

Презентация по лабораторной работе №5

Простые сети в GNS3. Анализ трафика

Галацан Николай

Российский университет дружбы народов, Москва, Россия

- Галацан Николай
- 1032225763
- уч. группа: НПИбд-01-22
- Факультет физико-математических и естественных наук
- Российский университет дружбы народов

Построение простейших моделей сети на базе коммутатора и маршрутизаторов FRR и VyOS в GNS3, анализ трафика посредством Wireshark.

Моделирование простейшей сети на базе коммутатора в GNS3

Выполнение лабораторной работы

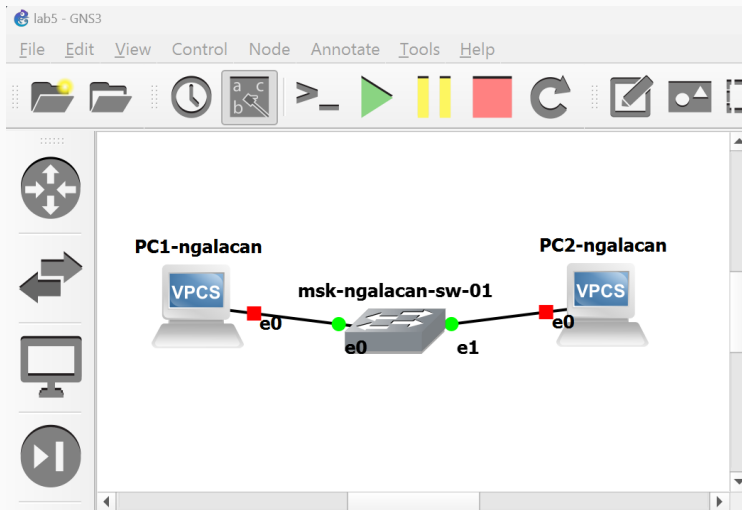
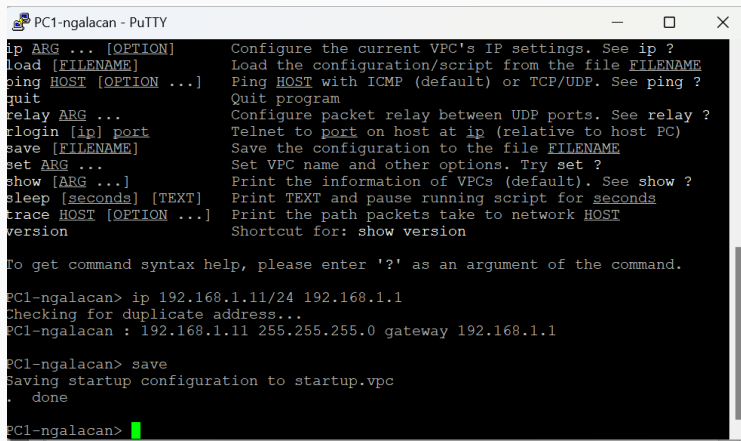


Рис. 1: Топология простейшей сети в GNS3

Выполнение лабораторной работы



```
PC1-ngalacan - PuTTY

ip ARG ... [OPTION]      Configure the current VPC's IP settings. See ip ?
load [FILENAME]          Load the configuration/script from the file FILENAME
ping HOST [OPTION ...]   Ping HOST with ICMP (default) or TCP/UDP. See ping ?
quit                     Quit program
relay ARG ...            Configure packet relay between UDP ports. See relay ?
rlogin [ip] port         Telnet to port on host at ip (relative to host PC)
save [FILENAME]          Save the configuration to the file FILENAME
set ARG ...              Set VPC name and other options. Try set ?
show [ARG ...]           Print the information of VPCs (default). See show ?
sleep [seconds] [TEXT]   Print TEXT and pause running script for seconds
trace HOST [OPTION ...]  Print the path packets take to network HOST
version                  Shortcut for: show version

To get command syntax help, please enter '?' as an argument of the command.

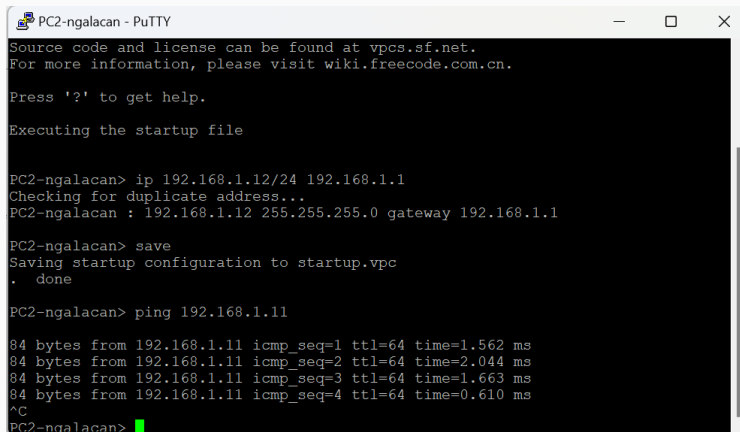
PC1-ngalacan> ip 192.168.1.11/24 192.168.1.1
Checking for duplicate address...
PC1-ngalacan : 192.168.1.11 255.255.255.0 gateway 192.168.1.1

PC1-ngalacan> save
Saving startup configuration to startup.vpc
. done

PC1-ngalacan> █
```

