/delivers/

No Help Desk for Light Switches

The Unbearable Lightness of Being Everywhere

Joe Ableyjoe

@ableyjoe

UKNOF 27

Technical Awareness of End Users in Decline

Let us rejoice together in our collective lack of surprise

- a consequence of the continued mainstreaming of the Internet as a conduit for all things
  - refrigerators, thermostats, door locks, alarms
  - news, dictionaries, travel, television, phone, mail, everything
- most end-users of bathrooms don't understand plumbing, either

Who do your customers call?

- if a service is broken, call the service operator (maybe)
- if a device is broken, call the shop (maybe)
- if the network is broken, call you (maybe)
- get your teenage child to look at it
- if none of those things work, you're stuck
  - stop using whatever it is
  - oh noes

Outsourced Reliability

- if you're an established outfit with revenue, you can build massive infrastructure
    - expensive, difficult
- if you're a tiny startup perhaps you can't afford the cost of a huge build-out, which is a shame because your idea depends on reliability, more so than the big guys even
    - rise of the data centre, rise of the cloud
    - compute, storage, operations, ... and DNS

Wide-Scale Distribution of DNS Service

- People have been using anycast to distribute DNS service for a long time
  - authoritative DNS service, recursive service
  - protocol is (often, usually) stateless
  - transactions are (often, usually) short-lived
  - largely unaffected by routing churn
    - probably, apparently

How much Anycast is Enough?

F: 56

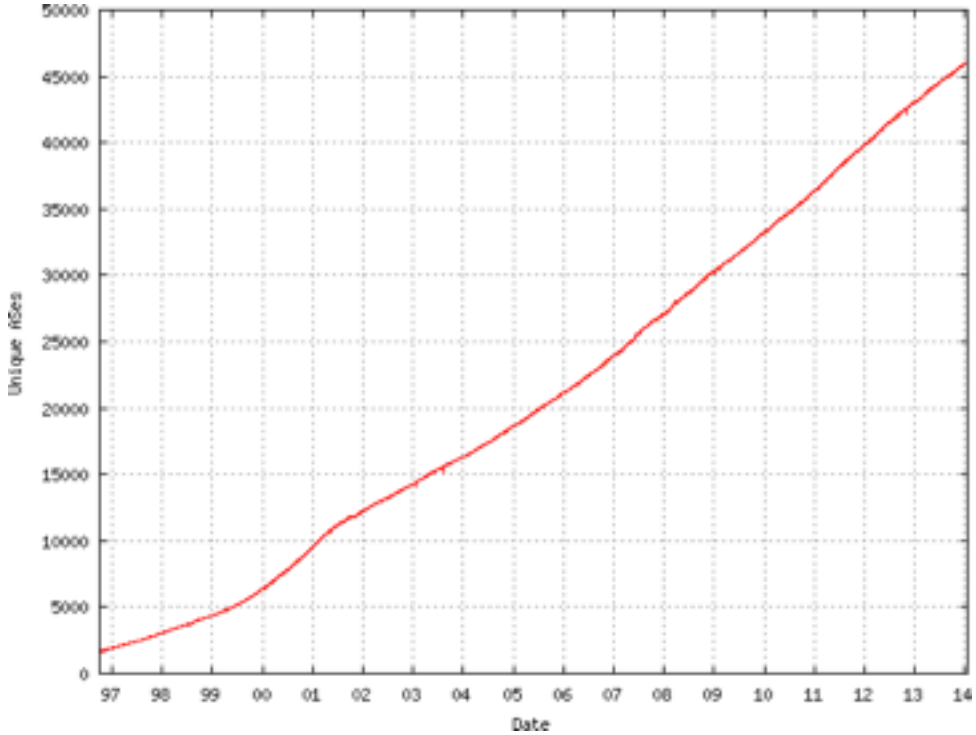
I: 43

J: 74

K: 17

L: 146

How many ASes are there?



Dyn

Aim to Scale

- If we're going to build out DNS service on a grand scale, we might as well aim big
  - "at least one node per AS"
- Keep attack flows on-net
- Minimise the RTT
- Reduce the hardware requirements of an individual node to something that can be built for $1,000 and treated as a network appliance

Operational Implications

- If we don't want to have to hire thousands more people, we need all these nodes to be heavily automated
  - self-service for network operators (renumbering, BGP session maintenance, etc)
  - ship direct from factory to site
  - installation and troubleshooting simplified to a level that would not challenge a small child
  - low-power appliance, suitable for mounting in a two-post rack (no shelves, no rails)

Security Considerations

- Every node (from our perspective) is installed in a hostile, remote network
- Starting point is to assume that Bad People are going to compromise the box immediately, if not sooner
  - no secrets on any node beyond those associated with the node itself
  - regular, frequent, automatic bare-metal reinstallation (like Crashmonkey... Reinstallmonkey?)
  - careful thinking required

Operational Management

- Patch and configuration management (plus associated test processes) completely automated
    - chef
- Element monitoring (centralised and distributed) provisioned along with each node, so the list of things to ping, etc is always complete and up-to-date
    - careful thinking for escalation, to avoid the situation where a single problem causes 50,000 alarms per second, and the NOC shoot themselves

Data Flow

- Many of these nodes will be in dark, cobwebby, poorly-connected parts of the Internet
    - need to be light on the network, and extremely tolerant of congestion and isolation
    - opportunistic peer-to-peer model whereby the swarm of nodes can exchange provisioning data, zone data and measurement summaries with each other
- We do not expect full centralisation of data to be possible, so we need to be able to distribute analysis to the edge

Add it together and what do we get?

- Massively-redundant, massively-distributed DNS service
  - more reliable, faster, very shiny
  - ridiculously scaleable
- A new level of service intelligence
  - as many views of the global routing table as we have nodes
  - an additional dimension for assessing client reputation, significantly less prone to error from external topology changes

Why should any ISP care?

- That's why I'm here. We want you to care. Tell us why you might care.
  - routing intelligence?
  - real-time feeds of information about your customers?
    - long-term trends in DNS use
    - indications of customer infections
  - faster, more reliable DNS service for services that your customers want to be up?

Why should any ISP care?

- recursive service for use by your customers?
- ability to monitor your own infrastructure from many places outside your network?
- DNS services (registration, hosting)?
- something else?

Dyn

SM