Network Security System Design of Big Data Platform in Tai'an of Health Based on IPV9 Technology

Hongwen Zhao, Chao Lu, Yuyu Li, Guangli Li, Guotao Wen
Tai’an Branch of China Radio and Television Shandong Network Co., LTD
E-mail: tagdglcs@qq.com

***Abstract*—At present, IPv4 is the core of the Internet. When it was designed, security protection was hardly considered. Therefore, the Internet has many security loopholes, which cause information leakage or even breakdown. Compared with IPv4, IPv6 has been improved in terms of security, but IPv6 packets are not encrypted and verified by default, and the problem of network layer being attacked is still unresolved. So, the Internet based ipv6 is still faces the risk of data being monitored and tampered, which cannot effectively prevent malicious attacks. China Decimal Network Standard working group developed the future network system, which adopts the zero-trust security mechanism of verification before communication. Big Data Platform in Tai’an of Health is responsible for the unified management of all medical and health institutions in the platform, and for the management, communication and maintenance of all data. Therefore, the establishment of the network security system of this platform should pay more attention to effective, scientific and comprehensive requirements. In this paper, the Future Network (IPV9) with independent intellectual property rights in China and its encryption technology are introduced, and the network security system of Big Data Platform in Tai ' an of Health is designed, and the corresponding simulation test is carried out, which achieves the expected effect. The design of network security system of Big Data Platform in Tai'an of Health based on IPV9 can play a certain role and reference value in solving network security problems in Big Data Platform of Health.**

Keywords—Big Data; Tai'an Health Platform; Network Security Architecture; Future Network (IPV9)

I. INTRODUCTION

With the development of science and technology, the medical and health platform is gradually becoming electronic, which provides strong support for the development of the medical system by managing, communicating and maintaining the file information of all medical and health institutions in the region. In the daily use and maintenance of Health Big Data Platform, the security of information transmission has attracted more and more attention.

The network security of the Big Data Platform of Health means that the hardware, software and transmitted information in the platform can be effectively protected. The specific contents include: the platform runs reliably, continuously and stably, the network service is not interrupted, and the information in the platform is not damaged, changed or leaked due to accidental or malicious behavior. In this paper, taking Big Data Platform in Tai'an of Health as a sample, the network security architecture of Big Data Platform of Health is designed by using IPV9 technology.

Big Data Platform in Tai ' an of Health is based on IPV9 technology with national independent intellectual property rights, and a five-level

DOI: 10.2478/ijanmc-2022-0003

dedicated network for medical and health safety covering cities, districts, counties, towns, villages and families is built. Based on the medical and health information system, with the Big Data Platform in Tai'an of Health as the core, the unified management of all medical and health institutions in the platform and the unified scheduling among all business modules in the platform are realized.

II. THE SECURITY OF INFORMATION IN CHINA

With the continuous development of cyberspace and technology, network attack means emerge one after another, so it is urgent to improve the level of network security.

The rapid development of China's Internet and the continuous improvement of network application level have made great contributions to promoting economic development and social progress. At the same time, many new situations have emerged, and many new problems and challenges have been encountered in the process of network and business development, such as network security problems encountered in the application of cloud computing, big data and other new technologies. In addition, many core information technologies were invented and created by other countries, and there are certain security risks. Therefore, we should invent and popularize our own controllable information technologies. Specific analysis has the following three points:

1) The IPv4 addresses are mainly used in domestic networks.

2) The technology and means to identify the source of network attacks are insufficient.

3) The dependence on foreign information technology and products is too high.

III. THE ANALYSIS OF DEMAND

The transmission line of Big Data Platform in Tai ' an of Health is mainly wired transmission security, with the following security risks.

1) An attacker can install a stealing device on the transmission cable of the wired network to steal the data transmitted through the wired network, and analyze it by technical means, so as to obtain important information such as the account password input by the user, and even change or delete the transmitted data, which will affect the reliability and authenticity of the data.

2) After intercepting the wired data, the attacker can attack the IP address according to the IP address in the transmission information. This makes the server address or user address in the Big Data Platform in Tai ' an of Health directly exposed to the attacker.

The risk of this communication link seriously threatens the security of Big Data Platform in Tai'an of Health. Therefore, IPV9 and IPV9 encryption technologies are used to encrypt the transmission information and address at the same time in the process of communication link transmission to ensure the security of information transmission.

IV. THE KEY TECHNOLOGIES OF IPV9

The IPV9 protocol starts with basic algorithm and uses decimal algorithm to assign addresses. The address of IPv6 is 128 bits, while IPV9 is expanded to 256 bits on this basis. The IPV9 can be compatible with IPv4 and IPv6, and it can be deployed without changing the existing IPv4 or IPv6 network environment.

The protocol family of IPV9 mainly consists of the following parts: the header protocol of IPV9; Address model of IPV9 address, address text representation of IPV9, unicast address of IPV9, any on-demand address of IPV9, multicast address of IPV9 and address required by IPV9 node; IPV9 digital message format protocol mainly includes message header extension, authentication and encryption; control message protocol of IPV9; Adjacent node detection protocol of IPV9; security architecture IPSEC protocol of IPV9; IPV9 mobile communication protocol; DNS extension protocol for digital domain name of IPV9; plug and play protocol of IPV9; Transition agreement of IPV9. IPv6 and IPV9 are both based on TCP/IP framework, but they are different. IPV9 integrates many telecommunication technologies, such as the concept of phone number, geographical location and so on.

V. THE SCHEME OF TECHNICAL

A. The encryption features of Future Network

The IPV9 can be compatible with the current IPv4 and IPv6 protocols at the same time, and at the same time, it is more in line with the requirements of future long-term network development, and it is a safe and reliable bridge to the future network.

Using IPV9 technology to set up IPV9 logical isolation private network has obvious advantages compared with the previous pure IPv4 private network. The communication address in the IPV9 private network uses the brand-new IPV9 address, which is compatible with IPv4 and IPv6 addresses. When using IPv4 address for data transmission, only the application layer data can be encrypted, but the address cannot be encrypted. Attackers can attack according to the address in the data. IPV9 protocol can not only encrypt the application layer of transmitted data, but also encrypt the IP address of the network layer. At the same time, the result of address encryption is different every time, which plays a better security effect.

B. The scheme of deployment

The user access terminal of the dedicated line of medical institutions uses the special equipment IPV9 router to ensure logical isolation from other network connection systems of users' office computers.

Use 1000M-IPV9 router at the user side of the hospital access terminal. 1000M-IPV9 router is connected to the hospital client as a dedicated terminal device. Because the device uses IPV9 address to access the network, it can act as a firewall to ensure isolation from other network-connected office systems on the hospital computer. In addition, at the data transmission level, the data is in the form of IPV9 messages, and the IPV9 private network is set up. By allocating IPV9 addresses, the network layer encryption is realized, which is more secure and reliable than IPv4 networks.

With the establishment of IPV9 private network, the networking mode and network topology of Health Tai 'an Big Data Platform are basically unchanged, except that IPv4/IPV9 routers and protocol conversion routers are added in the networking mode and network topology, and other functions such as users' online habits remain unchanged. IPV9 private network deployment is shown in Fig 1.

The core area consists of two data center-level switches, both of which use VRRP technology to back up each other. When one of the switches fails, the business on this switch will automatically switch to the other switch, which will not affect the normal business use and enhance the availability of the platform.

The access area is the access area for all health and medcal institutions. Now, six 10 Gigabit firewalls are used for isolation and convergence, one for each county.

