

US Congress Rules Huawei a 'Security Threat'

Posted by **timothy** on Monday October 08, @07:06AM
from the q-in-tel-is-totally-a-different-story dept.



dgharmon writes with the lead from a story in the Brisbane Time:

"Chinese telecom company Huawei poses a security threat to the United States and should be barred from US contracts and acquisitions, a yearlong congressional investigation has concluded. A draft of a report by the House Intelligence Committee said Huawei and another Chinese telecom, ZTE, 'cannot be trusted' to be free of influence from Beijing and could be used to undermine U.S.. security."

Entire Cities In World of Warcraft Dead, Hack Suspected

Posted by **timothy** on Sunday October 07, @05:40PM
from the just-some-reamde-plotlines-nothing-to-worry-about dept.



hypnosec writes

"Entire cities in the World of Warcraft have been destroyed with no one spared, not even the NPCs. About 13:00 GMT, forums on WOW started getting the first comments from users regarding players and NPCs dying on the Ragnaros-EU realm in Orgrimmar. Users of the online game started reporting that Draenor had a similar sight to offer. Some of the other realms where this was reported include Tarren Mill, and Twisting Nether."

DNS and BGP



CS642: Computer Security

Professor Ristenpart

<http://www.cs.wisc.edu/~rist/>

rist at cs dot wisc dot edu

DNS and BGP



DNS

Attacking the DNS system

BGP

BGP attacks

Defense mechanisms

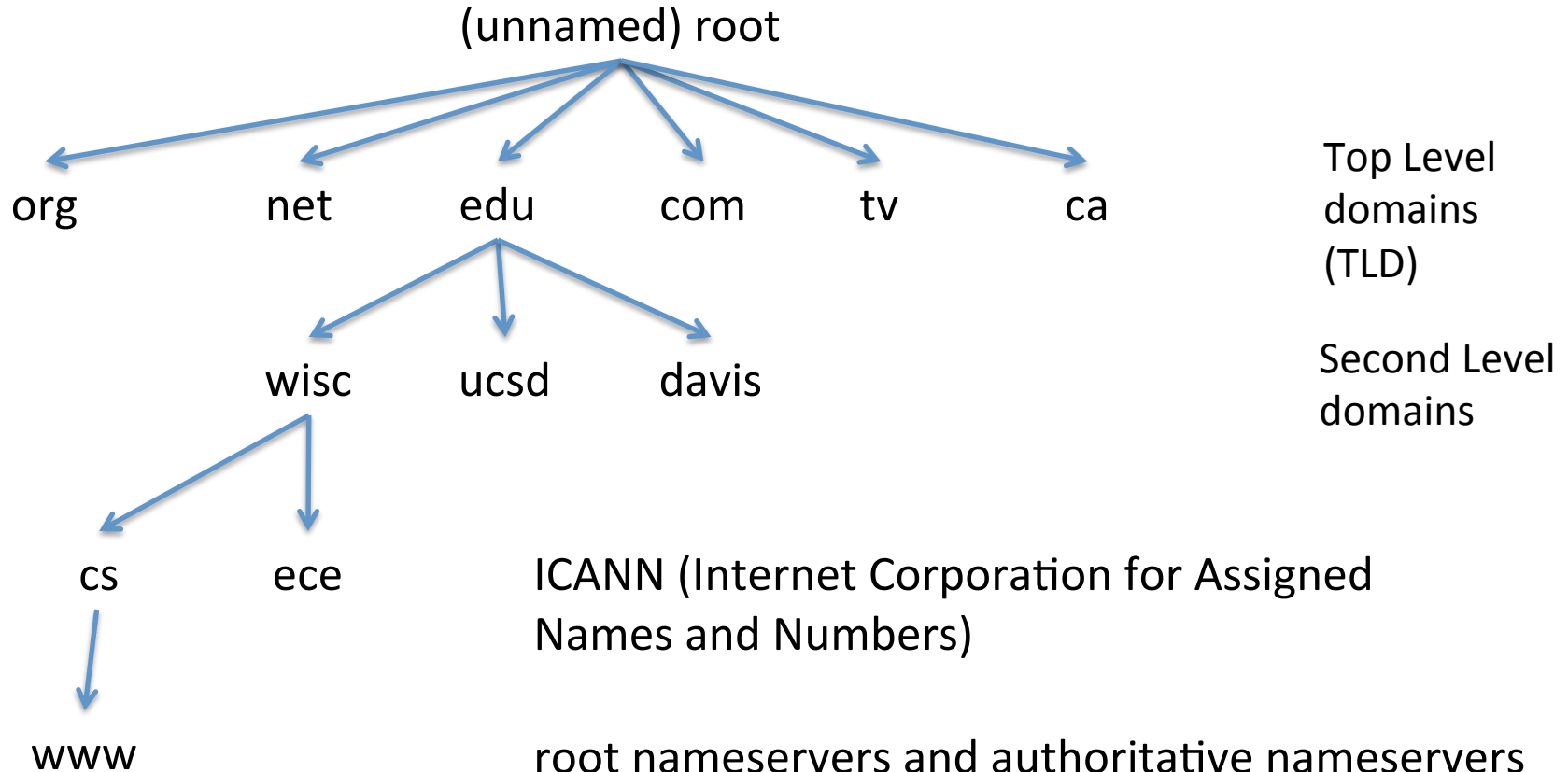
128.105.5.31

We don't want to have to remember IP addresses

```
[rist@seclab1] (17)$ head hosts
#
#      Wisconsin CS Local Host Table
#
127.0.0.1      localhost
128.105.6.39   smtp.cs.wisc.edu smtp
128.105.6.40   spam.cs.wisc.edu spam spam-test
128.105.6.42   spam.cs.wisc.edu spam spam-test
128.105.6.38   spam.cs.wisc.edu spam spam-test
128.105.1.1    ge-5-1.cisco-border1.cs.wisc.edu ge-5-1.cisco-border1
128.105.1.2    ge-1-2.cisco1.cs.wisc.edu ge-1-2.cisco1
[rist@seclab1] (18)$ █
```

Early days of ARPANET: manually managed hosts.txt served from single computer at SRI

