MPLS and VPLS Security

Enno Rey, erey@ernw.de

Agenda

- MPLS Basic Terms & Technology
- MPLS VPNs
- “Layer 2 VPNs“
- Virtual Private LAN Service (VPLS)
- A look at the future

Who I am

- “Old-school networker“
- Started working on Layer 2–4 in the early 90s
- With special focus on security since 1997
- Founder (2001) and CTO of a highly specialized IT security consultancy with 10 employes, located in Heidelberg/Germany (+ office in Lisbon)
- (Co-) Author of a book about pen-testing & regular speaker

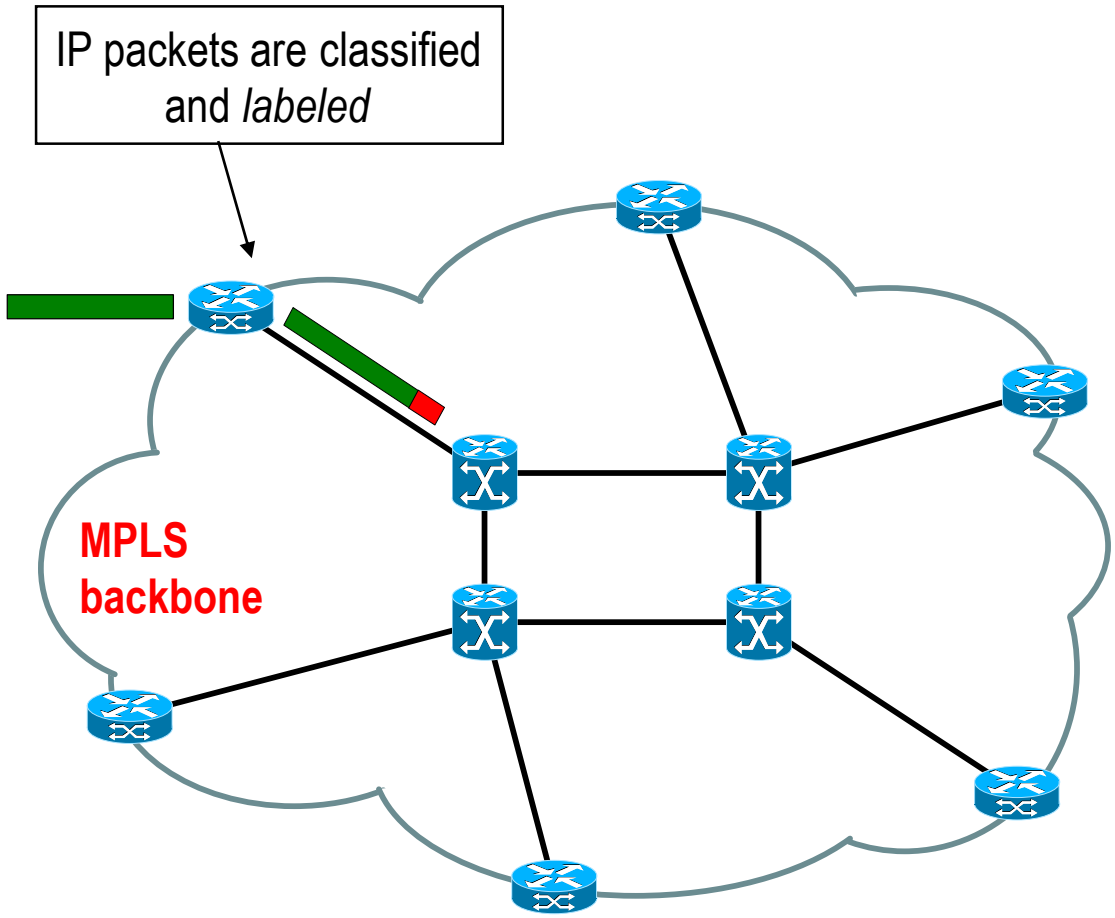
MPLS Basics

- *Multiprotocol Label Switching* [RFC 3031 et.al.]
- Technology used for forwarding packets, based on *Labels* (see below). Packets may carry multiple labels (for different purposes).
- Initial goal: more efficient forwarding than IP-based routing
- Used in most carrier backbones
- Serves as foundation for some '*Advanced Services*'

Tag ('Label') = 20 bits
S = Bottom of Stack, 1 bit

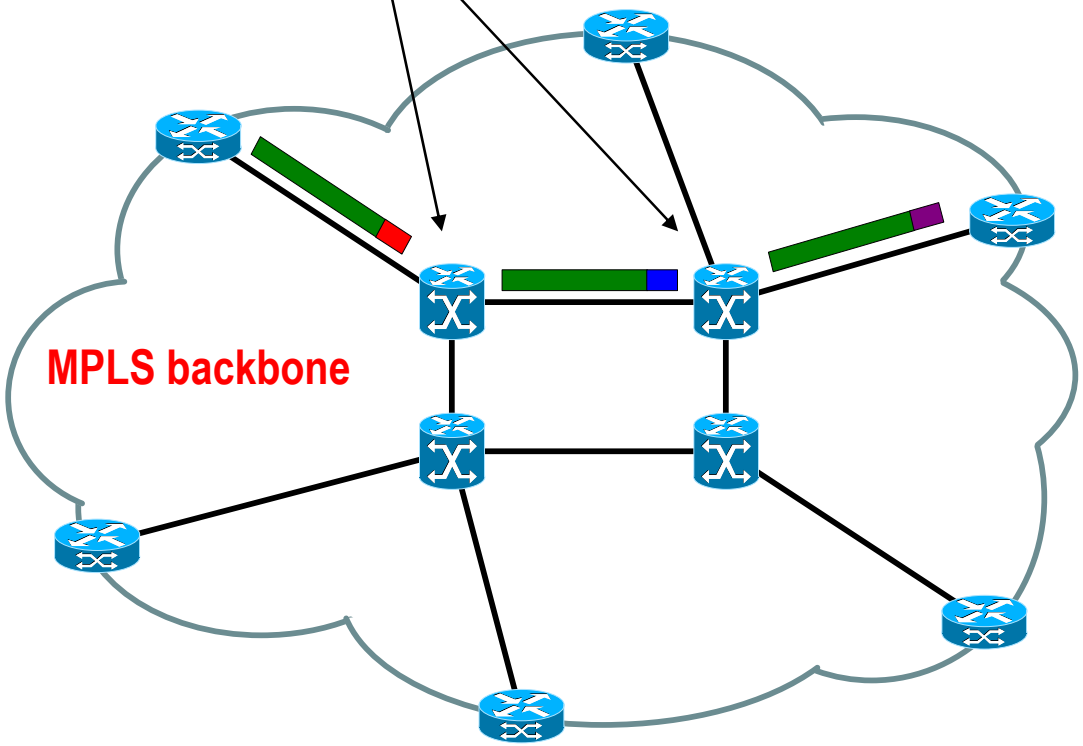
COS/EXP = Class of Service, 3 bits
TTL = Time to Live, 8 bits

MPLS Basics



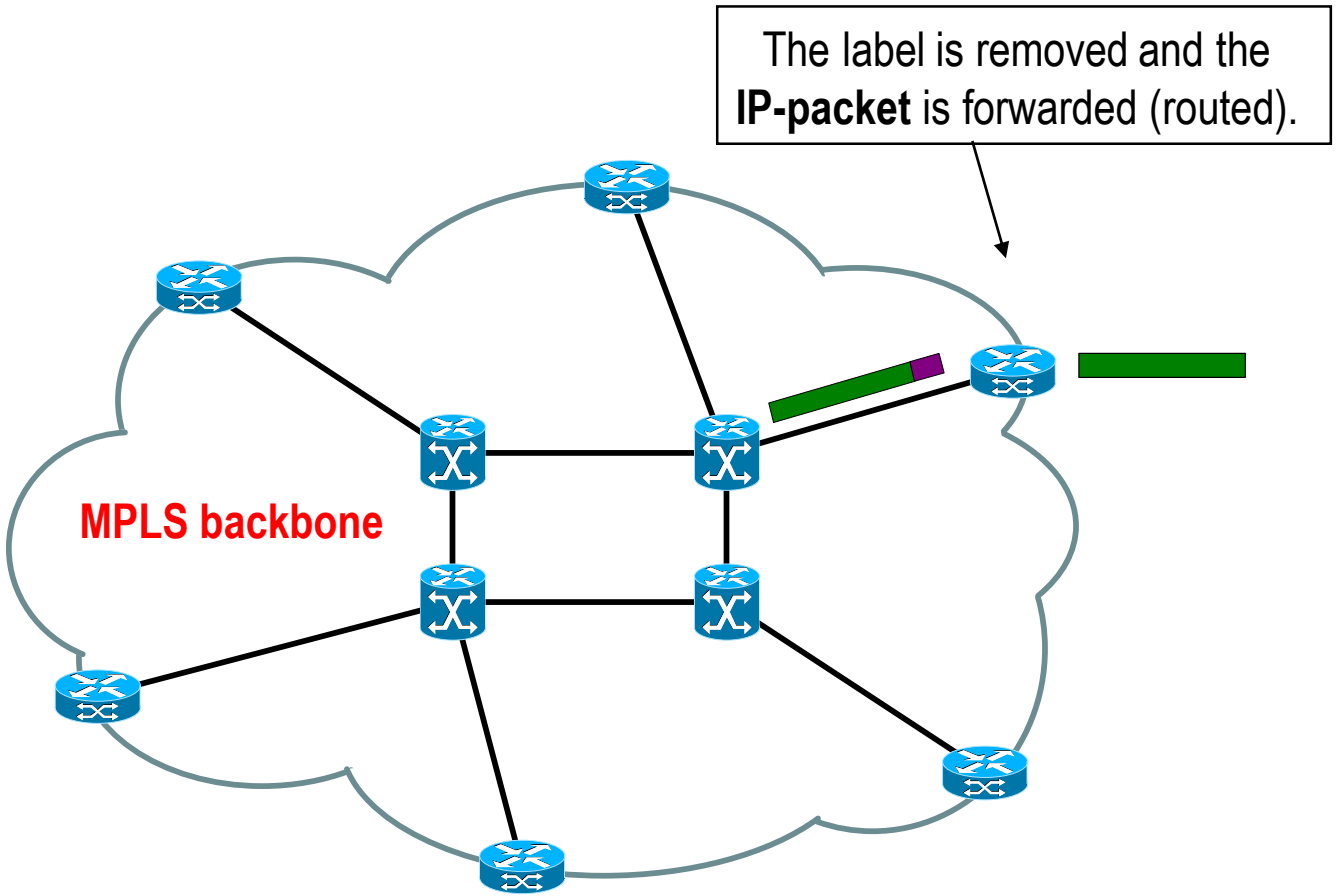
MPLS Basics

In the backbone packet forwarding is done based on labels. The **red** label is swapped for a **blue** label, the **blue** one for a **purple** one.