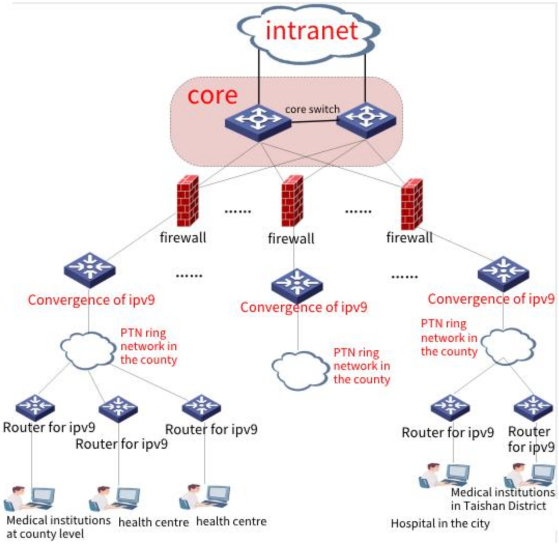


Figure 1. Deployment of IPV9 Private Network of Big Data Platform in Tai'an of Health

The network architecture of each county is the same, with IPV9 convergence router as the core, 10 Gigabit uplink data center firewall and PTN ring network as the link to ensure bandwidth and security. IPV9 convergence router encrypts and decrypts the address of the data transmitted by the access users, which makes the information transmission more secure, and accesses the PTN dedicated ring network of the county through the switch.

The IPV9 access routers with gigabit devices are deployed at the client side of all medical institutions. According to different network environments and security requirements of various institutions, strategies such as address translation, logical isolation and firewall protection are adopted.

The user still uses the address of IPv4. When the IPv4 message passes through the access router of IPV9, the header of IPV9 is automatically encapsulated. When the message passes through the IPV9 convergence router in the core area, the header of IPV9 is unsealed and restored to the IPv4 message. In this way, all IPv4 applications can run on IPV9, as shown in Fig 2. It can be seen that the network of IPV9 can be built without affecting and changing the use of IPv4 by existing terminals. Based on this, Big Data Platform in Tai'an of Health has gradually built the backbone network of IPV9.

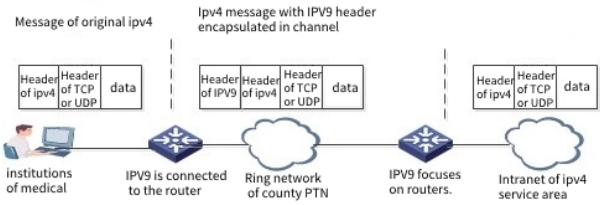


Figure 2. Encapsulation and decapsulation of IPV9 message

C. The scheme of encryption

In order to prevent the data of medical and health institutions in the access area from being tampered with or destroyed during the transmission to the core area, the Big Data Platform in Tai ' an of Health uses IPV9 encryption technology on the basis of IPV9 backbone network to encrypt the transmission. Different from the current single application encryption method, IPV9 innovatively designed address encryption, which extended the security protection to the network layer and greatly improved the security of information transmission.

In the Big Data Platform in Tai ' an of Health, the IPV9 convergence router and IPV9 access router deployed in the access area enable the conversion protocol between IPv4 and IPV9 at the same time, and enable the encryption technology of IPV9. The configuration is as follows (the eth0 network interface of two routers is the communication port of two routers):

set interface state eth0 up // Set the network interface of eth0 reverse enable eth0 4to9 // Set eth0 as the network interface supporting the conversion protocol between IPv4 and IPV9.

reverse keyset key// Set the key

The encryption principle of IPV9 in Big Data Platform in Tai ' an of Health is as follows: IPV9 convergence router A broadcasts the public key on the designated interface according to the configuration. When any device connected with the interface (such as access router B) sends data to the router, it can choose to use the public key to encrypt the data or address, and then send the encrypted IPV9 data to convergence router A and then decrypt it, thus ensuring the confidentiality of data transmission. Similarly, the same is true for IPV9 encrypted transmission from convergence router A to access router B. As shown in Fig 3.

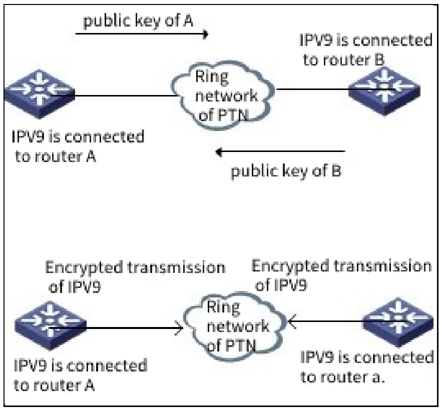

public key of A
IPV9 is connected to router B
Ring network of PTN
IPV9 is connected to router A
public key of B
Encrypted transmission of IPV9
Encrypted transmission of IPV9
Ring network of PTN
IPV9 is connected to router A
IPV9 is connected to router a.

Figure 3. Key transmission and encrypted transmission of IPV9

IPV9 communication protocol has a reasonable message structure design and clear message item functions. IPV9 protocol is superior to IPv4 in address space, service quality and security. The address expression and header structure of the data message of IPV9 protocol are different from those of IPv4 or IPv6 protocol, so the data message header of IPV9 protocol will not be recognized by IPv4 or IPv6 system and will not be directly spread in these systems. At present, all hacker attacks and all online eavesdropping software are developed based on IPv4, and IPV9 routers and network cards will not release these eavesdropping and hacker attack data packets, thus building a Great Wall against hacker attacks and wanton stealing of online information. IPV9 enables China to realize the security and controllability of the underlying Internet protocol. And the integration of advanced design concepts such as address and data double encryption mechanism has greatly improved the security of network information.

VI. THE EXPERIMENT OF ENCRYPTION SIMULATION OF IPV9

In the design scheme of this paper, the transmission from the user-side IPV9 access router to the IPV9 convergence router adopts IPV9 encryption processing to ensure the transmission security at both ends of the transmission, including address encryption and data encryption of IPV9 transmission. In this experiment, the address encryption in IPV9 transmission is simulated and tested. The topology diagram is shown in Fig 4.

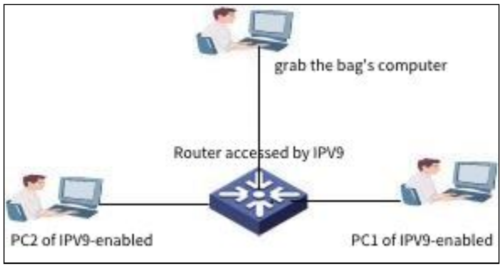


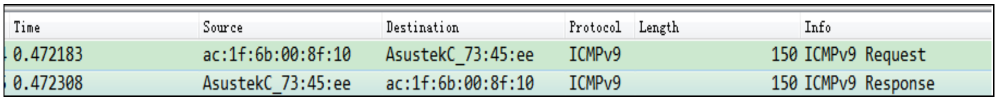
Figure 4. Packet capture test of IPV9 address encryption transmission

The process of the experiment:

1) Build a simulation test environment according to the above topology, connect two computers PC1 and PC2 that support IPV9 protocol under the IPV9 access router, and connect one computer to the IPV9 access router for wireshark packet capture analysis.

2) In order to compare the address encryption effect of IPV9, the address encryption function is enabled in the transmission direction from computer PC1 to computer PC2, but not enabled in the transmission direction from computer PC2 to computer PC1. In the test environment, the IPV9 address of PC1 is 32768[86[21[4]146, and that of PC2 is 32768[86[21[4]145.

