NOMINET

Running A Highly Scaled Registry DNS Platform

ICANN 55 Tech Day – Anycast Panel

Chris Griffiths - chris.griffiths@nominet.uk

About Nominet

WE ARE AN INTERNATIONAL INTERNET COMPANY DELIVERING PUBLIC BENEFIT

As an operator of one of the largest Registries on the planet, our DNS just needs to work

- We have millions of businesses and consumers that use our domains on a daily basis
- We need to provide a highly resilient and stable service for our ccTLD and gTLDs

.uk

.co.uk

.CYMRU
.WALES

So Why Anycast?

Anycast enables us to offer one IP from multiple geo-redundant locations for our name servers

- Provides significantly more resiliency than Unicast
- Enables reduced latency and better speed to sites since we can localize traffic to specific regions
- Reduces downtime from maintenance since we can take sites offline without causing an outage to a specific name server
- Helps with attack mitigation since it can increase surface area of your network to attacks

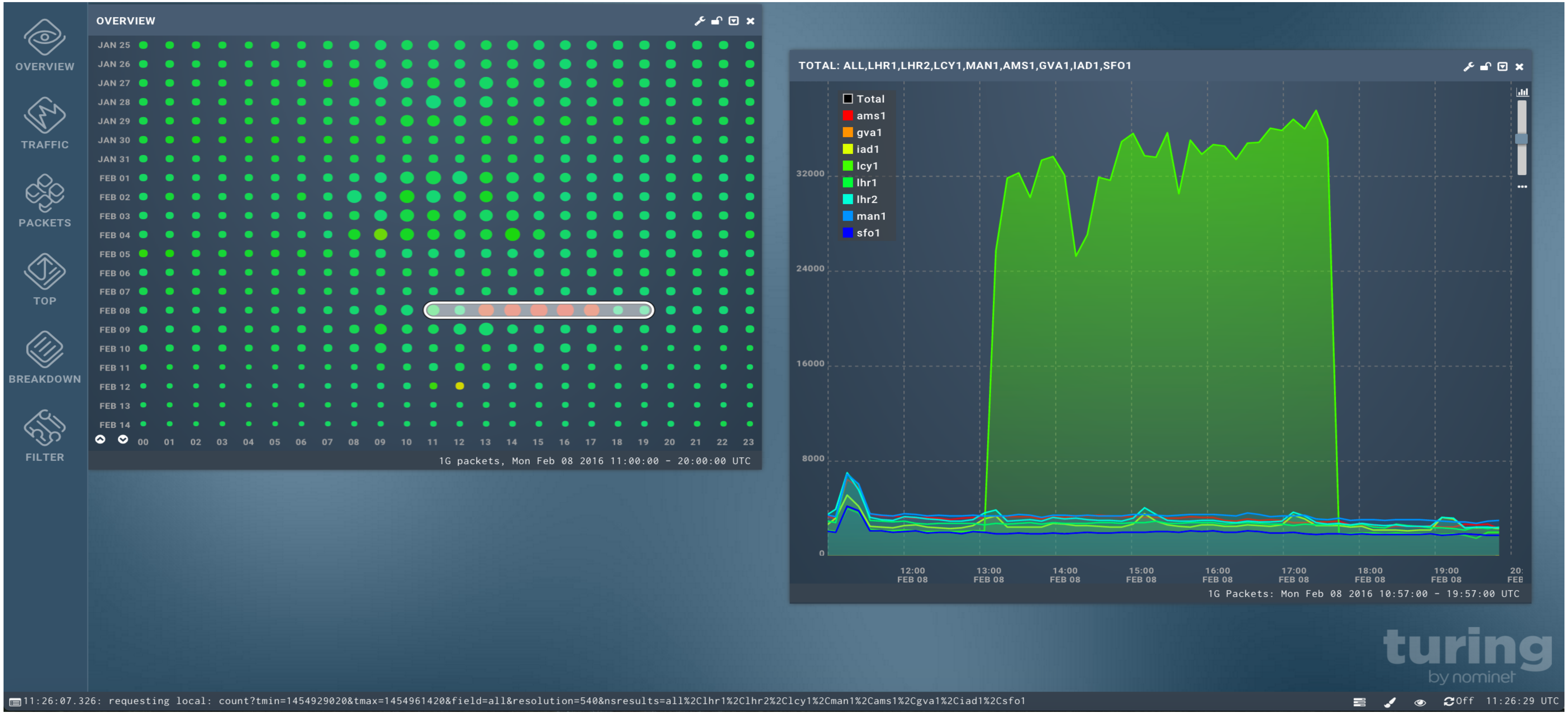
Anycast Deployments Are Not Trivial

Like any good service, Anycast requires a thoughtful design

- It is significantly more complex to deploy and operate than a unicast network
- Depending on your network design, you may need multiple transit and/or peering connections to make it work well
- You need to measure and monitor your services with good network monitoring
- Oh and you need to plan for when things go wrong

So When Things Go Wrong…DDoS

What does an attack look like?

