Aus *EINS* mach *VIELE*

Der Einzelplatz-zugang für die ganze WG

SALOMON AUTOMATION

Sprecher: Rene Schickbauer

WAMAS logistik software

Aus *EINS* mach *VIELE*

Eine Einführung in die Magie[1] der Netzwerke

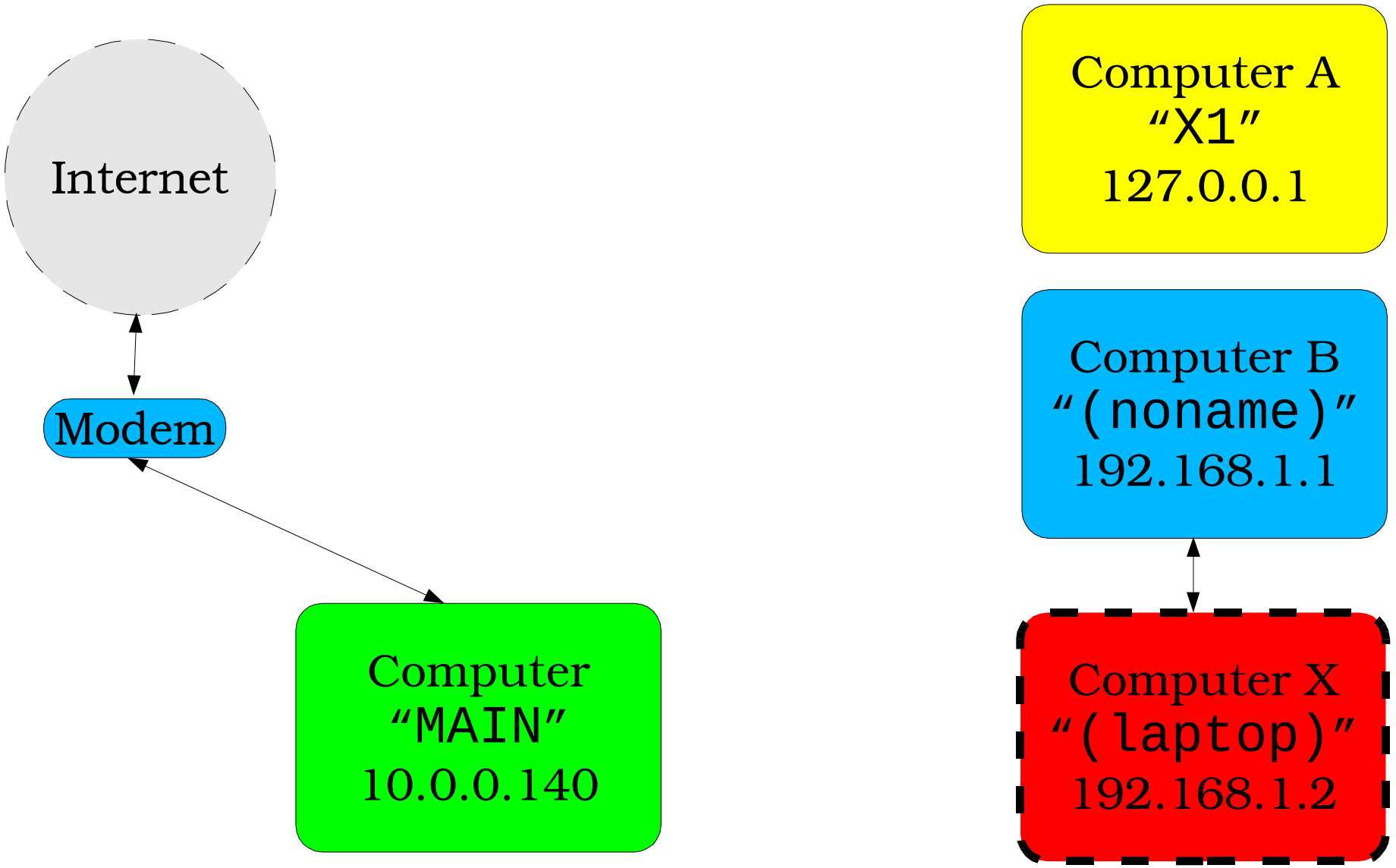
[1] Manche nennen es auch “Theorie” oder “Grundlagen”

