BGP Hijacking
Was ist das und wie funktionierts

Dipl.-Ing. Mathias Gärtner

NIFIS e.V.

Berkersheimer Bahnstraße 5

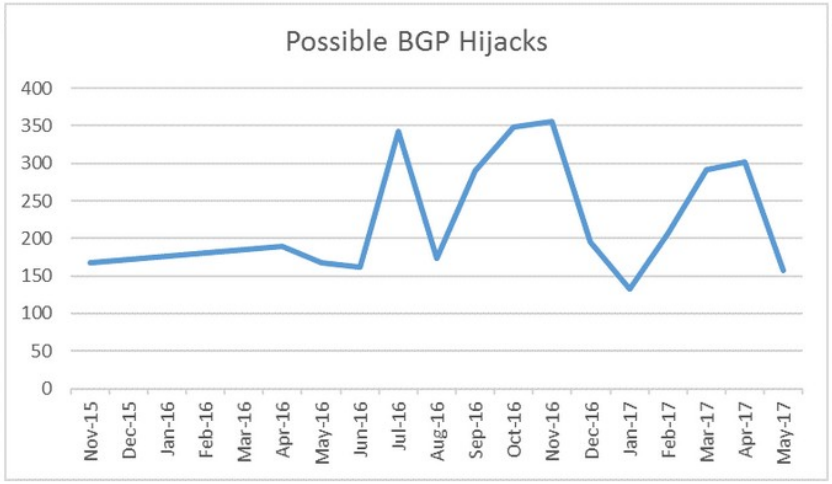
60435 Frankfurt am Main

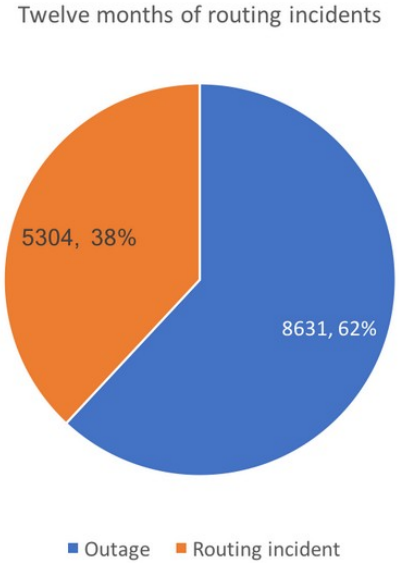
Tel: 069 24 44 47 57

Email: Mathias.Gaertner@nifis.de
https://www.nifis.de

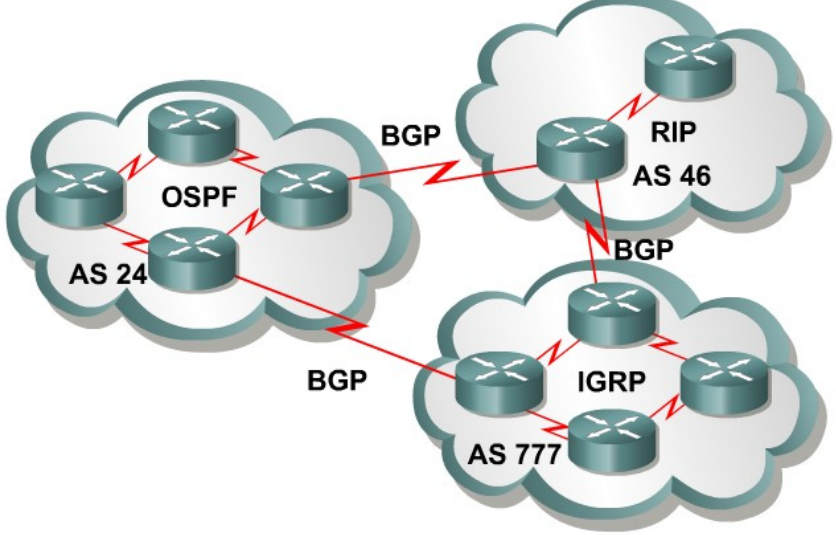
BGP Hijacking, was ist das Problem?

- BGP hijacking bedeutet, dass unautorisierte Quellen falsche Erreichbarkeitsinformationen bereit stellen (entweder absichtlich oder unabsichtlich). Dies führt dann zu Störungen im Internet
- In 2017 waren es 13935 Vorfälle
- 62 % davon (8631) verursachten Erreichbarkeitsausfälle, der Rest leitete den Datenverkehr über “falsche” Stellen um und ermöglichsten u.U. Man-In-The-Middle Angriffe
- Zwischen 15. Nov. und 17. Mai 2017 wurden 3482 echte Angriffe erkannt



