Internet Noise: a tale of two subnets

Tim Obezuk

Cloudflare

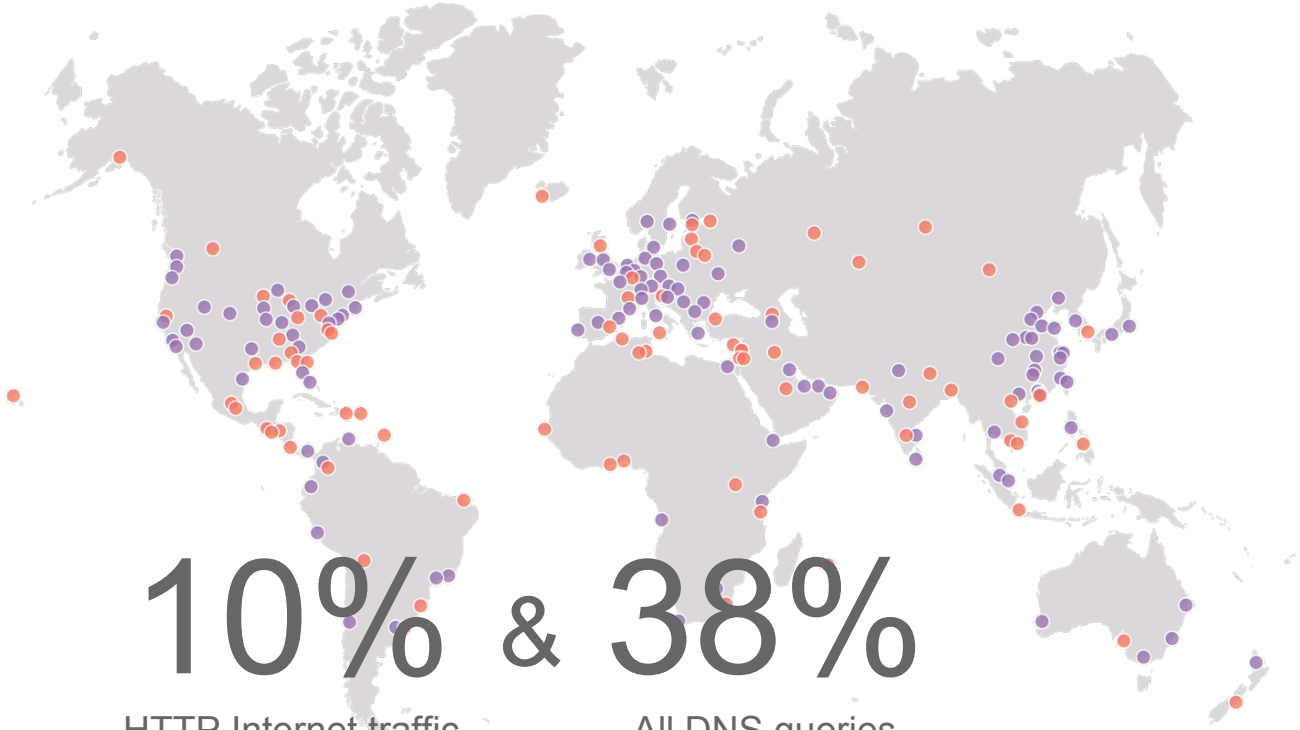
Who am I?

- Tim Obezuk
- Solutions Engineer at Cloudflare
- Helping Australian organisations build faster and more secure internet properties

CLOUDFLARE

You already use Cloudflare without knowing it.

CLOUDFLARE



10% & 38%

HTTP Internet traffic
600b reqs/day

All DNS queries
140bn/day

Live Data Center
In Progress/Planned

CLOUDFLARE

151+

PoPs in 74+
countries
15Tbps capacity

HURRICANE ELECTRIC INTERNET SERVICES

Search

Internet Exchange Report

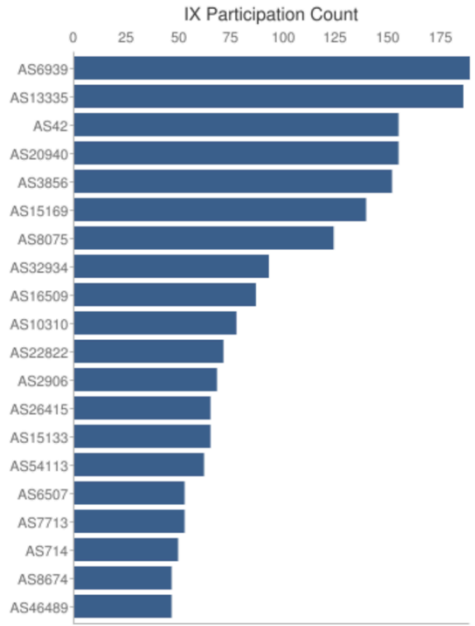
Quick Links

- BGP Toolkit Home
- BGP Prefix Report
- BGP Peer Report
- Exchange Report
- Bogon Routes
- World Report
- Multi Origin Routes
- DNS Report
- Top Host Report
- Internet Statistics
- Looking Glass
- Network Tools App
- Free IPv6 Tunnel
- IPv6 Certification
- IPv6 Progress
- Going Native
- Contact Us

