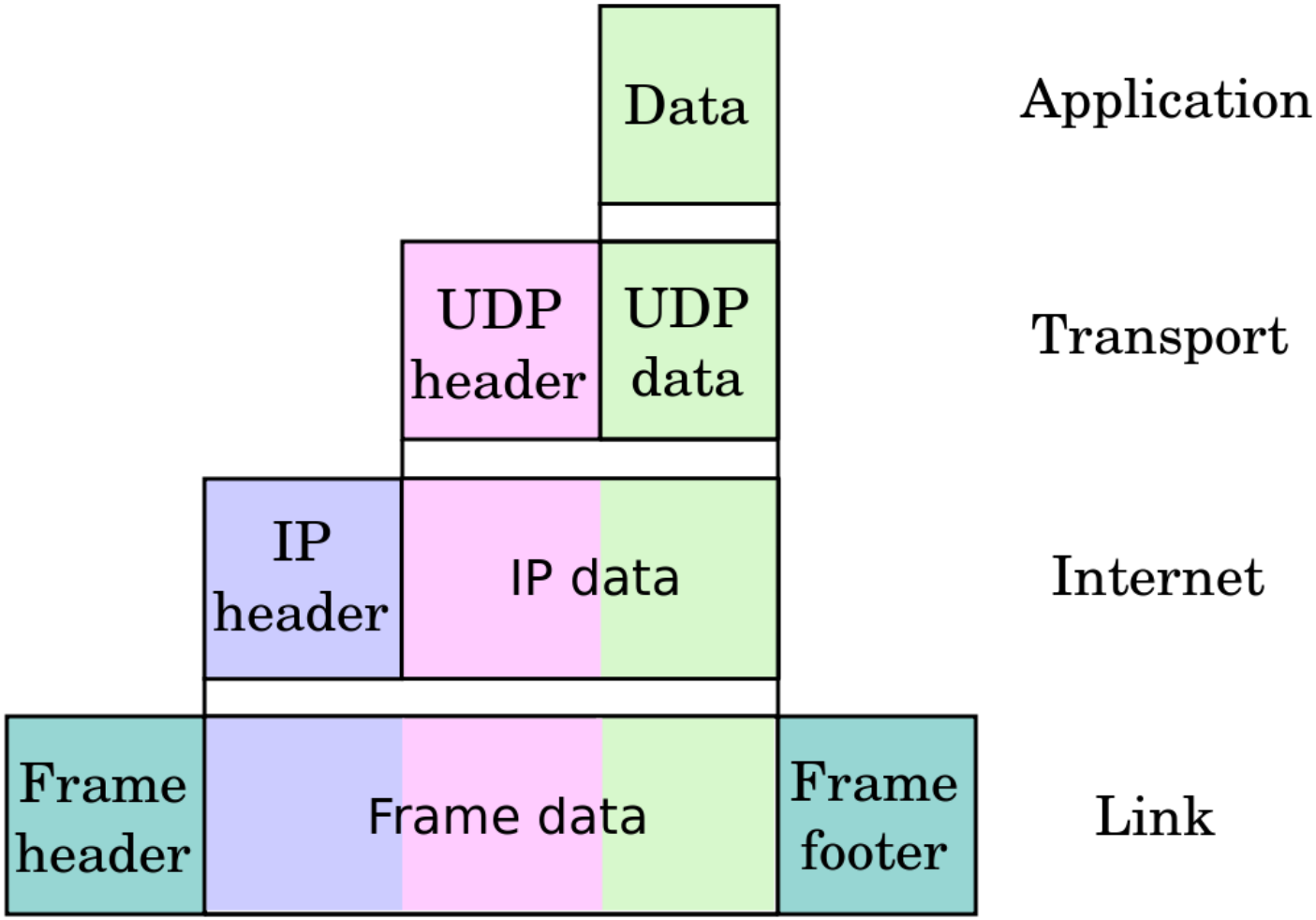
(In)security of Internet protocols

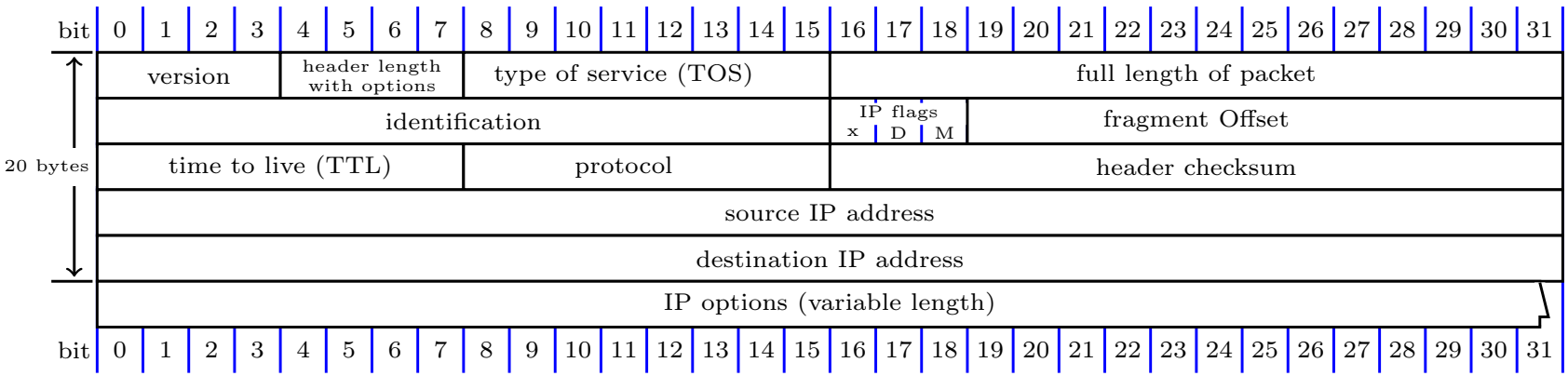
Tomáš Pevný

September 30, 2021

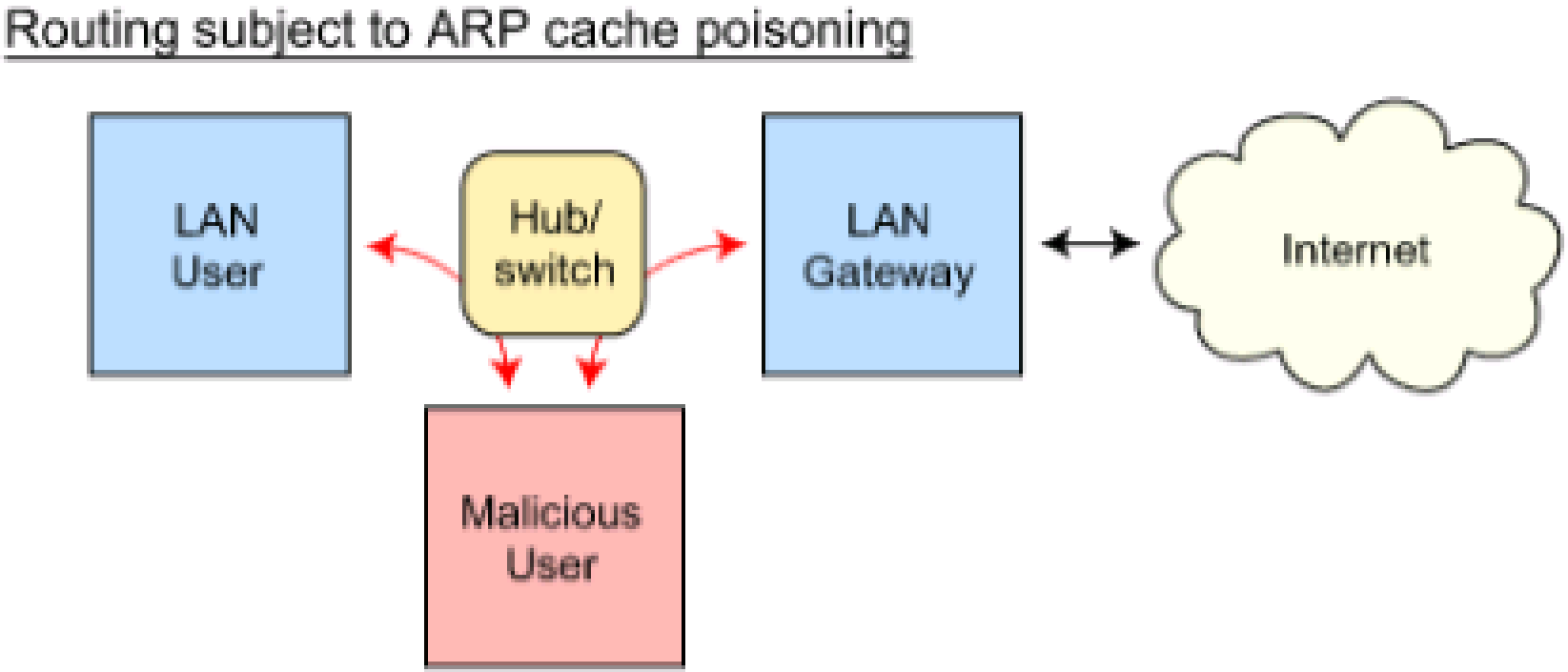
OSI layers


Data
Application
UDP header
UDP data
Transport
IP header
IP data
Internet
Frame header
Frame data
Frame footer
Link

