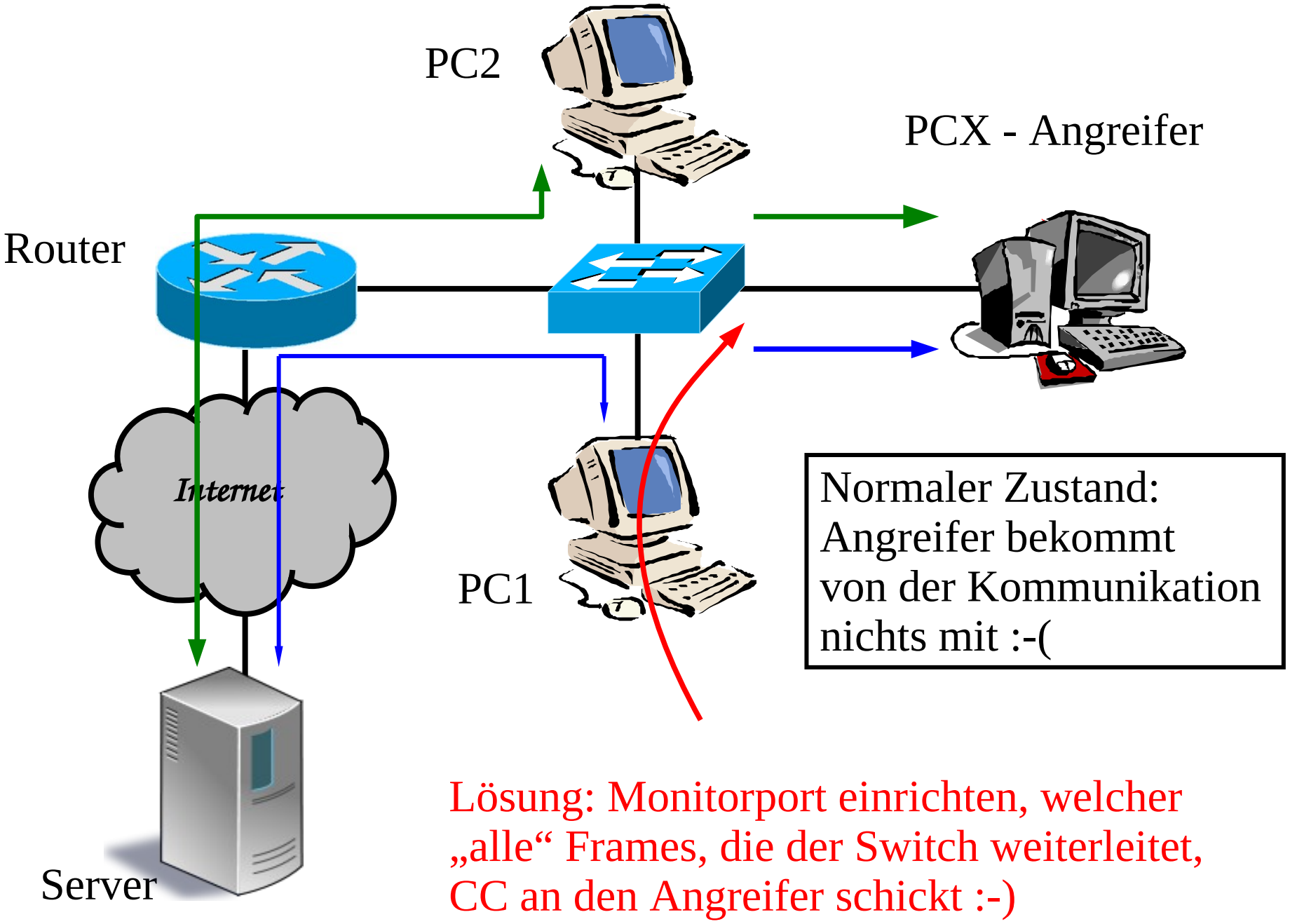

PC2
PCX - Angreifer
Router
Internet
PC1
Server
Normaler Zustand:
Angreifer bekommt
von der Kommunikation
nichts mit :-(
Lösung: Monitorport einrichten, welcher
„alle“ Frames, die der Switch weiterleitet,
CC an den Angreifer schickt :-)

