Security and Reliability Design of Olympic Games Network

Zimu Li\textsuperscript{1}, Xing Li\textsuperscript{1}, Jianping Wu\textsuperscript{1}, and Haibin Wang\textsuperscript{2}

\textsuperscript{1} Network Research Center, Tsinghua University, 100084 Beijing, China
{lzm,xing,jianping}@cernet.edu.cn

\textsuperscript{2} Technology Department, The Beijing Organizing Committee for the Games of the XXIX Olympiad, 100083 Beijing, China
wanghaibin@beijing2008.cn

Abstract. High security and reliability is the essential design principle of the Olympic Games Network. This paper depicts the organization and its functionality of security and reliability design in 29\textsuperscript{th} Olympic Games Network, such as architecture, 2-level DMZ, A/B systems, IP encoding and routing/switching. In addition, it describes the network optimization to meet the special requirements of Beijing MSTP MAN. In this paper, some experience of realizing a high security and reliability network is provided for reference.

1 Introduction

Games Network is the basic system of Olympic Games results distribution, information publication, media transmission and games management. As a critical system, high reliability and security of Games Network is the essential requirement for a successful Olympic Games. This paper gives an overview of the reliability and security design of 29\textsuperscript{th} Beijing Olympic Games Network.

2 Network Architecture

29\textsuperscript{th} Olympic Games Network is composed of more than 50 venues around Beijing, Tianjin, Qingdao, Shanghai, Shenyang, Qin Huangdao and HongKong. Many critical applications, such as Timing & Scoring, Results Diffusion System (IDS), Commentator Information System (CIS), Games Management System (GMS) and etc are running on it. The architecture is shown in Fig. 1.

In Fig.1, it shows that Games Network is typical 2-core architecture that two core switches are deployed in PDC (Primary Data Center) and SDC (Secondary Data Center, a total backup of PDC) respectively and connected by three high-speed Ethernet channels. Except few none-competition venues, most venues connect PDC and SDC through different geographic leased lines. In most venues, two aggregation switches are deployed and backed up each other. All venue access switches connect with aggregation switches by two uplinks. In venues, each server has two NICs connecting with two different access switches by “teaming”. Therefore, from servers to core
switches, each level of the network has two switches and two uplinks respectively. Any single device failure would not affect the Games.

Fig. 1 shows that the under layer transmission system is composed of ADM (Add/Drop Multiplexer) device and MSTP (Multiple Service Transportation Platform) which is the most popular MAN technology in recent years. MSTP is compatible with SDH and provides multiple types of Ethernet interface that can be connected with core switches in PDC and SDC directly without any additional device. By this way, it looks like all venues LANs are connected together with a virtual switch and thus complexity of management is reduced.

3 Security Architecture and 2-Level DMZ

Security architecture is in accordance with network architecture except firewalls are highlighted. Fig.2 gives an overview of Games Network Security Architecture.

In Fig.2, all venues without external leased line connect each other by MSTP ring. As MPC (Media and Press Center) and IBC (International Broadcast Center) provide service mainly to journalists that need communication with their home news agencies by leased lines and VPN, MPC and IBC are protected by firewalls so that only the permitted VPN traffic are allowed to get out to the pre-determined destinations.

![Fig. 1. Games Network architecture](image1)

![Fig. 2. Network Security Architecture](image2)

To ease management and improve physical security level, all global critical servers of Olympic Games are deployed in PDC/SDC. Some of the servers only provide service to internal clients and some others provide service to Internet clients. Hence, a 2-level DMZ (Demilitarized Zone) is constructed to protect these servers in PDC/SDC. In DMZ, from inside to outside direction, the 1st level firewall ensure servers in Internal DMZ can only be accessed by internal clients whereas Internet clients can access only servers in External DMZ by the 2nd level firewall. In addition, the 2-level firewall guarantees that data can only be transmitted from internal servers to external servers. The 2-level firewall architecture and single direction traffic filtering prevent network attacks from both outside and inside at the utmost level and gives the servers maximum protection.