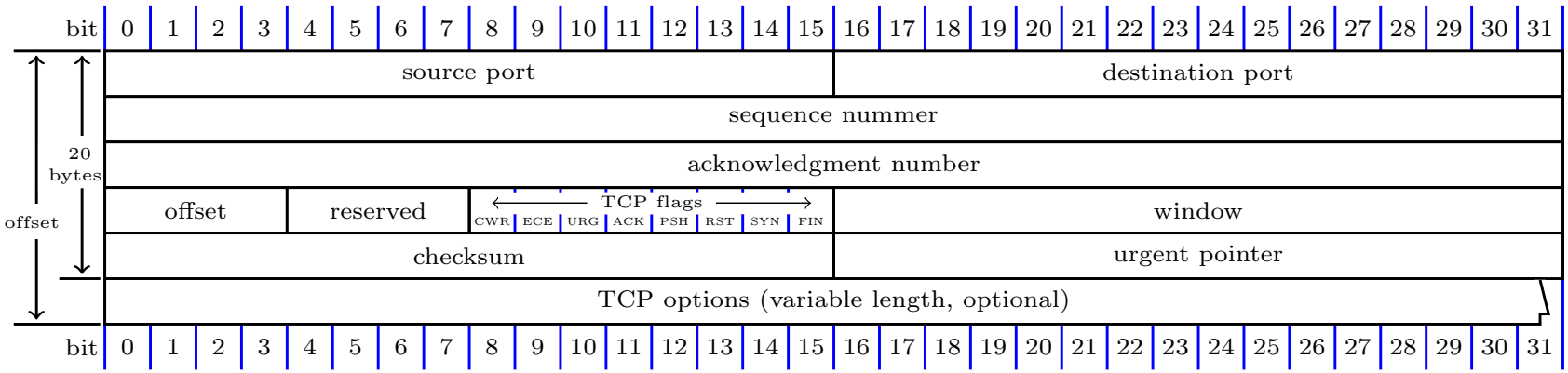
IP packet


bit
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
version
header length with options
type of service (TOS)
full length of packet
identification
IP flags
x
D
M
fragment Offset
time to live (TTL)
protocol
header checksum
source IP address
destination IP address
IP options (variable length)
20 bytes
bit
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31

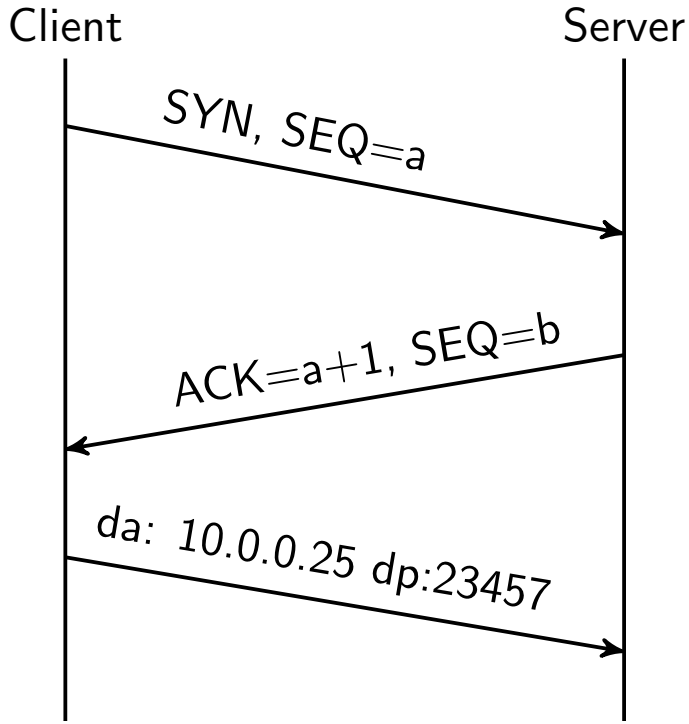
ARP spoofing



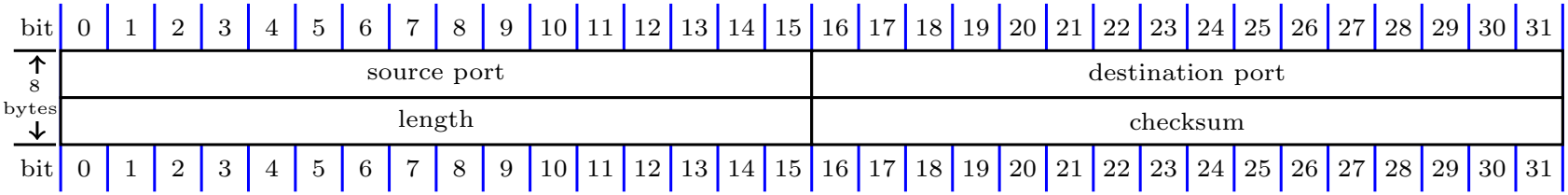
TCP packet


bit 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
source port
destination port
sequence nummer
acknowledgment number
offset
reserved
TCP flags
CWR ECE URG ACK PSH RST SYN FIN
window
checksum
urgent pointer
TCP options (variable length, optional)
20 bytes
offset
bit 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31

TCP handshake



UDP packet


bit 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
8 bytes
source port
destination port
length
checksum
bit 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31