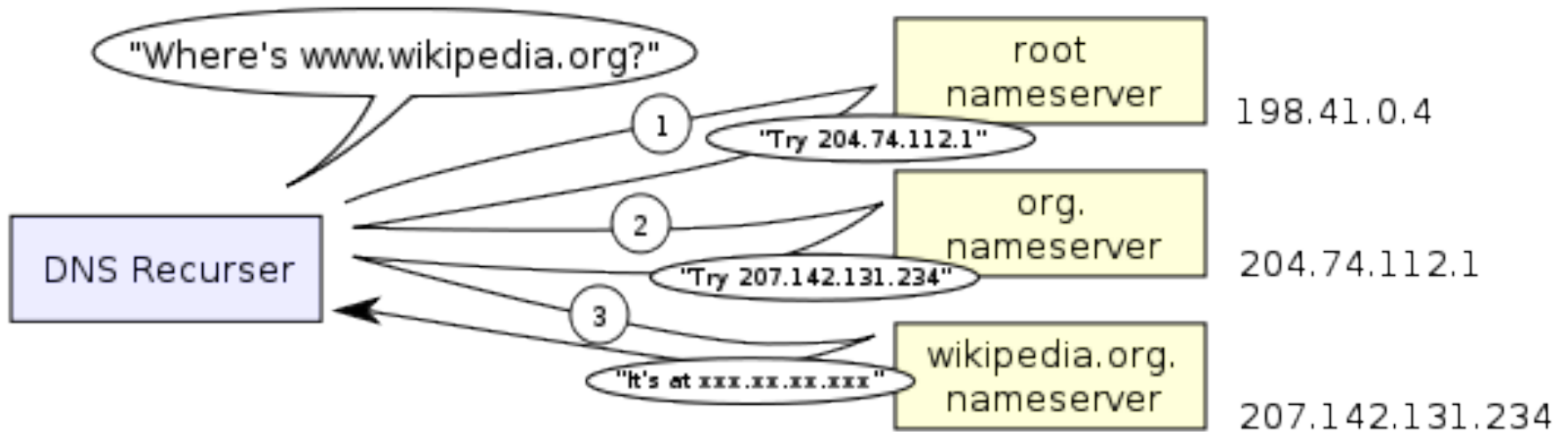
Heirarchical domain name space



max 63
characters

Zone: subtree

Resolving names



From

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

Example DNS query types

A	address (get me an IPv4 address)
AAAA	IPv6 address
NS	name server
TXT	human readable text, has been used for some encryption mechanisms
MX	mail exchange

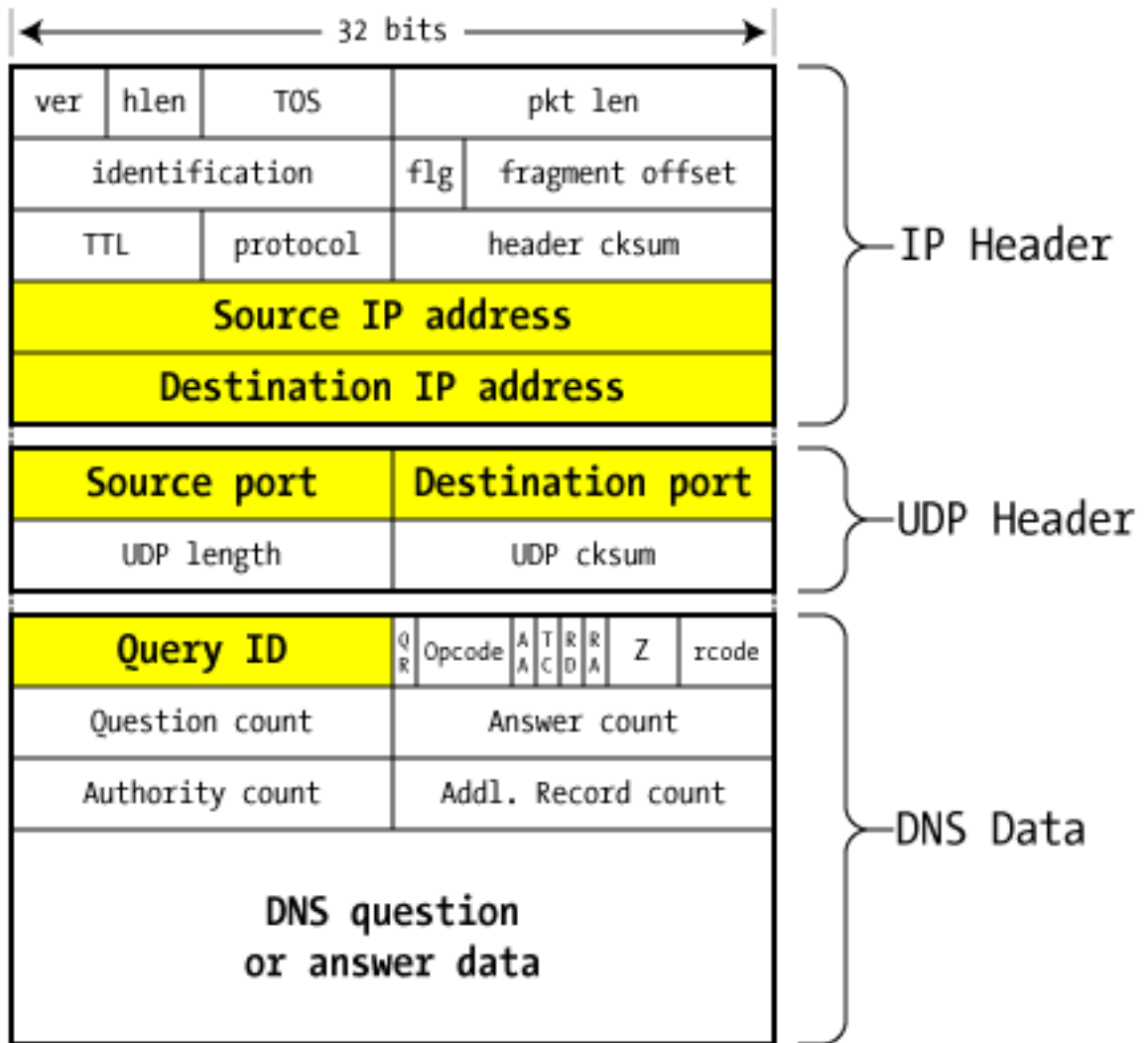
Caching

- DNS servers will cache responses
 - Both negative and positive responses
 - Speeds up queries
 - periodically times out. TTL set by data owner

