

# Internet Traffic 2009-2019

Craig Labovitz

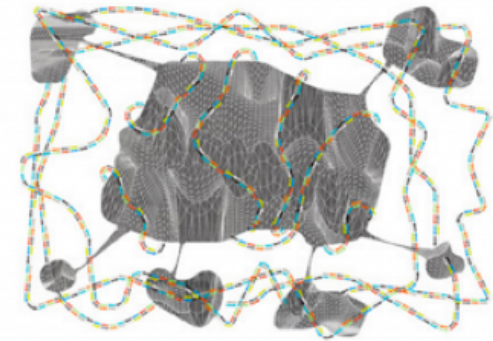
[craig.labovitz@nokia.com](mailto:craig.labovitz@nokia.com)

## Internet Traffic

- Large-scale study of Internet traffic
  - Anonymized IPFIX, gRPC, DNS responses, BGP, SNMP
  - 32 collaborating Nokia customer ISP / content
  - Biased towards NA (with 75% coverage of traffic)
  - But significant Asia Pacific and EU presence
- Methodology similar to 2009 NANOG
  - Preliminary 2019 results
  - Data still needs to be normalized, bias, etc.

### The New York Times

Scientists Strive to Map the Shape-Shifting Net



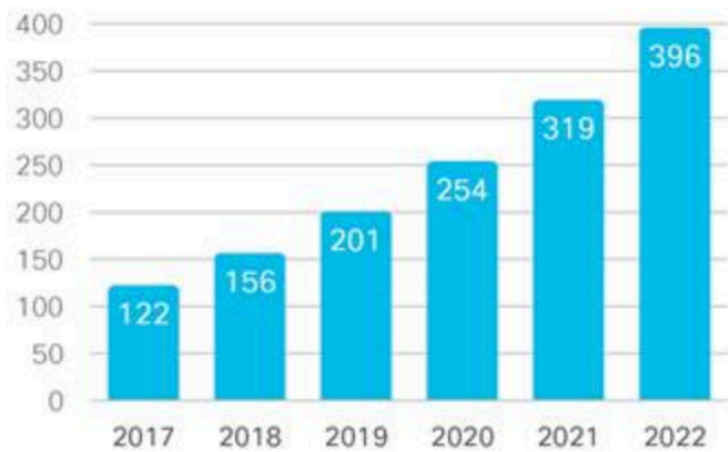
C. Labovitz, S. Iekel-Johnson, D. McPherson, J. Oberheide, F. Jahanian. Internet Inter-Domain Traffic. SIGCOMM 2010

## Observations

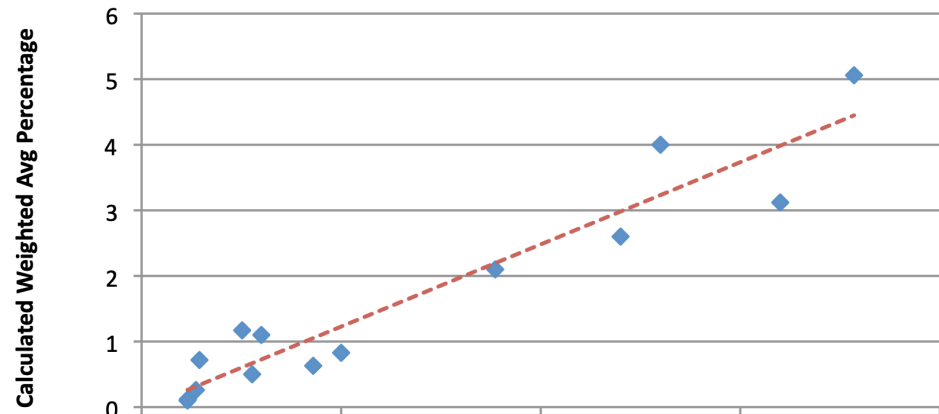
- Internet is getting bigger by traffic volume
- Internet is rapidly getting smaller by concentration of content sources
- By traffic volume, Internet almost entirely completed migration to CDN
- TLS for first time is majority of traffic by February 2019
- IPv6 now at 20% but percentage is no longer growing
- New and long-term existing challenges including regulatory, DDoS, TE time scales

