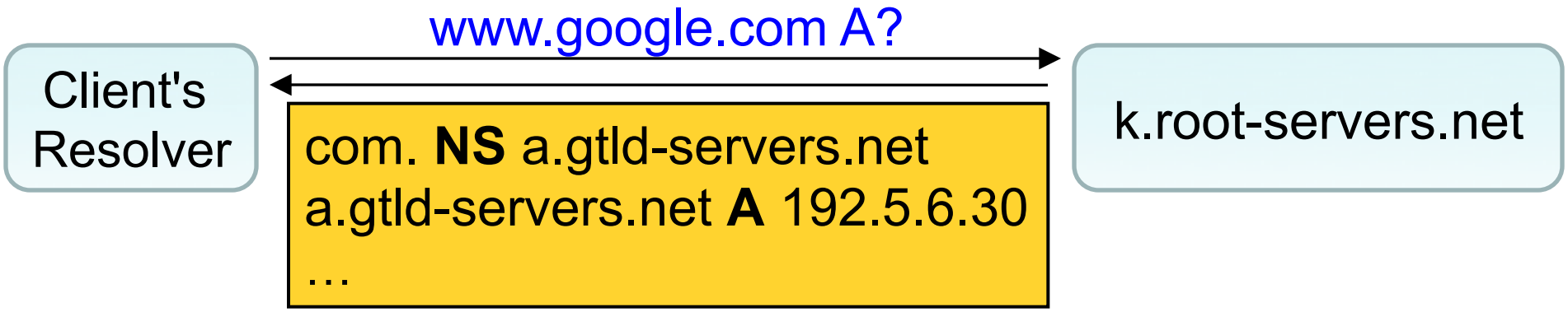
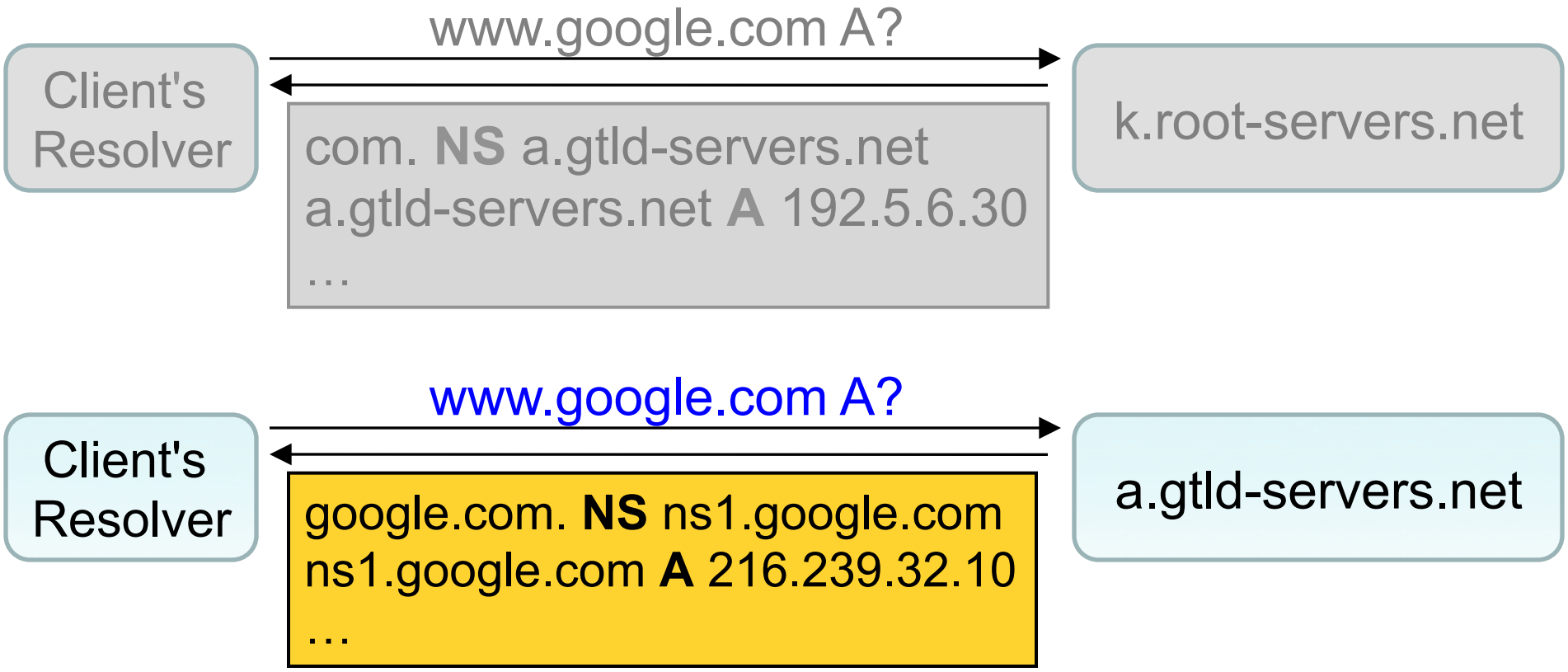
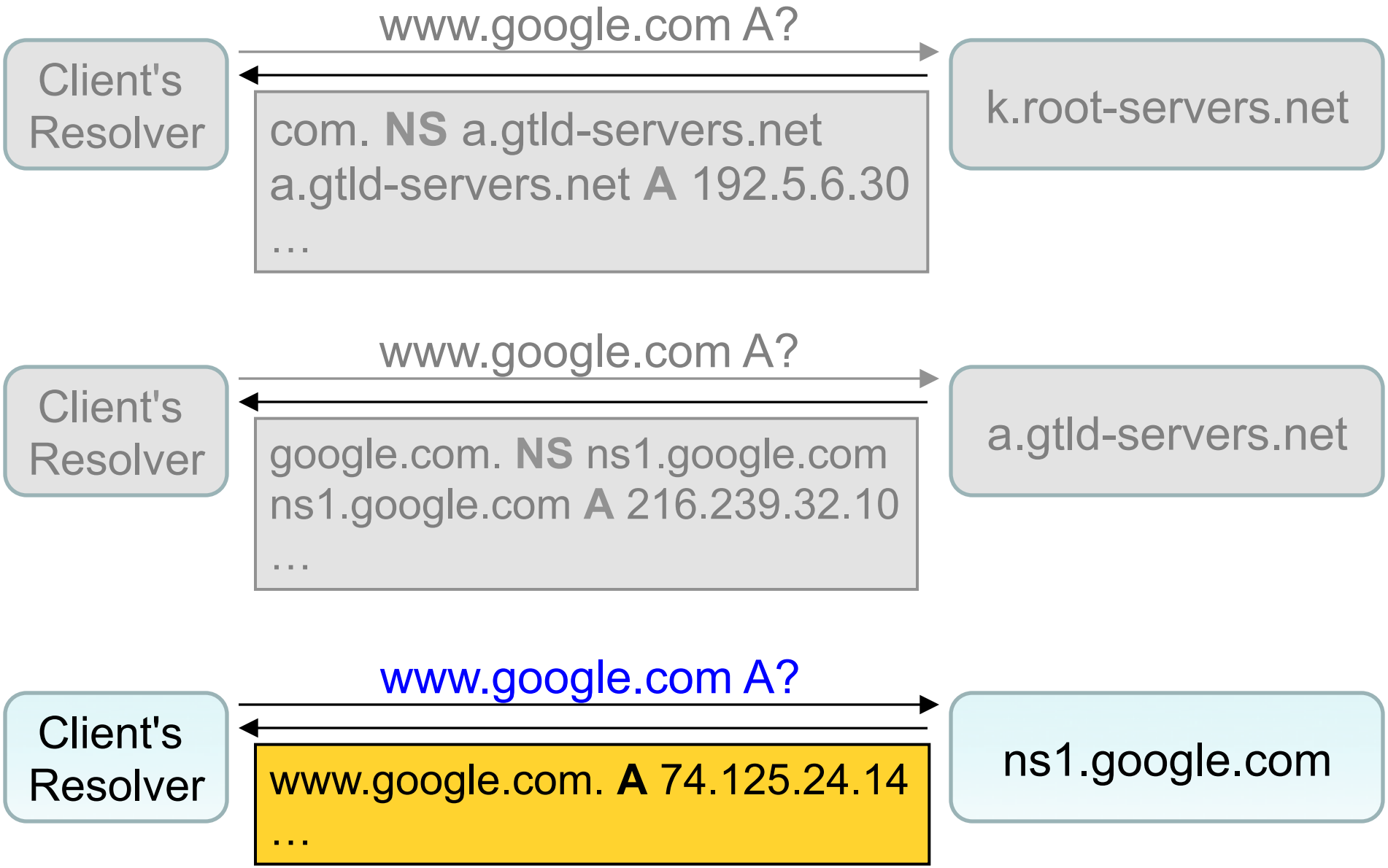
Ordinary DNS:



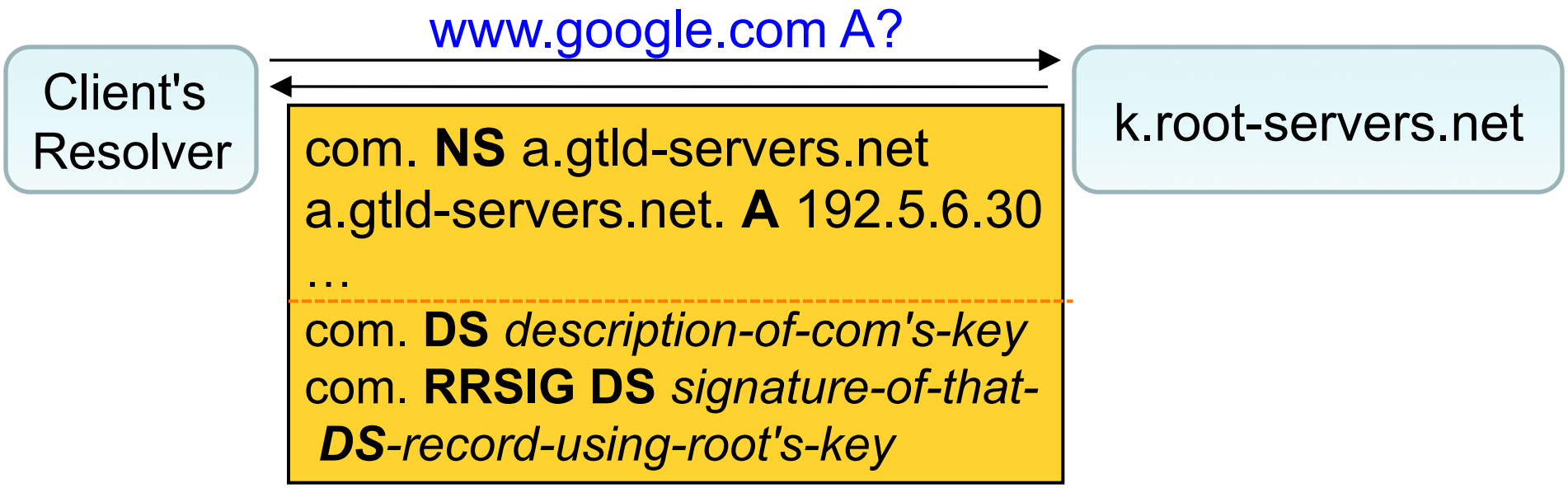
Ordinary DNS:



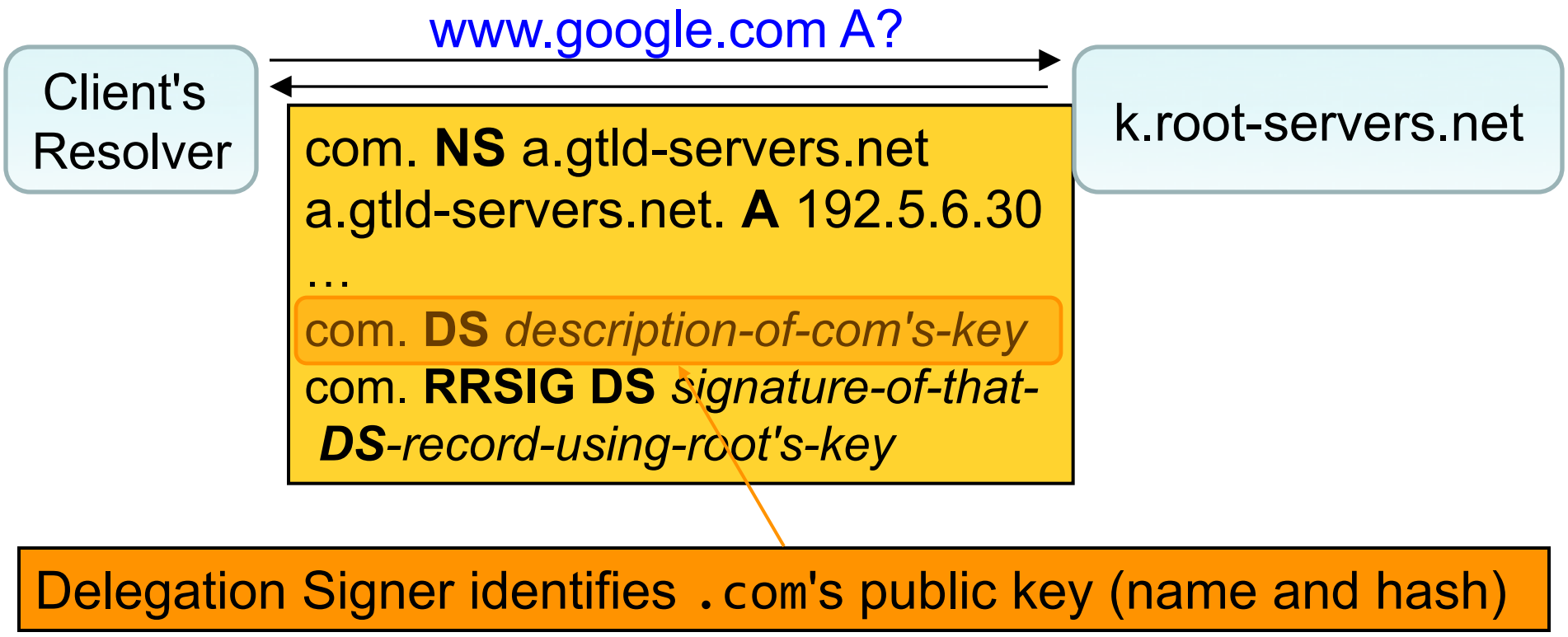
Ordinary DNS:



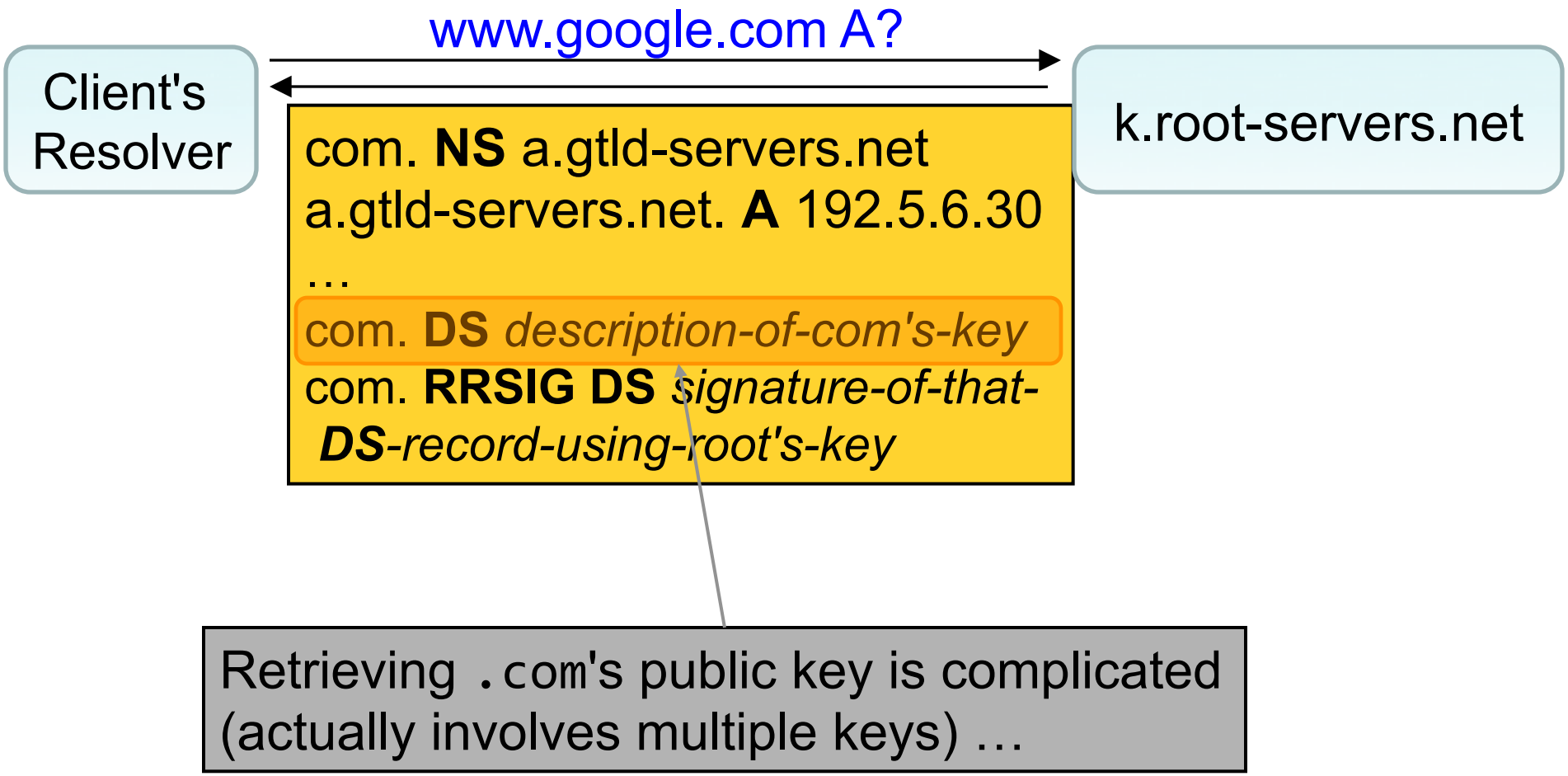
DNSSEC (with simplifications):



