Bachelor's Thesis (UAS)

Bachelor's Degree of Information Technology

2011

Zeng Qijia

Network Security and Implementation Based on IPV6

TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

BACHELOR'S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Information Technology | Internet Technology

Date: 06/2011 | Number of pages: 45

Instructor: Patric Granholm

Zeng Qijia

Network Security and Implementation Based on IPV6

With the application of Internet services continuing to develop, the portable demands for user mobility are growing rapidly. To solve the issue of the Internet, IPv6 protocol, based on IPv4, is proposed and studied. IPv6 replacing IPv4 and becoming a new IP protocol is an inevitable process, but IPv6 technology is not yet very mature, but it needs to be further improved.

Meanwhile, network operators work independently, they have their own network resources and equipment, and each of them uses different systems for supporting and managing programs. Users are continuously presented with a variety of service provider account numbers and passwords, which add burden and impede to use of network resources speed. Therefore, the corresponding authentication, authorization and accounting have become the urgent demand of business applications and enabling better integrations of the AAA IPv6 turns to a hotspot issue.

This thesis presents an overview of network security and studies the IPV6 basic characteristics on certain restricted network security. It also presents a comparison of the advantages and disadvantages of the transition tunnel IPv6 to IPv4 technology, dual stack technology and translation technology.

KEYWORDS:

IPv6; IPSec; Security Protocol

CONTENTS

FIGURES

ACRONYMS, ABBREVIATIONS

AH	Authentication Header
ARP	Address Resolution Protocol
ASBR	Autonomous System Border Router
Bastion Host	A special purpose computer on a network specifically designed and configured to withstand attacks.
ESP	Encapsulating Security Payload
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IPSEC	Internet Protocol Security
ISP	Internet Service Provider
Jumbo Payload	Internet Protocol version 6 (IPv6), a user data field that exceeds the IPv4 limit of 65,535 octets. A jumbo payload is indicated in the payload length field of the IPv6 header.
NAT	Network Address Translation
OSI	Open Systems Interconnection (OSI) protocols
RFID	Radio-frequency identification
VPN	Virtual Private Network

1 Introduction

1.1 Background

The innovation of computer science has deeply influenced every aspect of human daily life. Since the Internet was invented, it has been quickly utilized, dramatically shaped our society and science technology. However, network technologies have also plenty of threats while providing a convenient life. In the other words, with the development of internet technologies; these threats are always associated with network security.

The IPv4 protocol is the most widely used on the Internet for more than 30 years. However, with the rapid development of today's Internet technology and client devices, IPv4 no longer matches the enormous demands which cause the fatal issue of network security. The Internet had had some flaws since it was invented because it has not been considered as an entire security structure. The current security technologies are policies to revise the original structure. For resolving this issue, IPv6 standards come out, as proposed by IETF. Although it was immature at the beginning, after a decade’s development, IPv6 has become more completed as the backbone of next generation Internet standards.

IPv6 has two un-negligent advantages: On the one hand, IPv6 has an extremely enormous address pool for categorization of different layer addresses; this is really good news for clients. On the other hand, IPv6 provides a direction for establishing the latest Internet generation, meaning that it is also furnished with a feasible platform and technical support for network security.

Until now, most of the implementations of IPv6is just modifications based on IPv4, they are not independently established on IPv6 functions, they can only adapt to IPv6 environments. So these implementations are traceable from those previous technologies. Owing to this fact, the demand of inventing a new application based on IPv6 requires illustrating its advantages and powerful functions. Therefore, research on IPv6 implementations need to be isolated from environments run on IPv4. In this way, we can exemplify the comprehensive improvements on IPv6.

1.2 Research on IPv6

In the last decade, concerning international research on IPv6, many research institutions forced on different areas and got different achievements. China with the largest population in the world is also catching up with the West. By looking backward, IPv4 research in China has more than 30 years delay than another developed countries, but only a few year delay on IPv6. The time factor is not dominant, but the research has developed so rapidly because of government financial support. In a sense the Internet is the backbone of a country, it not only influences people's life, but it is also an insurance of political, military and economic development. In the recent future, China will occupy the leading position in IPv6 development. Applications of IPv6 are widely used in home networking, sensor networking and e-commerce. This is mainly caused by its security, auto-configuration capabilities and huge address space. In addition, the new generation of IP mobile technology, the special needed internet and high-speed portable internet, have become hot topics in our life. Most people began to realize that by combining it with other related technologies, such as broadband networks and RFID to achieve the best implementation of IPv6.

2 Analysis of Network Security

2.1 Network security

Network information can be divided into static information and dynamic information. The static information is stored in the network nodes, while dynamic information is transmitted between nodes in the network information. Either static or dynamic information could only have two states, some are open, but some are kept confidential. [1]

For security reasons, we must ensure that the network have certain attributions which are confidentiality, integrity, availability and authenticity. In the early of 21st century, the developed countries completed the security framework on the aspects of confidentially, availability, practicality, and occupancy. There are several aspects of information security that should be considered frequently and have been listed below:

(a) To ensure the confidentiality of information, isolating the information from un-secure users is important.

(b) Complete information means that information consistently remains unchanged regardless of utilization. In other words, there is no packet loss. Usually if the information is incomplete, this means that it is under threat, as well. The current general protocol only ensures the uniformity of data packets in the transition process, but does not allow unsecure users to exchange related information.

(c) The guarantees for valuable information are a correlation of non-static information and non-dynamic information.

(d) Ensuring that the information has high credibility also strengthens its authenticity. This is the significant method to identify the information.

(e) Network information is practical, because the encryption key network information is very important and we must ensure that it is not leaked. Keys and information are closely related.

(f) Network information has occupancy. Once information has been leaked on nodes, disks, or another carrier, the occupancy rights are lost at the same time.

In summary, the network information must ensure no disclosure, so the location of information on the network is extremely vital.

2.1.1The main goal of network security

The most important aspect of network security is the network information security. Therefore, the ultimate goal of network security is non-disclosure of network information security. It has two aspects: the safety of the stored information and the security of information transmitted [2, 3, 4].

(1) In the situation of the storage carrier, authentications identifications and permission settings are an important guarantee for security technologies.

(2) The information must be ensured at secure status in transmissions. That is mainly related to the transition process between users and the networks.

Therefore, several features must be implemented such as: confidentiality, integrity, and availability.

a. Confidentiality: This is priority No.1 to be considered in network security.
b. Integrity: It refers to information that cannot be changed without authorization.
c. Availability: Information can be changed very easily to by a user's action.

2.2 The security threats

Network security includes two aspects: the first one is the security of network data, the other one is the security of network devices. They are related to the safety of a variety of network threats, both objective and subjective factors. For example, when a message is transmitted through the network, it may encounter information disclosure, fake identity, or it can be tampered. [5,6]

A network can be very fragile and be easily attacked by malicious code. Meanwhile, the user's information is also threatened, as well. There are large numbers of malicious code, such as computer viruses, computer worms, Trojan horses and logic bombs.

2.3 Network attacks

2.3.1 Classification of network attacks

Network security is implemented through the use of technology and management to measure the normal operation of network systems to ensure data availability, data integrity and data confidentiality. Network security has specific meanings from different perspectives. For example: from the users' (individuals, businesses, etc.) point of view, their need privacy or commercial information is protected on transmission. Generally, the attacks can be divided into two categories [7, 8].

(1) Passive attacks

In such circumstances, an attacker can easily obtain secret information through monitors. These kinds of attacks depend on the networks and systems, but are also unlikely to be noticed by administrators.

(2) Active attacks

These attacks are related to changing the data flow and creating an error influx. The most common methods of attack include faking, relay, spoofing, and message tampering server rejection and so on. Usually, the attackers use the system's security vulnerabilities to gain access to the client or the server.

2.3.2 Categories of attacks

There are no absolutely safe networks, only relatively secure networks. The security is proportional to the data importance on the network. Network attack patterns show various means at the major subsystem level. The attacks include: denial of service attacks, using type attacks, information gathering type of attack, the false message attacks.

(1) Denial of Service attack

This method refers to crashing or rolling the target computer to abort the services. It is the most convenient method to produce aggressive behavior, such as:

a. Ping of death
b. Teardrop
c. UDP flood
d. SYN flood
e. Land attack
f. Smurf attack
g. Fraggle attack
h. E-mail bombs
i. Deformity message attack

(2) Use in attack

It attempts to control the computer directly, including the following forms:

a. password guessing
b. Trojan horse
c. buffer overflow

(3) Gathering information-based attacks

This kind of attack will not generate any threats on the target; it can provide lots of information for further invasion. It is mainly related to:

a. Scanning technology(address scan)
b. Port Scanning
c. Response mapping
d. Slow scanning
e. Architecture exploration

(4) False message attacks

These attacks are based on detecting the target incorrect configuration.

Such attacks include: DNS cache pollution and Forged E-mail.

