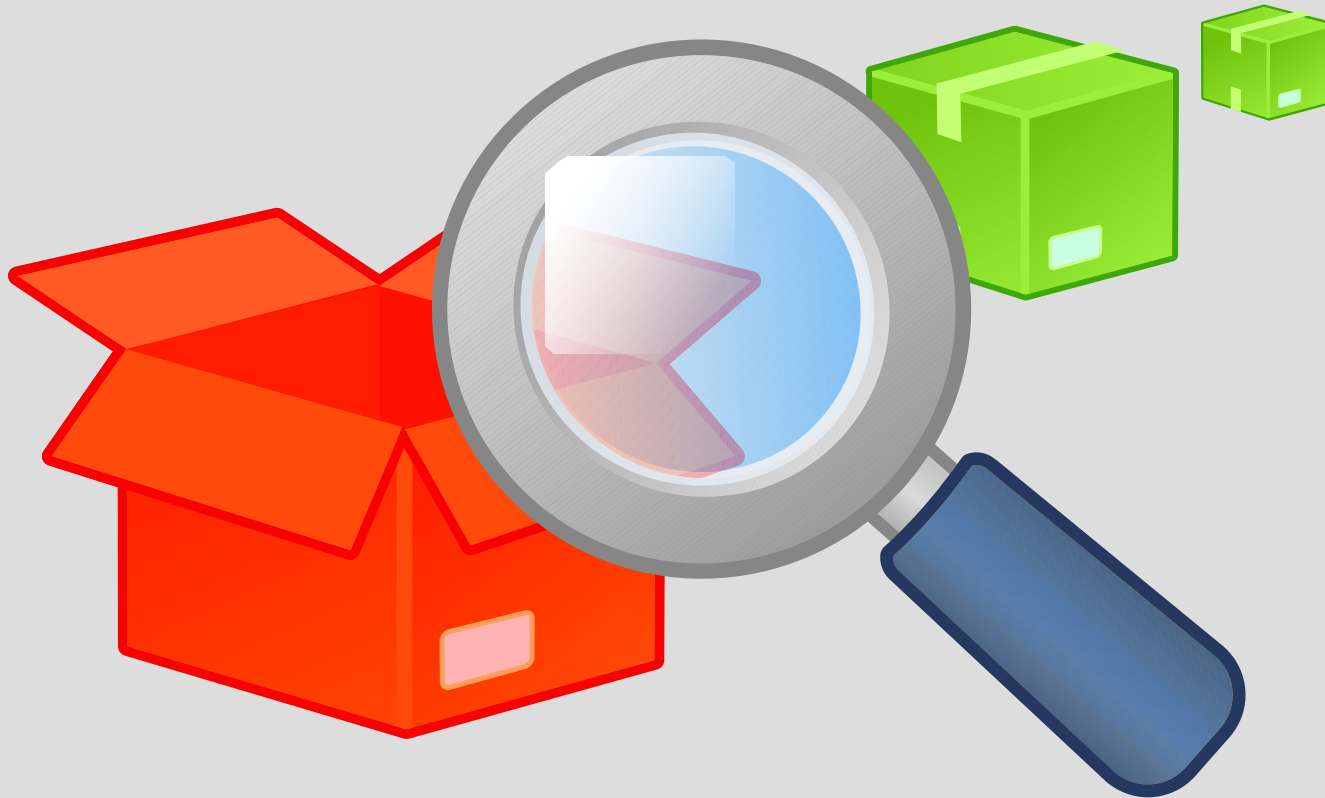


Sicherheit im Freifunk-Netz? Anomalie Erkennung

Mein Projekt und ich

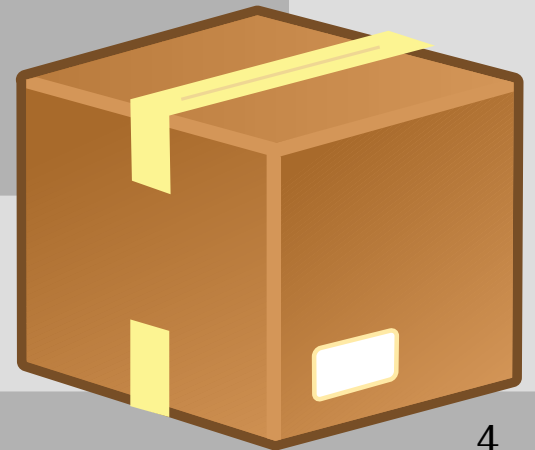


Martin | rom
U23@C4 2014
BCS Student

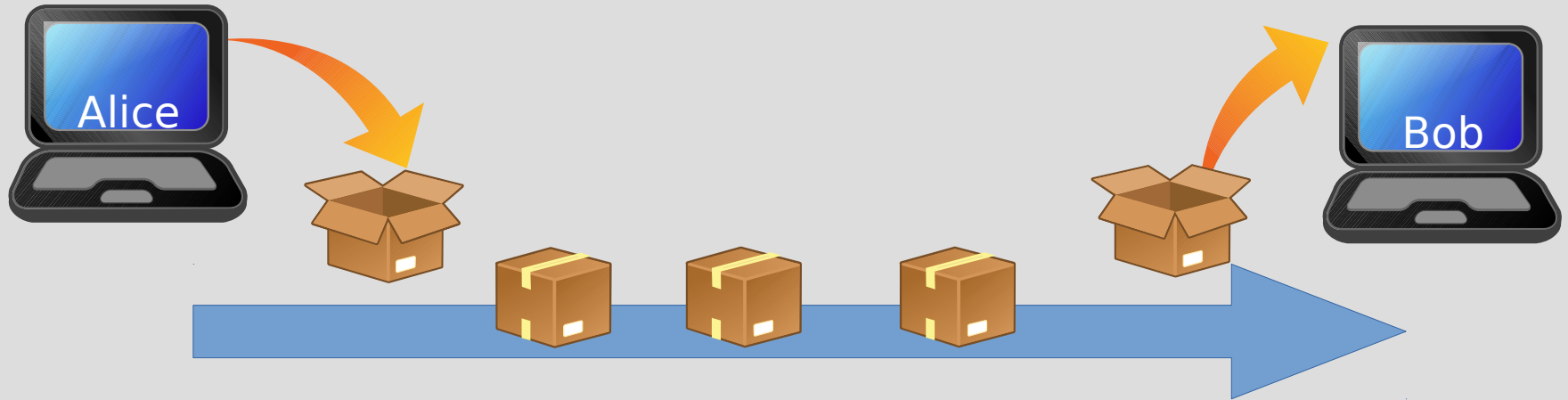