UDP and NAT

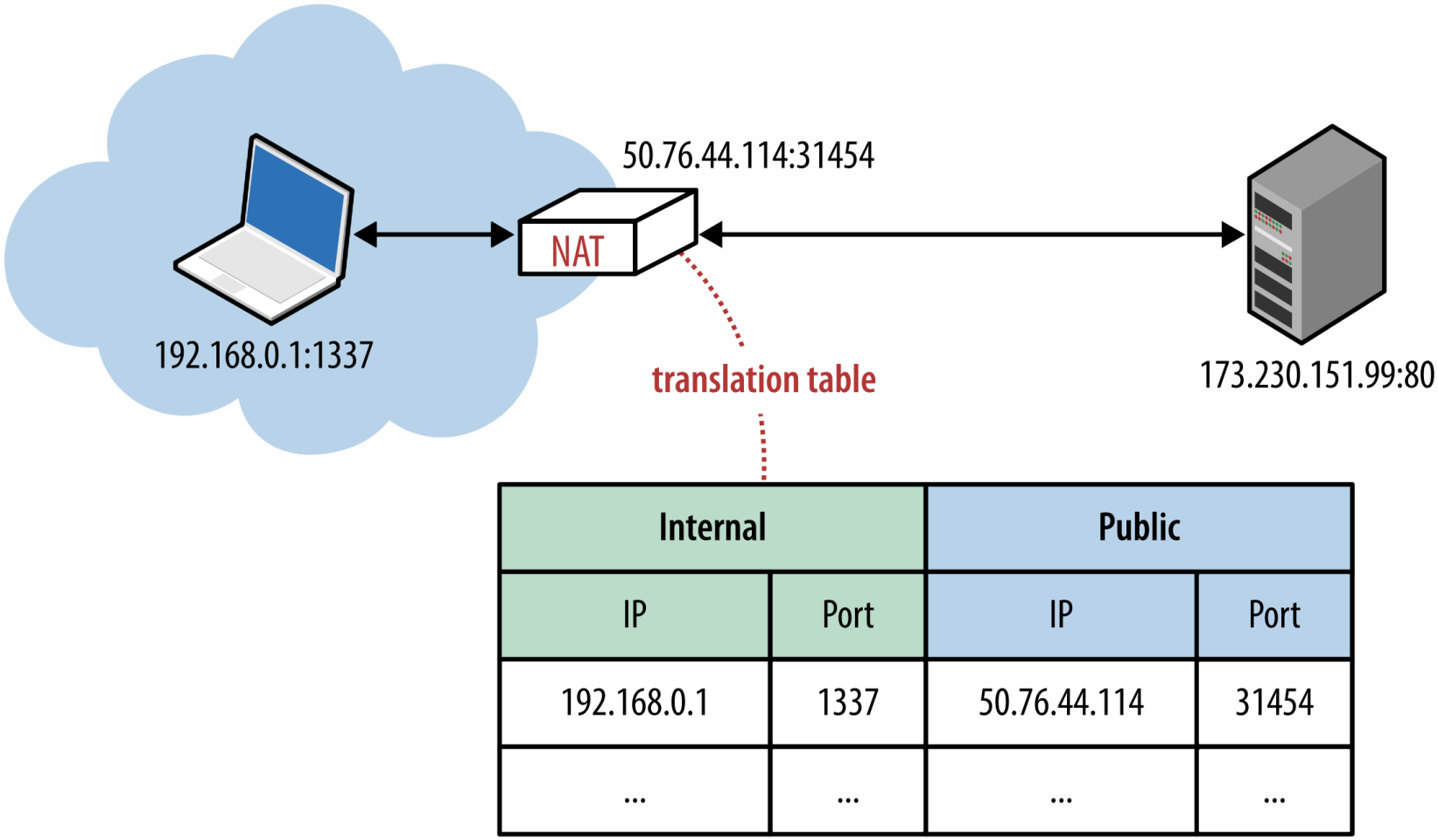


Figure 3-3. IP Network Address Translator

List of 13 DNS root servers

```
A.ROOT-SERVERS.NET.   IN   A   198.41.0.4
B.ROOT-SERVERS.NET.   IN   A   192.228.79.201
C.ROOT-SERVERS.NET.   IN   A   192.33.4.12
...
M.ROOT-SERVERS.NET.   IN   A   202.12.27.33
```

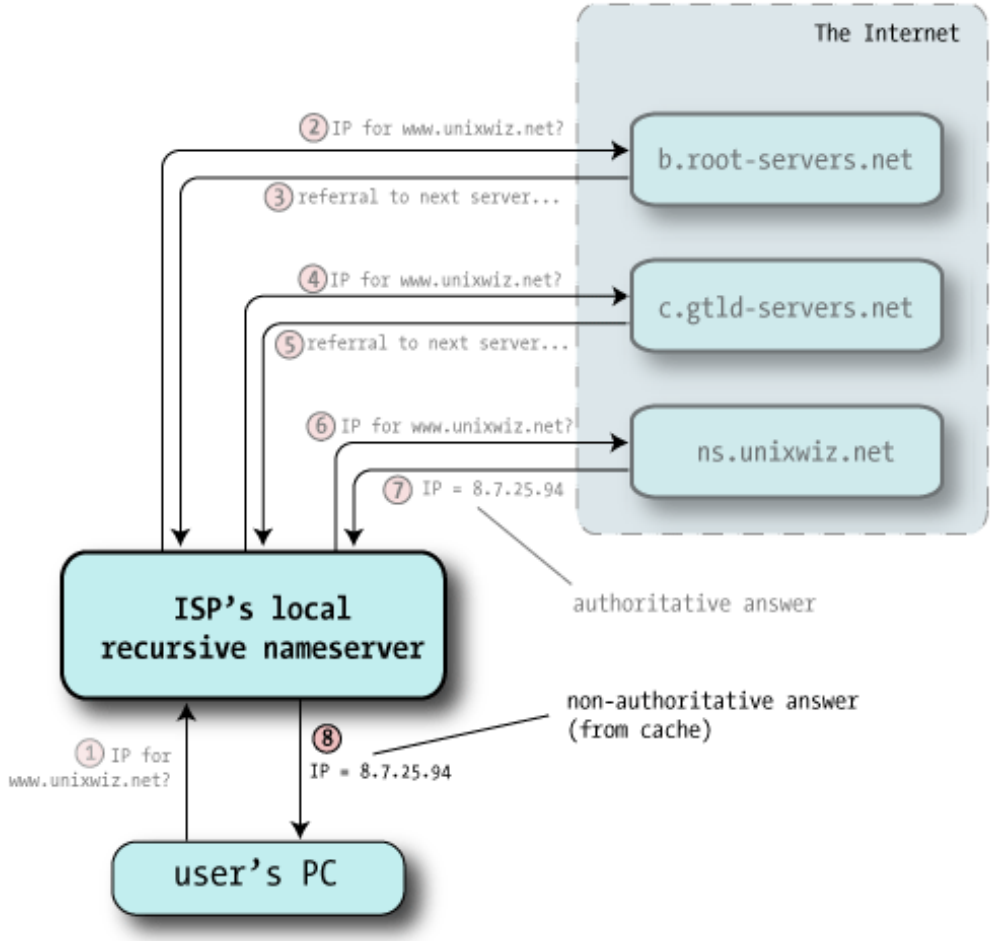
Answer of root server

```
/* Authority section */
NET.                    IN   NS A.GTLD-SERVERS.NET.
                        IN   NS B.GTLD-SERVERS.NET.
                        IN   NS C.GTLD-SERVERS.NET.
                        ...
                        IN   NS M.GTLD-SERVERS.NET.

/* Additional section - "glue" records */
A.GTLD-SERVERS.net.   IN   A   192.5.6.30
B.GTLD-SERVERS.net.   IN   A   192.33.14.30
C.GTLD-SERVERS.net.   IN   A   192.26.92.30
...
M.GTLD-SERVERS.net.   IN   A   192.55.83.30
```

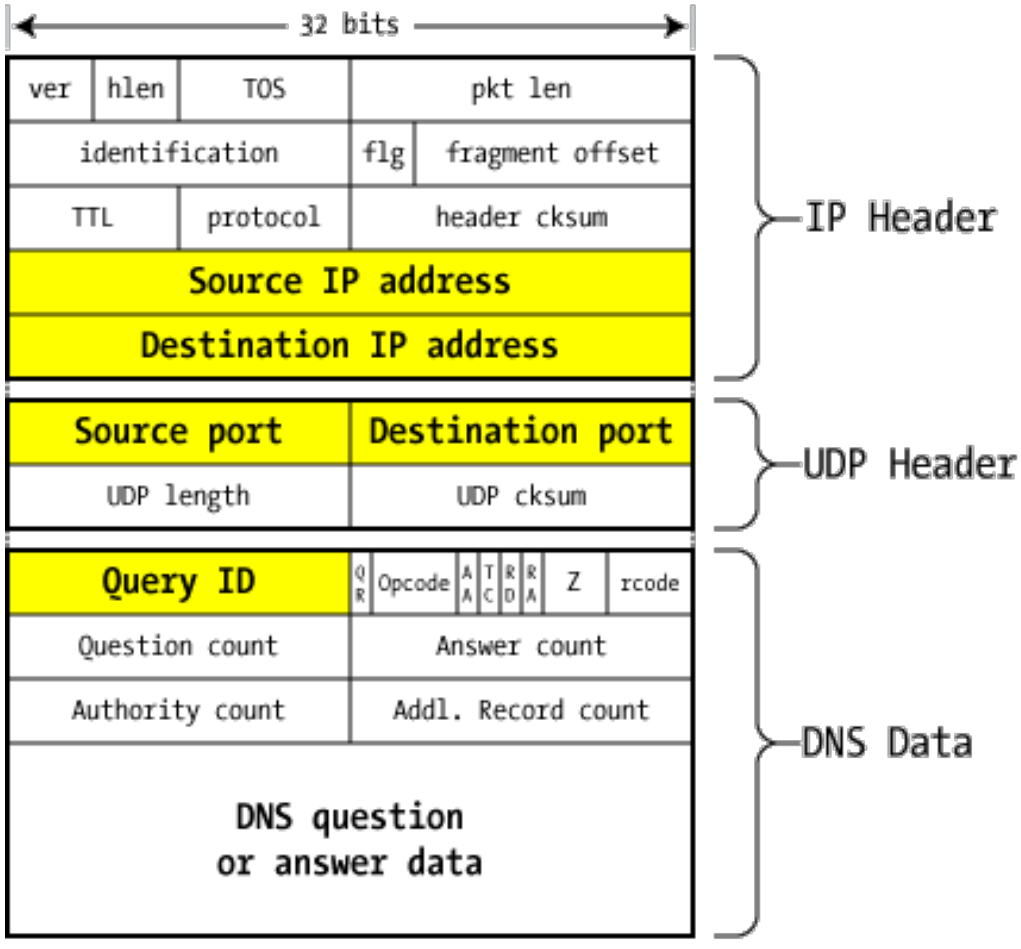
Answer of .net authoritative server

```
/* Authority section */
unixwiz.net.          IN  NS cs.unixwiz.net.
                      IN  NS linux.unixwiz.net.

/* Additional section - "glue" records */
cs.unixwiz.net.       IN  A  8.7.25.94
linux.unixwiz.net.    IN  A  64.170.162.98
```

