From Network Security to Network Autonomous

Wang Yubian*
Department of Railway Transportation Control
Belarusian State University of Transport
34, Kirova street,Gomel,246653
Republic of Belarus
*is the communication author.
e-mail: alika_wang@mail.ru

Yuri Shebzukhov
Department of the International Relations
Belarusian State University of Transport
Republic of Belarus
34, Kirovastreet, Gomel, 246653
Republic of Belarus
e-mail: oms@bsut.by

***Abstract*—In the 20th century, the emergence of the Internet has completely changed the work and life of human beings around the world. Today, people are increasingly inseparable from network. The Internet has been integrated with the global industry, agriculture, education, science,technologyand national defense. The current Internet was originated in the United States. The Internet systems based on IPv4 and IPv6,they are controlled by the United States completely. Computers connected to the Internet are subject to data retention and backup in the United States. Data security is greatly threatened. In addition, due to limitations and loopholes in the design of the Internet, the Internet is subject to many different types of attacks. Internet research which based on security autonomy has received the attention of sovereign countries in the world. This paper mainly introduces the Future Internet system developed by Chinese researchers based on the current research on Internet servers,which is a new generation network system,the research and application of this system will have a profound impact on the world's Internet.**

Keywords-Network Security; Root Server; Network Autonomous; Future Internet

People can't live without the internet;internet has become a necessity in daily life.The share of the network economy has accounted for 22% of the global GDP. The importance of the network has become more and more prominent, so the basic work about the network is even more important. Now the Internet has two biggest problems. One is the cyber sovereignty, which is about the network's belongs. It is obviously that the United Stateshold the internet. How to adhere to cyber sovereignty is still a challenge. Another problem is that many countries hope the operators will speed up and reduce the cost at the same time. It need the operators to reduce the bandwidth cost of access to the Internet by SMEs, and how to reduce the bandwidth fee for accessing the Internet is a problem. This two major problems are now more difficult to solve, and why? We need specific analysis of specific issues and tell everyone what solutions we have.

I. CYBERSPACE

First of all, there must be a definition of cyberspace. This is very important. How do we adhere to the sovereignty of cyberspace?Currently,there is noaccurate definition in the media, and we think it should be definedproperly. Cyberspace is a virtual space that contains three basic elements.In the space,virtual and real are contained, and dominated by virtual.

In this virtual cyberspace, it is not these infrastructures that are in the most important leadership position, nor our application environment, but the full root system. This must be clear, if this is not clear, many explanations will go wrong. The core embodiment of cyberspace sovereignty is the standard protocol for data communication technology. At present, it includes the IPv4, IPv6 and future network/IPV9 network data communication standards and protocols of the existing equipment running in the world, and the formed network space address naming rights, distribution rights, resolution rights and route addressing operation management rights.

The core resources of cyberspace include: the parent root server, the primary server, the 13 root name servers, the IP address of the address and domain name resolution system, asset equipment and operation management rights. Therefore, it can be said who owns the core assets of cyberspace, who masters the sovereignty of cyberspace.

DOI: 10.21307/ijanmc-2019-035

II. INTERNET SERVER

The working principle of the current public network is not thoroughly understood. Actually, this is very important. This determines how to adhere the cyberspace sovereignty. This is determined the basic principles. Any time we access the network, including any computer on the Internet, phone Internet access and mobile Internet access. Firstly, we must access the root server. The root system consists of the parent root server and the primary root server (the publishing host). This hidden publishing host only 13 root domain name servers (13 root domain name servers are equal rights) that can be accessed to maintain this hidden publishing host. The 13 root domain name servers read the primary root server, then read the parent root server and obtain the data, then read by the mirror server, and spread to the entire network.

The root server is mainly used to manage the home directory of the Internet. All parent, root, and sub-servers of IPv4 are managed by ICANN, an Internet domain name and number assignment authority authorized by the US government are responsible for the management of global Internet domain name root servers, domain name systems, and IP addresses. There are only 13 root name servers in the world. Ten of them are in the United States, two in Europe, in the United Kingdom and Sweden, and one in Asia in Japan. These 13 logical root servers direct web browsers such as Firefox or Internet Explorer and email programs to control Internet communications. Because the root server has more than 1000 Internet domain name suffixes (such as .edu, .com, etc.) approved by the US government and all national domain names (such as .us in the US, .cn in China, etc.).

Since the establishment of the Internet, the world has become very dependent on the United States. The United States has controlled the entire Internet by controlling the root server, posing a potentially major threat to cybersecurity in other countries. The so-called dependence, embodied in the working mechanism of the Internet, lies in the problem of "root server". In theory, any form of standard domain name to be analyzed, in accordance with the technical process, must be completed through the work of the global "hierarchical" domain name resolution system.

