Лабораторная работа № 12. Настройка NAT

12.1. Цель работы

Приобретение практических навыков по настройке доступа локальной сети к внешней сети посредством NAT.

12.2. Постановка задачи

Требуется подключить локальную сеть организации к сети Интернет (распределение внешних ip-адресов дано в табл. 12.1) с учётом ограничений, накладываемых на определённые подсети локальной сети (VLAN подсетей даны в табл. 12.2):

1) сеть управления устройствами не должна иметь доступ в Интернет;
2) оконечные устройства сети дисплейных классов должны иметь доступ только к сайтам, необходимым для учёбы (в данном случае к `www.yandex.ru`, `stud.rudn.university`);
3) пользователям из сети кафедр разрешено работать только с образовательными сайтами (в данном случае это `esystem.pfur.ru`);
4) пользователям сети администрации разрешено работать только с сайтом университета `www.rudn.ru`;
5) в сети для других пользователей компьютер администратора должен иметь полный доступ во внешнюю сеть, а другие пользователи — не должны выходить в Интернет;
6) ограничения для серверов:
   - WEB-сервер должен быть доступен по порту 80;
   - почтовый сервер должен быть доступен по портам 25 и 110;
   - файловый сервер должен быть доступен извне по портам протокола FTP;
7) компьютер администратора должен быть доступен из внешней сети по протоколу удалённого рабочего стола (Remote Desktop Protocol, RDP).

Таблица 12.1

Распределение внешних ip-адресов

IP-адреса	Примечание	VLAN
198.51.100.0/28	Выделено провайдером	4
198.51.100.1	Маршрутизатор провайдера	
198.51.100.2	msk-donskaya-gw-1	
198.51.100.2–198.51.100.14	Пул адресов для NAT	
198.51.100.2	Web	
198.51.100.3	File	
198.51.100.4	Mail	

Таблица 12.2

Таблица VLAN

№ VLAN	Имя VLAN	Примечание
1	default	Не используется
2	management	Для управления устройствами
3	servers	Для серверной фермы
4	nat	Линк в Интернет
5-100		Зарезервировано
101	dk	Дисплейные классы (ДК)
102	departments	Кафедры
103	adm	Администрация
104	other	Для других пользователей

12.3. Задание

1. Сделать первоначальную настройку маршрутизатора `provider-gw-1` и коммутатора `provider-sw-1` провайдера: задать имя, настроить доступ по паролю и т.п. (см. разделы 12.4.1, 12.4.2).
2. Настроить интерфейсы маршрутизатора `provider-gw-1` и коммутатора `provider-sw-1` провайдера: (см. разделы 12.4.3, 12.4.4).
3. Настроить интерфейсы маршрутизатора сети «Донская» для доступа к сети провайдера (см. раздел 12.4.5).
4. Настроить на маршрутизаторе сети «Донская» NAT с правилами, указанными в разделе 12.2 (см. разделы 12.4.6–12.4.8).
5. Настроить доступ из внешней сети в локальную сеть организации, как указано в разделе 12.2 (см. раздел 12.4.9).
6. Проверить работоспособность заданных настроек.
7. При выполнении работы необходимо учитывать соглашение об именовании (см. раздел 2.5).

12.4. Последовательность выполнения работы

12.4.1. Первоначальная настройка маршрутизатора provider-gw-1

```
provider-gw-1>enable
provider-gw-1#configure terminal

provider-gw-1(config)#line vty 0 4
provider-gw-1(config-line)#password cisco
provider-gw-1(config-line)#login
provider-gw-1(config-line)#exit

provider-gw-1(config)#line console 0
provider-gw-1(config-line)#password cisco
provider-gw-1(config-line)#login
provider-gw-1(config-line)#exit
```

```
provider-gw-1(config)#enable secret cisco
provider-gw-1(config)#service password-encryption
provider-gw-1(config)#username admin privilege 1 secret cisco
```

12.4.2. Первоначальная настройка коммутатора provider-sw-1

```
provider-sw-1>enable
provider-sw-1#configure terminal

provider-sw-1(config)#line vty 0 4
provider-sw-1(config-line)#password cisco
provider-sw-1(config-line)#login
provider-sw-1(config-line)#exit

provider-sw-1(config)#line console 0
provider-sw-1(config-line)#password cisco
provider-sw-1(config-line)#login
provider-sw-1(config-line)#exit

provider-sw-1(config)#enable secret cisco
provider-sw-1(config)#service password-encryption
provider-sw-1(config)#username admin privilege 1 secret cisco
```