CISCO – Switch (I)

- Switch-Reset und dabei zunächst einlesen der Konfiguration umgehen:
  - Switch mit gedrücker MODE-Taste starten
  - An der Eingabeaufforderung:

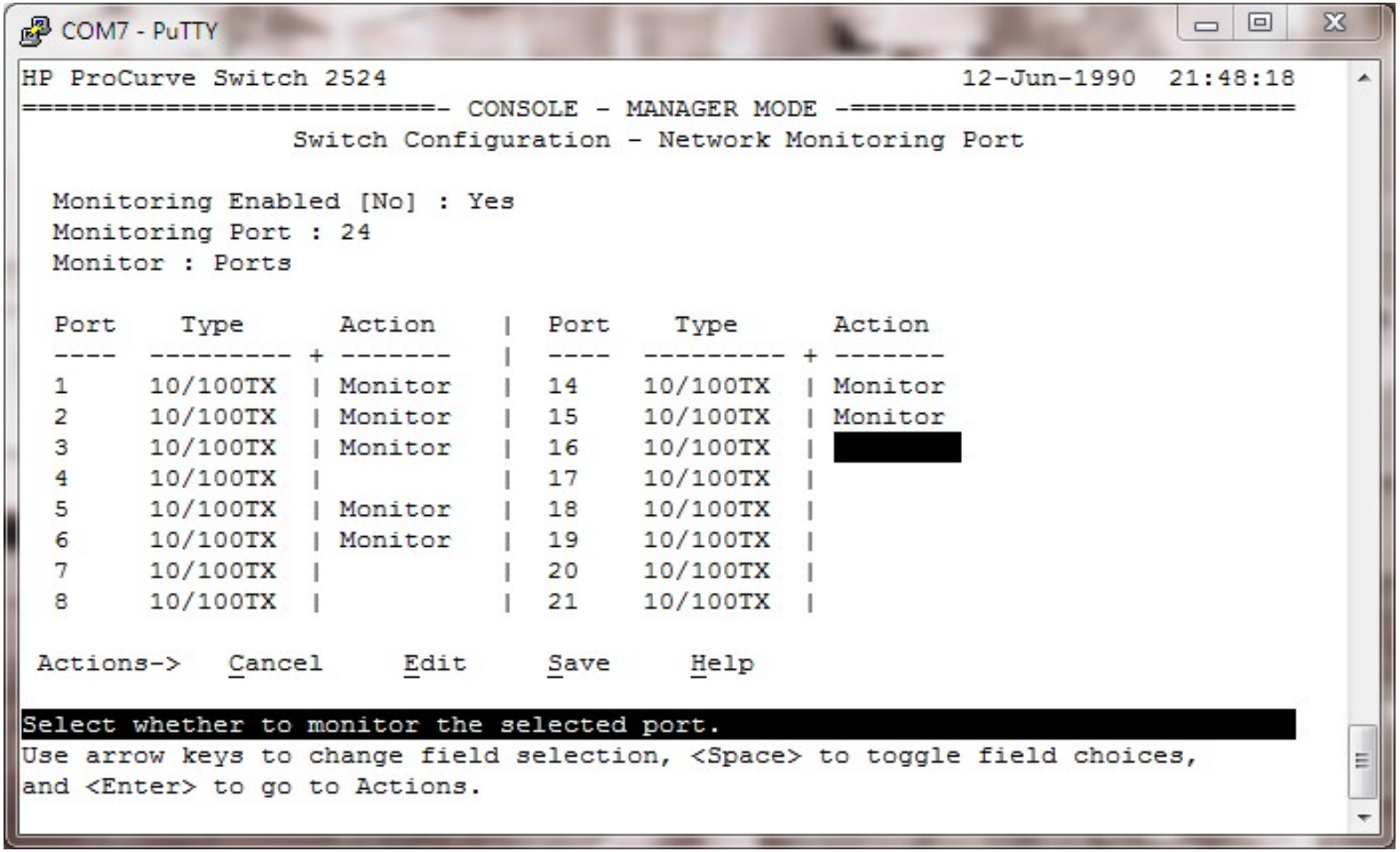
    ```
    flash_init
    load_helper
    rename flash:config.text flash:config.bak
    ```

  - Switch starten mit **`boot`**
- Im Privileged EXEC mode: Konfigurationsdatei wieder umbenennen, einlesen (Switch soll ja normal arbeiten) und sich zusätzlich einen Monitorport definieren.

