Routing entry for 10.0.0.0/8, 3234 known subnets

Att **Routing, NAT, Firewall**

Variably subnetted with 18 masks

Redistributing via eigrp 287

B 10.12.144.163/32 [200/0] via 212.55.

D EX 10.12.139.184/29

[170/26112] via 212.55.192.

[170/26112] via 212.55.192.19

B 10.220.224.0/20 [200/20000] via

B 10.212.232.0/24 [200/10] via 194.4

B 10.204.240.0/24 [200/10000] via 217.

B 10.192.252.0/24 [200/20000] via 212.5

B 10.150.170.0/24 [200/20000] via 212.55.

B 10.60.0.0/17 [200/20000] via 212.55.192.2

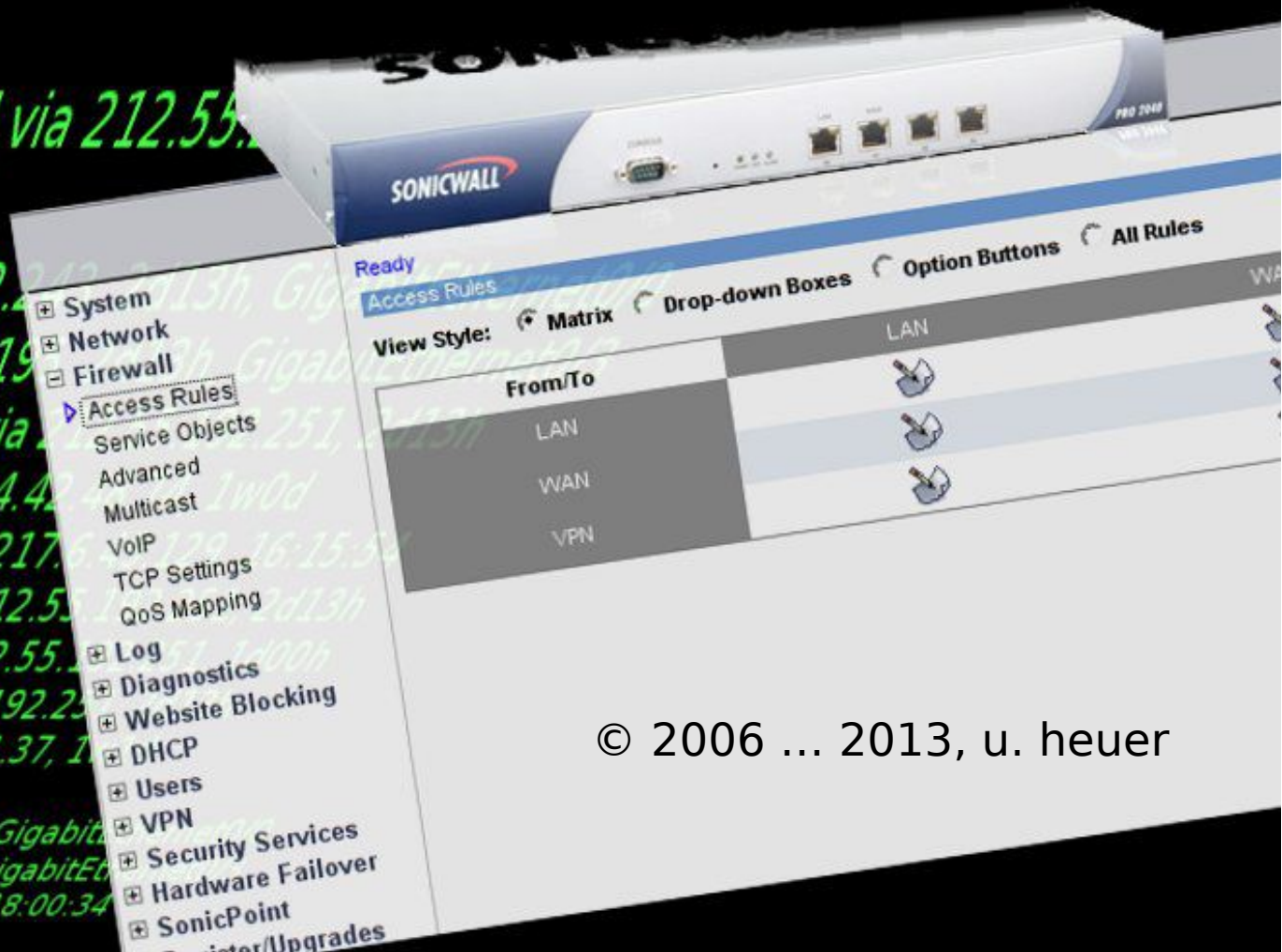
B 10.24.36.0/24 [200/10000] via 139.4.71.37, 1

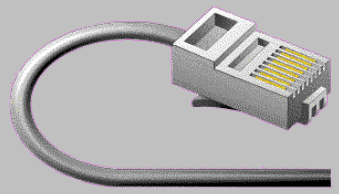
D EX 10.12.176.128/28

[170/28672] via 212.55.192.243, 2d13h, Gigabit

[170/28672] via 212.55.192.195, 2d13h, GigabitEt

B 10.12.168.152/29 [200/0] via 10.12.179.33, 18:00:34





Routing, NAT, Firewall

Host Routing

Wie leitet ein Host die IP-Pakete weiter

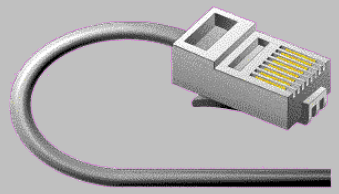
NAT / PAT

Wie funktioniert NAT / PAT

Firewall Zonen

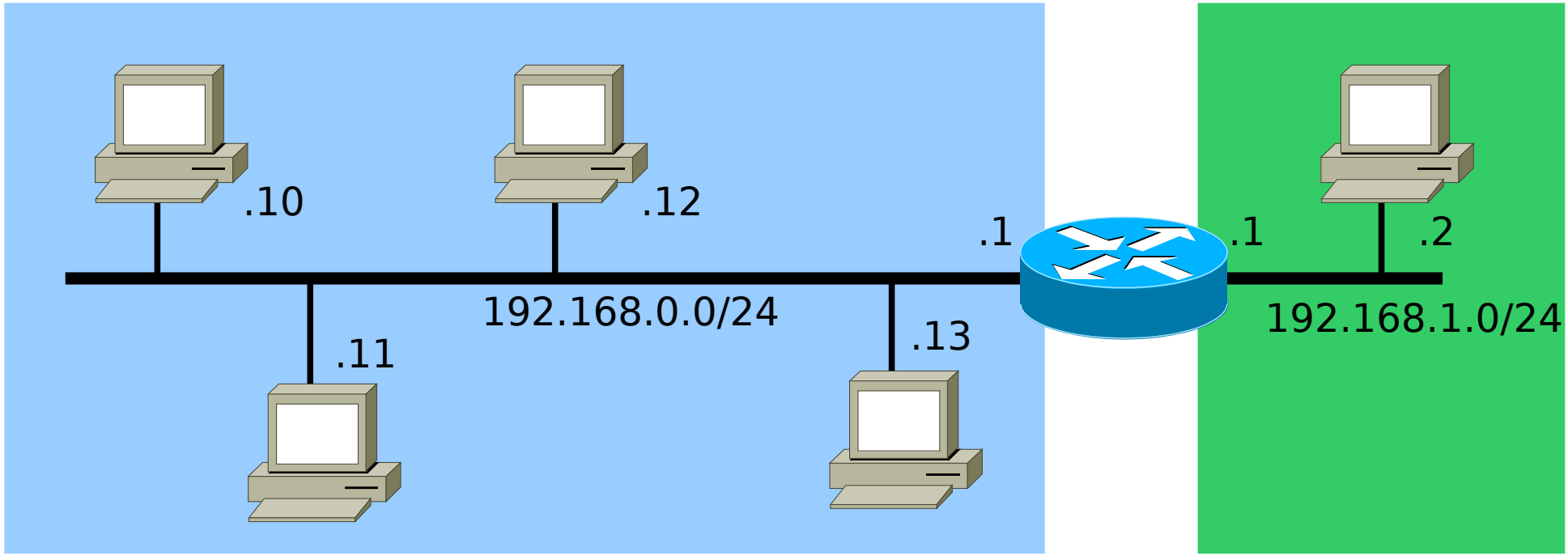
Warum werden Zonen erstellt

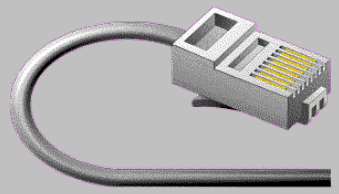
Wie muss man Regeln definieren



Host Routing

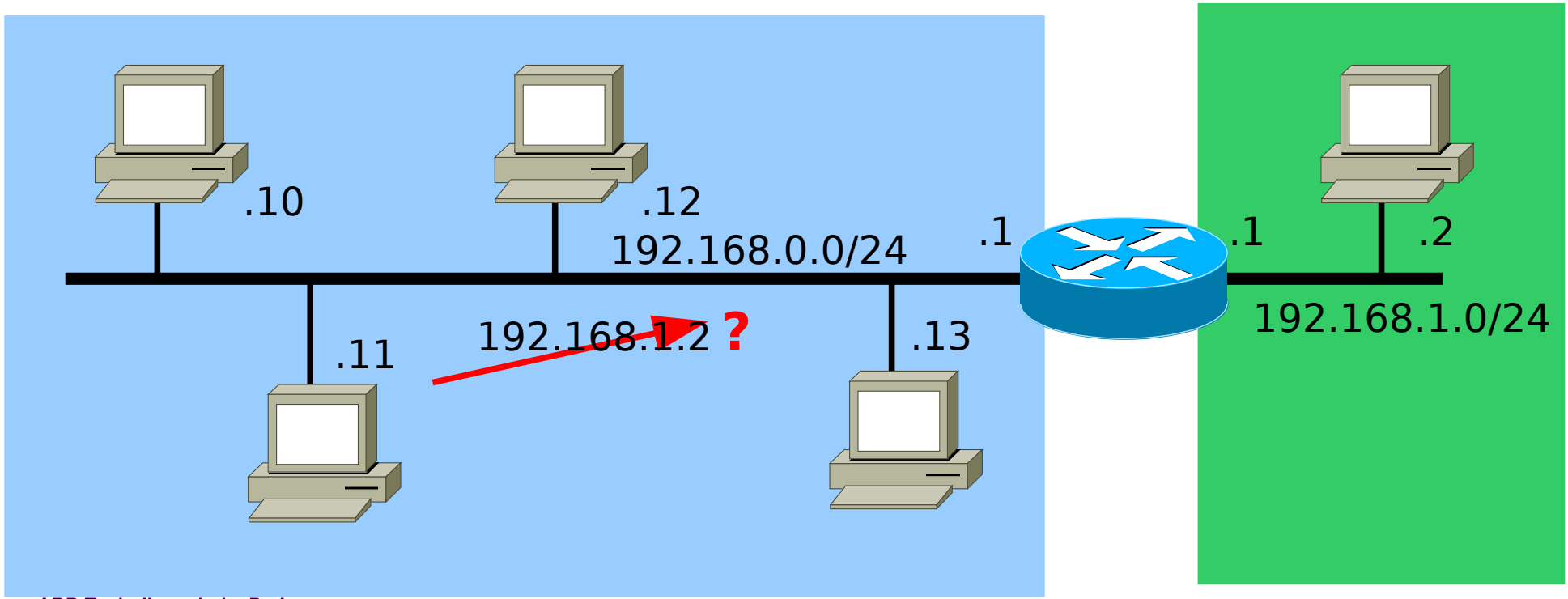
Ein Rechner kann alle Hosts, die sich im selben Subnetz befinden, direkt erreichen.
Jeder Rechner kann anhand seiner IP-Adresse und Netzmaske bestimmen, ob ein Host direkt ansprechbar ist

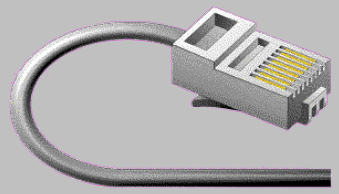




Host Routing

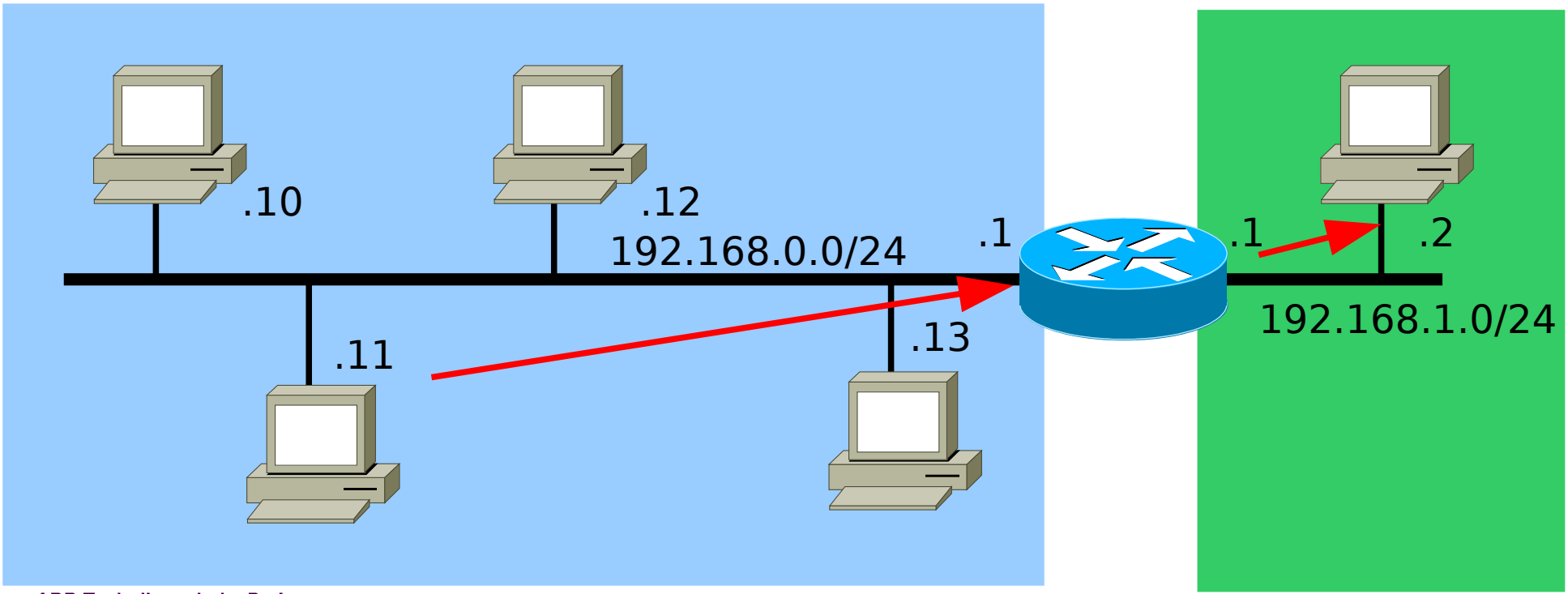
Ein Rechner aus dem blauen Subnetz kann nicht selber einen Rechner im grünen Subnetz ansprechen, da er das 'fremde' Netz nicht erreichen kann.

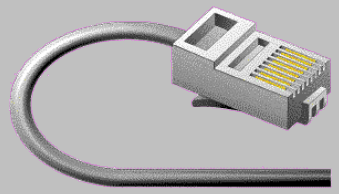




Host Routing

Um das 'fremde' Netz zu erreichen muss der blaue Rechner das Paket an den Router senden. Der Router kann das Paket ins 'grüne' Netz weiterleiten so, dass es ans Ziel kommt.

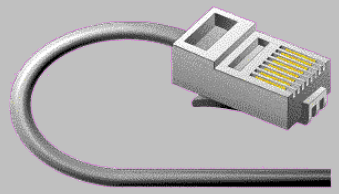




Host Routing

Jeder Host hat eine eigene Routing Tabelle, in der für jedes Netz das Interface und gegeben falls die notwendige Gateway IP-Adresse eingetragen ist.

Destination	Gateway	Genmask	Iface
212.55.196.64	0.0.0.0	255.255.255.248	eth0
192.168.1.0	0.0.0.0	255.255.255.0	eth1
0.0.0.0	212.55.196.65	0.0.0.0	eth0

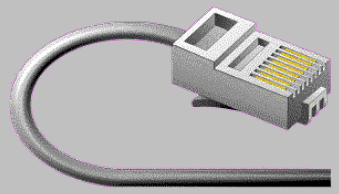


Host Routing

Muss ein Gateway für eine Ziel-Adresse gesucht werden, so wird der Eintrag gewählt, der das Ziel am genausten beschreibt.

Beispielsweise wird bei der folgenden Tabelle ein Paket an die Ziel-adresse 192.168.168.5 an den Gateway 172.16.23.2 gesendet. Der Eintrag für 192.168.168.0/24 beschreibt das Ziel genauer als 192.168.0.0/16! (most specific route)

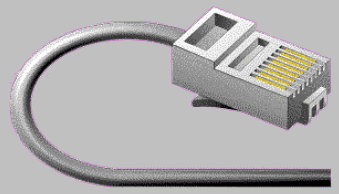
Destination	**Genmask**	**Gateway**	**Iface**
172.16.23.0/24	255.255.255.0	0.0.0.0	eth0.100
192.168.0.0/16	255.255.0.0	172.16.23.1	eth0.100
192.168.168.0/24	255.255.255.0	172.16.23.2	eth0.100



Host Routing

Oft sind die Routingtabellen nach der Netzmaske (absteigend) sortiert, so dass immer der erste passende Eintrag verwendet werden kann.

```
$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Iface
192.168.255.7   172.16.23.1     255.255.255.255 eth0.100
192.168.255.3   172.16.23.1     255.255.255.255 eth0.100
192.168.255.16  172.16.23.1     255.255.255.255 eth0.100
212.55.196.64   0.0.0.0         255.255.255.240 eth0.3
192.168.24.0    0.0.0.0         255.255.255.240 eth0.500
192.168.24.32   192.168.24.1    255.255.255.224 eth0.500
192.168.23.0    0.0.0.0         255.255.255.0   eth1
172.16.7.0      172.16.23.1     255.255.255.0   eth0.100
172.16.23.0     0.0.0.0         255.255.255.0   eth0.100
172.16.3.0      172.16.23.1     255.255.255.0   eth0.100
192.168.42.0    0.0.0.0         255.255.255.0   eth0.5
0.0.0.0         212.55.196.65   0.0.0.0         eth0.3
```

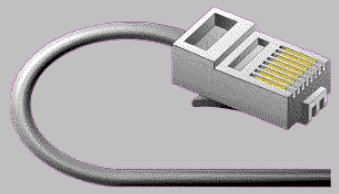


Host Routing

Wird kein passender Eintrag gefunden so kann das Paket **NICHT** weitergeleitet werden, das Paket wird verworfen und der Absender per ICMP (unreachable) informiert.

