MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
Boris Grinchenko Kiev University

BURIACHOK V.L., DURAVKIN Ie.V.,
LUKOVA-CHUYKO N.V., SKLADANNIY P.M.

METHODS OF INFORMATION PROTECTION IN TELECOMMUNICATION SYSTEMS

TUTORIAL

Approved by the Ministry of Education and Science of Ukraine
as a textbook for university students

Kiev 2019

BKK 39.973.26-018.2(4Укр)я73
B 91
UDK 004.7.056.5(477)(075.8)

Griffin provided the Ministry of Education and Science of Ukraine
according to the letter №1 / 11-8664 from 06.22.2015 p.

Recommended Academic Council
Boris Grinchenko Kiev University
for publishing and educational use
(from 25.04. 2019)

Atops:

V.L.BURIACHOK, doctor of technical sciences, professor;
Ie.V.DURAVKIN, doctor of technical sciences, associate professor;
N.V. LUKOVA-CHUYKO, doctor of technical sciences., associate professor;
P.M.SKLADANNIY, Senior lecturer

Rezenezent:

doctor of technical sciences, professor I.V. Ryban;
doctor of technical sciences, professor U.V. Kravchenko

B 91

Buriachok V.L. Methods of information protection in telecommunication systems: [manual]. / V.L.Buriachok, Ie.V.Duravkin, N.V. Lukova-Chuyko, P.M.Skladanniy / – К.:KUBG, 2019. – 74 с.

The manual covers the basics of information security in ITS. Examples of practical implementation of modern methods and means of providing security in local networks are given. Each example is designed as a laboratory work. Laboratory work contains basic information about methods of information protection in local networks, methodical instructions on the procedure for its implementation and requirements for the formulation of conclusions.

The material is aimed at a wide range of researchers and pedagogical staff who deal with information security and ITS safety issues, as well as graduate students and undergraduates of higher education institutions who study the specialty "Information and Communication Systems Security" in specialty 125 "Cybersecurity" in the field of knowledge " Information Technology".

CONTENT

INTRODUCTION

The purpose of discipline «Technologies for discovering vulnerabilities of web resources» is the formation and acquisition of basic knowledge on the theory and practice of solving problems of protection of information resources in current and future ITS. Studying discipline «Technologies for discovering vulnerabilities of web resources» based on knowledge obtained during the course of such subjects as «Fundamentals of telecommunication systems», «Local networks», «Methods of identification of objects and users», «Fundamentals cryptographic protection of information».

Contents of of laboratory work is directly related to the material of lectures and practical training of the discipline, which turns goal, general theoretical and technological principles of the system of protection of information resources in current and future ITS and requirements of new concepts about the prospects for further improvement of existing facilities software data protection.

Laboratory work is carried out using real telecommunication equipment placed in the laboratory of information security (State University of Telecommunications, SUT), such as routers (DI-804HV, DSL-G804V), switches (DES-3200-10, DGS-3200-10) and firewalls (DFL-810) produced by D-Link.

Students should consolidate the knowledge acquired in lectures and workshops, to acquire the necessary practical skills and be able to exercise informed choice means or protocols of information security in solving problems associated with limited access to network resources.

1. SECURITY TOOLS ANALYSIS IN LOCAL AREA NETWORKS (ACCESS CONTROL LIST)

1.1 Purpose of work

Configuration of the network fragment using network equipment. Setting access control lists on a switch. As filtering criteria used MAC- addresses and IP-addresses.

1.2 Background. Brief description of the safety provisions in local area networks

1.2.1 Access control lists (ACL)

Access Control List are the means of filtering data streams without loss of performance, as checking the contents of data packets is performed at the hardware level. Administrator can restrict types of applications approved for use on the network, control user access to the network and identifies the device to which they can be connect using the filtering of data streams. ACL also can be used to determine the policies QoS, by classifying traffic and redefining its priority.

ACLs are composed of Access Profile and Rules. Access profiles define the types of filtering criteria which must be verified in a data packet (MAC-address, IP-address, port number, VLAN, etc.), the rules specified directly the values of their parameters. Each profile may consist of a plurality of rules.

1.3 Methodical instructions and work order

Laboratory model description

A fragment of a telecommunication network consists of a switch, which is connected to 3 workstations and Internet gateway (see. Table 1.1).

Table 1.1

Equipment (on one work place):	
Switch DES-3200-10 or DGS-3200-10	1 unit
Work station	3 unit
Console cable	1 unit
Ethernet cable	3 unit
Internet gateway	1 unit

1.3.1 Configuration users access restriction to the Internet than based on MAC-address

Scheme of laboratory model is shown in Figure 1.1.

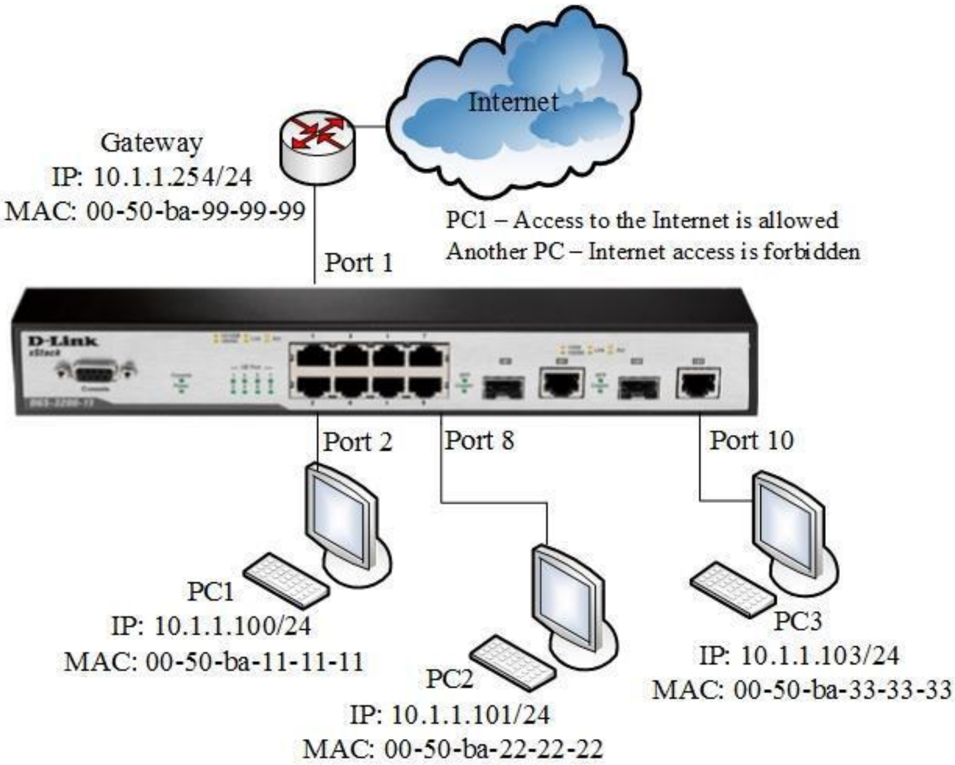


Figure 1.1 – Network model for laboratory work

Task

Allow PC1 and PC2 users Internet access; the other users are deny. Users identified by MAC addresses of their computers.

Rules:

Rule 1:

If the destination MAC address = Internet gateway MAC address and sourse MAC address = PC1 MAC address - permit;

If the destination MAC address = Internet gateway MAC address and sourse MAC address = PC2 MAC address - permit;

Rule 2:

If the destination MAC address = Internet gateway MAC address - deny;

Rule 3:

Otherwise, the default to allow access all nodes.

Before performing the tasks necessary to reset the switch to factory settings. Using command:

```
reset config
```

Before performing the laboratory exercises necessary to replace these commands in the MAC address to the real MAC address of the workstation and the Internet gateway.

Rule 1

Create an access profile 10:

```
create access_profile ethernet source_mac FF-FF-FF-FF-FF-FF destination_mac FF-FF-FF-FF-FF-FF profile_id 10
```

Create a rule for profile 10 that allowing access to PC1 which connected to port 2, to Internet:

```
config access_profile profile_id 10 add access_id 11 ethernet source_mac 00-50-ba-11-11-11 destination_mac 00-50-ba-99-99-99 port 2 permit
```

Create a rule for profile 10 that allowing access to PC1 which connected to port 8, to Internet:

```
config access_profile profile_id 10 add access_id 12 ethernet source_mac 00-50-ba-22-22-22 destination_mac 00-50-ba-99-99-99 port 8 permit
```

Rule 2

Create access profile 20:

```
create access_profile ethernet destination_mac FF-FF-FF-FF-FF-FF profile_id 20
```

Create a rule for profile 20, that deny access to other users on the Internet:

```
config access_profile profile_id 20 add access_id 21
ethernet destination_mac 00-50-ba-99-99-99 port 1-10 deny
```

Note: The new rule would prohibit passing frames containing the destination MAC address equal to the MAC address of an Internet gateway to all switch ports. If this rule must be applied to one of the ports in the configuration indicates a specific port that is connected to the station, the traffic that you want to block.

Rule 3

Allow all the rest:

Execute by default

Check the created profiles ACL: show access_profile

1. Connect the station PC1 and PC2, as shown in Figure 1.1. Test the connection to the Internet gateway using command ping.

2. Connect another workstation or connect PC1 and PC2 to other switch ports and then try to access the Internet gateway.

3. Remove the rule from the access profile (for example, to disable the Internet from PC2):

```
config access_profile profile_id 10 delete access_id 12
```

4. Remove ACL the profile (for example, allows Internet access stations PC1 and PC2):

```
delete access_profile profile_id 10
```

1.3.2 Configuration of user's access restriction to the Internet by IP-addresses

Scheme laboratory model is shown in Figure 1.2.

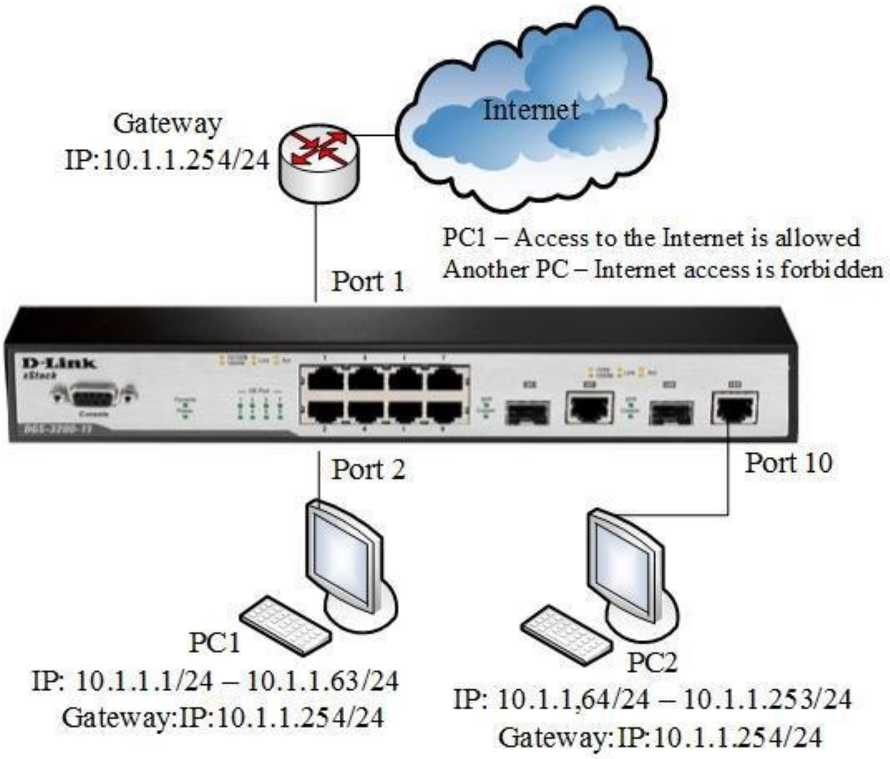

Gateway
IP:10.1.1.254/24
Internet
PC1 – Access to the Internet is allowed
Another PC – Internet access is forbidden
Port 1
D-Link
Port 2
Port 10
PC1
IP: 10.1.1.1/24 – 10.1.1.63/24
Gateway:IP:10.1.1.254/24
PC2
IP: 10.1.1,64/24 – 10.1.1.253/24
Gateway:IP:10.1.1.254/24

Figure 1.2 – Network model for laboratory work

Task

Permit the Internet access to users with IP-addresses from 10.1.1.1/24 to 10.1.1.63/24. Other users of the network 10.1.1.0/24, with addresses outside the permitted range, access to the Internet is deny.

Rules:

Rule 1:

If the source IP-address = IP-addresses from the range: 10.1.1.1 - 10.1.1.63 (subnet 10.1.1.1/26) - permit;

Rule 2:

If destination MAC address= The Internet gateway MAC address - deny;

Rule 3:

Otherwise, default allow access by everyone nodes.

Before executing the task, remove the last profile from previous task:

delete access_profile profile_id 20

Make sure that no more profiles on the switch: show access_profile

Rule 1.

Create access profile number 10, allowing access to the subnet 10.1.1.0/26 (nodes 1 to 63):

create access_profile ip source_ip_mask 255.255.255.192 profile_id 10

Create a rule for access profile 10:

config access_profile profile_id 10 add access_id 11 ip source_ip 10.1.1.0 port 1-10 permit

Note: The new rule permits traffic to pass IP-subnet 10.1.1.0/26 to all switch ports. If this rule must be applied to one of the ports in the configuration indicates a specific port that is connected to the station, whose traffic should be permitted.

Rule 2

Create access profile 40:

create access_profile ethernet destination_mac FF-FF-FF-FF-FF-FF profile_id 40

When the work is necessary to replace the specified MAC address as a team on the real MAC address of the Internet gateway.

1. Connect the equipment according with the scheme shown in Figure 1.2. Create a rule for access profile 40 that deny other stations connected to the Internet gateway:

config access_profile profile_id 40 add access_id 41 ethernet destination_mac 00-50-ba-99-99-99 port 1-10 deny

Rule 3

Permit all another:

Execute by default

Check the created profiles: show access_profile

2. Connect workstations PC1 (address in the range 10.1.1.1-63/24) and PC2 (address in the range 10.1.1.64-253/24) to the switch. Test the connection to the ping Internet gateway

ping 10.1.1.254

3. Remove ACL profile (for example, profile 10).

delete access_profile profile_id 10

Test the connection to the Internet gateway using ping command ping 10.1.1.254

1.4 Report content

Report on the implementation of laboratory work should include the following items:

1. Subject and purpose of the laboratory work

2. Block diagram of the network with the designation of ports, IP address, network mask interface of workstation and switch.

3. Order of the laboratory work performance (sequence of input commands with the relevant explanations). Graphic results of the commands.

4. Analysis and conclusions on the implementation of laboratory work.

2 SECURITY TOOLS ANALYSIS IN LOCAL AREA NETWORKS (PORT SECURITY, IP-MAC BILDING)

2.1 Purpose of work

To obtain experience of management nodes connection to switch ports. To investigate the principles of functions Port Security and IP-MAC-Port Binding.

2.2 Background. Brief description of the safety provisions in local area networks

2.2.1 Function Port Security

Port Security function allows to adjust any switch port so that network access could be granted only for certain devices. Devices authorized to be connected to a port are defined by their MAC addresses which can be studied dynamically or adjusted manually by a network administrator. Port Security function allows for restricting a number of MAC addresses studied by a port, therefore regulating a number of connected nodes.

Port Security is to protect the switch from the malicious MAC Address Attack by limiting the maximum number of MAC addresses that can be learned on the port. The port with Port Security feature enabled will learn the MAC address dynamically/statically.

There are three modes of operation Port Security functions:

- Permanent;
- Delete on Timeout;
- Delete on Reset.

Port Security feature is useful for building home networks, network providers of Internet and local area networks with high demands on safety, which requires exclusion of unregistered workstations to network services.

2.2.2 IP-MAC-Port Binding function

Function IP-MAC-Port Binding (IMPB) allows you to control access to the network of computers based on their IP- and MAC-addresses as well as the connection port.

The network administrator can create a record («white list»), linking the MAC and IP-addresses of the computers to connect to the ports on the switch. On the basis of these records, in the case of coincidence of all the components, users will get access to the network from their own computers

Function IP-MAC-Port Binding includes three operation modes: ARP mode (default), ACL mode and DHCP Snooping mode.

Administrator should provide the mode of its operation (configurationg IMPB):

- Strict Mode – in this mode, the port is disabled by default;
- Loose Mode – in this mode the default port is opened.

2.3 Methodical instructions and work order

Laboratory model description

A fragment of a telecommunication network consists of a switch, which is connected to 3 workstations and Internet gateway (Table 2.1).

Table 2.1

Equipment (on one work place):	
Switch DES-3200-10 and DGS-3200-10	1 unit
Work station	2 unit
Console cable	1 unit
Ethernet cable	2 unit
Internet gateway	1 unit

2.3.1 Management of number of users connecting to switch ports by restricting the maximum number of studied MAC addresses

Schematic of laboratory model is shown in Figure 2.1.

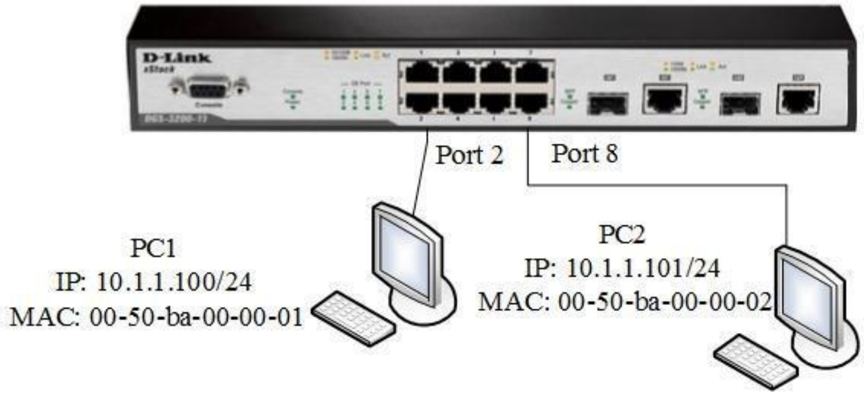


Figure 2.1 – Network model for laboratory work

1. Connect the equipment in accordance with the scheme shown in Figure 2.1 Reset the switch to factory default settings using command:

reset config

Check the information about the settings Port Security: show port_security

Set up the maximum number of learning MAC addresses for all ports equal 1. Activate this feature on all ports

```
config port_security ports all admin_state enable max_learning_addr 1
```

2. Connect PC1 and PC2 to the ports of the switch 2 and 8, respectively. View MAC-addresses, which have become known to ports 2 and 8:

```
show fdb port 2
show fdb port 8
```

To verify compliance with the registered address to the workstation addresses Check the information about the settings, Port Security on the switch ports: show port_security ports 1-10

Set up an entry in the log-file MAC-addresses that connect to the port stations and sending messages SNMP Trap:

```
enable port_security trap_Log
```

Test the accessibility of of nodes using ping command from PC1 to PC2 and vice versa.

3. Connect PC1 to port 8 and PC2 to port 2.

Retest the connection between workstations using ping command. Check the information in the log-file of the switch:

```
show log
```

Save the configuration and reboot the switch: save

reboot

Test the connection between the workstation using ping command.

4. Set to port 2 functions Port Security Mode Permanent and maximum number of investigated addresses of 1:

```
config port_security ports 2 admin_state enable max_learning_addr 1 lock_address_mode Permanent
```

Save the configuration and reboot the switch: save

Reboot

Check the information about the settings, Port Security on the switch ports:

```
show port_security ports 1-10
```

Check whether the information about the MAC-port binding.

5. Clear info about bind between MAC-port to port 22:

```
clear port_security_entry port 2
```

Disable Port Security on port 2 and provide the settings to the default state:

```
config port_security ports 2 admin_state disable
max_learning_addr 1 lock_address_mode DeleteOnReset
```

Look to timer lockout (it corresponds to the lifetime of MAC-address in the switching table):

```
show fdb aging_time
```

You can change the duration of the timer by setting the lifetime of the MAC-address in the switching table (times in seconds):

```
config fdb aging_time 20
```

Change the mode of the function on Port Security Delete on Timeout: config
port_security ports 2 admin_state disable

```
max_learning_addr 1 lock_address_mode DeleteOnTimeout
```

Check the MAC-addresses, which have become known port 2:

```
show fdb port 2
```

Check out the information about the settings, Port Security on the switch ports:

```
show port_security ports 1-10
```

Test the connection between PC1 and PC2 command ping. Check whether the information about the MAC-port binding. Disable Port Security function on ports:

```
config port_security ports 1-10 admin_state disable
```

Disable the entry in the log-file and send SNMP Trap:

```
disable port_security trap_Log
```

Note: *After learning process one can disable dynamic MAC addresses learning when studied addresses are saved in a forwarding table. Therefore, current network configuration will be saved and unauthorized connection of new devices will be impossible. New devices can be added by creating static records in a forwarding table.*

2.3.2 Configuration of port connection protection based on a static MAC addresses table

1. Disconnect the workstation from the switch. Reset the switch to factory settings command:

```
reset system
```

Activate the Port Security on all ports and disable MAC address learning (max_learning_addr parameters set as 0):

```
config port_security ports 1-10 admin_state enable max_learning_addr 0
```

Check the port status: show ports

Check the connection between PC1 and PC2 command ping.

Check the condition of the switching table: show fdb

2. Create a static entry for MAC-address of the workstation connected to ports 2 and 8 in the switching table.

Necessary to replace these commands in the MAC address to the real address of the workstation connected to the switch.

```
create fdb default 00-50-ba-00-00-01 port 2
```

```
create fdb default 00-50-ba-00-00-02 port 8
```

Check by static entries in the switching table:

```
show fdb
```

Check out the information about the Port Security settings on the switch ports:

```
show port_security ports 1-10
```

Check the connection between PC1 and PC2 using command ping.

3. Connect PC1 to port 8 and PC2 to port 2. Repeat the ping testing. Remove existing static entry from the MAC address table on port 2:

```
delete fdb default 00-50-ba-00-00-02 port 2
```

2.3.3 Configuring IP-MAC-Port Binding function in ARP mode

Schematic of laboratory model is shown in Figure 2.2.

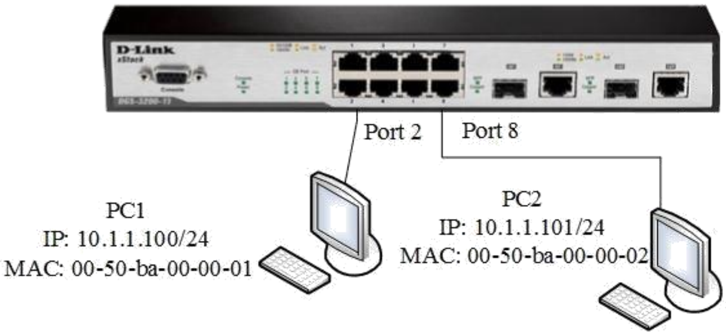


Figure 2.2 – Network model for laboratory work

Reset the switch to factory defaults using command: reset config

Necessary to replace these commands in the MAC address to the real MAC address of the workstation connected to the switch.