Internet Exchanges | Exchange Participants

IX Participation Count

ASN	Name	IXes
AS6939	Hurricane Electric LLC	189
AS13335	Cloudflare, Inc.	188
AS42	WoodyNet	158
AS20940	Akamai International B.V.	155
AS3856	Packet Clearing House	153
AS15169	Google LLC	141
AS8075	Microsoft Corporation	127
AS32934	Facebook, Inc.	93
AS16509	Amazon.com, Inc.	87
AS10310	Yahoo!	80
AS22822	Limelight Networks, Inc.	72
AS2906	Netflix Streaming Services Inc.	70
AS26415	VeriSign Global Registry Services	68
AS15133	EdgeCast Networks, Inc. d/b/a Verizon Digital Media Services	66
AS54113	Fastly	64
AS6507	Riot Games, Inc	55
AS7713	PT Telekomunikasi Indonesia	53
AS714	Apple Inc.	50
AS8674	NETNOD Internet Exchange i Sverige AB	49
AS46489	Twitch Interactive Inc.	49



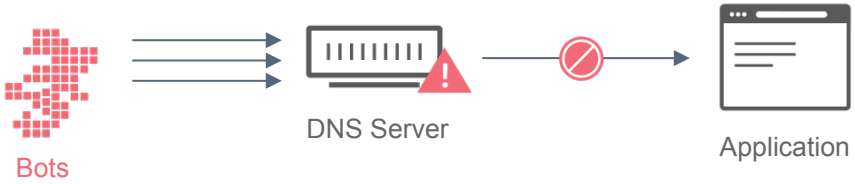
Updated 25 Aug 2018 19:44 PST © 2018 Hurricane Electric