Die **default Route** (0.0.0.0/0) ist eine Route, die das ganze Internet umfasst.

Destination	**Gateway**	**Genmask**	**Iface**
0.0.0.0	212.55.196.65	0.0.0.0	eth0.3



Routing Tabelle anpassen

Statisches Routing

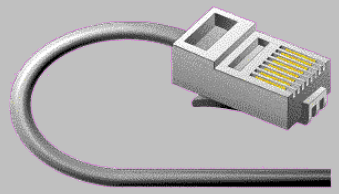
UNIX/Linux:

Anzeigen: `route` oder
`route -n` damit die IP-Adressen nicht aufgelöst werden.
Hinzufügen: `route add -net <a.b.c.d/n> gw <gw-ipaddr>`
Löschen: `route del -net <a.b.c.d/n> gw <gw-ipaddr>`

Als Zieladresse kann anstelle von gw <gw-ipaddr> auch reject angegeben werden. Die Paket werden dann verworfen.

IPv6
Anzeigen: `route -A inet6`
Hinzufügen: `route -A inet6 add -net <Ipv6Net/n> gw <gw-ipv6addr>`
Löschen: `route -A inet6 del -net <Ipv6Net/n> gw <gw-ipv6addr>`

Die Routing Tabelle kann auch mit dem Befehl ip(8) modifiziert werden.



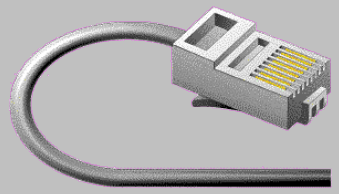
Routing Tabelle anpassen

Statisches Routing

OS X

Anzeigen: `netstat -rf inet`
Hinzufügen: `route add <a.b.c.d/n> <gw-ipaddr>`
Löschen: `route delete <a.b.c.d/n> <gw-ipaddr>`

IPv6
Anzeigen: `netstat -rf inet6`
Hinzufügen: `route add -inet6 <Ipv6Net> -prefixlen <n> <gw-ipv6addr>`
Löschen: `route delete -inet6 <Ipv6Net> -prefixlen <n> <gw-ipv6addr>`



Routing Tabelle anpassen

Statisches Routing

Windows:

Anzeigen: `route print`

Hinzufügen: `route add <netz> mask <mask> <gateway>`

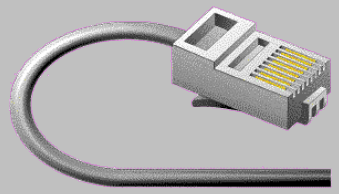
Löschen: `route delete <netz>`

IPv6

Anzeigen:

Hinzufügen: `netsh interface ipv6 add route <Ipv6>/<n> <Ipv6-gw>`

Löschen: `netsh interface ipv6 delete route <Ipv6>/<n> <Ipv6-gw>`



Routing Tabelle anpassen

Statisches Routing

Cisco/IOS

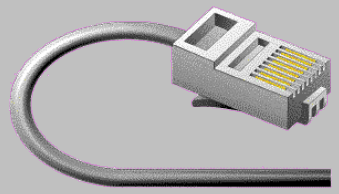
Anzeigen: `show ip route`
Hinzufügen: `ip route <netz> <mask> <gateway>`
Löschen: `no ip route <netz> <mask> <gateway>`

Cisco/Nexus:

Anzeigen: `show ip route`
Hinzufügen: `ip route <netz>/<mask> <gateway>`
Löschen: `no ip route <netz>/<mask> <gateway>`

Cisco IPv6

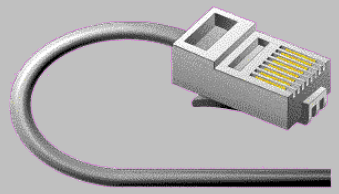
Anzeigen: `show ipv6 route`
Hinzufügen: `ipv6 route <netz>/<prefix> <gateway>`
Löschen: `no ipv6 route <netz>/<prefix> <gateway>`



Routing Tabelle anpassen

Statisches Routing funktioniert bei den anderen Betriebssysteme / Hardware-Hersteller analog den aufgeführten Beispielen.

Je nach Produkt kann die Anzahl der möglichen Einträge stark variieren.

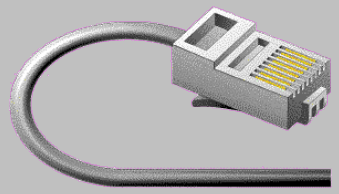


Routing Grundsätze

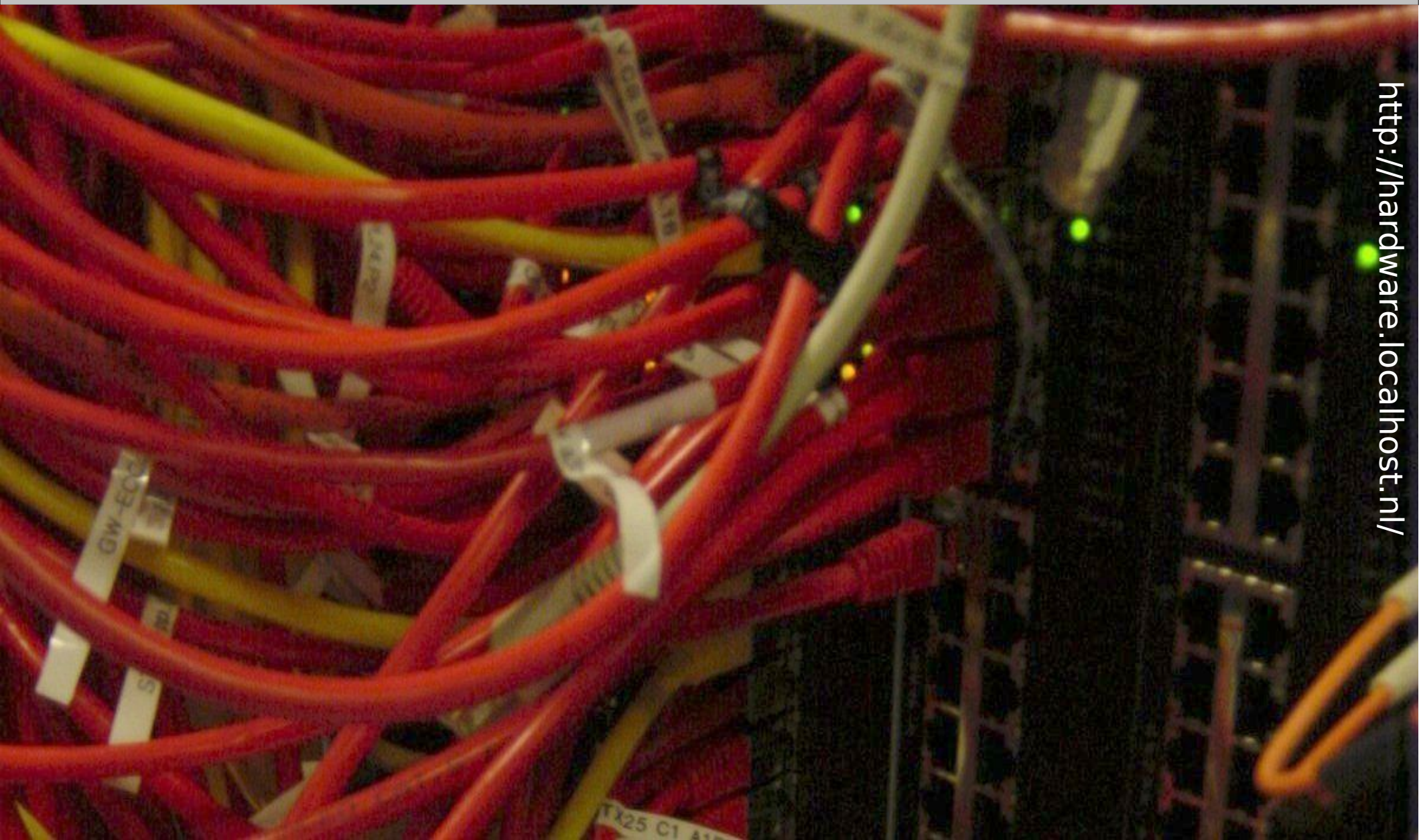
Einzig die *eigene* Routing-Tabelle ist relevant für das Routing vom Host.

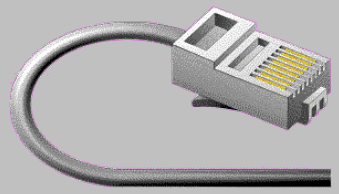
Der nächste Host muss seine eigene Routing-Tabelle konsultieren, um zu entscheiden, wo hin er das empfangene Paket weiter senden soll.

Routing Protokolle (RIP,OSPF,ISIS,BGP,...) sind einzig dazu da, um den Inhalt der Routing Tabelle zwischen verschiedenen Hosts zu synchronisieren.
Wie das funktioniert werden wir später sehen.



Fragen?

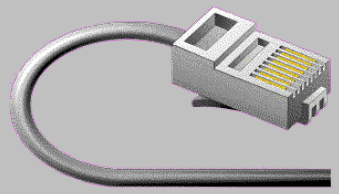




Andere Routing Ansätze

Neben dem normalen Routing gibt es weitere Ansätze um die Pakete weiterzuleiten.

- Policy routing
- Multi Protocol Label Switching (MPLS)

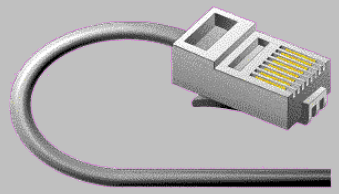


Policy Routing

Routing inspiziert die Ziel-Adresse vom Paket. Die Source-Adresse spielt keine Rolle!

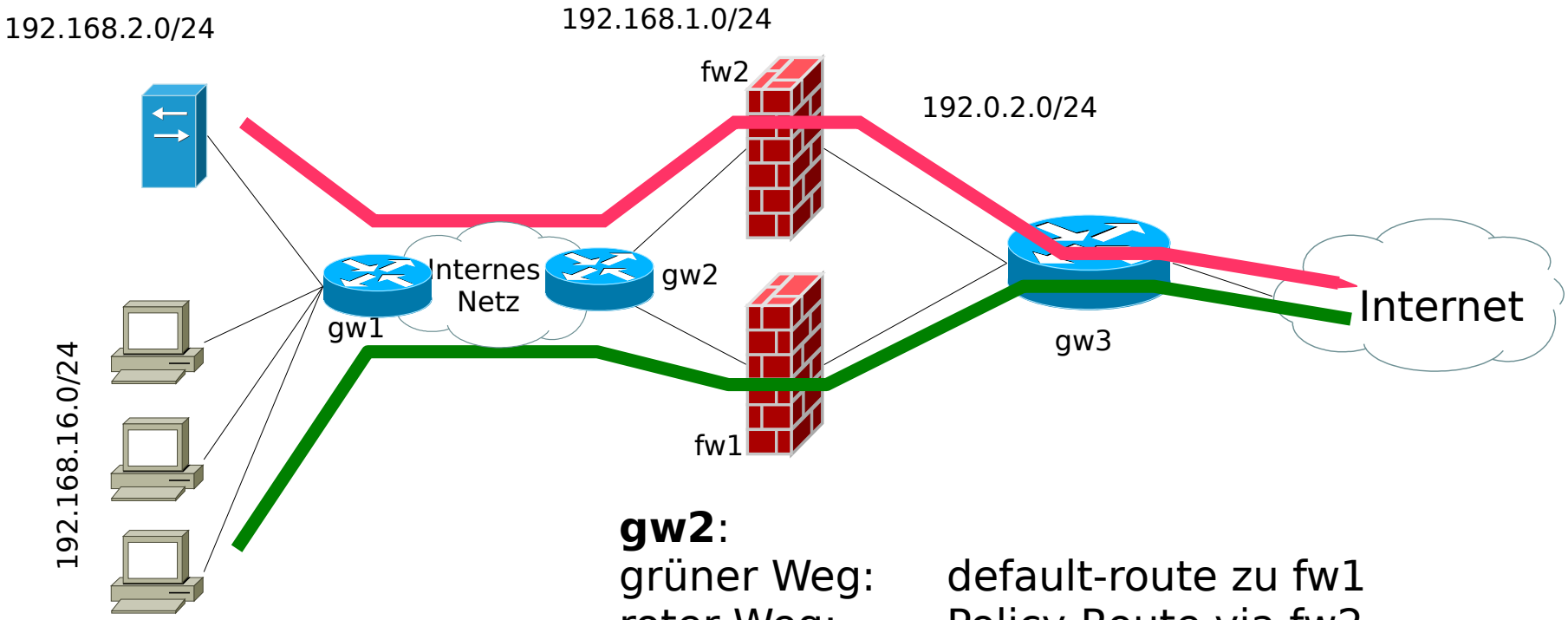
Soll das Paket aufgrund der Source-Adresse (oder auch anderen Kriterien) geroutet werden, so spricht man von Policy-Routing.

- Policy-Routing zu konfigurieren ist aufwendig und fehleranfällig.
- Policy-Routing soll nur dann verwendet werden, wenn es absolut nicht anders möglich ist

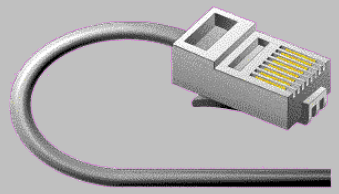


Policy Routing

Beispiel: Für die Telefon-Anlage aus dem Netz 192.168.2.0/24 soll ein zweite Firewall (fw2) verwendet werden. Alle anderen Benutzer müssen die erste Firewall verwenden.



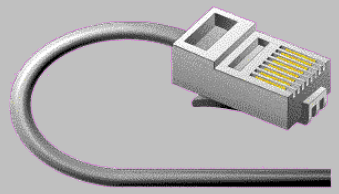
gw2:
grüner Weg: default-route zu fw1
roter Weg: Policy-Route via fw2



Routing / MPLS

Neben der Ziel-IP-Adresse können - zusätzlich definierte - Labels als Routing Information verwendet werden.

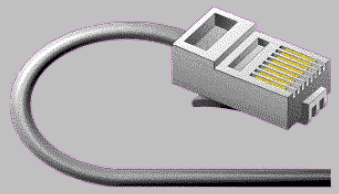
Der Router fügt jedem Paket aufgrund seier Ziel-Adresse ein Label hinzu.
Der Weg durch das Netzwerk wird aufgrund diesem Label bestimmt



Routing / MPLS

Hinter einem Label kann sich ein beliebiges Paket 'verstecken'. Einzig der Eintritts- und Austritts Router muss das Paket ohne Label verarbeiten können.

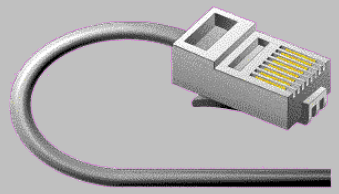
Da verschiedene Protokoll sich hinter den Labels der Pakete verstecken wird das als Multiprotocol Label Switching (MPLS) genannt.