DNS packet on wire

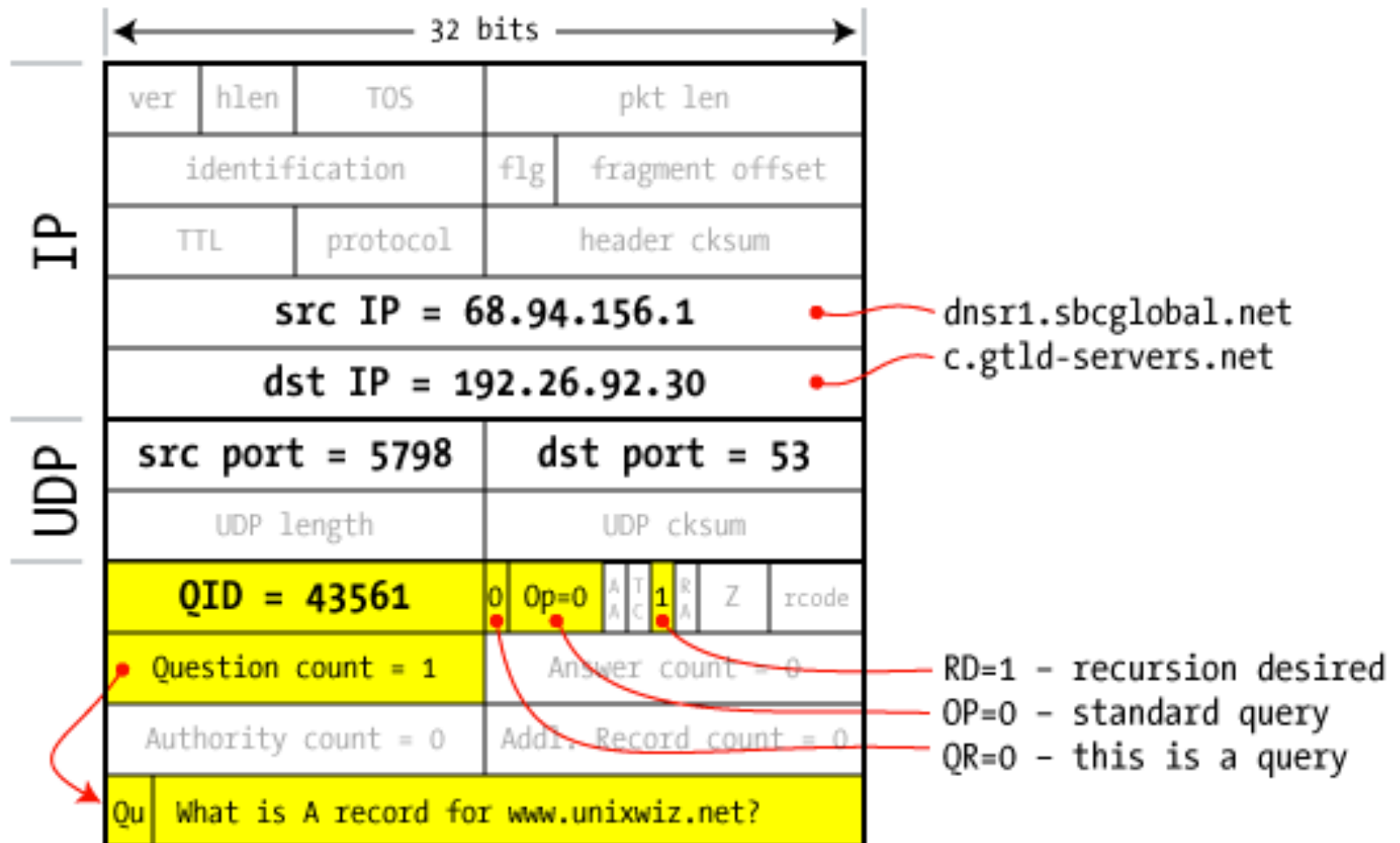
Query ID is 16-bit random value

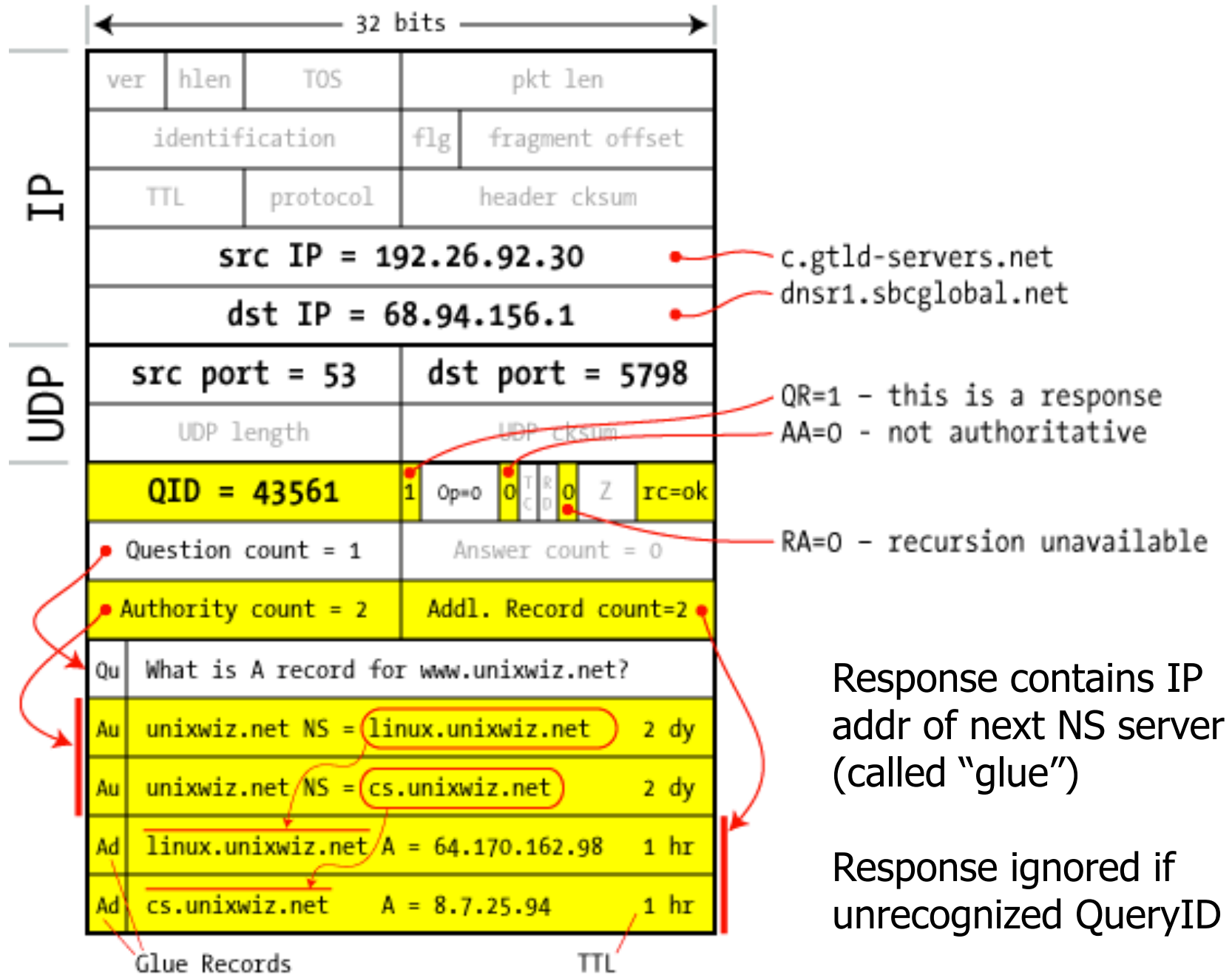
We'll walk through the example from Friedl's document

