Geoff Huston
November 2015

RIPE 71 Meeting Report

The RIPE 71 meeting took place in Bucharest, Romania in November. Here are my impressions from a number of the sessions I attended that I thought were of interest. It was a relatively packed meeting held over 5 days so this is by no means all that was presented through the week. More can be found at the RIPE meeting website (https://ripe71.ripe.net).

A presentation on Mobile Satellite services looked at the Inmarsat IP environment. This service uses a constellation of spacecraft parked in geostationary orbit, which means that any signal that is bounced off these spacecraft has to travel a minimum of 35,786km up, and the same back down. Of course if you aren't directly below the spacecraft it will be a longer trip. If you plug in the speed of light in a vacuum of some 299,792,458 m/s, and factor in the earth's roughly spherical geometry then its typically between one quarter to one third of a second to get a signal up to the spacecraft and back to earth. It also costs significant sums to build and launch these spacecraft into orbit, and they have a limited life due to the need to use thruster fuel to stop the oscillation induced by the moon. And of course there is the issue of spectrum. Ku band systems operate in the 12 - 18Ghz band, which offers a reasonable compromise between power, bandwidth and rain attenuation. Little wonder that such services are expensive and limited in their capability. That it works at all is a triumph of engineering. Inmarsat currently provides a broadband data carriage service, which can operate at speeds of up to 492Kbps. Issues with an IP service over this medium include issues of reliability, unwanted traffic and firewall setup and infected guest systems. The challenge of providing IP services in that of creating a robust unmanaged IP system that is fully functional, yet capable of defending itself not only from the toxic public Internet, but also capable of defending itself from infected connected user devices! The speed of light isn't changing anytime soon, nor is the mass and rotational velocity of the earth (or at least what's what we hope!) so geostationary satellite systems will always have delay to factor in. Low Earth Orbit (LEO) constellations can counter this, but these LEO spacecraft are moving relative to a fixed point on the earth so continuous service requires a larger constellation of spacecraft to offer the same global service coverage as 4 or 5 geostationary spacecraft. Inmarsat is responding by launching its I-5 spacecraft, each of which use 89 small Ka band transponders (at 27-31Ghz), which can provide a digital carrier of 60Mhz. Inmarsat are looking at the airline industry as a major customer for this high capacity IP service.

On a completely different note there was a presentation on Automated Certificate Management. For many years server security has been positioned as a luxury good. While a domain name might cost a few dollars a year, a security certificate can cost ten's or even hundred's of times that cost. In a world of pervasive surveillance and toxic attacks by highly capable agencies there has been a pushback to provide decent security services as a commodity good. One such project is the combination of ACME and Let's Encrypt. The problem that ACME is addressing is that not only is certificate issuance expensive, but its also needlessly complex and most potential users are deterred from even applying for a domain name certificate. The ACME work builds on the REST API framework to generate Certificate Signing Requests for EV domain name certificates that can be used by any CA to provide a largely automated service interface for certificate maintenance. ACME uses a proof of possession test by having the applicant place a named token on the domain name's website. One the applicant passes

the proof of possession test, the applicant can then generate certificate signing requests. The Let's Encrypt is a Certification Authority that will offer free certificates using this REST API interface. A Public Beta service for Let's Encrypt opens on the 3rd December and there are already a number of open source efforts (such as the rather neat https://meetings.icann.org/en/dublin54/schedule/mon-tech/presentation-iencrypt-19oct15-en.pdf) that are intended to make use of this interface to provide ready-to-use user tools.

The lightning talk on traffic dependences between IXPs showed that incidents at one major exchange point will have cross impacts on neighbouring exchanges. Traffic paths on the Internet are very often asymmetric, and altering the flows through one path will create impacts on other paths. I was amused to see the presenter advocate the widespread adoption of path symmetry as a possible response. I thought that the whole idea of packet switching was to improve the efficiency of networks by removing the overheads of maintaining virtual circuits across the network!