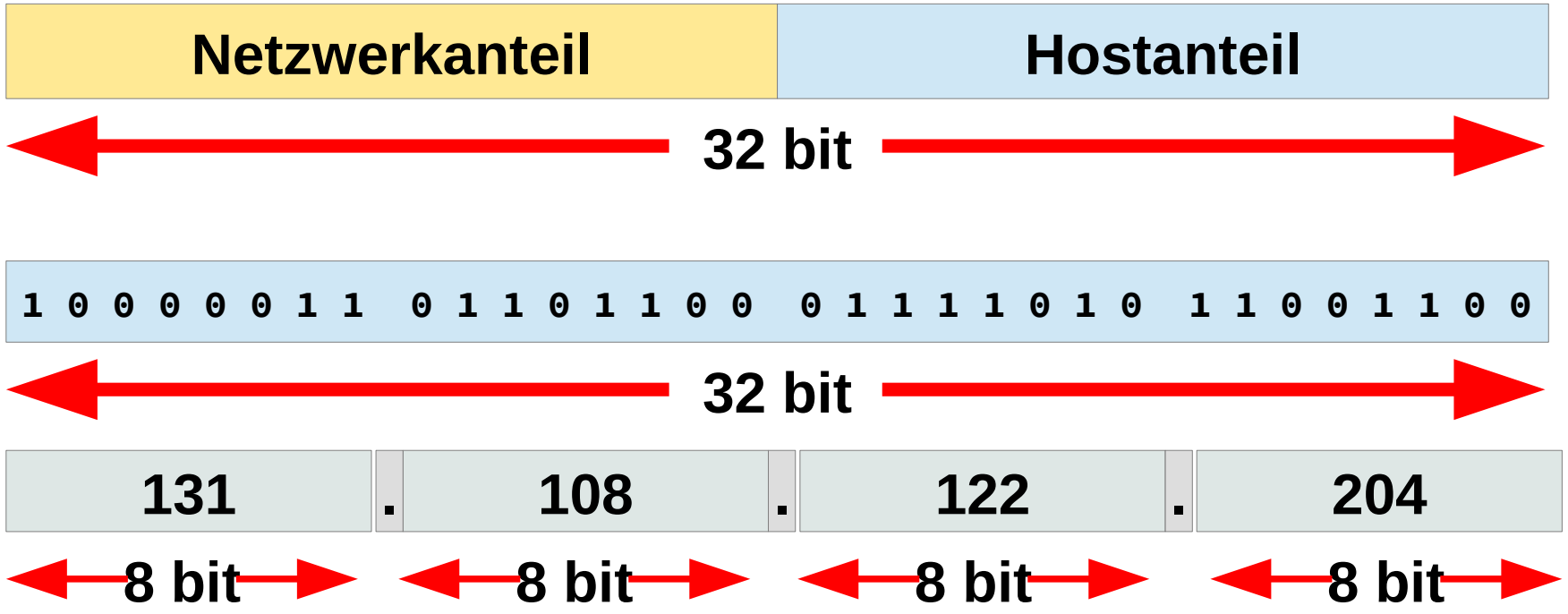


Begriffe

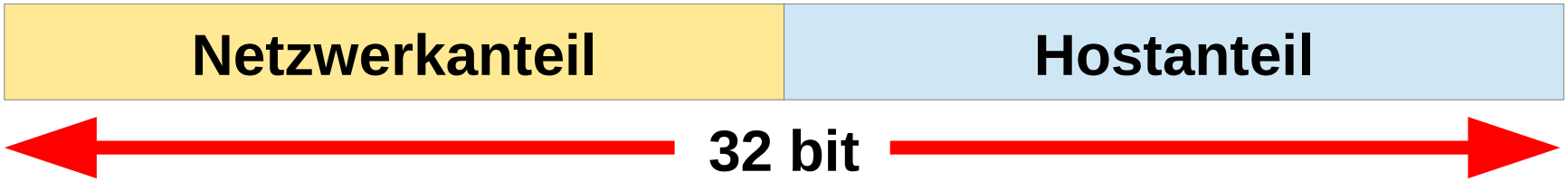


- **BGP (Border Gateway Protocol)** ist das Routingprotokoll mit dem Autonome Systeme Ihre Erreichbarkeiten austauschen
  - **BGP** - ist ein sog. “path vector” routing protocol.
- **Autonomes System**
  - (Aus RFC 1771) “Eine Menge an Routern die unter einer technischen Administration sind, die ein internes Routingprotokoll benutzen und eine gemeinsame Metrik zur Wegefindung innerhalb des internen Netzes haben und die ein EGB (also BGP) zur Weiterleitung an andere AS benutzen”

IPv4-Adresse



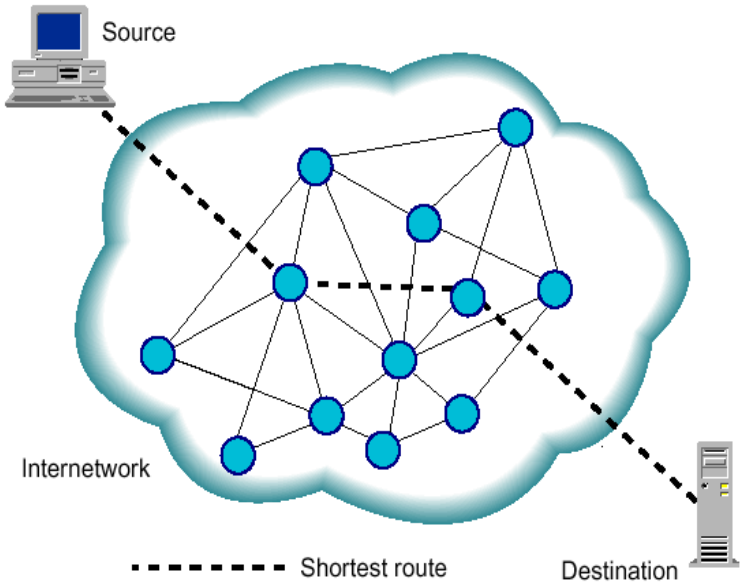
IPv4-Adresse



- Eine IP Adresse identifiziert genau einen Computer. Eine Routingtabelle könnte daher theoretisch bis zu 4 Milliarden Einträge groß werden.
- Das Verwalten und Nutzen einer solchen Tabelle ist (fast) nicht machbar, zumindest nicht mit der notwendigen Geschwindigkeit
- Daher wird mit Zusammenfassungen gearbeiten

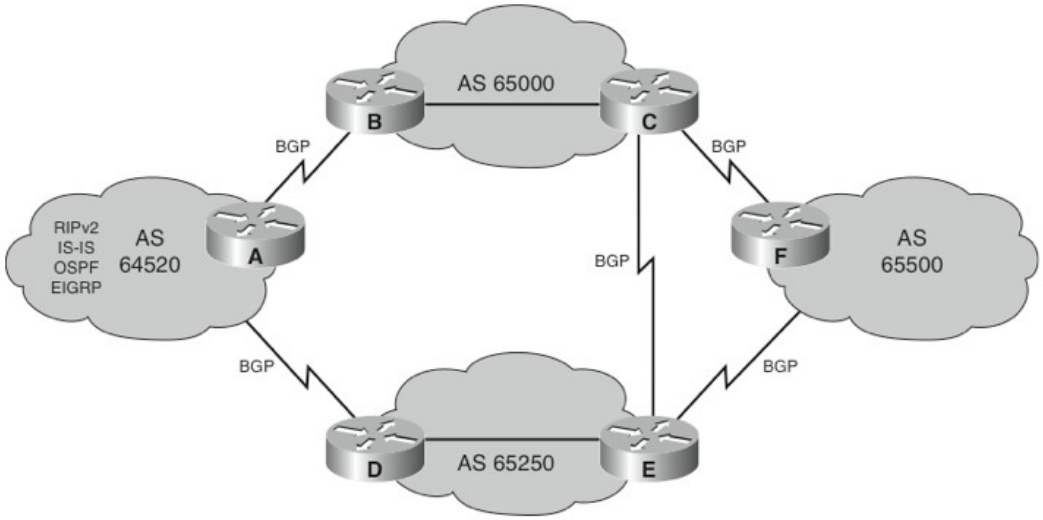
- Eine sog. Netzwerkmaske bestimmt wie viele Bits (aus 32) zusammengefasst werden sollen. Diese bestimmt also die Größe des Netzwerkanteils. Die Anzahl der Bits kann von 0 bis 32 reichen (Alle Computer bis EIN Computer)
- Nomenklatur ist <IP-NETWORK>**/**<NUMBER OF NETMASK BITS>, z.B. 131.108.122.0/24

Wegefindung im Generellen



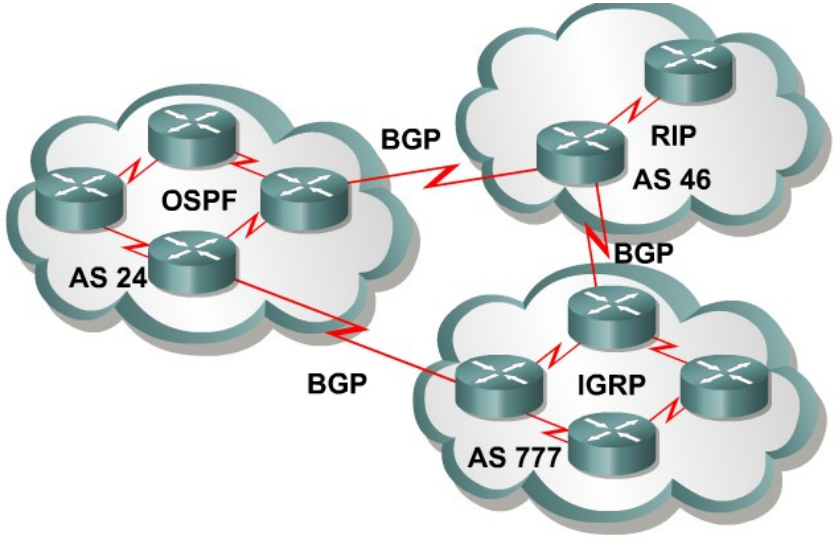
- Jeder Netzwerkknoten (Router) hat seine eigene Entscheidungstabelle. Er wird empfangene Datenpakete anhand der Tabelleneinträge an den entsprechenden Nachbarn weiterreichen.
- Die Tabelle wird mittels manueller oder automatischer Verfahren gefüllt. Automatische Verfahren sind u.a. eben das BGP-Protokoll.
- Was genau der “beste” Pfad ist, ist je nach eingesetzem Routingverfahren unterschiedlich.
- Allen gemein ist jedoch, dass Einträge mit einer größeren Netzwerkmaske (größere Nummer nach dem ‘/’) bevorzugt werden.