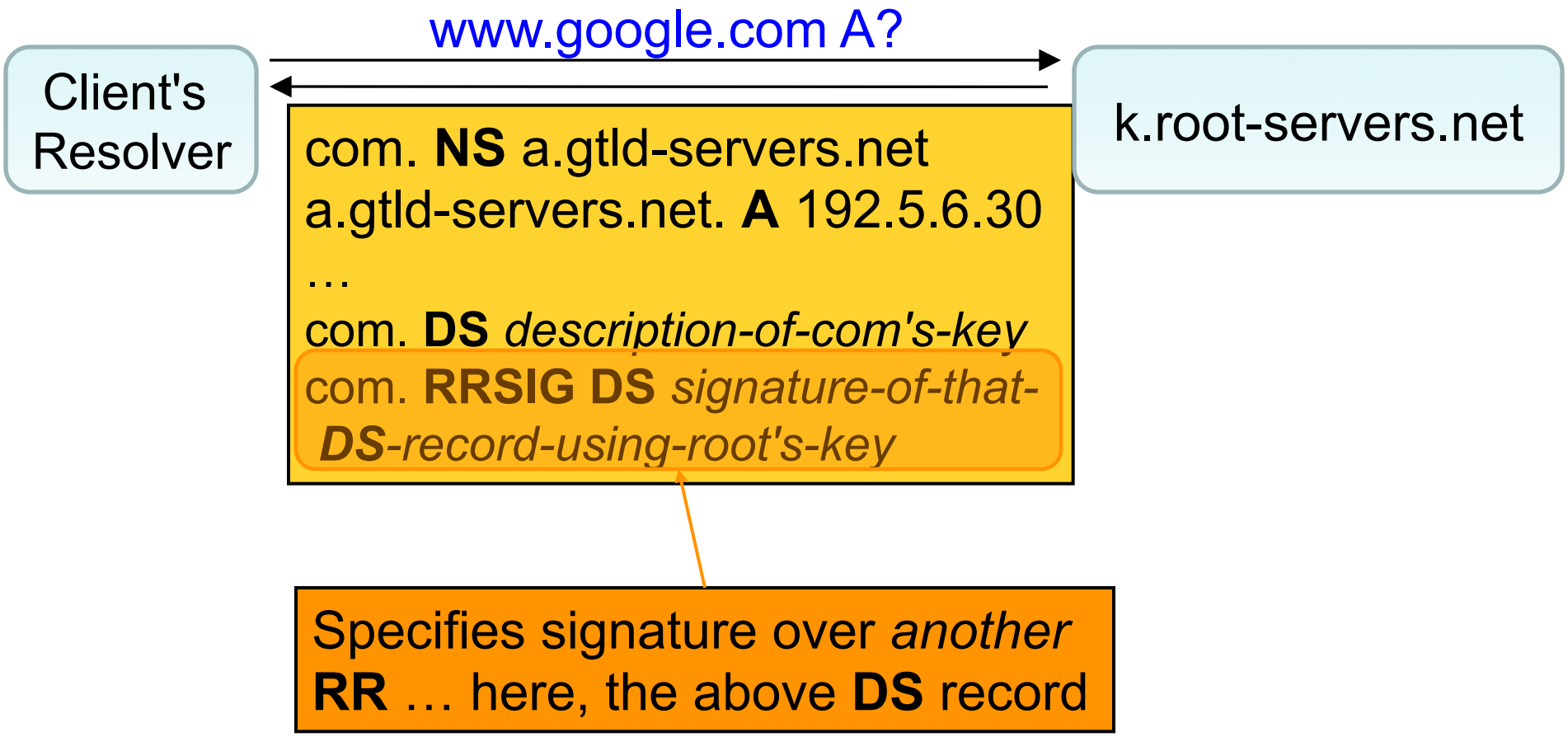
DNSSEC (with simplifications):



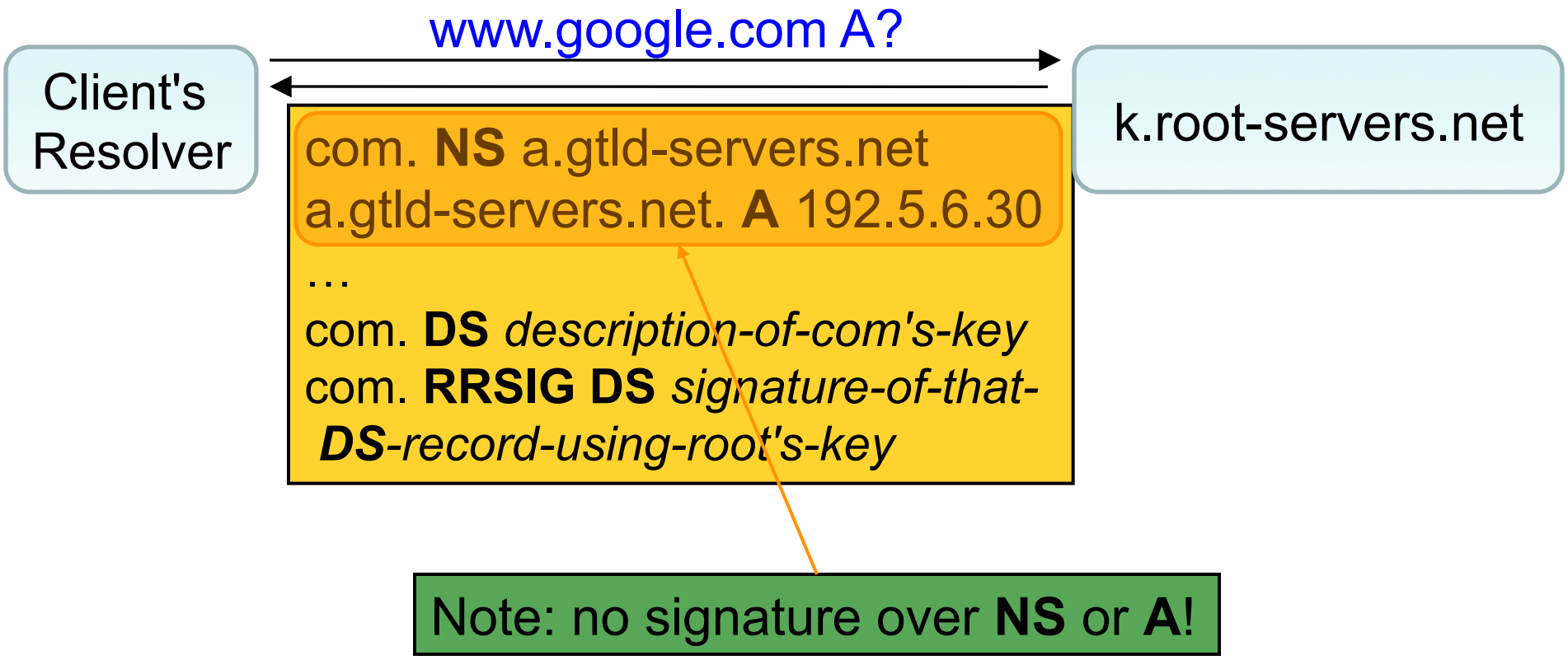
DNSSEC (with simplifications):