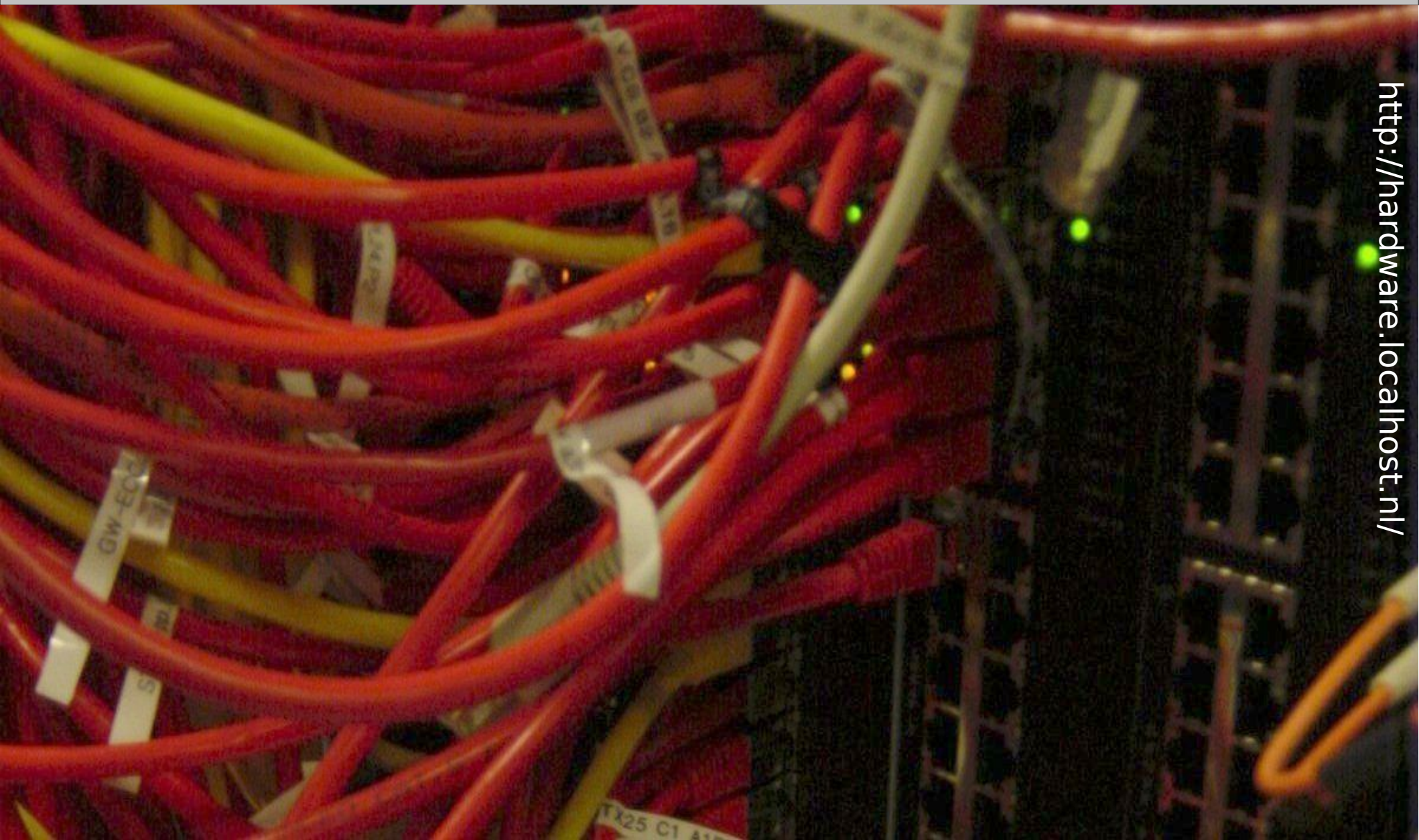
Routing / MPLS

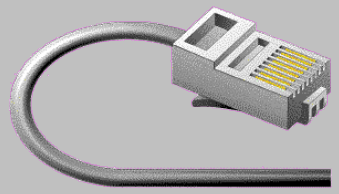
Es können mehrere Labels hintereinander hinzu gefügt werden. So können verschiedene Netze getrennt im gleichen globalen Netz voneinander geroutet werden. (MPLS VPN)

Für MPLS VPNs müssen die Router an den Eintrittspunkten die Routing Tabellen der verschiedenen Kunden getrennt halten. Man spricht von **Virtual Routing and Forwarding** (**VRF**).



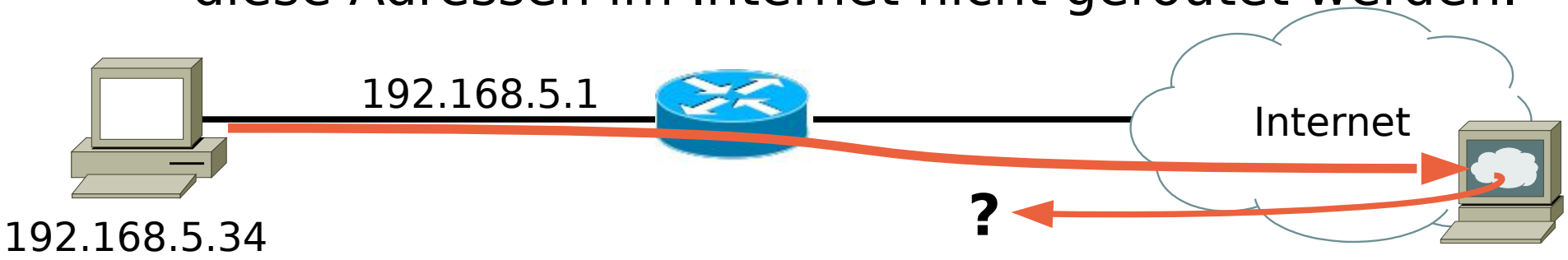
Fragen?





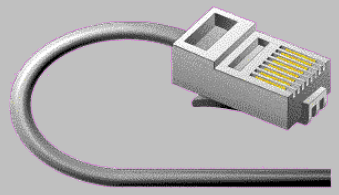
NAT / PAT

Werden private IP-Adressen (RFC1918) eingesetzt, sind diese Adressen im Internet nicht erreichbar, da diese Adressen im Internet nicht geroutet werden.

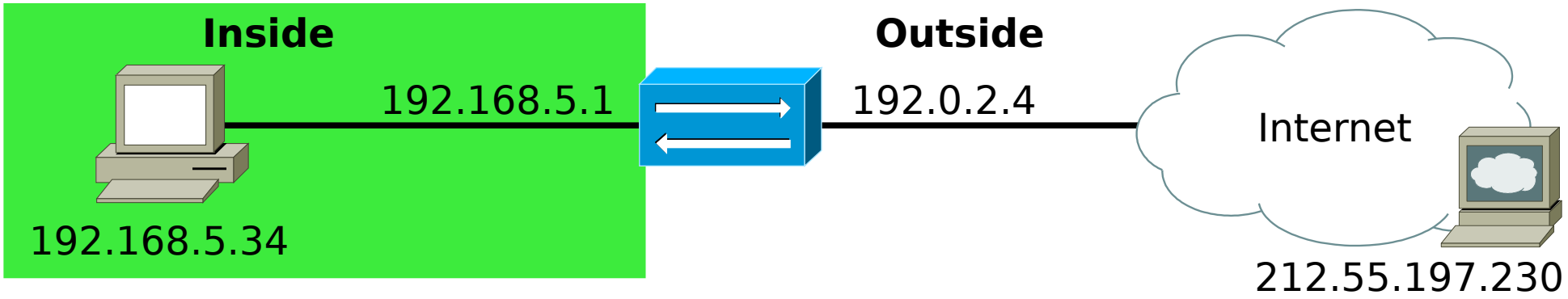


192.168.5.34:39218 → 212.55.197.230:80
192.168.5.34:39218 ← 212.55.197.230:80

Problem:
RFC1918 IP-Adressen werden im Internet nicht geroutet - d.H. das Antwort-Paket kann das Ziel nie erreichen



Network Address Translation NAT



192.168.5.34:39218 → 212.55.197.230:80

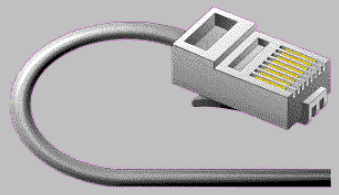
192.0.2.4:39218 → 212.55.197.230:80

192.0.2.4:39218 ← 212.55.197.230:80

192.168.5.34:39218 ← 212.55.197.230:80

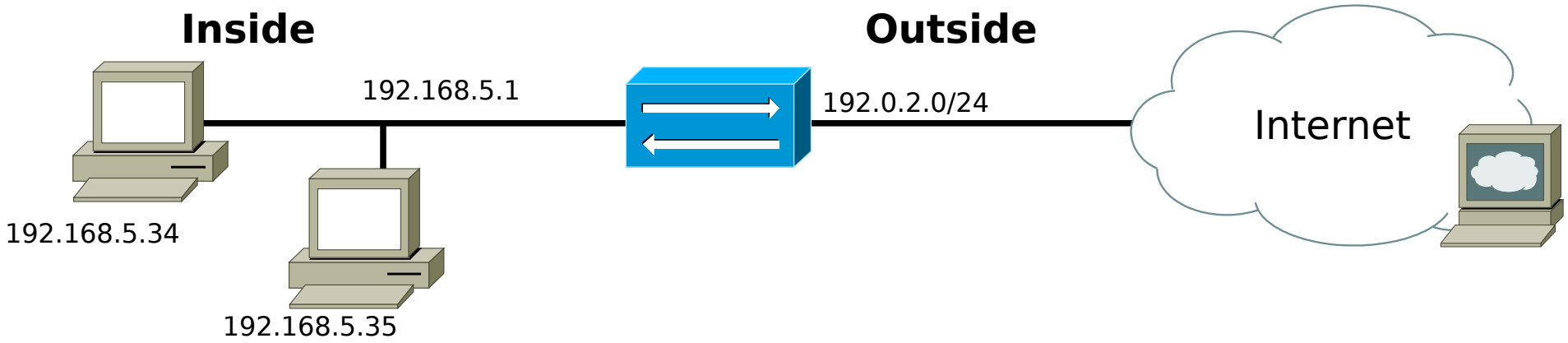
NAT-Tabelle

Inside	Outside
192.168.5.34:39218 ↔ 212.55.197.230:80	192.0.2.4:39218 ↔ 212.55.197.230:80



Network Address Translation NAT

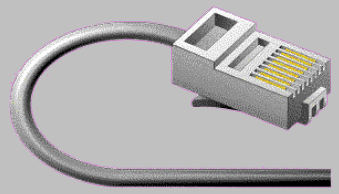
Sind mehrere inside Host vorhanden, so wird bei NAT für jeden Host eine externe IP-Adresse benötigt.



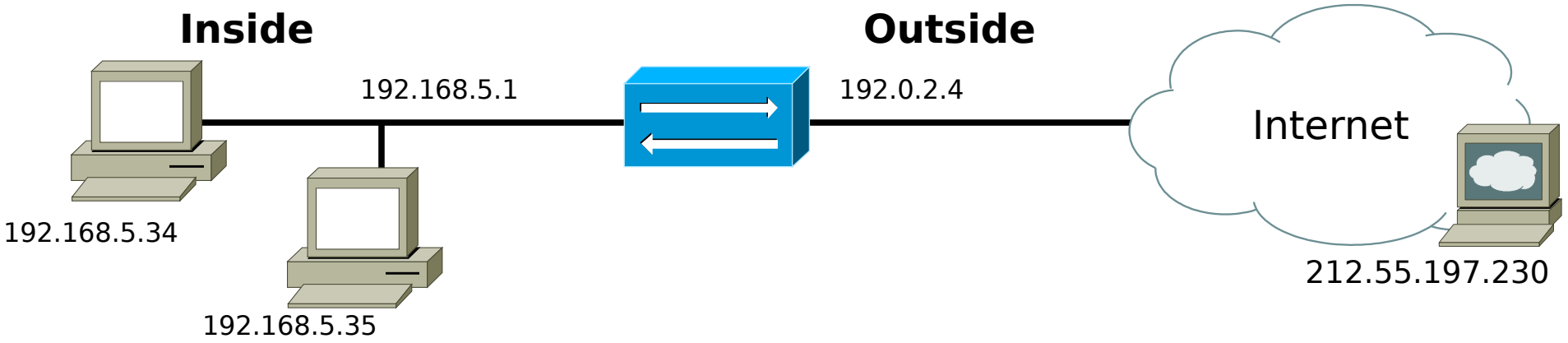
NAT-Tabelle

Inside	**Outside**
192.168.5.34:39218 ↔ 212.55.197.230:80	192.0.2.**4**:39218 ↔ 212.55.197.230:80
192.168.5.35:39218 ↔ 212.55.197.230:80	192.0.2.**5**:39218 ↔ 212.55.197.230:80

Diese Art bedingt, dass für jede intern verwendete IP-Adresse eine öffentliche Adresse vorhanden sein muss!



Port Address Translation PAT

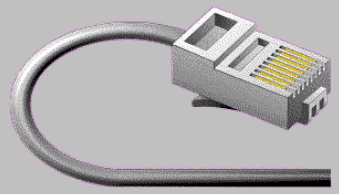


NAT-Tabelle

Inside	**Outside**
192.168.5.34:39218 ↔ 212.55.197.230:80	192.0.2.4:39218 ↔ 212.55.197.230:80
~~192.168.5.35:39218 ↔ 212.55.197.230:80~~	~~192.0.2.4:39218 ↔ 212.55.197.230:80~~
192.168.5.35:39218 ↔ 212.55.197.230:80	192.0.2.4:39219 ↔ 212.55.197.230:80

Um den roten - doppelten Eintrag zu verhindern muss auch der Source-Port bei den ausgehenden Paketen modifiziert werden.

Dieser Vorgang wird als **Port Address Translation** (**PAT**) bezeichnet

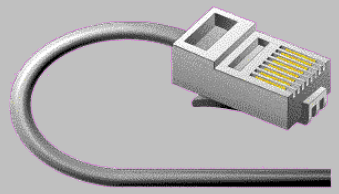


NAT/PAT Tabelle

Die Einträge in der NAT-Tabelle werden für Pakete in der Richtung inside ➔ outside dynamisch erzeugt und haben meist eine limitierte Lebensdauer, da der Speicher für die NAT/PAT-Tabelle nicht unendlich ist.

TCP-Verbindungen: Der Eintrag kann aus der Tabelle gelöscht werden, wenn die Verbindung terminiert wurde (FIN-Flag).
Werden sehr lange keine Pakete mehr ausgetauscht, so wird der Eintrag nach einer Zeit entfernt.

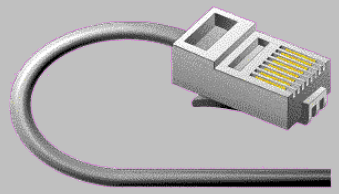
Dieses Zeit-Limit ist bei interaktiven Session ärgerlich, da die Verbindung nach einem Timeout wieder aufgebaut werden muss.



NAT Tabelle

UDP-Verbindungen:
UDP-Verbindungen haben keinen Status. Darum müssen die Einträge für UDP-Verbindungen nach einer bestimmten Zeit entfernt werden. Diese Zeit ist einstellbar. Zu spät eintreffende Pakete werden verworfen, da keine passenden Eintrag in der NAT/PAT Tabelle vorhanden sind.

Bei zuvielen Verbindungen kann es es vorkommen, dass der Speicher der NAT-Tabelle verbraucht ist und erst wieder neue Verbindungen erstellt werden können, wenn Speicherplatz frei wird (oder das NAT-Device neu gestartet wird).

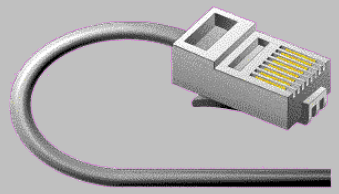


NAT Sicherheit

Das nur Pakete von bestehenden Verbindungen ins interne Netz gelangen, bietet einen gewissen Schutz.

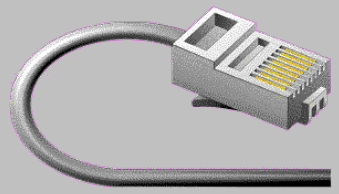
Das NAT/PAT-Device überprüft die Pakete nur anhand der Header-Daten. Wollen sie 'Deep inspection' verwenden, muss das eine Firewall mit den entsprechenden Optionen übernehmen.

NAT/PAT und Firewall-Funktionalitäten finden sie meistens kombiniert in Firewall Appliances (Checkpoint, Cisco, Fortigate, Juniper Sonicwall, Zyxel, ...).



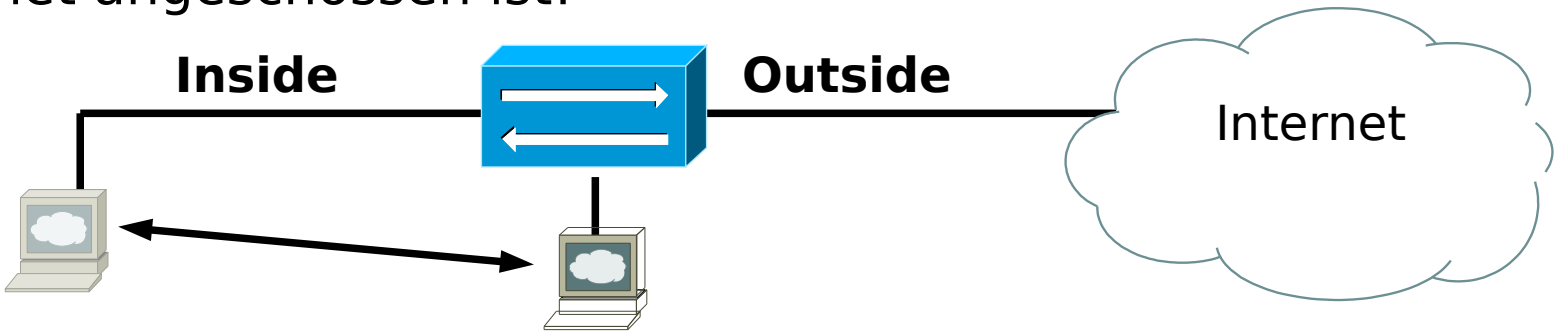
Spezielle NAT/PAT

Neben der klassischen Verwendung von NAT/PAT (mehre Client Rechner hinter einer öffentlichen IP-Adresse) gibt es verschieden andere Einsatzmöglichkeiten.



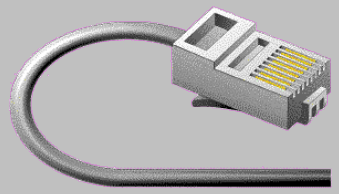
Spezielle NAT

1:1 NAT (one to one NAT)
Hier wird ein ganzer Rechner nach 'draussen' gesetzt. Alle seine Ports sind direkt im Internet erreichbar. Der NAT-Router muss für jeden internen Rechner für den ein 1:1 NAT eingerichtet wird eine eigene IP-Adresse verwenden.
Beachten sie, dass bei 1:1 der Rechner faktisch direkt am Internet angeschossen ist!



NAT-Tabelle

Inside	**Outside**
192.168.5.34 ← 0.0.0.0:0	192.0.2.5 ← 0.0.0.0:0



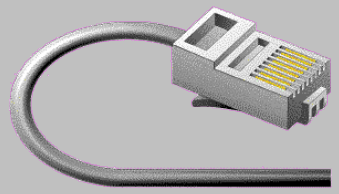
Spezielle NAT

Portforwarding

hier wird ein bestimmter Port an einen fix konfigurierten interner Rechner weitergeleitet. Dadurch können vom Internet auf den internen Rechner Verbindungen auf einen bestimmten Port geöffnet werden und der angebotene Service genutzt werden.

