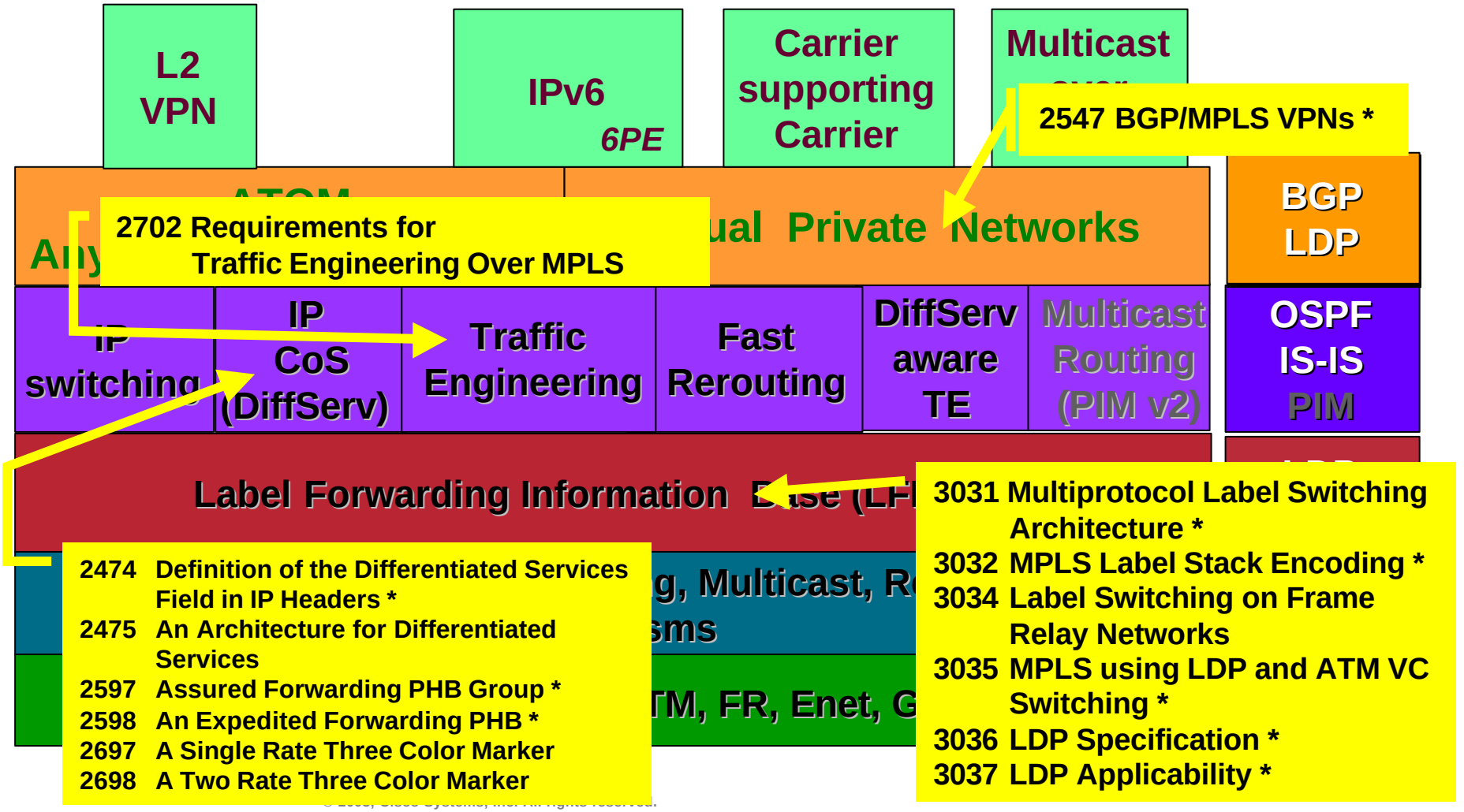
- Initiative of Cisco Systems in December 1996.
  BOF-Session at the IETF Meeting in San Jose.
- Multi Protocol Label Switching (MPLS) working-group established at IETF by beginning of 1997
- Base documents (Architecture, Label Encoding...) in RFCs 3031 bis 3038 defined.
  MPLS Support for DiffServ is described in RFC3270
- Informational Status: TE RFC2702, RSVP ext. RFC3210
  VPNs RFC2547bis

Details zu MPLS unter http://www.ietf.org/html.charters/mpls-charter.html

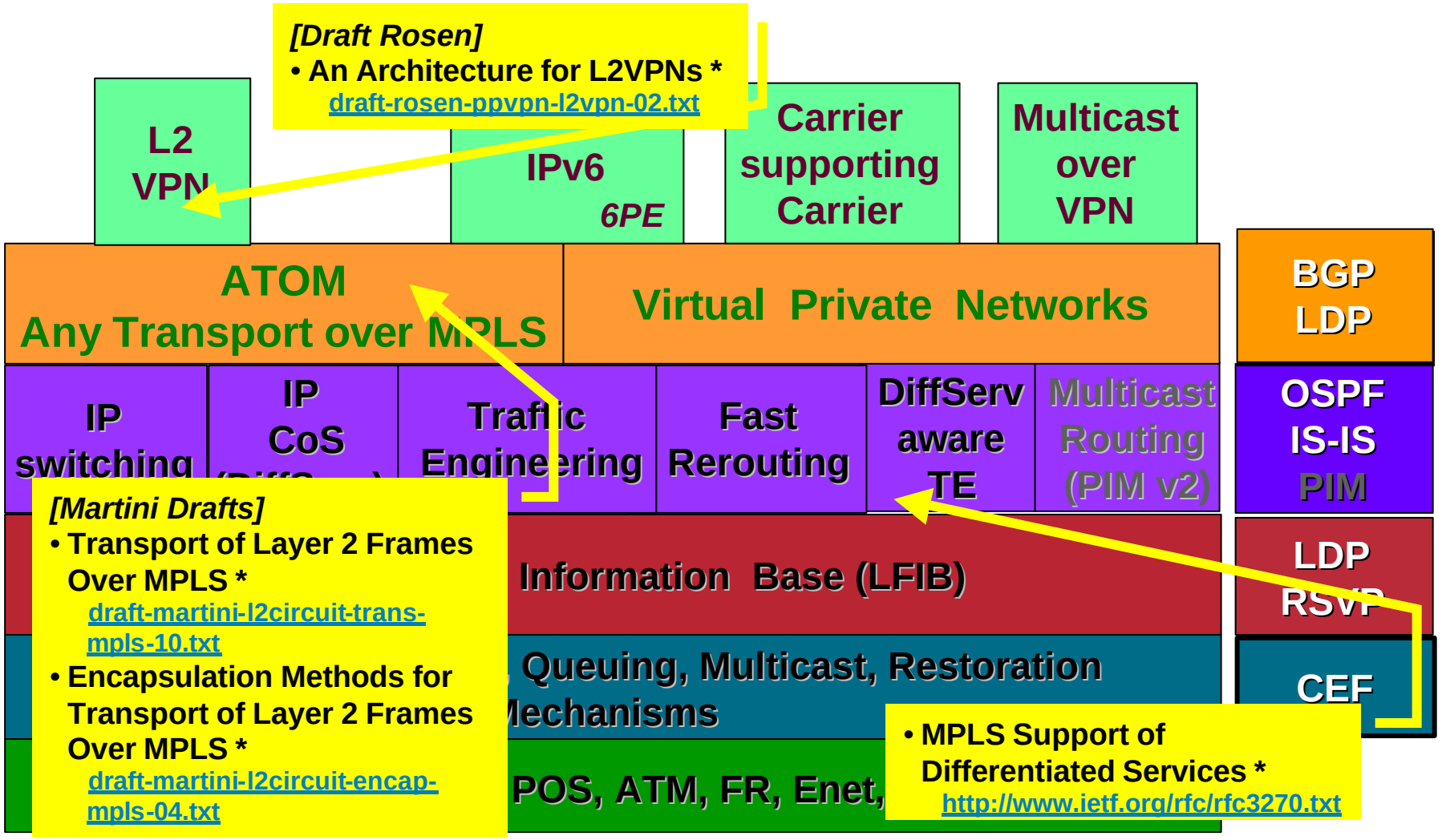
MPLS advanced services



MPLS Innovation & Standards

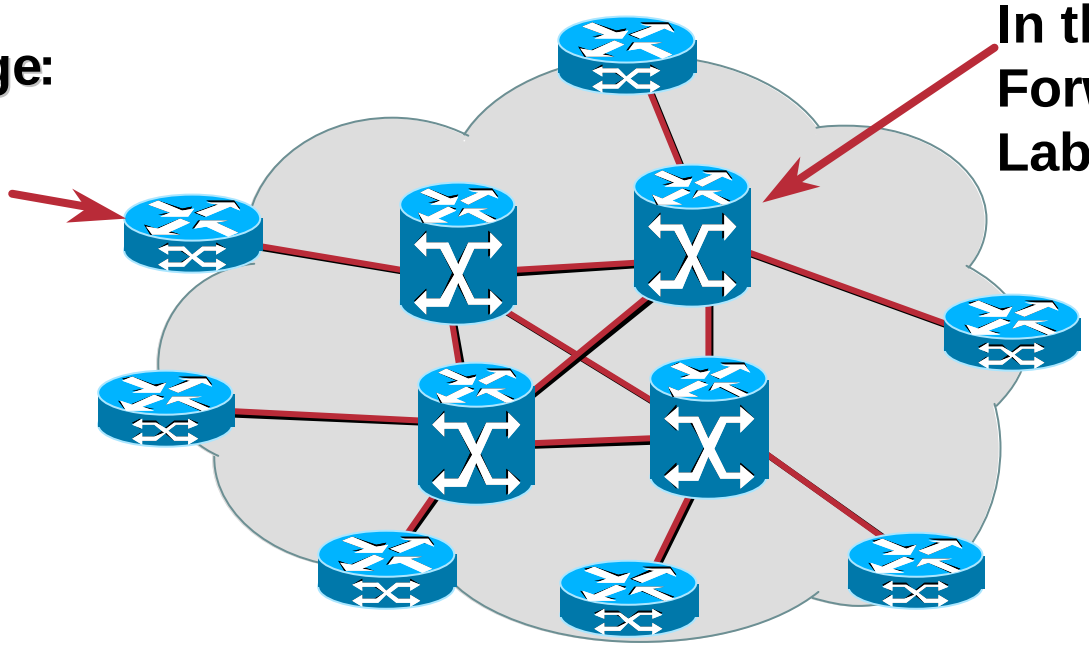


MPLS Innovation-in-Progress



MPLS Concept

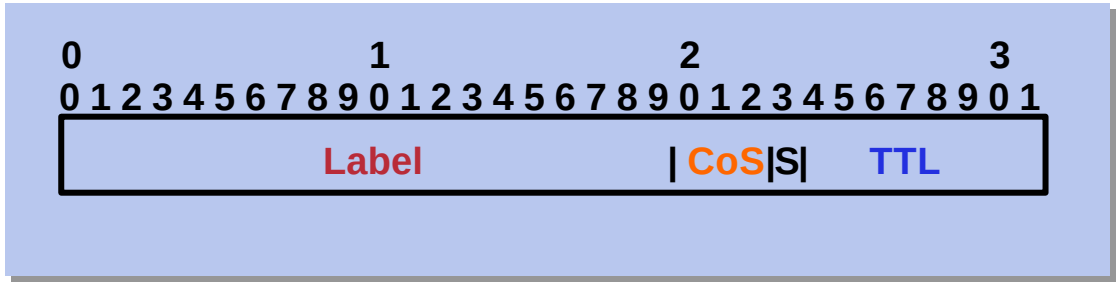
At the Edge:
- classify
- label



In the Core:
Forwarding based on Label instead of IP-Adr.

- **New services through separation of Forwarding and Control**

Generic MPLS Headerformat

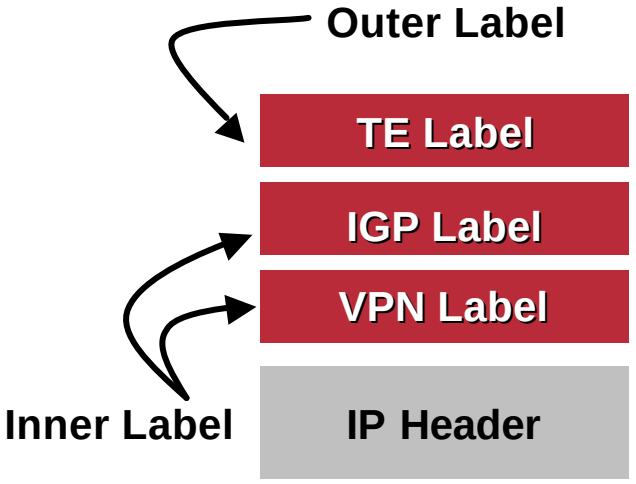


Label = 20 bits
CoS = Class of Service, 3 bits (EXPerimental Bits)
S = Bottom of stack, 1bit
TTL = Time to live, 8 bits

- **Generic: Usage over Ethernet, 802.3, POS, DPT, PPP Links, Frame Relay, ATM PVCs, etc.**
- **2 new Ethertypes / PPP PIDs / SNAP / etc. Values - one for Unicast, one for Multicast**
- **4 Byte (per MPLS Layer)**
- **Multiple Label-Stacks possible !**

