Optimization of Computer Network Designs and Promotion of Transmission Efficiency

Zhao Mingyang
Baoshan University, Baoshan Yunnan, 678000, China

Keywords: Analysis, Computer Network, Optimization Design, Promotion of Transmission Efficiency.

Abstract: The society has entered Internet information age, which connects people everywhere in work and life. With Internet popularized everywhere, all computer networks, large or small, are undergoing information communication and transmission. However, many problems still exist in the computer network. After analyzing factors influencing computer network, safety threats are classified in the work. Meanwhile, different ways of optimizing computer network are discussed, and technical measures of protecting computer network are given in the end.

1 INTRODUCTION

With the popularity of electronic information devices and fast development of computer technology, Internet users are increasing in great numbers. And it cannot be mentioned in the breath when compared with the early time. Nowadays, most people are enjoying the conveniences brought by public network. Meanwhile, higher demands are brought to computer network as people focus more on the reliability and safety. Therefore, the optimization of computer network designs and promotion of transmission efficiency is of great social significance.

2 FACTORS INFLUENCING THE CONSTRUCTION OF COMPUTER NETWORK

2.1 Network Equipment Factors

While constructing computer network, capital is mainly invested in the network equipment, which is directly connected with customer-oriented terminals. Among the various access and switching equipments that influence network efficiency, the key switching equipment is connected with the whole network efficiency. Meanwhile, China is still weak in the network equipment techniques. Most of the equipments are bought abroad. China gradually increases support for the companies that manufacture network equipments in their innovative abilities. So the leading places of foreign companies in the network equipment market may be broken. With the increased efforts in developing core devices of Chinese backbone networks, the necessary network equipments will definitely be localized.

2.2 Factors of Transfer Switching Equipments

People can see switchboards most in the lan network topology diagram of a certain size. The switchboards are very powerful, as they can both control flow and check data error. Some even have firewall that network security devices own and can be used as routing. The Switchboards account for a large percent in the network devices. And client is connected to the computer network through the access switch. Therefore, the switching equipment is vital in ensuring the smooth communication of computer network. The access switch plays the link role in the network topology and is critical to the network efficiency.

2.3 Factors of Network Management

Nowadays consumers have more network demands, and network digital and mechanical devices become complex. Thus, computer networks are becoming bigger. Although public network is mainly maintained by operators, various hidden troubles still exist due to the limited technology and

Mingyang Z.
Optimization of Computer Network Designs and Promotion of Transmission Efficiency.
DOI: 10.5220/0006024703000303
In *Proceedings of the Information Science and Management Engineering III (ISME 2015)*, pages 300-303
ISBN: 978-989-758-163-2

Optimization of Computer Network Designs and Promotion of Transmission Efficiency

incomplete management. The public network system includes: the physical infrastructures, the host (server), workstations, routers, switches, access devices, relationships between nodes and nodes on the network equipment, and network users (workstation) management interface. Meanwhile, the job of network administrators includes the management of network infrastructures, operating system, application system as well as users.

2.4 Factors of Network Topology

As an information manager, he should be familiar with the skeleton of network when he first comes. The network topology refers to how devices are connected in the network and shows their relationships. Thus, the network skeleton can be seen clearly in the topology. Whether the topology is scientific and reasonable influences network efficiency much. The administrator can have preliminary visual awareness with the general knowledge of devices and platforms of network topology in different levels. Thus, the following network maintenance and troubleshooting will be convenient.

3 THREATS OF COMPUTER NETWORK SAFETY

3.1 Threats of Natural Disasters

With the informationization, computer network extends worldwide, including mountains, plains and islands. As standards of machine rooms can not be applied to the arrangements of all computer networks, the network will be influenced by environment. The natural disasters will be the main threats. Therefore, considerations should be given in advance to avoid natural invasions when conducting network integration routing.

3.2 Threats of Hacker's Invasion

Hackers are a group of people obtaining network information illegally. As the network information size grows, they cannot be ignored while discussing network information security.

Hackers are definitely technically stronger than ordinary netizens. They are a special group, attacking the Internet in various ways with strong randomness. Thus, the following consequences cannot be predicted. As attacks of hackers emerge in an endless stream, the threats are becoming more common and unpredictable to the safety of network system. They are endangering individuals, even the whole society. There are many famous hackers worldwide, but they are not all criminals. Mitnick was ever the most wanted criminal of the America as he once attacked the computer network of the pentagon and digital equipment corporation. Surprisingly, the Apple co-founders Steve Jobs and Steve Wozinak are also on the list of hackers.

3.3 Threats of Computer Viruses

In fact, computer viruses are codes that endanger users. They generally parasitize in some programs and run with the programs. Thus, they influence the operating system, application platform and hardware. Viruses mainly attack clients, seldom endangering network devices. Besides, the codes reproduce themselves and are transmitted quickly online. The viruses are hidden, and users always trigger them accidently without knowing. Thus, more programs are infected and transmitted online. Nowadays, the protection software is becoming more mature, releasing wild list regularly to protect users. Therefore, users should install software in their own computers to avoid virus invasion.

3.4 Threats of Trash Mail and Spy Software

Users generally communicate through e-mails online. As e-mails carry many kinds of files, many people engage in illegal acts through them. Some spy groups transmit videos of illegal political activities or information not suitable for wide dissemination in free e-mails to affect users. Meanwhile, users' mails may also be supervised and stolen.

