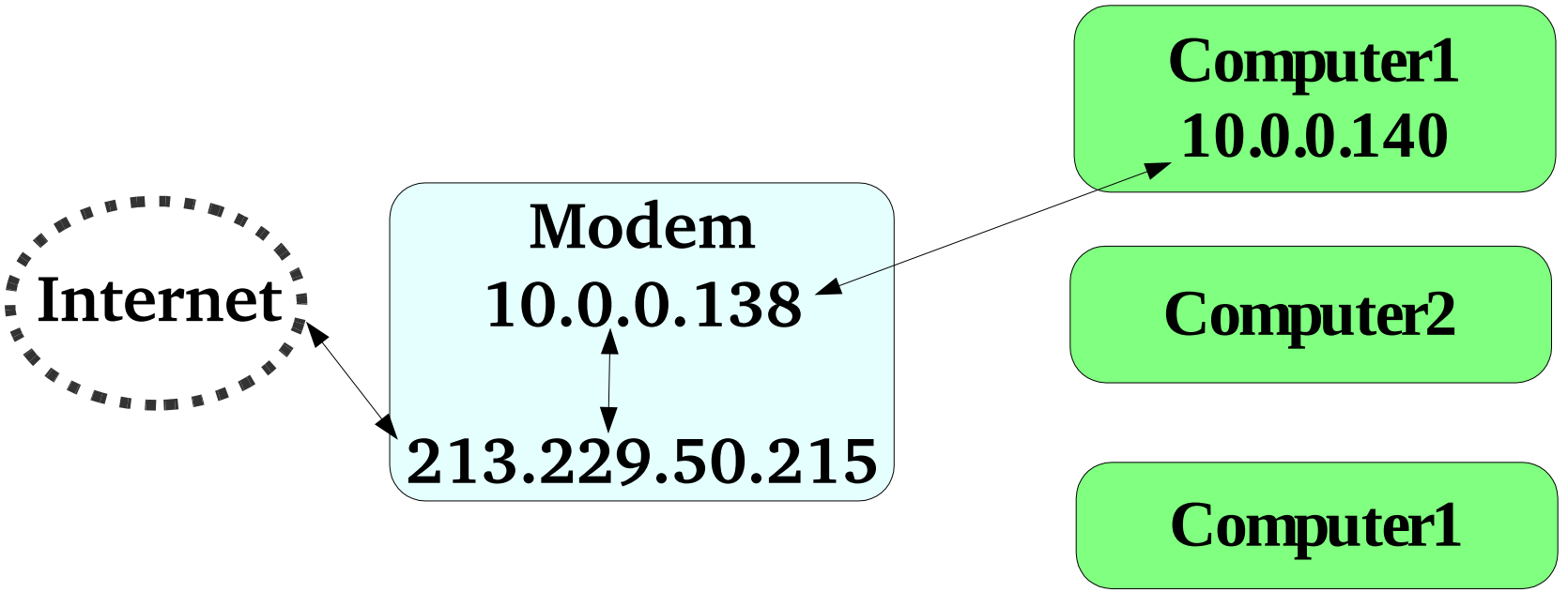
Aus Eins mach Viele

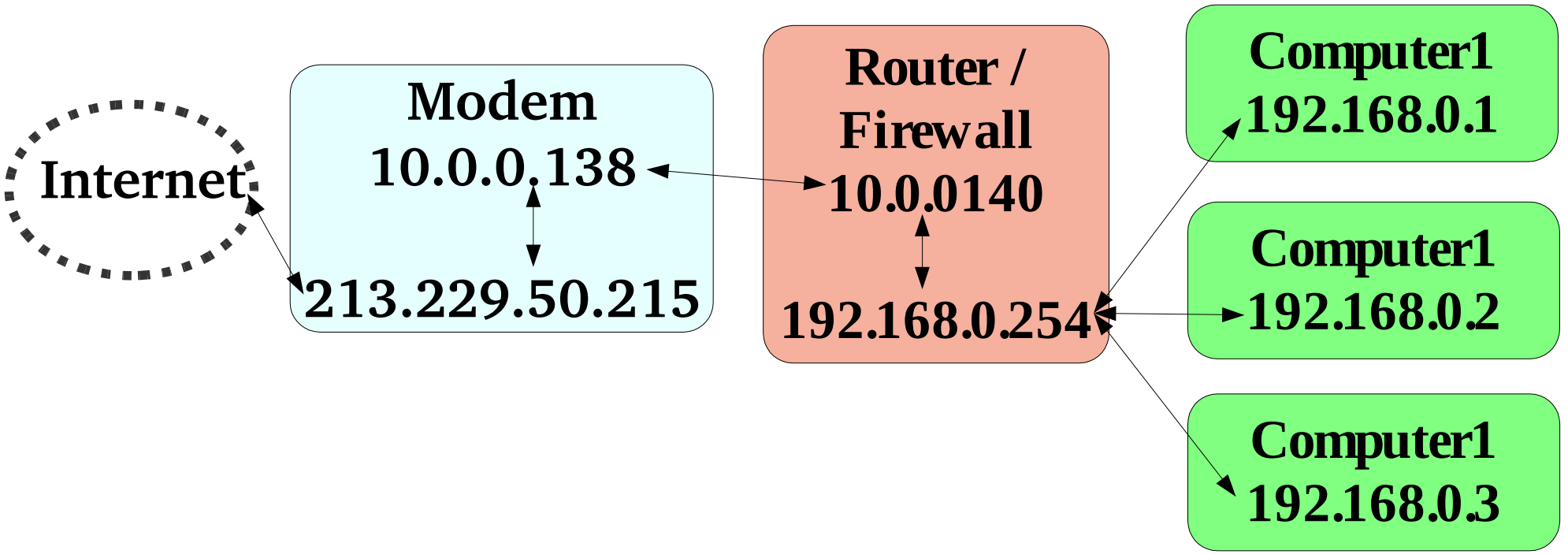
Der Einzelplatz-Zugang für die ganze WG

Sprecher: Rene “cavac” Schickbauer

Die Ausgangslage

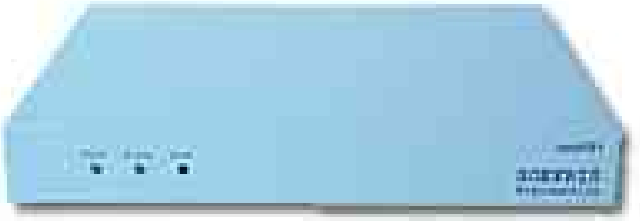


Die Zielkonfiguration



Zusätzlich benötigte Hardware (1/2)

10/100 Switch



Soekris net4801

Cat5-Verkabelung

Compact Flash 512MB

Zusätzlich benötigte Hardware (2/2)