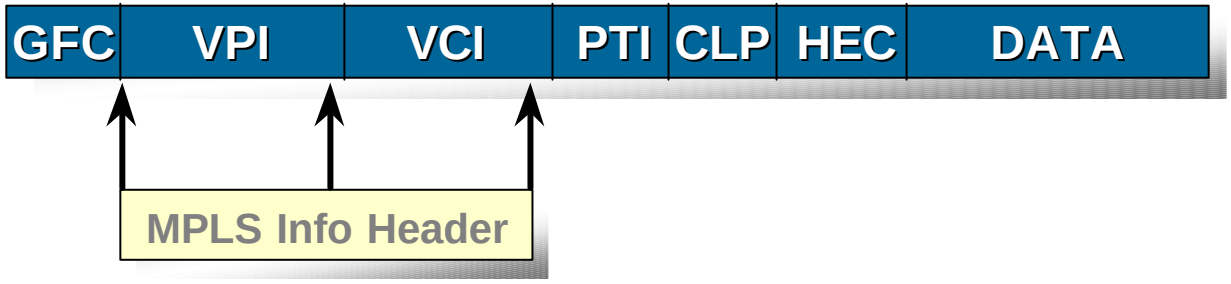
Label Stacking

- Arrange labels in a stack
- Inner labels can be used to designate services/FECs, etc.
  - E.g. VPNs, fast re-route
- Outer label used to route/switch the MPLS packets in the network
- Allows building services such as
  - MPLS VPNs
  - Traffic engineering and fast re-route
  - VPNs over traffic engineered core
  - Any transport over MPLS

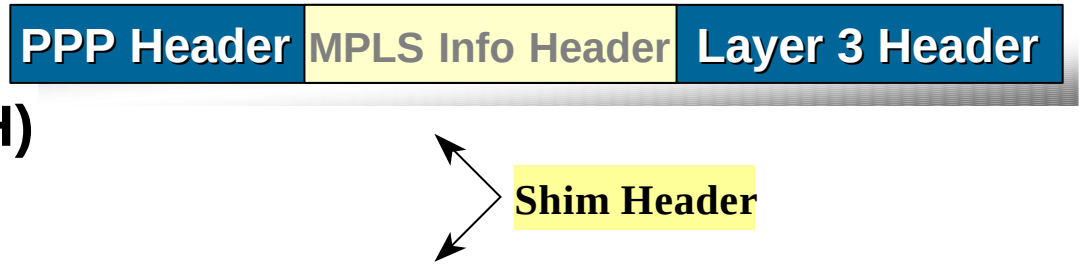


MPLS Encapsulations

ATM Cell Header



PPP Header
(Packet over SONET/SDH)



LAN MAC Tag Header

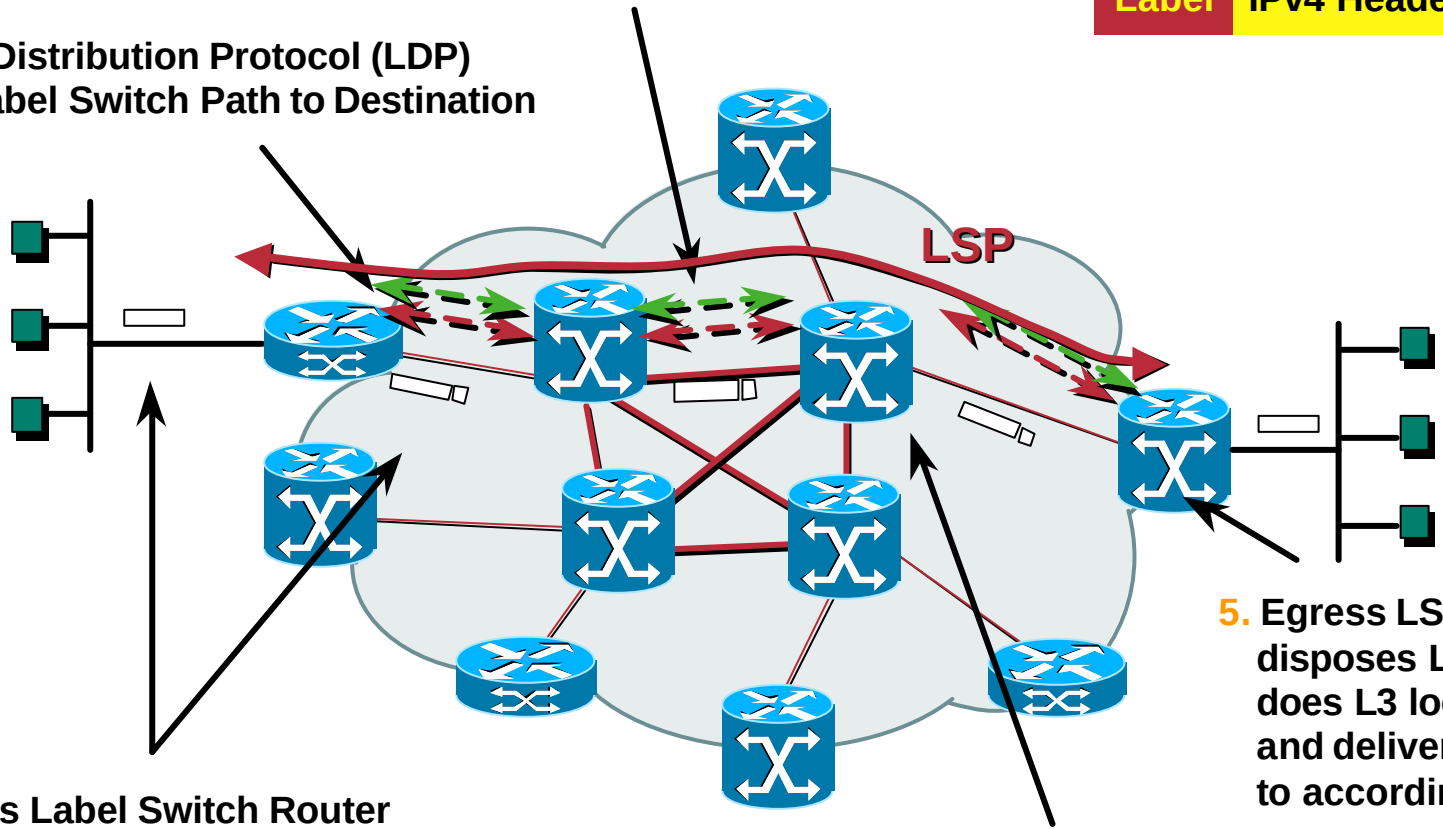
MPLS
...used Short-Terms/Acronyms

- **P** Router = Provider Router (Core LSR)
- **PE** Router = Provider Edge Router (Edge LSR)
  knows about VPNs and connects CEs
- **CE** Router = Customer Edge Router
- **LDP** = Label Distribution Protocol
- **FIB** = Forwarding Information Base
- **LFIB** = Label Forwarding Information Base
- **VPN** = Virtual Private Network
- **VRF** = VPN Routing/Forwarding Instance
- **RD** = Route Distinguisher
- **RT** = Route Target

MPLS: Operation

1. legacy IP Routing Protocols like OSPF, ISIS are used to create the network layer reachability information (NLRI)

2. Label Distribution Protocol (LDP) builds Label Switch Path to Destination



Label | IPv4 Header | Data

3. Ingress Label Switch Router receives Packet, does Layer-3 services(e.g. QoS) and *labels* the Packet

4. Core LSR switches Packets through Label Swapping mechanism

5. Egress LSR disposes Label , does L3 lookup and delivers Packet to according port

Separate Forwarding/Control

Forwarding Component

...also referred to as the data plane

Is responsible for forwarding packets/cells based on labels

Uses a label forwarding database maintained by the label switch

Simple Label Swapping

Separate Forwarding/Control

Control Component

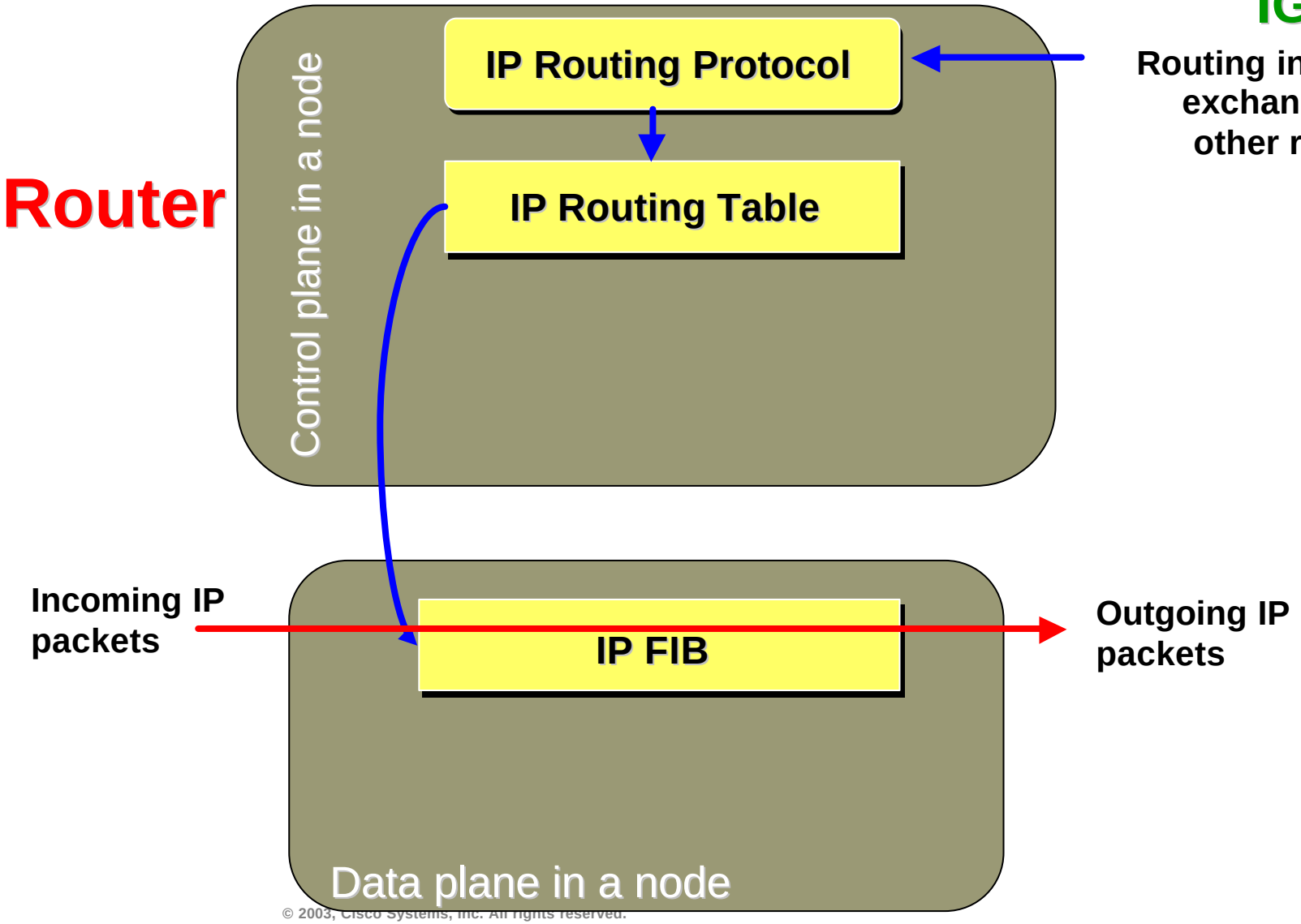
...also referred to as the **control plane**

Responsible for creating and maintaining label forwarding information (known as **label bindings**)

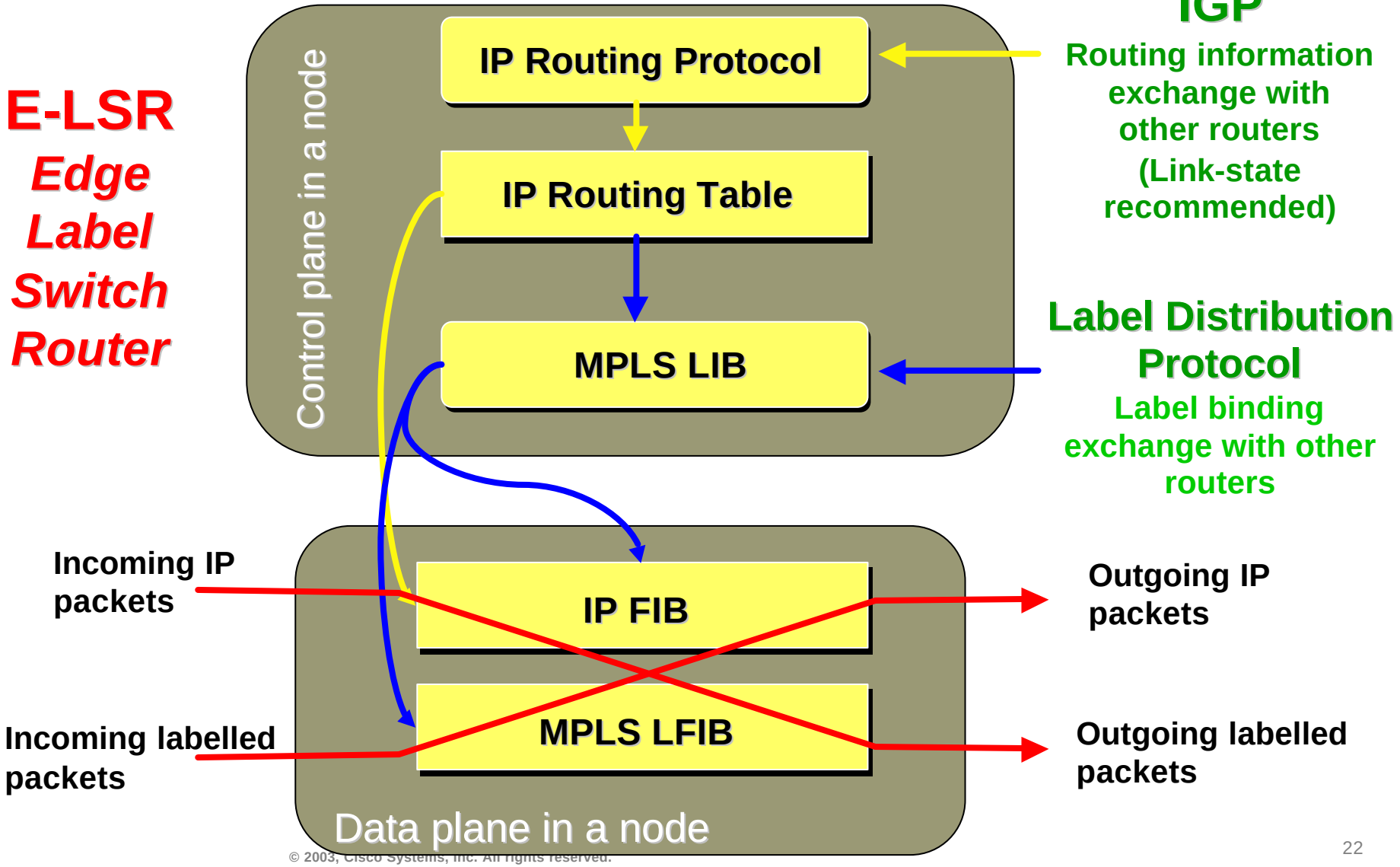
The forwarding information is taken from the FIB