## Estimates of Internet Size

Traffic volumes between 600-900 Tbps



600 Tbps 2019  
Cisco VNI  
(graph shows exabytes per month)



800 Tbps 2019  
Nokia Deepfield

Traffic estimate based on linear regression using known "ground-truth" values plotted against weighted ASN percentage of Internet traffic in all providers in study sample. See SIGCOMM 2009 paper for more discussion of estimation

## Rate of Growth

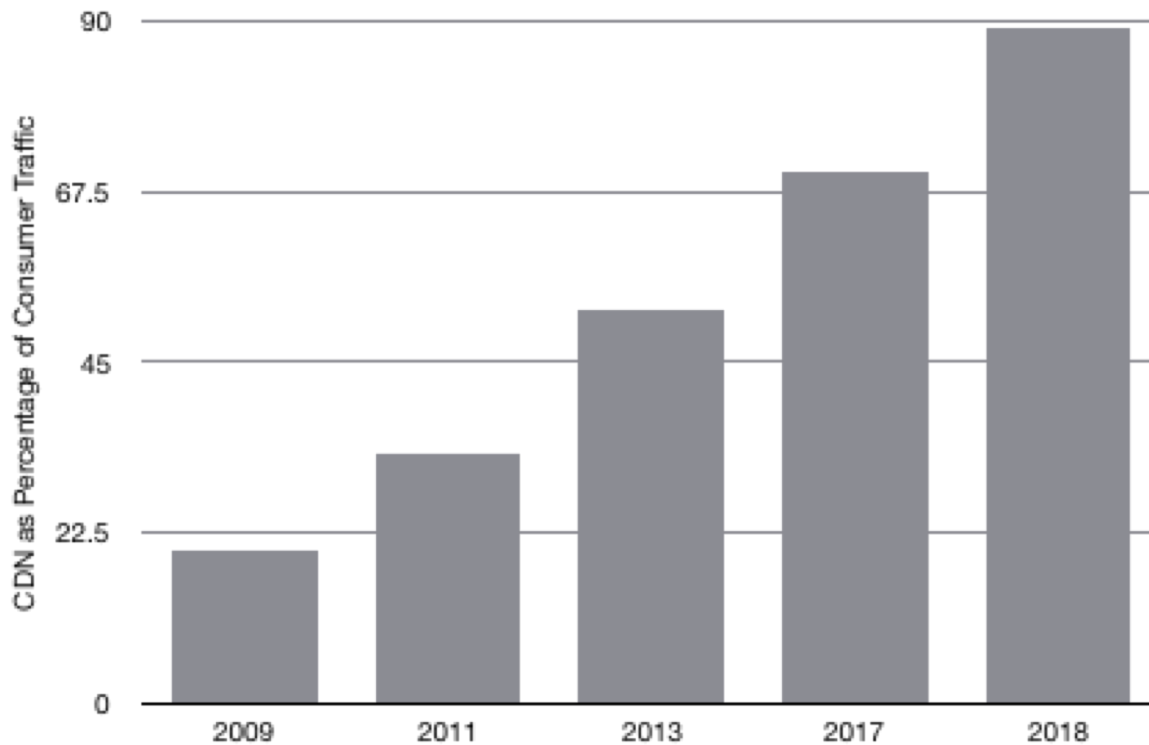
### Example Three Providers 2009 and 2019

Provider	2009 Tbps	2019 Tbps	Multiplier	Region	Type
A	1.6	41	25	NA	Consumer
B	0.5	6	12	Asia	Transit
C	0.14	5	28	NA	Hosting

- Consumer and content 40-50% growth annualized
- Transit growing considerably slower
- Definition of inter-domain traffic increasingly ill-defined (e.g. cloud exchange)