Inhaltsverzeichnis

- Pakete
- ICMPv6 (!?)
- Mathestunde
- Programm
- Demo

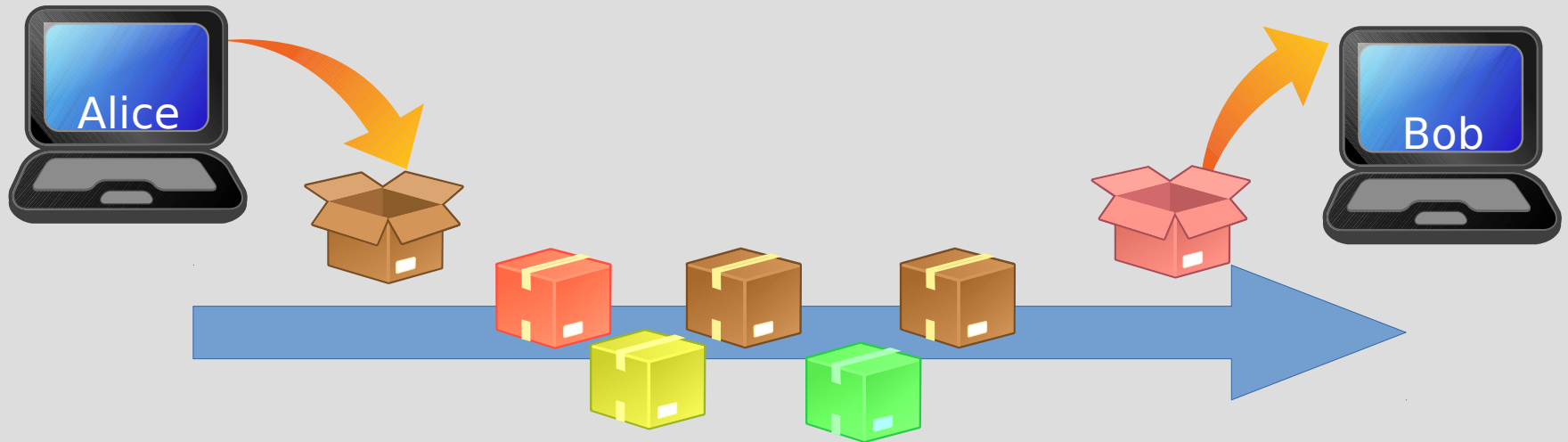
Pakete



Pakete



Pakete



IP Adressen

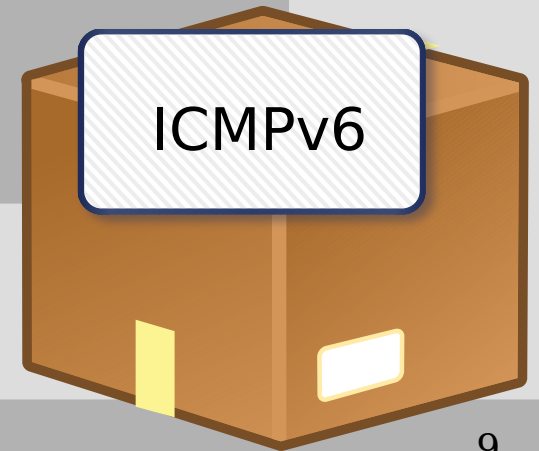


Herkunft
Ziel
<Blablabla>

IPv4:

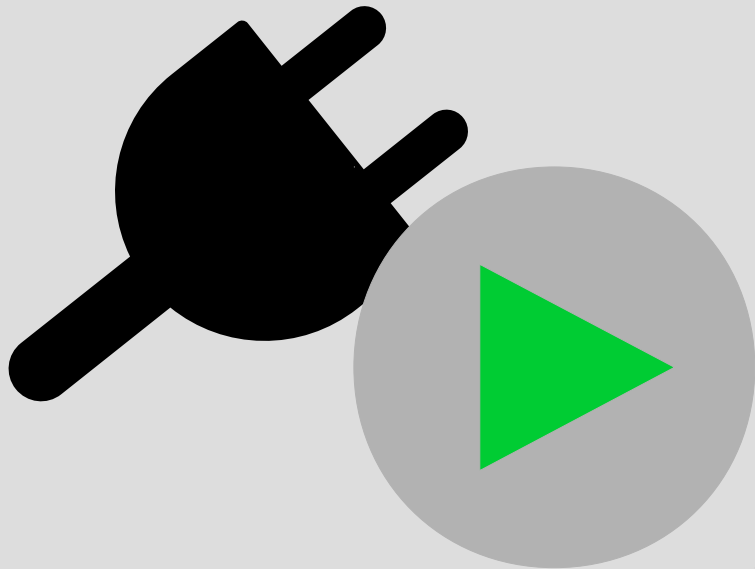
192.168.1.1
10.0.0.2
127.0.0.1

ICMPv6



IPv6 Adressen & Autokonfiguration

- „Plug and Play“

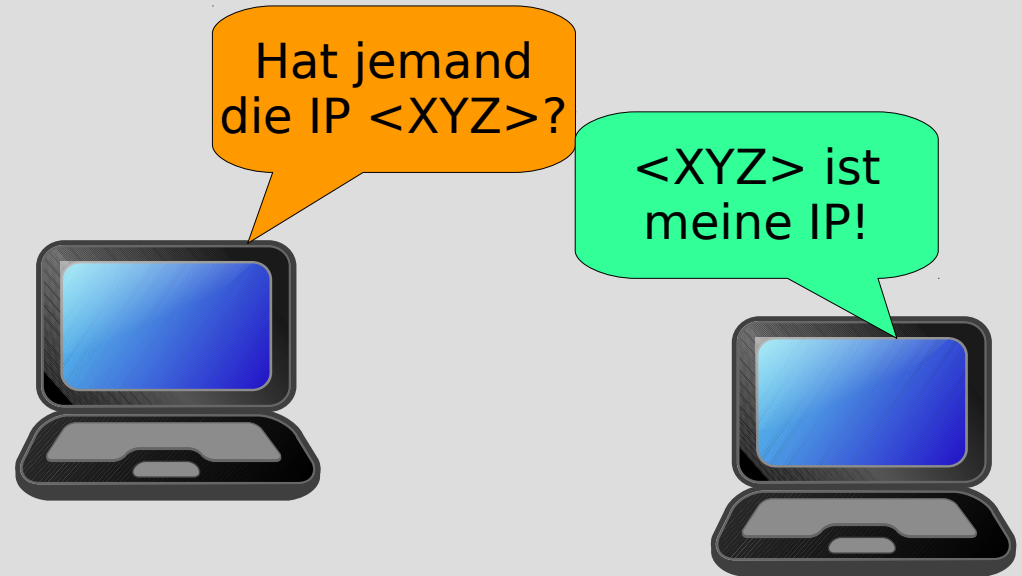


```
IPv6:  
  
::1  
fe80::a00:b1111:af3b:bb12  
2001:1001:a762:db7b:5cd4:eff5:21e3:6d
```