Label mappings are distributed via **Label Distribution Protocol**

Control-Plane to Data-Plane
Classical Router

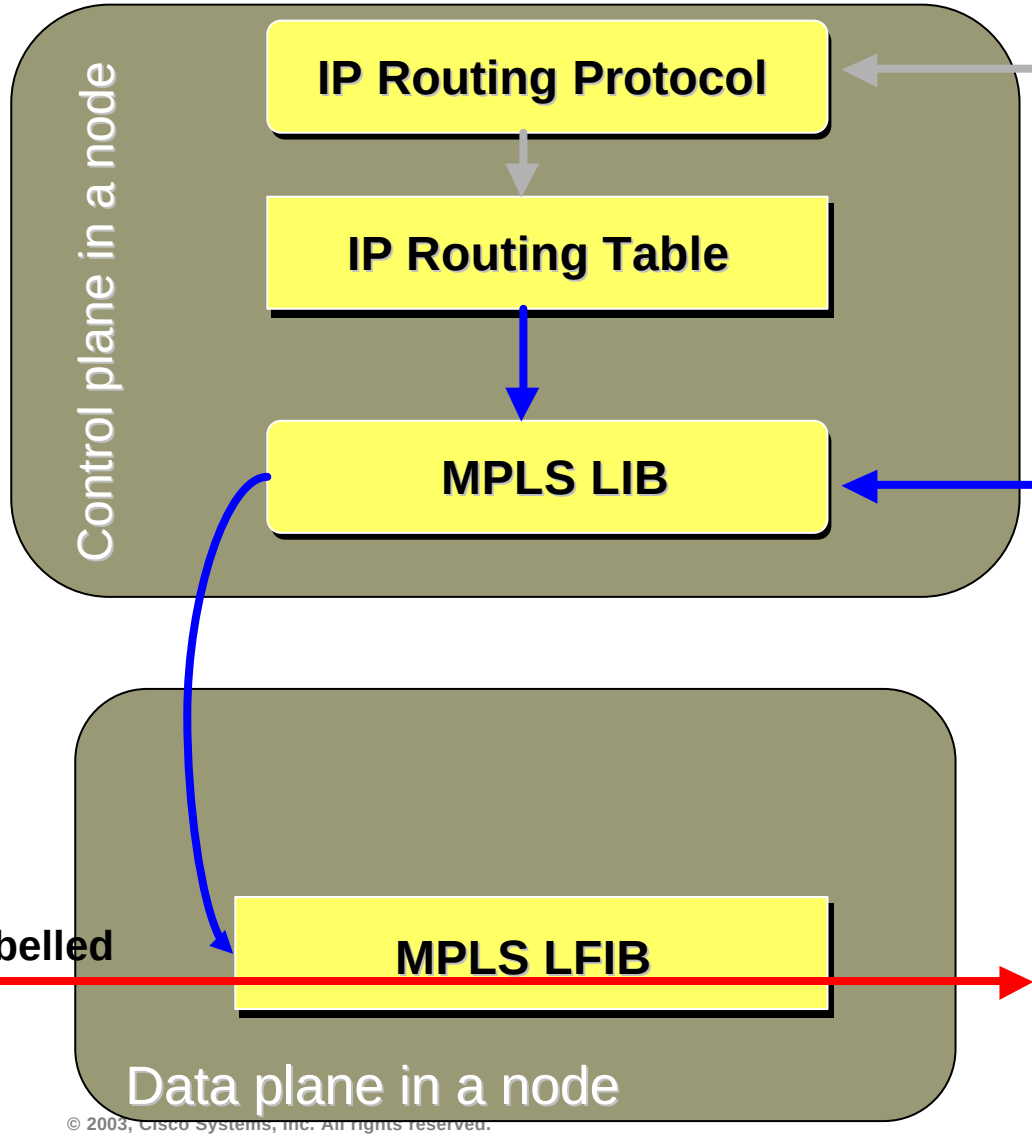


Control-Plane to Data-Plane
MPLS Edge-LSR



Control-Plane to Data-Plane
MPLS LSR

LSR
Label Switch Router



IGP
Routing information exchange with other routers
(Link-state recommended)

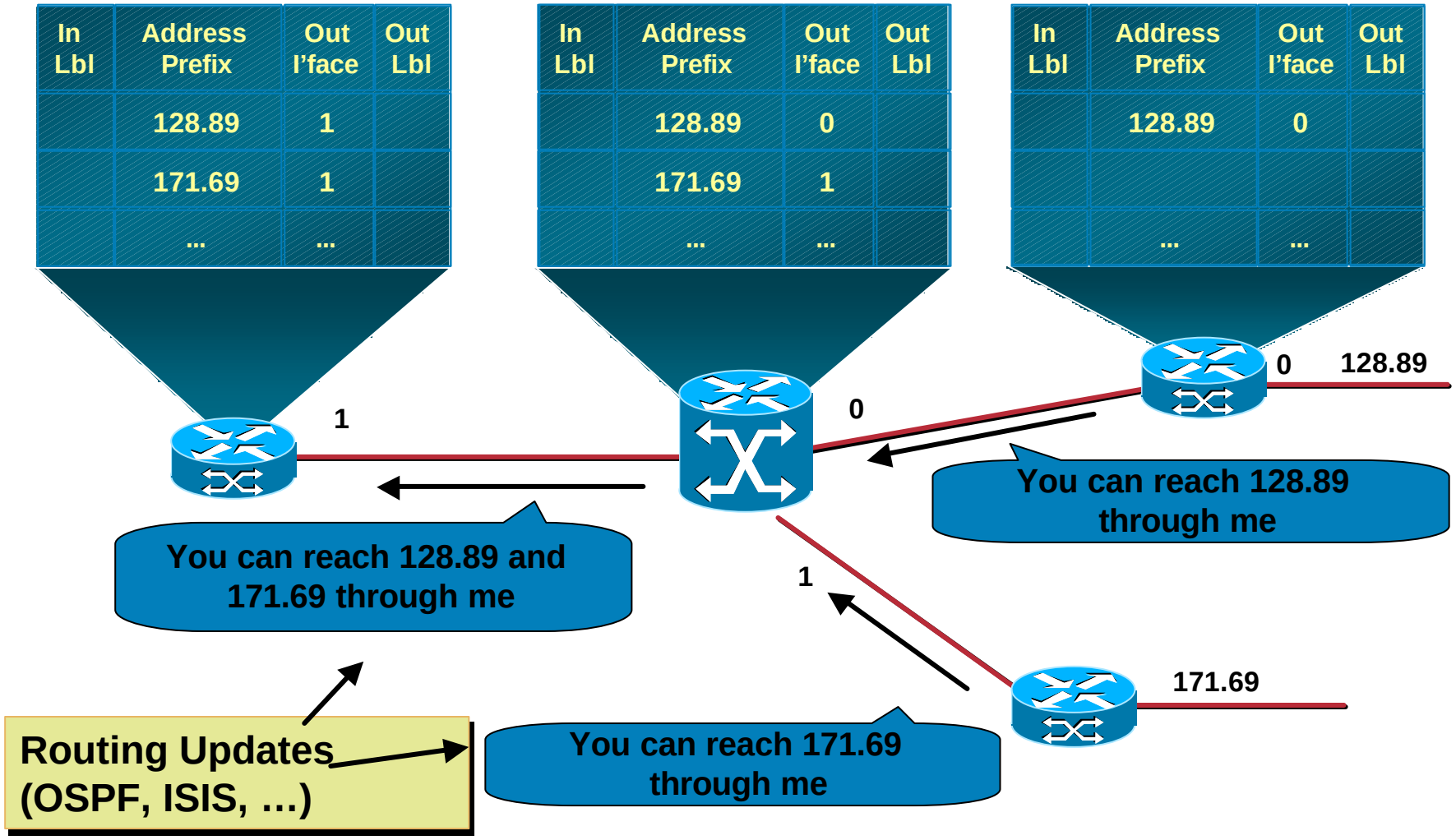
Label Distribution Protocol
Label binding exchange with other routers