Note: for simplicity‘s sake we‘ll neglect *pen-ultimate hop popping* here.

MPLS Basics



In this scenario, we'll call them 'forwarding labels' (as that's what they serve as here).

Security discussion

- The first thing joe hacker thinks of when speaking about some forwarding (“routing“ or “router‘s“) technology is… ‚spoofing or injection‘.

  Btw: this approach is a bit naïve… or have you ever seen a successful ‘ospf injection attack’?

- But: the just discussed ‘forwarding labels‘ have local significance only. Two neighboring peers agree on their significance by means of some *label distribution protocol*.

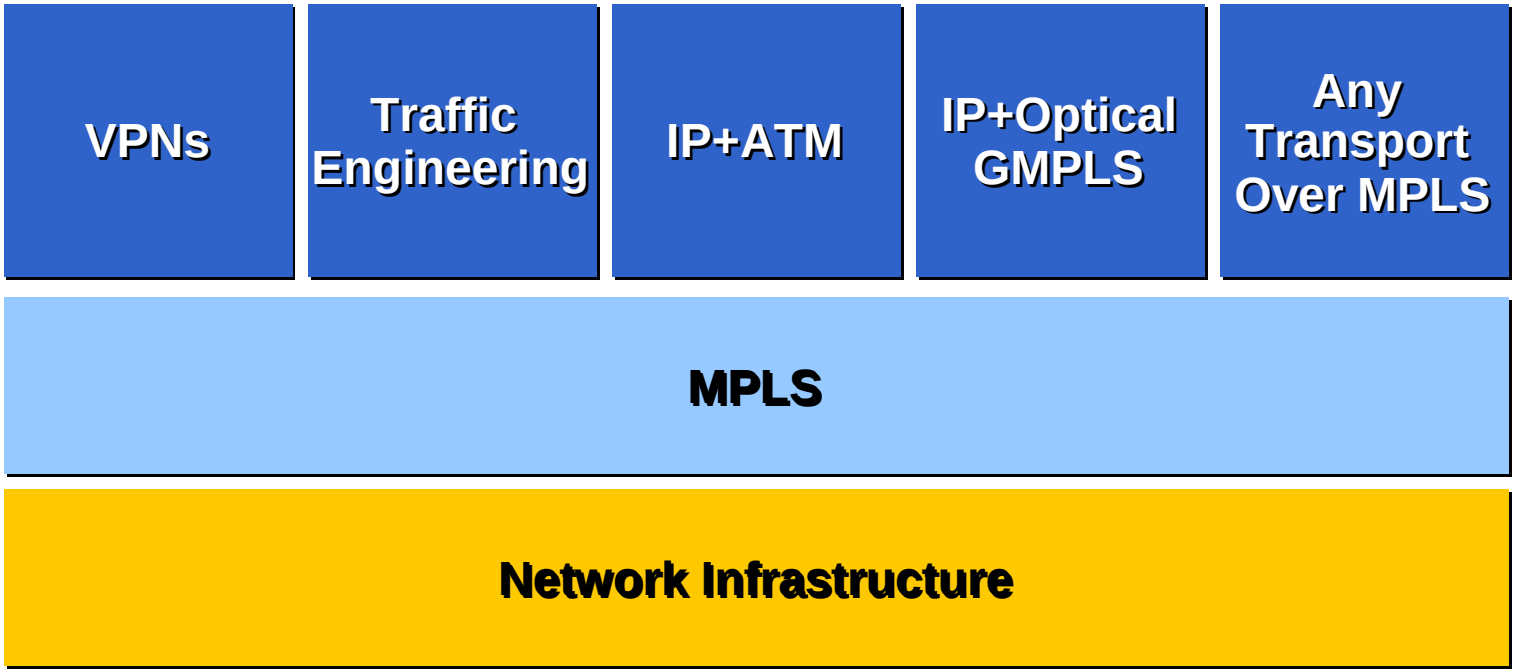
- So injecting/modifying ‘forwarding labels‘ would not allow much profit…

- However, those nice little shiny labels can serve many other purposes…

MPLS Services

- VPNs (“Layer 3“ or “Layer 2“)
- *Any Transport over MPLS*
- *Virtual Private LAN Service*
- MPLS Traffic Engineering
- *Generalized MPLS* (GMPLS)

MPLS as a Foundation for Advanced Services

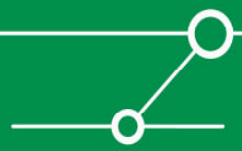


MPLS Services

- Some of these technologies (e.g. Traffic Engineering) are relevant for ISPs/carriers only.
- Others (“Layer 3 VPNs“, “Layer 2 VPNs“) may be rather important for organizations. Either for customers of a backbone provider or for use in campus networks.
- Increasingly “Layer 3 MPLS VPNs“ are used in enterprise networks, for traffic separation/segmentation
  (kind of “modern VLAN technology“).

MPLS VPNs (“Layer 3 VPNs“)

- MPLS-based technology [mainly RFCs 2547 & 2917] with it‘s own concepts and terminology.
- Comparable to Frame Relay/ATM in some respects.
- Highly ‘virtual‘ technology (shared infrastructure, separated routing).
- Additional (MPLS-) labels are used to establish logical paths/circuits for the traffic of single customers.
- Very flexible with regard to topologies (by means of *route targets*).



MPLS VPNs – Terminology

P network (Provider network)

- The ISP‘s backbone

P router (Provider router)

- Backbone router of ISP

PE router (Provider Edge router)

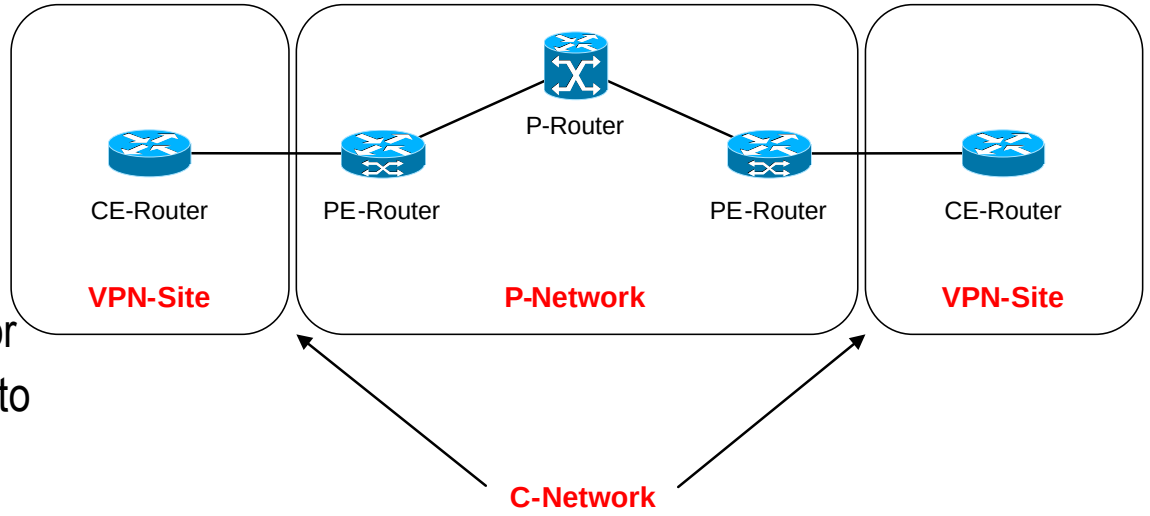
- ISP‘s router responsible for connecting the CE device to MPLS backbone

C network (Customer network)

- The customer‘s network

CE router (Customer Edge router)

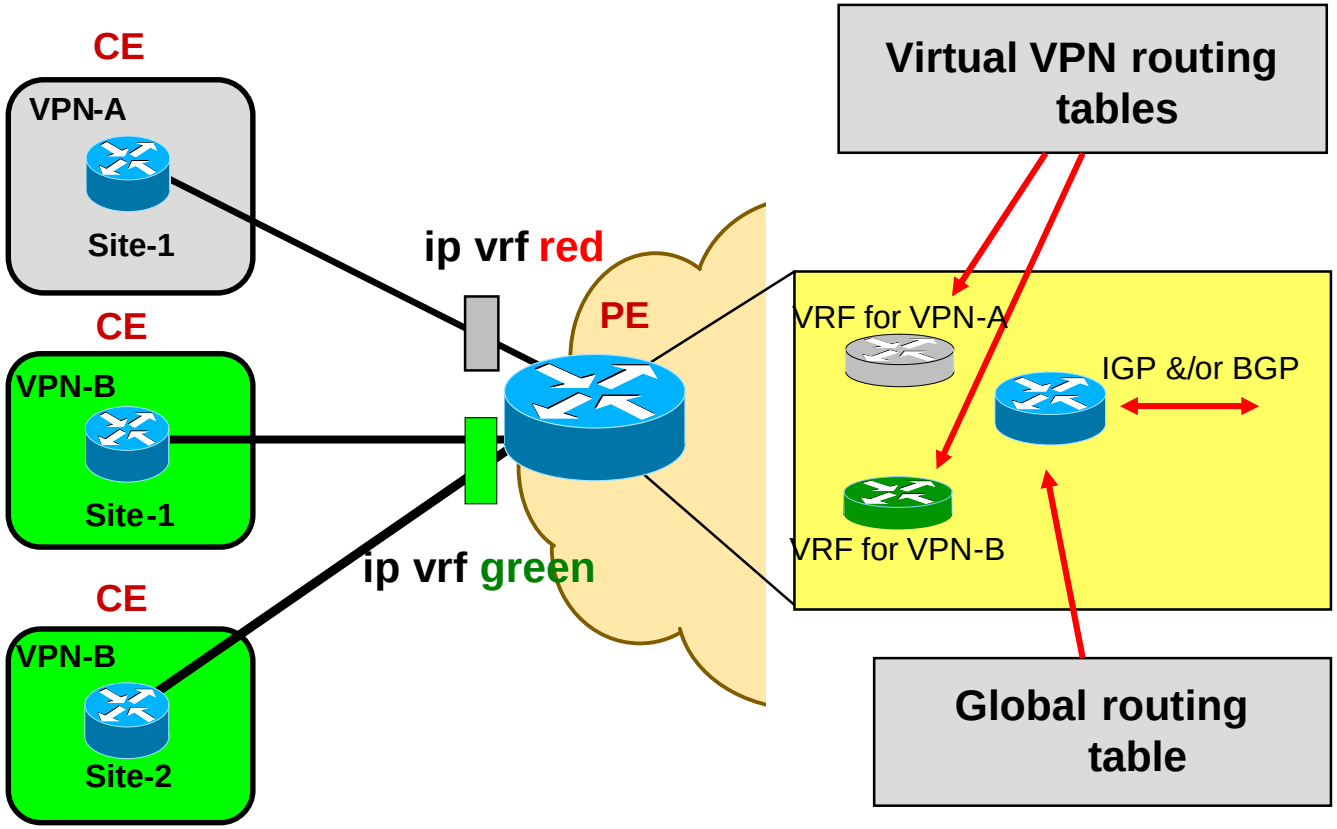
- Router connecting the C network to the PE (may be under control of customer or ISP)



During transport two labels are used: one to identify the ‘egress PE‘, the other one to identify the customer/a particular VPN.