2.4 Network security policy

2.4.1 Physical security policy

In the recent years, the network brought us more and more securtiy threats while benifiting our dialy lives. So the users must utilize certain network security measures.Today the main network security mainly involves the following aspects:[9]Physical security policy mainly includes the following aspects:

(1) The physical protections for computer systems, printers,network servers and other objects, that is, keeping the communication link away from natural disasters,malicious disturbances and console attacks.
(2) Checking the user's identity, and verifying specific permissions to prevent unauthorized operations.
(3) Ensuring that the computer systems run well in an compatible electromagnetic environment.
(4) Managing relatively complete rules and regulations to prevent external users, non-regular staff, and illegal entry into some of the operatinos room.

2.4.2 Access control policy

Access control is an essential policy for network security. Analysing access control strategiesis used to determine whether the network resources been used without authorization.

(1) Authentication control

Network access control provides the first layer of access control for network security. With this policy, only the users who have permisson can log on to the server, obtain network resources.Moreover it also enablesthe administrator to monitor login time control and login location control.

(2) Authorization control

This is a security control strategy, using network access control to authorize every single user with a certain privileges. The users could visit and modify the files according to the privileges they have.

(3) Directory level security control

To ensure network security, privilege access control has been implemented between users and directory,files, anddevice access. After setting the user's privileges level on the root directory, these privileges are automatically applied on all sub-directories and files. In order to strengthen the authority of the settings, the user can set the more particular permissions on certain sub-directories and files after the privileges control.The administrator of the network systems should configure different privilege based on user roles.

(4) Networking monitoring and locking control

To ensure real-time network security, network adminstrators should implement areal-time network monitoring. If there is someone trying to enter the network without authentication, the server automatically logs thisviolated access, meanwhile a counting alarm should also be implemented, so when the access tries reach the maximum number of settings, this unknown users or unlisted IP address should be locked until the administrator activates it manually again.

(5) Security control of the ports and nodes

The network server port is typicallysupplied with anautomated call back device; this device automaticlly responds to the call. The server could strengthen the protection policy by identifying the nodes with an encrypted ID.

(6) Firewall control

A firewall can be implemented between the internal networks and the external networks to improve network security.While a network is connected to the Internet, the unsecure information and services will be isolated. When a suspicious message invades the internal networks, the firewall will provide the alarm, and block the suspicous messages from the external network.Meanwhile, the firewall also prevents the leakage of internal network information. Through planning the resources of the internal networks, an administrator can manage and isolate the vital information and segments. By operating a partial network independently, we can prevent the problems widely propagating out to the entire network.

2.4.3 Information encryption policy

In order to effectively protect the data on the network,files,passwords and information transmission, using information encryption strategy for further encryption is a good choice. Generally, network encryption methods are divided in three categories:. link encryption, port encryption, and nodes encryptions.The link encrptions is the best options for protecting the information between network nodes.If the user is the initiator to the destination user data protection, we use end-to-end encryption. In order to protect the transmission link between the source node to destination node, then node encrytion is needed. By understanding the three characteristics of information encryption strategies, the user can select specific network conditions to meet the current network situations.

Network information encryptions correspond to different type of networks,so we can use a variety of different encyption algorithms to achieve encryption of information,but the whole process of information encryption is a combinations of all these encryption algorithms. In many cases, the information encryption is the only effective method to protect securtiy withlimited financial support.

(1) General key cryptography

For instance, when we send a secret letter to our friends, in order to ensure the confidentiality of the letter we sent, we usually encypted it with a key. The receiver needs to decrypt the letter with the key before reading it. So the encyption key and the decryption key are equivalent,which is the conventional encryption method. The

advantages of this method are: the degree of confidentiality is generally strong, it is able to withstand the test of time and attacks,but the problem is the transmission process of the key must be under secure status.

(2) Public key cryptography

The differece between the general key cryptography and the public key cryptography is that we use a differnet key to decrypt the letter. That means that the encryption key and the decryption key are not equvialent and there is not any formula or rule to derived one from the other. So this creates a certain amount of difficulties on the decryption side. Nowadays, modern electronic technology and encryption technologies are developing rapidly. Public key cryptography in the practical applicationsis very common. However, to be realistic, people usuallyntergrate the two methods.

2.4.4 Network Security Management

In the computer network system, an important guarantee for network security is the developed safety management, that uses all the tools and techniques to minimize the potential threats.Strengthening the standardization of network security management, forcusing on development of security technologies and improving staff and managers' awareness of security are significant in the century ofinformation explosion. IP addresses is a resource that had previously been igored by managers. In order to implement a secure network, unified management and allocations of IP addresses are necessary.

2.5 Technologies of network security

With the continuous development of computer network technologies, more and more people are involved in the discussion and concerns fo the network security issues.Although so many people are distributed to security of computer networks,there are still potencial unkown threats and attacks. In order to achieve the security of computer networks, we could begin todeal with the following problems. They are repairing network vulnerabilities, data encryptions, authentication of network information, network security transmission protocol and establishing a stable firewall.[10]

2.5.1 Data encryption

We have already mentioned above that there are many methods to implement network security but data encryption is recognized as the one of most basic technologies. It is an active method to encrypt the transmitted data on the network. In terms of maintaining network security, it costs less but it is effective. However, it has its own flaws due to the relatively diffcult manintance. Therefore, in practical applications, it can not be widely accepted. In the original data transmission network through encrypted encyption technology, the transmission process in the network is not concerned withhackers intercepting those clasdified documents. After this encryption process, this information can hardly be leaked and intercepted. This makes the network more secure.

The network transport protocol is still based on the OSI seven layer protocol, so data encryption can be implemented on several layers. Considering the aspect of the logical location from the network transmisstion, we can divide encryption technologies into following three forms:

(1) Link encryption

Generally, the network of data transmission has been divided into synchronous encryption and asynchronous encryption.Synchronous encryption is further divided into byte synchronous communication encryption and bit encryption. The encryption process is usually completed by online encryption devices to protect the communication securtiy between nodes. This encryption process has been made below the network layer of the OSI model. This techology of encryption is referred to as link encryption.

(2) Node encryption

Owing to the fact that data transmission between nodes in the network is vulnerable to unauthoried access, to eliminate the security problems, node encryption has been proposed following the improvements of link encryption technology. Node encryption technology is implemented by encrypting the transmission data between the source node and the destination node. The difference with the link encryption is that this encryption algorithm is dependent on the module of node encryption.

(3) End –to-end encryption

With the rapid development of modern enterprises, large-scale enterpirse network systems are constantly emerging, information transmission happen on muti-senders

and muti-receivers. In order to easily apply this process to enterprise application software, end-to-end encryption has proposed on the OSI network layer.This encryption technology is called end-to-end encryption technologies.

Encryption can be simply divded into three types, easy-decyption, private key encryption technology(also known as pirvate key encryption algorithms), private key encryption, which i uses the same key for encryption and decryption. For example, the sender encrypts the original data with a key, while the receiver receives the encypted data; the same key is used to decrypt these data. The advantage of this method is the degree of confidentiality of information encryption is generally strong, able to withstand the test of time and attacks, but the problem is the transmition process of the key must be under the secure status. In fact,this encryption is called conventional encryption.

Diffie-Hellman first proposed a new encryption mechanism in 1976, the public key encryption system.When sending information or receiving information, each network user has a pair of keys. In this pair of keys, one is the public key and the other one is the private key. When sending the messages, the sender uses the public key to encrypt data. After information has been issued, the recipient uses their private key to decrypt data. The public key encryption algorithm uses a one-way trap door function for processing the message. This function has its own inadequancies, which is that from one side, the value is relatively easy to find, but from the opposite direction it is not easy to to calculate. This encryption application causes difficulties in its implementation. So in securtiy and management, public key encryption technology has some advantages, but the decryption process often takes a lot of time.

Public key encryption a very mature technology.There are some famous encryption algorithms, such as the knapsack algorithm and the McEliece algorithm.However, both

of them have been deciphered. Nowadays, the RSA algorithm and the Rabin algorithm variant of RSA and discrete logarithm algorithms have been recognized as more secure.

The first encryption technology mainly focuses on type as the password encryption, it only needs to be encrypted compared with previous encryption; the second and the third encryption are based on using the different segments of key.

2.5.2Firewall Technology

Firewall technology is established in the modern communication network and information securtiy technology, and it is increasingly used in private network and public network interconnection enviroments, paricularly in the border network with the Internet. Today firewalls are used to protect computer networks from the harassment of non-authorized users and hackers. They arejust like a barrier across the protected internal network and insecurity non-trusted network.The current widely used Internet is the world's largest unsecure network, as many hacking incidents and attack occur through the Internet.

