# Post Incident Review

datanet.co.uk
Private Cloud Solutions

**Date:** 11th February 2016

**Author:** Neil Sperring, Technical Director
Case ref: 33-22239 – Major Service Outage (MSO) 10/02/16 between approximately 15:00hrs and 16:20hrs.

**Contents:**


**1. Report Aims**
This report has been produced by Datanet to provide further detail and clarification of the issues which impacted the entire Datanet core network, resulting in a loss of services on the 10th February 2016.

**2. Customer Impact, Experience & Affected Infrastructure**
A complete loss of connectivity across the Datanet core network resulting in Co-Location, Hosting, Broadband and Point-to-Point circuits terminating through the core network being unavailable between the hours of approximately 15:00hrs and 16:20hrs.

**3. Incident Summaries**
At approximately 15:00hrs, the Support desk started receiving calls from customers describing a complete loss of services and reachability to the Aspen House Fleet (AHF) Data Centre. At the same time, our internal monitoring started alerting us to a loss of connectivity to our two London Data Centre sites. Immediate checks were carried out to ensure there were was no major incident on the data centre floor or within the Telco room at AHF.

It was swiftly discovered that both our London sites were unreachable due to the extensive load on the core equipment at both sites. We therefore instructed remote hands to reboot the equipment in both sites and disconnect our LINX peering connections as it was suspected by tools external to our network that we had suffered a complete loss of BGP services.

Taking this action forced all traffic to go over our Transit connections and gradually services were restored and customers were reporting that connectivity had been restored with the exception of two Co-Location customers in the Aspen House DC which required further attention. The incident was concluded at around 16:20hrs.

**4. Root Cause**
The root cause of the failure has been identified as a route leak into our core network caused by a peer on our LINX peering. All our LINX peers should have a MAX PREFIX LIMIT applied to prevent a large number of routes being advertised into our network.

Our procedure since late 2014 is such that all peers facing us from LINX have a MAX PREFIX LIMIT applied and whilst this has been adhered to, we have since discovered historic entries which have not followed best practice with a number of peers at our Telecity HEX site not having the necessary filters applied to protect us from such incidents.

**5. Risk Mitigation, Key Observations & Lessons Learnt**
The process whereby we add peers to our LINX connections since late 2014 have been carried out in accordance with best practice. The observation here is that steps should have been taken to retrospectively check all the existing peers for MAX PREFIX LIMIT values.

These checks are now being performed prior to us bringing our LINX connectivity back online.

The Management Team sincerely apologise for the impact caused to our partners and their customers as a result of this unplanned event on our core network. Should you wish to have a detailed conversation surrounding this incident, please contact our Technical Director on 01252 810010.