Crypto ransomware targets called by name in spear-phishing blast

Once the domain of espionage, personalized scams embraced by profit-driven scammers.

by **Dan Goodin** - Apr 6, 2016 10:07am CDT


Incident at [redacted]. - For the attention of [redacted] - Message (HTML)

FILE MESSAGE

Thu 3/10/2016 3:39 PM

Jamie Byrom <motellanancy@aol.com>

Incident at [redacted]. - For the attention of [redacted]

To [redacted]

Message Incident at [redacted]. - For the attention of [redacted]_Id.005107.doc (78 KB)

Dear ([redacted]) [redacted]

I have been told to contact you in reference to the conflict that happened at [redacted] ([redacted] BENTONVILLE, AR, [redacted]) on Tuesday. Please see the enclosed document for comprehensive details on the incident.

Would you mind if I asked you to view the complaint and respond with your thoughts on this?

Good Luck!
Jamie Byrom

Enlarge / An e-mail targeting a retail company to deliver point-of-sale malware.

Proofpoint

For the past decade, spear phishing—the dark art of sending personalized e-mails designed to trick a specific person into divulging login credentials or clicking on malicious links—has largely been limited to espionage campaigns carried out by state-sponsored groups. That made sense. The resources it takes to research the names, addresses, and industries of large numbers of individuals was worth it when targeting a given organization that had blueprints or some other specific piece of data prized by the attacker. But why go through the trouble to spread crypto ransomware or banking trojans to the masses when a single scam e-mail could do the trick?

network security

cs642

adam everspaugh
ace@cs.wisc.edu

computer security

today

* Domain name system (DNS)
* CIDR
* Border Gateway Protocol

dns

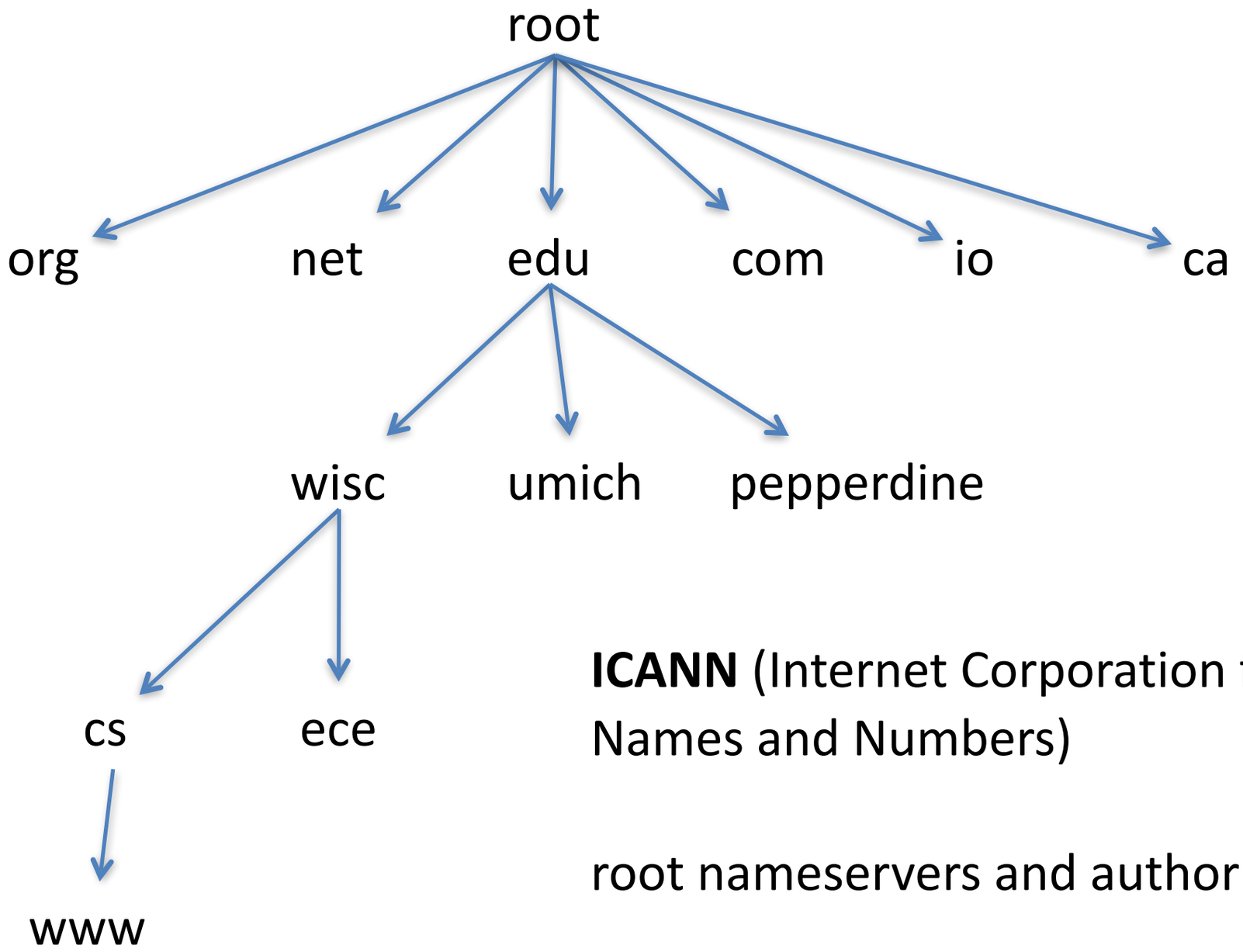
Domain Name	IP addresses
www.amazon.com	54.239.25.208
theverge.com	172.111.64.124
googlemail-smtp.l.google.com	74.125.193.16
hosted-cdn.statuspage.io	23.235.40.65
p05-calendars.icloud.com	17.172.100.13
print-gw.cs.wisc.edu	128.105.123.66

Which one is easier to remember?

Domain Name System (DNS)

translates domain names->IP addresses

Hierarchical domain name space



Top Level domains (TLD)

Second Level domains

ICANN (Internet Corporation for Assigned Names and Numbers)