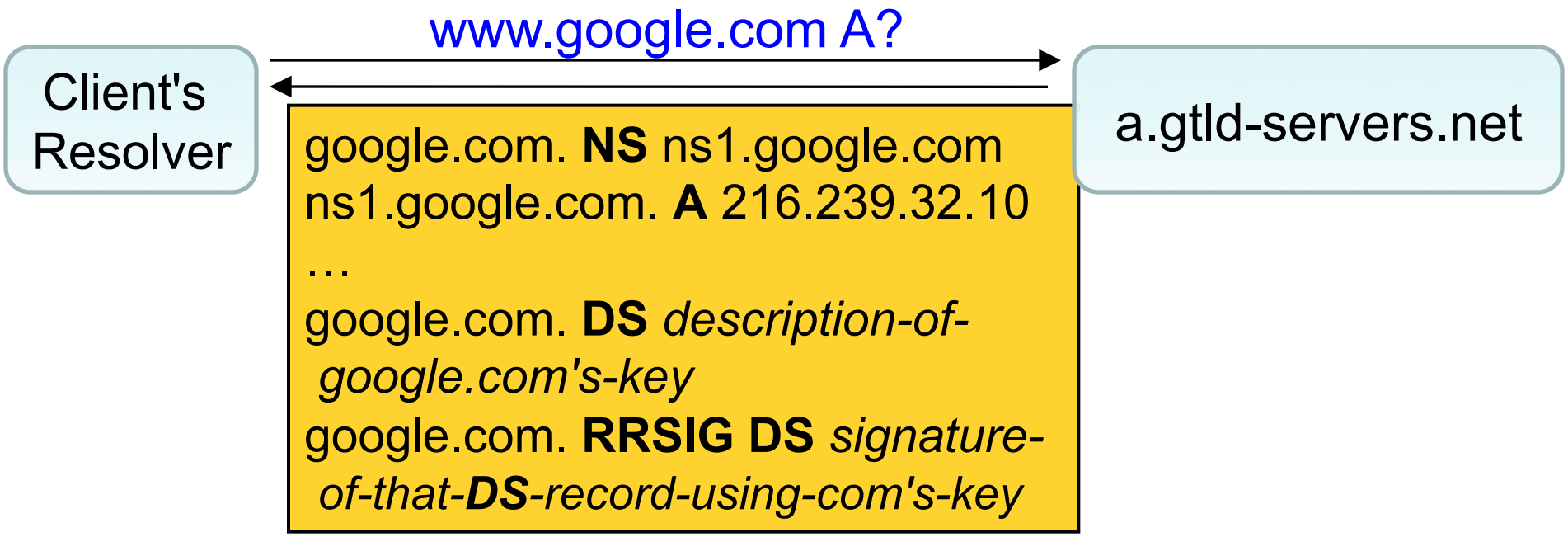
DNSSEC (with simplifications):



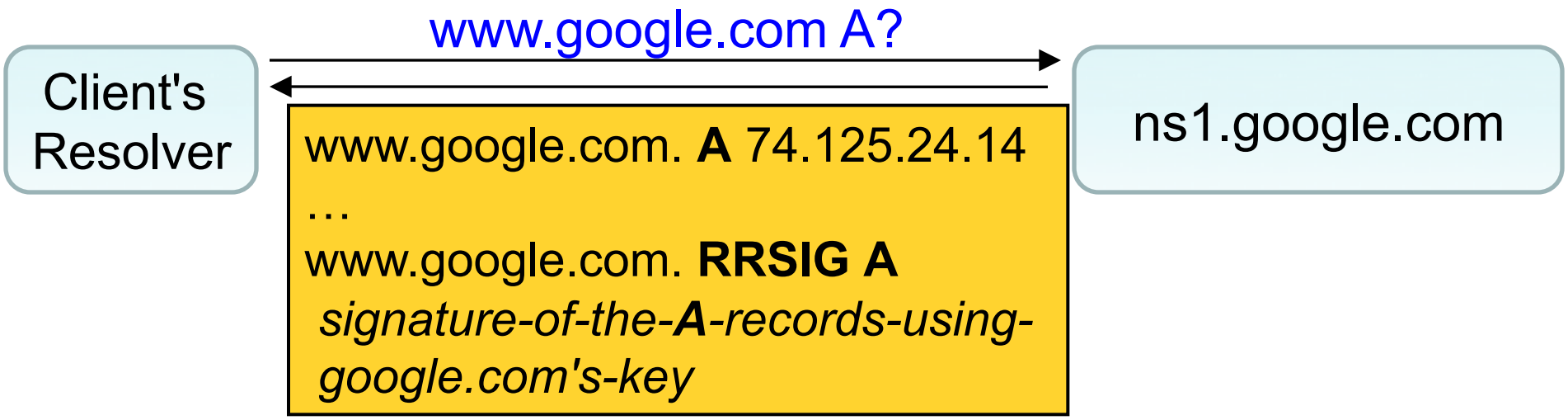
DNSSEC (with simplifications):



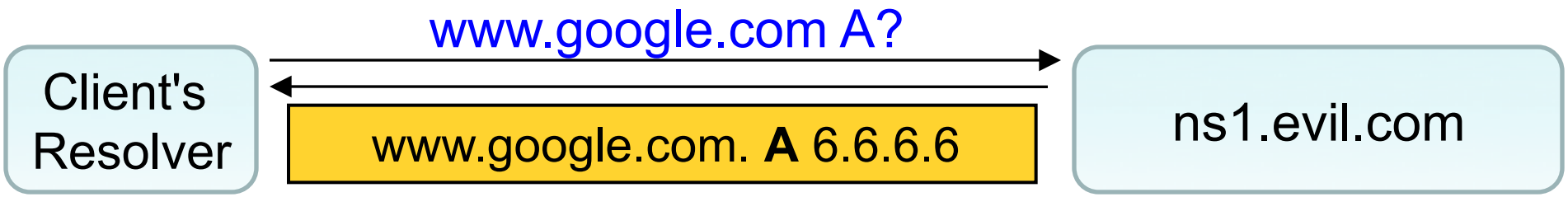
DNSSEC (with simplifications):



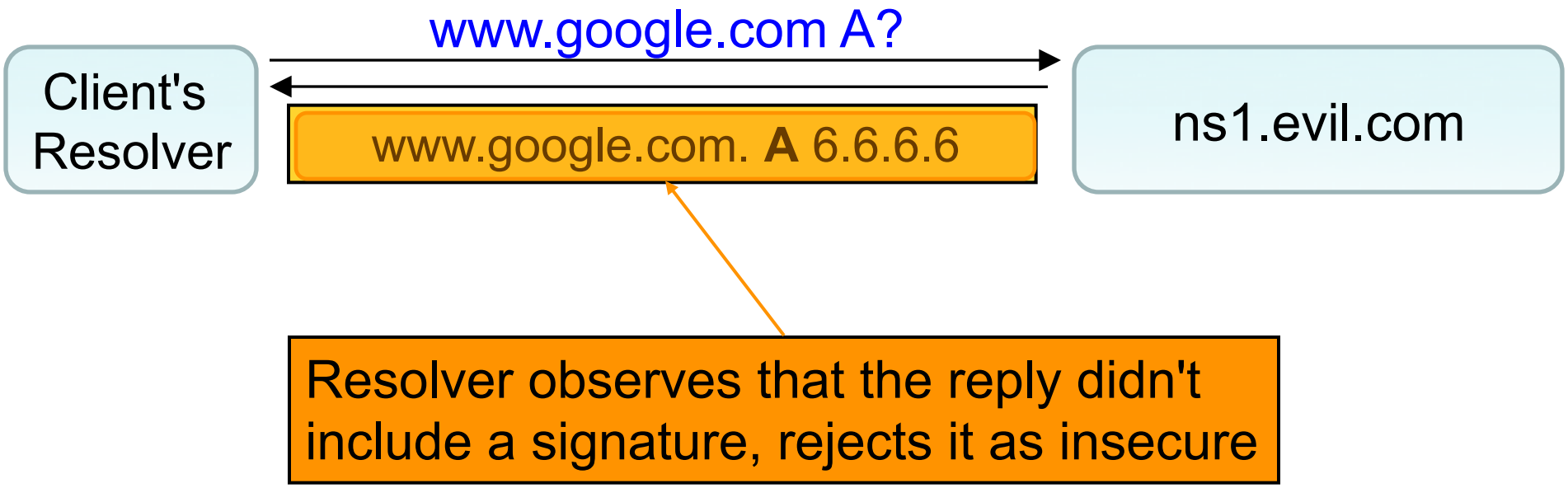
DNSSEC (with simplifications):