SALOMON AUTOMATION

Sprecher: Rene Schickbauer

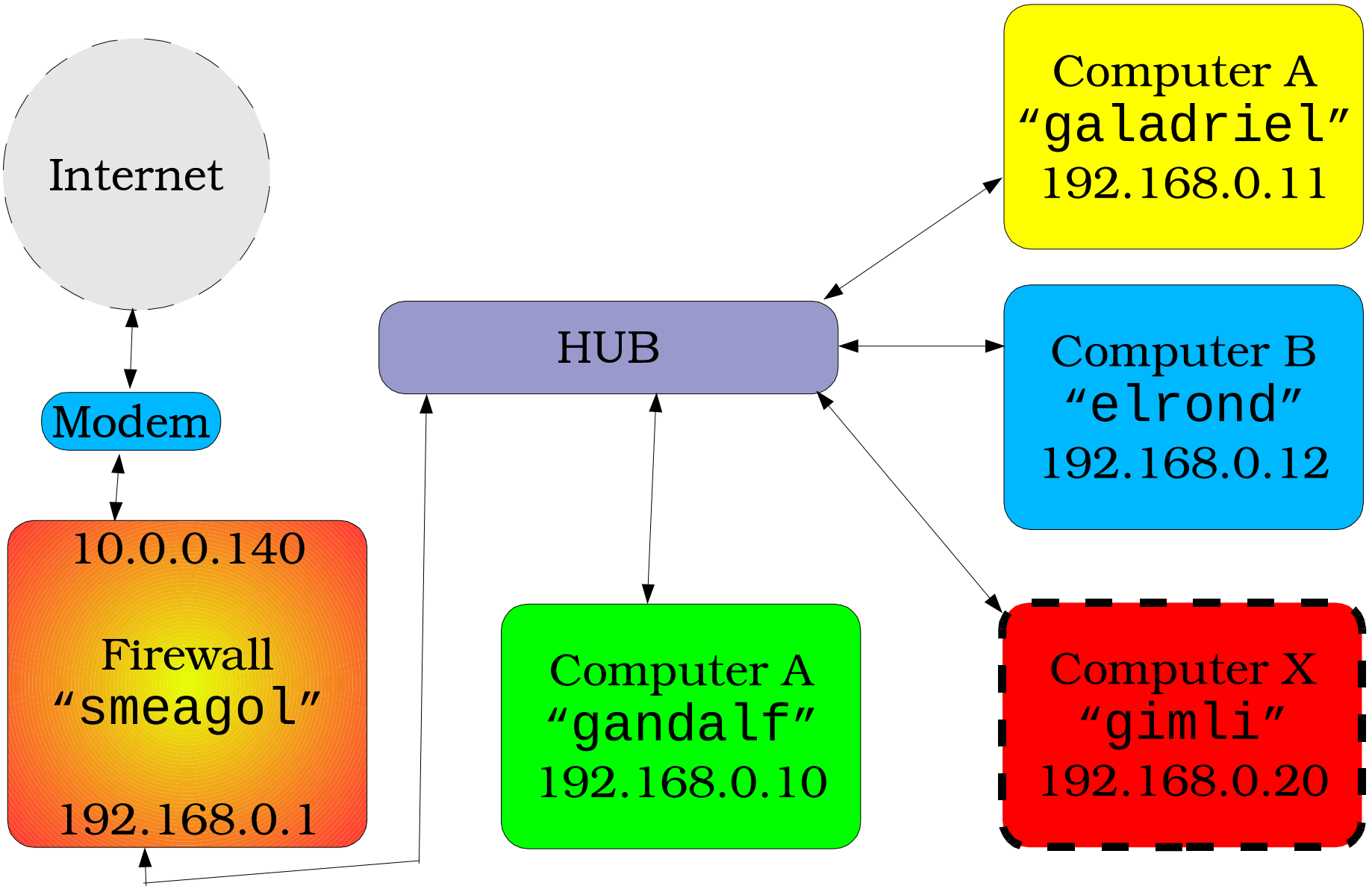
WAMAS logistik software

Aus *EINS* mach *VIELE*



Die Ausgangslage

Aus *EINS* mach *VIELE*



Das Ziel

Grundlagen: Hardware

Benötigte Hardware für das Netzwerk:

*) Hub 10MBit 5 Ports (Minimum!)
*) Netzwerkkabel (gleich mehr kaufen, schadet nie :-)
*) Netzwerkkarten für alle Clients

Benötigte Hardware für die Firewall:

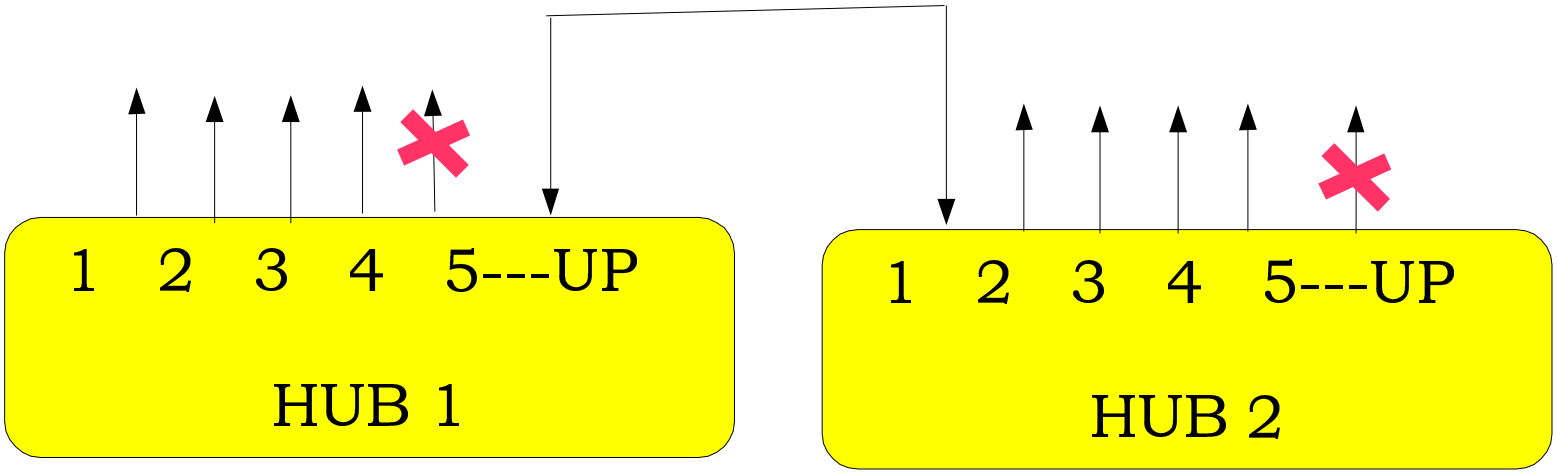
*) Ausgemusterter Rechner, mind. 100MHz, 3 Gig Platte, 40 MB Ram
*) 2 Netzwerkkarten
*) u.U. 1 ausgekreuztes Cat5-Kabel

Benötigte Software für die Firewall:

*) Linux- oder BSD-Unix-Distribution
(Code-Beispiele sind aus NetBSD)

Aus *EINS* mach *VIELE*

Verwenden von zwei HUBs



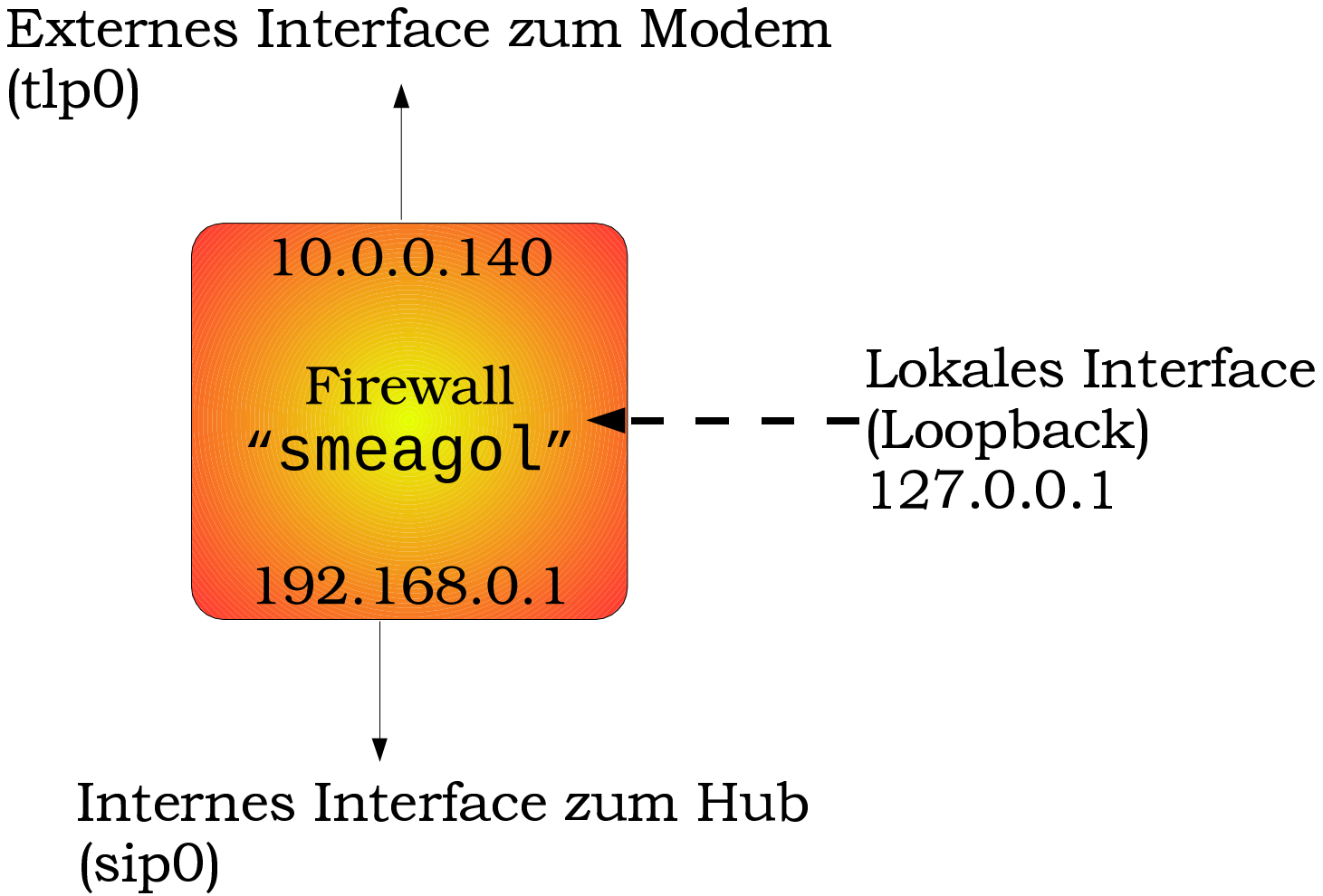
Max. 3 Hubs in Serie!