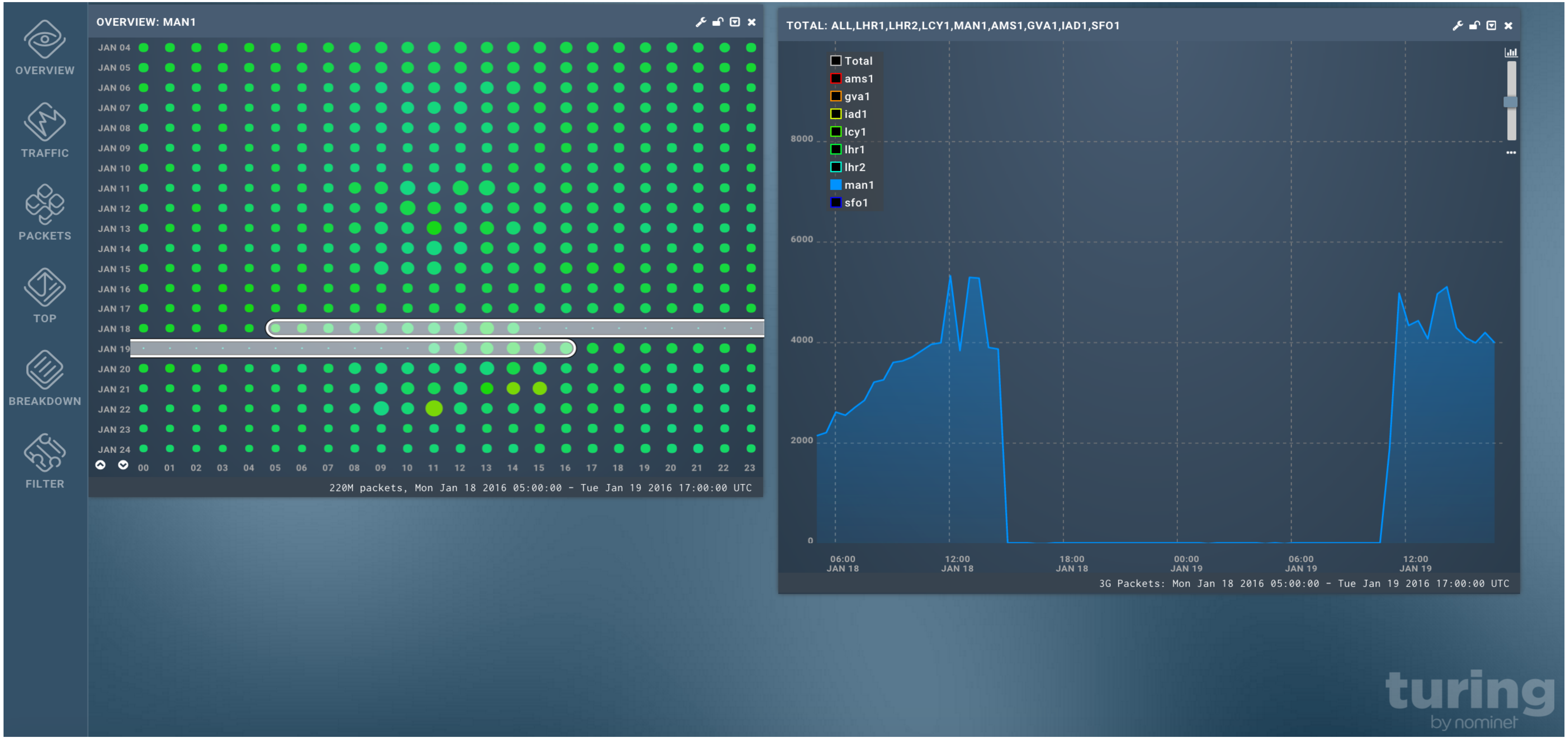


```
11:26:07.326: requesting local: count?tmin=1454929020&tmax=1454961420&field=all&resolution=540&nsresults=all%2Clhr1%2Clhr2%2Clcy1%2Cman1%2Cams1%2Cgva1%2Ciad1%2Csfo1
```

So Where To Put All Of That Traffic

- You can sinkhole the traffic if you plan your network design and have good network monitoring
- Having access to scrubbing equipment either on your network or via a service provided by transit is a good practice
- Build in significant capacity into your network design
- Plan for failure because it will happen

