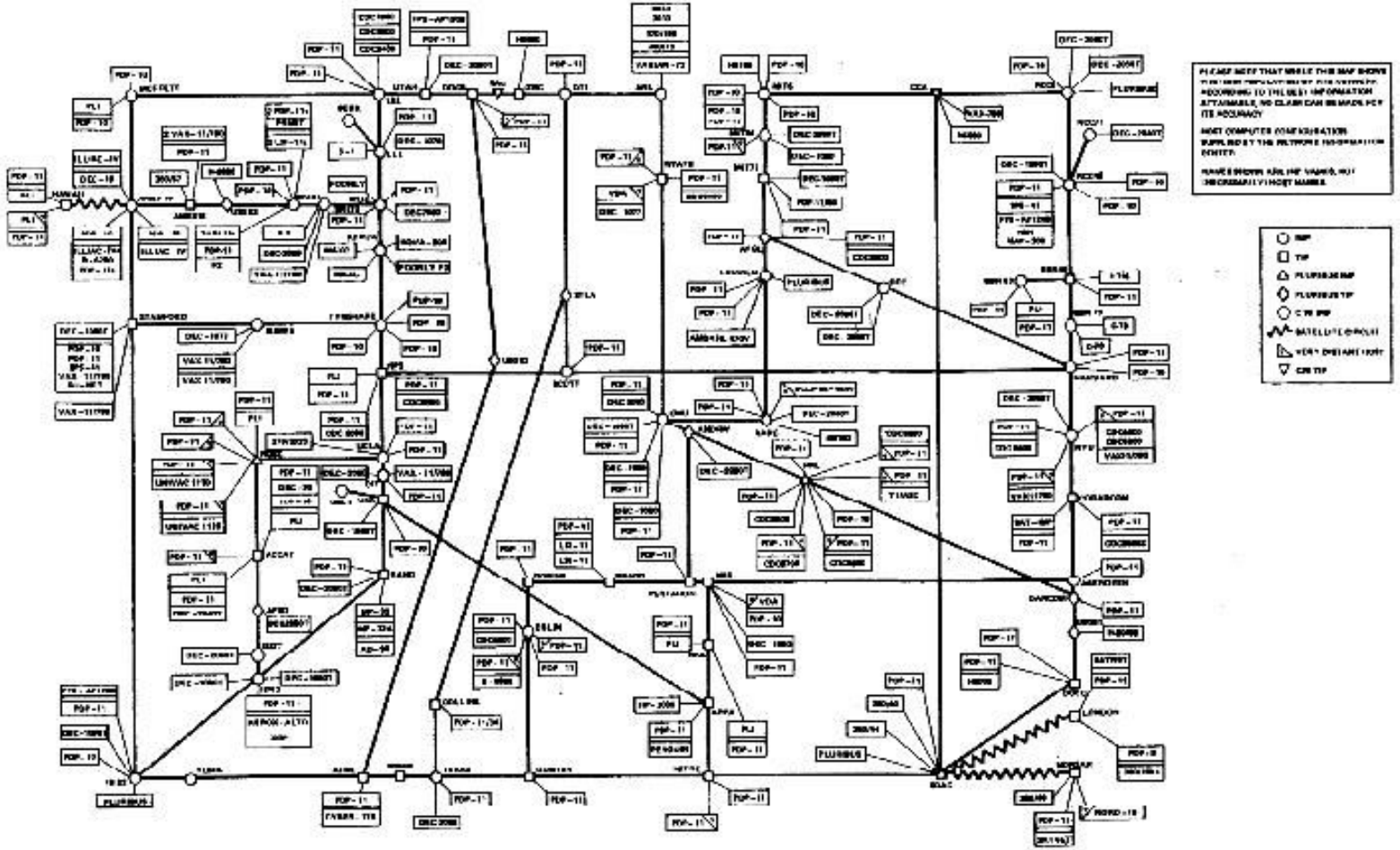
This was not an intended use of the internet