Рис. 2: Настройка IP-адресации на PC-1

Выполнение лабораторной работы



```
PC2-ngalacan - PuTTY
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

Executing the startup file

PC2-ngalacan> ip 192.168.1.12/24 192.168.1.1
Checking for duplicate address...
PC2-ngalacan : 192.168.1.12 255.255.255.0 gateway 192.168.1.1

PC2-ngalacan> save
Saving startup configuration to startup.vpc
. done

PC2-ngalacan> ping 192.168.1.11

84 bytes from 192.168.1.11 icmp_seq=1 ttl=64 time=1.562 ms
84 bytes from 192.168.1.11 icmp_seq=2 ttl=64 time=2.044 ms
84 bytes from 192.168.1.11 icmp_seq=3 ttl=64 time=1.663 ms
84 bytes from 192.168.1.11 icmp_seq=4 ttl=64 time=0.610 ms
^C
PC2-ngalacan>
```

Рис. 3: Проверка работоспособности сети с помощью ping

Анализ трафика в GNS3 посредством Wireshark

Выполнение лабораторной работы

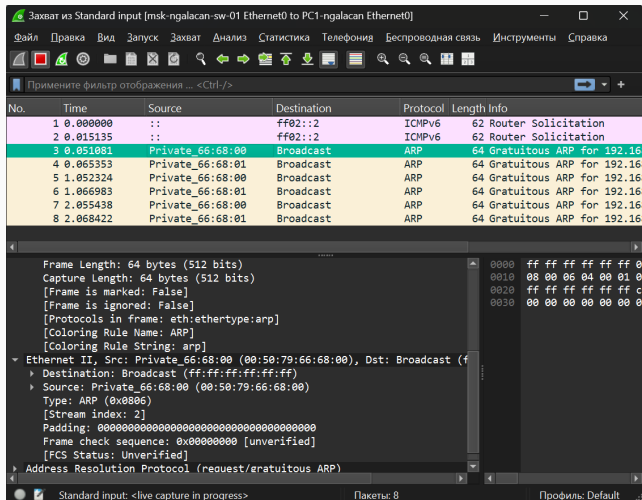


Рис. 4: Захват трафика между PC-1 и коммутатором: протокол ARP

Выполнение лабораторной работы

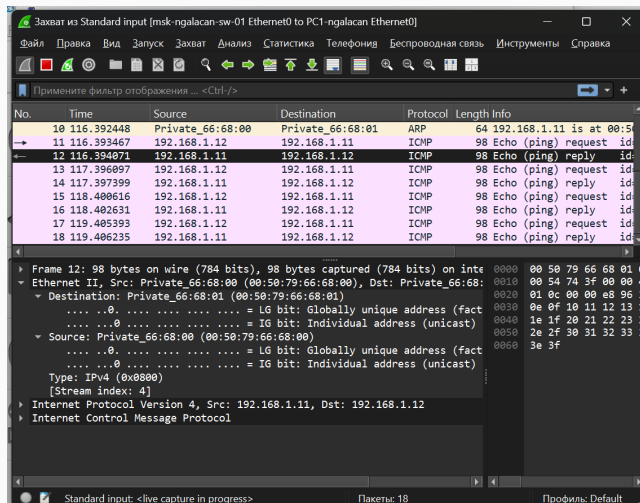


Рис. 5: Захват трафика между PC-1 и коммутатором: ICMP

Выполнение лабораторной работы

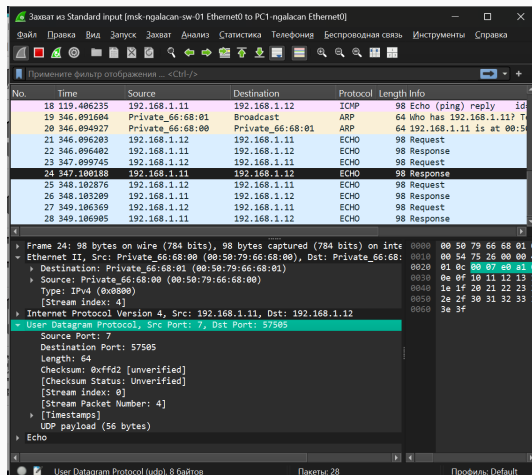


Рис. 6: Захват трафика между PC-1 и коммутатором: UDP

Выполнение лабораторной работы

