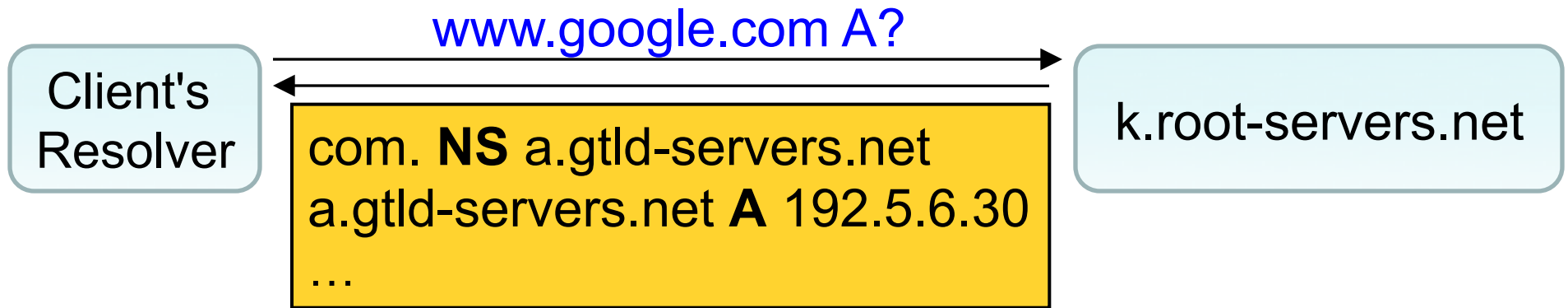
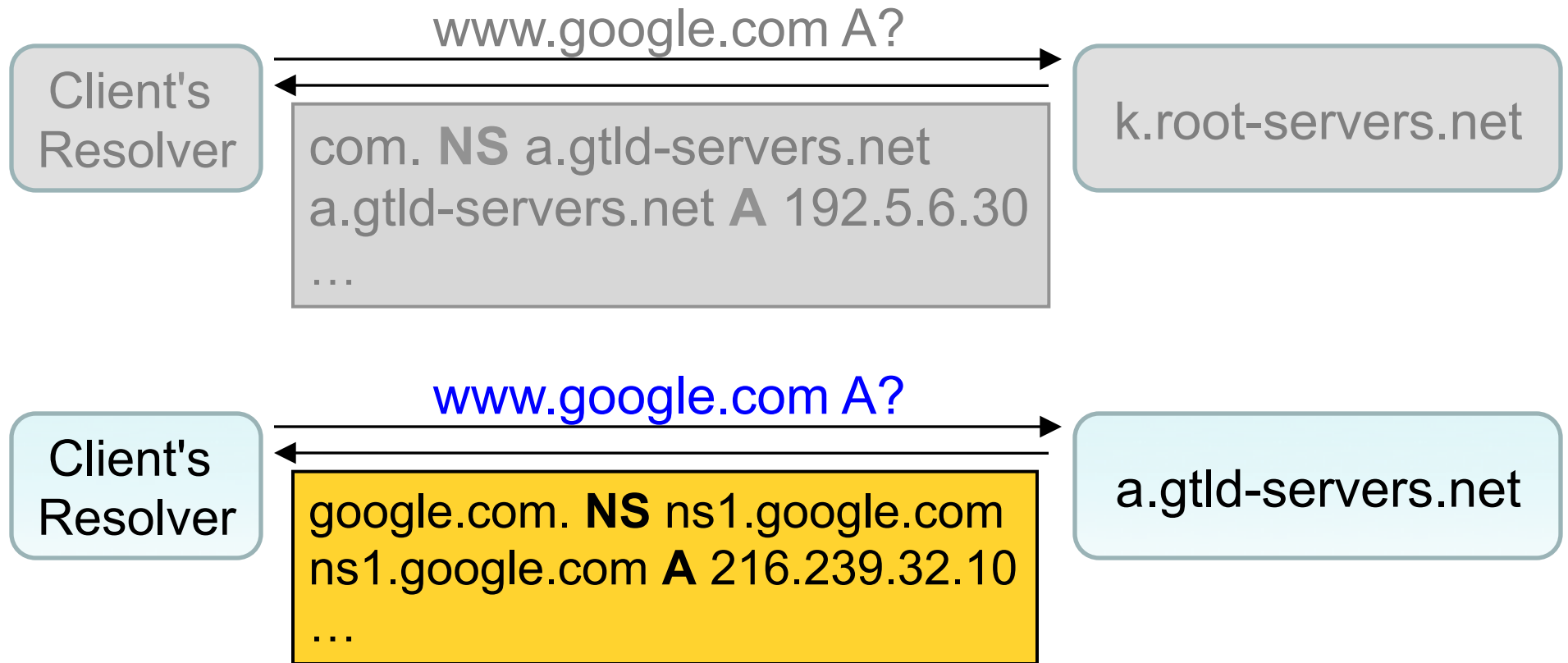


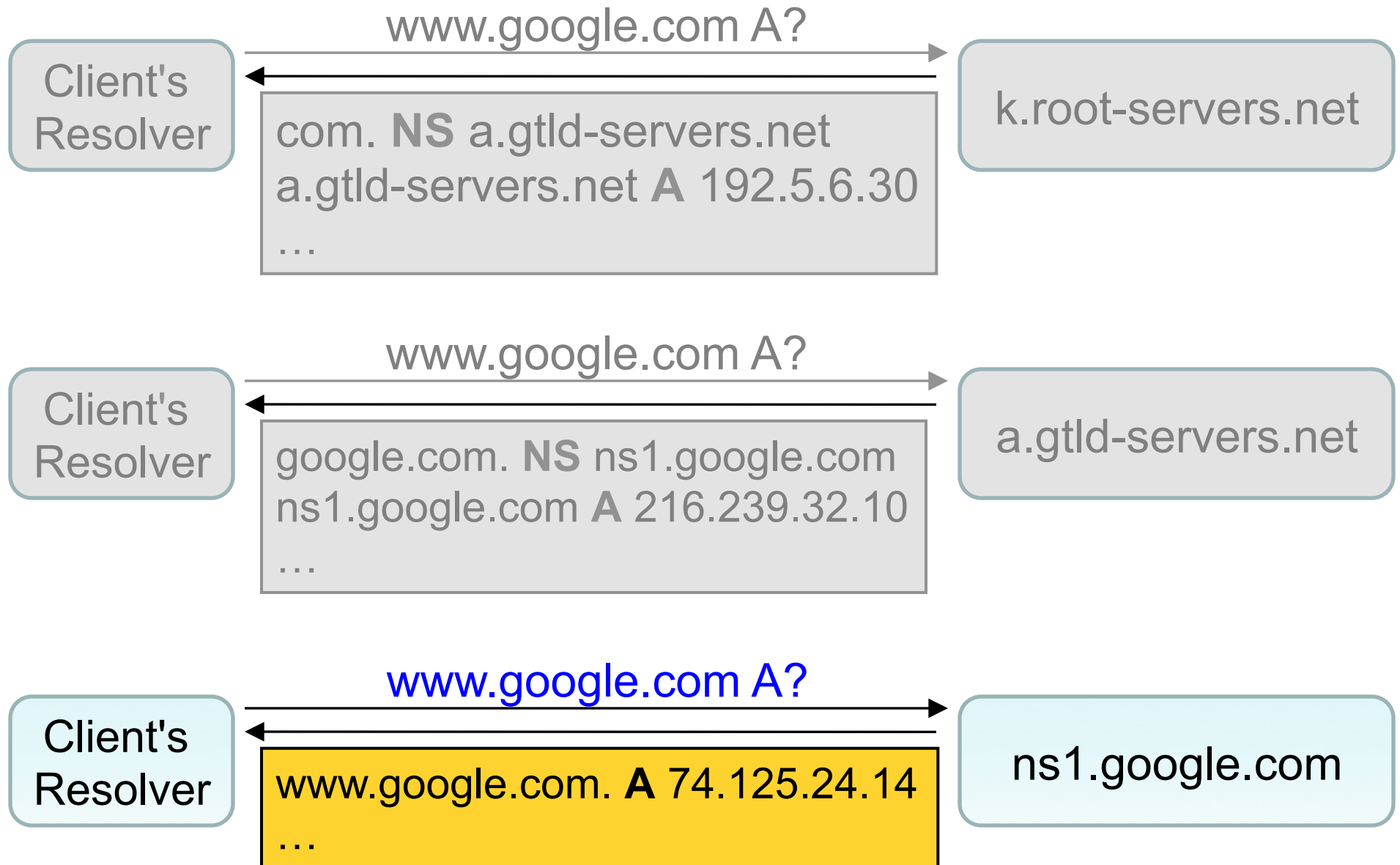
Ordinary DNS:



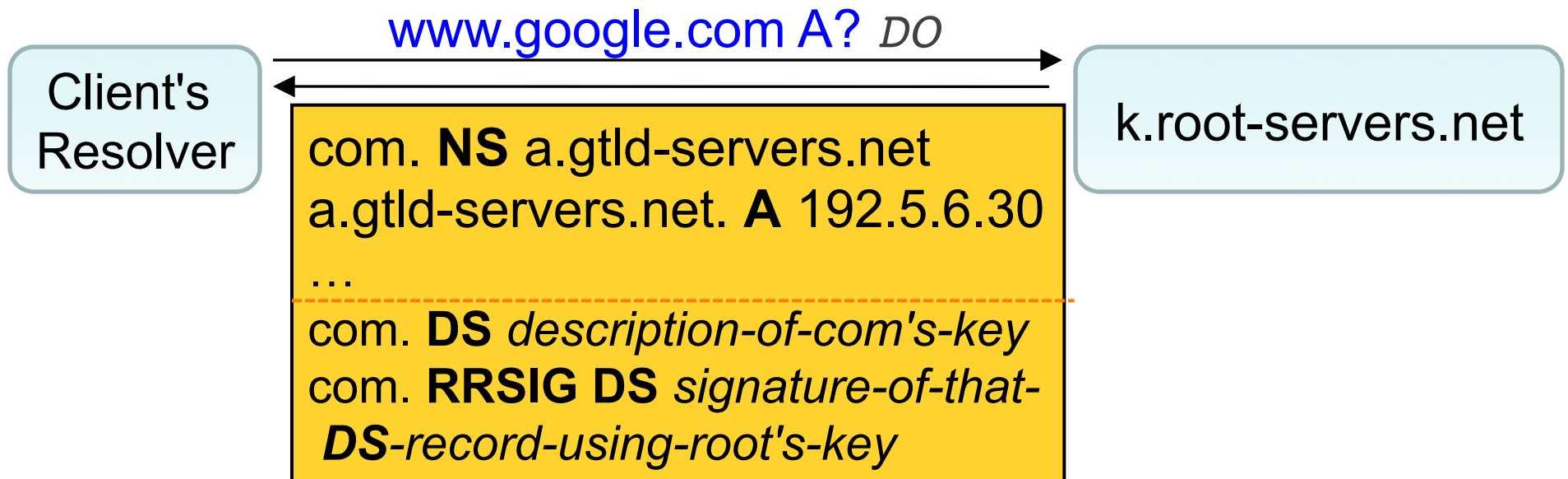
Ordinary DNS:



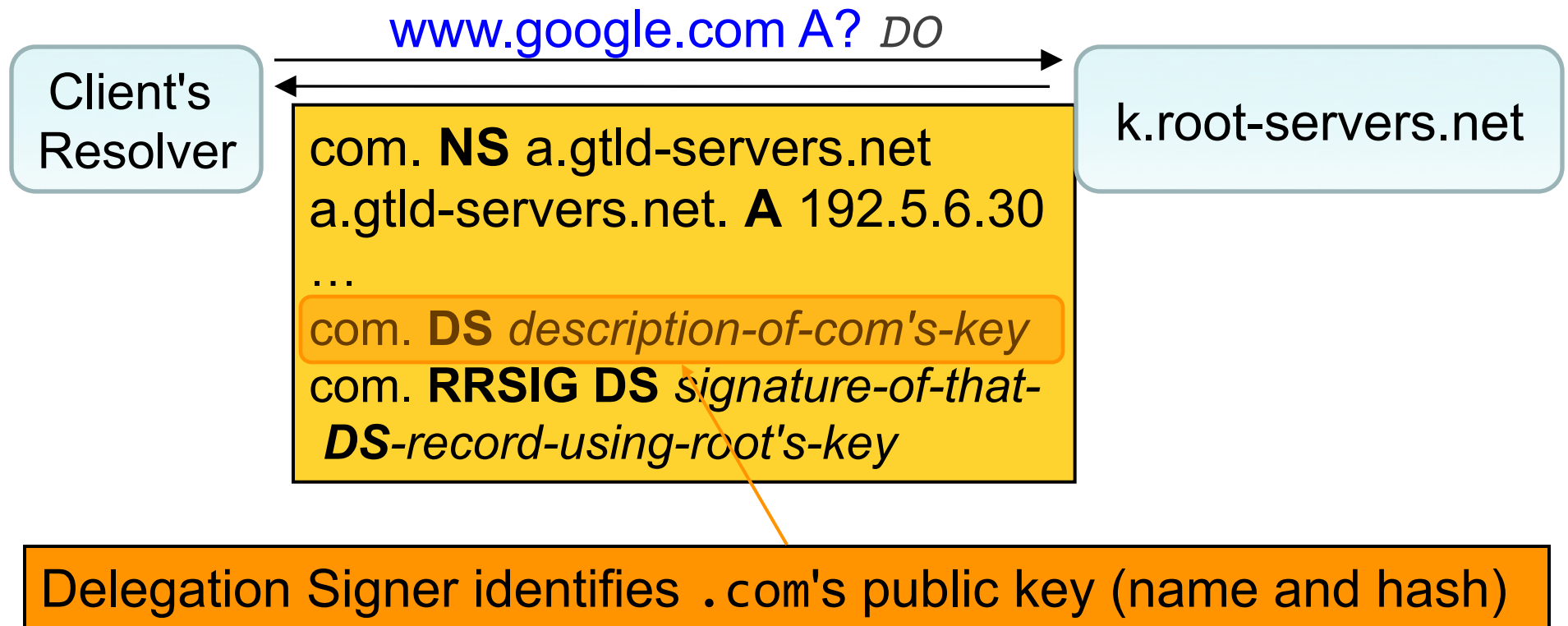
Ordinary DNS:



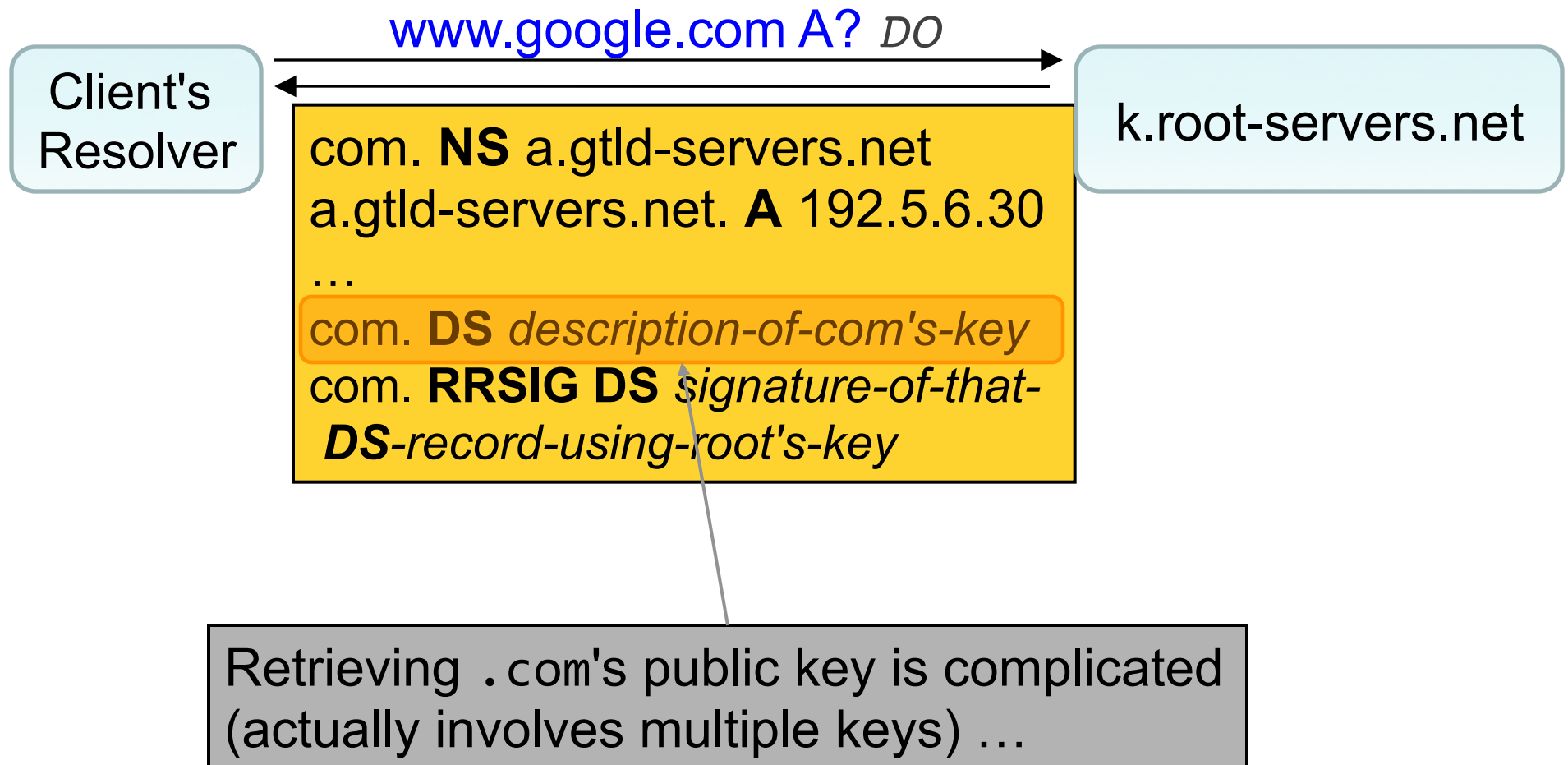
DNSSEC (with simplifications):