Computers are awesome

Computers are awesome

The internet is awesome

ARPANET LOGICAL MAP, JUNE 1981



It’s also a demonstration of standards somewhat working

TRANSMISSION CONTROL PROTOCOL

DARPA INTERNET PROGRAM

PROTOCOL SPECIFICATION

September 1981

TRANSMISSION CONTROL PROTOCOL

DARPA INTERNET PROGRAM

PROTOCOL SPECIFICATION

September 1981

Network Working Group
Request for Comments: 1035

Obsoletes: RFCs 882, 883, 973

P. Mockapetris
ISI
November 1987

DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION

1. STATUS OF THIS MEMO

TRANSMISSION CONTROL PROTOCOL

DARPA INTERNET PROGRAM

PROTOCOL SPECIFICATION

September 1981

Network Working Group
Request for Comments: 1035

Obsoletes: RFCs 882, 883, 973

P. Mockapetris
ISI
November 1987

DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION

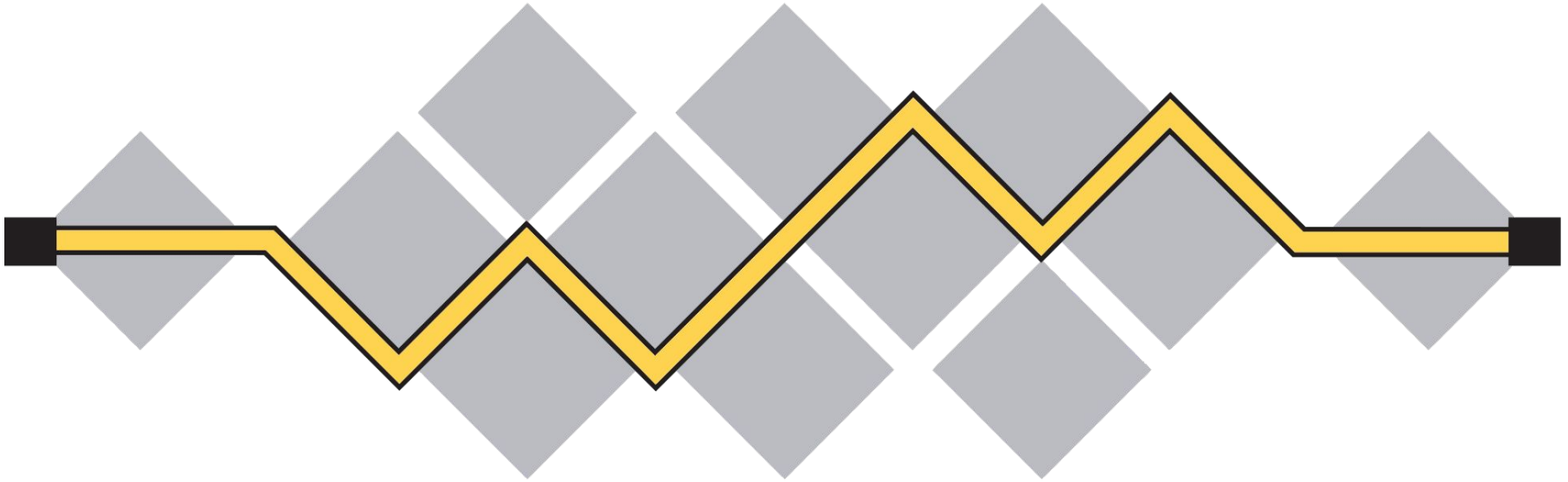
1. STATUS OF THIS MEMO

Network Working Group
Request for Comments: 4253
Category: Standards Track

T. Ylonen
SSH Communications Security Corp
C. Lonvick, Ed.
Cisco Systems, Inc.
January 2006

The Secure Shell (SSH) Transport Layer Protocol

Status of This Memo



IETF®

Network Working Group
Request for Comments: 3514
Category: Informational

The Security Flag in the IPv4 Header

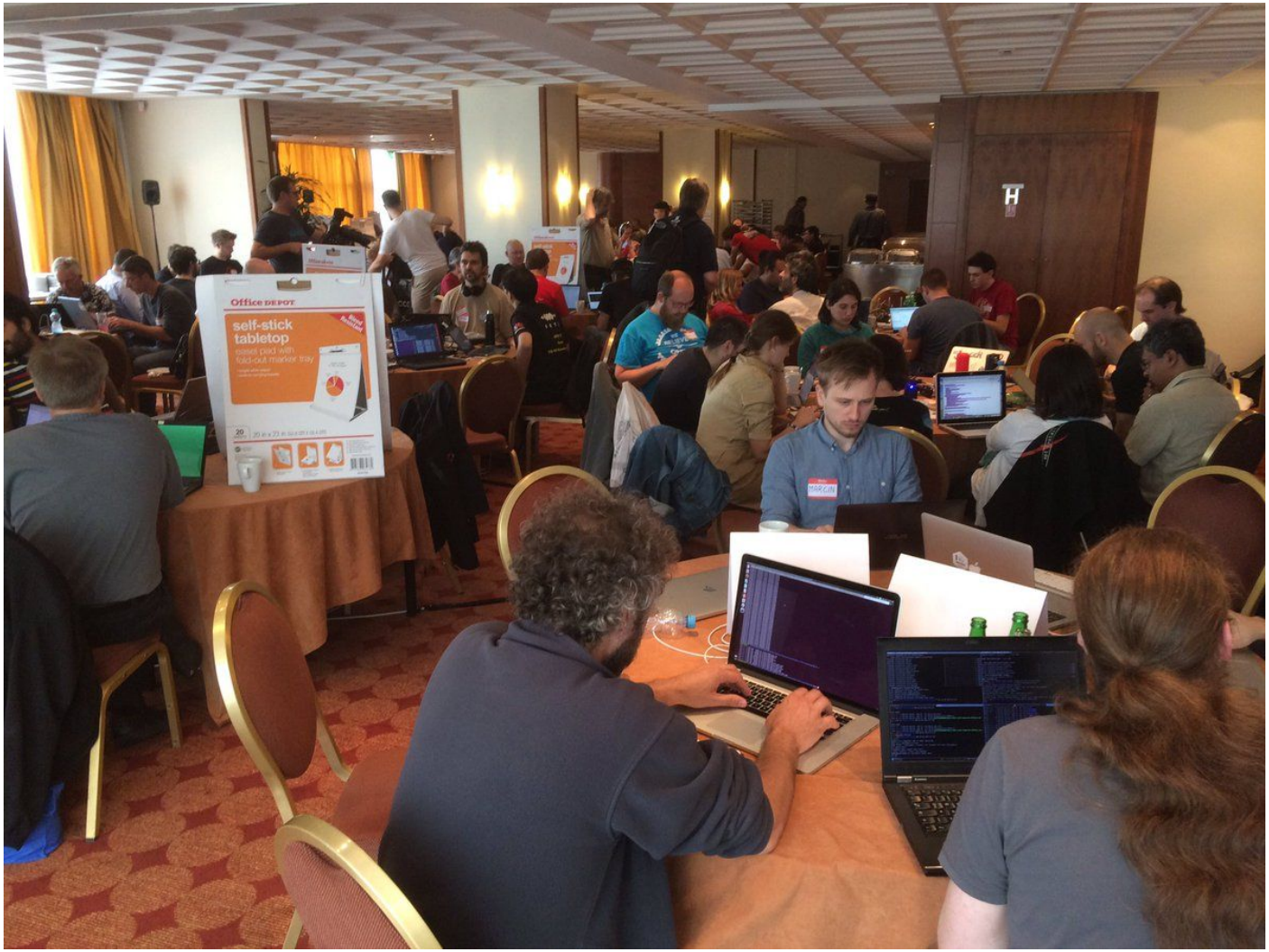
Status of this Memo

Network Working Group
Request for Comments: 5246
Obsoletes: 3268, 4346, 4366
Updates: 4492
Category: Standards Track

The Transport Layer Security (TLS) Protocol Version 1.2

I guess my point is


NOPE


Office DEPOT
self-stick
tabletop
MARCIN


IETF 99
Mostly dudes though :/
Office DEPOT
self-stick
tabletop

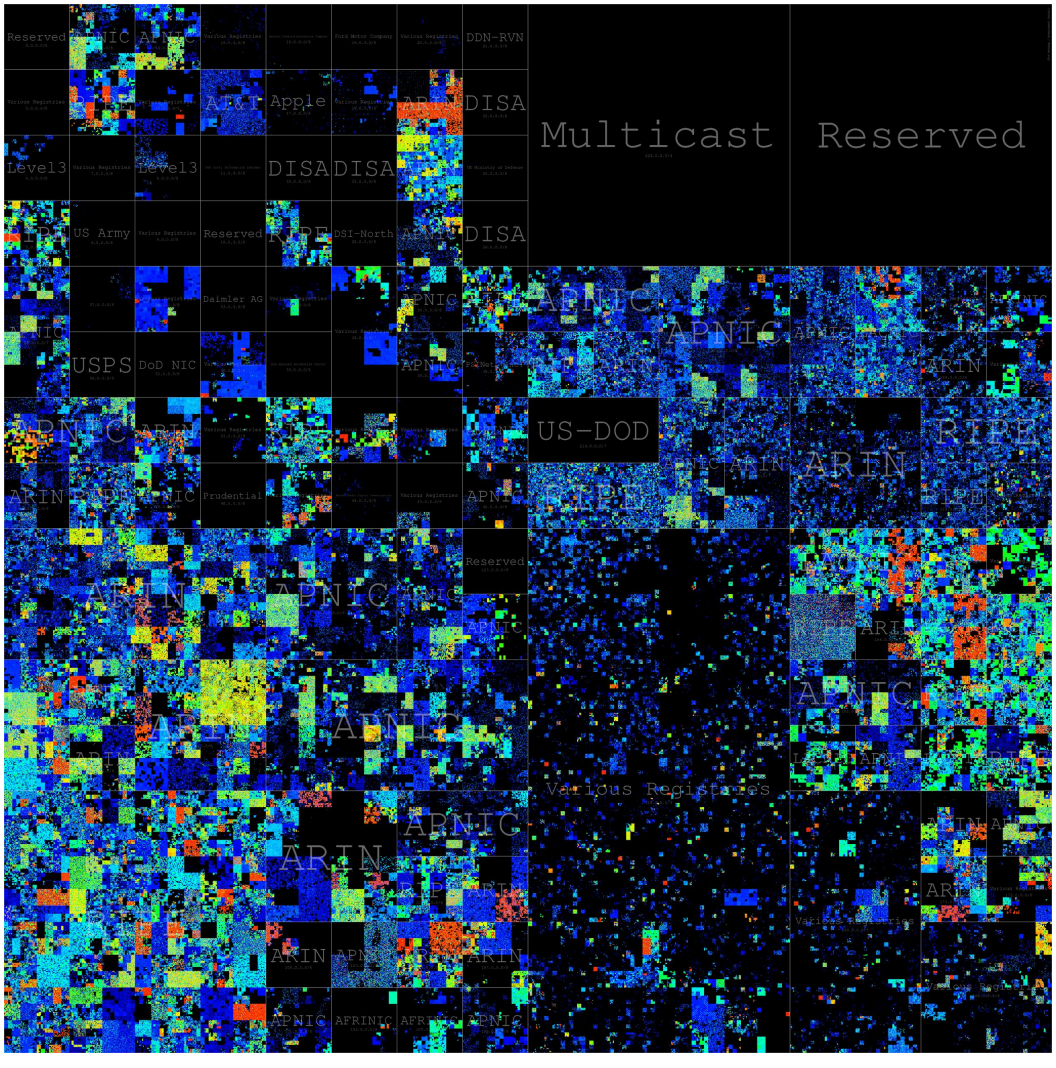
What can you ***also*** do with these protocols?

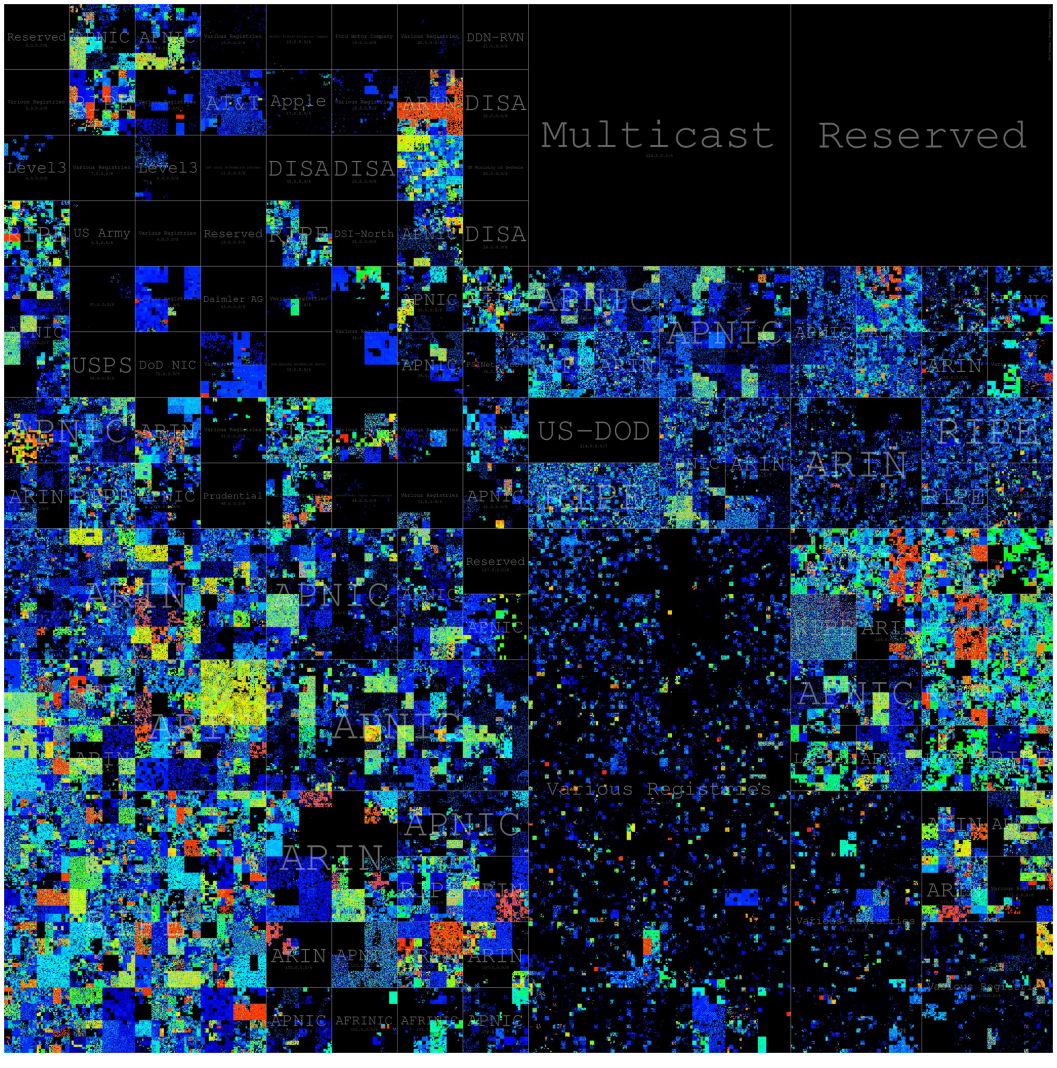
```
ben@eshwil:~$ whois AS206924
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See http://www.ripe.net/db/support/db-terms-conditions.pdf

% Note: this output has been filtered.
% To receive output for a database update, use the "-B" flag.
% Information related to 'AS206924'

% Abuse contact for 'AS206924' is 'noc@benjojo.co.uk'

aut-num:        AS206924
as-name:        BENJOJONET
```

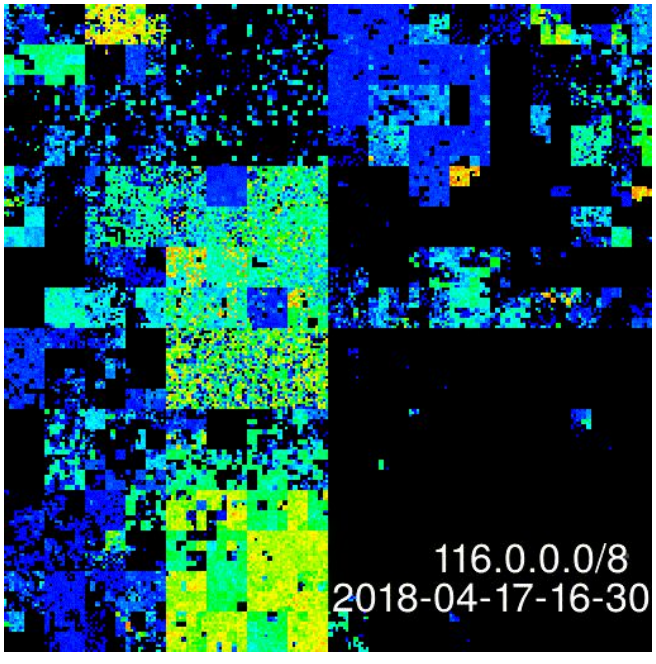
Why?

