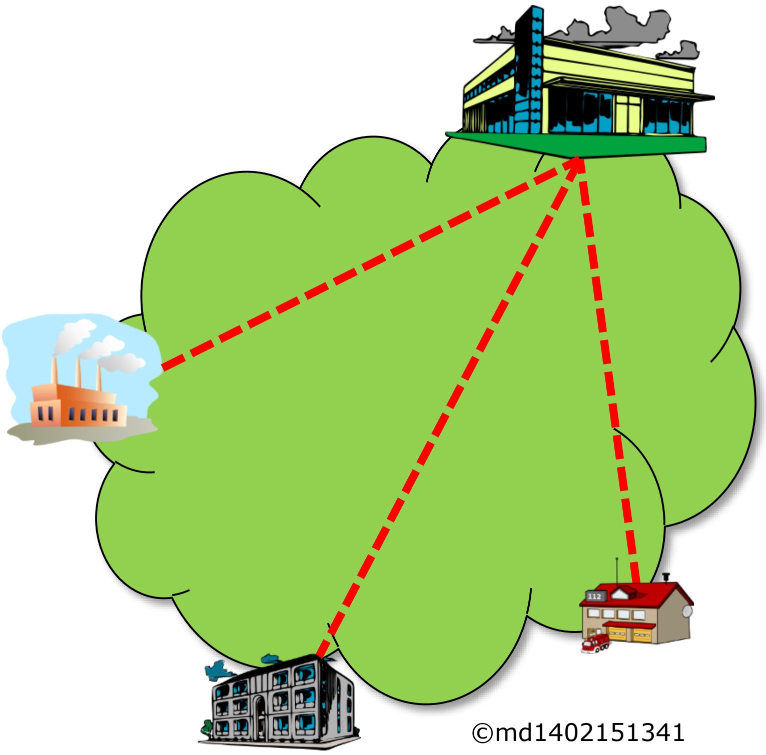
md brasil
TI & TELECOM



MPLS VPNs Security

Implementations with Mikrotik RouterOS

European MUM – 2014 - Venice / Italy

Wardner Maia

Copyright Notice
(Aviso sobre direitos autorais)

Introduction

Wardner Maia

Electronic and Telecommunications Engineer;
Internet Service Provider since 1995;
Radio Frequency Trainings since 2002;
Certified Mikrotik Trainer since 2007;
MD Brasil IT & Telecom CTO;
Member of the board of directors of LACNIC.

md brasil
TI & TELECOM

Introduction

MD Brasil IT & Telecom

Internet Access Provider in São Paulo state - Brazil;
Telecom equipment manufacturer and integrator;
Mikrotik Training Center since 2007;
Consulting services worldwide.

http://mdbrasil.com.br http://mikrotikbrasil.com.br

Previous Participations on European MUMs

Wireless Security (2008 – Krakow/PL)

Wireless Security for OLPC project (2009 – Prague/CZ)

Layer 2 Security (2010 – Wroclaw/PL)

Routing Security (2011 – Budapest/HU)

IPv6 Security (2012 - Warsaw/PL)

BGP Filtering (2013 – Zagreb/CR)

http://mikrotikbrasil.com.br/artigos

Motivations to talk about MPLS VPNs Security...

Motivation

MPLS

- Originally conceived to enhance network forwarding speed and for traffic engineering applications;
- MPLS enlarged its role becoming widely used as a solution for Layer 2 and Layer connectivity between sites.
- VPNs based on MPLS, are responsible for great part of big operators' revenue.
- Small and medium ISPs can be, at the same time, users and providers of such services

Motivation

MPLS Security

- Usually MPLS is considered as a trusted service provided by equally trusted operators.

- Configuration mistakes or malicious attacks can seriously compromise the availability of the services and also break the confidentiality and integrity of the virtual private networks.

Motivation

Purpose of the presentation

- To give an overview of the MPLS services and its implementations, the involved concepts, common topologies and its characteristics related to security.

- Tools and techniques to break into a MPLS VPN will be overviewed, as well as the countermeasures and best practices to make such services really secure.

Motivation

Target Audience:

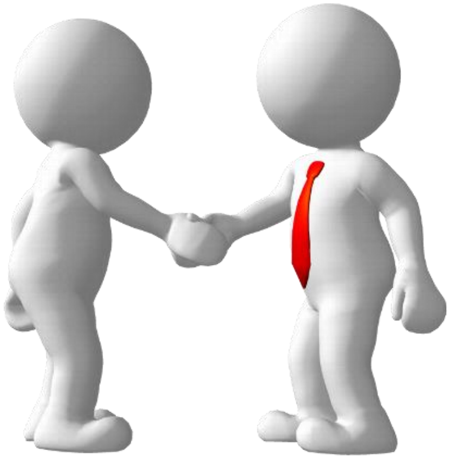
- ISPs and Telecom operators **providing** MPLS services

- ISPs and Telecom operators **using** MPLS services.

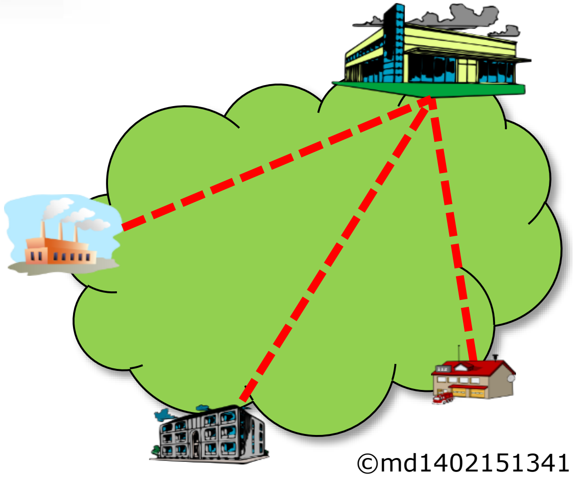
Types of VPNs
(security)

Secure VPNs

X



Trusted VPNs



©md1402151341

Types of VPNs (security)

Secure VPNs:

→ Authentication method

Parts are who they say they are;

→ Confidentiality

Data is not readable (understandable) by other parts;

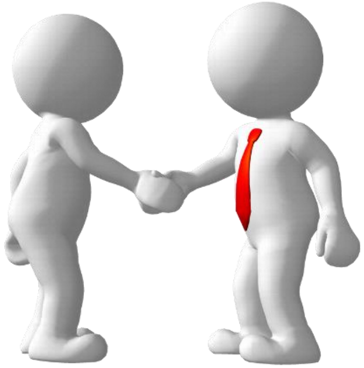
→ Integrity

Data cannot be modified in transit.

Confidentiality and Integrity should be ensured by an encryption method.

Examples: PPtP/L2TP with MPPE, L2TP with IPSec, etc.

Types of VPNs (security)



Trusted VPNs:

→ In fact no mandatory security feature

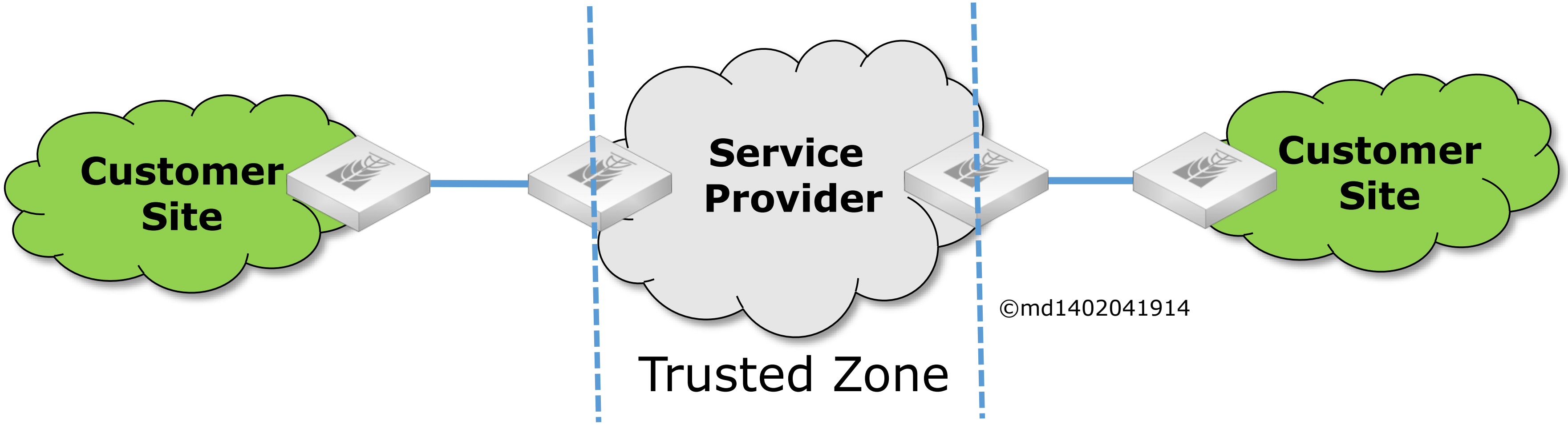
→ Customers **trust** that the data traffic is kept secure by the Service Provider inside its edges.

Examples: Frame Relay, ATM and **MPLS VPN’s**

Secure x Trusted VPNs

Trusted VPNs:

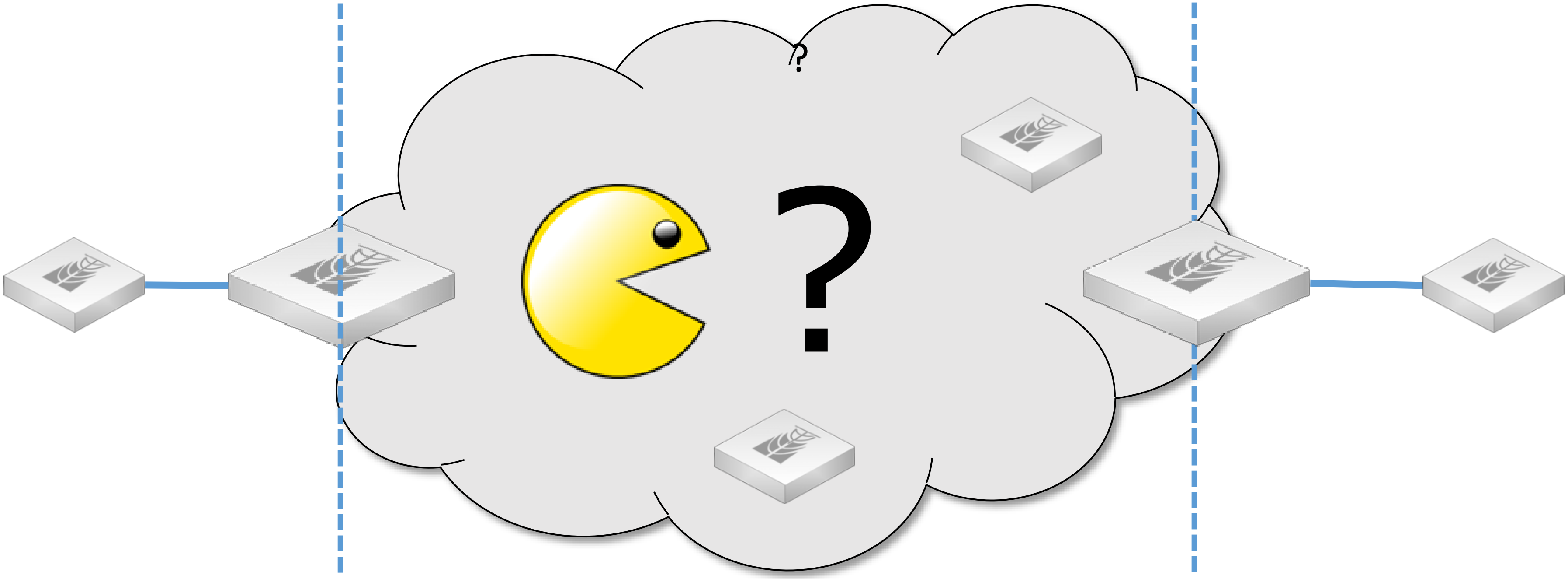
A “trusted zone” is assumed between Service Provider’s edges.



Examples: Frame Relay, ATM and MPLS VPN’s

Secure x Trusted

How (In)Secure could be your (Un)Trusted Zone when it comes to MPLS VPNs?



Trusted Zone

Customer’s and Provider’s thoughts

Thinking as a Customer:

If I bought an Internet Service, I have to mind my own security (Firewall, anti-virus, etc.)

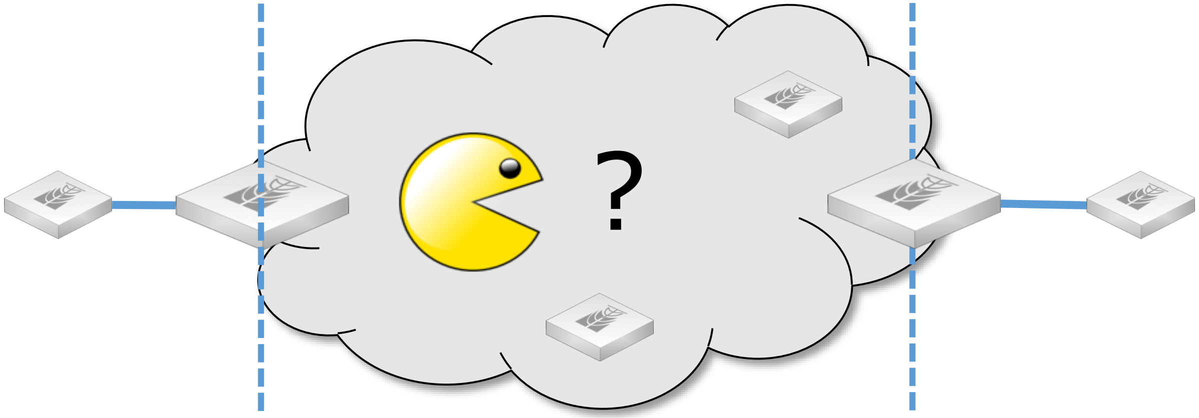
If I bought a VPN Service, my Service Provider has to provide me security. Few security measures are required.

Thinking as a Service Provider:

If I provide Internet Service, Customers Know that they should take appropriate measures to protect themselves.

If I provide A VPN Service, it’s supposed that Customers trust me. What should I do to deserve that confidence?

What Users and Providers should know about MPLS VPNs



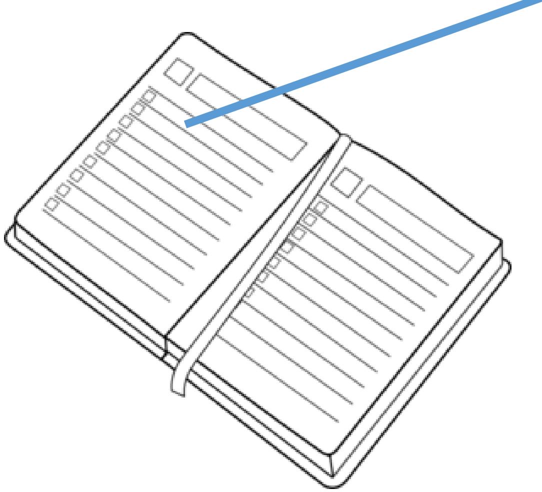
As a user:

You have to know the risks and decide if you will trust 100% in your Service Provider or you'll do something to improve your security.

As a Service Provider:

You have to know the possible risks and how to ensure that your network do not expose your customers.

Agenda



Introduction and Motivations ✓

MPLS and VPNs Background

Layer 2 and Layer 3 VPNs configurations

A Working Scenario

MPLS VPNs Threats / Hands on

Defenses – Good practices and recommendations

Conclusions

MPLS Basics

MPLS Basics

MPLS is a framework typically used to enhance an IP network. MPLS ***is not a routing protocol*** - it works with layer 3 routing protocols (BGP, OSPF, static) to integrate network layer routing with label switching.

Main advantages of MPLS:

→ multiple types of traffic coexisting on the same network;

→ traffic management and fast restoration after failures;

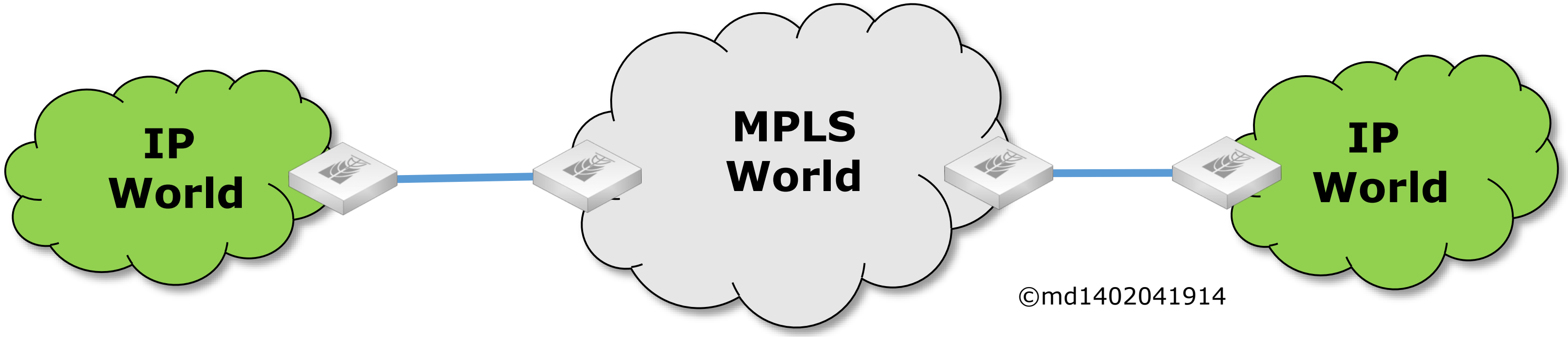
→ Higher performance for forwarding.

How MPLS works:

→ Routers on the incoming edge of the MPLS network add an 'MPLS label' to the top of each packet.

→ This label is based on some criteria (e.g. destination IP address) and is then used to steer it through the subsequent routers.

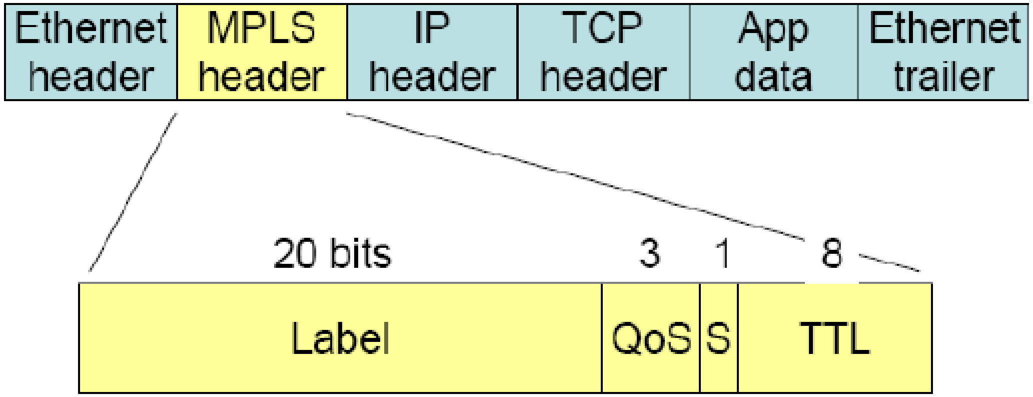
→ The routers on the outgoing edge strip it off before final delivery of the original packet.