Aus *EINS* mach *VIELE*

Grundlagen: Firewall

Firewall (1)

Aus *EINS* mach *VIELE*



Grundlegende Maßnahmen:

*) Alle nicht benötigten Programme deinstallieren

*) Nicht UNBEDINGT benötigte Services ausschalten

*) SICHERE Passwörter verwenden!

*) Wer telnet verwenden will, sollte den Raum jetzt verlassen: Plaintext-Protokolle mit Login (telnet, pop3) haben auf einer Firewall nichts verloren.

Blocken aller Ports

```
block in all
block out all
```

Freigeben des lokalen Netzes (Loopback)

```
pass  in quick on lo0 all
pass out quick on lo0 all
```

Freigeben des internen Netzes (sip0) für PC's mit richtiger Adresse:

```
pass   in quick on sip0 from 192.168.0.0/24 to any
pass  out quick on sip0 from any to 192.168.0.0/24
```

Freigeben des externen Netzes zum Modem:

```
pass  in quick on tlp0 from 10.0.0.138/32 to 10.0.0.140/32
pass  in quick on tlp0 from 10.0.0.140/32 to 10.0.0.138/32
```

Blocken von Adressen auf dem virtuellen PPP-Device:

```
block in on ppp0 proto tcp/udp from any to any port < 1000
```

Freigeben von Adressen auf dem virtuellen PPP-Device:

```
Pass  in on ppp0 proto tcp/udp from any to any port
  4000><6000
```

Aus *EINS* mach *VIELE*

Grundlagen: NAT

Firewall (8): NAT

Aus *EINS* mach *VIELE*

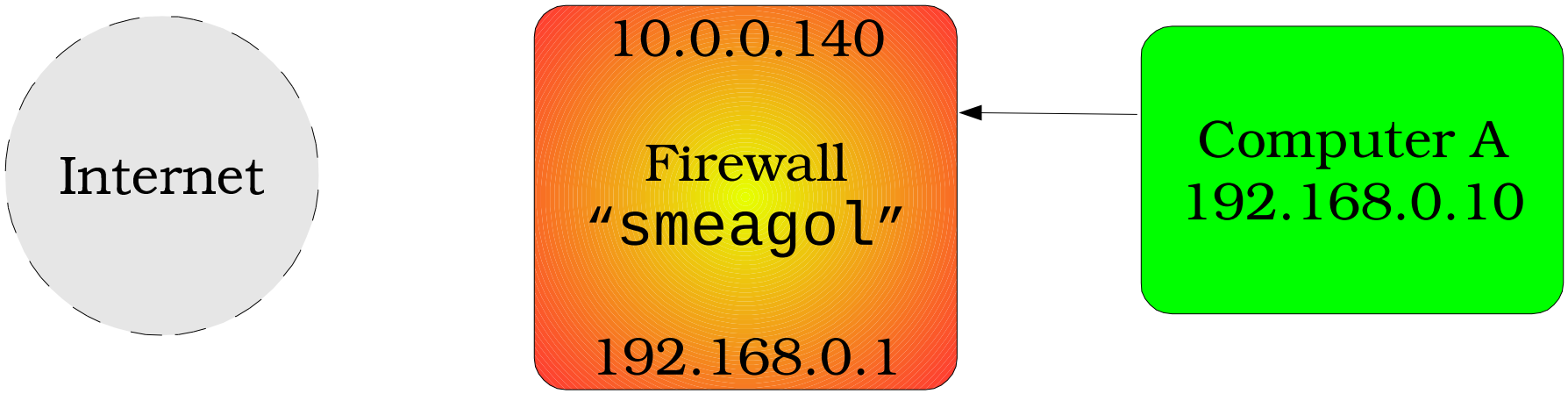
Das NAT-Prinzip (auch bekannt als Masquerading)