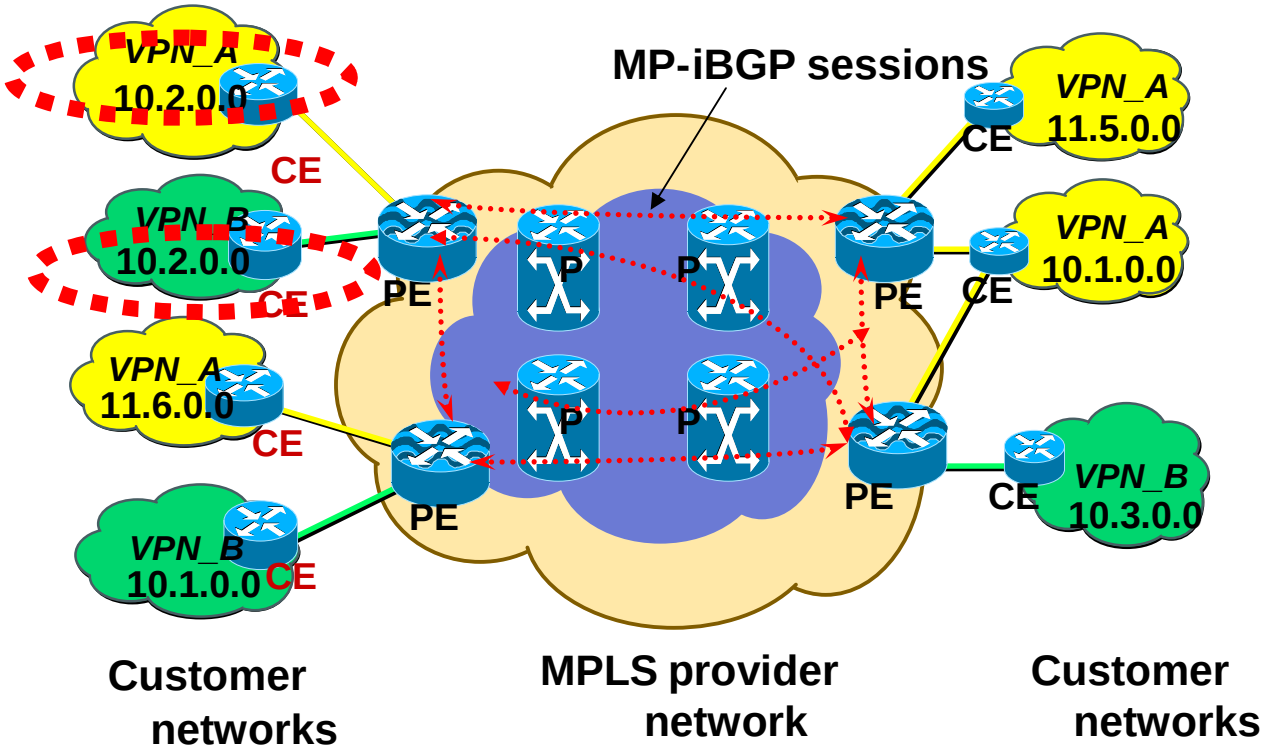
MPLS VPNs ("Layer 3 VPNs")

- 'Shared' router handles different VRFs



MPLS VPNs (“Layer 3 VPNs“)

A more complex view



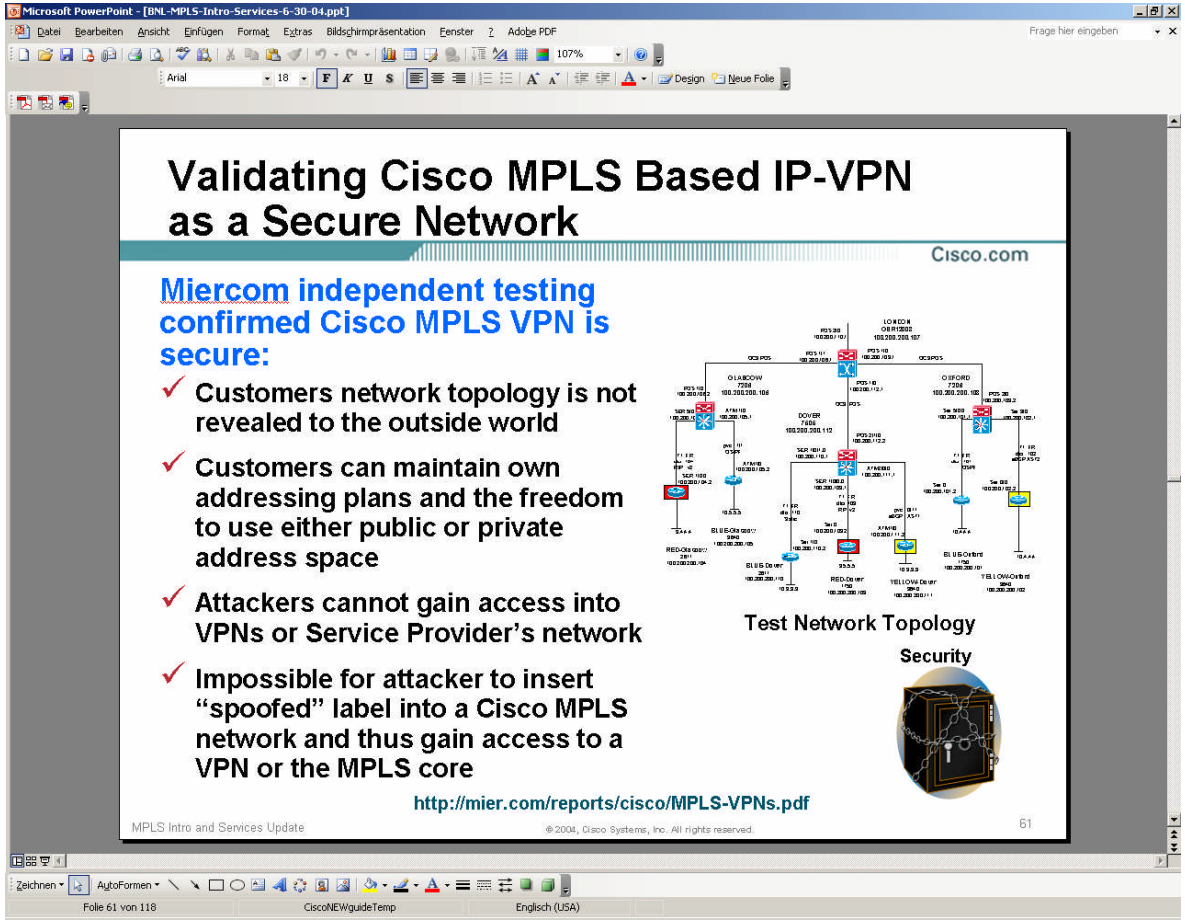
What happens here in detail

- PE routers assign labels to prefixes per VPN (*route distinguisher*).
- This information (label, route distinguisher, prefix) is then exchanged between PEs by *Multiprotocol BGP* [RFC 2283].
- => 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) two labels:
  - one ‘forwarding label‘ for transport to the egress PE across the backbone.
  - a second one identifies the VPN (and prefix) of the destination.
- In short: “labels do the whole VPN thing here“.

Security – the ‘official point of view‘

from ([1])



Security – you should consider...

- No encryption
- PE device (usually) is shared with other customers.
- What about internal audit requirements?

  => Risk assessment needed
- You all certainly knew these things ;-)

- Let‘s talk about possible attacks then…

Attacks against MPLS VPNs

Given it‘s a ‘VPN‘ technology, interesting attacks include eaves-dropping and/or unauthorized access. We are not interested in DoS…

- Injection of (pre-) labeled traffic from a CE
- Injection of (pre-) labeled traffic from the internet
- Modification of MP-iBGP sessions to establish ‘incorrect VPNs‘
- Label modification/injection in the backbone
- Attacks against management tools/boxes

Attacks against MPLS VPNs

Injection of labeled traffic from a CE
(Customer A tries to insert packets into Customer B‘s VPN)

- **According to RFC 2547 “labeled packets are not accepted by backbone routers from untrusted or unreliable sources”.**

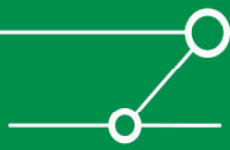
  => a PE should discard labeled packets arriving from CEs
  (as those are ‘untrusted’).

- **This seems to be true (tested against Cisco routers).**

Attacks against MPLS VPNs

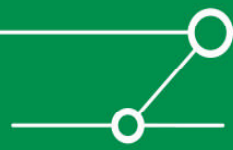
Injection of labeled traffic from the internet
(internet based attacker tries to insert packets into some customer's VPN).

- **Requires:**
  - knowledge of IP addresses and labels, e.g. by simple guessing (not too difficult).
  - reachability of PE or P-router from the internet
  (depending on design probably more difficult).
  - transport of labeled packet from origin to router in question (not clear).
- **As of RFC 2547 (see above) such packets should be discarded anyway (given their 'untrusted origin').**
  However *Behringer/Morrow* state this attack is possible under certain conditions/with certain Cisco IOS versions [5].
- **We tested against some current *IOS Service Provider images*… without success.**



Label bruteforcing (tool at [4])

```
mpls-lbf(1)



NAME
       mpls-lbf - a MPLS LSP label brute-forcer

SYNOPSIS
       mpls-lbf  -m hw_addr -d hw_addr -s IP -t IP -p port -o port -l maxlabel
       [-l maxlabel]

DESCRIPTION
       mpls-lbf is a small tool which sends a series of TCP SYN packets  to  a
       specified  port  on  a specified (fixed) host, and labels these packets
       with MPLS labels. The labels are encoded in the TCP sequence number  in
       such a way that the expected SYN ACK or RST reply can be used to recon-
       struct the labels along the LSP traversed by the TCP SYN packets.

       If the this label enumeration is carried out from the core, it might be
       used  as  an information gathering tool, which can then be used in con-
       junction with mpld-fwd to forward  MPLS-labelled  traffic  outside  the
       core.

       It  makes  sense to set up a sniffing device that receives this traffic
```