root nameservers and authoritative nameservers

Zone: subtree

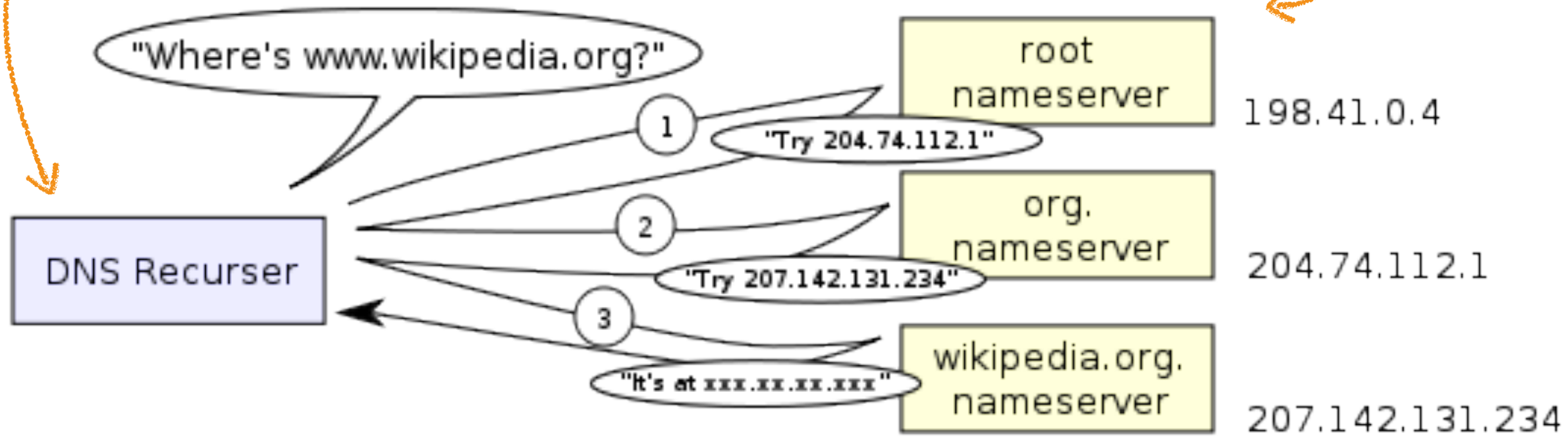
Name Servers

Recurser

Recursively hunts down an answer

Authoritative name servers

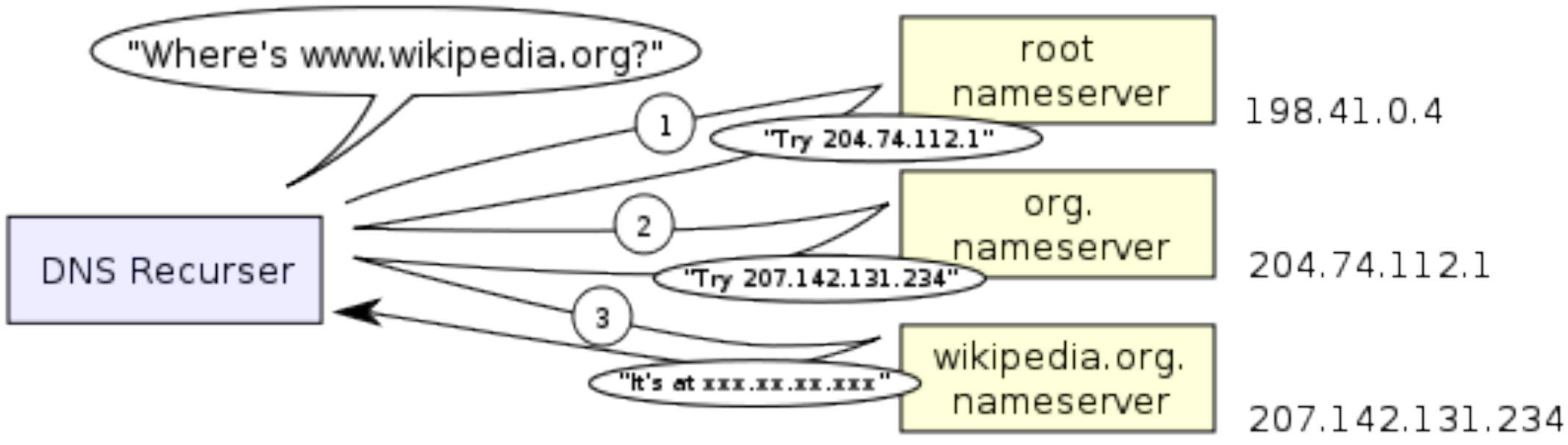
Programmed by an original source



[http://en.wikipedia.org/wiki/File:An_example_of_theoretical_DNS_recursion.svg]

Caching

- DNS servers will cache responses
  - Both negative and positive responses
  - Speeds up queries
  - Entries expire periodically. Time-to-live (TTL) set by data owner