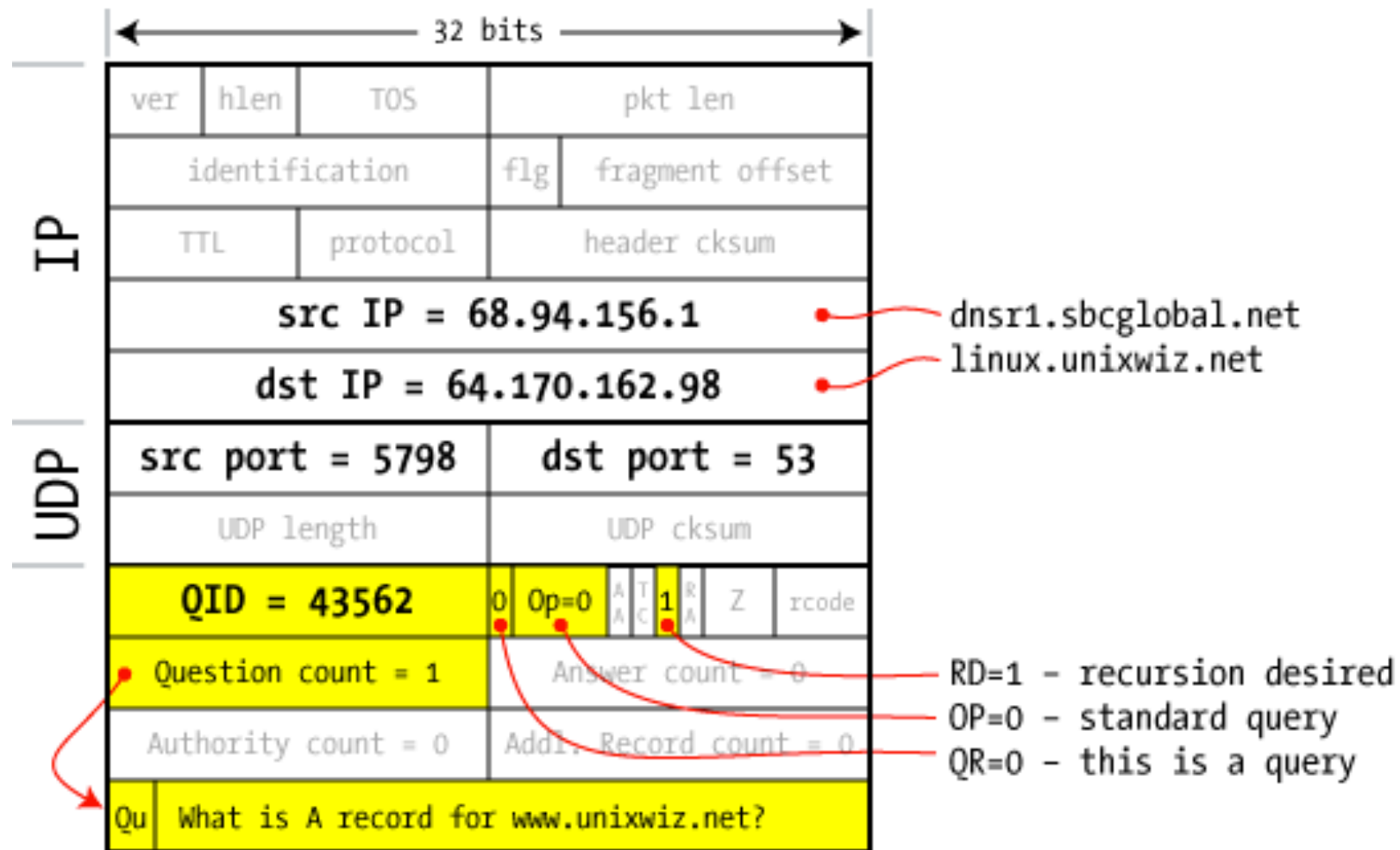


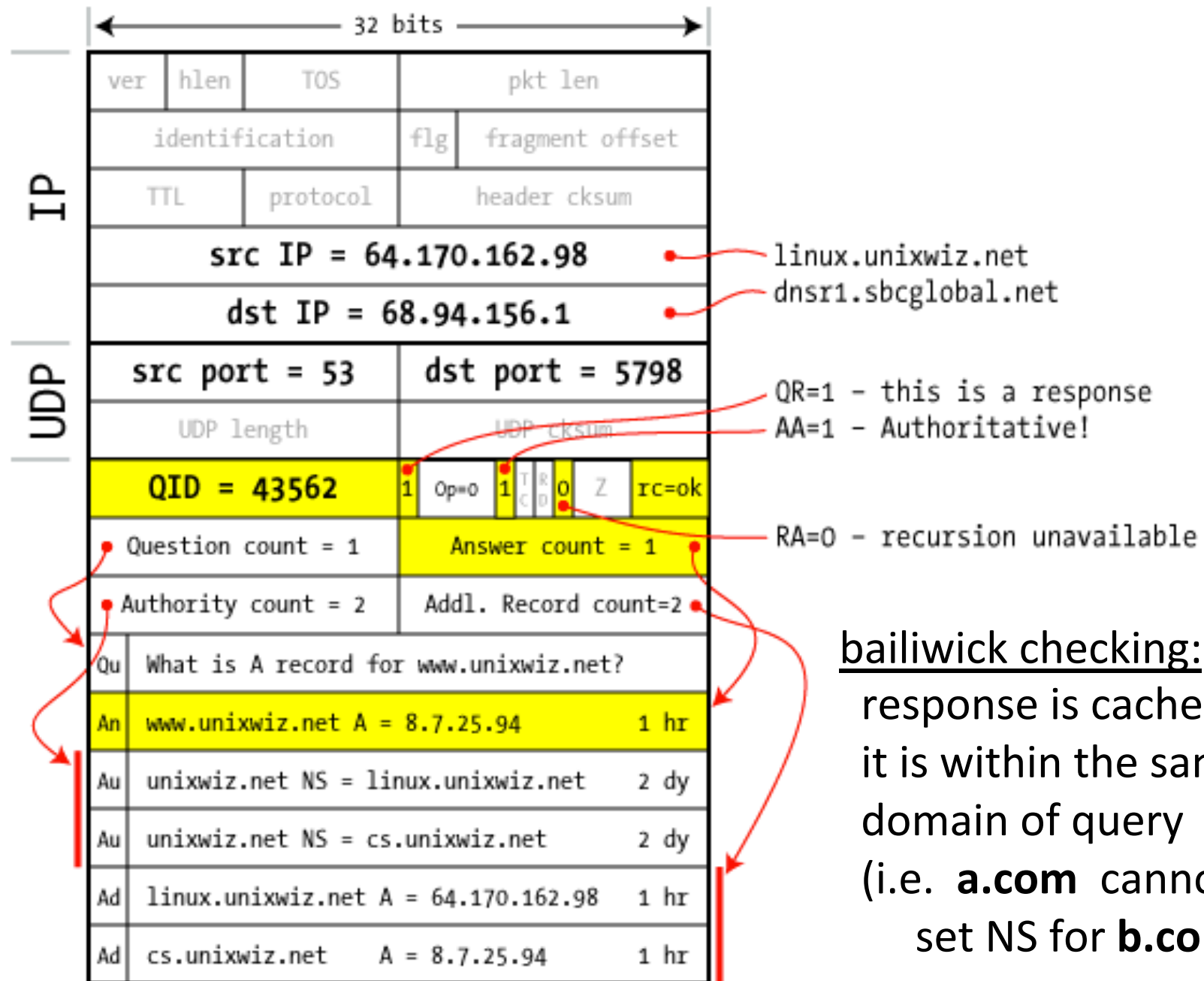
From Friedl explanation of DNS cache poisoning, as are following diagrams