A firewall can be a very simple filter, it may be a well-configured gateway as well, but the principle is the same, itis used to monitor and filter all information exchanges between aninternal network and anexternal network. Afirewall protects the sensitive data from theft and destruction, meanwhile it also records the status of internal and external communication logs, such as communication time and place of the operations

and so on. Firewalls are usually run on a separate computer on a special service that can identify and shielding illegal requests.

According to the security needs of an enterprise, a firewall can t control the flow of information that is generated by security services, network and information securtiy infrastructure. The firewall has a very strong resistance to attacks. By configuring a combination of security policy in different security network domains or safety areas, a firewall is established. It is the only outlet for information.

The firewall can effectively monitor any activities between an internal network and the Internet. It was been recognized as a separator, a limiter, but also an analyzer. A standard firewalls shown in Figure 1.

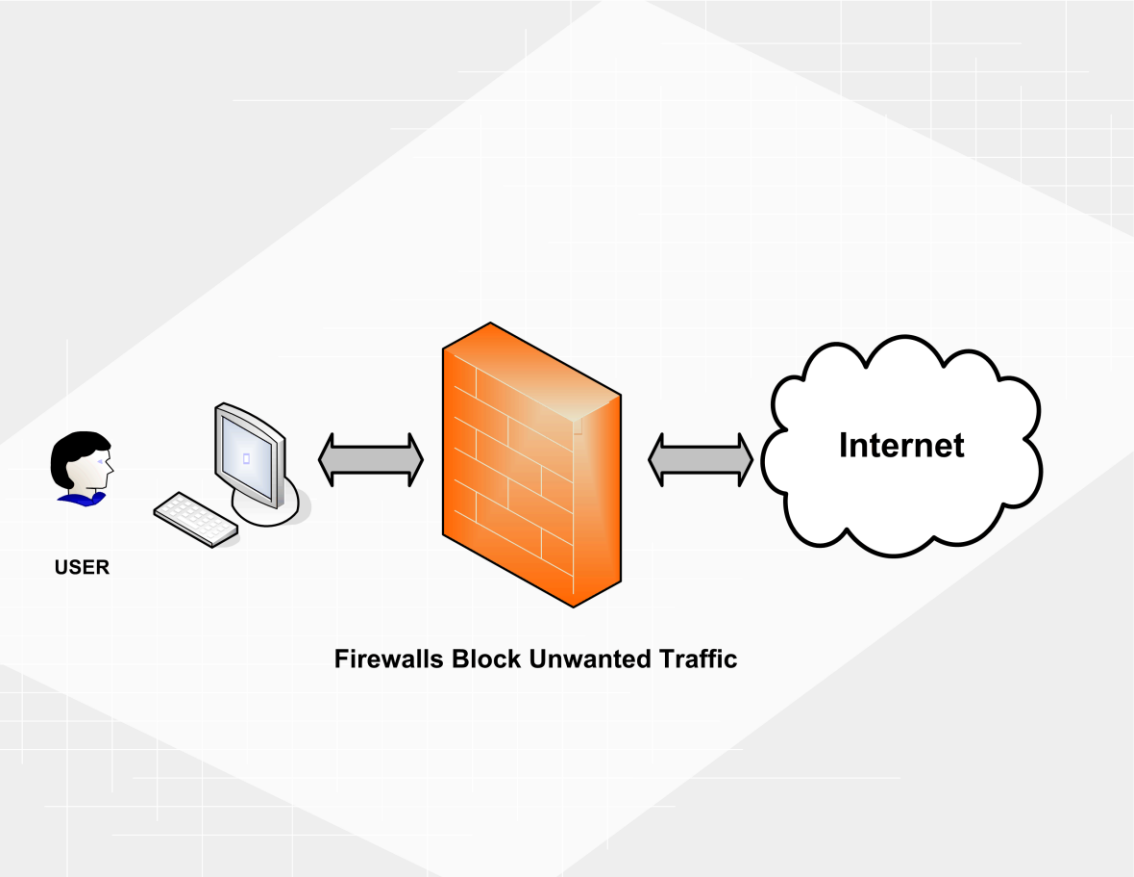


Figure 1. A standard firewall

Firewalls can be divided into three types according to defending features and the variety of emphases which are packet filtering, application proxy, and the compound firewall.

(1) Packet filtering

This process is based on packet header source address, destination address, port number and protocol type to determine whether the data are qualified to pass through.Only the packets which fullfill the conditions can be forwarded to the

destination while the unqualified packet will be dropped. This process happens at the network and transport layer.

(2) Application proxy

It is also called application gateway, which acts at the application layer and is usually achieved by a dedicated workstation, implemented as the first layer of the OSI layer module. The main feature of the application gateway is that for each application service there is a particular application agent for monitoring and controlling the data flow over the application layer. The application gateway is the isolation point between the internal and the external network. It does not only monitor and isolate the traffic at application layer, but it is also intergrated into filter functions. The application gateway holds all the information about security decisions.

(3) The compound firewall

The compound firewall is based on packet filtering and application proxy; it is a combination of application proxy and packet filtering.It has very high security requirements. A complex combination of firewalls usually has two ways to screen host firewall architecture and subnet firewall architecture.

a. Shielding the host firewall arhitecture is the packet filtering router or firewall that is connected with the Internet, while bastion hostis installed in the internal network.By configuring the filter rules on routers or firewall, the firewall becomes the only one node that can be reached from the Internet. In this way, the internal network is kept away from non-authorization attacks.

b. Shielding the subnet firewall architecture This means that the bastion host is located inside the sub-network, forming a demilitarized zone and the two packet filtering routers areconfigured at the two terminals of this sub-network, making this sub-network isolated from the internal network. The bastion host and packet filtering routers consititude the basis of the entire firewall security.These two architectures are Shown in Figure 2and 3.

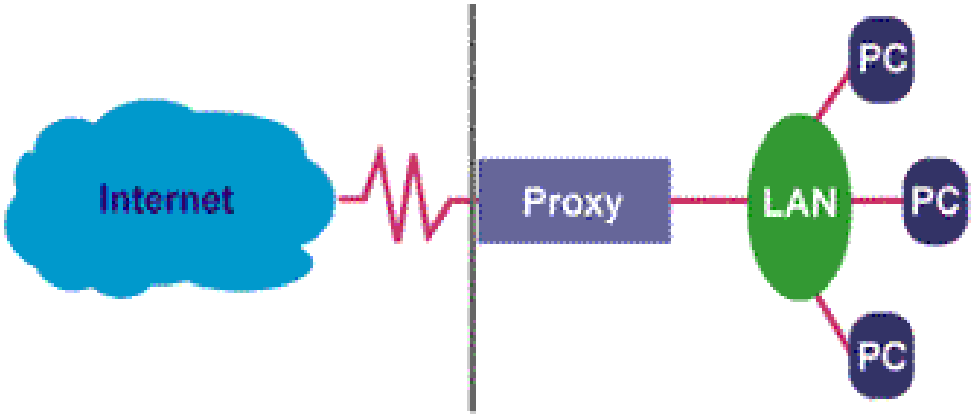


Figure 2. Application proxy

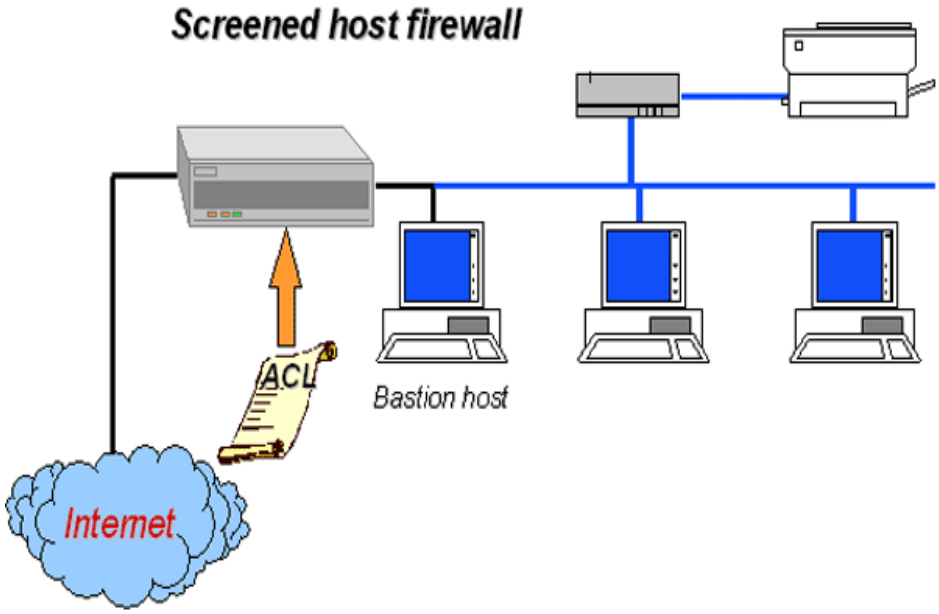


Figure 3. Screened host firewall

3 IPv6Overview

Currently, the global Internet protocol suite is TCP/IP protocol. IP is the core of the agreement protocol family and is proposed as the network layer protocol. The current IP protocol version number is 4(called IPv4). It is the core technology belonging to the U.S.A.. The greatest problem for IPv4 is that it provides limited network addresses. Although theoretically speaking, it can provide more than 16 million network address and 40 million host address. The current IP address in many regional areas have been exhausted. Moreover, due to historical reasons and other factors, IP address allocation

is unbalanced, about 30 billion in North America take up75% of the whole address pool, while Asia with a much larger population has less than 400 million address. China has only 3 million addresses,the same amount as the Massachusets Institute of Technology.