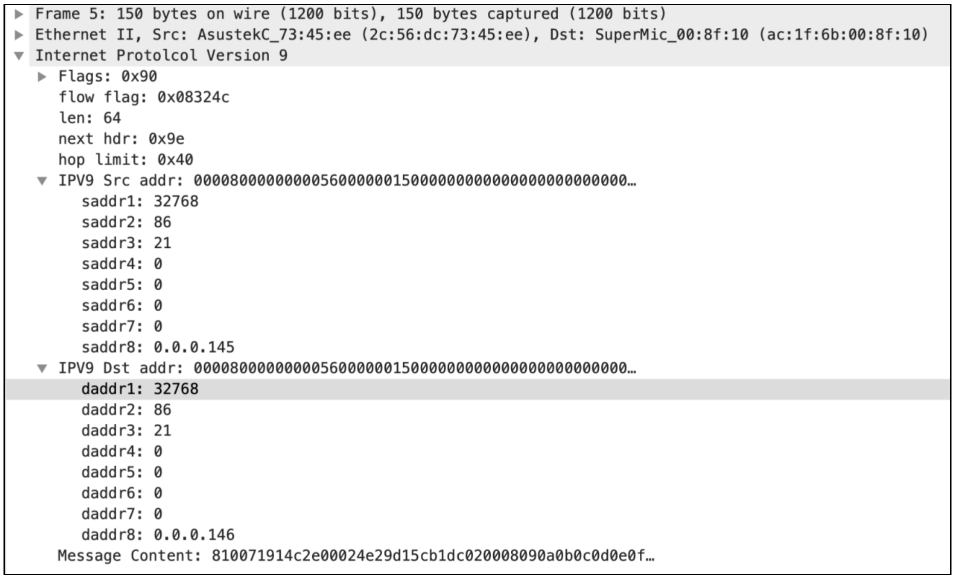
3) Ping the IPV9 address of PC2 on PC1. Then, by grabbing the packets, we found the packets of ICMPv9 protocol. As shown in Fig 5.



Time	Source	Destination	Protocol	Length	Info
0.472183	ac:1f:6b:00:8f:10	AsustekC_73:45:ee	ICMPv9	150	ICMPv9 Request
0.472308	AsustekC_73:45:ee	ac:1f:6b:00:8f:10	ICMPv9	150	ICMPv9 Response

Figure 5. Wireshark grab package 1 of ICMPV 9

4) Analyze these two ICMPV9 bags in detail. Look at the response packet of ICMPV9 first, that is, the packet with IPV9 address encryption function not enabled in the transmission direction. As shown in Fig 6.

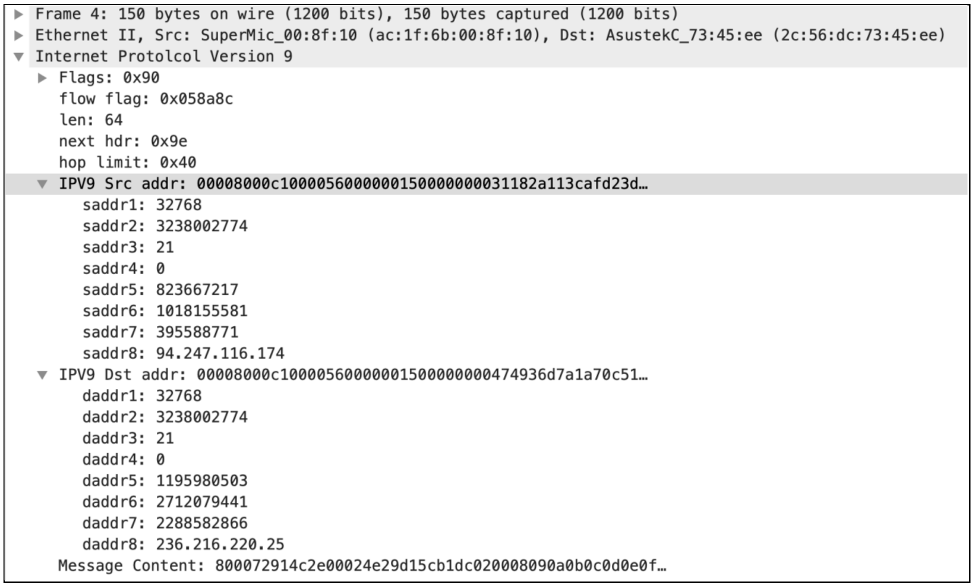


```
▶ Frame 5: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits)
▶ Ethernet II, Src: AsustekC_73:45:ee (2c:56:dc:73:45:ee), Dst: SuperMic_00:8f:10 (ac:1f:6b:00:8f:10)
▼ Internet Protolcol Version 9
  ▶ Flags: 0x90
    flow flag: 0x08324c
    len: 64
    next hdr: 0x9e
    hop limit: 0x40
  ▼ IPV9 Src addr: 000080000000005600000015000000000000000000000000…
      saddr1: 32768
      saddr2: 86
      saddr3: 21
      saddr4: 0
      saddr5: 0
      saddr6: 0
      saddr7: 0
      saddr8: 0.0.0.145
  ▼ IPV9 Dst addr: 000080000000005600000015000000000000000000000000…
      daddr1: 32768
      daddr2: 86
      daddr3: 21
      daddr4: 0
      daddr5: 0
      daddr6: 0
      daddr7: 0
      daddr8: 0.0.0.146
    Message Content: 810071914c2e00024e29d15cb1dc020008090a0b0c0d0e0f…
```

Figure 6. ICMPv9 response packet (address encryption direction is not used)

As can be seen from Figure 6, in the response packet of ICMPV9, the address of source IPV9 is 32768[86[21[4]145, that is, the address of computer PC2 IPV9; The destination IPV9 address is 32768[86[21[4]146, that is, the IPV9 address of computer PC1. That is to say, when the encryption function of IPV9 address is not enabled, the IPV9 addresses of both parties can be seen.

The ICMPV9 request packets are packets with IPV9 address encryption enabled in the transport direction. As shown in Fig 7.

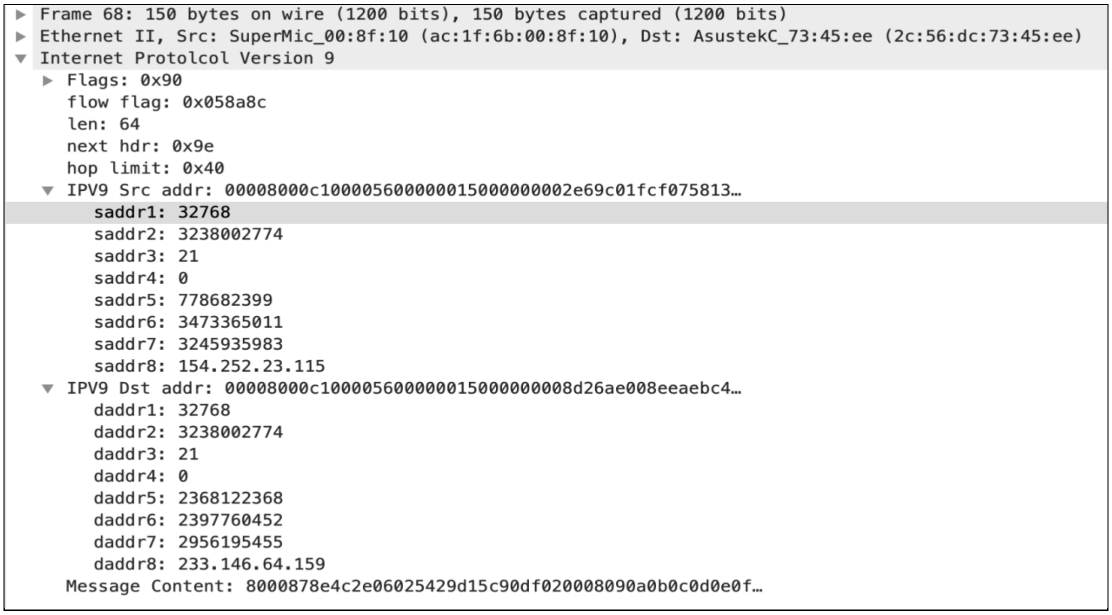


```
▶ Frame 4: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits)
▶ Ethernet II, Src: SuperMic_00:8f:10 (ac:1f:6b:00:8f:10), Dst: AsustekC_73:45:ee (2c:56:dc:73:45:ee)
▼ Internet Protolcol Version 9
  ▶ Flags: 0x90
    flow flag: 0x058a8c
    len: 64
    next hdr: 0x9e
    hop limit: 0x40
  ▼ IPV9 Src addr: 00008000c10000560000001500000000031182a113cafd23d…
      saddr1: 32768
      saddr2: 3238002774
      saddr3: 21
      saddr4: 0
      saddr5: 823667217
      saddr6: 1018155581
      saddr7: 395588771
      saddr8: 94.247.116.174
  ▼ IPV9 Dst addr: 00008000c1000056000000150000000004749367a1a70c51…
      daddr1: 32768
      daddr2: 3238002774
      daddr3: 21
      daddr4: 0
      daddr5: 1195980503
      daddr6: 2712079441
      daddr7: 2288582866
      daddr8: 236.216.220.25
    Message Content: 800072914c2e00024e29d15cb1dc020008090a0b0c0d0e0f…
```