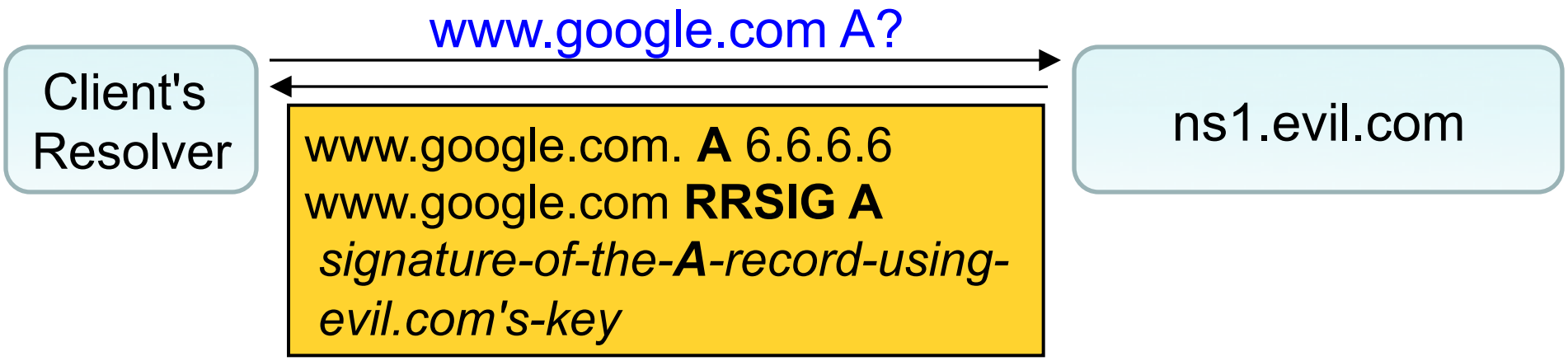
DNSSEC - Mallory attacks!



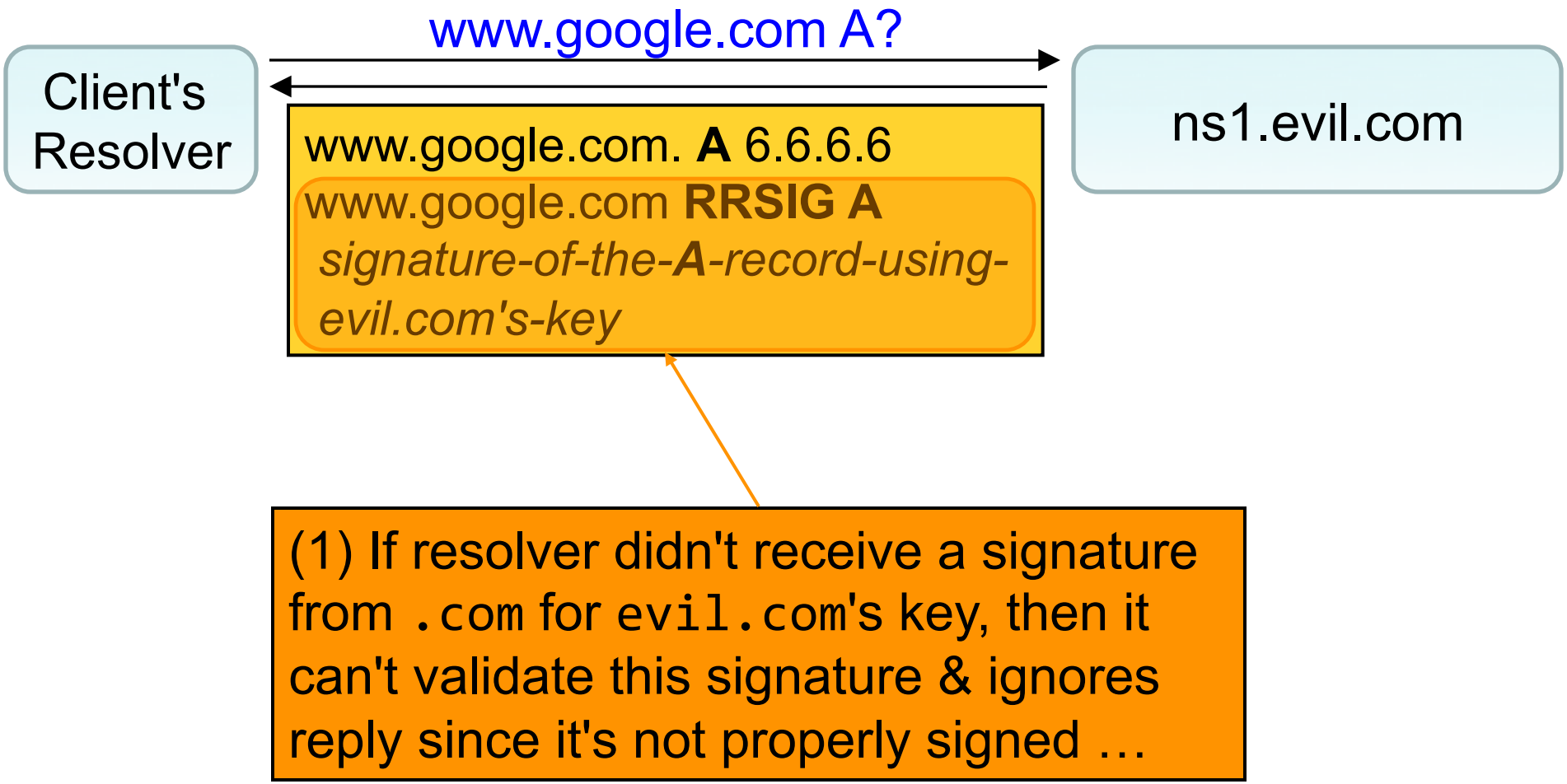
DNSSEC - Mallory attacks!



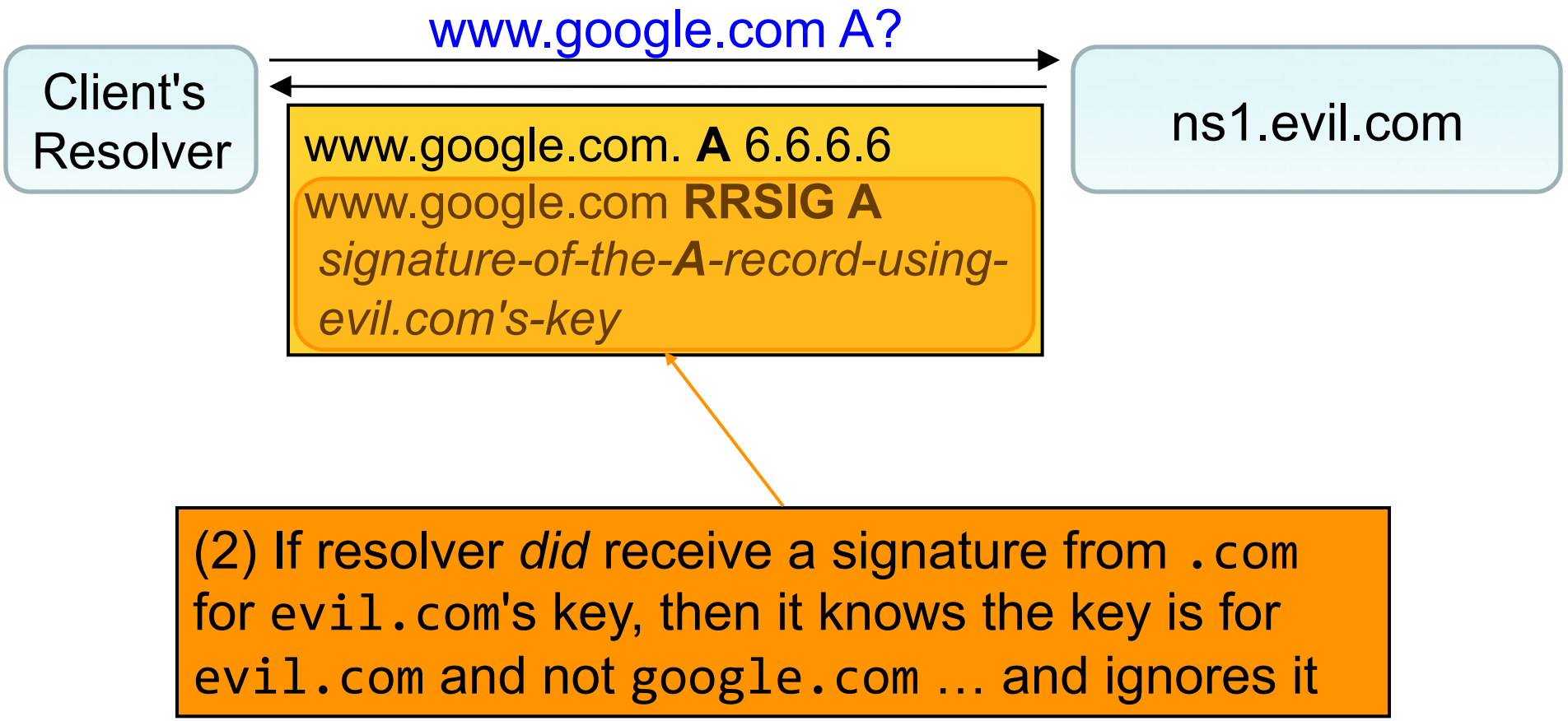
DNSSEC - Mallory attacks!