The first layer of the "hierarchical" domain name resolution system is the root server, which is responsible for managing domain name information of countries all over the world. Below the root server is a top-level domain name server, that is, a database of relevant national domain name management institutions, such as CNNIC in China, and then at the next level. The domain name database and the ISP's cache server. A domain name must first be parsed by the root database before it can be redirected to the top-level domain name server.

III. INTERNET ACCESS AND SECURITY

Any network access in the world should firstvisit the United States, and now some people say that many visits are not going abroad, and indeed some businesses do not feel abroad for the time being. In fact, the mirror root serversare working and cache serversare working. The Internet set up mirror servers in some countries without root servers, but these servers are completely controlled by the United States. Commonly used URLs can be parsed locally, and data can cache locally to prevent network congestion. However, the root of the Internet can back up the entire network. Traffic can still go out, although most of the data traffic business is domestic. This is why the United States monitors the world through the Internet, and because of economic reasons, the data traffic to the root system is two-way billing.

Since the widespread use of the Internet, the Internet has been constantly challenged, and various types of attacks from all over the world have continued. Typical server failures are as follows.

A. Failure in 1997

In July 1997, a new general list of Internet address assignments was automatically passed between these domain name servers, but this list is actually blank. This human error led to the most severe local service disruption on the Internet, resulting in inaccessible web pages within a few days and the inability to send emails.

B. Attack in 2002

On October 21, 2002, at 4:45 pm ET, the 13 servers were hit by the most serious and largest cyber-attack in history. The attack was a DDoS attack (Distributed Denial of Service). With the help of client/server technology, this attack combines multiple computers as attack platforms and launches attacks on one or more targets, thus doubling the power of denial of service attacks. Data that is 30 to 40 times more than the conventional number rushed to these servers and caused 9 of them to not function properly. Seven units lost their ability to handle network communications, and the other two were immediately behind.

This attack may not be affected by the average user. If you only analyze from the "consequences" of this incident, some people may think that "not all root name servers will be attacked, so you can rest assured", or

"the root name server has no problem with the root name server", it is still too early. But they are not clear about the root cause.

Not all root name servers are affected; the attack ends in a short period of time; the attack is relatively simple, so it is easy to take appropriate measures. Since there is no particularly effective solution for DDoS attacks, imagine that if the attack time is extended, the attack is a bit more complicated, or there is one more server, the global Internet will have quite a few web browsing and e-mail services. This will be completely interrupted.

C. DNS failure at the beginning of 2014

Beginning around 15:00 on January 21, 2014, there was a problem with DNS resolution of a large number of Internet domain names around the world. Some well-known websites and all non-existent domain names were incorrectly pointed to 65.49.2.178 (Fremont, California, United States, Hurricane Electric). China's DNS domain name resolution system has experienced a wide range of access failures, which have been confirmed by several DNS domain name resolution service providers, including DNSPod. The accident affected the whole country. Nearly two-thirds of the websites had access faults in different areas and network environments to varying degrees.

The framework of the entire network information security can be divided into three levels.

- Information security of various services at the network application layer, killing viruses, anti-Trojans, hardening firewalls and proactively defending against network attacks are the main tasks of network security departments in different countries. Andmany information security is mainly supported by encryption technology. As long as they are targeted by capable hackers, it is only a matter of time before information encryption and decryption are made.
- The network core equipment and terminal equipment, including the CPU core chip and the OS operating system/database are all from the United States. The information of this equipment is transparent to the United States and the NSA, and there is no security possibility.
- The problem of network information security caused by the lack of network sovereignty is a more global problem. Each bit under each communication IP address is monitored by the US Internet root system. All data is analyzed by the US National Security Bureau for big data analysis, and then stored and archived. The encrypted information is decrypted according to the specific situation!

In order to change the situation, China's cyberspace is in a serious strategic passive situation, in order to defend the network sovereignty and build a new generation of sovereign networks with domestically controllable security, some countries have carried out research and development of some network system structures.

IV. THE NEW GENERATION OF THE INTERNET

In 2001, Ministry of Information Industry of China established the "Decimal Network Standard Working Group". In 2007, Ministry of Information Industry of Chinadefined IPV9 as a new generation Internet to distinguish IPv6 officially.

In order to break through the future network basic theory and support the next generation Internet experiment and build the future network test facilities, including: original network equipment system, resource monitoring management system, covering cloud computing services, Internet of things applications, spatial information network simulation, network information security open network test systems such as high-performance integrated circuit verification and quantum communication networks.

In December 2014, the core parts of the future international standards published by ISO/IEC, such as "Name and Addressing" and "Safety", are dominated by Chinese experts and have core intellectual property rights. The future network has clear and unique definitions. Major countries such as the United States, Russia, Canada, and South Korea have voted in favor.