*) Interne IP-Adressen werden von der Firewall dynamisch auf die externe Adresse umgewandelt und von einem dynamisch zugewiesenen Port weitergeleitet

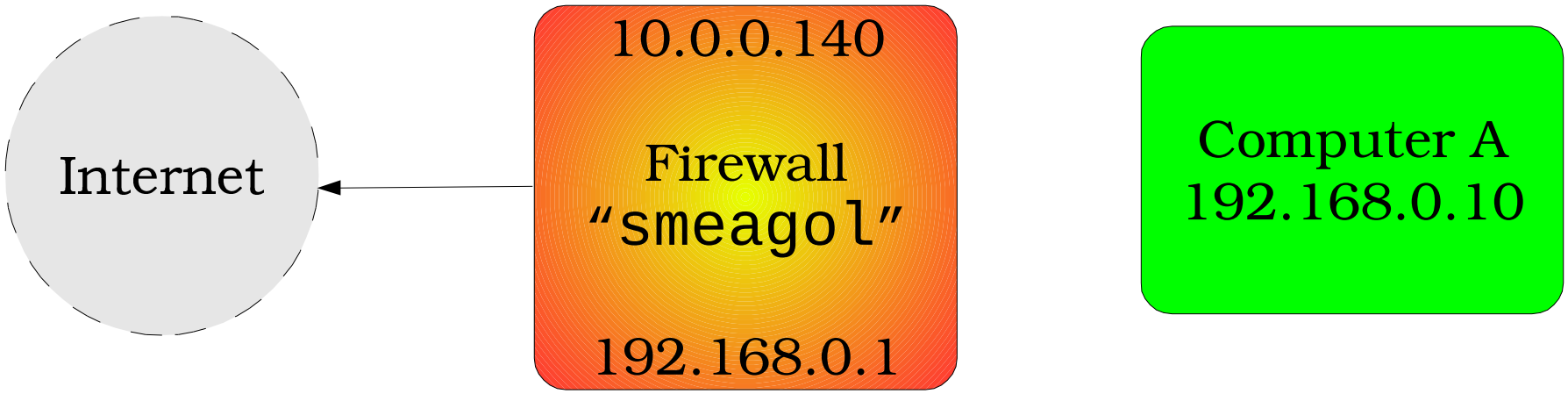
*) Antwortpakete auf diesen Port werden wieder an die ursprüngliche interne Adresse/Port-Kombination geschickt

Aus *EINS* mach *VIELE*

Anfrage an den Server
`192.168.0.10 #12345  -> 123.123.123.123 #80`

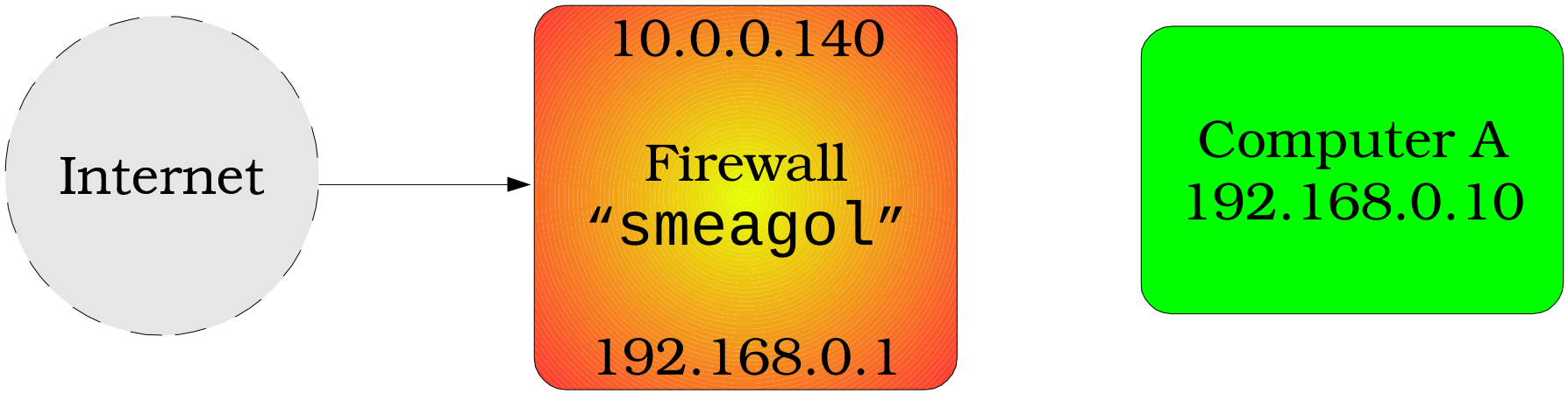


Firewall schickt Paket unter eigener Adresse weiter
`192.168.0.1 #55555  -> 123.123.123.123 #80`