Figure 7. ICMPV9 request packet (using address encryption direction)

In Fig 7, although there are source and destination IPV9 addresses for both sides of the transport, they are no longer the IPV9 addresses of PC1 and PC2. Note Address encryption is enabled for the transmission direction from PC PC1 to PC PC2.

5) Analyze the remaining ICMPV9 response packets in the packets captured by wireshark. As shown in Fig 8.

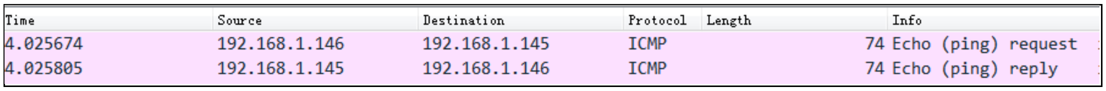


```
▶ Frame 68: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits)
▶ Ethernet II, Src: SuperMic_00:8f:10 (ac:1f:6b:00:8f:10), Dst: AsustekC_73:45:ee (2c:56:dc:73:45:ee)
▼ Internet Protolcol Version 9
  ▶ Flags: 0x90
    flow flag: 0x058a8c
    len: 64
    next hdr: 0x9e
    hop limit: 0x40
  ▼ IPV9 Src addr: 00008000c100005600000015000000002e69c01fcf075813…
      saddr1: 32768
      saddr2: 3238002774
      saddr3: 21
      saddr4: 0
      saddr5: 778682399
      saddr6: 3473365011
      saddr7: 3245935983
      saddr8: 154.252.23.115
  ▼ IPV9 Dst addr: 00008000c100005600000015000000008d26ae008eeaebc4…
      daddr1: 32768
      daddr2: 3238002774
      daddr3: 21
      daddr4: 0
      daddr5: 2368122368
      daddr6: 2397760452
      daddr7: 2956195455
      daddr8: 233.146.64.159
    Message Content: 8000878e4c2e06025429d15c90df020008090a0b0c0d0e0f…
```

Figure 8. ICMPv9 Request Packet 2 (using address encryption direction)

In Fig 8, it can be seen that the IPV9 addresses of both parties are still encrypted, but the encrypted data is different from that in Fig 5.

6) By comparing the ICMP packet of IPv4, we can see that the address in the packet of IPv4 is not encrypted by default. As shown in Fig 9.



Time	Source	Destination	Protocol	Length	Info
4.025674	192.168.1.146	192.168.1.145	ICMP	74	Echo (ping) request
4.025805	192.168.1.145	192.168.1.146	ICMP	74	Echo (ping) reply

Figure 9. Request and corresponding packet of icmpv4

In Fig 9, we can see the IPv4 addresses of both parties. When the attacker intercepts this data packet, it can forge the source IP address or the destination IP address for address spoofing attack.

This experiment shows that the IPV9 address encryption function can encrypt the IPV9 addresses of both parties. And it is one encryption at a time, that is, the result of each encryption is different. With IPV9 address encryption, even if an attacker intercepts or listens to transmitted packets, it cannot identify the real IPV9 addresses of the sending parties or the source or destination of the packets, ensuring network security for both parties.

VII. SUMMARY AND OUTLOOK

In the design of the network security system of Big Data Platform in Tai ' an of Health, the IPV9 technology independently developed by China was used to build the network, and the IPV9 encryption technology was used to ensure the security of information transmission. This is the first application of IPV9 technology and IPV9 encryption technology in the field of health care, which demonstrates the independent innovation capability of national network information technology.

This paper studies the potential threats and harms of the network transmission process of Big Data Platform in Tai ' an of Health, including transmission information theft, source address attack, etc. By using IPV9 and its encryption technology, the network security architecture of the platform is designed and implemented in a targeted way, and a lot of basic work is carried out and corresponding simulation experiments are conducted. Practice proves that the network security architecture of the platform can really improve the security coefficient of the network transmission of Healthy Tai 'an Big Data Platform.

REFERENCES

[1] Decimal network working group. Decimal network address protocol [R]. http://www.em777.net/v9bt.html, 2010

[2] Decimal Network Working Group. Digital Domain Name Specification DDNS [R]. http://www.em777.net/1.html, 2010

[3] Decimal Network Working Group. Digital Domain Name Specification DDNS [R]. http://www.em777.net/1.html, 2010

[4] Li Guoling. IPV9 transition technologyresearch and test validation [D].Chongqing Universityof Post and Telecommunications, 2018

[5] Wang Zhongsheng， Xie Jianping. Technology and Application of Future Network [M]， Tsinghua University Press，2021.02

[6] Wang Zhongsheng， Xie Jianping. Technology and Application of Decimal Network [M]， Publishing House of Electronics Industry [M]，2021.10

[7] Wang Wenfeng, Xie Jianping. Product and service digital identification format for information procession. SJ/T11603-2016, 2016. 06

[8] Xie Jianping etc. A method of assigning addresses to network computers using the full decimal algorithm [P]. CN: ZL00135182.6, 2004.2.6.

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

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

基于未来网络的健康泰安网络安全系统研究

赵洪汶 路 超 李浴宇 李广立 温国涛
中国广电山东网络有限公司泰安分公司

摘要: **目前因特网的核心是 IPv4，在当初设计时，几乎没有考虑安全防护方面的问题，因此基于 IPv4 的因特网存在诸多安全漏洞，极易受到攻击而造成信息泄露甚至网络瘫痪。相较 IPv4 而言，IPv6 在安全方面得到了一定的提升，但 IPv6 数据包默认情况下不加密和校验，网络层被攻击的问题仍然没有解决，因此基于 IPv6 的因特网仍面临数据被监听和篡改的风险，无法有效阻止被恶意攻击。中国十进制网络标准工作组开发了未来网络系统，建成了未来网络系统，该系统采用先验证后通信零信任安全机制。健康泰安大数据平台承载了泰安市所有医疗卫生机构的所有医疗健康数据的通讯、管理和维护，因此健康大数据平台的网络安全体系设计应该建立在有效、科学和全面的基础上。本文采用了我国自主知识产权的未来网络（IPV9）及其加密技术来设计健康泰安大数据平台的网络安全体系，并进行了相应的仿真模拟测试，达到了预期的效果。基于未来网络（IPV9）的健康泰安大数据平台网络安全体系设计，对解决健康大数据平台中网络安全问题能起到一定的借鉴作用和参考价值。**

关键词：健康大数据；网络安全；体系结构；未来网络（IPV9）

1. 网络安全现状

在安全方面，网络空间与现实空间融合发展使网络具有了超级基础设施的属性，网络安全问题已全面渗透到社会各个领域。网络主权已成为各国网络空间乃至国家安全与发展的重要保障。在发展方面，网络及其相关技术已经成为全球经济增长的主要驱动力，网络主权不仅关乎一个国家经济社会转型能否成功，还关系到该国未来的核心竞争力建设问题。