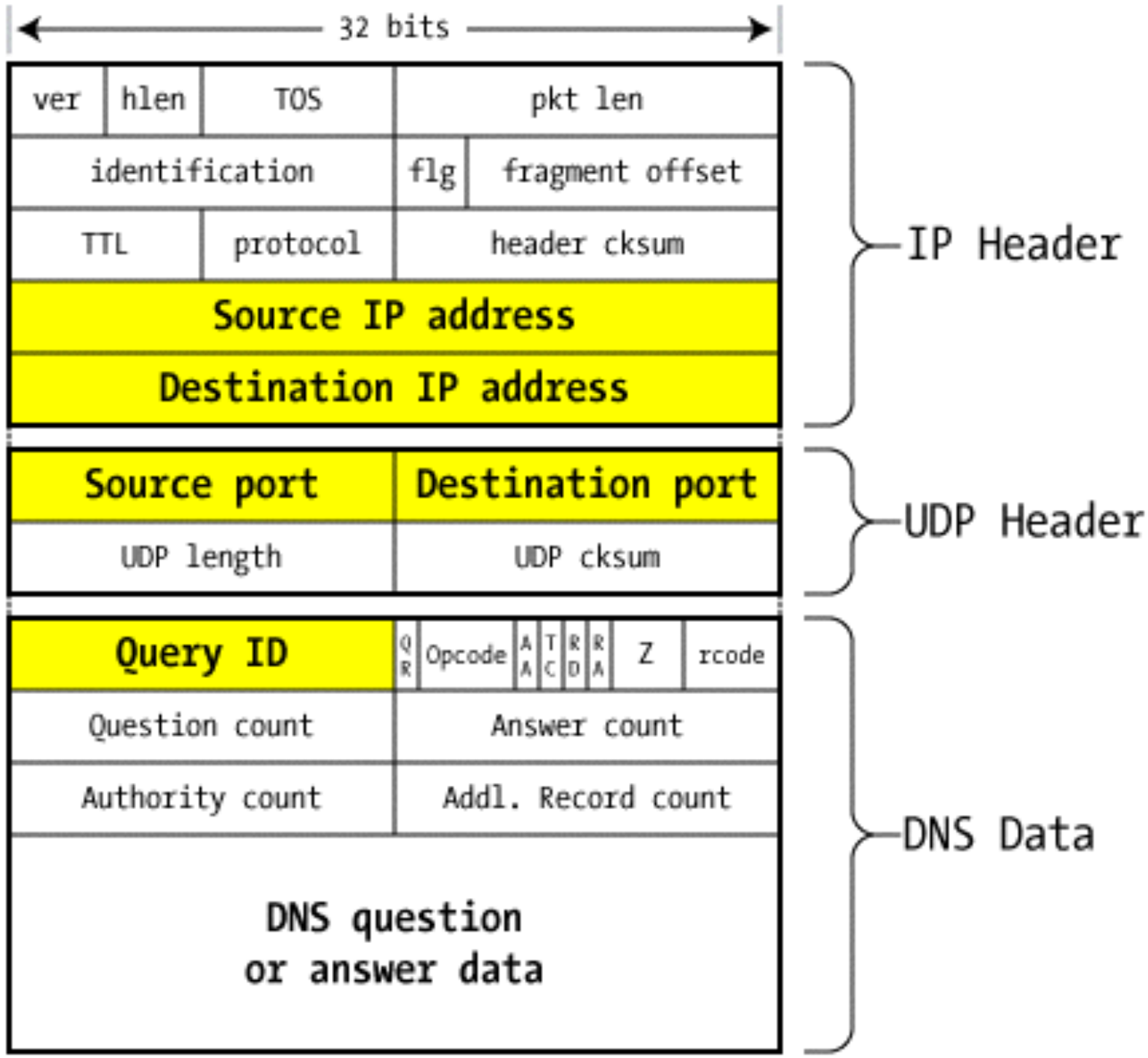


Example DNS query types

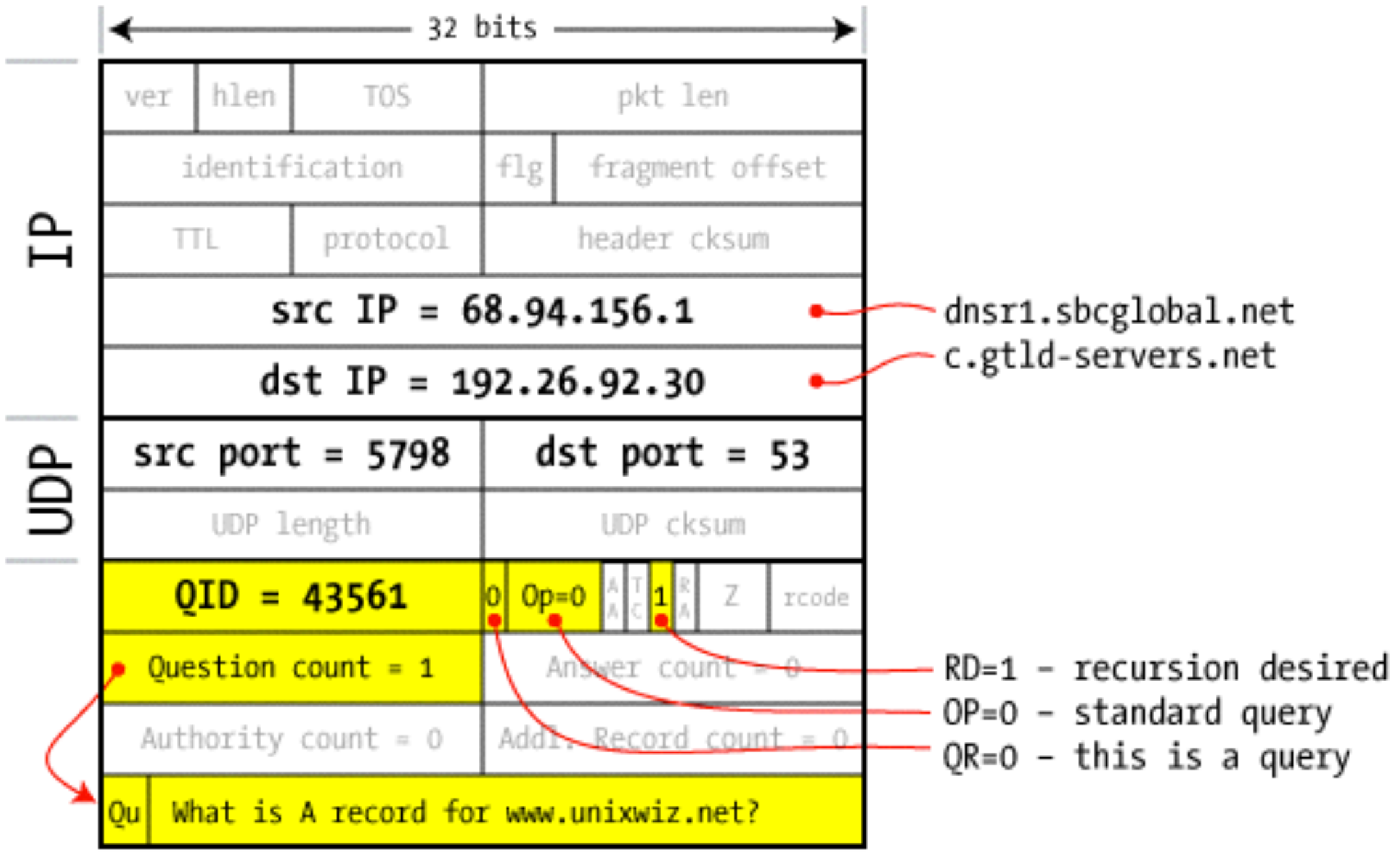
A	**IPv4 address**
AAAA	IPv6 address
NS	**name server**
TXT	human readable text
MX	mail exchange