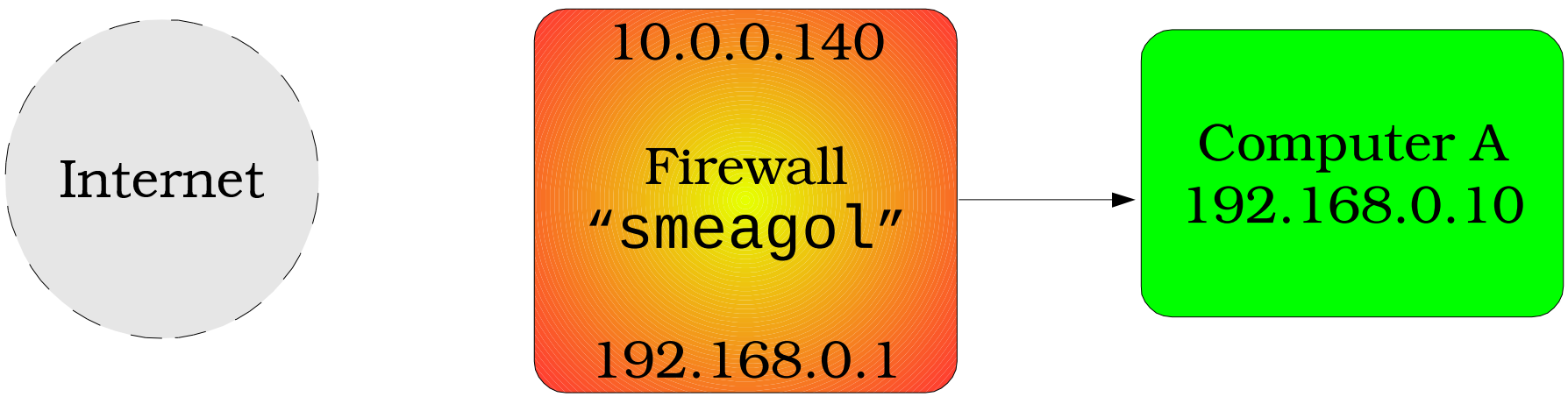
Antwort vom Server an IP-Adresse der Firewall (mit gleichem Port)

```
123.123.123.123 #80   -> 192.168.0.1 #55555
```



Firewall erkennt den NAT-Port und schick Paket an Intern

```
123.123.123.123 #80   -> 192.168.0.10 #12345
```



NAT-Rules für dieses Beispiel:

```
map ppp0 192.168.0.1/24 -> 213.229.50.215/32 portmap
     tcp/udp 40000:60000

map ppp0 192.168.0.1/24 -> 213.229.50.215/32
```

Aus *EINS* mach *VIELE*

Wo bist du? Der “Domain Name Service”

Domain Name Service

Aus *EINS* mach *VIELE*

DNS

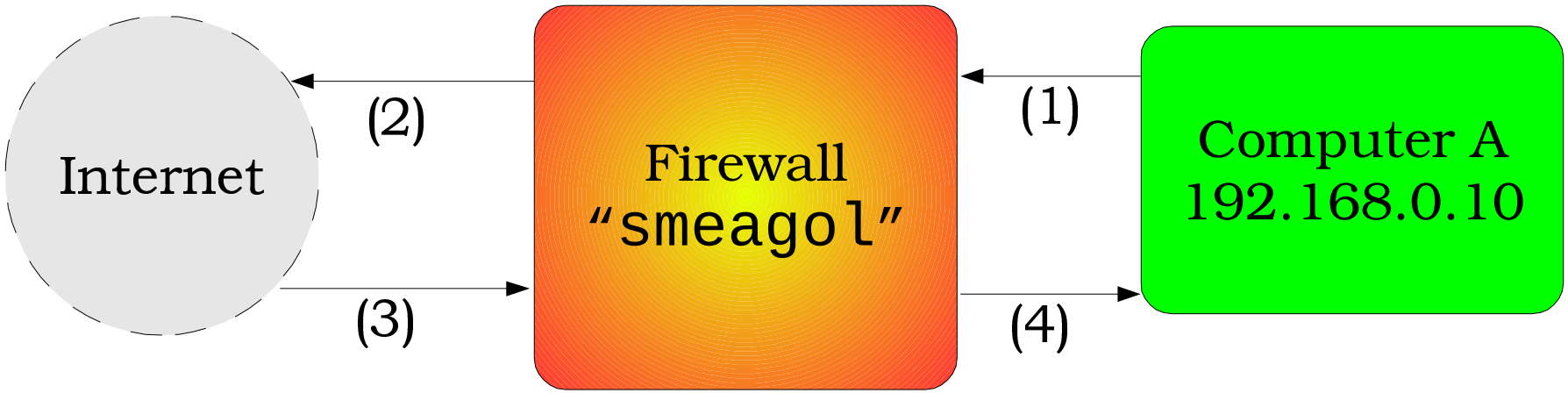
*) DNS wandelt Hostnamen in IP-Adressen (und umgekehrt) um