1.1 Internet 的安全性

目前，全球因特网的总枢纽、Web 总站、主干、建设与规划总部等机构实体全部在美国。美国通过对它们的控制而牢牢地控制了全球因特网，也控制了中国的互联网。从 2016 年 10 月 1 日起，ICANN 不是共管，而是永久性地划归美国管理。2017 年 12 月 14 日美国联邦通信委员会（FCC）正式废除网络中立法则，互联网具有了明显的政治色彩。2022 年 3 月俄乌之战，美国几乎所有的互联网企业对俄罗斯断网断服。

美国不仅控制了全球因特网和中国互联网，而且建立了美国军队赛博司令部和黑客队伍，研制了大量赛博（网络）武器，对敌对国家（尤其是中国）的网络安全造成巨大威胁。3 月 2 日，网络安全企业 360 公司发布《网络战序幕：美国国安局 NSA(APT-C-40)对全球发起长达十余年无差别攻击》的报告，外交部发言人汪文斌谴责报告曝光的恶意网络活动，再次强烈敦促美方作出解释，并立即停止此类活动。

从技术角度看，目前因特网的核心是 IPv4。IPv4 在当初设计时，几乎没有考虑安全防护方面的问题，因此基于 IPv4 的因特网存在诸多安全漏洞，极易受到攻击而造成信息泄露甚至网络瘫痪。相较 IPv4 而言，IPv6 在安全方面得到了一定的提升，但 IPv6 数据包默认情况下不加密和校验，同时其网络层被攻击的问题仍然没有解决，因此基于 IPv6 的因特网仍面临数据被监听和篡改的风险，同时无法有效阻止被恶意攻击。

工信部十进制网络标准工作组、上海十进制网络信息科技有限公司等多所高等院校和科研机构在自主可控网络方面进行了二十多年的研究，开发了整套十进制网络框架体系，完成了具有中国自主知识产权的自主可控网络 IPV9 系统。获得的专利得到包括中国、美国、英国、俄罗斯等多个国家的认可，同时得到中国工信部、国家标准委等部委的大力支持，取得了一系列创造性、国家战略性的新成果，建成了除美国之外的第二个互联网络体系。

1.2 网络安全面临的风险

网络攻击的技术和手段随着网络的不断发展层出不穷，提升网络安全水平刻不容缓。世界经济论坛《2018 年全球风险报告》中首次将网络攻击纳入全球风险前五名，成为 2018 年全球第三大风险因素。

《2017-2022 年网络安全设备市场监测与投资可行性研究报告》显示，中国互联网的快速发展和网络应用水平的不断提高，为推动经济发展和社会进步做出了巨大贡献。同时，也有许多新的情况,网络和业务发展的过程中遇到了很多新的问题和挑战，如云计算、大数据和其他新技术的应用中遇到的网络安全问题。

一是国内网络主要使用 IPv4 地址。但 IPv4 地址资源有限,特别是在 2019 年 11 月 25 日，欧洲网络协调中心（RIPE NCC）宣称 IPv4 地址都已分配。虽然国内很多地方都在推广 IPv4 地址到 IPv6 地址的过渡，但 IPv4 与 IPv6 是由国外主导的技术,存在一定的安全隐患。因此，需要保证地址资源充足的同时，也要推广我国自主可控的互联网协议，不能过度依赖 IPv4 协议与 IPv6 协议。

二是甄别网络攻击源头的技术和手段不足。特别是在使用 IPv4 地址进行网络通信时，只能针对应用层的传输数据进行加密，而不对网络层的 IP 地址进行加密。当攻击者截获数据时，可以分析出传输双方的 IPv4 地址。进而可以伪造其中一方的 IPv4 地址对另一方发起网络攻击，事后很难判断真正的网络攻击源头。

三是对国外信息技术和产品的依赖过高，内存、芯片等核心基础产品主要依靠进口，网络通信协议更是依赖于 IPv4/IPv6 的通信协议。然而，2018 年，美国封杀中兴；2019 年，美国封杀华为。越来越多的人意识到信息技术和产品能自主可控的重要性。迫切需要开发实用、易用的信息技术和产品；同时需要评估、支持和推广自主可控的产品和技术，尽快减少对国外信息技术和产品的依靠。

1.3 健康数据的重要性

健康大数据平台的网络安全是指平台内的硬件、软件及传输的信息受到保护。它包括平台的可靠、连续、稳定地运行,网络服务不中断,平台中的信息不因偶然的或恶意的行为而遭到破坏、更改或泄露。本文以健康泰安大数据平台为例，通过使用未来网络（IPV9）技术来实现健康大数据平台网络安全体系设计。

未来网络（IPV9）是由我国自主研发的通信协议，是对未来网络的一种积极探索。未来网络（IPV9）能同时兼容当下的 IPv4 与 IPv6 协议，同时更符合未来长期的网络发展要求，是既安全又可靠的未来网络的桥梁。

健康泰安大数据平台建设基于国家自主知识产权的未来网络（IPV9）技术，建设覆盖市、区县、乡镇、村、家庭五级医疗卫生安全专用网络。以医疗卫生信息系统为基础，以健康泰安大数据平台为核心，实现平台内各医疗卫生机构的统一管理、业务之间的统一调度。

2. 未来网络技术及安全

2.1 未来网络安全技术

未来网络协议从基本算法入手，使用十进制算法来分配地址。IPv6 的地址是 128 位，而未来网络在此基础上扩充到了 256 位。未来网络与 IPv4、IPv6 兼容，可以在不改变现有的 IPv4 或 IPv6 的网络环境来部署 IPV9。未来网络的协议族主要有以下几部分组成：包括未来网络报头协议;未来网络地址的寻址模型、未来网络的地址文本表示、未来网络单播地址、任意点播地址、组播地址以及未来网络节点需要的地址；

未来网络数报文格式协议,主要是报文首部扩展及认证、加密；控制报文协议；未来网络邻节点探测协议；未来网络的安全体系结构 IPSEC 协议；未来网络移动通信协议；未来网络数字域名 DNS 扩展协议；未来网络即插即用协议；未来网络过渡期协议。IPv6 与未来网络 IPV9 都是基于 TCP/IP 框架，但又有所不同。未来网络中融合了很多电信技术，例如电话号码概念、地理位置概念等。

在未来网络中，一台路由器 A 按照配置在指定接口广播公钥，任何与该接口相连的设备(如B)向该路由器发送数据时，可选择使用该公钥进行地址加密（也可选不加密）。路由器根据地址中的是否加密标志自行判断是否进行解密，注意该过程仅影响单方向的数据流向(B->A)。双向加密就是上面概念中，增加把 B 和 A 互换的过程，即 B 广播公钥，A 使用接收到的 B 的公钥进行地址加密并将数据传送到 B(A->B)。

以下为地址加密系统中对地址编码产生影响的部分：

（1）地址中总长 32 个字节中的第 5 个字节必须为 0，该字节会用于标记地址是否加密以及相关标志。（2）地址加密系统仅对总长 32 个字节中的后 16 个字节进行加密。

2.2 健康数据传输安全研究

健康泰安大数据平台的传输线路主要是有线传输安全，主要存在以下安全隐患。

攻击者可以在有线网络的传输线缆上安装窃取装置，窃取通过有线网络传输的数据，并通过技术手段进行分析，可能会得到用户输入的账户密码等重要信息，甚至可能会更改或删除传输数据，影响数据的可靠性和真实性。攻击者截取到有线传输的数据后，可以根据传输信息中的 IP 地址，针对该 IP 地址发起攻击。这使得健康泰安大数据平台中的服务器地址或用户地址直接暴露在攻击者面前。