Create an account IP-MAC-Port Binding, binding IP-MAC-address of the workstation PC1 with port 2 (the default ARP mode):

create address_binding ip_mac ipaddress 10.1.1.100 mac_address 00-50-ba-00-00-01 ports 2

Create an account IP-MAC-Port Binding, binding IP-MAC-address of the workstation PC2 to port 8:

create address_binding ip_mac ipaddress 10.1.1.101 mac_address 00-50-ba-00-00-02 ports 8

Activate the on ports 2 and 8 (the default port mode "Strict"):

config address_binding ip_mac ports 2,8 state enable

Check the records IP-MAC-Port Binding:

show address_binding ip_mac all

Check the ports on which set of functions and their operation mode:

show address_binding ports

1. Connect the equipment in accordance with the scheme shown in Figure 2.1. Check the availability of connections between workstations ping command:

ping <IP-address>

Set up an entry in the log-file and send messages to SNMP Trap in case of non-ARP-packet IP-MAC binding:

enable address_binding trap_log

2. Connect PC1 to port 8 and PC2 to port 2.

Retest the connection between workstations using ping command. Check locked workstations:

show address_binding blocked all

Check if there are blocked stations in the log-file: show log

3. Remove an address from the list of blocked addresses:

delete address_binding blocked vlan_name System mac_address 00-50-ba-00-00-01

Delete the entry IP-MAC-Port Binding:

delete address_binding ip_mac ipaddress 10.1.1.100 mac_address 00-50-ba-00-00-01

Disable the IP-MAC-Port Binding function on ports 2 and 8:

config address_binding ip_mac ports 2,8 state disable

2.3.4 Configuring IP-MAC-Port Binding function in ACL mode

1. Create an account IP-MAC-Port Binding, binding IP-MAC-address of the station PC1 with port 2:

create address_binding ip_mac ipaddress 10.1.1.100 mac_address 00-50-ba-00-00-01 ports 2

Create an account IP-MAC-Port Binding, binding IP-MAC-address of the station PC2 with port 8:

create address_binding ip_mac ipaddress 10.1.1.101 mac_address 00-50-ba-00-00-02 ports 8

Activate the on ports 2 and 8 (the default port mode Strict), turn on allow_zeroip mode, through which the switch will not block sites that send ARP-packets with source IP-address 0.0.0.0. Set the work function IMPB in ACL mode:

config address_binding ip_mac ports 2,8 state enable allow_zeroip enable mode acl

Check the created records IP-MAC-Port Binding:
show address_binding ip_mac

Check the ports on which set of functions and their operation mode:

show address_binding ports

Check created access profiles ACL:

show access_profile

2. Connect workstations PC1 and PC2 to the switch as shown in Figure 2.2. Check the availability of connections between workstations command ping:

ping <IP-address>

Connect PC1 to port 8 and PC2 to port 2. Repeat the test connection between workstations command ping.

Check locked workstations:

show address_binding blocked all

3. Remove an address from the list of blocked addresses:

delete address_binding blocked vlan_name System mac_address 00-50-ba-00-00-01

Remove all blocked addresses:

delete address_binding blocked all

Delete all note list IP-MAC-Port Binding:

delete address_binding ip_mac ipaddress 10.1.1.100 mac_address 00-50-ba-00-00-01

delete address_binding ip_mac ipaddress 10.1.1.101 mac_address 00-50-ba-00-00-02

Disable the IP-MAC-Port Binding on ports 2 and 8:

config address_binding ip_mac ports 2,8 state disable

Make a conclusion about the work function of IP-MAC-Port Binding mode ACL.

2.4 Contents of report

1. Report on the implementation of laboratory work should include the following items:

2. The theme and purpose of the laboratory work.

3. Block diagram of the network with the designation of ports, IP address, network mask interface of workstation and switch.

4. Order of performance laboratory work (sequence of input commands with the relevant explanations).

5. Graphical results.

6. The analysis and conclusions about laboratory work implemention.

3 ANALYSIS OF 802.1X STANDART (PORT-BASED, MAC-BASED, GUEST VLAN)

3.1 Purpose of work

To study process of configuring a network hardware authentication protocol 802.1X port-based and MAC-based. To obtain experiences of 802.1X Guest VLAN configuration

3.2 Brief overview of 802.1X standard

The IEEE 802.1X protocol describes the use of EAP (Extensible Authentication Protocol) to support authentication via an authentication server and defines the process of data encapsulation EAP transferred between clients (requesting device) and authentication servers. The IEEE 802.1X provides access control and prevents unauthorized devices to connect to the LAN ports on the switch.

The authentication server Remote Authentication in Dial-In User Service (RADIUS) checks the permissions of each client connected to a switch port before allowing access to any of the services provided by the switch or the LAN. Figure 3.1 describes the main function.

In the IEEE 802.1X standard defines three roles that can perform device:

- Client/Supplicant;
- Authenticator;
- Authentication Server.

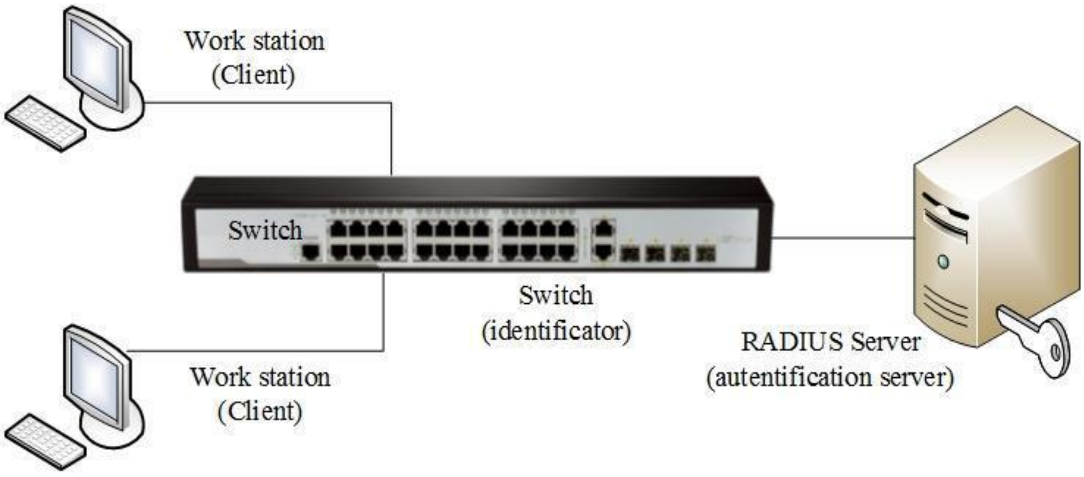


Figure 3.1 – Architecture of IEEE 802.1X standard

In the D-Link switches are supported by two implementations of the 802.1X authentication:

- Port-Based 802.1X;
- MAC-Based 802.1X.

802.1X Guest VLAN function is used to create a guest VLAN with limited rights for users who are not authenticated. When a client connects to a switch port to enable authentication and 802.1X function Guest VLAN, the process of authentication (either locally or remotely using the server RADIUS). In the event that the client is not authenticated, it is placed in the Guest VLAN with limited rights and access.

3.3 Methodical instructions and work order

Laboratory model description

A fragment of a telecommunication network consists of a switch, which is connected to 3 workstations and Radius-сервер (see Table 3.1).

Table 3.1

Equipment (on one work place):	
Switches L3 DES-3200-10 or DGS-3627	2 unit
Switch L2 DES-1005D	1 unit
Work station	3 unit
Console cable	1 unit
Cable Ethernet	5 unit
Radius-server	1 unit

It is necessary that in a laboratory environment was created infrastructure PKI (Public Key Infrastructure) based on Microsoft Windows, Unix and installed Radius server (for example, IAS MS Windows 2003):

Table 3.2

Standard ports of the RADIUS protocol

Application protocol	**Protocol**	**Ports**
Legacy RADIUS	UDP	1645
Legacy RADIUS	UDP	1646
RADIUS Accounting	UDP	1813
RADIUS Authentication	UDP	1812

You must install the client software for 802.1X on the workstation, if it is absent (802.1X client OS Window XP).

3.3.1 Port-Based 802.1X

Schematic of laboratory model is shown in Figure 3.2.

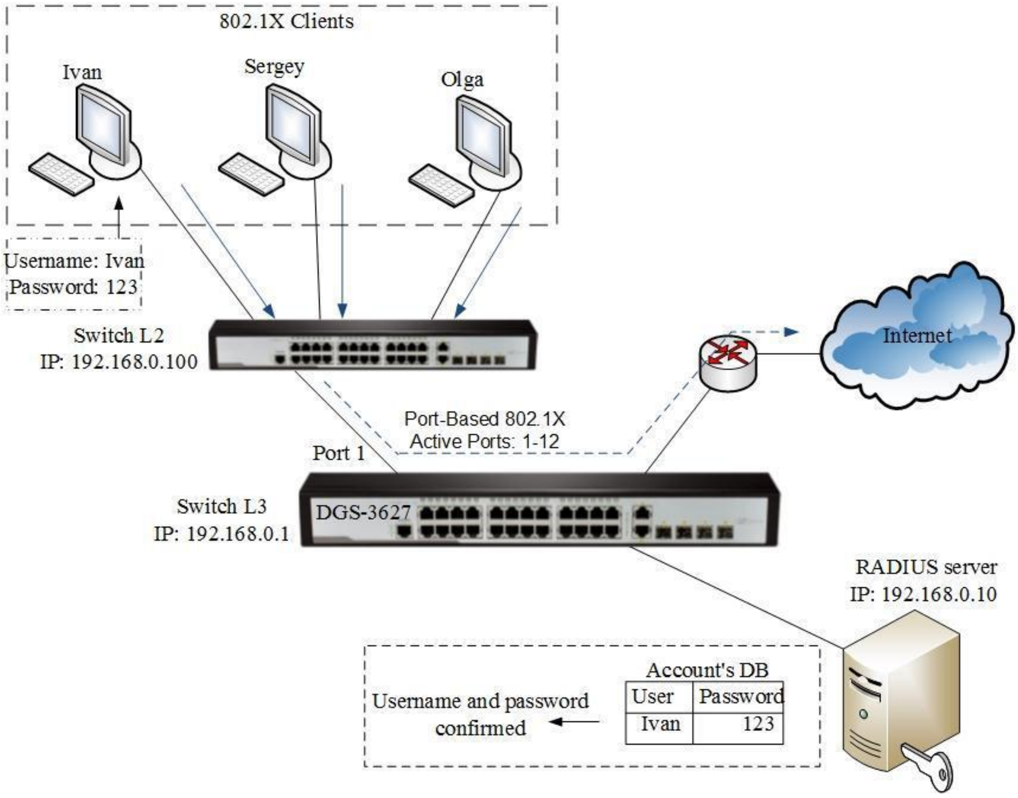


Figure 3.2 – Fragment of network for laboratory work

Task

Configure authentication on the basis of the standard 802.1X Port-Based Before carrying out the laboratory work is necessary to reset the switch to

factory setting using defaults command: reset config

Switch Configuration L3:

Configure user authentication on the RADIUS server config 802.1x auth_protocol radius_eap

Configure the authentication type 802.1X: Port-Based

config 802.1x auth_mode port_based

Any user connected to the port can access the network after the port has been authorized (when using 802.1X port-based authentication)

Configure the ports to which users are connected as authenticators (one should not configure “authenticator” mode on uplink ports connected to overlying switches).

config 802.1x capability ports 1-12 authenticator

Turn on 802.1X function

enable 802.1x

Configure the RADIUS server parameters

config radius add 1 192.168.0.10 key 123456 default

Check the current status of the 802.1X authentication on ports 1-24
show 802.1x auth_state ports 1-12

Check the current configuration of the 802.1X

show 802.1x auth_configuration

Check the availability of connections between workstations and ISP by ping command: ping <IP-address>
Make a conclusion about the results of the commands

3.3.2 MAC-Based 802.1X

Task

Configure authentication based on the standard 802.1X MAC-Based on switches fragment network.

Before carrying out the laboratory work is necessary to reset the switch to factory setting using defaults command: reset config

Switch Configuration L3 (DGS-3627):

Configure user authentication on the RADIUS server

config 802.1x auth_protocol radius_eap

Configure the authentication type 802.1X: MAC-based
config 802.1x auth_mode mac_based

Configure the ports to which users are connected as authenticators config 802.1x capability ports 1-12 authenticator

Turn on 802.1X

enable 802.1x

Configure the RADIUS server parameters
config radius add 1 192.168.0.10 key 123456 default

Check the current status of the 802.1X authentication on ports 1-12

show 802.1x auth_state ports 1-12

Check the current configuration of the 802.1X

show 802.1x auth_configuration

Check the availability of connections between workstations and ISP by ping command:

ping <IP-address>

Make a conclusion about the results of the commands

3.3.2 802.1X Guest VLAN

Scheme of laboratory model is shown in Figure 3.3.

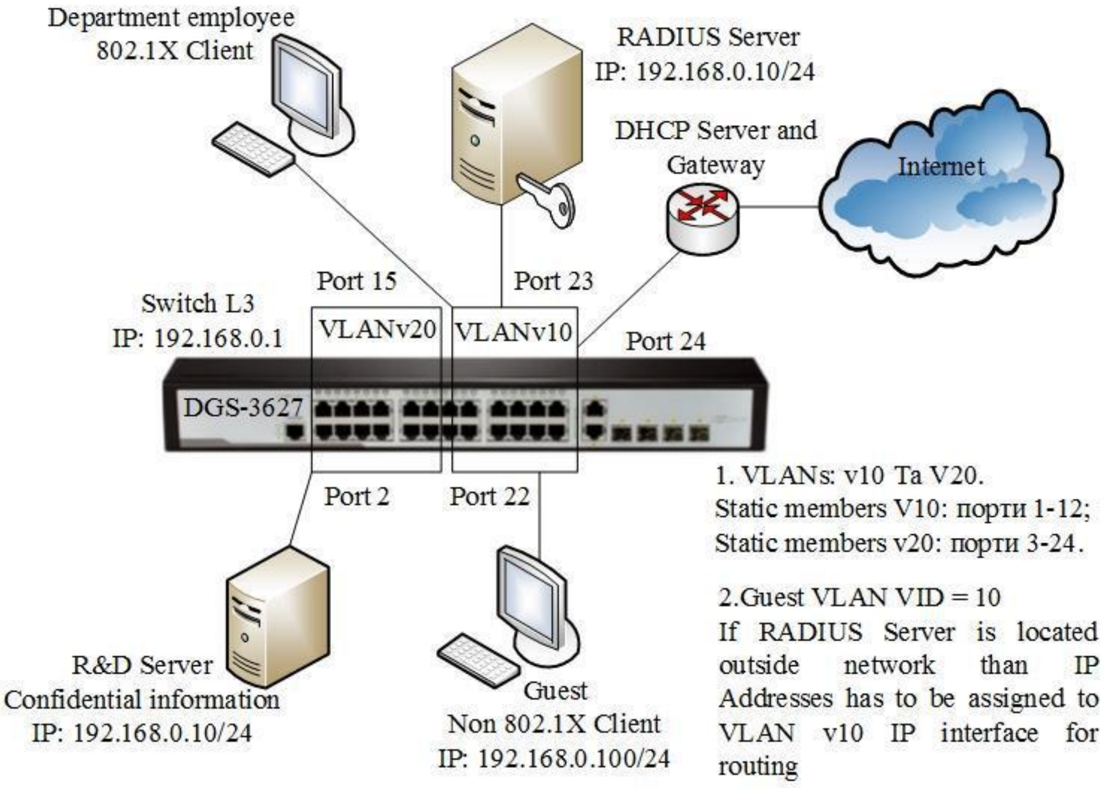


Figure 3.3 – Fragment of network for laboratory work

Task

Configure the fragment network scheme, which is not authenticated users in VLAN 10, is allowed to access the Internet. After successful authentication, the user ports to which they are connected, will be added to VLAN 20.

Configuration Switch L3 (DGS-3627):

Switch VLAN configuration v10 and v20. config vlan default delete 1-24 create vlan v10 tag 10

config vlan v10 add untagged 13-24 create vlan v20 tag 20

config vlan v20 add untagged 1-12

config ipif System ipaddress 192.168.0.1/24 vlan v10

Turn on 802.1X and Guest VLAN enable 802.1x

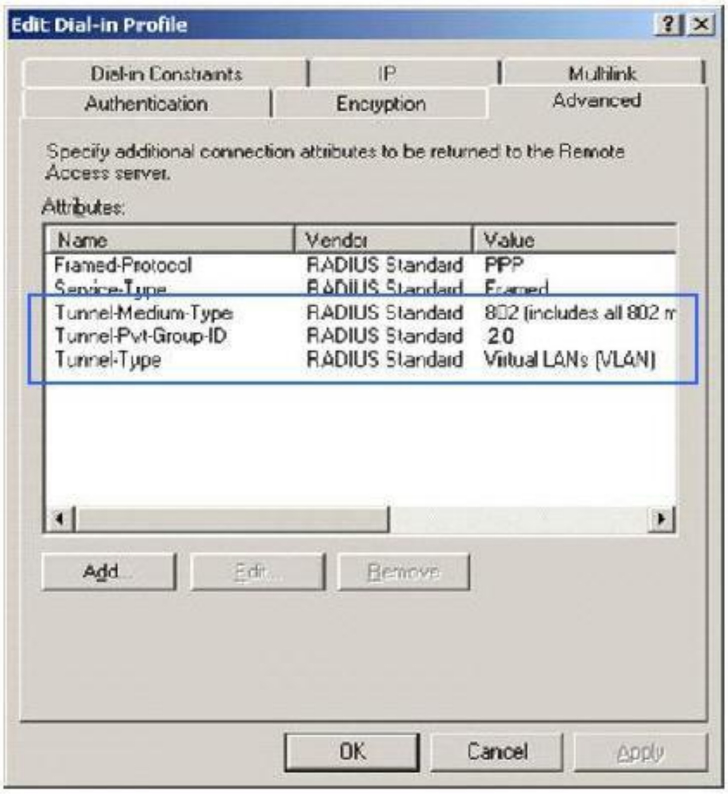
create 802.1x guest_vlan v10

config 802.1x guest_vlan ports 13-24 state enable

Configure the switch as an authenticator and specify the RADIUS server. config 802.1x capability ports 13-24 authenticator config radius add 1 192.168.0.10 key 123456 default

RADIUS Server configuration installation includes the following user-defined attributes (Figure 3.4):

Tunnel-Medium-Type (65) = 802 Tunnel-Pvt-Group-ID (81) = 20 ←VID Tunnel-Type (64) = VLAN



Specify additional connection attributes to be returned to the Remote Access server.

Attributes:

Name	Vendor	Value
Framed-Protocol	RADIUS Standard	PPP
Service-Type	RADIUS Standard	Framed
Tunnel-Medium-Type	RADIUS Standard	802 (includes all 802 m
Tunnel-Pvt-Group-ID	RADIUS Standard	20
Tunnel-Type	RADIUS Standard	Virtual LANs (VLAN)

Figure 3.4 – Custom attributes on the RADIUS server

Perform the test configuration on the switch with the following commands

```
DGS-3627#show 802.1x auth_configuration Command: show 802.1x auth_configuration
   802.1X                                      : Enabled
   Authentication Mode                         : Port_based
   Authentication Protocol                     : RADIUS_EAP
   Port number          : 1
   Capability           : None
   AdminCrlDir          : Both
   OpenCrlDir           : Both
   Port Control         : Auto
   QuietPeriod          : 60 sec
   TxPeriod             : 30 sec
   Supp Timeout         : 30 sec
   Server Timeout       : 30 sec
   MaxReq               : 2 times
   ReAuthPeriod         : 3600 sec
   ReAuthenticate       : Disabled
```

```
DGS-3627#show 802.1x guest_vlan

Command: show 802.1x guest_vlan

Guest VLAN Setting

Guest VLAN : v10

Enable Guest VLAN Ports : 13-24 DGS-3627#show radius

Command: show radius

   Idx  IP Address        Auth-Port      Acct-Port      Status     Key
   --   -----------       --------       ----------     -----      -----
   1    192.168.0.10      1812           1813           Active     123456

Total Entries: 1
```

If the user is connected to the port 22 does not pass authentication, and the current state of VLAN 802.1X authentication on the switch are as follows:

```
DGS-3627#show vlan
VID       : 1                                VLAN Name: default

VLAN Type   : Static Advertisement : Enabled
```

```
Member  Ports                                   : 25-27
Static      Ports                               : 25-27
Current Tagged Ports                            :
Current Untagged Ports                          : 25-27
Static Tagged Ports                             :
Static Untagged Ports                           : 25-27
Forbidden Ports                                 :
VID   :     10     VLAN Name                    : v10
VLAN Type    : Static Advertisement             : Disabled
Member Ports                                    : 13-24
Static Ports                                    : 13-24
Current Tagged Ports                            :
Current Untagged Ports                          : 13-24
Static Tagged Ports                             :
Static Untagged Ports                           : 13-24
Forbidden Ports                                 :
VID   : 20         VLAN Name                    : v20
VLAN Type    : Static Advertisement             : Disabled
Member Ports                                    : 1-12
Static Ports                                    : 1-12
Current Tagged Ports                            :
Current Untagged Ports                          : 1-12
Static Tagged Ports                             :
Static Untagged Ports                           : 1-12
Forbidden Ports                                 :

    Total Entries : 3

    DGS-3627#show 802.1x auth_state

    Command: show 802.1x auth_state

Port      Auth PAE State        Backend State        Port State
-----     -------------         --------------       ----------
1         ForceAuth             Success              Authorized
2         ForceAuth             Success              Authorized
3         ForceAuth             Success              Authorized
4         ForceAuth             Success              Authorized
5         ForceAuth             Success              Authorized
6         ForceAuth             Success              Authorized
```

```
7     ForceAuth              Success      Authorized
8     ForceAuth              Success      Authorized
9     ForceAuth              Success      Authorized
10    ForceAuth              Success      Authorized
11    ForceAuth              Success      Authorized
12    ForceAuth              Success      Authorized
13    Disconnected           Idle         Unauthorized
14    Disconnected           Idle         Unauthorized
…
…     … …
22    Connecting             Idle         Unauthorized
```

After authentication, the client's current VLAN settings and status of the 802.1X authentication will change as follows:

```
DGS-3627#show vlan
VID  : 1        VLAN Name                        : default
VLAN Type  : Static Advertisement                : Enabled
Member Ports                                     : 25-27
Static Ports                                     : 25-27
Current Tagged Ports                             :
Current Untagged Ports                           : 25-27
Static Tagged Ports                              :
Static Untagged Ports                            : 25-27
Forbidden Ports                                  :
VID  : 10       VLAN Name                        : v10
VLAN Type  : Static Advertisement                : Disabled
Member Ports                                     : 13-21,23-24
Static Ports                                     : 13-21,23-24
Current Tagged Ports                             :
Current Untagged Ports                           : 13-21,23-24
Static Tagged Ports                              :
Static Untagged Ports                            : 13-21,23-24
Forbidden Ports                                  :

VID  : 20       VLAN Name                        : v20
VLAN Type  : Static Advertisement                : Disabled
Member Ports                                     : 1-12,22
```

```
Static Ports                              : 1-12,22
Current Tagged Ports                      :
Current Untagged Ports                    : 1-12,22
Static Tagged Ports                       :
Static Untagged Ports                     : 1-12,22
Forbidden Ports                           :
Total Entries : 3
DGS-3627#show 802.1x auth_state
Command: show 802.1x auth_state
Port        Auth PAE State      Backend State     Port State
---         --------------      -------------     ----------
1           ForceAuth           Success           Authorized
2           ForceAuth           Success           Authorized
3           ForceAuth           Success           Authorized
4           ForceAuth           Success           Authorized
5           ForceAuth           Success           Authorized
6           ForceAuth           Success           Authorized
7           ForceAuth           Success           Authorized
… …         … …
22          Authenticated       Idle              Authorized
```

Make a conclusion about the results of the commands

3.4 Contents of report

Report on the implementation of laboratory work should include the following items:

1. The theme and purpose of the laboratory work.

2. Block diagram of the network with the designation of ports, IP address, network mask interface of workstation, Radius server and switch.