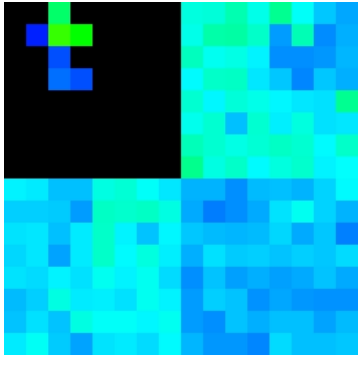
- I am now my own ISP
- I own IP addresses
- I consume memory in everyone else's expensive routers :)
- The abuse emails only go to me.

$ ping *.*.*.*


Multicast
Reserved
US-DOD
Various Registries


Reserved
DDN-RVN
AT&T
Apple
DISA
Multicast
Reserved
Level3
DISA
US Army
Reserved
DSI-North
Daimler AG
USPS
DoD NIC
US-DOD
Prudential
Various Registries


116.0.0.0/8
2018-04-17-16-30



Internet sins

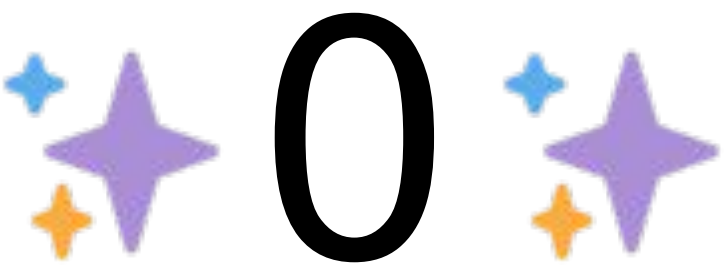
- 3,706,650,624 IP addresses pinged
- All of Asia was pinged every 30 mins

Total abuse emails?

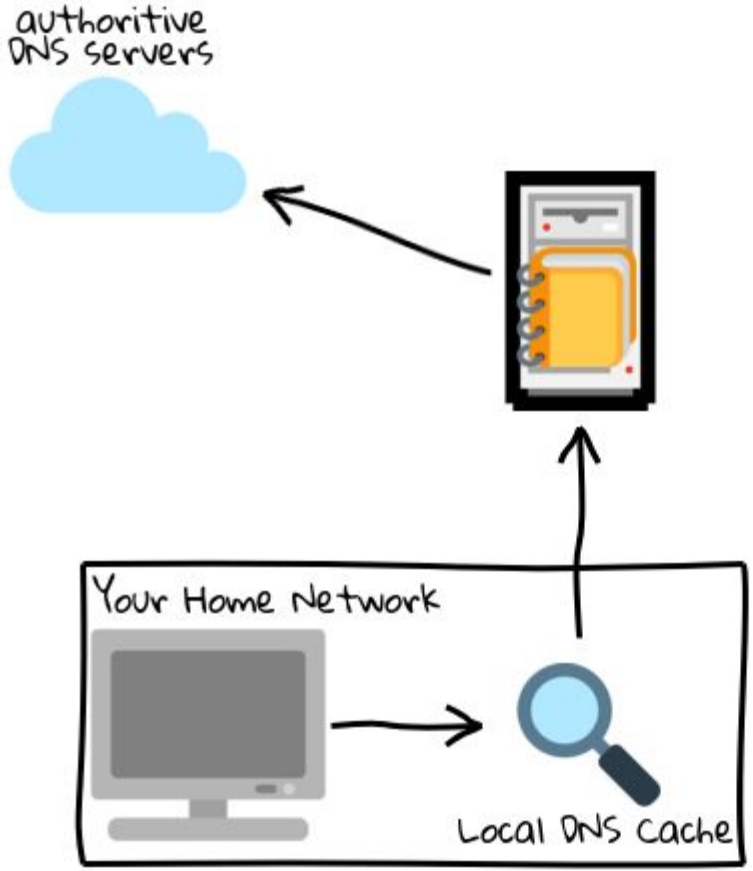
Internet sins

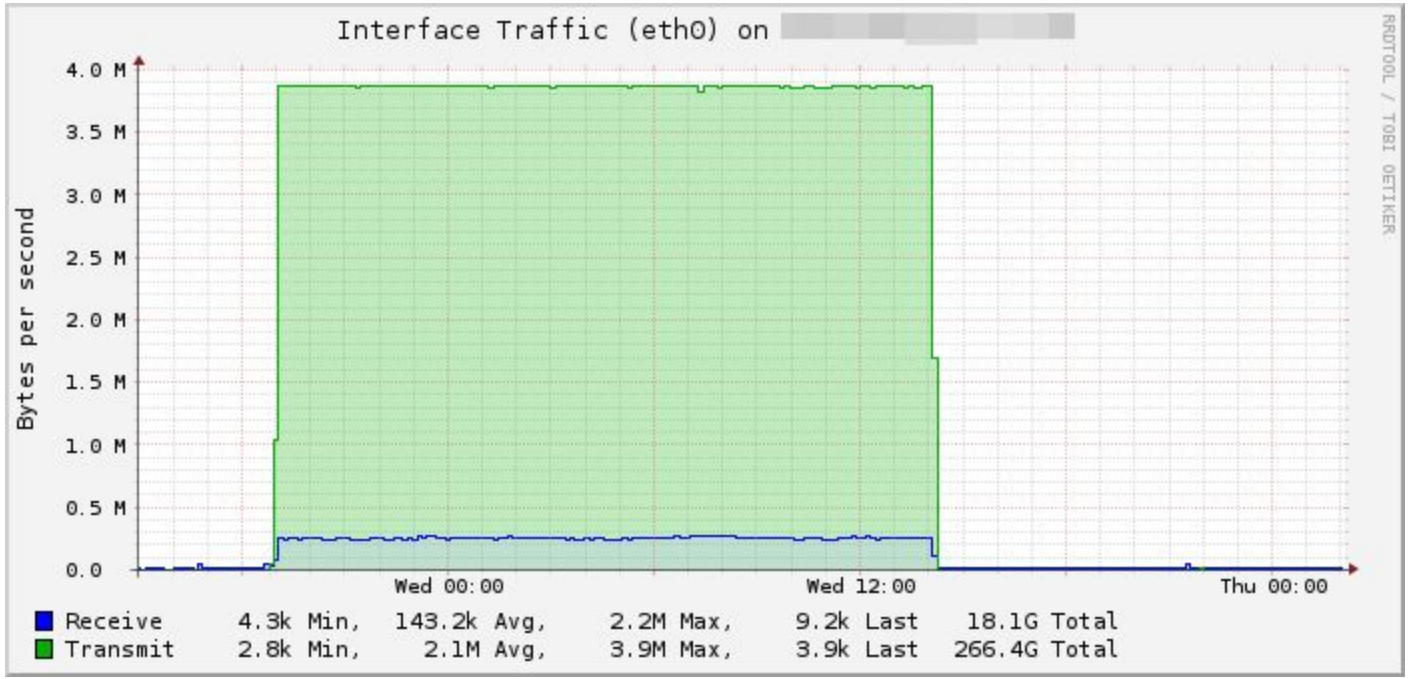
- 3,706,650,624 IP addresses pinged
- All of Asia was pinged every 30 mins

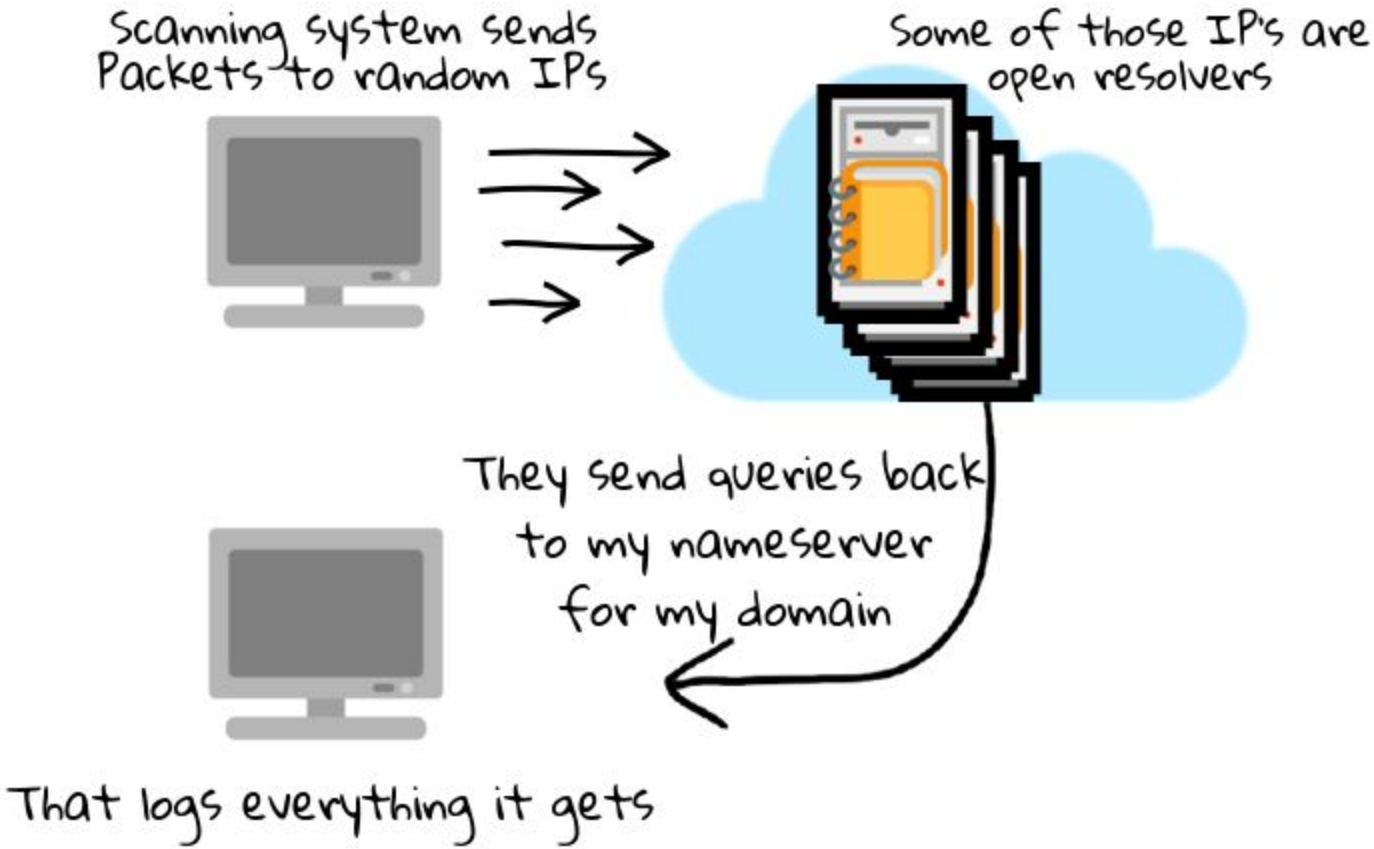
Total abuse emails?