NAT-Tabelle

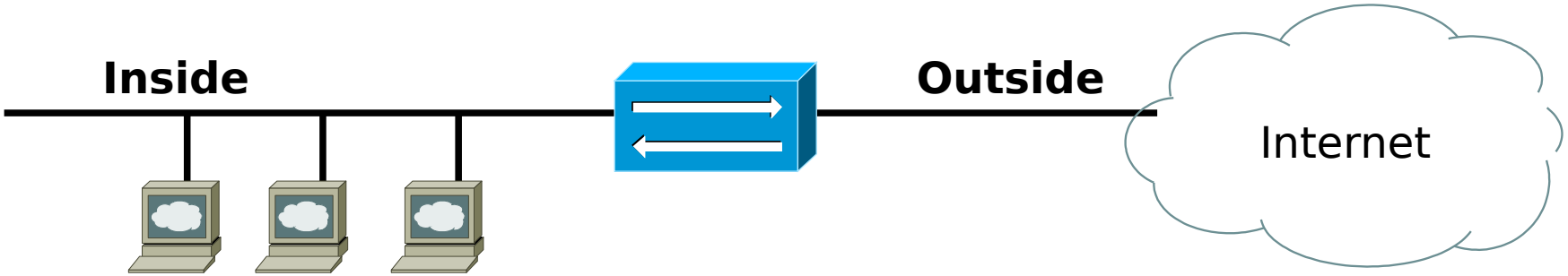
Inside (Sicht vom Client)	**Outside** (Sicht vom Server)
192.168.5.34:25(TCP) ← 0.0.0.0:0	192.0.2.4:25(TCP) ← 0.0.0.0:0
192.168.5.30:80(TCP) ← 0.0.0.0:0	192.0.2.4:80(TCP) ← 0.0.0.0:0



Spezielle NAT

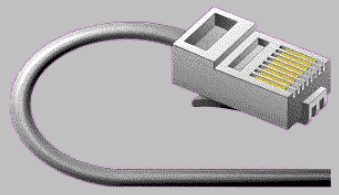
Loadbalancing

Es werden für den gleichen externen Service mehrere interne Rechner definiert.
Die NAT/PAT-Applikation kann diese die Last auf die verschiedene Rechner verteilen. Je nach 'Intelligenz' der NAT/PAT-Applikation können Rechnerausfälle detektieren und die Anfragen auf die verbleibenden Rechner verteilt werden.

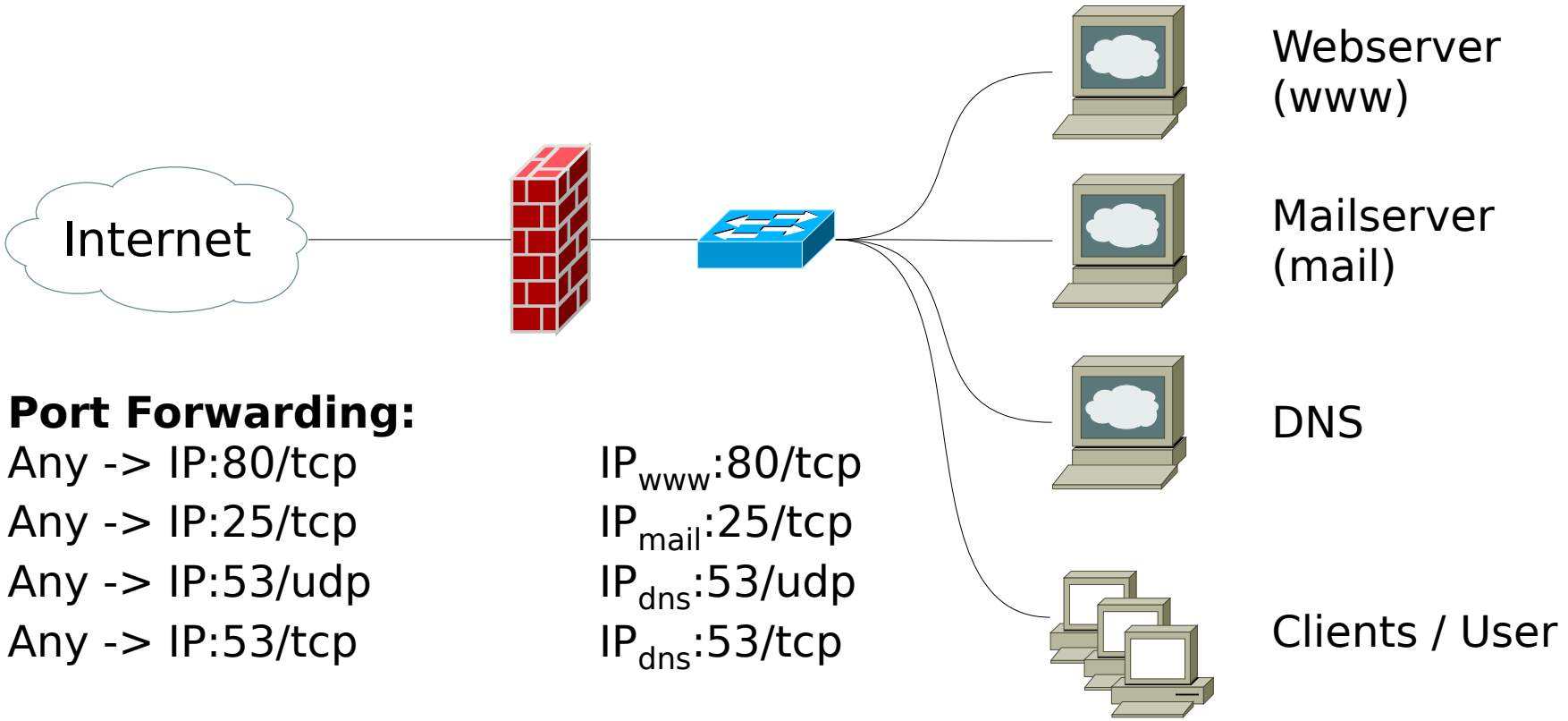


NAT-Tabelle

Inside		Outside	
192.168.5.34:80(TCP)	← 0.0.0.0:0	192.0.2.4:80(TCP)	← 0.0.0.0:0
192.168.5.35:80(TCP)	← 0.0.0.0:0	192.0.2.4:80(TCP)	← 0.0.0.0:0
192.168.5.36:80(TCP)	← 0.0.0.0:0	192.0.2.4:80(TCP)	← 0.0.0.0:0



Kombination Port-Forwarding, -Translation

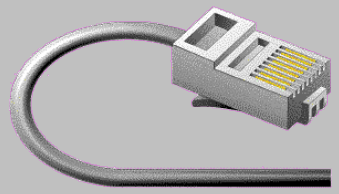


Port Forwarding:

Any -> IP:80/tcp	IP_{www}:80/tcp
Any -> IP:25/tcp	IP_{mail}:25/tcp
Any -> IP:53/udp	IP_{dns}:53/udp
Any -> IP:53/tcp	IP_{dns}:53/tcp

Port Forwarding und Port Translation

Any -> IP:6000/udp	IP_{www}:161/udp
Any -> IP:6001/udp	IP_{mail}:161/udp
Any -> IP:6002/udp	IP_{dns}:161/udp

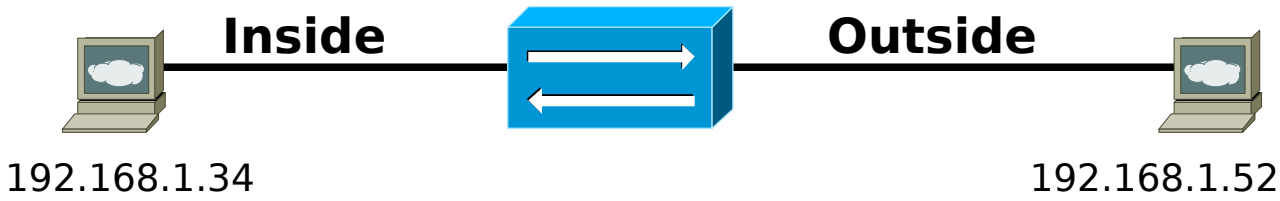


Spezielle NAT

Doppelts NAT

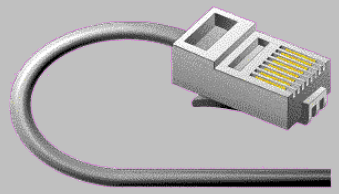
Wenn zwei Netzwerke – die die gleichen IP-Adressen verwenden – zusammen geschlossen werden müssen und eine neu Adressierung nicht möglich ist, so kann doppeltes NAT eine Lösung sein.

Rechner sehen beispielsweise die outside Rechner unter dem Netz 192.168.100.0/24 während dem die outside Rechner die internen Rechner unter dem Netz 192.168.200.0/24 sehen.
Probleme bereiten alle Protokolle die IP-Adressen in der Payload enthalten, da diese Adressen eventuell auch entsprechend angepasst werden müssen (beispielsweise DNS-Abfragen)



NAT-Tabelle

Inside		Outside	
192.168.1.34	←→ 192.168.100.52	192.168.200.34	←→ 192.168.1.52

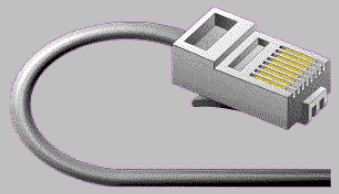


Problem bei NAT

Da NAT die Header der Pakete modifiziert, haben verschiedene Anwendungen ihre Mühe damit.

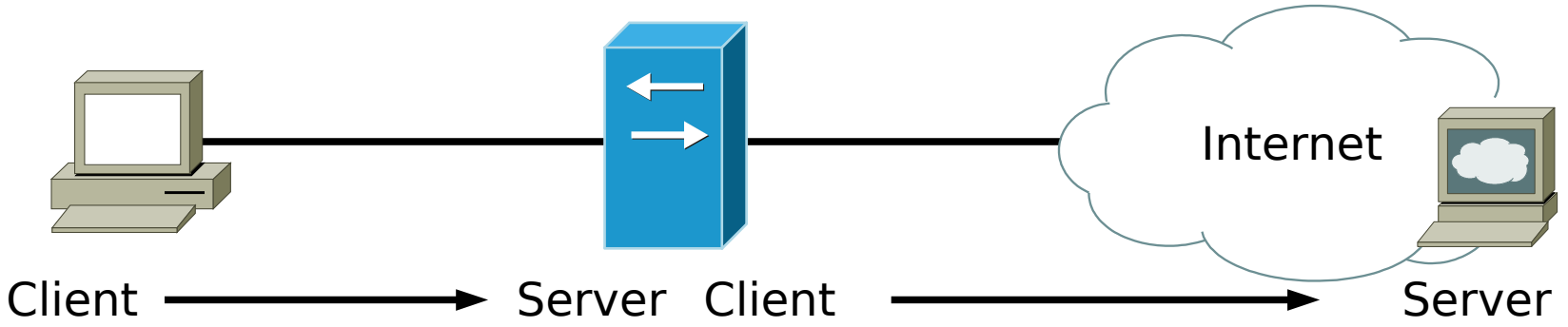
So können Anwendungen, die weitere Verbindungen zum Client hinter dem NAT-Gerät öffnen wollen, nur dann korrekt arbeiten wenn das NAT-Gerät diese korrekt erkennt und entsprechend reagiert.

Bekanntestes Vertreter sind FTP, SIP (VoIP) sowie VPN-Tunnels funktionieren nur beschränkt hinter einem NAT-Gerät.

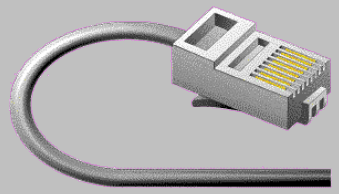


Alternativen

Alternativ zu NAT können auch Proxy-Lösungen eingesetzt werden.
Ein Proxy ist eine Software, die sich gegenüber dem Client wie der entsprechende Server verhält, gegenüber dem wirklichen Server im Internet tritt der Proxy wie ein Client auf.

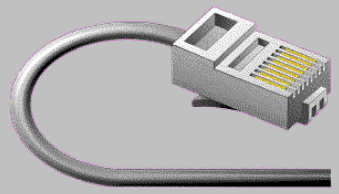


Für jedes Protokoll muss ein separater Proxy installiert werden!

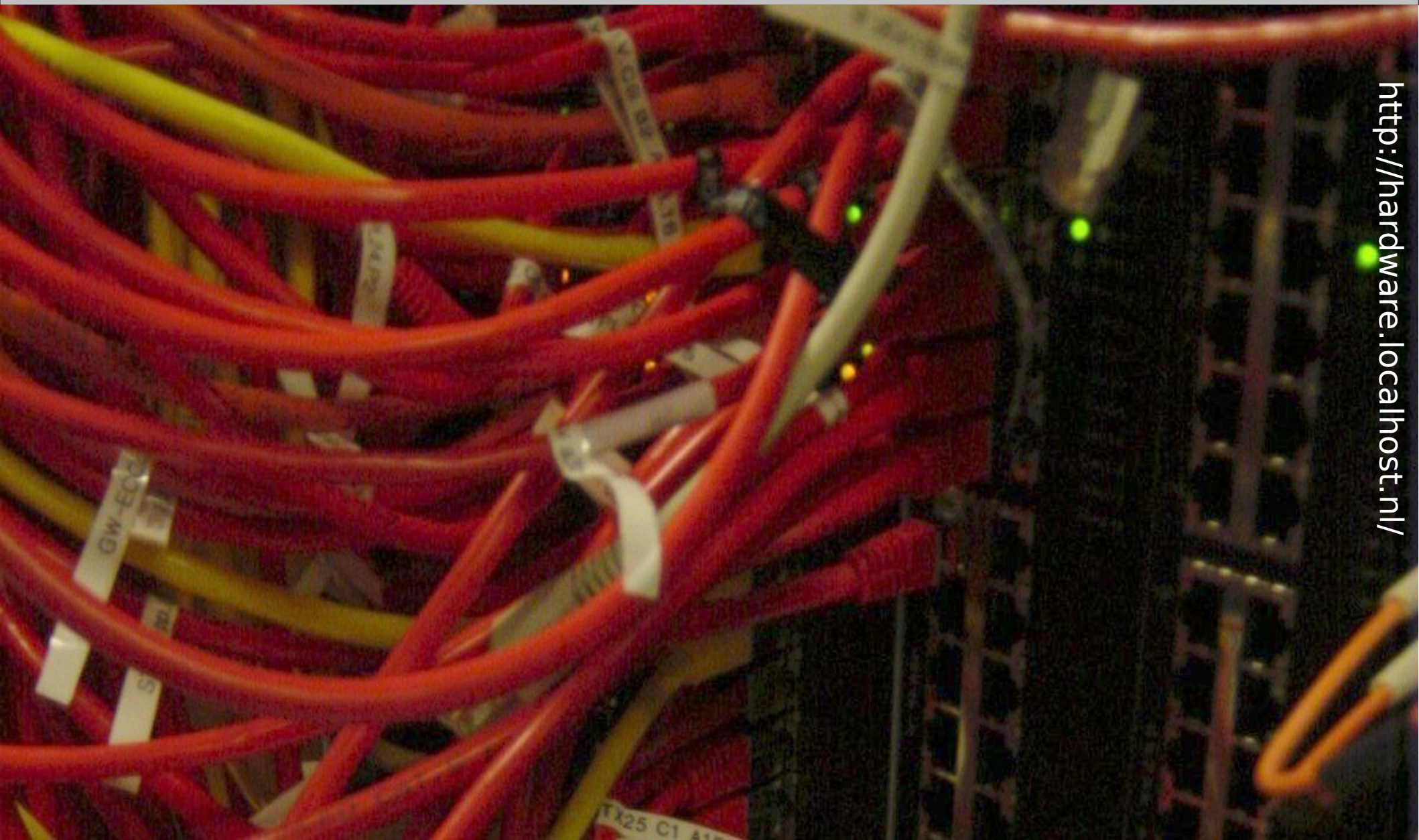


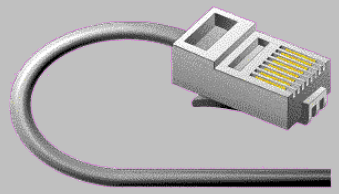
Alternativen zu NAT

Lösung	Vorteil	Nachteil
NAT	- Transparent - Private Adressen - Geringer Aufwand bei den Clients	- Adresskonflikte möglich - Nicht alle Protokolle möglich - Eingehende Verbindungen sind nur beschränkt möglich
Proxy	- Caching ist möglich - Grösserer Schutz gegen Angriffe von aussen - Private Adressen möglich	- Clients müssen eingerichtet sein - Nicht alle Protokolle möglich - Zusätzliche Hardware not-wendig



Fragen?



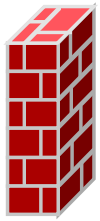


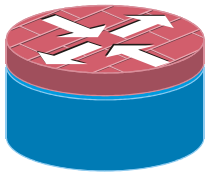
Firewall

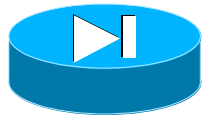
Firewall dienen dazu den IP-Verkehr zu kontrollieren und nur gewünschte Verbindungen zu erlauben.

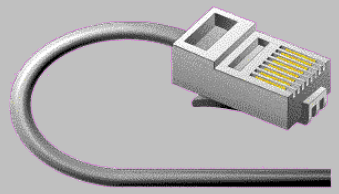
Firewall werden in den Datenstrom geschaltet, damit diese - falls notwendig – die unerwünschte Pakete entfernen zu können.