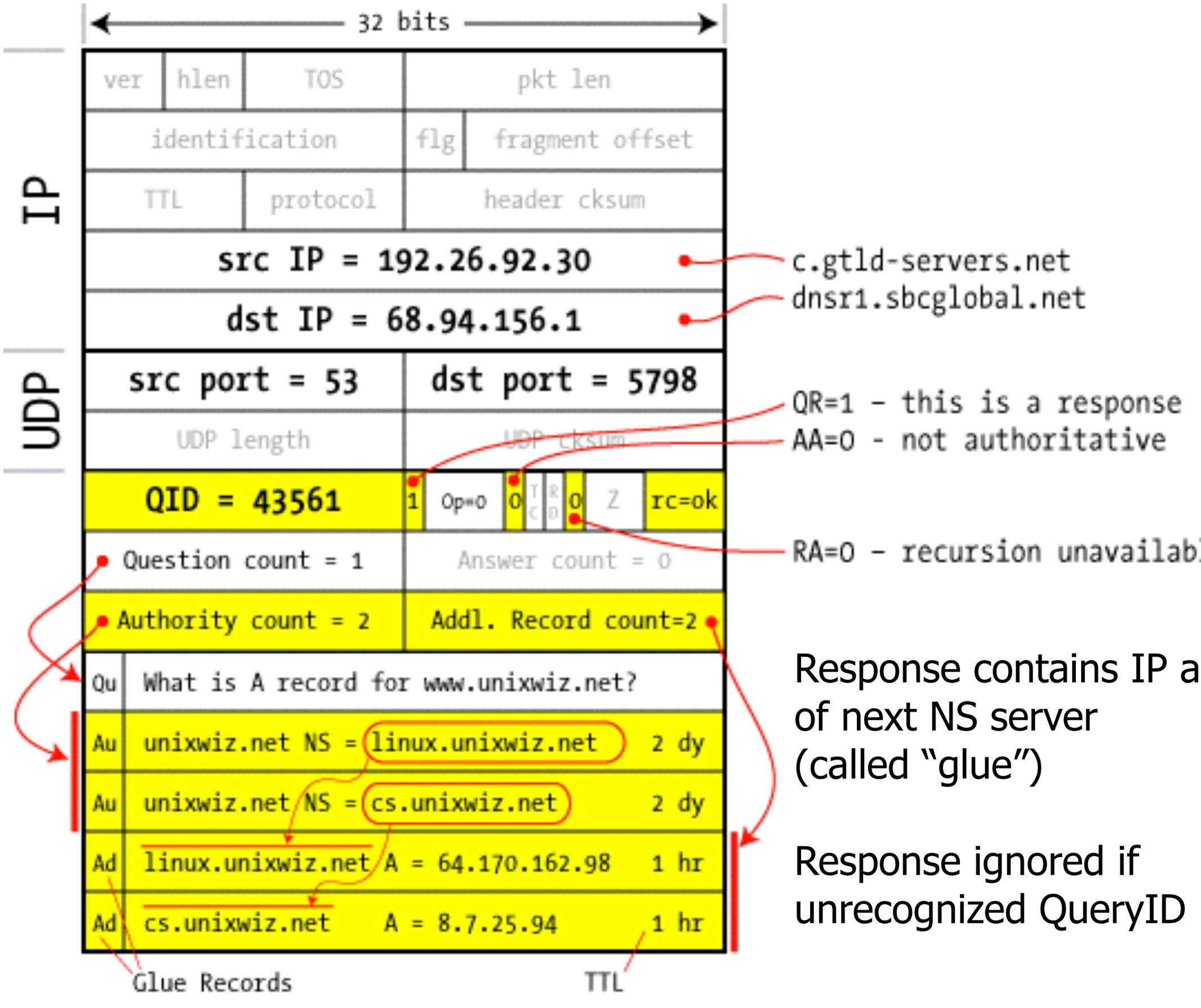
DNS packet on wire

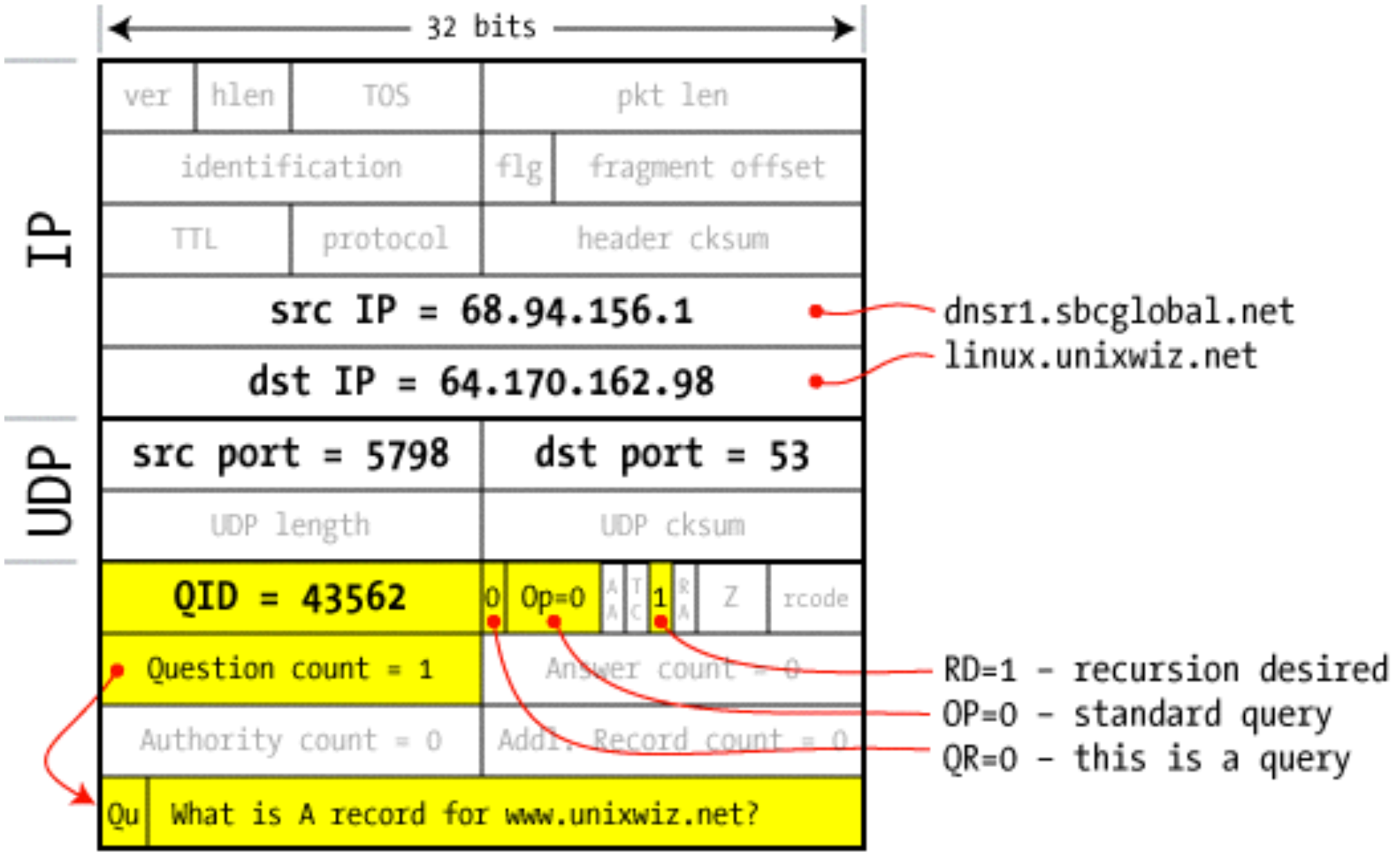
Query ID is 16-bit random value

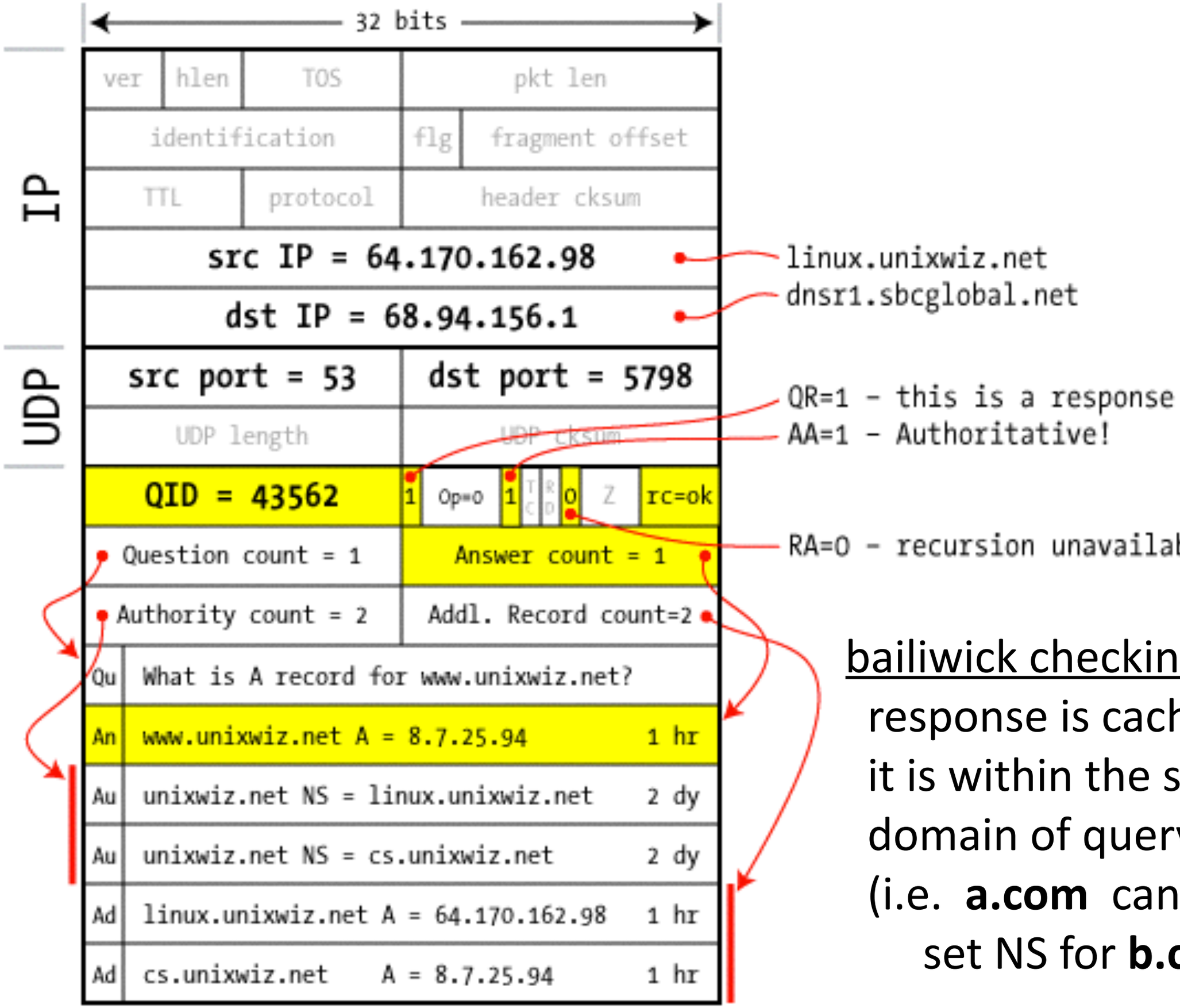


Query from resolver to NS




32 bits
IP
UDP
ver
hlen
TOS
pkt len
identification
flg
fragment offset
TTL
protocol
header cksum
src IP = 192.26.92.30
dst IP = 68.94.156.1
src port = 53
dst port = 5798
UDP length
UDP cksum
QID = 43561
1
Op=0
0
T C
R D
0
Z
rc=ok
Question count = 1
Answer count = 0
Authority count = 2
Addl. Record count=2
Qu
What is A record for www.unixwiz.net?
Au
unixwiz.net NS = linux.unixwiz.net
2 dy
Au
unixwiz.net NS = cs.unixwiz.net
2 dy
Ad
linux.unixwiz.net A = 64.170.162.98
1 hr
Ad
cs.unixwiz.net A = 8.7.25.94
1 hr
Glue Records
TTL
c.gtld-servers.net
dnsr1.sbcglobal.net
QR=1 - this is a response
AA=0 - not authoritative
RA=0 - recursion unavailable
Response contains IP addr
of next NS server
(called “glue”)
Response ignored if
unrecognized QueryID


32 bits
IP
ver
hlen
TOS
pkt len
identification
flg
fragment offset
TTL
protocol
header cksum
src IP = 68.94.156.1
dst IP = 64.170.162.98
dnsr1.sbcglobal.net
linux.unixwiz.net
UDP
src port = 5798
dst port = 53
UDP length
UDP cksum
QID = 43562
0
Op=0
AA
TC
1
RA
Z
rcode
Question count = 1
Answer count = 0
Authority count = 0
Addl. Record count = 0
Qu
What is A record for www.unixwiz.net?
RD=1 - recursion desired
OP=0 - standard query
QR=0 - this is a query



<u>bailiwick checking:</u>

response is cached if it is within the same domain of query (i.e. **a.com** cannot set NS for **b.com**)

DNS Security

- What security checks are in place?
  - Random query ID's to link responses to queries
  - Bailiwick checking (sanity check on response)
- No authentication
- Many things trust hostname↔IP mapping
  - Browser same-origin policy
  - URL address bar
  - Every application that accesses the internet