There was an interesting report on BGP hijacks (https://ripe71.ripe.net/presentations/33-bgp-experiment-ripe71.pdf). In this experiment they deliberately announced a 'borrowed" route on exchanges, targeting the route announcement at each exchange point in turn, and counted the number of peers at these large exchanges that picked up and learned the route without any reference to a route registry entry of any other form of pre-provisioning. The experiment used simple pings to the exchange neighbour with a "borrowed" address as the source of the ping. In some ways this experiment just confirms what we see each and every day with routing leaks: few folk filter and stuff just permeates through a loose fabric of mutual trust. Little wonder that abuses are so common!

The presentation on high speed packet capture was somewhat esoteric. Their goal was to perform packet capture at rates up to 15M packets per second. This gives a time budget of 67 nanoseconds per packet, which is beyond the capabilities of most systems. In this case they used Intel's Data Plane Development Kit (DPDK), a library that permits the network interface to DMA directly into memory. The approach is to use an Openflow switch to create a set of segmented packet streams and perform packet capture on each stream and then reunite the packet logs offline. This is a classic application of the scaling technique of splitting a hard serial problem into a number of parallel smaller and tractable serial problems.

There is a continued interest in exploring remote-triggered black holes as a means of pushing the route filter rules for DDOS mitgation closer to the sources of the DOS traffic. The presentation on fastmon was on the combination of sflow traffic monitors with thresholds and the translation of over threshold traffic into a BGP flowspec for remote black holing.

There has been considerable interest in recent times in mapping and monitoring the network. Of interest these days is the challenge of mapping the instance of anycast services, such as the location of Google's public DNS servers, or the location of instances of Cloudflare's points of presence. Better overall Internet performance in terms of the user experience is all about the combination of adequate capacity and reducing delay. Understanding the relative location of users and the content that they are attempting to access, and the networks paths that lie between these two points can lead to better performing networks. One presentation was concerned with geo-locating anycast service instances, using distributed traceroute measurements and probabilistic determination of location using speed of signal propagation times. The second concerns a new program to monitor mobile networks by using in-band active measurement (Monroe).

Its good to see the network management story finally improving. For decades the state of the art was SNMP and Expect scripts driving the equipment's CLI. If you were really sophisticated you also ran Rancid to detect config changes to the production network components. But that was where it sat. And it's not very good. The presentation by Facebook is illustrative of a number of large scale provider's efforts to improve upon this story. They have tried to use a suite of conventional artificial intelligence techniques to detect patterns in reported network events and to associate remediation actions to these events, with considerable success evidently. The underlying tool set now includes Git to support shared

code and versioning, and tools such as Ansible, Puppet, Chef and Salt to manage the various configurations and their dissemination. Behind all of this is a long anticipated away from ASN.1 as the lingua franca of network management and in its place its now JSON or YAML. It's a long anticipated and welcome move in the area of network management.

The weekend prior to the RIPE meeting there was a two day "hackathon." Out of this came a rather neat piece of code, arising from a hack team lead by Martin Levy of Cloudflare, "ASNtryst" (https://ripe71.ripe.net/presentations/102-RIPE71_ASNtryst_RIPE_Atlas_Hackathon_Project.pdf). The approach is delightfully simple: take a set of hop-by-hop traceroute records and locate in the traceroute those steps where the originating AS changes, and geolocate these points of AS exchange. By analysing enough of these traceroutes, the result is a surprisingly good map of where networks interconnect.

As is usual for RIPE meetings it was a well organised, informative and fun meeting to attend in every respect! If you are near Copenhagen in late May next year I'd certainly say that it would be a week well spent.

Author

Geoff Huston B.Sc., M.Sc., is the Chief Scientist at APNIC, the Regional Internet Registry serving the Asia Pacific region. He has been closely involved with the development of the Internet for many years, particularly within Australia, where he was responsible for building the Internet within the Australian academic and research sector in the early 1990's. He is author of a number of Internet-related books, and was a member of the Internet Architecture Board from 1999 until 2005, and served on the Board of Trustees of the Internet Society from 1992 until 2001 and chaired a number of IETF Working Groups. He has worked as a an Internet researcher, as an ISP systems architect and a network operator at various times.

www.potaroo.net

Disclaimer