3. Order of performance laboratory work (sequence of input commands with the relevant explanations).

4. Graphical results.

5. The analysis and conclusions about laboratory work implementation.

4 CONFIGURATION OF TRAFFIC SEGMENTATION INSIDE VIRTUAL LOCAL AREA NETWORKS (802.1Q, 802.1V, TRAFFIC SEGMENTATION)

4.1 Purpose of work

To configure network equipment for network fragment. To configure VLANs (Virtual Local Area Network, VLAN). To obtain the skills of VLAN standards 802.1Q, 802.1v.configuration. to investigate the principles of Traffic Segmentation functions.

4.2 Brief description of the methods of traffic differentiation within the LAN

VLAN is a logical grouping of nodes, where traffic, including broadcast, the link layer is completely isolated from the other nodes in the network. This means that the transfer of frames between different virtual networks based on MAC-addresses are not independent of the type of address - a unique, group, or broadcast. At the same time within a virtual network frames transmitted by switching technology, i.e., only to the port which is associated with the destination address of the frame.

The following types of VLAN can be implemented on switches:

- Port-based;
- based on IEEE 802.1Q standard;
- based on IEEE 802.1ad standard (Q-in-Q VLAN);
- based on IEEE 802.1v standard;
- MAC-based address;
- asymmetric VLAN.

The switch can be configured, and other features to distinguish the network link-layer model of OSI, for example, Traffic Segmentation also

4.3 Methodical instructions and work order

Laboratory model description

A fragment of a telecommunication network consists of a switch, which is connected to 4 workstations and Internet gateway (see Table 4.1).

Table 4.1

Equipment (on 2 work place):	
Switch DES-3200-10 or DGS-3200-10	2 unit
Work station	4 unit
Console cable	2 unit
Ethernet cable	5 unit

4.3.1 Configure VLAN (based on IEEE 802.1Q standard)

Schematic of laboratory model is shown in Figure 4.1.

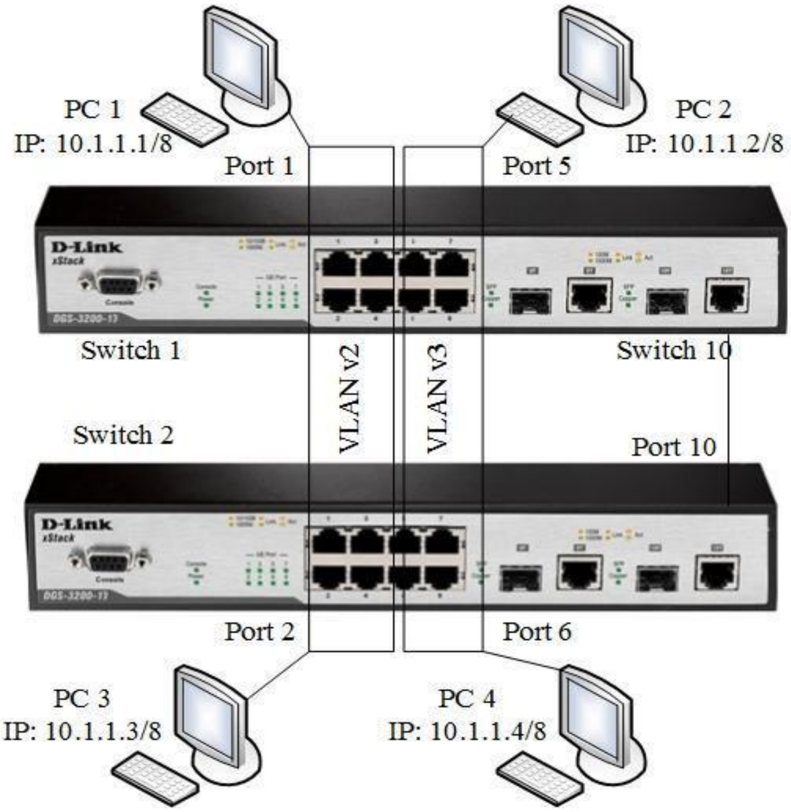


Figure 4.1 - Scheme of fragment network

<u>Task</u>

Configure VLANv2 VLANv3 on switches and track network based on the IEEE 802.1Q standard

Before performing the laboratory work is necessary to reset the switch to default setting using command:

```
reset config
```

Ports which used in new VLAN configuration must be removed from the default VLAN, since according to the standard IEEE 802.1Q. Untagged ports cannot simultaneously belong to multiple VLAN.

Configure switch №1

Remove corresponding ports from the default VLAN and create a new VLAN:

```
config vlan default delete 1-10
config vlan default add tagged 10
```

Create a VLAN v2 and v3, add the appropriate VLAN ports that must be configured like unmarked. Configure the port 10 as marked:

```
create vlan v2 tag 2
config vlan v2 add untagged 1-4 config vlan v2 add tagged 10 reate vlan v3 tag 3
config vlan v3 add untagged 5-8 config vlan v3 add tagged 10
```

Check the VLAN configuration:

```
show vlan
```

Perform the same configuration for switch №2

Check the availability of connections between workstations by command ping: ping <IP-address>

Make a conclusion about the results of the commands

4.3.2 Configure traffic segmentation within the VLAN

Task

Configure the switch ports 5-8 1, which belong to the VLAN v3 using the function of segmentation traffic. Workstations that are connected there to cannot communicate, but they can transmit data through the main channel.

Configure switch №1

Configure the Traffic Segmentation functions:

```
config traffic_segmentation 5 forward_list 10
config traffic_segmentation 6 forward_list 10
config traffic_segmentation 7 forward_list 10
config traffic_segmentation 8 forward_list 10
```

Check the settings:

```
show traffic_segmentation
```

Connect PC1 to port 6 Switch 1.

Check the availability of connections between workstations by command ping: ping <IP-address>

Make a conclusion about the results of the commands

4.3.3 Configure VLAN based on the IEEE 802.1v standard

Scheme of laboratory model is shown in Figure 4.2

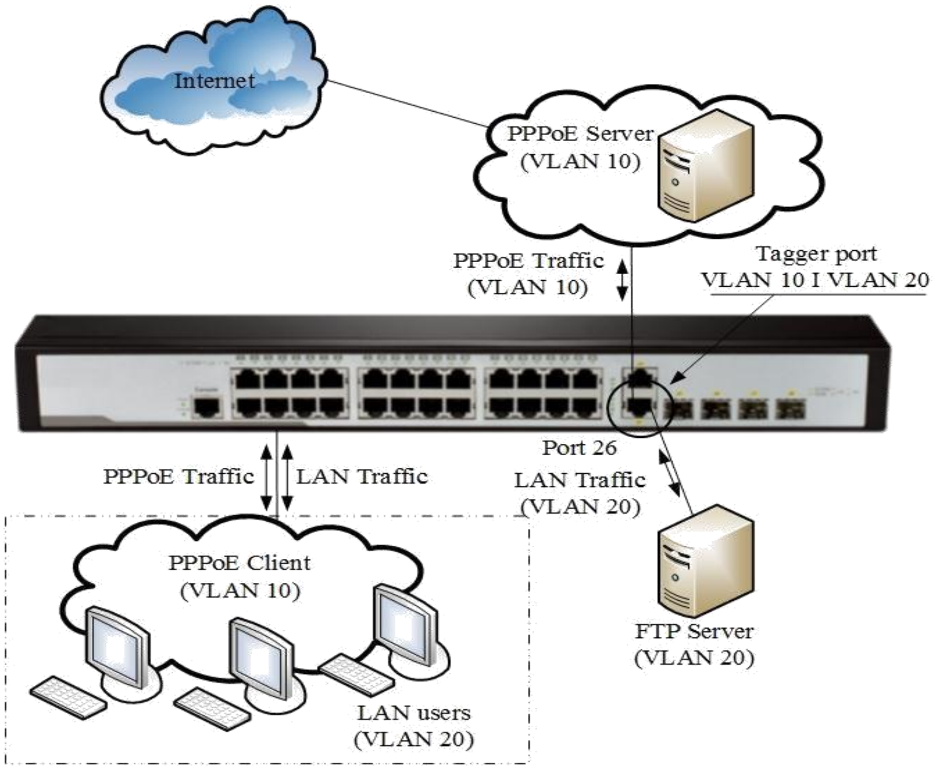


Figure 4.2 - VLAN scheme

Task

LAN users are dedicated network VLAN 20. Their connection to the ISP through a PPPoE server (VLAN 10). You need to create a VLAN 802.1v identifier VID = 10 on switch to PPPoE protocol for the separation of LAN traffic from PPPoE traffic.

Configure the switch

Configure the new 802.1Q VLAN.

```
config vlan default delete 1-28 create vlan pppoe tag 10
config vlan pppoe add untagged 1-24 config vlan pppoe add tagged 26 create vlan
base tag 20
config vlan base add tagged 26 config vlan base add untagged 1-24
```

Configure the PVID on the ports to which users are connected

```
config port_vlan 1-24 pvid 20
```

Create 802.1v VLAN protocol PPPoE (the first group of protocols configured for PPPoE frames transmitted at the research stage, the second - for PPPoE frames established session).

```
create dot1v_protocol_group group_id 1 group_name pppoe_disc

config dot1v_protocol_group group_id 1 add protocol ethernet_2 8863
```

```
create dot1v_protocol_group group_id 2 group_name pppoe _session
config dot1v_protocol_group group_id 2 add protocol
ethernet_2 8864
config port dot1v ports 1-24 add protocol_group group_id
1 vlan pppoe
config port dot1v ports 1-24 add protocol_group group_id
2 vlan pppoe
```

Check the availability of connections between workstations and ISP by ping command:

```
ping <IP-address>
```

Make a conclusion about the results of the commands

4.4 Contents of report

Report on the implementation of laboratory work should include the following items:

1. The theme and purpose of the laboratory work.

2. Block diagram of the network with the designation VLAN, port, IP address, network mask interface workstation and switch.

3. Order of performance laboratory work (sequence of input commands with the relevant explanations).

4. Graphical results.

5. The analysis and conclusions about laboratory work implementation.

5 PPTP VPN PERFORMANCE EVOLUATION (USER-LAN, LAN-LAN)

5.1 Purpose:

To configure a network equipment. Configurate VPN based on PPTP on network router. To study influence of encryption algorithms for performance VPN routers.

5.2 Brief PPTP overview

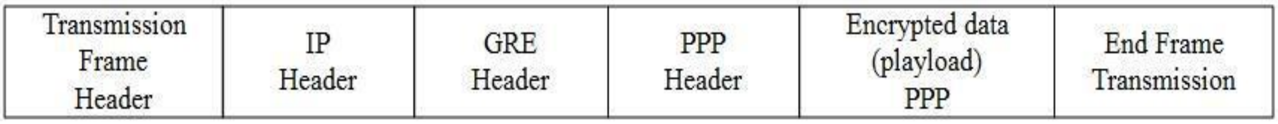
PPTP (Point-to-Point Tunneling Protocol) - point-to-point tunneling protocol that allows your computer to establish a secure connection to the server by creating a tunnel in an unprotected network.

A PPTP tunnel is instantiated by communication to the peer on TCP port 1723. This TCP connection is then used to initiate and manage a second GRE tunnel to the same peer.

The PPTP GRE packet format is non standard, including an additional acknowledgement field replacing the typical routing field in the GRE header. However, as in a normal GRE connection, those modified GRE packets are directly encapsulated into IP packets, and seen as IP protocol number 47.

Packets transmitted within PPTP sessions, have the following structure (Fig. 5.1):

1. Link layer header, used in the Internet, such as Ethernet header frame;
2. IP header, which contains the address of the sender and receiver of the package;
3. GRE (Generic Routing Encapsulation) header;
4. PPP source package that includes a package of IP, IPX or NetBEUI.



Transmission Frame Header	IP Header	GRE Header	PPP Header	Encrypted data (playload) PPP	End Frame Transmission

Figure 5.1 – Structure packet that forwarded on PPTP tunnels

This method of encapsulation provides independence of network layer protocols of the OSI model and enables secure remote access over IP-based networks are open to any local networks (IP, IPX or NetBEUI). According to the protocol PPTP in creating a secure virtual channel remote user authentication is performed and encryption of transmitted data (Fig. 5.2).

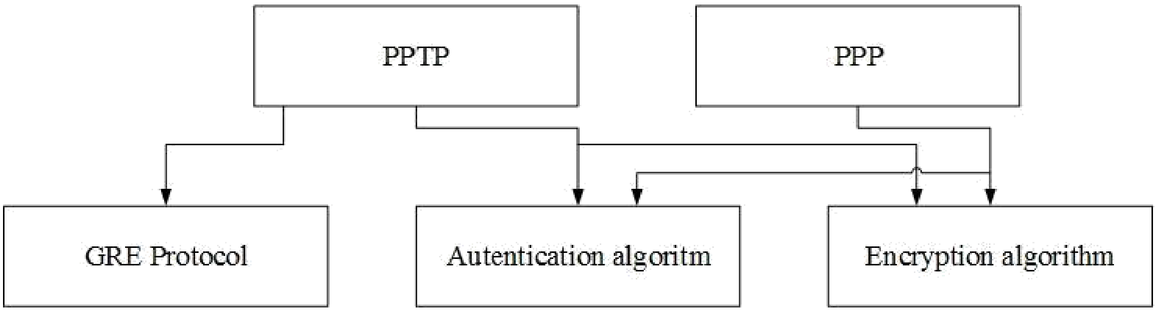


Figure 5.2 – PPTP protocol architecture

PPTP-traffic can be encrypted using MPPE. For authentication, clients can use a variety of mechanisms, such as - MS-CHAPv2 and EAP-TLS.

PPTP also supports VPN connectivity via a LAN. ISP connections are not required in this case, so tunnels can be created directly as in Step 2 above.

Once the VPN tunnel is established, PPTP supports two types of information flow:

- control messages for managing and eventually tearing down the VPN connection. Control messages pass directly between VPN client and server.
- data packets that pass through the tunnel, to or from the VPN client.

PPTP Security. PPTP supports authentication, encryption, and packet filtering. PPTP authentication uses PPP-based protocols like EAP, CHAP, and PAP. PPTP supports packet filtering on VPN servers. Intermediate routers and other firewalls can also be configured to selectively filter PPTP traffic.

PPTP and PPP. In general, PPTP relies on the functionality of PPP for these aspects of virtual private networking.

- authenticating users and maintaining the remote dial-up connection
- encapsulating and encrypting IP, IPX, or NetBEUI packets

PPTP directly handles maintaining the VPN tunnel and transmitting data through the tunnel. PPTP also supports some additional security features for VPN data beyond what PPP provides.

5.3 Methodical instructions and work order

Laboratory model description

A fragment of the telecommunications network consists of Firewall that provides protection perimeter LAN. The list of equipment is presenting in Table. 5.1, and topology - Fig. 5.2 and Fig. 5.3

Table 5.1

Equipment (one work place):	
Work station	1 unit
Ethernet cable	3 units
Firewall DFL-810	2 unit

5.3.1 Configuring VPN based on PPTP (user-LAN)

Fragment of the practice network is depicted on Figure 5.3

Task

Configure remote user to connect to LAN resources located on VPN Router DI-804HV, using a protocol PPTP.

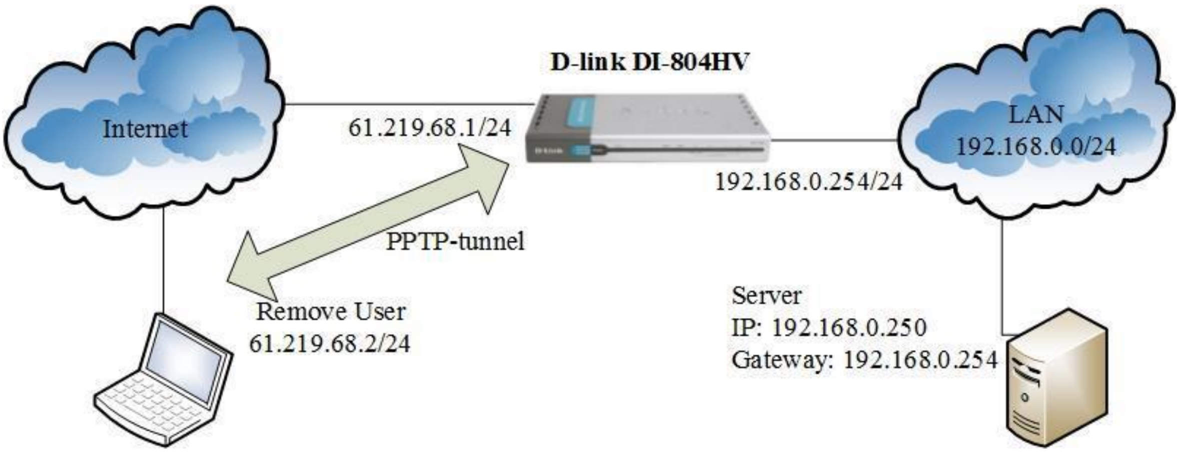


Figure 5.3 – Fragment network scheme

1. Internal IP-address of DI-804HV for default is 192.168.0.1, so on your PC that connected to the router DI-804HV, should be assighed IP-address from the range 192.168.0.2 - 192.168.0.254

2. Login for default - "Admin", password is empty;

3. To make changes to the configuration of the router after all necessary manipulations on the relevant page web interface you must click "Apply" and then "Restart".

4. IP addressing in this document is given as an example. To configure the WAN and LAN use the IP address specified by the teacher.

Step 1. Change DI-804HV settings

Before performing laboratory work must reset the DI-804HV to defaults. Tools => System. In tab System chose Reset to Default (рис.5.4)

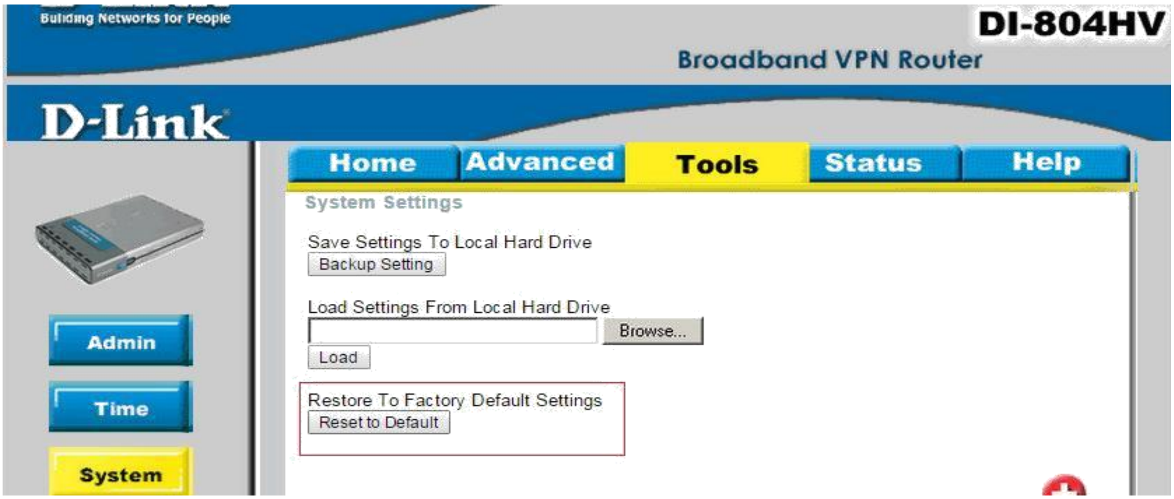
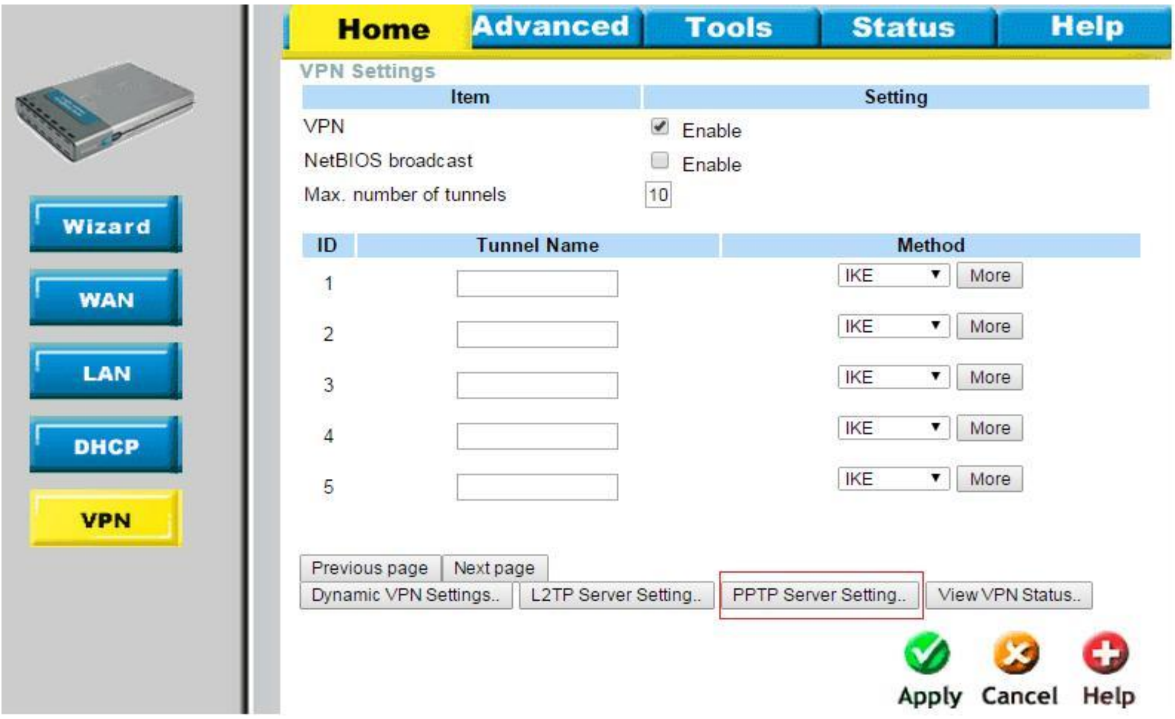


Figure 5.4 – DI-804HV Web-interface

In accordance with the scheme (Fig. 5.3) define network settings routers: LAN, WAN IP, subnet mask, default gateway. In tab ***Home -> VPN*** chose ***PPTP Server Settings***:



Item	Setting
VPN	☑ Enable
NetBIOS broadcast	□ Enable
Max. number of tunnels	10

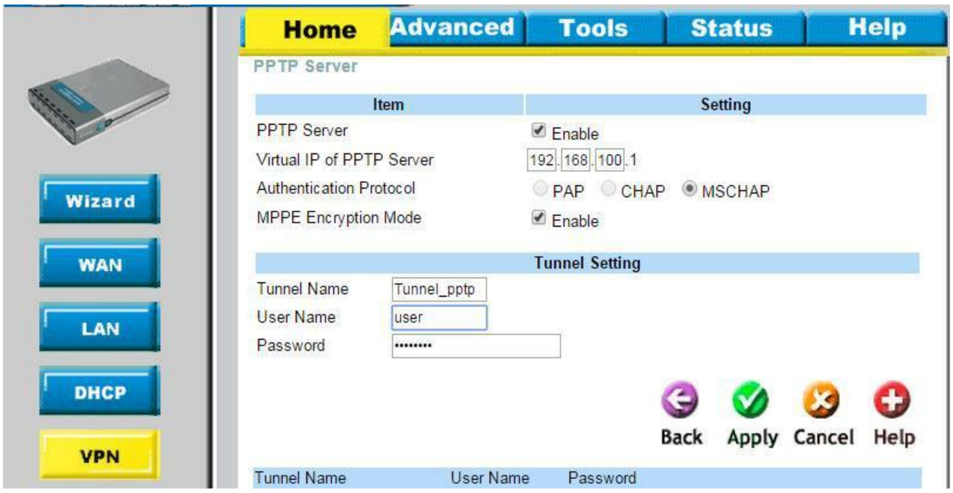
ID	Tunnel Name	Method
1		IKE ▾ More
2		IKE ▾ More
3		IKE ▾ More
4		IKE ▾ More
5		IKE ▾ More

Figure 5.5 – VPN configuration

In the tab **PPTP Server Settings**, must perform the following settings:

- **PPTP Server** – switch on PPTP-server, checkmark Enable;
- **Virtual IP of PPTP Server** * - specify the start address pool of addresses for clients PPTP, for example, 192.168.100.1 (first IP-address will be 192.168.100.2);
- **Authentication Protocol** - specify the authentication protocol, for example, MSCHAP (as in this case allowed MPPE-Encryption);
- **Tunnel Name -** specify the tunnel name, for example, Tunnel_pptp;

- **MPPE Encryption Mode** – switch on/ switch off MPPE-encryption (If it is nessesary), checkmark Enable;
- **User Name** - specify the user name, for example, user;
- **Password** – specify the password, for example, 1234567.