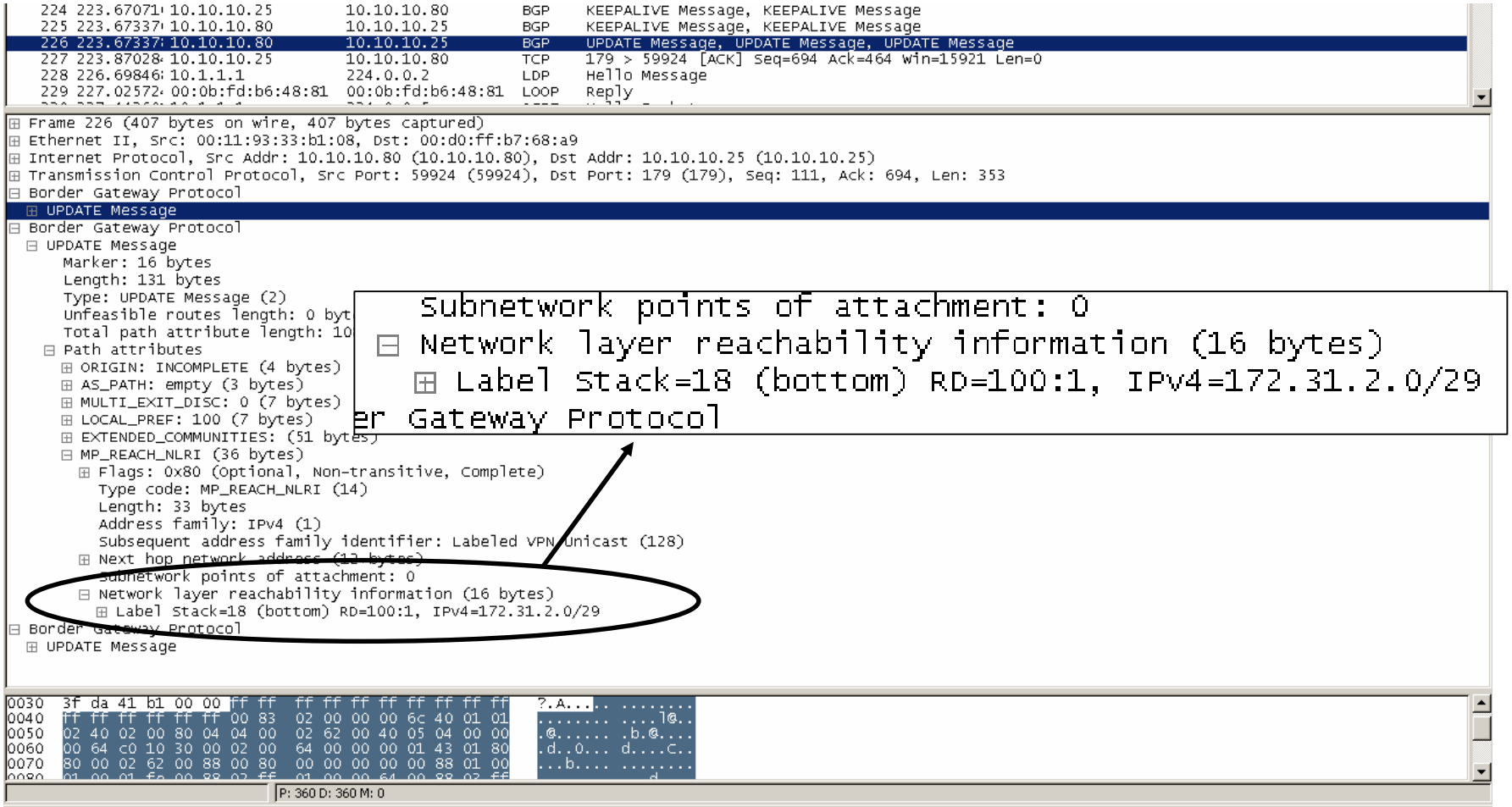


Attacks against MPLS VPNs

Modification of MP-iBGP sessions to establish ‘incorrect VPNs‘

- Definitely possible (with potentially broad impact).
- Requires:
  - access to core (debatable, see below).
  - the right tools at point of attack
    (may be difficult, as point of attack is probably a router)
- As BGP information is not updated regularly, an attacker will
  - either have to be able to intercept the inital MP-BGP exchange
  - or have to withdraw VPN routes (BGP update with other *NLRI*) and insert new ones.
- Both scenarios may be difficult to obtain.

MP-BGP session



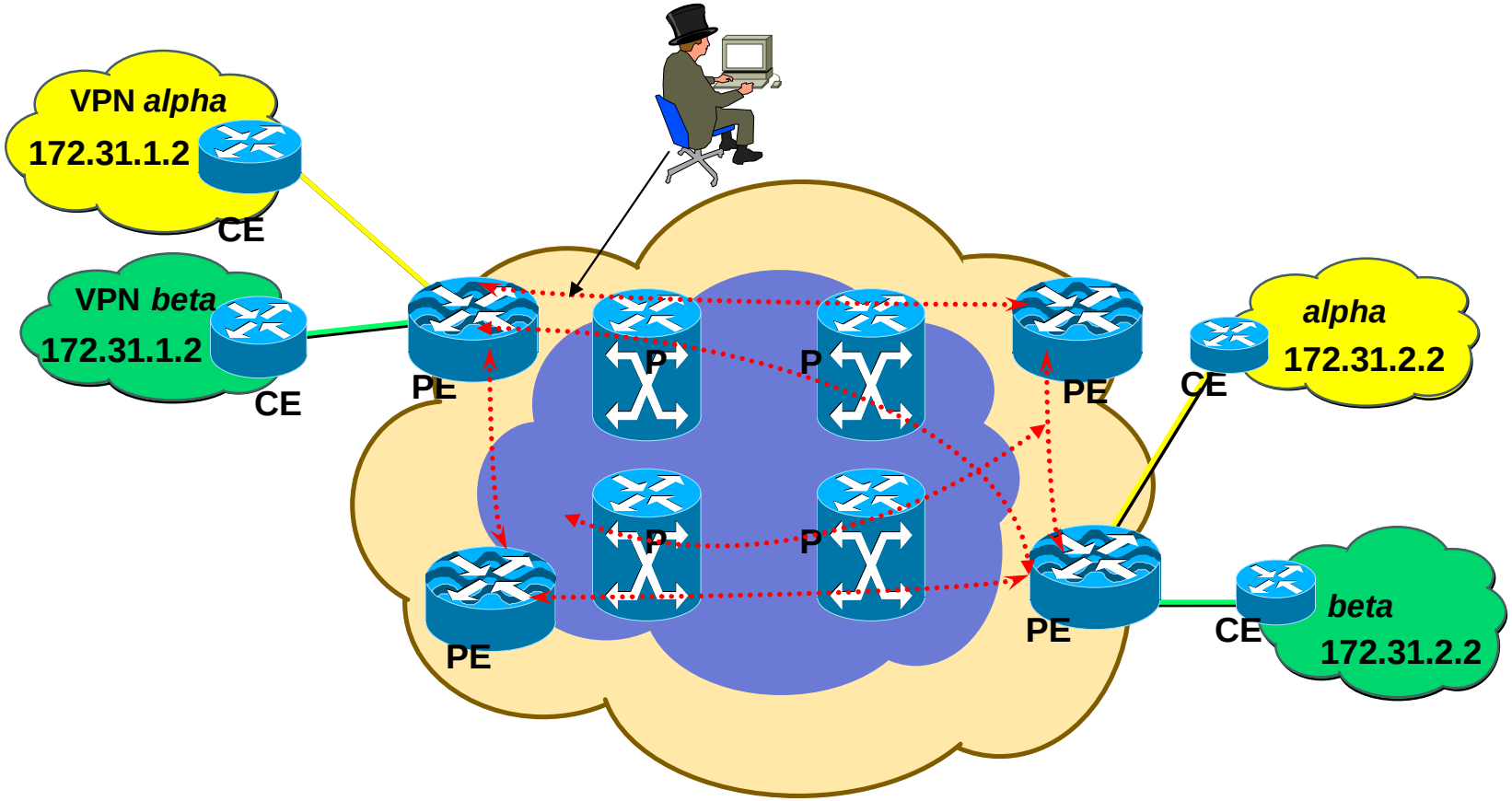
Attacks against MPLS VPNs

Modification of label in the core to insert packets into VPNs

- Requires:
  - access to core (debatable, see below).
  - the right tools at point of attack
    (may be difficult, as point of attack is probably a router).

- If these requirements are met… the attack itself is easy.

Attack scenario

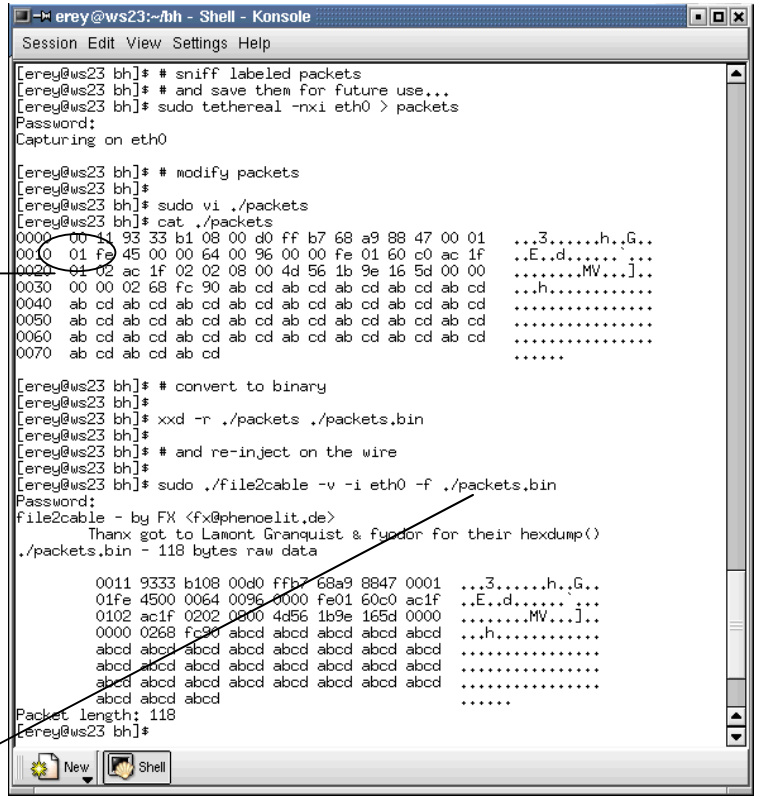


Label modification/injection in the backbone

(1) These are the labels on one PE

```
pe_7204vxr>sh ip vp vpnv4 vrf alpha labels
   Network          Next Hop      In label/Out label
Route Distinguisher: 100:1 (alpha)
   20.20.20.21/32   10.10.10.25     nolabel/17
   20.20.20.40/32   172.31.2.2      19/nolabel
   172.31.1.0/29    10.10.10.25     nolabel/18
   172.31.2.0/29    0.0.0.0         17/aggregate(alpha)
   192.168.5.0      10.10.10.25     nolabel/19

pe_7204vxr>sh ip bgp vpnv4 vrf beta labels
   Network          Next Hop      In label/Out label
Route Distinguisher: 100:2 (beta)
   172.31.1.0/29    10.10.10.25     nolabel/20
   172.31.2.0/29    0.0.0.0         16/aggregate(beta)
```