Firewallsymbole:

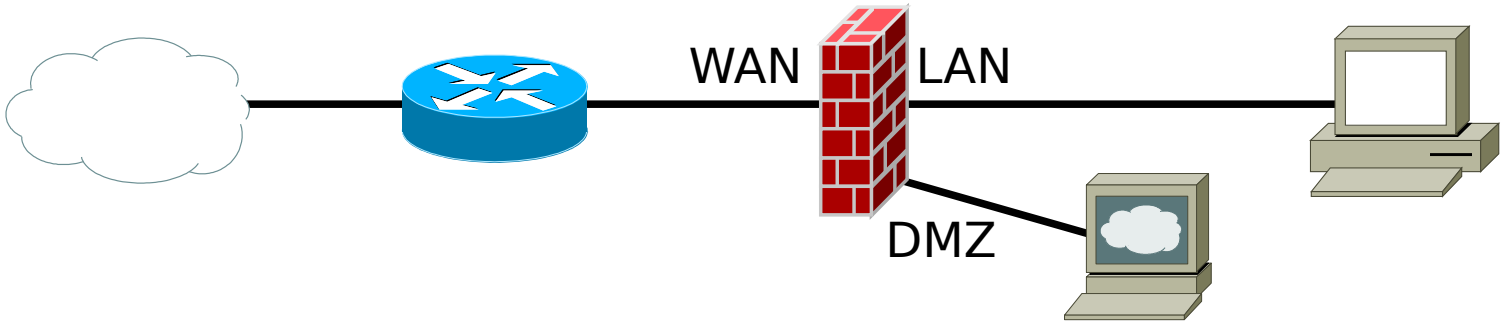




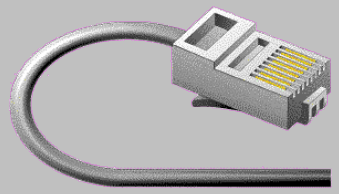




Firewall



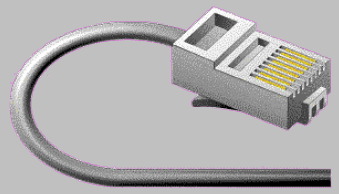
Firewalls haben in der Regel mehrere Anschlüsse oder Zonen. Üblich sind die Zonen WAN, LAN und DMZ – manchmal auch Optional Zone genannt.
Weitere Zonen sind möglich!



Firewall Zonen

WAN:Hier ist nichts vertrauenswürdig.
Alle ankommenden Pakete werden als 'böse', nicht vertrauenswürdig Pakete angesehen.

Um in eine andere Zone zu gelangen müssen diese Paket die definierten Regeln erfüllen.

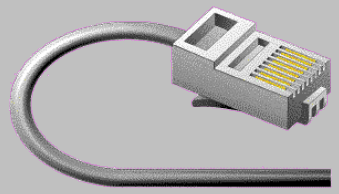


Firewall Zonen

LAN: Im LAN sind die vertrauenswürdigen Rechner angeschlossen.

In der Regel ist hier nur der Zugriff vom LAN nach WAN/DMZ erlaubt.

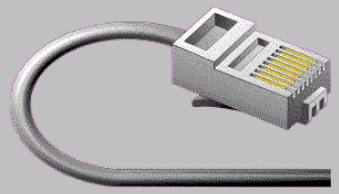
Oft ist vom LAN aus der Zugriff nach überall erlaubt. Dies kann ein Sicherheitsrisiko sein, denn ein komprimierter Rechner kann so Daten nach überall transferieren.



Firewall Zonen

DMZ: Hier werden die Server, auf die vom WAN zugegriffen werden darf platziert. Es sollten nur die Ports erlaubt sein, die benötigt werden um die gewünschte Dienste anzubieten.

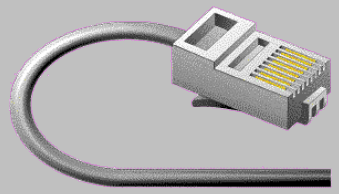
Wird trotz der Vorsichtsmassnahme ein Server übernommen, so sind die Rechner in der LAN-Zone weiterhin geschützt.



Firewall arbeitsweise

Stateless:
Die Firewall überprüft die Paket. Wenn die Regeln erlauben das Paket weiterzuleiten, so wird es weitergeleitet.
Das Regelwerk der Firewall muss die Antworte-Pakete explizit erlauben - sonst wird keine Kommunikation zustande kommen.

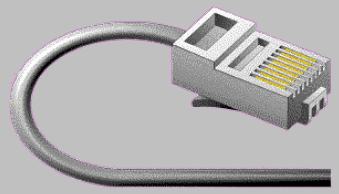
+ Die Software dieser Firewall ist einfacher zu schreiben
- Der Anwender muss mehr überlegen und entsprechend mehr konfigurieren



Firewall arbeitsweise

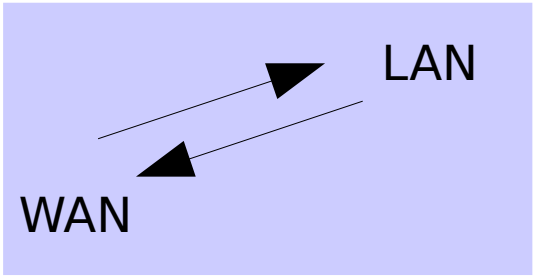
Statefull:
Die Firewall überprüft das Paket. Ist das Paket ein erstes Paket einer erlaubten Verbindung, so erstellt die Firewall eine dynamische Regel, damit die Antwort-Pakete auf dieses Verbindung die Firewall passieren kann.

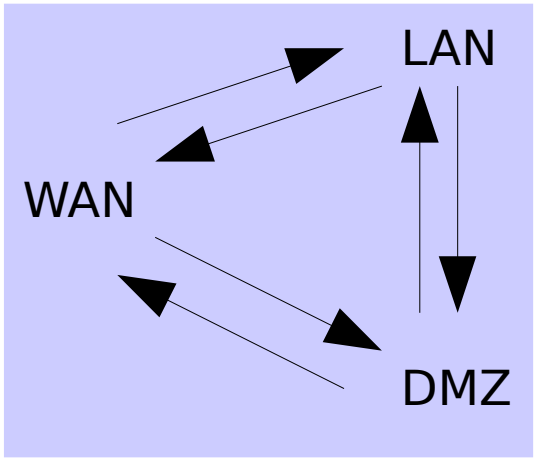
\+ Der Anwender hat es einfacher
\- Die Software ist komplizierter zu schreiben



Firewall Regeln

Bei der Konfiguration der Firewall muss von jeder Zone zu jeder anderen Zone die notwendigen Regel definiert werden.

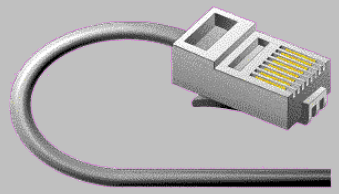




Bei einer 2 Zonen Firewall sind das 2 Richtungen die untersucht werden müssen.

Bei einer 3 Zonen Firewall sind das schon 6 Richtungen die untersucht werden müssen.

Kommen noch weiter Zonen (VPN-Tunnel, VPN-Clients) hinzu, so steigt die Komplexität stark an!

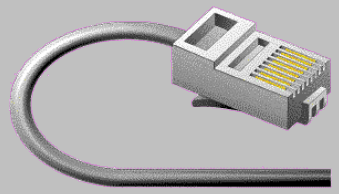


Firewall Regeln

Wird eine Firewall konfiguriert, so achten sie darauf, dass die Firewall von einem sicheren Rechner aus konfiguriert wird.

Achten sie, dass die Kommunikation zwischen dem Konfigurations-Rechner und der Firewall nicht kompromittiert werden kann/ist.

Unterbinden sie nicht notwendige Protokolle! (beispielsweise ICMP Port unreachable ist für IP lebensnotwendig. Ping kann bei Problemen sehr hilfreich sein (Der 'ping of death' stellt für aktuelle Betriebsysteme keine Bedrohung dar)

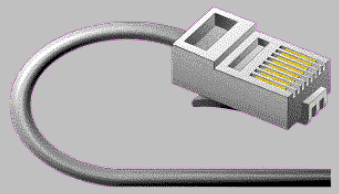


Firewall Regeln

Achten sie, dass die Konfiguration der Firewall simple ist.

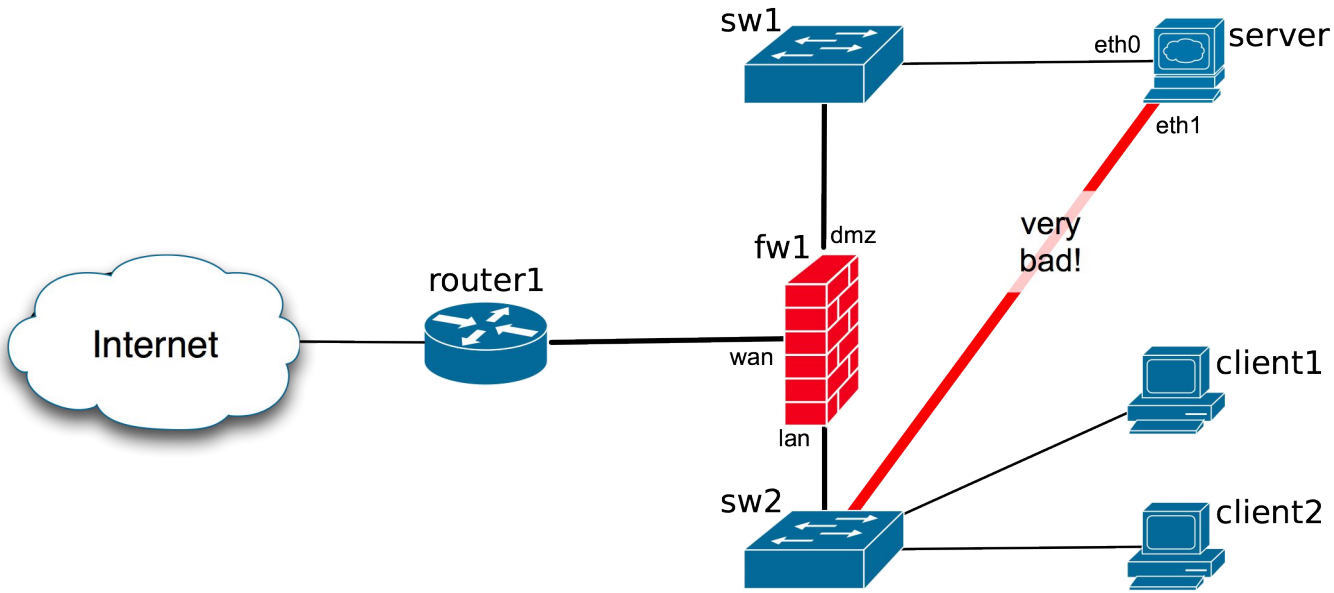
Komplizierte Regelwerke sind nicht überschaubar und Fehler anfällig! (KISS: Keep it short and simple)

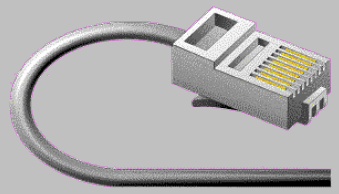
Haben sie für alle verwendeten Protokolle (IPv4, IPv6) entsprechende Regeln definiert? Speziell Routing-Protokolle, Ipsec-VPN Verbindungen verwenden andere Protokolle als TCP/UDP auf Layer 4.



Firewall Regeln

Achten sie, dass keine Zweit-Wege im Netzwerk vorhanden sind, die Firewall umgehen:





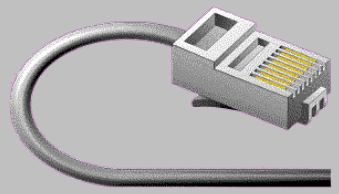
Deep Packet Inspection

Oft kommen auch 'Packet Deep Inspection' zum Einsatz.

Zusätzlich zu den Headern des Pakets wird die Payload überprüft, ob wirklich das definierte Protokoll verwendet wird.

Bei einer Firewall wird der Port 80 (http) für ausgehende Verbindungen erlaubt. Ohne Deep Inspektion kann - entsprechende konfiguriert Server vorausgesetzt - auch VPN Tunnels, FTP-Transfers, ... über den Port 80 transportiert werden und so Firmen Richtlinien umgangen werden.

Deep Inspection wird die Pakete, die nicht dem definierten Protokoll entsprechen, blockieren.

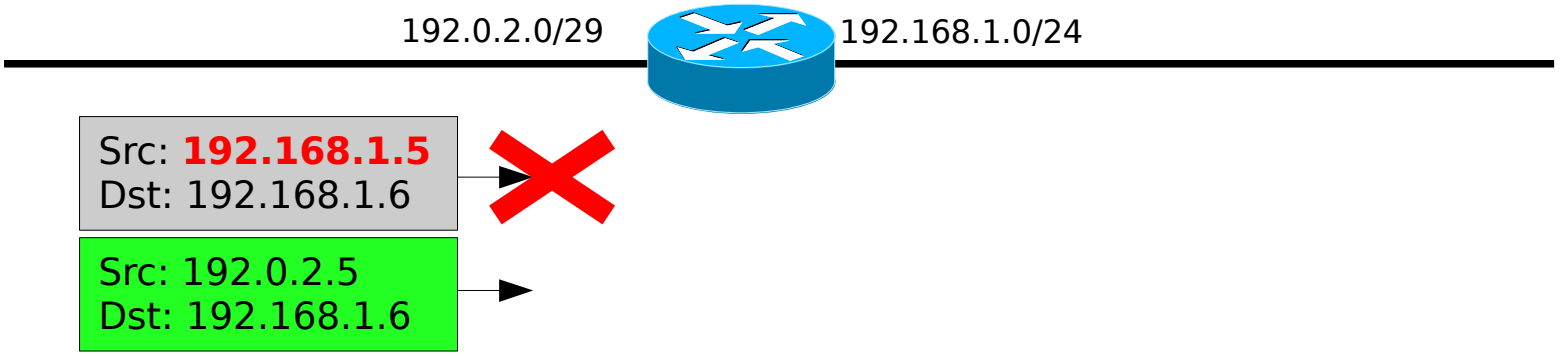


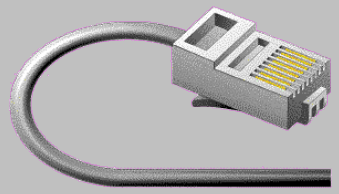
Firewall

Adress Spoofing:

Es wird ein Paket mit einem modifizierten Header - der vortäuscht, dass das Paket von einem Host der geschützten Zone gehört - an die Firewall gesendet.

Der Absender hofft, dass die Firewall/Router meint, dass sie das Paket irrtümlich erhalten hat und das unverändert Paket weiterleitet.



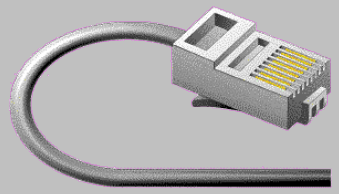


(D)DoS

Bei einer Denial of Service (DoS) oder Distributed Denial od Service (DDoS) ist das Ziel einen Service abzuschalten. Der Angreifer will sich dabei nicht zeigen. Dies kann auf verschiedene Arten erfolgen:

Request Flut:

An die Server werden zu viele Anfragen gesendet, so dass diese nur noch langsam antworten. Dauert die Antwortszeit zu lange, "laufen" die Benutzer davon.



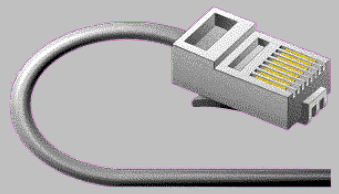
(D)DoS

SYN-Flood:

Es werden nur TCP-SYN-Pakete gesendet. Der Ziel-Host kann keine neuen echten Session mehr annehmen.

Traffic-Flood:

Es wird massenhaft Traffic an die Ziel-Adresse gesendet, so dass die Router und Leitungen auf dem Weg zum Ziel überlastet sind, die Firewall vor den Ziel-Rechner oder die Ziel-Rechner überlastet werden.



(D)DoS

DNS Server blockieren

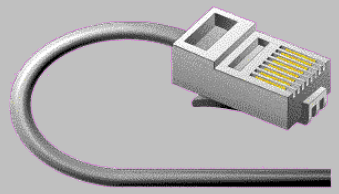
Die DNS-Server, wo die Domain vom Ziel-Service gehosted wird, wird mit anfragen überlastet. Können keine Hostnamen aufgelöst werden, können auch keine Anfragen an den Server gesendet werden.

Fehler im Betriebssystem:

Ping of Death, WinNuke, Land-Attacke, Teardrop, ...

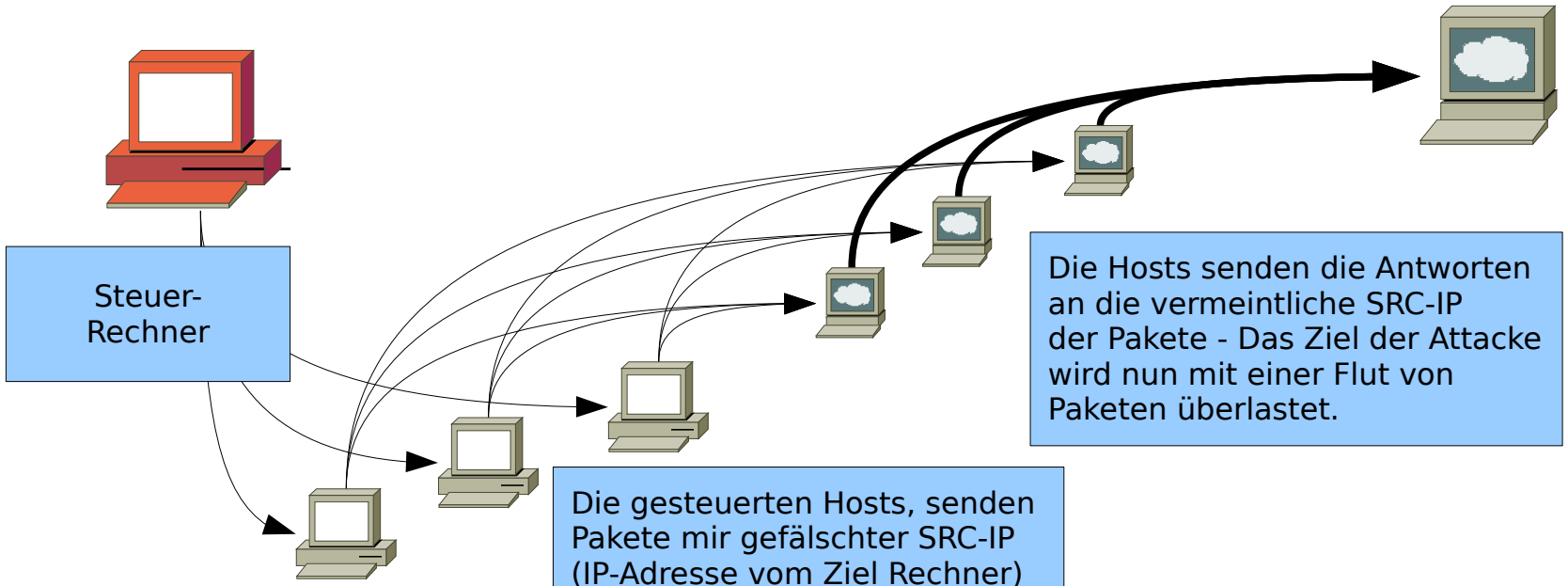
Genauere Beschreibungen könne sie unter [1] nachlesen.

