УДК 681.327.8

А-471

**Рецензент: к.т.н. О.А. Назаркин**

**Алексеев, В.А.**

**A471** Маршрутизация и удаленный доступ в сетях TCP/IP [Текст]: методические указания к проведению лабораторных работ по курсу «Сетевые технологии» / В.А. Алексеев. – Липецк: Издательство ЛГТУ, 2011. – 32 с.

В методических указаниях рассматриваются принципы маршрутизации и удаленного доступа в сетях TCP/IP. Приведены задания по настройке программного маршрутизатора на базе ОС Linux и конфигурированию удаленного доступа к сети по технологии xDSL.

Предназначены для студентов направлений 230100.62 «Информатика и вычислительная техника», 231000.62 «Программная инженерия», 010500.62 «Математическое обеспечение и администрирование информационных систем» и специальностей 230102.65 «Автоматизированные системы обработки информации и управления», 010503.65 «Математическое обеспечение и администрирование информационных систем», 230401.65 «Прикладная математика».

Ил. 9. Библиогр.: 7 назв.

© Липецкий государственный

технический университет, 2011

**Лабораторная работа №1**

**Маршрутизация с использованием программного маршрутизатора**

***Цель работы***

Изучить принципы маршрутизации в IP-сетях, получить практические навыки настройки программных маршрутизаторов на базе операционной системы (ОС) Linux с применением маршрутизации интерфейсов и маршрутизации виртуальных локальных сетей (VLAN).

***Теоретические сведения***

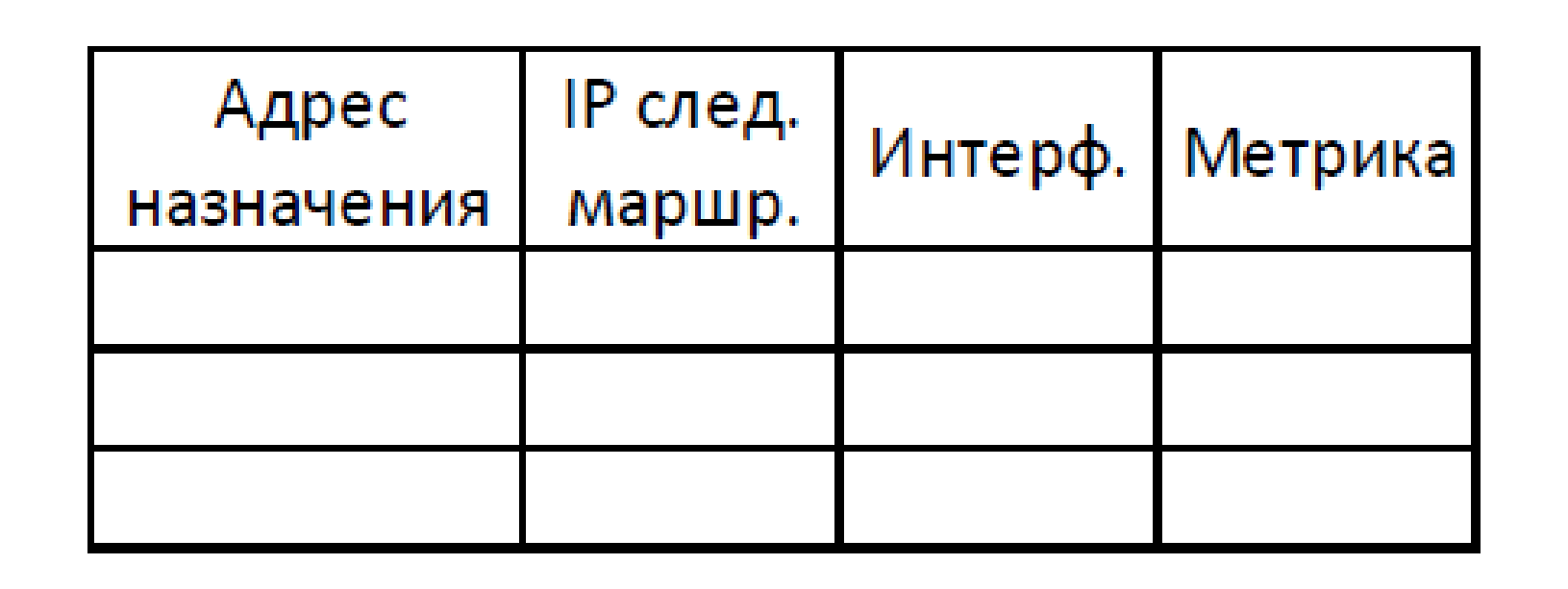
Маршрутизация включает в себя следующие частные задачи:

1. Обмен информацией о топологии сети. Реализуется протоколами маршрутизации.
2. Определение оптимальных маршрутов и построение таблиц маршрутизации.
3. Продвижение пакета маршрутизаторами на основании таблиц маршрутизации.

В данной лабораторной работе рассматриваются вопросы продвижения пакетов. Информация об оптимальных маршрутах представляется в маршрутизаторе в виде таблицы маршрутизации. В случае адресации без масок таблица маршрутизации имеет вид:

**Таблица 1.**

**Формат таблицы маршрутизации без масок**



В таблице:

* Адрес назначения – это IP-адрес сети или конкретного узла.
* IP следующего маршрутизатора – адрес следующего транзитного маршрутизатора на пути к адресу назначения.
* Интерфейс – это идентификатор сетевого интерфейса маршрутизатора, через который нужно передавать данные следующему маршрутизатору.
* Метрика – абстрактная характеристика качества маршрута. В качестве метрики может выступать количество транзитных узлов («хопов»), пропускная способность и т.п. Меньшее значение метрики всегда соответствует лучшему маршруту.

При поиске маршрута для продвижения IP-пакета предпочтение отдается специфическим маршрутам (то есть маршрутам до конкретного узла, а не сети), даже в том случае, если метрика этого маршрута хуже.