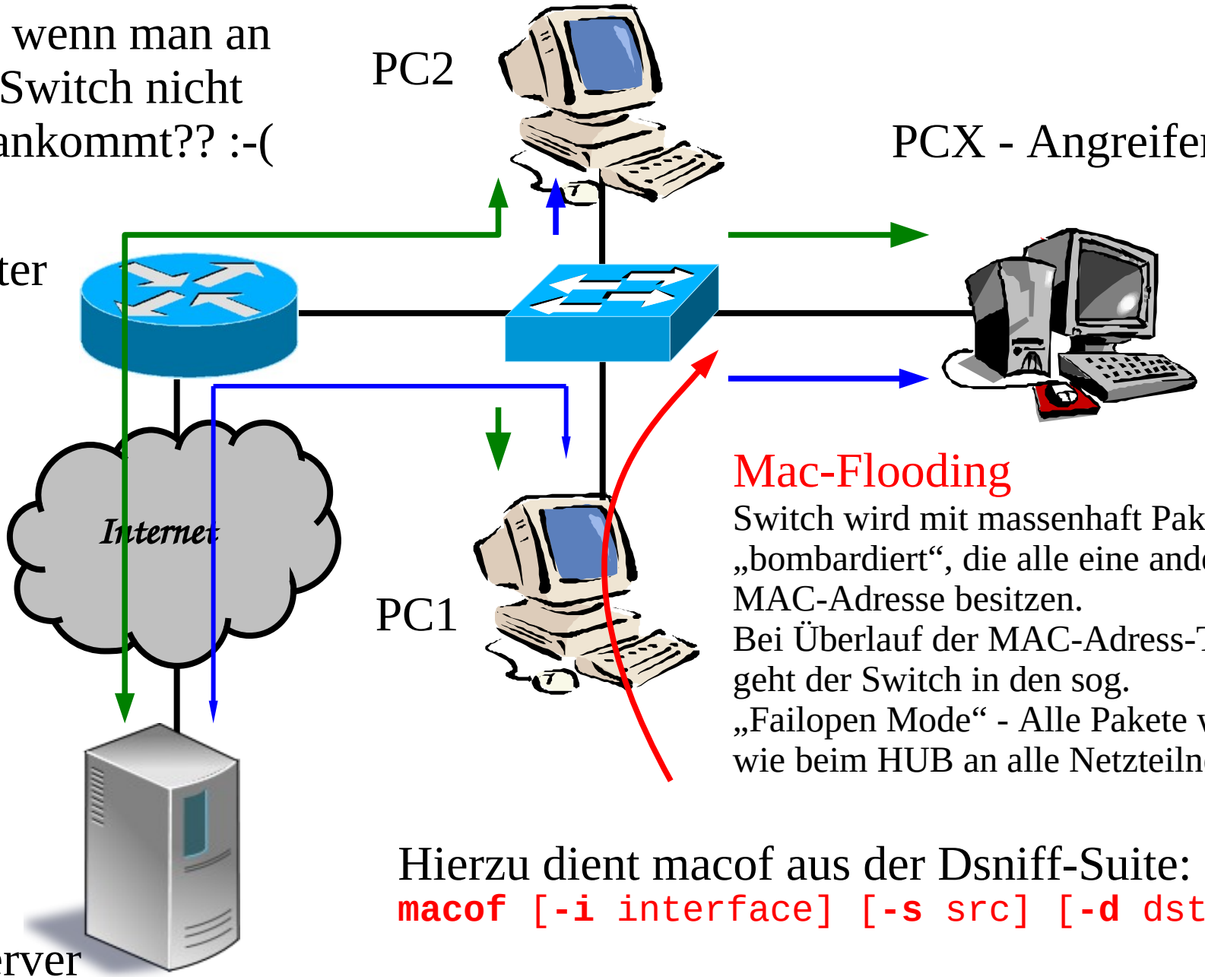
```
..
Continue with configuration dialog? [yes/no]: n
..
Press RETURN to get started.
...
Switch>

Switch>enable
Switch#rename flash:config.bak flash:config.text
Destination filename [running-config]

Switch#copy flash:config.text system:running-config
Destination filename [running-config]
workgroup_sw1#

workgroup_sw1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.

workgroup_sw1(config)#monitor session 1 source interface fa0/1 - 23
workgroup_sw1(config)#monitor session 1 destination interface fa0/24

workgroup_sw1(config)#end
workgroup_sw1#
00:07:16: %SYS-5-CONFIG_I: Configured from console by console
workgroup_sw1#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
workgroup_sw1#exit
```