The screenshot displays the Wireshark interface with a packet capture from 'Standard input [msk-ngalacan-sw-01 Ethernet0 to PC1-ngalacan Ethernet0]'. The packet list shows several TCP packets. Packet 61 is selected, showing details for an IP packet from 192.168.1.12 to 192.168.1.11, and a TCP segment with sequence number 57, acknowledgment number 1, and flags FIN, PSH, ACK. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
54	447.784397	192.168.1.11	192.168.1.12	TCP	54	7 → 28929 [FIN, ACK] Seq=58
55	447.787512	192.168.1.12	192.168.1.11	TCP	66	28929 → 7 [ACK] Seq=58
56	448.707944	192.168.1.12	192.168.1.11	TCP	74	[TCP Port numbers reused]
57	448.708205	192.168.1.11	192.168.1.12	TCP	54	7 → 28929 [SYN, ACK] Seq=58
58	448.710357	192.168.1.12	192.168.1.11	TCP	66	28929 → 7 [ACK] Seq=1
59	448.712063	192.168.1.12	192.168.1.11	ECHO	122	Request
60	448.712598	192.168.1.11	192.168.1.12	TCP	54	7 → 28929 [ACK] Seq=1
61	448.715502	192.168.1.12	192.168.1.11	TCP	66	28929 → 7 [FIN, PSH, ACK] Seq=58
62	448.715748	192.168.1.11	192.168.1.12	TCP	54	7 → 28929 [ACK] Seq=1
63	448.715774	192.168.1.11	192.168.1.12	TCP	54	7 → 28929 [FIN, ACK] Seq=58
64	448.717853	192.168.1.12	192.168.1.11	TCP	66	28929 → 7 [ACK] Seq=58

Details for selected packet (No. 61):

- Source: Private_66:68:01 (00:50:79:66:68:01)
- Type: IPv4 (0x0800)
- Internet Protocol Version 4, Src: 192.168.1.12, Dst: 192.168.1.11
- Transmission Control Protocol, Src Port: 28929, Dst Port: 7, Seq: 57, Ack: 1, Window: 2920
- Flags: 0x019 (FIN, PSH, ACK)