CLOUDFLARE

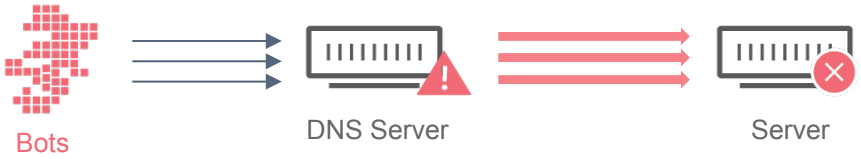
188+

Internet Exchanges

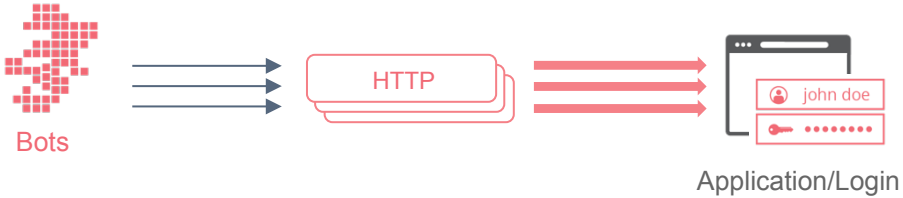
1 Volumetric DNS Flood



2 Amplification (Layer 3 & 4)



3 HTTP Flood (Layer 7)



CLOUDFLARE

942Gbps

Largest attack mitigated

500Gbps

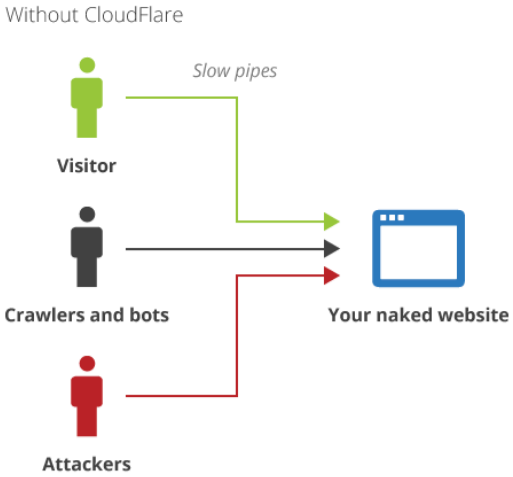
300M pps

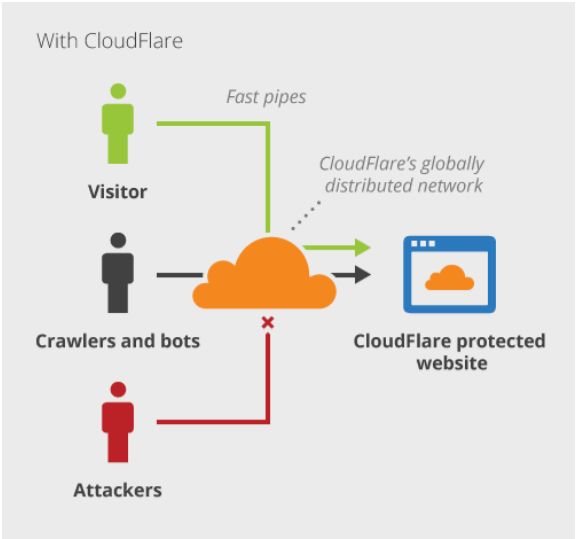
Common attack size

About Cloudflare

Cloudflare makes websites faster and safer using our globally distributed network to deliver essential services to any website

- Performance
- Content
- Optimisation
- Security
- 3rd party services
- Analytics
- Edge Computing





CLOUDFLARE

The IP Blocks

INTERESTING IP RANGES:

- 1.1.1.0/24
- 1.0.0.0/24

APNIC

Get IP | Manage IP | Training | Events | Research | Community

APNIC Labs enters into a research agreement with Cloudflare

By Geoff Huston on 2 Apr 2018

Category: Tech matters

APNIC Labs is partnering with Cloudflare for a joint research project relating to the operation of the DNS.

CLOUDFLARE

PROP-109: APNIC allocated as research prefixes

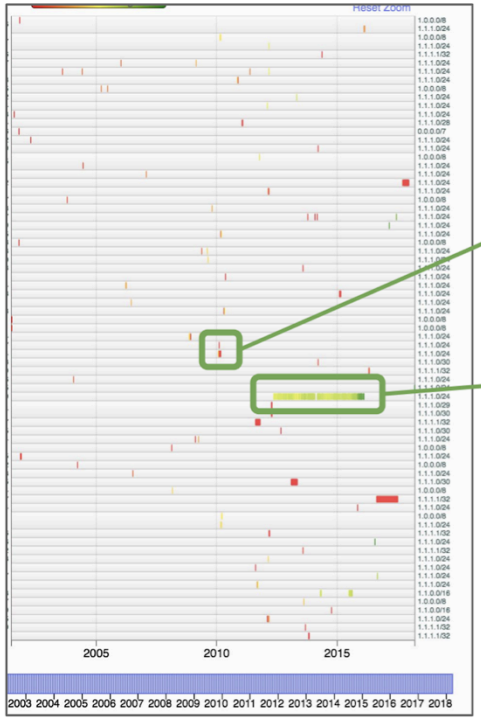
Bogon prefixes before 2010

Known to receive unwanted traffic:

- Misconfigurations (proxies, internal use)
- Misuse

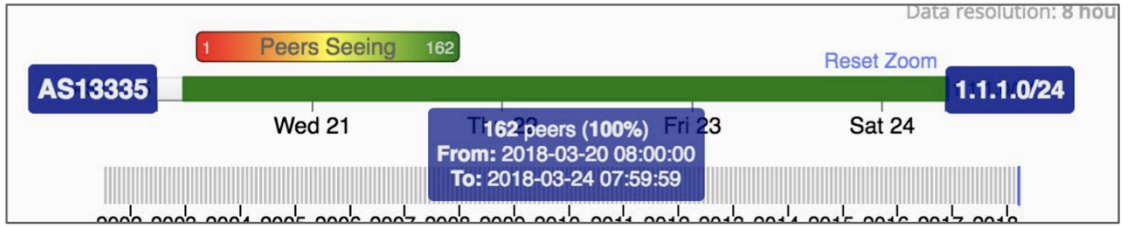
Partnership with Cloudflare in 2018

Routing History

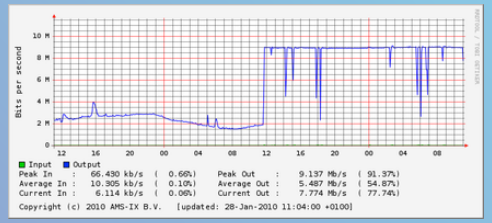


RIPE, Merit

GOOGLE/YOUTUBE



RIPE - 10Mb/s maxed



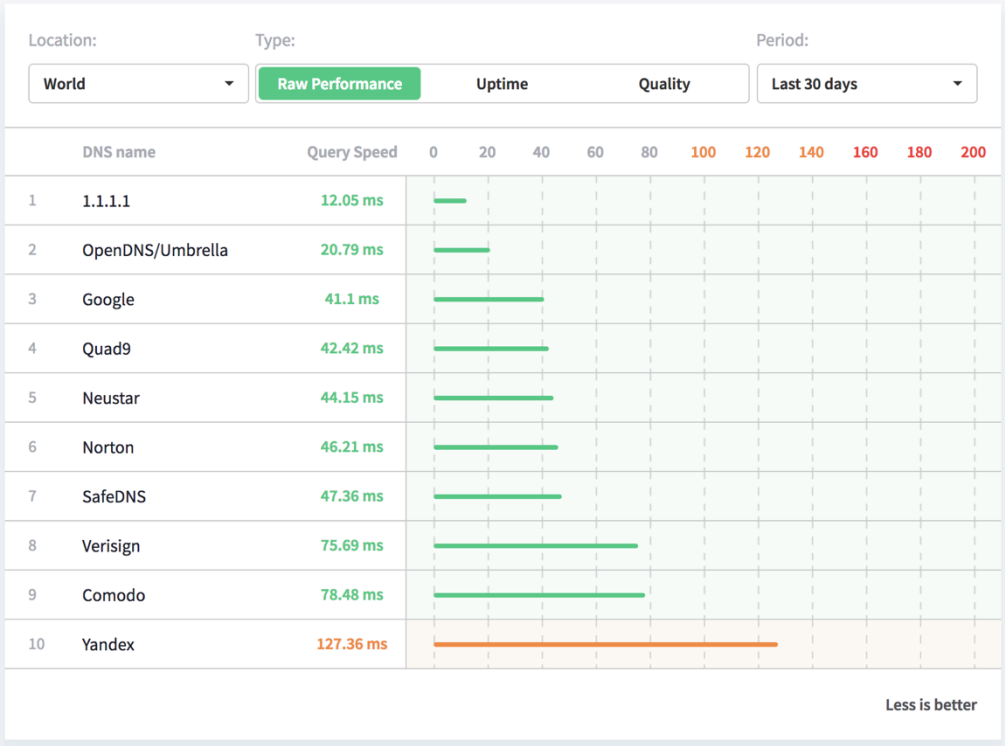
Merit announced 1.0.0.0/8 from 23/02/2010 to 01/03/2010 and collected **7.9Tb** of pcap

http://www.potaroo.net/studies/1slash8/1slash8.html

https://labs.ripe.net/Members/franz/content-pollution-18

CLOUDFLARE

1.1.1.1



CLOUDFLARE

FREE

FAST

Privacy-first recursive resolver for everyone

APNIC has the IP Address

Cloudflare has the network.

7.05ms in Oceania (dnsperf)

What’s the Noise / Junk?