BGP Nutzung bei den Autonomen Systeme



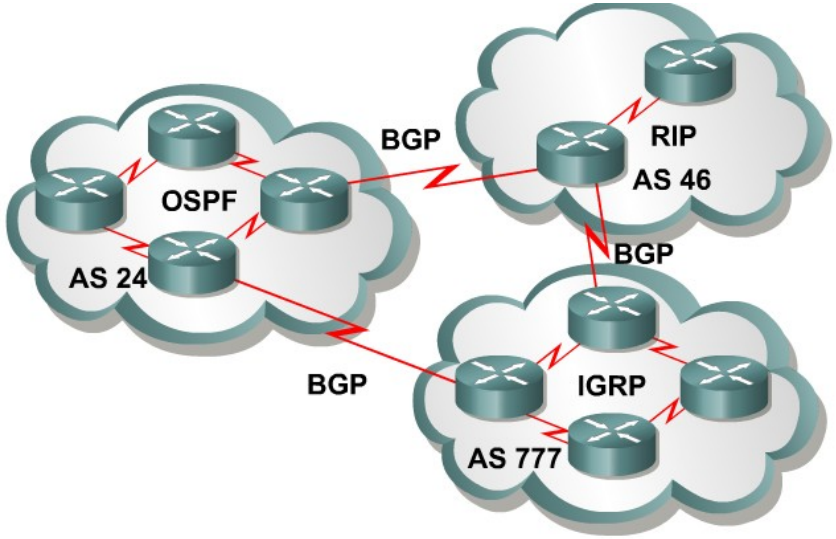
- Das Hauptziel ist es, ein Interdomain Routing system aufzubauen das ein schleifenfreies Austauschen von Erreichbarkeitsinformationen zwischen den AS ermöglicht
- BGP-4 ist ein sog. “classless” routing Protokoll. Es unterstützt:
  - VLSM
  - CIDR
    - Es gibt zur Zeit mehr als 400,000 CIDR blocks
    - Ohne CIDR würde die Routingtabelle mehr als 2,000,000 Einträge haben.

Kurzübersicht Autonomes System



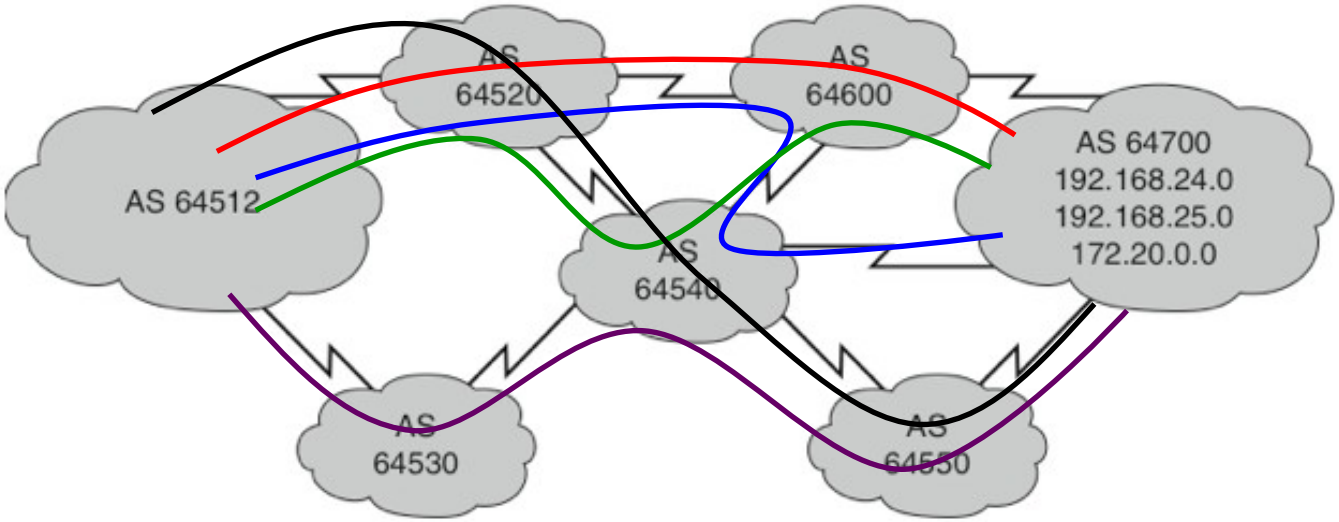
- **AS** - Eine Gruppe von Routern die eine gleichartige Policy aufweisen und von einer Administration verwaltet werden
- Ein AS kann sein:
  - Eine Sammlung von Routern, die ein gemeinschaftliches internes Routingprotokoll verwenden (z.B. Firmennetz)
  - Eine Sammlung von Routern, die unterschiedliche Routingprotokolle verwenden aber alle zu ein und derselben Organisation gehören (z.B. ein ISP)
- In beiden Fällen ist das von aussen gesehen ein und das selbe System

Kurzübersicht Autonomes System



AS Nummern

- Die ICANN vergibt eine eineindeutige Identifikationsnummer
- AS-Nummern reichen von **1 bis 65,535**.
- **0 - Reserviert**
- **1 bis 64,495 – „Echte“ AS-Nummern**
- **64,512 bis 65,535** - **Private AS-Nummern, nicht für das Internet nutzbar**
- **65,535 - Reserviert**
- Da die Anzahl der AS-Nummern begrenzt ist, muss man schon eine gute Begründung liefern warum man so etwas benötigt.



- Mögliche Pfade des AS 64512 um die Netzwerke im AS 64700, durch das AS 64520 zu erreichen:
  - 64520 64600 64700
  - 64520 64600 64540 64550 64700
  - 64520 64540 64600 64700
  - 64520 64540 64550 64700
- AS 64512 sieht aber nicht alle möglichen Pfade.
- AS 64520 reicht nur seinen besten Pfad zum AS 64512 weiter:
  - 64520 64600 64700 (dies ist durch lokale Policies beeinflußbar)
- AS 64512 könnte auch einen besten Pfad vom AS 64530 erhalten
- AS 64512 würde dann aufgrund eigener Policies entscheiden, welcher Pfad (via 64530 oder via 64520) der “beste” wäre.