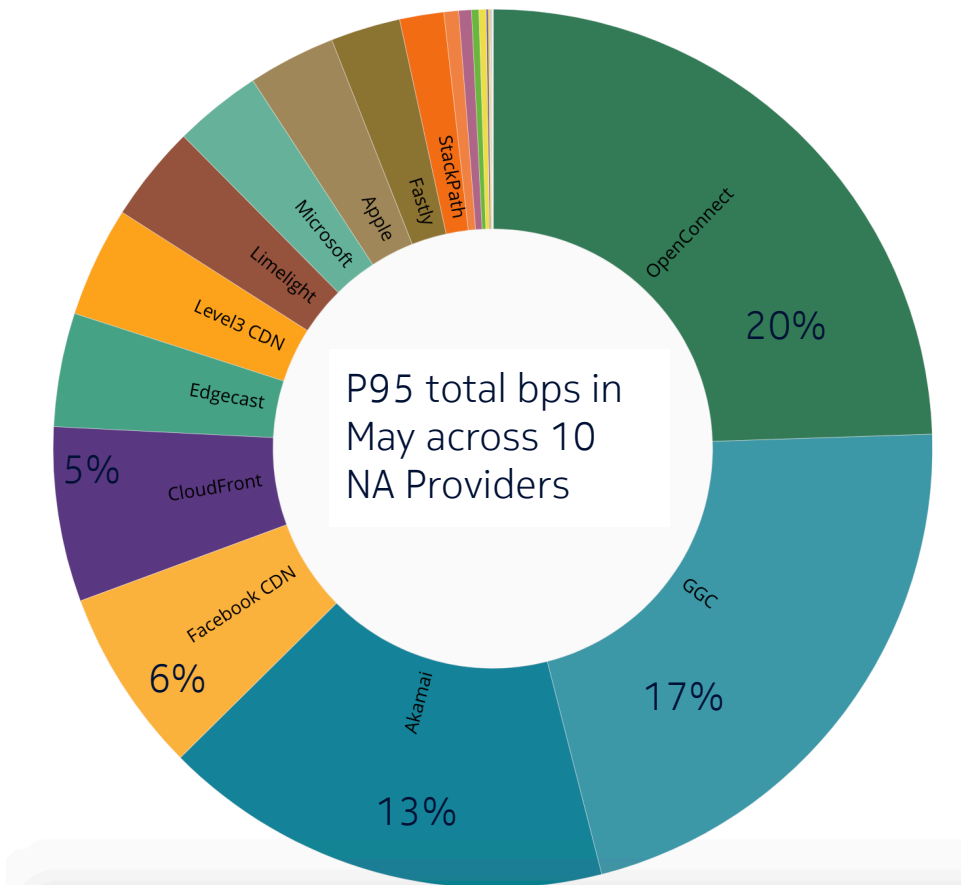
# CDN

## Growth CDN 2009 - 2019



- Globally CDN account for 90% of consumer traffic by 2018
- Definition of CDN blurs as more content providers deploy edge cache and compute
- Nature of traffic changes as adaptive bit rate becomes the norm with automated traffic direction

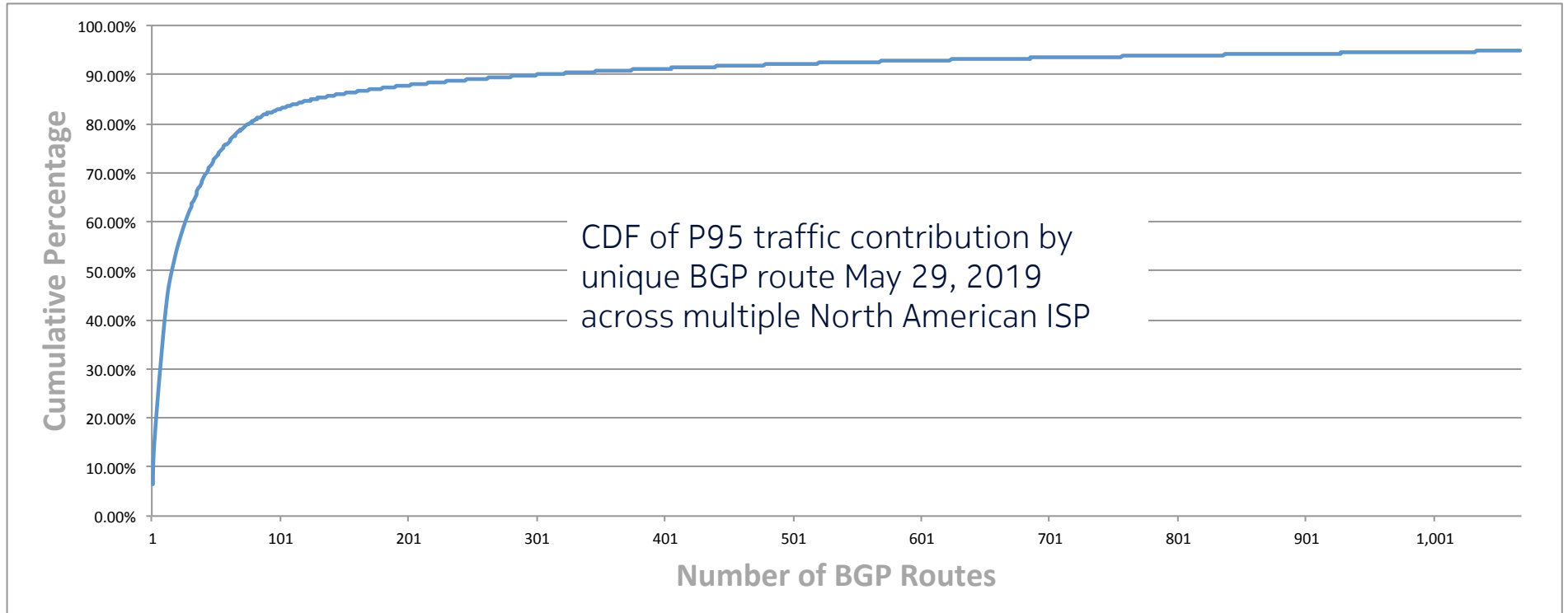
## Largest CDN North America by Traffic Volume