这种通信链路的风险严重威胁健康泰安大数据平台的安全性。为此，使用未来网络地址及未来网络加密技术，在通信链路传输的过程中同时对传输信息和地址的进行加密，来保障信息传输过程中的安全性。

3. 系统安全技术设计

未来网络 IPV9 能同时兼容现有的 IPv4 与 IPv6 协议，同时更符合未来长期的网络发展要求，是既安全又可靠的过渡到未来网络的桥梁。健康泰安大数据平台建设基于国家自主知识产权的未来网络技术，建设覆盖市、区县、乡镇、村、家庭五级医疗卫生安全专用网络。以医疗卫生信息系统为基础，以健康泰安大数据平台为核心，实现平台内各医疗卫生机构的统一管理、业务之间的统一调度。

利用未来网络技术组建逻辑隔离专网，与以前单纯 IPv4 专网区别如下：未来网络专网中的通信地址使用全新的十进制地址，同时可以兼容 IPv4 与 IPv6 的地址。使用 IPv4 的地址进行数据传输时，只能针对应用层数据加密，不能对地址进行加密，攻击者可以根据数据中的地址发起攻击。而未来网络协议不仅可以对传输数据的应用层加密，还可以对网络层的 IP 地址加密，而且每次地址加密的结果都不一样，起到了更好的安全效果。

医疗卫生机构专线用户接入端使用专用设备未来网络路由器，保证与用户办公电脑其他网络连接系统的逻辑隔离。在医院接入端的用户侧使用 1000M-未来网络（IPV9）路由器。1000M-未来网络路由器作为专用终端设备与医院客户端相连，由于该设备接入网络使用的是十进制地址，可以起到防火墙的作用，确保与医院电脑上其他网络连接办公系统相隔离。另外在数据传输层面，数据是未来网络报文形式，组建的是未来网络专网，通过分配十进制地址实现了网络层的加密，与 IPv4 网络相比，具有更高的安全性，更加可靠。

健康泰安大数据平台的组网方式、网络扑拓结构与原有网络基本相同，只是在组网方式、网络扑拓中增加了 IPv4/ IPV9 路由器和协议转换路由器，网络拓扑如图 1 所示。

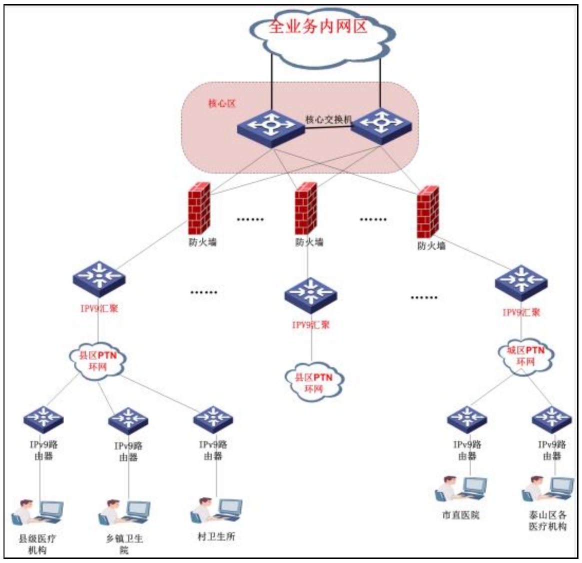


图 1 健康泰安大数据平台拓扑结构图

核心区为两台数据中心级交换机，并且都采用了 VRRP 技术进行互为备份，当其中一台交换机发生故障时，这台交换机上的业务会自动切换到另一台交换机上，不会影响正常业务的使用，增强了平台的可用性。接入区为所有卫生医疗机构接入区域，现使用 6 台万兆防火墙进行隔离及汇聚，每个县区各接入一台。各县区网络架构相同，核心为未来网络汇聚路由器，万兆上联数据中心防火墙,链路使用 PTN 环网，确保带宽及安全。

未来网络汇聚路由器针对接入用户传输的数据进行地址加密和解密，使得信息的传输具有更高安全性。通过交换机接入县区 PTN 专线环网。所有医疗机构均部署未来网络接入路由器，根据各机构的不同的网络环境及安全需求，采用地址转换、逻辑隔离、防火墙防护等策略。

未来网络接入路由器均采用千兆级别设备。用户侧仍使用 IPv4 的地址,在 IPv4 的报文经过未来网络的接入路由器时，自动封装上未来网络的报头，报文经过核心区的未来网络汇聚路由器时，再将未来网络的报头解封出来，还原成 IPv4 的报文。这种方式可以使所有 IPv4 应用都可在未来网络上运行。如图 2 所示。

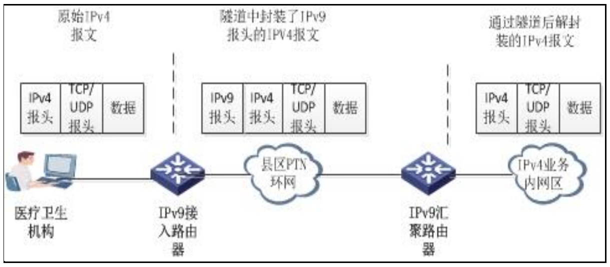


图 2 IPv4 报文封装未来网络（IPV9）与解封装

未来网络在实施中，可以在不影响和改变现有终端使用 IPv4 的情况下进行。健康泰安大数据平台以此为依据，逐步搭建了未来网络骨干网络。

为防止接入区医疗卫生机构的数据到核心区传输的过程中被篡改或破坏，健康泰安大数据平台在未来网络骨干网的基础上启用了未来网络加密技术，对传输进行加密。不同于目前的单一对应用加密的手段，未来网络创新的设计了地址加密，将安全保护延伸至网络层，极大的提高了信息传输安全性。

健康泰安大数据平台中，接入区部署的未来网络汇聚路由器和未来网络接入路由器上同时启用 IPv4 与未来网络的转换协议，并启用未来网络的加密技术。配置如下（以两台路由器的 eth0 网络接口为两个路由器的通信口）。

set interface state eth0 up //使能 eth0 网络接口

reverse enable eth0 4to9 //设置 eth0 为支持 IPv4 与未来网络的转换协议的网络接口

reverse keyset 密钥//设置加密密钥

健康泰安大数据平台中加密原理如下：未来网络汇聚路由器 A 按照配置在指定接口广播公钥，任何与该接口相连的设备(如接入路由器 B)向该路由器发送数据时，可选择使用该公钥进行数据或地址加密，然后将加密后的未来网络数据发送到汇聚路由器 A 后再解密，保障了数据传输的保密性。同理，汇聚路由器 A 到接入路由器 B 进行未来网络加密传输也是这样。如图 3 所示。

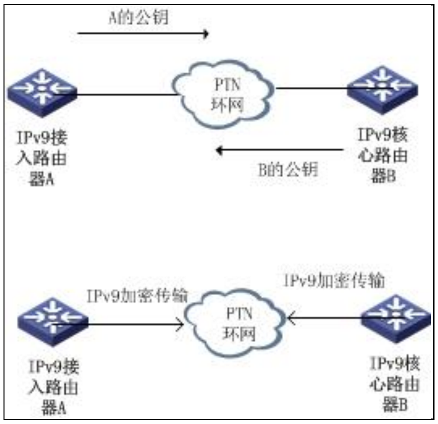


图 3 未来网络（IPV9）密钥传输与加密传输

未来网络通信协议报文结构设计合理，报文项目功能明确，未来网络协议在地址空间、服务质量、安全性等方面的设计优于 IPv4 协议。未来网络协议数据报文的地址表示方式与报文报头结构同 IPv4 或 IPv6 协议不同,所以未来网络协议的数据报文报头将不会被 IPv4 或 IPv6 系统识别，不会直接在这些系统中进行传播。目前所有黑客的攻击及所有网上窃听软件都是基于 IPv4 开发的。未来网络路由器及网卡对这些窃听及黑客的攻击数据包将不予放行，对黑客攻击及网上情报的肆意窃取筑起长城。未来网络使得我国实现了互联网底层协议的安全可控。地址和数据双重加密机制等先进设计理念极大的提高了网络信息的安全性。