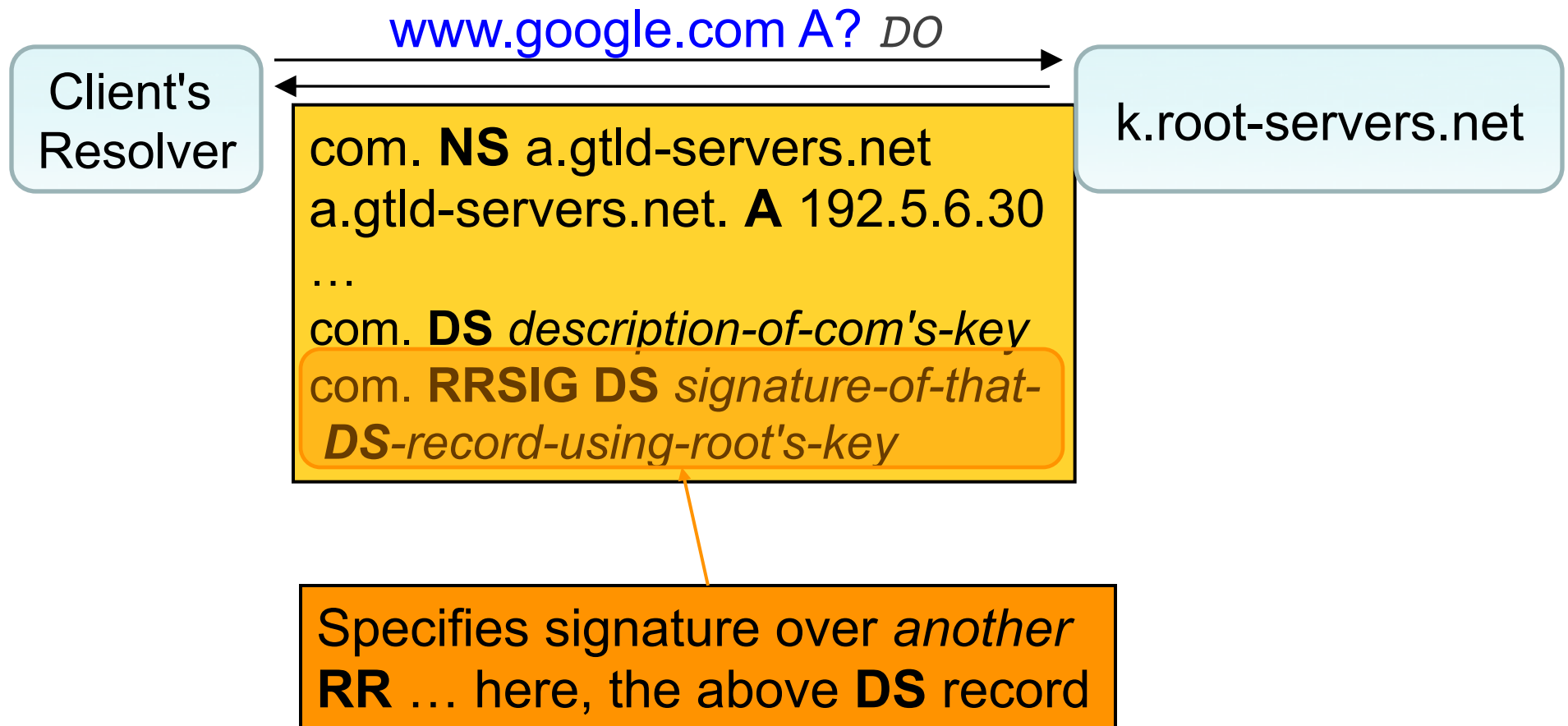
DNSSEC (with simplifications):



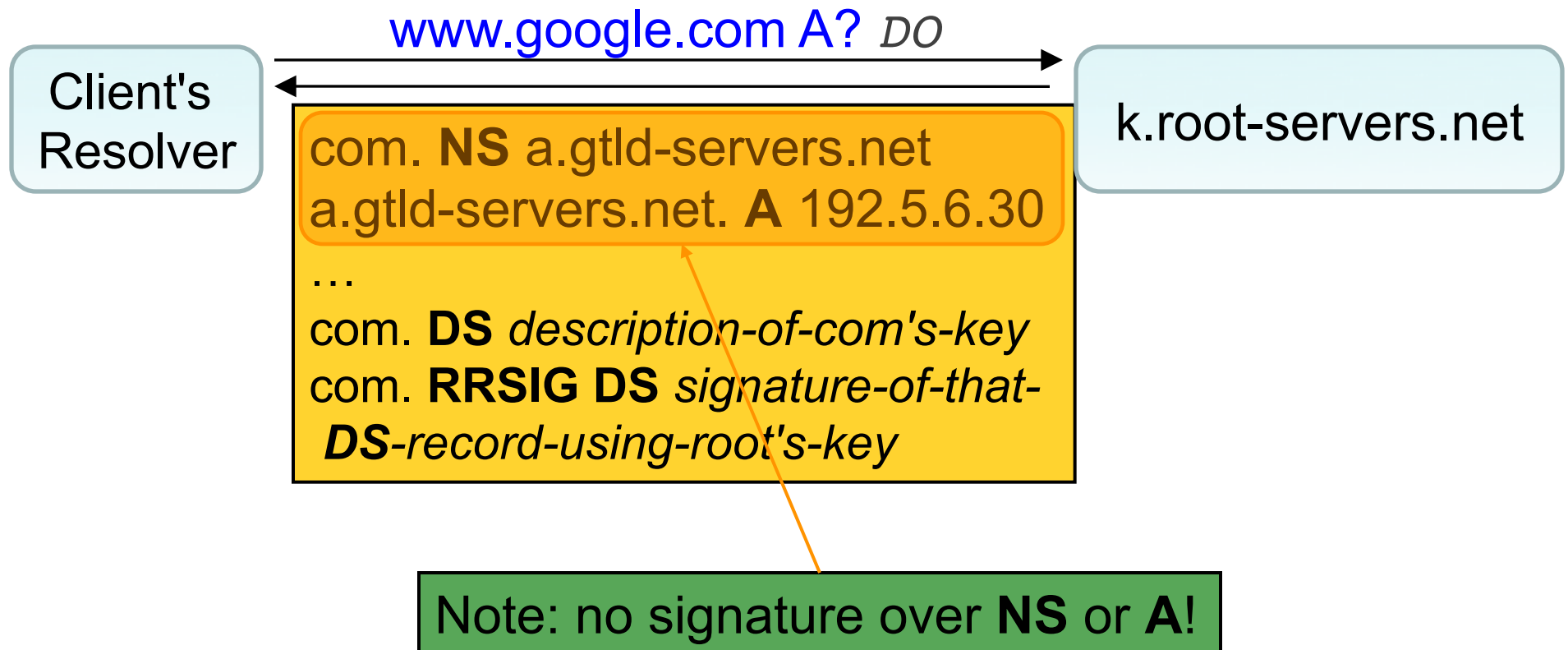
DNSSEC (with simplifications):



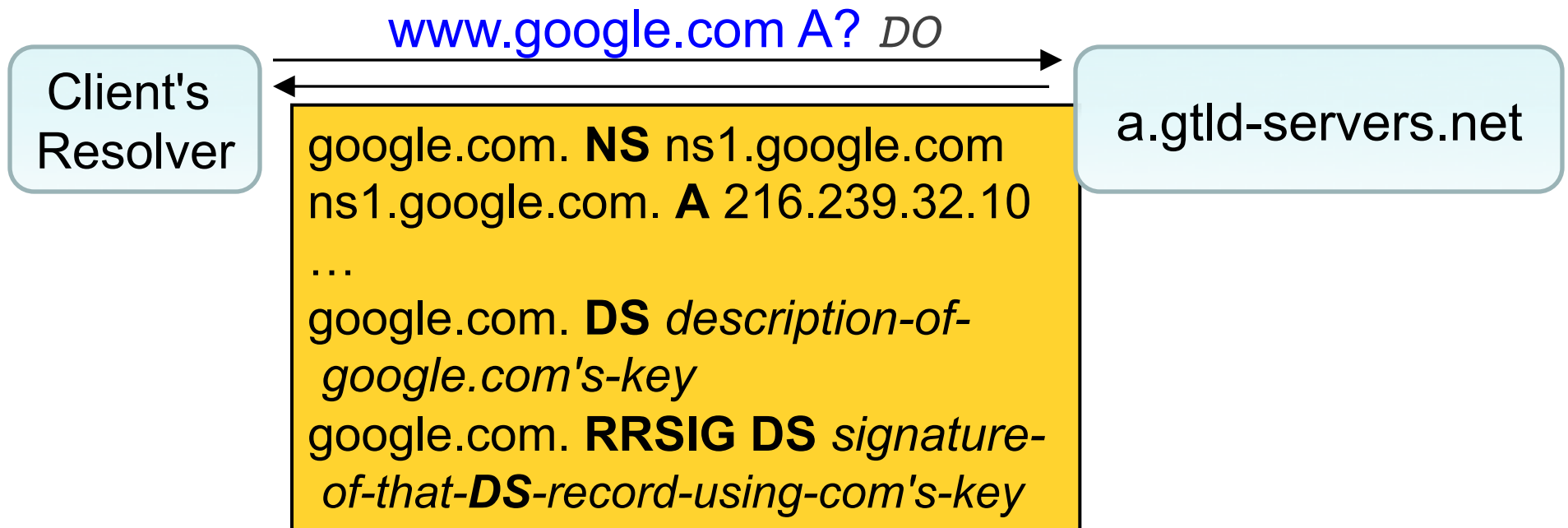
DNSSEC (with simplifications):