Nullmodem-Kabel

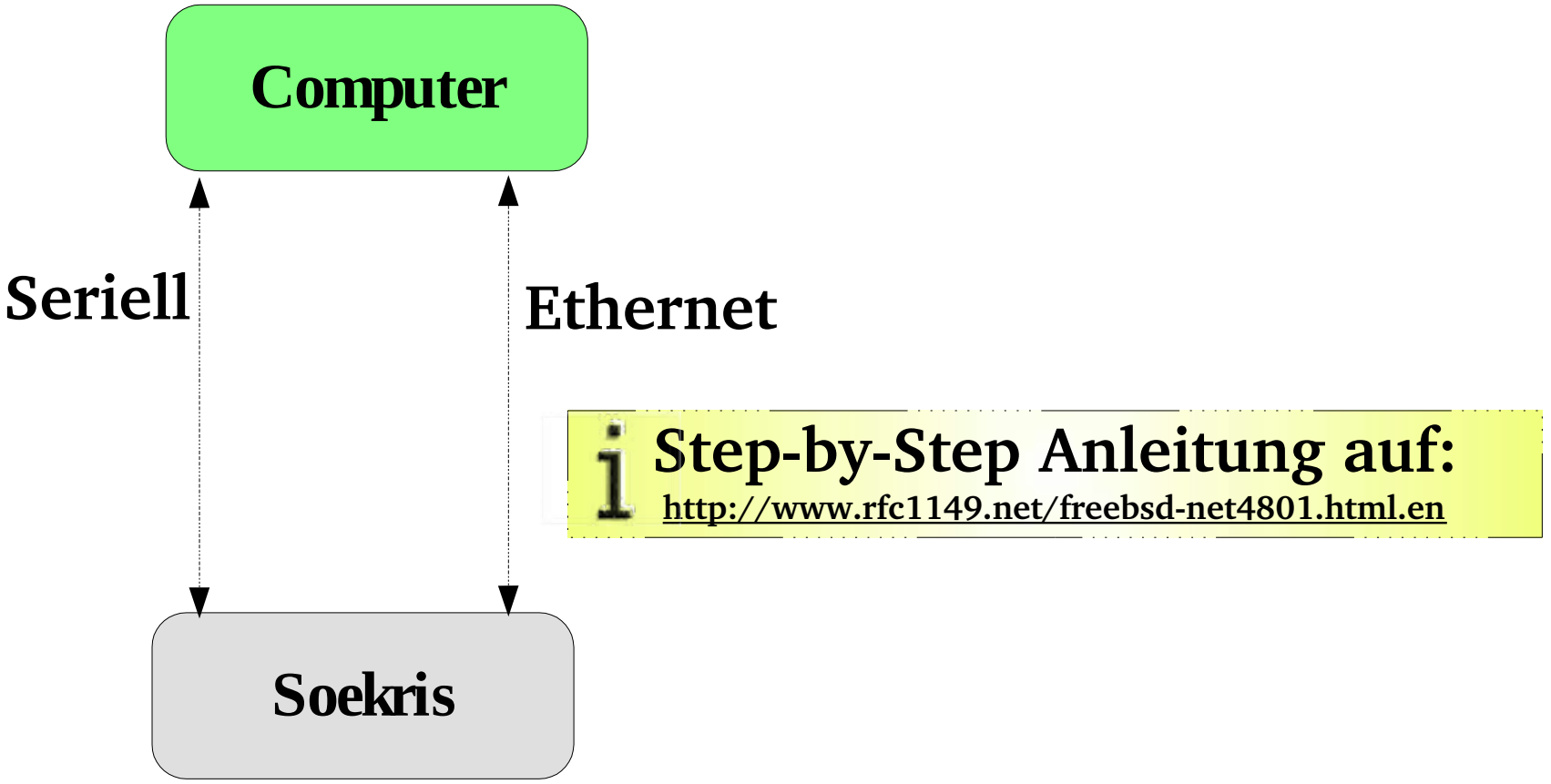
Netzteil für Soekris

FreeBSD CD

Energy-Drinks

Soekris-Board “net4801”

Installation von FreeBSD



Step-by-Step Anleitung auf:
http://www.rfc1149.net/freebsd-net4801.html.en

Einrichten von Internet auf Soekris/FreeBSD

Unterschiedliche Provider verwenden Unterschiedliche Protokolle!

Eine Detailbeschreibung aller möglichen Installationsarten würde hier leider den Rahmen sprengen!

Remote Logging

Um Schreibzyklen und Speicher am Flash zu sparen, werden syslog-Einträge an einen Arbeitsrechner geschickt statt lokal gespeichert.

/etc/syslog.conf:

```
*.* @192.168.0.1
```

/etc/rc.conf:

```
syslogd=YES  syslogd_flags=""
```

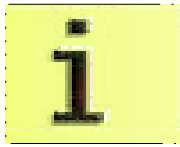
Die Konfiguration ist Systemabhängig:

man syslogd

Ports in Soekris

Soekris

```
sis0 = 192.168.0.254   -> Internes Netz
sis1 = 10.0.0.140      -> Modem
tun0 = 213.229.50.215 -> Internet
sis2 = reserviert
```



`tun0` ist ein *virtuelles* Interface

DHCP und DNS(1/5)

