

**Legislative Council Panel on
Information Technology and Broadcasting**

**Access problem affecting some Hong Kong-based websites
on 1 November 2004**

(Paper from Hong Kong Internet Registration Corporation Ltd)

Purpose

1. This paper informs Members about the access problem affecting some Hong Kong-based websites on 1 November 2004 and reports on the causes of the incident and follow on measures HKDNR¹ has taken or will take in order to prevent a similar incident from happening in the future.

Background

2. On 1 November 2004, a limited number of web sites and e-mail addresses of certain '.com.hk' domain name customers were not accessible from around 2:30am onwards. Normal service resumed at around 9:30am. Due to the nature of the global Internet Domain Name Service (DNS), some Internet users were not able to gain access to the affected ".com.hk" web sites until two hours later, however, most Internet users who accessed the Internet through local ISPs based in Hong Kong were able to gain access to all affected ".com.hk" instantaneously once normal service was resumed. HKDNR has promptly conducted a thorough investigation into this incident.
3. HKDNR has also reviewed the existing provisions for safeguarding the integrity, reliability and performance of its service.

¹ The Hong Kong Domain Name Registration Company Limited (HKDNR) is responsible for administering the DNS that translates Internet domain names ending with '.hk' to facilitate access to and communication on the Internet. HKDNR is a wholly-owned subsidiary of the Hong Kong Internet Registration Corporation (HKIRC).

Existing setup for safeguarding the integrity, reliability and performance of HKDNR's service

4. HKDNR has deployed a system infrastructure based on industry proven components to provide the '.hk' domain name resolution service for all domain names ending with the suffix '.hk'. The production hardware (for providing the live service) is located in the HKNet data centre in Kwai Chung. A set of development and test hardware is located in the HKDNR office in Kowloon Tong.
5. All '.hk' domain name master records, which contain the IP addresses for the corresponding '.hk' domain names, are stored in "zone files" in HKDNR's primary name server. There are eight (8) secondary name servers in different countries such as China, Taiwan, Australia, US and Netherlands. Each of these secondary name servers contains a replica of the '.hk' zone files. Together, the primary name server based in Hong Kong and the secondary name servers based overseas form a highly resilient domain name system for resolving '.hk' domain names. For example, if the primary name server is down, any one of the other secondary servers will be able to resolve '.hk' domain names. In other words, any one of the primary and secondary name server can perform the same function as the others.
6. From time to time, the '.hk' domain name master records in the "zone files" in the primary name server need to be updated to reflect any addition or deletion of domain names or any change of IP addresses.
7. Changes made to the "zone files" in the primary name server are automatically sent to secondary name servers to synchronize the changes with all secondary name servers, and are subsequently sent to all other name servers in the whole world. A complete propagation of changes normally takes around three hours, depending on the setting on different servers and the volume of Internet traffic.

8. HKDNR's name servers are protected by secure and industry proven firewalls in both the HKNet data centre and at HKDNR's office. This high level of security enforced by such firewalls ensures that HKDNR's systems are robust and resilient enough to withstand most if not all of the hacking attempts by outside hackers.
9. In order to provide a responsive service to HKDNR customers, the "zone files" are updated five times daily. All updating is performed automatically by way of a batch program. The first scheduled update is set to run from around 2am to 3am. The four other updates are performed during office hours between 9am to 6pm. Any changes made to '.hk' domain names should therefore become effective throughout the world within as short a time space as 2 hours.

Investigation results of recent incidents and follow on measures

10. HKDNR first received complaints on the non-availability of ".hk" domain name services from some customers and service partners at around 9am on 1 November 2004. HKDNR's technical staff immediately inspected the system and discovered that a limited number of ".hk" domain names were not recorded on the primary name server because the overnight updating job could not be completed properly. HKDNR's technical staff restored the service by activating the most recent working copy of the domain name "zone file" on HKDNR's primary name server at 9:16am. Due to the time lag in propagating the updated domain name records to all other name servers on the Internet, the affected domain names may become available at around 9:30am.
11. HKDNR took immediate steps in order to prevent similar incidents from happening as follows:-
 - HKDNR's technical staff will now monitor the updating process manually every night to ensure that all domain name records are successfully applied to the primary name server.
 - Additional end-to-end automatic checking was put in place to

reconcile the number of domain name records expected to be generated and actually generated. Where there is a discrepancy, the new set of records will not be applied to the name server, and email alerts will be sent to HKDNR's technical staff informing them to take immediate action.