The next version of Internet protocol is IPv6(Internet Protocol Version 6). It is desiged by IETF to replace IPv4. IPv6 is in continuous development and improvement.

The current development of the Internet, can be described as in a diffcult stage. On one hand, the number of IP address are limited. On the other hand, with the rapid development of electronic technology, the computer network becomes an indispensable part of our life as more and more electronic device are needed to connect to the Internet. IPv6 is proposed under this situation. The total amount address of IPv6 is 2^{128} -1, it is about $8*10^{28}$ times more than IPv4. IPv6 can not only resolve the problem of insufficent IP addresses, but also provide enough addresses for other electronic devices. Figure 4 shows the challenge of Internet technology in IPv6.

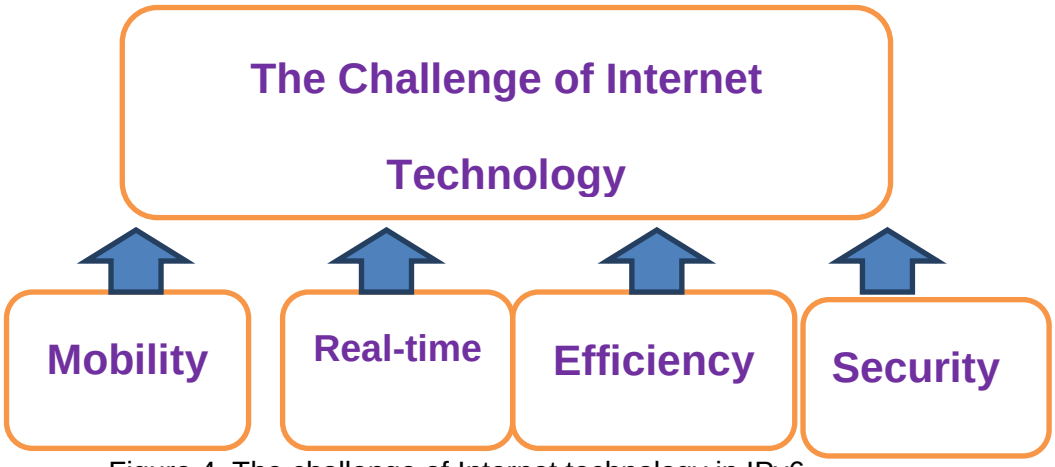


Figure 4. The challenge of Internet technology in IPv6

3.1.1 Extension header

The IPv6 packet header design is based on IPv4, but it has a lot of improvements. One of the main differencesareis the optional fields which exist in the IPv4 header, has been added into the extended header. Because the extended header does not need to traverse the router, this reduces the number of packet processing steps, so IPv6 data transmission efficiency is greatly increased. In the IPv6 network, if routers do not need to consider the packet, then the extended header is not required, the routers only need to packet or join the packets and the extended header will be created in order to save the information of the destination addresses.

The following are some common extension headers:

(1) Hop-by-Hop Options header: the extension header is included in the packet transmission process and each router must examine and deal with the specific parameters of the option. Among them, the option type is 0 which is responsible for filling the single byte. PadN option type is 1, usually carried out by the Jumbo Payload- The Jumbo Palyload option type is 194; for the load more than 65.535 bytes of data packets are also delivered by Jumbo Payload.

(2) Destination Options: The destination options header must be in the extension header because in the process of data transmission, transit routers need to traverse the destination address for delivery. This reduces the workload of processing the destination addresses for the nodes.

(3) Sub-Header:When the data packet transmitted is large, the sub-header comes in much useful, which is mainly responsible for large data packets fragmentation and reinstall.

(4) Routing Header: The Routing Header is one of the IPv6 extension headers and is identified by a value of 43 in the Next Header field. A routing header can appear either as the first extension header after the IPv6 basic header, or after another extension header.

(5) Authentication Header: The authentication header does not ecypt the data directly but the header can be conbined with the ESP protocol to protect data and ensure data integrity.

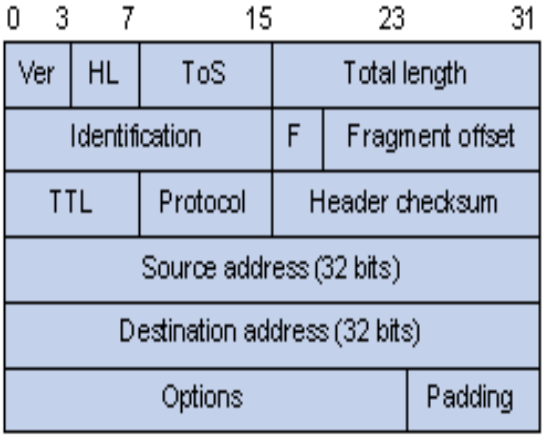
(6) ESP protocol header: As mentioned in the authentication header, the ESP header is responsible for the data encyption protocol to ensure data security.

3.1.2 The structure of IPv6 address.

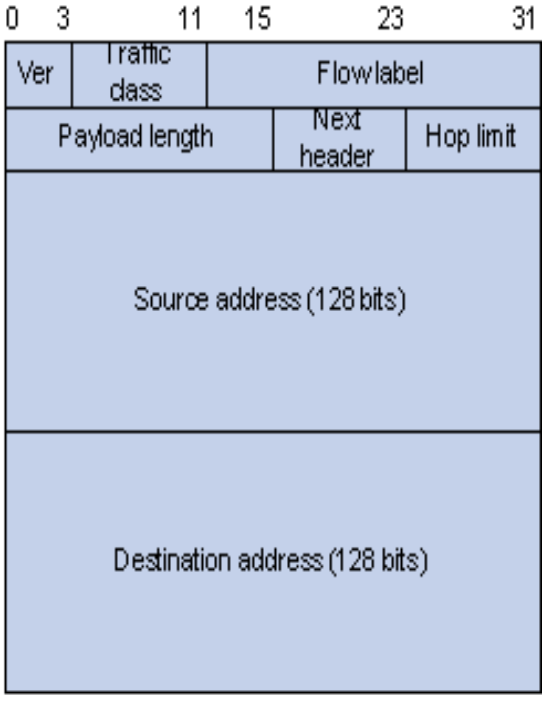
IPv4 addresses are 32 bits, with ” . ”.The IP address is divided into four sections, such as: 192.168.0.1. While IPv6 addresses are 128 bits, they use the” : ” to into divide into eight segments,such as: 123E:0102:1B2D:0000:0000:11CE:CBA3.

To simplify the notation, The in front 0 can be omitted, the number of consective 0 can be marked as " : ", but only once.For example: 123F:0108:1A1D:0000:0000:010C:2045:CBA6 can be abbreviated as: 123F:108::010C:2045:CBA6.

Differently from IPv4, IPv6 uses the prefix to indicate the addresses space. For instance, 124F:0107:1A1C: /48, that means the prefix 48 bit is the address space. Two of 80 powers of subsequent addresses can be assigned to the network host. Here are some of the common IP addresses???, :::/128 isthe same as 0:0:0:0:0:0:0:0, the source address can not be used as the destination address andcan not be assigned to a real network interface as well. ::1/128, the same as 0:0:0:0:0:0:0:1, it is an equivalent to the local host in IPv4 (127.0.0.1). Globally aggregated addresses are allocated by IANA and ISP according to regions. Figures5 and 6 show the differences between IPv4 and IPv6 addresses.