DNSFS


authoritive
DNS servers
Your Home Network
Local DNS Cache


Interface Traffic (eth0) on
RRDTOOL / TOBI OETIKER
Bytes per second
4.0 M
3.5 M
3.0 M
2.5 M
2.0 M
1.5 M
1.0 M
0.5 M
0.0
Wed 00:00
Wed 12:00
Thu 00:00
Receive 4.3k Min, 143.2k Avg, 2.2M Max, 9.2k Last 18.1G Total
Transmit 2.8k Min, 2.1M Avg, 3.9M Max, 3.9k Last 266.4G Total


Scanning system sends
Packets to random IPs
Some of those IP's are
open resolvers
They send queries back
to my nameserver
for my domain
That logs everything it gets

Internet sins

- 3,706,650,624 IP addresses got a UDP packet
- Some of those IP’s would have logged my attempt to use them

Total abuse emails?

Internet sins

- 3,706,650,624 IP addresses got a UDP packet
- Some of those IP’s would have logged my attempt to use them

Total abuse emails?

DNS abuse

geoip/United Kingdom Inbox

B

Bob Goddard

to noc

Hide details

From: Bob Goddard
abuse@2.abuse.bgcomp.co.uk

To: noc@benjojo.co.uk

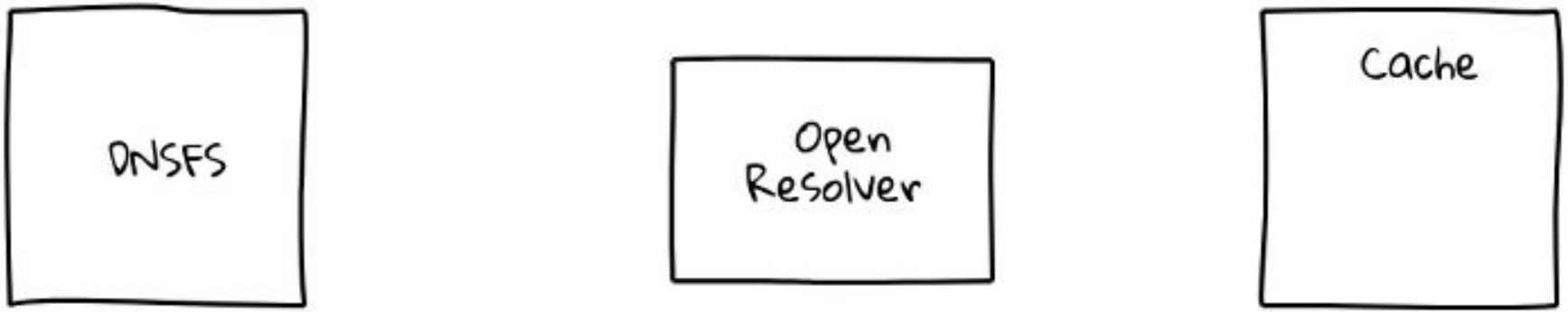
Date: 17 Nov 2017, 17:43

See security details

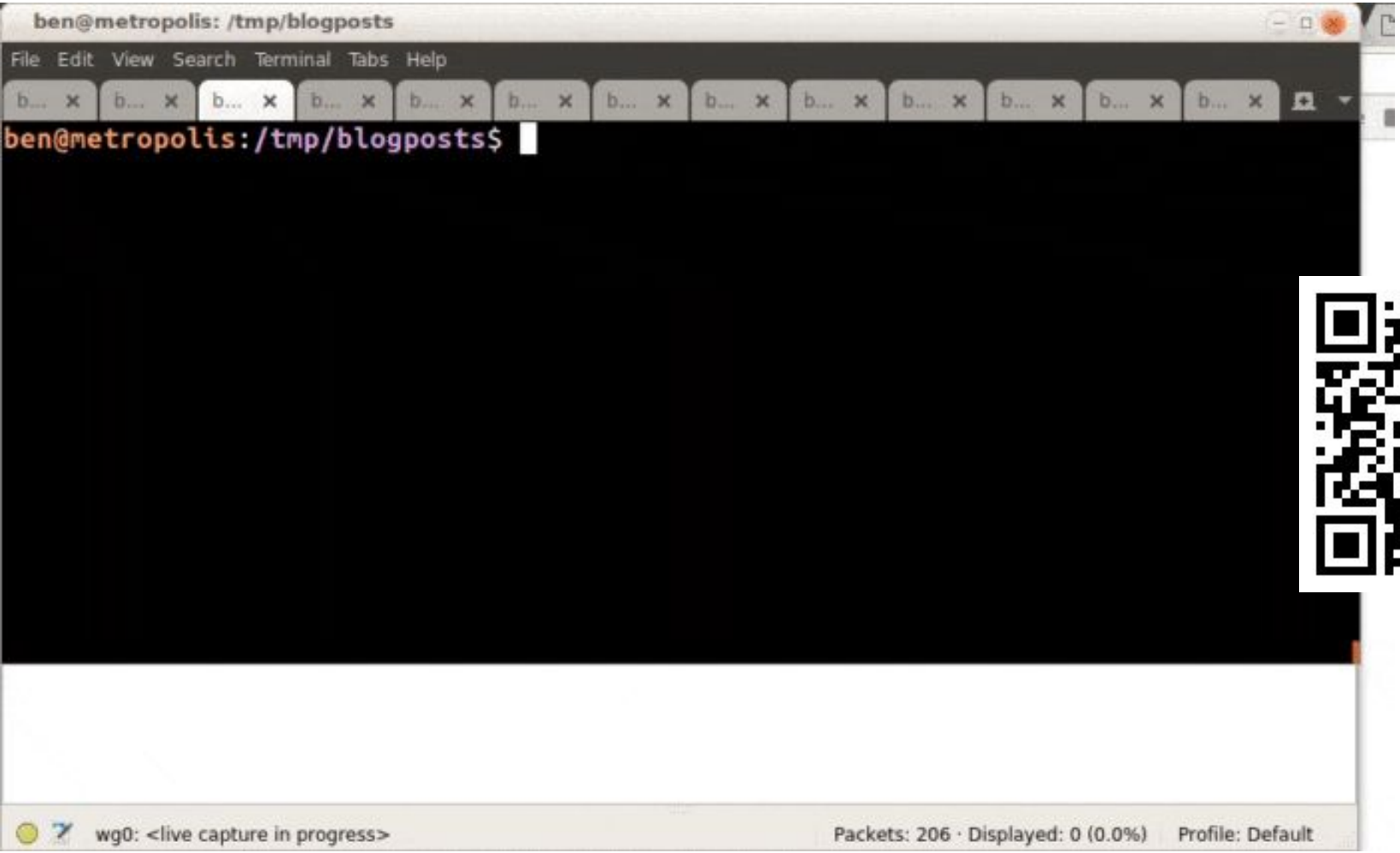
Fuck off and die scum.

2017-11-17T01:46:49.623403+00:00 eth7 named[1568]: client 185.230.223.69#52332 (openresolvertest.benjojo.co.uk): query (cache) 'openresolvertest.benjojo.co.uk/A/IN' denied
2017-11-17T08:40:21.756454+00:00 eth7 named[1568]: client 185.230.223.69#52332 (openresolvertest.benjojo.co.uk): query (cache) 'openresolvertest.benjojo.co.uk/A/IN' denied