Рис. 7: Захват трафика между PC-1 и коммутатором: TCP

Моделирование простейшей сети на базе маршрутизатора FRR в GNS3

Выполнение лабораторной работы

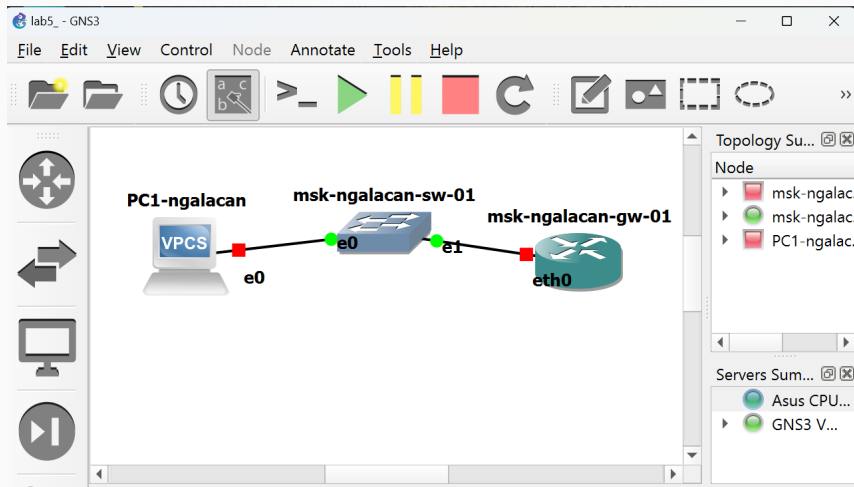


Рис. 8: Топология простейшей сети с маршрутизатором в GNS3

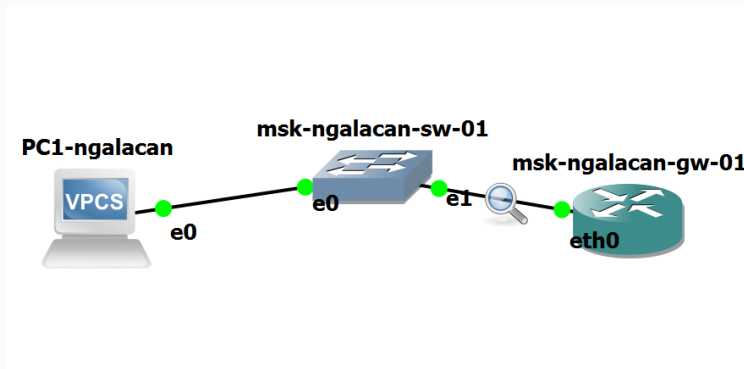
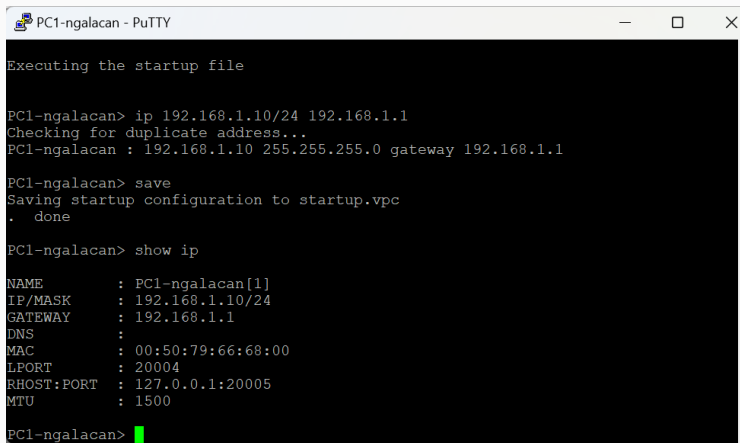


Рис. 9: Запуск устройств и захват трафика между коммутатором и маршрутизатором

Выполнение лабораторной работы



```
PC1-ngalacan - PuTTY

Executing the startup file

PC1-ngalacan> ip 192.168.1.10/24 192.168.1.1
Checking for duplicate address...
PC1-ngalacan : 192.168.1.10 255.255.255.0 gateway 192.168.1.1

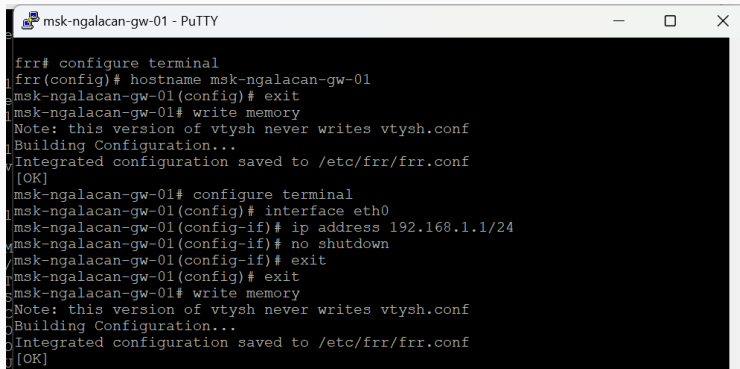
PC1-ngalacan> save
Saving startup configuration to startup.vpc
. done

PC1-ngalacan> show ip

NAME       : PC1-ngalacan[1]
IP/MASK    : 192.168.1.10/24
GATEWAY    : 192.168.1.1
DNS        :
MAC        : 00:50:79:66:68:00
LPORT      : 20004
RHOST:PORT : 127.0.0.1:20005
MTU        : 1500

PC1-ngalacan> 
```