ICMPv6



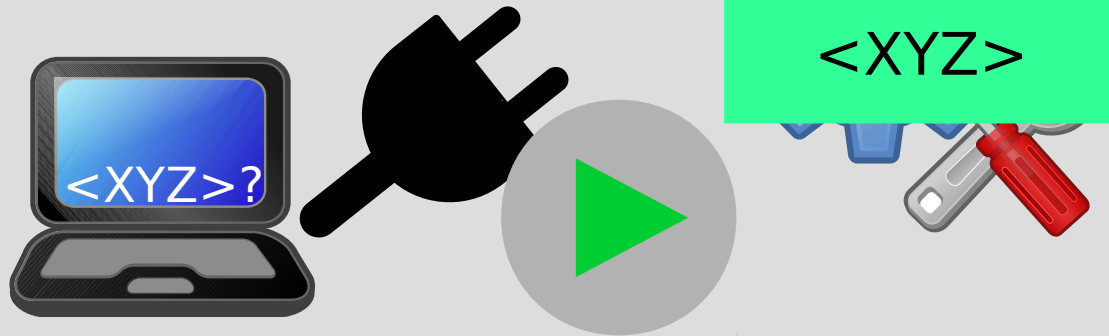
Router Advertisement



Neighbour Solicitation

Neighbour Advertisement

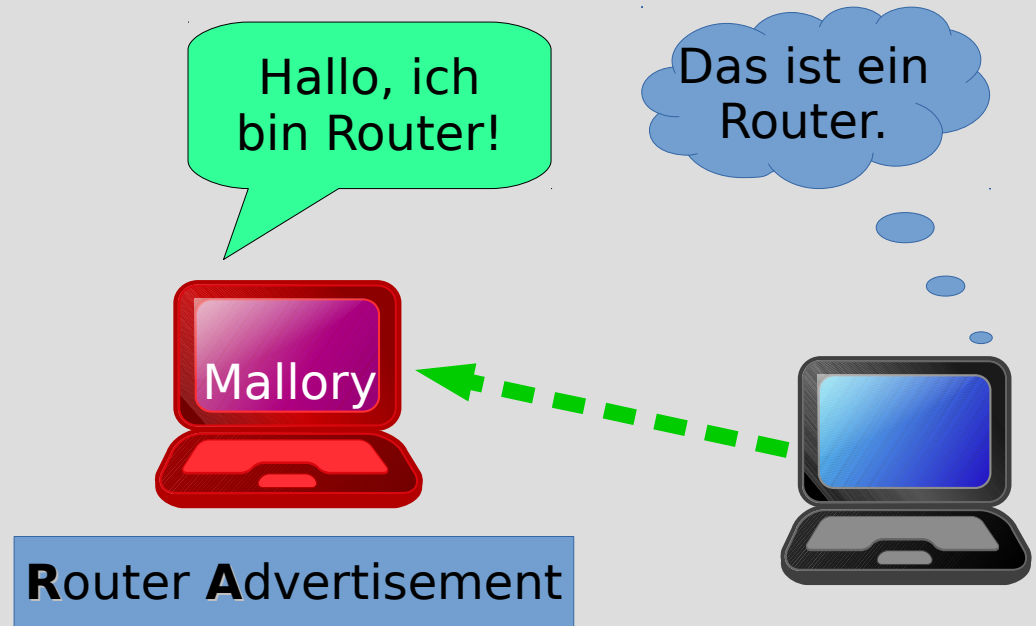
Autokonfiguration Part II



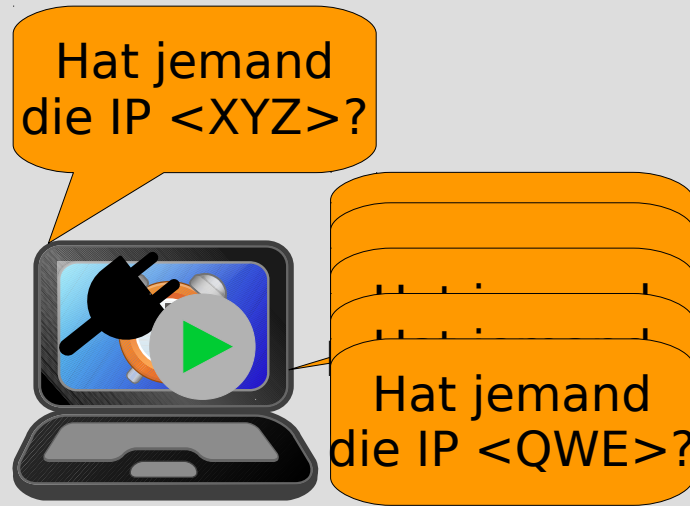
Hat jemand
die IP <XYZ>?