Putting data into cache



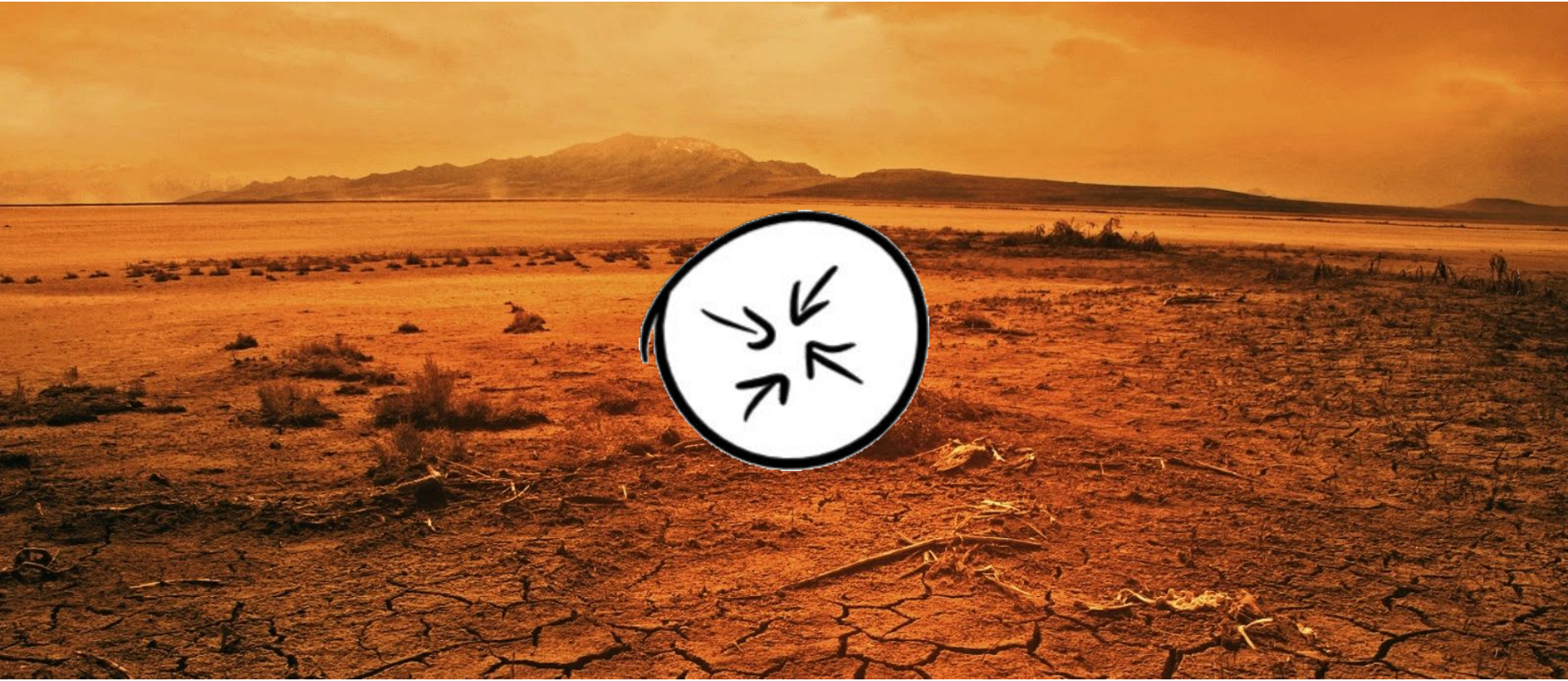
Say we want to store some data in a DNS cache...

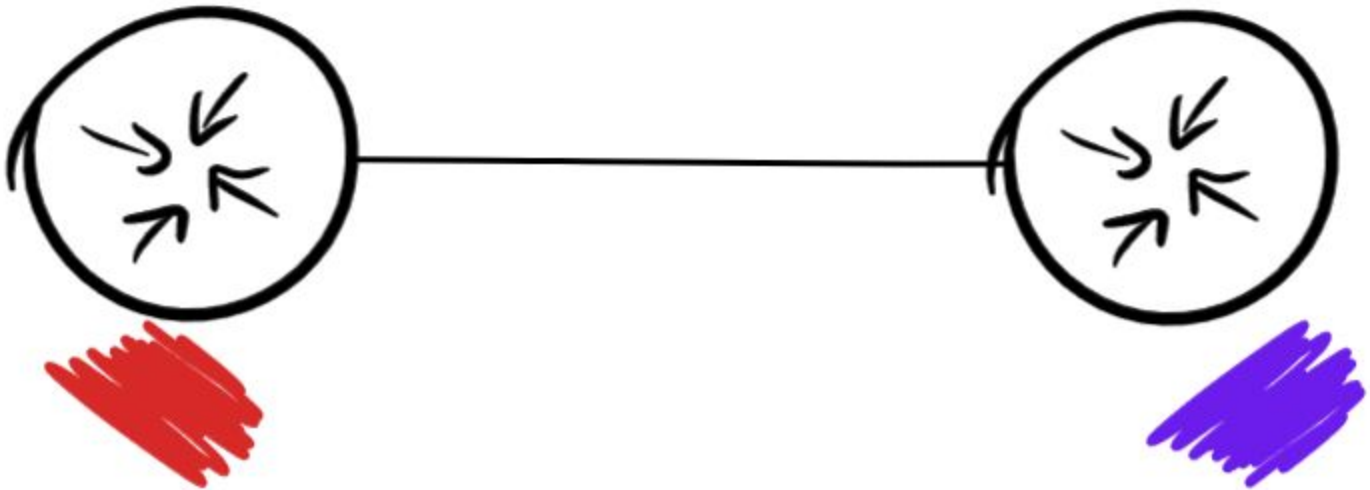

ben@metropolis: /tmp/blogposts
File Edit View Search Terminal Tabs Help
ben@metropolis:/tmp/blogposts$
wg0: <live capture in progress>
Packets: 206 · Displayed: 0 (0.0%)
Profile: Default