*) DNS funktioniert mit einer dezentralen Serverstruktur (Zone-Transfer)

*) Einrichten einer lokalen Zone mit Zone-Transfer zum restlichen Internet ist ganz leicht

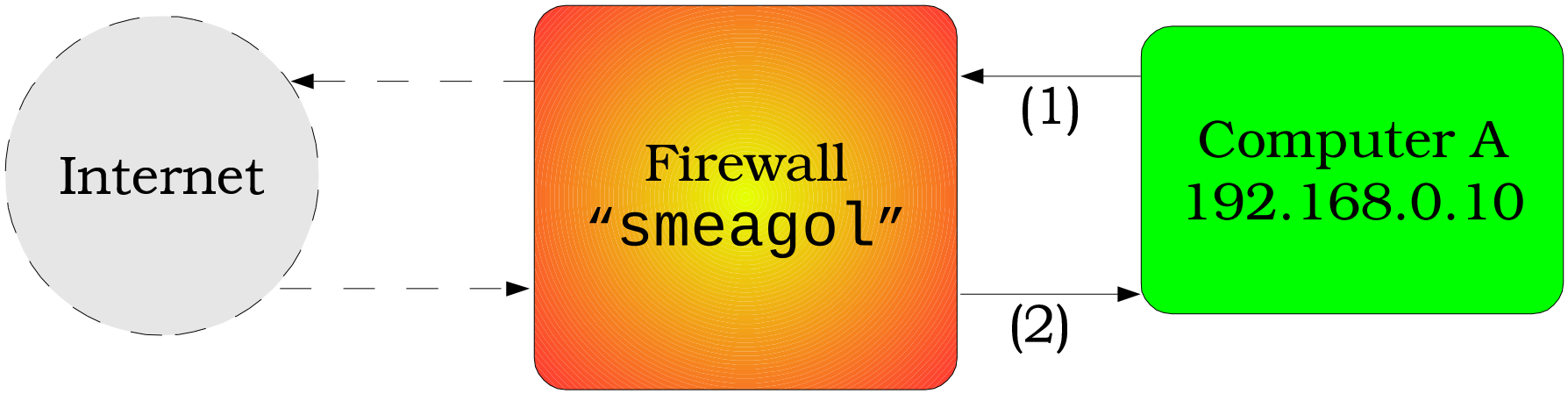
1.) DNS-Anfrage für einen externen Hostname

1) Anfrage an lokalen DNS-Server
2) Zone-Transfer zu Root-Name-Server
3) Antwort aus dem Netz (wird in lokalem DNS gecached)
4) Antwort an lokalen Computer



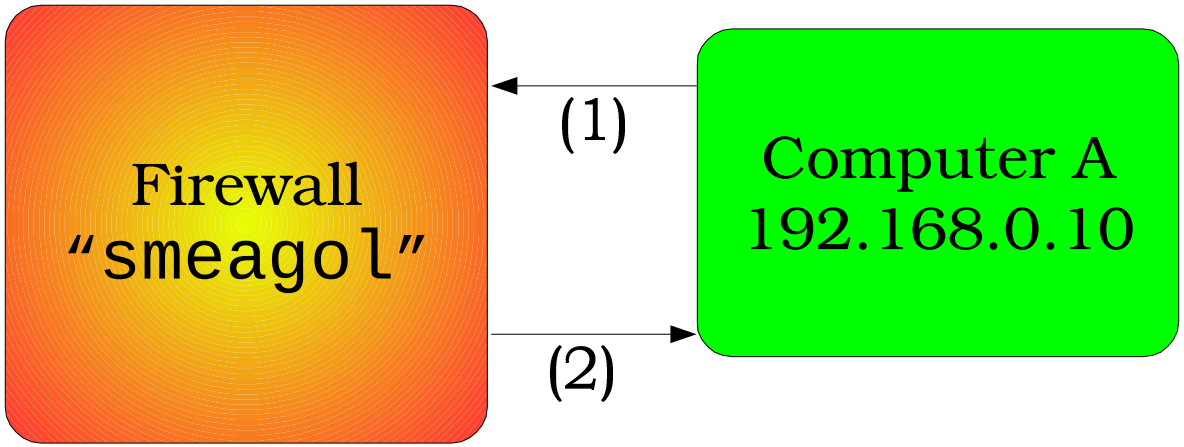
2.) DNS-Anfrage für diesen externen Hostname