PPTP Server

Item	Setting
PPTP Server	☑ Enable
Virtual IP of PPTP Server	192.168.100.1
Authentication Protocol	○ PAP ○ CHAP ● MSCHAP
MPPE Encryption Mode	☑ Enable

Tunnel Setting

Tunnel Name	Tunnel_pptp
User Name	user
Password	••••••••

Tunnel Name	User Name	Password

Figure 5.6 – Configuring PPTP server

Step 2: Setting client PPTP (for example, Windows XP)

1) The properties of the network environment, select "Create a new connection" in order to create the initial connection VPN-PPTP.
2) The "Master Network". Click "Next"
3) Select "Connect to the workplace." Click "Next" button.
4) Select "Connect to a virtual private network." Click "Next" button.
5) Enter the user name (eg, PPTP). Click "Next" button.
6) Enter the name or IP address of the VPN-server. Click "Next" button.
7) Click "Ready" or "Finish", then PPTP-connection will be established.
8) The properties of the network environment, select VPN-PPTP connection and run.

Note: *For additional instructions on configuring PPTP client contact's user guide for your operating system.*

Step 3. Tasks for research

Students should generate traffic using iperf-2.0.5 to evaluate the router performance. Performance of PPTP connection defined as follows:

PPTP-client on WAN-segment connect to PPTP-server, then made standard speed tests.

1) Investigate VPN connection performance without encryption mode (remove the check mark MPPE Encryption Mode).

2) Investigate VPN connection performance with encryption mode (tick opposite MPPE Encryption Mode).

5.3.2 Configuring VPN based on PPTP (LAN-LAN)

Laboratory model scheme is depicted on Figure 5.7.

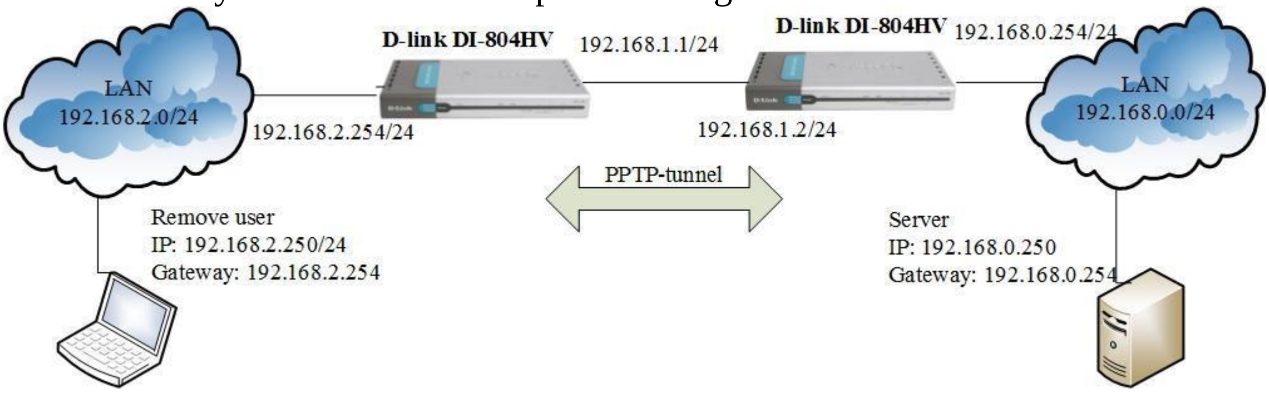


Figure 5.7 – Laboratory model scheme

Task

Configure connect users with the same LAN to LAN resources located on VPN routers DI-804HV, using a protocol PPTP.

Configuration routers DI-804HV

1) In accordance with the scheme (Fig. 5.7) create the network settings routers: LAN, WAN IP, subnet mask, default gateway.

2) In accordance with paragraph 5.3.1 Step 1 configures router DI-804HV.

3) In accordance with paragraph 5.3.1 Step 3 Perform tasks for research.

5.4 Contents of report

1. Report on the implementation of laboratory work should include the following items:
2. The theme and purpose of the laboratory work.
3. Block diagram of the network with the designation of ports, IP address, network mask interface of workstation, firewall and switch.
4. Order of performance laboratory work (sequence of input commands with the relevant explanations).
5. Graphical results.
6. The analysis and conclusions about laboratory work implementation.

6VPN IPSEC PERFORMANCE EVALUATION (USER-LAN, LAN-LAN)

6.1 Purpose

To obtaine experience VPRN IPSec configuration. To investigate the influence of encryption algorithms on the performance of VPN routers.

6.2 Background. Brief IPSec overview

IPSec described in RFC from 2401 to 2412.

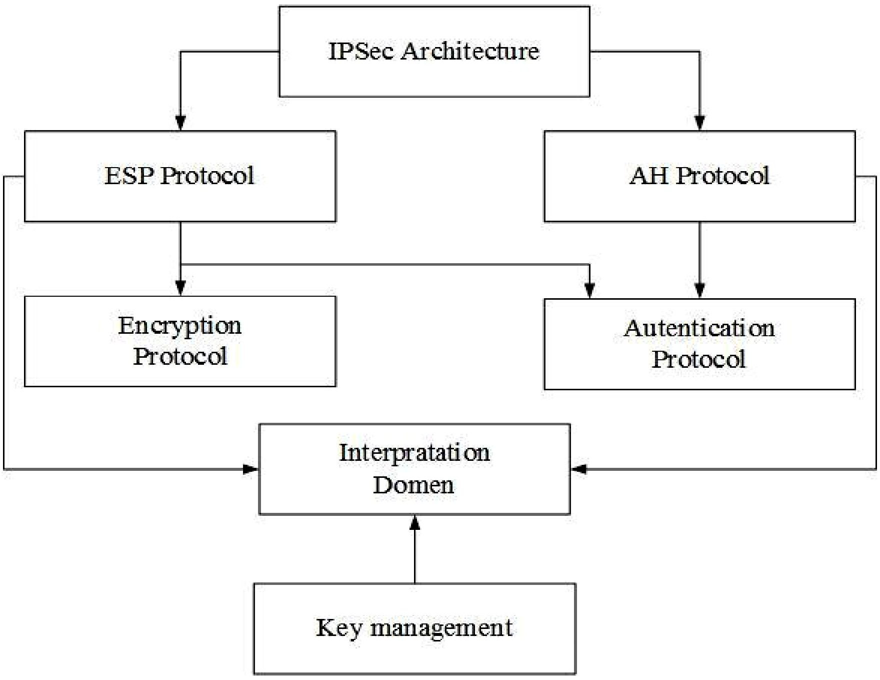


Figure 6.1 - Relationship certain directions and parts of IPSec

AH (*Authentication header*) is a protocol that provides *authentication* of either all or part of the contents of a datagram through the addition of a *header* that is calculated based on the values in the datagram. What parts of the datagram are used for the calculation, and the placement of the header, depends on the mode (tunnel or transport) and the version of IP (IPv4 or IPv6).

The operation of the AH protocol is surprisingly simple—especially for any protocol that has anything to do with network security. It can be considered analogous to the algorithms used to calculate checksums or perform CRC checks for error detection. In those cases, a standard algorithm is used by the sender to compute a checksum or CRC code based on the contents of a message. This computed result is transmitted along with the original data to the destination, which repeats the calculation and discards the message if any discrepancy is found between its calculation and the one done by the source.

This is the same idea behind AH, except that instead of using a simple algorithm known to everyone, we use a special hashing algorithm and a specific key known only to the source and the destination. A security association between two devices is set up that specifies these particulars so that the source and destination know how to perform the computation but nobody else can. On the source device, AH performs the computation and puts the result (called the *Integrity Check Value* or *ICV*) into a special header with other fields for transmission. The destination device does the same calculation using the key the two devices share, which enables it to see immediately if any of the fields in the original datagram were modified (either due to error or malice).

It's important that I point out explicitly that just as a checksum doesn't change the original data, neither does the ICV calculation change the original data. The presence of the AH header allows us to verify the integrity of the message, but doesn't encrypt it. Thus, AH provides ***authentication*** but not ***privacy***

Encapsulating Security Payload (ESP) provides confidentiality, in addition to authentication, integrity, and anti-replay. ESP can be used alone, or in combination with AH. ESP does not normally sign the entire packet unless it is being tunneled — ordinarily, just the IP data payload is protected, not the IP header.

For example, Alice on Computer A sends data to Bob on Computer B. The data payload is encrypted and signed for integrity. Upon receipt, after the integrity verification process is complete, the data payload in the packet is decrypted. Bob can be certain it was really Alice who sent the data, that the data is unmodified, and that no one else was able to read it.

ESP indicates itself in the IP header using the IP protocol ID of 50. As shown in the Figure 8.3, the ESP header is placed prior to the transport layer header (TCP or UDP) or the IP payload data for other IP protocol types.

The ESP header contains the following fields:

Security Parameters Index Identifies, when used in combination with the destination address and the security protocol (AH or ESP), the correct security association for the communication. The receiver uses this value to determine the security association with which this packet should be identified.

Sequence Number Provides anti-replay protection for the SA. It is 32-bit, incrementally increasing number (starting from 1) that indicates the packet number sent over the security association for the communication. The sequence number is never allowed to cycle. The receiver checks this field to verify that a packet for a security association with this number has not been received already. If one has been received, the packet is rejected.

The ESP trailer contains the following fields:

Padding 0 to 255 bytes is used for 32-bit alignment and with the block size of the block cipher.

Padding Length Indicates the length of the Padding field in bytes. This field is used by the receiver to discard the Padding field.

Next Header Identifies the nature of the payload, such as TCP or UDP. The ESP Authentication Trailer contains the following field:

Authentication Data Contains the Integrity Check Value (ICV), and a message authentication code that is used to verify the sender's identity and message integrity. The ICV is calculated over the ESP header, the payload data and the ESP trailer.

Transport mode

As its name suggests, in transport mode, the protocol protects the message passed down to IP from the transport layer. The message is processed by AH/ESP and the appropriate header(s) added in front of the transport (UDP or TCP) header. The IP header is then added in front of that by IP.

Another way of looking at this is as follows. Normally the transport layer packages data for transmission and sends it to IP. From IP's perspective, this transport layer message is the payload of the IP datagram. When IPSec is used in transport mode, the IPSec header is applied only over this IP payload, ***not*** the IP header. The AH and/or ESP headers appears between the original, single IP header and the IP payload. This is illustrated in Figure 6.2.

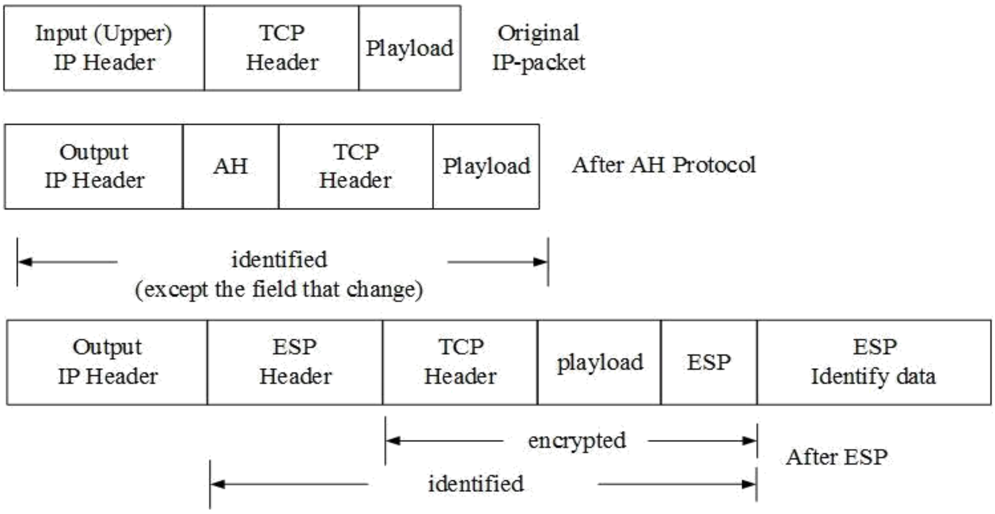


Figure 6.2 - IPSec Transport Mode Operation

When IPSec operates in transport mode, it is integrated with IP and used to transport the upper layer (TCP/UDP) message directly. After processing, the datagram has just one IP header that contains the AH and/or ESP IPSec headers.

Tunnel mode

In this mode, IPSec is used to protect a complete ***encapsulated*** IP datagram after the IP header has already been applied to it. The IPSec headers appear in front of the original IP header, and then a ***new*** IP header is added in front of the IPSec header. That is to say, the entire original IP datagram is secured and then encapsulated within another IP datagram. This is shown in Figure 6.3

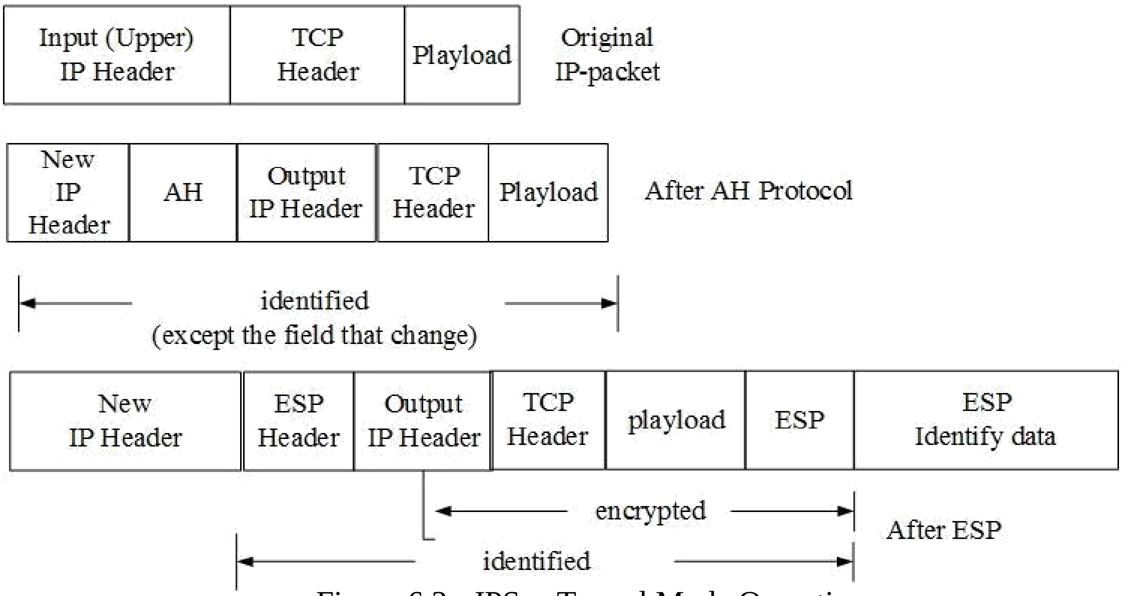


Figure 6.3 - IPSec Tunnel Mode Operation

IPSec tunnel mode is so named because it represents an encapsulation of a complete IP datagram, forming a virtual tunnel between IPSec-capable devices. The IP datagram is passed to IPSec, where a new IP header is created with the AH and/or ESP IPSec headers.added.

IPSec Security Associations. The concept of a security association (SA) is fundamental to IPSec. An SA is a relationship between two or more entities that describes how the entities will use security services to communicate securely. IPSec provides many options for performing network encryption and authentication. Each IPSec connection can provide encryption, integrity, authenticity, or all three services. When the security service is determined, the two IPSec peers must determine exactly which algorithms to use (for example, DES or 3DES for encryption; MD5 or SHA-1 for integrity). After deciding on the algorithms, the two devices must share session keys. As you can see, there is quite a bit of information to manage. The security association is the method that IPSec uses to track all the particulars concerning a given IPSec communication session.

Sets of all SA, installed on the node to communicate with another node (node) is stored in a database of security associations (Security Association Database - SAD). Each node maintains two SAD: one for incoming and one for outgoing traffic. Depending on implementation, may require several pairs SAD interface nodes for the multi - one for each interface SAD.

Internet Key Exchange.Before either AH or ESP can be used, however, it is necessary for the two devices to exchange the ―secret‖ that the security protocols themselves will use. The primary support protocol used for this purpose in IPSec is called Internet Key Exchange (IKE).

IKE is defined in RFC 2409, and is one of the more complicated of the IPSec protocols to comprehend. In fact, it is simply impossible to truly understand more than a real simplification of its operation without significant background in cryptography. I don't have a background in cryptography and I must assume that you, my reader, do not either. So rather than fill this topic with baffling acronyms and unexplained concepts, I will just provide a brief outline of IKE and how it is used.

The purpose of IKE is to allow devices to exchange information required for secure communication. As the title suggests, this includes cryptographic keys used for encoding authentication information and performing payload encryption. IKE works by allowing IPSec-capable devices to exchange security associations (SAs), to populate their security association databases (SADs). These are then used for the actual exchange of secured datagrams with the AH and ESP protocols.

IKE is considered a ― hybrid‖ protocol because it combines (and supplements) the functions of three other protocols. The first of these is the *Internet Security Association and Key Management Protocol (ISAKMP)*. This protocol provides a framework for exchanging encryption keys and security association information. It operates by allowing security associations to be negotiated through a series of phases.

ISAKMP is a generic protocol that supports many different key exchange methods. In IKE, the ISAKMP framework is used as the basis for a specific key exchange method that combines features from two key exchange protocols:

OAKLEY: Describes a specific mechanism for exchanging keys through the definition of various key exchange ―modes‖. Most of the IKE key exchange process is based on OAKLEY.

SKEME: Describes a different key exchange mechanism than OAKLEY. IKE uses some features from SKEME, including its method of public key encryption and its fast re-keying feature.

6.3 Methodical instructions and work order

Laboratory model description

A fragment of the telecommunications network consists of Firewall that provides protection perimeter LAN. The list of equipment is presenting in Table. 6.1, Topology - Fig. 6.3.

Table 6.1

Equipment (one work place):	
Work station	2 unit
Ethernet cable	3 units
Firewall DFL-810	2 unit
Switch L2	1 unit

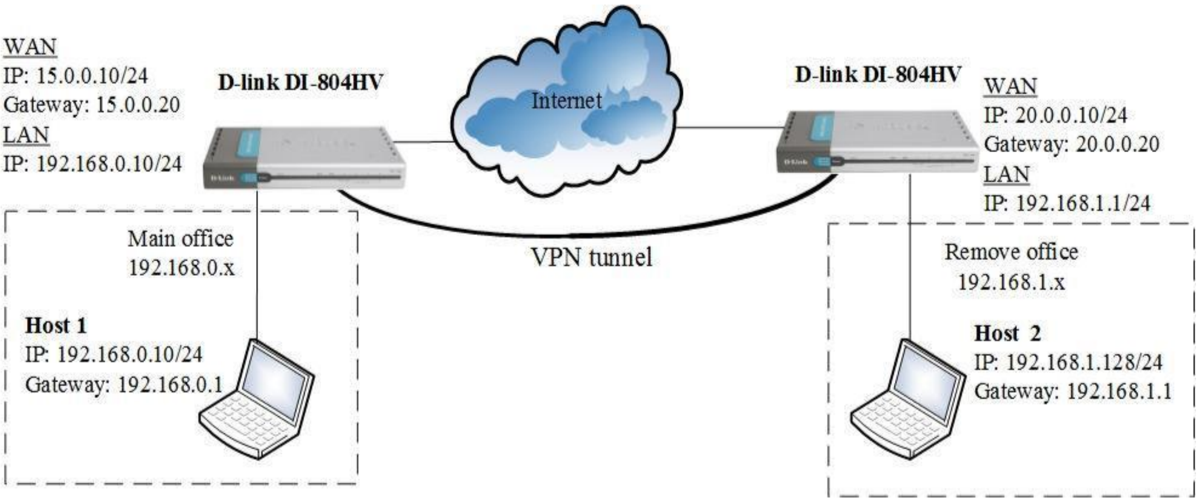


Figure 6.4 – Laboratory model scheme

6.3.1 Configuring the first DI-804HV:

Note

1. Internal IP-address of DI-804HV for default is 192.168.0.1, so on your PC that connected to the router DI-804HV, should be assighed IP-address from the range 192.168.0.2 - 192.168.0.254$;

2. Login for default - "Admin", password is empty;

3. To make changes to the configuration of the router after all necessary manipulations on the relevant page web interface you must click "Apply" and then "Restart";

4. IP addressing in this document is given as an example. To configure the WAN and LAN use the IP address specified by the teacher.

Step 1

- In accordance with the scheme (Fig. 6.1) Specifies the network router configuration: LAN, WAN IP,, subnet mask, default gateway.
- Setting up VPN using IKE.

On the contrary ID1 in the «Tunnel Name» inscribe the name of the tunnel, in the drop down menu «Method» choose IKE, press the button «More».