YouTube Hijacking: Ein RIPE NCC RIS Fallbeispiel

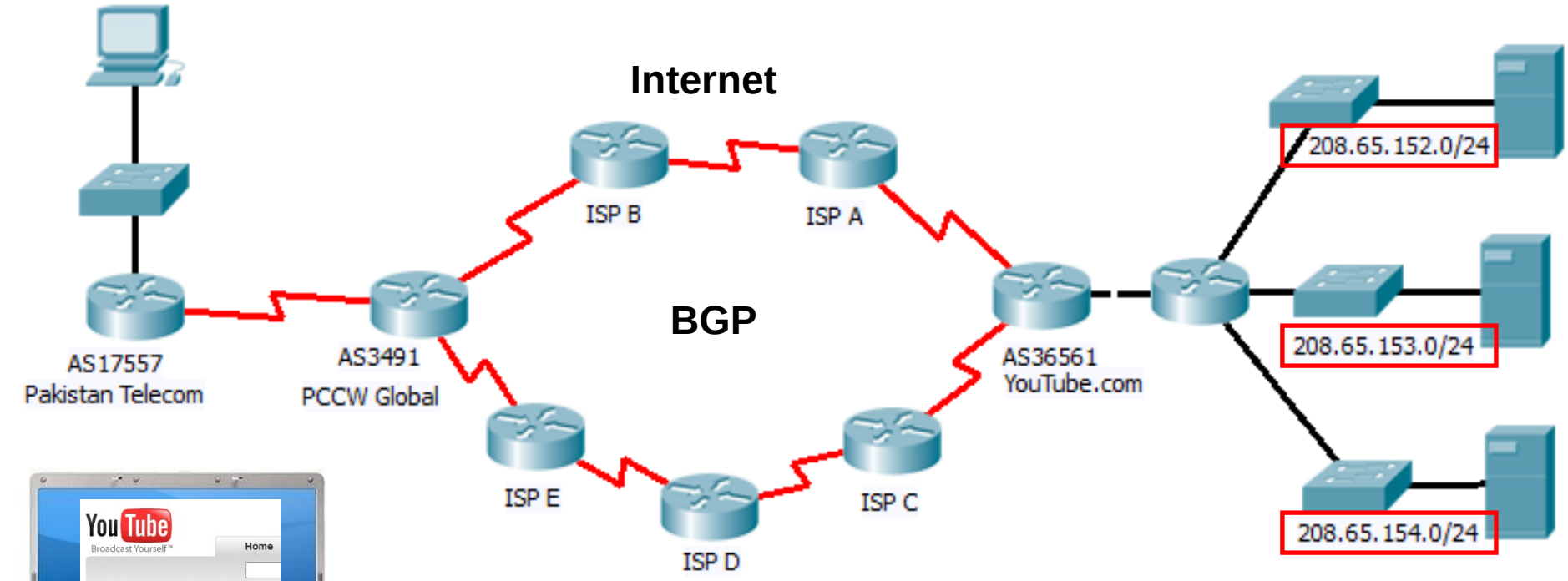
YouTube Hijacking: RIPE NCC RIS Fallbeispiel

- Die Präsentation wurde von der RIPE NCC Webseite genommen.
- Für mehr Informationen siehe
  - http://www.ripe.net/news/study-youtube-hijacking.html

- Das Folgende ist eine genaue Beschreibung der Ereignisse dieses Vorfalls, jedoch wurden die technischen Details vereinfacht.

- Am Sonntag, den 24 Februar 2008, Pakistan Telecom (AS17557) begann die Verbreitung des nicht genehmigten Prefixes 208.65.153.0/24.
- Einer der Upstream-Provider von Pakistan Telecom, PCCW Global (AS3491) reichte diese Informationen ungeprüft an den rest des Internets weiter. Dies resultierte in dem “Kidnapping” der Erreichbarkeit von Youtube auf einem weltweiten Level.

Vor, während und nach Sonntag, 24 Februar 2008

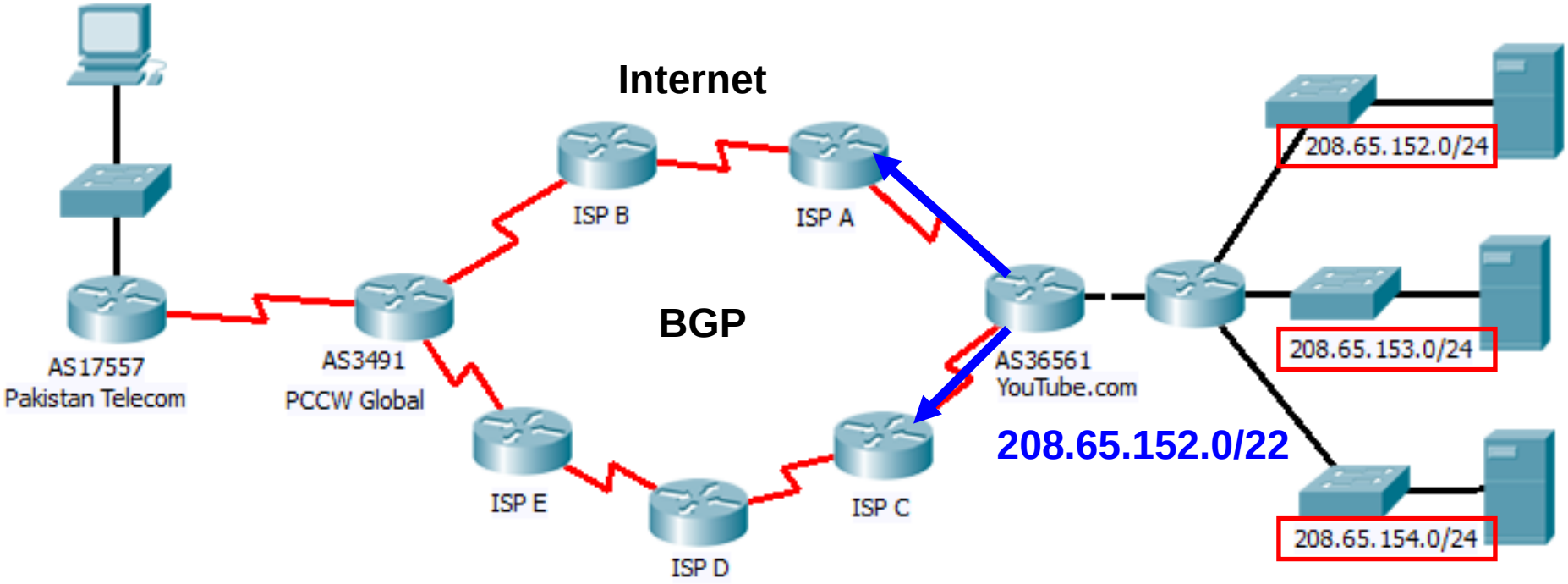



```
C:\Users\rigrazia>nslookup www.youtube.com
Server:  cns.sanjose.ca.sanfran.comcast.net
Address:  68.87.76.178:53

Non-authoritative answer:
Name:    www.youtube.com
Addresses:  208.65.153.251, 208.65.153.253, 208.65.153.238
```

- DN Server zeigten www.youtube.com als:
  - 208.65.153.251
  - 208.65.153.253
  - 208.65.153.238