(2) Here packets from VPN *alpha* are sniffed + ‚re-labeled' as belonging to VPN *beta*

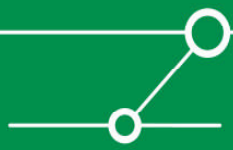


(3) This is a tcpdump from a system in VPN *beta* that first gets pinged 'normally' and then receives the re-labeled ping from VPN *alpha*

```
01:55:45.993783 IP 172.31.1.2 > 172.31.2.2: icmp 40: echo request seq 17408
01:55:45.993815 IP 172.31.2.2 > 172.31.1.2: icmp 40: echo reply seq 17408
01:55:46.995175 IP 172.31.1.2 > 172.31.2.2: icmp 40: echo request seq 17664
01:55:46.995211 IP 172.31.2.2 > 172.31.1.2: icmp 40: echo reply seq 17664
01:55:47.996723 IP 172.31.1.2 > 172.31.2.2: icmp 40: echo request seq 17920
01:55:47.996756 IP 172.31.2.2 > 172.31.1.2: icmp 40: echo reply seq 17920

01:59:14.136855 IP 172.31.1.2 > 172.31.2.2: icmp 80: echo request seq 5725
01:59:14.136906 IP 172.31.2.2 > 172.31.1.2: icmp 80: echo reply seq 5725
```

Conclusions

- Label modification & subsequent “VPN hopping“ can be done.
- It‘s a one-way street, though
  => can only be used for ‘stateless attacks‘ (e.g. via SNMP) or UDP-based worms
- Note: attacks will go undetected as there‘s no checksum or sth.
- Modifying MP-BGP packets may offer road to more efficient attacks. But probably more difficult to perform.
- Both attacks require ‘access to core‘.

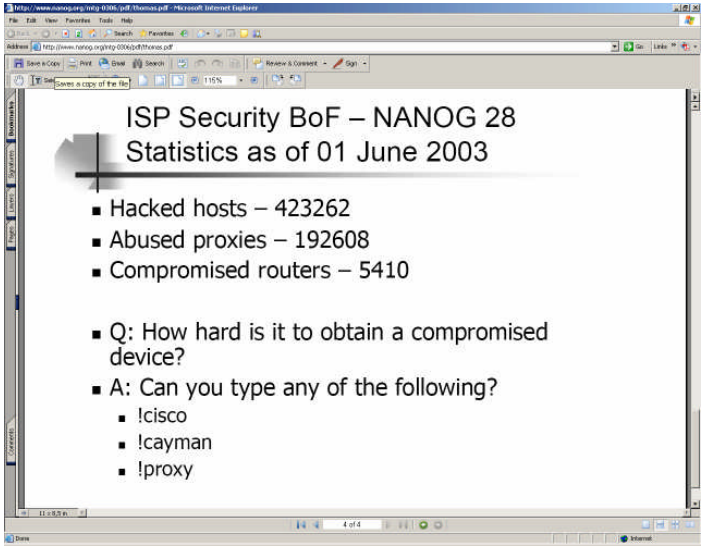


Access to core

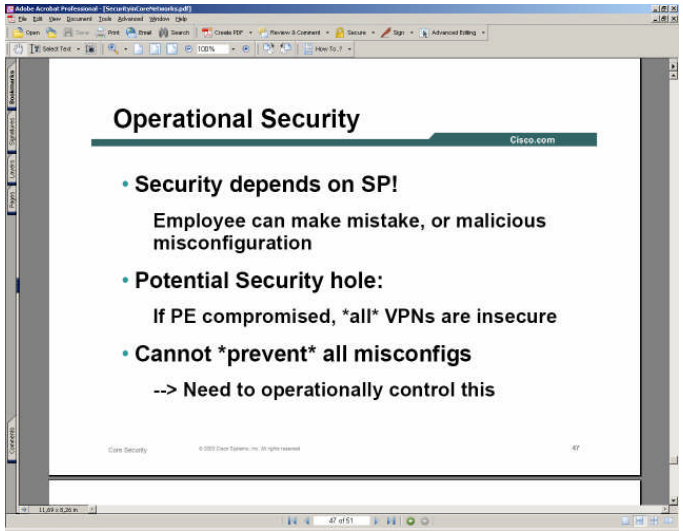
In most security discussions the core is assumed to be trusted (e.g. [1]).

This sounds a bit naïve, however I tend to agree. But:

- MPLS VPNs are used more and more in campus networks.
- Providers may be connected via IXPs.
- And:



from [2]



from [3]

Comparison to FR/ATM

"Attacking VPNs from within the core was possible with FR/ATM as well."

True, but..

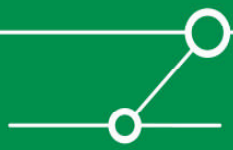
- There where dedicated devices then (e.g. FR/ATM Switches)...
  and not big multi-function, mainly IP-oriented, *Hybrids*
- There was a protocol world besides IP ...
  and IP-based (attack) tools. You ever heard of sth like"*libnet for ATM*"?

MPLS “Layer 2 VPNs“

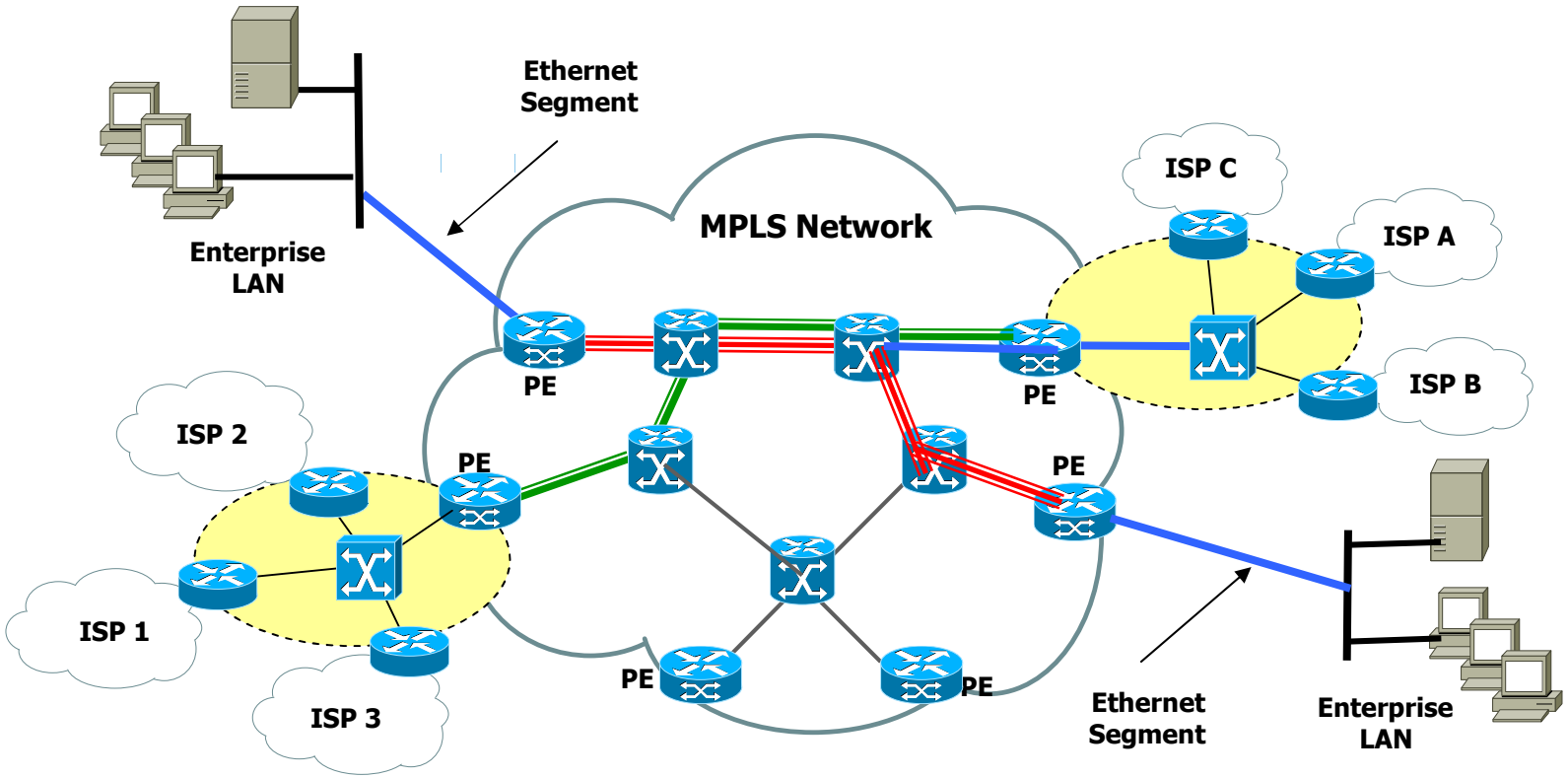
- Term usually designates *Any Transport over MPLS* [AToM]
- AToM: Technology for transport of different layer 2 protocols (e.g. ATM, Frame Relay, Ethernet, PPP, HDLC) over MPLS backbone.
- Can be very useful for providers or customers, for various reasons.
- Operates with *Pseudo Wires* = logical circuits established between MPLS capable backbone devices.
- Several L2 protocols may be encapsulated, labeled and transported over these pseudo wires, e.g. FRoMPLS, AAL5oMPLS, CRoMPLS.