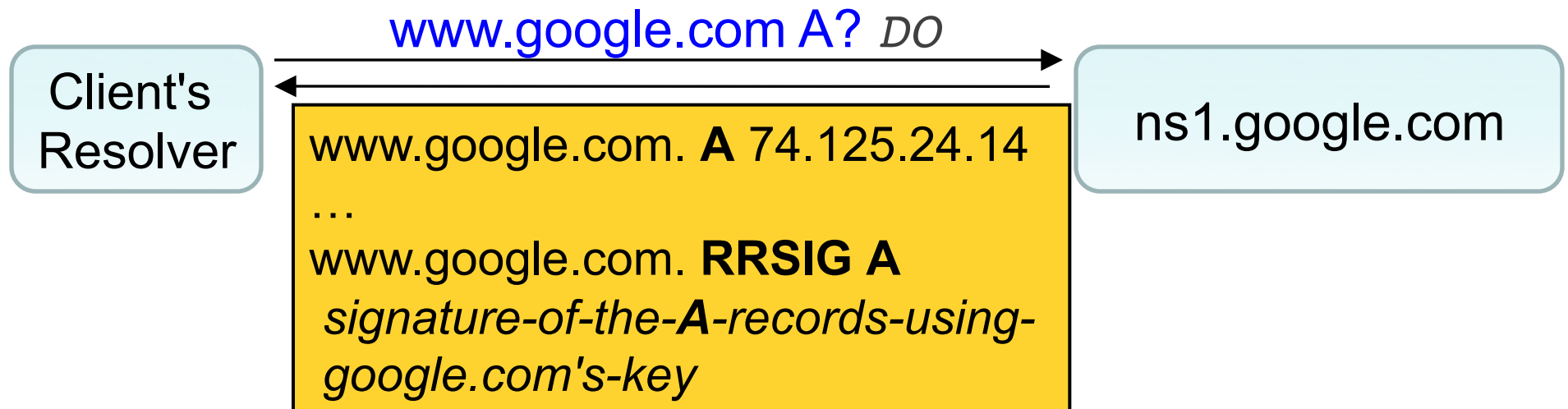
DNSSEC (with simplifications):



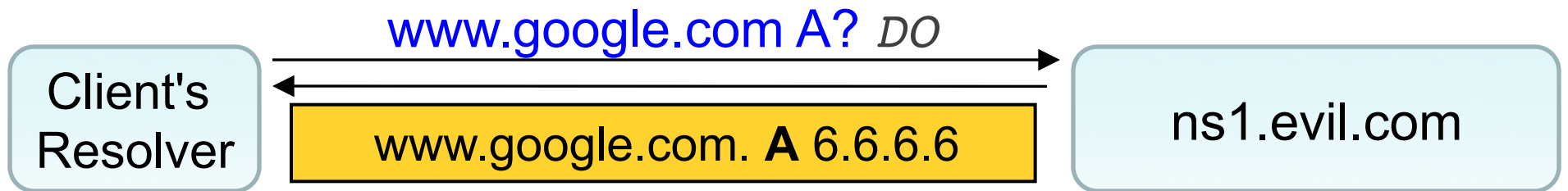
DNSSEC (with simplifications):



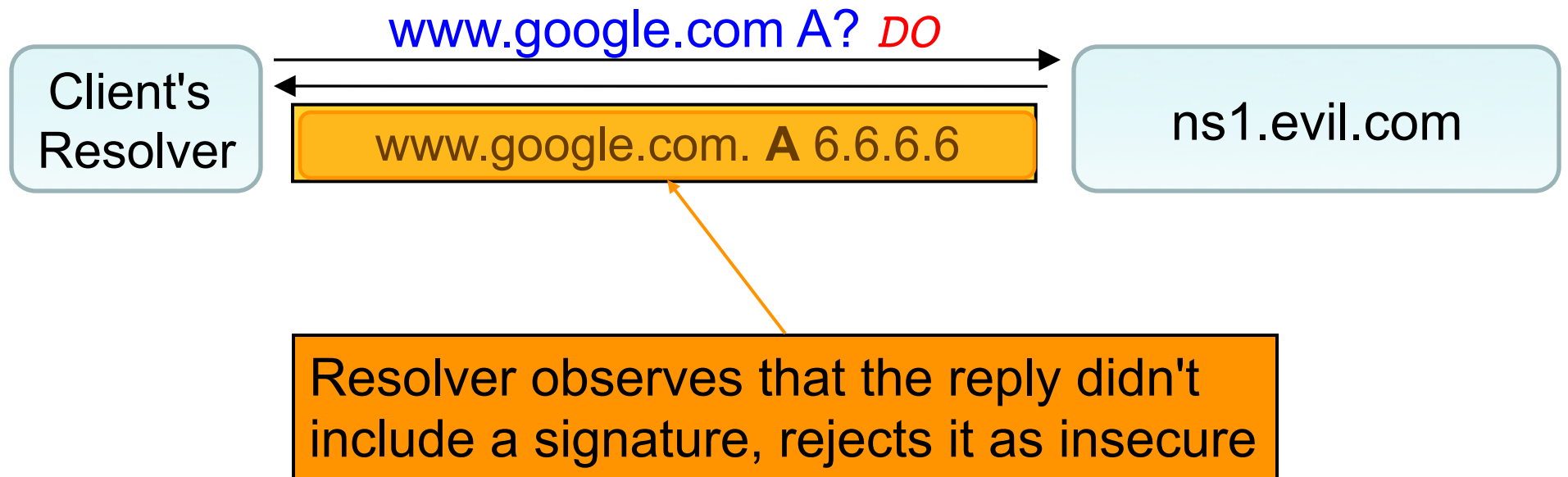
DNSSEC (with simplifications):



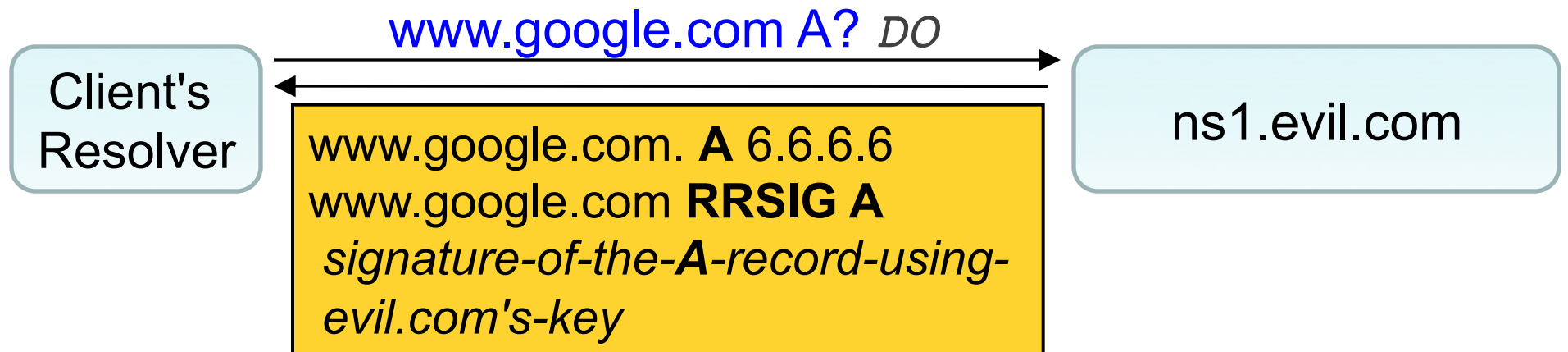
DNSSEC - Mallory attacks!



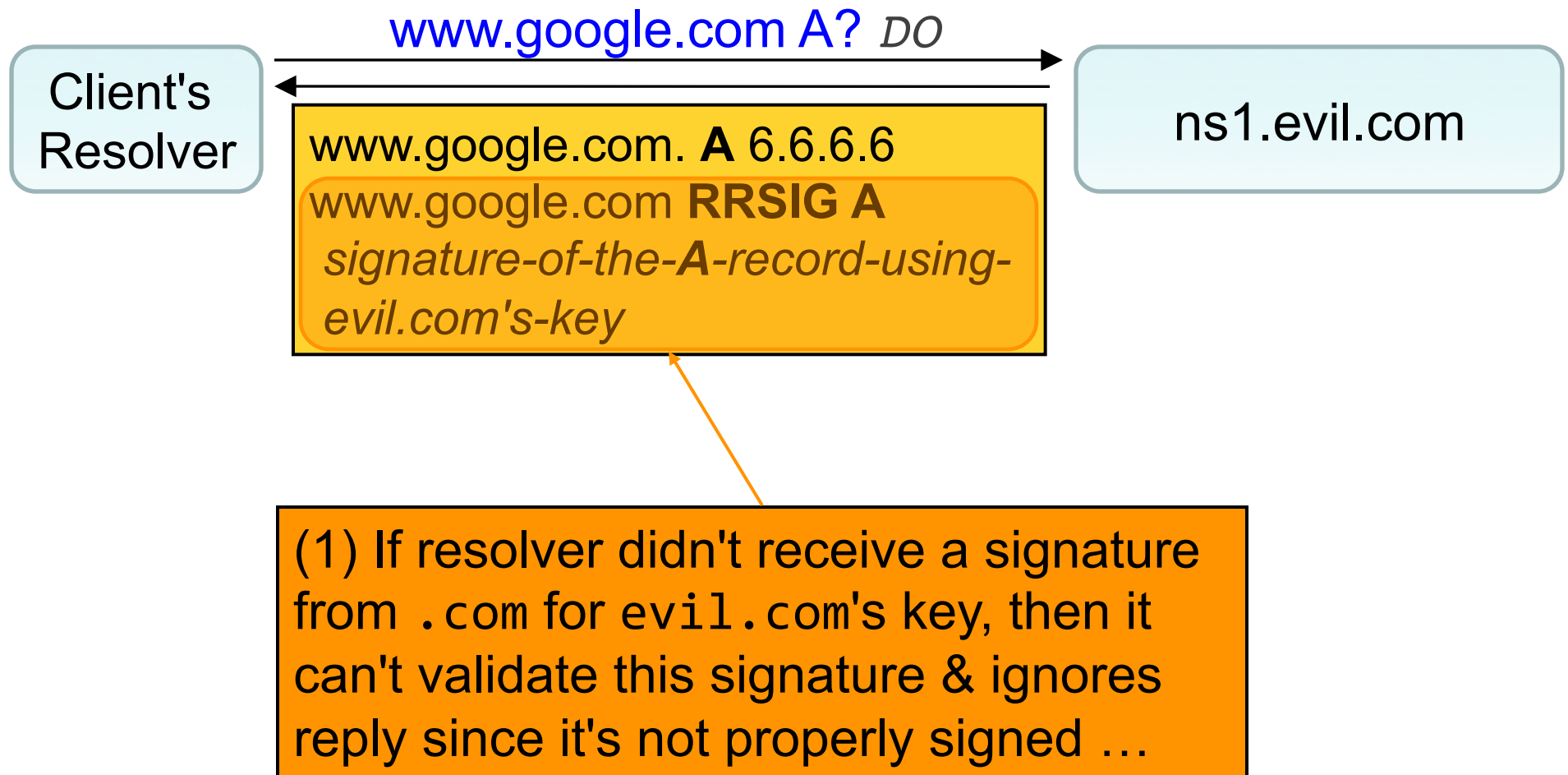
DNSSEC - Mallory attacks!