Рис. 10: Настройка IP-адресации на PC-1

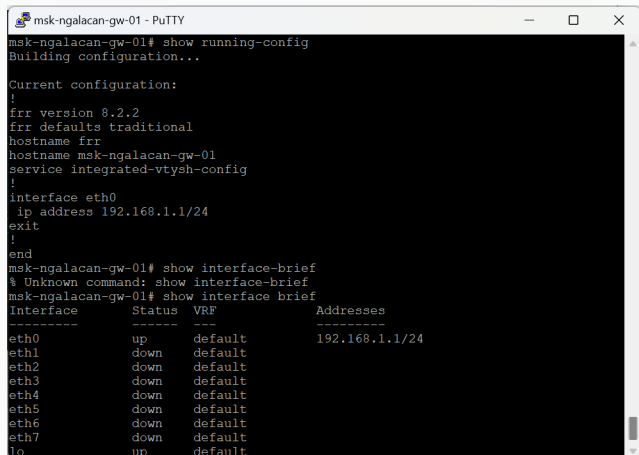


```
msk-ngalacan-gw-01 - PuTTY

frr# configure terminal
frr(config)# hostname msk-ngalacan-gw-01
msk-ngalacan-gw-01(config)# exit
msk-ngalacan-gw-01# write memory
Note: this version of vtysh never writes vtysh.conf
Building Configuration...
Integrated configuration saved to /etc/frr/frr.conf
[OK]
msk-ngalacan-gw-01# configure terminal
msk-ngalacan-gw-01(config)# interface eth0
msk-ngalacan-gw-01(config-if)# ip address 192.168.1.1/24
msk-ngalacan-gw-01(config-if)# no shutdown
msk-ngalacan-gw-01(config-if)# exit
msk-ngalacan-gw-01(config)# exit
msk-ngalacan-gw-01# write memory
Note: this version of vtysh never writes vtysh.conf
Building Configuration...
Integrated configuration saved to /etc/frr/frr.conf
[OK]
```

Рис. 11: Настройка образа маршрутизатора FRR

Выполнение лабораторной работы

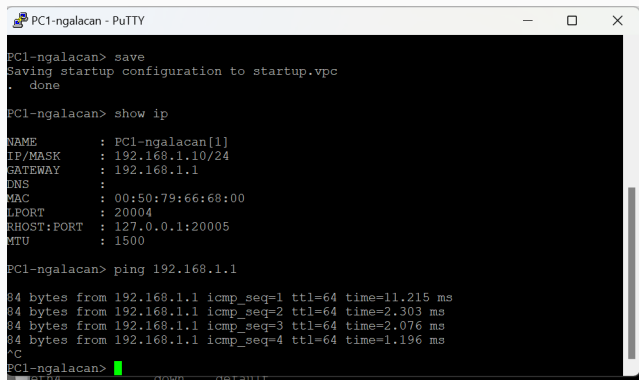


```
msh-ngalacan-gw-01 - PuTTY
msh-ngalacan-gw-01# show running-config
Building configuration...

Current configuration:
!
frr version 8.2.2
frr defaults traditional
hostname frr
hostname msh-ngalacan-gw-01
service integrated-vtysh-config
!
interface eth0
 ip address 192.168.1.1/24
exit
!
end
msh-ngalacan-gw-01# show interface-brief
% Unknown command: show interface-brief
msh-ngalacan-gw-01# show interface brief
Interface      Status   VRF      Addresses
-----
eth0            up       default  192.168.1.1/24
eth1            down     default
eth2            down     default
eth3            down     default
eth4            down     default
eth5            down     default
eth6            down     default
eth7            down     default
lo              up       default
```