DNSsec

- Authenticated DNS protocol
- Used by TLDs :)
- But no one else :(

DNSstat zone information categories

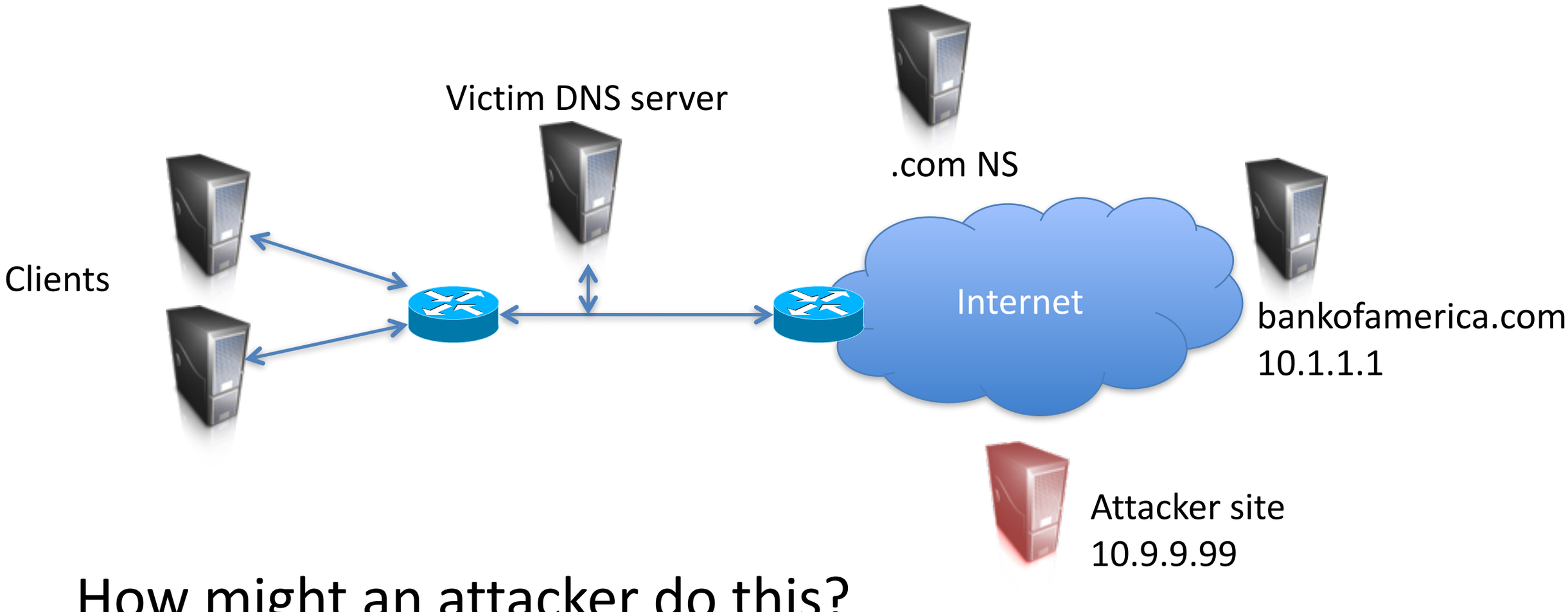
Category	Description	Total Domains	DNSSEC Enabled
internet2	Internet2 Members	267	26 (9.7%)
esnet	ESNet community	11	9 (81.8%)
ivyleague	The Ivy League	8	1 (12.5%)
nysernet	NYSERNet members	30	0 (0.0%)
gigapop	Internet2 GigaPoPs	20	3 (15.0%)
usnews_20	US News Top 20 universities	20	2 (10.0%)
times_hied_50	Times Higher Ed Top 50	50	8 (16.0%)
techcom	Top Tech Companies	53	5 (9.4%)
tld	Top Level Domains	1272	1111 (87.3%)
new_gtld	New GTLD	957	957 (100.0%)
cctld	Country-Code Top Level Domains	292	137 (46.9%)

[https://www.huque.com/app/dnsstat/] retrieved: April 6, 2016

What are obvious problems?

- Corrupted nameservers
- Intercept & manipulate requests (on-path active attacker)
- Other obvious problems?

DNS cache poisoning

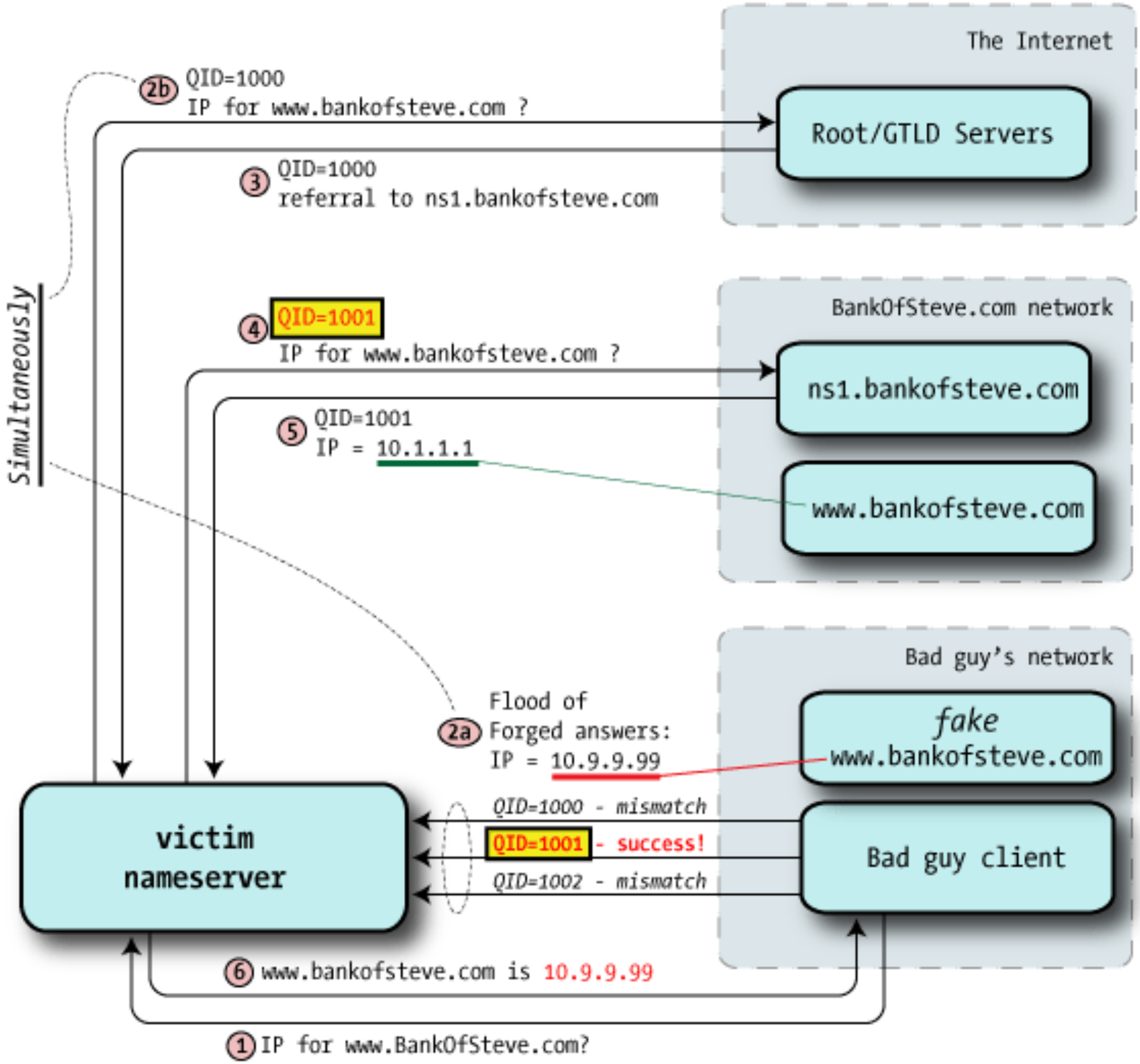


How might an attacker do this?

What security features must an attacker overcome?

