TelcoSwitch

INCIDENT REPORT

Service Impact	Intermittent issues with inbound calls from upstream carrier
Internal Severity Classification	Major incident
Incident Timeframe	25/01/2023, 11:15 - 11:54 GMT

1. Synopsis

- Inbound calls failed to successfully complete, with inbound callers experiencing no dialling tone when attempting to dial numbers routed through specific upstream carriers.
- Issue was not systemwide and impacted a small cohort of customers.

2. Additional Facts

- Extension-to-extension calls routed successfully.
- CallSwitch servers remained operational.
- All network elements were operational and working as expected throughout.
- No major changes made to the environment prior to the incident.

3. Timeline

Time	Event
11:15 GMT	Reports received of inbound calls failing on certain tenants.
11:18 GMT	Incident scope increased to customers using CC servers.
11:20 GMT	P1 incident raised within TelcoSwitch technical services team.
11:21 GMT	Unconfirmed reports of upstream carrier issues.
11:25 GMT	Network inspected for any anomalous behaviour. Routes to major carriers not shown to have any issues.
11:26 GMT	Upstream carrier identified as source. Information gathering and testing commencing to determine full incident scope.
11:29 GMT	Ticket updated with upstream carrier.
11:40 GMT	Manual checks against equipment that peers with upstream carrier is showing a drop in traffic. BGP peers are working as expected.
11:45 GMT	Monitoring checks report that calls per second dropped.
11:54 GMT	Upstream carrier tests running – calls now routing normally.
12:07 GMT	Issue is being monitored for any further issues.
12:25 GMT	Calls per second monitoring has reported normal call behaviour.
12:30 GMT	Escalation team stood down. Commence extended monitoring period.

3. Conclusions

The root cause of the loss of service has been traced back to carriers upstream of TelcoSwitch who utilise Microsoft Azure infrastructure.

As well documented in the press this morning (25.01.2023) Microsoft determined that a change made to the Microsoft Wide Area Network (WAN) impacted connectivity between clients on the internet to their Azure infrastructure and connectivity between services within regions that included Western Europe. Azure will issue their own Post Incident Report as per their own operational process.

Further information regarding the wider Azure impact can be found on the following:

[Microsoft Azure Status Page]

1/25	**Azure Networking - Multiple regions - Mitigated (Tracking ID VSG1-B90)** **Summary of Impact:** Between 07:05 UTC and 09:45 UTC on 25 January 2023, customers experienced issues with networking connectivity, manifesting as network latency and/or timeouts when attempting to connect to Azure resources in Public Azure regions, as well as other Microsoft services including M365 and PowerBI.

4. Actions & Lessons

- Automated monitoring tools detected the issue and alerted TelcoSwitch staff prior to customers experiencing issues.
- Escalation paths shown to work, with the P1 incident being handled within the new ITIL framework.
- Internal test calls made by the infrastructure (RPM probes).
- Azure failures have indicated a SPOF with Hardware Infrastructure monitoring, forcing engineers to run a local example of monitoring on their own equipment. Plans to use space compute to run a new example of Hardware Infrastructure monitoring. Call and software monitoring was recently upgraded into a HA cluster.