Public Version

Hong Kong Broadband Network Limited

Final Report on Service Degradation on Saturday 8 June 2019

1. Introduction

This final report is submitted by Hong Kong Broadband Network Limited ("HKBN") pursuant to its Unified Carrier Licence #045 under which HKBN provides fixed broadband service and IP telephony service to customers.

This report summarizes the two service degradation incidents on 8 June 2019 which were caused by the instability of HKBN's route processors. The two incidents in total affected an estimated [✂] customers of fixed broadband service and an estimated [✂] customers of IP telephony service.

2. Incident Descriptions

The service degradation first occurred at around 02:21 ("1st Incident") on 8 June 2019 when all the route processors kept resetting one by one in a pair of routers installed at HKBN's Central Offices (i.e. [✂]), leading to the disconnection of IP telephony service and intermittent connection to the Internet experienced by customers.

When HKBN's Network Operation Centre ("NOC") engineers detected the network abnormality during network monitoring, the engineers immediately conducted testing to ascertain the service impact and escalated the case to senior management. NOC also deployed more engineers at senior level and the engineers from the vendor of the affected routers ("Vendor") for onsite trouble-shooting. After a series of diagnosis, the possible causes of the instability of the routers were narrowed down. As suggested by Vendor, NOC engineers modified the relevant configuration of the routers at the Central Offices by removing the NetFlow[1] commands for monitoring in order to lessen the routers' loading without degrading the monitoring level. Services were resumed at 06:51 on the same day.

[1] NetFlow is a feature that provides the ability to collect IP network traffic as it enters or exits an interface. By analyzing the data provided by NetFlow, a network administrator can determine the source and the destination of traffic, class of service and the causes of congestion.

Subsequently at 13:11 on the same day ("2nd Incident"), NOC noticed that the fixed broadband service and IP telephony service became unstable again. The Research and Development Team of the Vendor ("Vendor R&D Team") studied the error logs of the router at [✂] and shut down the router temporarily. The services were resumed at 13:50 on the same day. Although affected services were resumed, NOC and Vendor R&D Team continued with the diagnosis and it was revealed that the Border Gateway Protocol ("BGP") packet with an abnormally long AS-PATH length from one particular upstream carrier might have caused the inability of the relevant software to handle the long path therefore triggering the instability. NOC then shut down the suspected faulty WAN Link and discovered that the erroneous activity had stopped along with the shutdown. NOC further applied safeguarding measures to the entire network to discard the abnormal BGP announcement. The router at [✂] was switched on again on the same day to re-enable the network redundancy and resilience.

3. Services and Customers Affected

The incidents affected fixed broadband service and IP telephony service.

Below is our estimation of the numbers of customers affected:-

	1st Incident	**2nd Incident**
Fixed broadband service customers	[✂]	[✂]
IP telephony service customers	[✂]	[✂]

A total number of 3,333 complaints were received by HKBN. All these complaints have been satisfactorily settled with customers.

4. Event Log on 8 June 2019 on Incident and Recovery Actions

1st Incident

Time	**Event**
02:21	NOC engineers observed multiple ping monitor fail records.
02:50	NOC engineers completed testing and confirmed service impacts.

03:05	NOC engineers escalated the case to senior management and Vendor for investigation.
03:15	NOC senior engineers onsite joined the investigation.
03:33	Vendor onsite support joined the investigation.
03:46	NOC engineers performed hardware reset on the router at [✂].
04:10	NOC engineers performed hardware reset on the router at [✂].
04:38	Vendor R&D Team conducted logging analysis.
05:50	The router at [✂] was stabilized after removing the NetFlow commands which might trigger the router software instability as per Vendor's advice.
06:51	The router at [✂] was also stabilized after deploying the same measures as that at [✂]. Affected services were resumed.

2nd Incident

Time	**Event**
13:11	Services became unstable again.
13:15	Vendor R&D Team checked the error logs of the router at [✂].
13:50	The router at [✂] was shut down. Services were resumed as there was no abnormal AS-PATH announcement.
15:20	Vendor R&D Team further found that the BGP packet with an abnormally long AS-PATH length from upstream to the network might trigger the software stability.
15:41	NOC shut down the suspected faulty WAN link and the error logs of the router subsequently stopped.
16:37	Filtering commands as safeguarding measures were applied to the entire network to discard the abnormal BGP announcement.
16:45	The router at [✂] was powered on again to normalize the network redundancy and resilience.

5. Remedial Actions

NOC and Vendor diagnosed that the incidents were caused by master/slave main control board switchovers by the AS-PATH attribute which was too long to be handled. Services were resumed to normal after applying the AS-PATH-LIMIT command for discarding the abnormal AS-PATH announcement.