Рис. 12: Проверка настройки образа маршрутизатора FRR

Выполнение лабораторной работы



```
PC1-ngalacan> save
Saving startup configuration to startup.vpc
. done

PC1-ngalacan> show ip

NAME          : PC1-ngalacan[1]
IP/MASK       : 192.168.1.10/24
GATEWAY       : 192.168.1.1
DNS           :
MAC           : 00:50:79:66:68:00
LPORT        : 20004
RHOST:PORT    : 127.0.0.1:20005
MTU           : 1500

PC1-ngalacan> ping 192.168.1.1

34 bytes from 192.168.1.1 icmp_seq=1 ttl=64 time=11.215 ms
34 bytes from 192.168.1.1 icmp_seq=2 ttl=64 time=2.303 ms
34 bytes from 192.168.1.1 icmp_seq=3 ttl=64 time=2.076 ms
34 bytes from 192.168.1.1 icmp_seq=4 ttl=64 time=1.196 ms
^C
PC1-ngalacan>
```

Рис. 13: Проверка подключения, пинг маршрутизатора с PC-1

Выполнение лабораторной работы

The screenshot shows the Wireshark interface with a packet capture from the interface 'eth0' on 'msk-ngalacan-gw-01'. The packet list on the left shows several ICMP Echo (ping) requests and replies. Packet 21 is selected, showing details of an ICMP Echo (ping) reply from 192.168.1.1 to 192.168.1.10. The packet structure is as follows:

- Frame 21: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
- Ethernet II, Src: 0c:3e:de:6c:00:00 (0c:3e:de:6c:00:00), Dst: Private_66:68:00:00:50:79:66:68:00:00:4
- Destination: Private_66:68:00:00:50:79:66:68:00:00:4
- Source: 0c:3e:de:6c:00:00 (0c:3e:de:6c:00:00)
- Type: IPv4 (0x0800)
- [Stream index: 4]
- Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.10
 - 0100 = Version: 4
 - 0101 = Header Length: 20 bytes (5)
 - Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 - Total Length: 84
 - Identification: 0x44de (17630)
 - 000. = Flags: 0x0
 - ...0 0000 0000 0000 = Fragment Offset: 0
 - Time to Live: 64
 - Protocol: ICMP (1)
 - Header Checksum: 0xb26f [validation disabled]
 - [Header checksum status: Unverified]
 - Source Address: 192.168.1.1

Рис. 14: Захват трафика между коммутатором и маршрутизатором: ICMP-пакеты

Моделирование простейшей сети на базе маршрутизатора VyOS в GNS3

Выполнение лабораторной работы

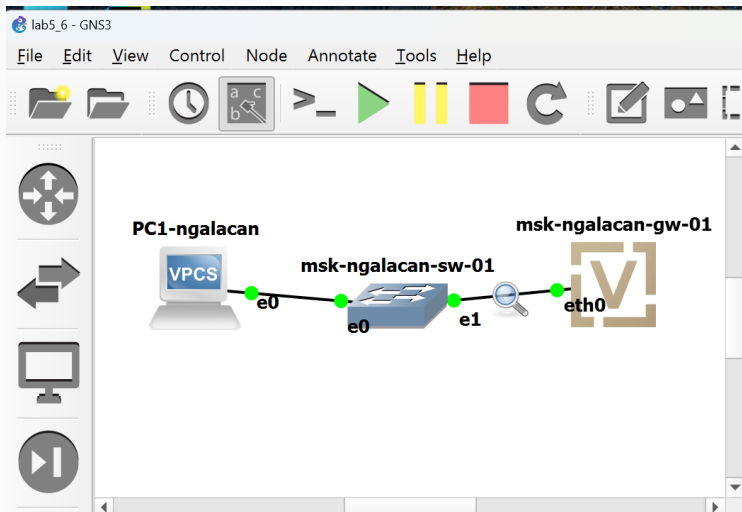
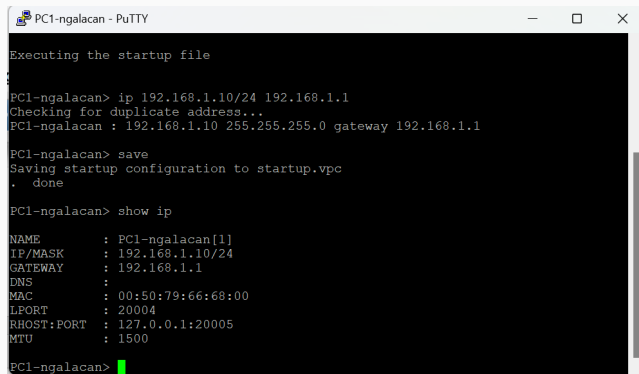