Incoming labelled packets

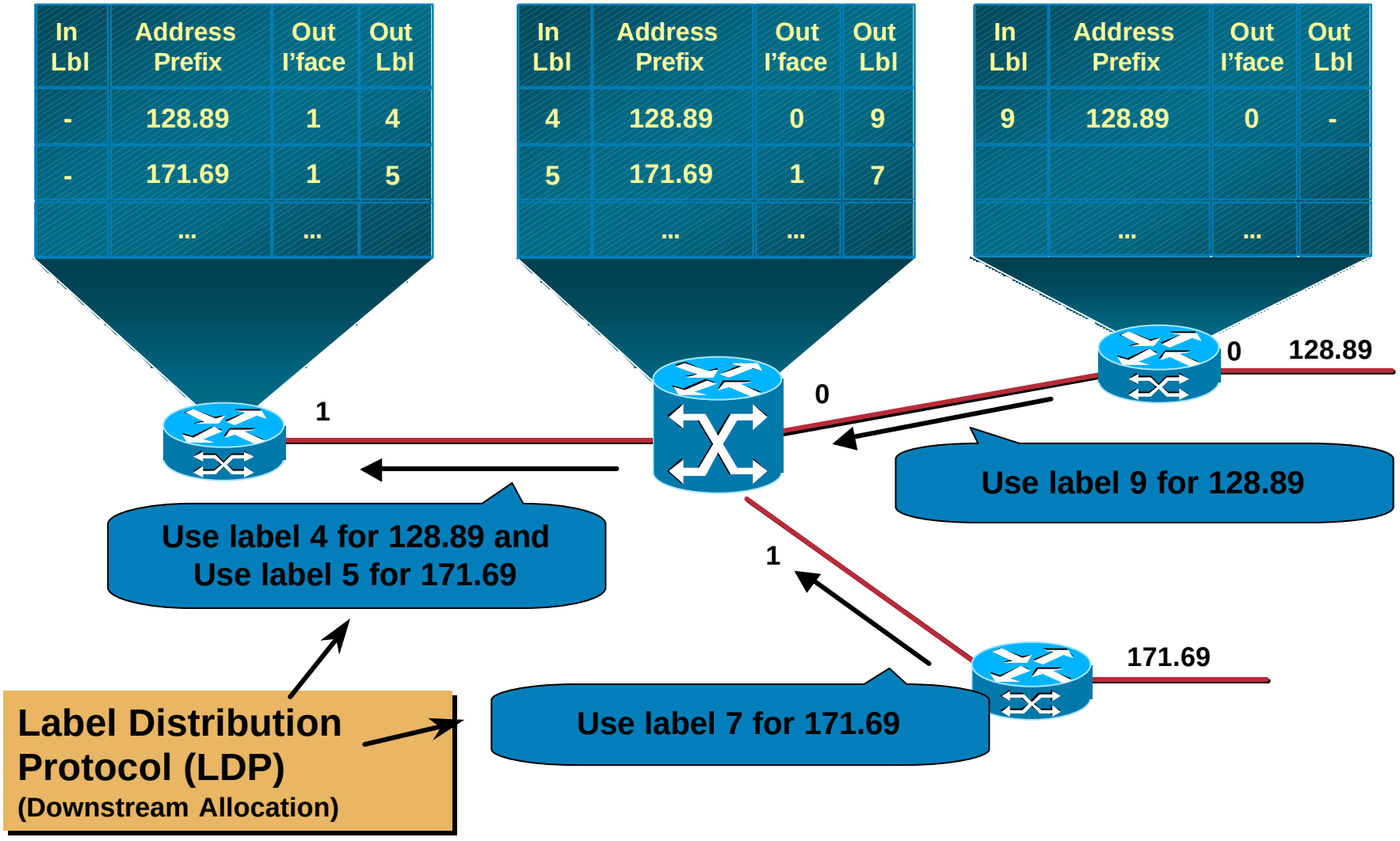
Outgoing labelled packets

Sample : MPLS

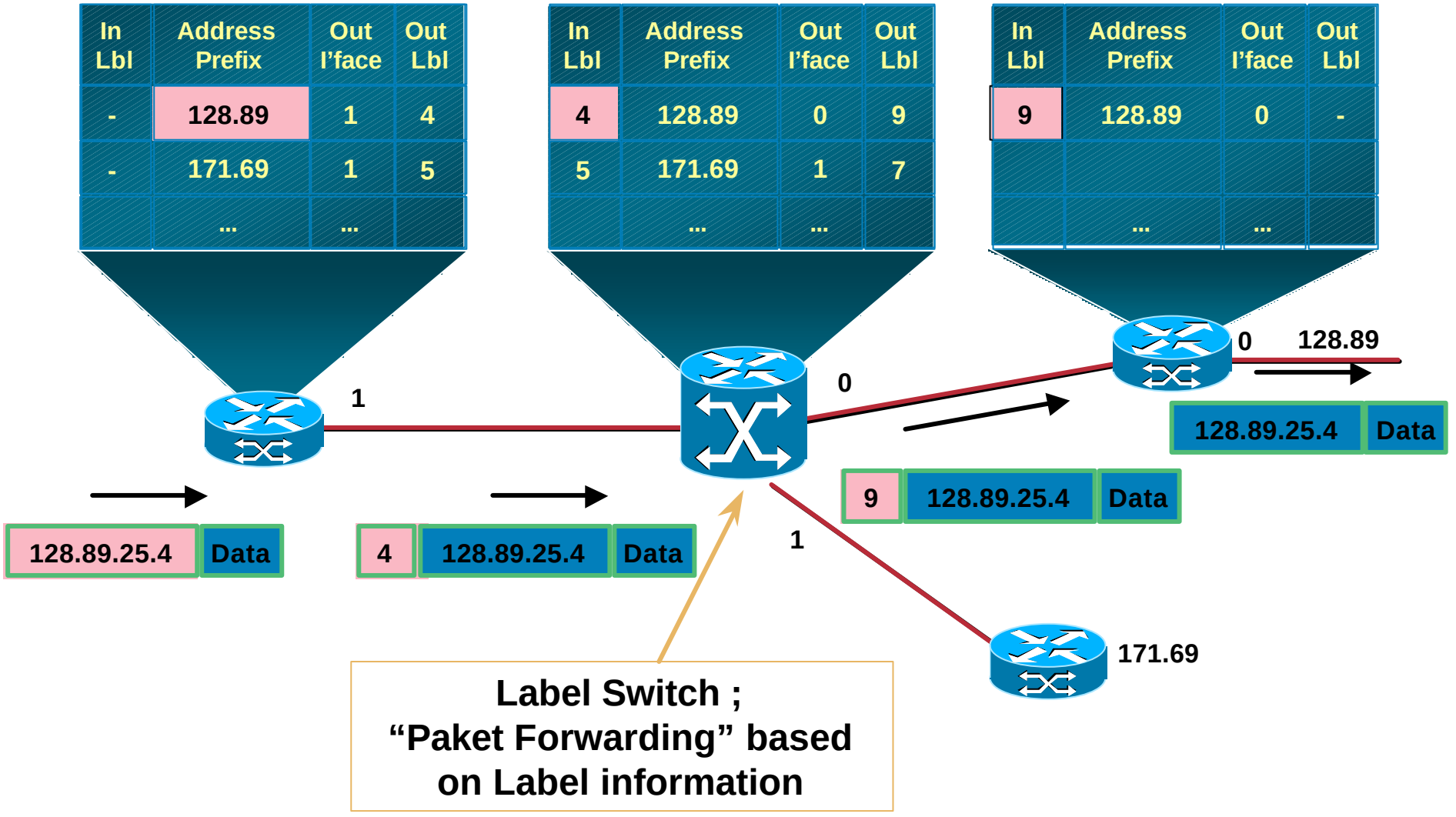
Routing Information, NLRI



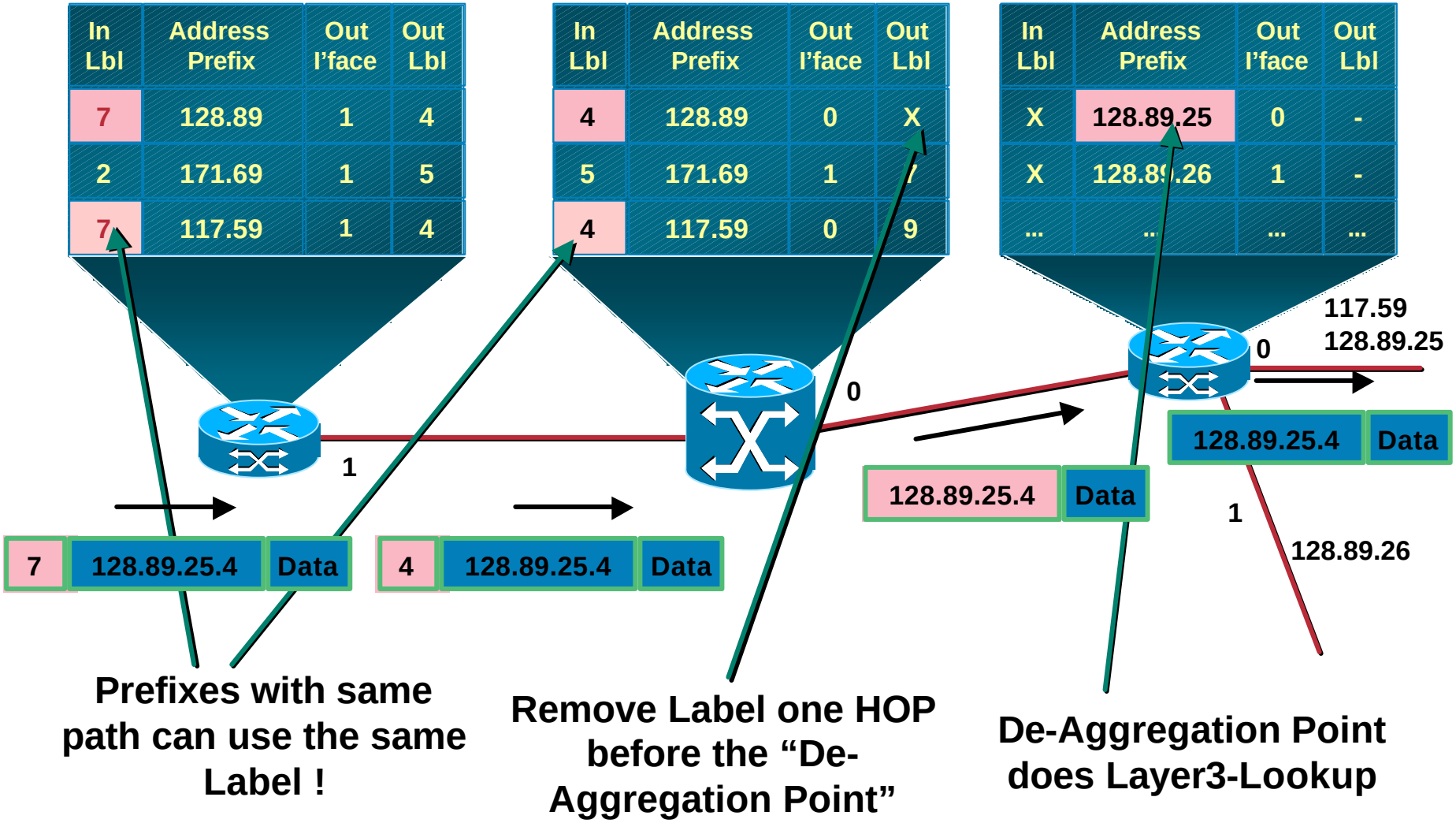
Sample : MPLS
Assigning the Labels



Sample : MPLS
Packet Forwarding



Sample : MPLS
…more Details



Enabling LDP / MPLS


```
PE1
mpls label protocol ldp
mpls ldp loop-detection
tag-switching tdp router-id Loopback0
!
interface POS4/0  --> to P2 POS4/0
 ip address 192.168.0.118 255.255.255.252
 mpls label protocol ldp
 tag-switching ip
 crc 32
 clock source internal
```

```
P2
mpls label protocol ldp
mpls ldp loop-detection
tag-switching tdp router-id Loopback0
!
interface POS4/0  --> to PE1 POS4/0
 ip address 192.168.0.117 255.255.255.252
 mpls label protocol ldp
 tag-switching ip
 crc 32
 clock source internal
```

“LDP port UDP (646)” “dst=224.0.0.2(646)”

LDP between two directly connected LSRs

- UDP broadcast HELLOs to 224.0.0.2
- most common use of LDP

Verify LDP Operation


```
p2#sho mpls interfaces
Interface              IP         Tunnel   Operational
POS4/0                 Yes (ldp)  Yes      Yes

gsr6-p2#sho mpls ldp discovery
 Local LDP Identifier:
    192.168.0.2:0
    Discovery Sources:
    Interfaces:
        POS2/0 (ldp): xmit/recv
            LDP Id: 192.168.0.3:0
        POS3/0 (ldp): xmit/recv
            LDP Id: 192.168.0.5:0
        POS4/0 (ldp): xmit/recv
```

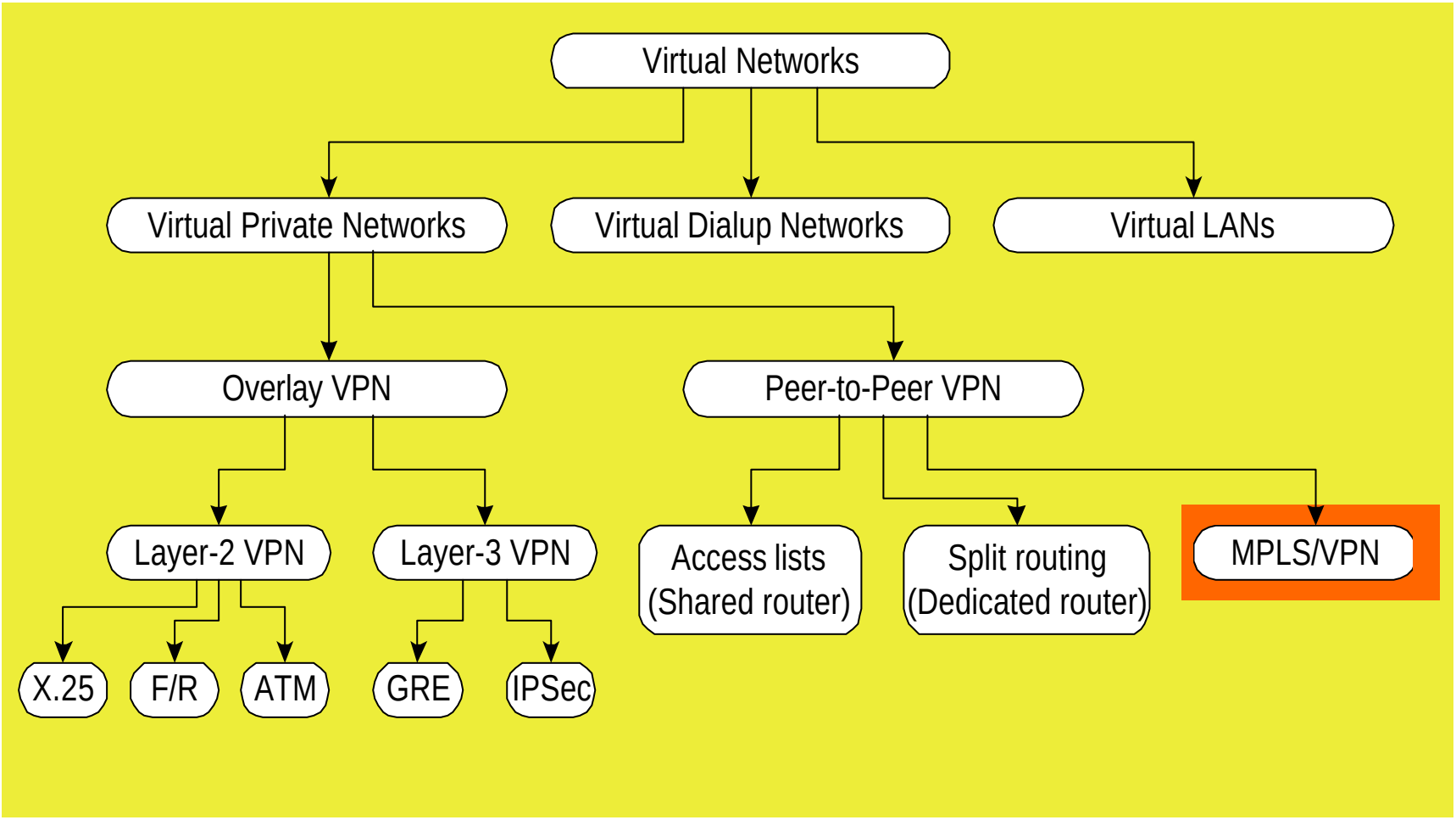
gsr6-p2#sho mpls forwarding-table | include PO4/0

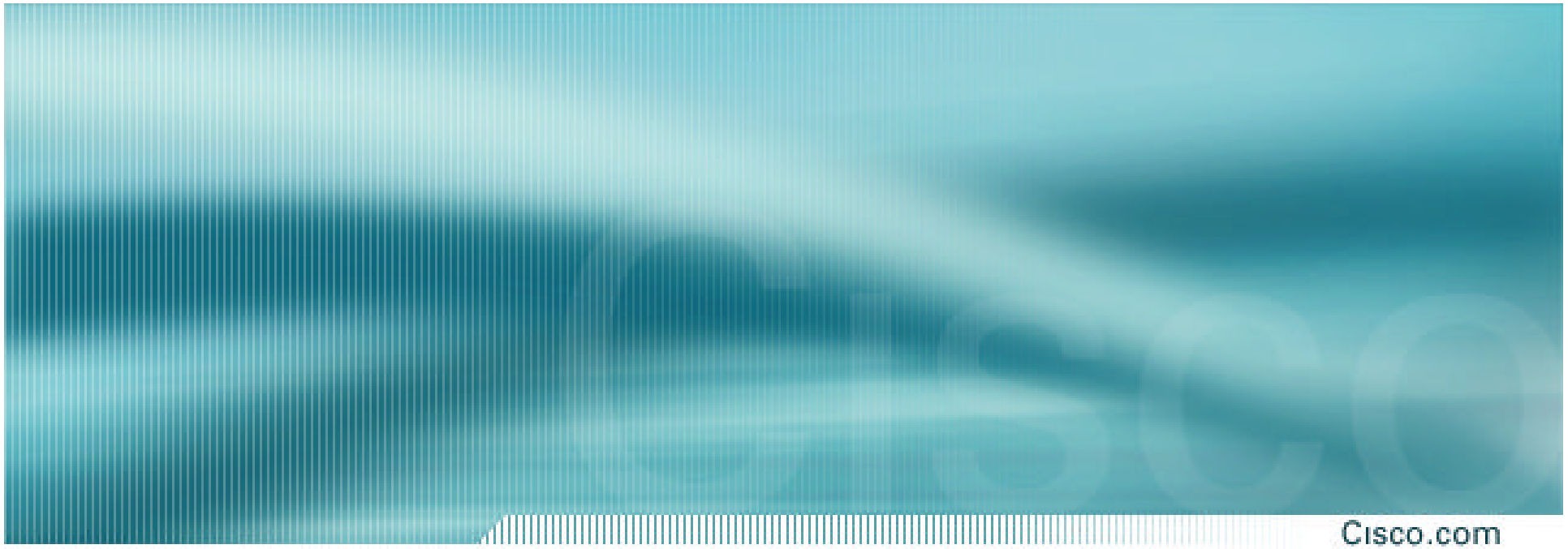
12304	**Pop tag**	192.168.0.4/32	0	PO4/0	point2point
12305	Pop tag	192.168.0.200/30	0	PO4/0	point2point
12306	Pop tag	192.168.0.192/30	0	PO4/0	point2point
12307	Pop tag	192.168.0.188/30	0	PO4/0	point2point
12308	Pop tag	192.168.0.176/29	0	PO4/0	point2point
12309	12349	172.21.56.62/32	504	PO4/0	point2point
12310	12334	192.168.4.12/30	0	PO4/0	point2point
12311	12335	192.168.4.16/30	0	PO4/0	point2point
12312	12336	192.168.6.12/30	0	PO4/0	point2point
12313	12337	192.168.6.16/30	0	PO4/0	point2point
12314	12338	192.168.0.8/32	0	PO4/0	point2point
12318	12339	192.168.0.196/30	0	PO4/0	point2point
12322	12340	192.168.4.8/30	0	PO4/0	point2point
12336	12352	192.168.0.21/32	2069	PO4/0	point2point