- Netflix and Google largest dedicated CDN
- Significant growth in CloudFront and Fastly
- Traffic not a financial indicator

P95 total de-duplicated traffic to subscribers in May 2019 across 10 NA providers. Excludes provider CDN / VoD, transparent cache and cache fill / origin server.







## BGP Routing Table








~800k routes in default free table but majority traffic due to < 500



# Applications

Sites	Peak Total
 taobao.com	368.1 Gbps
 video.qq.tencent.com	187.6 Gbps
 kwai.com	125.7 Gbps
 baidu.com	123.7 Gbps
 video.baidu.com	96.2 Gbps
 cloud.huawei.com	93.6 Gbps

Asia (anonymous ISP data)

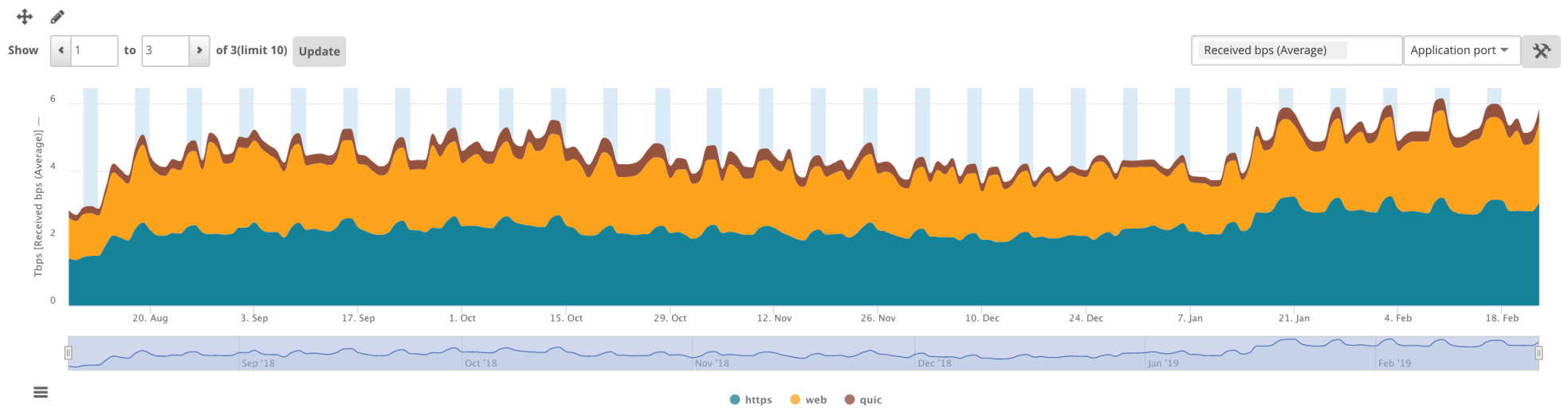
Sites	Peak Total
 netflix.com	762.3 Gbps
 youtube.com	460.5 Gbps
 streaming.amazon.com	325.3 Gbps
 hulu.com	324.6 Gbps
 xboxlive.com	304.5 Gbps
 playstation.com	275 Gbps