In the tab will appear specify:

- Address/local subnet mask (Local Subnet)/ (Local Netmask);
- Address/ remote subnet mask (Remote Subnet)/ (Remote Netmask);
- In the «Remote Gateway» Asking external IP-address of the remote VPN router;
- In the field «Preshare Key» - gthdsq key that will be used for the organization mechanism IKE VPN-tunnel. This key must be the same on both ends of the VPN-tunnel.

Chose the tab «Select IKE Proposal …», fill in the next fields:

 Proposal name – IKE Proposal;
 DH Group – Group1;
 Encrypt algorithm – 3DES;
 Auth algorithm – SHA1;
 Life Time –28800 sec.

Choose from the dropdown menu «Proposal ID» — «1» and click the button «Add to». Than choose buttons «Apply» and «Restart».

Go to menu «Set IPSEC Proposal». fill in the next fields:

 Proposal name – IPSec Proposal;
 DH Group – None;
 Encap protocol – ESP;
 Encrypt algorithm – 3DES;
 Auth algorithm – MD5;
 Life Time – 3600sec.

Choose from the dropdown menu «Proposal ID» — «1» and click the button «Add to». Than choose buttons «Apply» and «Restart».

Configure the second DI-804HV router similarly.

After configuration run the command ping from one host to another for VPN initialization

6.4 Tasks for research

Students should generate traffic using iperf-2.0.5 to evaluate the router performance. VPN configuration:

1. IKE – Group1/3DES/MD5/28800sec;
2. IPsec – ESP/3DES/MD5/3600sec.

6.4.1 Without VPN

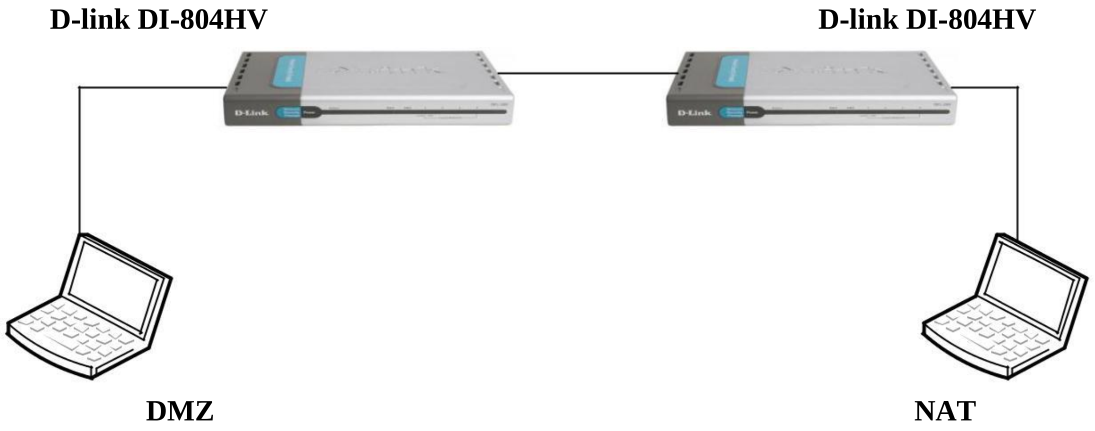


Figure 6.5 - Network topology without using VPN

6.4.2. Performance NAT DI-804HV

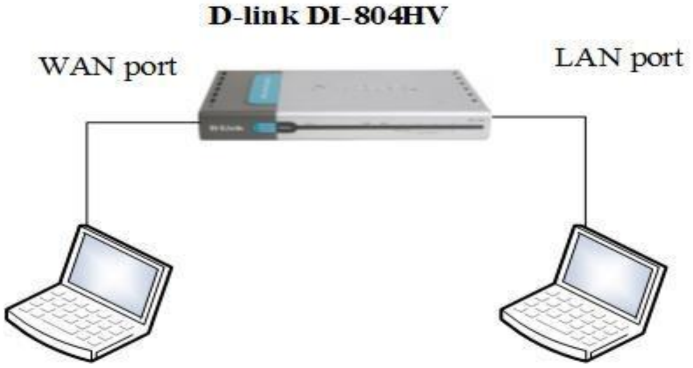


Figure 6.6 - Network topology for using NAT

6.4.3. Using DES and 3DES

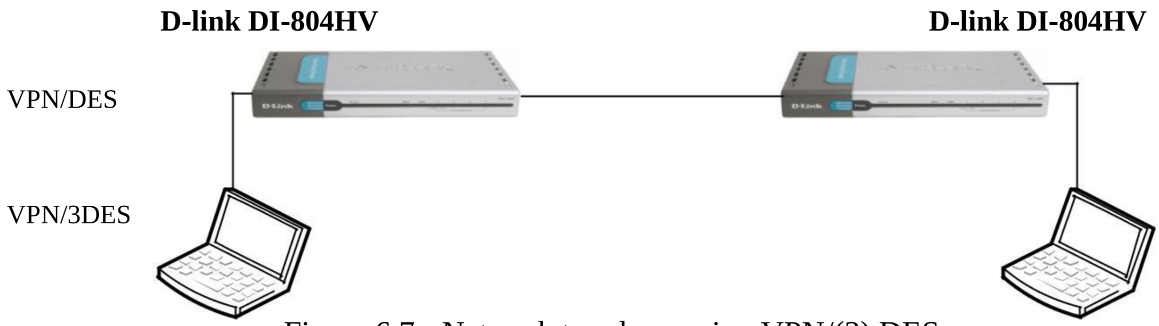


Figure 6.7 - Network topology using VPN/(3) DES

6.4.4 Using AH

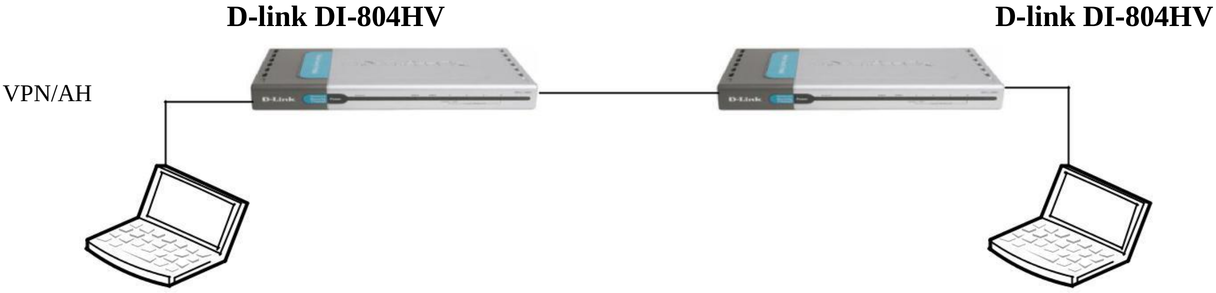


Figure 6.8 - Network topology for using VPN / AH

VPN configuration:

- IKE – Group1/3DES/MD5/28800sec;
- IPsec — AH/none/MD5/3600sec.

6.5 Contents of report

1. Report on the implementation of laboratory work should include the following items:

2. The theme and purpose of the laboratory work.

3. Block diagram of the network with the designation of ports, IP address, network mask interface of workstation, firewall and switch.

4. Order of performance laboratory work (sequence of input commands with the relevant explanations).

5. Graphical results.

6. The analysis and conclusions about laboratory work implementation.

7 DESIGNING LAN PERIMETER SECURITY (FIREWALL)

7.1 Purpose of work

To obtaining skills of logical objects configuration: address book services, interfaces, passing traffic rules and firewall ALG lists.

7.2 Brief overview. Configuring firewalls NetDefend

The system configuration consists of configuration objects, where each object is a configurable element of various types. The objects of the configuration include: routing table entries, address book entries, service description, IP-rules and other. Each object has a set of configuration properties, which make the value of the object.

7.2.1 Objects (facilities) creating and testing

Object - is the simplest configuration element such as IP-address, network key etc. Each object has a name and can be used in many locations of device configuration. Objects - the basic unit of the device configuration, they are used almost everywhere: in the routing tables, the rules in the configuration interface, VPN, etc.

Address Book. Address Book contains objects with the given name, with different addressing, including the IP-addresses of interfaces and a range of network addresses. When you use object names instead of addresses themselves, will need to change only one field value, not everyone, where meets this address.

IPv4 Address Object for information about addresses of hosts, networks, and IP-ranges of addresses. Each host is represented by its unique IP-address (eg: 192.168.1.1). IP-based network is presented by using Classless Inter Domain Routing (CIDR) or otherwise with a subnet mask, for example: 192.168.1.1/24. The range represents the sequential order of host addresses, for example: the range includes 5 192.168.1.10-192.168.1.14 hosts.

Automatic generation of objects addresses. When first put certain objects is done automatically. These include:

□ Interface Addresses:

For each Ethernet-interface system predetermined IP-addressing for two objects - one object with the actual IP-address and a second interface is a LAN interface for this purpose. The interface object is registered as the *interfacename ip* (e.g., *lan_ip*), and network interface object – *interfacename net* (e.g., *lannet*). Default Gateway:

IP-address of object, prescribed *interfacename_gw*, is a gateway system default. For example, an object used primarily wan1_gw routing table, except that - DHCP-client subsystem to store address information received from the DHCP-server. If the IP-address of the default gateway to change wan1_gw object will contain the specified address. If you do not make any changes, the value of the object will be the default 0.0.0.0.

□ All-nets:

IP-address of object *all-nets* initialized value like 0.0.0.0/0, thus rendering all possible IP-addresses. This object is actively used when configuring many configurations.

□ When using a DHCP-client or PPPoE connection on the interface automatically given two additional subject matters: *interfacename_dns1* and *interfacename_dns2*. For example, these interface objects wan1 expressed as *wan_dns1* and *wan_dns2*, and for the PPPoE interface can be designated as *pppoe_dns1* and *pppoe _dns2*.

Objects Ethernet-addresses are using to refer to symbolic names Ethernet-address (or MAC-addresses). They are using, for example, when filling the ARP-table static ARP-data, or in another part of the configuration, where the symbolic name rather numeric (hexadecimal) Ethernet-address. When Ethernet-address determining – next format is used: aa-bb-cc-dd-ee-ff. ALG with AV/WCF.

ALG (Application Layer Gateway) - a mechanism to analyze traffic. Analyzed data protocols and take action based on the configured rules. ALG is determining by the desired configuration of the service (Service). Traffic that falls within the parameters of the service will be processed using the selected ALG.

Services. Determined by the IP-protocol and its parameters. For example, the http service is defining as the TCP destination port 80, and the SMTP service uses port 25. When installing the filter rules you can use the service object all_services, referring to all protocols, but in terms of security more efficient use of certain types of services.

Note: Http-all service does not include the DNS-protocol. Required for Web-surfing DNS-protocol part of the service dns-all, which can add to the group service http-all and bind with IP-rules.

Schedules. Schedule lets you apply the rules only at certain times. Authentication Objects. Specifies the user authentication and gateways using

Pre-shared-key certificates and X.509.

7.2.2 Rules Creating

Section Rules (Rules) is designing to create a list of rules. A rule consists of two parts: the filter parameters and the actions to be taken after the filtration. As described above, the parameters of any rules NetDefendOS, including IP-rules include:

- Source Interface
- Source Network
- Destination Interface
- Destination Network
- Service.

Rules are the primary filter, which allows or denies a particular type of traffic through the firewall. Rules are also used to control the bandwidth limitation function bandwidth traffic passing through the interface WAN. Basic rule sets of NetDefendOS define security policies and are using to filter parameters. These include:

IP-rules that determine what traffic will pass through the NetDefend firewall and a traffic requires address translation.

Pipe-rules that define which traffic activates the bandwidth limit traffic Traffic Shaping.

Rules-based routing policies that determine the routing table for the traffic. **Authentication rules** that determine what traffic will activate the authentication process.

There are two ways to pass traffic through the firewall NetDefend:

□ Reject all traffic except authorized.

□ Allows all traffic except banned. The default is applied the first method.

To choose the desired action is performing when creating a rule in the Action field**: Drop –** Packets matching the rule with the action «Drop», will be immediately rejected. Information about these packages will be logged (log), if the Logging Settings page is enabled logging has.

Reject – Action «Reject» works just like the Drop. But other than that, the firewall sends a message back to the sender ICMP UNREACHABLE packet or if the package was rejected package TCP, Message TCP RST. Information about these packages will be logged (log), if the Logging Settings page is enabled logging has.

Allow – Packets matching the rule with the action «Allow», will be held later in the content control system, which will be remembered for a connection has been open. Information about open connections recorded in the connection table. Therefore, the rules for return traffic is not required, since the bandwidth of the open connections are automatically skipped, not getting to the validation rules. If the Logging Settings page logging is enabled check traffic to be recorded in the log relevant messages (log).

NAT – Rule with the action «NAT» dynamically translates addresses and "hides" the sender address. It is mainly using to hide the internal protected network addresses - all computers on a local network using a single external address.

Forward fast – Packets that match the rule with the action «Forward fast», passage permitted immediately. The firewall does not record a compound according to the rules in the table of connections, and thus does not track the connection context for these packets. This method works faster for protocols that do not use the connection. For protocols with a large volume of traffic over a single connection Allow the action faster.

SAT – Rule with the action «SAT» defines a static address translation from external to internal. The decision to allow traffic to pass adopted by other rules.

Option assignment:

Adrress Filter – Filter by source and destination addresses.

Source Interface – Specifies the interface from which the packet is receiving. Can be specified VPN-tunnel.

Source Network – Specifies a range of IP-addresses to be compared to the source address of the received packet.

Destination Interface – Specifies the interface that sends the received packet. Can be specified VPN-tunnel.

Destination Network – Specifies a range of IP-addresses to be compared to the destination address of the received packet.

With regard to the firewalls are two logical interface: **core** and **any**.

Core is in the "heart" of the firewall on the physical interface; all traffic is forwarding to the core interface to manage security policies.

Any - means all possible interfaces, including the core.

7.3 Methodical instructions and work order

Laboratory model description

A fragment of a telecommunication network consists of firewall that performs perimeter protection network. The list of equipment is presenting in Table 7.1, Topology - Fig. 7.1.

Table 7.1

Equipment (one work place):	
Switch L2	1 unit.
Work station	1 unit
Ethernet cable	3 units
Firewall DFL-810	1 unit

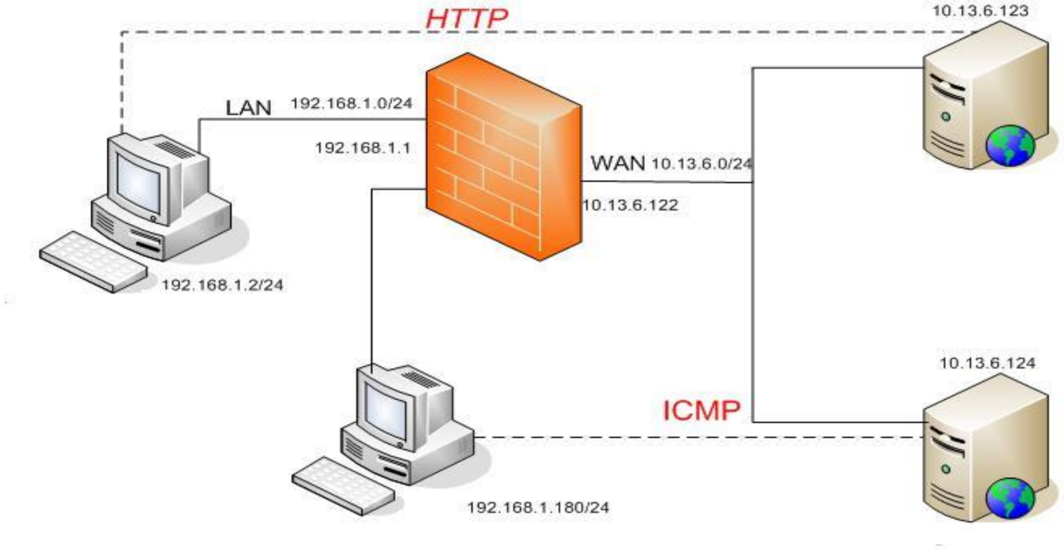
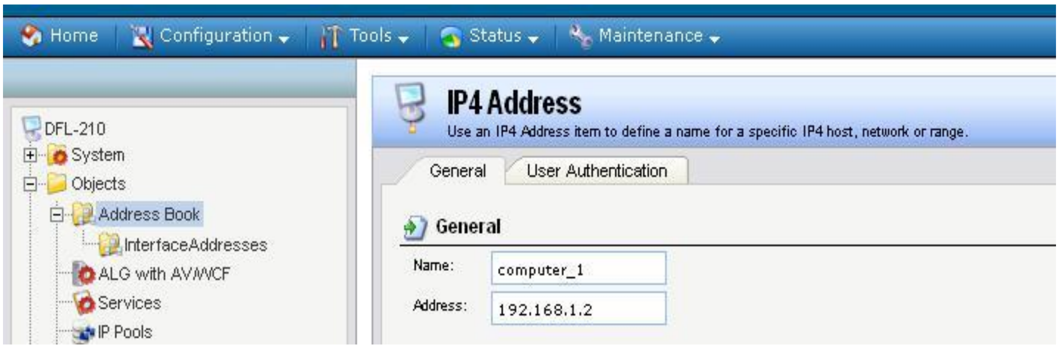


Figure 7.1 - Laboratory model scheme

7.3.1 Creating objects in the address book

Create an «IP-address" for Workstation 1 (192.168.1.2). Go to the folder

Objects→Address Book→Add→IP4 Address. In the tab *General* input next parameters:



IP4 Address

Use an IP4 Address item to define a name for a specific IP4 host, network or range.

General

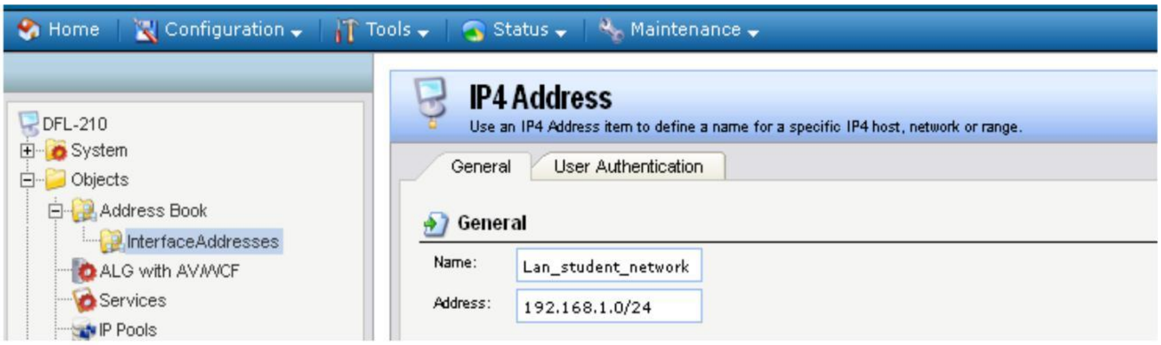
Name: computer_1

Address: 192.168.1.2

Repeat for Workstation 2 (192.168.1.180)

Create an “IP-address” of the network for the LAN interface: *Objects→Address Book→ InterfaceAddresses→Add →IP4 Address.* In the tab *General* input next parameters:

Create an “IP-address” of the network for the WAN interface: *Objects→Address Book→ InterfaceAddresses→Add →IP4 Address.* In the tab *General* input next parameters:



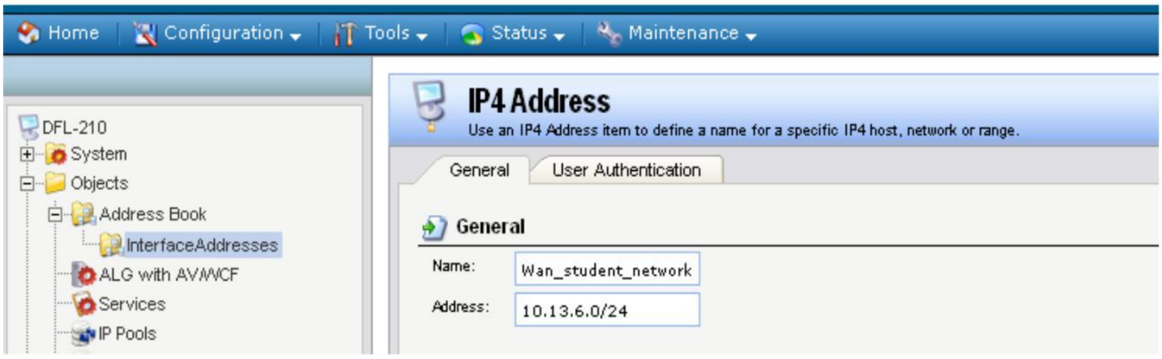
IP4 Address

Use an IP4 Address item to define a name for a specific IP4 host, network or range.

General

Name: Lan_student_network

Address: 192.168.1.0/24



IP4 Address

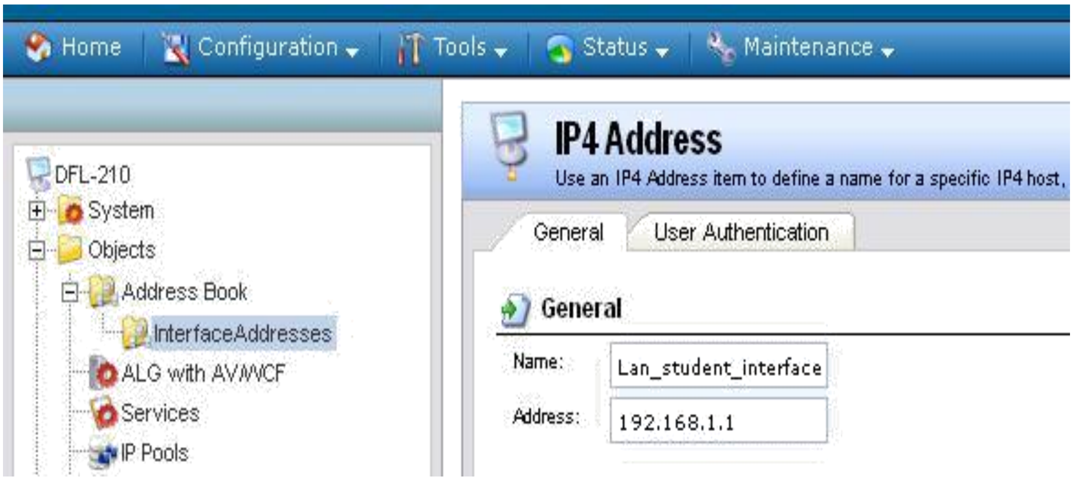
Use an IP4 Address item to define a name for a specific IP4 host, network or range.

