



Incident Report

A temporary 3G Mobile Data Service Degradation on 29 June 2012

INTRODUCTION

This is a full report by us, Hutchison Telephone Company Limited, to the Office of the Communications Authority on an incident relating to a temporary 3G mobile data service degradation occurred on 29 June 2012, following our preliminary report on 4 July 2012.

We consider that our extensive telecommunications network infrastructure is of utmost importance in our services to the consumers. We, on a daily basis, strive for continuous improvements in our network infrastructure. This report is part of such extensive and continuous effort. In this report, we cover a number of areas including a description of the incident, issues relating to our customers and urgent remedies immediately undertaken. This report is based on the information available to us to date.

NAME OF OPERATOR

Hutchison Telephone Company Limited (“HTCL”)

DESCRIPTION OF INCIDENT

A temporary degradation of 3G mobile data service was found to be unexpectedly caused by a rarely seen software bug in one of the IP network routing components, which is responsible for, among others, (i) IP assignments of new mobile data connections and (ii) IP-MSISDN mapping to other platforms in our 3G network. Our voice and SMS services remained normal and unaffected throughout the period.

DATE AND TIME OF ONSET OF THE INCIDENT

Around 11:00, 29 June 2012

TYPES AND ESTIMATED NUMBER OF CUSTOMERS AFFECTED

Around 40,000 to 50,000 of our 3G mobile data customers were affected.

AFFECTED AREAS

Various locations in Hong Kong

DETAILS OF THE INCIDENT

Time	Tasks Description
11:05	HTCL's Network Operations Centre ("NOC") detected sudden alarms in one of the IP network routing components, namely "AAA (Authentication Authorization and Accounting) Server". The component is mainly responsible for (i) IP assignments of new mobile data connections and (ii) IP-MSISDN mapping to other platforms in our 3G network. We immediately escalated the problem to our vendor – Nokia Siemens Networks LTD (NSN) for urgent inspection.
11:05 - 12:45	<ul style="list-style-type: none"> • The degradation of our 3G mobile data service became apparent. Our records revealed that whilst our 3G mobile data users who had been using our 3G mobile data service before 11:00 were not affected during the period, only those users requesting new mobile data session after 11:00 were intermittently experiencing difficulty in accessing our 3G mobile data service. • Support engineers had performed immediate recovery action but the problem still persisted throughout the period. • Our voice and SMS services remained normal and unaffected.
12:00	Within an hour of the receipt of alarms, HTCL NOC communicated with OFCA that there was unexpected mobile data service degradation. Our voice and SMS services remained normal and unaffected.
12:45	As service degradation in the AAA Server still persisted, HTCL decided to bypass the AAA Server so as to recover the 3G mobile data service first.
13:00	HTCL informed OFCA that there was proven instability of our 3G mobile data service. Our voice and SMS services remained normal and unaffected.
13:15 – 13:55	The bypass of AAA Server action was completed. 3G mobile data service started to resume gradually during the period.

ROOT CAUSE ANALYSIS

Starting from 11:05, we intensively worked with NSN support team to perform a series of emergency checking on the following performance indicators of AAA Server:

- database usage level
- processors loading
- physical interface status
- RAM usage
- Radius message capture and analysis in the AAA Server

At the same time, we also performed emergency checking on the healthiness of the other mobile network elements which we consider might affect our mobile data service performance.

Having checked the aforesaid items, we noted that there was an abnormal and unusual failure in assigning IP address to new incoming data call connections which should be undertaken by the AAA Server. We, together with NSN's continuous efforts, undertook further investigation via call testing with system debugging logs turning on whereupon it was revealed that the IP assignment failure was caused by the sudden unavailability of IP pool.

Finally at or around 12:45, it was identified that the IP assignment failure was caused by an unexpected bug in the software of the AAA Server holding up the resources, resulting in the reduction of the number of unallocated IP addresses in the IP Pool. As a result, when there was new attempt of IP allocation from 3G mobile data users, no IP address was available for allocation to these users. Thus the request of the relevant 3G mobile data users was rejected if such users hit the affected IP Pool.

According to NSN, the software bug of this kind is rarely seen in worldwide and the permanent fix of which is still under development.

REMEDIAL ACTION TAKEN

In order to effectively and efficiently minimize the impact brought by the AAA Server's failure, we promptly started the remedial action at or around 12:45 with NSN's assistance to bypass the AAA Server and to enable the 3G GGSN to take up the role to assign IP addresses to the 3G mobile data users.

Since the required procedures to bypass the AAA Server has been all along well in place since the AAA server was launched, we managed to complete the entire process within 30 minutes upon which our 3G mobile data started to resume progressively.



- The required procedures involved changing the 3G GGSN configuration in a per IP Pool basis and the conduct of certain call tests to ensure the effectiveness of new parameters.

COMMUNICATIONS WITH THE PUBLIC

Three holding statements, in both Chinese and English, were prepared and emailed to internal and frontline staff for handling media, customer and public enquiries.

At about 13:30, the first holding statement giving initial information on the incident, such as time of onset of the incident and affected services, was sent.

At about 14:30, the second holding statement on service resumption at 14:00 and apologies to the public was sent.

At about 19:00, the third holding statement giving details on the number of customer enquiries and complaints received were sent. To counter the misleading information on some discussion forums, the statement also made it clear that the incident had only affected the 3G mobile data service of HTCL. Its 2G and 4G mobile data service remained normal.

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 first and second holding statements were posted on HTCL's official Facebook and its website at www.three.com.hk as a pop-up at 14:00 and 15:00 respectively.
- 2) Retail outlets: Frontline staff posted a special notice, based on HTCL's second holding statement on service resumption, at prominent areas in all 3Shops to help inform and update customers.
- 3) Customer hotline: HTCL pulled together all manpower at the call centre to cope with the surge in customer enquiries. Replies to customer enquiries were based on the three holding statements.
- 4) SMS: A text message was sent to corporate customers who called respective sales representatives for enquiries on the incident in the initial stage. An email, containing the second holding statement on service resumption, was sent to update affected corporate customers.
- 5) Media: The three holding statements were sent to the media to update the press on the latest development of the incident. During the incident and after 19:00, HTCL had been calling the media to follow up with further enquiries.

IMPROVEMENT MEASURES TO PREVENT SIMILAR INCIDENTS

In order to effectively prevent and/or cope with the occurrence of any unexpected similar incidents of this nature, we and our vendor have taken out and reinforced the following measures:-

- 1) Recovery procedures have been prepared to clean up the cached IP address in case problem occurs as well as to monitor the number of cached IP address online on continuous basis.
- 2) NSN shall continue to provide 7x24 special and intensive support in respect of the AAA Server and will apply corrective actions if an unusual increase in the number of cached IP addresses is detected in the future.
- 3) NSN will develop a permanent fix of the software bug of the AAA Server that was identified as the root cause of the incident. It will strive to complete all necessary acceptance and load testing procedures in the testbed AAA Server by the end of August 2012.
- 4) NSN will conduct on regular basis and until the permanent fix is fully developed a full review on the current network architecture such that all the network node resilience, equipment and database failover as well as system loading in order to identify any abnormal and unusual behaviour of any IP network routing component..
- 5) NSN will regularly share with us as an alert the product fault cases reported from the global operators of the same AAA Server.
- 6) We will continue to review and enhance recovery procedures with NSN and hold crisis drills on a regular basis.
- 7) We will continue to maintain additional network capacity and resilience to ensure network stability and service reliability.
- 8) We will review and enhance the company's crisis management procedures regularly in order to respond to critical network incidents and disseminate information to customers and the public in a timely and efficient manner.