При использовании масок алгоритм работы маршрутизатора при продвижении пакета несколько усложняется. В таблицу маршрутизации добавляется колонка с маской, соответствующей адресу назначения. Рассмотрим пример:



**Рис. 1. Пример структуры сети**

Для данного примера в таблице маршрутизации R2 могут быть следующие записи:

**Таблица 2.**

**Пример таблицы маршрутизации с масками**

| Адрес назначения | Маска | Адрес след. маршр. | Интерфейс | Метрика |
| --- | --- | --- | --- | --- |
| 192.168.1.16 | 255.255.255.240 | - | 192.168.1.18 | 0 |
| 192.168.3.0 | 255.255.255.0 | - | 192.168.3.1 | 0 |
| 192.168.2.0 | 255.255.255.192 | - | 192.168.2.1 | 0 |
| 192.168.2.64 | 255.255.255.192 | - | 192.168.2.65 | 0 |
| 192.168.1.0 | 255.255.255.240 | 192.168.1.17 | 192.168.1.18 | 1 |
| Default | 0.0.0.0 | 192.168.1.17 | 192.168.1.18 | 16 |

  Продвижение пакета основывается на следующем алгоритме:

* 1. Маршрутизатор извлекает из пакета IP-адрес назначения.
  2. Поиск специфического маршрута, то есть записи, в которой адрес назначения равен целевому IP-адресу. Если запись найдена, то используется этот маршрут, иначе на шаг 3.
  3. Поиск неспецифического маршрута. Включает следующие шаги:
     + для каждой записи таблицы маршрутизации выполняется операция IPd & M, где IPd – целевой адрес из пакета, M - маска из записи таблицы маршрутизации;
     + если результат равен адресу назначения IP, запись отмечается подходящей.
  4. Из всех подходящих маршрутов выбирается наиболее специфический. Такой маршрут содержится в записи с наиболее длинной маской.
  5. Среди подходящих маршрутов, обладающих одинаковой "специфичностью", выбирается маршрут с меньшей метрикой.

***Задание***

Настроить взаимодействие двух IP-сетей между собой и с внешней сетью средствами программного маршрутизатора на базе ОС Linux (рис. 2). Настроить простейшие правила фильтрации трафика средствами ОС Linux.

Ситуация 1. Сети изолированы друг от друга физически, т.е. построены на различных коммутаторах, не связанных друг с другом непосредственно.

Ситуация 2. Изоляция сетей обеспечивается за счет применения технологии виртуальных локальных сетей.

Проверить настройку маршрутизации и фильтров на примере взаимодействия рабочих станций PC-1 и PC-2, принадлежащих различным сетям.



**Рис. 2. Принципиальная схема взаимодействия сетей для лабораторной работы №1**

***Схема ЛВС***

В приведённых примерах схем ЛВС для лабораторной работы указана адресация для компьютеров PC151 (ПК-1), PC152 (ПК-2), PC154 (ПК-4) лаборатории. При использовании других компьютеров IP-адреса будут другими (см. прил. 1).



**Рис. 3. Физическая схема ЛВС для лабораторной работы №1 (ситуация 1)**



**Рис. 4. Логическая схема ЛВС для лабораторной работы №1 (ситуация 1). IP-сеть 1 имеет адрес 192.168.201.0/24, IP-сеть 2 имеет адрес 192.168.200.0/24, внешняя сеть подключена через 192.168.132.0/24**



**Рис. 5. Физическая схема ЛВС для лабораторной работы №1 (ситуация 2)**



**Рис. 6. Логическая схема ЛВС для лабораторной работы №1 (ситуация 2). IP-сеть 1 имеет адрес 192.168.201.0/24, IP-сеть 2 имеет адрес 192.168.200.0/24, внешняя сеть подключена через 192.168.142.0/24**

***Порядок выполнения работы***

Перед выполнением лабораторной работы необходимо:

1. Подготовить схемы сети с указанием ip-адресов в соответствии с вариантом.
2. Подготовить виртуальные машины PC-1, PC-2, на которых может быть установлена любая сетевая операционная система, например Microsoft Windows XP или Linux.
3. Подготовить виртуальную машину, которая будет выполнять роль маршрутизатора. Рекомендуется использовать дистрибутив Debian GNU/Linux. Для данной виртуальной машины использовать сетевые адаптеры «PCnet», обеспечивающие передачу тэгированных кадров VLAN.

В установленной ОС Linux должна быть включена поддержка VLAN. В Debian необходимо установить соответствующий пакет командой

apt-get install vlan

Рекомендуется также установить графическую версию текстового редактора vi. В Debian соответствующий пакет устанавливается командой

apt-get install vi-gnome

***Только для Debian!*** В случае, если образ ОС Debian Linux копируется/клонируется, необходимо отключить контроль MAC-адресов интерфейсов в файле «/etc/udev/rules.d/75-persistent-net-generator.rules» (изменять файл можно только с правами администратора). Для этого внести в приведенный ниже раздел строку с маской сетевых адаптеров VirtualBox и перезагрузить операционную систему.

# ignore interfaces with locally administered or null MAC addresses

# and VMWare virtual interfaces

ENV{MATCHADDR}=="?[2367abef]:\*", ENV{MATCHADDR}=""

ENV{MATCHADDR}=="00:00:00:00:00:00", ENV{MATCHADDR}=""

ENV{MATCHADDR}=="00:0c:29:\*|00:50:56:\*", ENV{MATCHADDR}=""

**ENV{MATCHADDR}=="08:00:27:\*", ENV{MATCHADDR}=""**

1. Подготовить коммутаторы 3COM Switch 1100 (SW-1, SW-2) для моделирования ситуаций 1, 2 задания (при подключении к коммутаторам использовать имя «manager», пароль – «superuser»). Для этого настроить:

* порты 1-2 коммутаторов SW-1, SW-2 для работы в VLAN-2 без тегирования;
* порты 3, 4 коммутатора SW-1 для работы в VLAN-3 без тегирования;
* порты 3, 4 коммутатора SW-2 для работы в VLAN-4 без тегирования;
* порты 5, 6 коммутаторов SW-1, SW-2 для работы в VLAN-2/3/4 с тегированием.