General

Name: Wan_student_network

Address: 10.13.6.0/24

Create an “IP-address” of the network for the LAN interface: *Objects→Address Book→ InterfaceAddresses→Add →IP4 Address.* In the tab General input next parameters:



IP4 Address

Use an IP4 Address item to define a name for a specific IP4 host,

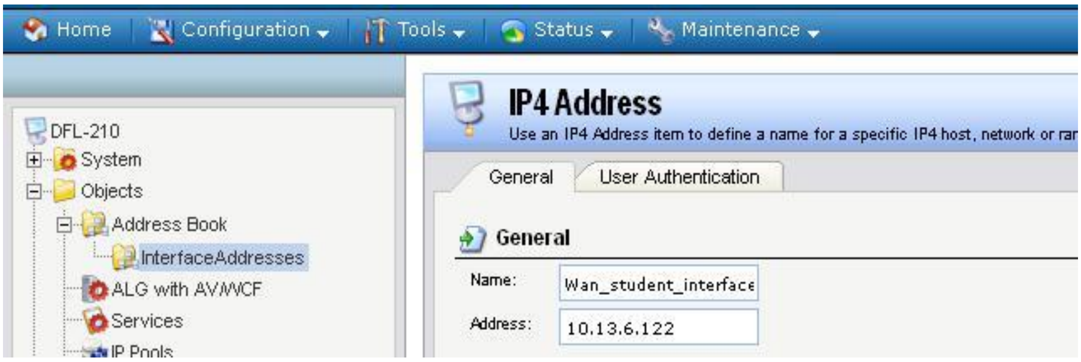
General

Name: Lan_student_interface

Address: 192.168.1.1

Create an “IP-address” of the network for the WAN interface: *Objects→Address Book→ InterfaceAddresses→Add →IP4 Address.* In the tab

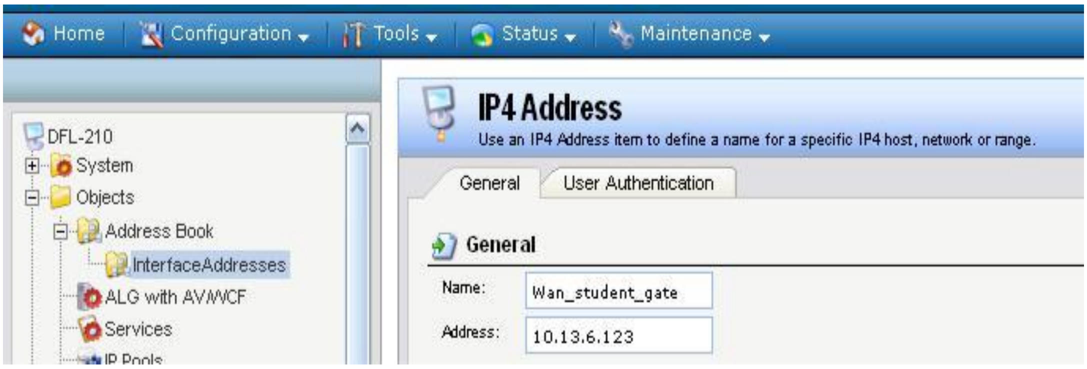
General input next parameters:



Name: Wan_student_interface

Address: 10.13.6.122

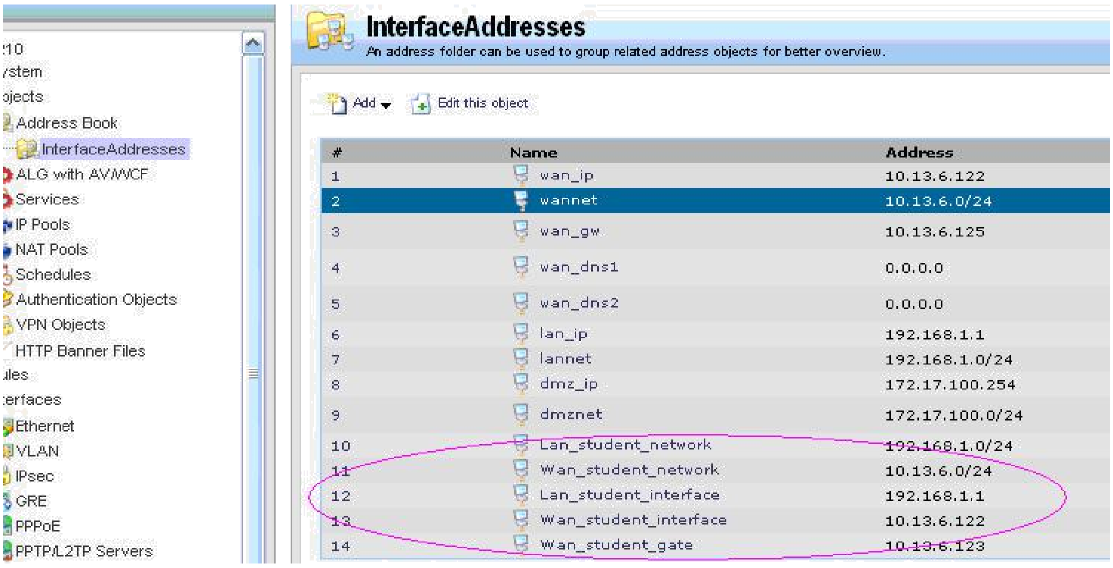
Create an gateway's "IP-address" (IP-address of the Web server) for the WAN interface: *Objects→Address Book→ InterfaceAddresses→Add →IP4 Address*. In the tab General input next parameters:



Name: Wan_student_gate

Address: 10.13.6.123

Go to the folder *Objects → Address Book → InterfaceAddresses* and make sure that the objects have been created:

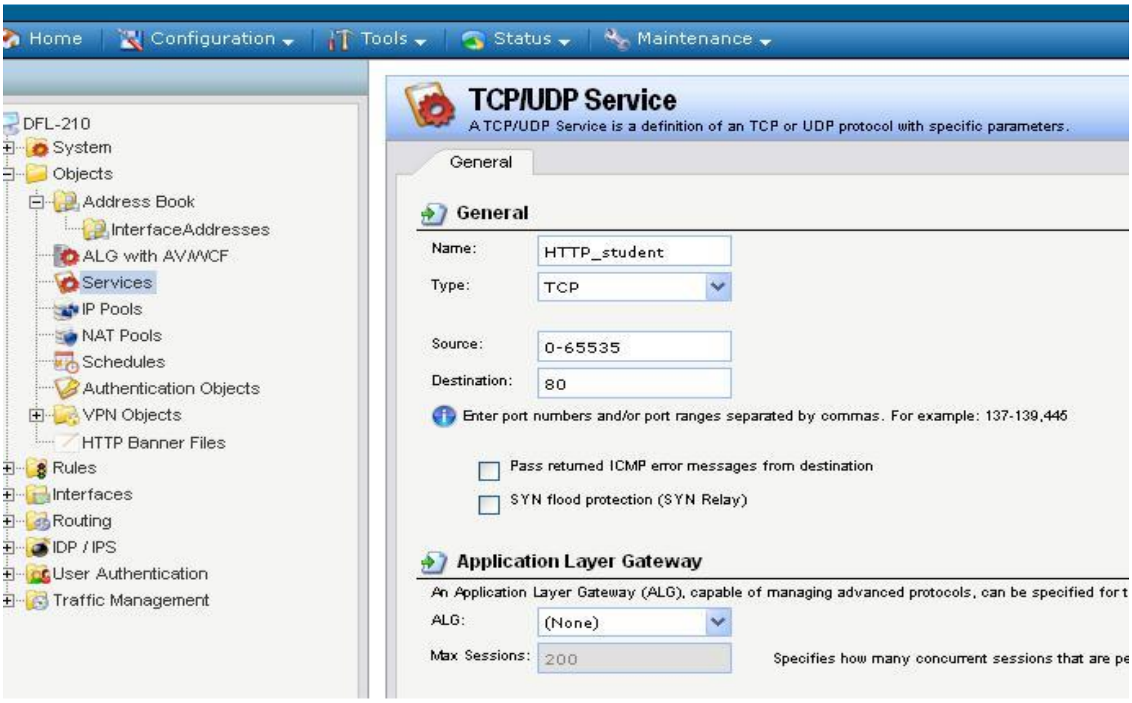


#	Name	Address
1	wan_ip	10.13.6.122
2	wannet	10.13.6.0/24
3	wan_gw	10.13.6.125
4	wan_dns1	0.0.0.0
5	wan_dns2	0.0.0.0
6	lan_ip	192.168.1.1
7	lannet	192.168.1.0/24
8	dmz_ip	172.17.100.254
9	dmznet	172.17.100.0/24
10	Lan_student_network	192.168.1.0/24
11	Wan_student_network	10.13.6.0/24
12	Lan_student_interface	192.168.1.1
13	Wan_student_interface	10.13.6.122
14	Wan_student_gate	10.13.6.123

7.3.2 Creating objects-services based on TCP and UDP

Create a TCP- service for HTTP.

Go to the folder *Objects→Services→Add→TCP/UDP Service*. In the tab General input next parameters:



TCP/UDP Service

A TCP/UDP Service is a definition of an TCP or UDP protocol with specific parameters.

General

Name: HTTP_student

Type: TCP

Source: 0-65535

Destination: 80

Enter port numbers and/or port ranges separated by commas. For example: 137-139,445

□ Pass returned ICMP error messages from destination

□ SYN flood protection (SYN Relay)

Application Layer Gateway

An Application Layer Gateway (ALG), capable of managing advanced protocols, can be specified for t

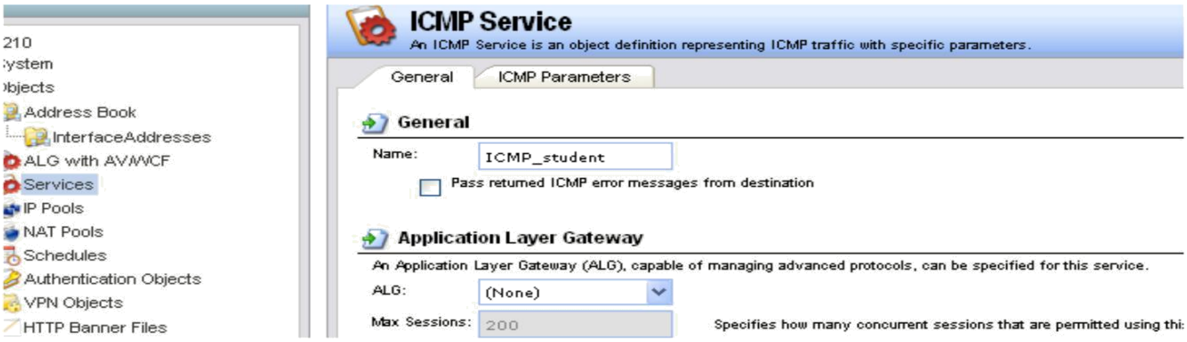
ALG: (None)

Max Sessions: 200 Specifies how many concurrent sessions that are pe

7.3.3 Creating objects based on ICMP

Creating ICMP service.

Go to the folder *Objects→Services→Add→ICMP Service.* In the tab General input next parameters:



ICMP Service

An ICMP Service is an object definition representing ICMP traffic with specific parameters.

General

Name: ICMP_student

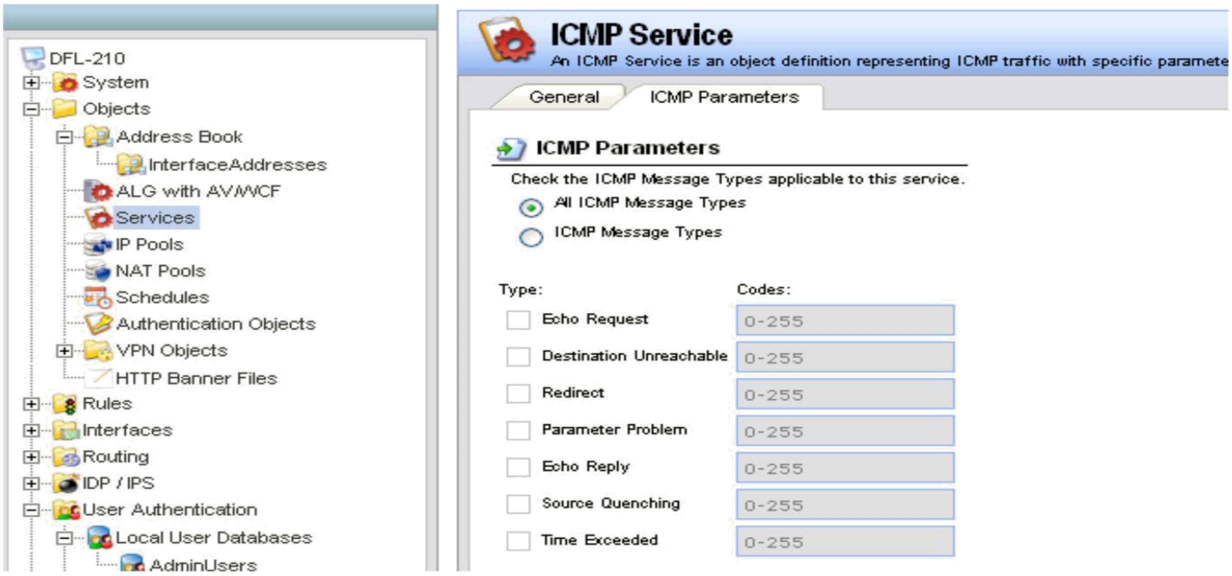
□ Pass returned ICMP error messages from destination

Application Layer Gateway

An Application Layer Gateway (ALG), capable of managing advanced protocols, can be specified for this service.

ALG: (None)

Max Sessions: 200 Specifies how many concurrent sessions that are permitted using thi



ICMP Service

An ICMP Service is an object definition representing ICMP traffic with specific paramete

ICMP Parameters

Check the ICMP Message Types applicable to this service.

● All ICMP Message Types

○ ICMP Message Types

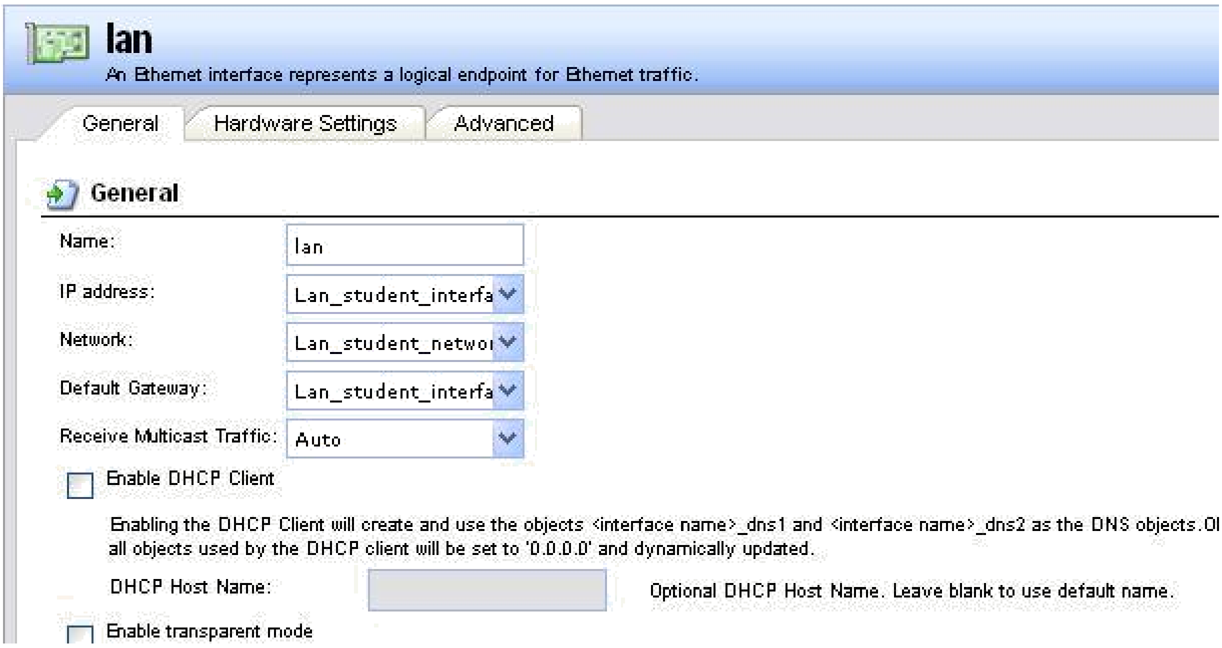
Type:	Codes:
□ Echo Request	0-255
□ Destination Unreachable	0-255
□ Redirect	0-255
□ Parameter Problem	0-255
□ Echo Reply	0-255
□ Source Quenching	0-255
□ Time Exceeded	0-255

7.3.4 Snapping address book objects to the interface

Note: *If you change the IP-addresses on the LAN interface need to go to DFL on a new IP-address within 30 seconds (the time period set by default, you can change it in the folder System → Remote Management → Advanced Settings →Validation Timeout). Otherwise, the LAN settings remain unchanged.*

Go to the folder *Objects→Interfaces→Ethernet.*

Chose the ***lan***-interface. In the tab General input next parameters:


lan

An Ethernet interface represents a logical endpoint for Ethernet traffic.

General

Name: lan

IP address: Lan_student_interfa

Network: Lan_student_networ

Default Gateway: Lan_student_interfa

Receive Multicast Traffic: Auto

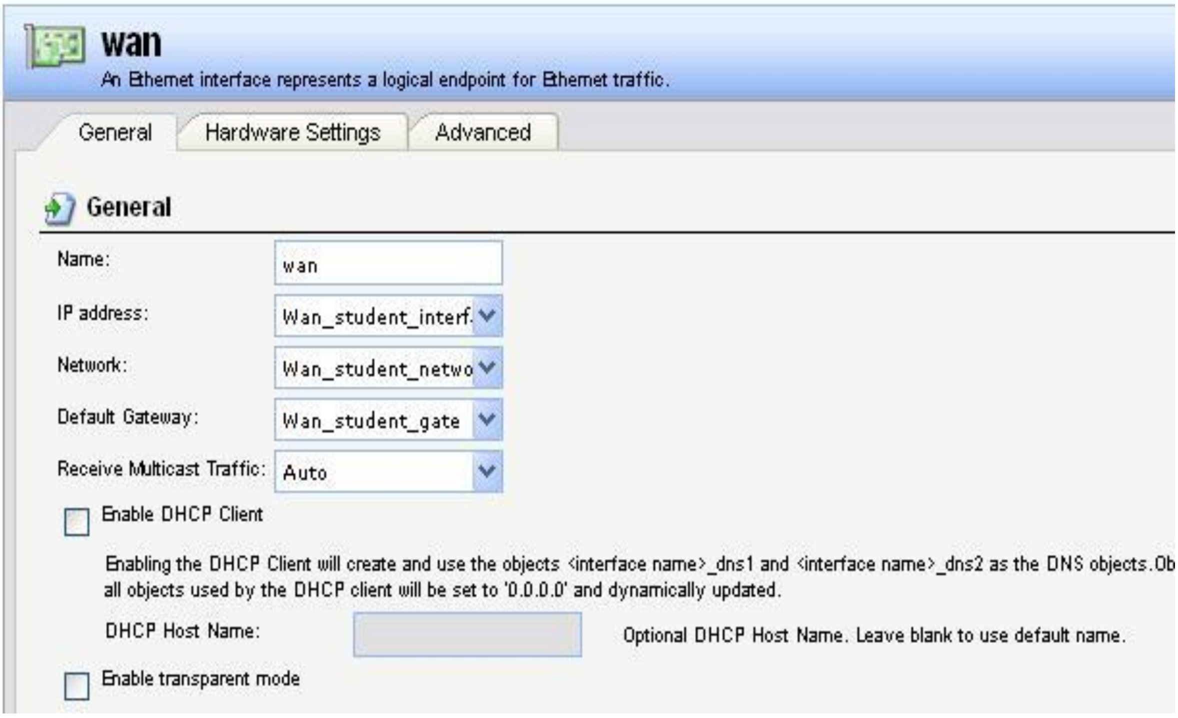
□ Enable DHCP Client

Enabling the DHCP Client will create and use the objects <interface name>_dns1 and <interface name>_dns2 as the DNS objects.Ol all objects used by the DHCP client will be set to '0.0.0.0' and dynamically updated.

DHCP Host Name: Optional DHCP Host Name. Leave blank to use default name.

□ Enable transparent mode

Chose the ***wan***-interface. In the tab General input next parameters:


wan

An Ethernet interface represents a logical endpoint for Ethernet traffic.

General

Name: wan

IP address: Wan_student_interf.

Network: Wan_student_netwo

Default Gateway: Wan_student_gate

Receive Multicast Traffic: Auto

□ Enable DHCP Client

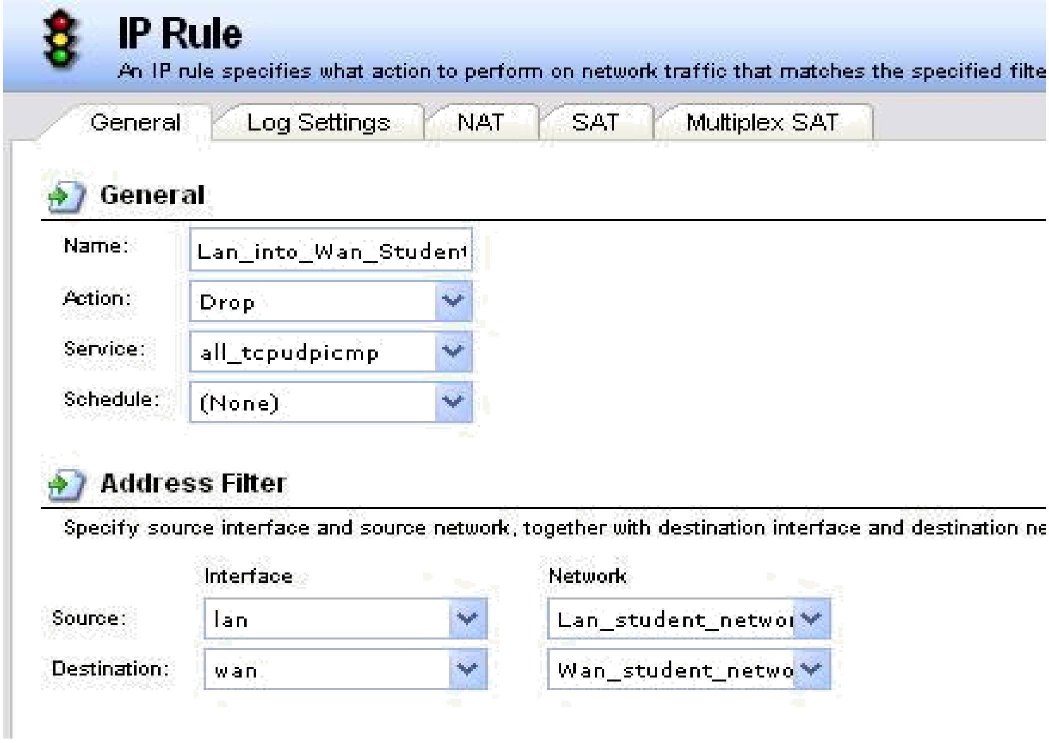
Enabling the DHCP Client will create and use the objects <interface name>_dns1 and <interface name>_dns2 as the DNS objects.Ob all objects used by the DHCP client will be set to '0.0.0.0' and dynamically updated.

DHCP Host Name: Optional DHCP Host Name. Leave blank to use default name.