Рис. 15: Топология простейшей сети с маршрутизатором в GNS3



```
PC1-ngalacan - PuTTY

Executing the startup file

PC1-ngalacan> ip 192.168.1.10/24 192.168.1.1
Checking for duplicate address...
PC1-ngalacan : 192.168.1.10 255.255.255.0 gateway 192.168.1.1

PC1-ngalacan> save
Saving startup configuration to startup.vpc
. done

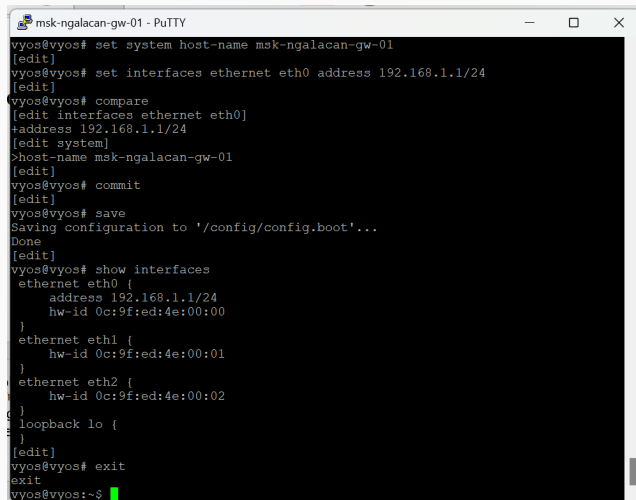
PC1-ngalacan> show ip

NAME       : PC1-ngalacan[1]
IP/MASK    : 192.168.1.10/24
GATEWAY    : 192.168.1.1
DNS        :
MAC        : 00:50:79:66:68:00
LPORT      : 20004
RHOST:PORT : 127.0.0.1:20005
MTU        : 1500

PC1-ngalacan>
```

Рис. 16: Настройка IP-адресации на PC-1

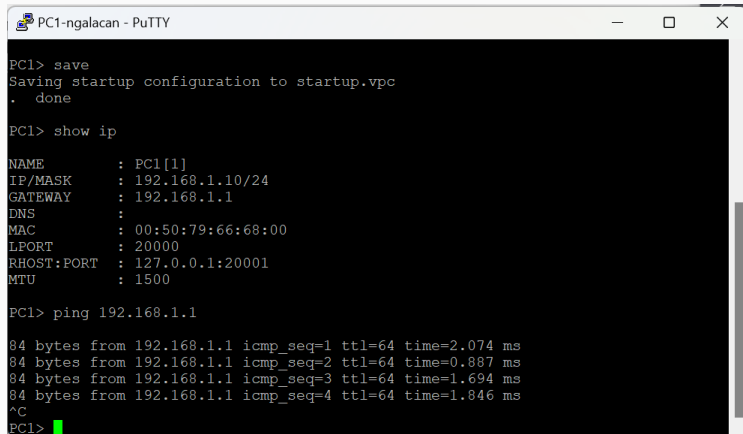
Выполнение лабораторной работы



```
msk-ngalacan-gw-01 - PuTTY
vyos@vyos# set system host-name msk-ngalacan-gw-01
[edit]
vyos@vyos# set interfaces ethernet eth0 address 192.168.1.1/24
[edit]
vyos@vyos# compare
[edit interfaces ethernet eth0]
+address 192.168.1.1/24
[edit system]
>host-name msk-ngalacan-gw-01
[edit]
vyos@vyos# commit
[edit]
vyos@vyos# save
Saving configuration to '/config/config.boot'...
Done
[edit]
vyos@vyos# show interfaces
  ethernet eth0 {
    address 192.168.1.1/24
    hw-id 0c:9f:ed:4e:00:00
  }
  ethernet eth1 {
    hw-id 0c:9f:ed:4e:00:01
  }
  ethernet eth2 {
    hw-id 0c:9f:ed:4e:00:02
  }
  loopback lo {
  }
[edit]
vyos@vyos# exit
exit
vyos@vyos:~$
```