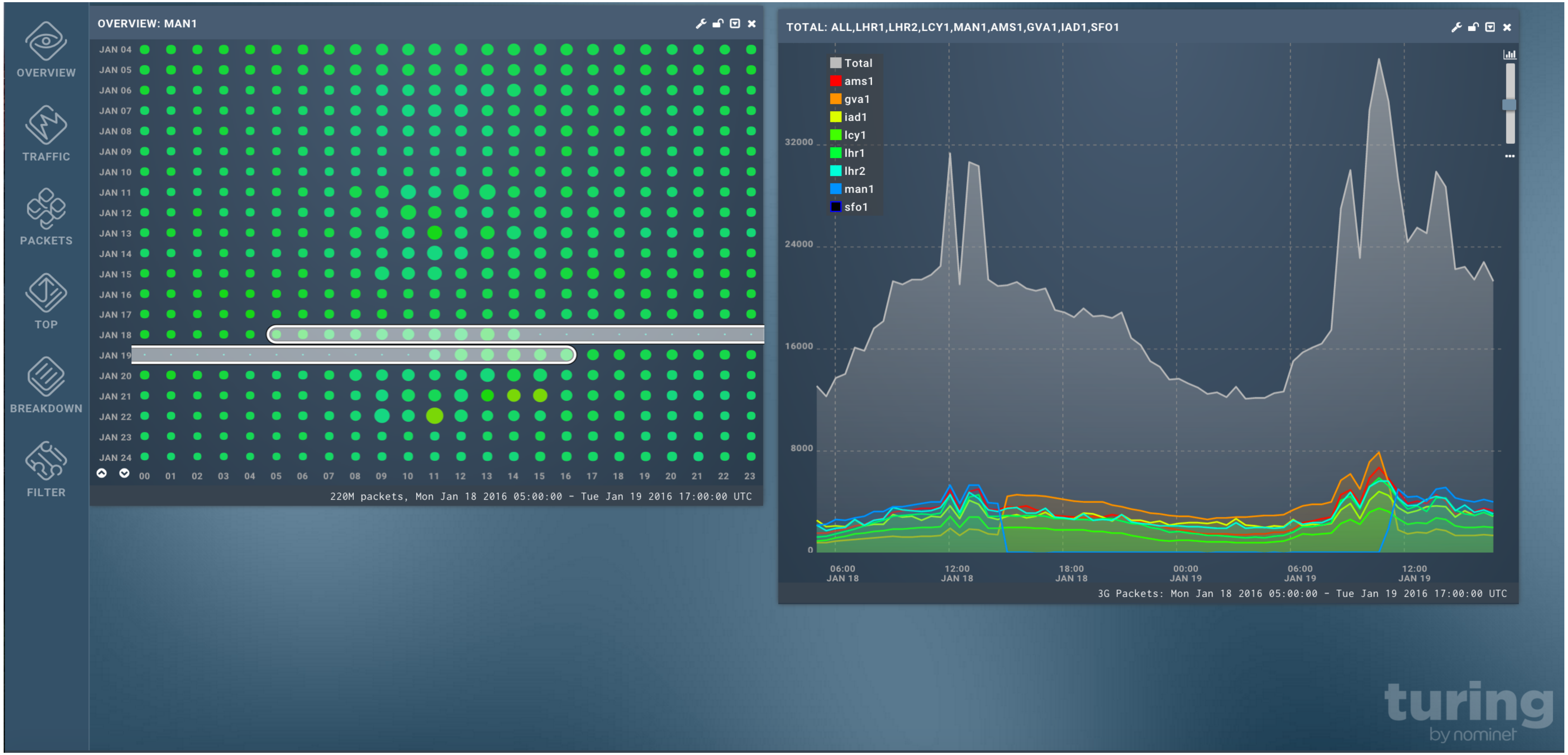
What Does Anycast Maintenance Look Like



```
220M packets, Mon Jan 18 2016 05:00:00 - Tue Jan 19 2016 17:00:00 UTC
```

```
3G Packets: Mon Jan 18 2016 05:00:00 - Tue Jan 19 2016 17:00:00 UTC
```

What Does Anycast Maintenance Look Like



220M packets, Mon Jan 18 2016 05:00:00 - Tue Jan 19 2016 17:00:00 UTC

3G Packets: Mon Jan 18 2016 05:00:00 - Tue Jan 19 2016 17:00:00 UTC

Multiple Vendors = Diversity

- We use different transport providers across multiple sites
- We announce only some of our prefixes out of different regions using different transport providers
- We standardize our hardware using two different vendors and alternate these at each of our sites to ensure diversity
- We have also standardized our DNS software on two different vendors and also alternate these per site

A Bit About Our Platform

Data Center	Prefix 1	Prefix 2	Prefix 3	Prefix 4	DNS Transit	Hardware	DNS Software
LHR1	YES	YES	NO	NO	Provider 1	HW Provider 1	DNS Software 1
LHR2	NO	NO	YES	YES	Provider 2	HW Provider 2	DNS Software 2
LCY1	NO	NO	YES	YES	Provider 3	HW Provider 1	DNS Software 1
MAN1	YES	YES	NO	NO	Provider 4	HW Provider 2	DNS Software 2
AMS1	NO	NO	YES	YES	Provider 1	HW Provider 1	DNS Software 1
GVA1	YES	YES	NO	NO	Provider 1	HW Provider 2	DNS Software 2
IAD1	YES	YES	NO	NO	Provider 4	HW Provider 1	DNS Software 1
SFO1	NO	NO	YES	YES	Provider 3	HW Provider 2	DNS Software 2

Further Distribute Your DNS Via Secondary

- Pick a good secondary DNS provider who can scale with you and supports your network needs
- Create an even larger surface area for your Anycast network
- For our Registry, we want it globally available and to have DNS resolution as close to end users as possible
- Make sure they have good designs and a well thought out security plan

THANK YOU!