Выполнение лабораторной работы включает следующие этапы:

1. **Подключение и запуск рабочих станций PC-1, PC-2**

Цель данного этапа состоит в подготовке моделей IP-сетей, взаимодействие между которыми будет настраиваться в лабораторной работе.

1. Подключить образ виртуальной машины в системе VirtualBox на одном из компьютеров лаборатории. В настройках виртуальной машины в разделе «Сеть» включить 1 сетевой адаптер, для которого указать тип подключения «Сетевой мост» и сетевой адаптер «Realtek 8029» или «3COM» (в зависимости от компьютера).
2. Запустить виртуальную машину.
3. Настроить IP-адрес сетевого интерфейса виртуальной машины в соответствии с вариантом.
4. Подключить компьютер через соответствующий разъем патч-панели «B-0x» на порт коммутатора 1 или 2 (для 1-й ситуации из задания).
5. Повторить шаги 1-5 для 2-й виртуальной машины (на другом компьютере).
6. **Подключение и настройка маршрутизации. Ситуация 1**

Цель данного этапа состоит в настройке маршрутизации средствами ОС Linux для ситуации, когда на маршрутизаторе установлено 3 сетевых интерфейса. Фильтры на данном этапе не настраиваются. Выход во внешнюю сеть обеспечивается через VirtualBox Host-Only Network (адрес сети 192.168.13х.0/24) и маршрутизируется хост-компьютером.

1. Подключить хост-компьютеры в сеть в соответствии с физической схемой для ситуации 1. Использовать порты 1, 2 коммутаторов.
2. Подключить образ виртуальной машины под управлением ОС Linux в системе VirtualBox на одном из компьютеров лаборатории. В настройках виртуальной машины в разделе «Сеть» включить 3 сетевых адаптера и настроить следующим образом:

* адаптер 1: тип подключения «Сетевой мост» и сетевой адаптер «Realtek 8029» или «3COM» (в зависимости от компьютера);
* адаптер 2: тип подключения «Сетевой мост» и сетевой адаптер «D-Link DGE-528»;
* адаптер 3: тип подключения «Виртуальный адаптер хоста» и сетевой адаптер «VirtualBox Host-Only Ethernet Adapter».

1. Запустить ОС Linux на виртуальной машине, запустить консоль с правами администратора.
2. Выключить сетевые интерфейсы командой

ifdown --all

1. Настроить статические адреса сетевых интерфейсов маршрутизатора. Для этого в файле /etc/network/interfaces для каждого сетевого интерфейса (eth0, eth1, eth2) задать ip-адрес, маску подсети и шлюз:

auto eth0

iface eth0 inet static

address x.x.x.x

netmask x.x.x.x

gateway x.x.x.x

1. Включить сетевые интерфейсы с заданными настройками:

ifup --all

1. Проверить с помощью команды ifconfig, что требуемые настройки сетевых интерфейсов установлены.
2. Включить перенаправление пакетов с использованием команды:

echo 1 > /proc/sys/net/ipv4/ip\_forward

1. С использованием утилиты ping проверить возможность сетевого взаимодействия виртуальных рабочих станций PC-1, PC-2 с сервером и между собой (проверять по ip-адресам!). Проверить возможность доступа с сервера Linux к серверу кафедры Asuserv (для доступа к Asuserv с PC-1, PC-2 потребуется выполнить настройку NAT, см. п. 4).
2. **Подключение и настройка маршрутизации. Ситуация 2**

Цель данного этапа состоит в настройке маршрутизации средствами ОС Linux для ситуации, когда на маршрутизаторе установлен 1 сетевой интерфейс, а сегменты сети разделены за счет использования VLAN. Фильтры на данном этапе не настраиваются. Выход во внешнюю сеть обеспечивается через сеть 192.168.14х.0/24 и маршрутизируется хост-компьютером.

1. Подключить хост-компьютеры в сеть в соответствии с физической схемой для ситуации 2:

* ПК-1 (PC-1) включить в VLAN-3;
* ПК-4 (PC-2) включить в VLAN-4;
* ПК-2 (Router Linux): сетевой интерфейс 1 («Realtek 8029» или «3COM») через разъем B-0x включить в VLAN-2; сетевой интерфейс 2 (адаптер «D-Link DGE-528») через разъем C-0x включить в порт коммутатора, настроенный для передачи тегированных кадров 802.1Q (VLAN-2/3/4);
* коммутаторы соединить друг с другом через порты, настроенные для передачи тегированных кадров 802.1Q (VLAN-2/3/4).

1. Подключить образ виртуальной машины под управлением ОС Linux в системе VirtualBox на одном из компьютеров лаборатории. В настройках виртуальной машины в разделе «Сеть» включить 1-й виртуальный сетевой адаптер и настроить его на работу в режиме «Сетевой мост» через физический адаптер «D-Link DGE-528». Другие виртуальные сетевые адаптеры выключить.
2. Запустить ОС Linux на виртуальной машине, запустить консоль с правами администратора.
3. Создать виртуальные интерфейсы для каждой VLAN с использованием команды:

//добавление виртуального интерфейса для VLAN-2 на физический интерфейс eth0

vconfig add eth0 2

1. Настроить способ формирования имен виртуальных интерфейсов в виде eth0.x, где x – идентификатор VLAN:

vconfig set\_name\_type DEV\_PLUS\_VID\_NO\_PAD

1. Выключить сетевые интерфейсы командой

ifdown --all

1. Настроить статические адреса виртуальных интерфейсов маршрутизатора. Для этого в файле /etc/network/interfaces для каждого виртуального интерфейса (eth0.х) задать ip-адрес, маску подсети и шлюз. При этом на сам физический интерфейс адрес не назначать:

auto eth0

iface eth0 inet static

address 0.0.0.0

netmask 0.0.0.0

auto eth0.2

iface eth0.2 inet static

address x.x.x.x

netmask x.x.x.*x*

1. Включить сетевые интерфейсы с заданными настройками:

ifup -all

1. Проверить с помощью команды ifconfig, что требуемые настройки сетевых интерфейсов установлены.
2. Включить перенаправление пакетов с использованием команды:

echo 1 > /proc/sys/net/ipv4/ip\_forward

1. С использованием утилиты ping проверить возможность сетевого взаимодействия виртуальных рабочих станций PC-1, PC-2 с сервером и между собой (проверять по ip-адресам!). Проверить возможность доступа с сервера Linux к серверу кафедры Asuserv (для доступа к Asuserv с PC-1, PC-2 потребуется выполнить настройку NAT, см. п. 4).
2. **Настройка правил фильтрации и NAT**

Цель данного этапа состоит в настройке простейших правил фильтрации на маршрутизаторе средствами ОС Linux для разграничения доступа между IP-сетями на уровне адресов и сетевых служб (по номерам портов). Средствами стандартного межсетевого экрана Linux настраивается также режим NAT для выхода во внешнюю сеть.