Query from resolver to NS









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

Here we go again...

- What security checks are in place?
 - Random query ID's to link responses to queries
 - Bailiwick checking (sanity check on response)
- No authentication
 - DNSsec is supposed to fix this but no one uses it yet
- Many things trust hostname to IP mapping
 - Browser same-origin policy
 - URL address bar

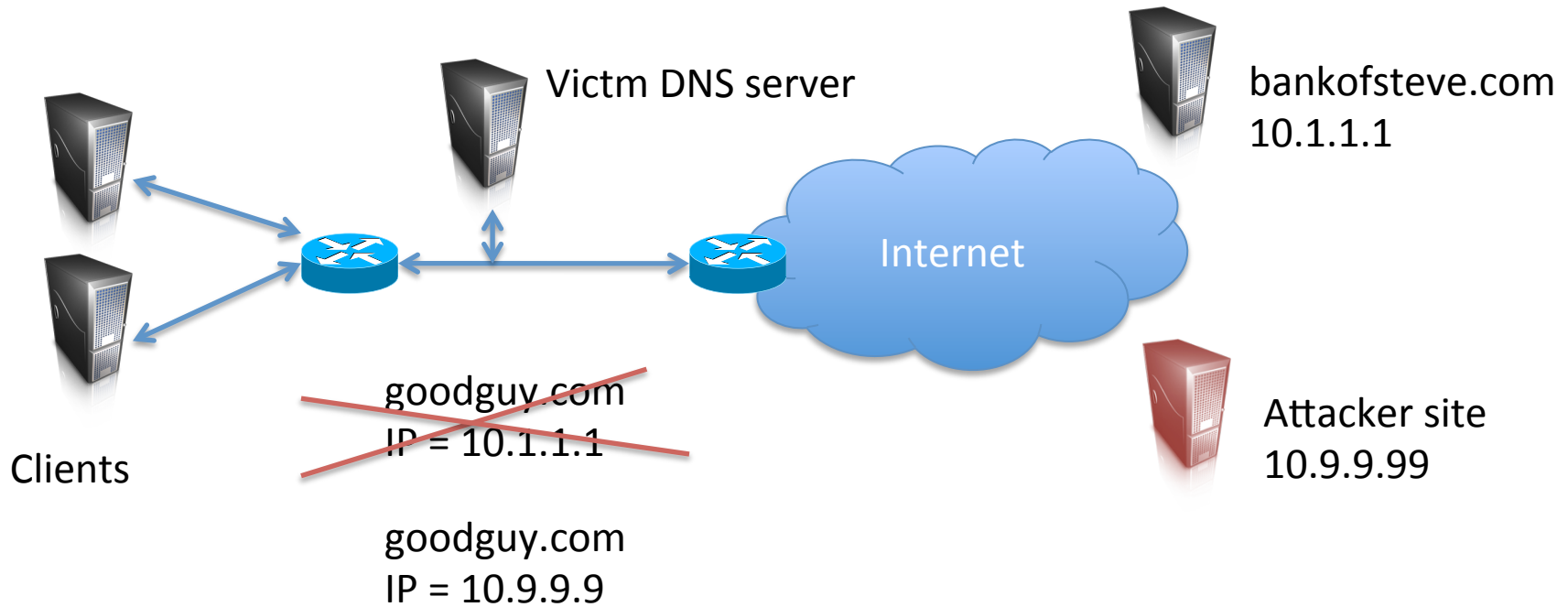
What are clear problems?

- Corrupted nameservers
- Intercept & manipulate requests
 - BGP route hijacking (stay tuned)
- Other obvious issues?