Neighbour Solicitation

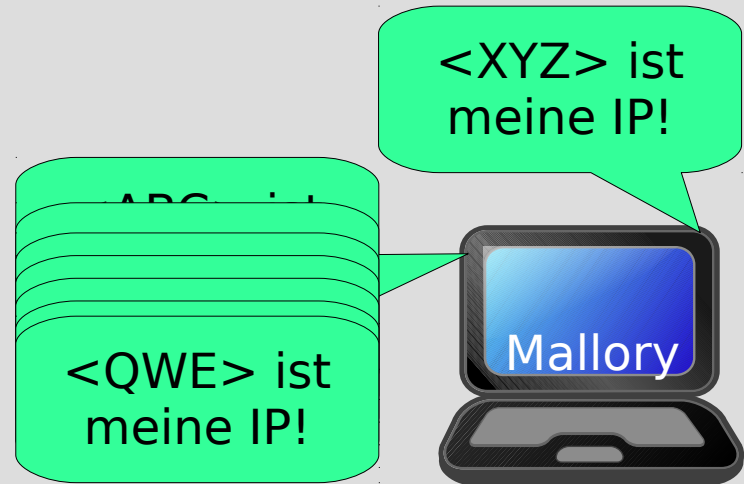
Was wäre wenn...? RA



Was wäre wenn...? NA



Neighbour Solicitation



Neighbour Advertisement

Mathestunde



16.12.2014

Martin Rosso, U23@C4
Chaos Computer Club Cologne

15

Wie erkennt man soetwas?