В примерах команд настройки правил фильтрации, приведённых ниже, предполагается, что через интерфейсы eth0, eth1 подключены сегменты локальной сети, а через eth2 организован выход во внешнюю сеть.

1. Настроить трансляцию адресов для интерфейса, обеспечивающего выход во внешнюю сеть (необходимо для корректной маршрутизации во внешней сети):

iptables -t nat -A POSTROUTING -o eth2 -j MASQUERADE

1. Проверить возможность доступа с виртуальных рабочих станций к внешнему серверу по адресу 172.19.42.10.
2. Очистить все цепочки таблицы фильтрации и установить правила по умолчанию для цепочек INPUT, FORWARD, обеспечивающие удаление явно не обрабатываемых пакетов (для всех вариантов):

iptables -F

iptables -P INPUT DROP //отбрасывание всех входящих пакетов,

//предназначенных для самого маршрутизатора

iptables -P FORWARD DROP //отбрасывание всех пакетов, //требующих перенаправления на другой интерфейс

1. Разрешить прохождение ICMP-трафика между сетями для обеспечения работы утилит ping и traceroute (для всех вариантов):

//для проверки связи с самим маршрутизатором

iptables -A INPUT -i eth0 -p icmp -j ACCEPT

iptables -A INPUT -i eth1 -p icmp -j ACCEPT

//для проверки связи между подсетями

iptables -A FORWARD -i eth0 -p icmp -j ACCEPT

iptables -A FORWARD -i eth1 -p icmp -j ACCEPT

1. Настроить правила доступа к ресурсам сети в соответствии с вариантом, например:

//разрешаем подключаться к Asuserv на порт TCP-110 (протокол //доступа к почтовому ящику POP3) из сети, подключенной на //интерфейс eth0

iptables -A FORWARD -i eth0 -d 172.19.42.10 -p tcp --dport 110 -j ACCEPT

//разрешаем прохождение трафика в обратном направлении

//для установленных соединений

iptables -A FORWARD -m state --state ESTABLISHED, RELATED -j ACCEPT

//разрешаем подключаться клиентам из сети 10.1.1.0/24 к //рабочей станции 10.1.2.1 по любому протоколу

iptables -A FORWARD -s 10.1.1.0/24 -d 10.1.2.1 -p ANY -j ACCEPT

1. Проверить взаимодействие узлов сети в соответствии с заданием, предусмотренным вариантом. Проверить невозможность других видов взаимодействия между сетями. Проверить невозможность доступа к маршрутизатору из внешней сети.
2. **Сохранение сценария настройки маршрутизатора**

Цель данного этапа состоит в создании файла сценария, определяющего сетевые настройки ОС Linux для работы в качестве маршрутизатора с правилами доступа, определенными вариантом. Сценарий должен обеспечивать конфигурацию экранирующего маршрутизатора, заданную вариантом, после перезагрузки операционной системы.

***Содержание отчета***

1. Титульный лист.
2. Цель работы, задание.
3. Схемы ЛВС с указанием IP-адресов по варианту.
4. Маршрутизация интерфейсов.
   1. Содержание файла «etc/network/interfaces» для ситуации 1.
   2. Результаты проверки достижимости из сети 1 для сети 2 и внешней сети.
5. Маршрутизация VLAN.
   1. Содержание файла «etc/network/interfaces» для ситуации 2.
   2. Результаты проверки достижимости из сети 1 для сети 2 и внешней сети.
6. Правила фильтрации.
   1. Результаты проверки доступности сетевых служб, предусмотренных вариантом.
   2. Результаты проверки невозможности сетевого доступа, не предусмотренного вариантом.
7. Сценарий запуска (файл сценария для п.5).

***Контрольные вопросы***

1. Протокол ARP.
2. Маршрутизация без масок.
3. Маршрутизация с масками.
4. Технология бесклассовой междоменной маршрутизации (CIDR).
5. Классификация протоколов маршрутизации.
6. Алгоритмы маршрутизации дистанционно-векторного типа.
7. Алгоритмы состояния связей.

**Лабораторная работа №2**

**Настройка удаленного доступа к сети по технологии xDSL**

***Цель работы***

Изучить технологии удаленного доступа к сети Интернет, получить практические навыки настройки xDSL-модема для организации удаленного доступа по телефонному абонентскому окончанию.

***Теоретические сведения***

Под удалённым доступом понимается доступ отдельных пользователей или небольших сетей к сети Интернет или корпоративной сети. В технологиях удалённого доступа можно выделить средства 2-х уровней:

1. Нижний - организация физического канала связи между отдельными пользователями и небольшой локальной сетью и оператором связи, предоставляющим доступ к ресурсам Интернет и/или корпоративной сети.
2. Верхний - в случае доступа к корпоративной сети обеспечивает защиту передаваемых данных.