4 WAY TO OPTIMIZE COMPUTER NETWORK DESIGN

4.1 Emphasis on Rationality of Fault-Tolerant Design of Computer Network

Computer network will definitely make mistakes while communicating with each other. However, it can be dealt with by improving the adaptability.

(1) Parallel method is used when building

301

network, and dual module hot spare is applied in general computer network. To protect against accidents, two network centers are used. Thus, if one center has faults, the other will work in emergency. Two centers are applied to ensure the balanced load of network system.

(2) Interconnecting network devices include: routers, wan, and data-link. They can reduce the fault to the minimum level to ensure the least impacts on computer network.

(3) Selection of sever: sever takes very important position in the computer network, and many application platforms rely on severs. If the sever has high reliability and strong fault tolerance, few failures will exist.

4.2 Implementation of Redundant Design of the Dual Network

Now network design should focus on users, and redundancy is designed to ensure network systems with double insurance. In general, it takes advantage of dual- core redundant design in case of need. In computer networks, dual network redundancy is designed between layers and between links. Thus, it ensures the network infrastructure with backup regardless of where the problem occurs. The redundant design is generally applied in core switches and servers in computer network systems. When problem occurs, links can be open and application platforms can normally operate. Therefore, the reliability of computer networks will be effectively protected.

4.3 Emphasis on the Hierarchy and Architecture of Computer Network

Now network can be seen in clients, and the services provided are real. Generally, only the network cable connected to the client can be seen. However, it is not a sweeping view of the rest. Network architecture is built following the idea of the designer, while cabling designers are not involved in. The administrator and designer just care about the network architecture and level, which is objective but not intuitive. However, the reasonability of network architecture is associated with reliability and performance of computer network. Therefore, attention should be paid to the network architecture and level design.

4.4 Construction of Computer Network System with Hierarchical Layout

Anyone with certain knowledge knows computer network contains four levels: network service layer, application layer, the network physical hardware layer and network operating system layer. After the initial design of the four layers, the improvement of network system is conducted for the application of computer network. Network service layer provides network services, such as online videos and websites. Network physical hardware layer can be seen by network designer, such as network topology, server, core switches, access switches. Network operating system layer is the multiple versions of operating system similar to SERVER from Microsoft. As the computer network is complicated, the reasonable design will make it reliable, otherwise it will be unreliable.

5 TECHNICAL PROTECTING MEASURES TO MAINTAIN COMPUTER NETWORK

5.1 Firewall Technology

Firewall, a common word in information security field, adds a layer of protective barriers for the networks in its image. It is a barrier set to guard against the threat at cyberspace security edge, isolating the attacks outside the barrier. Thus, users will be protected. Small and medium-sized enterprises network or public network may be attacked by network safety threats. Installing firewall to prevent viruses and attacks will increase the reliability of network information system and safety of users.

5.2 Access Control Technology

The identification of network information access will restrict people's permission to access to network. Thus, numbers of users are reduced to a certain extent, which is beneficial to the smooth operation of network. As there are many ways of access control, authorized software can be installed between client and server to allow the permitted guests to have network access. The access control technology offers permissions with minimum principle, allowing users to access in their least privilege. The network information manager should assign permissions to each user properly and post

Optimization of Computer Network Designs and Promotion of Transmission Efficiency

audit data of system access. Meanwhile, he should manage the information of all users.

5.3 Network Monitoring and Locking Control Strategy

The job of network information system managers is to maintain the network and supervise acts. Therefore, network stability can be protected. Now many monitoring platforms have been developed, some can trace back all the acts in the client and have data stored in the database. The giant database information set threshold for network alerting. Thus, illegal network uses will be selected. Any user violating the rules will be restricted.

5.4 Devices Attacking Detection System

Firewall technology is one of Internet safety technologies. However, it is not unbreakable. Hacking the firewall through bugs is one way of attacking the Internet. Therefore, the combination of firewall and invasion detection system as the defense of network information system will make network security stronger. In recent years, some high-tech companies are devoted to the development of network safety technology. The invasion detection system produced by them is improved. Meanwhile, the companies also produce firewall and vulnerability scanner. Invasion detection system is equipped in medium and small sized internal network to record network behaviors. Therefore, the information of network attacks will be found. Comprehensive analysis of the recorded information and summary of attacking sources will be beneficial to strengthen the prevention of network system. Invasion detection system protects both inside and outside, providing a technology for network safety. Therefore, it is worthy of further development for network application.

6 CONCLUSIONS

As the society develops rapidly with information technology, computer network is used more common, and people rely more on it. The optimization of computer network to protect the overall transmission efficiency is the urgent need of society. With the improvement of computer network reliability, the more convenient the services provided by computer networks are, the more meaningful social life will be.

REFERENCES

Sun Fuguo, Wide Area Network Design and Security Mangement in Tobacco Company of the municipality, Journal of Chuzhou University, 2011(5):32-34

Wang Yikai, Reliability Analysis and Design of Computer Network, Charming China, 2014(13):249

Wang Zhaohua, Network wiring Design and Realization of Intelligent Flexible Campus Computers, Computer Disc Software and Application, 2013(04):207-208

303