HP ProCurve

- Zunächst mit Clear-Button (Gerätevorderseite) Passwort löschen
- Mit dem Befehl `menu` eben dieses starten
- Dort *2. Switch Configuration* anschl. *3. Network Monitoring Port*



Und wenn man an den Switch nicht Herankommt?? :-(



Mac-Flooding

Switch wird mit massenhaft Paketen „bombardiert“, die alle eine andere MAC-Adresse besitzen.
Bei Überlauf der MAC-Adress-Table geht der Switch in den sog. „Failopen Mode“ - Alle Pakete werden wie beim HUB an alle Netzteilnehmer.

Hierzu dient macof aus der Dsniff-Suite:

```
macof [-i interface] [-s src] [-d dst]
```

VLANs!?

```
Switch#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
10   MGMT                             active
20   DMZ                              active
30   LAN                              active    Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24

Switch#show run
...
interface FastEthernet0/1
...
interface FastEthernet0/17
 switchport access vlan 30
 switchport mode access
...
interface GigabitEthernet0/1
 switchport mode trunk
...
```

Trunking Modes, DTP

- Neben direktem Trunk-Status "*on*" (**`switchport mode trunk`**) weitere Modis möglich
- Aushandlung Trunkmode zw. Catalysts über proprietäres "*Dynamic Trunking Protocol (DTP)*

	Dynamic Auto	Dynamic Desireable	Trunk	Access
Dynamic Auto	Access	Trunk	Trunk	Access
Dynamic Desireable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	Not Recommended
Access	Access	Access	Not Recommended	Access

Note: Table assumes DTP is enabled at both ends.
`* show dtp interface` - to determine current settings

Defaultmode eines Ports beim Catalyst 2950

Defaultmode eines Ports beim Catalyst 2960

Deaktivierung von DTP:
`S2(config-if)#switchport nonegotiate`

Trunk aktivieren

Yersinia 0.7.1

File Protocols Actions Options Help

Launch attack | Edit interfaces | Load default | List attacks | Clear stats | Capture | Edit mode | Exit

1

Protocols	Packets
CDP	12
DHCP	17
802.1Q	12
802.1X	0
DTP	33
HSRP	0
ISL	0
STP	231

Field	Value
Source MAC	00:14:6
Destination MAC	01:00:0
Version	01
Neighbor-ID	001469
Status	03
Type	A5
Domain	

09:20:26

CDP DHCP 802.1Q 802.1X DTP HSRP ISL STP VTP Yersinia log

Neighbor-ID	Status	Domain	Interface	Count	Last seen
001469867641	03 ACCESS/DESIRABLE		eth0	2	13 Apr 09:13:25
0C7CE846D595	03 ACCESS/DESIRABLE		eth0	3	13 Apr 09:13:49
001469867641	83 TRUNK/DESIRABLE		eth0	16	13 Apr 09:20:20
0C7CE846D595	83 TRUNK/DESIRABLE		eth0	12	13 Apr 09:20:01

2

Dynamic Trunking Protocol

Source MAC 0C:7C:E8:46:D5:95 Destination MAC 01:

Version 01 Neighbor-ID 0C7CE846D595 Status 0

Domain

```
0x0000:  0100 0ccc cccc 0014 6986 7641 0022 aaaa  ......
0x0010:  0300 000c 2004 0100 0100 0500 0002 0005  ......
0x0020:  0300 0300 05a5 0004 000a 0014 6986 7641  ......
0x0030:  0000 0000 0000 0000 0000 0000            ......
```