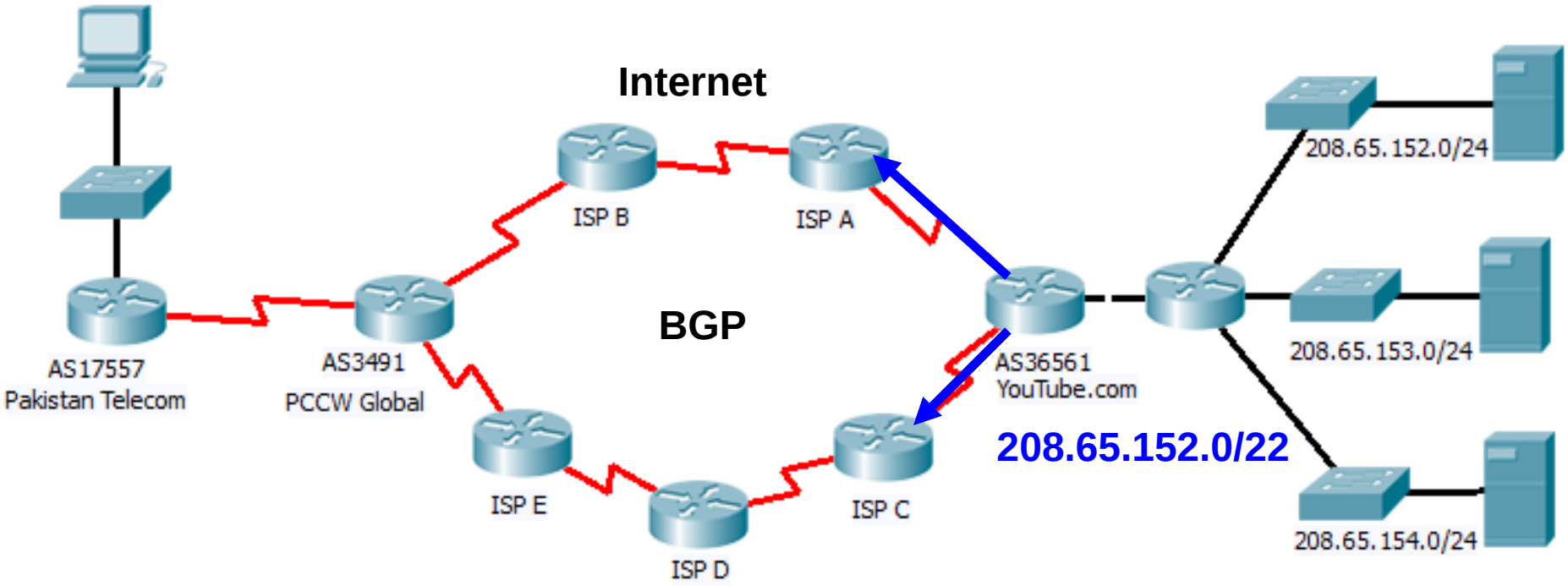
Vor, während und nach Sonntag, 24 Februar 2008



YouTube fasst (CIDR) seine /24 Netzwerke zu einem /22 Eintrag zusammen:

```
208.65.152.0/24  11010000. 01000001.10011000.00000000
208.65.153.0/24  11010000. 01000001.10011001.00000000
208.65.154.0/24  11010000. 01000001.10011010.00000000
                 ----------------------------------
208.65.152.0/22  11010000. 01000001.10011000.00000000
```

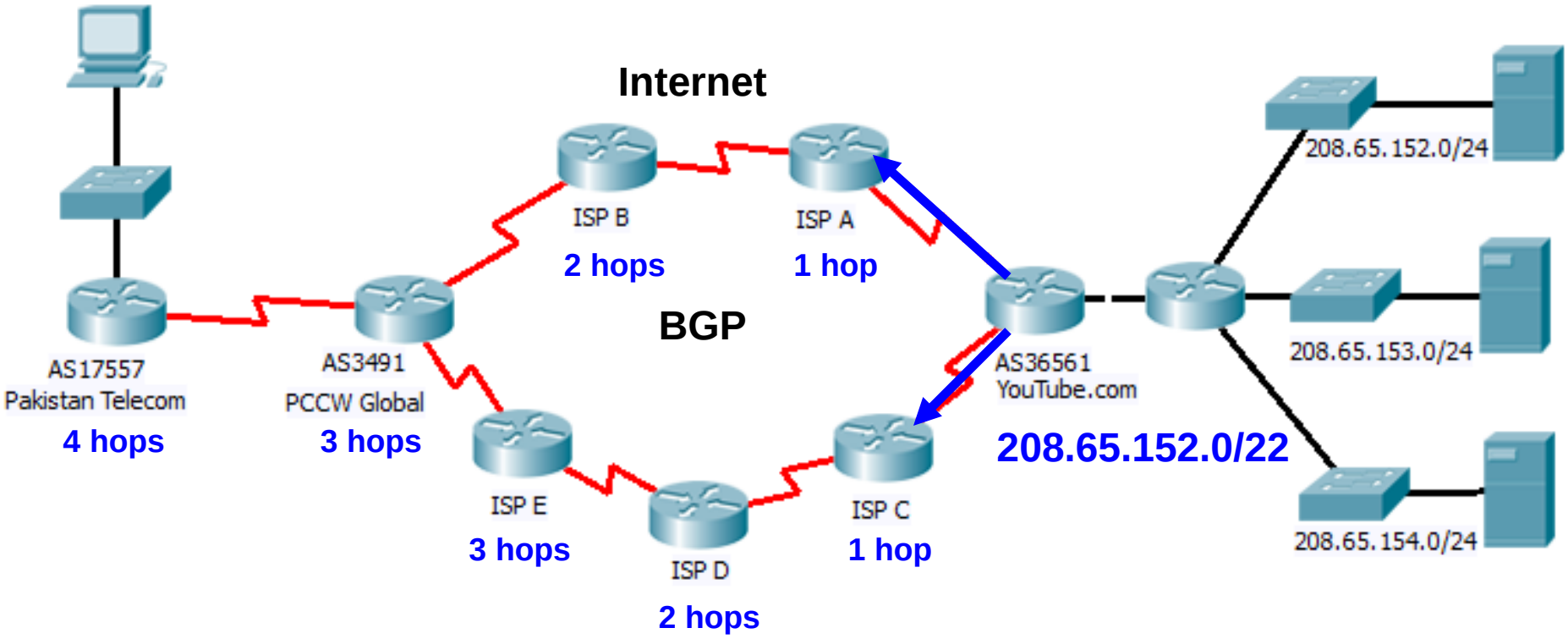
Vor, während und nach Sonntag, 24 Februar 2008



Vor, während und nach Sonntag, 24 Februar 2008:

- AS36561 (YouTube) verteilt 208.65.152.0/22.
- Hinweis: AS36561 verteilt(e) auch noch andere Prefixe, diese haben jedoch mit dem Fall nichts zu tun

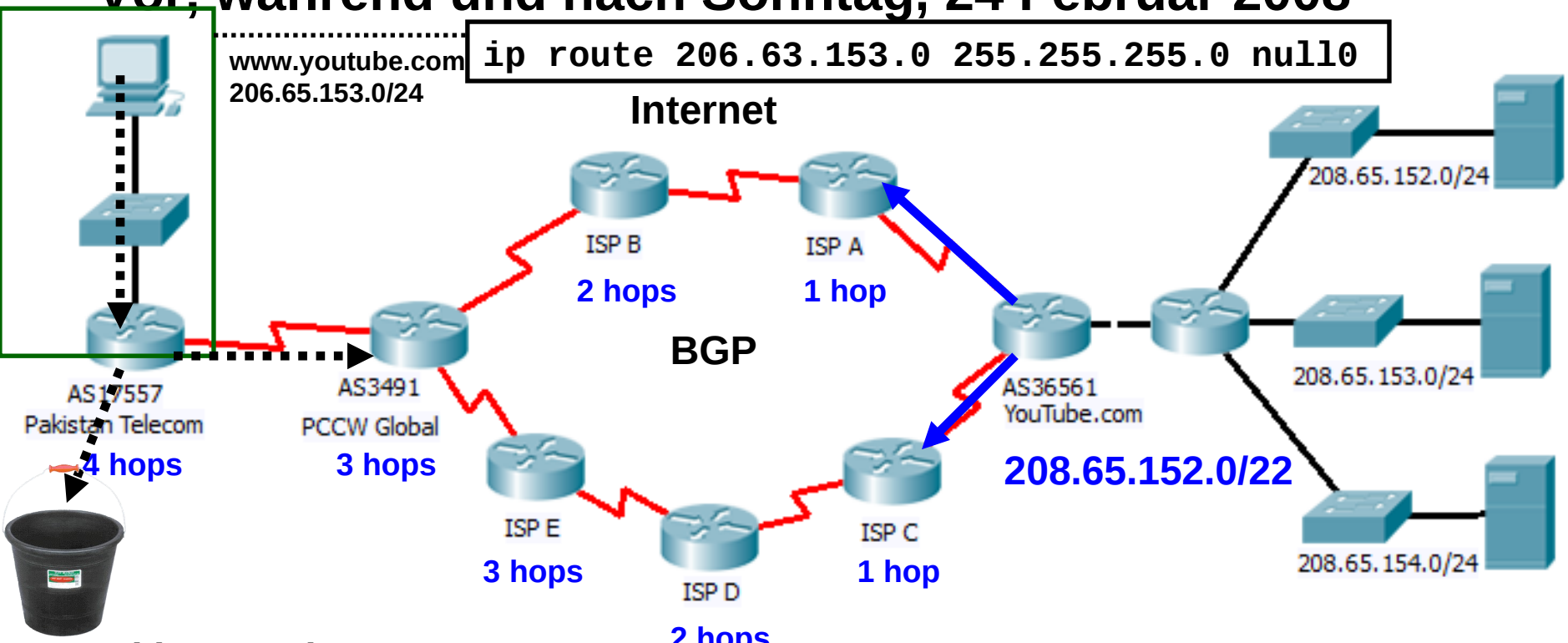
Vor, während und nach Sonntag, 24 Februar 2008