MPLS “Layer 2 VPNs“

- Inner workings are roughly the same as with *Layer 3 VPNs*: packets have (at least) two labels, one for forwarding purposes, another to identify a customer site/virtual circuit.
- In some cases there may be an additional *control word* carrying supplementary information (e.g. FR BECN/FECN). Some attacks may be possible here (though not covered in this presentation).
- Modifying labels should allow “VPN hopping“ as described above.
- There are two variants that are of particular interest for us:
  Ethernet over MPLS [EoMPLS]
  Virtual Private LAN Service [VPLS]

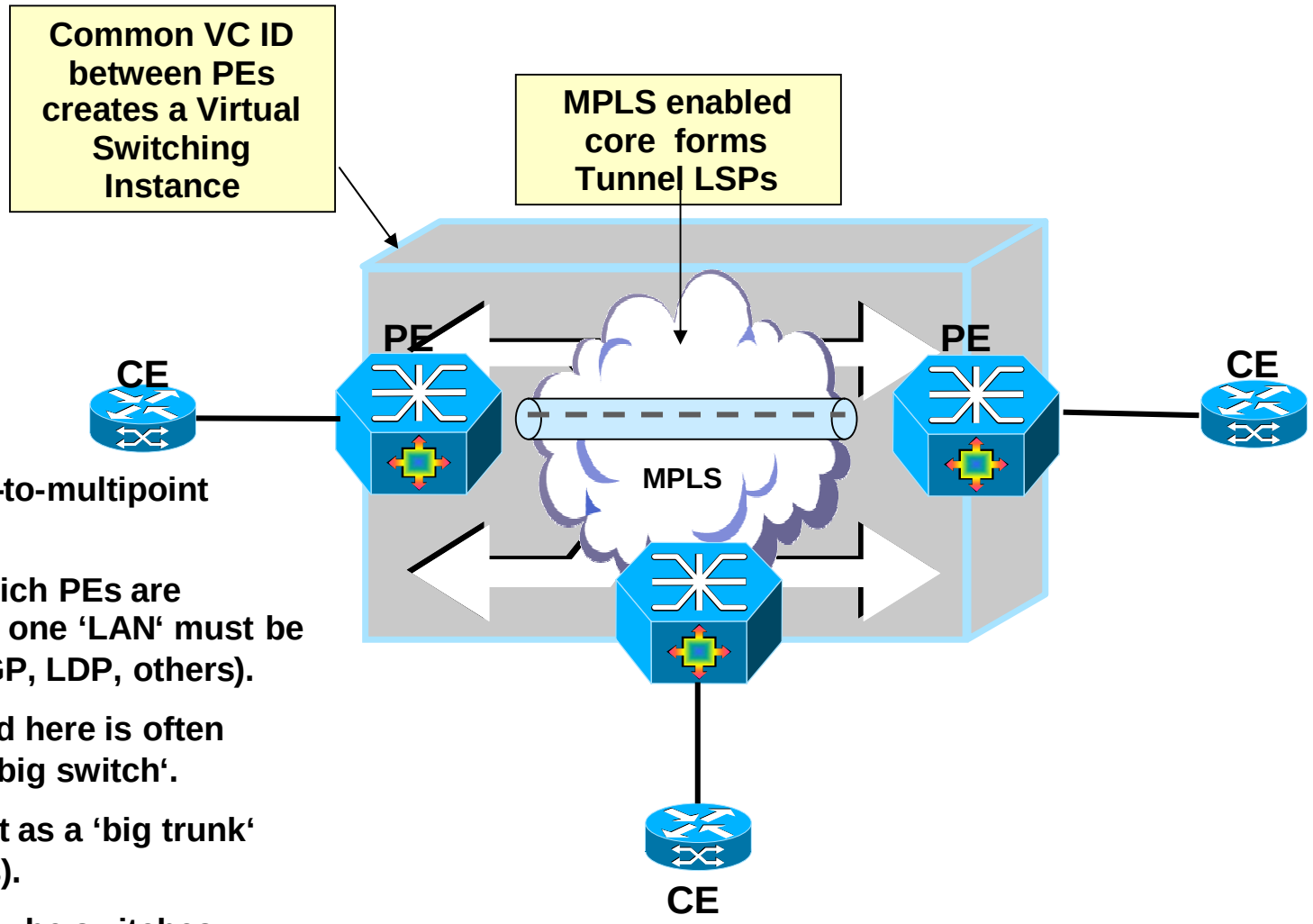


Ethernet over MPLS



This provides point-to-point connectivity only. Therefore does not scale.

VPLS



Provides point-to-multipoint connectivity.

Information which PEs are participating in one ‘LAN‘ must be exchanged (BGP, LDP, others).

The VPLS cloud here is often regarded as a ‘big switch‘.

I prefer to see it as a ‘big trunk‘ (in Cisco terms).

CE devices may be switches.

Refresher: some characteristics of Ethernet

- Broadcast medium
- MAC learning on switches
- Multicast/broadcast/unicast-frames with unknown destination MAC are flooded
- Loop avoidance by means of *Spanning Tree Protocol[s]*, STP
- VLANs
- And *trunks*

- All this might/must be emulated by these technologies.

EoMPLS/VPLS ‘parameters‘

- **Transparency: what is transported?**
  [ethernet traffic with/without VLAN tags, may VLAN IDs be chosen by customer?, what BPDUs are transported/must those be IEEE-compliant? etc.].

  If ‘fully transparent‘: a packet is thrown in on one side and leaves on the other exactly as thrown-in. In this case it may not be too important who owns & manages the CE as the main purpose is to provide transparent *ethernet* connectivity. Customers usually are identified then based on the ingress interface.

- **Responsibility: who is responsible for what kind of filtering, if any required?**
  And who has the necessary knowledge?

- **Design: is there some Layer 2 device between the (‘MPLS-performing‘) PE and the CE?**
  If so: how are the VCs built up now? What about transparency & security then?

- **Most of these parameters seem to be not yet definitely clear…**
  … to none of the participating parties ;-))

Hypothesis

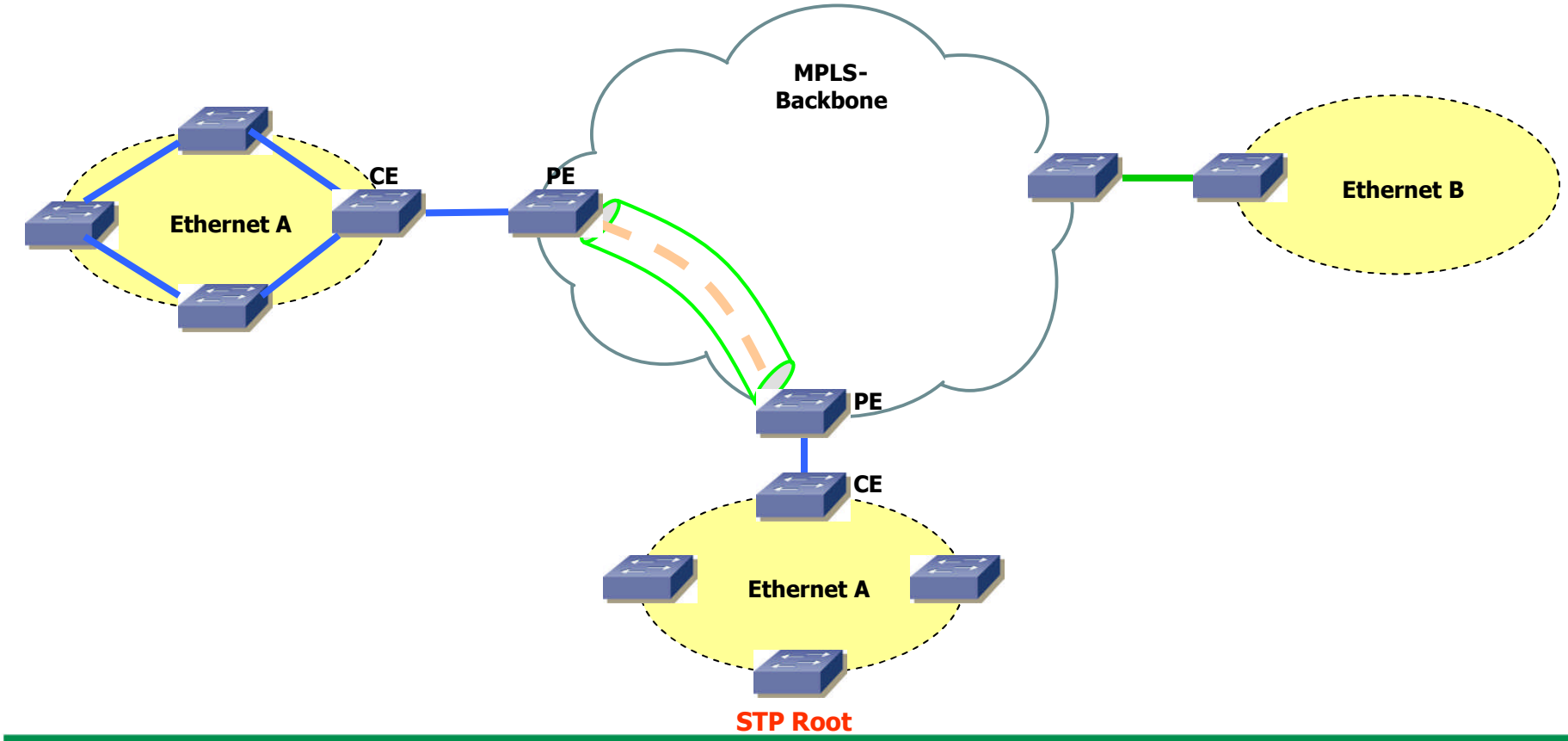
“Implementing ethernet via WAN technologies (here: MPLS) will create new challenges in terms of network security.“

- **Current state of affairs: carriers do not sell *transparent* ethernet.**
- **=> customers do not get “real ethernet“ (e.g. they can‘t choose VLAN numbers)**
- **=> carriers *will have* to offer “real“ (transparent) ethernet.**
- **And this is already the case in some vendors‘ implementations (e.g. Juniper‘s VPLS implementation).**
- **Other vendors (Cisco) have proprietary protocols for the very same purpose (Cisco *Layer2 Protocol Tunneling* [L2PT, do not confuse with L2TP]).**