4. 未来网络加密仿真测试

在本文的设计方案中，从用户测未来网络接入路由器到未来网络汇聚路由器之间的传输采用了未来网络加密处理，来保障传送两端的传输安全。其中包括未来网络传输的地址加密与数据加密。本实验针对未来网络传输中的地址加密进行仿真测试。测试拓扑图如下 4 所示。

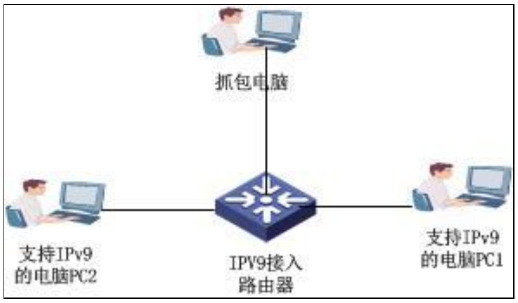


图 4 未来网络（IPV9）地址加密传输的抓包测试

测试过程如下。

（1）按上述拓扑搭建好仿真测试环境，未来网络（IPV9）接入路由器下接入两台支持未来网络协议的电脑 PC1 和 PC2，同时在未来网络接入路由器上连接一台电脑进行 wireshark 进行抓包分析。

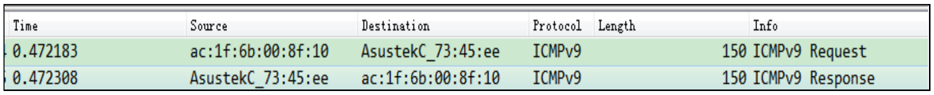
（2）为了对比未来网络的地址加密效果，在电脑 PC1 到电脑 PC2 的传输方向启用地址加密功能，在电脑 PC2 到电脑 PC1 的传输方向上不启用地址加密功能。其中测试环境中电脑 PC1 的未来网络地址为 32768[86[21[4]146，电脑 PC2 的未来网络地址为 32768[86[21[4]145。

（3）在 PC1 上 ping PC2 的未来网络地址。然后通过抓包,发现了 ICMPv9 协议的数据包。如图 5 所示。

（4）具体分析抓到的这两个 ICMPv9 的包。先看 ICMPv9 的响应包，即传输方向上没有启用地址加密功能的数据包。具体如图 6 所示。

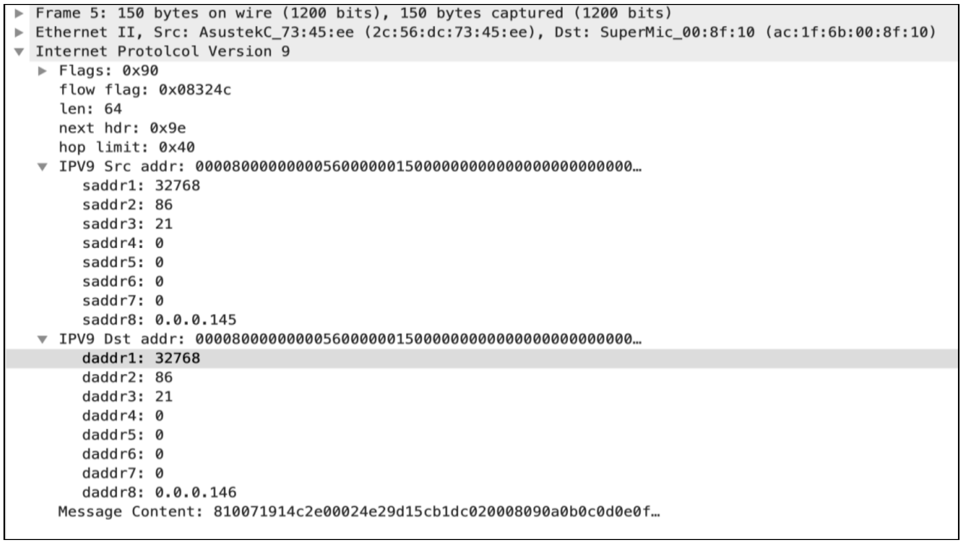
从图 6 可以看出，在 ICMPv9 的响应包中，未来网络源地址为 32768[86[21[4]145，即电脑 PC2 的地址；目的地址为 32768[86[21[4]146，即电脑 PC1 的未来网络地址。也就是说，在未启用未来网络（IPV9）地址加密功能时，能看到通信双方的未来网络（IPV9）地址。

再看 ICMPv9 的请求包，即传输方向上启用未来网络（IPV9）地址加密功能的数据包。具体如图 7 所示。



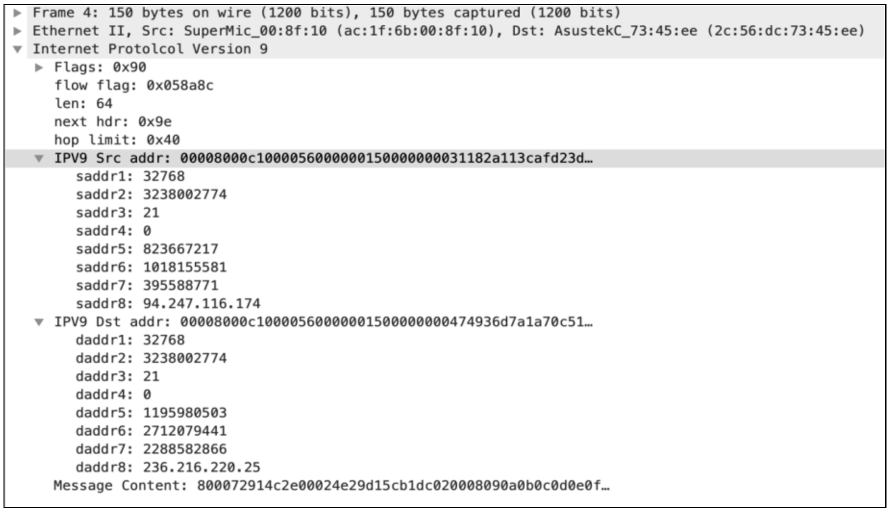
Time	Source	Destination	Protocol	Length	Info
0.472183	ac:1f:6b:00:8f:10	AsustekC_73:45:ee	ICMPv9	150	ICMPv9 Request
0.472308	AsustekC_73:45:ee	ac:1f:6b:00:8f:10	ICMPv9	150	ICMPv9 Response

图 5 ICMPv9 的 Wireshark 抓包



```
▶ Frame 5: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits)
▶ Ethernet II, Src: AsustekC_73:45:ee (2c:56:dc:73:45:ee), Dst: SuperMic_00:8f:10 (ac:1f:6b:00:8f:10)
▼ Internet Protolcol Version 9
  ▶ Flags: 0x90
    flow flag: 0x08324c
    len: 64
    next hdr: 0x9e
    hop limit: 0x40
  ▼ IPV9 Src addr: 00008000000000560000001500000000000000000000000000…
      saddr1: 32768
      saddr2: 86
      saddr3: 21
      saddr4: 0
      saddr5: 0
      saddr6: 0
      saddr7: 0
      saddr8: 0.0.0.145
  ▼ IPV9 Dst addr: 00008000000000560000001500000000000000000000000000…
      daddr1: 32768
      daddr2: 86
      daddr3: 21
      daddr4: 0
      daddr5: 0
      daddr6: 0
      daddr7: 0
      daddr8: 0.0.0.146
    Message Content: 810071914c2e00024e29d15cb1dc020008090a0b0c0d0e0f…
```