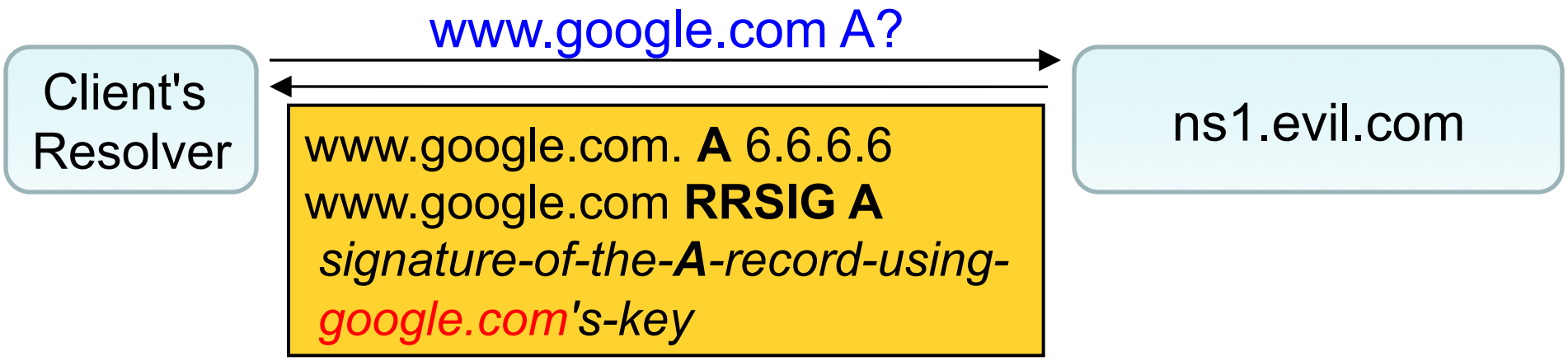
DNSSEC - Mallory attacks!



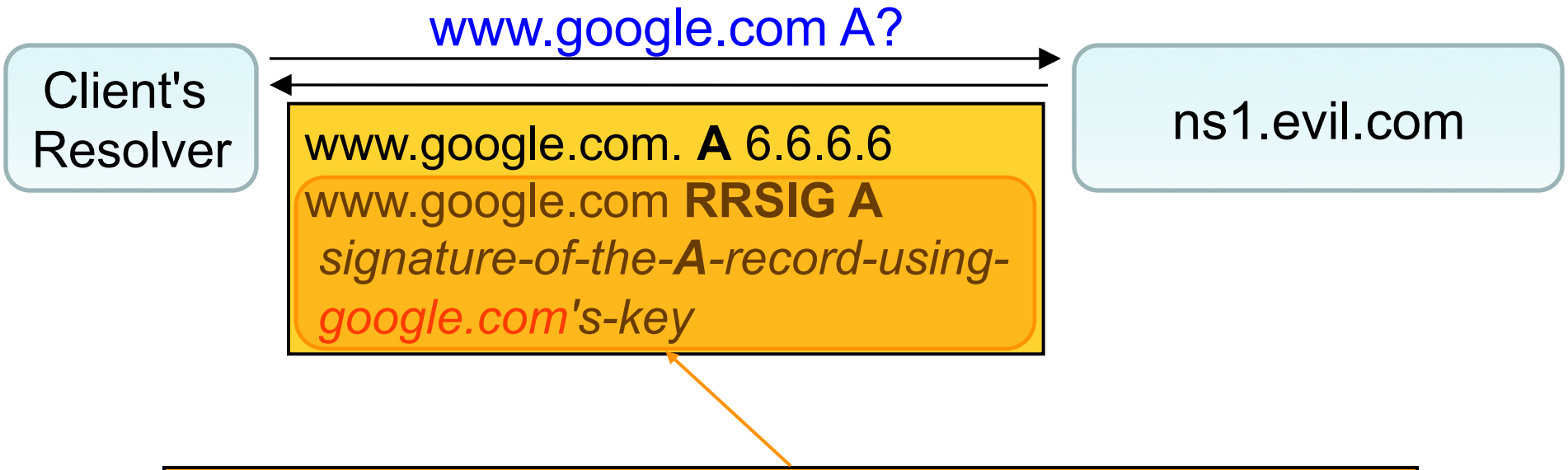
DNSSEC - Mallory attacks!