The full picture of DNS resolution

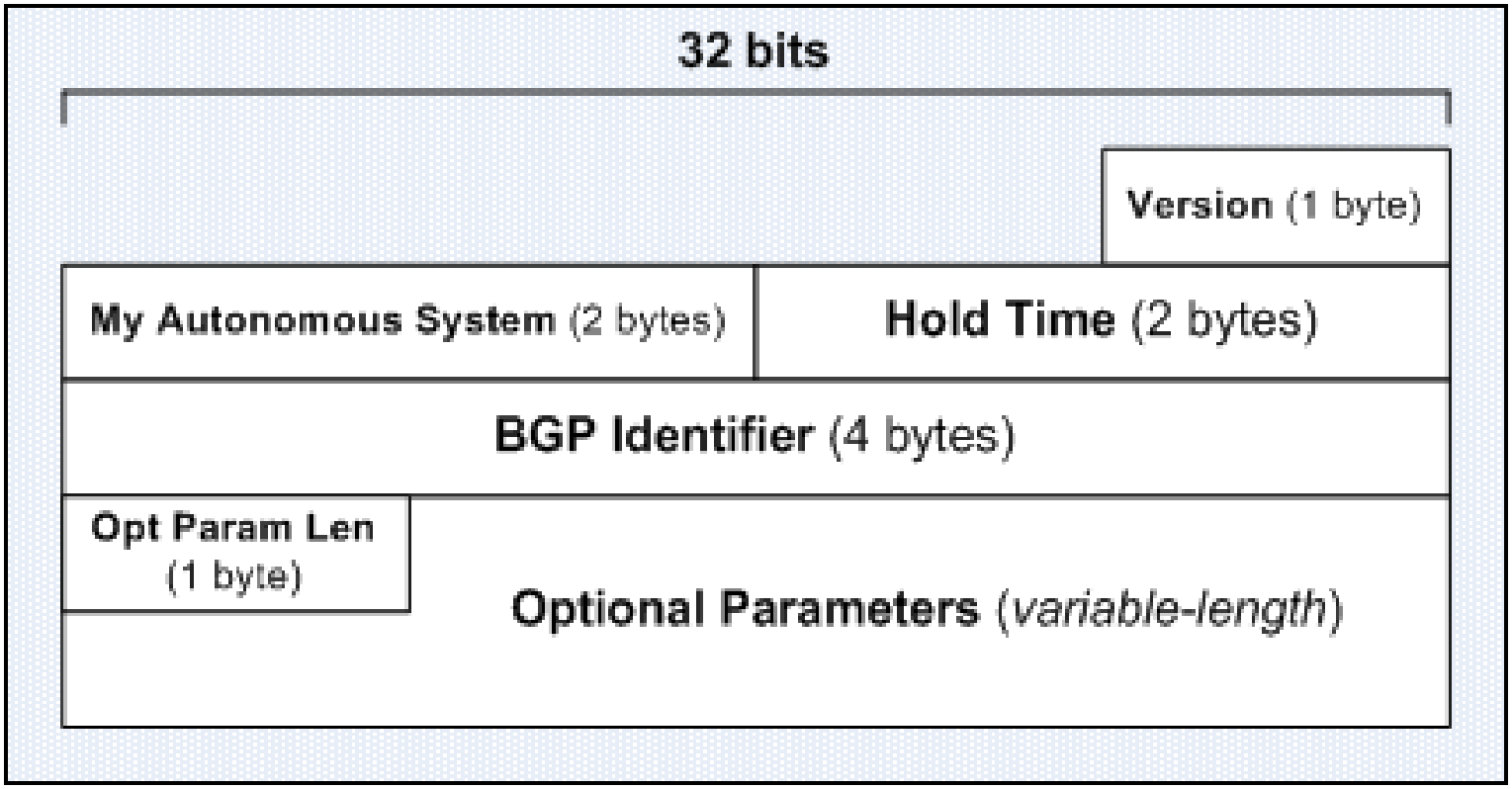


Schema DNS query request

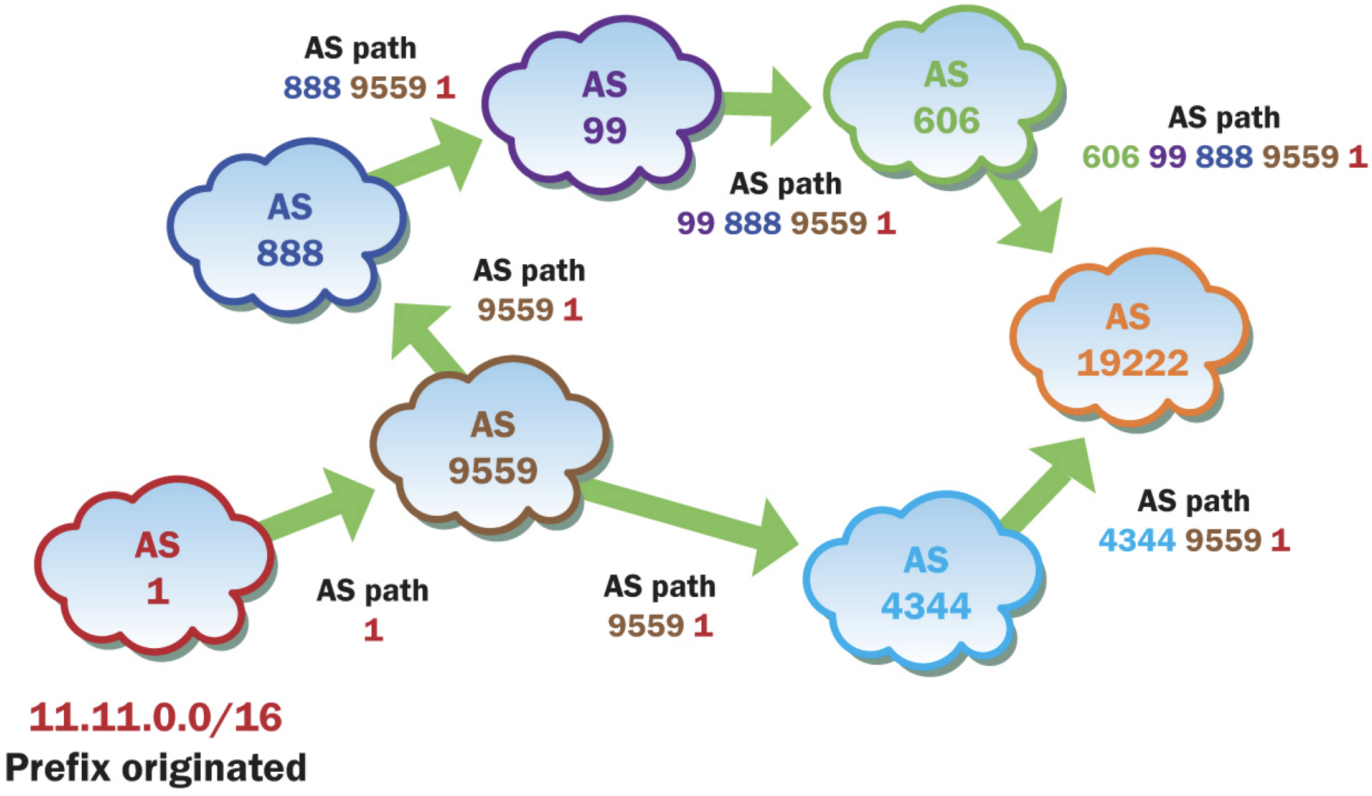


DNS packet on the wire

BGP open request



BGP propagation



Youtube takedown order

Pakistan Govt. Notice

Corrigendum- Most Urgent

GOVERNMENT OF PAKISTAN
PAKISTAN TELECOMMUNICATION AUTHORITY
ZONAL OFFICE PESHAWAR
Plot-11, Sector A-3, Phase-V, Hayatabad, Peshawar.
Ph: 091-9217279- 5829177 Fax: 091-9217254
www.pta.gov.pk

NWFP-33-16 (BW)/06/PTA February ,2008

Subject: **Blocking of Offensive Website**

Reference: This office letter of even number dated 22.02.2008.