12.4.3. Настройка интерфейсов маршрутизатора provider-gw-1

```
provider-gw-1>enable
provider-gw-1#configure terminal

provider-gw-1(config)#interface f0/0
provider-gw-1(config-if)#no shutdown
provider-gw-1(config-if)#exit

provider-gw-1(config)#interface f0/0.4
provider-gw-1(config-subif)#encapsulation dot1Q 4
provider-gw-1(config-subif)#ip address 198.51.100.1 255.255.255.240
provider-gw-1(config-subif)#description mks-donskaya
provider-gw-1(config-subif)#exit

provider-gw-1(config)#interface f0/1
provider-gw-1(config-if)#no shutdown
provider-gw-1(config-if)#ip address 192.0.2.1 255.255.255.0
provider-gw-1(config-if)#description internet
provider-gw-1(config-if)#exit
provider-gw-1(config)#exit
```

12.4.4. Настройка интерфейсов коммутатора provider-sw-1

```
provider-sw-1>enable
provider-sw-1#configure terminal

provider-sw-1(config)#interface f0/1
provider-sw-1(config-if)#switchport mode trunk
provider-sw-1(config-if)#exit

provider-sw-1(config)#interface f0/2
provider-sw-1(config-if)#switchport mode trunk
```

```
provider-sw-1(config-if)#exit

provider-sw-1(config)#vlan 4
provider-sw-1(config-vlan)#name nat
provider-sw-1(config-vlan)#exit

provider-sw-1(config)#interface vlan4
provider-sw-1(config-if)#no shutdown
provider-sw-1(config-if)#exit
```

В этой лабораторной работе можно использовать подключение маршрутизатора `provider-gw-1` напрямую к медиаконвертеру `provider-mc-1`.

12.4.5. Настройка интерфейсов маршрутизатора msk-donskaya-gw-1

```
msk-donskaya-gw-1>enable
msk-donskaya-gw-1#configure terminal

msk-donskaya-gw-1(config)#interface f0/1
msk-donskaya-gw-1(config-if)#no shutdown
msk-donskaya-gw-1(config-if)#exit

msk-donskaya-gw-1(config)#interface f0/1.4
msk-donskaya-gw-1(config-subif)#encapsulation dot1Q 4
msk-donskaya-gw-1(config-subif)#ip address 198.51.100.2 255.255.255.240
msk-donskaya-gw-1(config-subif)#description internet
msk-donskaya-gw-1(config-subif)#exit
msk-donskaya-gw-1(config)#exit


msk-donskaya-gw-1>enable
msk-donskaya-gw-1#configure terminal

msk-donskaya-gw-1(config)#ip route 0.0.0.0 0.0.0.0 198.51.100.1
msk-donskaya-gw-1(config)#exit
```

12.4.6. Настройка пула адресов для NAT

```
msk-donskaya-gw-1>enable
msk-donskaya-gw-1#configure terminal

msk-donskaya-gw-1(config)#ip nat pool main-pool 198.51.100.2
    ↪ 198.51.100.14 netmask 255.255.255.240
```

12.4.7. Настройка списка доступа для NAT

```
msk-donskaya-gw-1>enable
msk-donskaya-gw-1#configure terminal

msk-donskaya-gw-1(config)#ip access-list extended nat-inet
```

12.4.7.1. Сеть дисплейных классов

Хосты из сети дисплейных классов имеют доступ только к сайтам, необходимым для учёбы (`www.yandex.ru` (192.0.2.11), `stud.rudn.university` (192.0.2.12)).

```
msk-donskaya-gw-1(config-ext-nacl)#remark dk
msk-donskaya-gw-1(config-ext-nacl)#permit tcp 10.128.3.0 0.0.0.255 host
    ↪ 192.0.2.11 eq 80
msk-donskaya-gw-1(config-ext-nacl)#permit tcp 10.128.3.0 0.0.0.255 host
    ↪ 192.0.2.12 eq 80
```

12.4.7.2. Сеть кафедр

Сеть кафедр работает только с образовательными сайтами (`esystem.pfur.ru` (192.0.2.13)).

```
msk-donskaya-gw-1(config-ext-nacl)#remark departments
msk-donskaya-gw-1(config-ext-nacl)#permit tcp 10.128.4.0 0.0.0.255 host
    ↪ 192.0.2.13 eq 80
```

12.4.7.3. Сеть администрации

Сеть администрации имеет возможность работать только с сайтом университета (`www.rudn.ru` (192.0.2.14)).

```
msk-donskaya-gw-1(config-ext-nacl)#remark adm
msk-donskaya-gw-1(config-ext-nacl)#permit tcp 10.128.5.0 0.0.0.255 host
    ↪ 192.0.2.14 eq 80
```

12.4.7.4. Доступ для компьютера администратора

В сети для других пользователей компьютер администратора имеет полный доступ в Интернет. Другие не имеют доступа.

```
msk-donskaya-gw-1(config-ext-nacl)#remark admin
msk-donskaya-gw-1(config-ext-nacl)#permit ip host 10.128.6.200 any
```