1) Anfrage an lokalen DNS-Server
2) Antwort an lokalen Computer aus dem lokalen Cache



DNS-Anfrage für internen Hostname

1) Anfrage an lokalen DNS-Server
2) Antwort an lokalen Computer aus dem lokalen Cache



Aus *EINS* mach *VIELE*

Wer bin ich?
Das “DHCP”

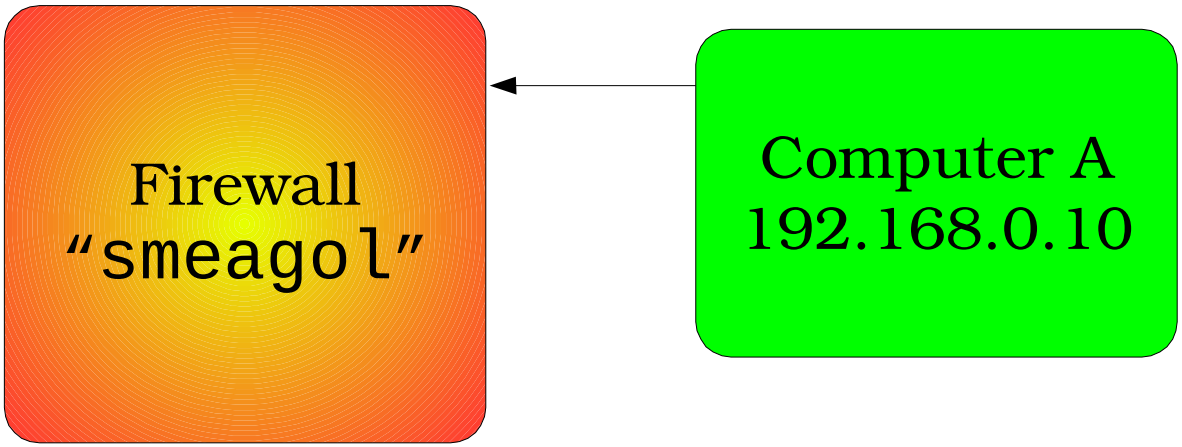
Dynamic Host Configuration Protocol

DNS-Anfrage für internen Hostname

Anfrage “Ich habe Hardware-Adresse X, bitte gib mir die Daten zum lokalen Netz”

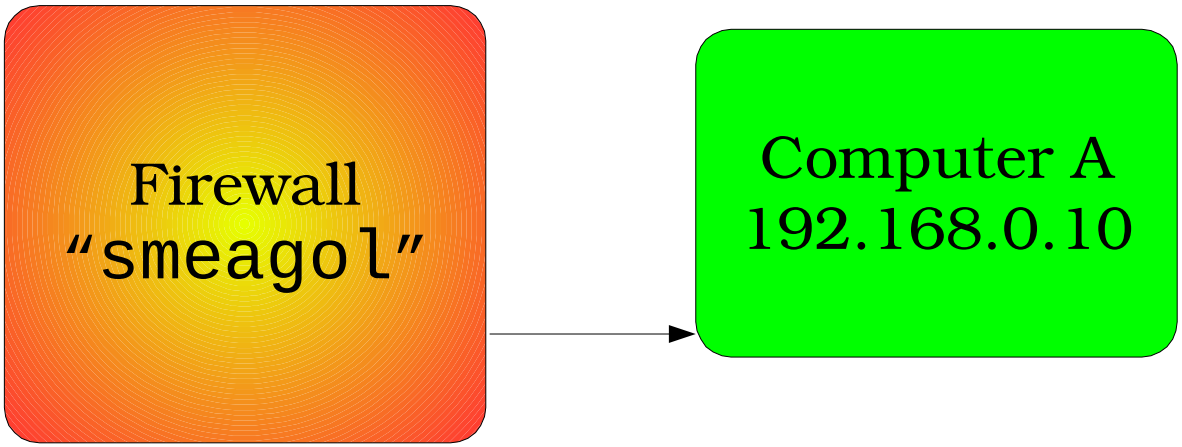
DHCP-Anfrage

“Ich habe Hardware-Adresse X, bitte gib mir die Daten zum lokalen Netz”



DHCP-Antwort

Antwort “Hallo X, deine IP-Adresse ist 192.168.0.10, die lokale Subnet-Mask ist 255.255.255.0. Dir wurde der Nameserver 192.168.0.1 zugewiesen. Der Gateway ins Internet ist ebenfalls 192.168.0.1”



Sparen beim Surfen: Proxy-Server

Proxy

Proxy

*) Speichert Anfragen/Antworten von von und zum Internet in einem lokalen Cache

*) Ein Proxy erhöht die Zugriffsgeschwindigkeit und verringert den Traffic

*) Funktionsweise ähnlich DNS

Vielen Dank fürs zuhören