Agenda

- Gründe für MPLS VPN´s
- Einführung in MPLS
- MPLS/VPNs
- Supported Cisco HW

Virtual Networks - Overview -

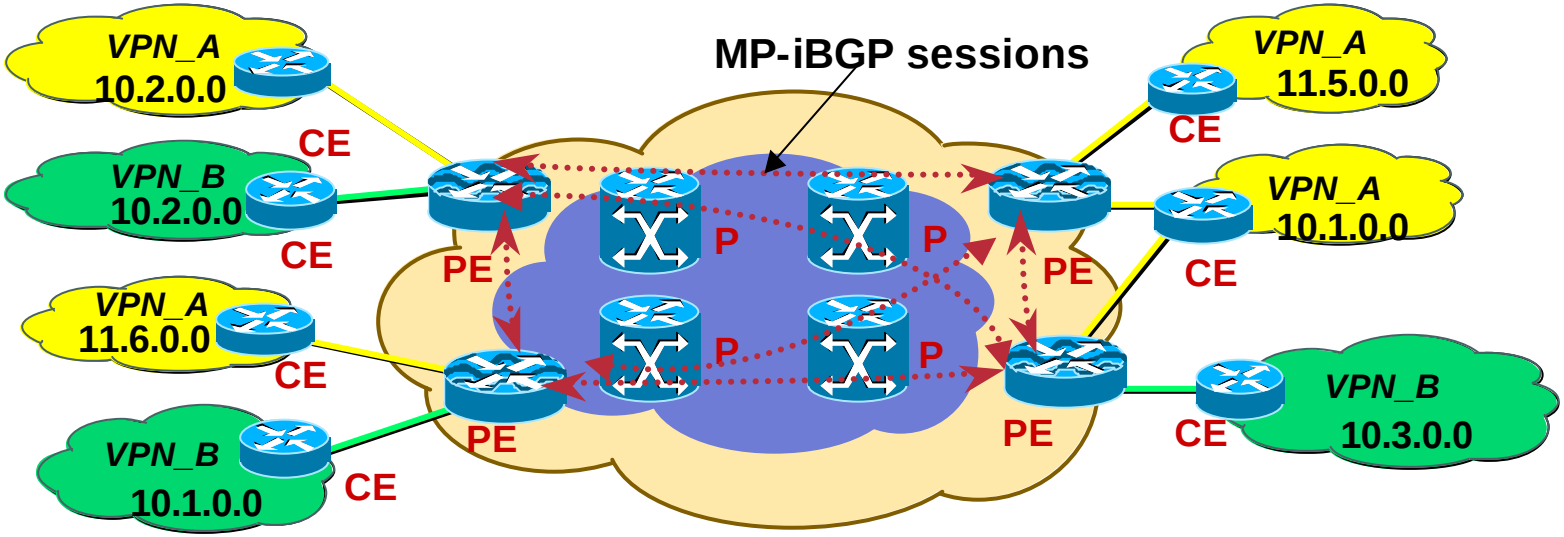




Concepts of MPLS/VPNs

MPLS VPN Connection Model

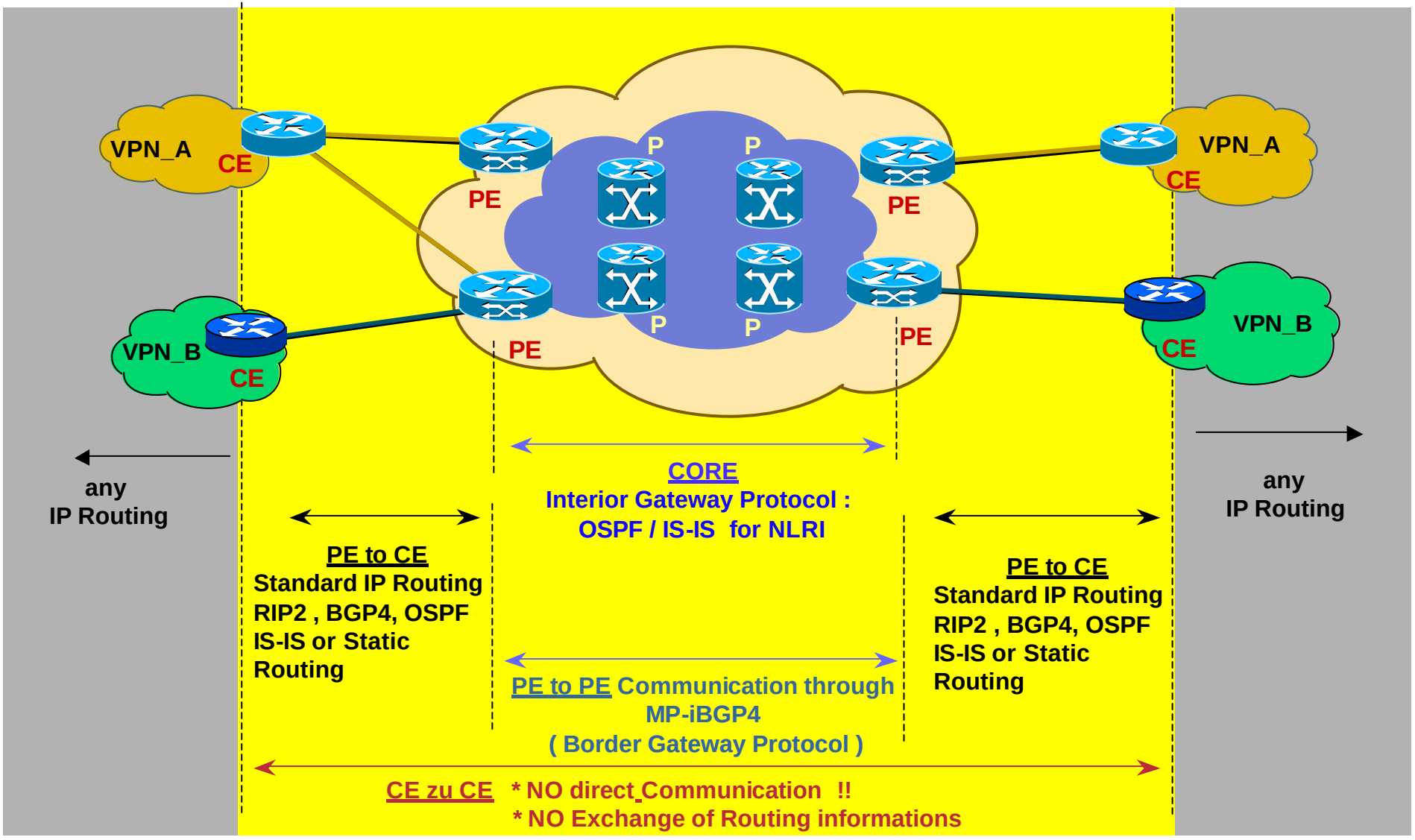
Overview



- **P (rovider) Router represent the core of the network – MPLS LSR**
- **P(rovider) E(dge) Router are using MPLS to talk with the Core and normal IPv4 to talk to the C(ustomer)E(dge) Router**
- **P und PE Routers utilize a common IGP (e.g. OSPF or ISIS)**
- **PE Routers are fully-meshed via MP-iBGP**

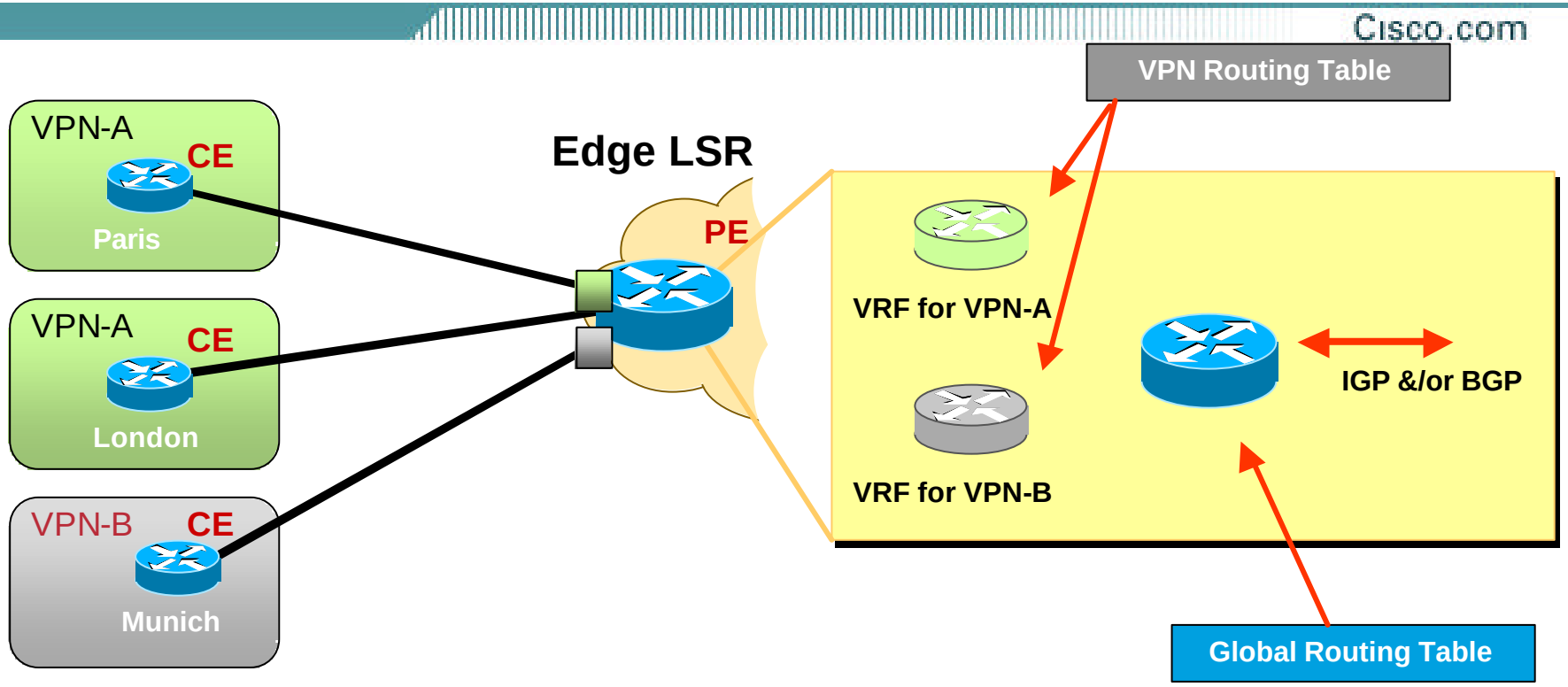
MPLS VPNs

The use of Routing Protocols



MPLS VPN Connection Model

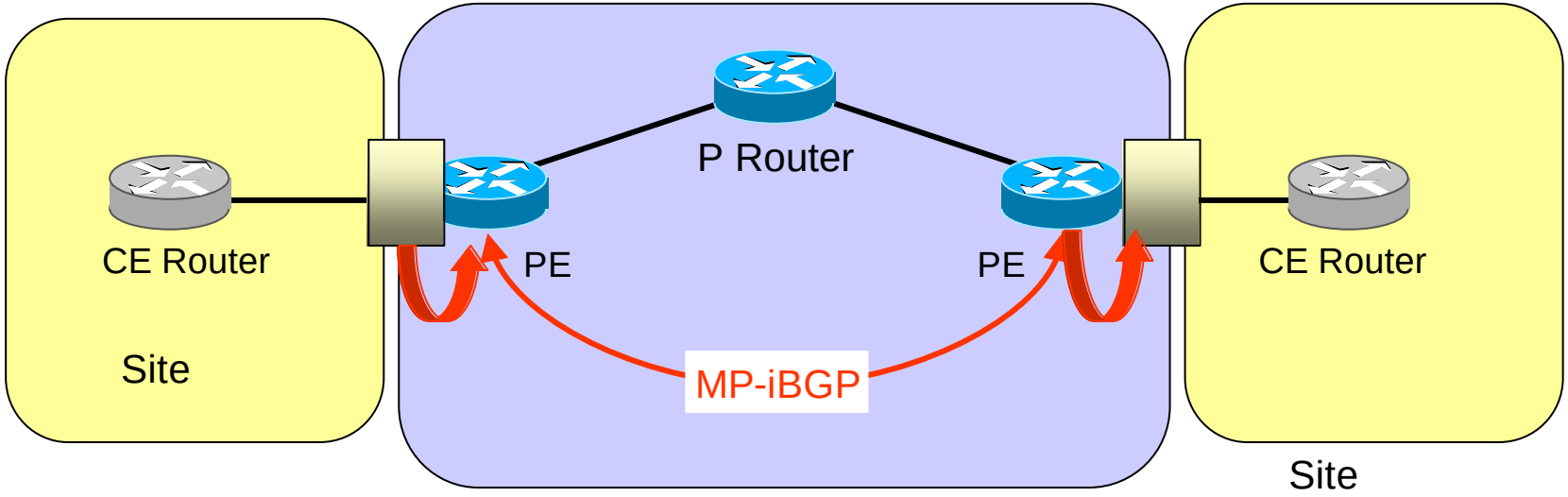
VRFs – VPN Routing Forwarding



- **Multiple Routing Tables (VRFs) on the PEs**
  - **Each VRF contains customer routes**
  - **Customer IP-addresses may overlap**
  - **Security**
- **MP-BGP for propagation between the PE Routers**