  Нижний уровень представлен, в частности, следующими технологиями:

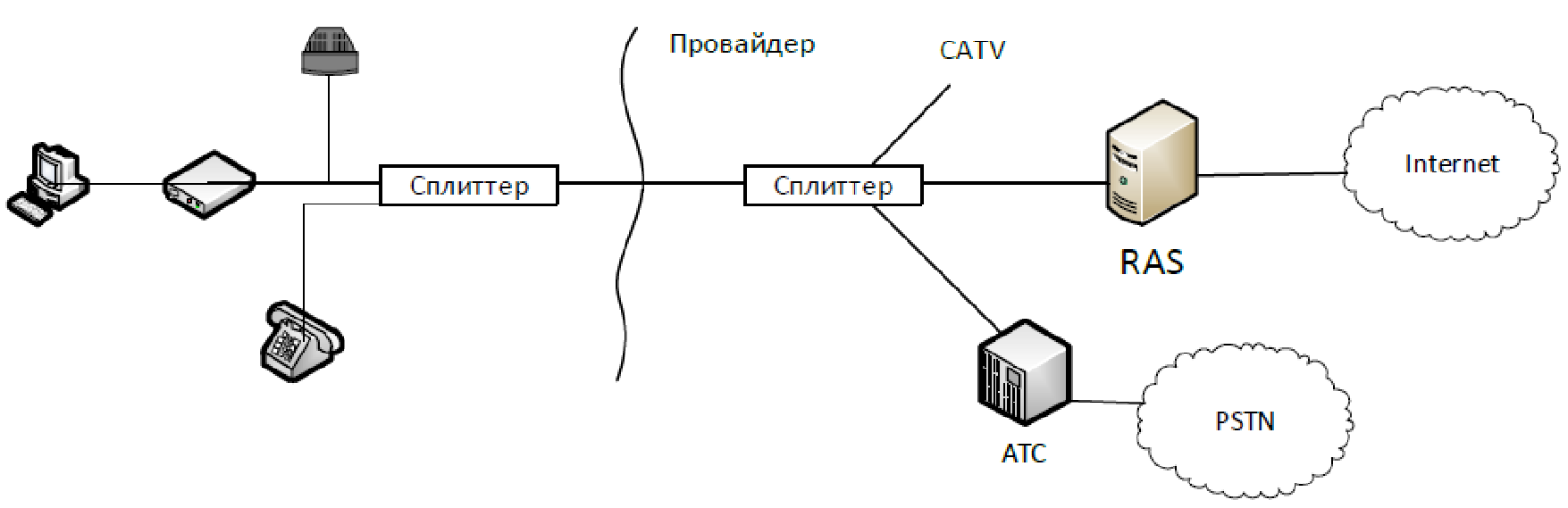
1. Проводные:
   * коммутируемый доступ через телефонные сети общего пользования (PSTN);
   * технологии семейства xDSL;
   * доступ через кабельные сети CATV;
   * PLC - Power Line Communication - доступ по силовым сетям;
   * FTTx - (Ethernet).
2. Беспроводные технологии:
   * Wi-Fi;
   * WiMax;
   * Radio Ethernet;
   * GSM/GPRS/EDGE/3G/4G.
3. Спутниковые:
   * однонаправленный спутниковый канал;
   * двунаправленный спутниковый канал.

Верхний уровень обычно реализуется с помощью технологии VPN.

Абоненты, использующие удалённый доступ, могут быть классифицированы следующим образом:

1. По видам используемых услуг:
   * телевидение;
   * телефон;
   * передача данных;
   * абоненты, использующие несколько видов услуг.
2. По доступным типам абонентских окончаний (физических линий связи):
   * витая пара – телефонный кабель;
   * коаксиальный кабель – абоненты кабельного телевидения;
   * GPRS канал – абоненты сетей мобильной связи.
3. По количеству узлов (компьютеров, смартфонов и т.п.) у абонентов:
   * один узел;
   * несколько узлов.

Как правило, абонентам требуется передавать трафик нескольких видов через единственный канал. В этом случае используется мультиплексирование, обычно частотное FDM.



**Рис. 7. Общая схема частотного мультиплексирования при удаленном доступе**

***Задание***

Настроить подключение локальной сети офиса организации к сети Интернет по каналу xDSL.

Ситуация 1: провайдер предоставляет маршрутизируемое подключение к сети Интернет и выделяет один «внешний» IP-адрес. Необходимо настроить доступ к сети Интернет с использованием технологии NAPT и доступ к заданному сетевому сервису локальной сети из сети Интернет.

Ситуация 2: провайдер предоставляет доступ в сеть Интернет через двухточечное PPP-подключение.



**Рис. 8. Принципиальная схема взаимодействия сетей для лабораторной работы №2**

***Схема ЛВС***

В приведённых схемах ЛВС для лабораторной работы используются компьютеры PC151 (ПК-1), PC152 (ПК-2) лаборатории. При выполнении работы могут быть использованы любые компьютеры лаборатории.



**Рис. 9. Физическая схема ЛВС для лабораторной работы №2**



**Рис. 10. Логическая схема ЛВС для лабораторной работы №2 (ситуация 1)**



**Рис. 11. Логическая схема ЛВС для лабораторной работы №2 (ситуация 2)**

***Порядок выполнения***

Перед выполнением лабораторной работы необходимо:

1. Подготовить схемы сети с указанием IP-адресов в соответствии с вариантом.
2. Подготовить виртуальную машину PC-1, на которой может быть установлена любая сетевая операционная система, поддерживающая установление PPP-соединений, например Microsoft Windows XP или Linux. Установить основной IP-адрес сетевого интерфейса в соответствии с вариантом. Назначить на сетевой интерфейс дополнительный IP-адрес из сети 192.168.1.0/24 для обеспечения подключения к модему Zyxel.
3. Собрать лабораторную сеть в соответствии с физической схемой ЛВС.
4. Проверить, что порты коммутатора 3COM Switch 1100, к которым подключен ПК-1 (Host) и SHDSL-модем Zyxel, находятся в одной VLAN и для них не настроено тегирование.
5. Подключиться к «клиентскому» SHDSL-модему Zyxel (IP-адрес 192.168.1.254) с использованием telnet (пароль «1234») и установить следующие настройки:
   1. В меню «2. WAN Setup» установить тип сервиса «Client» и стандарт «ETSI Annex B».
   2. В меню «3. LAN Setup»-«3.2. TCP/IP and DHCP Setup» установить IP-адрес интерфейса LAN модема в соответствии с вариантом.
   3. В меню «12. Static Routing Setup»-«12.1. IP Static Route» настроить маршрут по умолчанию, обеспечивающий передачу пакетов через удаленный шлюз в соответствии с вариантом.
   4. В меню «12. Static Routing Setup»-«12.1. IP Static Route» удостовериться, что настроенный маршрут активен (в списке маршрутов должен быть указан признак «+»). Если маршрут неактивен, перейти в меню «11. Remote Node Setup» и для подключения №1 задать параметры соединения с оборудованием «провайдера»: тип протокола, мультиплексирования. Здесь же включить режим маршрутизатора («Route IP») и задать в настройках IP («Edit IP options») адреса, заданные по варианту. После этого выполнить п. «в» повторно.