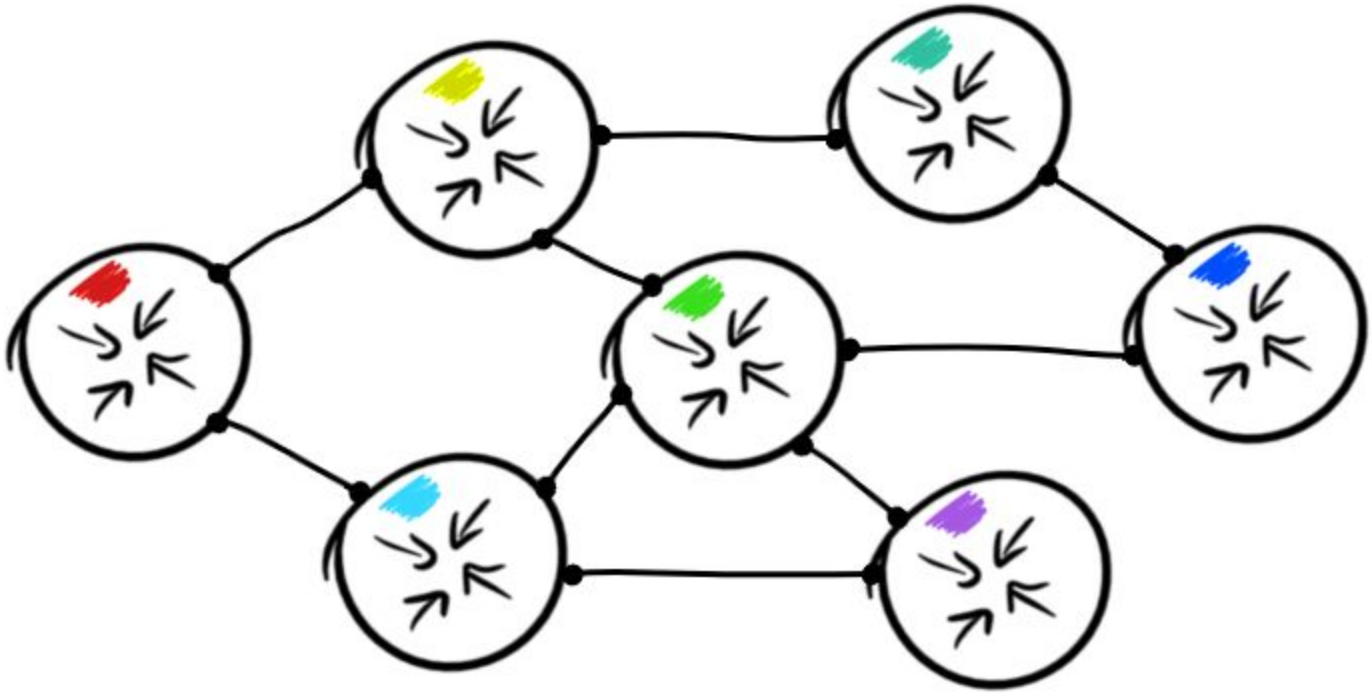
Next

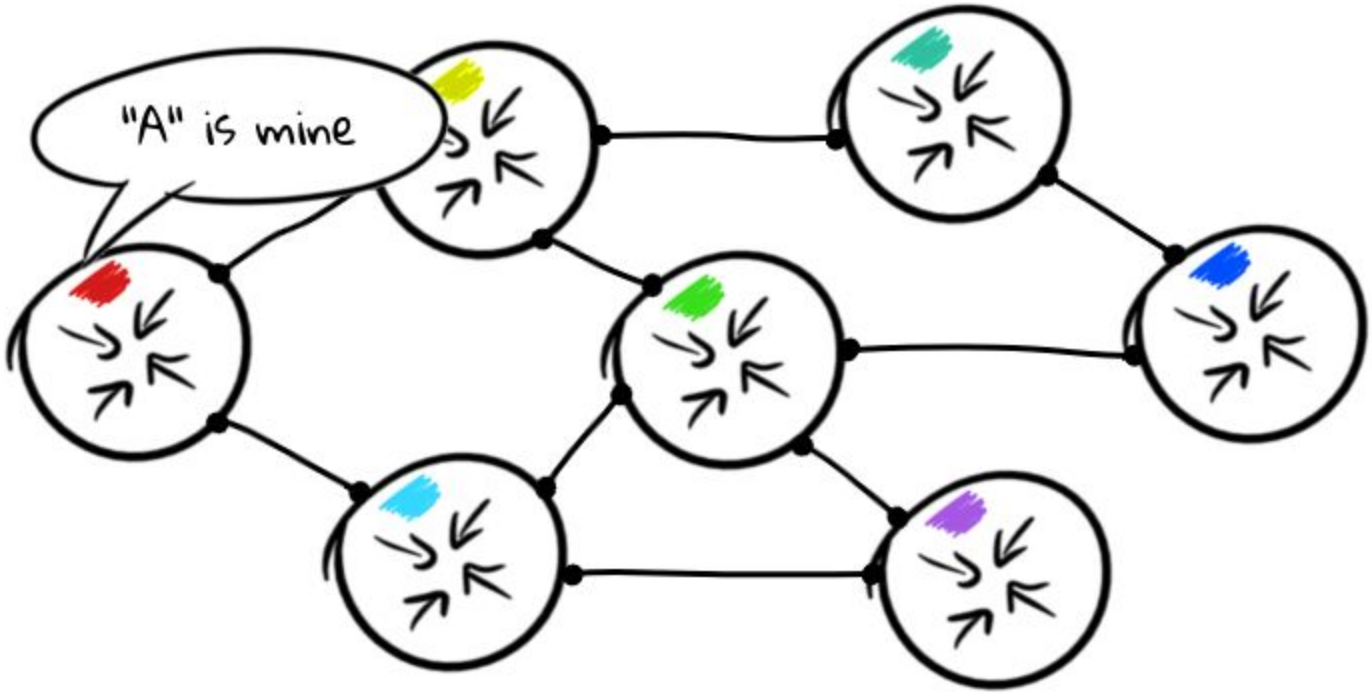
~~Border Gateway~~ Protocol

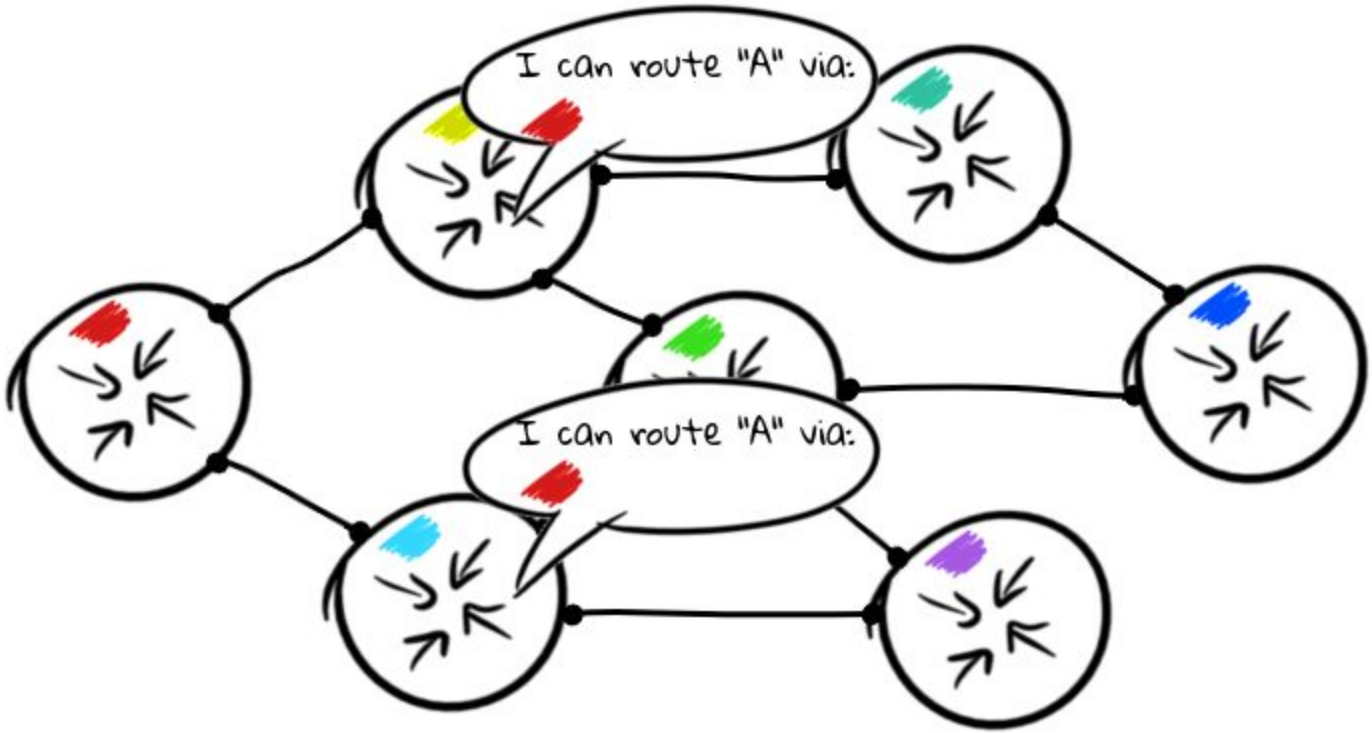
Battleship Game Protocol

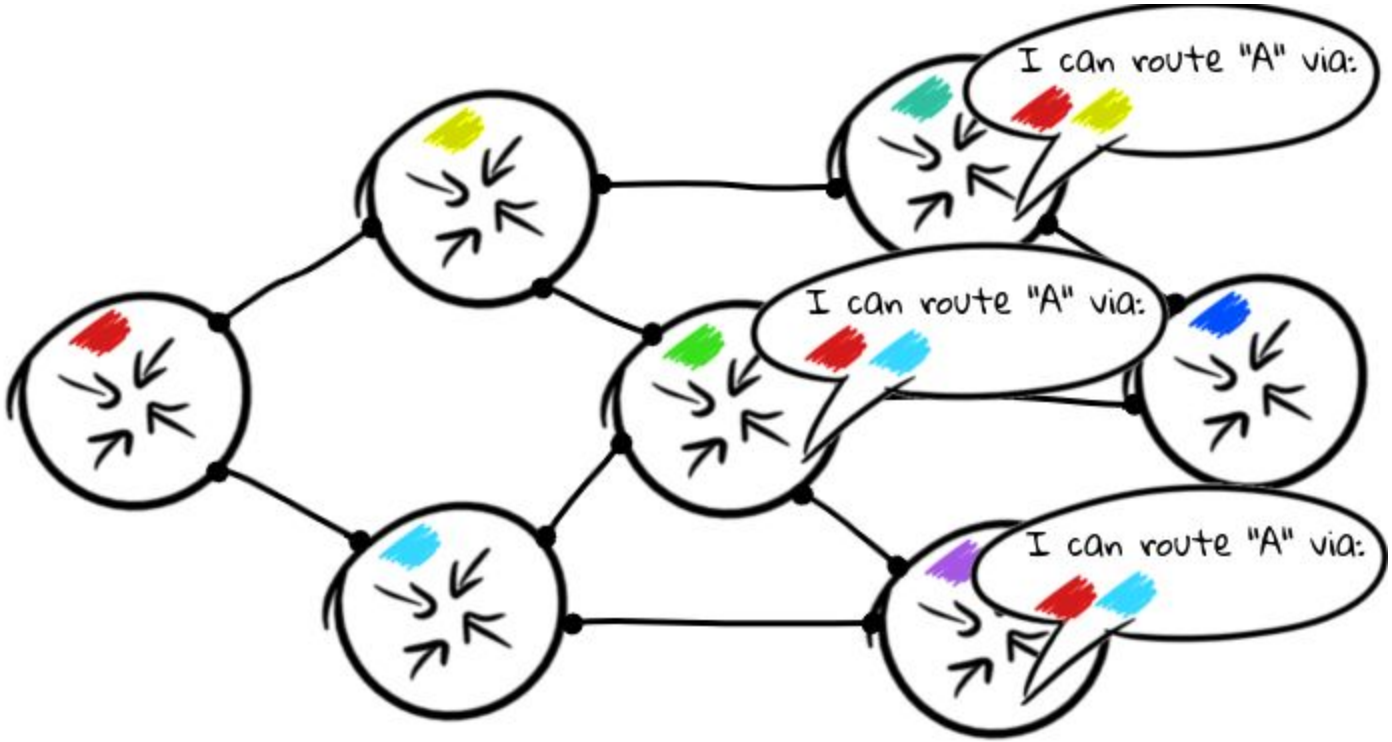


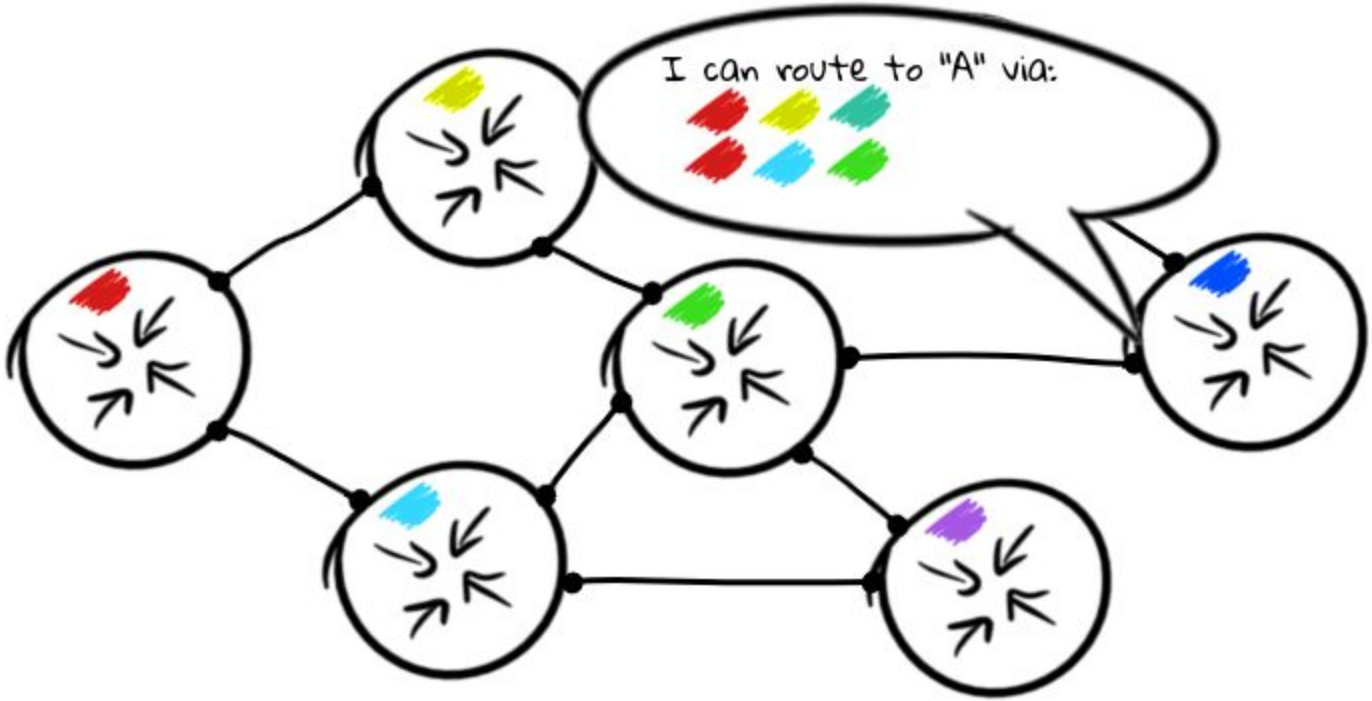




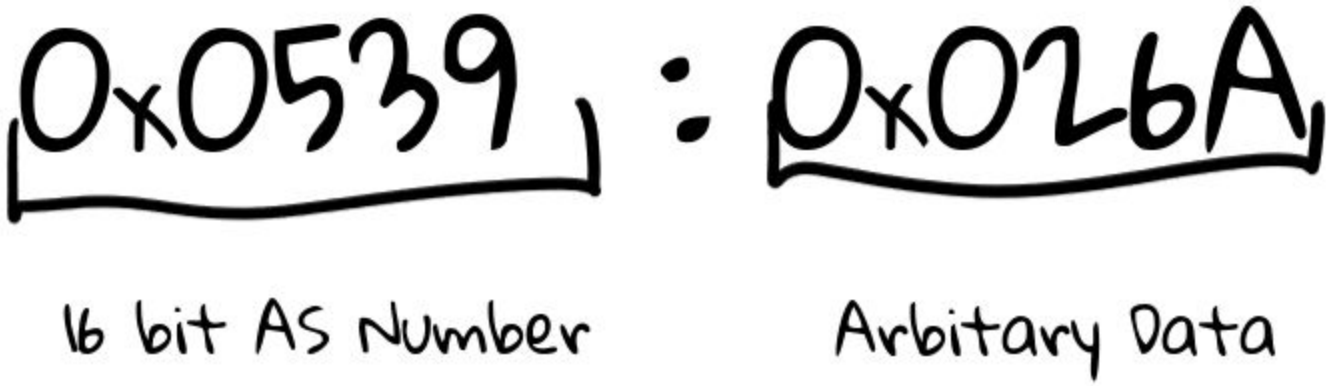

"A" is mine


I can route "A" via:
I can route "A" via:

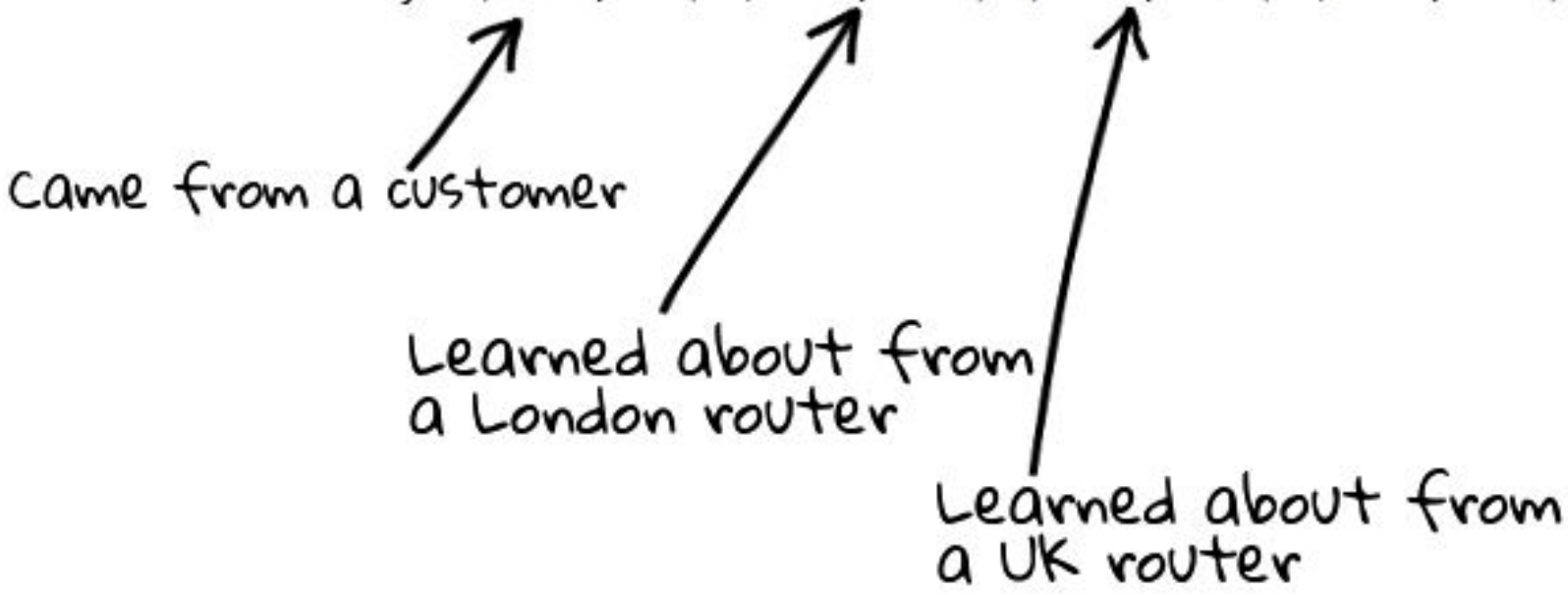

I can route "A" via:
I can route "A" via:
I can route "A" via:


I can route to "A" via:

```
BIRD 1.6.3 ready.
103.49.80.0/24     via 103.105.50.65 on eth0 [vmhaus 2018-05-15] * (100)
        Type: BGP unicast univ
        BGP.origin: IGP
        BGP.as_path: 136620 62240 2914 43519
        BGP.next_hop: 103.105.50.65
        BGP.med: 0
        BGP.local_pref: 100