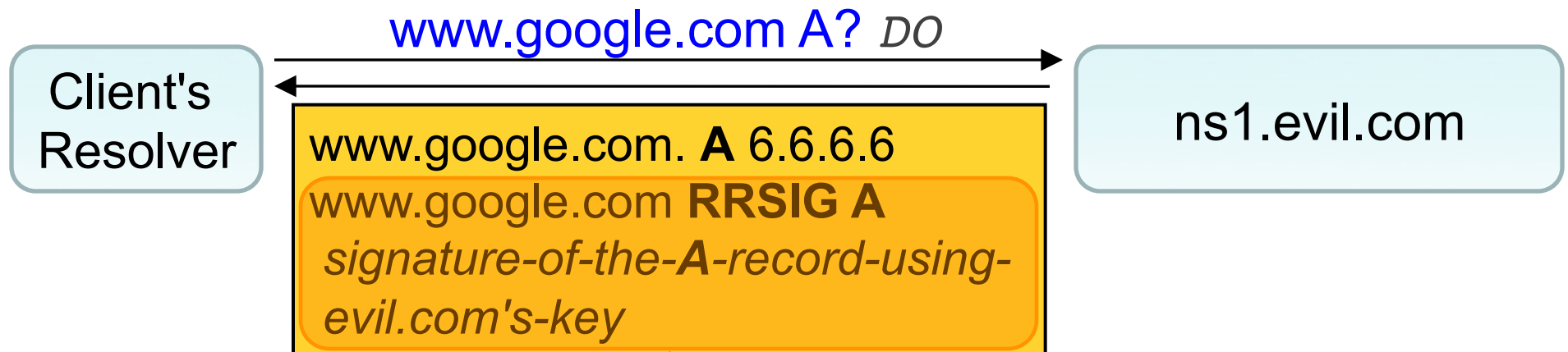
DNSSEC - Mallory attacks!



DNSSEC - Mallory attacks!

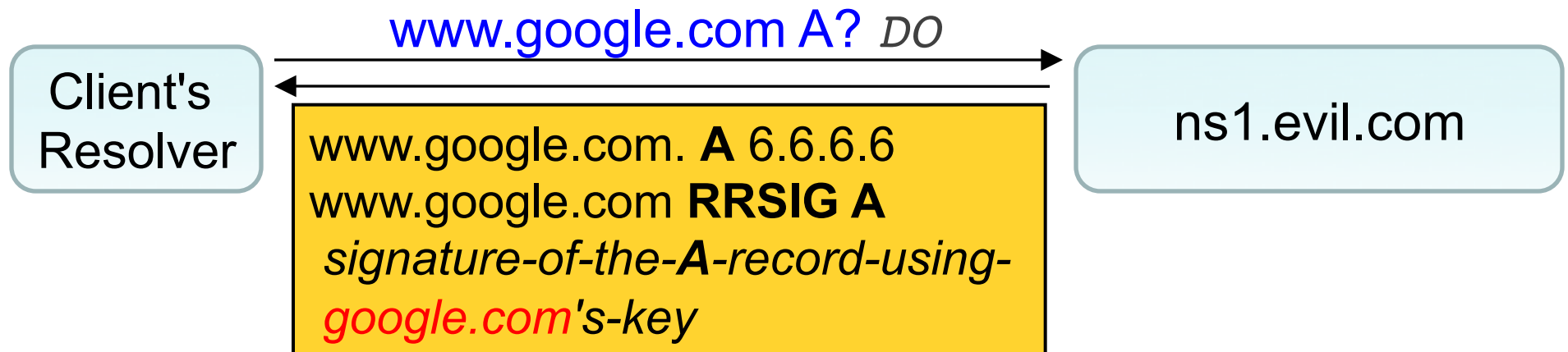


DNSSEC - Mallory attacks!

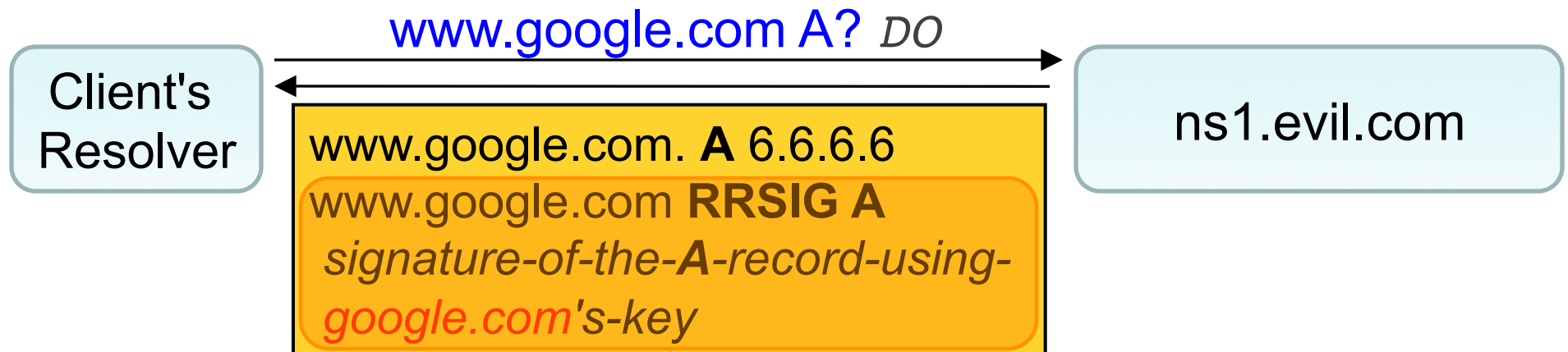


(2) If resolver *did* receive a signature from .com for evil.com's key, then it knows the key is for evil.com and not google.com ... and ignores it

DNSSEC - Mallory attacks!



DNSSEC - Mallory attacks!



If signature **actually** comes from `google.com`'s key, resolver will believe it ...

... but no such signature should exist unless either:

- (1) `google.com` *intended* to sign the RR, or
- (2) `google.com`'s private key was compromised

```
% dig +dnssec berkeley.edu
```