Traffic levels

PREVIOUS STUDIES

- 2010: > 100Mb/s on 1.1.1.0/24
- 2014: > 100-1Gb/s on 1.0.0.0/8

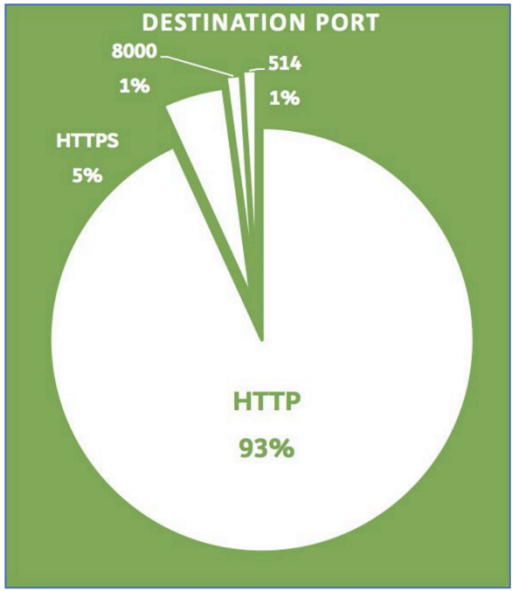
2018

- 8-13Gb/s
- 1Gb/s solely on 1.1.1.1

CLOUDFLARE

Traffic levels

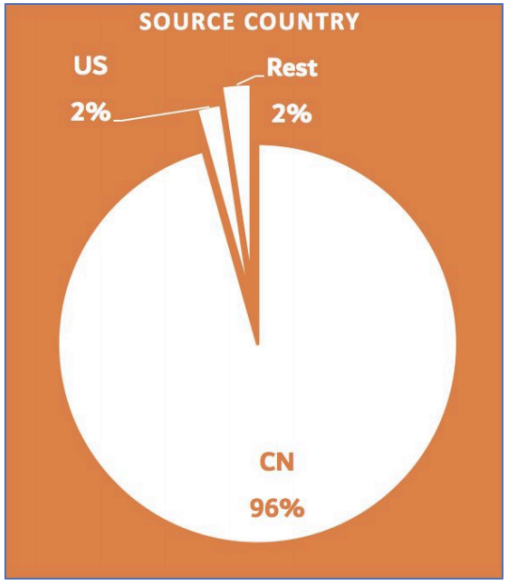
- TCP traffic (mostly HTTP proxy, services).
  - Ports 443, 80, 8000, 8080, 8090, 8765
- UDP traffic (some DNS, syslogs).
  - Ports 53, 514, 8000, 80, 8090
- TP-Link DNS 1.0.0.19
  - https://serverfault.com/questions/365613/ tp-link-routers-send-dns-queries-to-1-0-0-19-what-is-that/365630



CLOUDFLARE

Traffic source

- Aligned with internet populations:
  - Heavily weighted to source from China
  - USA, Other large Internet populations.

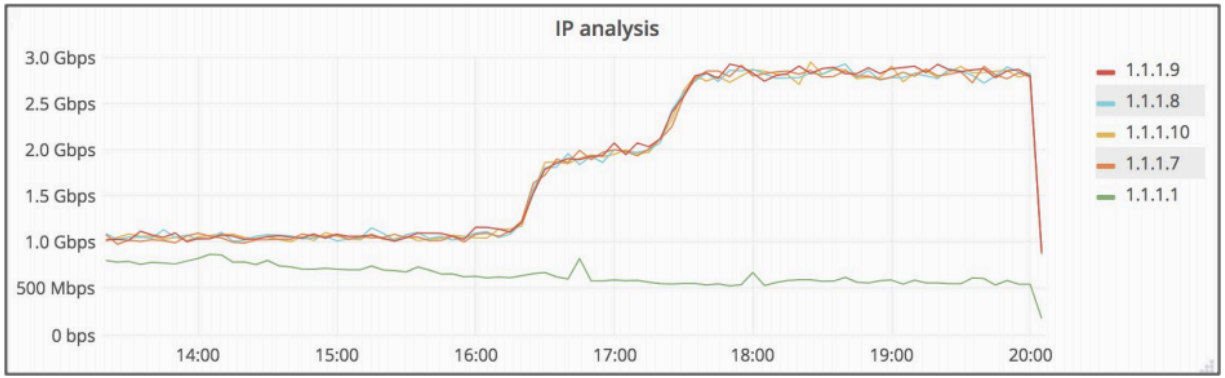


CLOUDFLARE

Bursts and patterns

Two increases:

- 5 Gb/s → 8 Gb/s between 1600 and 1715 UTC
- 8 Gb/s → 12.5 Gb/s between 1715 and 2300 UTC



Mostly on 1.1.1.7, 1.1.1.8, 1.1.1.9 and 1.1.1.10

Destination 80

Increase from China

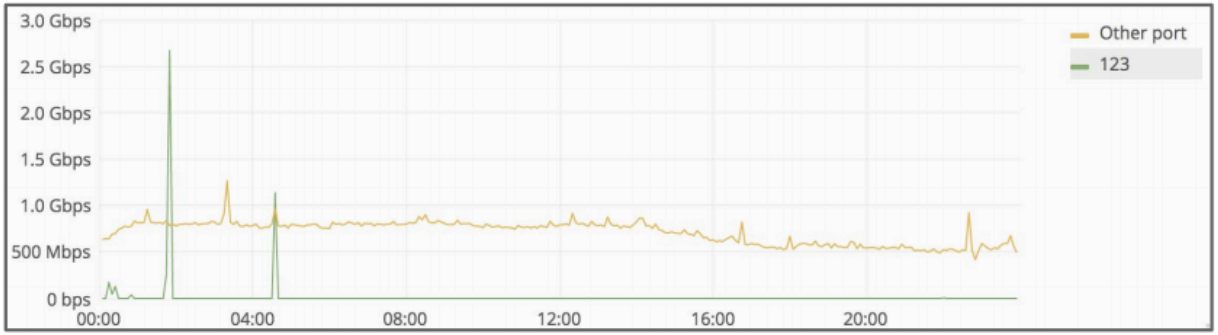
No particular difference on source IP/net

CLOUDFLARE

Bursts and patterns

Short bursts:

- Only on 1.1.1.1 between 0100 and 0200 UTC for a few minutes



1-10 gigabits/sec

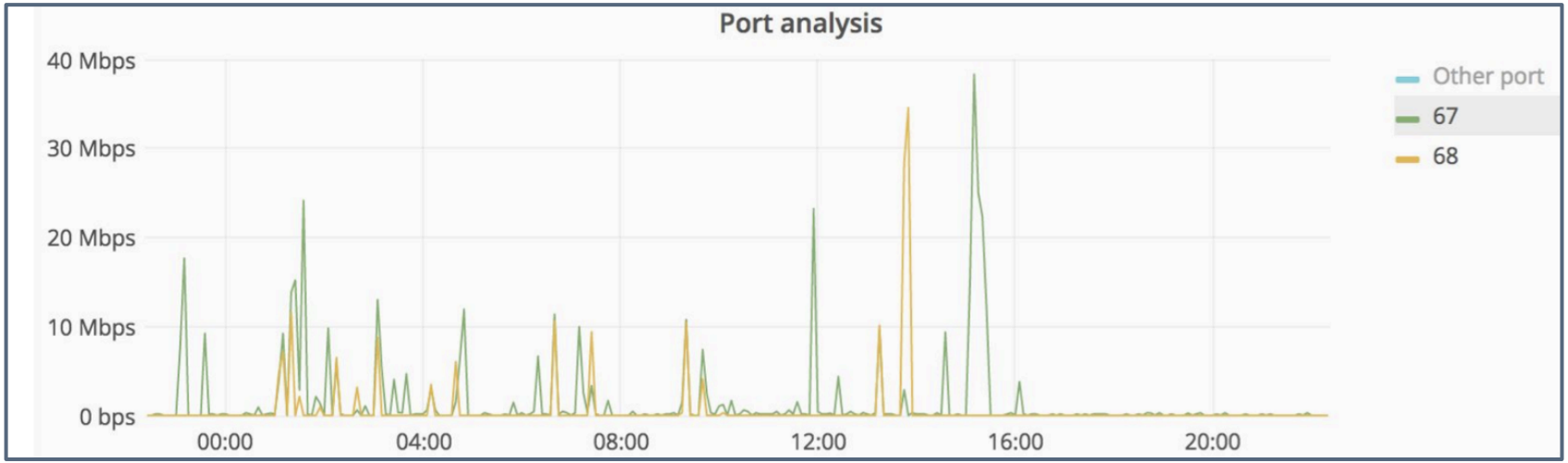
UDP traffic source 123 (NTP) and 11211 (memcached)

Misconfigured network devices?

CLOUDFLARE

Bursts and patterns

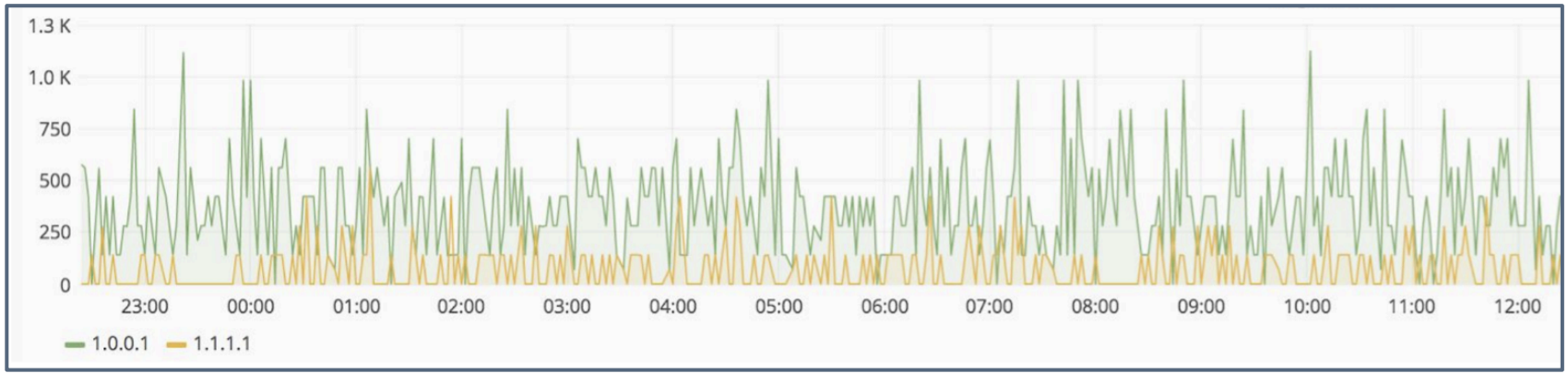
Also **DHCP** spikes. From **Macau**.



CLOUDFLARE

Legitimate Traffic?