- Zahl der **N**eighbour **A**dvertisements (NA) von einem Node
- Zahl der **N**eighbour **S**olicitations von einem Client
- Zahl der **N**eighbour **S**olicitations von allen Clients



Wahrscheinlichkeitsrechnung

- EUI64
- Zufall

62bit der IPv6 $\rightarrow n = 2^{62}$ (ca. 5 Trillion)


$n!$ ca. 5 Trillionen Nullen

.....

\rightarrow unwahrscheinlich

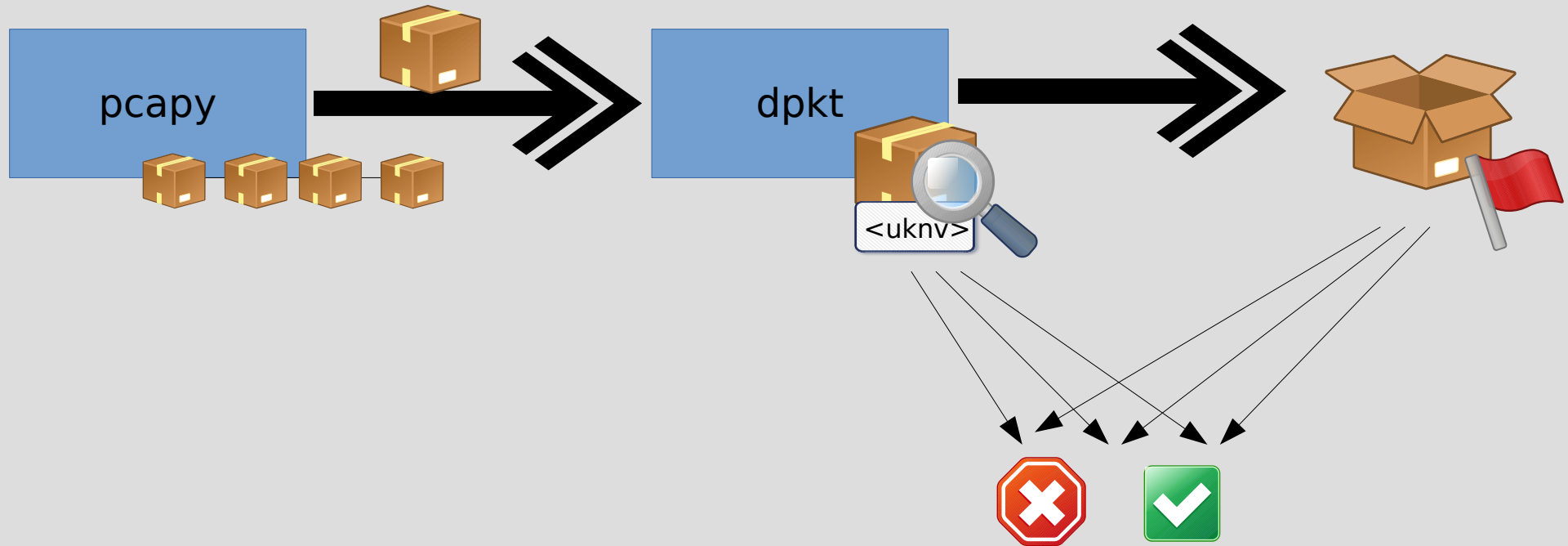
$$\frac{n!}{k!(n-k)!} = \binom{n}{k}$$

Programm



```
Ajhfi wnfafkglmia  
wo8e()  
Jndodvdso(„56“)  
Isdgj = „nsa“ + s
```

Funktionsweise



Quellcode

Live Demo



Zukunft und Pläne

- Code umstrukturieren, säubern
- Mehr Features
- Veröffentlichen
- Einsatz



Fragen?

Pakete – ICMPv6 – Mathe

Vielen Dank