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. gmM9EappMSDAofCz0+PHMEhVDz/2qXvMbq5QLD/LsqyvDWf0nUzSQ7/4 3JFgOqdZT5n2JwM9XKlaEpZ8sSqP5ohM+fau
wynT6M07zOOvsY9z6jGs xvzAzyg2fybXtub9Rvd/0gFgzPPUu76mFIAqUUuabt81syJbOcCiFBzR 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. la5Miouа87Ekb1a9lHGNO3gXmGnSJ96gECVyWnsYfZ4esmjQxiog9QnF gGUsI763T7gceb7IVI2a1etCWdC2jcXH
04akXjlWhrMl7jHelo8bewHt kHr/hO55qVz4bOwFlYrgoNKVMMQRXse6q+mf2AD6dN92ZmnP2F9cjR8v 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:fffe::e
ns.v6.berkeley.edu.     78306   IN      A       128.32.136.6
ns.v6.berkeley.edu.     85587   IN      AAAA    2607:f140:ffff:fffe::6
adns1.berkeley.edu.     78294   IN      A       128.32.136.3
adns1.berkeley.edu.     3596    IN      AAAA    2607:f140:ffff:fffe::3
sns-pb.isc.org.         842     IN      RRSIG   A 5 3 7200 20121121233449 20121022233449 4442 isc.org. 1ceskiNs+YR0l1b3psUHipvp6RDx4U3m+6cYCY2h3nLuTikiK2z4dCba 2oM1Y8FaB+UfGrJw+7Go40XOaNAR78P64Q1BVEANb/
Fwe2hc+2ibDjwy 4osCQb+g0PQ1Zf9AehvZoiiEnqByz3LV2ow3bZAwsR+QqHAdsje0fMhu WI4=
sns-pb.isc.org.         248     IN      RRSIG   AAAA 5 3 7200 20121121233449 20121022233449 4442 isc.org. BLuidvyB5lKl1CjikfmTchBTbGUv1o/OoI+r13qpdbbOwKwpScC7U47u A3RpHa49Cj82E42mUIrFgw38C0jsFxVo9VWn+0R
P2Yxmk0vU6HfhWBQE A1sBpCi1nmCVickU5BgTL4fF//uN7zLnz1KCKAdioBXX7epAPbcMvsi/ ieA=
aodns1.berkeley.edu.    3029    IN      RRSIG   A 10 3 3600 20121129202230 20121025202230 28219 berkeley.edu. njoXHhNOmBTgmxQK9Ff9TrW9RLMhyDquDyAERa3pJOzvQjnIcr2WddLm YOFsDuopYnF8KbXtEmzNfWiyXfsHvHaDGLr
h+u3UZ+Cfq5Cbugt5p+Ht Hh7DAcPpfGXrSDSzio1bse5TSzIkRR63GLDEGrk++VMq/u4Cq4iLMEJ1 lsU=