BGP

- Solange es keine anderen Policies gibt, wählt BGP immer den kürzesten AS-Pfad als “besten” Pfad.

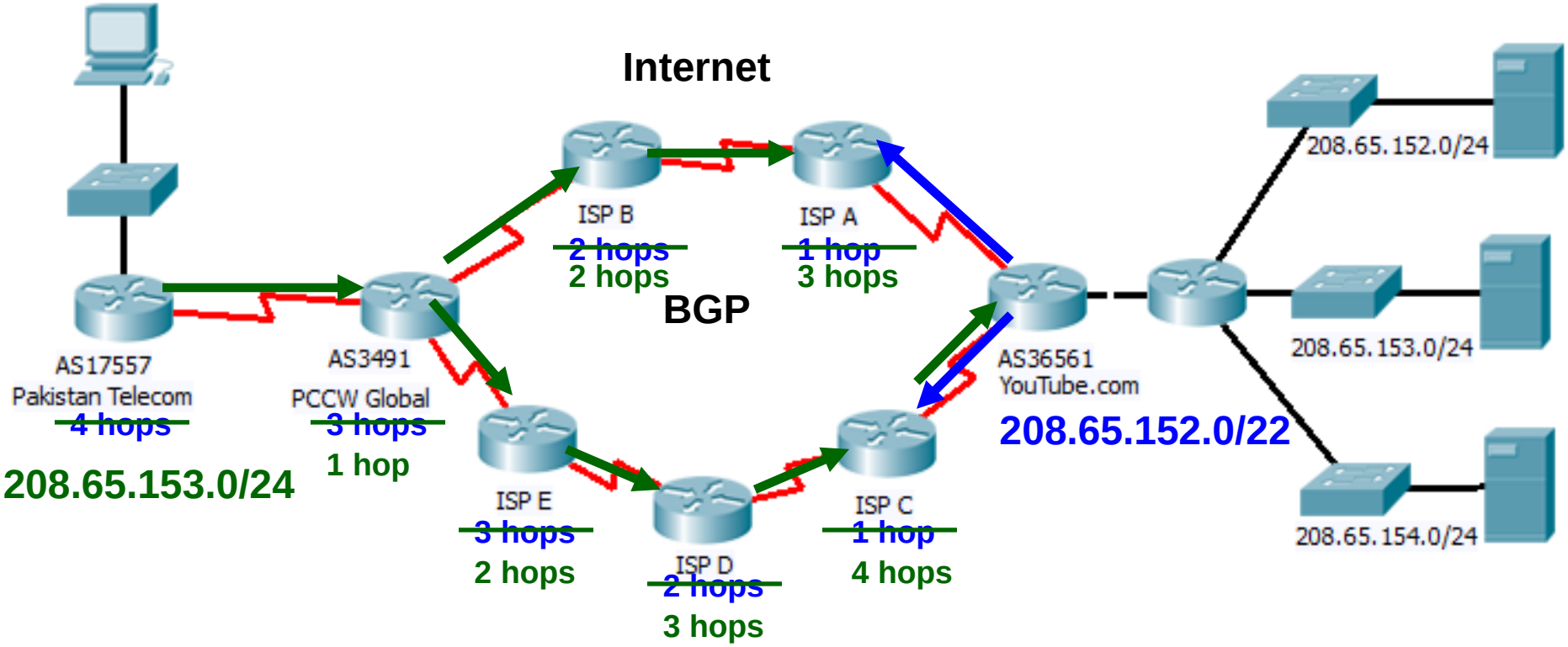
Vor, während und nach Sonntag, 24 Februar 2008



Pakistan Telecom

- Ziel war es, den Datenverkehr zu Youtube zu blockieren (Gerichtsbeschluss).
- Sehr wahrscheinlich wählten Sie die Methode einen Routingeintrag zu erstellen, der Datenpakete zu Youtube (208.65.153.0/24, DNS Adresse für www.youtube.com) zu einem nicht existenten Netzwerk zu leiten und somit den Datenverkehr zu Youtube zu verhindern
- Ihr Fehler war es, diese Routinginformation an PCCW Global weiter zu reichen.

Sonntag, 24 Februar 2008, 18:47 (UTC)

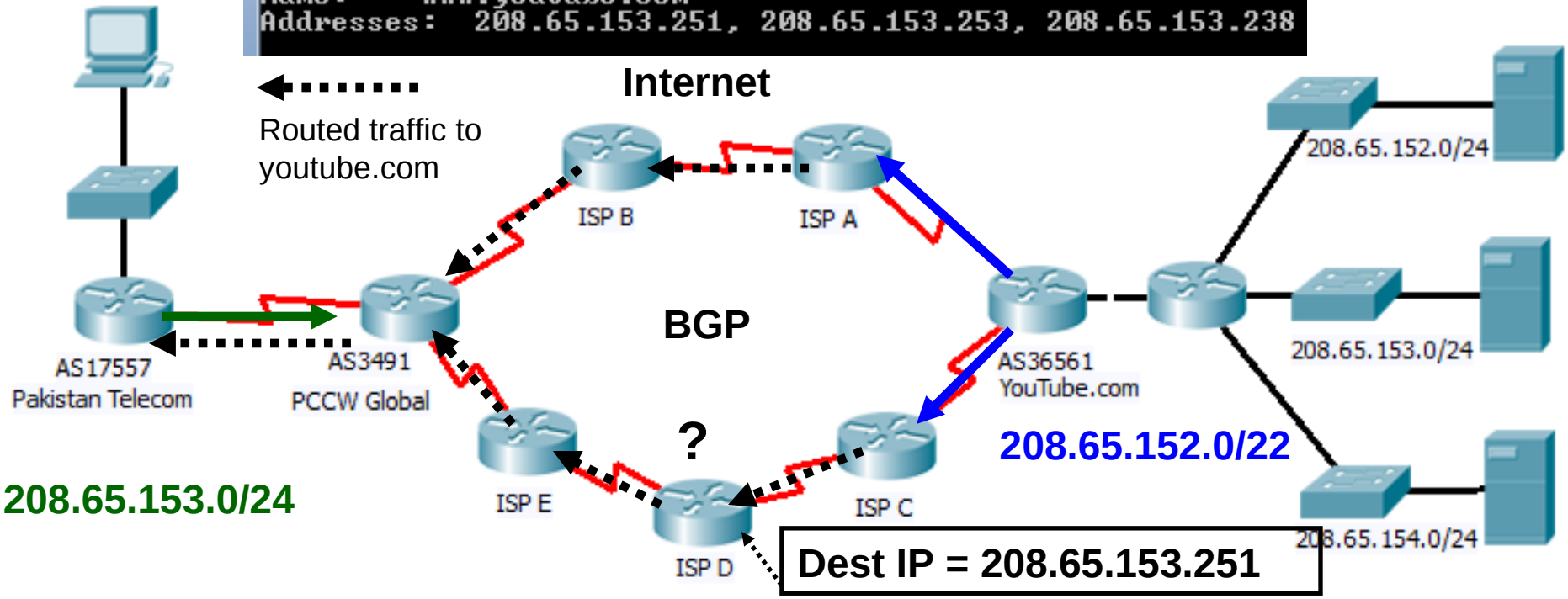


Sonntag, 24 Februar 2008, 18:47 (UTC):