North America (anonymous ISP data)

Traffic in EU, NA and Asia dominated by ~10 large sources (though a different 10)

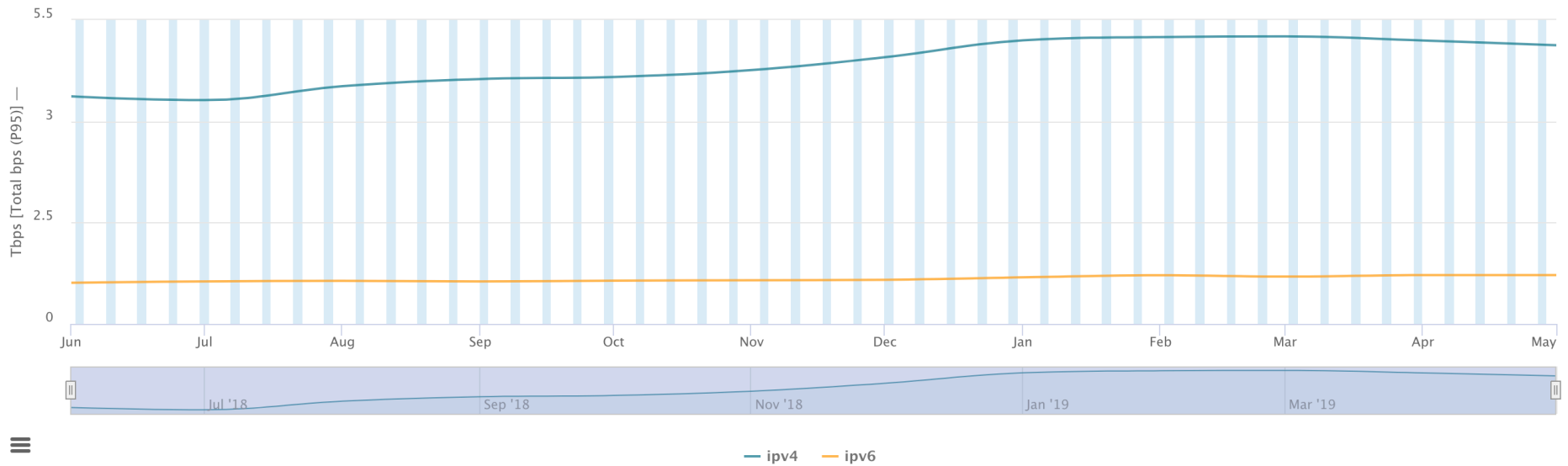
# TLS

## Across Global Sample of Providers



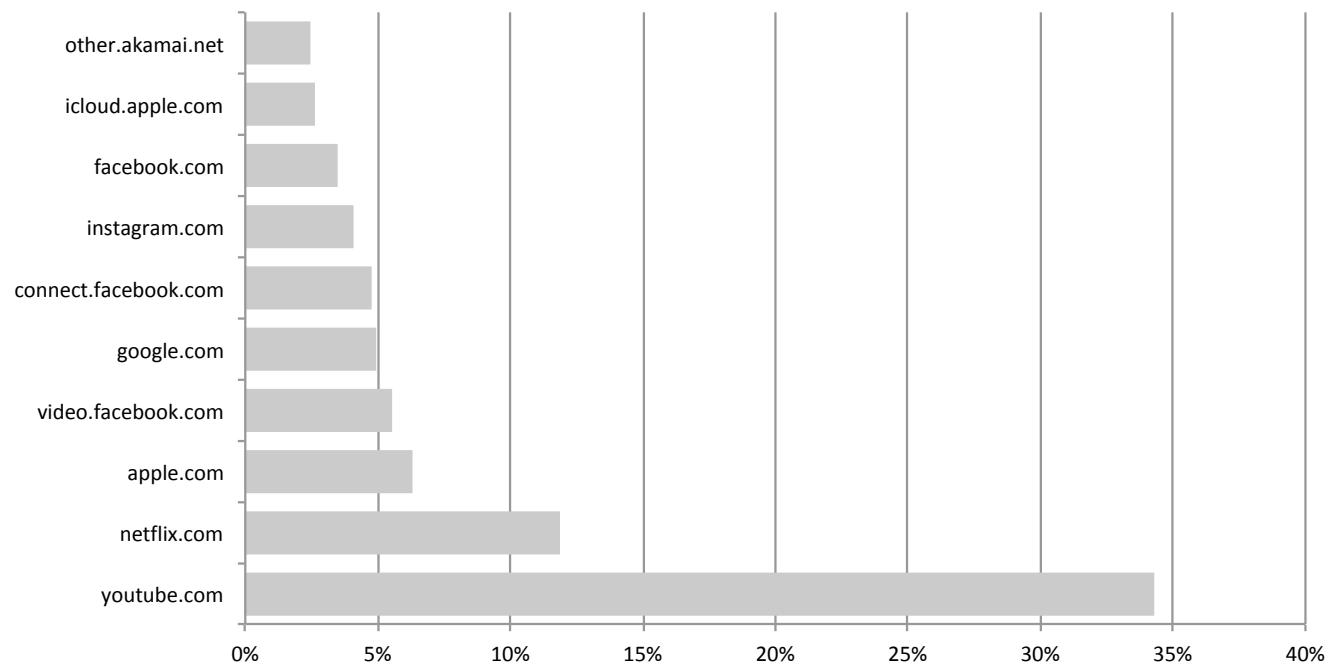
- SSL is majority of traffic in NA by February 2019