IPv4 header



Basic IPv6 header

Figure 5. Comparison of IPv4 and IPv6 header

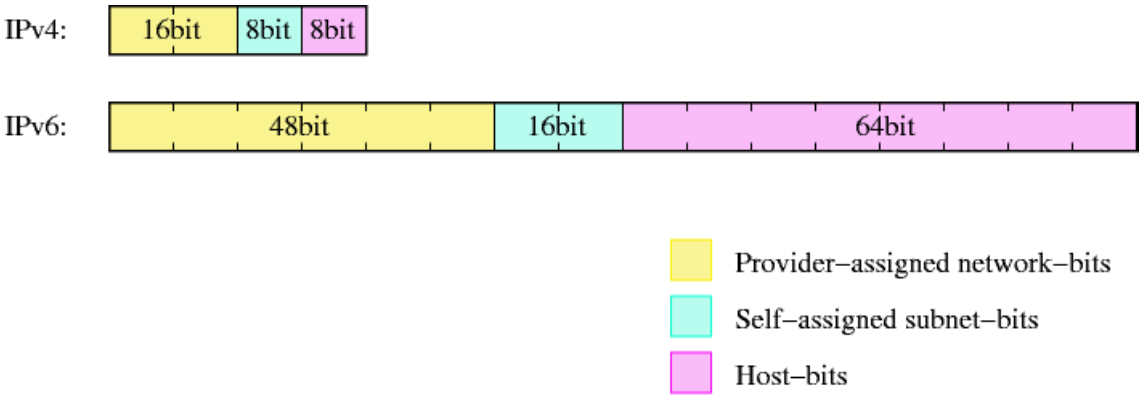


Figure 6. Comparison of IPv4 and IPv6 headers

3.1.3 IPv6 addressing

We know that IPv6 has an address length of 128 bits. So why should we expand the address space so much compared to IPv4. There are two main reasons: firstly. the expansion of addresses will be available to reflect the internet topology which is subdivided into a hierarchy of routing domains; secondly, we can map the network adapter by expansion addresses. IPv6 provides an inner function that can resolve the address at the network interface layer with automatic configuration. An IPv6 unicast address has two parts, one is containing the prefix andthe other contains the interface indentifier. IPv6 addresses can be separated into two types as well, unicast addresses

and multicast addresses. The unicast addresses are generally used for a single interface indentifer, sent to the unicast address of the packet and then passed to the interface indentified. Unicast and multicast address areas are differentiated by the value of the high-order octet, a muticast address octet sequence is the FF. Comparedwith other value unicast address, there are three types of unicast addresses, link local address, the sit local address and global IPv6 unicast address. [11]

The link-local address is generally used in a link between the various nodes, for automatic address configuration, neighbour discovery and no-router-provided situations. It is mainly used at the initial processes or does not havea broader range of address used before. Sit local addresses are generally used for addressing which does not need global prefix. A global IPv6 unicast address can be used in the Internet while the multicast address broadcast address is used to replace IPV4.

3.1.4 The features of IPv6

In a sense, IPv4 has achieved the dialogue between human and machine, but IPv6 expands the dialogue between anything. It is not only the service of humanity, but also for many other equipment services. Therefore, IPv6 is conducive to the sustained and long-term development of the Internet. Compared with IPv4, IPv6 has the following characteristics:

(1) The IPv6 address length is 128 bits; address space is increased 2^{96} times.

(2) Flexible IP packet header format. The expansion of fixed format using a series of headings replaced IPv4 options in variable-length fields.

(3) IPv6 has simplified the format of the message headerfaster message forwardingand higher throughput.

(4) IPv6 has improved security and authentication and privacy are key features.

(5) It supports more types of services.

(6) With capability of evolution, it adapts to future technology

3.2 IPv6 network security

3.2.1 Exploration for IPv6 network security

In the 21st century, computers and networks are already inseparable in our daily life. The network has brought us convenience, but it also brings many novel problems, one of which is the large number of network attacks.

To solve the security issueint next generation IPv6 network, we still have a way to go, but the good news is that in the present situation, the various agencies and researchers have a certain consensus while facing the security challenges. The improvements are mainly about increasing the scalability, improving performance, enhancing mobility and reinforcing security.

3.2.2 Security improvements in the IPv6 network

As IPv6 was proposed to solve the problems and deficiencies of IPv4, it also made improvements in many aspects, such as routing and auto-configuration. After a long

period of coexistence with IPv4, IPv6 will eventually completely take the dominant position in the Internet. Comparing IPv4 and IPv6, IPv6 has these advantages: simplified and flexible extension header; hierarchical address structure; plug and play network approach; network layer authentication and encryption; service quaility improvement and better support for mobile communications. Thus, IPv6 has the following significant advantages.

3.3Transitional Technologies

(1) Tunnel technology

Tunnel technology is proposed based on the situation that IPv4 is still in dominant position, but IPv6 has to be implemented for the furture. The process of tunnel technology is: firstly all IPv6 packet are encapsulated as the IPv4 due to the current devices on network can only deal with IPv4 packets. Therefore, the packaged data can be sent to the specified node.After decapsulation, we finally obtain the IPv6 packet. If the sender and the receivers are both IPv6 nodes, then encapsulation and decapsulation are nessessary, but if only one nodes are IPv6 node, then only one encapsulation or decapsulation is needed. This technique has the advantage of lower requirements on the network routers and other equipment, and easing transmission. At this phase, it is a relatively smooth transition technology.[12]

(2) Dual-stack technology

Dual-stack technology is designed for the current IPv4 nodes, a temporary transitional technology for coexistence with IPv4 and IPv6. The main advantage of this technique is that by using dual-stack technology, regardless of the data packets being IPv4 or IPv6, the transmition process proceeds smoothly. This technique is easier to achieve in software, but hardware requirements are relatively much higher, so the sender and receiver need to be supported by dual-stack at the same time.Thus, there are some difficulties in the implemention of this technology.[12]

(3) Conversion Technolgoy

Conversion technology is currently developing a transition technology between IPv4 to IPv6, however, the general conversion technology can only achieve IPv6 to IPv6 or IPv4 to IPv4. Protocol conversion techniques are more complicated. In addition to the other limitations , conversion technology also faces two problems, how to authenticate and how to encrypt in the coexisting network. These technology requirements for hardware is a challenge, as well.

3.4 ESP encapsulation protocol

As we know, IPv6 network security has been implemented mainly through three aspects: security protocol, network security, and hardware encryption. IPv6 network security mechanisms can be expressed as the following areas compared with IPv4:

(1) All the header information and authentications have been encapsulated, located in the extension header in IPv6, whereas in IPv4, authentications and security information are independent of the IPv4 protocol stack, this guarantees

the implementation of IPv6 network security authentication and encryption package.

(2) Using standard IP authentication and some other security mechanisms. Because of the address resolution in Internet Control Message Protocol (ICMP), coupling is smaller between the medium than the Address Resolution Protocol(ARP). Therefore, including the standard IP authentication and some of the securtiy mechanisms can be widely used among the IPv6 network.

(3) TheIPv6 protocol itself has a relatively good protection from securtiy risks. For example: A link on multiple interfaces simultaneously launches a neighbor request message and sends the link congestion caused by the hidden dangers. IPv6 uses the randomizationmethod to reduce the delay of sending the link congestion in a certain range, it also reduces the competition possiblities on the number of nodes, at the same time with one address.

(4) Retained effectiveness of other security mechanisms in IPv6. Net address Translation - Protocol Translation can provide the same protection as in NAT; based on Virtual Private LAN Segment and Virtual Private Wire Service Tunnel Technology and Virtual Private Network Technology in IPv6.

3.4.1 Security implementation

By considering the current network environment, artificial configuration of key management can be used, but also taking into account the future technology and the expansion of large-scale security network, the interface of key exchanges have been reserved.

The various encryption algorithms of Authentication Header(AH) and Encapsulating Security Payload(ESP) ensure the security at protocol layer. In the Xuzhi Kun study of the ESP routing protocol[7], AH authentication IPv6 neighbor discovery and stateless address configuration been used. DES-BC, 3DES-BC and Null algorithms are implemented for ESP encapsulation. HMAC_MD5_96, MAC_SHA_1_96 authenticated encryptions algorithms are used for AH certification.