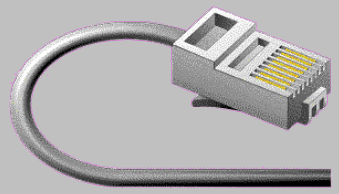
[1] http://de.wikipedia.org/wiki/Denial_of_Service



DDoS

Address Spoofing wird bei Distributed Denial of Service Attacken (DDoS) oft verwendet um den Angreifer zu verstecken und die Attacke überhaupt durchführen zu können. Ein Steuer Rechner instruiert übernommene Rechner gespoofte Pakete zu senden. Die Antworten überlasten den Ziel Rechner.



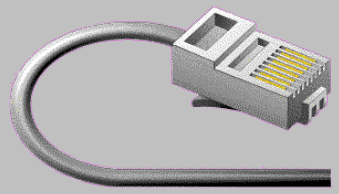


DDoS

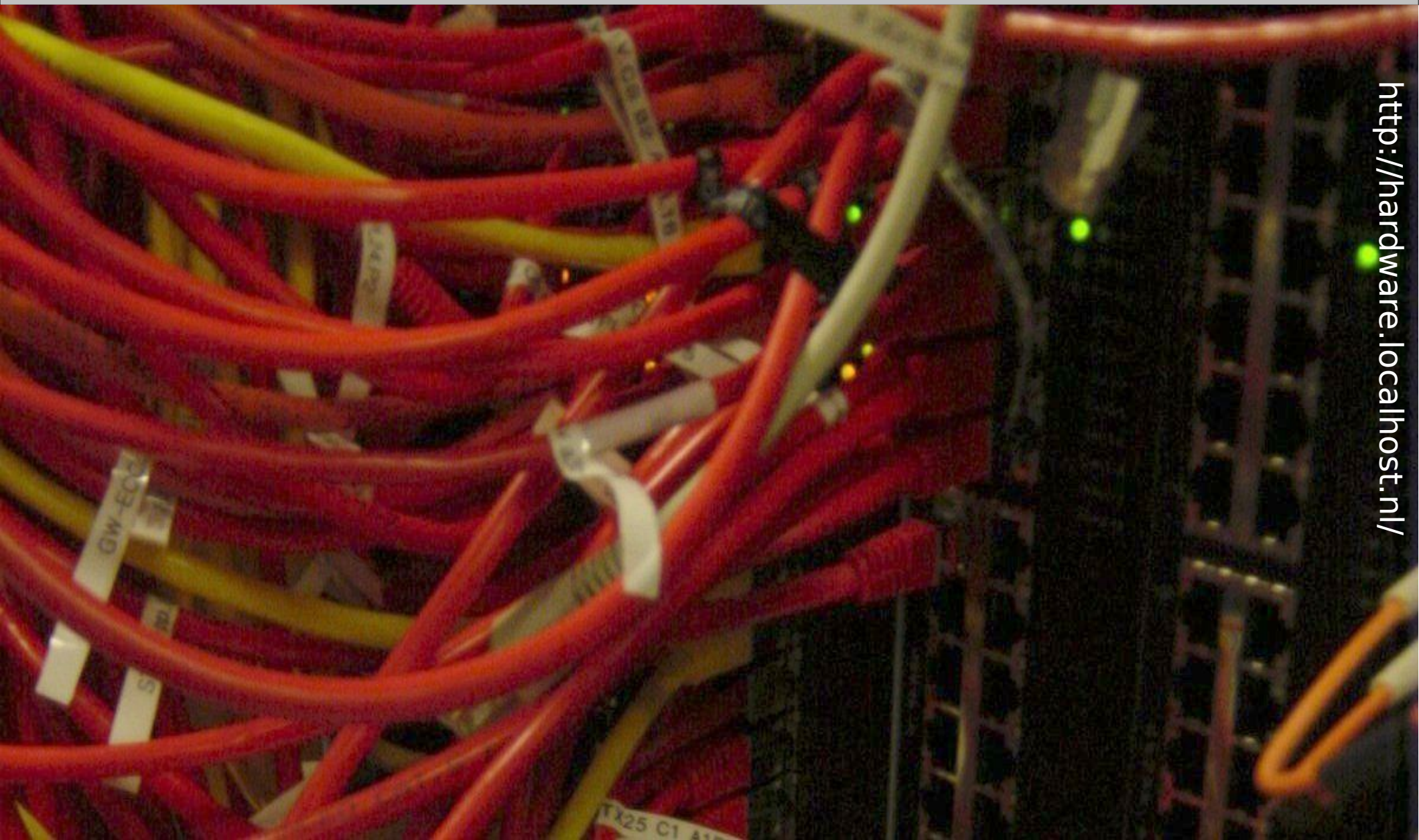
Nicht alles was nach DDoS oder DoS aussieht ist ein Angriff.

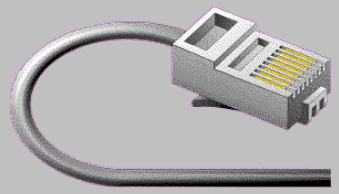
Plötzliche hohe Netzaktivitäten können durch aktuelle Ereignisse, Erwähnung in Newsseiten, ... erfolgen. Wenn der Zielserver die Last nicht handeln kann ist der Effekt derselbe, die Ursache jedoch eine komplett andere. [1]

[1] Slashdot-Effekt oder geheist, http://de.wikipedia.org/wiki/Slashdot-Effekt



Fragen?

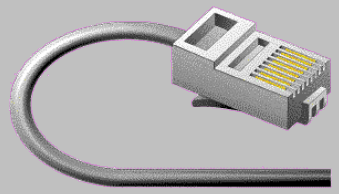




Routing Tabellen

Statisches Routing
Dynamisches Routing
- Distanz Vektoren Routing Protokolle
- Link State Routing Protokolle

Ziele:
- Unterschiede vom statischen und dynamischen Routing kennen
- Wissen wie funktionieren die Distanz Vektoren Routing Protokolle



Routing

Jeder Host hat eine eigene Routingtabelle aus der die Gateway Adresse ermitteln wird, an die ein Paket gesenden werden muss um das Ziel zu erreichen.
Findet der Rechner keinen passenden Eintrag, so kann das Paket nicht weitergeleitet werden und der Absender muss über ICMP Destination unreachable informiert werden.
Das Problem ist, dass diese Routingtabellen à jour gehalten werden müssen.

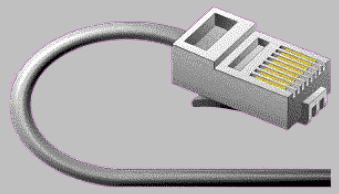
Das kann entweder **statisch** oder **dynamisch** erfolgen.
Dementsprechend wird auch von

statischem Routing

und vom

dynamischen Routing

gesprochen.

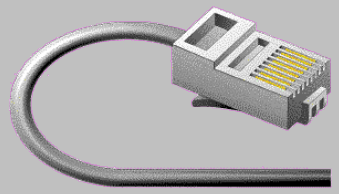


statisches Routing

- Beim statischen Routing werden die Routen manuell in die Routing-Tabelle eingetragen.
  (Siehe Folie: "Routing Tabelle anpassen")

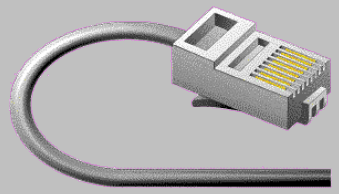
- Bei Servern und Workstation wird in der Regel die Default-Route statisch eingetragen (entweder von Hand oder via DHCP). Dies verringert den Konfigurationsaufwand auf ein absolutes minimum.

```
heuer@linux:~$ /sbin/route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.168.0   0.0.0.0         255.255.255.0   U     0      0        0 eth0
0.0.0.0         192.168.168.1   0.0.0.0         UG    0      0        0 eth0
```



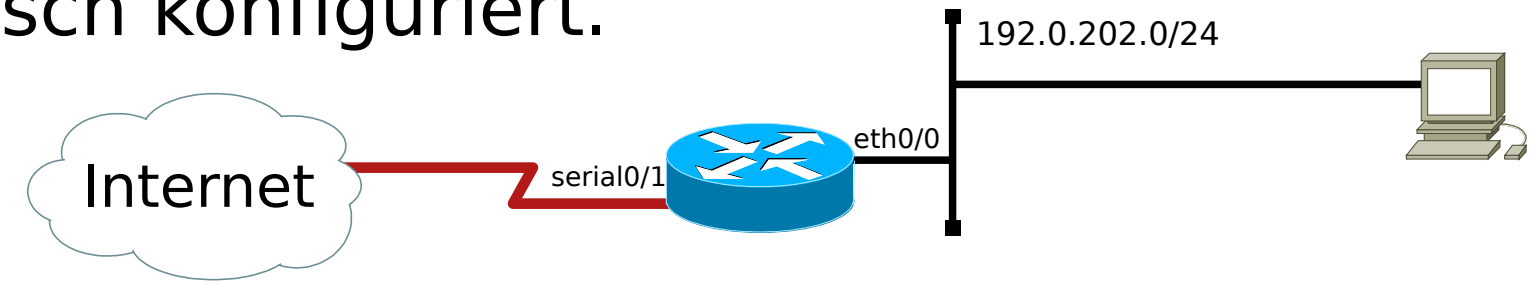
statisches Routing

```
C:\>route print
===========================================================================
Schnittstellenliste
0x1 ........................... MS TCP Loopback interface
0x1000003 ...00 0c 29 39 42 f5 ...... VMware Accelerated AMD PCNet Adapter
===========================================================================
===========================================================================
Aktive Routen:
     Netzwerkziel    Netzwerkmaske          Gateway   Schnittstelle  Anzahl
          0.0.0.0          0.0.0.0     192.168.23.1   192.168.23.34       1
        127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1       1
     192.168.23.0    255.255.255.0    192.168.23.34   192.168.23.34       1
    192.168.23.34  255.255.255.255        127.0.0.1       127.0.0.1       1
   192.168.23.255  255.255.255.255    192.168.23.34   192.168.23.34       1
        224.0.0.0        224.0.0.0    192.168.23.34   192.168.23.34       1
  255.255.255.255  255.255.255.255    192.168.23.34   192.168.23.34       1
Standardgateway:      192.168.23.1
===========================================================================
Ständige Routen:
  Keine
```



statisches Routing

Bei kleinen Netzwerken oder auch Routern mit nur 2 Anschlüssen werden die Routen oft statisch konfiguriert.

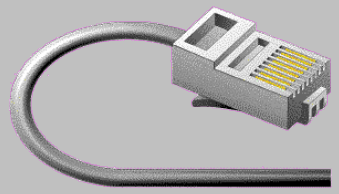


Routing Tabelle Router:

Dest	**Interface**
192.0.202.0/24	eth0/0
0.0.0.0/0	serial0/1

Routing Tabelle PC:

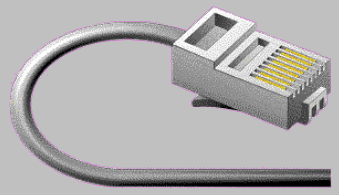
Dest	**Interface**
192.0.202.0/24	eth0
0.0.0.0/0	192.0.202.1



dynamisches Routing

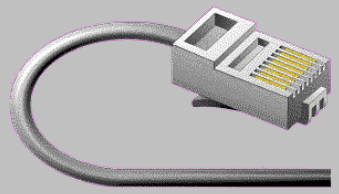
Wird das Netzwerk grösser, so werden in der Regel die Routen dynamisch konfiguriert, weil der Aufwand um die Routen statisch einzutragen, zu umständlich und fehleranfällig wird.

Beim dynamischen Routing sollen die Router selber den Weg durch das Netzwerk suchen.



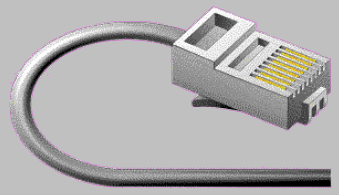
dynamisches Routing Prinzip

- Der Router kennt seine direkt angeschlossenen Netzwerke die er in seine Routing-Tabelle einträgt.
- Die Router senden diese Routing-Einträge an seine Nachbar Routern
- Der Router bekommt von seinen Nachbarn auch entsprechende Listen mit erreichbaren Netzwerken. Aus diesen Listen erstellt der Router neue Einträge für seine Routing-Tabelle zusammen.
- Die Einträge der Routing-Tabelle sendet der Router an seine Nachbarn weiter.



dynamisches Routing

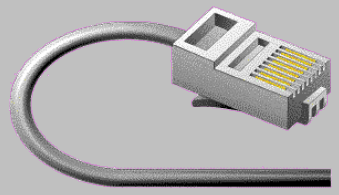
- Auf einem Router können verschiedene Routing-Protokolle parallel aktiv sein.
- Sind mehrere Routing-Protokolle aktiv, und beide Protokolle kennen je eine Route für ein bestimmtes Netzwerk, so muss definiert sein, welches Protokoll die höhere Priorität besitzt und bevorzugt wird.
- Der Router verwendet nur seine eigene Routing-Tabelle um die Pakete weiterzuleiten



Ziele der dynamischen Routing-Protokolle

Die dynamischen Routing-Protokolle müssen - damit sie ihre Aufgabe erfüllen - folgende vier Ziel erfüllen:

- **Routenoptimierung**
- **Flexibilität**
- **Konvergenz**
- **Effektivität**



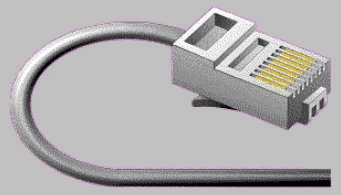
Ziele der dynamischen Routing-Protokolle

Routenoptimierung:

die schnellste und kosten günstigste Route soll ermittelt und verwendet werden.

Flexibilität:

fällt eine Weg aus, oder kommt ein neuer Weg hinzu, so soll dies in der Auswahl der Route berücksichtigt werden.



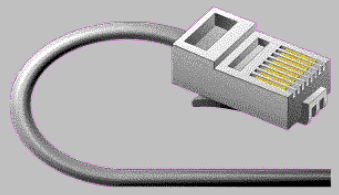
Ziele der dynamischen Routing-Protokolle

Konvergenz:

Ein Routing-Protokoll soll Änderungen möglichst schnell auf alle Router im Netzwerk verteilen, damit das Netzwerk möglichst schnell in einem konsistenten Zustand befindet (Alle Router haben dieselbe Informationen)

Effektivität:

Das Routing-Protokoll soll so wenig resourcen (Bandbreite, CPU, Memory) wie möglich verwenden.



Unterschiede zwischen den Routing Protokollen (1)

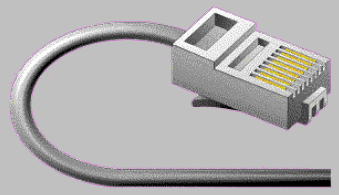
Flache- Hierachische-Protokolle:

Das Routing Protokoll unterstützt mehrere Regionen und kann so die Router ausserhalb der eignen Region entlasten.

Single- Multi-Path:

Wenn ein Routing Protokoll unterschiedliche Wege mit eventuell unterschiedlichen Kosten berücksichtigen kann, so ist es ein **Multipath-Protokoll**.

Wird nur ein bester Pfad verwendet, so ist es ein **Single-Path Protokoll**



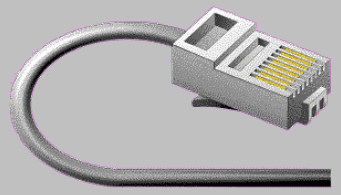
Unterschiede zwischen den Routing Protokollen (2)

Multiprotokoll:

Kann ein Routing Protokoll die Wege für verschiedene L3-Protokolle (IP,IPv6,IPX, Appletalk, ...) berechnen so ist es ein MultiProtokoll

Intern/Externe:

Routing Protokolle werden innerhalb von einem Netzwerk verwendet (intern) oder um verschiedene Netzwerke zu verbinden (extern)



Dynamische Routing Protokolle

Interne Routing Protokolle:

RIP	Routing Information Protocol
OSPF	Open Shortest Path First
ISIS	Intermediate System-to-Intermediate System Protocol
EIGRP	Enhanced Interior Gateway Routing Protocol

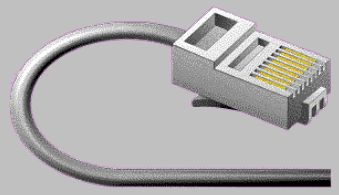
Externe Routing Protokolle

BGP	Border Gateway Protocol

Veraltete Routing Protokolle

EGP	Exterior Gateway Protocol
IGRP	Interior Gateway Routing Protocol

[1] RIP gibt es in 2 Versionen RIPv1, RIP v2
[2] EIGRP und IGRP sind proprietäre Protokolle, die nur von Cisco Geräten unterstützt werden

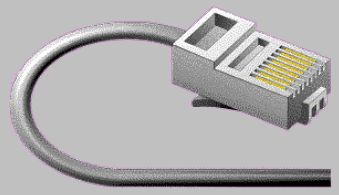


dynamische Routing Protokolle

Protokoll	Struktur	Path	Multi Protokoll	Art	Einsatz
RIPv1[1]	flach	~single	ja	DV	intern
RIPv2	flach	~single	ja	DV	intern
OSPF	hierarchisch	multi[2]	ja	LS	intern
ISIS	hierarchisch	multi	ja	LS	intern
EIGRP	(flach)	multi	ja	DV/LS	intern
BGP	hierarchisch	multi	ja	DV	extern
EGP[1]	hierarchisch	multi	ja	DV	extern
IGRP[1]	(flach)	multi	ja	DV	intern

Art: DV → Distanz Vektor, LS → Link State

[1] Diese Protokolle basieren auf classfull IP-Adressen, das bedeutet, dass sie keine variablen Netzmasken kennen
[2] Nur wenn die Kosten auf dem alternativen Weg gleich hoch sind wie auf dem ersten Weg
Distanz Vector oder Link Stat Protokolle unterscheiden sich wie sie die Routen berechnen.