I am directed to request all ISPs to immediately block access to the following website

URL: http://www.youtube.com/watch?v=o3s8jtvvg00

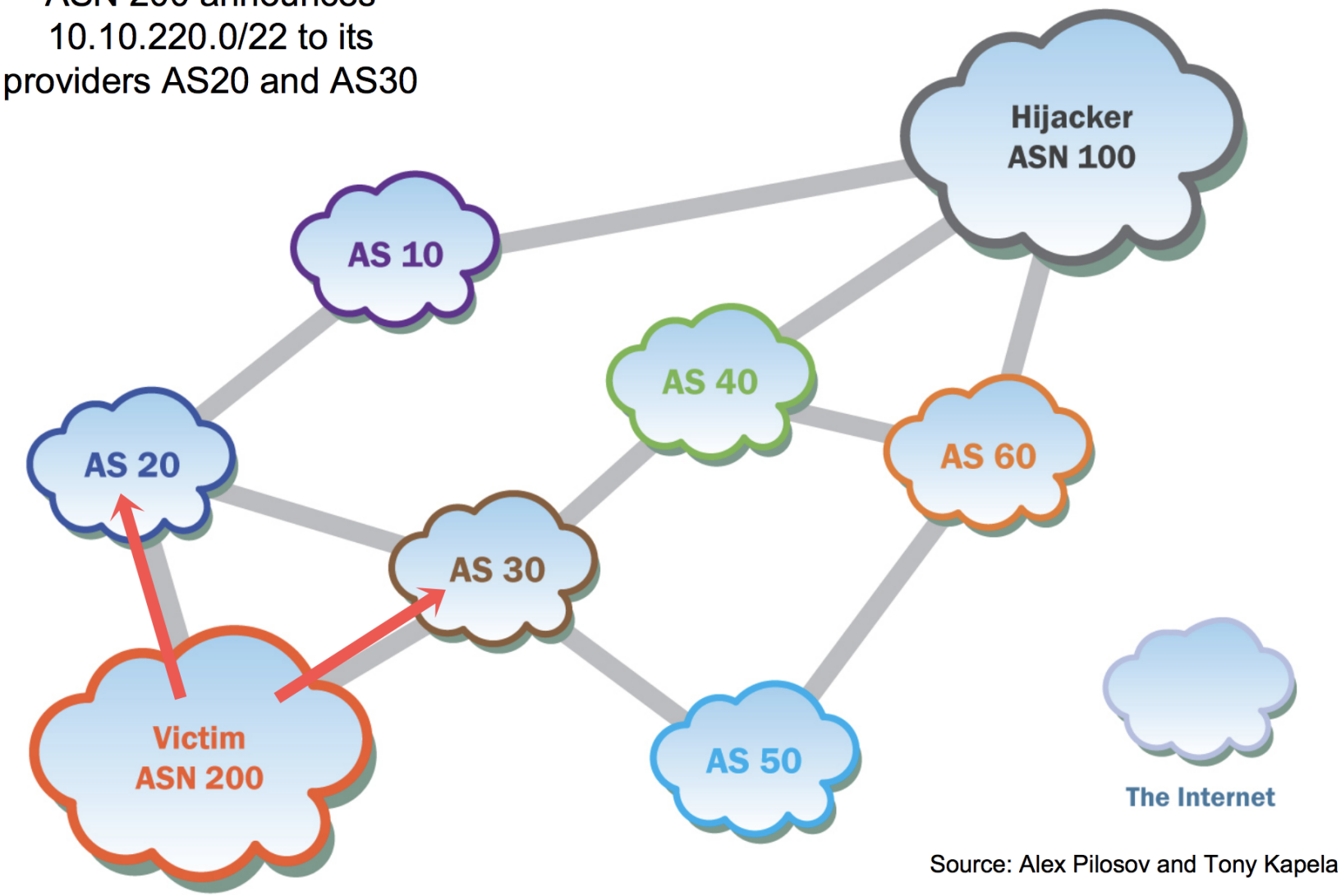
IPs: 208.65.153.238, 208.65.153.253, 208.65.153.251

Compliance report should reach this office through return fax or at email peshawar@pta.gov.pk today please.