- HKDNR is arranging to set up additional monitoring service by the Data Centre staff to further ensure that manual checking is performed and timely escalation to management staff takes place if any problem with the update process could not be resolved within a set timeframe.
12. Affected customers and service partners were very concerned that they would not be able contact HKDNR after office hours should service outage ever happen again. Contact numbers of the IT Manager, Operations Manager and Chief Executive Officer were made available to all affected customers and partners for timely assistance when needed. HKDNR is in the process of arranging the extension of the availability of its customer hotline service to 24 hours 7 days and its senior staff will be available for assistance when needed.
 13. The root cause of the incident has been identified. It was traced back to a "watchdog" program which monitored the health of one particular process. The purpose of the "watchdog" program is to restart that process if it was found to be inactive. At the time the updating batch program was running on 1 November 2004, the particular process failed to respond to the "watchdog" program. As a result, the "watchdog" program attempted to restart the non-responding process, but by doing so, the "watchdog" program inadvertently terminated the updating batch program while the latter was still running. The occurrence of such an event is extremely rare.

14. Further analysis of the whole incident identified areas where improvements can be made as follows:-

- Reassess fault tolerance and risk management especially for critical activities
- Need for tighter process control and higher level of systems operation, system administration and technical support discipline
- Conduct periodic software testing
- Upgrade customer service especially after office hours and during weekends and holidays and establish the need for alternate channels of communications

15. Further, HKDNR has decided to strengthen its risk management by performing the following:-

- Conduct a full system audit as soon as possible to identify weaknesses in the system development and testing procedures, change management and deployment process, security and access control policies, systems operations and administration practices, hardware and software configuration, disaster recovery plan, technical management and organizational arrangement.
- Conduct an overall risk assessment in November of the different functions and activities of HKDNR and revise the risk management plan accordingly.

16. To strengthen the system and process control, the following will be undertaken -

- Enhance system control mechanism such as providing additional functions of auto-detection of problems, suspension of system actions that cause the problem and auto-notification to IT staff for immediate rectification. This enhancement is now in the final stage of testing and will be implemented as

soon as possible.

- Introduce system monitoring tool, in particular, to check '.hk' domain name availability using random sampling.
 - Arrange for alternate manual and automatic monitoring and notification of untoward events in the systems and automatic processes through outsourced service provider.
 - Organise regular drills to ensure that the system and process control processes are up and running and functioning as intended.
17. To enhance the effectiveness and reliability of system testing and deployment, HKDNR shall review its testing procedures and deployment process to ensure that sufficient code inspection is performed for critical software codes and to increase the level and depth of testing when necessary to ensure that the required reliability level is achieved. More emphasis will also be placed on system testing to ensure unintended inter-process interactions are minimized. System configurations to be deployed will be more critically reviewed to minimize potential risks, and where necessary, dedicate a server to a single process to ensure higher software reliability.
18. On the customer service side, HKDNR shall consider the most cost-effective option to extend the service hours of HKDNR's customer hotline to 24 hours 7 days. The key requirement here is to ensure all service-related complaints after office hours will be timely attended to by a human operator and redirected to a staff with the right technical expertise to address the problem. In addition, escalation of the problem to different level of personnel will ensure that all non-attendances or undue delay in attending a problem will be rectified in the shortest time possible.
19. HKDNR is now conducting manual end-to-end checking every evening to uncover any problems in the domain name record generation irrespective of what caused the problem.

Conclusion

20. Domain name service problems causing temporary inaccessibility to web sites and e-mail services by the public are a serious matter. HKDNR will strive to take all reasonable and possible measures to reduce the likelihood of such incidents occurring.

21. HKDNR is committed to take all reasonable and possible steps to prevent a similar incident from happening again and HKDNR will continually strive to improve its service and technical infrastructure to meet the needs of the local Internet community.

Hong Kong Internet Registration Corporation Limited
November 2004