Filtering to only UDP/TCP 53, receiving a substantial amount of DNS traffic even before launch.



CLOUDFLARE

What's changed?

Lots of previous studies into traffic profiles:

- Presentation from 10 years ago at NANOG49 https://www.nanog.org/meetings/nanog49/presentations/Monday/karir-1slash8.pdf - Merit, APNIC & UMich
- We still see iperf traffic (port 5000/5001)
- Around 10-20 times more traffic than previous studies.

We estimate legitimate traffic to be around 7-13%

CLOUDFLARE

Availability?

Availability

Thanks to the Atlas probes, we've run thousands of tests:

Time (UTC)	RTT		Hops	Success	
2018-03-28 11:43	7.504		11	✗	ⓘ
2018-03-28 11:43	6.292		11	✗	ⓘ
2018-03-28 11:43	6.260		11	✗	ⓘ
2018-03-28 11:43	8.558		11	✗	ⓘ
2018-03-28 11:43	7.308		11	✗	ⓘ
2018-03-28 11:43	3.412		11	✗	ⓘ
2018-03-28 11:43	33.123		11	✗	ⓘ
2018-03-28 11:43	1.879		1	✓	ⓘ
2018-03-28 11:43	21.928		7	✓	ⓘ
2018-03-28 11:43	11.641		8	✗	ⓘ
2018-03-28 11:43	26.318		4	✓	ⓘ

Null-routes

CPE installed in ISP

…

Suddenly an open FTP Server

CLOUDFLARE

Availability

More than **30** major Internet Service Providers all around the world having issues.

- Many null-routing 1.1.1.1/32
- 1.1.1.1/30 is a favorite point-to-point address
- But also using 1.0.0.0/24 for internal purposes (finding devices)
- Most of the ISPs are cleaning their configurations (more than a dozen fixed in less than a week).
- Few non-responses

Documentation

Documentation

RFC-5737

Internet Engineering Task Force (IETF)
Request for Comments: 5737
Updates: 1166
Category: Informational
ISSN: 2070-1721

J. Arkko
Ericsson
M. Cotton
L. Vegoda
ICANN
January 2010

IPv4 Address Blocks Reserved for Documentation

Abstract

Three IPv4 unicast address blocks are reserved for use in examples in specifications and other documents. This document describes the use of these blocks.

192.0.2.0/24
198.51.100.0/24
203.0.113.0/24

Exist for the soul purpose of documentation, diagrams, etc.

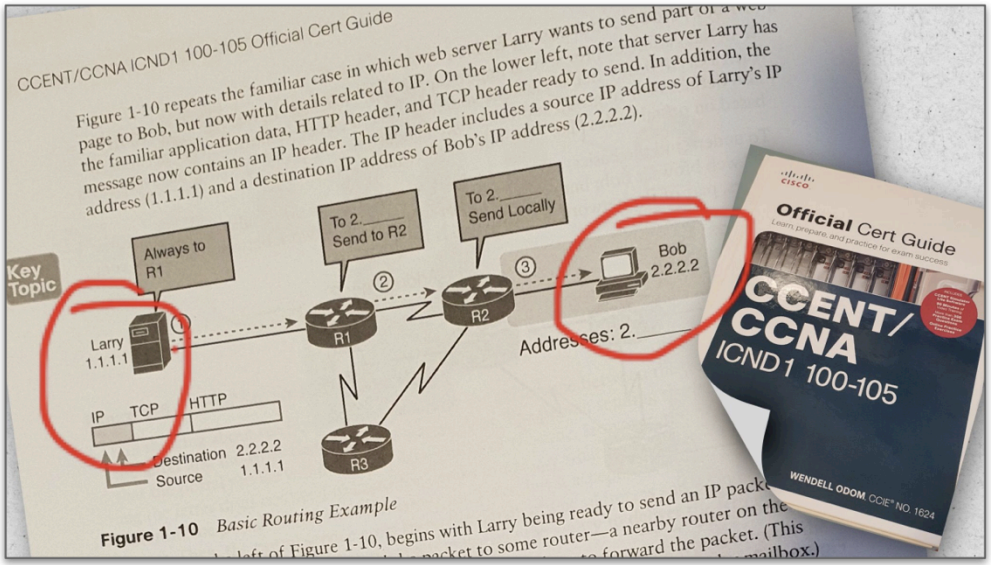
HOWEVER...