## IPv6 and IPv4 Across Global Sample of Providers



- Graph of P95 daily total bps per AF averaged across several smaller NA consumer providers
- IPv6 15-20% of de-duplicated traffic but percentage of IPv4 roughly constant

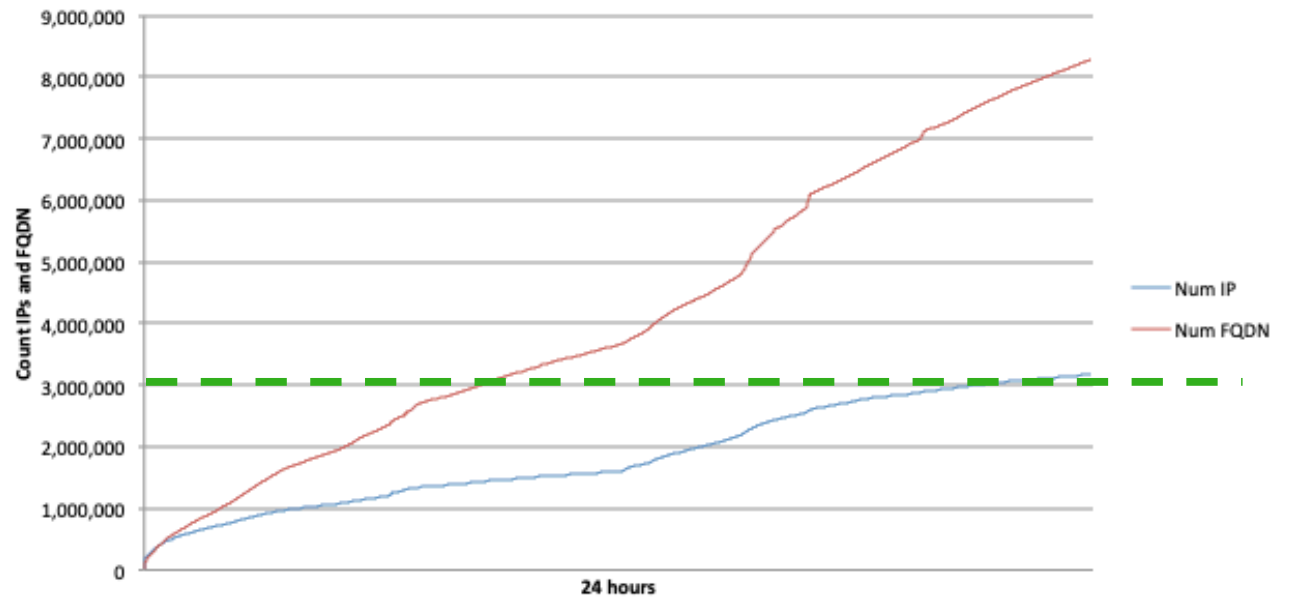
## Small Number of Content Responsible for Majority IPv6



