Thinking about IPv6 Failover

Rob Currie, Edinburgh University/GridPP-UK
Context

• Recently suffered networking incident datacentre at Edinburgh Tier2 which impacted only IPv6 traffic.

• Site is still running DPM (there is a plan to migrate) which didn’t react well to broken IPv6. Effectively this took our storage offline.

• Communicating that the loss of IPv6 was important to an external contractor via a university networking team proved challenging.

• In conversations there was concern that dual-stacking IPv6 might be seen as additional point of failure rather than adding resiliency.
Quick Testing

• IPv4 hosts could access any un-impacted resources that were dual-stacked form testing. External access from dual-stacked clients proved problematic.

• XRootD (and some http(s)) transfers from remote (dual-stacked) hosts were incorrectly being flagged as failed due to timing out.

• xrdcp took 90s before failing over to IPv4 which is like the openSSH client.

However, curl downgraded almost instantly when querying a https endpoint.
What should we expect?

• Site was incorrectly **not** marked as unavailable.
  (Availability/Reliability tests appeared to be unexpectedly timing out, need to investigate)

• Initially it wasn’t clear what services were impacted or how.
  (as normally happens after an unexpected a networking incident, the initial panic from admins is to find out how the service has died assuming software first)

• Should HEP tools be expected follow the example of *openSSH* or *curl*?