% dig +dnssec berkeley.edu

```
; <<> DiG 9.6-ESV-R4-P3 <<> +dnssec berkeley.edu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10036
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 7, ADDITIONAL: 21

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;berkeley.edu.          IN      A

;; ANSWER SECTION:
berkeley.edu.          60      IN      A        169.229.216.200
berkeley.edu.          60      IN      RRSIG   A 10 2 300 20121129202230 20121025202230 28219 berkeley.edu. gM19EappM5DAofCz0+PHMEhVdz/2qXvMbg5QLD/LsqyvDwf0nUzS07/4 3JFg0qdZT5n2JwM9XKLaEpZ8sSqP5ohM+fau
wynT6M07z00vsY9z6jGs xvzAzyg2fybXtub9Rvd/0gFgzPPUu76mFIAqUuUabt81sy3b0cc1FBzR Ld0=

;; AUTHORITY SECTION:
berkeley.edu.          78276   IN      NS      sns-pb.isc.org.
berkeley.edu.          78276   IN      NS      adns1.berkeley.edu.
berkeley.edu.          78276   IN      NS      phloem.uoregon.edu.
berkeley.edu.          78276   IN      NS      adns2.berkeley.edu.
berkeley.edu.          78276   IN      NS      aodns1.berkeley.edu.
berkeley.edu.          78276   IN      NS      ns.v6.berkeley.edu.
berkeley.edu.          78306   IN      RRSIG   NS 10 2 172800 20121129002244 20121025002244 28219 berkeley.edu. la5Mioua87Ek1a9lHGNO3gXmGnS396gECVYwSfYfZ4esmJqxiog9QnF gGUsI763T7gceb7IV12a1etCwDC2jcXH
04akXj1WhtM17JHe1o8bewHt kHr/h055qVz4b0wF1YrgoNKMQRXse6q+mf2AD6dN922mmP2F9cjR8v u/4=

;; ADDITIONAL SECTION:
sns-pb.isc.org.         842     IN      A        192.5.4.1
sns-pb.isc.org.         78279   IN      AAAA    2001:500:2e::1
aodns1.berkeley.edu.   3029    IN      A        192.35.225.133
aodns1.berkeley.edu.   89287   IN      AAAA    2607:f010:3f8:8000::ff:fe00:53
phloem.uoregon.edu.    78351   IN      A        128.223.32.35
phloem.uoregon.edu.    55046   IN      AAAA    2001:468:d01:20::80df:2023
adns2.berkeley.edu.    78306   IN      A        128.32.136.14
adns2.berkeley.edu.    3596    IN      AAAA    2607:f140:ffff:ffff::e
ns.v6.berkeley.edu.    78306   IN      A        128.32.136.6
ns.v6.berkeley.edu.    85587   IN      AAAA    2607:f140:ffff:ffff::6
adns1.berkeley.edu.    78294   IN      A        128.32.136.3
adns1.berkeley.edu.    3596    IN      AAAA    2607:f140:ffff:ffff::3
sns-pb.isc.org.         842     IN      RRSIG   A 5 3 7200 20121121233449 20121022233449 4442 isc.org. 1ceskiNs+YR0l1b3psUHhipv6RDx4U3m+6cYCY2h3nLuTikiK2z4dCba 2oM1Y8FaB+UfGrJw+7Go40X0aNAR78P64Q1BVEANb/
Fwe2hc+2ibDjwy 4osCQb+g0PQ1Zf9AehvZoiEnqByz3LV2ow3bZAwsR+QgHAdsje0fMhu WI4=
sns-pb.isc.org.         248     IN      RRSIG   AAAA 5 3 7200 20121121233449 20121022233449 4442 isc.org. BLuidvyB5IK11CjikfMchBtBGUv1o/0oI+r13apdbb0wKwpSc7U47u A3RpHa49Cj82E42mUIrFgw38C0jsfXVo9VWn+0R
P2Yxmk0vU6HfHwBQE A1sBpCi1nmCVickU5BgTL4FF//uN7zLnz1KCKAdioBXX7epAPbcMvsi/ ieA=
aodns1.berkeley.edu.   3029    IN      RRSIG   A 10 3 3600 20121129202230 20121025202230 28219 berkeley.edu. njoXhHn0mBtgmXQK9Ff9Trw9RLMhyDquDyAera3pJ0zvQjnIcr2WddLm Y0FsDuopYnF8kXtEmzNfWiyXfshvHADGLr
h+u3UZ+Cfq5Cbugt5p+Ht Hh7DacPpfGXrSDSzio1bse5TSzIkRR63GLDEGrk++VMq/u4Cq4ILMEJ1 lsU=
adns1.berkeley.edu.    3533    IN      RRSIG   AAAA 10 3 3600 20121129202230 20121025202230 28219 berkeley.edu. XNvdohhvNrk0y95z62K1nxP5fEia2HYWMMvtKkptxHtpYzVjshRC+o+/Y c4MGKEFvfp4HPMHSW2u4sAA8nq17Sv0T
92ZMLwVvDEpcrG1xGgMVqRRX c25hqt0RsF1U1/Fy0zXXPj9xBD7wi013kyjDNcf0KI6T9e8tzHBm/0VQ tAA=
adns2.berkeley.edu.    78306   IN      RRSIG   A 10 3 172800 20121129002244 20121025002244 28219 berkeley.edu. GEm0ddcBT9k56kA+n94f2es428pKW/M/T2RqwbmftMT1TmqiLY4+jm+rV W3rdsrpy4rV6Jr4ydMMeEwd7Espd/i60
Va3ThwzTFdgrfU5JZl0z1toG mL19umqKAKggqLTP9T3hqdTcDG20Gj05pE0sEnuibczTBKtp7Y3rxqZJ mcE=
adns2.berkeley.edu.    3596    IN      RRSIG   AAAA 10 3 3600 20121129202230 20121025202230 28219 berkeley.edu. FyQrnninwU5D0dQv9R3dbr7Xk1YpIAN0AteBj1GarT3E/GJrfUPTIRZ7z S0uxF7VjwXQWphdLcb5VMSZCQAJxNMci
qLkp4DnXZjwGsQvfcY2Ah1/0 nQeYB20VTI4sX4avb8Lx2zxsDE7dUbwPZbiGmyRfCeGR0JgTL5c/fv0p Ces=
adns1.berkeley.edu.    78294   IN      RRSIG   A 10 3 172800 20121129002244 20121025002244 28219 berkeley.edu. LEwqPKb3gKHUxojV3lVeZwH85VoZkMjZg8awWpjsi9fdLS+kwVcsL+yf ctsdAw5UgB3tq5iAxlyPhVU/tmGgk6/ZZ
C706/d2yUd+3Ugtov6b9bcV Lz4eSKj9EpD5h9R+yGVh/EvkV3JfFMcS/muI2rKekjrjPYvJawWfYAI6 yCU=
adns1.berkeley.edu.    3596    IN      RRSIG   AAAA 10 3 3600 20121129202230 20121025202230 28219 berkeley.edu. OdPnw+kYy8M6Q79bfN6mXhneU2yNEF2CUvDy5s7qvwvDDQgqkmcR0iJQ oamV0De+VrouFieTspplLcAp21KcTWlpg
NcosMiajnlgae74hjAKDoo3d jHI31HWTHkTQsGiWxD5qKogt+9RDNRVNL5lGRcFe8SenB4npMChc/j cxQ=
```

IPv6 Traffic Growth

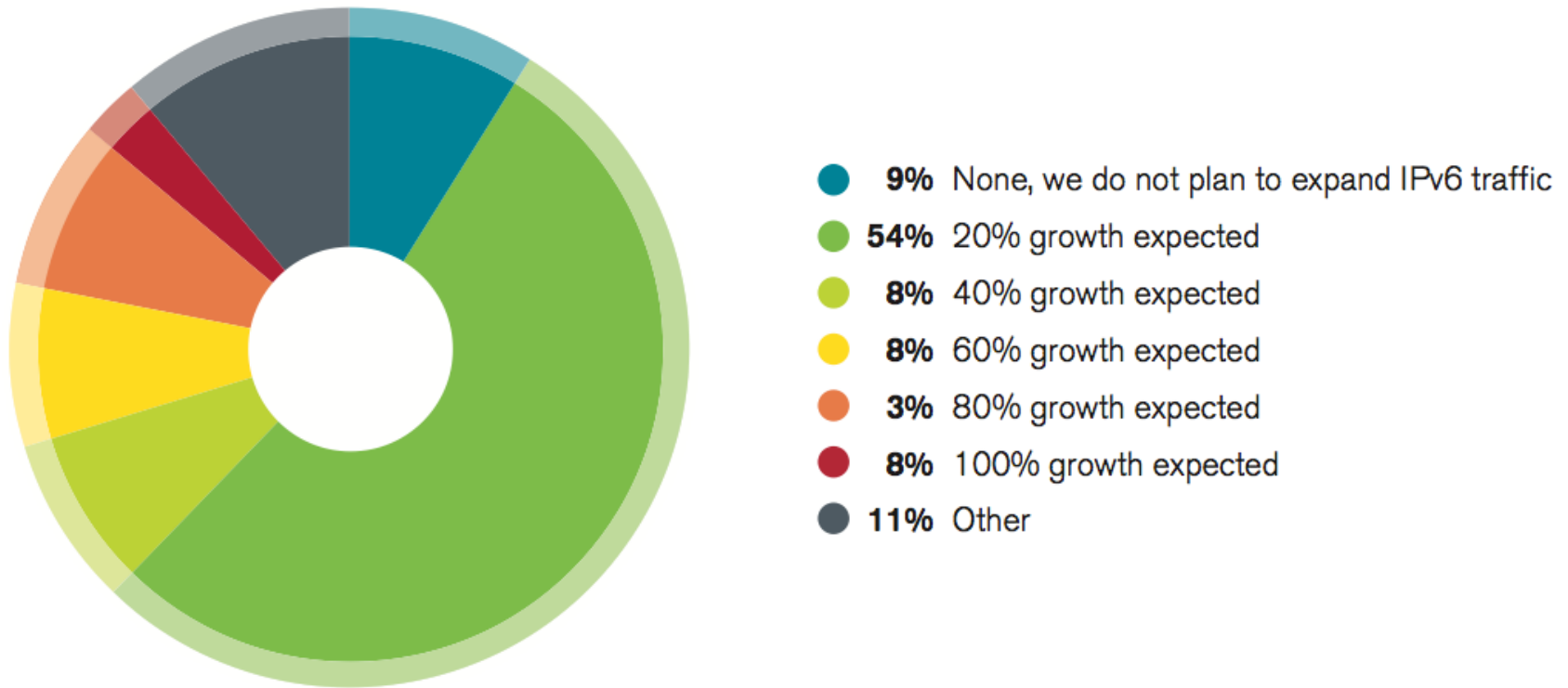
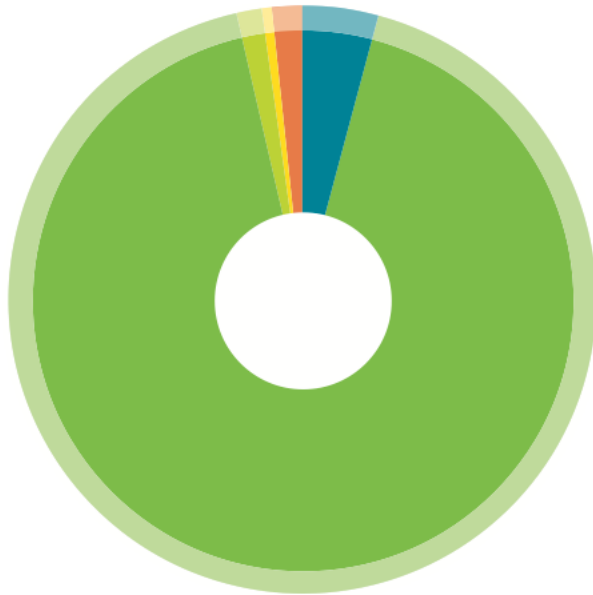


Figure 50 Source: Arbor Networks, Inc.