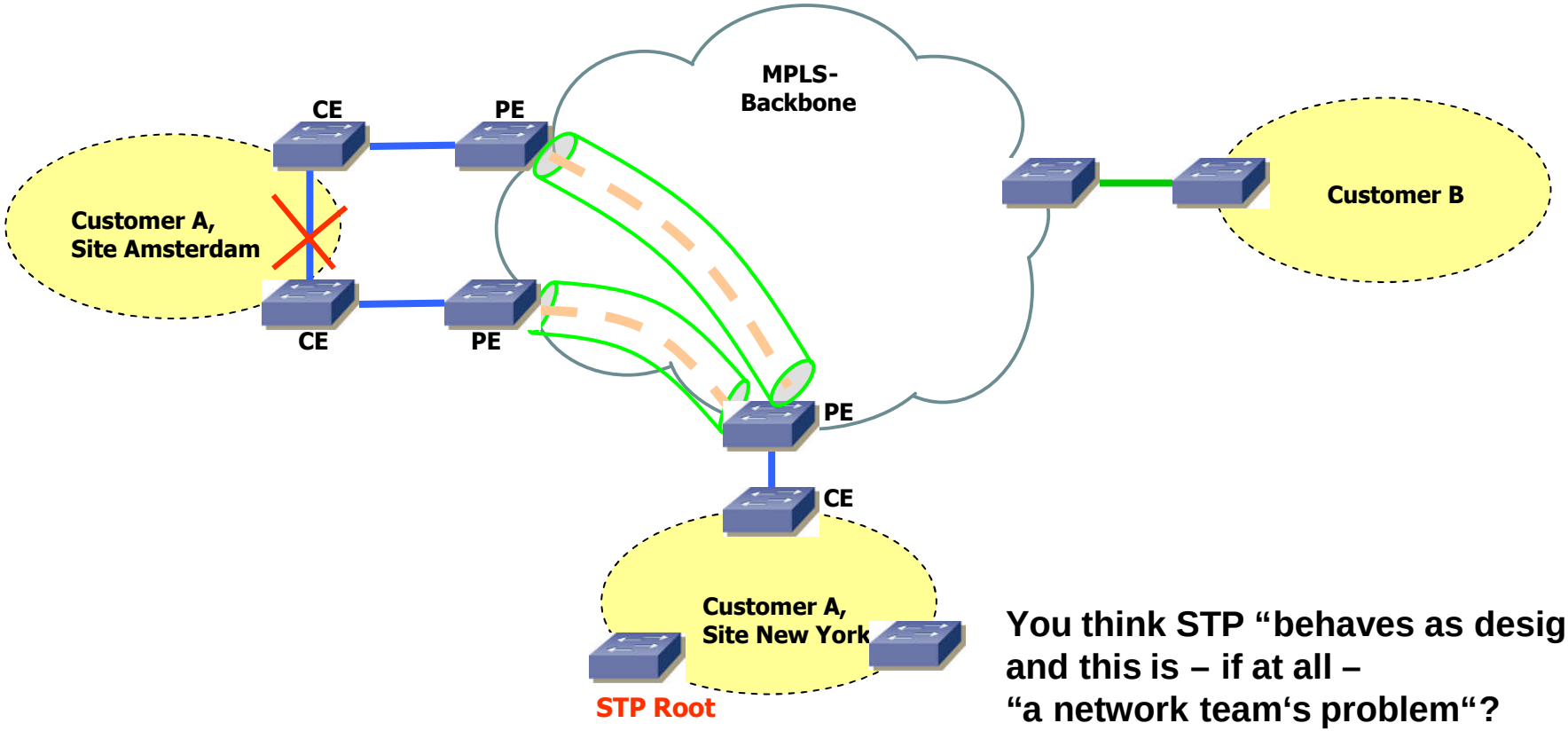
Imagine a fully transparent ethernet connection was provided…

then some interesting scenarios would evolve ;-))

STP Root Election



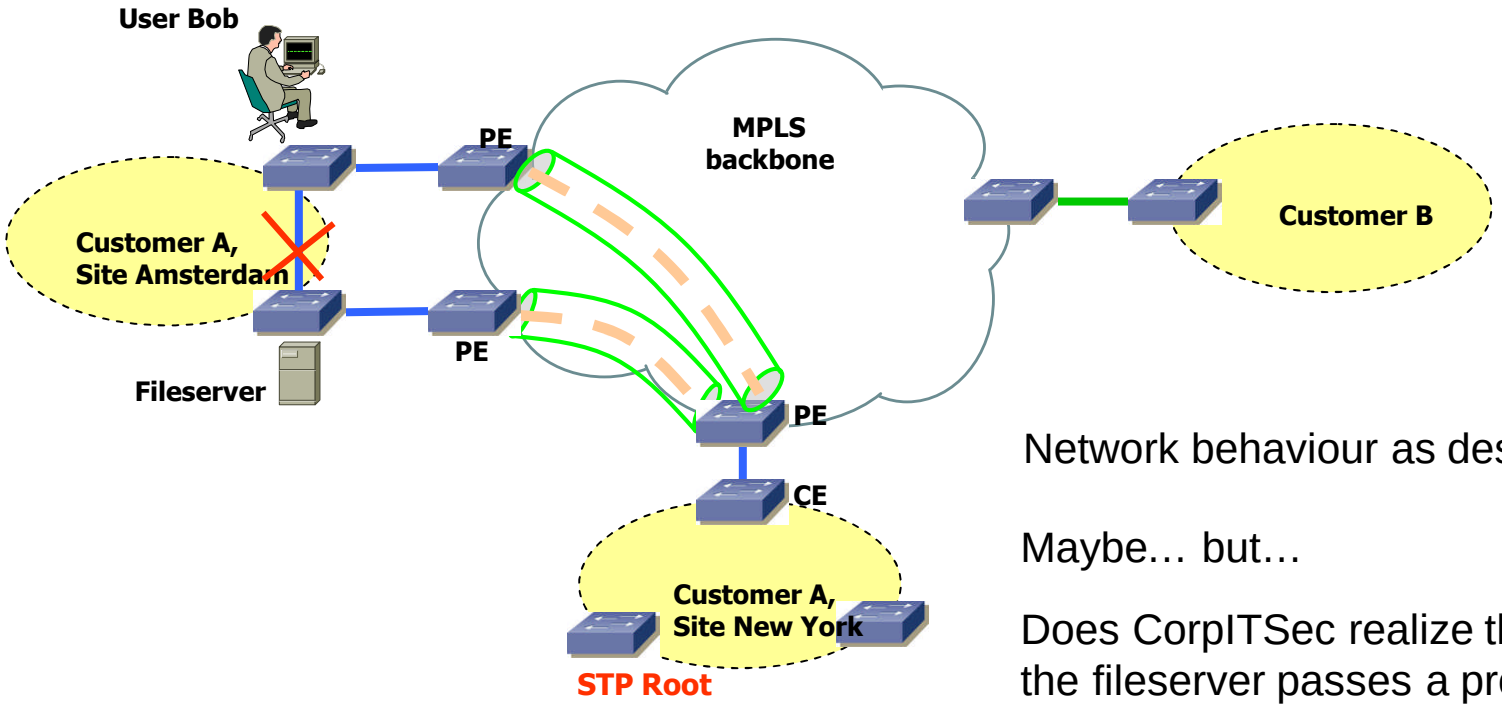
Some customers may want redundant connections…



You think STP "behaves as designed" and this is – if at all – "a network team's problem"?

Note (for all network admins here): there is no easy solution for this one.

Some customers may want redundant connections…



Network behaviour as designed?

Maybe… but…

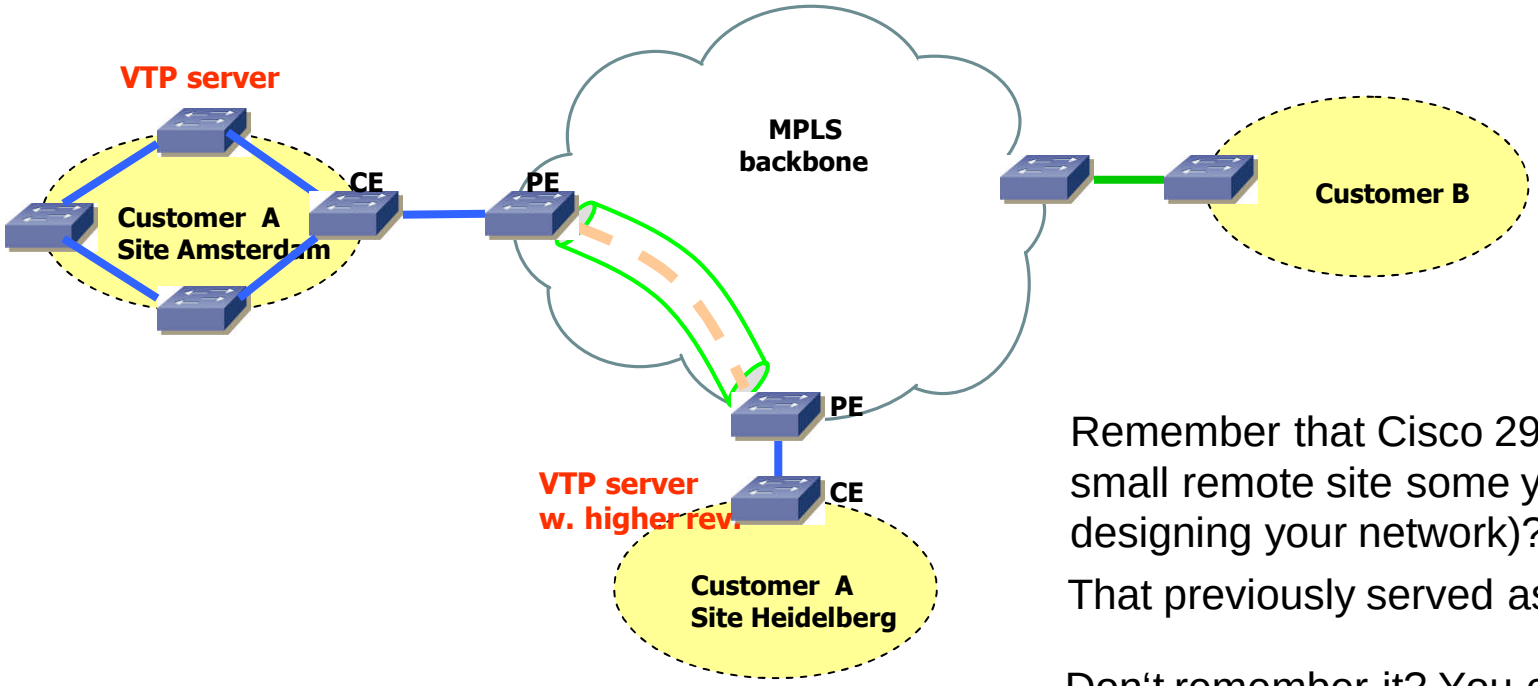
Does CorpITSec realize that Bob‘s access to the fileserver passes a provider backbone?

In another country…

where *Carnivore/DCS 1000* applies (or a different ‘understanding of intellectual property‘ exists)…

Unencrypted!