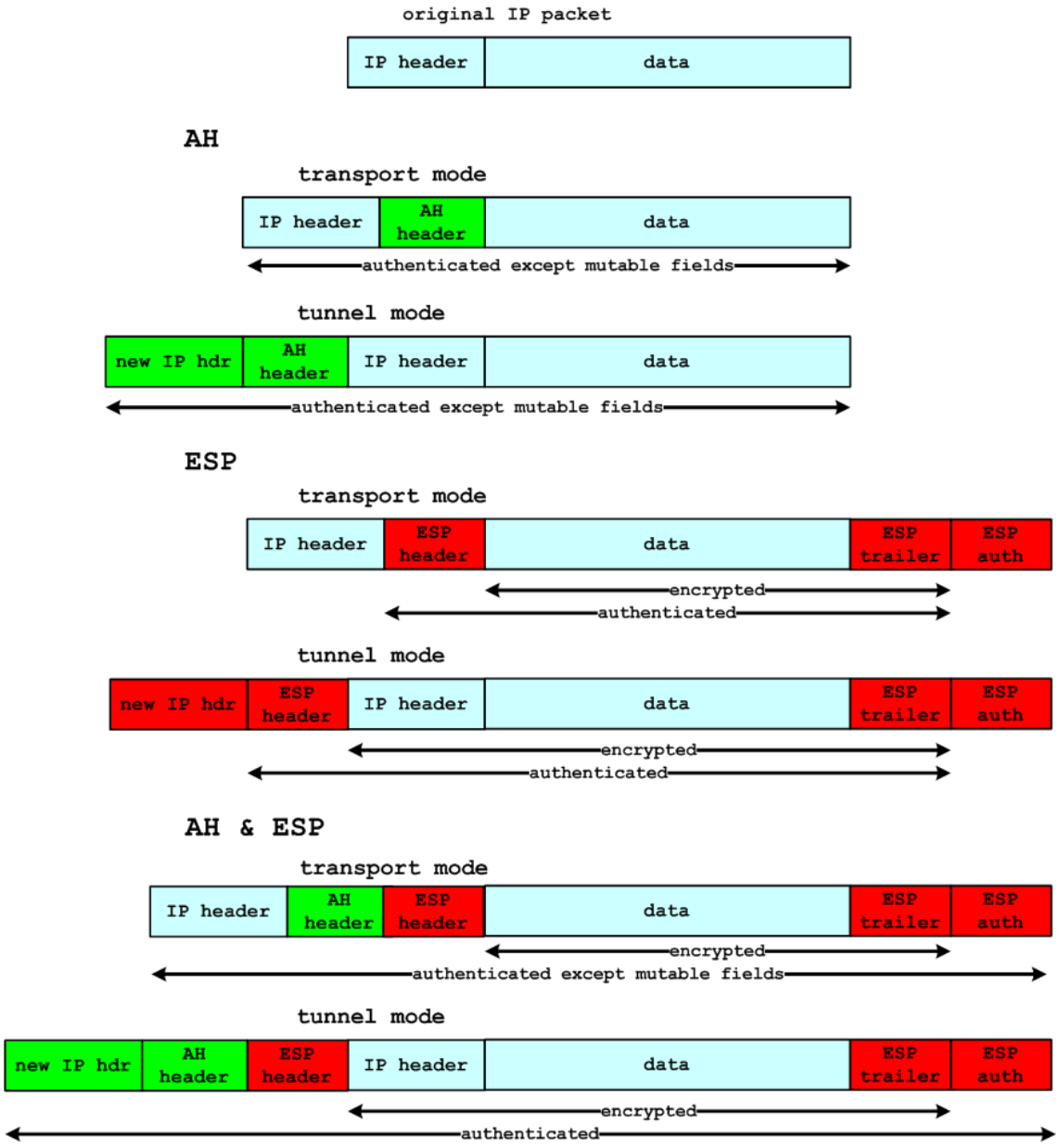


Figure 7. *Authentication Header and Encapsulating Security Payload*

The IPv6 router system authenticates the AH by takinginto account the path of MTU, neighbor discovery and stateless address auto configuration. In order to ensure the security of routing protocol packets, AH or ESP authenticaiton would be used. The basic senario is shown in Figure 8.

The User icon management module can be flexibly configured, the router can have multiple modes add to the packets Dense and certification,such as: port of destination and source, address of destination, and source.

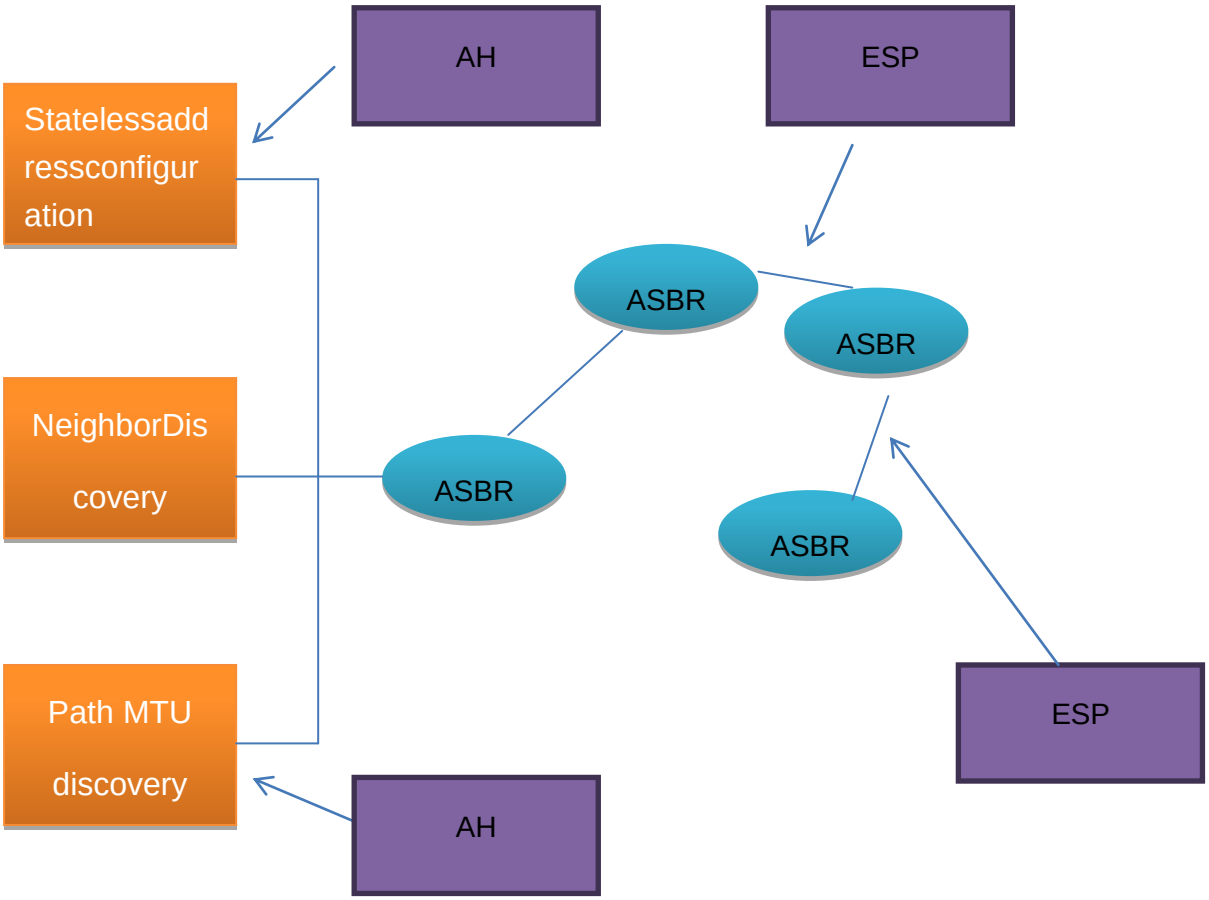


Figure 8. ESP routing protocol study

3.4.2 Network security implementation

Transmission mode and IPD and the application of various combinations of the tunnellingcan guarantee the security of all layers in network. Combinations of tunnelling include: building a secure tunnel through the security VPN, internal network security, end-to-end security guarantees, to achieve different security levels through the nesting tunnel. The IPsec working processis shown in Figure 9.

