Routing Problems in West Cambridge
24 January 2022

Paul Mazumdar (HEAT Incident #625464)

Background

The Major Incident initially masqueraded as desktops on the ACN and in a number of Institutions in West Cambridge intermittently experiencing connectivity failures. Subsequent investigation traced the issue to a router that had reached an unstable state. Rebooting this router solved the problems.

Timeline of Events

<table>
<thead>
<tr>
<th>Date/Time</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>24 January 8:30</td>
<td>Approximate time of router generating problems.</td>
</tr>
<tr>
<td>(estimated)</td>
<td></td>
</tr>
<tr>
<td>9:08</td>
<td>First call to Service Desk, from a user in the Anne Maclaren Building on the Addenbooke’s site. At this stage the problem is perceived to be on the ACN.</td>
</tr>
<tr>
<td>9:43</td>
<td>Post to Investigation Room channel on Teams draws responses that reveal that the issue is not limited to the ACN, but seems to be confined to West Cambridge in some manner. The School of Veterinary Medicine and Clare Hall are reported as affected. Later it also became apparent that there had been issues with wireless APs. The ACN as a whole was affected because traffic is transferred between the ACN and the UDN through two firewalls which connect at two sites, one of which is in West Cambridge.</td>
</tr>
<tr>
<td>10:17</td>
<td>An e-mail is sent from the Service Desk to ACN users reporting that there is a problem that is being investigated.</td>
</tr>
<tr>
<td>10:18</td>
<td>The Incident is declared a Major Incident. The MI Manager sets up a dedicated Teams channel, invites interested parties to join it and sets an MI meeting for 10:30.</td>
</tr>
<tr>
<td>10:26</td>
<td>HEAT alert is set on Analyst dashboards.</td>
</tr>
<tr>
<td>10:27</td>
<td>Announcement created on Service Desk phone number.</td>
</tr>
</tbody>
</table>

1 dist-nms & dist-west
10:30  **MI meeting 1.** There was a lack of technical information as Network Systems were already having their own investigative meeting. The Communications Lead for the incident agreed to set the ITSS status to Amber with a short explanation and send a message to uis-announce broadly echoing the earlier e-mail to the ACN. The next MI meeting was set for 11:00 in the hope that someone from Network Systems would be available by then.

10:43  ITSS set to Amber and message sent to uis-announce.

11:00  **MI meeting 2.** The Network Systems team believed that by mapping systems experiencing difficulty they had identified that a particular router\(^2\) was at fault. They had decided to reboot that router and it was in the process of restarting. Preliminary tests during the meeting were positive but as the original fault had been intermittent it was decided to meet again at 11:30 and check that there had been no recurrence.

11:30  **MI Meeting 3**
There had been no repeated issues reported since the router had restarted so the Comms lead was asked to send out a message reporting the restoration of the service and the Major Incident was declared closed.

11:41  ITSS status set to green.

11:42  All-clear message sent to uis-announce

11:45  Resolution message sent from Service Desk to ACN staff

25 January  Subsequent to closing the Major Incident, it became apparent that some Institutions were still having issues. These were all connected to the router that was originally rebooted, which suggested that the problem might not have been resolved; further investigation led to the rebooting of a second router\(^3\) and at the time of writing this appears to have resolved the final issues.

**Analysis**

Network Systems resolved the problem swiftly and efficiently by identifying the perimeter surrounding the problems and focussing on the network device at its boundary. It had not been immediately apparent that the routers had been the problem as the majority of sites connected to them had not presented any problems and the routers were reporting normal levels of load, link errors, memory usage, etc. There were a number of confounding factors that slowed this process including one Institution doing a black building test that was originally perceived as a fault, another creating a network loop that caused local effects and a lack of detail on some of the HEAT tickets.

---

\(^2\) dist-west

\(^3\) dist-mwest
There was no obvious original cause, though the original router had been running without a restart for over two years. The timing suggested that the network loop may have been the trigger, but this is heavily circumstantial.

In the absence of a smoking gun, it is hard to point toward specific lessons to learn for next time. After the discussion in the third MI meeting, Networks would be looking at whether the length of uptime of the router may be a factor and, if it were, restarting them more frequently while the Service Desk would be looking at whether there could be a series of forms put together for network problems, e-mail problems etc. for Service Desk analysts to use to solicit further details in cases of reported faults. On this front, Networks were also considering a web page containing recommended diagnostics to which Computer Officers could be pointed or the running of short courses on this. All these are ongoing discussions.

PM 26.1.22