A COMMUNICATION EXCEPTION EVENT CAUSED BY AN INAPPROPRIATE CONFIGURATION OF FIREWALL IN DATA CENTER (DISASTER RECOVERY CENTER) OF STATE GRID SHANGHAI MUNICIPAL ELECTRIC POWER COMPANY

HU Junyi
State Grid Shanghai Municipal Electric Power Company – China
hhhy2j_hu@hotmail.com

LU Rong
State Grid Shanghai Municipal Electric Power Company – China
vivirong1122@hotmail.com

ABSTRACT

In this paper, a communication exception event happened in DATA CENTER (DISASTER RECOVERY CENTER) of State Grid Shanghai Municipal Electric Power Company was introduced. The whole process of occurrence, disposal and recovery was elaborated.

INTRODUCTION

Disaster recovery information systems of eastern China and central China province power companies and some information systems of State Grid Company were deployed in DATA CENTER (DISASTER RECOVERY CENTER) of State Grid Shanghai Municipal Electric Power Company which was an important component of Smart Grid. Now, safe and reliable operation of information systems becomes more and more crucial to power grid enterprises.

EVENT OCCURRENCE

One day of March 2016, monitoring personnel of DATA CENTER (DISASTER RECOVERY CENTER) of State Grid Shanghai Municipal Electric Power Company found that long network delay and communication exception in some information systems were occurred in succession. They tried to use PING command for testing packet loss rate to different IP addresses in Internet immediately. Packet loss was discovered indeed, the highest packet loss rate was up to 10%. If worsened, information systems (OA, ERP, PMS, marketing system etc.) outrage would cause power system unstable directly.

MALFUNCTION ELIMINATION

Maintenance personnel went to computer room to check out the physical equipment at once, meanwhile, they logged in management interface of servers, network equipments, safety equipments, information systems etc for health inspection. After emergent examination, status of all hardware equipments (including firewalls) was in normal range.

Since the symptom of packet loss, maintenance personnel put their emphasis of inspection on network equipments. By using substitution method, firewalls were confirmed to cause this situation.

MALFUNCTION ANALYSIS

After logging in management interface of firewall for second time, it was found that although current CPU temperature, utilization ratio of CPU and memory, port status was all in normal range, the number of sessions would not change when increasing up to 2000000, shown as Fig1.

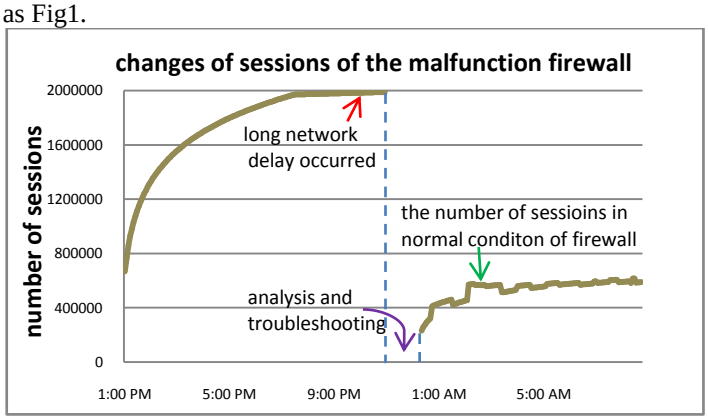

Fig1. changes of sessions of the malfunction firewall

After confirmation, it was known that the maximum allowance number of sessions of firewall for this type was 2 million. It meant that when the number of sessions reaching 2 million at one moment, new session would not be created unless an old session was aged and terminated.

Furthermore, protocol analysis was made for those 2 million sessions. It was discovered that DNS (Domain Name System) and NTP (Network Time Protocol) requests accounted for above 50% of the whole, and they were maintained all through.

Generally speaking, DNS and NTP services were provided to all users in State Grid Company by DATA CENTER (DISASTER RECOVERY CENTER) of State Grid Shanghai Municipal Electric Power Company. Sessions could be terminated and released after domain name resolution and network timing was complete, and it is no need to be kept.

However, in some packet filtering policies of the firewall, DNS and NTP services were chosen for long connection, the default retention time for long connection of the firewall was 24 hours. It could be inferred that this network congestion was due to an inappropriate configuration of retention time for long connection which made sessions cannot be aged and terminated.

PROCESS HYPOTHESIS

It was supposed that at that day, a lot of users delivered their DNS and NTP requests to servers which deployed in DATA CENTER (DISASTER RECOVERY CENTER) of State Grid Shanghai Municipal Electric Power Company. Then after completion of requests, sessions could not be aged and terminated in time because of being improperly chosen for long connection. As time went by, the number of sessions increased up to 2 million. When reaching its maximum allowance number, following connection requests could not be established until old one was aged or terminated. Therefore, long latency time and network congestion was occurred.

CONCLUSION

Finally, the retention time for long connection was reevaluated and optimized from 24 hours to 12 hours. In the mean time, all packet filtering policies of firewall was rechecked, policies applied for information systems which ought to be chosen for long connection were strictly defined. After emptying all sessions and restarting the malfunction firewall, the network condition came to recovery by applying new packet filtering policies.

Fortunately, communication interrupt in DATA CENTER (DISASTER RECOVERY CENTER) of State Grid Shanghai Municipal Electric Power Company was not happened by proper disposal. However, along with tight combination of information technology (IT) and power system, proper configuration of information systems and dealing with events occurred in DATA CENTER of power grid enterprises in time was equally important as maintaining power system stable operation.