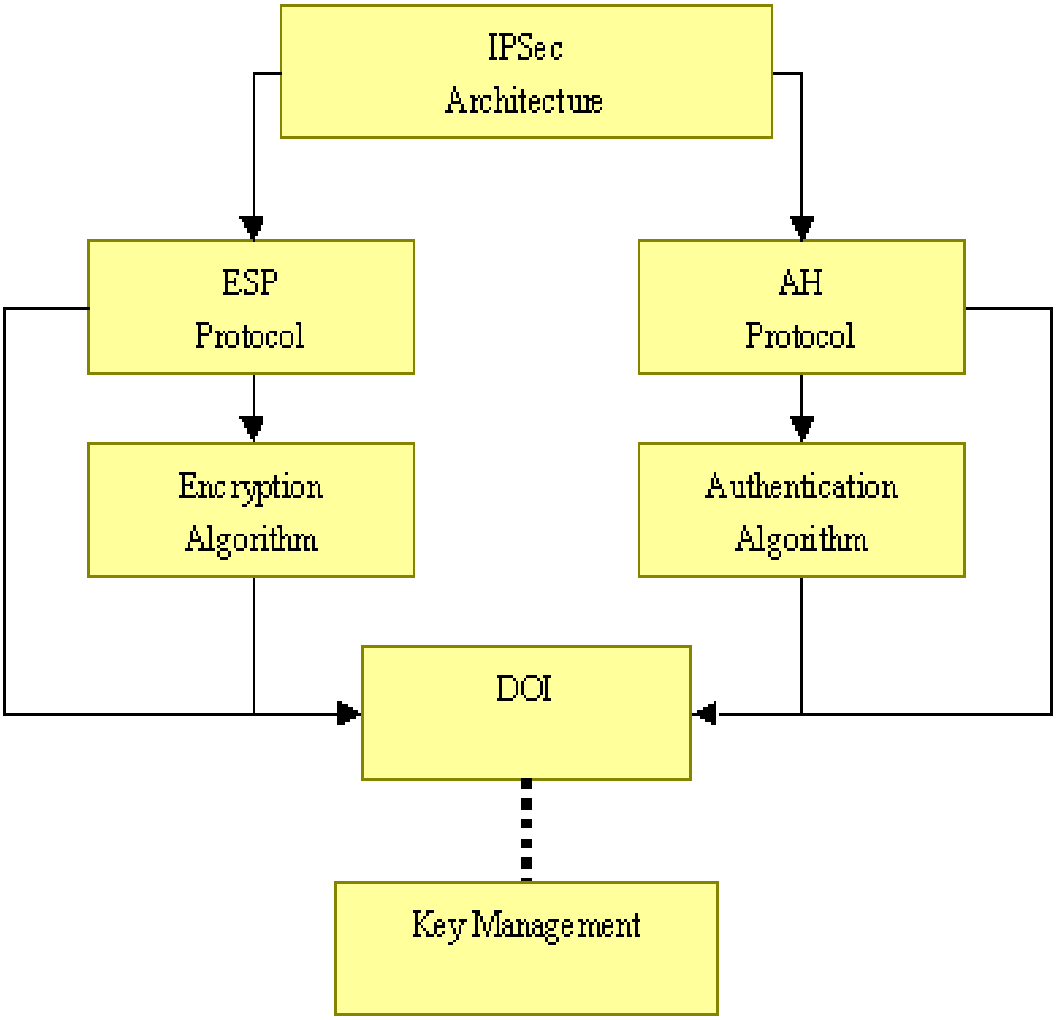


Figure 9. IPsec working processing

(1) VPN secure tunnel using IPsec

The scenario was first made by YuanDa using the most common way to set up a secure network- router secure tunnel established between IPsec.[8] In order to meet the requirements of forwarding performance, the experiment used a dedicated encryption card. An IPsec secure tunnel had been established. The end point and start point are actualy a router as an IPsec gateway[8]. Figure 10 illustrates this experiment.

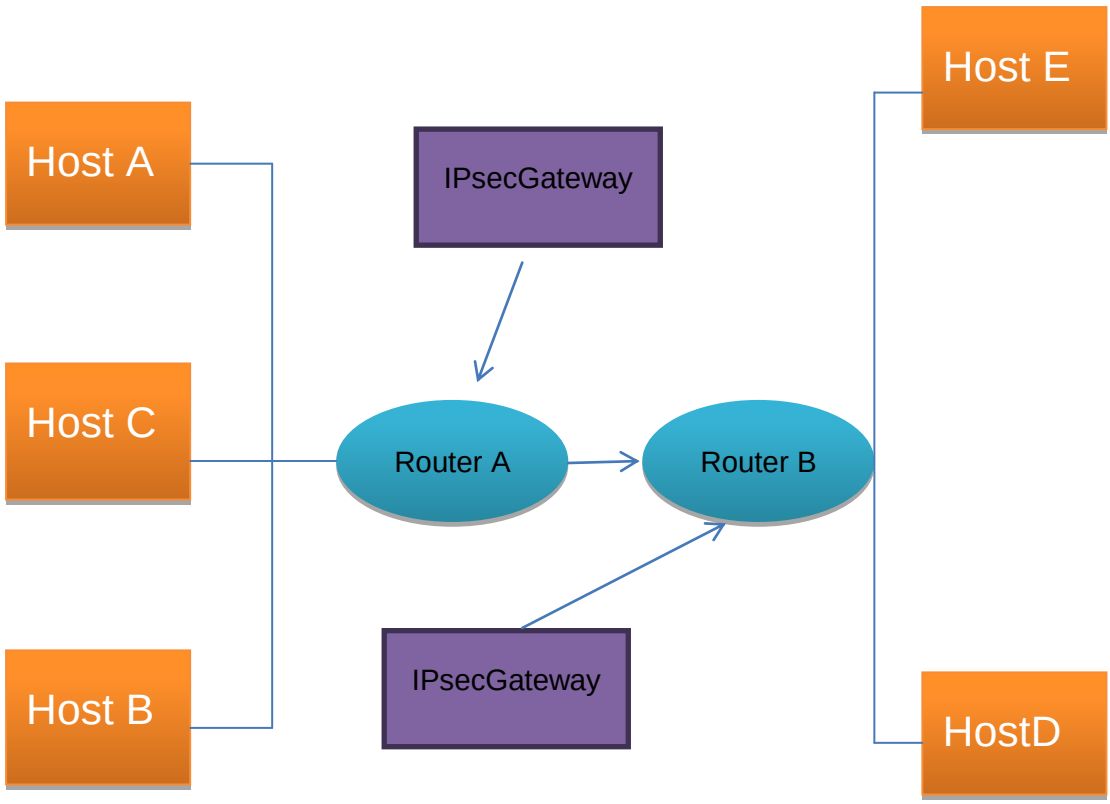


Figure 10. VPN secure tunnel using IPsec study

(2) Internal network security

IPv6 extension header IPsec cannot be analytically processed at the intermediate routers but it can be analyzed by the destination node. Therefore,by configuring the gatways, IPsec can be garanteed while the internal host communicates with external hosts. The IPsec gateway can be achieved by the extended header, option headers of hops and application layer gateway technologies.The IPSec tunnel can also complete this task, but the first method ismore flexible and ensures a more comprehensive security internal network . Figure 11illustrates this complex approach.[13]

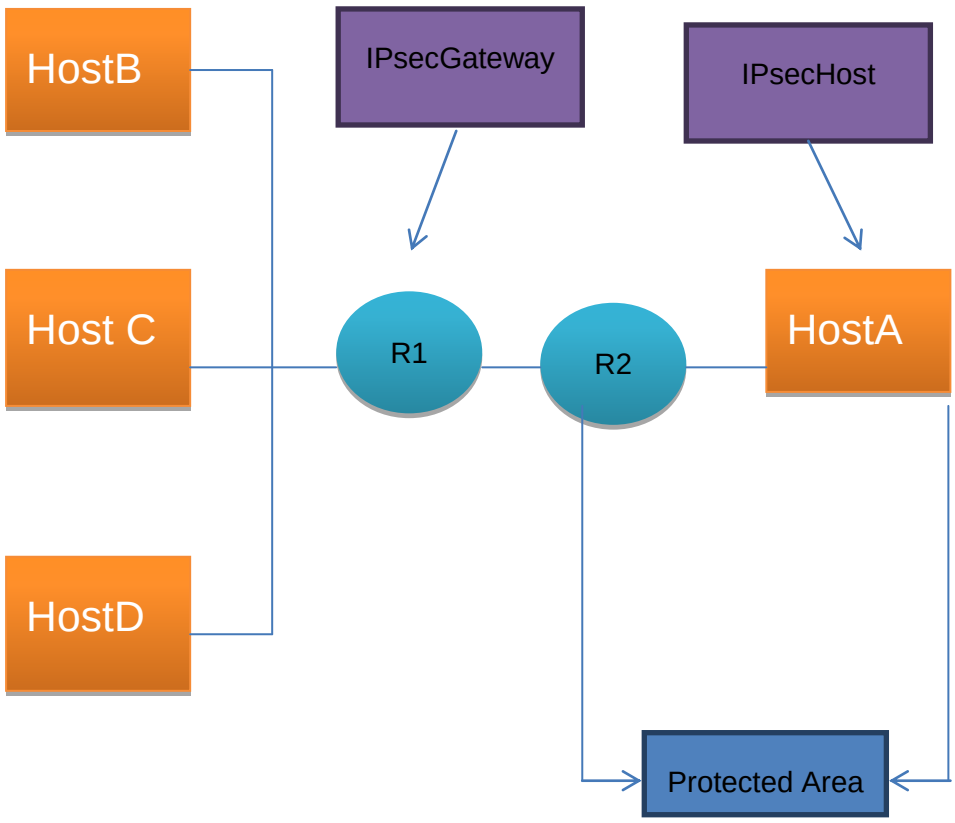


Figure 11. Internal network security

(3) End-to-end network security

Compared with the other ways, end-to-end network security can be said to be more convenient.As shown in Figure 3.5, the middle router completes the work of passing through the IPsec extension header packet in IPv6, encapsulating the end-to-end packets. The end-to-end network security is assured by the encapsulation on the end host through the middle routers.

(4) Different level of network security by nesting tunnel technology

We know that in order to obtain multiple security protection, we can implement it through the tunnel. The author of this thesis configured IPsec for hostC, and put it through the secure tunnel access to the router, RouterA, for the IPsec gateway router configuration. At this time, the internal security of the tunnel has formed the isolation of internal network. The router, RouterB, as the end point of the tunnel has stripped encapsulation of the package coming from the outside network, the tunnel endpoint as an internal router RouterB connects hostC to hostD.