©md1402041914

MPLS Basics

The Label:



→ Label value (0 to 15 reserved for special use)

→ QoS: Quality of service

→ S: Bottom of Stack (set to 1 for the last entry in the label)

→ TTL: Time to live

MPLS Background

MPLS Terminology:

Label Switch Router (LSR)—A device that forwards labeled entities based upon the label’s value.

Label Edge Router (LER)—Resides at the edge of an MPLS network and assigns and removes the labels from the packets.

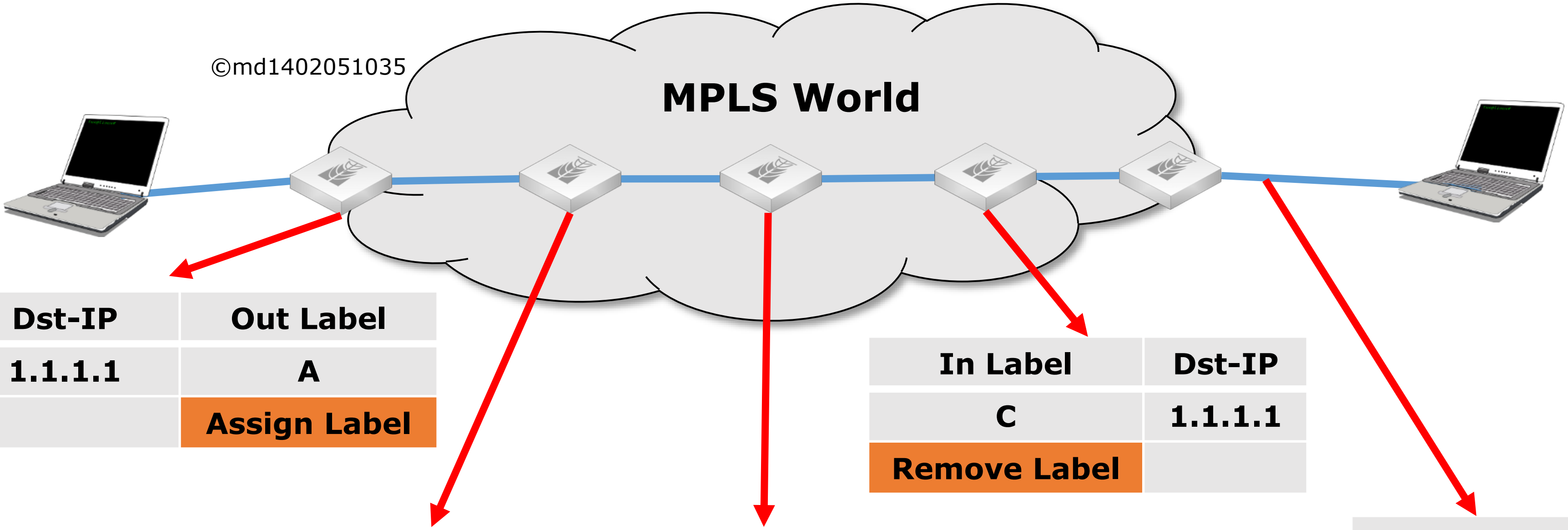
MPLS Background

MPLS Terminology:

Label-Switched Path (LSP)—The path defined by the labels through LSRs between end points.

Forward Equivalence Class (FEC) – A representation of a group of packets that share the same requirements for their transport. The assignment of a particular packet to a particular FEC is done just once (when the packet enters the network).

MPLS in action



Dst-IP	Out Label
1.1.1.1	A
	Assign Label

In-Label	Out-Label
A	B
Label Swapping	

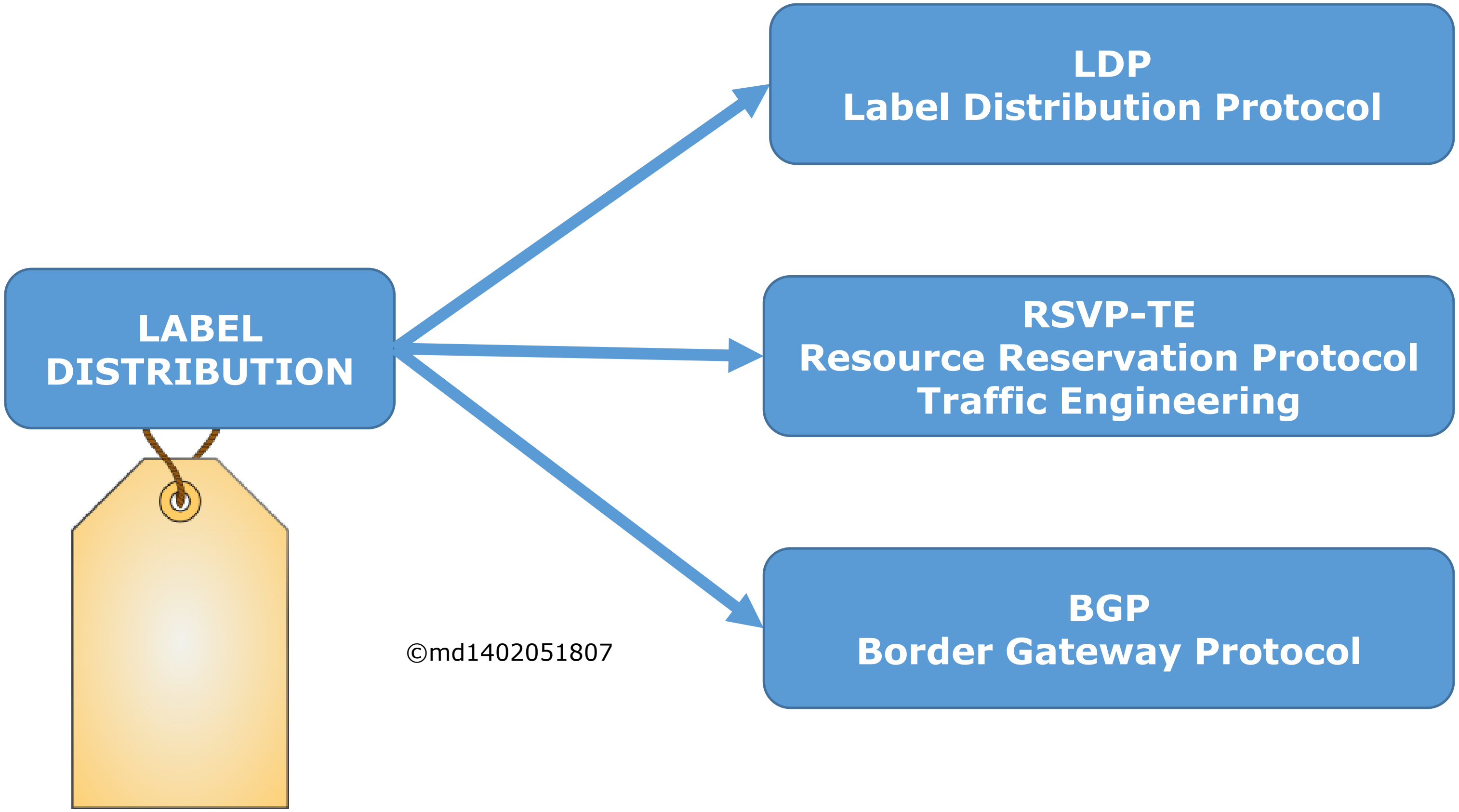
In-Label	Out-Label
B	C
Label Swapping	

In Label	Dst-IP
C	1.1.1.1
Remove Label	

IP
1.1.1.1

Label Distribution:

There are 3 methods for Label distribution:



MPLS Background

LDP (Label Distribution Protocol)

→ LDP is used between nodes in an MPLS network to establish and maintain the label bindings;

→ LDP has 4 kind of functions:

- → Discovery;
- → Management;
- → Advertisement;
- → Notification.

MPLS Background

LDP (Label Distribution Protocol)

→ In order to MPLS to operate correctly, label distribution information needs to be transmitted reliably. TCP is used to establish sessions between LSR's;

→ UDP is used for functions like discovery and advertisement. Such messages are sent to 224.0.0.2 "all routers in this subnet". It's supposed that all routers are trustworthy;

→ MD5 encryption for LDP messages (RFC5036 session 2.9) isn't yet supported by RouterOS ☹

MPLS Background

RSVP-TE (Resource Reservation Protocol – Traffic Engineering)

→ RSVP-TE is an extension of RSVP protocol and supports the reservation of resources across an IP Network;

→ Applications running on IP end systems can use RSVP to indicate to other nodes the nature of the packet streams they want to receive.

→ RSVP-TE generally allows the establishment of MPLS label switched paths (LSPs), taking into consideration network constraint parameters such as available bandwidth and explicit hops.

MPLS Background

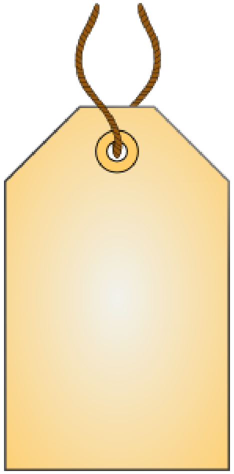
BGP (Border Gateway Protocol)

BGP can be used to transport various protocols besides IPv4. (BGP Multiprotocol or M-BGP)

In MPLS context BGP can be used to signalize information about:

→ Layer 2 VPN’s

→ Layer 3 VPN’s (VPN-IPv4, or VPNv4)



MPLS VPNs

Types of VPNs
(topology and technology)

→ **"Traditional" VPNs**

Frame Relay, ATM (Layer 2)

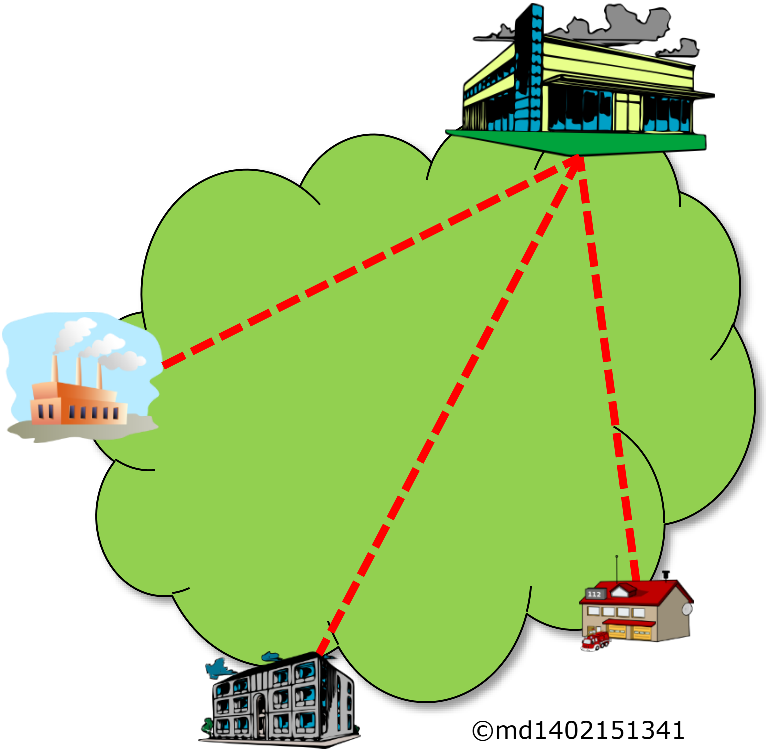
→ **CPE-based VPNs**

L2TP, PPTP, SSTP, etc.

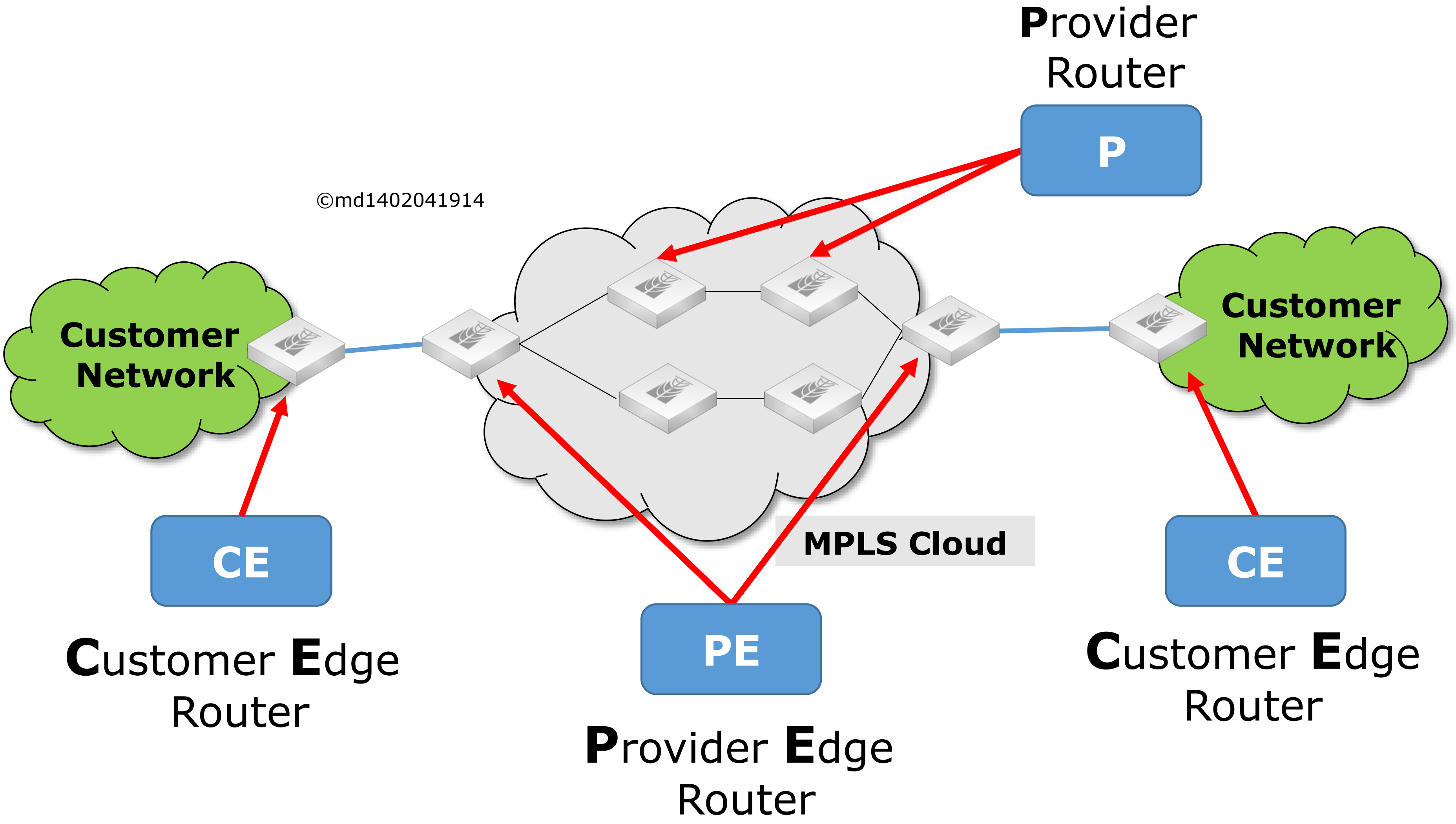
→ **Provider Provisioned VPNs**

MPLS-based Layer 2 and

Layer 3 VPNs



MPLS VPNs Terminology



Provider
Router

P

©md1402041914

Customer Network

Customer Network

MPLS Cloud

CE

Customer **E**dge
Router

PE

Provider **E**dge
Router

CE

Customer **E**dge
Router

Layer2 x Layer3 VPNs

MPLS VPNs
(Layer 2 x Layer 3)

Layer 2:

Transparent to underlying protocols;

Service Provider does not manage customers networks

Layer 3:

Currently only for IPv4 protocol;

More complexity on implementation;

Robust and reliable;

Service Provider manages customer’s routing tables.

MPLS VPNs
(Layer 2 x Layer 3)

The decision about the appropriate type of MPLS VPN to use should consider:

→ Type of traffic to be transported;

(when a customer needs transparent connection, definitely he needs Layer2 VPNs)

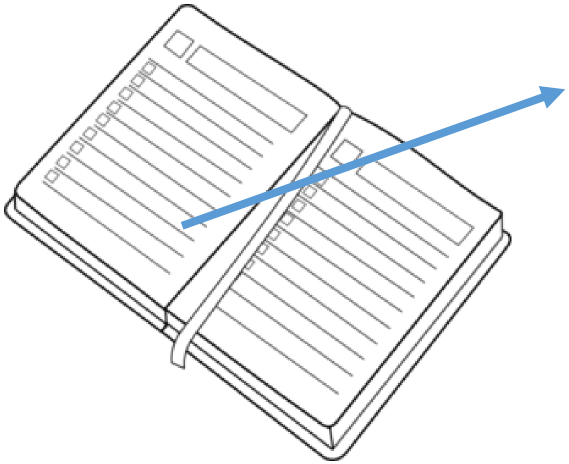
→ Role of the Service Provider related to Customer’s network.