DDoS against DNS

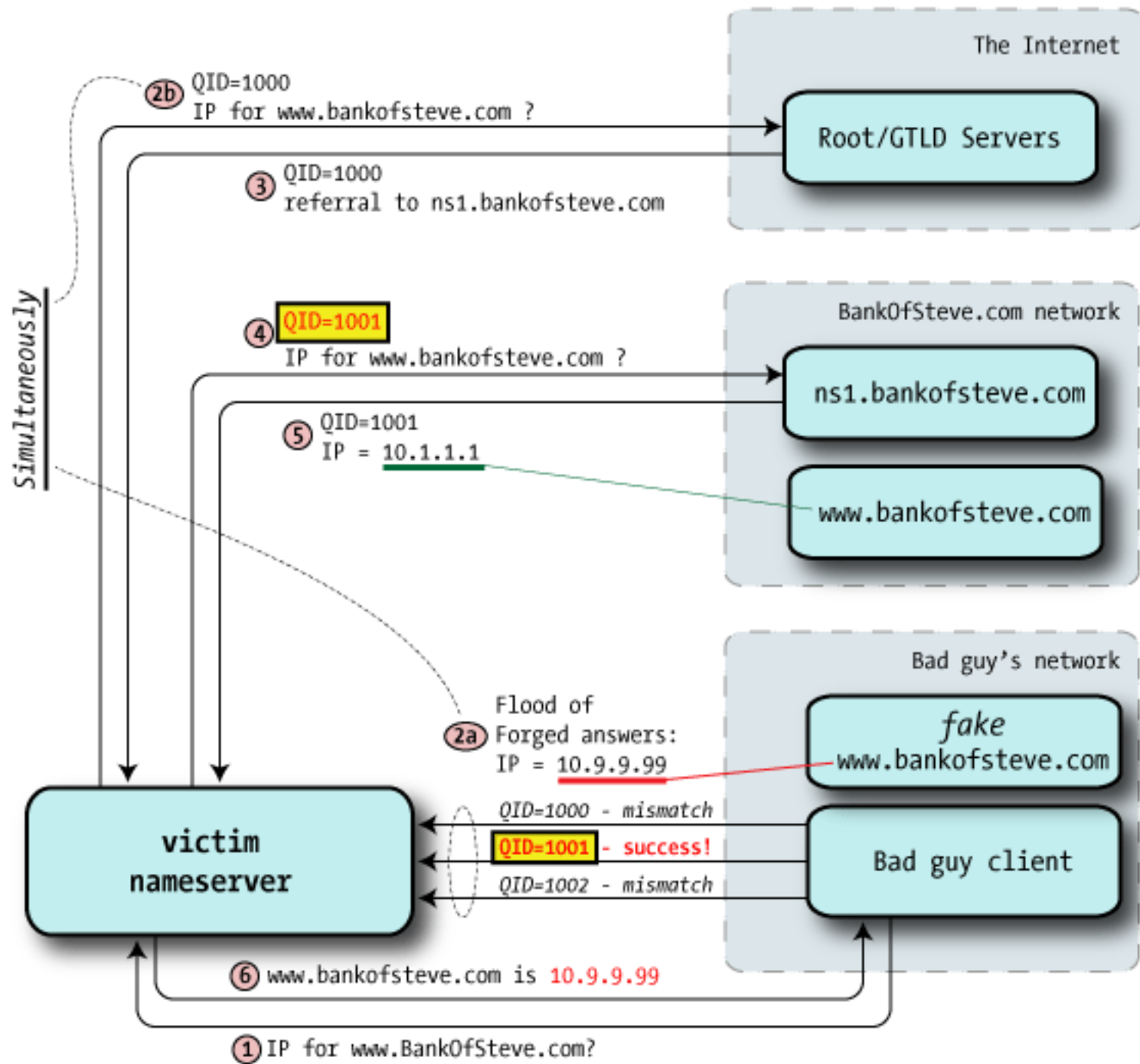
- Denial of Service
 - take down DNS server, clients can't use Internet
 - Feb 6, 2007 attack against 6 of 13 root servers:
 - 2 suffered very badly
 - Others experienced heavy traffic
- DoD purportedly has interesting response:
 - “In the event of a massive cyberattack against the country that was perceived as originating from a foreign source, the United States would consider launching a counterattack or bombing the source of the cyberattack, Hall said. But he noted the preferred route would be warning the source to shut down the attack before a military response.”
 - http://www.computerworld.com/s/article/9010921/RSA_U.S._cyber_counterattack_Bomb_one_way_or_the_other

DNS cache poisoning



How might an attacker do this?

Assume DNS server uses predictable UDP port

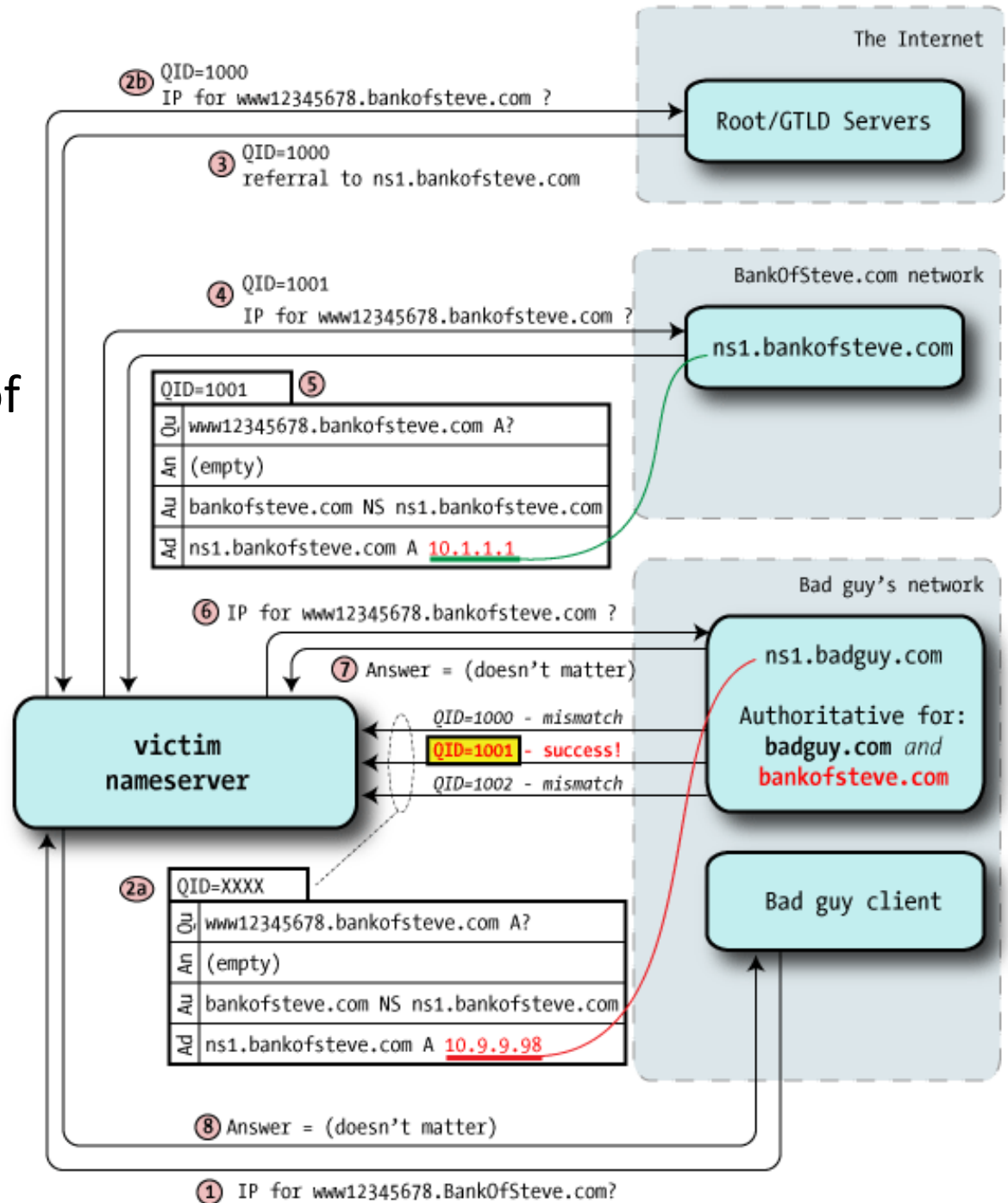


Another idea:

- 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
- Do about 256 attempts



Does happen in the wild

HD Moore pwned with his own DNS exploit, vulnerable AT&T DNS servers to blame

By Dancho Danchev | July 30, 2008, 8:08am PDT

Summary: *A week after |)ruid and HD Moore release part 2 of DNS exploit, HD Moore's company BreakingPoint has suffered a traffic redirection to a rogue Google site, thanks to the already poisoned cache at AT&T servers to which his company was forwarding DNS traffic : "It happened on Tuesday morning, when Moore's company, BreakingPoint had some [...]*

<http://www.zdnet.com/blog/security/hd-moore-pwned-with-his-own-dns-exploit-vulnerable-at-t-dns-servers-to-blame/1608?tag=content;siu-container>

Defenses

- Query ID size is fixed at 16 bits
- Repeat each query with fresh Query ID
 - Doubles the space
- Randomize UDP ports
 - Dan Bernstein's DJBDNS did this already
 - Now other implementations do, too
- DNSsec
 - Cryptographically sign DNS responses, verify via chain of trust from roots on down

Phishing is more common

- Typo squatting:
 - www.ca.wisc.edu
 - www.goggle.com
- Other shenanigans:
 - [www.badguy.com/\(256 characters of filler\)/www.google.com](http://www.badguy.com/(256 characters of filler)/www.google.com)
- Phishing attacks
 - These just trick users into thinking a malicious domain name is the real one



GOOGLE



As our thanks to you, our visitors,
please select a ***Free*** gift!

Free [Apple iPad 2[©]](#) . ***Free*** [Apple iPhone 4S[©]](#)

Apple iPad 2



Claim FREE gift

Apple iPhone 4S





Claim FREE gift

Other abuses, so-called DNS pharming

First case of "drive-by pharming" identified in the wild

By [Ellen Messmer](#), Network World

January 22, 2008 02:24 PM ET

 9 Comments  Print

 Like  1

 +1  0

The theory is now a reality. [Symantec](#) reported Tuesday that drive-by pharming, in which a hacker changes the DNS settings on a customer's broadband [router](#) or [wireless](#) access point and directs the link to a fraudulent Web site, has been [observed](#) in the wild.

SEO Via DNS "Piggybacking"

Posted by samzenpus on Wednesday October 12, @04:03PM
from the slip-in-there dept.



An anonymous reader writes

"There is an interesting story over at the SANS Internet Storm Center that shows details on about 50 organizations that have had new machine names added to their DNS zone information. These were then pointed to sites used to [boost the search engine cred](#) of pharma, personals, and porn sites. If you outsource your DNS, how would you ever catch something like this?"

Read the **67** comments



fraud seo it

DNS piggybacking

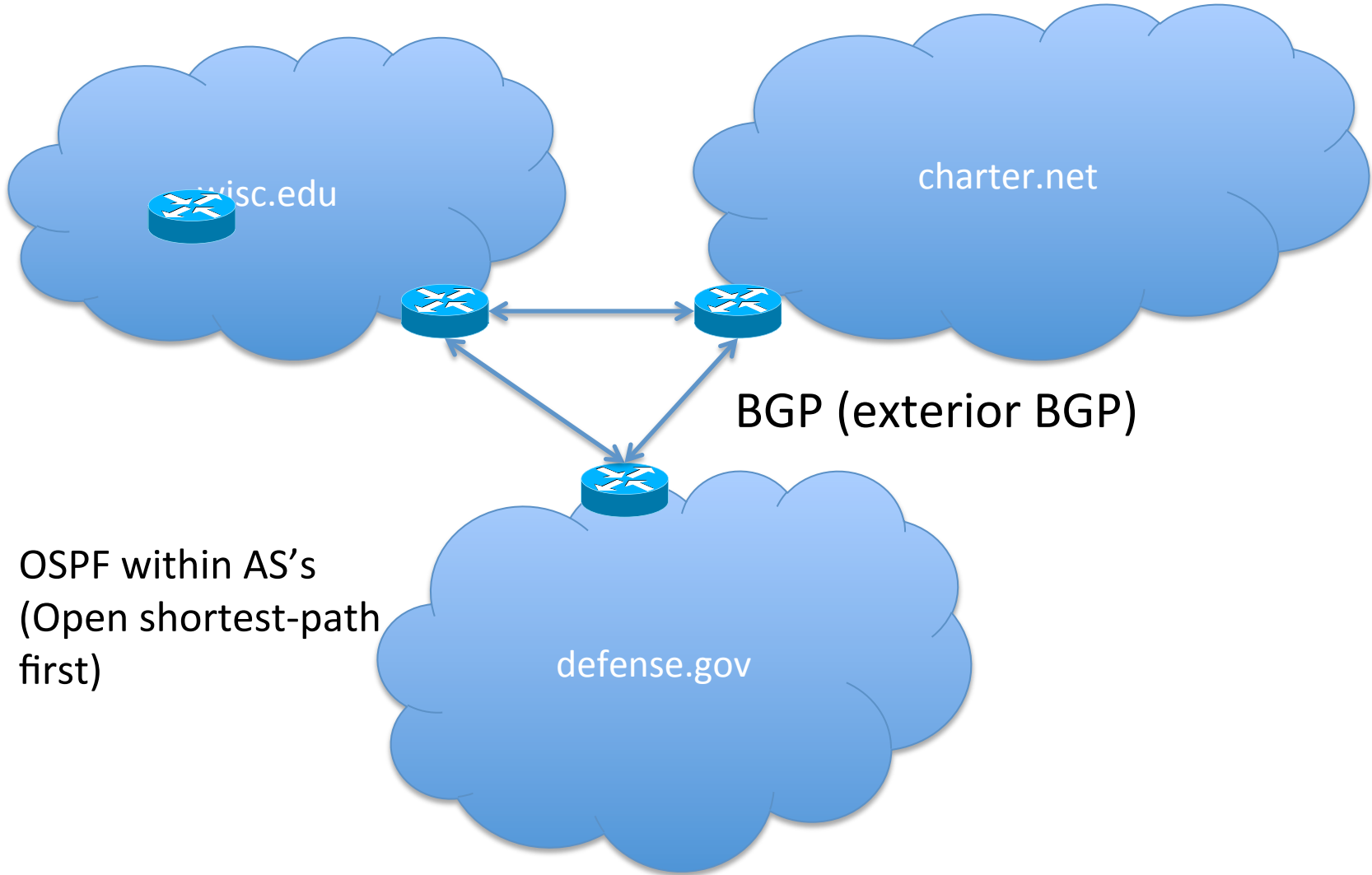
buy-cialis.sacmetrofire.ca.gov			
buy-viagra.sacmetrofire.ca.gov			
drugs.sacmetrofire.ca.gov	74.220.215.210	www.sacmetrofire.ca.gov	66.147.240.176
mgdrugs.sacmetrofire.ca.gov			
rxdrugs.sacmetrofire.ca.gov			