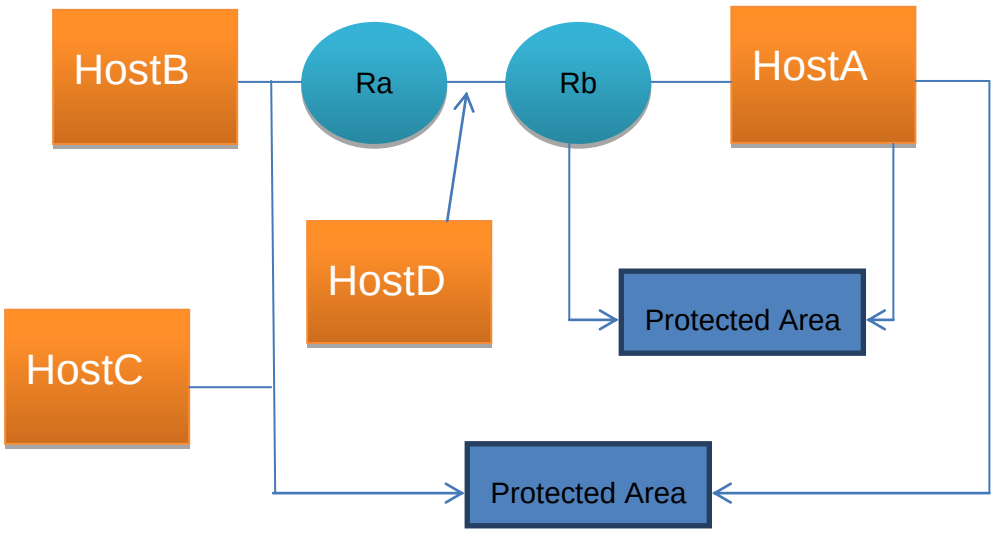


Figure 11. Different level of network security by nesting tunell technology

3.4.3 Ensuring high-performance forwarding

IPv6 will inevitably reduce the router's forwarding performance and processing performance when a large number of IPsec tunnels has been implemented to secure the network. To eliminate the similar effect, ASIC has been used for encryption processing. The encryption and forwarding can also be completed by the network processor. Firstly, the encryption unit interface board mainly contains logic devices and a securtiy processor, used for network interface data encryption and forwarding. In the encryption unit interface board, the security processor can complete IPsec functions,such as data encyption standard support, advanced encryption algorithm, River Shainir Adleman signture, data encryption, decryption, authentication, digital signature, Secure Hash Algorithm and Message Digest Algorithm hash algorithm.

Generally, the IPsec encryption speed is more than 200Mbit/S, while the signature speed is more than 60 1/S.

3.4.4 IPSec and firewall

Although both IPsec and firewallscan effectively ensure network security, the essential point of IPsec is tomaximize the hidden contents of the packet on the intermediate nodes while the firewall filtering model requires the upper layer protocol and port based packet filtering. Therefore, IPsec is not a substitute for firewall, similarly, the firewall cannot replace IPsec either. The network will be more secure if we can make a proper combination of these two technologies.

4 IPv6 security policies

4.1 Firewall filtering rules

IPSec for this problem can be solved well. The firewall does not drop the IPsec framework. This is the easiest combination of firewall and IPsec. The firewall only detects the entrance of the destination address packets which contains the header of AH or ESP, but it does not continue to do the following processes. These are the firewall filtering rules for a simplified security structure.

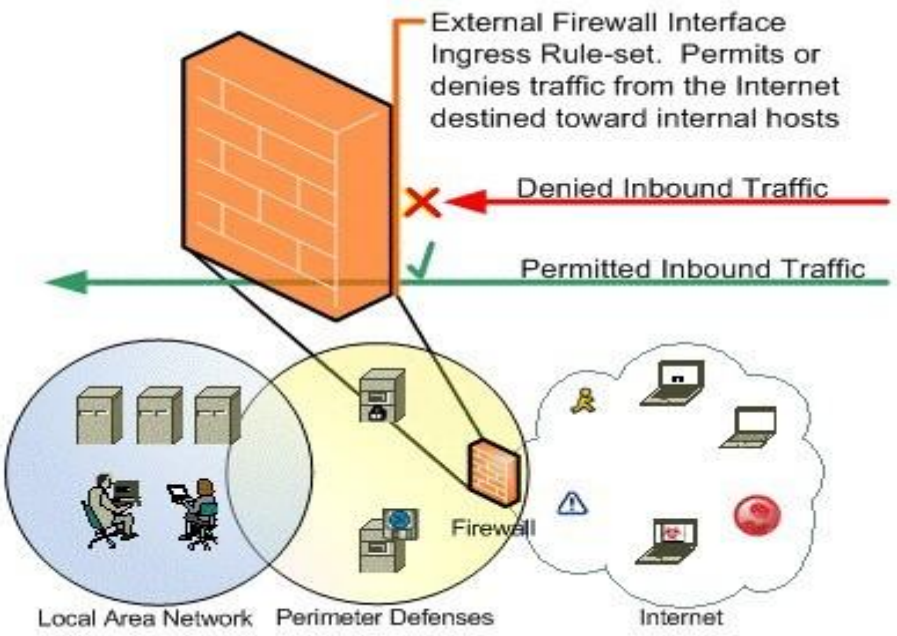


Figure 12. An example of firewall ingress filter

This design is very simple, but there are more disadvantages. Those disadvantages are summarized asfollows:

(1) The host in local area network only verifies the authenticity of the packet. As the forged packets are dropped. the entire local area network security also depends on the security of the destination host.

(2) If we do not use strong key data packets in the communication process, this will result in the firewall not being able to decidewhether communication is on a powerful key or anunsafe key. In this case the informationsecuritycan be guaranted even under the application of the IPsec protocol framework.

(3) There are two situations in network traffic: the first one is encrypted by ESP, the firewall can not obtain TCP/UDP port information; the second situation is when the firewall fundamentally fails to obtain IP address information which is more much worse than the first situation under the tunnel communication mode. In this way, hosts would be attacked by hacker within the ESP tunnel mode.

4.2 The firewall system of the screened gateway host

Screening the host gateway firewall system is designed by configuring a packet filtering router and a base station in the local network subnet host between external networks.

In this scenario, the local network subnet host is configured on a base station host, then apacket filtering router is placed between the host and external network. The packet filtering principle is: only the base station can be connected by the external host, meanwhile all other traffic is denied in the internal LAN subnet.

The base station host completes the packet authentication, decryption and filtering as the only external access interface. These features reduce the work of the packet filtering router, only explicit part informations are filtered under this kind of packet filtering routers. The decrypted messages filtering is performed by the base station host.

5 Conclusion and future work

Thethesis compared the advantages and differences between tunnel protocols, dual stack protocols and protocol conversion at apects of IPV6 network security, described the next generation Internet with its unparalleled and great advantages, and described a wide range usage of IPv6. The researchon IPv6 technology has been made by comparing three different transition functions, illustrating the improvements on network security in IPv6 network which are established based on the ESP encapsulation protocol. By learning the network security structure, an initial possible solution has been made for the next-generation Internet.IPv6 technologies protect the protocol security, network security and hardware securtiy by As the next generation Internet is still under construction, this thesis on the use of IPv6 protocol for the next generation Internet research remains at the literature stage, the next step is to use the basis of the experiment and continue the research efforts for the smooth transition and security aspects of IPv6.

REFERENCES

[1] Zhang Min, XuYuejin, Network Security Test Tutorials, Tsinghua University Press, 2007.

[2] Wu Shizhong, Ma Fang, Network Information Security, Machinery Industry Press, 2003.

[3] Yao Qifu. Network Security Technology. Zhejiang University Press, 2006.

[4] Lu Chi classes. Network Security Technology. Shanxi: The Northern Arts Publishing House, 2006.

[5] Xuzhi Kun, Wang Wei, GuoTiansen, Yang Jilong, Network Penetration Technology, 2005.

[6] Wu Xinhua, DizhangSen, Hacker Attack Cheats Exposed, Tsinghua University Press, 2006,

[7] Zhang Yongmei. On the Intrusion Detection in Network Security Role. Sichuan Institute of Technology, 2006,

[8] YuanDa Cao. Intrusionand DetectionTechnology. Beijing: People's Posts and Telecommunications Press, 2007.

[9] T.Stibor, J.Timmis, and C.Eekert. Appropriateness of Negative Selection Defined over Hamming Network Intrusion Detection System Evolution, 2005.

[10] Du Guangyu, Huang Shu, and Li Qi. Network Intrusion Detection Artificial Immune Dynamic "self" definition model. Computer Engineering, 2006.

[11] Anup K. Ghosh, Learning program behavior profiles for intrusion detection, 1st conference on Workshop on Intrusion Detection, 2000.

[12]Sean Convery, Darrin Miller. IPv6 and IPv4 Threat comparison and best practice evaluation. Cisco Systems, 2004,

[13] Joseph Davies, Understanding IPv6, Cisco Systems 2002.