(which grade of efforts on management and provisioning, Providers are willing to have)

Agenda

Introduction and Motivations ✓

MPLS and VPNs Background ✓



Layer 2 and Layer 3 VPNs configurations

A Working Scenario

MPLS VPNs Threats / Hands on

Defenses – Good practices and recommendations

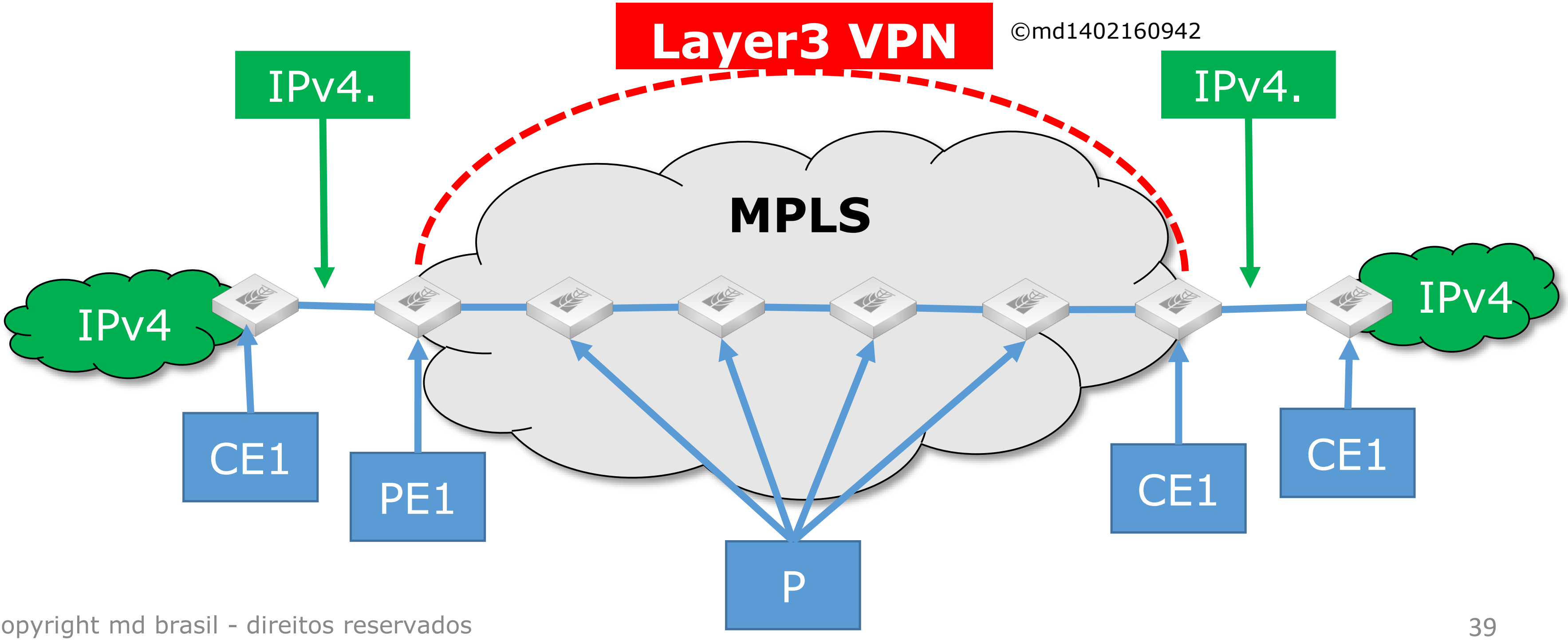
Conclusions

Layer3 VPNs

Layer 3 MPLS VPNs

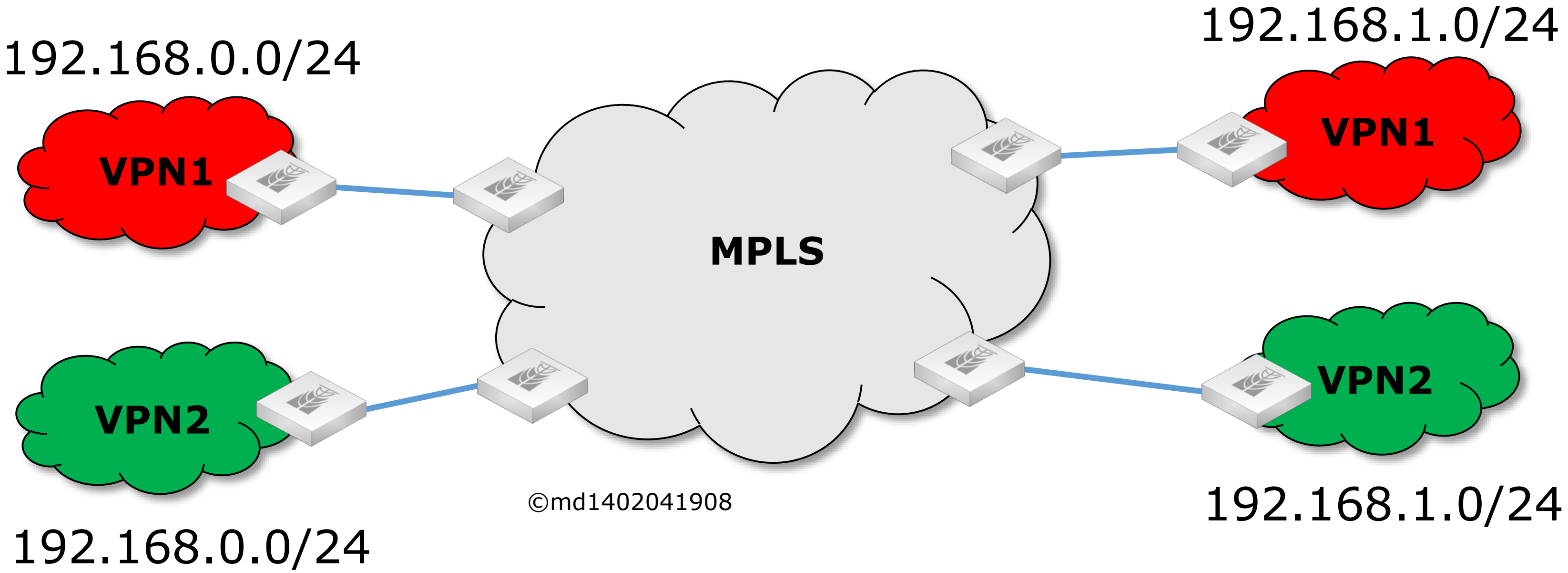
Layer3 VPNs are used to forward IPv4 traffic through a MPLS cloud using a LSP.

Based on RFC 2547 and 2547bis (BGP/MPLS)



Layer 3 MPLS VPNs

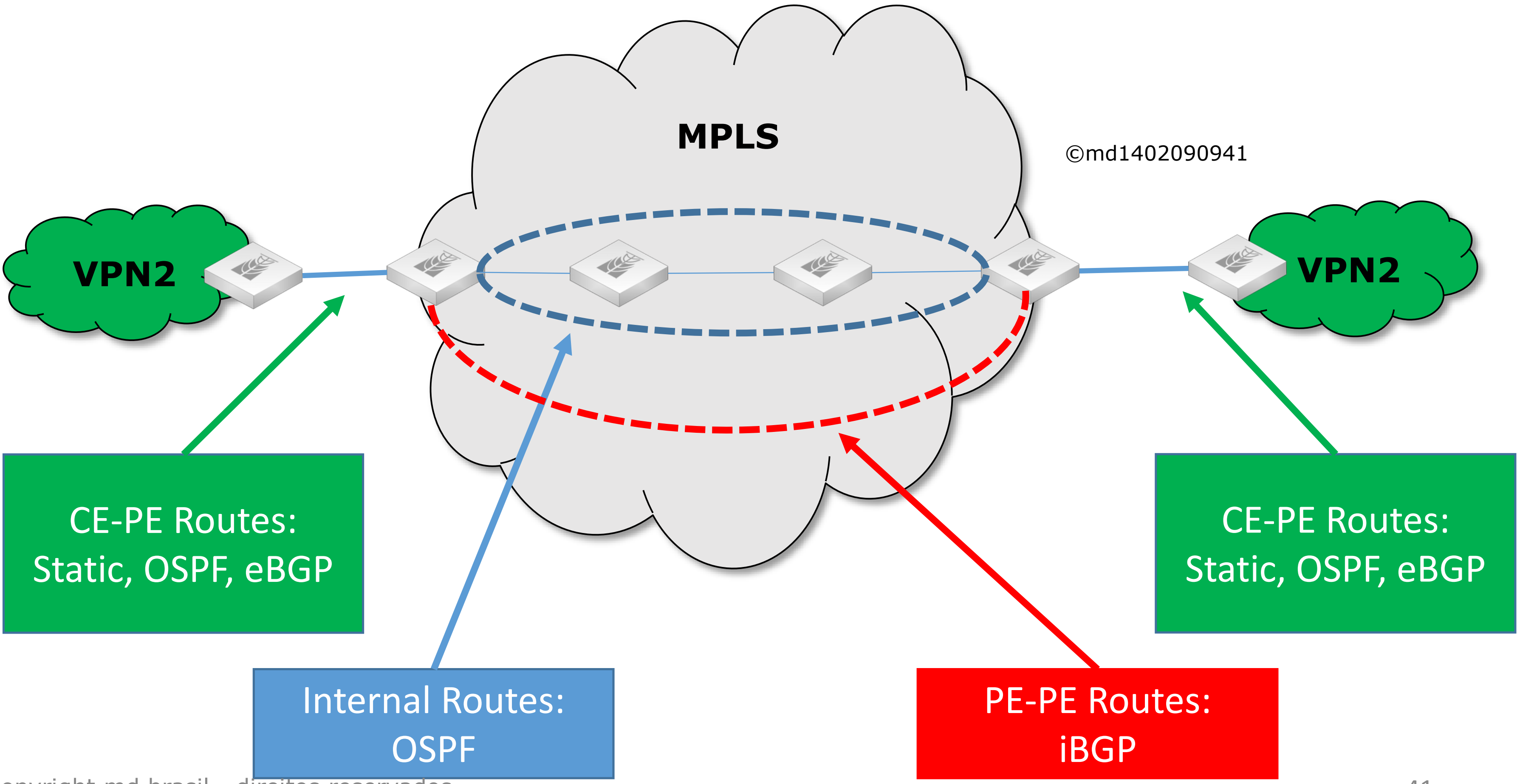
With layer 3 MPLS VPNs we can share an infrastructure and run separated virtual routing tables (VRF) without customer's prefixes overlapping.



©md1402041908

Layer 3 MPLS VPNs

Different routing protocols can be used in a L3 VPN implementation



CE-PE Routes: Static, OSPF, eBGP

Internal Routes: OSPF

PE-PE Routes: iBGP

CE-PE Routes: Static, OSPF, eBGP

Layer 3 MPLS VPNs

Virtual Routing and Forwarding (VRF)

Layer 3 MPLS VPNs have 2 important characteristics:

→ On client side can be used either public (exclusive) or private (non exclusive) IP addresses;

→ The same site can be part of more than one VPN;

To use the same set of IP addresses without overlapping, PE routers use multiples routing tables called **VRFs** (Virtual Routing and Forwarding). For each VPN, there is one VRF on PE routers.

Route Distinguisher (RD) [1/2]

Each PE router receives updates via BGP from other PE routers;

The default behavior of BGP would be to choose only one route based on BGP decision criteria;

Because of the possibility of using overlapping IP addresses, there is necessary an attribute called **Route Distinguisher (RD)** to separate routes from different VPNs;

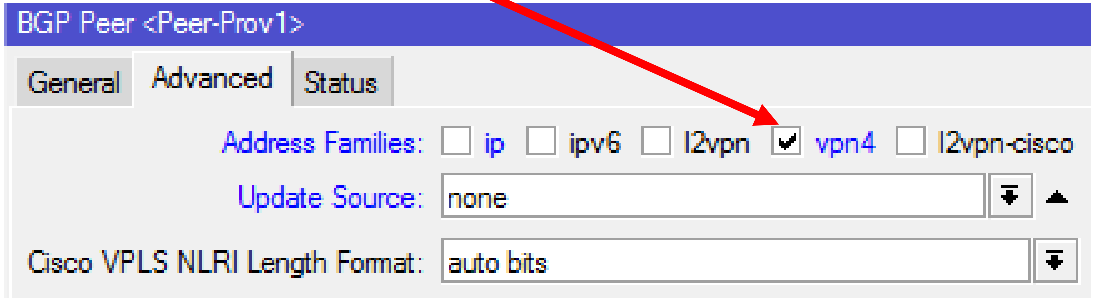
RD is a 64 bit number.

Route Distinguisher (RD) [2/2]

The result of Route Distinguisher + IPv4 is a 96 (64 + 32) bit number

Route Distinguisher	IPv4 Address

This combination creates a new family of addresses, called VPN-IPv4 or VPNv4.



BGP Peer <Peer-Prov1>

Address Families: □ ip □ ipv6 □ l2vpn ☑ vpn4 □ l2vpn-cisco

Update Source: none

Cisco VPLS NLRI Length Format: auto bits

Route Target (RT) [1/2]

As stated previously, one site can participate in more than one VPN;

To separate traffic between sites participating in several VPNs, preventing one PE router to accept routes from VPNs that it not belongs to, attributes from BGP extended communities are used;

Route Target attribute is inserted in each announced route to indicate to which VPN this route belongs to.

Route Target (RT) [2/2]

Each VPN has an exclusive value for Route Target;

When a PE router receives a routing update, it verifies based on the attribute if the corresponding VPN is part of the ones it is configured to work with. Case positive it accepts the route, otherwise, the route is discarded;

The use of Route Targets prevent that PEs work with all routes of all VPNs, helping on scalability of the network.

How Layer3 VPN works

→ PE routers assign label to prefixes per VPN (Route Distinguisher);

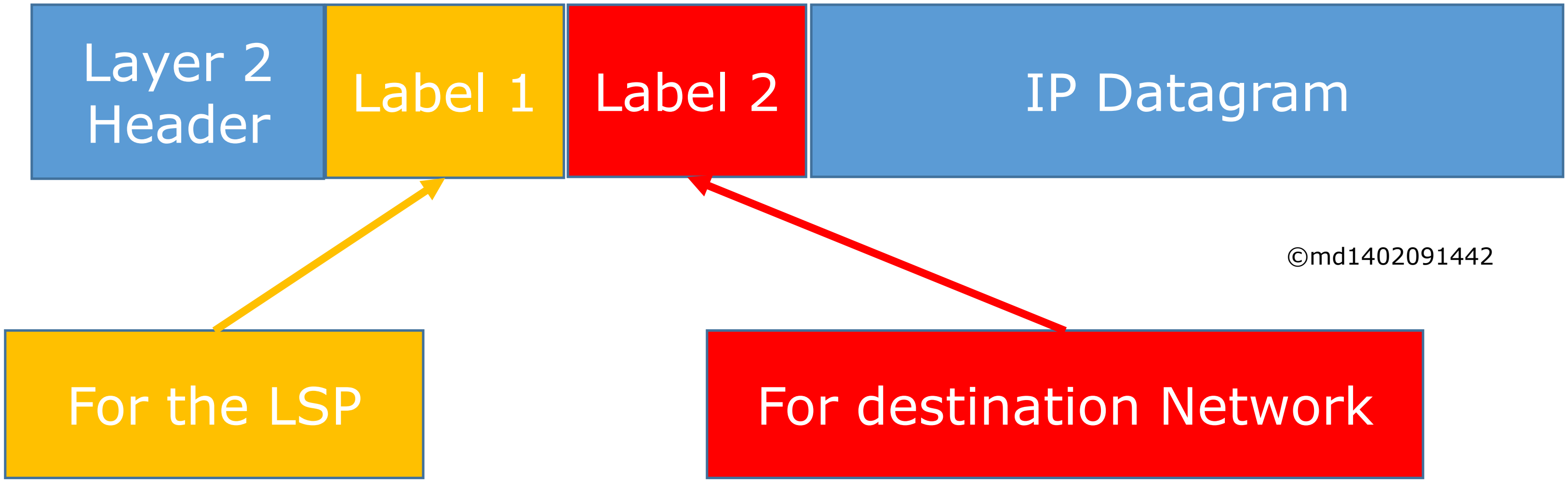
→ Label, route distinguisher and prefixes are exchanged between PEs by BGP Multiprotocol;

→ One PE knows which other PE is responsible for a given prefix in a given VPN;

→ When a packet leaves an ingress PE, the packet has at least 2 labels – one to forward across MPLS cloud and other to identify the VPN and prefix of destination.

Labels for L3 VPNs

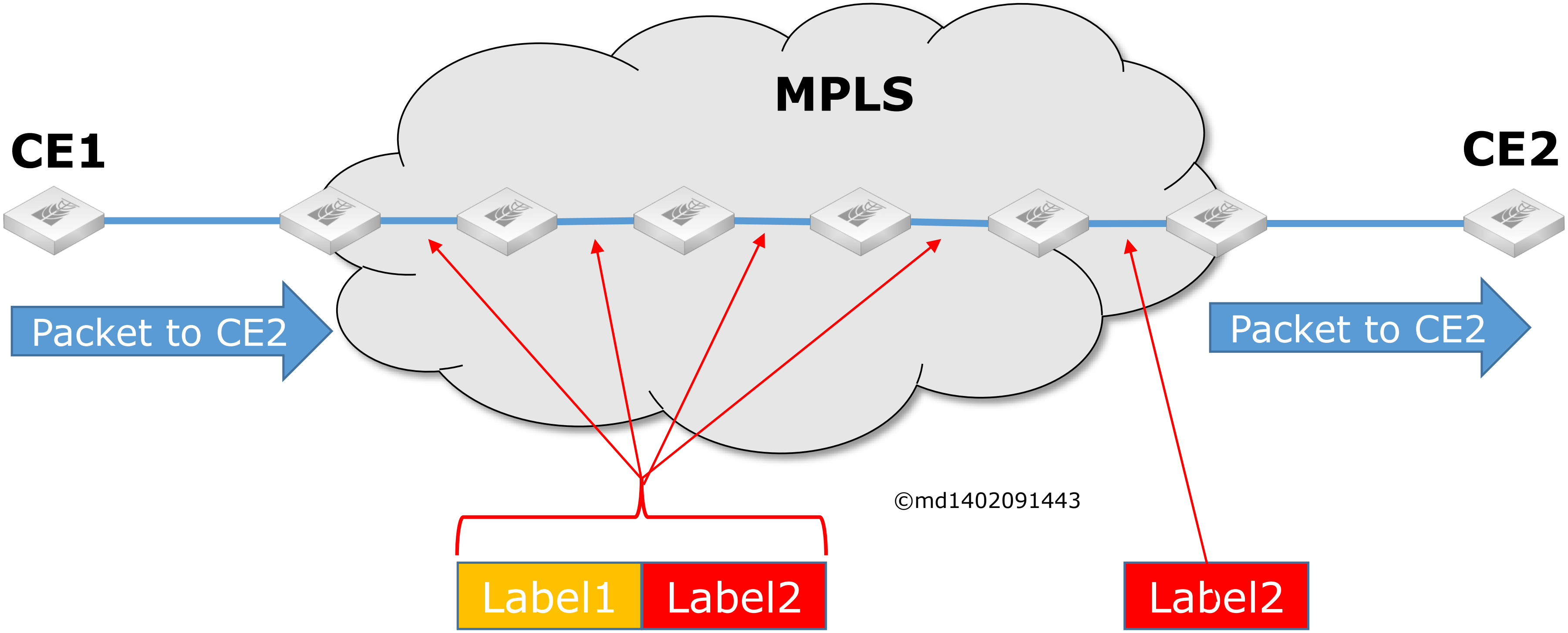
When a PE receives a packet destined to a remote site, 2 Labels are inserted:



©md1402091442

MPLS Layer 3 VPN in action

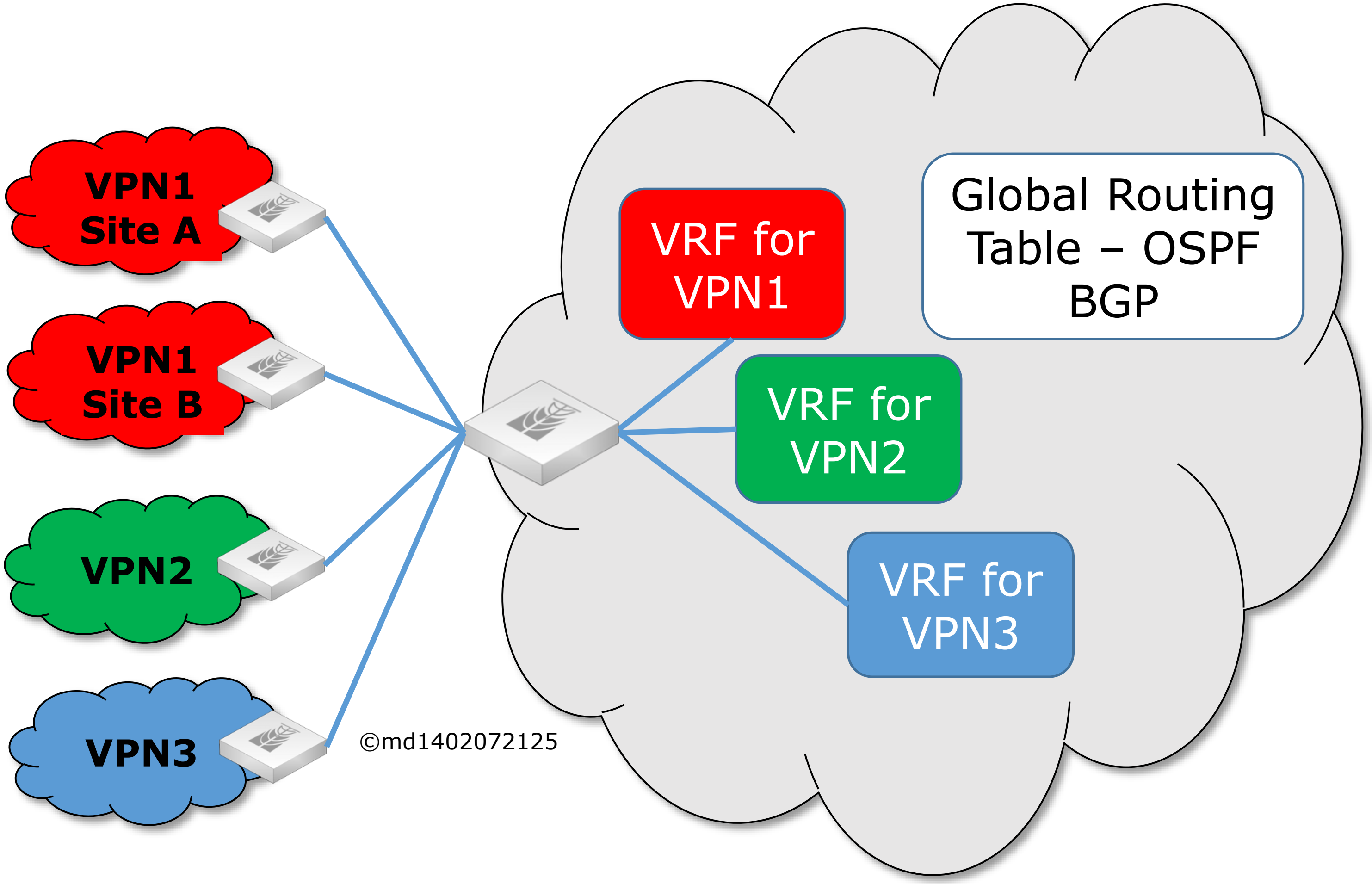
CE1 sends a packet to CE2 and PE router insert 2 Labels. First label is used along LSP. Penultimate router strips out first label and the egress router strips out the second label



©md1402091443

Layer 3 MPLS VPNs

One important detail about L3 VPNs is that a “shared” PE router can handle different VRFs



Layer2 VPNs

Layer 2 MPLS VPNs

Layer 2 VPN’s

Can be used to transparently transport frames from one site to another, regardless layer 3 protocols.

There is no routing exchange between CE and PE

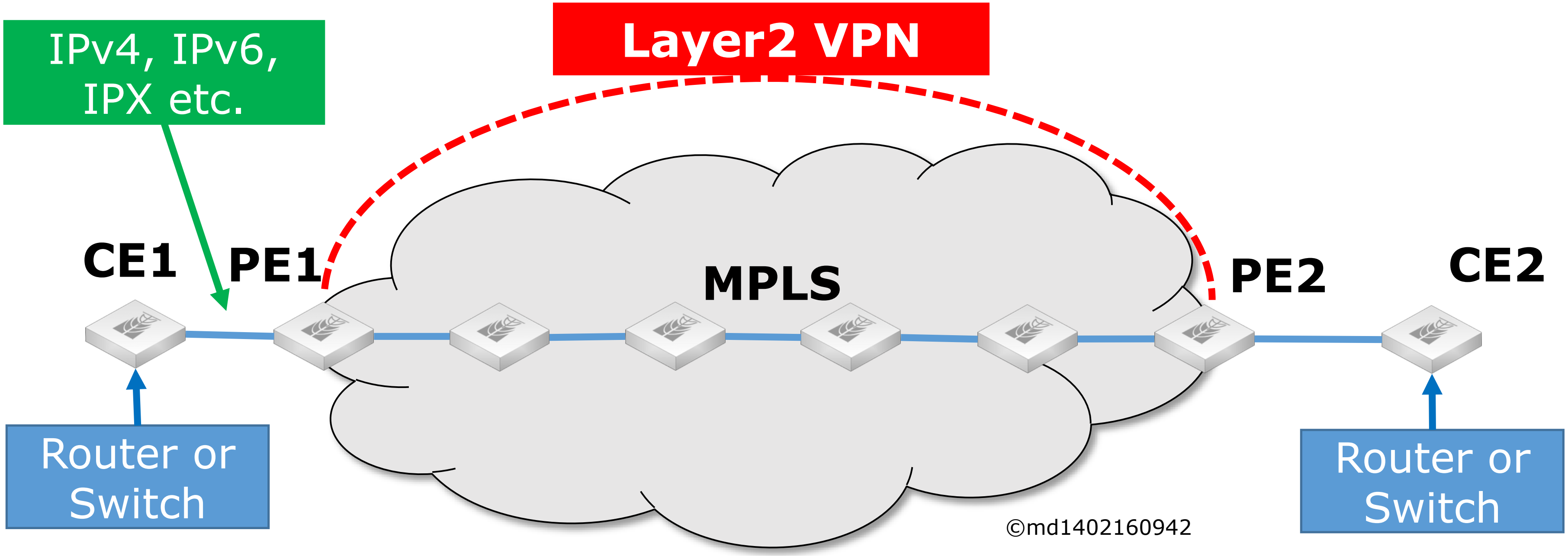
They can be point-to-point or point-multipoint.

One site can be viewed as a “Big Switch”

Layer 2 MPLS VPNs

Layer2 VPNs establish a tunnel between Ingress (PE) and Egress (PE) routers to transport **any** protocol;

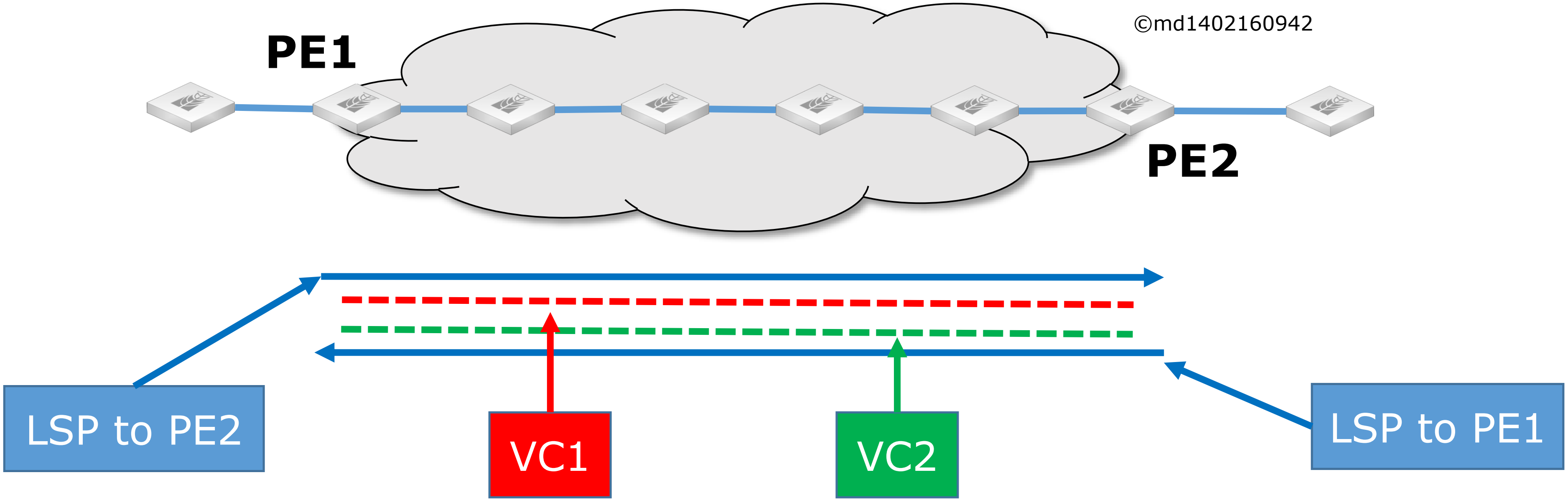
On Customer's Edge, equipment can be routers or single layer2 devices.



Layer 2 MPLS VPNs

Layer 2 VPN's

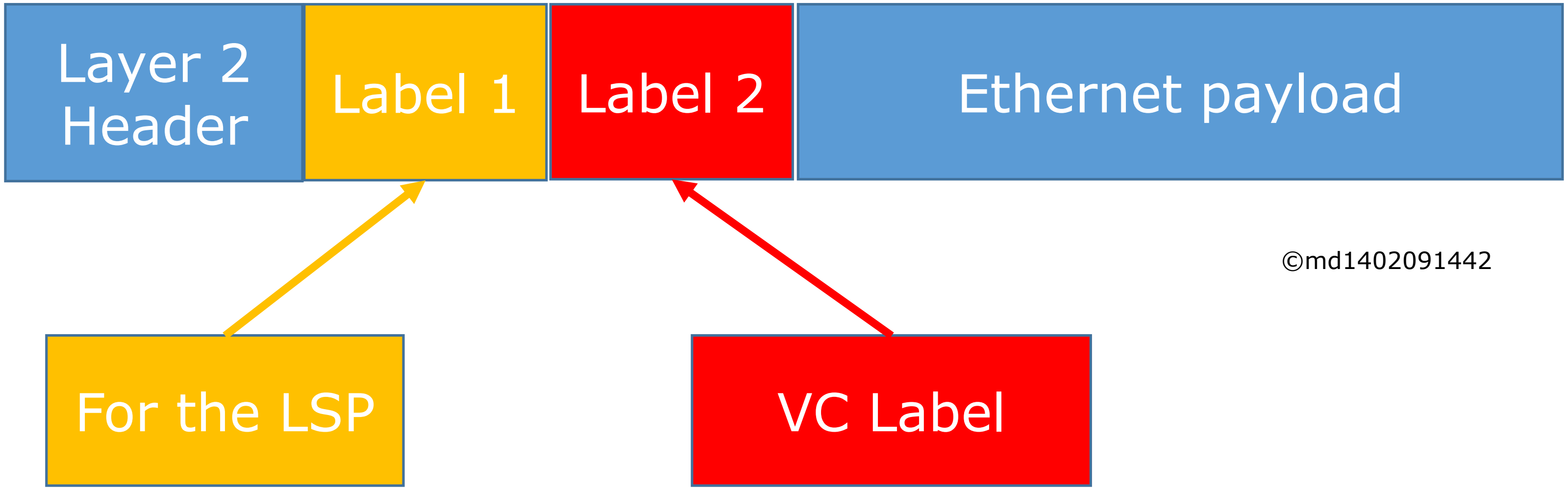
→ Each L2 VPN establishes a Virtual Circuit (VC) where a VC is a kind of LSP "inside" another LSP



Layer 2 MPLS VPNs

Tunnel Label and VC Label

→ LSPs are responsible to connect PEs and VCs to transport user’s frames;



©md1402091442

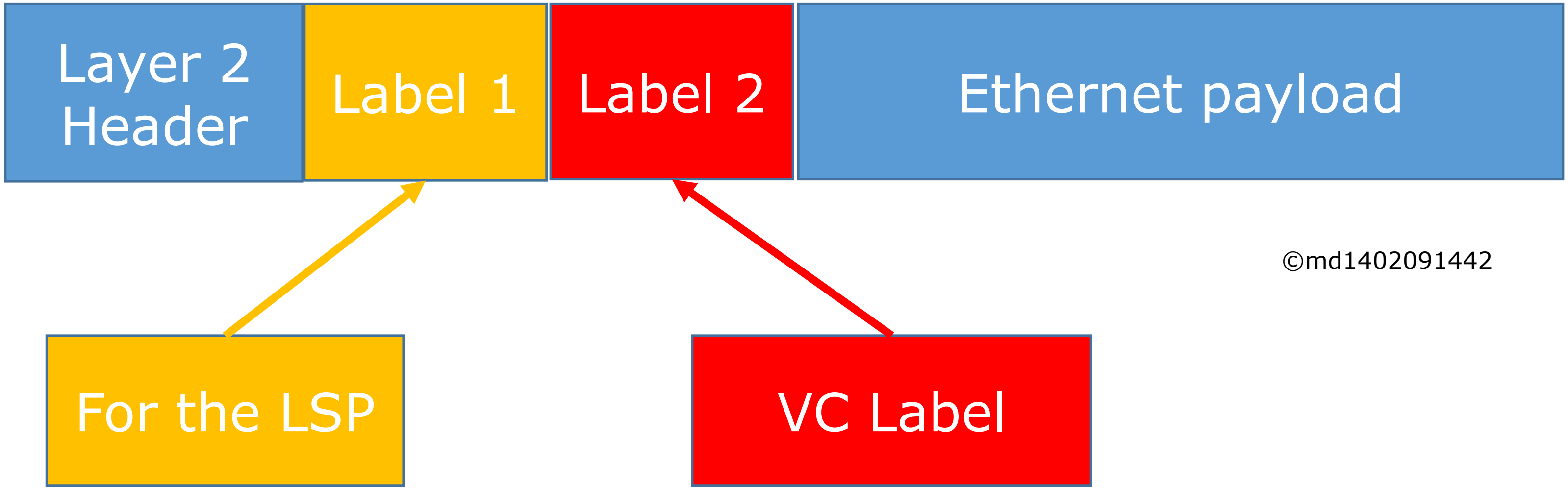
Layer 2 MPLS VPNs

VPLS (Virtual Private LAN Service)

→ VPLS is used for Point-Multipoint Layer2 VPNs;

→ VPLS creates a complete mesh of VCs (for each traffic direction);

→ Clients VPNs are identified by a unique VPN ID (32 bit)

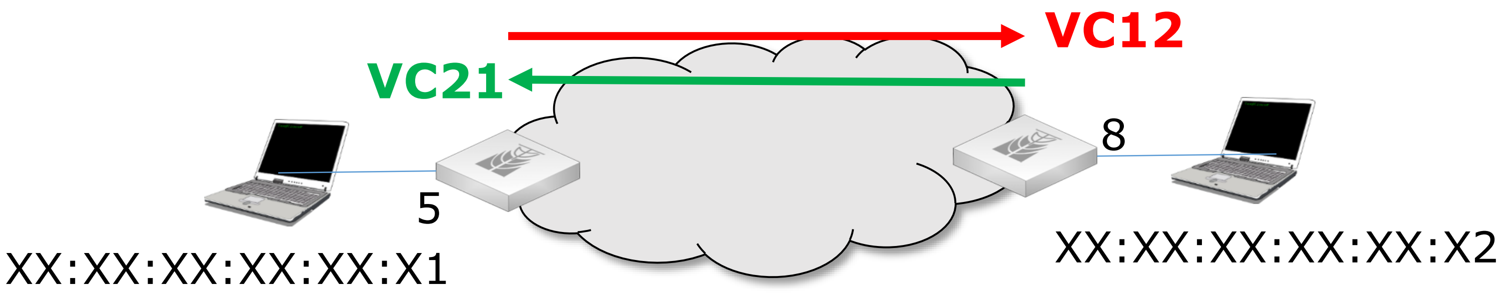


©md1402091442

How VPLS works (1/3)

→ Like regular switches learn MAC addresses on physical ports, PE routers learn on their VCs;

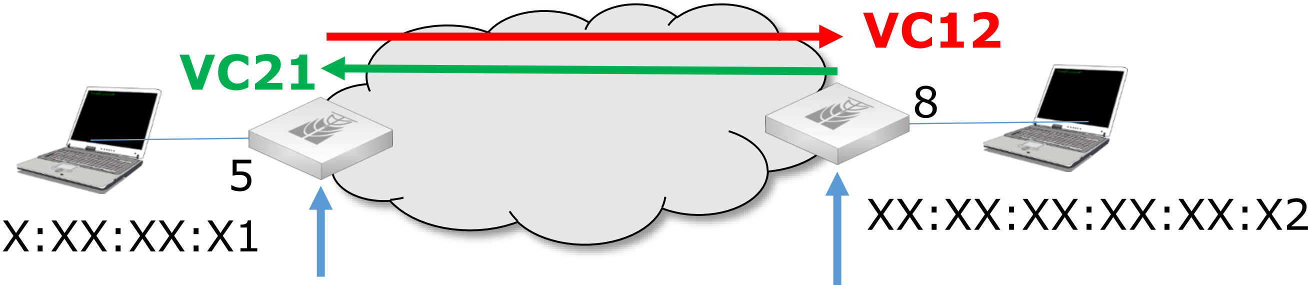
→ Each PE keeps, for each VPN, a separate forwarding table called VFI (Virtual Forwarding Instance);



©md1402161239

How VPLS works (2/3)

When a PE receives a frame destined to a MAC address it doesn’t have yet in its table, it floods the frame to all VC’s. When a response is received, PE insert an entry for the MAC pointing to the VC it received the response.