Hijacking routes

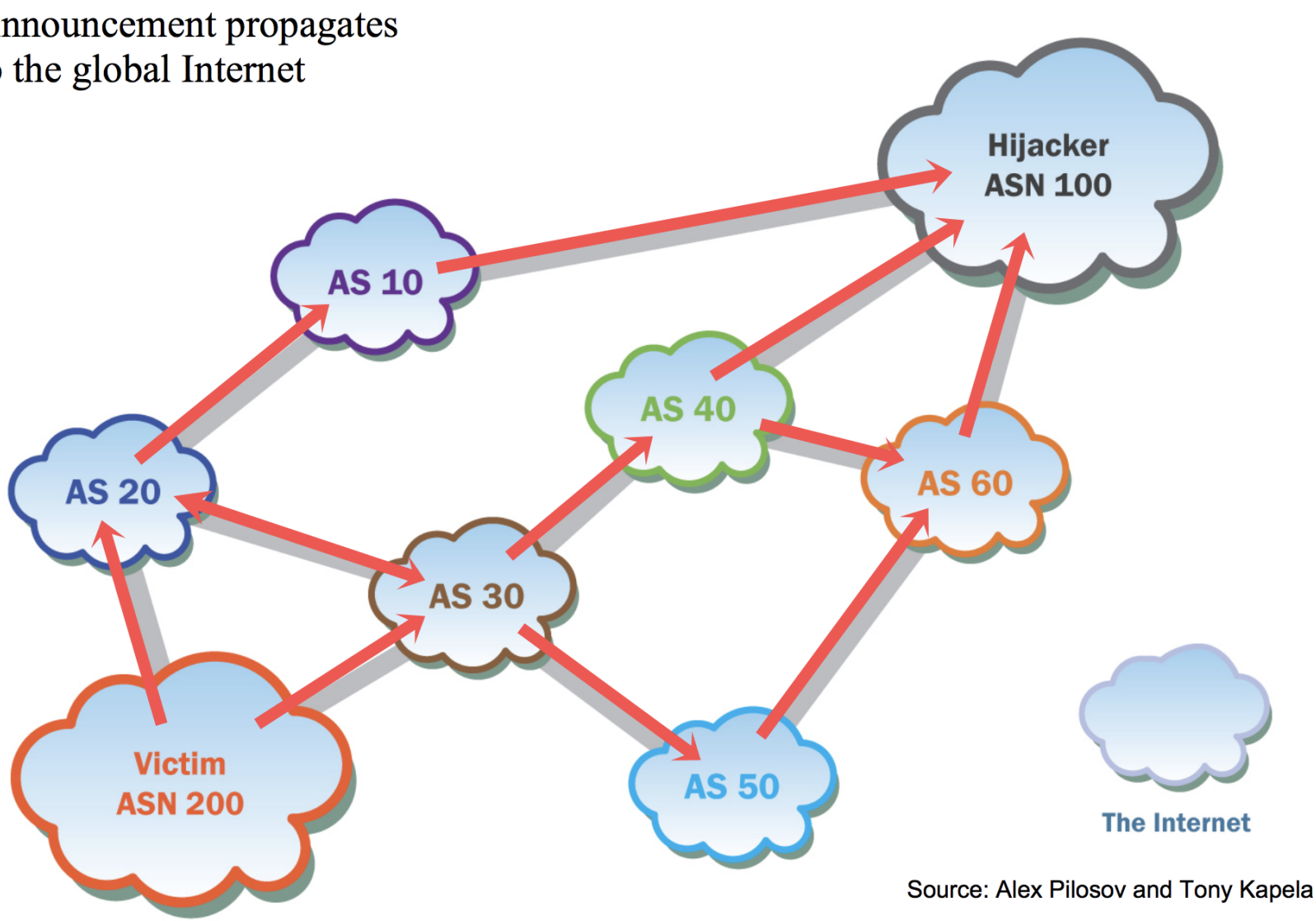
Hijacking routes

BGP hijacking



Source: Alex Pilosov and Tony Kapela

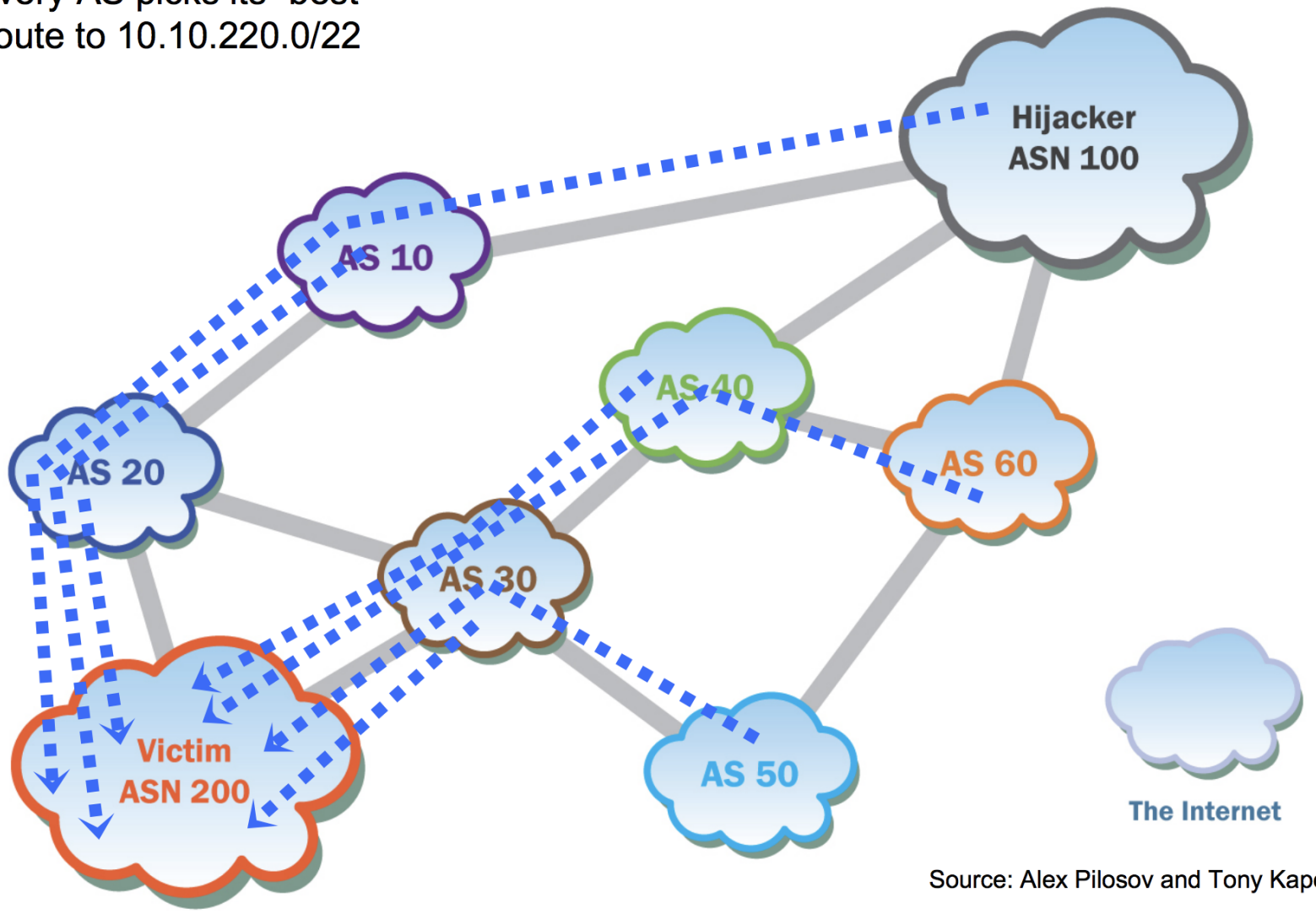
BGP hijacking



Source: Alex Pilosov and Tony Kapela

BGP hijacking

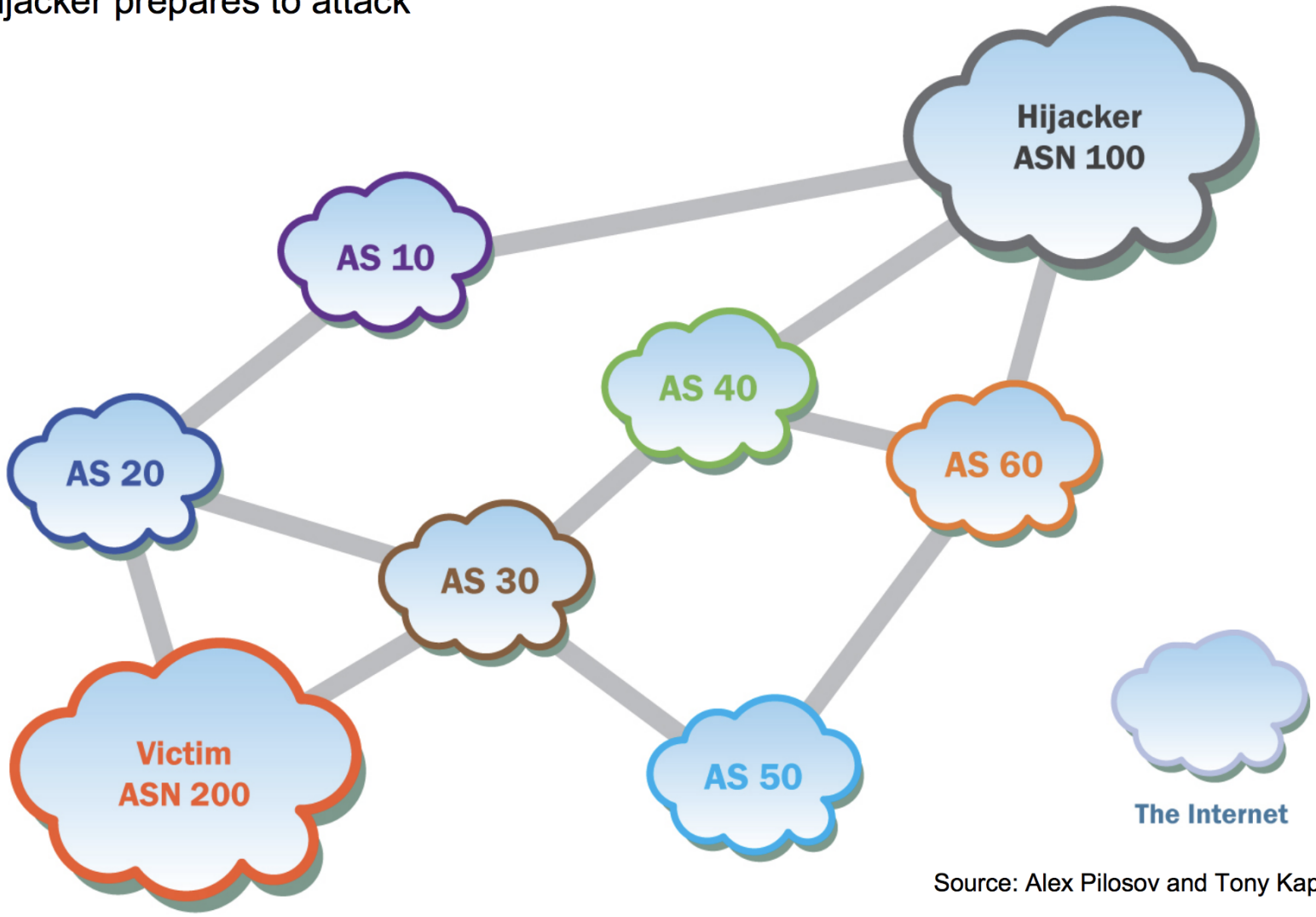
Every AS picks its “best” route to 10.10.220.0/22