Внимание! Запрещено редактировать дополнительные IP-адреса («alias») LAN-интерфейса модема.

Выполнение лабораторной работы включает следующие этапы:

1. **Настройка модема для ситуации 1**

Цель данного этапа состоит в настройке SHDSL-модема в режиме маршрутизатора в соответствии с настройками подключения, заданными «провайдером». В данном режиме SHDSL-модем работает на сетевом уровне модели OSI, между абонентским (клиентским) модемом и оборудованием провайдера настраивается IP-сеть.

1. В меню модема «1. General Setup» включить режим маршрутизатора («Route IP»), режим моста («Bridge») отключить.
2. В меню «4. Internet Access Setup» задать параметры соединения с оборудованием «провайдера»: тип протокола, мультиплексирования и номер виртуального канала в соответствии с вариантом. Для протокола PPPoA потребуется также задать имя пользователя и пароль.
3. Проверить, что соединение с оборудованием «провайдера» установлено с использованием диагностических средств модема, доступных через меню «24. System Maintenance»-«24.1. System Status».
4. В меню «4. Internet Access Setup» задать IP-адрес, выданный «провайдером», в соответствии с вариантом или установить динамическое назначение адреса.
5. Проверить, что виртуальная рабочая станция получает доступ по внешним WAN-адресам 2-х модемов. Соответствующий протокол с трассировкой маршрутов сохранить для отчета.
6. **Настройка и проверка NAT для ситуации 1**

Цель данного этапа состоит в настройке маршрутизации и NAT для доступа во внешнюю сеть и разрешении доступа из внешней сети для заданной сетевой службы.

1. В меню «4. Internet Access Setup» включить трансляцию сетевых адресов (NAT) в режиме SUA – Single User Account (фирменное название для технологии трансляции адресов и портов NAPT).
2. Проверить, что виртуальная рабочая станция получает доступ по адресам внешней сети, включая сеть «провайдера» и Интернет (на примере сервера «www.stu.lipetsk.ru»). Соответствующий протокол с трассировкой маршрутов сохранить для отчета.
3. Настроить доступ в сеть Интернет через прокси-сервер «proxy.lstu:8080». Проверить доступ к ресурсам Интернета. Соответствующий протокол с указанием даты и времени подключения сохранить для отчета.
4. С использованием меню «15. NAT Setup»-«15.2. NAT Server Setup» для режима трансляции SUA настроить доступ к ресурсу внутренней сети («проброс» порта) в соответствии с вариантом.
5. Проверить доступ к ресурсу внутренней сети с одного из компьютеров лаборатории (доступ осуществляется по «внешнему» IP-адресу, выданному «провайдером»). Соответствующий протокол сохранить для отчета.
6. **Настройка модема для ситуации 2**

Цель данного этапа состоит в настройке SHDSL-модема в режиме моста в соответствии с настройками подключения, заданными «провайдером». В данном режиме SHDSL-модем работает на канальном уровне модели OSI, между абонентским (клиентским) модемом и оборудованием провайдера передается весь трафик с LAN-интерфейсов, включая широковещательный трафик и кадры, не содержащие IP-пакеты.

1. В меню модема «1. General Setup» включить режим моста («Bridge»), режим маршрутизатора («Route IP») отключить.
2. В меню «11. Remote Node Setup» для подключения №1 задать параметры соединения с оборудованием «провайдера»: тип протокола, мультиплексирования. Для протокола PPPoA потребуется также задать имя пользователя и пароль («outgoing»). Здесь же включить режим моста («Bridge»), режим маршрутизатора («Route IP») отключить. Задать также номер виртуального канала для моста в соответствии с вариантом через меню «Edit ATM Options».
3. Проверить, что соединение с оборудованием «провайдера» установлено с использованием диагностических средств модема, доступных через меню «24. System Maintenance»-«24.1. System Status».
4. **Настройка и проверка подключения для ситуации 2**

Цель данного этапа состоит в настройке PPP-соединения с сервером удаленного доступа провайдера.

1. Создать PPP-подключение с использованием стандартных средств операционной системы.

В Microsoft Windows XP воспользоваться «Мастером новых подключений» в «Сетевых подключениях». При настройке выбрать «Подключение к Интернет», «Установить подключение вручную», «Высокоскоростное подключение с запросом имени и пароля».

1. В настройках PPP-подключения указать:
   1. «Включать в домен входа в Windows».
   2. В параметрах безопасности – разрешить подключение без шифрования; установить протокол аутентификации MS-CHAP-v2, остальные – запретить.
   3. В параметрах TCP/IP установить автоматическое получение адреса.
2. Подключиться к удаленной сети через PPP-соединение, используя учетные данные, предоставленные «провайдером» (используемые для доступа в ЛВС кафедры).
3. Проверить доступность ресурсов сети «провайдера». Соответствующий протокол с трассировкой маршрутов сохранить для отчета.
4. Настроить доступ в сеть Интернет через созданное PPP-подключение и прокси-сервер «proxy.lstu:8080». Проверить доступ к ресурсам Интернета. Соответствующий протокол с указанием даты и времени подключения сохранить для отчета.

***Содержание отчета***

1. Титульный лист.
2. Цель работы, задание.
3. Схемы ЛВС с указанием IP-адресов по варианту.
4. Протоколы проверки работоспособности подключения.