MPLS VPN Connection Model
VRF Route Distribution

- **PE Routers distribute local VPN informations across MPLS Backbone...**
  - through MP-iBGP & Redistribution of the VRFs
  - Receiving PE imports the routes to according VRFs



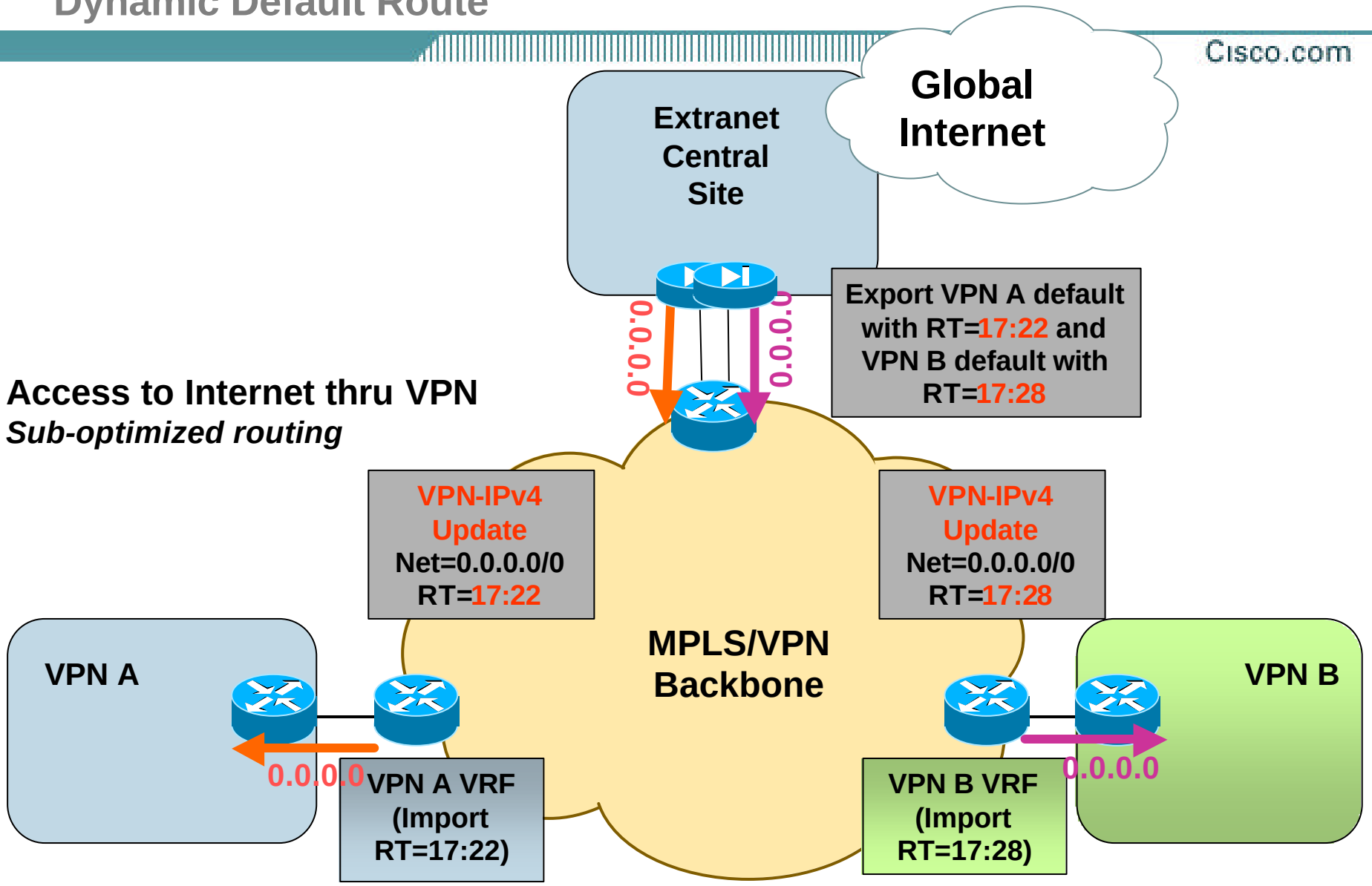
Differentiation through Route Distinguisher & Route Target

Internet Access

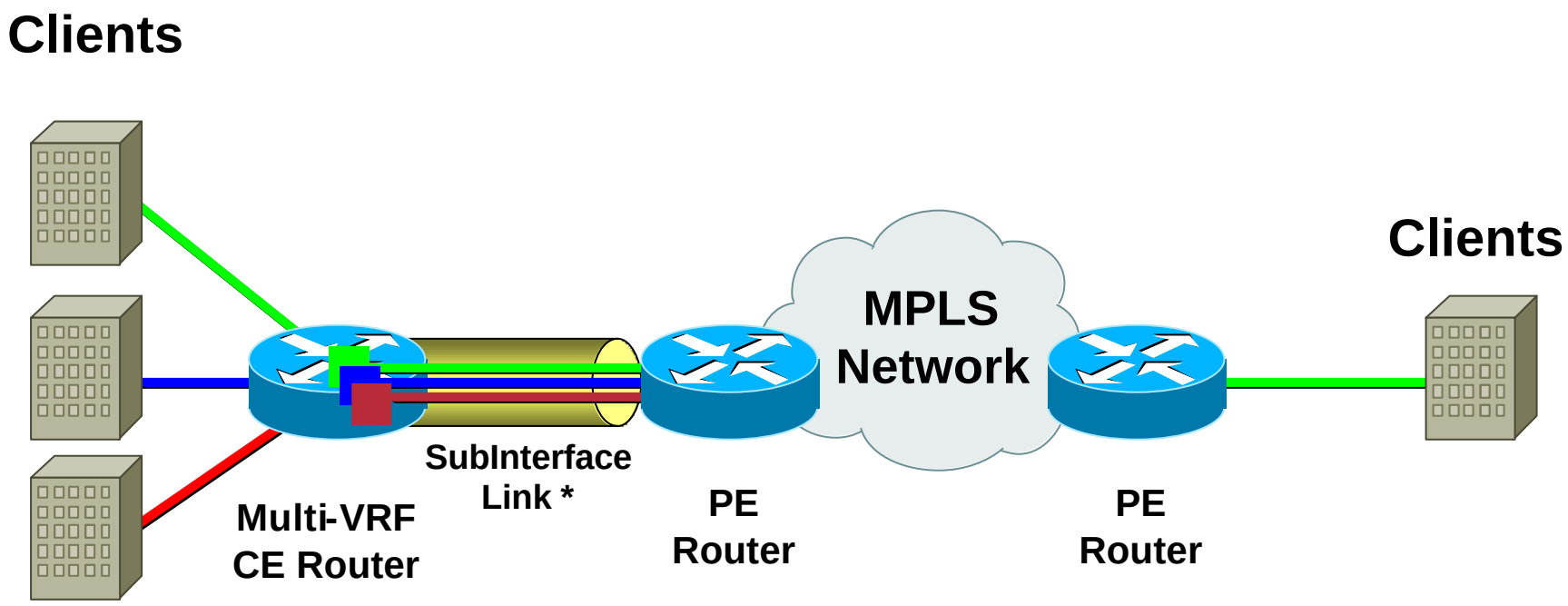
- **The problem:**
  - **The Internet table is too big to be populated in VRF**
    - **Example: 100 VRF * 110.000routes = 11.000.000 !!!**
    - **And even 110.000 VPNv4 @ is a lot…**
  - **Basic MPLS switching allows not to distribute Internet routes into the core**
    - **No label is given to external BGP routes**
    - **One label is given to Next-Hop**
  - **Some customer requires optimum access to Internet @**

MPLS/VPN Internet Connectivity

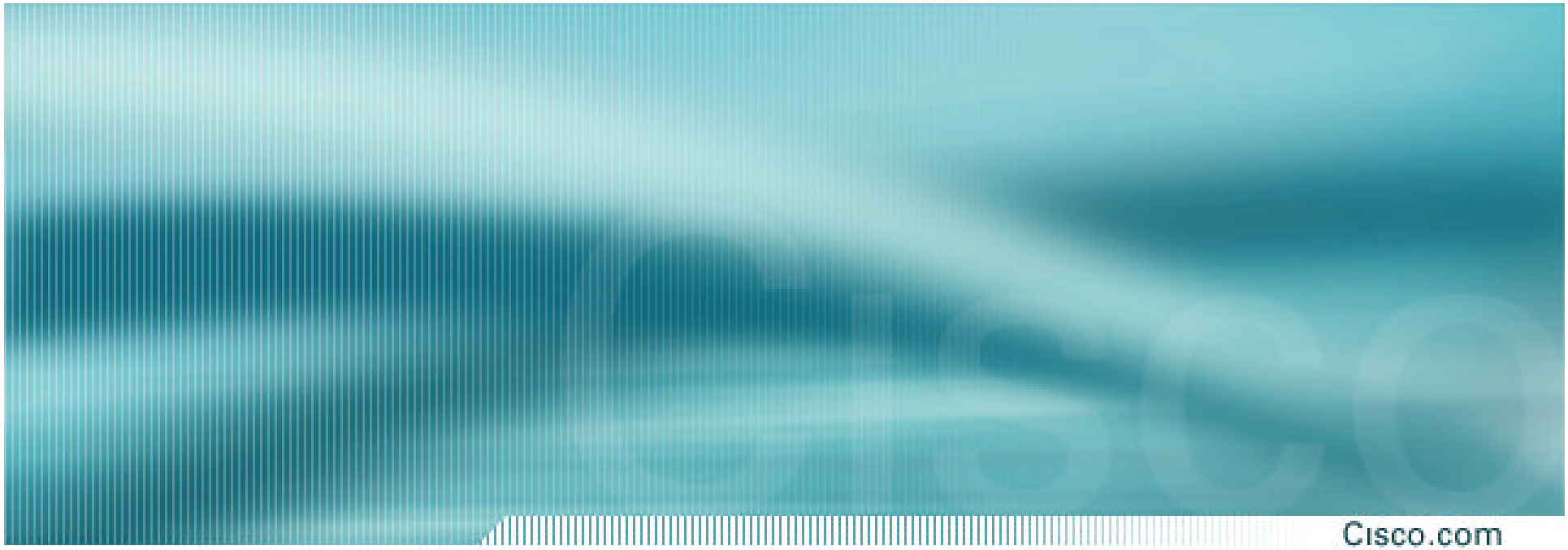
Dynamic Default Route



Multi-VRF CE - Extending MPLS-VPN



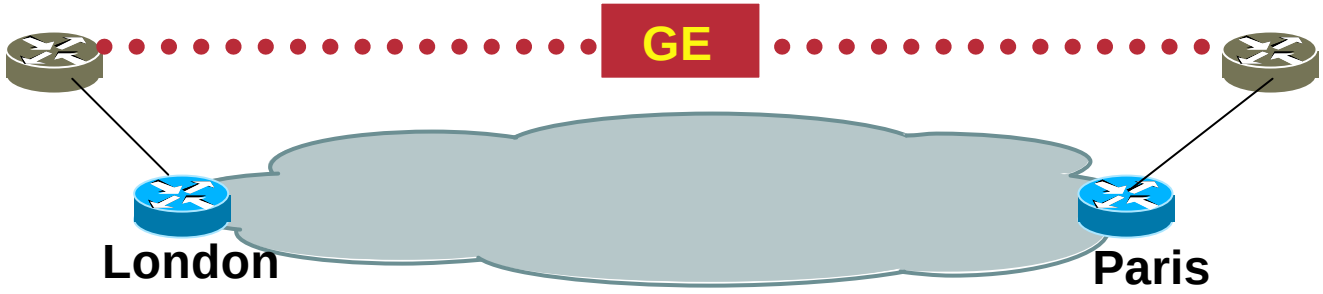
SubInterface Link – Any Interface type that supports Sub Interfaces, FE/GE-Vlan, Frame Relay, ATM VC's



Any Transport over MPLS (AToM)

…some sample applications

Layer Two Transport



- **Connect a GE in London with a GE in Paris over an IP/MPLS could**

  Same with FR, ATM, PoS, HDLC, PPP, TDM…

What is „Draft-martini“...?