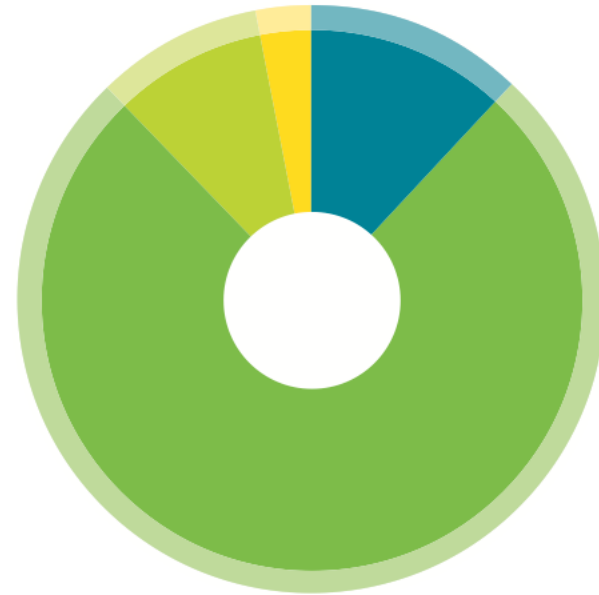
Subscriber IPv6 Usage



- 26% None, we do not offer IPv6 services to end-users
- 53% 1-25
- 9% 26-50
- 3% 51-75
- 9% 76-100

Figure 47 Source: Arbor Networks, Inc.

Business Customer IPv6 Service Usage



- 12% None, we do not offer IPv6 service to business customers
- 75% 1-24
- 9% 26-50
- 3% 76-100

Figure 48 Source: Arbor Networks, Inc.

IPv6 Security Concerns

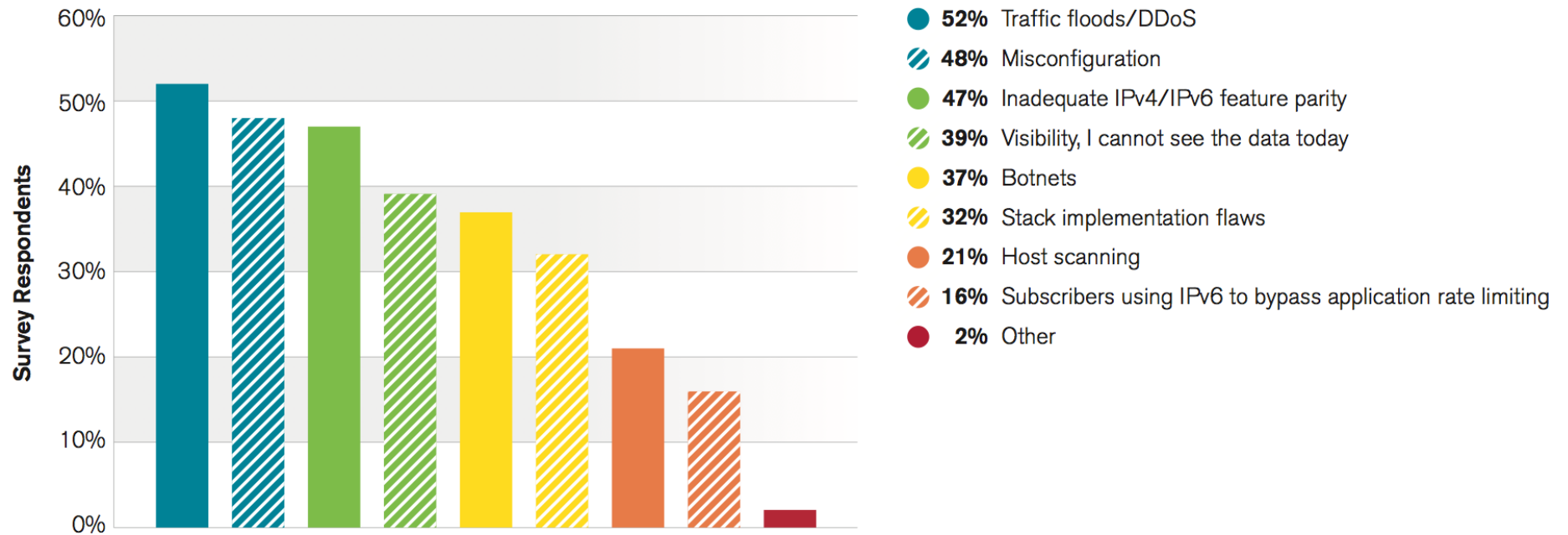


Figure 51 Source: Arbor Networks, Inc.

IPv6 Flow Telemetry

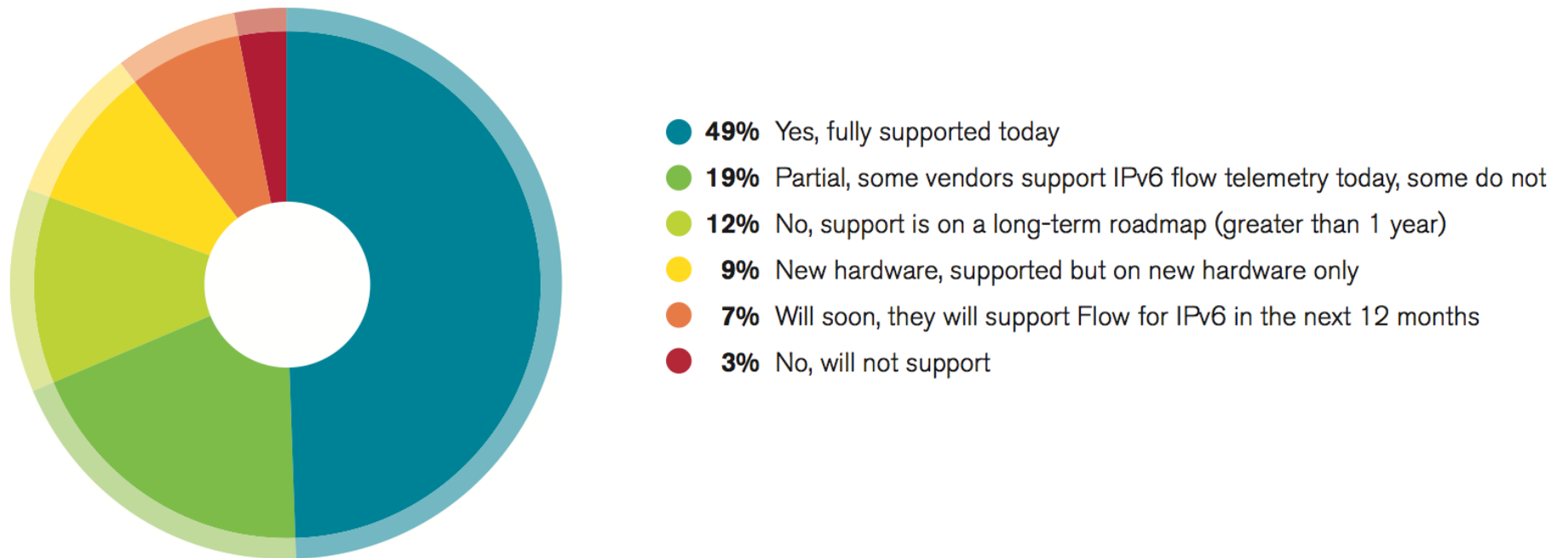
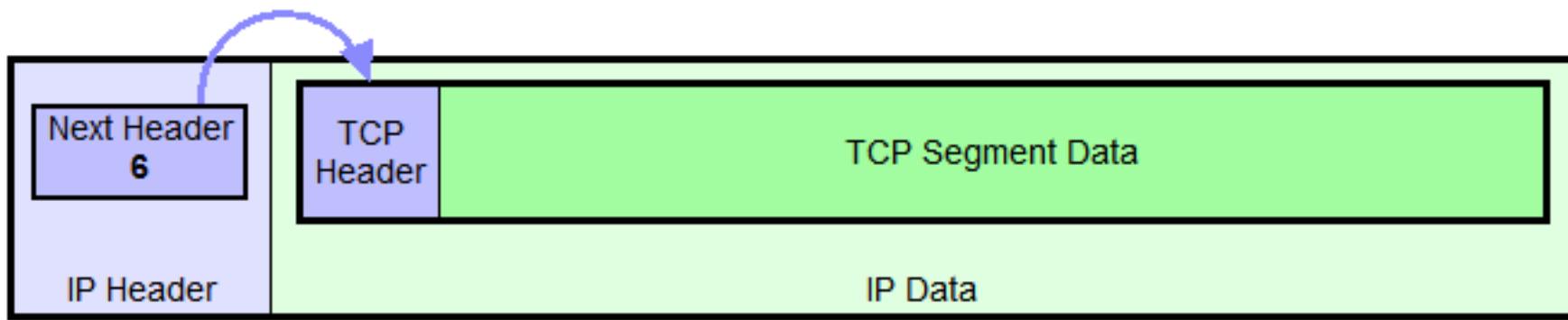
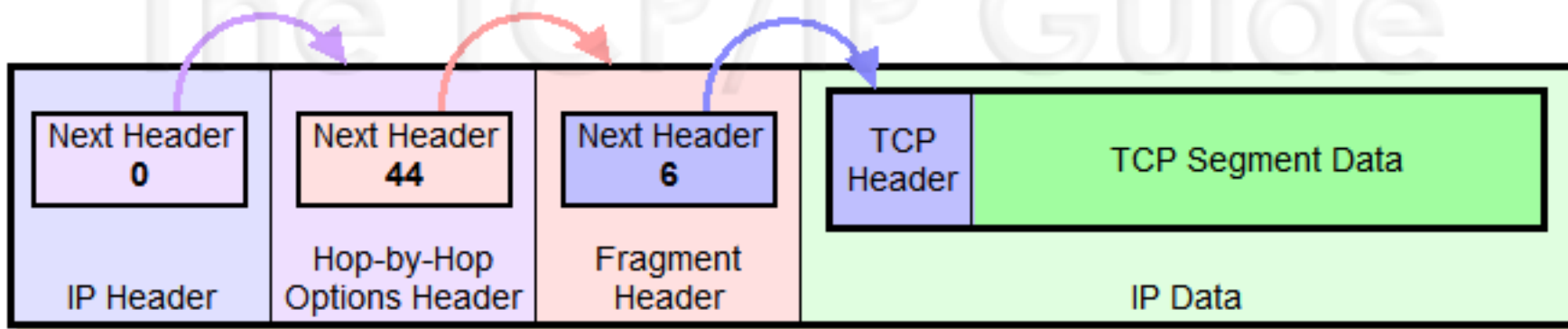