After further investigation by Vendor, software version update was suggested by Vendor to improve the BGP route convergence performance. The processor of BGP in the new

version software is improved from the incumbent deployment, where memory overflow will not occur during BGP AS-PATH processing.

Software version upgrade of the router at [✂] was completed on 16 June 2019 and its performance is currently under close monitoring. Subject to the monitoring result, software version upgrade of the router at [✂] will be performed at the end of September 2019.

After the WAN Link of the one particular upstream carrier was re-activated at 03:00 on 19 June 2019, it was confirmed that no more abnormal BGP announcement was found.

Currently, both routers function normally, and Vendor continues to undertake hourly performance check on HKBN network.

6. Root Cause

Our Vendor was not aware that the incumbent software version of the main control boards could not tackle this kind of abnormal activity coming from the internet. AS-PATH is used in BGP for routing loop-free function. The memory allocation of the incumbent software was designed in the way that [✂] could handle the length of AS-PATH up to [✂]. In general, the AS-PATH length should not exceed 100. When the AS-PATH length exceeds [✂], the memory overflow of all the main control boards will automatically trigger the self-healing active/standby switchover leading to service degradation in the two incidents.

Although HKBN's network was built with full redundancy and resilience, the investigation result indicates that the two incidents were caused by the simultaneous switchovers of all main control boards arising from an abnormally long AS-PATH exceeding [✂] received from one particular upstream carrier with connection to the Central Offices, thus leading to service degradation.

For the 2nd Incident, NOC observed a switchover log from the router of [✂] but not from the one of [✂]. Although the services had been resumed to normal after the shutdown of the router of [✂], in order to minimize the potential risks, the connection with that one particular upstream carrier was also shut down. As no more abnormal AS-PATH announcement was passed through, the situation was under control subsequently.

Please refer to Network Diagram 1 depicting the connection of the routers in the Central Offices.

7. Communications with Customers on 8 June 2019

- HKBN deployed more manpower resources to the Customer Services hotline to handle customer enquiries.

- 08:08 - HKBN put up announcement on its Facebook page to inform customers of the incidents and service resumption.

- 17:34 - HKBN put up an announcement about the incident on its own website www.hkbn.net to inform customers of the incident and service resumption.

- 18:12 – HKBN put up an announcement on its corporate services landing page in its own website www.hkbn.net to inform customers of the incident and service resumption.

8. Communications with OFCA on 8 June 2019

- 08:24 – Telephone call was made to OFCA and notified OFCA of the services affected and that affected services were already resumed at 06:51.

- 14:09 – Informed OFCA of the 2nd Incident and the relevant services were resumed at 13:50.

- 17:07 – Updated OFCA that NOC has rectified the problem and network was returned to normal and HKBN would continue close monitoring.

9. Improvement / Preventive Actions

In order to prevent reoccurrence, the following measures have been implemented by HKBN with their status as indicated:

- Filtering commands as safeguarding measures have been applied to the entire network of HKBN to discard the abnormal AS-PATH announcement on 8 Jun 2019.

(Status - Completed)

- Vendor has provided a patch to prevent the software instability from the abnormal AS-PATH announcement received from upstream providers.

  (Please refer to the third paragraph of Section 5 above)

- All relevant systems supported by the Vendor have been thoroughly reviewed and audited to ensure the correct functioning.

  (Status - Completed)

- The recovery procedures have been enhanced with the Vendor to improve the service recovery performance in terms of time.

  (Status - Completed)

- The internal and external communication procedures on incident response have been reviewed and reinforced.

  (Status - Completed)

- To commence evaluation and engagement of an independent professional consultant to review and audit the network architecture and configuration.

10. Conclusion

HKBN regrets that the incidents have caused service impacts to its valued customers and concerns to OFCA. HKBN takes seriously the stability and proper functioning of its network and understands the need to ensure that its network performs and continues to provide satisfactory level of service to its customers. HKBN undertakes regular review, maintenance and upgrades of its network. Unfortunately these incidents were not within the reasonable contemplation of HKBN and could not have been reasonably prevented.

HKBN is aware of the requirement to provide its telecommunications services in a manner satisfactory to the Communications Authority and the public. These two incidents have

received the attention of the senior management of HKBN who will ensure that similar incidents will not occur, and that HKBN will review and enhance its network to assure its customers of a high level of service provisioning in the future.

HKBN will co-operate fully with OFCA in its investigation and will answer any queries that OFCA may have concerning the incidents.

Submitted by Hong Kong Broadband Network Limited.
27 June 2019 (revised on 3 July 2019)

Network Diagram 1

[✂]