Automatisches Zuweisen von IP-Adressen, Hostnamen und Gateway

Soekris

/etc/rc.conf:

```
dhcpd_enable="YES"
dhcpd_ifaces="sis0"
named_enable="YES"
```

/usr/local/etc/dhcpd.conf:

```
option domain-name "grumpfzotz.org";
option domain-name-servers 192.168.0.254;
option routers 192.168.0.254;
authoritative;
ddns-update-style none;
default-lease-time 100000;
max-lease-time 200000;

group {
use-host-decl-names on;

host gandalf {
  hardware ethernet 00:C0:C3:7A:E0:7C;
  fixed-address gandalf.grumpfzotz.org;
}
.....[Insert more known hosts here].....
}

# Dynamic no-names for temporary hosts
subnet 192.168.0.0 netmask 255.255.255.0 {
        range 192.168.0.100 192.168.0.110;
        allow unknown-clients;
        option subnet-mask 255.255.255.0;
}
```

DHCP und DNS(2/5)

Automatisches Zuweisen von IP-Adressen, Hostnamen und Gateway

Soekris

/etc/namedb/named.conf:

```
option domain-name "grumpfzotz.org";
options {
        directory "/etc/namedb";
        allow-transfer { 192.168.0.0/16; };
        recursion yes;
        allow-query { 192.168.0.0/16; };
        listen-on port 53 { 192.168.0.254; };
};

zone "localhost" {
        type master;
        notify no;
        file "localhost";
};

zone "127.IN-ADDR.ARPA" {
        type master;
        notify no;
        file "127";
};
```

```
zone "grumpfzotz.org" {
        type master;
        notify no;
        file "grumpfzotz.org";
};

zone "0.168.192.in-addr.arpa" {
        type master;
        notify no;
        file "0.168.192";
};

zone "." {
        type hint;
        file "root.cache";
};
```

DHCP und DNS(3/5)

Automatisches Zuweisen von IP-Adressen, Hostnamen und Gateway

Soekris

/etc/namedb/grumpfzotz.org:

```
$TTL    3600
@       IN      SOA     soekris.grumpfzotz.org. hostmaster.grumpfzotz.org.  (
                                2005030501      ; Serial
                                3600            ; Refresh
                                300             ; Retry
                                3600000         ; Expire
                                3600 )          ; Minimum
                IN      NS      soekris.grumpfzotz.org.
                IN      MX      10 mail.mymailhost.org.
gandalf         IN      A       192.168.0.1     ; Rechner1
soekris         IN      A       192.168.0.254   ; Soekris
gateway         IN      CNAME   soekris.grumpfzotz.org.
```

DHCP und DNS(4/5)

Automatisches Zuweisen von IP-Adressen, Hostnamen und Gateway

Soekris

/etc/namedb/grumpfzotz.org:

```
$TTL    3600
@       IN      SOA     soekris.grumpfzotz.org. hostmaster.grumpfzotz.org.  (
                                2005011401      ; Serial
                                3600            ; Refresh
                                300             ; Retry
                                3600            ; Expire
                                3600 )          ; Minimum
                IN      NS      soekris.grumpfzotz.org.
1               IN      PTR     gandalf.grumpfzotz.org.
254             IN      PTR     soekris.grumpfzotz.org.
```

DHCP und DNS(5/5)

Automatisches Zuweisen von IP-Adressen, Hostnamen und Gateway

Computer1

/etc/rc.conf:

```
dhclient=YES
dhclient_flags="sip0"
```

Bei Windows-Clients kann man über “Netzwerk-Einstellungen” und “Adresse automatisch zuweisen” DHCP verwenden.

Bei Problemen kann der Soekris-Rechner über die serielle Konsole konfiguriert werden.