Source: Alex Pilosov and Tony Kapela

BGP hijacking

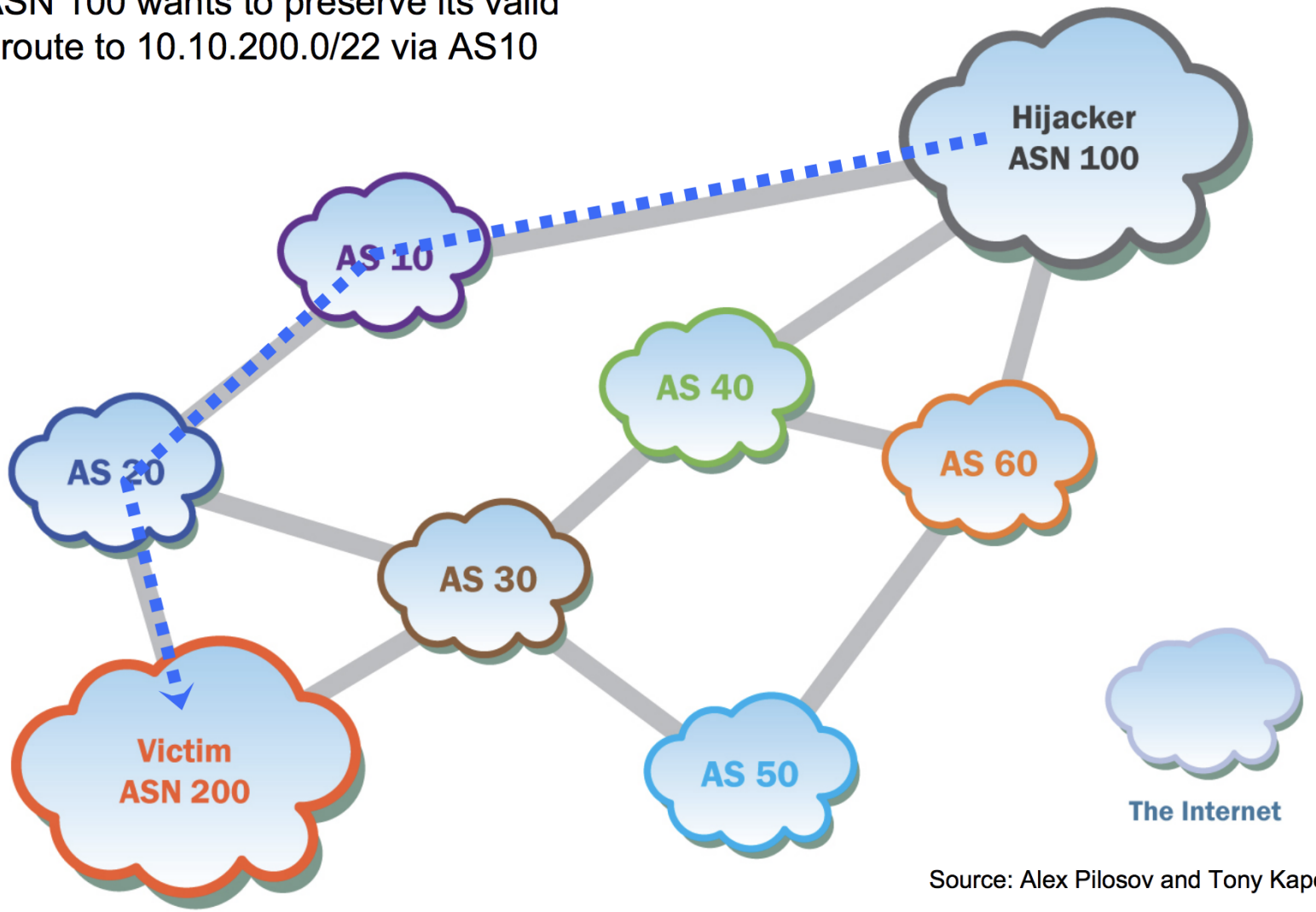
Hijacker prepares to attack



Source: Alex Pilosov and Tony Kapela

BGP hijacking

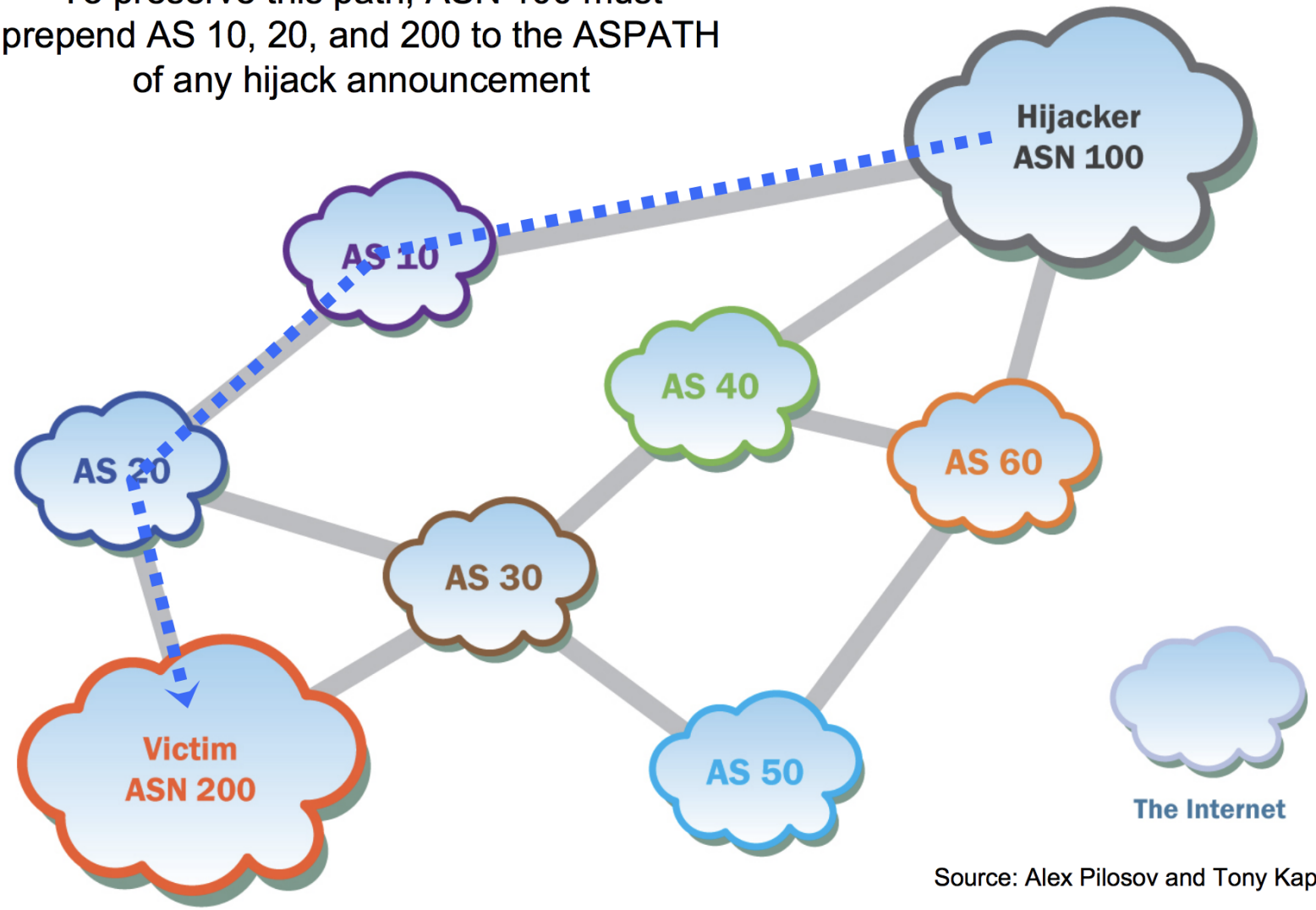
ASN 100 wants to preserve its valid route to 10.10.200.0/22 via AS10