- AS17557 (Pakistan Telecom) begann die Weitergabe einer "**genaueren**" Routinginformation für 208.65.153.0/24.
- AS3491 (PCCW Global) reichte diese Information einfach weiter.
- Die Router in der gesamten Welt empfingen diese Information und verwendeten sie, da sie ja genauer war als die von Youtube selbst gelieferte

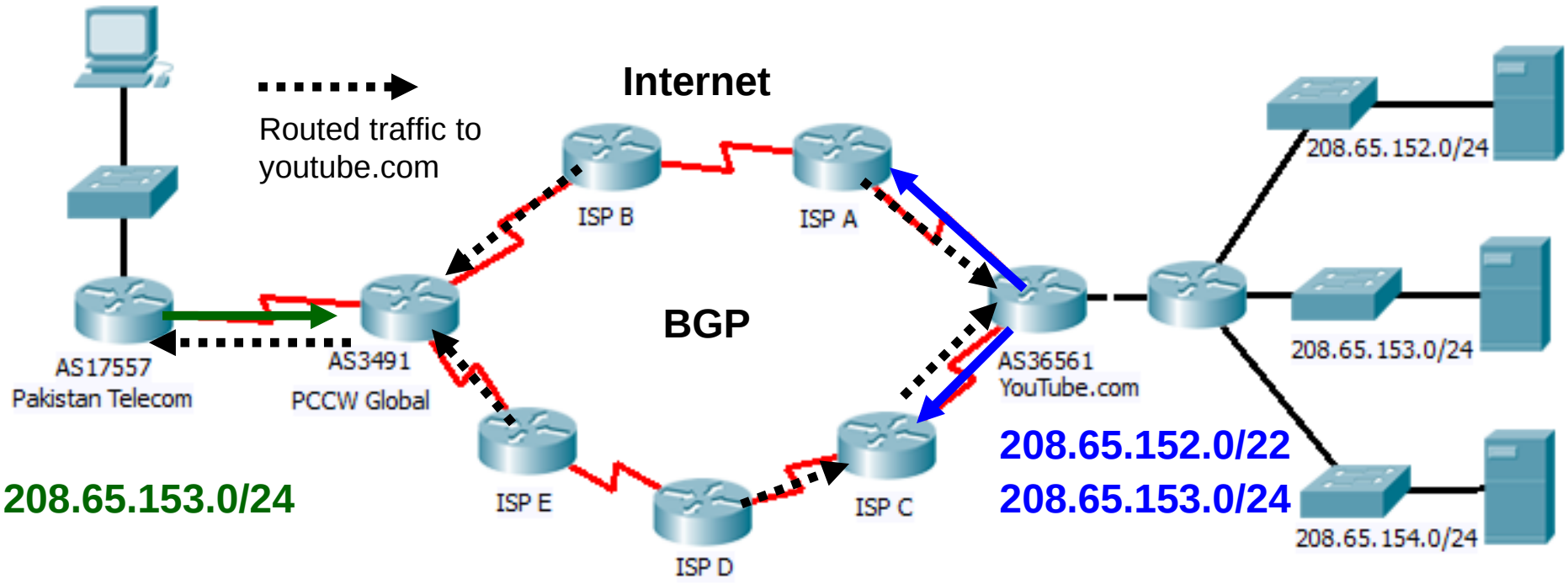
```
C:\Users\rigrazia>nslookup www.youtube.com
Server:  cns.sanjose.ca.sanfran.comcast.net
Address:  68.87.76.178:53

Non-authoritative answer:
Name:    www.youtube.com
Addresses:  208.65.153.251, 208.65.153.253, 208.65.153.238
```



- Warum wird der Datenverkehr an Pakistan Telecom weitergeleitet?
- Wenn ein Router ein Datenpaket zum Ziel **208.65.153.251** erhält, welcher Pfad wird gewählt?
  - Die Router lernen zwei Wege, den für **208.65.153.0/24** und den für **208.65.152.0/22.** Beide werden in der Tabelle eingetragen.
  - Wenn der Router nun ein Paket zum Ziel **208.65.153.251** erhält, so wird er den Eintrag mit der längsten Netzwerkmaske verwenden und das ist: **208.65.153.0/24**
  - 24 bits sind länger (also genauer) als 22 bits

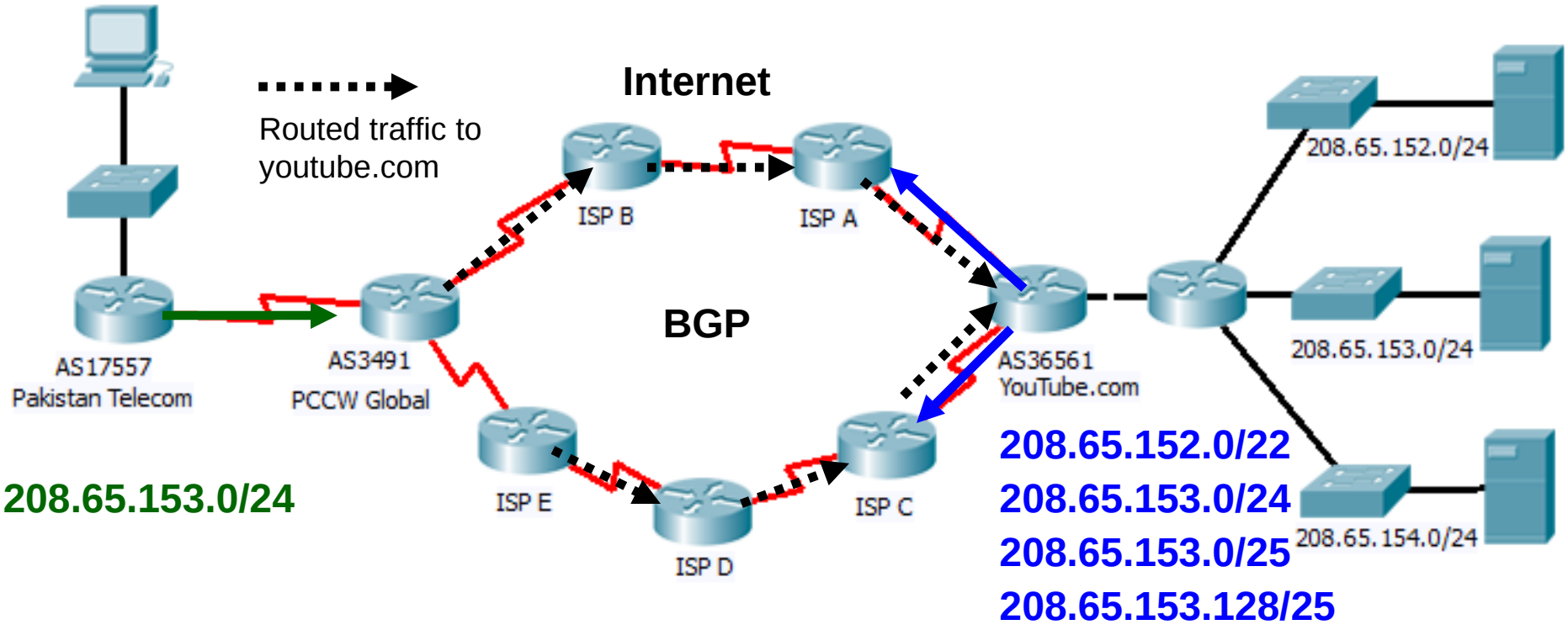
Sunday, 24 February 2008, 20:07 (UTC):