Рис. 17: Настройка образа маршрутизатора VyOS

Выполнение лабораторной работы



```
PC1-ngalacan - PuTTY

PC1> save
Saving startup configuration to startup.vpc
. done

PC1> show ip

NAME       : PC1[1]
IP/MASK    : 192.168.1.10/24
GATEWAY    : 192.168.1.1
DNS        :
MAC        : 00:50:79:66:68:00
LPORT      : 20000
RHOST:PORT : 127.0.0.1:20001
MTU        : 1500

PC1> ping 192.168.1.1

84 bytes from 192.168.1.1 icmp_seq=1 ttl=64 time=2.074 ms
84 bytes from 192.168.1.1 icmp_seq=2 ttl=64 time=0.887 ms
84 bytes from 192.168.1.1 icmp_seq=3 ttl=64 time=1.694 ms
84 bytes from 192.168.1.1 icmp_seq=4 ttl=64 time=1.846 ms
^C
PC1> 
```

Рис. 18: Проверка подключения, пинг маршрутизатора с PC-1

Выполнение лабораторной работы

The screenshot shows the Wireshark interface with a packet capture from the interface 'msk-ngalacan-gw-01 eth0'. The packet list on the left shows several ICMP Echo (ping) requests and replies. Packet 17 is selected, showing its details in the middle pane and the raw packet data in hexadecimal and ASCII in the right pane.

No.	Time	Source	Destination	Protocol	Length	Info
12	466.111510	0c:9f:ed:4e:00:00	Private_66:68:00	ARP	60	192.168.1.1 is at 0c:9f:ed:4e:00:00
13	466.112974	192.168.1.10	192.168.1.1	ICMP	98	Echo (ping) request id=1
14	466.114786	192.168.1.1	192.168.1.10	ICMP	98	Echo (ping) reply id=1
15	467.116221	192.168.1.10	192.168.1.1	ICMP	98	Echo (ping) request id=2
16	467.116951	192.168.1.1	192.168.1.10	ICMP	98	Echo (ping) reply id=2
17	468.119709	192.168.1.10	192.168.1.1	ICMP	98	Echo (ping) request id=3
18	468.121017	192.168.1.1	192.168.1.10	ICMP	98	Echo (ping) reply id=3
19	469.125533	192.168.1.10	192.168.1.1	ICMP	98	Echo (ping) request id=4
20	469.127086	192.168.1.1	192.168.1.10	ICMP	98	Echo (ping) reply id=4
21	471.269639	0c:9f:ed:4e:00:00	Private_66:68:00	ARP	60	Who has 192.168.1.10? T=0
22	471.270591	Private_66:68:00	0c:9f:ed:4e:00:00	ARP	60	192.168.1.10 is at 00:50:79:66:68:00

Details of Frame 17:

- Frame 17: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
- Ethernet II, Src: Private_66:68:00 (00:50:79:66:68:00), Dst: 0c:9f:ed:4e:00:00
- Destination: 0c:9f:ed:4e:00:00 (0c:9f:ed:4e:00:00)
- Source: Private_66:68:00 (00:50:79:66:68:00)
- Type: IPv4 (0x0800)
- [Stream index: 3]
- Internet Protocol Version 4, Src: 192.168.1.10, Dst: 192.168.1.1
- 0100 = Version: 4
- 0101 = Header Length: 20 bytes (5)
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 84
- Identification: 0x8ac4 (35524)
- 0000 = Flags: 0x0
- ...0 0000 0000 0000 = Fragment Offset: 0
- Time to Live: 64
- Protocol: ICMP (1)
- Header Checksum: 0x6c89 [validation disabled]
- [Header checksum status: Unverified]
- Source Address: 192.168.1.10

Рис. 19: Захват трафика между коммутатором и маршрутизатором: ICMP-пакеты

В результате выполнения работы было изучено построение простейших моделей сети на базе коммутатора и маршрутизаторов FRR и VyOS в GNS3, произведен анализ трафика посредством Wireshark.