        BGP.community: (2914,410) (2914,1203) (2914,2201) (2914,3200)
```


0x0539 : 0x026A
16 bit AS Number
Arbitary Data

```
BIRD 1.6.3 ready.
103.49.80.0/24     via 103.105.50.65 on eth0 [vmhaus 2018-05-15] * (100)
        Type: BGP unicast univ
        BGP.origin: IGP
        BGP.as_path: 136620 62240 2914 43519
        BGP.next_hop: 103.105.50.65
        BGP.med: 0
        BGP.local_pref: 100
        BGP.community: (2914,410) (2914,1203) (2914,2201) (2914,3200)
```




MB
KEY
TO FUN
FOR
AGES
8 TO
ADULT
MILTON
BRADLEY
COMPANY
SPRINGFIELD
MASSACHUSETTS
4730
MADE IN U.S.A.
AMERICA'S ALL TIME
FAVORITE GAME
BATTLESHIP
IT'S A HIT
G-4
BATTLESHIP
GAME

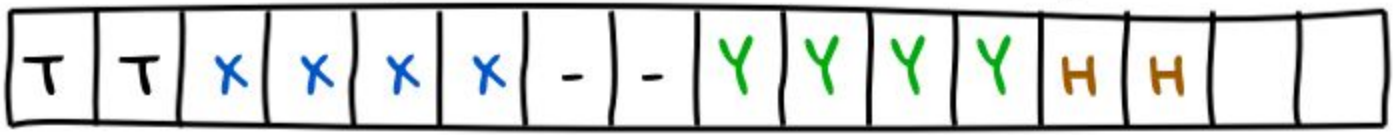
"Counter" Community

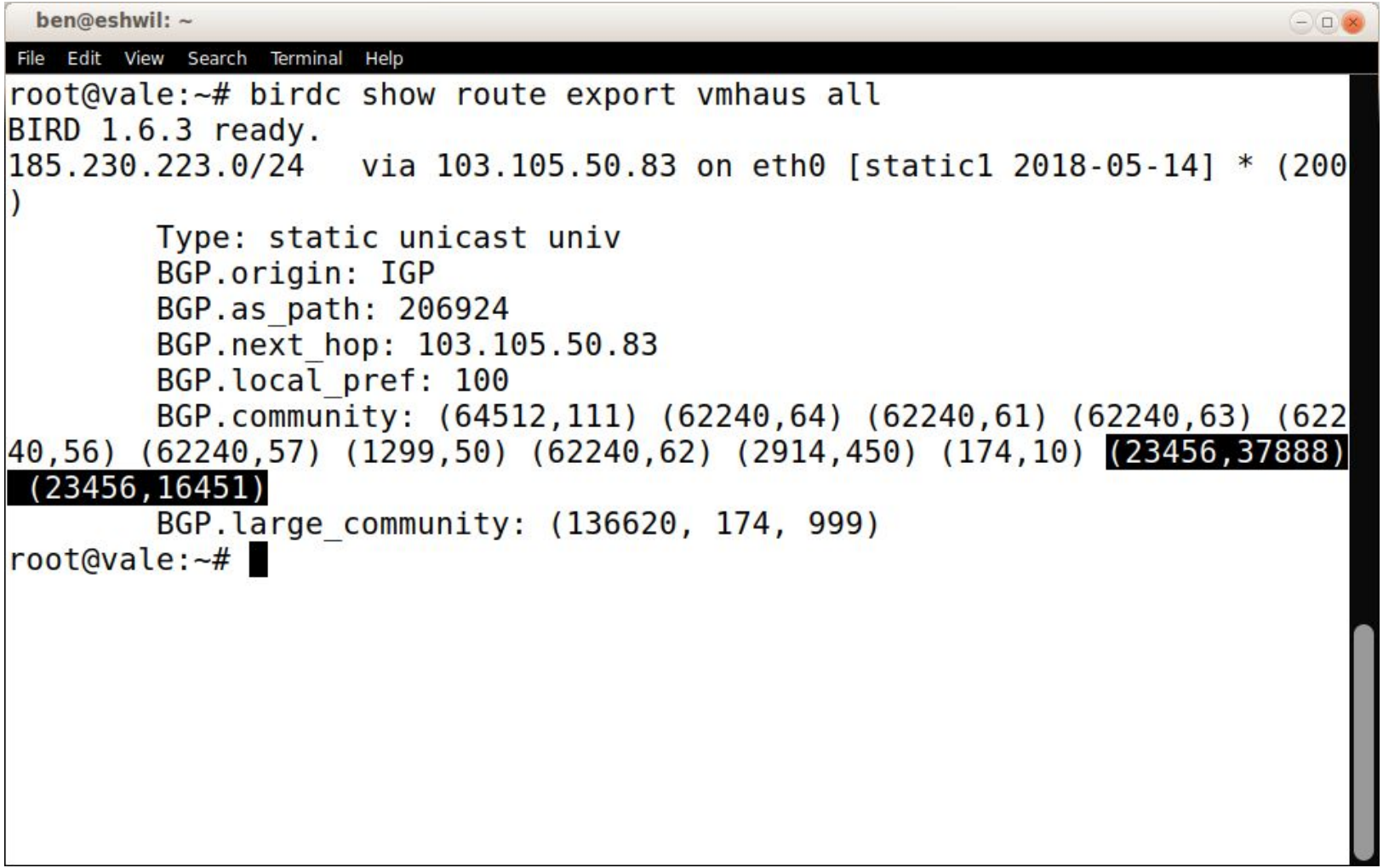
T = Type (Always 1) Z = 14 bit Interger counter