12.4.8. Настройка NAT

Настроить Port Address Translation (PAT)[1]:

```
msk-donskaya-gw-1>enable
msk-donskaya-gw-1#configure terminal

msk-donskaya-gw-1(config)#ip nat inside source list nat-inet pool
    ↪ main-pool overload
```

Настройка интерфейсов для NAT:

[1]Другие названия: NAT Overload, IP Masquerading, Many-to-One NAT, Network Address Port Translation (NAPT).

```
msk-donskaya-gw-1(config)#int f0/0.3
msk-donskaya-gw-1(config-subif)#ip nat inside
msk-donskaya-gw-1(config)#interface f0/0.101
msk-donskaya-gw-1(config-subif)#ip nat inside
msk-donskaya-gw-1(config-subif)#exit
msk-donskaya-gw-1(config)#interface f0/0.102
msk-donskaya-gw-1(config-subif)#ip nat inside
msk-donskaya-gw-1(config-subif)#exit
msk-donskaya-gw-1(config)#interface f0/0.103
msk-donskaya-gw-1(config-subif)#ip nat inside
msk-donskaya-gw-1(config-subif)#exit
msk-donskaya-gw-1(config)#interface f0/0.104
msk-donskaya-gw-1(config-subif)#ip nat inside
msk-donskaya-gw-1(config-subif)#exit
msk-donskaya-gw-1(config)#interface f0/1.4
msk-donskaya-gw-1(config-subif)#ip nat outside
msk-donskaya-gw-1(config-subif)#exit
```

12.4.9. Настройка доступа из Интернета

12.4.9.1. WWW-сервер

```
msk-donskaya-gw-1(config)#ip nat inside source static tcp 10.128.0.2 80
     ↪ 198.51.100.2 80
```

12.4.9.2. Файловый сервер

```
msk-donskaya-gw-1(config)#ip nat inside source static tcp 10.128.0.3 20
     ↪ 198.51.100.3 20
msk-donskaya-gw-1(config)#ip nat inside source static tcp 10.128.0.3 21
     ↪ 198.51.100.3 21
```

12.4.9.3. Почтовый сервер

```
msk-donskaya-gw-1(config)#ip nat inside source static tcp 10.128.0.4 25
     ↪ 198.51.100.4 25
msk-donskaya-gw-1(config)#ip nat inside source static tcp 10.128.0.4 110
     ↪ 198.51.100.4 110
```

12.4.9.4. Доступ по RDP

Компьютер администратора доступен из Интернета по RDP.

```
msk-donskaya-gw-1(config)#ip nat inside source static tcp 10.128.6.200
     ↪ 3389 198.51.100.10 3389
```

12.5. Содержание отчёта

1. Титульный лист с указанием номера лабораторной работы и ФИО студента.
2. Формулировка задания работы.
3. Описание результатов выполнения задания:

   - скриншоты (снимки экрана), фиксирующие выполнение лабораторной работы;
   - подробное описание настроек сетевого оборудования в соответствии с заданием;
   - результаты проверки корректности настроек сетевого оборудования в соответствии с заданием (подтверждённые скриншотами).
4. Выводы, согласованные с заданием работы.
5. Ответы на контрольные вопросы.

12.6. Контрольные вопросы

1. В чём состоит основной принцип работы NAT (что даёт наличие NAT в сети организации)?
2. В чём состоит принцип настройки NAT (на каком оборудовании и что нужно настроить для из локальной сети во внешнюю сеть через NAT)?
3. Можно ли применить Cisco IOS NAT к субинтерфейсам?
4. Что такое пулы IP NAT?
5. Что такое статические преобразования NAT?

При ответах на вопросы рекомендуется ознакомиться с информацией из источников [8; 9; 20; 25; 27].

