Incident Report

A Temporary Mobile Data Service Degradation on 22 January 2014

INTRODUCTION

This is a report by Hutchison Telephone Company Limited to the Office of the Communications Authority on an incident relating to a temporary mobile data service degradation which occurred on 22 January 2014.

NAME OF OPERATOR

Hutchison Telephone Company Limited ("HTCL")

DESCRIPTION OF INCIDENT

A temporary degradation of the mobile data service was found on 22 Jan 22:00. Data connections instability on some interfaces was found and subsequently it was proved that a module of network switch was malfunctioned. The datapath system in HTCL follows highly resilient design rules. The system comes with capabilities of equipment failover within a single site as well as failover to another site. Similar design is commonly used by other service providers in Hong Kong. However, before the switch completely malfunctioned, instability of data connections found. The service degradation was caused by rarely seen scenario occurred simultaneously.

DATE AND TIME OF ONSET OF THE INCIDENT

As confirmed by call test, it was found that the service started to degrade at around 22:00, 22 January 2014.

TYPES AND ESTIMATED NUMBER OF CUSTOMERS AFFECTED

The incident affected the following types of internet traffic:

1) Some of the handset might fail to access internet after switching off and on
2) Some of the internet traffic which requires domain name resolution, such as web browsing and email, were affected.
3) Some of the internet traffic was unstable, which caused by one of the suspected core switches.

It is estimated that the total number of affected customers was less than 200,000.

AFFECTED AREAS

Various locations in Hong Kong

DETAILS OF THE INCIDENT

Time Tasks Description

Time	Task Description
22 Jan 2014	
21:53	Operation Centre received alarms on data path core switches and Accounting Server.
21:55	Operation Centre escalated to 2nd tier network support team for investigation, then shared the alarm information with them.
22:00	As confirmed by call test, it was found that the service started to degrade
22:05	2nd tier network support team couldn't remote access the core switch and arranged network engineer on site support.
22:20	Accounting Server was confirmed to be working normally.
22:45	Network support team arrived on site and found that the faulty data switch had no response on console.
22:52	Network Operation Centre received enquiry from OFCA and reported to OFCA that the case was under investigation.
23:00	The suspected core switch was switched over and service started to resume.
23:30	It was found high loading on Accounting Server and the application was restarted manually to relieve the loading.
23:38	The remedial action was completed
23 Jan 2014	
00:30	The service was totally resumed

ROOT CAUSE ANALYSIS

The data connections of the data network were detected unstable in some network segments. After detailed troubleshooting, a supervisor module of a core switch was found to be not functioning. In our design, we have redundancy in equipment level and in the site level. Unfortunately, there was data network instability event which affected the automatic failover mechanism. The user traffic which passed through those data network path could be degraded. Finally, we triggered the manual failover procedures to resume the degradation of the network. According to the design, the network should have the tolerance to handle the hardware failure or data connection problem in the network which can be resumed the service seamlessly to users. However, the network failed to resume when there is a rarely seen scenario.

REMEDIAL ACTION TAKEN

The suspected core switch was switched over at 23:00, and the degraded service started to resume. The remedial action was completed at 23:38. The service was totally resumed at 00:30.

COMMUNICATIONS WITH THE PUBLIC

At about 00:30 (23 January, 2014), a statement (in both Chinese and English) was emailed to internal and frontline staff for handling media, customer and public enquiries. The statement made it clear that the incident had only affected the data service of HTCL. It also included information on time of onset of the incident, time of service resumption and apologies to the public.

HTCL communicated with customers, the media and the general public via the following channels immediately after service degradation had been identified.

1) Facebook and 3HK Website: The holding statement was posted on HTCL's official Facebook and its website at www.three.com.hk as a pop-up at 00:50 and 00:55 on 23 January 2014 respectively.

2) Customer hotline: The holding statement was posted on the hotline's Interactive Voice Response System ("IVRS") as a pop up voice message at 02:15 on 23 January 2014. HTCL pulled together all necessary manpower at the call centre to cope with the surge in customer enquiries. Replies to customer enquiries were based on the holding statement after it was released.

3) Email: For corporate customers with pre-arrangement on outage notification, an email to update incident status was sent.

4) Media: The statement was sent to the media to inform the press on the investigation and findings of the incident at about 00:52 (23 January). HTCL had been calling the media to follow up with further enquiries.

IMPROVEMENT MEASURES

We have completed the interim preventive measures including the followings:

- Vendor performed health checking on all similar data switches to ensure all hardware is under good condition.

- Vendor reviewed the current alarm detection mechanism to make sure alarm can be fired promptly for the event.

In order to prevent the occurrence of similar incidents in future, we together with our vendor have implemented the following measures:

- Our vendor will enhance the recovery procedures to handle this kind of double fault situation which shall shorten the service resume time

- Our vendor will inspect the data connection protection configuration of all data path switches which will minimize the impact from the data connection instability problem

- We will continue to review the network resilience mechanism to enhance the network stability and service reliability