## DNS as Metric of Internet Scale

For practical purposes the Internet is 3M IPs

Analysis of ~1 billion DNS queries across four large consumer networks and sampled recursive responses across 24 hours



And for given ISP, reach 50% traffic with < 100k IPs in a given day  
FQDN continues to grow linearly because abuse and used encode signaling

## Challenges

- CCPA / GDPR impacting low level probe deployment
  - QoE and marketing
- DDoS economics
  - Scale, nature of attacks and response latency
  - Improvements vendor / merchant silicon
- QoE

# Changing DDoS



## Continued Growth Amplifiers and Emergence IoT DDoS IPs seen in traffic / DDoS and responding to external crawls

As of February 23, 2019

Server Type	IP Count
Web Cameras	904,079
Open DNS Resolver (used in ddos)	256,048
Hikvision	126,133
Google GGC	184,092
Open NTP Monlist (used in ddos)	84,090
Google Safe Browsing Malware	12,551

- Same IPs seen in multiple IoT and reflector DDoS across set of providers
- Most traffic not synthetic
- Set attacking IPs often fit within TCAM via FlowSpec / NetConf

Note:

- Directly Internet reachable (i.e. not behind NAT)
- Netcraft reports 8,048,899 IPs in 2018



## Example

### Constant stream CLDAP 1 Gbps across multiple dozen subscribers

Tags: xxxxxxxxxxxxxx

Devices: Playstation

Sampling: 5000,20480

# DDOS 0.878 Gb (93.97 %)

<-	108.49.186.52		29.00 Mb	ddos	udp	123	59272	fios.verizon.net
<-	123.199.53.247	10066	19.33 Mb	ddos	udp	123	59272	
<-	203.109.145.178	9500	19.33 Mb	ddos	udp	123	59272	vodafone.co.nz
<-	122.2.223.146	9299	19.33 Mb	ddos	udp	123	16900	pldt.com
<-	110.47.163.12	17839	19.17 Mb	ddos	udp	123	59272	
<-	118.241.234.135	2527	19.17 Mb	ddos	udp	123	16900	so-net.ne.jp
<-	106.176.204.11	2516	19.17 Mb	ddos	udp	123	16900	kddi.com
<-	122.2.223.146	9299	19.17 Mb	ddos	udp	123	15217	pldt.com
<-	219.95.86.112	4788	9.67 Mb	ddos	udp	123	15217	webcam tm.com.my
<-	90.63.224.232	3215	9.67 Mb	ddos	udp	123	59272	webcam orange.fr
<-	81.250.129.58	3215	9.67 Mb	ddos	udp	123	59272	orange.fr
<-	100.38.4.8		9.67 Mb	ddos	udp	123	15217	fios.verizon.net
<-	219.95.86.112	4788	9.67 Mb	ddos	udp	123	15217	webcam tm.com.my
<-	80.14.230.235	3215	9.67 Mb	ddos	udp	123	16900	orange.fr
<-	216.210.104.172	19662	9.67 Mb	ddos	udp	123	16900	
<-	80.14.234.1	3215	9.67 Mb	ddos	udp	123	15217	orange.fr
<-	110.167.168.198	4134	9.67 Mb	ddos	udp	123	16900	163.telecom.com
<-	217.92.2.83	3320	9.67 Mb	ddos	udp	123	15217	telekom.com
<-	193.248.49.220	3215	9.67 Mb	ddos	udp	123	16900	orange.fr
<-	173.59.112.14		29.67 Mb	ddos	udp	123	15217	fios.verizon.net
<-	61.133.125.174	4837	9.67 Mb	ddos	udp	123	59272	169.chinaunicom.com
<-	114.255.160.168	4808	9.67 Mb	ddos	udp	123	59272	beijing.chinaunicom.com
<-	117.53.253.15	9770	9.67 Mb	ddos	udp	123	59272	

# Questions