Литература по теме

1. 802.1D-2004 - IEEE Standard for Local and Metropolitan Area Networks. Media Access Control (MAC) Bridges : тех. отч. / IEEE. — 2004. — С. 1—277. — DOI: 10.1109/IEEESTD.2004.94569. — URL: http://ieeexplore.ieee.org/servlet/opac?punumber=9155.
2. 802.1Q - Virtual LANs. — URL: http://www.ieee802.org/1/pages/802.1Q.html.
3. *A J.* Packet Tracer Network Simulator. — Packt Publishing, 2014. — ISBN 9781782170426. — URL: https://books.google.com/books?id=eVOcAgAAQBAJ&dq=cisco+packet+tracer&hl=es&source=gbs_navlinks_s.
4. *Cotton M., Vegoda L.* Special Use IPv4 Addresses : RFC / RFC Editor. — 01.2010. — С. 1—11. — № 5735. — DOI: 10.17487/rfc5735. — URL: https://www.rfc-editor.org/info/rfc5735.
5. *Droms R.* Dynamic Host Configuration Protocol : RFC / RFC Editor. — 03.1997. — С. 1—45. — № 2136. — DOI: 10.17487/rfc2131. — URL: https://www.ietf.org/rfc/rfc2131.txt%20https://www.rfc-editor.org/info/rfc2131.
6. *McPherson D., Dykes B.* VLAN Aggregation for Efficient IP Address Allocation, RFC 3069. — 2001. — URL: http://www.ietf.org/rfc/rfc3069.txt.
7. *Moy J.* OSPF Version 2 : RFC / RFC Editor. — 1998. — С. 244. — DOI: 10.17487/rfc2328. — URL: https://www.rfc-editor.org/info/rfc2328.
8. NAT Order of Operation. — URL: https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/6209-5.html.

9. NAT: вопросы и ответы / Сайт поддержки продуктов и технологий компании Cisco. — URL: https://www.cisco.com/cisco/web/support/RU/9/92/92029_nat-faq.html.

10. *Neumann J. C.* Cisco Routers for the Small Business A Practical Guide for IT Professionals. — Apress, 2009.

11. *Odom S.*, *Nottingham H.* Cisco Switching: Black Book. — The Coriolis Group, 2001. — ISBN 9781576107065. — URL: http://books.google.sk/books?id=GYsLAAAACAAJ.

12. *Tetz E.* Cisco Networking All-in-One For Dummies. — Indianapolis, Indiana : John Wiley & Sons, Inc., 2011. — (For Dummies). — URL: http://www.dummies.com/store/product/Cisco-Networking-All-in-One-For-Dummies.productCd-0470945583.html.

13. ГОСТ Р ИСО/МЭК 7498-1-99. — «ВОС. Базовая эталонная модель. Часть 1. Базовая модель». — ОКС: 35.100.70. — Действует с 01.01.2000. — URL: http://protect.gost.ru/v.aspx?control=7&id=132355.

14. *Кларк К.*, *Гамильтон К.* Принципы коммутации в локальных сетях Cisco. — М. : Вильямс, 2003. — (Cisco Press Core Series). — ISBN 5-8459-0464-1.

15. *Королькова А. В.*, *Кулябов Д. С.* Архитектура и принципы построения современных сетей и систем телекоммуникаций. — М. : Издательство РУДН, 2009.

16. *Королькова А. В.*, *Кулябов Д. С.* Прикладные протоколы Интернет и www. Курс лекций. — М. : РУДН, 2012. — ISBN 9785209049500.

17. *Королькова А. В.*, *Кулябов Д. С.* Прикладные протоколы Интернет и www. Лабораторные работы. — М. : РУДН, 2012. — ISBN 9785209049357.

18. *Королькова А. В.*, *Кулябов Д. С.* Сетевые технологии. Лабораторные работы. — М. : РУДН, 2014. — ISBN 785209056065.

19. *Куроуз Д. Ф.*, *Росс К. В.* Компьютерные сети. Нисходящий подход. — 6-е изд. — М. : Издательство «Э», 2016. — (Мировой компьютерный бестселлер).

20. *Одом У.* Официальное руководство Cisco по подготовке к сертификационным экзаменам CCENT/CCNA ICND1 100-101. — М. : Вильямс, 2017. — (Cisco Press Core Series). — ISBN 978-5-8459-1906-9.

21. *Одом У.* Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2 200-101. Маршрутизация и коммутация. — М. : Вильямс, 2016. — (Cisco Press Core Series).

22. *Олифер В. Г.*, *Олифер Н. А.* Компьютерные сети. Принципы, технологии, протоколы. — 5-е изд. — Питер : Питер, 2017. — (Учебник для вузов). — ISBN 978-5-496-01967-5.

23. Сети и системы передачи информации: телекоммуникационные сети / К. Е. Самуйлов [и др.]. — М. : Изд-во Юрайт, 2016. — ISBN 978-5-9916-7198-9.

24. *Таненбаум Э.*, *Уэзеролл Д.* Компьютерные сети. — 5 изд. — Питер : Питер, 2016. — (Классика Computer Science). — ISBN 978-5-496-00831-0.

25. *Хилл Б.* Полный справочник по Cisco. — М. : Вильямс, 2009. — ISBN 978-5-8459-1309-8.

26. Цикл статей «Сети для самых маленьких». — URL: http://linkmeup.ru/blog/11.html.

27. Часто задаваемые вопросы технологии NAT / Сайт поддержки продуктов и технологий компании Cisco. — URL: https://www.cisco.com/c/ru_ru/support/docs/ip/network-address-translation-nat/26704-nat-faq-00.html.