VPLS ID	MAC Address	VC	Port
100:0	XX:XX:XX:XX:XX:X1	---	5
100:0	XX:XX:XX:XX:XX:X2	VC12	---

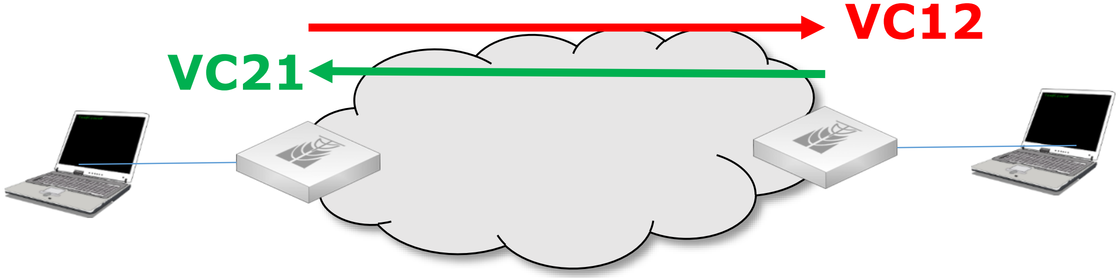
©md1402161239

VPLS ID	MAC Address	VC	Port
100:0	XX:XX:XX:XX:XX:X1	VC12	---
100:0	XX:XX:XX:XX:XX:X2	---	8

How VPLS works (3/3)

→ PE routers learn only MAC addresses from the VPNs it belongs to.

→ P Routers don’t learn MACs. They only forward traffic based on MPLS Labels.



Implementations with Mikrotik RouterOS

Static VPLS:

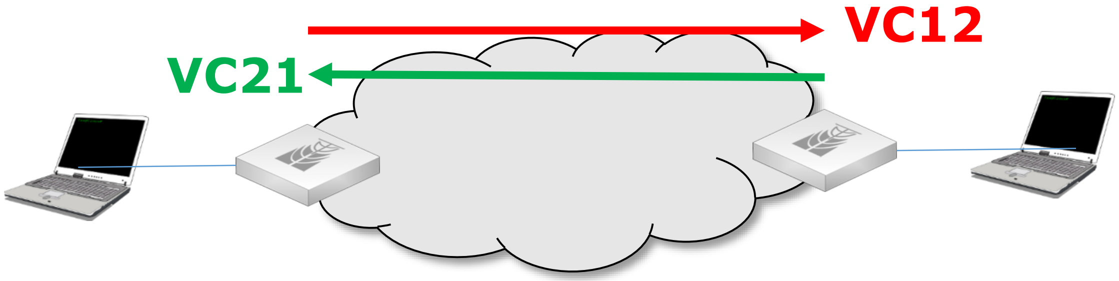
Very simple and functional;

Depends on LDP.

BGP VPLS:

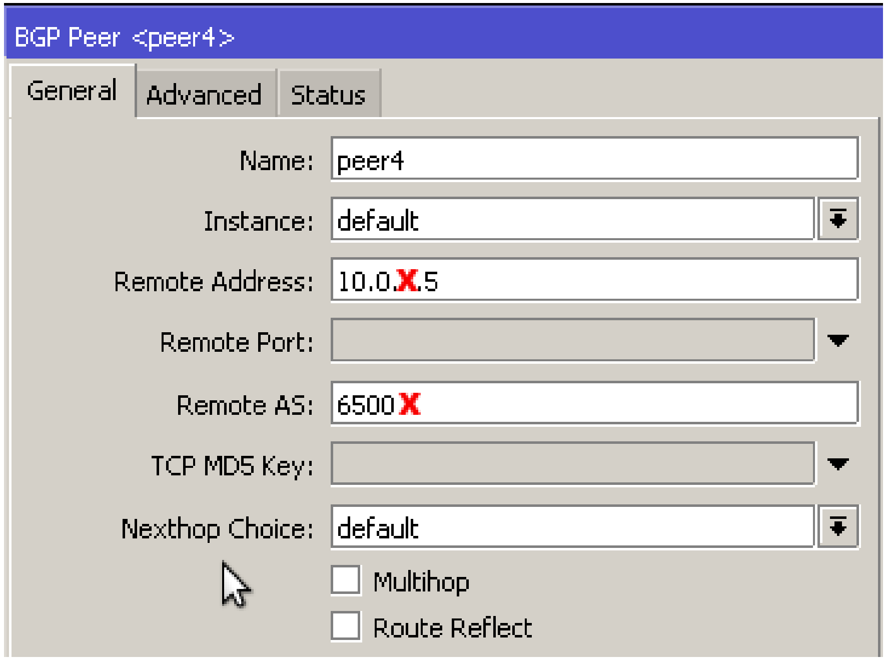
Requires Full Mesh iBGP between routers;

More Scalable.

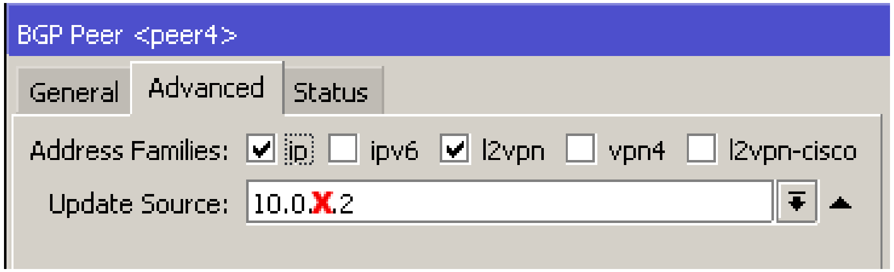


Implementations with Mikrotik RouterOS – BGP VPLS

- Configure peering between routers
- enable address family l2vpn



Name: peer4
Instance: default
Remote Address: 10.0.X.5
Remote Port:
Remote AS: 6500X
TCP MD5 Key:
Nexthop Choice: default
□ Multihop
□ Route Reflect

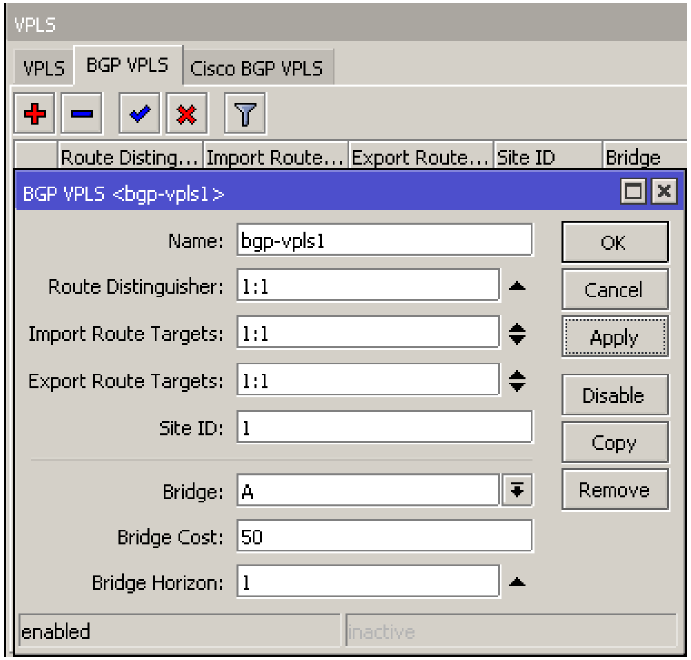


Address Families: ☑ ip □ ipv6 ☑ l2vpn □ vpn4 □ l2vpn-cisco
Update Source: 10.0.X.2

Layer 2 MPLS VPNs

Implementations with Mikrotik RouterOS – BGP VPLS

Configure BGP VPLS, route distinguisher, route targets



BGP VPLS <bgp-vpls1>

Name: bgp-vpls1

Route Distinguisher: 1:1

Import Route Targets: 1:1

Export Route Targets: 1:1

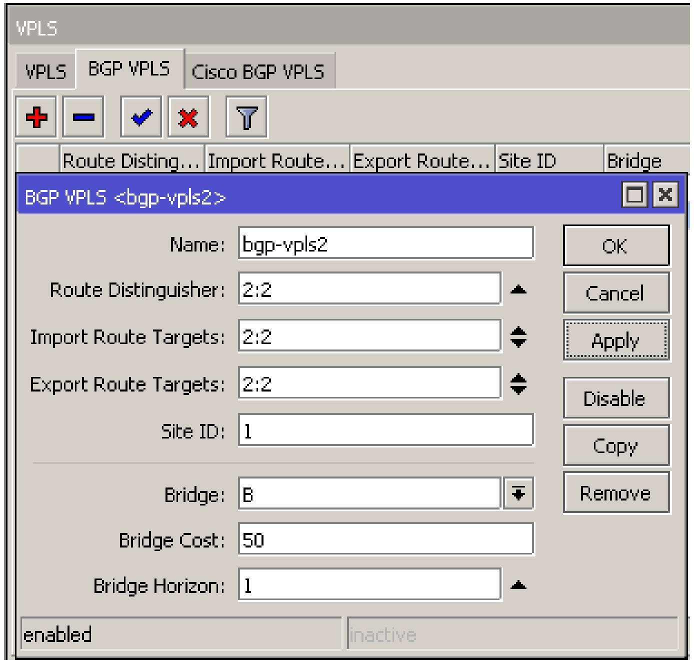
Site ID: 1

Bridge: A

Bridge Cost: 50

Bridge Horizon: 1

enabled | inactive



BGP VPLS <bgp-vpls2>

Name: bgp-vpls2

Route Distinguisher: 2:2

Import Route Targets: 2:2

Export Route Targets: 2:2

Site ID: 1

Bridge: B

Bridge Cost: 50

Bridge Horizon: 1

enabled | inactive

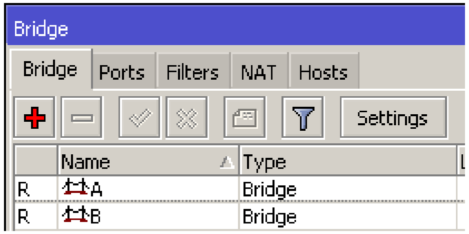
Layer 2 MPLS VPNs

Implementations with Mikrotik RouterOS – BGP VPLS

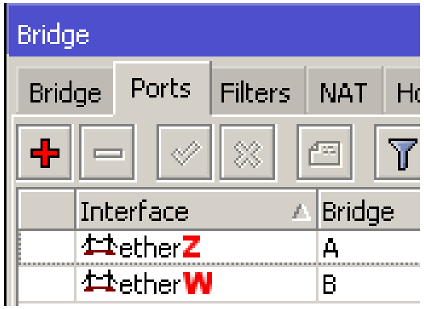
- Configure a bridge

- Insert only physical ports we want to participate in that bridge;

- VPLS interfaces will appear automatically



	Name	Type
R	A	Bridge
R	B	Bridge



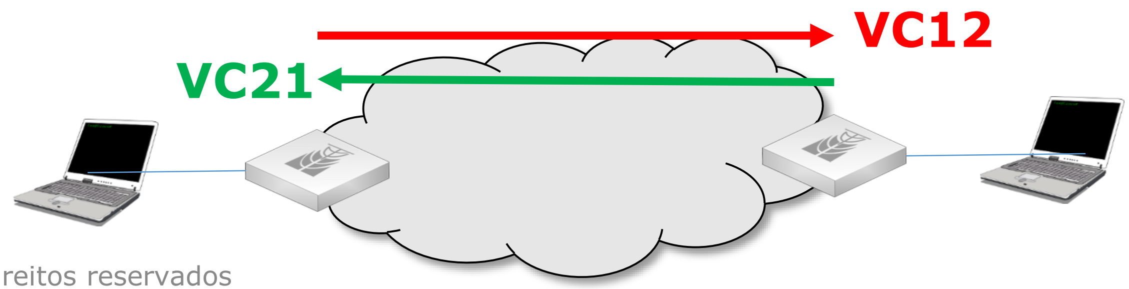
	Interface	Bridge
	etherZ	A
	etherW	B

Layer 2 MPLS VPNs

VPLS and Spanning Tree

→ Unlike regular switches, PE routers do not rely only on (R)STP – (Rapid) Spanning Tree Protocol to avoid loops in a redundant network.

→ VPLS can use “Split Horizon” technique, ensuring that a frame received from a customer only can be transmitted to another directly connected and not to another participating in the same VPN.

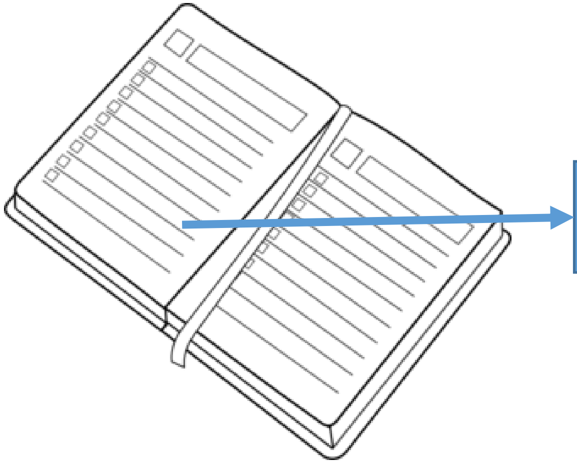


Agenda

Introduction and Motivations ✓

MPLS and VPNs Background ✓

Layer 2 and Layer 3 VPNs configurations ✓



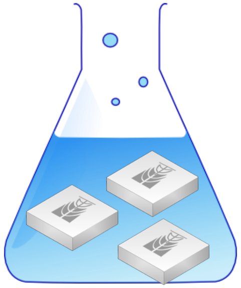
A Working Scenario

MPLS VPNs Threats / Hands on

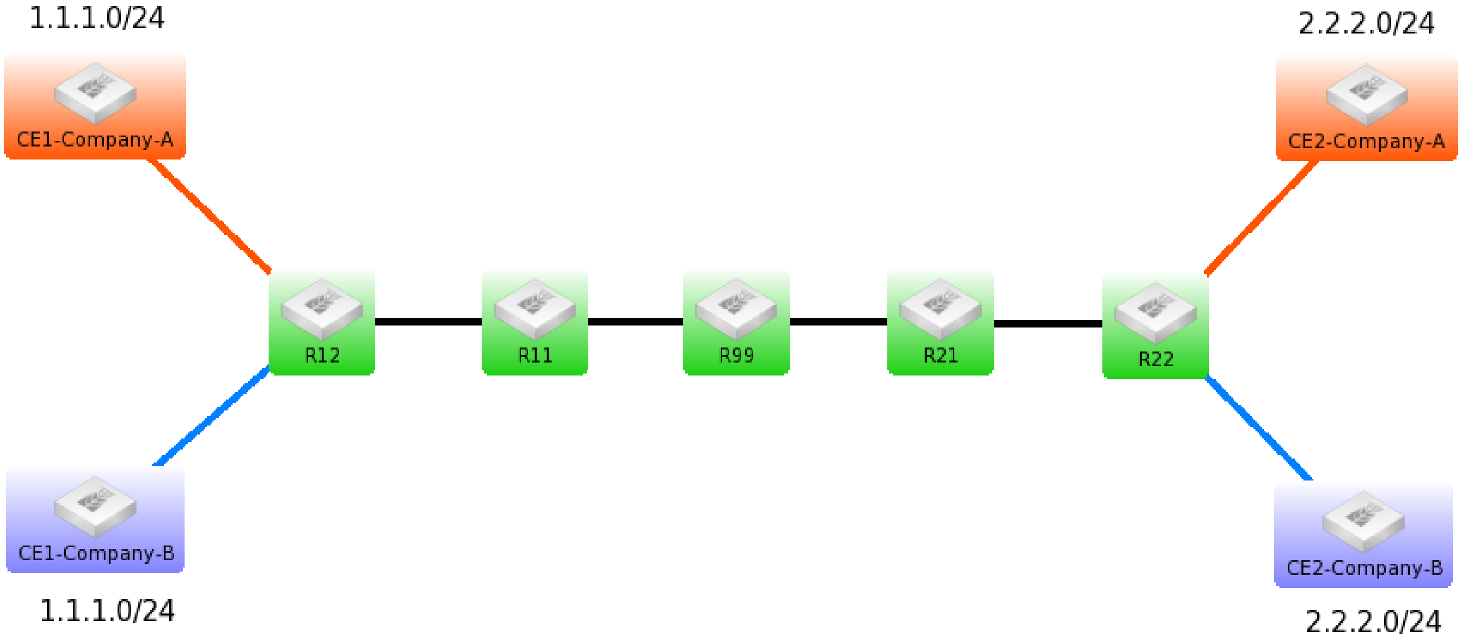
Defenses – Good practices and recommendations

Conclusions

Layer3 VPN Working Lab

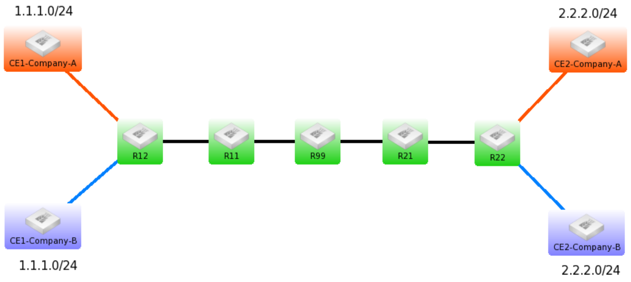


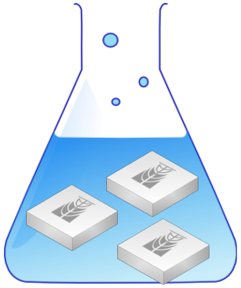
Company A (orange) and B (Blue) are different companies and both use the same address space. VRFs will keep VPNs separated



NB: For sake of simplicity we’re using public address space (1.1.1.0/24 and 2.2.2.0/24).

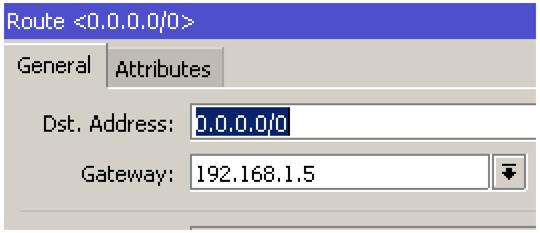
Layer3 VPN Working Lab





CE-1-A and CE-1-B have only default route pointing to PE-1.