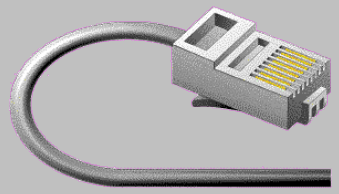


Technik bei Routing Protokollen

Maximum Hop Count
Der maximale Hop Count dient dazu zirkulierende Update zum verschwinden zu bringen. Bei RIPv1 und RIPv2 sind dies maximal 15 Hops, EIGRP kann maximal 255 Hops 'vertragen'

Route Poisoning
Verschwindet eine eigene Route, so announcet der Router diese Route mit dem maximalem Hop Count. Dadurch lernen die anderen Router schneller, das es diese Route nicht mehr gibt.

Hold Down Timer
Werfen innerhalb kurzer Zeit Updates für die gleiche Route erzeugt, so werden diese Updates eine bestimmte Zeit lang ignoriert (HoldDown Time)

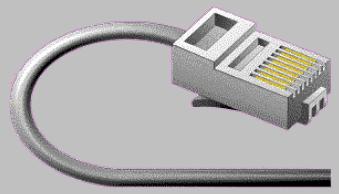


Technik bei Routing Protokollen

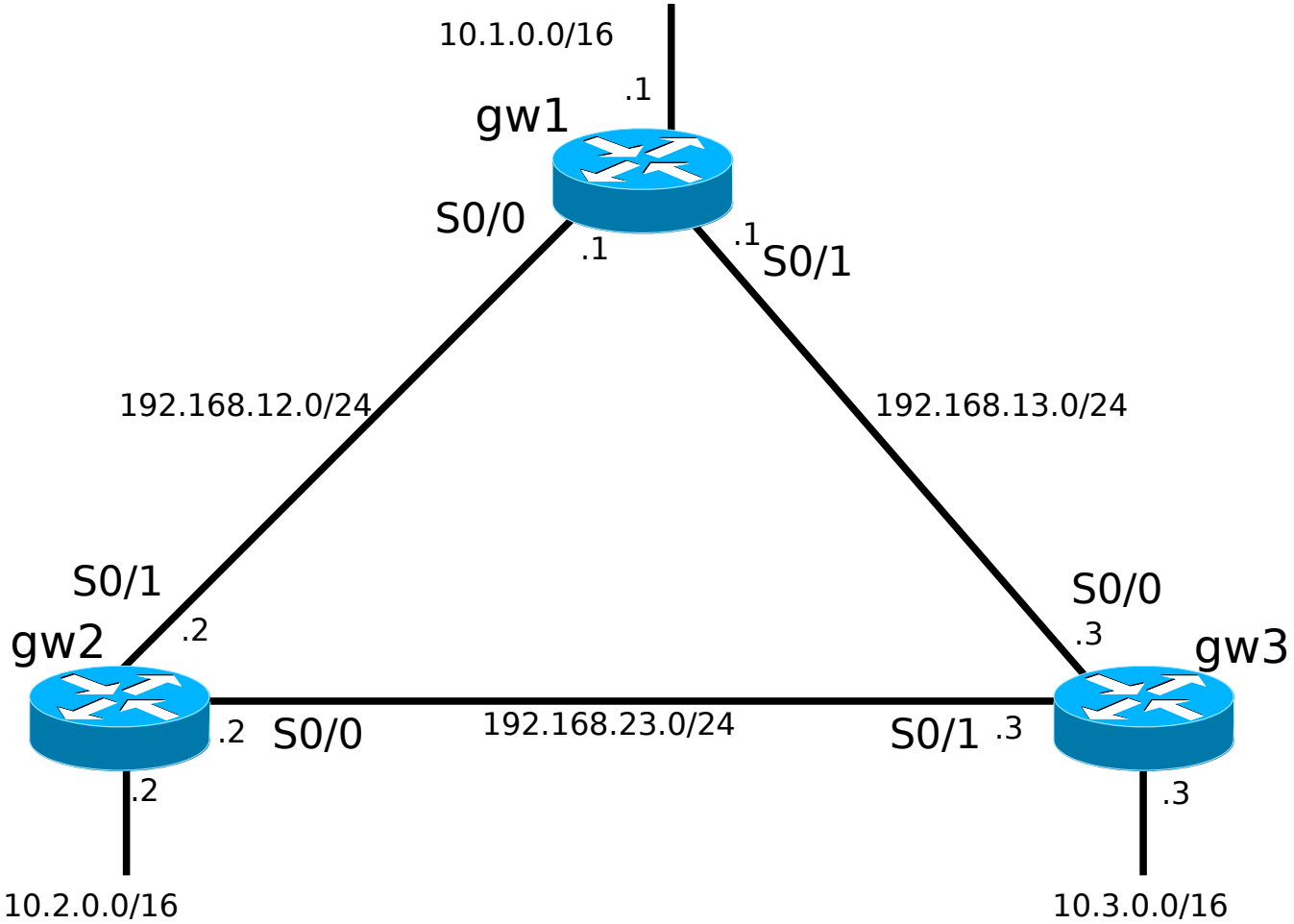
Split Horizon

Eine Route wird nie über das gleiche Interface announce wie über das Interface welches die Route gelernt wurde.

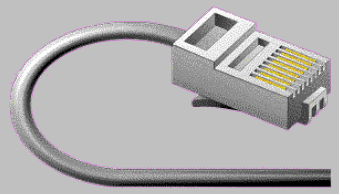
(Der Router der die Route announcte, kennt die Route ja schon. Da ist es (in der Regal) sinnlos, ihm die gleiche Route mit einem grösseren Hop Count zu announcen.)



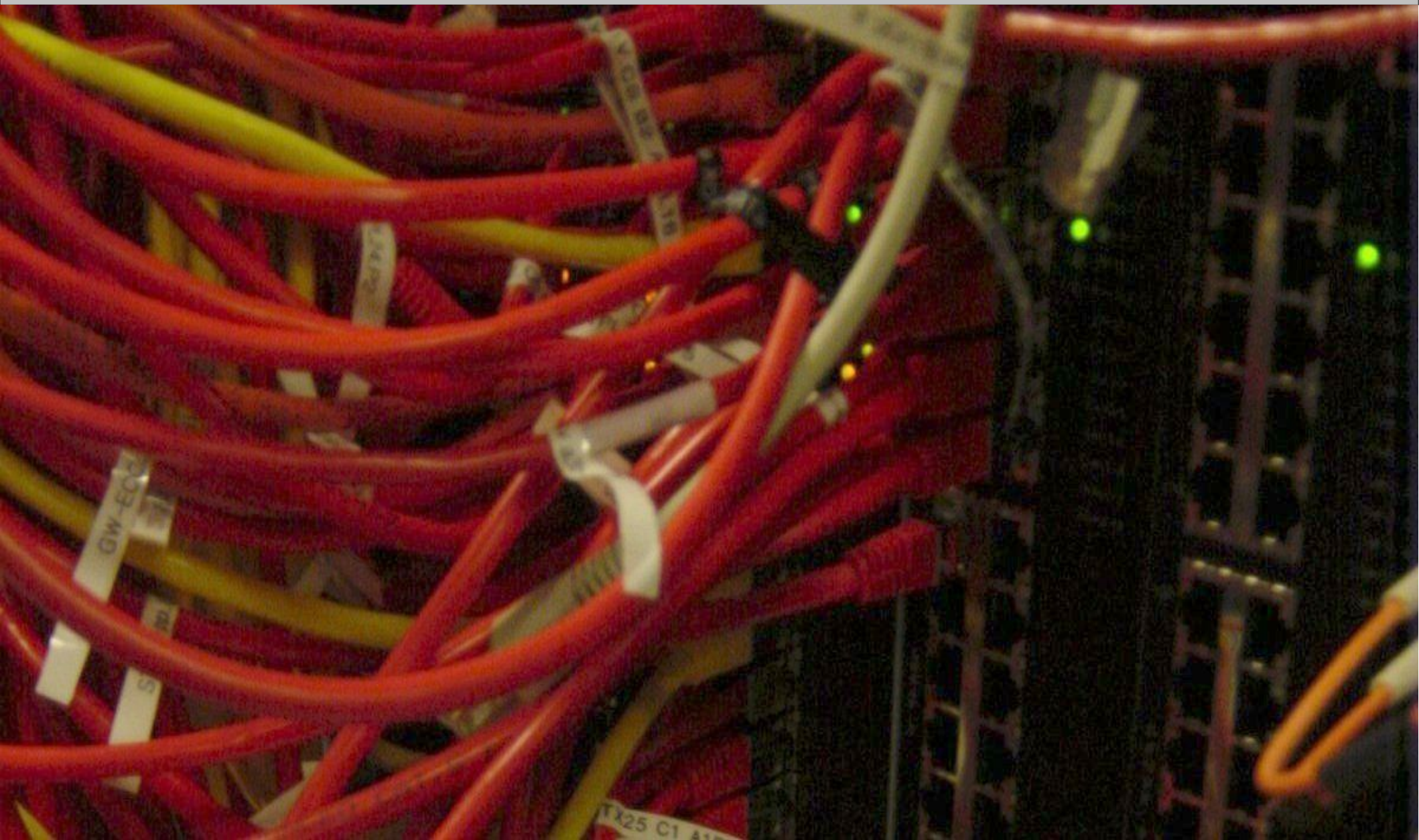
Beispiel

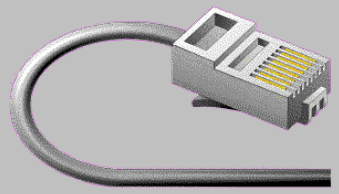


Siehe Zusatzblatt: 06_routing_distanzvektor.pdf

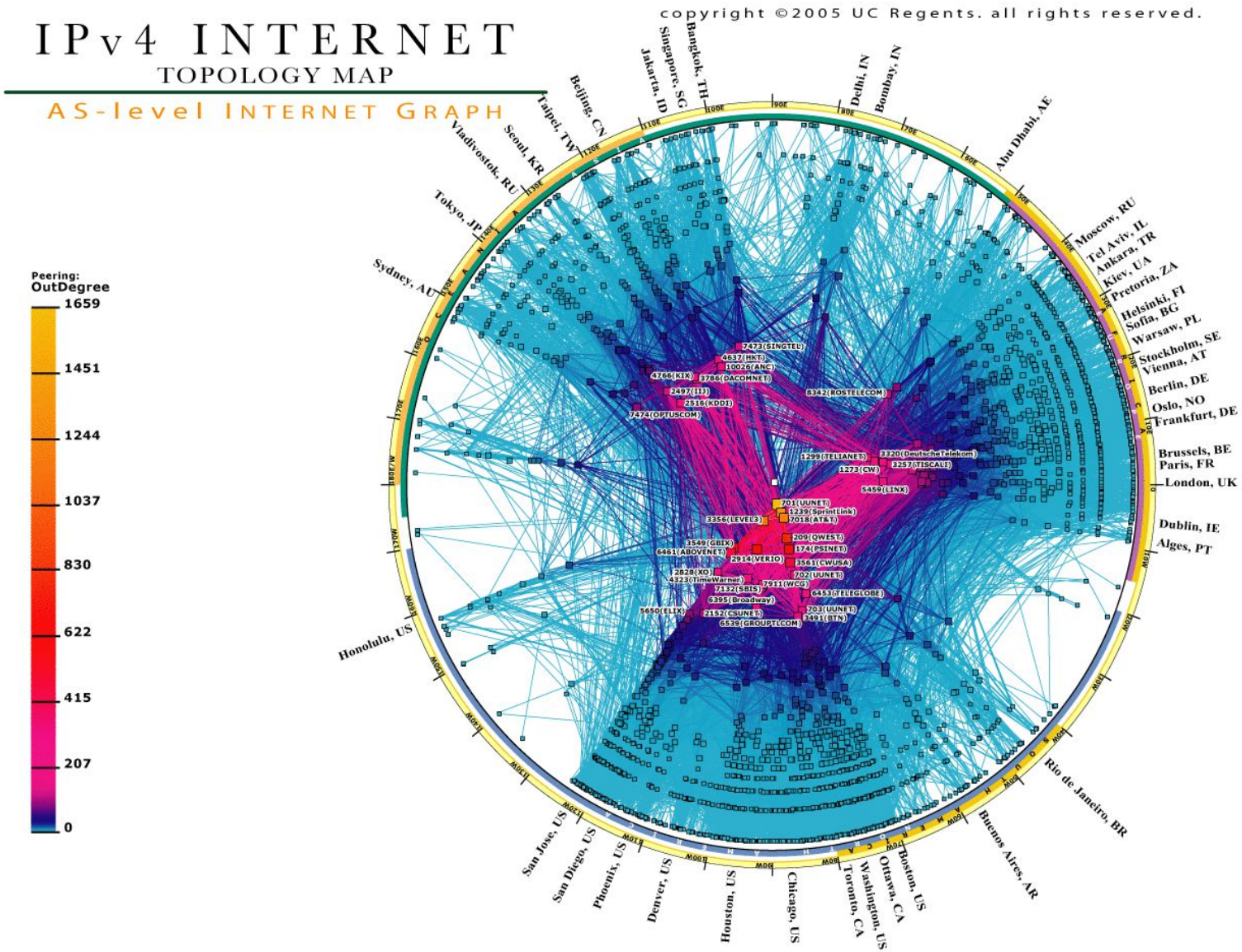


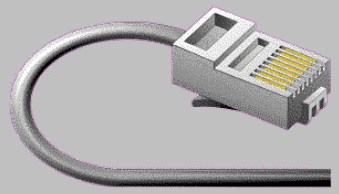
Fragen?





Internet Routing (BGP)





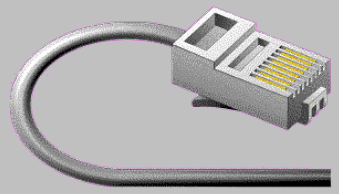
BGP

Jeder ISP (Internet Service Provider) stellt eine eigne, in sich administrierte Zone dar.

Diese werden als Autonomes Systems (AS) bezeichnet.

Jedes AS hat eine weltweit eindeutige Nummer ASN (Autonome System Number) zugeordnet.

Die ASN ist eine Zahl zwischen 1 und 64999; Der Bereich 65000 - 65535 ist für private Zwecke reserviert.

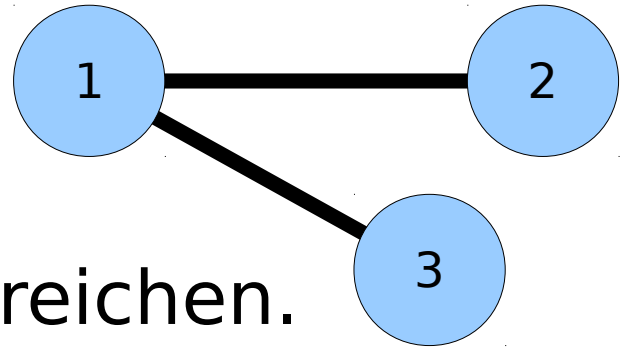


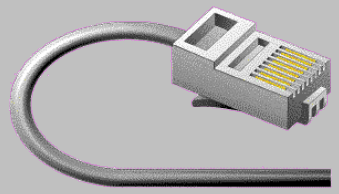
BGP peering

- Jedes AS kann mit jedem anderen AS die bekannten Routen austauschen (Es müssen beide Seiten einverstanden sein).
  d.h. sie peeren miteinander.

- Gibt eine Peer auch die Routen, die es von anderen Peers gelernt hat weiter, so bietet dieses AS Transit an.

  Beispielsweise:
  AS2 kann AS3 via AS1 erreichen.





BGP AS Path

- Kennt BGP mehrere Wege zum Ziel AS, so ist die Länge des AS-Pfades (AS-PATH) ein wichtiges Kriterium um den Weg zu bestimmen.