aodns1.berkeley.edu.    3533    IN      RRSIG   AAAA 10 3 3600 20121129202230 20121025202230 28219 berkeley.edu. XNvdohhvNrKOy95zb2K1nxP5fEia2HYWMVtKkptxHtpYZvJshRC+o+/Y c4MGKEFVfp4HPMHSw2u4sAA8nq17Sw0T
92ZMLwWvDEpcrG1xGgMVqRRX c25hqtORsF1Ul/Fy0zXXPJ9xBD7wiOl3kyjDNcf0KI6T9e8tzHBm/0VQ tAA=
adns2.berkeley.edu.     78306   IN      RRSIG   A 10 3 172800 20121129002244 20121025002244 28219 berkeley.edu. GEmOddcBT9k56kA+n94f2es428pKW/M/T2RqwbmfT1MTyqilY4+jm+rV VW3rdspvy4rVGjR4ydMMeEWd7Espd/i60
Va3ThwzTFdgfuSJZl0zltoG mL19umqKAkggqlTP9T3hqdTcDG20GjG5pEOsEnuibczTBKtp7Y3rxqZJ mcE=
adns2.berkeley.edu.     3596    IN      RRSIG   AAAA 10 3 3600 20121129202230 20121025202230 28219 berkeley.edu. FyQrnninwU5DdQV9R3dbr7Xk1YpIAn0ATeBj1GarT3E/GJrfUPTlRZ7z SOuxF7VjwXQWphdLcb5VMSZCQAjxNMci
qLkp4DnXZjwGsQvfcY2Ahl/O nQeYB20VTI4sX4avb8Lx2zxsDE7dUbWPZbiGmyRFCeGROJgTL5c/fv8p Ces=
adns1.berkeley.edu.     78294   IN      RRSIG   A 10 3 172800 20121129002244 20121025002244 28219 berkeley.edu. LEwqPKb3gKHUxojV3lVeZwH85VoZkMjZg8awWpjsi9fdLS+kwVcsL+yF ctsdAw5UgB3tqSiAxlYPhVU/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+kYY8M6QF9bfN6mxHneU2vNEF2CUvDy5s7qvwvDDQgqkmcROiJQ oaMVODe+VrouFieTsppLCAp21KcTWlpg
NcosMiqjnlgae74hjAKDoo3d jMI31HWTHKtQSgiWxDSqKGogt+9RDNRVNQL5lGRcFeBSenB4npMChc/j cxQ=
```

Anticipated IPv6 Traffic Growth

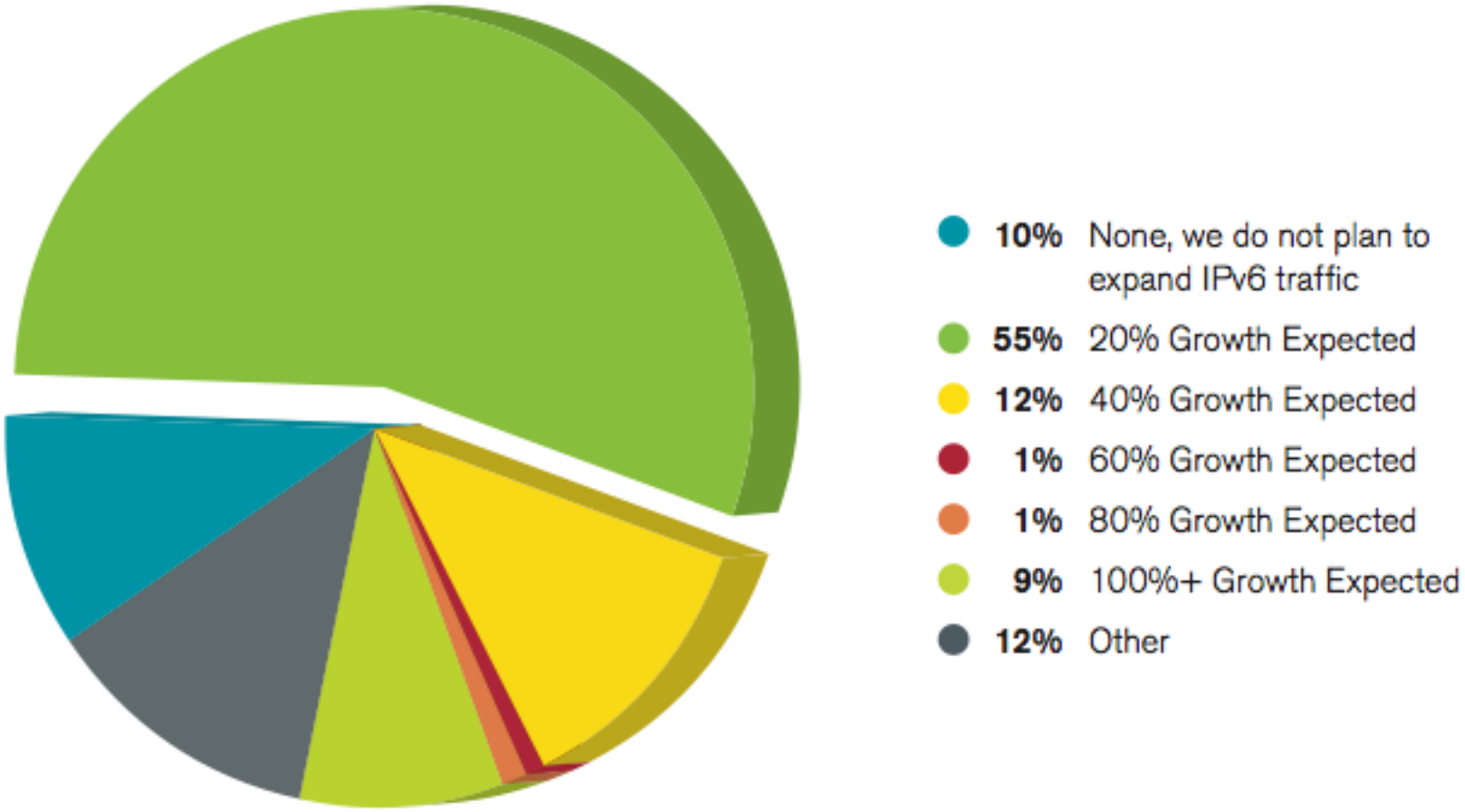


Figure 51 *Source: Arbor Networks, Inc.*

IPv6 Security Concerns

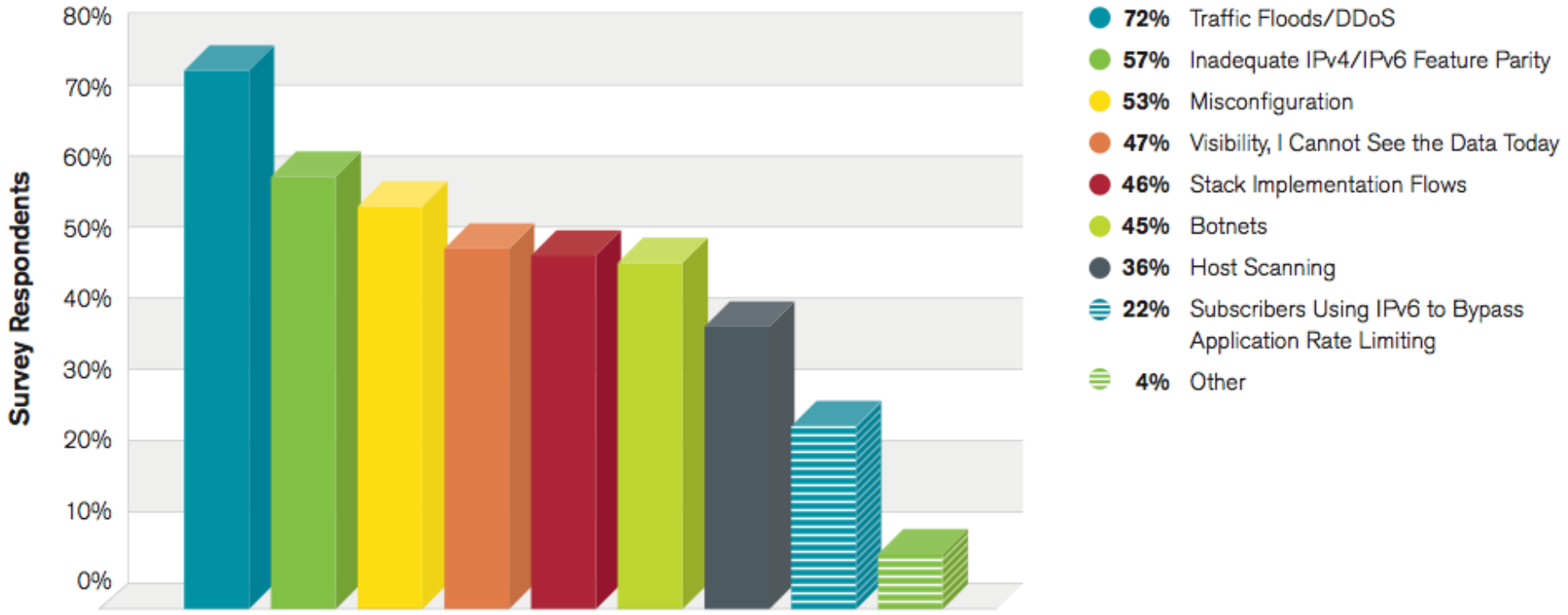
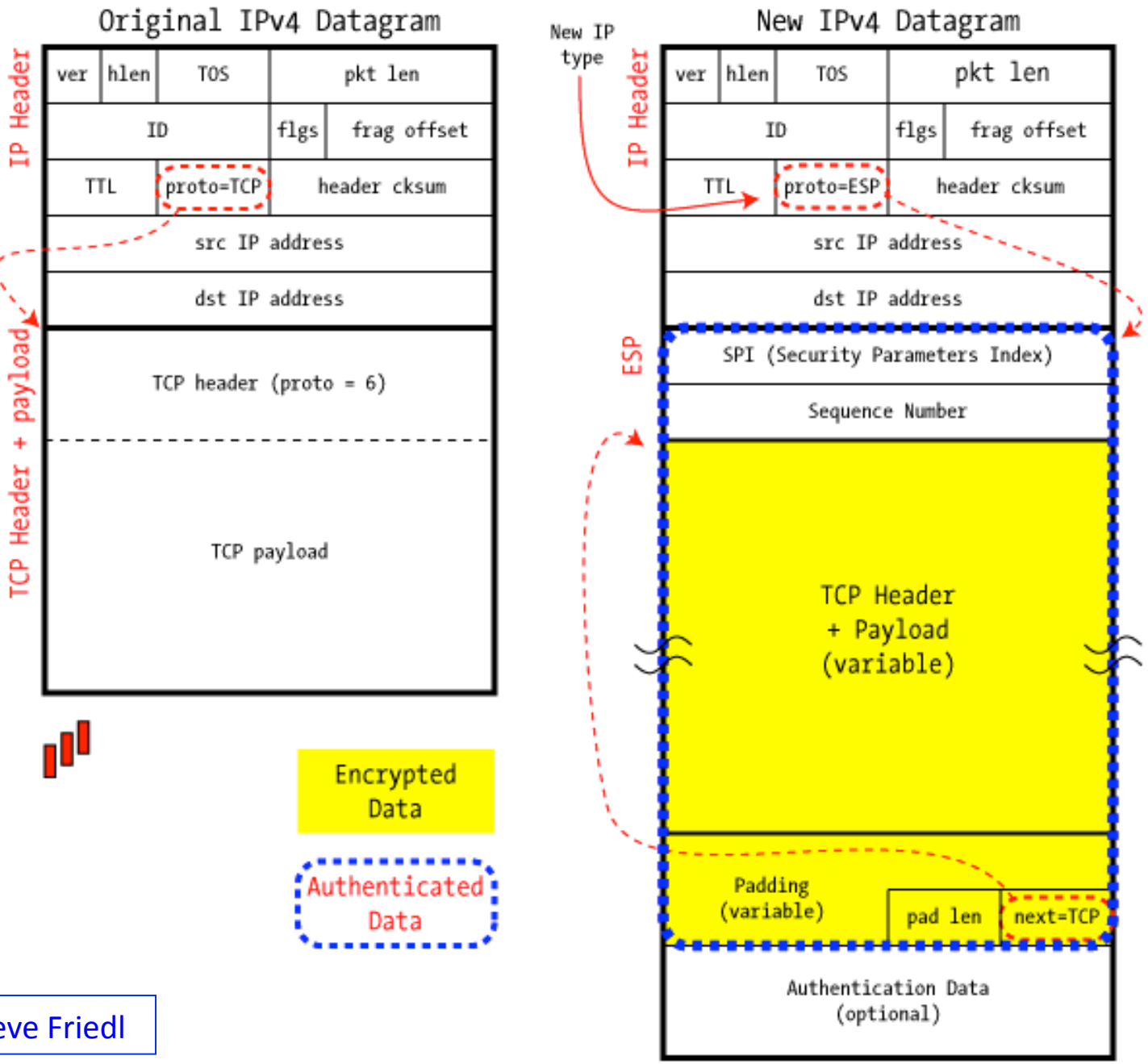


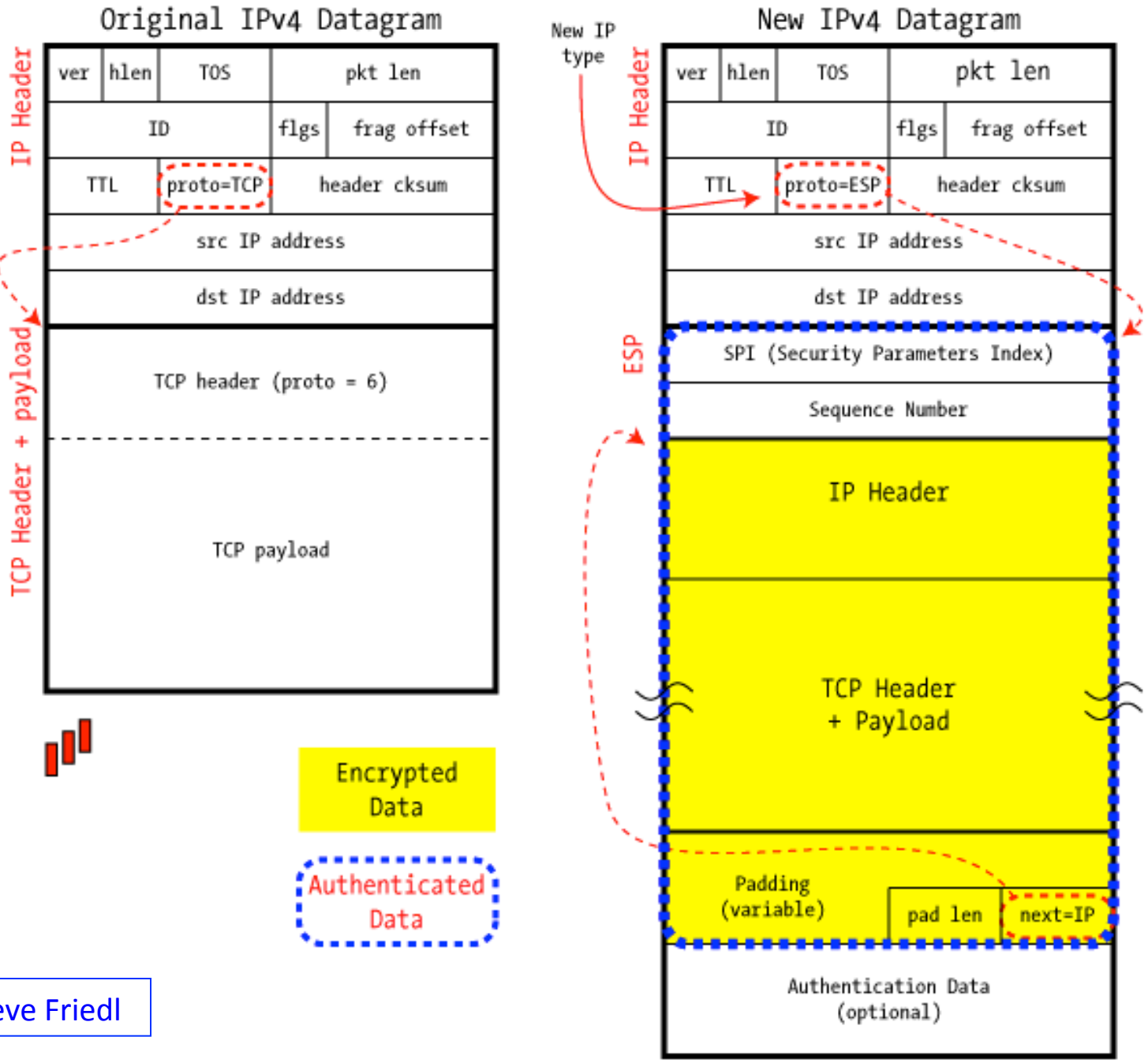
Figure 52 *Source: Arbor Networks, Inc.*

IPSec in ESP Transport Mode



Credit: Steve Friedl

IPSec in ESP Tunnel Mode



Credit: Steve Friedl