The same for CE-2-A and Ce-2-B

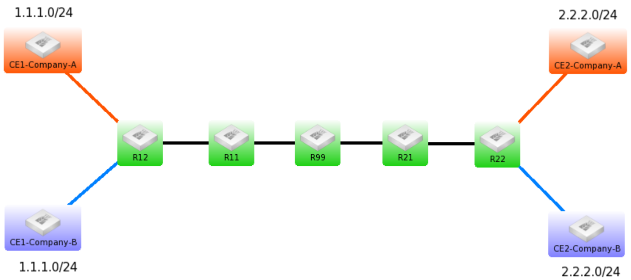


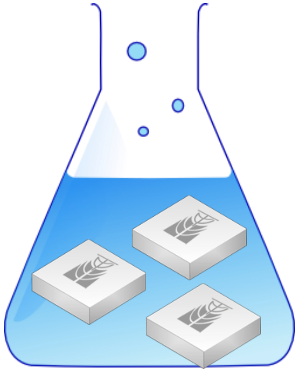
Route <0.0.0.0/0>

Dst. Address: 0.0.0.0/0

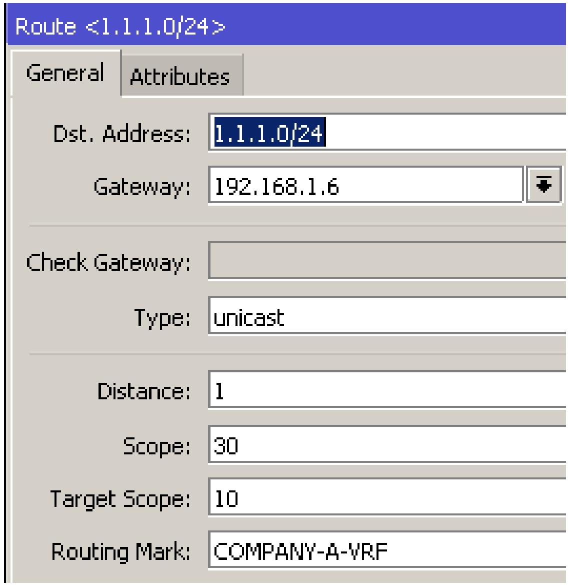
Gateway: 192.168.1.5

Layer3 VPN Working Lab





PE-1 VRF configuration



Route <1.1.1.0/24>

General | Attributes

Dst. Address: 1.1.1.0/24

Gateway: 192.168.1.6

Check Gateway:

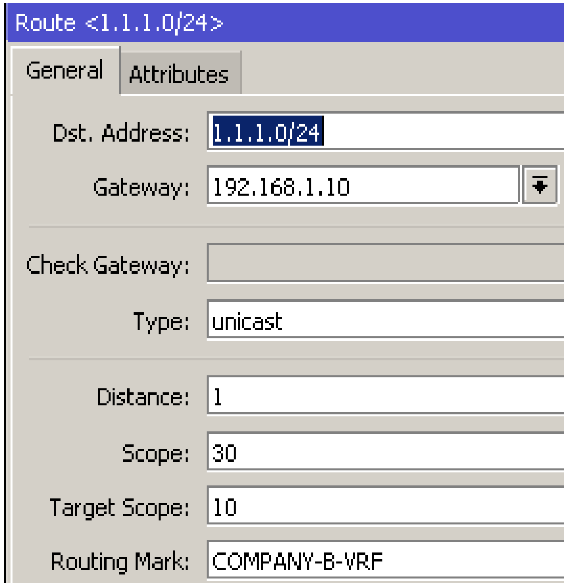
Type: unicast

Distance: 1

Scope: 30

Target Scope: 10

Routing Mark: COMPANY-A-VRF



Route <1.1.1.0/24>

General | Attributes

Dst. Address: 1.1.1.0/24

Gateway: 192.168.1.10

Check Gateway:

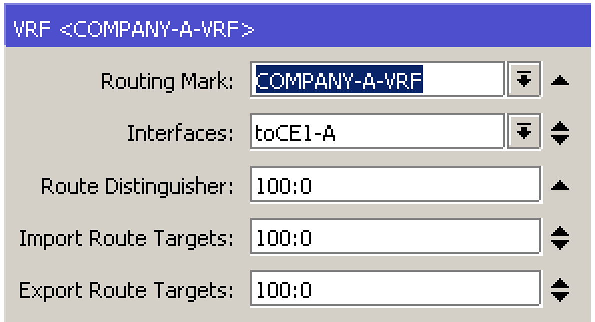
Type: unicast

Distance: 1

Scope: 30

Target Scope: 10

Routing Mark: COMPANY-B-VRF



VRF <COMPANY-A-VRF>

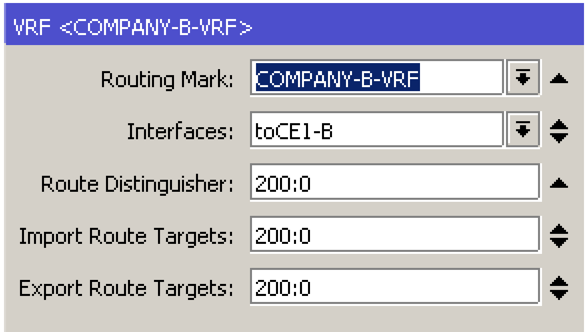
Routing Mark: COMPANY-A-VRF

Interfaces: toCE1-A

Route Distinguisher: 100:0

Import Route Targets: 100:0

Export Route Targets: 100:0



VRF <COMPANY-B-VRF>

Routing Mark: COMPANY-B-VRF

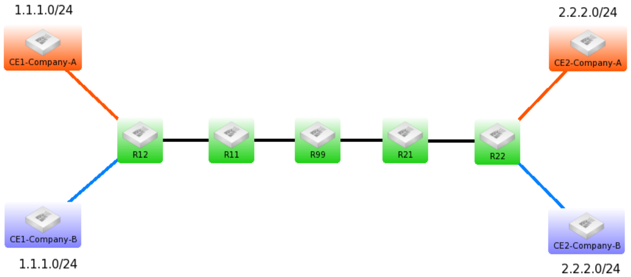
Interfaces: toCE1-B

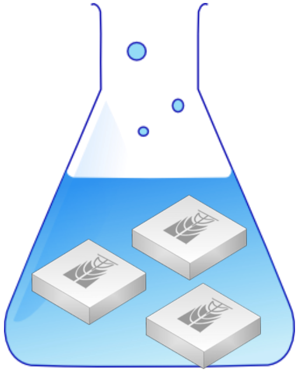
Route Distinguisher: 200:0

Import Route Targets: 200:0

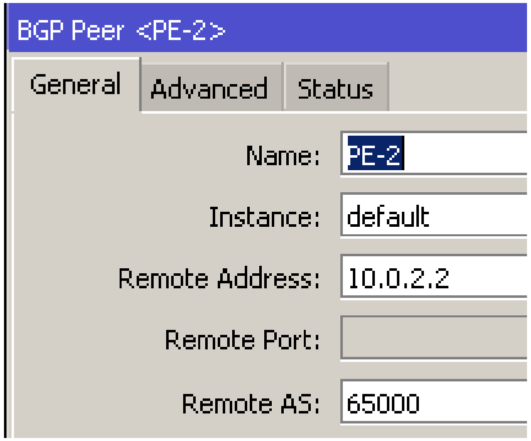
Export Route Targets: 200:0

Layer3 VPN Working Lab





PE-1 BGP / VRF configuration



BGP Peer <PE-2>

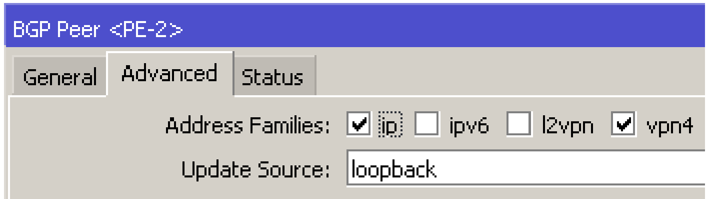
Name: PE-2

Instance: default

Remote Address: 10.0.2.2

Remote Port:

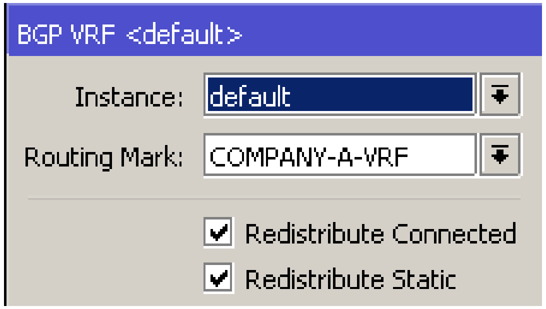
Remote AS: 65000



BGP Peer <PE-2>

Address Families: ☑ ip □ ipv6 □ l2vpn ☑ vpn4

Update Source: loopback



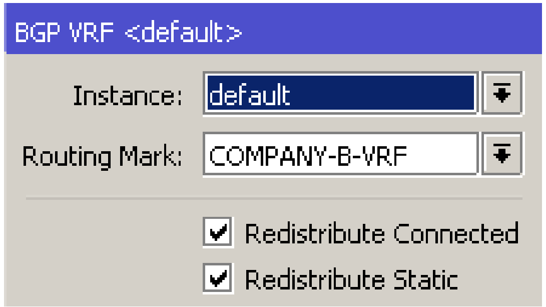
BGP VRF <default>

Instance: default

Routing Mark: COMPANY-A-VRF

☑ Redistribute Connected

☑ Redistribute Static



BGP VRF <default>

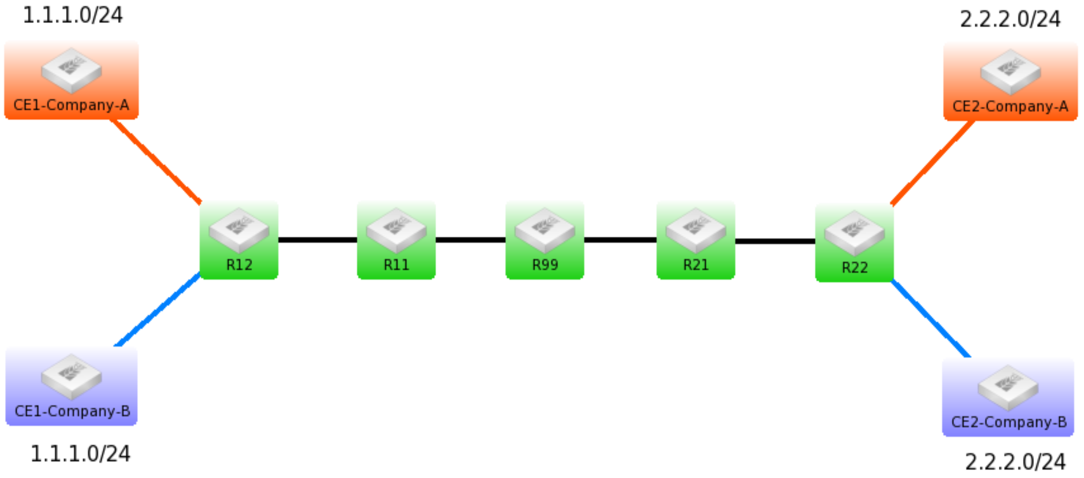
Instance: default

Routing Mark: COMPANY-B-VRF

☑ Redistribute Connected

☑ Redistribute Static

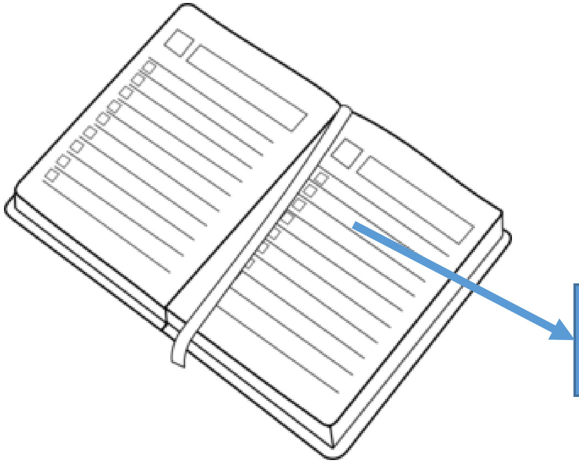
Layer3 VPN Working Lab



CE-1-A will ping 2.2.2.2 and so does CE-1-B;

/system ssh 2.2.2.2 from will show

Agenda



Introduction and Motivations ✓

MPLS and VPNs Background ✓

Layer 2 and Layer 3 VPNs configurations ✓

A Working Scenario ✓

MPLS VPNs Threats / Hands on

Defenses – Good practices and recommendations

Conclusions

Attacks against MPLS VPNs

Attacks against MPLS VPNs

Attacks can be divided in Intrusions and Denial of service

Intrusions:

→ Starts with reconnaissance - Label info disclosure and enumeration

→ Injection of rogue Labels and exploration of underlying routing protocols to divert or sniff traffic.

Denial of Service:

→ Exploring topology characteristics (e.g. shared VPN/Internet connection)

→ Again, injection of rogue Labels and exploration of underlying routing protocols to create blackholes.

Attacks against MPLS VPNs

The success of attacks will depend basically of the position of the attacker, that can be

Attacks from other VPNs:

In this case a real customer or a compromised device on customer premises is the vector of attack.

Attacks from the Internet:

As we will see, depending on the Network topology routers can be target for Intrusions/DoS attacks

Attacks from the Core:

Week topologies, physical insecurity and compromised devices can be explored to launch attacks.

Sounding theoretically?

Attacks against MPLS VPNs

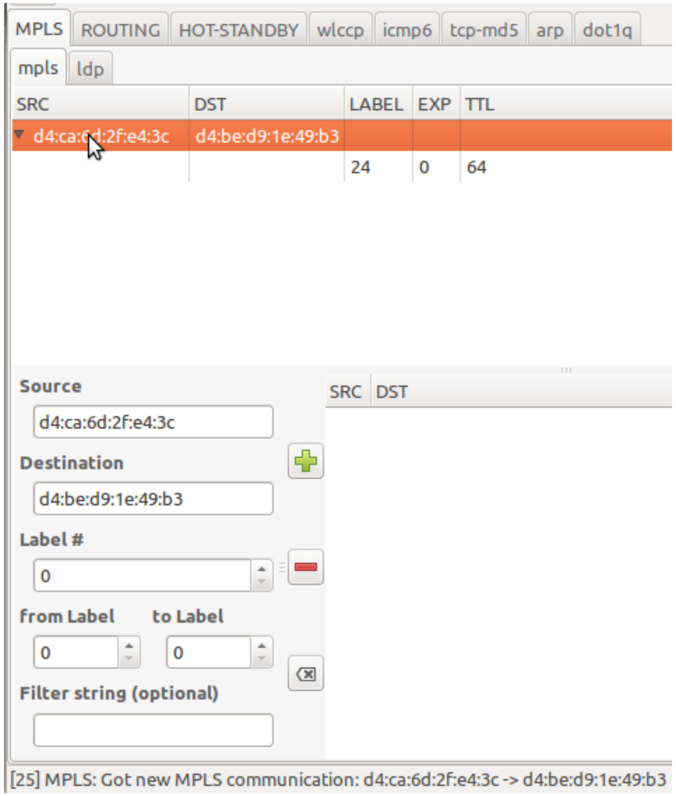
If all those things sound theoretical to you, just take a look on the appropriate tool!

→ Yersinia: Powerful tool for Layer 2 attacks

→ Loki: Complete framework for exploring infrastructure protocols

→ Scapy: Multipurpose packet generator

→ Dsniff, THC, and much more…



SRC	DST	LABEL	EXP	TTL
d4:ca:6d:2f:e4:3c	d4:be:d9:1e:49:b3			
		24	0	64

Source: d4:ca:6d:2f:e4:3c

Destination: d4:be:d9:1e:49:b3

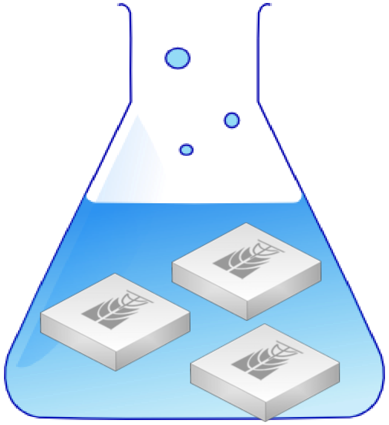
Label #: 0

from Label: 0 to Label: 0

Filter string (optional):

SRC	DST

```
[25] MPLS: Got new MPLS communication: d4:ca:6d:2f:e4:3c -> d4:be:d9:1e:49:b3
```



Pause for Hands On!

Breaking into OSPF, BGP and MPLS

Attacks against MPLS VPNs

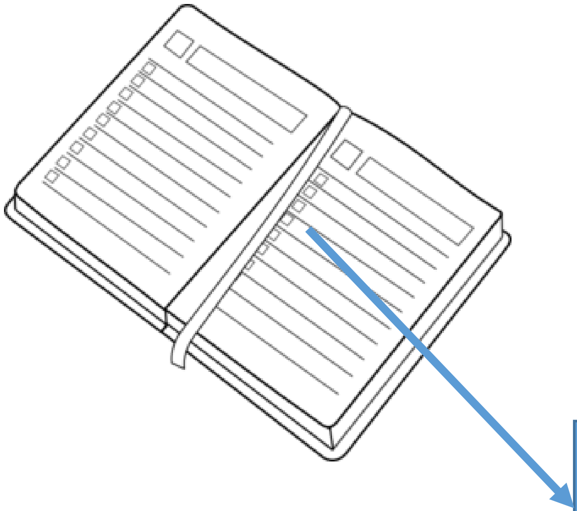
Tools exist for any kind of attack.

The success of an attack will depend basically on:

- → Position of the attacker
- → Topology of the network
- → How the devices are managed

Only **good practices** can make the Trusted Zone really trustable!

Agenda



- Introduction and Motivations ✓
- MPLS and VPNs Background ✓
- Layer 2 and Layer 3 VPNs configurations ✓
- A Working Scenario ✓
- MPLS VPNs Threats / Hands on ✓
- Defenses – Good practices and recommendations
- Conclusions

Good practices and recommendations

1) Operational and devices security

2) Security practices for layer 3 and layer 2 routing and forwarding protocols

3) Topology considerations

4) Using IPSec

Operational and Devices Security

Operational Security (1/2)

Administrators and operators can make mistakes and malicious misconfiguration could also happen. Some guidelines to improve the security:

→ Use RADIUS for router access – no user in the box.

→ Use RANCID to log and notify configuration changes:
http://falz.net/tech/rancid-mikrotik

→ Operators shouldn’t have access to logging facilities.

Operational Security (2/3)

→ Prevent password discovery. Never leave a **.backup** file neither in the box, nor in the cloud, nor in your computer.