***Контрольные вопросы***

1. Технология виртуальных каналов.
2. Классификация технологий удаленного доступа.
3. Классификация абонентов по требованиям к средствам удаленного доступа.
4. Протокол PPP (RFC1661).
5. Протокол PPPoA (RFC2364).
6. Инкапсуляция по протоколу RFC1481.
7. Протокол PPPoE (RFC2516).

**БИБЛИОГРАФИЧЕСКИЙ СПИСОК**

1. Олифер, В.Г. Компьютерные сети. Принципы, технологии, протоколы [Текст]: учебник для вузов. / В.Г. Олифер, Н.А. Олифер. – СПб.: Питер, 2009. – 944 с.
2. Танненбаум, Э. Компьютерные сети. [Текст] / Э. Танненбаум. – СПб.: Питер, 2007. – 992 с.
3. Бройдо, В.Л. Вычислительные системы, сети и телекоммуникации [Текст]: учебник для вузов. / В.Л. Бройдо, О.П. Ильина. - СПб.: Питер, 2008. – 720 с.
4. Олифер, В.Г. Основы компьютерных сетей [Текст]: учебное пособие / В.Г. Олифер, Н.А. Олифер. – СПб.: Питер, 2009. – 352 с.
5. Колисниченко, Д.Н. LINUX: полное руководство [Текст] / Д.Н. Колисниченко. – СПб.: Наука и техника, 2007. – 784 с.
6. Немет, Э. Руководство администратора Linux [Текст]: пер. с англ. / Э. Немет, Г. Снайдер, Т. Хейн. – М.: Издательский дом «Вильямс», 2005. – 880 с.
7. Prestige 791R EE. Маршрутизатор G.SHDSL. Руководство пользователя [Текст] – Zyxel, 2007. – 231 c.

***Приложение 1. Адреса предустановленных сетей для хост-компьютеров***

| Компьютер | Внешний адрес | VirtualBox Host-Only Network, шлюз | Выход во внешнюю сеть, шлюз |
| --- | --- | --- | --- |
| ПК-1 (PC-151) | 172.19.42.151 | 192.168.131.0/24  GW: 192.168.131.254 | 192.168.141.0/24  GW: 192.168.141.254 |
| ПК-2 (PC-152) | 172.19.42.152 | 192.168.132.0/24  GW: 192.168.132.254 | 192.168.142.0/24  GW: 192.168.142.254 |
| ПК-3 (PC-153) | 172.19.42.153 | 192.168.133.0/24  GW: 192.168.133.254 | 192.168.143.0/24  GW: 192.168.143.254 |
| ПК-4 (PC-154) | 172.19.42.154 | 192.168.134.0/24  GW: 192.168.134.254 | 192.168.144.0/24  GW: 192.168.144.254 |
| ПК-5 (PC-155) | 172.19.42.155 | 192.168.135.0/24  GW: 192.168.135.254 | 192.168.145.0/24  GW: 192.168.145.254 |
| ПК-6 (PC-156) | 172.19.42.156 | 192.168.136.0/24  GW: 192.168.136.254 | 192.168.146.0/24  GW: 192.168.146.254 |

***Приложение 2. Варианты адресов сетей для лабораторной работы №1***

| **№** | **Сеть 1** | **Сеть 2** | **№** | **Сеть 1** | **Сеть 2** |
| --- | --- | --- | --- | --- | --- |
| 1 | 10.100.1.0/24 | 10.100.200.0/24 | 21 | 10.100.21.0/24 | 10.100.180.0/24 |
| 2 | 10.100.2.0/24 | 10.100.199.0/24 | 22 | 10.100.22.0/24 | 10.100.179.0/24 |
| 3 | 10.100.3.0/24 | 10.100.198.0/24 | 23 | 10.100.23.0/24 | 10.100.178.0/24 |
| 4 | 10.100.4.0/24 | 10.100.197.0/24 | 24 | 10.100.24.0/24 | 10.100.177.0/24 |
| 5 | 10.100.5.0/24 | 10.100.196.0/24 | 25 | 10.100.25.0/24 | 10.100.176.0/24 |
| 6 | 10.100.6.0/24 | 10.100.195.0/24 | 26 | 10.100.26.0/24 | 10.100.175.0/24 |
| 7 | 10.100.7.0/24 | 10.100.194.0/24 | 27 | 10.100.27.0/24 | 10.100.174.0/24 |
| 8 | 10.100.8.0/24 | 10.100.193.0/24 | 28 | 10.100.28.0/24 | 10.100.173.0/24 |
| 9 | 10.100.9.0/24 | 10.100.192.0/24 | 29 | 10.100.29.0/24 | 10.100.172.0/24 |
| 10 | 10.100.10.0/24 | 10.100.191.0/24 | 30 | 10.100.30.0/24 | 10.100.171.0/24 |
| 11 | 10.100.11.0/24 | 10.100.190.0/24 | 31 | 10.100.31.0/24 | 10.100.170.0/24 |
| 12 | 10.100.12.0/24 | 10.100.189.0/24 | 32 | 10.100.32.0/24 | 10.100.169.0/24 |
| 13 | 10.100.13.0/24 | 10.100.188.0/24 | 33 | 10.100.33.0/24 | 10.100.168.0/24 |
| 14 | 10.100.14.0/24 | 10.100.187.0/24 | 34 | 10.100.34.0/24 | 10.100.167.0/24 |
| 15 | 10.100.15.0/24 | 10.100.186.0/24 | 35 | 10.100.35.0/24 | 10.100.166.0/24 |
| 16 | 10.100.16.0/24 | 10.100.185.0/24 | 36 | 10.100.36.0/24 | 10.100.165.0/24 |
| 17 | 10.100.17.0/24 | 10.100.184.0/24 | 37 | 10.100.37.0/24 | 10.100.164.0/24 |
| 18 | 10.100.18.0/24 | 10.100.183.0/24 | 38 | 10.100.38.0/24 | 10.100.163.0/24 |
| 19 | 10.100.19.0/24 | 10.100.182.0/24 | 39 | 10.100.39.0/24 | 10.100.162.0/24 |
| 20 | 10.100.20.0/24 | 10.100.181.0/24 | 40 | 10.100.40.0/24 | 10.100.161.0/24 |