- Packet spoofing ← Assume SRC port spoofing
- Guess UDP port ← Assume predictable UDP port
- Guess QID

think-*pair*-share

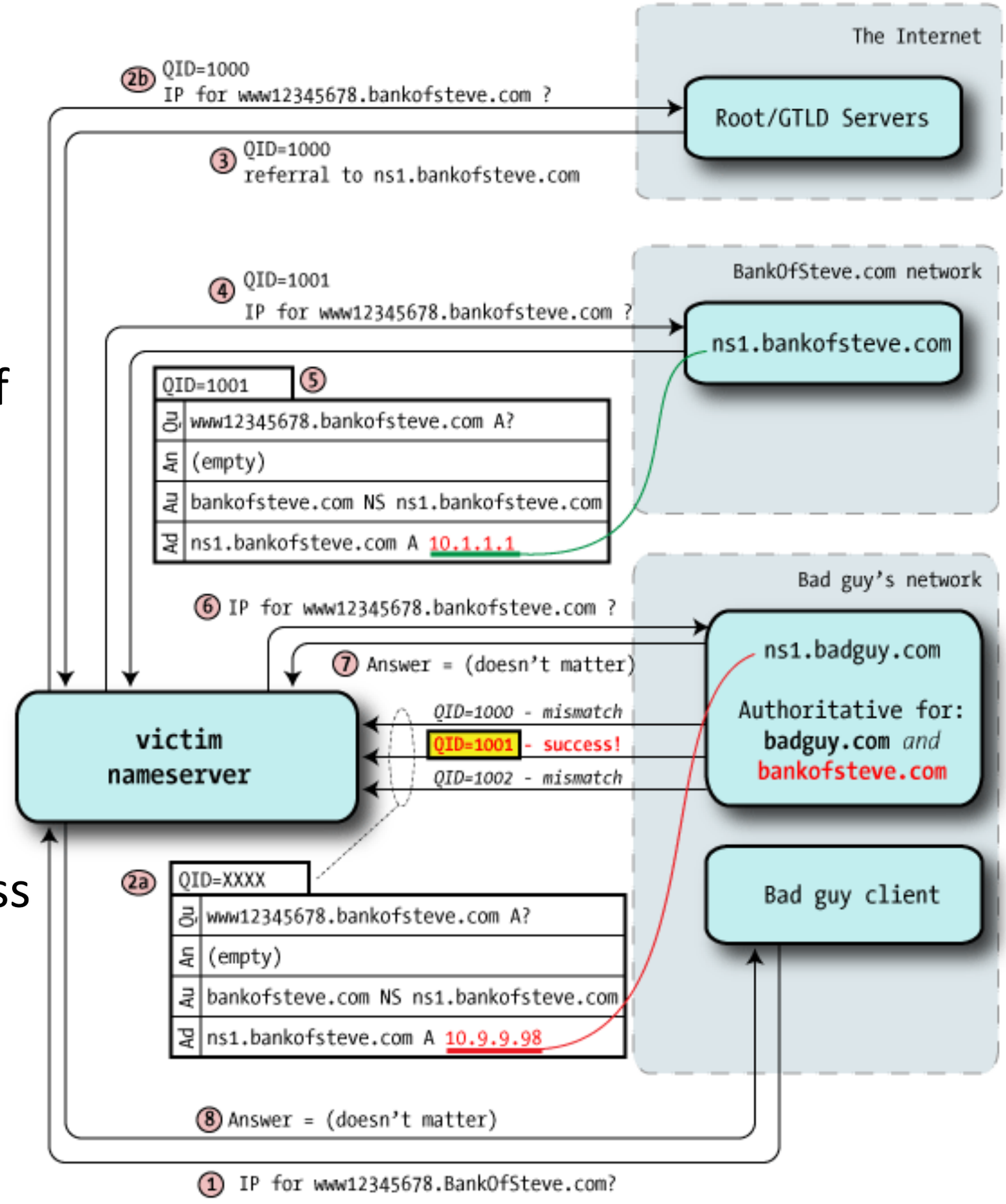

The Internet
Root/GTLD Servers
2b QID=1000
IP for www.bankofsteve.com ?
3 QID=1000
referral to ns1.bankofsteve.com
BankOfSteve.com network
4 QID=1001
IP for www.bankofsteve.com ?
ns1.bankofsteve.com
5 QID=1001
IP = 10.1.1.1
www.bankofsteve.com
Simultaneously
Bad guy's network
Flood of
2a Forged answers:
IP = 10.9.9.99
fake
www.bankofsteve.com
QID=1000 - mismatch
QID=1001 - success!
QID=1002 - mismatch
victim
nameserver
Bad guy client
6 www.bankofsteve.com is 10.9.9.99
1 IP for www.BankOfSteve.com?

Another idea:

- Poison cache for NS record instead
- Now can take over all of second level domain

How many tries does this require?

- Try 256 different QIDs
- Good chance of success



Brazilian Boletos Stolen Through DNS Cache Poisoning

Crooks compromise DNS resolution of local ISP network

Feb 12, 2015 14:13 GMT · By Ionut Ilascu

Cybercriminals in Brazil have resorted to a new method to steal the much coveted boletos, a nation-wide payment method, by poisoning the domain name system (DNS) entry used by a bank's website so that the IP address to the legitimate location point to a site controlled by the cybercriminals.

Boleto payments are highly popular in Brazil. They consist in a voucher generated by banks that can be used instead of payment cards. An expiration date is set for each of them, defining a time frame during which merchants can accept it.

When they expire, the customer can re-generate another one, with a different identification number, through online banking services.

When a website is accessed, its name is converted into its IP address by a DNS server maintained by the ISP (Internet Service Provider). If the DNS server is compromised, attackers can assign any website an address under their control, in order to point visitors to malicious content.

Defenses

- Query ID size is fixed at 16 bits
- Repeat each query with fresh Query ID
  - Doubles the space
- Randomize UDP ports
- DNSsec
  - Cryptographically sign DNS responses, verify via chain of trust from roots on down

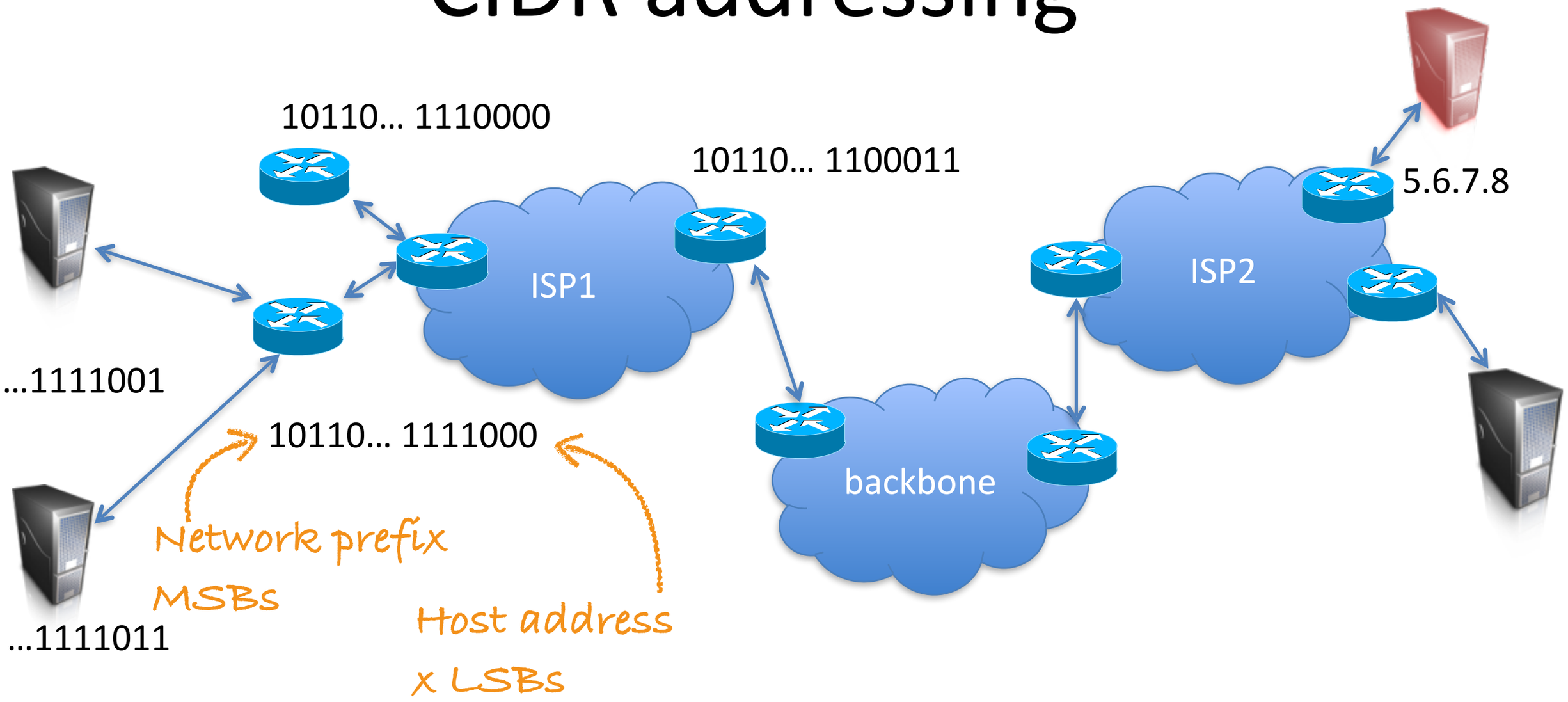
- Other problems?