See: http://www.mikrotikpassworddiscovery.com

→ Remember that a reset could make a automated backup. Make sure force-backup-booter is disabled.

```
/system routerboard settings set force-backup-booter=no
```

Devices Security

Operational Security (3/3)

→ Follow guidelines for Layer 2 Security

Layer 2 Security - MUM 2010

→ Follow guidelines to routing security

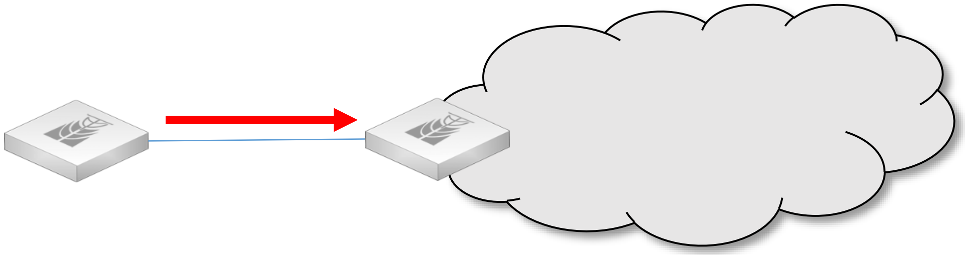
Routing Security MUM 2011

→ Follow general security recommendations

Router OS v6 Security MUM 2013 by Tom Smyth

CE specifics (1/3)

Use preferably static routing on the link CE - PE;



Use BGP on CE-PE only if necessary (multi-homed customer)

Do not use neither OSPF, nor RIP at all

CE Security (2/3)

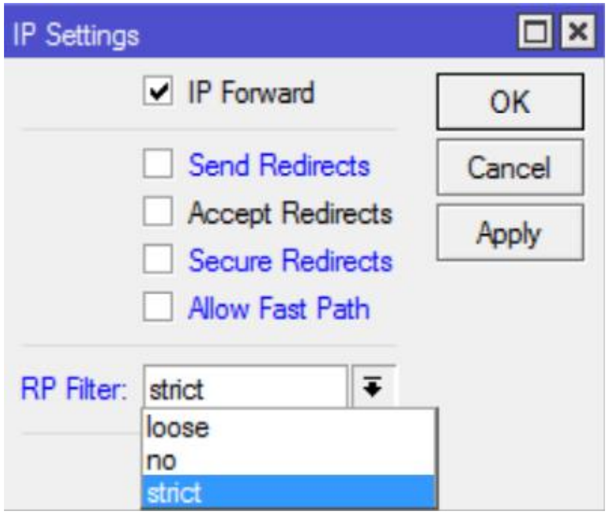
CEs are part of **your** network. Don’t let the customer to take control over it (again take special care on passwords in the box)

Hint → If required give the customer a personal Firewall using Metarouter but keep the main router under your control.

Good practices and recommendations

CE Security (3/3)

Protect network against IP address spoofing by enabling uRFP



IP Settings

☑ IP Forward

□ Send Redirects

□ Accept Redirects

□ Secure Redirects

□ Allow Fast Path

RP Filter: strict

Good practices and recommendations

PE and P specifics

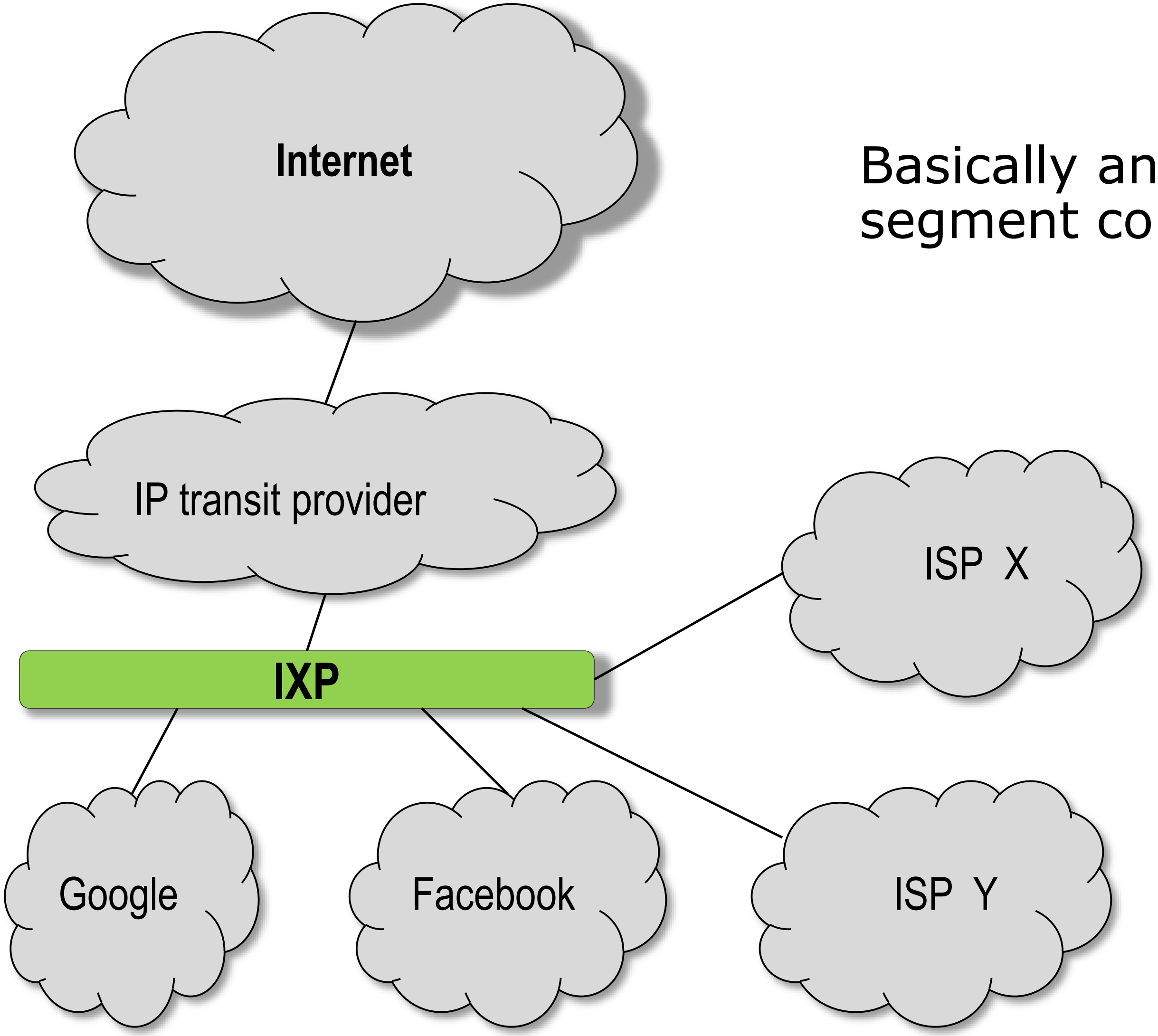
PEs are the most critical point in a MPLS VPN. Never install a PE on customer premises (physical security)

Use all previous configurations for CE (except uRPF)

Deny access from CE on all IP addresses that are not necessary for CE operation;

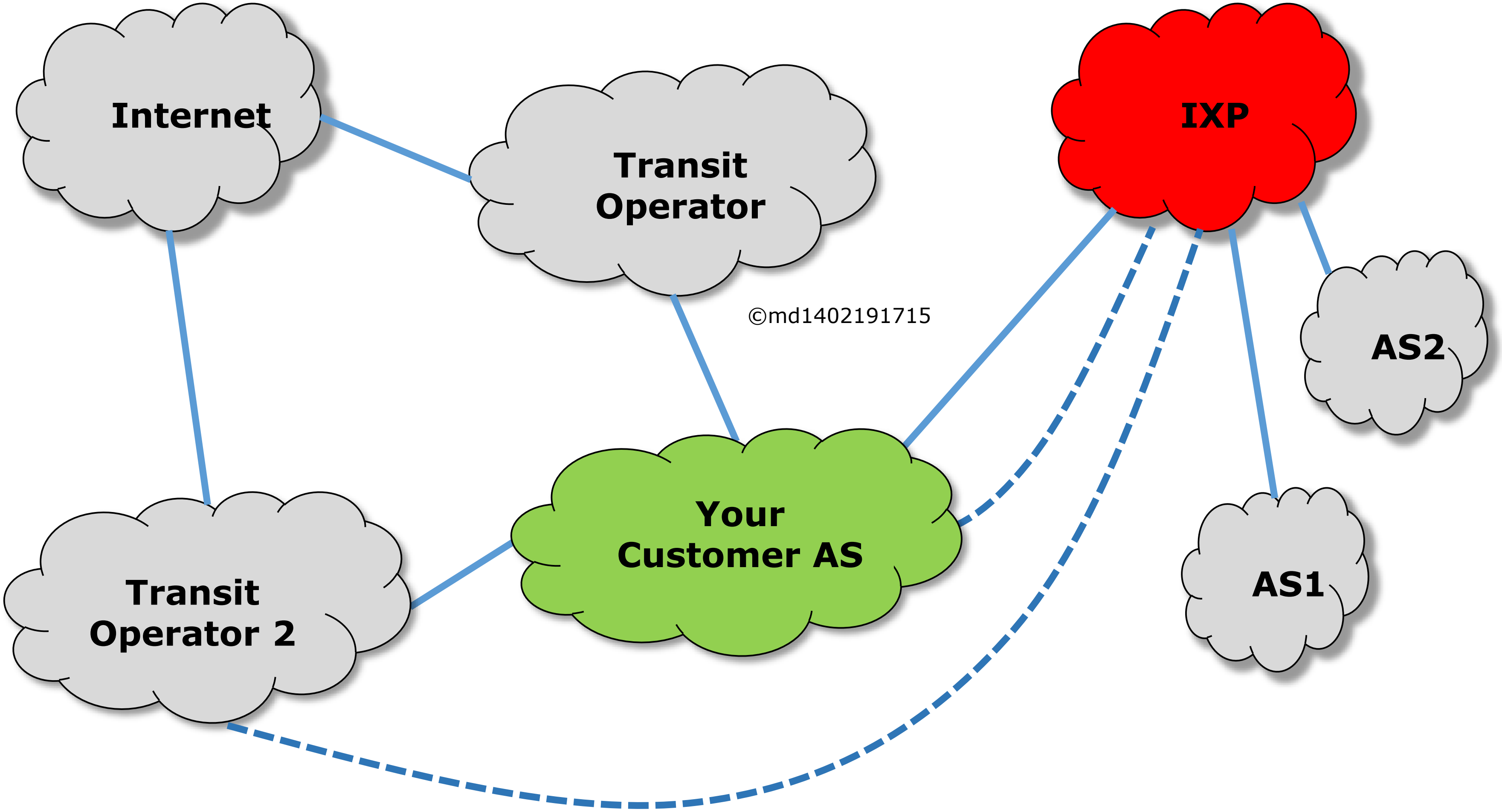
Topology Considerations

Topology considerations (Layer 2 Connections)

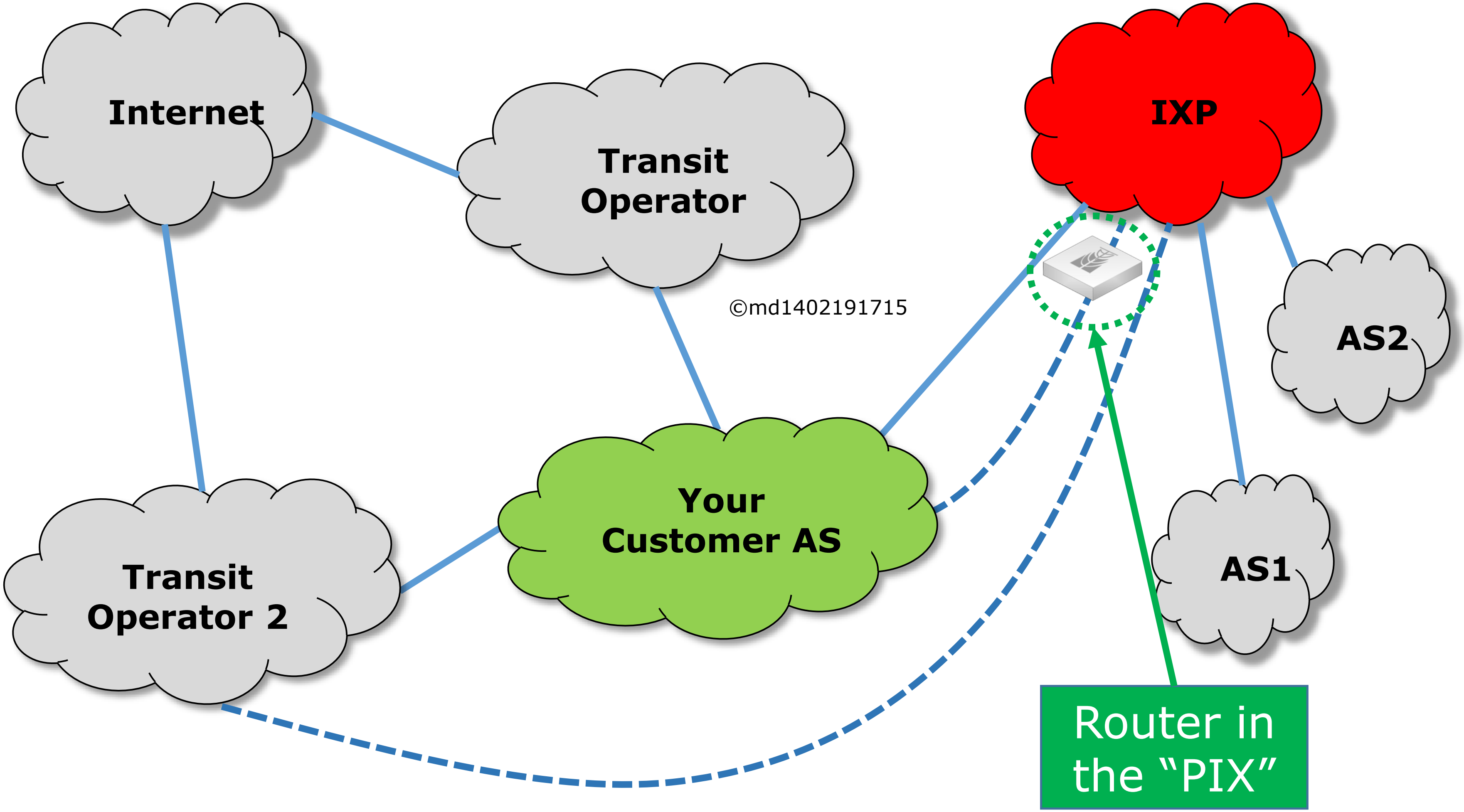


Basically an IXP is a Layer2 segment connecting AS's

Topology considerations (Layer 2 Connections)



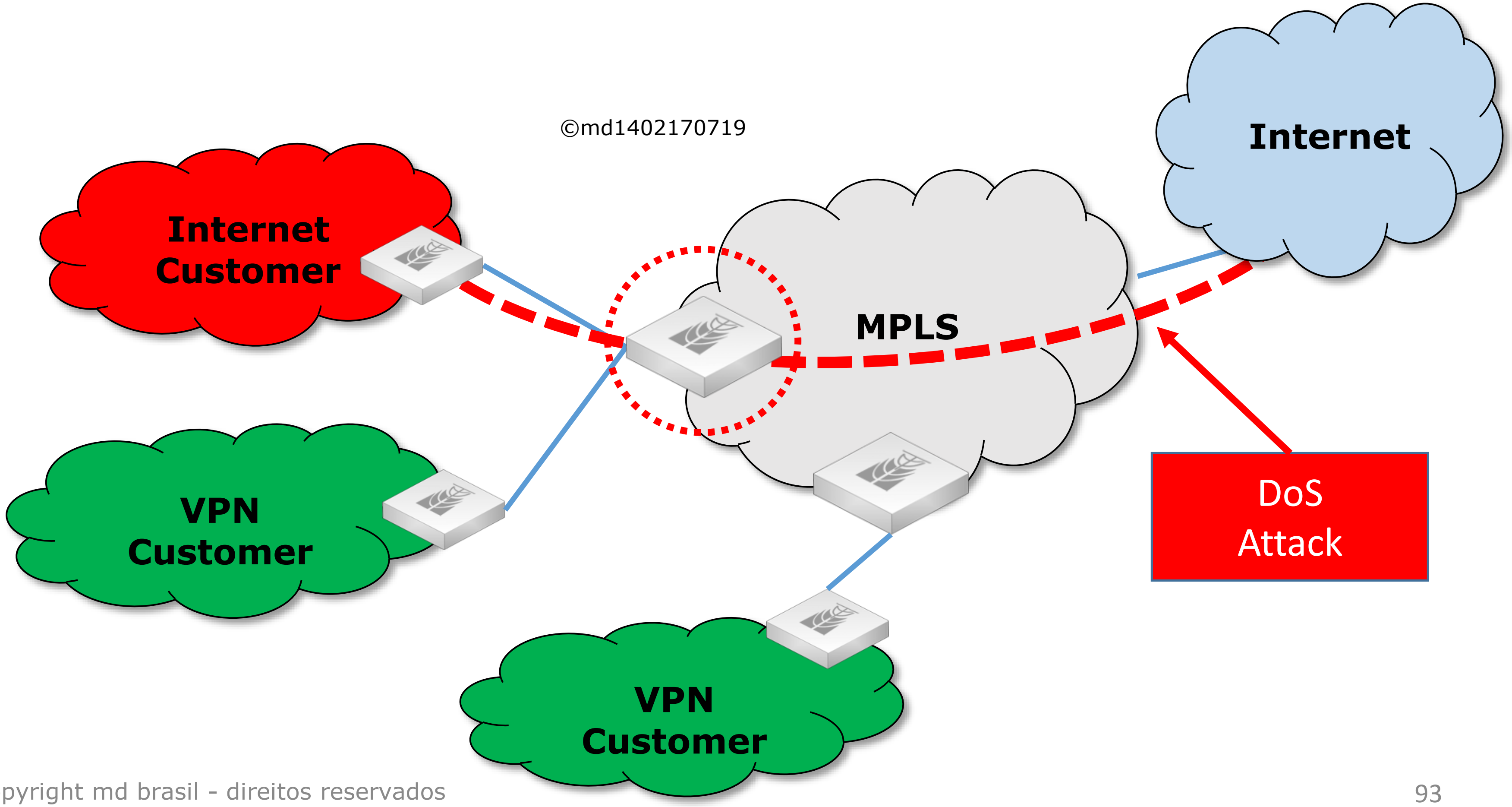
Topology considerations (Layer 2 Connections)



Topology Considerations (Internet Provisioning)

PES have limited resources: CPU, memory and bandwidth;