□ Enable transparent mode

7.3.5 Filtering traffic with IP Rule

Create IP Rule *Lan_into_Wan_Student_drop* to prohibit the passage of any type of traffic in Lan_student_network Wan_student_network. On the *General* tab, enter:



IP Rule

An IP rule specifies what action to perform on network traffic that matches the specified filte

General

Name: Lan_into_Wan_Student

Action: Drop

Service: all_tcpudpicmp

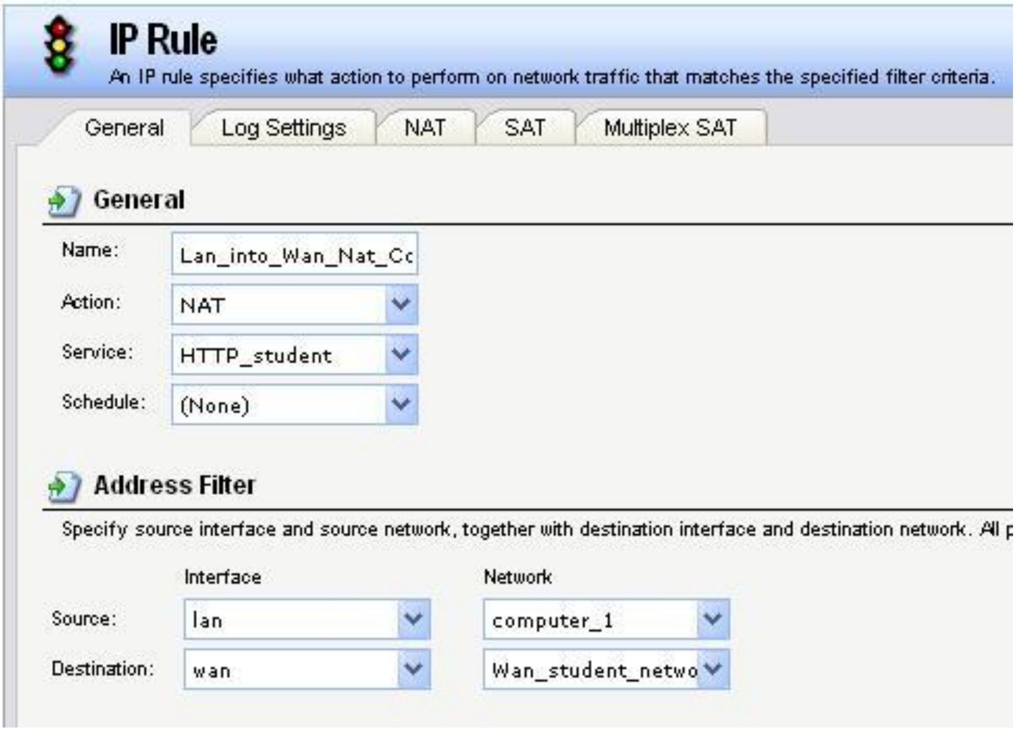
Schedule: (None)

Address Filter

Specify source interface and source network, together with destination interface and destination ne

	Interface	Network
Source:	lan	Lan_student_netwoı
Destination:	wan	Wan_student_netwo

Create IP Rule *Lan_into_Wan_Nat_Computer_1* to allow traffic to pass only the HTTP protocol from the Workstation 1 Wan_student_network. On the tab *General*, type:



IP Rule

An IP rule specifies what action to perform on network traffic that matches the specified filter criteria.

General

Name: Lan_into_Wan_Nat_Cc

Action: NAT

Service: HTTP_student

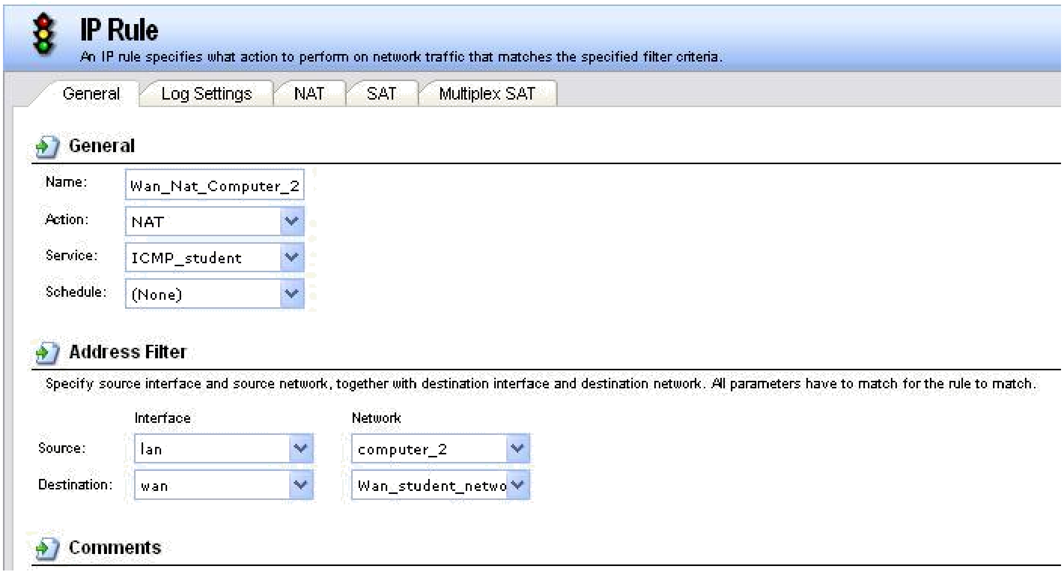
Schedule: (None)

Address Filter

Specify source interface and source network, together with destination interface and destination network. All p

	Interface	Network
Source:	lan	computer_1
Destination:	wan	Wan_student_netwo

Create IP Rule *Lan_into_Wan_Nat_Computer_2* to allow traffic to pass only an ICMP from Workstation 2 Wan_student_network. On the General tab, enter:



IP Rule

An IP rule specifies what action to perform on network traffic that matches the specified filter criteria.

General

Name: Wan_Nat_Computer_2

Action: NAT

Service: ICMP_student

Schedule: (None)

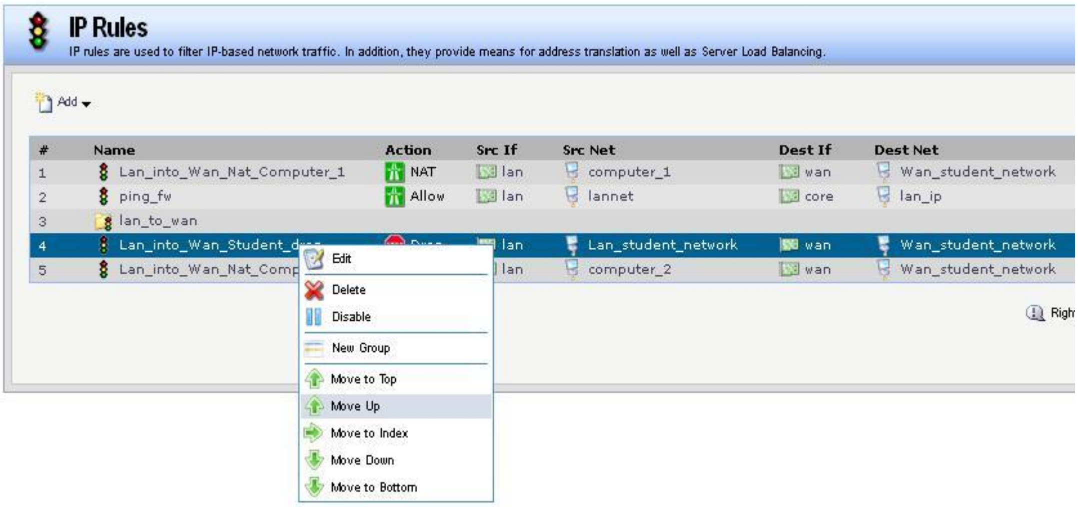
Address Filter

Specify source interface and source network, together with destination interface and destination network. All parameters have to match for the rule to match.

	Interface	Network
Source:	lan	computer_2
Destination:	wan	Wan_student_netwo

Comments

Arrange the rules of priority: first, the rules allow the traffic. Click on the desired line, right-click, and select the appropriate action:



IP Rules

IP rules are used to filter IP-based network traffic. In addition, they provide means for address translation as well as Server Load Balancing.

#	Name	Action	Src If	Src Net	Dest If	Dest Net
1	Lan_into_Wan_Nat_Computer_1	NAT	lan	computer_1	wan	Wan_student_network
2	ping_fw	Allow	lan	lannet	core	lan_ip
3	lan_to_wan					
4	Lan_into_Wan_Student_d		lan	Lan_student_network	wan	Wan_student_network
5	Lan_into_Wan_Nat_Comp		lan	computer_2	wan	Wan_student_network

<u>Note:</u> In order for changes to the firewall configuration to take effect, it is not necessary to save and activate: go to the menu Configuration→Save and Active.

7.4 Tasks for research

From workstation 1 try to come to your web server via a browser: in with address bar of your browser type in IP-address of the web server1 10.13.6.123.

What do you see in the browser window? Why?

With Workstation 1 try to ping a web server1 command «ping 10.13.6.123». What you see on the command line? Why?

With Workstation 2 try to ping a web server2 command «ping 10.13.6.124» . What you see on the command line? Why?

From Workstation 2 try to enter to a web server via a browser: in with address bar of your browser type in IP-address of the web server1 10.13.6.124.What do you see in the browser window? Why?

The list of rules put the highest priority rule banning the passage of traffic. From Workstation 1 try to enter to a web server via a browser: in with address bar of your browser type in IP-address of the web server1 10.13.6.123. What do you see in the browser window? Why?

With Workstation 2 try to ping a web server2 command «ping 10.13.6.124» . What you see on the command line? Why?

7.5 Contents of report

1. Report on the implementation of laboratory work should include the following items:
2. The theme and purpose of the laboratory work.
3. Block diagram of the network with the designation of ports, IP address, network mask interface of workstation, firewall and switch.
4. Order of performance laboratory work (sequence of input commands with the relevant explanations).
5. Graphical results.
6. The analysis and conclusions about laboratory work implementation.

8 ANALYSIS OF NAT ORGANISATION METHODS (STATIC, ADDRESS POOL)

8.1 Purpose

To cofigurare network fragment using routers. To obtaine experience of NAT configuration on routers and firewalls.

8.2 Brief description of NAT (Network Address Translation) technology

Network Address Translation allows a single device, such as a router, to act as an agent between the Internet (or "public network") and a local (or "private") network. This means that only a single, unique IP address is required to represent an entire group of computers. The NAT is described in RFC 1631, RFC 3022. Network Address Translation is used by a device (firewall, router or computer that sits between an internal network and the rest of the world. NAT has many forms and can work in several ways:

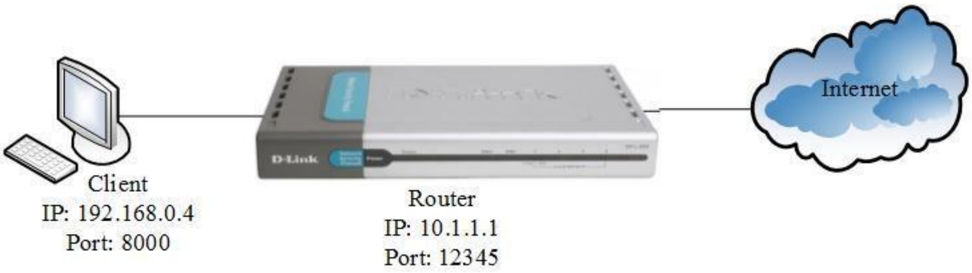


Figure 8.1 - Full Cone NAT implementation

In static NAT, the computer with the IP address of 192.168.32.10 will always translate to 213.18.123.110**.**

- **Static NAT -** Mapping an unregistered IP address to a registered IP address on a one-to-one basis. Particularly useful when a device needs to be accessible from outside the network.

In dynamic NAT, the computer with the IP address 192.168.32.10 will translate to the first available address in the range from 213.18.123.100 to 213.18.123.150.

 Dynamic NAT - Maps an unregistered IP address to a registered IP address from a group of registered IP addresses.

 Overloading - A form of dynamic NAT that maps multiple unregistered IP addresses to a single registered IP address by using different ports. This is known also as PAT (Port Address Translation), single address NAT or port-level multiplexed NAT.

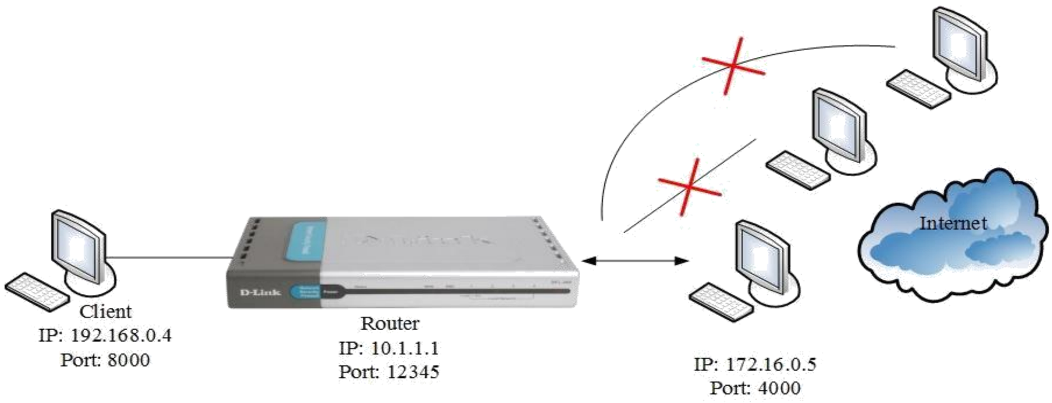


Figure 8.2 - Restricted Cone NAT implementation

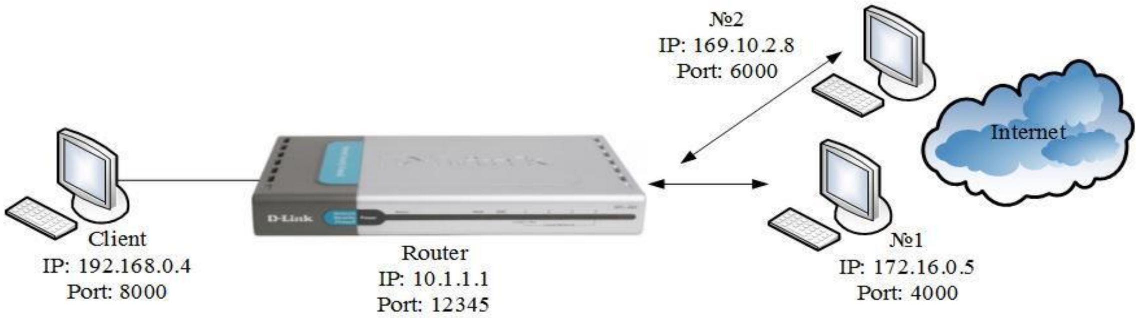


Figure 8.3 - Symmetric NAT implementation

In overloading, each computer on the private network is translated to the same IP address (213.18.123.100), but with a different port number assignment.

Overlapping - When the IP addresses used on your internal network are registered IP addresses in use on another network, the router must maintain a lookup table of these addresses so that it can intercept them and replace them with registered unique IP addresses.

The internal network is usually a **LAN (Local Area Network)**, commonly referred to as the **stub domain**. A stub domain is a LAN that uses IP addresses internally. Most of the network traffic in a stub domain is local, so it doesn't travel outside the internal network. A stub domain can include both registered and unregistered IP addresses. Of course, any computers that use unregistered IP addresses must use Network Address Translation to communicate with the rest of the world.

NAT performs three important functions.

1. Allows you to save IP-addresses, translating several internal IP-addresses to one external public IP-address (or more, but fewer than internal). According to this principle, most built networks in the world: a small area of your home network provider or local office is allocated 1 public (external) IP-address, followed by work and access interfaces with private (internal) IP-address.

2. Allows you to prevent or limit the circulation outside the internal hosts, leaving the possibility of treatment of internal to external network. When you initiate a connection from inside the network created broadcast.

Response packets coming from the outside, corresponding to the new translation and therefore skipped. If the packets coming from the external network, the corresponding translation does not exist (and it can be created at the initiation of the compound or static), they are not skipped.

However, it should also mention the disadvantages of this technology:

1. Not all protocols can “overcome” NAT. Some fail to work if the path between the communicating hosts have address translation. Certain firewalls to broadcast IP-address can correct this deficiency, appropriately, replace the IP-addresses are not titles only IP, but also at higher levels (eg, protocol commands FTP).

2. Due to the address translation, "many to one" creates additional complexity to the identification of users and the need to keep the complete logs broadcasts.

3. DoS attacks from the node performing NAT. If NAT is used to connect many users to the same service, it can cause the illusion of DoS-attack on the service (many successful and unsuccessful attempts). For example, an excess amount of ICQ users behind NAT causes a problem connecting to the server for some users due to overspeed connections.

8.3 Methodical instructions and work order

Laboratory model description

A fragment of a telecommunication network consists of a firewall, which performs defense of network perimeter. The list of equipment is presenting in Table. 8.1, Topology - Fig. 8.4.

Table 8.1

Equipment (one work place):	
Firewall DFL-810	1 unit
Workstation	2 unit
Ethernet cable	3 unit
DNS-server	1 unit
	Trafficgeneration
	program iperf

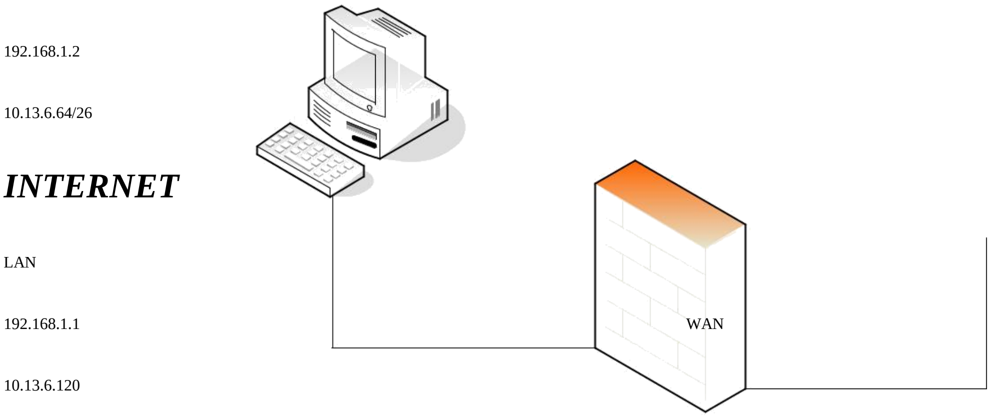
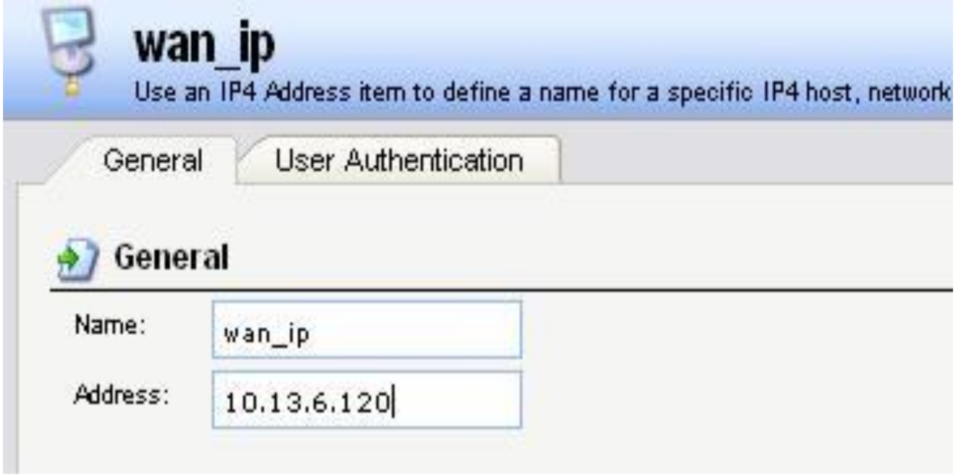


Figure 8.4 - Scheme of network fragment

8.3.1 A simple NAT configuration

Go to the folder *Interfaces → Ethernet → wan*. Deselect *Enable DHCP Client*. Go to the folder *Objects → Address Book → InterfaceAddresses → wan_ip*.