Phishing is common problem

- Typo squatting:
  - www.LansdEnd.com
  - www.goggle.com
  - secure.bank0fAmerica.com
  - wíkipedia.org
- Phishing attacks
  - Trick users into thinking a malicious domain name is the real one

ip routing

CIDR addressing

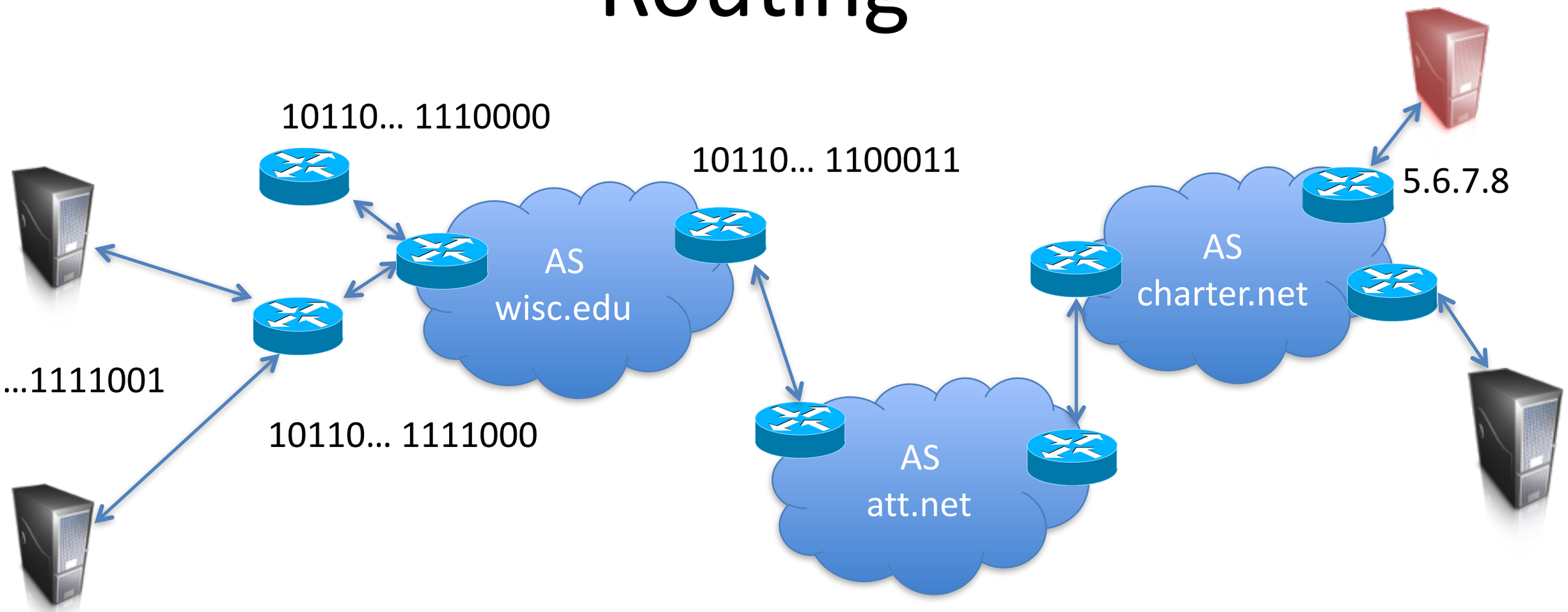


Classless inter-domain routing (CIDR)

Prefixes used to setup hierarchical routing:

- An organization assigned a.b.c.d/x
- It manages addresses prefixed by a.b.c.d/x

Routing



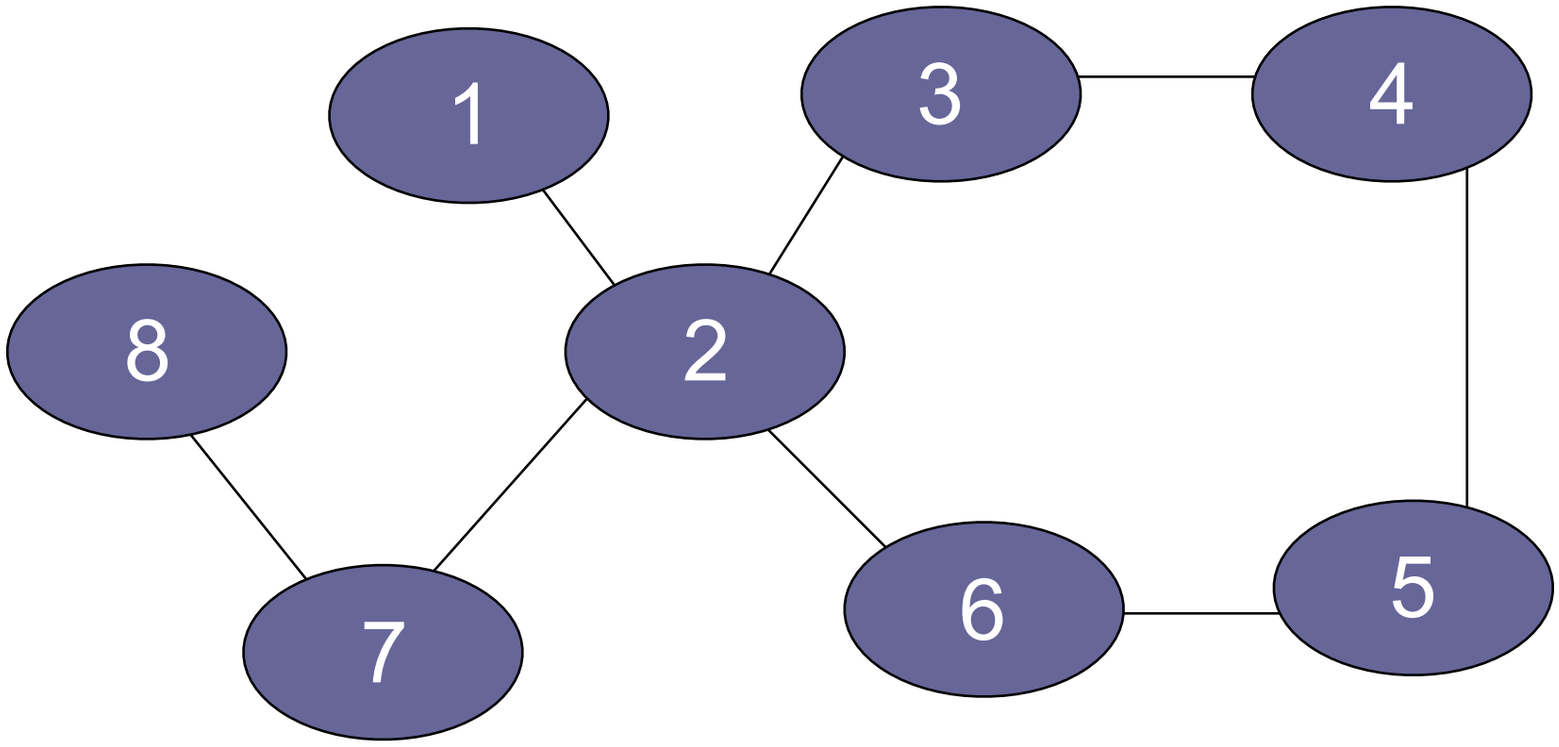
Autonomous systems (AS) are organizational building blocks

- Collection of IP prefixes under single routing policy
- wisc.edu

Within AS, might use RIP (Routing Information Protocol)