From <https://isc.sans.edu/diary/What+s+In+A+Name+/11770>

Attackers maliciously added extra domain lower level domain names to valid domain name

This is helpful for search engine optimization

BGP and routing

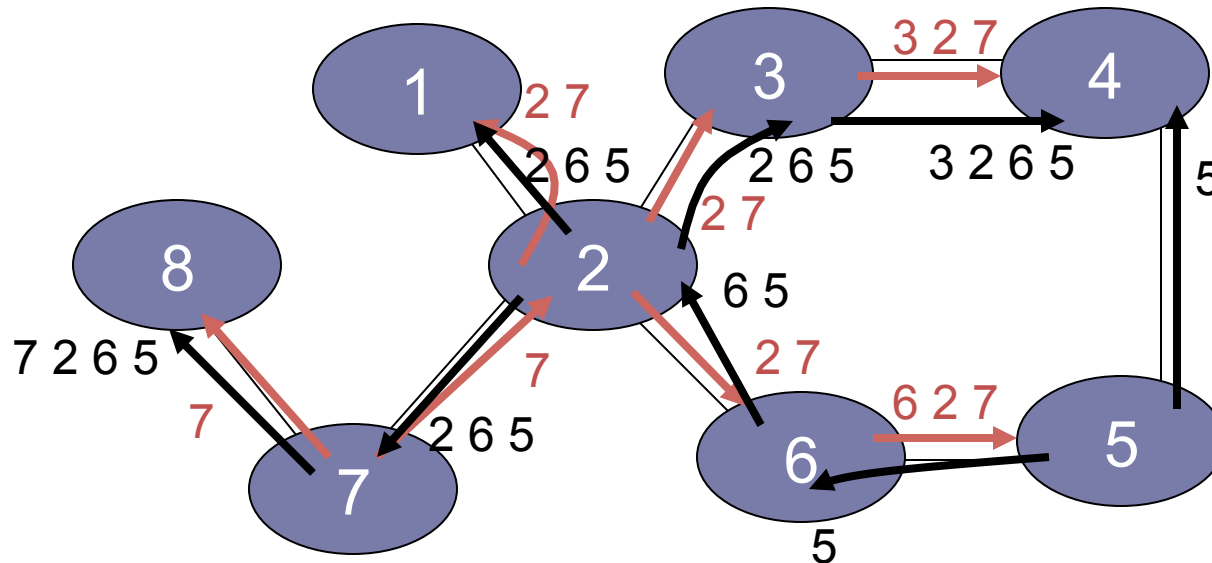


BGP

- 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 is does not respond well to frequent node outages

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

Malicious or misconfigurations?

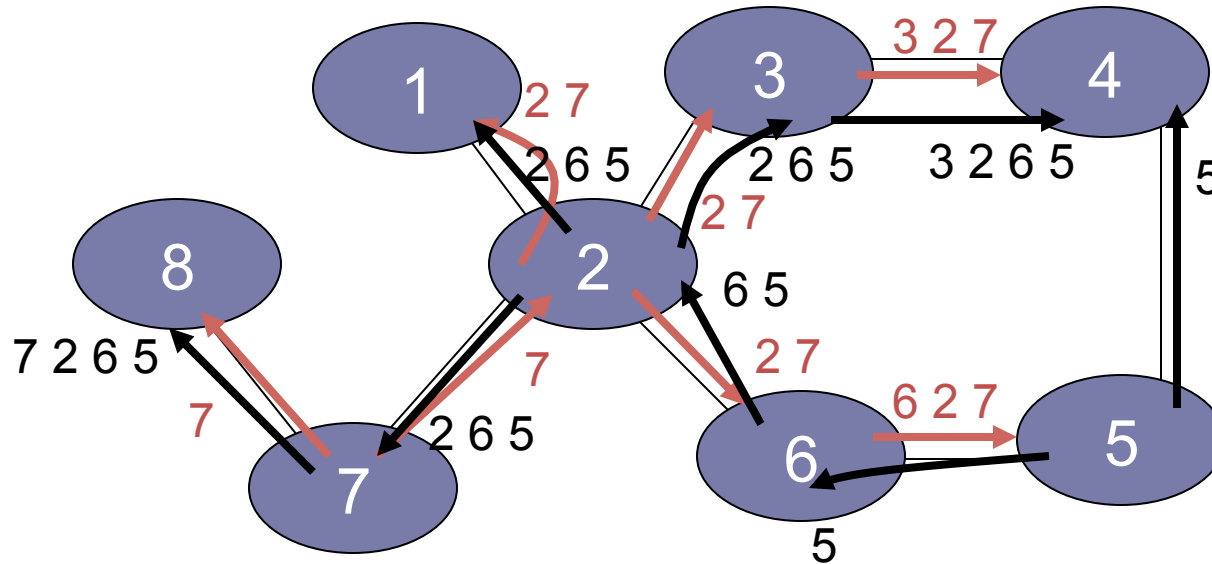
- AS 7007 incident in 1997
 - “Okay, so panic ensued, and we unplugged *everything* at 12:15PM almost to the second.” [sic]
 - <http://www.merit.edu/mail.archives/nanog/1997-04/msg00444.html>
- China Telecom hijacks large chunks of Internet in 2010
 - <http://bgpmon.net/blog/?p=282>

Youtube incident

- 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
 - more specific, prefix hijacking
- Internet thinks youtube.com is in Pakistan
- Outage resolved in 2 hours...

BGPsec

[D. Wetherall]



- Route announcements must be cryptographically signed
 - AS can only advertise as itself
 - AS cannot advertise for IP prefixes it does not own
- Requires a public-key infrastructure (PKI)
- Still in development:
 - <http://tools.ietf.org/html/draft-lepinski-bgpsec-protocol-00#ref-7>

Internet Security

- Recurring themes:
 - Built without any authenticity mechanisms in mind
 - Functionality mechanisms (sequence #'s) become implicit security mechanisms
 - New attempts at backwards-compatible security mechanisms
 - IP -> IPsec
 - DNS -> DNSsec
 - BGP -> BGPsec

Shady Reshipping Centers Exposed

Posted by **timothy** on Thursday October 13, @08:52AM
from the shady-shipping-containers-make-cool-houses dept.



[Dynamoo](#) writes

"Ever wondered how criminals can spirit away the products they buy with stolen credit cards? The answer is that they use surprisingly sophisticated but very [shady reshipping centers](#) to launder the goods on their way to Eastern Europe. The bad guys make the money, but it's the mules doing the reshipping who will eventually get caught."

Read the **86** comments



crime fraud russia