图 6 ICMPv9 响应包（未使用地址加密方向）



```
▶ Frame 4: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits)
▶ Ethernet II, Src: SuperMic_00:8f:10 (ac:1f:6b:00:8f:10), Dst: AsustekC_73:45:ee (2c:56:dc:73:45:ee)
▼ Internet Protolcol Version 9
  ▶ Flags: 0x90
    flow flag: 0x058a8c
    len: 64
    next hdr: 0x9e
    hop limit: 0x40
  ▼ IPV9 Src addr: 00008000c10000560000001500000000031182a113cafd23d…
      saddr1: 32768
      saddr2: 3238002774
      saddr3: 21
      saddr4: 0
      saddr5: 823667217
      saddr6: 1018155581
      saddr7: 395588771
      saddr8: 94.247.116.174
  ▼ IPV9 Dst addr: 00008000c10000560000001500000000474936d7a1a70c51…
      daddr1: 32768
      daddr2: 3238002774
      daddr3: 21
      daddr4: 0
      daddr5: 1195980503
      daddr6: 2712079441
      daddr7: 2288582866
      daddr8: 236.216.220.25
    Message Content: 800072914c2e00024e29d15cb1dc020008090a0b0c0d0e0f…
```

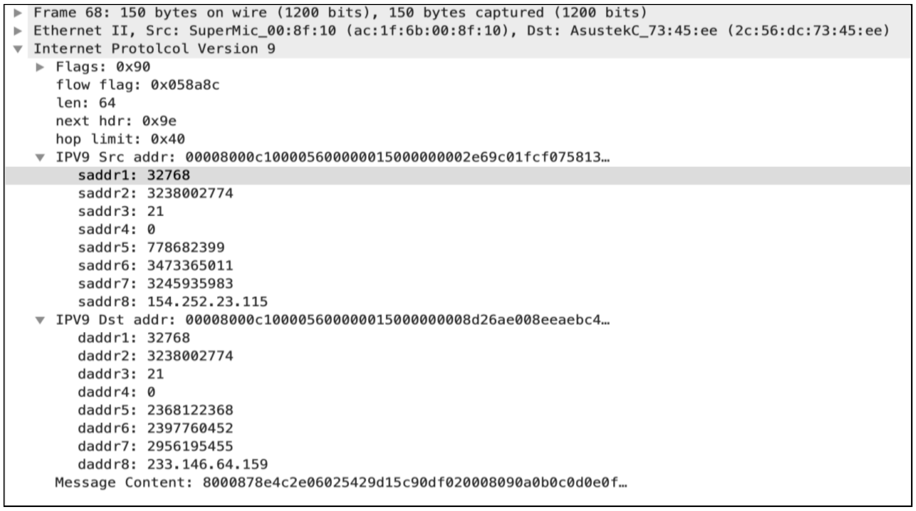
图 7 ICMPv9 请求包（使用地址加密方向）

在上图中，虽然有传输双方的未来网络（IPV9）源地址和目的地址，但已经不是 PC1 的地址和 PC2 的地址。说明电脑 PC1 到电脑 PC2 的传输方向启用地址加密功能已经生效。

（5）再分析通过 wireshark 抓的包中其余的 ICMPv9 响应包。如图 8 所示。

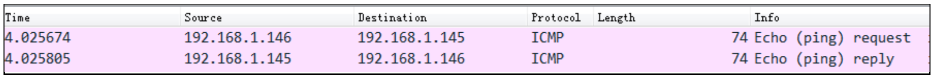
在图 8 中，可以看出通信双方的未来网络（IPV9）地址仍然进行了加密，但加密后的数据与原图中的数据是不一样的。

（6）再对比 IPv4 的 ICMP 的包，可以看到 IPv4 的数据包中的地址默认是没有加密的。如图 9 所示。



```
▶ Frame 68: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits)
▶ Ethernet II, Src: SuperMic_00:8f:10 (ac:1f:6b:00:8f:10), Dst: AsustekC_73:45:ee (2c:56:dc:73:45:ee)
▼ Internet Protolcol Version 9
  ▶ Flags: 0x90
    flow flag: 0x058a8c
    len: 64
    next hdr: 0x9e
    hop limit: 0x40
  ▼ IPV9 Src addr: 00008000c10000560000001500000000 2e69c01fcf075813…
      saddr1: 32768
      saddr2: 3238002774
      saddr3: 21
      saddr4: 0
      saddr5: 778682399
      saddr6: 3473365011
      saddr7: 3245935983
      saddr8: 154.252.23.115
  ▼ IPV9 Dst addr: 00008000c10000560000001500000000 8d26ae008eeaebc4…
      daddr1: 32768
      daddr2: 3238002774
      daddr3: 21
      daddr4: 0
      daddr5: 2368122368
      daddr6: 2397760452
      daddr7: 2956195455
      daddr8: 233.146.64.159
    Message Content: 8000878e4c2e06025429d15c90df020008090a0b0c0d0e0f…
```

图 8 ICMPv9 请求包 2（使用地址加密方向）



```
Time          Source          Destination     Protocol  Length       Info
4.025674      192.168.1.146   192.168.1.145   ICMP                74 Echo (ping) request
4.025805      192.168.1.145   192.168.1.146   ICMP                74 Echo (ping) reply
```

图 9 ICMPv4 的请求与相应包

在上图中，可以看到通信双方的 IPv4 地址，当攻击者截获这个数据包后，可以伪造源 IP 地址或目的 IP 地址进行地址欺骗攻击。

通过本实验，可以看出未来网络的地址加密功能能对传输双方的地址进行加密，并且是一次一密，即每次加密的结果都不一样。通过未来网络（IPV9）地址加密，攻击者即使截获或侦听了传输的数据包，也无法判断发送双方的真实未来网络（IPV9）地址，无法判断信息来源或去往，保障了通信双方的网络安全性。

5. 结论

健康泰安大数据平台网络安全体系设计中，使用了我国自主研发的未来网络（IPV9）技术进行了网络建设，并使用了未来网络（IPV9）加密技术来保障信息传输安全。这是未来网络（IPV9）技术及未来网络（IPV9）加密技术首次在健康医疗领域的应用，彰显了国家网络信息技术的自主创新能力。本文研究健康泰安大数据平台的网络传输过程的潜在威胁和危害,包括传输信息窃取、源地址攻击等等，通过使用未来网络地址及其加密技术，有针对性地进行了平台网络安全体系架构设计与实现，开展了大量基础工作并进行了相应的仿真实验测试，实践证明该平台网络安全体系确实能提高健康泰安大数据平台的网络传输的安全系数，具有一定的应用价值。

参考文献

[1] 十进制网络工作组.十进制网络地址协议[R].http://www.em777.net/v9bt.html，2010

[2] 十进制网络工作组.十进制网络地址协议[R]. http://www.em777.net/v9add.html，2010

[3] 十进制网络工作组.数字域名规范 DDNS[R]. http://www.em777.net/1.html，2010

[4] 李国领. 十进制网络过渡技术研究及测试验证[D].重庆邮电大学,2018

[5] 王中生，谢建平. 未来网络技术及应用[M]. 北京：清华大学出版社，2021.

[6] 王中生，谢建平. 十进制网络技术及应用[M]. 北京：电子工业出版社，2021

[7] 王文峰，谢建平用于信息处理产品和服务数字识别格式. SJ/T 11603-2016, 2016. 06

[8] 谢建平. 联网计算机全十进制算法分配计算机地址的方法[P]. CN: ZL00135182.6, 2004.2.6.

[9] 谢建平等. 采用全数字编码为计算机分配地址的方法[P]. US: 8082365, 2011.12.

[10]信息技术-未来网络- 问题陈述与请求-Part 2: 命名与寻址, ISO/IEC DTR 29181-2, 2014,