NAT + Firewall (1/5)

Internet-Routing einschalten

Soekris

/etc/rc.conf:

```
gateway_enable="YES"
ipnat_enable="YES"
ipnat_program="/sbin/ipnat"
ipnat_rules="/etc/ipnat.conf"
ipnat_flags=""
```

/etc/rc.conf:

```
map sis0 from 192.168.0.0/24  ! to 192.168.0.0/16 -> 213.229.50.215/32 proxy port
ftp ftp/tcp

map sis0 from 192.168.0.0/24 ! to 192.168.0.0/16 -> 213.229.50.215/32 portmap
tcp/udp 40000:65000

map sis0 from 192.168.0.0/24  ! to 192.168.0.0/16 -> 213.229.50.215/32
```

NAT + Firewall (2/5)

Firewall einschalten

Soekris

/etc/rc.conf:

```
ipfilter_enable="YES"
ipfilter_program="/sbin/ipf"
ipfilter_rules="/etc/ipf.conf
ipfilter_flags=""

ipmon_enable="YES"
ipmon_program="/sbin/ipmon"
ipmon_flags="-Ds"
```

Vor dem Einschalten der Firewall sollten die internen Rechner bereits auf das Internet zugreifen können!

NAT + Firewall (3/5)

Externe Verbindung auf tun0

Soekris

/etc/ipf.conf:

```
# Block non-routeable packets
block in log quick on tun0 from 192.168.0.0/16 to any
block in log quick on tun0 from 172.16.0.0/12 to any
block in log quick on tun0 from 10.0.0.0/8 to any
block in log quick on tun0 from 127.0.0.0/8 to any
block in log quick on tun0 from 192.0.2.0/24 to any

# Keep state on allowed outgoing packets
pass out quick on tun0 proto tcp all flags S/SA keep state keep frags
pass out quick on tun0 proto udp all keep state
pass out quick on tun0 proto icmp all keep state

# Block everything else
block return-rst in log on tun0 proto tcp all
block in log quick on tun0 all
block out log quick on tun0 all
```

NAT + Firewall (4/5)

Verbindung von sis1 zu ADSL-Modem

Soekris

/etc/ipf.conf:

```
# Allow connection to Modem
pass out quick on sis1 from 10.0.0.140/32 to 10.0.0.138/32 keep state
pass in quick on sis1 from 10.0.0.138/32 to 10.0.0.140/32 keep state

# Block everything else
block in log quick on sis1 all
block out log quick on sis1 all
```

NAT + Firewall (5/5)

SSH absichern (nur von “gandalf” erlauben)

Soekris

/etc/ipf.conf:

```
# SSH von “gandalf” erlauben
pass out quick on sis0 proto tcp from 192.168.0.254/32 to 192.168.0.1/32 port =
22 flags S/SA keep state keep frags

pass in quick on sis0 proto tcp from 192.168.0.1/32 to 192.168.0.254/32 port = 22
flags S/SA keep state keep frags

block in log quick on sis0 proto tcp all port = 22
block out log quick on sis0 all port = 22
```

ADSL: Automatischer Neustart (1/2)

/sbin/checkadsl:

Soekris

```
#!/usr/bin/perl
use strict;
use warnings;

sub checkpptp();
checkpptp();

sub checkpptp() {
        my $cnt = 4;
        my @hosts = qw[www.inode.at slashdot.org heise.de];

        my @pings;
        foreach my $host (@hosts) {
                push @pings, `ping -c $cnt $host 2>/dev/null`;
        }
        my $ok = 0;
        foreach my $line (@pings) {
                 $ok++ if($line =~ /time=\d+\.\d+/);
        }
        if(!$ok) {
                `killall pptp 2>/dev/null`;
                sleep 10;
                system "/bin/sh /sbin/startpptp 2>/dev/null &";
                sleep 10;
                `/etc/rc.d/ipfilter reload 2>/dev/null`;
                `/etc/rc.d/ipnat reload 2>/dev/null`
        }
}
```

ADSL: Automatischer Neustart (2/2)

Soekris

/sbin/startpptp:

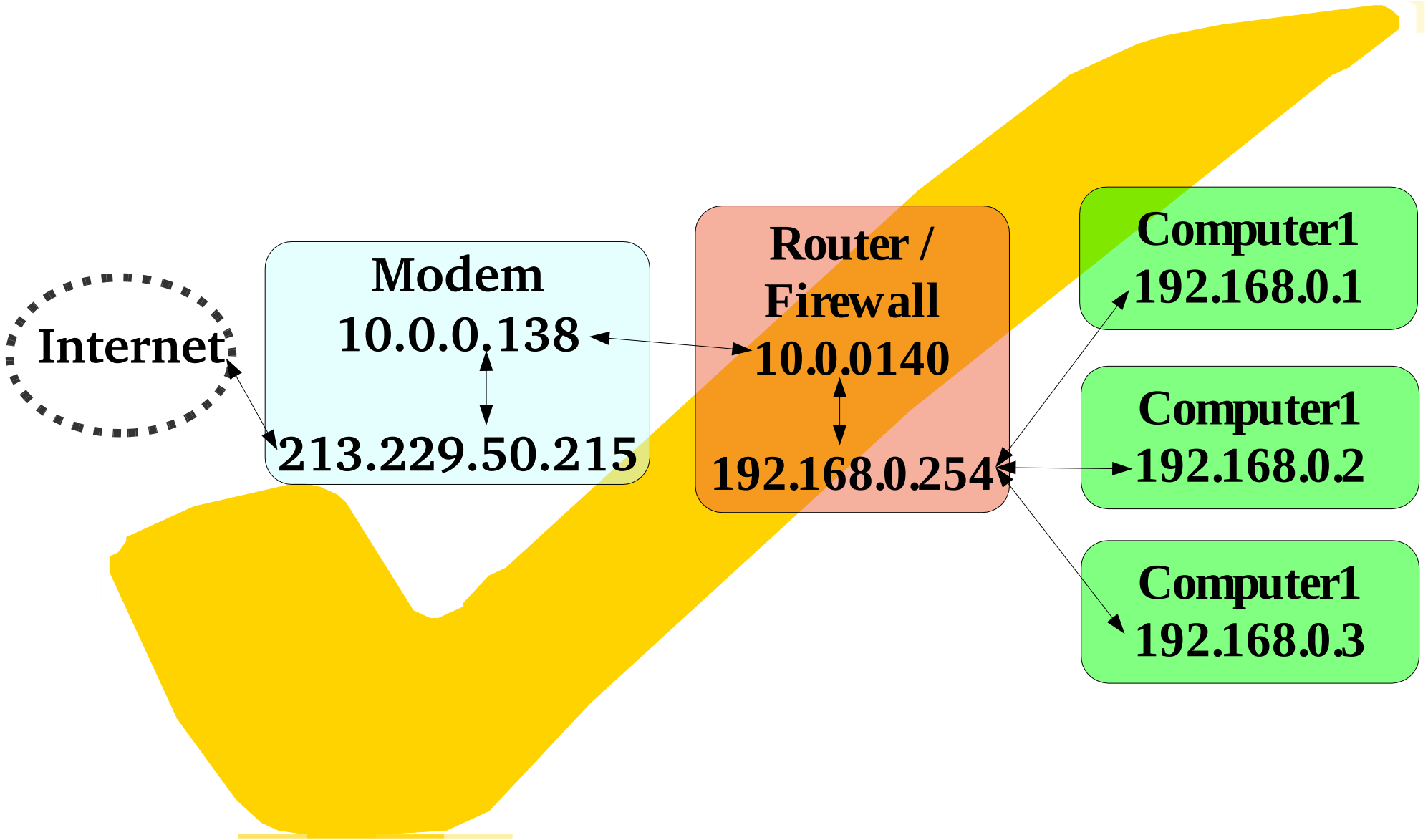
```
#!/bin/sh

/usr/local/sbin/pptp 10.0.0.138 PPTPCONFIG 2> /dev/null &
```

crontab:

```
/5 * * * * /usr/bin/perl /sbin/checkadsl
```

Die Zielkonfiguration



Fragen...?

...und hoffentlich Antworten!

Vielen Dank fürs Zuhören

Der Einzelplatz-Zugang für die ganze WG
ist jetzt betriebsbereit