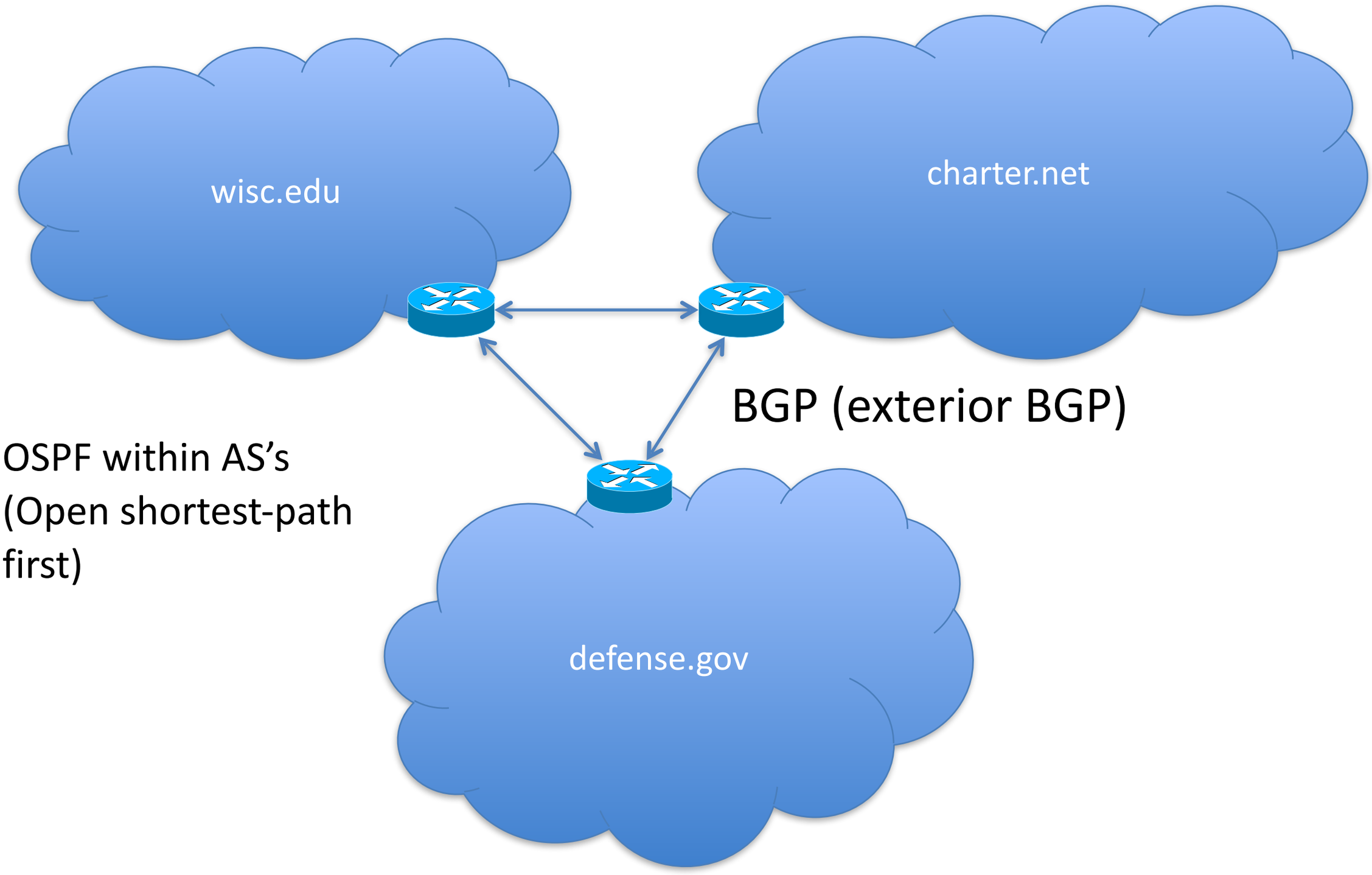
Between AS, use BGP (Border Gateway Protocol)

AS Categories



- **Stub:** connected to only on other AS
- **Multi-homed:** connected to multiple other AS
- **Transit:** routes traffic through it's AS for other AS's

BGP and routing

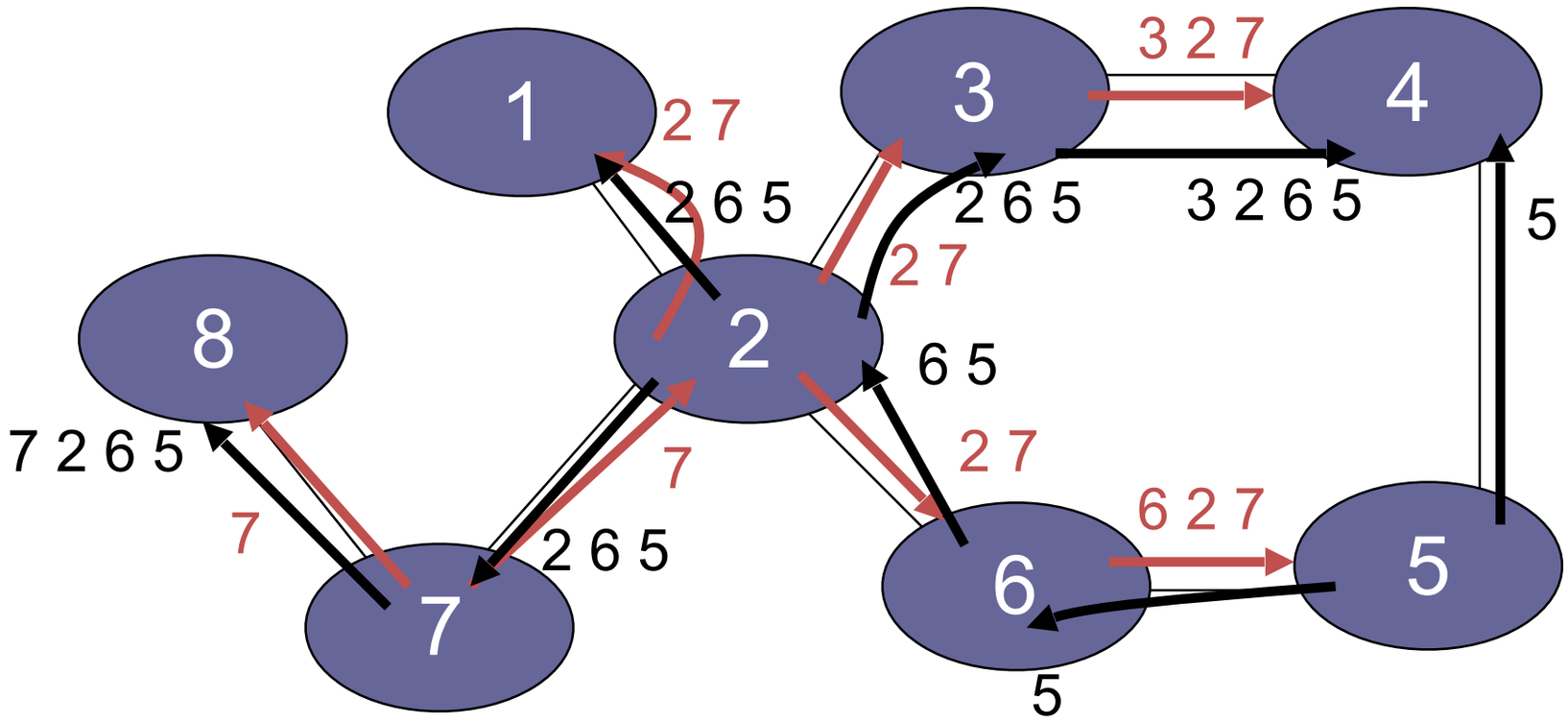


Border Gateway Protocol (BGP)

- Policy-based routing
  - AS can set policy about how to route
    - economic, security, political considerations
- BGP routers use TCP connections to transmit routing information
- Iterative announcement of routes

BGP example

[D. Wetherall]



- 2, 7, 3, 6 are Transit AS
- 8, 1 are Stub AS
- 4,5 multihomed AS
- Algorithm seems to work OK in practice
  - BGP does not respond well to frequent node outages

- 2008: Pakistan attempts to block YouTube
  - youtube is 208.65.152.0/22
  - youtube.com = 208.65.153.238
- Pakistan ISP advertises 208.65.153.0/24 via BGP
  - more specific, prefix hijacking
- Internet thinks youtube.com is in Pakistan
- Outage resolved in 2 hours…

IP hijacking

- BGP unauthenticated
  - Anyone can advertise any routes
  - False routes will be propagated
- This allows IP hijacking
  - AS announces it originates a prefix it shouldn’t
  - AS announces it has shorter path to a prefix
  - AS announces more specific prefix

recap

* DNS
  / DNS insecurity
  / DNS cache poisoning
  / Typosquatting

* CIDR, BGP
  / IP route hijacking

* Exit slips
  / 1 thing you learned
  / 1 thing you didn't understand