Source: Alex Pilosov and Tony Kapela

BGP hijacking

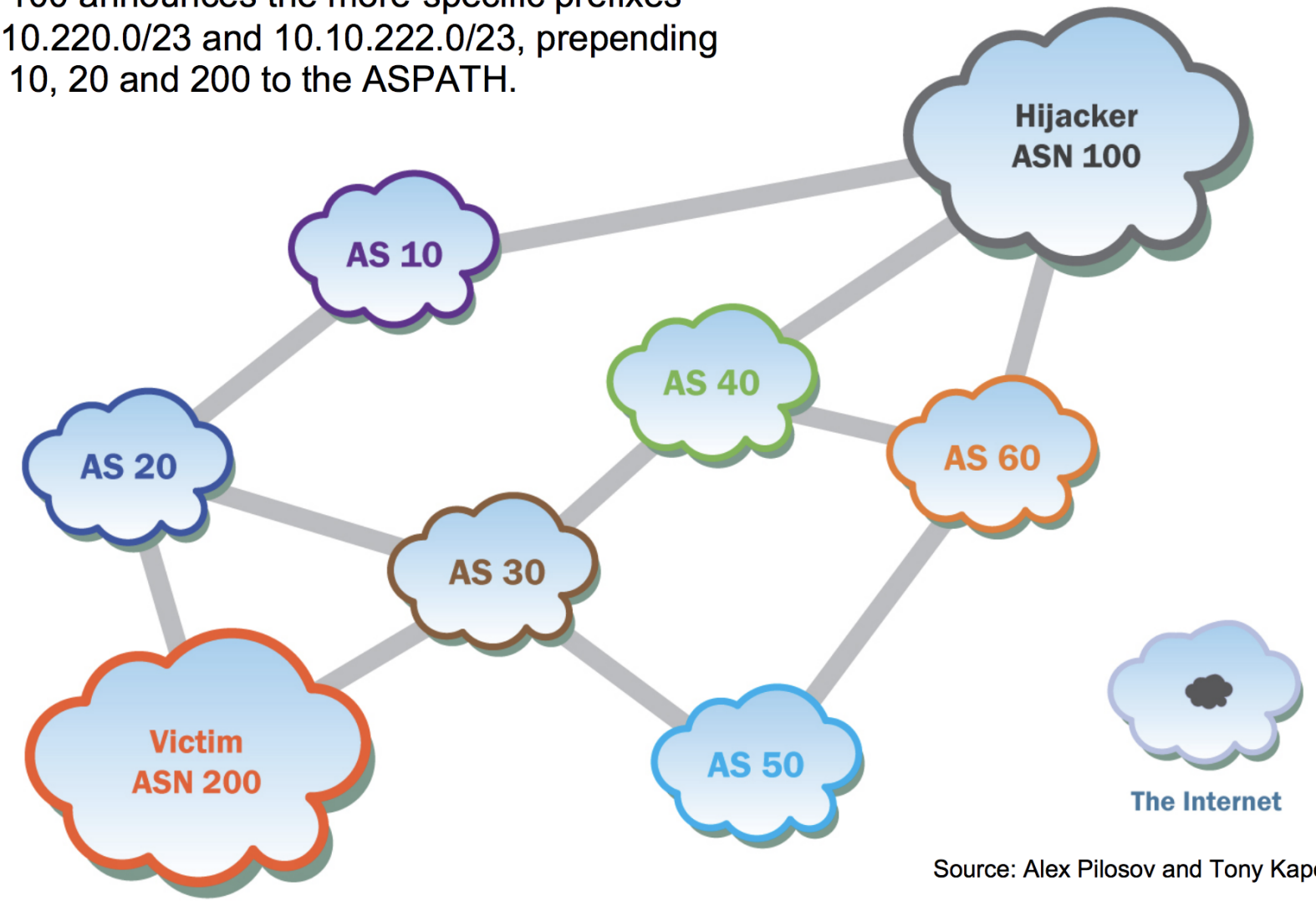
To preserve this path, ASN 100 must prepend AS 10, 20, and 200 to the ASPATH of any hijack announcement



Source: Alex Pilosov and Tony Kapela

BGP hijacking

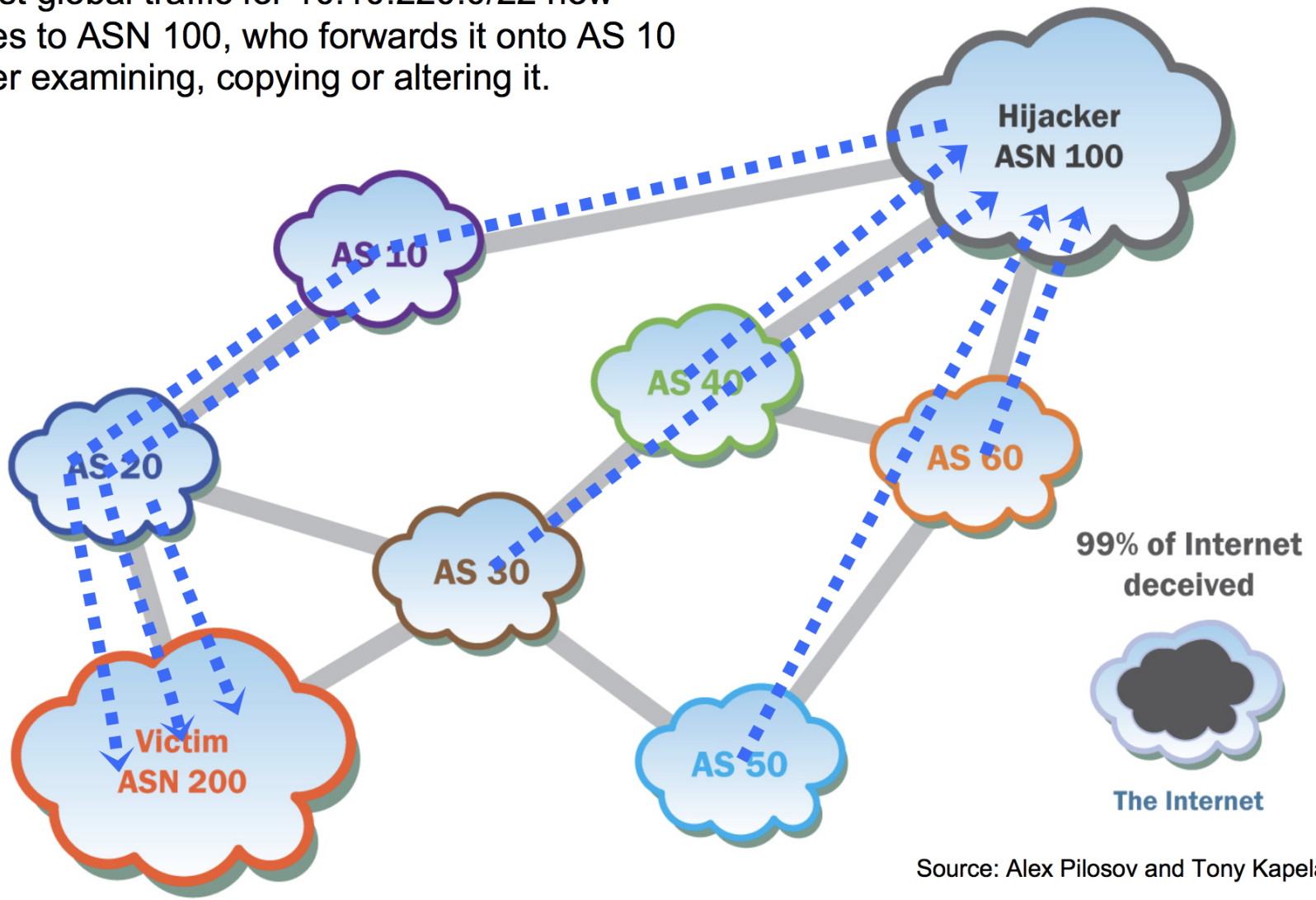
AS 100 announces the more-specific prefixes 10.10.220.0/23 and 10.10.222.0/23, prepending AS 10, 20 and 200 to the ASPATH.



Source: Alex Pilosov and Tony Kapela

BGP hijacking

Most global traffic for 10.10.220.0/22 now goes to ASN 100, who forwards it onto AS 10 after examining, copying or altering it.



Source: Alex Pilosov and Tony Kapela