"Position" Community

T = Type (Always 2) X = 4 bit int for attack X

Y = 4 bit int for attack H = 2 bit int for Hit/Miss




ben@eshwil: ~
File Edit View Search Terminal Help
root@vale:~# birdc show route export vmhaus all
BIRD 1.6.3 ready.
185.230.223.0/24   via 103.105.50.83 on eth0 [static1 2018-05-14] * (200
)
Type: static unicast univ
BGP.origin: IGP
BGP.as_path: 206924
BGP.next_hop: 103.105.50.83
BGP.local_pref: 100
BGP.community: (64512,111) (62240,64) (62240,61) (62240,63) (622
40,56) (62240,57) (1299,50) (62240,62) (2914,450) (174,10) (23456,37888)
(23456,16451)
BGP.large_community: (136620, 174, 999)
root@vale:~#

The first ever board game conducted over BGP

Internet sins

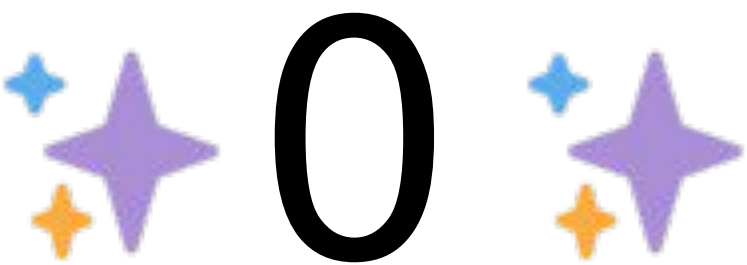
- All “full table” BGP routers in the world spent CPU on this
- Two ISPs used a routing protocol to transfer information between each other rather than actually sending packets

Total abuse emails?

Internet sins

- All “full table” BGP routers in the world spent CPU on this
- Two ISPs used a routing protocol to transfer information between each other rather than actually sending packets

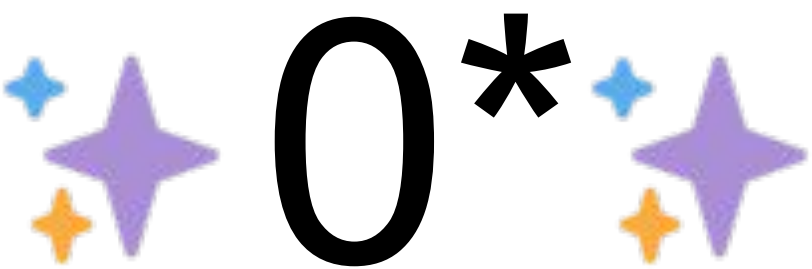
Total abuse emails?



Internet sins

- All “full table” BGP routers in the world spent CPU on this
- Two ISPs used a routing protocol to transfer information between each other rather than actually sending packets

Total abuse emails?



* Level 3 did automatically ban me for 20 mins during the game.

1.25 per router on average
700W
30 ms to process a route update in total

1.25 per router on average
700W
30 ms to process a route update in total

Level(3)

Has 7726 downstream networks that would have seen these updates
Educated guess that 1.5 is the average amount of routers per network


Seattle
Bellevue
Spokane
Helena
Billings
Bozeman
Vancouver
Portland
Hillsboro
Salem
Eugene
Bandon
Boise
Medford
Redding
Casper
Ogden
Cheyenne
Salt Lake City
Fort Collins-Loveland
Greeley
Boulder
Denver
Colorado Springs
Grand Junction
Grand Island
Omaha
Chico
Reno
Roseville
Manchester
Sacramento
Arden-Arcade
San Francisco
Oakland
San Mateo
Modesto
San Jose
Palo Alto
Sunnyvale
Fresno
Salinas
San Luis Obispo
Las Vegas
Grover Beach
Bakersfield
Lompoc
Burbank
San Bernardino
Santa Barbara
Riverside
Los Angeles
Anaheim
Orange County
Carlsbad
San Diego
Tijuana
Phoenix
Tucson
Santa Teresa
El Paso
Cuidad Juarez
Albuquerque
Amarillo
Stratford
Lubbock
Abilene
Midland
Wichita
Arkansas City
Wichita Falls
Fort Worth
Plano
Dallas
Waco
Round Rock
Austin
San Antonio
Laredo
Monterrey
McAllen
Harlingen
Reynosa
Corpus Christi
Houston
Sugar Land
Baytown
Lafayette
New Orleans
Lake Charles
Beaumont
Port Arthur
Bryan
Zavalla
Tyler
Shreveport
Monroe
Jackson
Raton Rouge
Mobile
Pensacola
Panama City
Tallahassee
Brent
Ferry Pass
Montgomery
Columbus
Macon
Atlanta
Birmingham
Augusta
Savannah
Charleston
Wilmington
Jacksonville
Gainesville
Ocala
Orlando
Tampa
Clearwater
Saint Petersburg
Sarasota
Fort Myers
Miami
Fort Lauderdale
Daytona Beach
Titusville
Winter Haven
Melbourne
Lakeland
West Palm Beach
Boca Raton
Deerfield Beach
Nassau
Minneapolis
Eagan
Eau Claire
Green Bay
Owatonna
Grand Rapids
Saginaw
Battle Creek
Livonia
Milwaukee
Lansing
Madison
Kalamazoo
Cedar Rapids
Chicago
Des Moines
South Bend
Toledo
Detroit
Dearborn
Mentor
Cleveland
Elyria
Akron
Youngstown
Pittsburgh
Columbus
Dayton
Cincinnati
Indianapolis
Springfield
Bethany
Kansas City
Council Bluffs
Lincoln
Topeka
Salina
Maryland Heights
St. Louis
Louisville
Middletown
Lexington-Fayette
Bowling Green
Sikeston
Springfield
Wichita
Arkansas City
Tulsa
Bentonville
Oklahoma City
Memphis
Nashville
Knoxville
Shelbyville
Manchester
Chattanooga
Little Rock
Greenville
Spartanburg
Atlanta
Columbia
Augusta
Macon
Montreal
Burlington
Mississauga
Toronto
Rochester
Utica
Schenectady
Troy
Springfield
Worcester
Boston
Albany
Syracuse
Niagara Falls
Buffalo
Erie
Southfield
Detroit
New York
Philadelphia
Baltimore
Washington, D.C.
Ashburn
Winchester
Harrisonburg
Staunton
Fredericksburg
Charlottesville
Lynchburg
Richmond
Roanoke
Danville
Norfolk
Chesapeake
Kingsport-Bristol
Tri-Cities
Johnson City
Greensboro
Rocky Mount
Winston-Salem
Gastonia
Charlotte
Raleigh
Fayetteville
Wilmington
Harrisonburg
Fredericksburg
GTT ATLANTIC (NORTH)
TAT-14
AC-1 (NORTH)
AECONNECT
APOLLO NORTH
YELLOW (AC-2)
TGN-A
AC-1 (SOUTH)
APOLLO SOUTH
FLAG NORTH (FA-1)
FLAG SOUTH (FA-1)
GLOBENET
MID-ATLANTIC CROSSING (MAC)
MAC
AAG
SCCN


Seattle
Bellevue
Vancouver
Portland
Hillsboro
Salem
Eugene
Bandon
Medford
Redding
Chico
Manchester
Sacramento
San Francisco
Oakland
San Mateo
Palo Alto
Sunnyvale
Salinas
Grover Beach
Lompoc
Santa Barbara
Los A
Orang
AAG
SCCN
Inverness
Aberdeen
Dundee
Glasgow
Edinburgh
Carlisle
Newcastle
Manchester
York
Leeds
Liverpool
Sheffield
Dublin
Wexford
Birmingham
Norwich
Kilmore Quay
Cambridge
Swansea
London
Bristol
Slough
Bude
Brighton
Plymouth
Whitesands
Truro
Caen
Rouen
Paris
Lannion
Rennes
Lille
Bredene
Bruessels
Beverwijk
Amsterdam
Haarlem
Rotterdam
Antwerp
Dusseldorf
Cologne
Luxembourg
Ludwigshafen
Frankfurt
Nuremberg
Stuttgart
Strasbourg
Kehl
Munich
Basel
Zuhhrich
Geneva
Lyon
Milan
Turin
Bordeaux
Toulouse
Marseille
Monaco
Bilbao
Barcelona
Madrid
Valencia
Lisbon
Rome
WACS
EIG
HAWK
SEA-ME-WE-4
Stockholm
Tallinn
Gothenburg
Copenhagen
Malmo
Sylt
Hamburg
Bremen
Hanover
Berlin
Poznan
Warsaw
Leipzig
Dresden
Prague
Katowice
Kraków
Brno
Ivancice
Bratislava
Vienna
Budapest
Zagreb
Ljubljana
Belgrade
Bucharest
Sofia
Istanbul

1.25 per router on average
700W
30 ms to process a route update in total

Level(3)

Has 7726 downstream networks that would have seen these updates
Educated guess that 1.5 is the average amount of routers per network

Level(3)

Has 721 internal routers

0.0000038KwH per route update

0.0000038KwH per route update

0.0000038 * 12310 =
0.0467KwH

0.0000038KwH per route update

0.0000038 * 12310 =
0.0467KwH

25g

25g of meat = 35.75 cal

=

0.041~ KwH

I think it’s time for me to stop

I think it’s time for me to stop

Questions?

@Benjojo12 / 🌐AS206924

blog.benjojo.co.uk