- **draft-martini-l2circuit-encap-mpls-04.txt**

  “Encapsulation Methods for Transport of Layer 2 Frames over IP and MPLS Networks”

  Generic (IP/MPLS) Encapsulation scheme for

  FR, AAL5, cell, 801.q-VLAN, Eth, PPP, HDLC

  MPLS-specific: specification of the VC label format

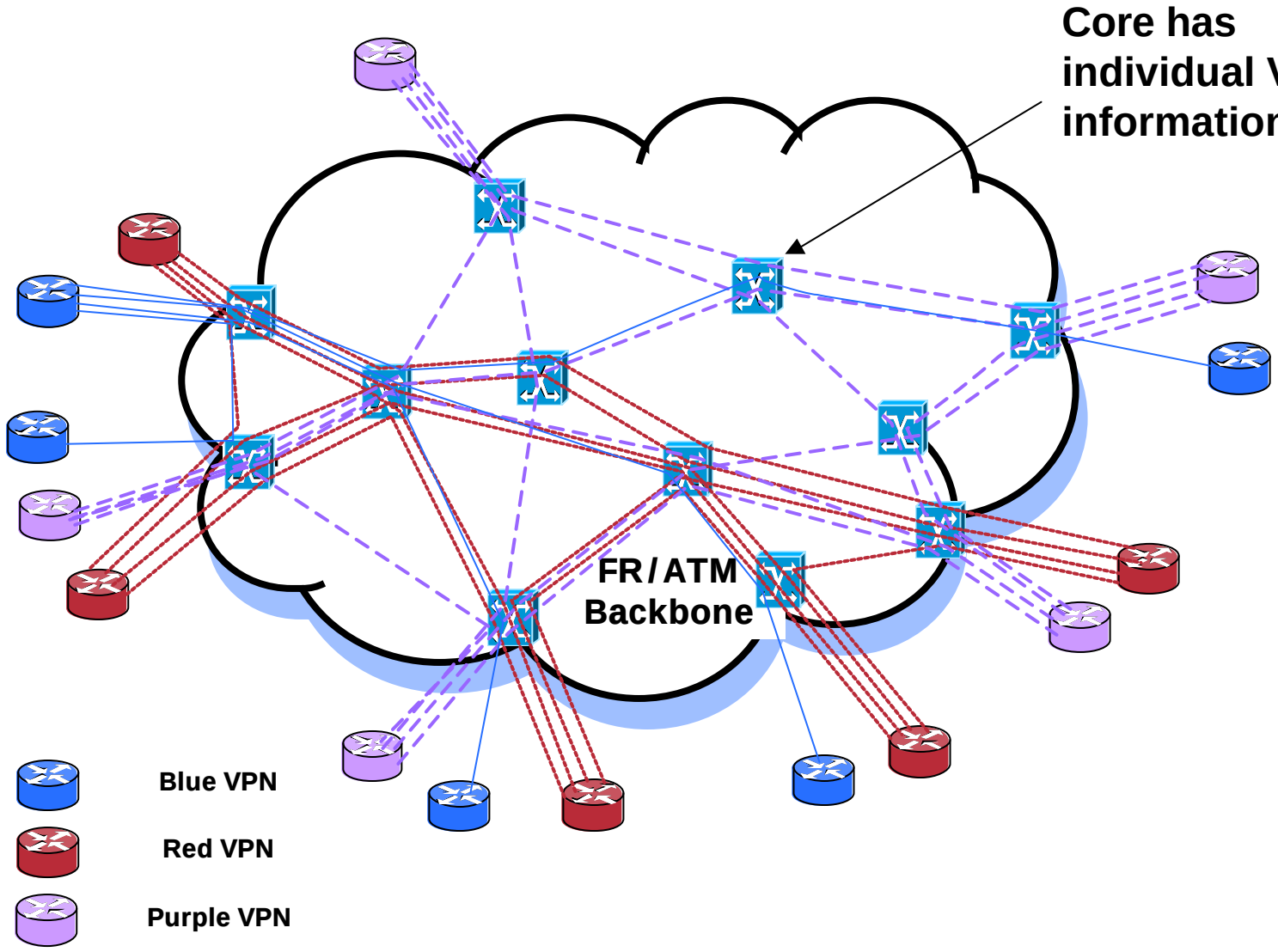
- **draft-martini-l2circuit-trans-mpls-10.txt**

  “Transport of Layer 2 Frames Over MPLS”

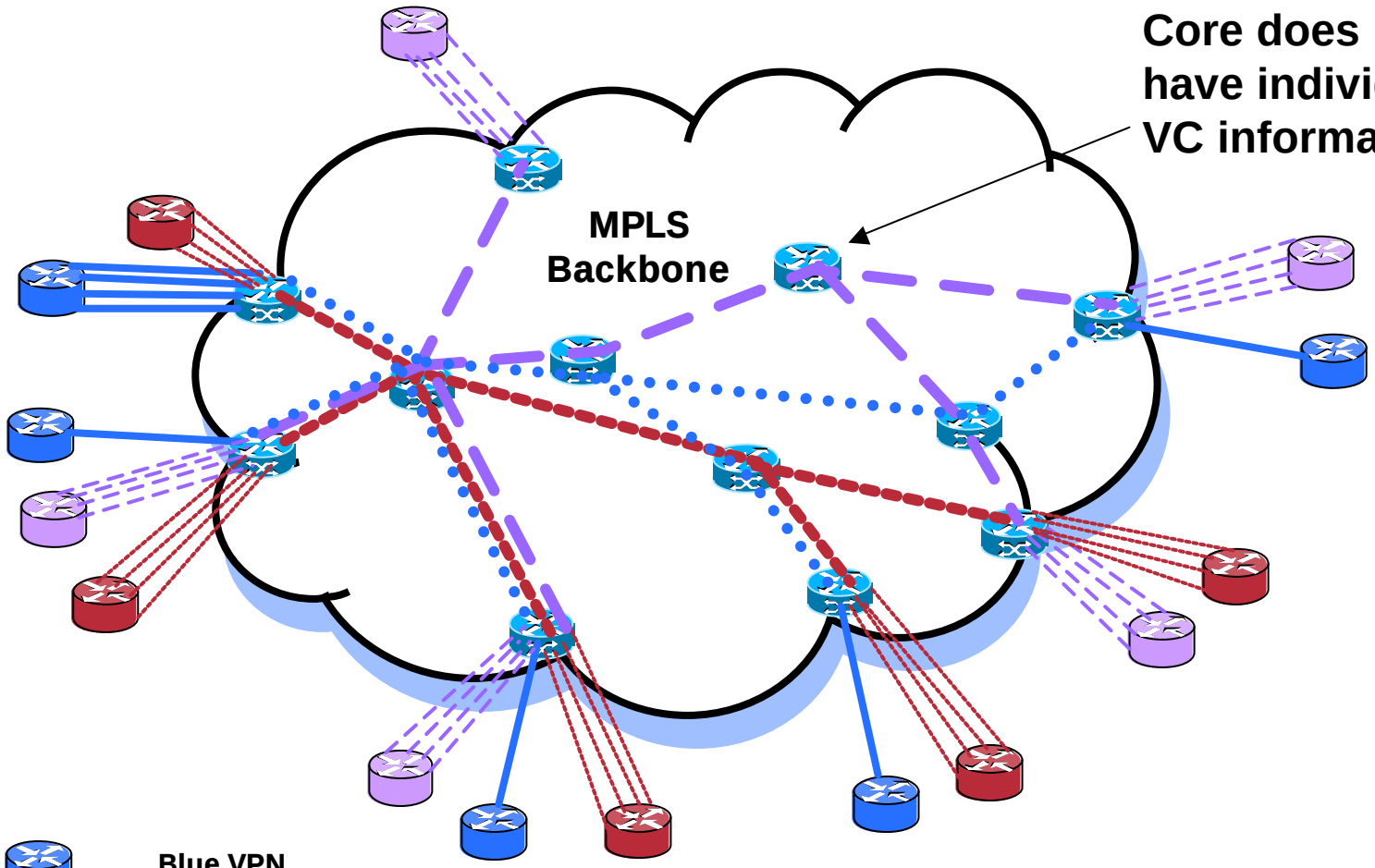
  Payload Encapsulation: refers to the previous draft

  Control Plane: defines the LDP extension

Current Layer 2 VPNs – With FR & ATM

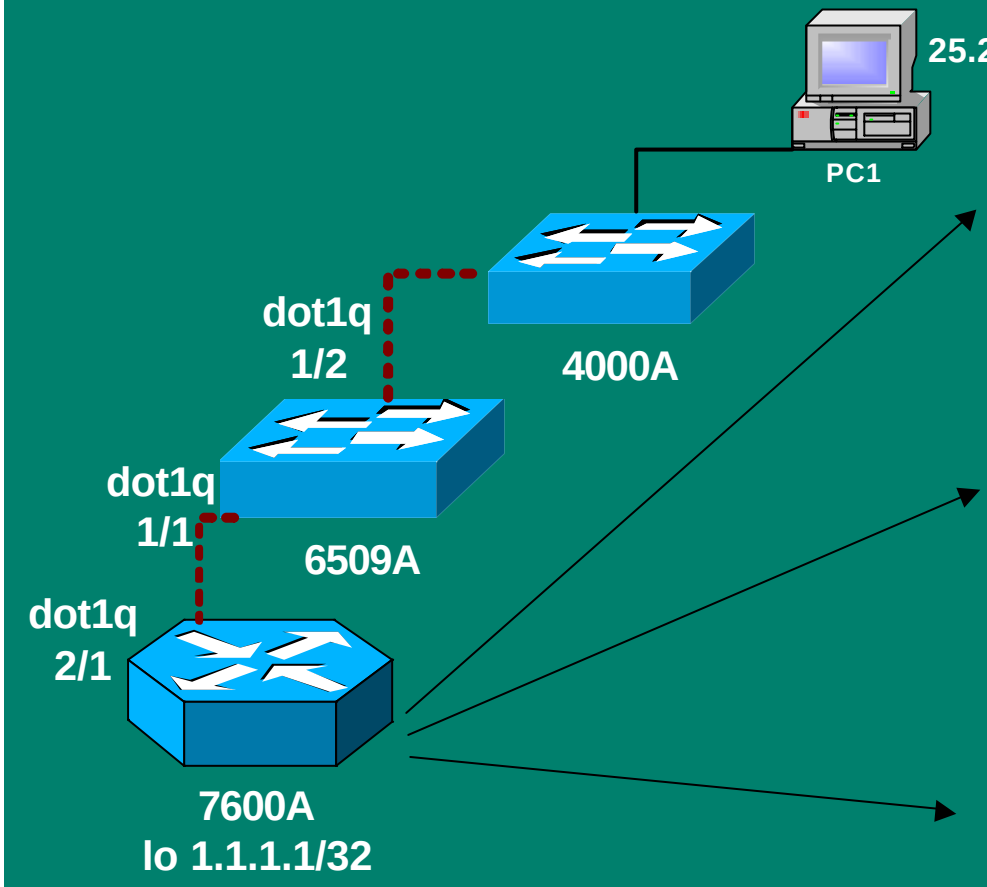


Any Transport over MPLS



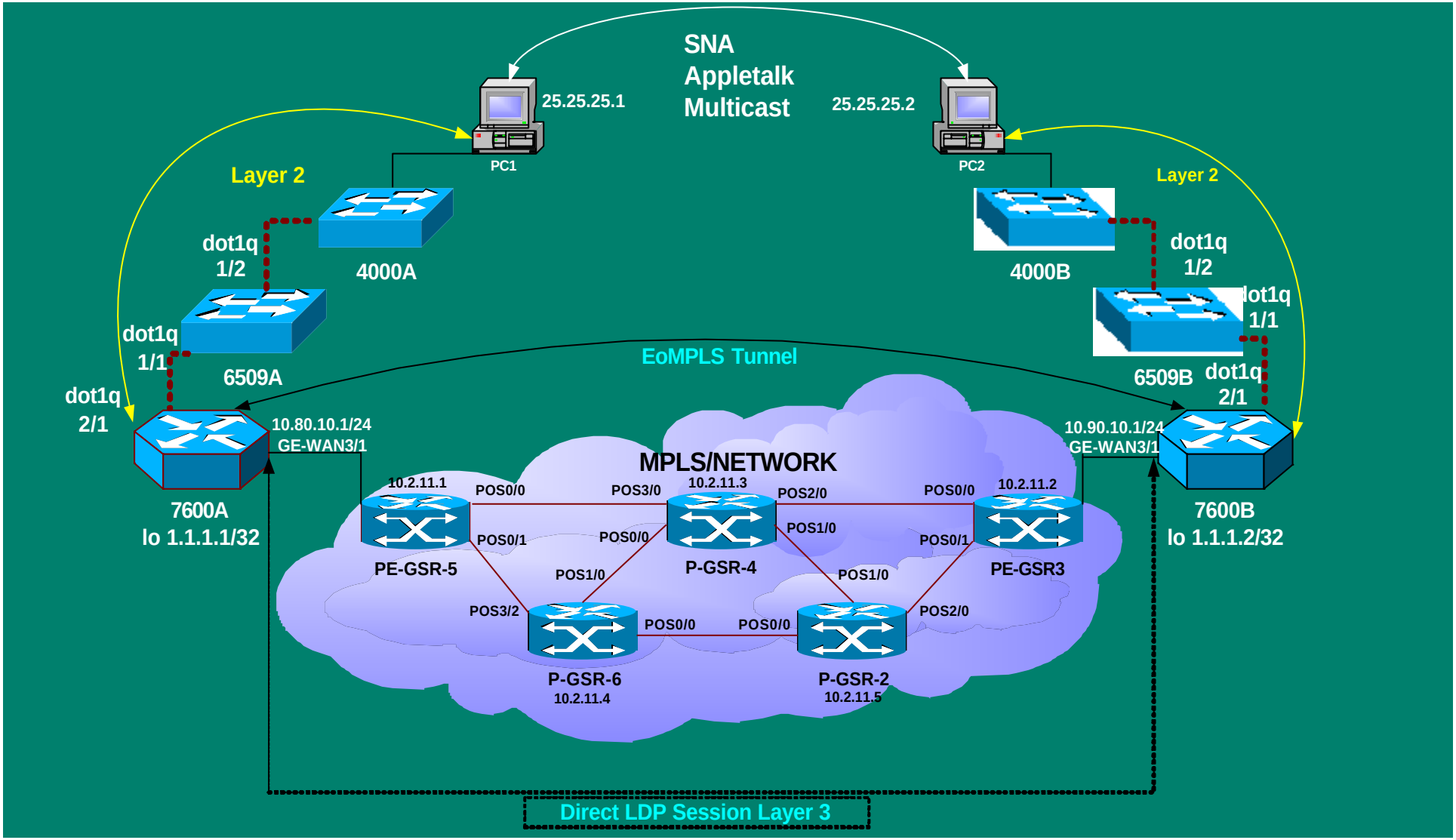
Idea is to do the same as ATM & FR
Transport layer 2 frames in MPLS packet
Create mapping of layer 2 circuits to LSPs
Scale better by using label stacking