Figure 49 Source: Arbor Networks, Inc.

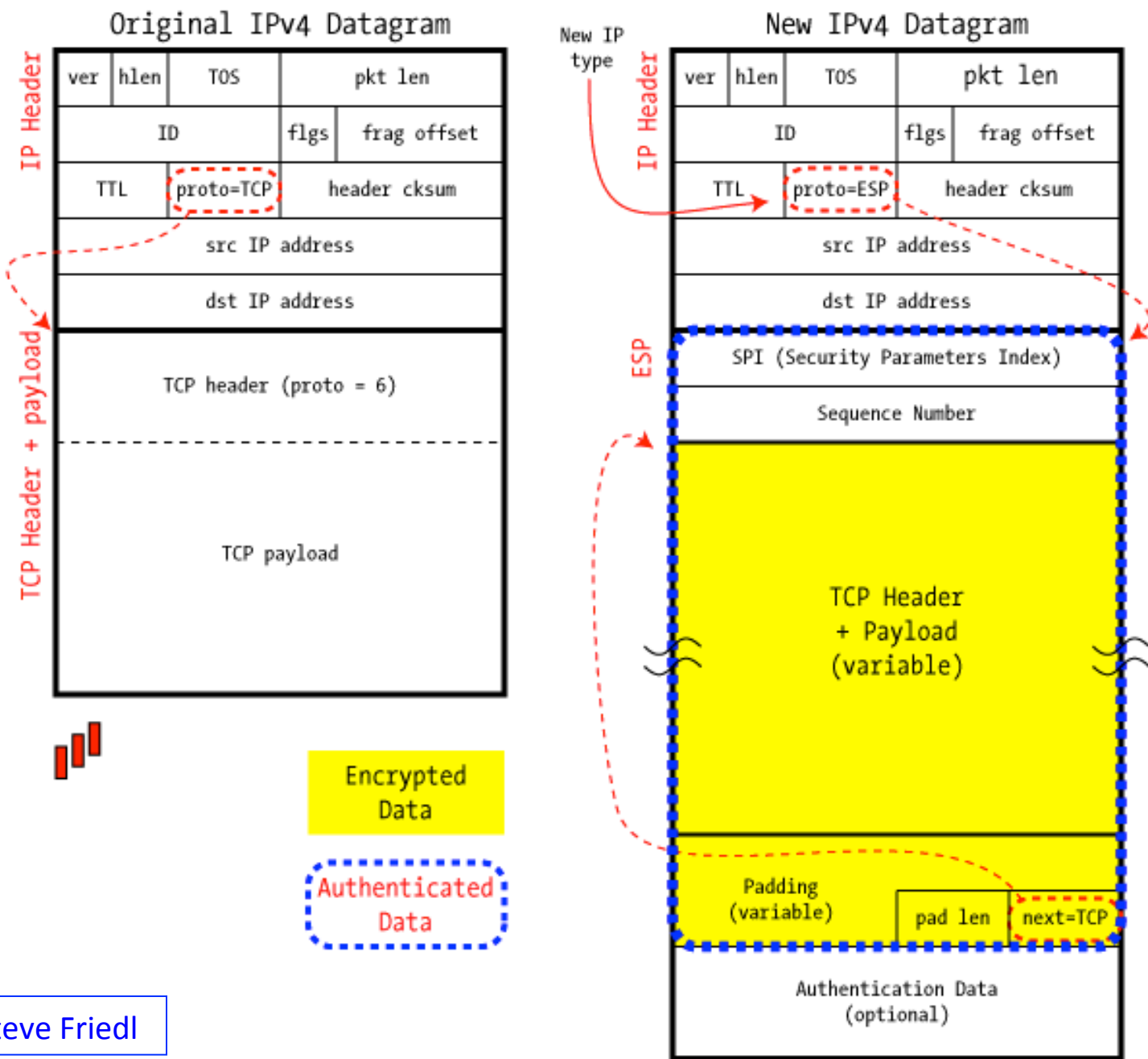


IPv6 Datagram With No Extension Headers Carrying TCP Segment



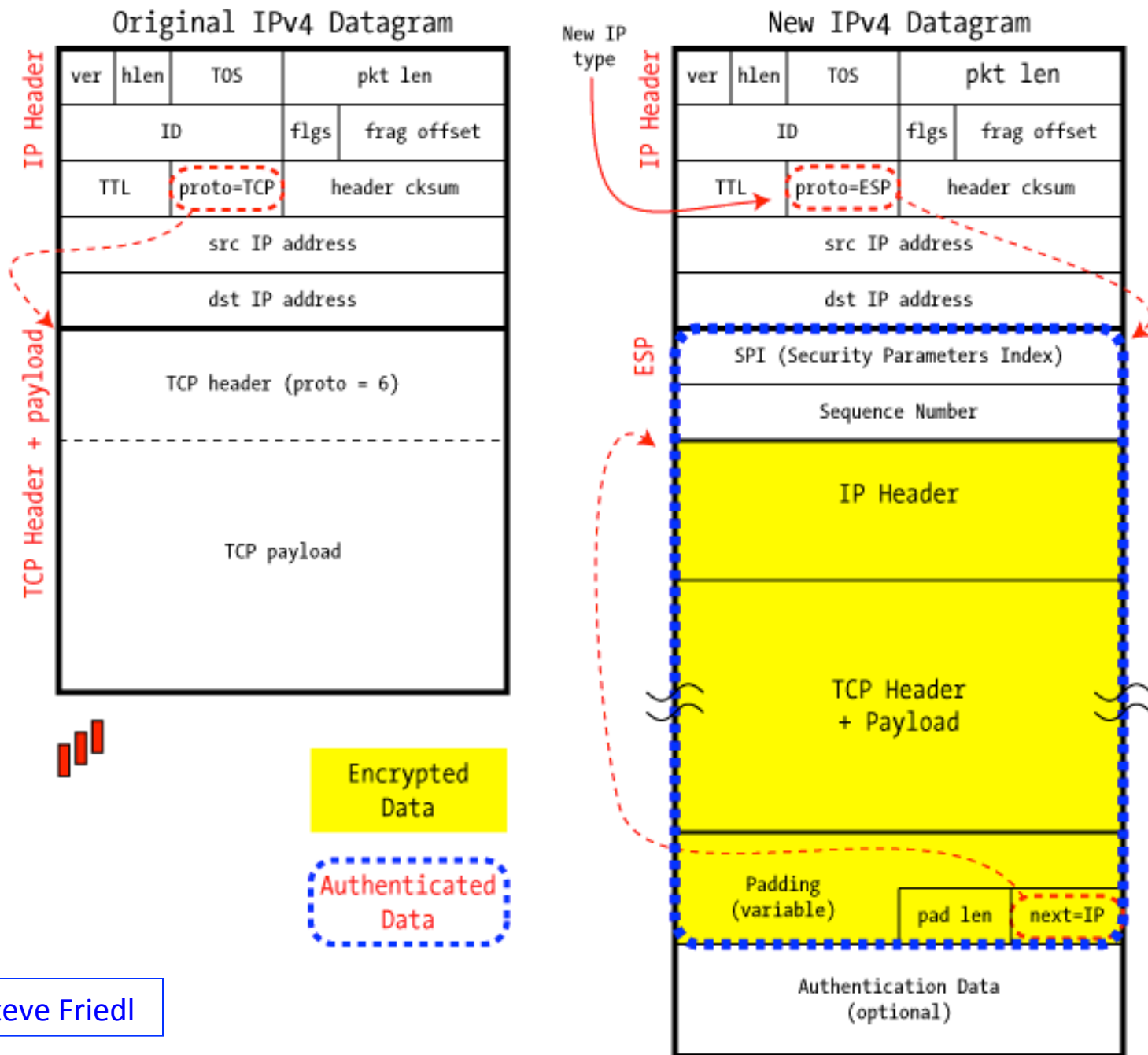
IPv6 Datagram With Two Extension Headers Carrying TCP Segment

IPSec in ESP Transport Mode



Credit: Steve Friedl

IPSec in ESP Tunnel Mode



Credit: Steve Friedl