Enter the following parameters:



wan_ip

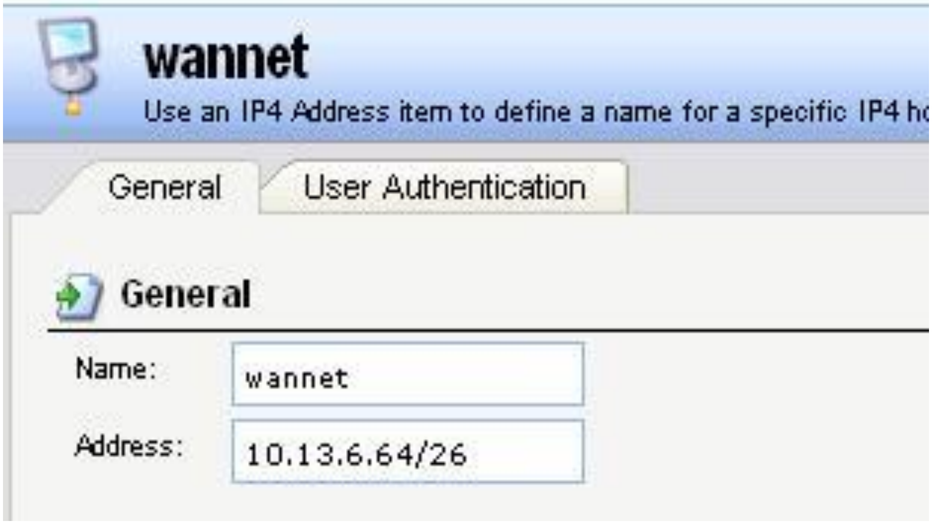
Use an IP4 Address item to define a name for a specific IP4 host, network

General

Name: wan_ip

Address: 10.13.6.120

Go to the folder *Objects→Address Book→InterfaceAddresses→wannet.* Enter the following parameters:



wannet

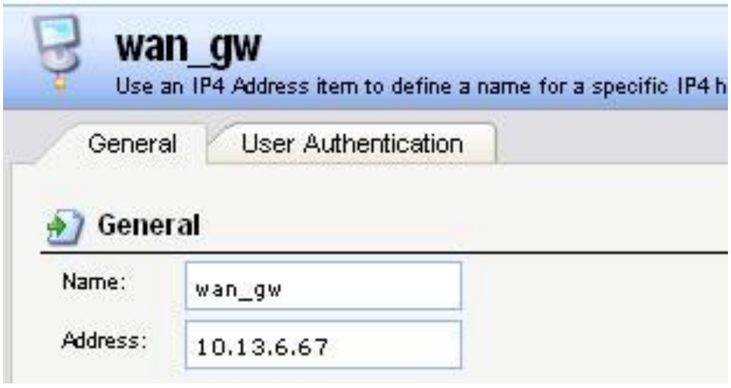
Use an IP4 Address item to define a name for a specific IP4 h

General

Name: wannet

Address: 10.13.6.64/26

Go to the folder *Objects→Address Book→InterfaceAddresses→wan_gw.* Enter the following parameters:



wan_gw

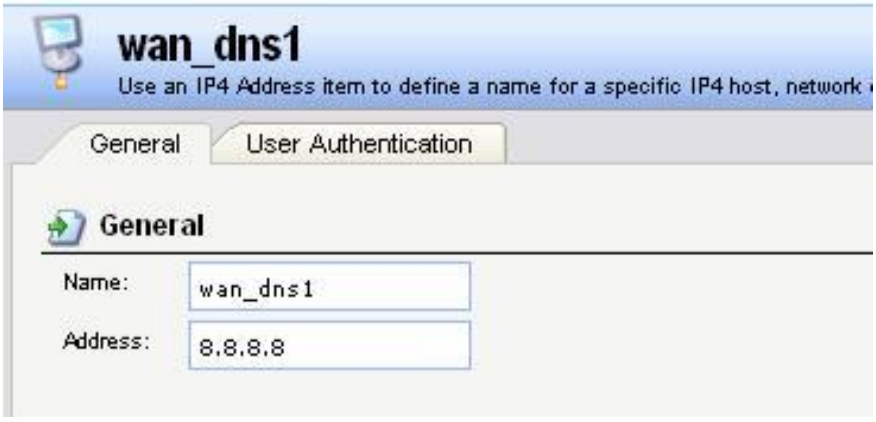
Use an IP4 Address item to define a name for a specific IP4 h

Name: wan_gw

Address: 10.13.6.67

Go to the folder *Objects→Address Book→InterfaceAddresses→wan_dns1.*

Type the next parameters:



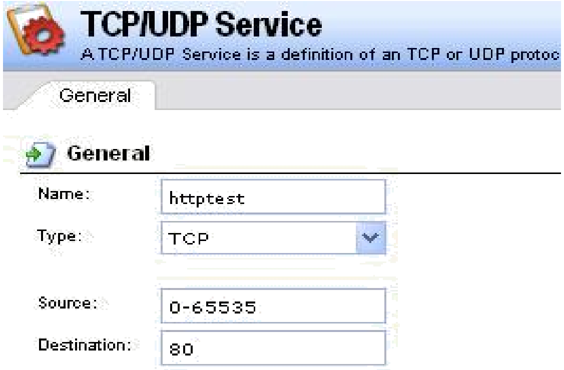
wan_dns1

Use an IP4 Address item to define a name for a specific IP4 host, network

Name: wan_dns1

Address: 8.8.8.8

Go to the folder *Objects→Services→Add→TCP/UDP Service.* Enter the following parameters:



TCP/UDP Service

A TCP/UDP Service is a definition of an TCP or UDP protoc

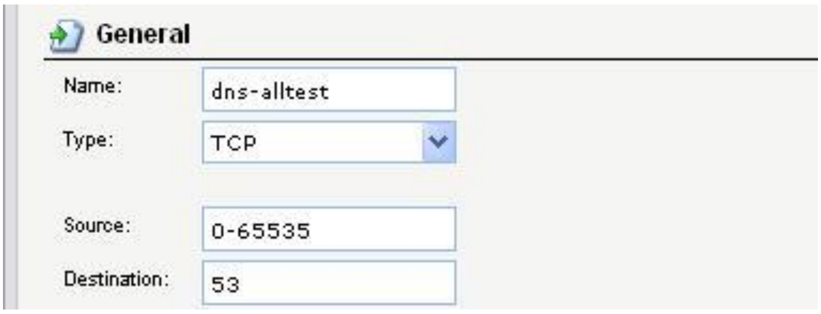
Name: httptest

Type: TCP

Source: 0-65535

Destination: 80

Go to the folder *Objects→Services→Add→TCP/UDP Service.* Enter the following parameters:



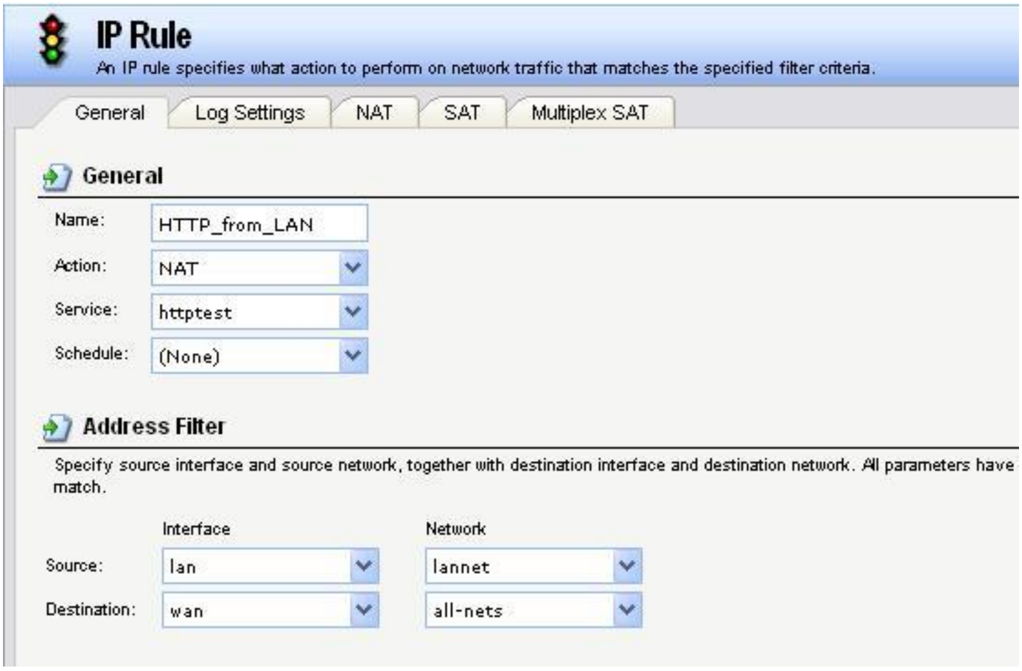
Name: dns-alltest

Type: TCP

Source: 0-65535

Destination: 53

Go to the folder *Rules→IPRules.* Create new IP Rule with NAT action. In the tab *General* enter:



IP Rule

An IP rule specifies what action to perform on network traffic that matches the specified filter criteria.

General

Name: HTTP_from_LAN

Action: NAT

Service: httptest

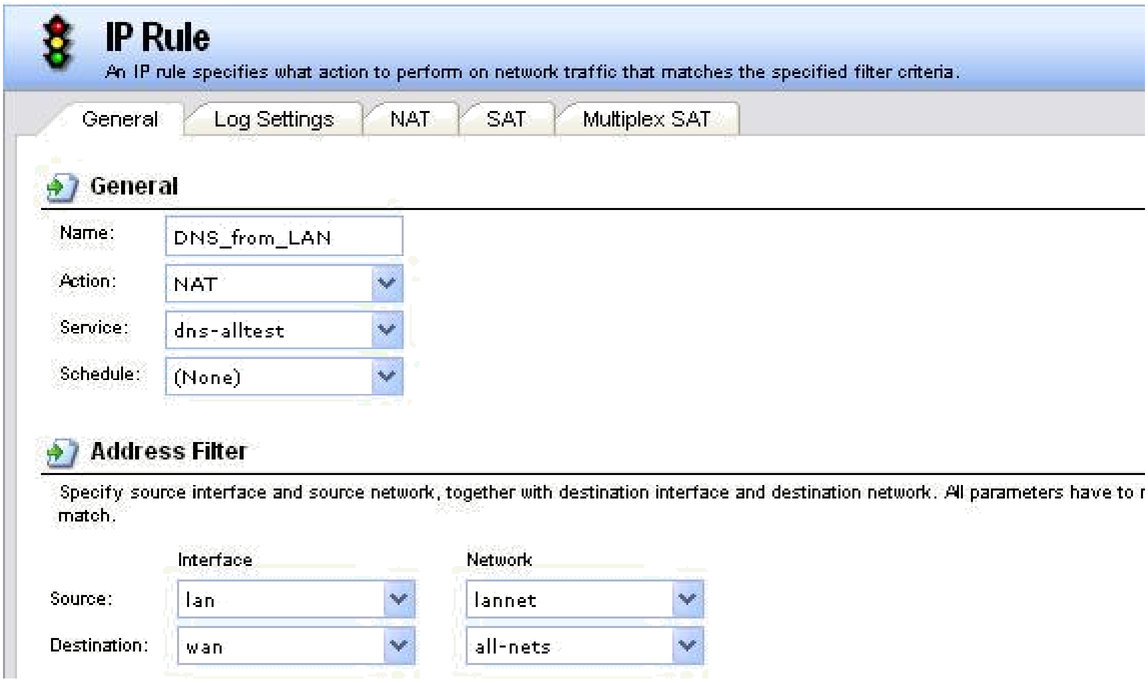
Schedule: (None)

Address Filter

Specify source interface and source network, together with destination interface and destination network. All parameters have match.

	Interface	Network
Source:	lan	lannet
Destination:	wan	all-nets

Create new IP Rule for DNS. In the tab *General* enter:



IP Rule

An IP rule specifies what action to perform on network traffic that matches the specified filter criteria.

General

Name: DNS_from_LAN

Action: NAT

Service: dns-alltest

Schedule: (None)

Address Filter

Specify source interface and source network, together with destination interface and destination network. All parameters have to r match.

	Interface	Network
Source:	lan	lannet
Destination:	wan	all-nets

Go to the Configuration menu and select Save and Activate.

<u>Task:</u>

Check the dynamic NAT firewall and computer connected to the ***lan***-based interface.

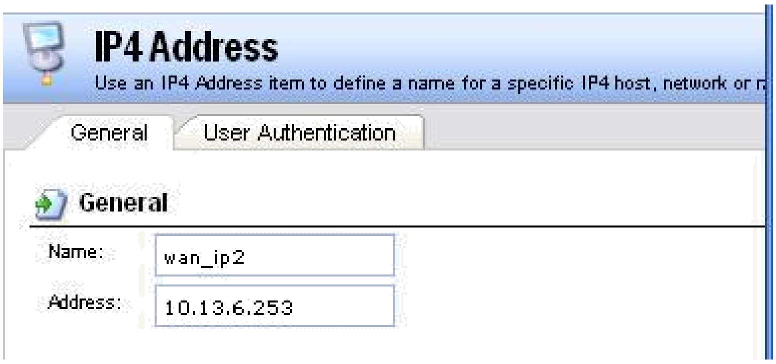
Go to menu *Status→Connections*, review in this folder the network address translation.

*1. In **CMD** OS Windows (computer in wan1net subnets with IP-adress 10.13.6.123) type the command:* C:\>iperf –s –t –p 5001

*2. In **CMD** OC Windows (computer in lannet subnet) type the command:* C:\>iperf – c 10.13.6.123 –t –p 5001

8.3.2 NAT Pool Configuration

Go to folder *Objects→Address Book→Add→IP4 Address.* In tab *General* enter:



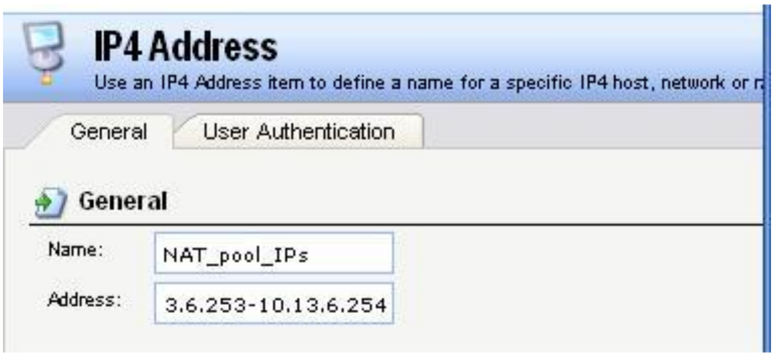
IP4 Address

Use an IP4 Address item to define a name for a specific IP4 host, network or r

Name: wan_ip2

Address: 10.13.6.253

Go to the folder *Objects→Address Book→Add→IP4 Address.* In tab *General* enter:



IP4 Address

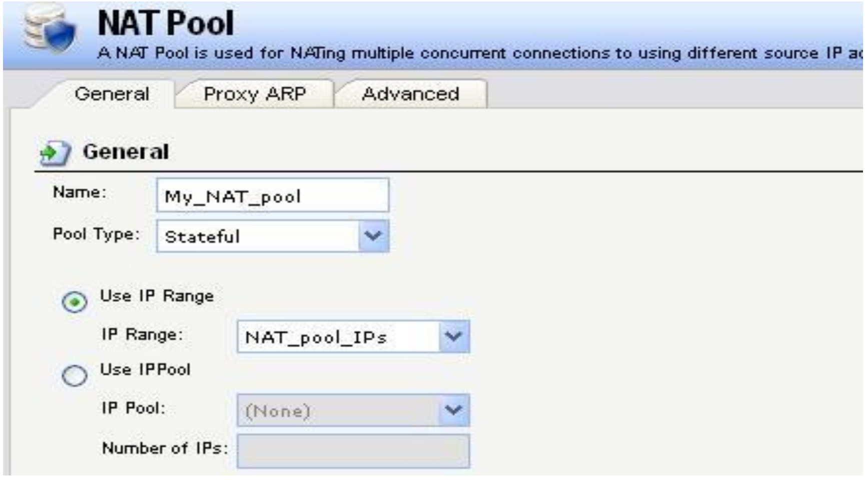
Use an IP4 Address item to define a name for a specific IP4 host, network or r

Name: NAT_pool_IPs

Address: 3.6.253-10.13.6.254

Address: 10.13.6.253-10.13.6.254

Go to the folder *Objects→NAT Pools→Add→NAT Pool.* In tab *General* enter:



NAT Pool

A NAT Pool is used for NATing multiple concurrent connections to using different source IP ac

Name: My_NAT_pool

Pool Type: Stateful

● Use IP Range

IP Range: NAT_pool_IPs

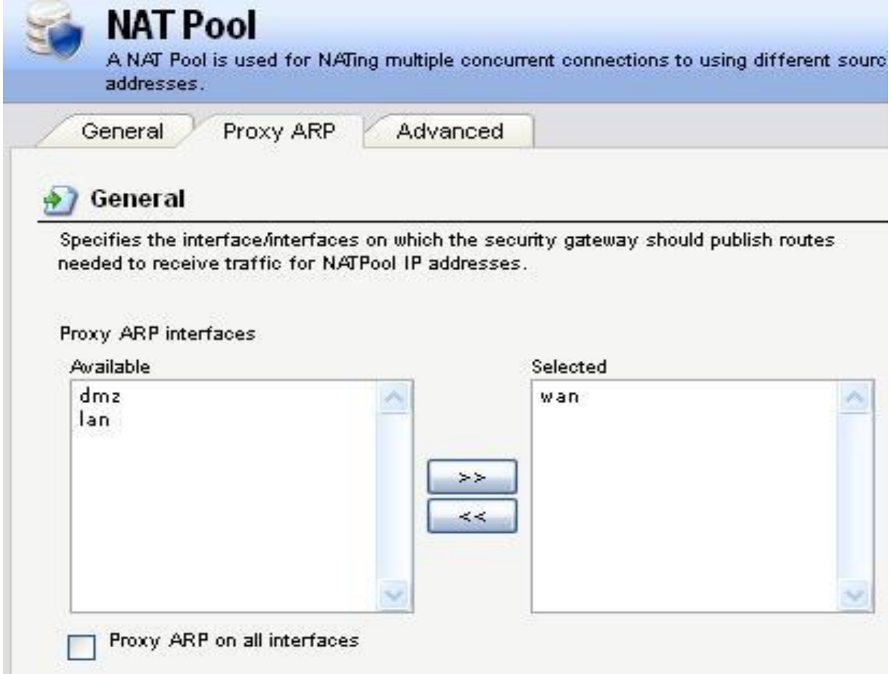
○ Use IPPool

IP Pool: (None)

Number of IPs:

There are three types of NAT-pools, each of which produces a distribution of new connections in different ways: Stateful (check connection status), Stateless (without checking the status of the connection), Fixed (Fixed). In appointing the external IP-addresses in the NAT-pool is not necessary to register them manually. You can select an object «IP-pool" system NetDefendOS.

In the folder *Proxy ARP* ***wan*** remove in Selected



NAT Pool

A NAT Pool is used for NATing multiple concurrent connections to using different sourc addresses.

General

Specifies the interface/interfaces on which the security gateway should publish routes needed to receive traffic for NATPool IP addresses.

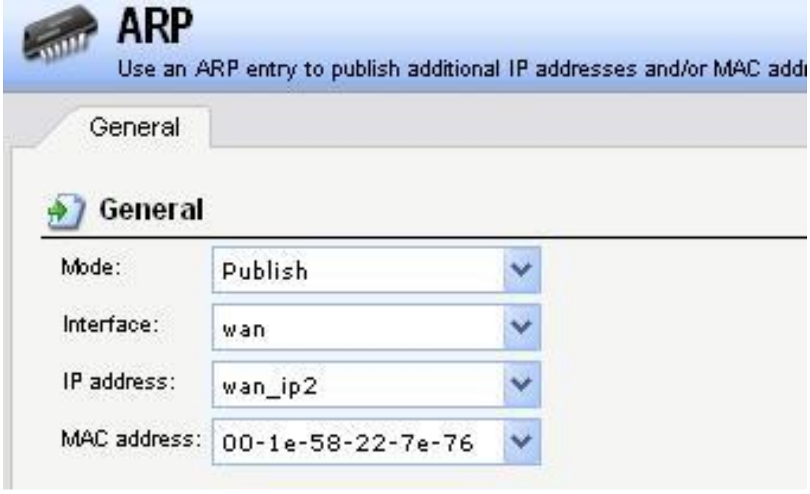
Proxy ARP interfaces

Available: dmz, lan

Selected: wan

□ Proxy ARP on all interfaces

Go to the folder *Interfaces→ARP→Add→ARP.* In tab *General* enter:



ARP

Use an ARP entry to publish additional IP addresses and/or MAC addı

General

Mode: Publish

Interface: wan

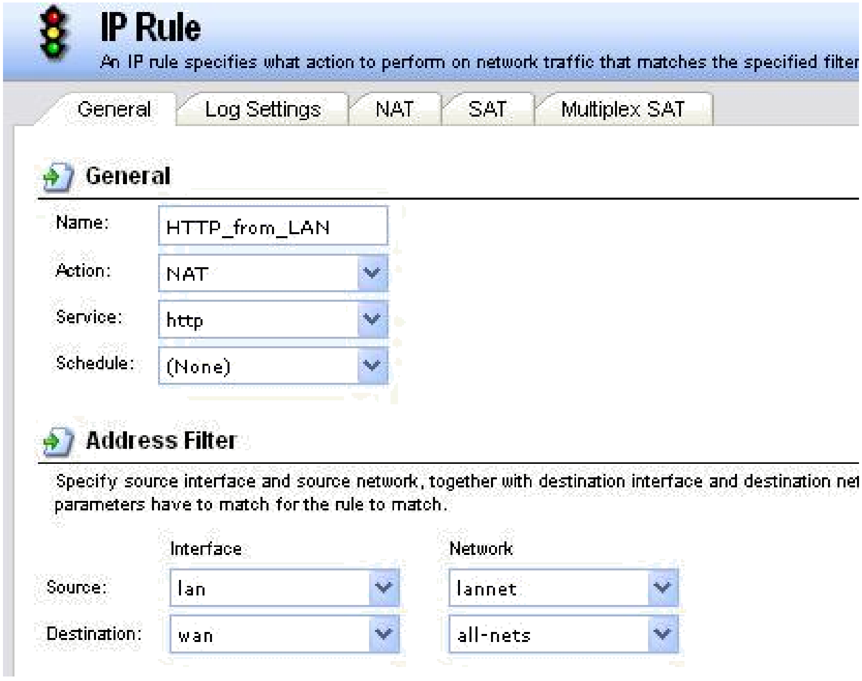
IP address: wan_ip2

MAC address: 00-1e-58-22-7e-76

<u>*Note:*</u> *Enter the MAC address of the interface for which you are setting the second IP-addresses*

Go to folder *Rules→IPRules.* Create new IP Rule with NAT action. In the tab

General enter:



IP Rule

An IP rule specifies what action to perform on network traffic that matches the specified filter

General

Name: HTTP_from_LAN

Action: NAT

Service: http

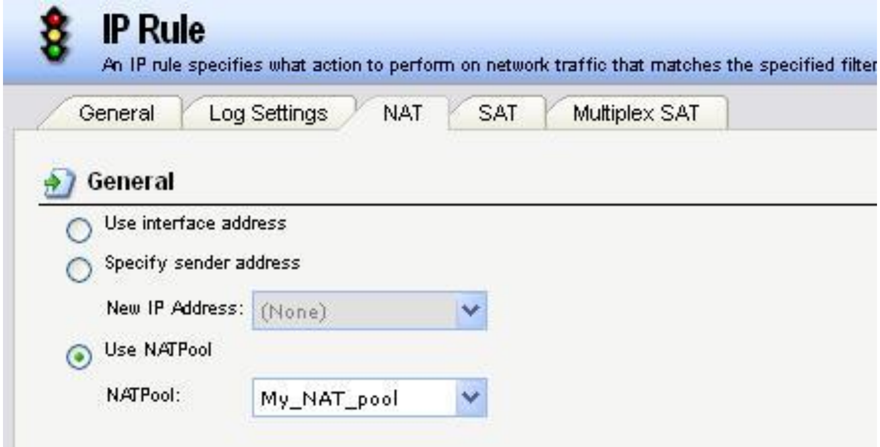
Schedule: (None)

Address Filter

Specify source interface and source network, together with destination interface and destination net parameters have to match for the rule to match.

	Interface	Network
Source:	lan	lannet
Destination:	wan	all-nets

In the folder *NAT* enter follow:



IP Rule

An IP rule specifies what action to perform on network traffic that matches the specified filter

General

○ Use interface address

○ Specify sender address

New IP Address: (None)

● Use NATPool

NATPool: My_NAT_pool

Go to *Configuration menu* and select *Save and Activate*.

Task:

Check the dynamic NAT firewall and computer connected to the lan-interface and computer connected wan-interface:

Go to menu *Status→Connections*, review the network address translation for the two public addresses – wan_ip и wan_ip2.

1. In **string CMD** OS Windows (computer in wan1net subnets with IP-adress 10.13.6.123) type the command:

```
C:\>iperf –s –t –p 80
```

2. In **CMD** OC Windows (computer in lannet subnet) type the command: C:\>iperf – c 10.13.6.123 –t –p 80

8.4 Contents of report

1. Report on the implementation of laboratory work should include the following items:

2. The theme and purpose of the laboratory work.

3. Block diagram of the network with the designation of ports, IP address, network mask interface of workstation, firewall and switch.

4. Order of performance laboratory work (sequence of input commands with the relevant explanations).

5. Graphical results.

6. The analysis and conclusions about laboratory work implemention.

LIST OF REFERENCES

1. N. Zhilkina. Exchangeable interfaces.// ―Network solutions magazine/ [Text] LAN‖. —2004 —№05

2. QoS in IP networks.: Vegesna Srinivas [Text]. – M.: ―Williams‖ publishing, 2003 —p.256

3. «SciVerse ScienceDirect». Electronic resource. Available at: http://www.sciencedirect.com

4. N. Olifer, V.Olifer Telecommunication technologies.: http://www.olifer.co.uk

5. Training materials of company D-Link. [Electronic resource]. Available at: ftp://ftp.dlink.ru/pub/Trainings/