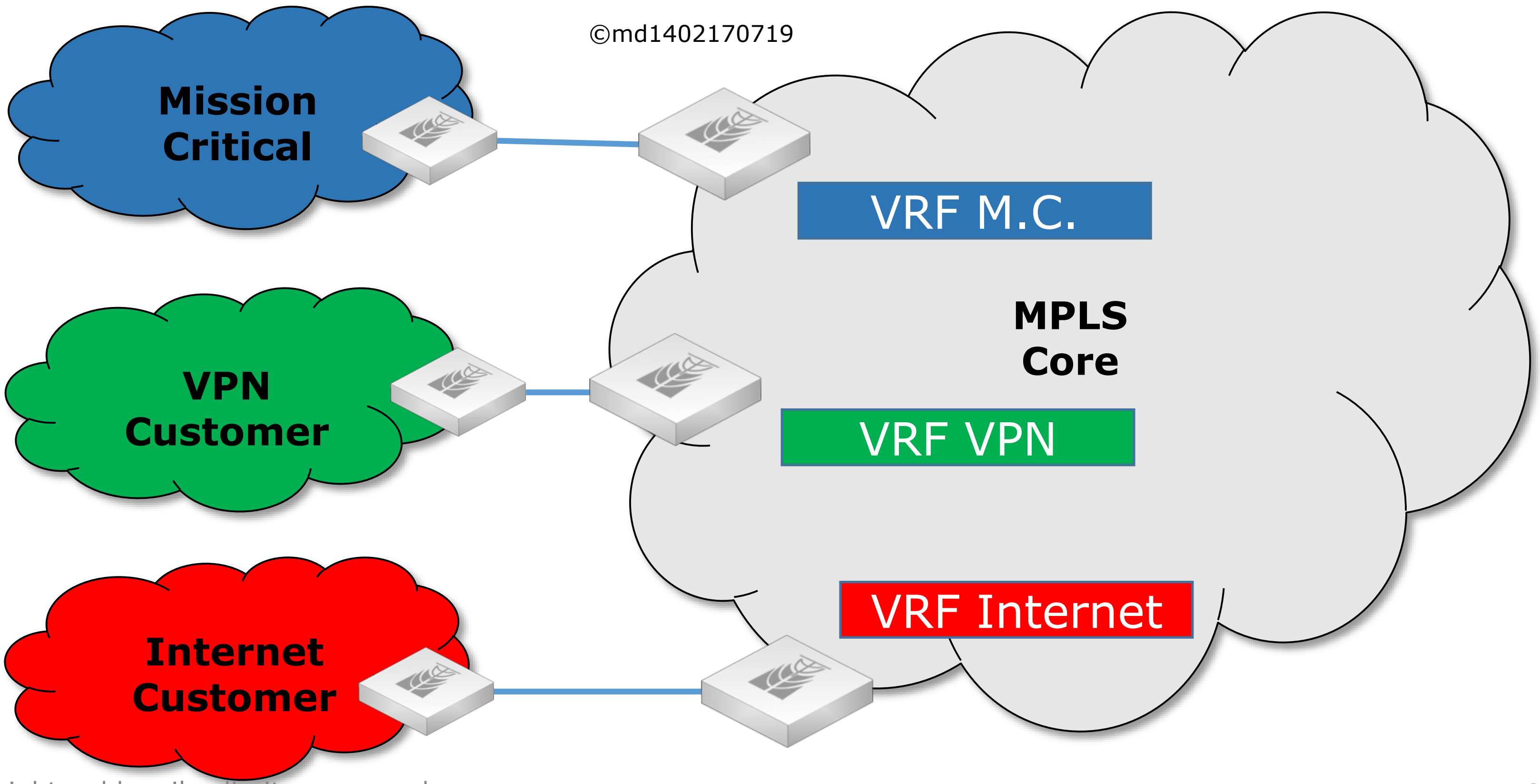
DoS attacks from the Internet can jeopardize VPNs



Topology Considerations (Internet Provisioning)

BCP Recommendation:

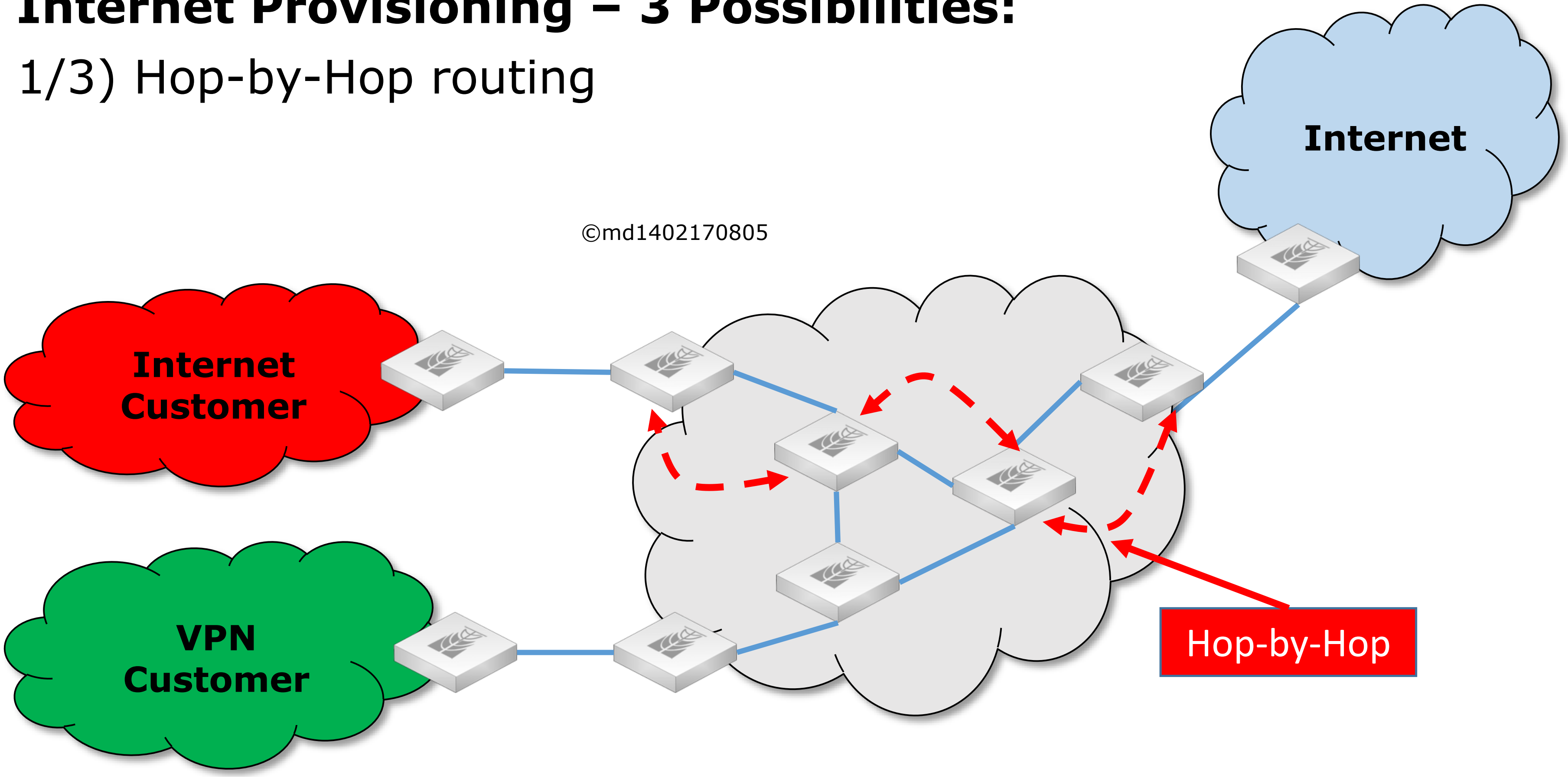
→ PE Routers Should Contain Only VRFs of the Same Security Level.



Topology Considerations (Internet Provisioning)

Internet Provisioning – 3 Possibilities:

1/3) Hop-by-Hop routing

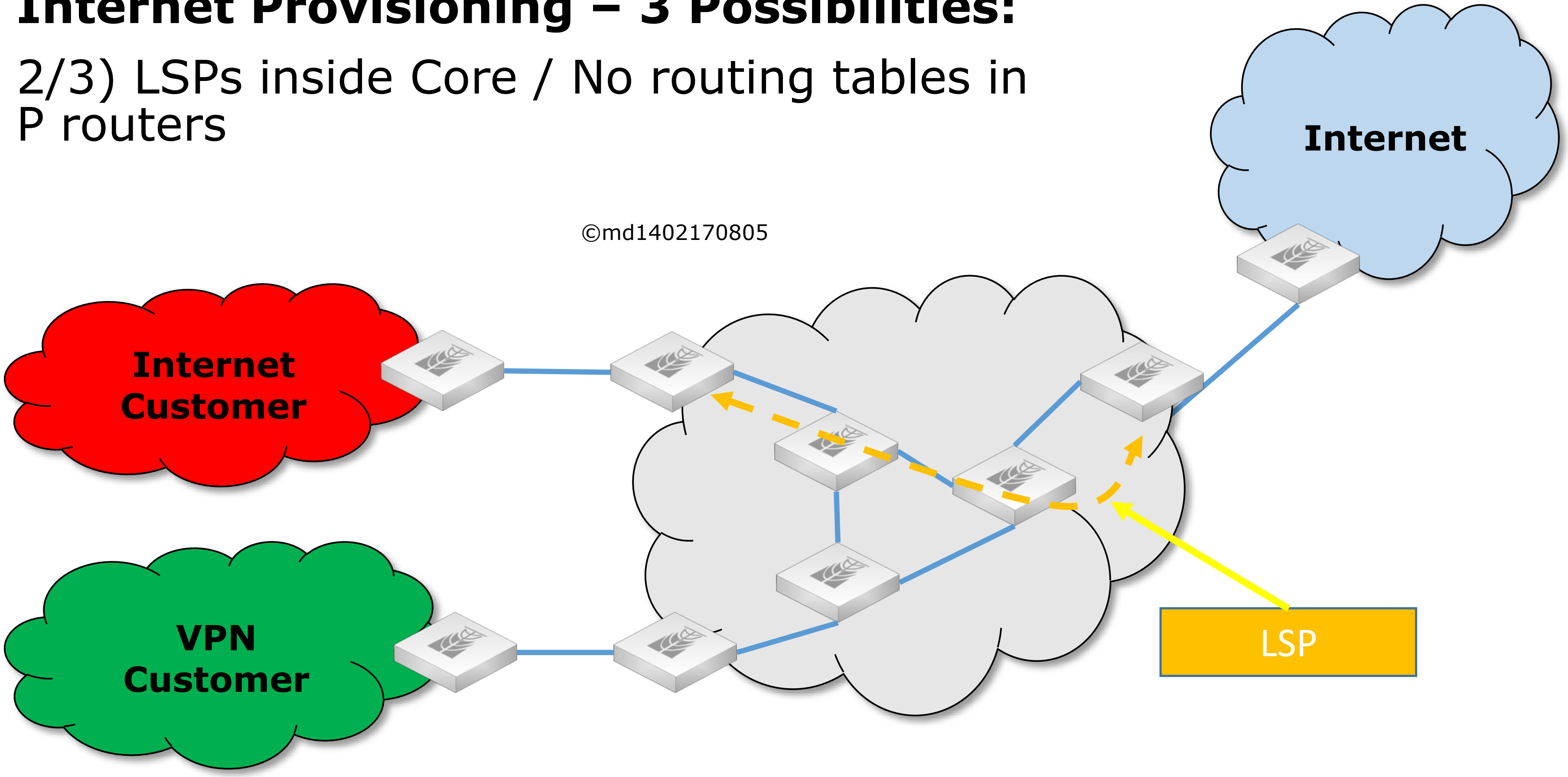


→ Full access to Core from Internet!

Topology Considerations (Internet Provisioning)

Internet Provisioning – 3 Possibilities:

2/3) LSPs inside Core / No routing tables in P routers



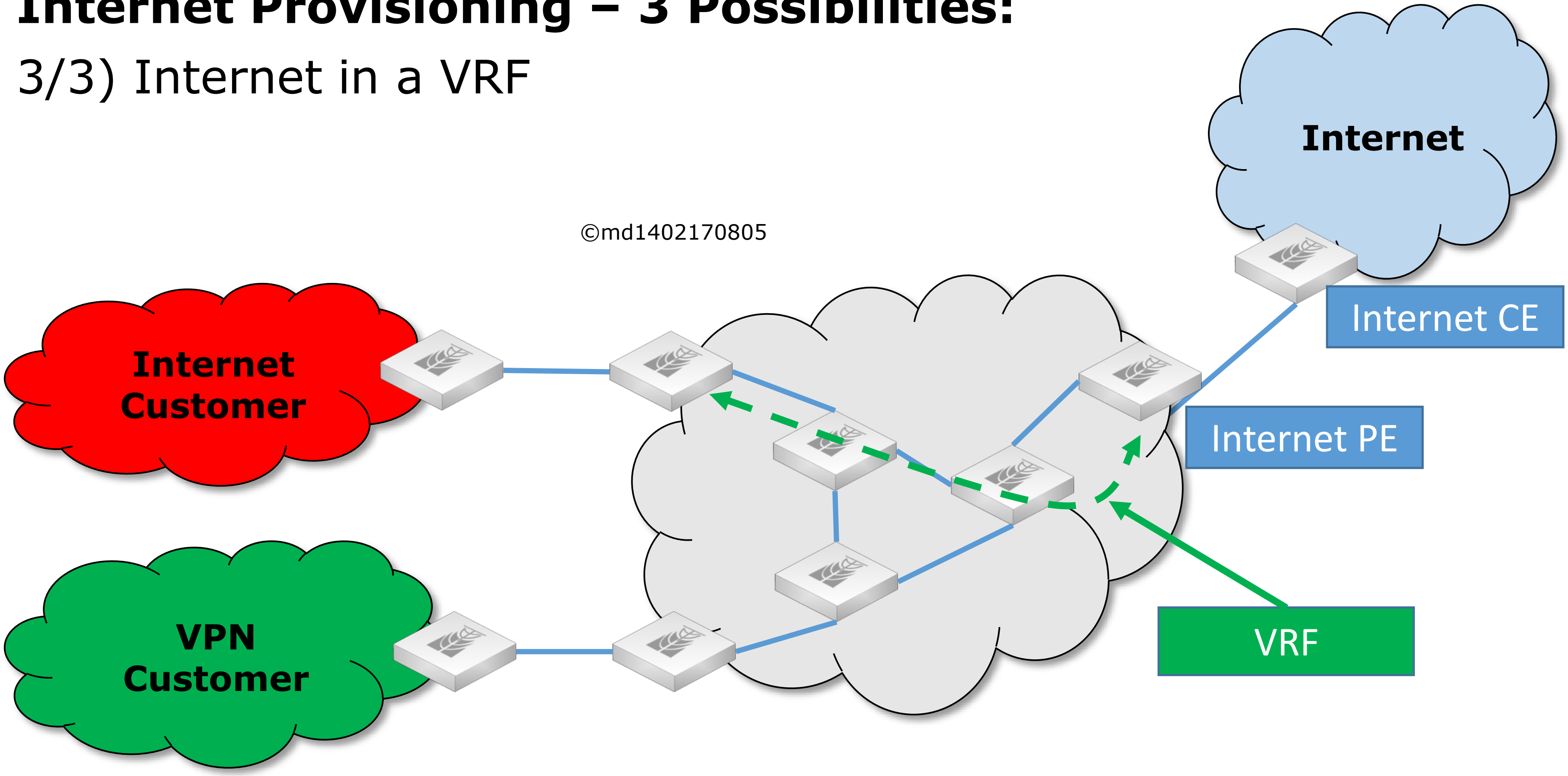
→ Full access to PEs / limited access to Ps from Internet

Topology Considerations (Internet Provisioning)

Internet Provisioning – 3 Possibilities:

3/3) Internet in a VRF

©md1402170805



→ **No access to core from the Internet!**

Securing VPNs with IPSec

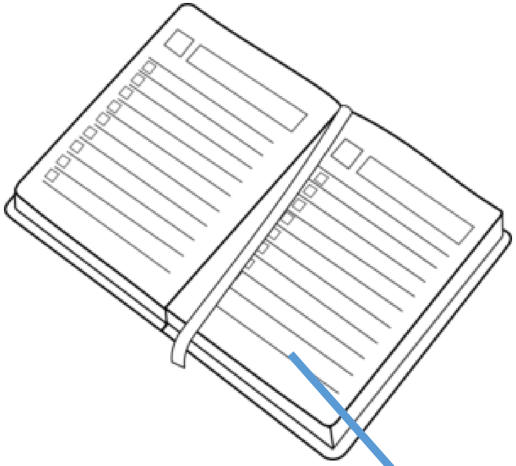
Securing VPNs with IPSec

IPSec configurations is out of scope of this work, but is important to mention that

As a user you can prevent your own security using IPSec between devices near to CEs on both sides

As a provider you can make a more robust network using IPSec between PEs.

Agenda



- Introduction and Motivations ✓
- MPLS and VPNs Background ✓
- Layer 2 and Layer 3 VPNs configurations ✓
- A Working Scenario ✓
- MPLS VPNs Threats / Hands on ✓
- Defenses – Good practices and recommendations ✓
- **Conclusions and references**

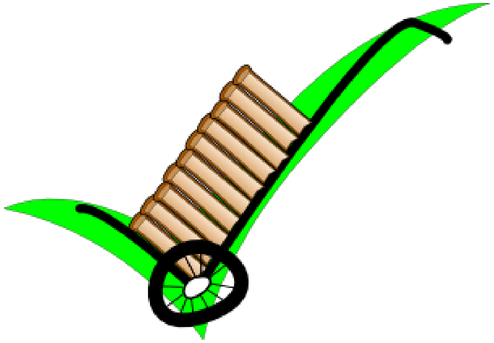
Conclusions

Considering:

- Multiple use of protocols, each one with its particular security issues;
- Diversity or Topologies;
- No intrinsic security for the framework;
- Physical location of equipment not always in real secure places;
- Possible operational issues

To secure MPLS VPNs is not a simple task. Only correct planning and strict operational processes will guarantee a acceptable level of security.

References



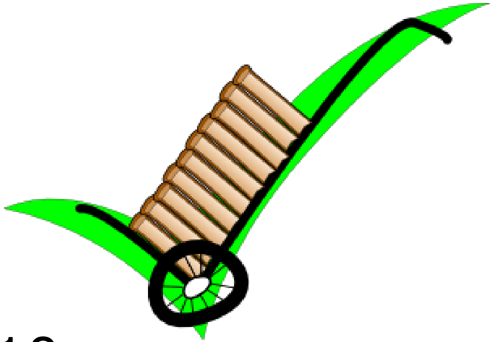
RFC 5920 - Security Framework for MPLS and GMPLS Networks
http://tools.ietf.org/search/rfc5920

RFC 2547 e RFC 2547bis – BGP/MPLS VPNs
http://tools.ietf.org/html/rfc2547.html

Security of the MPLS Architecture [MPLS] - Cisco Systems
http://migre.me/hYcet

MPLS Workshop – APRICOT 2012
http://migre.me/hXXSC

References



Book: MPLS VPN Security (Self Study Guide)
Behringer, Michael H. and Morrow, Monique J

An Introduction to the tool Loki – Blackhat 2010
Rene Graff, Daniel Mende, Enno Rey

Attacking Internet Backbone Technologies – Blackhat 2009
Rene Graff, Daniel Mende, Enno Rey

Tools:
Loki: http://c0decafe.de
Yersinia: http://www.yersinia.net
Scapy: http://www.secdev.org/projects/scapy/
Dsniff: http://www.monkey.org/~dugsong/dsniff/

Download Now

This presentation will be available on Mikrotik Web Site and at the below URL:

www.mikrotikbrasil.com.br/artigos

Grazie!