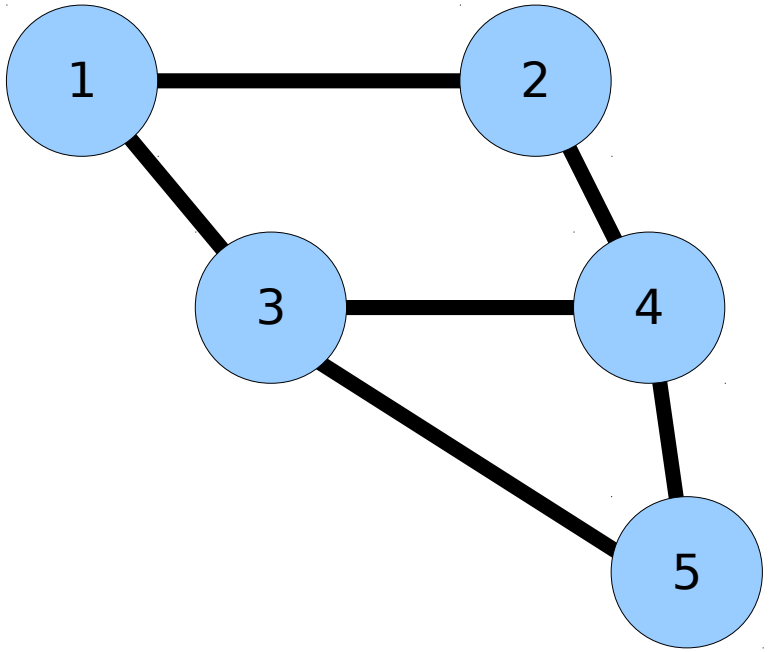
AS1 → AS5

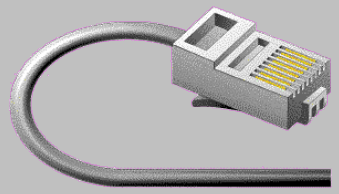
1-2-4-5

1-2-4-3-5

1-3-5

1-3-4-5





BGP AS Path

- Je nach Bedürfnisse kann man die eigene AS-Nummer einfügen, um den Traffic steuern zu können.

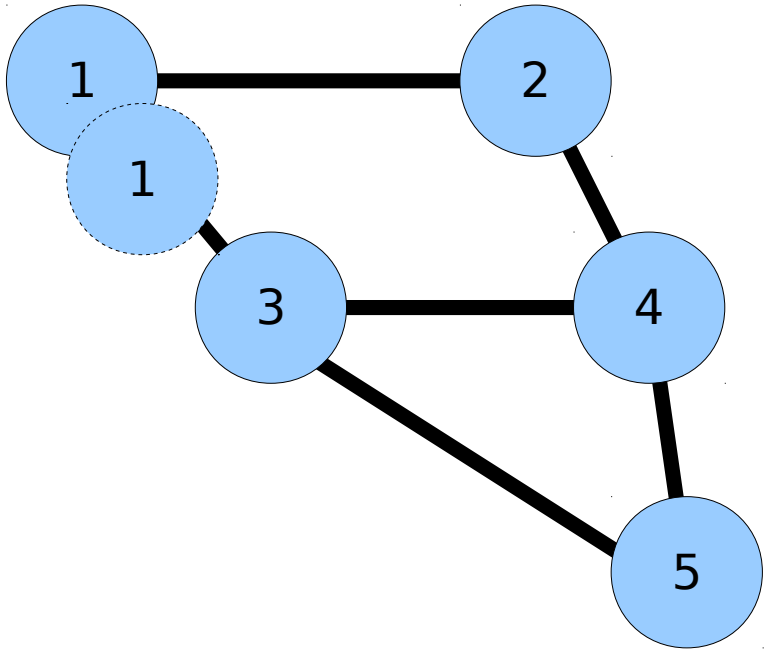
AS1 → AS5

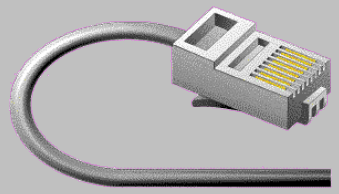
1-2-4-5

1-2-4-3-5

1-1-3-5

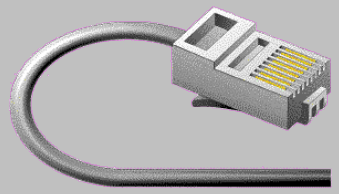
1-1-3-4-5





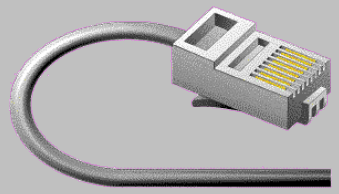
BGP AS Path

```
glbix-br1#sh ip bgp 130.59.138.34
BGP routing table entry for 130.59.0.0/16, version 476502
Paths: (2 available, best #1, table Default-IP-Routing-Table)
Multipath: eBGP iBGP
  Advertised to update-groups:
     4
  559
    194.242.34.53 from 194.242.34.53 (130.59.32.30)
      Origin IGP, metric 421, localpref 150, valid, external, best
      Community: 15623:2003
  702 559
    139.4.71.37 from 139.4.71.37 (146.188.0.13)
      Origin IGP, metric 10000, localpref 100, valid, external
      Community: 15623:1001
```



BGP AS Path

```
zhtix-cr1>sh ip bgp 130.59.138.34
BGP routing table entry for 130.59.0.0/16, version 557412
Paths: (3 available, best #1, table Default-IP-Routing-Table)
Multipath: eBGP iBGP
  Advertised to update-groups:
     2           4           5           6
  559, (Received from a RR-client)
    194.242.34.53 (metric 28416) from 212.55.222.5 (212.55.222.5)
      Origin IGP, metric 421, localpref 150, valid, internal, multipath, best
      Community: 15623:2003
  559, (Received from a RR-client)
    194.242.34.53 (metric 28416) from 212.55.222.48 (212.55.222.48)
      Origin IGP, metric 421, localpref 150, valid, internal
      Community: 15623:2002
  559, (Received from a RR-client)
    194.42.48.11 (metric 28416) from 212.55.222.49 (212.55.222.49)
      Origin IGP, metric 421, localpref 150, valid, internal, multipath
      Community: 15623:2001
```

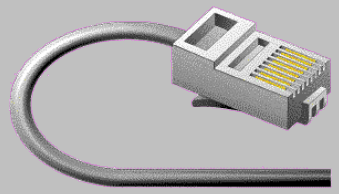


BGP

```
zhtix-cr1>tr ip www.switch.ch
Translating "www.switch.ch"...domain server (62.12.130.66) [OK]

Type escape sequence to abort.
Tracing the route to oreius.switch.ch (130.59.138.34)

  1 zhtix-br2.cyberlink.ch (212.55.192.197) 76 msec
    zhtix-br1.cyberlink.ch (212.55.192.196) 0 msec
    zhtix-br2.cyberlink.ch (212.55.192.197) 316 msec
  2 swiIX1-G3-5.switch.ch (194.242.34.53) [AS 20612] 0 msec
    swiix1-g2-1.switch.ch (194.42.48.11) [AS 8235] 0 msec
    swiIX1-G3-5.switch.ch (194.242.34.53) [AS 20612] 0 msec
  3 swiEZ2-10GE-1-3.switch.ch (130.59.36.249) [AS 559] 0 msec 4 msec 0 msec
  4 swiLS2-10GE-1-1.switch.ch (130.59.36.205) [AS 559] 4 msec 4 msec 4 msec
  5 swiCP2-G1-0-28.switch.ch (130.59.36.14) [AS 559] 4 msec 4 msec 4 msec
  6 oreius.switch.ch (130.59.138.34) [AS 559] 4 msec 4 msec 4 msec
```



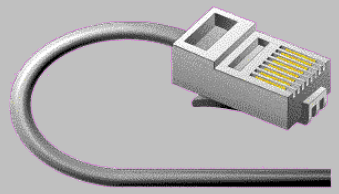
BGP Tools

Looking Glass: (Webfrontends)
http://www.ris.ripe.net/cgi-bin/lg/index.cgi
http://traceroute.org/#Looking%20Glass

Route Server: (direktes Login auf einem Router)
http://traceroute.org/#Route%20Servers

BGPlay: Graphische Darstellung vom AS-Path
http://www.ris.ripe.net/bgplay/

Traceroute:
http://traceroute.org/

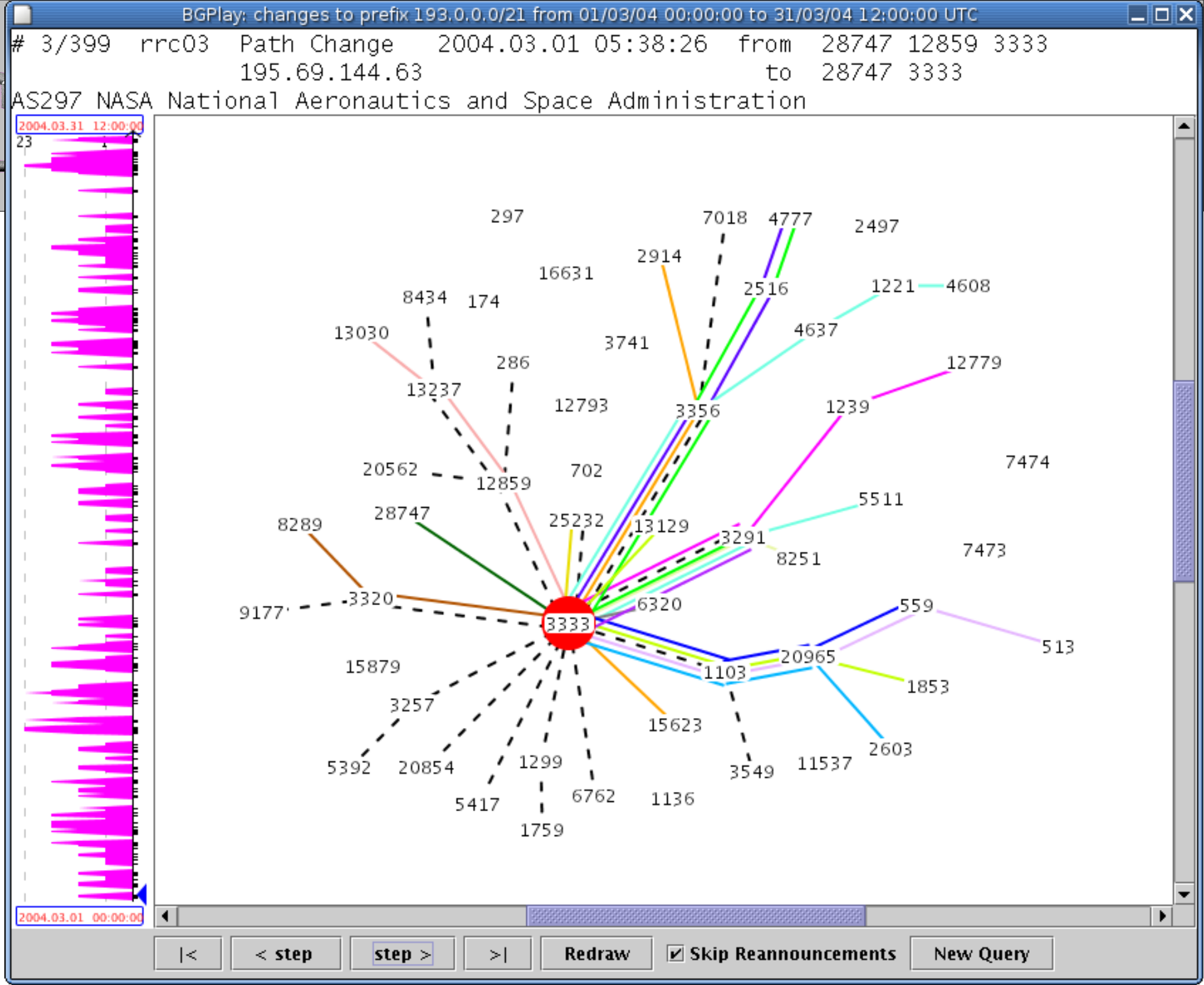


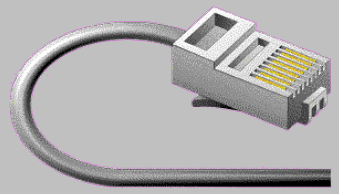
BGP Tools

Statistiken

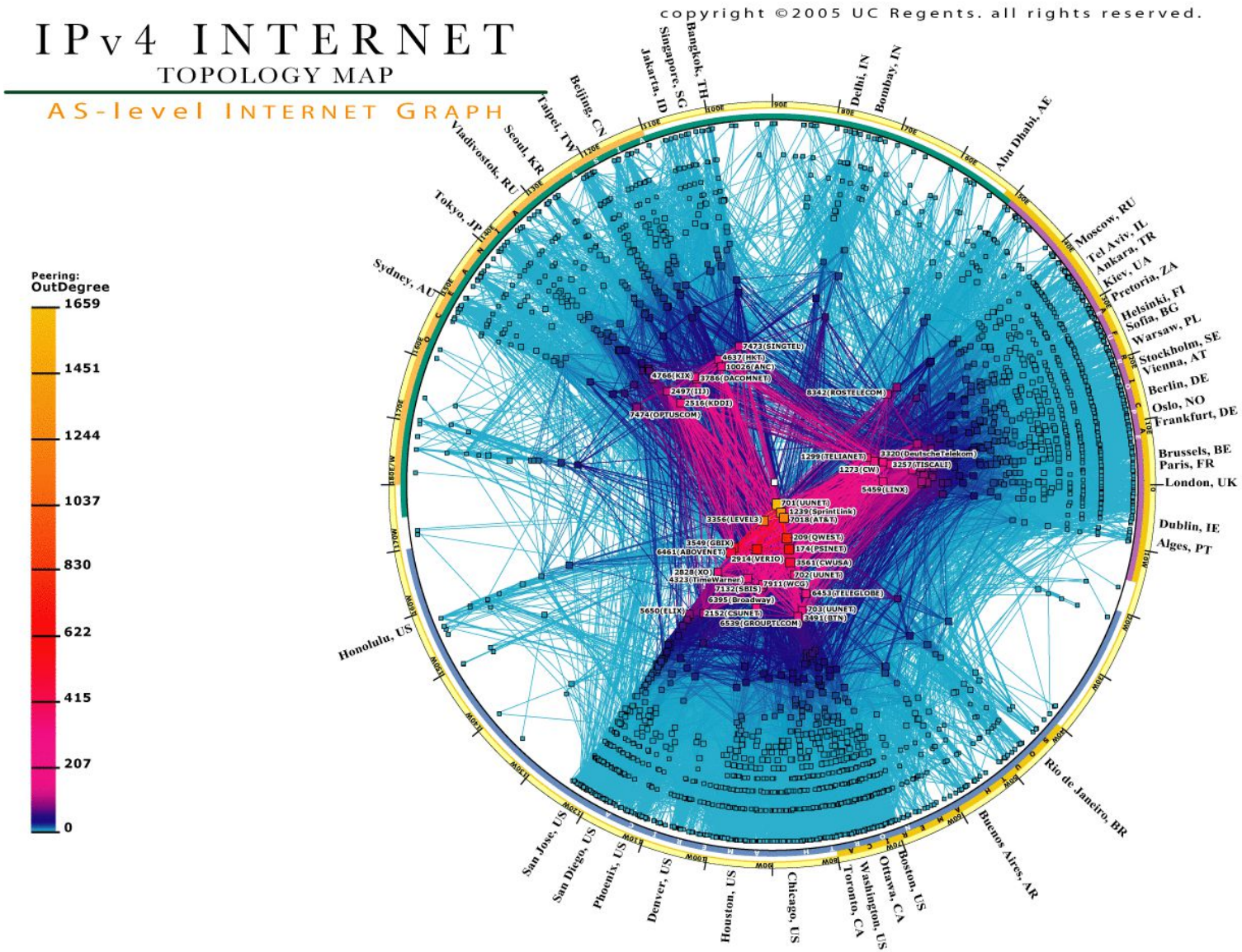
http://www.caida.org/

http://www.ripe.net/projects/ris/


BGPlay: changes to prefix 193.0.0.0/21 from 01/03/04 00:00:00 to 31/03/04 12:00:00 UTC
3/399 rrc03 Path Change 2004.03.01 05:38:26 from 28747 12859 3333
195.69.144.63 to 28747 3333
AS297 NASA National Aeronautics and Space Administration
2004.03.31 12:00:00
23
1
2004.03.01 00:00:00
297
7018
4777
2497
2914
16631
2516
1221
4608
8434
174
4637
13030
3741
286
12779
13237
12793
3356
1239
20562
12859
702
7474
5511
28747
25232
13129
3291
8289
8251
7473
3320
9177
6320
559
3333
513
20965
15879
1103
1853
3257
15623
2603
5392
20854
1299
3549
11537
6762
5417
1136
1759
|<
< step
step >
>|
Redraw
Skip Reannouncements
New Query



Fragen?


IPv4 INTERNET
TOPOLOGY MAP
AS-level INTERNET GRAPH
copyright ©2005 UC Regents. all rights reserved.
Peering:
OutDegree
1659
1451
1244
1037
830
622
415
207
0
Singapore, SG
Jakarta, ID
Bangkok, TH
Delhi, IN
Bombay, IN
Abu Dhabi, AE
Moscow, RU
Tel Aviv, IL
Ankara, TR
Kiev, UA
Pretoria, ZA
Helsinki, FI
Sofia, BG
Warsaw, PL
Stockholm, SE
Vienna, AT
Berlin, DE
Oslo, NO
Frankfurt, DE
Brussels, BE
Paris, FR
London, UK
Dublin, IE
Alges, PT
Rio de Janeiro, BR
Buenos Aires, AR
Boston, US
Ottawa, CA
Washington, US
Toronto, CA
Chicago, US
Houston, US
Denver, US
Phoenix, US
San Diego, US
San Jose, US
Honolulu, US
Sydney, AU
Tokyo, JP
Vladivostok, RU
Seoul, KR
Taipei, TW
Beijing, CN
7473(SINGTEL)
4637(HKT)
10026(ANC)
4766(KIX)
9786(DACOMNET)
2497(IIJ)
2516(KDDI)
7474(OPTUSCOM)
8342(ROSTELECOM)
1299(TELIANET)
3320(DeutscheTelekom)
3257(TISCALI)
1273(CW)
5459(LINX)
701(UUNET)
1239(SprintLink)
7018(AT&T)
3356(LEVEL3)
209(QWEST)
3549(GBIX)
6461(ABOVENET)
174(PSINET)
2914(VERIO)
3561(CWUSA)
2828(XO)
4323(TimeWarner)
702(UUNET)
7911(WCG)
7132(SBIS)
6453(TELEGLOBE)
6395(Broadway)
5650(ELIX)
2152(CSUNET)
703(UUNET)
6539(GROUPTLCOM)
3491(BTN)