***Приложение 3. Варианты правил фильтрации для лабораторной работы №1***

| № | Откуда | Куда | Разрешение |
| --- | --- | --- | --- |
| 1 | Сеть 1 | Сеть 2 | Полный доступ |
| Сеть 2 | Сеть 1 | RDP |
| Сеть 1 | Внешняя сеть | HTTP, POP3, SMTP |
| Сеть 2 | Внешняя сеть | HTTP, HTTPS |
| 2 | Сеть 1 | Сеть 2 | Полный доступ |
| Сеть 2 | Сеть 1 | SNMP, Telnet, TFTP |
| Сеть 1 | Внешняя сеть | HTTP, IMAP, NNTP |
| Сеть 2 | Внешняя сеть | RDP |
| 3 | Сеть 1 | Сеть 2 | SNTP, Telnet, POP3, SMTP |
| Сеть 2 | Сеть 1 | Полный доступ |
| Сеть 1 | Внешняя сеть | IMAP, POP3, SMTP |
| Сеть 2 | Внешняя сеть | HTTP, HTTPS, FTP |
| 4 | Сеть 1 | Сеть 2 | SMTP, HTTP |
| Сеть 2 | Сеть 1 | RDP, Telnet |
| Сеть 1 | Внешняя сеть | HTTPS, POP3, IMAP |
| Сеть 2 | Внешняя сеть | HTTP |
| 5 | Сеть 1 | Сеть 2 | RDP, POP3, SMTP, IMAP |
| Сеть 2 | Сеть 1 | Полный доступ |
| Сеть 1 | Внешняя сеть | HTTP, HTTPS |
| Сеть 2 | Внешняя сеть | POP3 |

***Приложение 4. Варианты адресов сетей и сетевых служб для лабораторной работы №2***

| **№** | **Адрес сети** | **Сетевая служба** | **№** | **Адрес сети** | **Сетевая служба** |
| --- | --- | --- | --- | --- | --- |
| 1 | 10.100.1.0/24 | RDP | 21 | 10.100.21.0/24 | RDP |
| 2 | 10.100.2.0/24 | HTTP | 22 | 10.100.22.0/24 | HTTP |
| 3 | 10.100.3.0/24 | SNMP | 23 | 10.100.23.0/24 | SNMP |
| 4 | 10.100.4.0/24 | POP3 | 24 | 10.100.24.0/24 | POP3 |
| 5 | 10.100.5.0/24 | SMTP | 25 | 10.100.25.0/24 | SMTP |
| 6 | 10.100.6.0/24 | RDP | 26 | 10.100.26.0/24 | RDP |
| 7 | 10.100.7.0/24 | HTTP | 27 | 10.100.27.0/24 | HTTP |
| 8 | 10.100.8.0/24 | SNMP | 28 | 10.100.28.0/24 | SNMP |
| 9 | 10.100.9.0/24 | POP3 | 29 | 10.100.29.0/24 | POP3 |
| 10 | 10.100.10.0/24 | SMTP | 30 | 10.100.30.0/24 | SMTP |
| 11 | 10.100.11.0/24 | RDP | 31 | 10.100.31.0/24 | RDP |
| 12 | 10.100.12.0/24 | HTTP | 32 | 10.100.32.0/24 | HTTP |
| 13 | 10.100.13.0/24 | SNMP | 33 | 10.100.33.0/24 | SNMP |
| 14 | 10.100.14.0/24 | POP3 | 34 | 10.100.34.0/24 | POP3 |
| 15 | 10.100.15.0/24 | SMTP | 35 | 10.100.35.0/24 | SMTP |
| 16 | 10.100.16.0/24 | RDP | 36 | 10.100.36.0/24 | RDP |
| 17 | 10.100.17.0/24 | HTTP | 37 | 10.100.37.0/24 | HTTP |
| 18 | 10.100.18.0/24 | SNMP | 38 | 10.100.38.0/24 | SNMP |
| 19 | 10.100.19.0/24 | POP3 | 39 | 10.100.39.0/24 | POP3 |
| 20 | 10.100.20.0/24 | SMTP | 40 | 10.100.40.0/24 | SMTP |

***Приложение 5. Варианты настроек подключения для лабораторной работы №2***

| **№** | **Инкапсуляция / мультиплекси-рование** | **VPI / VCI** | **Внешний**  **IP-адрес / маска** | **Шлюз** | **Дополни-тельно** |
| --- | --- | --- | --- | --- | --- |
| 1 | 1483  VC | IP: 1/51  Bridge: 2/51 | 192.168.160.2  255.255.255.252 | 192.168.160.1 |  |
| 2 | 1483  LLC | 2/52 | 192.168.160.6  255.255.255.252 | 192.168.160.5 |  |
| 3 | PPPoA  VC | 2/53 | 192.168.160.10  255.255.255.252 | 192.168.160.9 | ATM Login: user3  Password: pass3 |
| 4 | PPPoA  LLC | 2/54 | 192.168.160.14  255.255.255.252 | 192.168.160.13 | ATM Login: user4  Password: pass4 |
| 5 | 1483  VC | IP: 1/55  Bridge: 2/55 | 192.168.160.18  255.255.255.252 | 192.168.160.17 |  |
| 6 | 1483  LLC | 2/56 | 192.168.160.22  255.255.255.252 | 192.168.160.21 |  |

Владимир Александрович Алексеев

МАРШРУТИЗАЦИЯ И УДАЛЕННЫЙ ДОСТУП В СЕТЯХ TCP/IP

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

к проведению лабораторных работ по курсу

«СЕТЕВЫЕ ТЕХНОЛОГИИ»

Редактор Т.М. Курьянова

Подписано в печать . Формат 60х84 1/16. Бумага офсетная.

Ризография. Печ. л. 2,0. Тираж 100 экз. Заказ № .

Издательство Липецкого государственного технического университета.

Полиграфическое подразделение Издательства ЛГТУ.

398600, Липецк, ул. Московская, 30.