Sonntag, 24 Februar 2008, 20:07 (UTC):

- AS36561 (YouTube) starts announcing the same, **more specific prefix** of 208.65.153.0/24.
- With two identical prefixes in the routing system, BGP policy rules, such as preferring the shortest AS path, determine which route is chosen.
- This means that AS17557 (Pakistan Telecom) continues to attract some of YouTube's traffic.

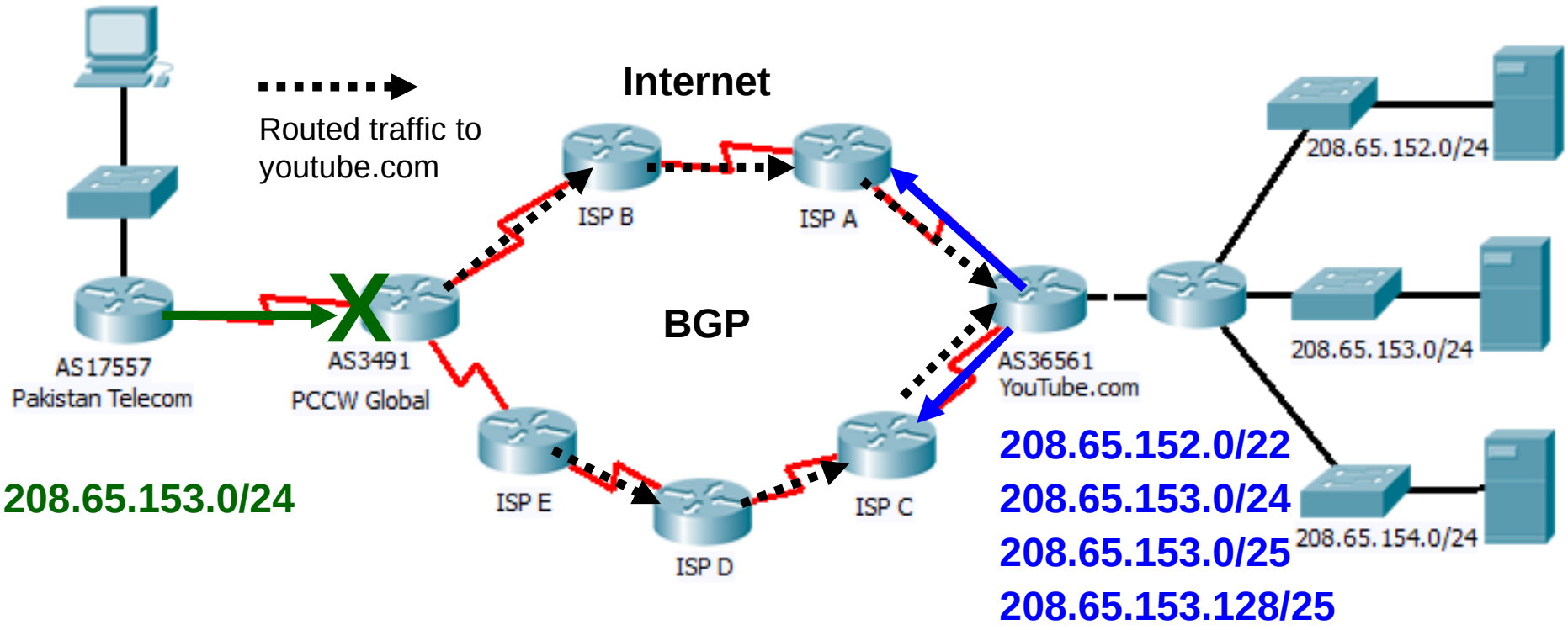
Sonntag, 24 Februar 2008, 20:07 (UTC):



Sonntag, 24 Februar 2008, 20:18 (UTC):

- AS36561 (YouTube) startet die Angabe einer noch “genaueren” Information über 208.65.153.128/25 und 208.65.153.0/25.
- Weil /25 länger als /24 ist wird jeder Router nun diesen Pfad benutzen und der zeigt auf YouTube

Sonntag, 24 Februar 2008, 20:07 (UTC):



Sonntag, 24 Februar 2008, 21:01 (UTC):

- AS3491 (PCCW Global) entfernt ALLE Prefixe, die vom AS17557 (Pakistan Telecom) kommen, stoppt also das Hijacking des Netzwerkes 208.65.153.0/24.
- Das AS17557 wird nicht komplett aus dem Netz entfernt, was möglich wäre.
- Andere Pakistani prefixes werden weiterhin durchgeleitet

Mögliche Lösungen gegen Hijacking

- Route Filter. An den “Ecken” des internets kann ein Provider Filter einsetzen, die falsche Annouoncements verhindern, da es dort unwahrscheinlich ist, dass der Kunde tatsächlich andere Netzwerke als seine eigenen kennt
- Das funktioniert bei ISPs mit Endkunden und gegen unabsichtliche Weitergabe
- Die Kern-ISPs (die in der Mitte des Internets) können dies aber nicht so machen, da nicht bekannt ist ob nicht der Nachbar nun doch einen neuen Pfad eingerichtet hat
- ISPs können jeweils Filter einsetzen, die auf Basis der AS-Nummer, die durchlaufen werden müsste, filtern. Aber das würde dann auch den Automatismus des Internet-Reroutings verhindern.
- Die Benutzung von RPKI/BGPsec. Jeder Provider signiert seine Prefixe mit einem Zertifikat und jeder Durchleiter hängt sein Zertifikat an. Jeder Empfänger kann nun die Zertifikate prüfen und entscheiden ob er die Route akzeptiert oder nicht
- Aber, wer pflegt diese Datenbank? Und wieviele Nachfragen pro Zeiteinheit sind möglich?

Zusammenfassung

- Es ist sehr einfach falsche Routinginformationen in das “Internet” einzuspeisen.
- Es ist sehr schwer diese “Funktion” auszuschalten, da die Architektur des Internet-routings genau darauf basiert.
- Filter sind grundsätzlich möglich, jedoch nicht immer zielführend. Schließlich weiss man nicht welche echten Pfade der Nachbar nun wirklich besitzt (oder dessen Nachbar)
- Die zur Zeit sicherste Lösung: Überwachen der Routing-Tabelle und manuelles Prüfen und Entscheiden bei einer Änderung ob diese Änderung akzeptiert wird. Dies verlangsamt das Entscheidungssystem und erzeugt wahrscheinlich viele „false Positive“ Alarme, stabilisiert aber das Gesamtsystem.