On June 1,2016, Ministry of information Industry of China published the relevant industry standards for IPV9 implementation in the country: SJ/T11605, SJ/T11604, SJ/T11603, SJ/T11606.

This marks the 20-years hard workingreceive rewards. The Chinese government has adopted the mature IPV9 main root/mother root/13 root name server system named from NZ. The core backbone router and user router product series have begun to build autonomous, intellectual property rights, and computer communication networks that are independent of the US Internet but are Internet compatible.

The main features of the future network/IPV9 are as following.

A. *Increasing the geographical and national concepts get increase*

It is distributed and managed by countries, and it is close to the analysis, and the flow of information is reasonable. End-to-end communication can be realized according to requirements, and it is not necessary to be controlled by the United States like IPv4 and IPv6. It is low-cost, high-efficiency, and it saves network expenses andachieves environmental protection.

B. *Realizing the unification of electronic tag and barcodes*

The huge address capacity of IPv9 realizes the uniqueness of address allocation. The combination of IP address, digital domain name and electronic tag and bar code coding technology will extends the network to every corner of sensor technology. IPv9 enables bar codes to have the same Internet access function as electronic tags, and can track and control the circulation of goods and equipment from the production plant. The bar code can also be identified when the RFID electronic tag wireless channel is disturbed. China's unique barcode and RFID electronic label hybrid technology will greatly reduce the management costs of the global manufacturing and logistics industries.

C. *Realize multi-code integration*

IPv9 not only makes the domain name and IP address unified, but also can be combined with the global unique identifier of the person or thing, so that the phone number, mobile phone number, domain name and IP address can be combined into one number; The same code for electronic tags and barcodes is a solution and application platform for the future information society and the realization of “ubiquitous” networks.

D. *Real-name Internet access*

IPv9 network can realize real-name Internet access, and can also protect customers' privacy rights. It can open up a certain number of anonymous addresses for blog use, but it does not allow anonymous address users to enter banks, government, social welfare, commodity circulation, etc.

E. *IPv9 has address encryption*

Different from the current means of encrypting applications, IPv9 innovatively designed address encryption to extend security protection to the network layer, greatly improving the country's information security. Whether it is IPv4 currently in use or the next-generation Internet protocol IPv6 proposed by foreign countries is unmatched.

The IPv9 communication protocol packet structure is designed reasonably, and the packet item function is clear. The IPv9 protocol is better than the IPv4 protocol in terms of address space, service quality, and security. When the application support and network device support are mature, the IPv9 protocol can replace the IPv4 protocol and become a communication protocol for network interconnection.

The address representation of the data packets of the IPv9 protocol is different from that of the IPv4 or IPv6 protocol. Therefore, the data packet header of the IPv9 protocol will not be recognized by the IPv4 or IPv6 system and will not be directly transmitted in these systems. Therefore, using IPv9 protocol communication, its data messages will not be directly transmitted to other protocols' networks, thus controlling the data transmission range and improving the security of communication to a certain extent.

F. *Currently, all hacker attacks and all online eavesdropping software are developed based on IPv4*

IPv6 routers and V9 NICs will not release these attack packets from hackers and hackers, and will build a Great Wall for hacking and online intelligence.

V. SUMMARY

The new generation Internet based on IPV9, the main root/mother root server system, the domain name resolution system, the backbone router/user router are all independently developed and produced by China, and are compatible with IPv4/IPv6. They support all existing applications of IPv4, and the underlying network itself adds IPv4/IPv6. There is no security mechanism, the address itself can be encrypted, and the communication can be verified first. At the same time, the new generation network address is extremely rich, and it also includes information such as geographic location/industry category. In the future, the network/IPV9 starts with the address 2^256 power, and the number of addresses for managing digital assets can reach 2^2048 power, future network. /IPV9 can not only meet the global 750-year communication address demand, but also an important tool for digital asset management. It is the core foundation for the future digital world/digital global and the future community of cyberspace destiny.

REFERENCES

[1] Xie Jianping etc.Method of using whole digital code to assign address for computer [P]. US: 8082365, 2011.12.

[2] S. Deering, R. Hinden, Network Working Group. Internet Protocol, Version 6 (IPv6)-Specification, RFC-1883, 1995.12.

[3] M. Crawford. Network Working Group. Transmission of IPv6 Packets over Ethernet Networks.RFC-2464, 1998.12.

[4] J. Onions, Network Working Group. A Historical Perspective on the usage of IP version 9. RFC1606. 1994.04.

[5] V. Cerf, Network Working Group. A VIEW FROM THE 21ST CENTURY, RFC1607. 1994.04.

[6] Information technology-Future Network- Problem statement and requirement-Part 2: Naming and addressing, ISO/IEC DTR 29181-2, 2014, 12.

[7] Radio frequency identification tag information query service network architecture technical specification. SJ/T11606-2016, 2016. 06.