IOS EoMPLS Configuration for 7600A

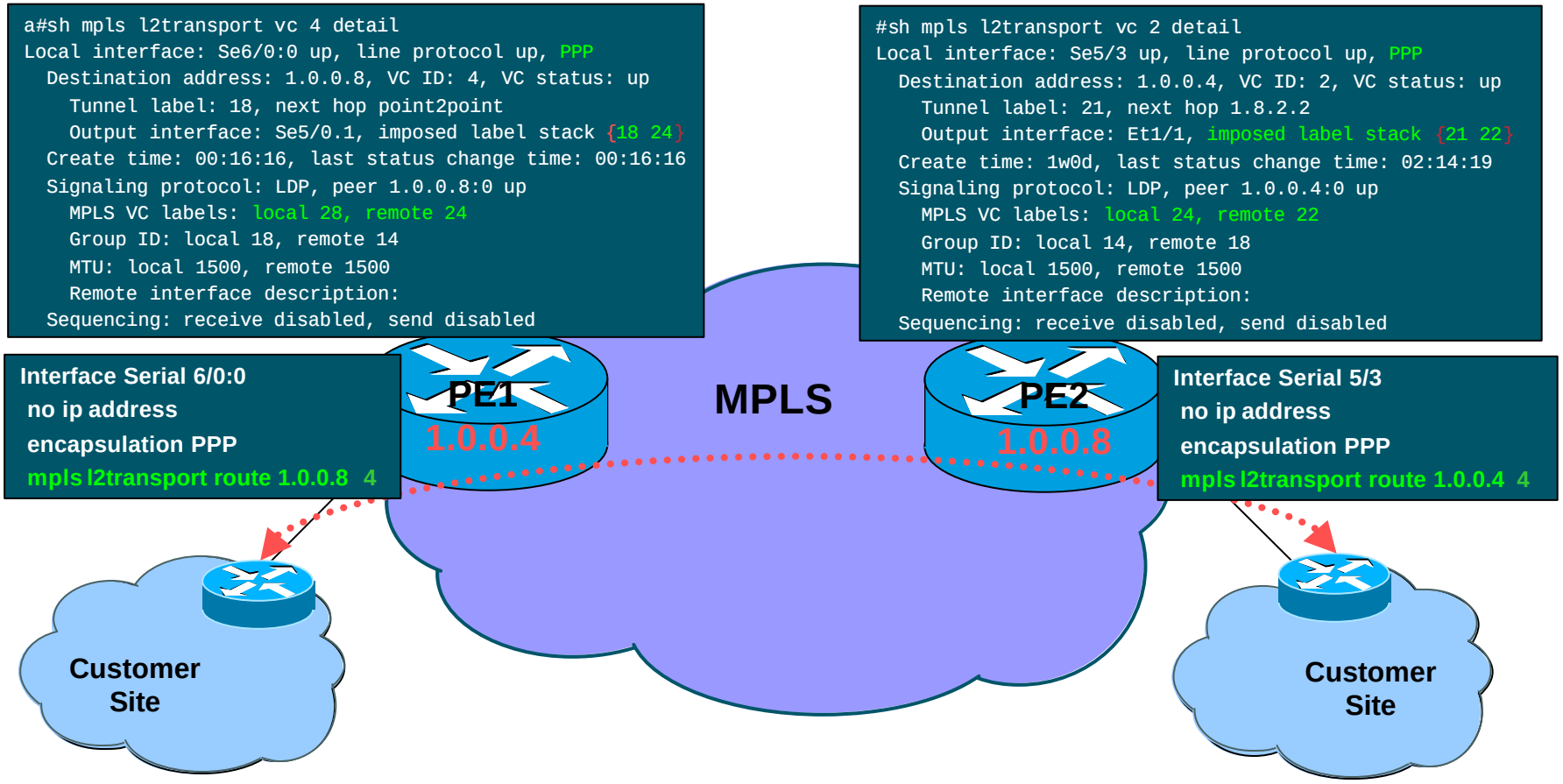



```
mpls label protocol ldp
mpls ldp loop-detection
tag-switching tdp router-id Loopback0
!
interface Loopback0
ip address 1.1.1.1 255.255.255.255
ip router isis EPGN
isis circuit-type level-2-only
!
interface GE-WAN3/1  OSM Module
ip address 10.90.10.1 255.255.255.0
ip router isis EPGN
mpls label protocol ldp
tag-switching mtu 1548
tag-switching ip
isis circuit-type level-2-only
!
interface Vlan1
mpls l2transport route 1.1.1.2 1 ← to 7600B
!
router isis EPGN
 net 49.0000.0000.0111.00
 is-type level-2-only
```

Basic EoMPLS Scenario



PPP over MPLS Example

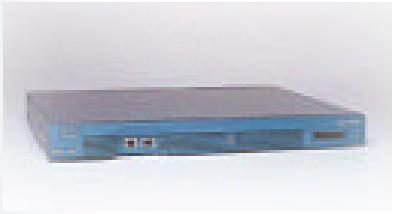


Agenda

- Gründe für MPLS VPN´s
- Einführung in MPLS
- MPLS/VPNs
- Supported Cisco HW

Routers supporting MPLS (partial list)

3600 Series Routers
3700 Series Routers
Cisco 6400 Series
Catalyst 6500
7200 Series Routers
7300 Series Routers
7400 Series Routers
7500 Series Routers
7600 Series Routers
10720 Series Routers
10000 Series Routers
12000 Series Routers



Cisco 3725 & 3745 Access Routers

- Highest Performance Branch Office Routers
- Integrated Advanced Services: Reduced TCO
- Cisco 3745: high availability, density and serviceability
- Cisco 3725: high density in a compact form factor

	3725	3745
10/100 FE ports	2	2
WIC Slots	3	3
AIM Slots	2	2
NM/HDSM Slots	2/1	4/2
HDSM Slots	1	2
Performance - kpps	100	225
Optional RPS	External	Internal
Optional Phone Power	Internal	Internal
Minimum Cisco IOS	12.2(8)T	12.2(8)T
Price	$8,500	$12,000

- Investment Protection: Shares 1700, 2600, 3600 interfaces
- Advanced QoS support
- Management: CiscoWorks2000 RME, CiscoView, SNMP

Cisco 7200 Overview

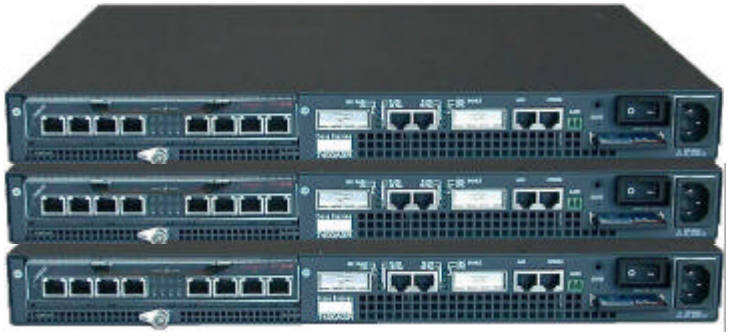
- **Compact Form Factor**
  - 3 RU size
  - 4 or 6 Port Adaptor (PA) slots
- **Diverse Set of Interfaces**
  - WAN interface range: DS0 to OC-3, and OC-12DPT
  - Up to 48 ports per chassis
  - Support for over 70 different LAN, WAN, VPN, and IBM PA's
- **Fully Modular**
  - Upgradeable network processors, including 225, 300, 400 Kpps, and 1 Mpps engines
- **Proven Architecture**
  - Over 250 thousand units shipped worldwide
- **Designed for Edge Applications:**
  - WAN Aggregation
  - Broadband Aggregation
  - Managed Services/CPE
  - VPN and Security

Cisco 7400 ASR - Übersicht

Stackable Form Factor

1 HE mit Front → Back Airflow

Niedriger Stromverbrauch – 50W



Nutzt Cisco 7200 Infrastructure

NEBS Level 3-compliant Chassis

NSE-1 Processor

7x00 Portadapter Interfaces

Application Specific IOS

350 Kpps CEF-based Internet Routing

Bis zu 512MB Memory für Internet Routing Tables

Service Provider WAN Edge IP Routing

High-performance IP Routing mit "Stackable" Bandwidth

High-touch IP Services

"Adaptive" Network Processing

Catalyst 3550 Series
Product Overview

- **Enterprise-class services**
  - High Availability: IP Routing, HSRP, STP enhancements, 802.1s/w, IGMP snooping
  - Enhanced Security: 802.1x, SSH*, SNMPv3*, ACL, Port Security, MAC address notification, RADIUS/TACAC+
  - Advanced QoS: L2-L4 QoS with CoS/DSCP, WRR, WRED, Strict Priority Queuing
- **High performance**
  - GE configurations provide dynamic IP routing at 17 Mpps forwarding rate
  - FE configurations provide wire-speed switching and routing
    - 10.1 Mpps forwarding rate on Catalyst 3550-48
    - 6.6 Mpps forwarding rate on Catalyst 3550-24
  - CEF based forwarding
- **Ease of management**
  - Extends Web-based Cluster Management Suite to Layer 3/4 services
- **Ease of deployment**
  - Boots as a traditional Layer 2 Catalyst switch, configurable for Layer 3 routing and services
  - 1 or 1.5 rack unit (RU) stackable form factor
- **Full Cisco GBIC support**
  - All existing GBICs (GigaStack™ GBIC, 1000BaseT, 1000Base-SX, LX, ZX)

* Available Q3CY02

Cisco 7600 / Catalyst 6500

- **Bis zu 30 Mpps Routing Performance**
- **Bis zu 256 Gbps Bandbreite**
- **Skalierbarster High-Speed Edge Router:**
  - **Interfaces von DS0 bis OC-48/STM-16**
  - **Ethernet von 10Mbps bis 10Gbps**
  - **Höchste Portdichte für T3/E3, OC-3/STM-1 und OC-12/STM-4**
  - **Bis zu 6 Mpps per linecard IP services application für Security, QoS, MPLS und Layer 4-7 Content Recognition & Routing**
  - **Carrier-class element Management & Provisioning**
- **Designed for Edge IP Service application:**
  - **WAN Edge Aggregation**
  - **Metro Ethernet Aggregation**
  - **Internet Data Center**

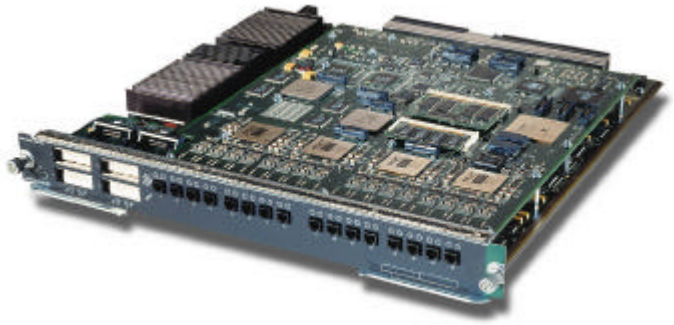
Cisco 7603

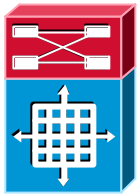
New!

Cisco 7606

Cisco 7609

Cisco 7600 - WAN Connectivity *(Packet over SONET/SDH)*





Powered by PXF

8 or 16-port OC-3c / STM-1 POS

Optic choices: MM, SM-IR or SM-LR

2 or 4-port OC-12c / STM-4 POS

Optic choices: MM, SM-IR or SM-LR

1-port OC-48c / STM-16 POS

Optic choices: SM-SR, SM-IR or SM-ELR

Common Features

Hardware:

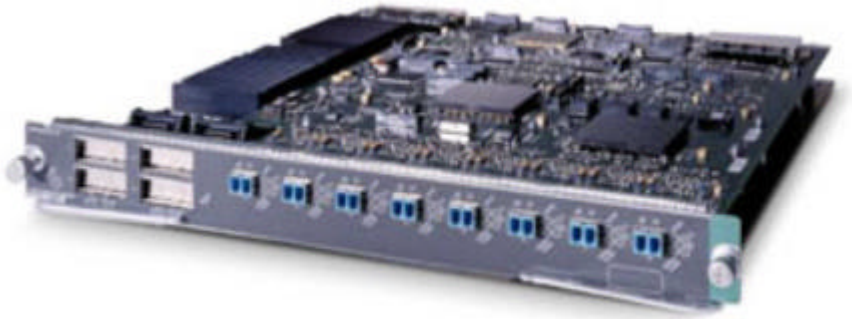
- **Includes 4 ports of switched GBIC-based GE**
- **Processor Memory: 64MB to 512MB**
- **Packet Buffer Memory: 64MB to 128MB**

Software:

- **1+1 SONET APS / SDH MSP**
- **PPP, HDLC**

Cisco 7600 - WAN Connectivity *(Channelized Optical Aggregation)*

Cisco.com



4 or 8-port CHOC-12/CHSTM-4 to T3/E3

Optic choices: SM-IR

1 or 2-port CHOC-48/CHSTM-16 to T3/E3

Optic choices: SM-SR

Common Features

Hardware:

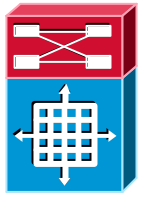
- **Includes 4 ports of switched GBIC-based GE**
- **Processor Memory: 64MB to 512MB**
- **Packet Buffer Memory: 128 MB**

Software:

- **1+1 SONET APS / SDH MSP**
- **PPP, HDLC**

Channelization Options:

- **OC-48 -> OC-12 -> OC-3 -> T3 -> Subrate T3**
- **STM-16 -> STM-4 -> STM-1 -> E3**



Powered by PXF

Don’t Try this at Home!