CLOUDFLARE

*In addition to performance improvements resulting from the CDN

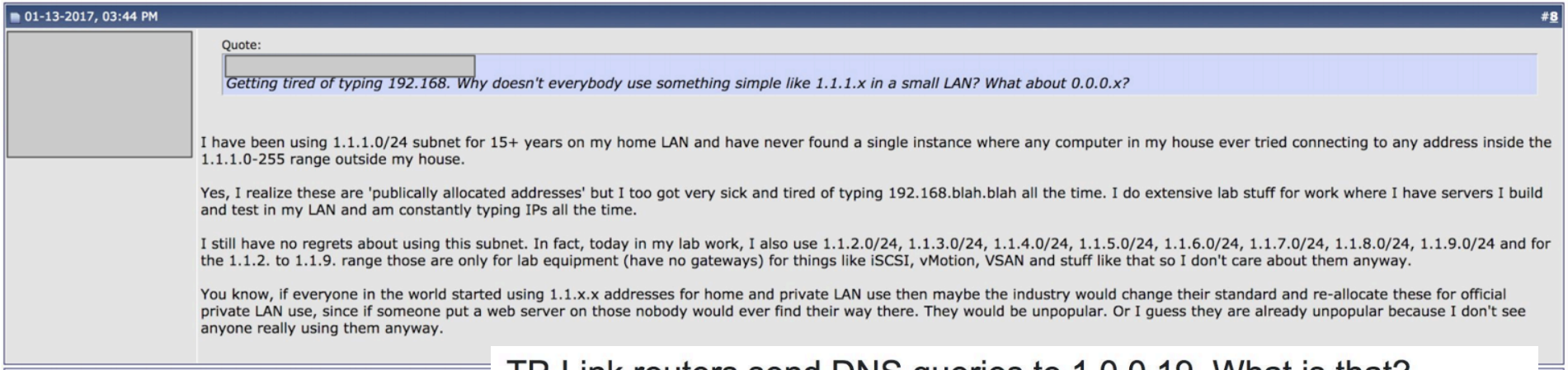
Documentation

Step 32 In the IP Address text box, enter the IP address of the controller's virtual interface. You should enter a fictitious, unassigned IP address such as 1.1.1.1.



CLOUDFLARE

Just doing it wrong



01-13-2017, 03:44 PM #8

Quote:

Getting tired of typing 192.168. Why doesn't everybody use something simple like 1.1.1.x in a small LAN? What about 0.0.0.x?

I have been using 1.1.1.0/24 subnet for 15+ years on my home LAN and have never found a single instance where any computer in my house ever tried connecting to any address inside the 1.1.1.0-255 range outside my house.

Yes, I realize these are 'publically allocated addresses' but I too got very sick and tired of typing 192.168.blah.blah all the time. I do extensive lab stuff for work where I have servers I build and test in my LAN and am constantly typing IPs all the time.

I still have no regrets about using this subnet. In fact, today in my lab work, I also use 1.1.2.0/24, 1.1.3.0/24, 1.1.4.0/24, 1.1.5.0/24, 1.1.6.0/24, 1.1.7.0/24, 1.1.8.0/24, 1.1.9.0/24 and for the 1.1.2. to 1.1.9. range those are only for lab equipment (have no gateways) for things like iSCSI, vMotion, VSAN and stuff like that so I don't care about them anyway.

You know, if everyone in the world started using 1.1.x.x addresses for home and private LAN use then maybe the industry would change their standard and re-allocate these for official private LAN use, since if someone put a web server on those nobody would ever find their way there. They would be unpopular. Or I guess they are already unpopular because I don't see anyone really using them anyway.

TP-Link routers send DNS queries to 1.0.0.19. What is that?

4

I've got a problem with TP-Link soho routers. The DNS forwarder of those routers tends to ignore the DNS servers obtained by DHCP and instead tries sending all DNS requests to this strange IP: 1.0.0.19? That IP doesn't respond.

Has anyone else seen that happen?

domain-name-system

CLOUDFLARE

Just doing it wrong

Not the first time:

- https://en.wikipedia.org/wiki/NTP_server_misuse_and_abuse

Connectivity testing on TP-Link WiFi extenders [edit]

Firmware for TP-Link WiFi extenders in 2016 and 2017 hardcoded five NTP servers, including Fukuoka University in Japan and the Australia and New Zealand NTP server pools, and would repeatedly issue one NTP request and five DNS requests every five seconds consuming 0,72 GB per month per device.[20] The excessive requests were misused to power an Internet connectivity check that displayed the device's connectivity status in their web administration interface.[20]

- Won't be the last...

CLOUDFLARE

Conclusions

Conclusions

Many different types of misconfiguration

Companies possibly leak their private data:

- Syslog
- DHCP data
- Other unknown

We throw away all data, maintain privacy, but not everyone else is nice.

Be vigilant about your own network and follow the best common practices.

CLOUDFLARE

Questions?

Thank you!