Choose attack

CDP DHCP 802.1Q 802.1X DTP HSRP ISL STP VTP

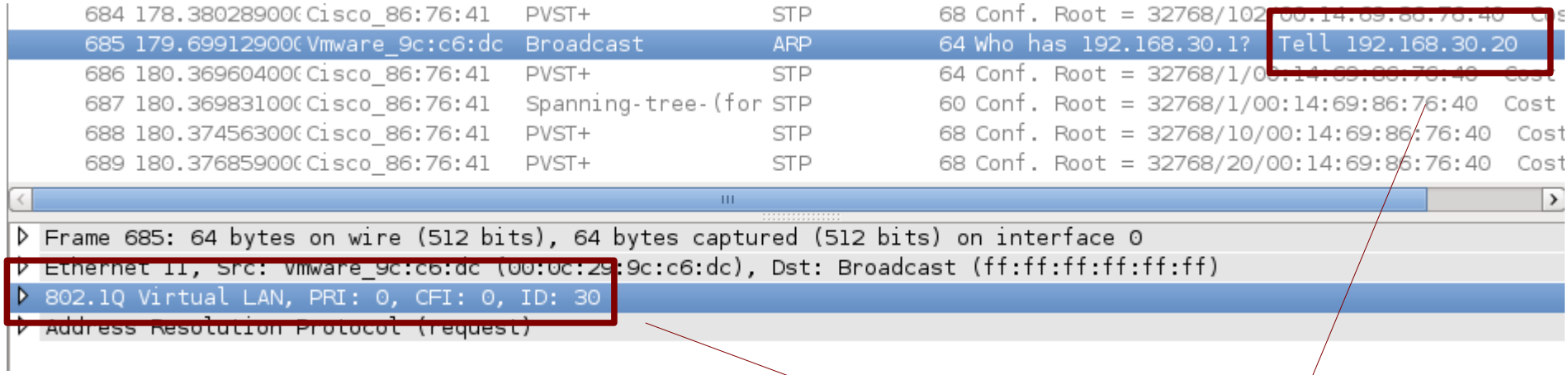
Choose attack

Description DoS

- sending DTP packet
- enabling trunking

Cancel OK

Infos aus und über die VLAN´s mit Wireshark ermitteln



Offensichtlich gibt es ein VLAN mit der ID 30

… und darin einen Host mit der IP 192.168.30.20

Jetzt ein entsprechendes VLAN-Interface aktivieren und Verbindung aufnehmen

root@tkali: ~

Datei Bearbeiten Ansicht Suchen Terminal Hilfe

```
root@tkali:~# vconfig add eth0 30
Added VLAN with VID == 30 to IF -:eth0:-
root@tkali:~# ifconfig eth0.30 up
root@tkali:~# ifconfig eth0.30 192.168.30.250/24
root@tkali:~# ifconfig eth0.30
eth0.30   Link encap:Ethernet  Hardware Adresse f4:ce:46:e4:2e:ec
          inet Adresse:192.168.30.250  Bcast:192.168.30.255  Maske:255.255.255.0
          inet6-Adresse: fe80::f6ce:46ff:fee4:2eec/64 Gültigkeitsbereich:Verbindung
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metrik:1
          RX packets:17 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3 errors:0 dropped:0 overruns:0 carrier:0
          Kollisionen:0 Sendewarteschlangenlänge:0
          RX bytes:850 (850.0 B)  TX bytes:258 (258.0 B)

root@tkali:~# ping 192.168.30.20
PING 192.168.30.20 (192.168.30.20) 56(84) bytes of data.
64 bytes from 192.168.30.20: icmp_req=1 ttl=128 time=1.31 ms
64 bytes from 192.168.30.20: icmp_req=2 ttl=128 time=0.329 ms
64 bytes from 192.168.30.20: icmp_req=3 ttl=128 time=0.451 ms
64 bytes from 192.168.30.20: icmp_req=4 ttl=128 time=0.313 ms
^C
--- 192.168.30.20 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3001ms
rtt min/avg/max/mdev = 0.313/0.601/1.312/0.414 ms
root@tkali:~#
```