The impacts of VTP…



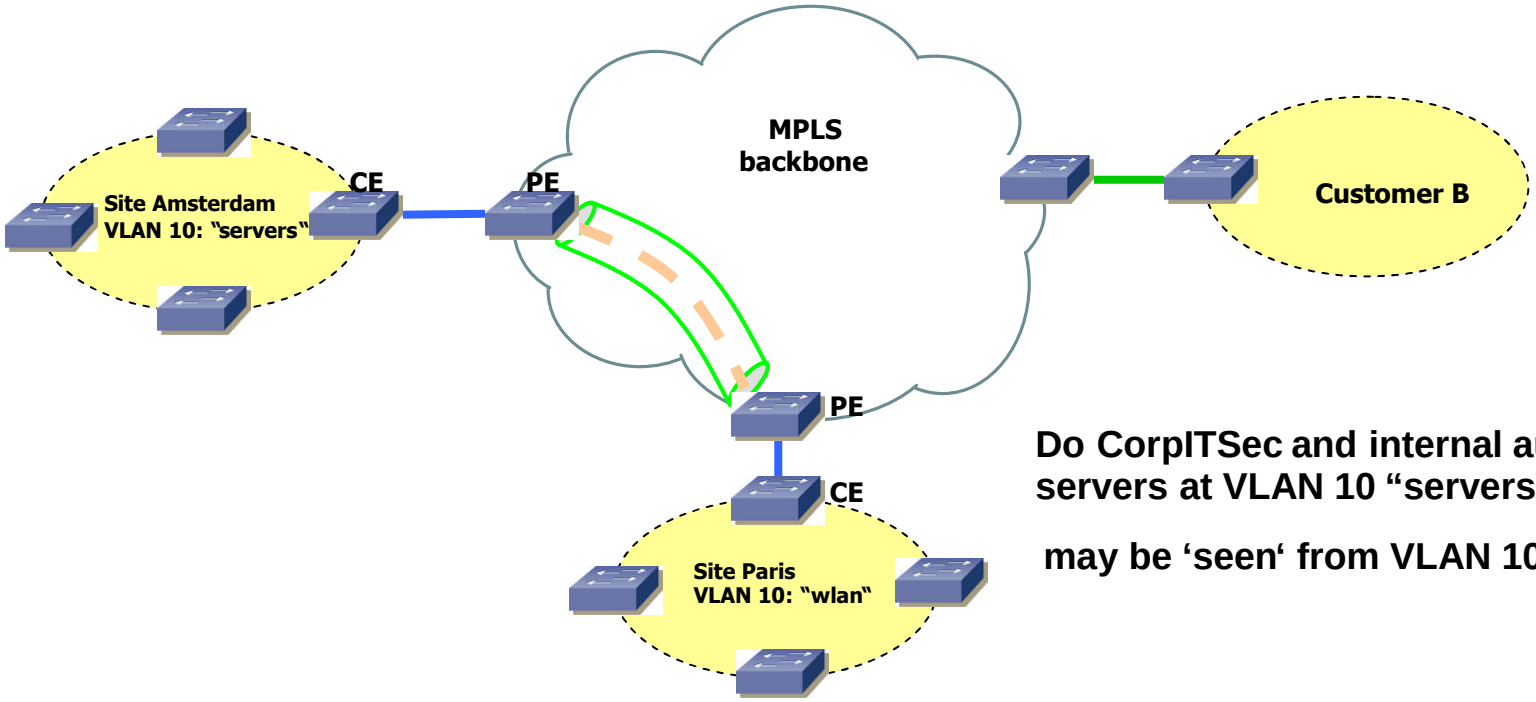
Remember that Cisco 2980 you moved to a small remote site some years ago (when re-designing your network)?

That previously served as *VTP server*…

Don‘t remember it? You certainly will ;-))

… when it melts down your whole network.
[as it still holds a high *VTP revision number*]

What about VLANs?



Do CorpITSec and internal audit know that all servers at VLAN 10 “servers“ in site Amsterdam…

may be ‘seen‘ from VLAN 10 “wlan“ at Paris?

Most organizations have organization-wide IP addressing plans (i.e. Layer 3), but no organization-wide VLAN structures (Layer 2).

Assessment

- All these may be “network problems“.
- But they *do have* security impact!
- And always remember aspects like ‘no encryption‘, ‘shared PE‘ etc. (see above)

- We should now focus attacks again...

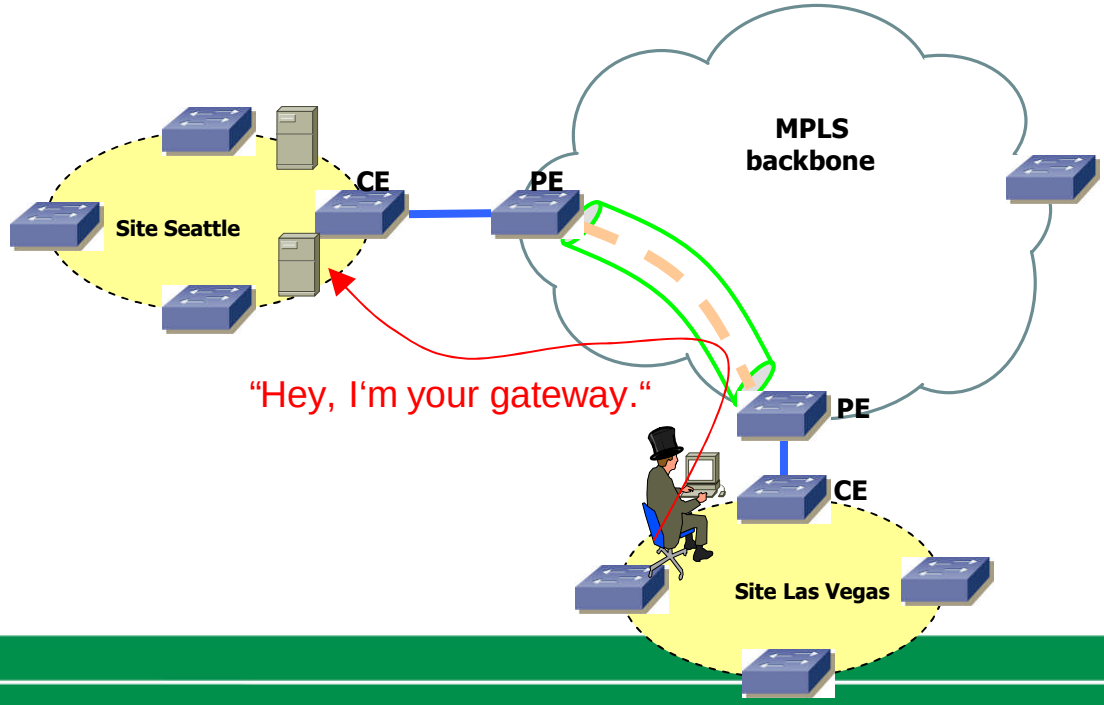
Attacks in the age of VPLS

Can be divided into:

- Attacks “over the cloud“
- Attacks against VPLS-performing devices

Attacks “over the cloud“

- Depend highly on the level of transparency the “VPLS cloud“ provides.
- Given full transparency (as in *Juniper*-based testbed we used)…
- … you can perform any classical layer 2 attack over the cloud.
- We tested this successfully with *yersinia*.
- This is pretty cool: sitting in Las Vegas and arp-spoofing/sniffing some boxes located in Seattle…



Attacks against VPLS-performing devices

- Depend highly on the functions they perform.
- Remember: the image “VPLS cloud = big virtual switch“ is not entirely correct (e.g. as those devices usually do not participate in STP/other infrastructure protocols).
- So many layer 2 attacks may not be feasible.
- But those devices do learn (and store) MAC addresses.
- You thought *MAC table flooding* nowadays no longer works?

This is what we saw in a testbed

- Bunch of Juniper M7i routers (note: these are considered ‘big iron‘).
- Just sitting around doing nothing at all.

```
lab@JESSICA# run show chassis cfeb
CFEB status:
  State                          Online
  Intake Temperature          27 degrees C / 80 degrees F
  Exhaust Temperature         34 degrees C / 93 degrees F
  CPU utilization              2 percent
  Interrupt utilization        0 percent
  Heap utilization             8 percent
  Buffer utilization          26 percent
  Total CPU DRAM             128 MB
  Internet Processor II          Version 1, Foundry IBM, Part
number 164
  Start time:                    2006-01-20 08:34:29 CET
  Uptime:                       4 hours, 10 minutes, 21 seconds
```

This is what we saw in a testbed

```
lab@JESSICA# run show chassis cfeb
CFEB status:
  State                          Online
  Intake Temperature          27 degrees C / 80 degrees F
  Exhaust Temperature         35 degrees C / 95 degrees F
  CPU utilization             11 percent
  Interrupt utilization        0 percent
  Heap utilization             9 percent
  Buffer utilization          26 percent
  Total CPU DRAM             128 MB
  Internet Processor II          Version 1, Foundry IBM, Part
number 164
  Start time:                    2006-01-20 08:34:29 CET
  Uptime:                      4 hours, 12 minutes
```

(1) Mac flooding with *macof* [default mac address maximum of 512 applied].

(2) Mac flooding with *macof* [mac address maximum set to 65000].

```
lab@JESSICA# run show chassis cfeb
CFEB status:
  State                          Online
  Intake Temperature          28 degrees C / 82 degrees F
  Exhaust Temperature         35 degrees C / 95 degrees F
  CPU utilization             25 percent
  Interrupt utilization        1 percent
  Heap utilization            40 percent
  Buffer utilization          27 percent
  Total CPU DRAM             128 MB
  Internet Processor II          Version 1, Foundry IBM, Part
number 164
  Start time:                    2006-01-20 07:34:29 UTC
  Uptime:                      5 hours, 1 minute, 13 seconds
```

Note:
- **'big iron'**
- **doing *nothing* else at the moment**
- **attacked by *one* 'customer'**
- **box supposed to support thousands of customers…**

Back to my hypothesis

- “Implementing ethernet via WAN technologies (here: MPLS) will create new challenges in terms of network security.“
- You get the idea (hopefully)…

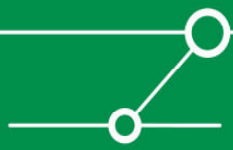
So what can/should be done

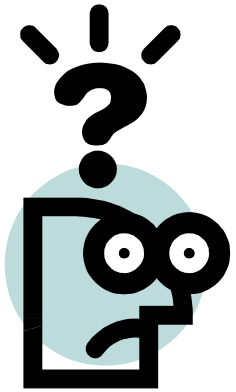
- Get familiar with filtering mechanisms/ACLs on layer 2.
- Define responsibilites (ISP vs. customer)
- Closely monitor CE devices and infrastructure traffic entering/leaving on ‘uplinks to cloud‘.

- We will develop config templates for Cisco-based CE devices in the near future. If interested in those drop me an e-mail (erey@ernw.de).

Summary

- MPLS is not just a forwarding technology but serves as a foundation for various ‘services‘ also.
- Amongst these are different ‘VPN technologies‘.
- Under certain conditions these may be attacked or security problems may arise, so thorough risk assessment should be performed.
- There are new technologies emerging that provide ‘ethernet services‘ over MPLS, namely *Virtual Private LAN Service*.
- The subsequent merger of Layer 2 and Layer 3 will have broad implications for current paradigms of network security.





Questions?

… and answers.

Thanks for your time!

Sources

[1] Presentation *MPLS Basics and In-Depth*:
http://www.rhic.bnl.gov/RCF/UserInfo/Meetings/Technology/Archive/06-30-04-CISCO/BNL-MPLS-Intro-Services-6-30-04.ppt

[2] http://www.nanog.org/mtg-0306/pdf/thomas.pdf

[3] Cisco presentation *Security in Core Networks*:
http://www.cisco.com/global/HU/rendezvenyek/presentations/SecurityinCoreNetworks.pdf

[4] MPLS attack tools: www.irmplc.com/Tools/irm-mpls-tools-1.0.tar.bz2

[5] Michael H. Behringer/Monique J. Morrow: MPLS VPN Security (Indianapolis 2005)