

# Лабораторная работа №1

## Создание виртуальной частной сети на базе PPTP сервера РОРТОР

### Цель работы

Установка и конфигурирование сервера РОРТОР под операционной системой Linux. Конфигурирование клиентов виртуальной частной сети под операционными системами Linux и Windows.

### Теоретические сведения

Виртуальная частная сеть (Virtual Private Network – VPN) – логическая сеть, создаваемая поверх другой сети, например интернет. Несмотря на то, что коммуникации осуществляются по публичным сетям, с использованием небезопасных протоколов, за счёт шифрования создаются закрытые от посторонних каналы обмена информацией.

Чаще всего для создания виртуальной сети используется инкапсуляция протокола PPP (Point-to-Point Protocol – протокол двухточечного соединения RFC1331), который изначально был создан для коммуникации линий, в какой-нибудь другой протокол. Из наиболее распространенных можно отметить PPTP (Point-to-Point Tunneling Protocol) – GRE-инкапсуляцию (Generic Routing Encapsulation – общая инкапсуляция маршрутов) PPP через существующую TCP/IP-сеть, и PPPoE (Point-to-Point Protocol over Ethernet) – инкапсуляцию PPP в кадры Ethernet. Также существуют другие протоколы предоставляющие возможность формирования защищенных каналов (IPSec, SSH, ViPNet и др.).

Протокол PPP состоит из двух частей. Первая это механизмы фрагментирования и декодирования пакетов, вторая это группа протоколов именуемых LCP (Link Control Protocol), IPCP (Internet Protocol Control Protocol), PAP (Password Authentication Protocol) и CHAP (Challenge Handshake Authentication Protocol) и др. для согласования настроек соединения и для идентификации.

PAP протокол – это протокол простой проверки подлинности, предусматривающий отправку имени пользователя и пароля на сервер удаленного доступа открытым текстом (без шифрования). Протокол PAP крайне ненадежен, поскольку пересылаемые пароли можно легко читать в пакетах PPP, которыми обмениваются стороны в ходе проверки подлинности. Обычно PAP используется только при подключении к старым серверам удаленного доступа на базе UNIX, которые не поддерживают никакие другие протоколы проверки подлинности.

CHAP протокол основан на широко распространенном алгоритме проверки подлинности, предусматривающем передачу не самого пароля

пользователя, а косвенных сведений о нем. При использовании SHAR сервер удаленного доступа отправляет клиенту строку запроса. На основе этой строки и пароля пользователя клиент удаленного доступа вычисляет хеш-код MD5 (Message Digest-5). Хеш-функция является алгоритмом одностороннего (необратимого) шифрования, поскольку значение хеш-функции для блока данных вычислить легко, а определить исходный блок по хеш-коду с математической точки зрения невозможно. Хеш-код MD5 передается серверу удаленного доступа. Сервер, которому доступен пароль пользователя, выполняет те же самые вычисления и сравнивает результат с хеш-кодом, полученным от клиента. В случае совпадения учетные данные клиента удаленного доступа считаются подлинными.

В операционной системе Linux сервером PPTP выступает POPTOP, распространяемый по лицензии GPL. POPTOP сам всего лишь инкапсулирует PPP в GRE-соединение. Для создания PPP-соединения он использует rppd. В качестве PPPoE-сервера может выступать gr-rppoe. Как и POPTOP, gr-rppoe использует rppd для создания rpp-соединений. Для BSD существует еще несколько реализаций PPTP- и PPPoE-серверов, в частности mpd и rppoe. Они имеют свои плюсы и минусы по сравнению с POPTOP и gr-rppoe.

Пакет rpp состоит из нескольких частей:

- код ядра (уже включён в ядра старше 2.2) компилируемый или в само ядро или в модуль ядра, который создаёт сетевой интерфейс и производит обмен пакетами между последовательным портом, сетевой частью ОС и демоном PPP (rppd);
  - демон PPP (rppd), который взаимодействует со стороной устанавливающей соединение и настраивает сетевые интерфейсы rpp. Rppd включает поддержку идентификации, таким образом возможно производить контроль кто может создавать PPP соединение и какой IP адрес можно использовать;
  - дополнительные модули (плагины) демона PPP.
- Пакет pptpd состоит из нескольких частей:
- VPN демон PPTP;
  - менеджер управления PPTP соединениями.

## **Ход работы**

- 1 Установить необходимые пакеты для создания виртуальной частной сети

В состав необходимых пакетов входят:

- rpp (<ftp://ftp.samba.org/pub/ppp/>)
- pptpd (<http://poptop.sourceforge.net/>)

Данные пакеты уже могут быть установлены в системе, в таком случае данный этап работы является не обязательным. В противном случае и в случае необходимости обновит уже установленные версии пакетов их необходимо загрузить из сети и установить. Существует несколько способов установки пакетов в систему: при помощи менеджера пакетов используемого

дистрибутива Linux (apt, yum и т.д.) (загрузка и установка будут происходить автоматически); загрузка и установка уже собранного пакета для используемого дистрибутива Linux (deb, rpm и т.д.); загрузка исходного кода пакета с последующей его сборкой и установкой.

Рассмотрим наиболее универсальный вариант – установка пакетов из исходных кодов.

Для этого необходимо загрузить исходные коды пакетов, обычно помимо официального ресурса разработчика в сети существуют множество зеркал хранящих разные версии пакетов.

### 1.1 Загрузите пакеты

Пакеты необходимые для лабораторной работы можно загрузить с адреса <ftp://kid/pub/LECTURES/5KURS/ProectKSM-labs/lab1-vpn/>, а именно ppp-2.4.4.tar.gz и pptpd-1.3.3.tar.gz.

### 1.2 Разархивируйте пакеты

Разархивирование можно сделать командами:

```
$ tar -zxvf ppp-2.4.4.tar.gz
$ tar -zxvf pptpd-1.3.3.tar.gz
```

В результате разархивации должны быть созданы одноимённые с именами пакетов папки без префикса tar.gz.

### 1.3 Установите пакет rpp

Войдите в корневую папку пакета rpp-2.4.4. Соберите пакет rpp, это можно сделать следующими командами:

```
$ ./configure
```

По умолчанию пути дальнейшей установки файлов пакета настроены на /usr/local (бинарные файлы) и /etc (настройки). Их можно поменять параметрами --prefix и --sysconfdir.

```
$ make
```

Следующие команды обычно необходимо выполнять с правами администратора:

```
# make install
# make install-etcppp
```

### 1.4 Установите пакет pptpd

Войдите в корневую папку пакета pptpd-1.3.3. Соберите пакет pptpd, это можно сделать следующими командами:

```
$ ./configure
```

По умолчанию путь дальнейшей установки файлов пакета настроены

на /usr/local. Его можно поменять параметром --prefix. Также существуют параметры для более детального задания путей для каждой части пакета, их все можно увидеть набрав команду ./configure --help.

```
$ make
```

Следующие команды обычно необходимо выполнять с правами администратора:

```
# make install
```

## 2 Создать конфигурационные файлы и скрипт запуска сервера РРТР

Примеры конфигурационных файлов пакетов rpp и pptpd находятся соответственно в папках ./rpp-2.4.4/scripts и ./pptpd-1.3.3/samples. Описание параметров конфигурационных и командных файлов описаны в соответствующих man страницах.

РРТР сервер РОРТОР можно запустить следующей командой:

```
# ./pptpd \  
--conf <путь к конфигурационному файлу pptpd>/pptpd.conf
```

По умолчанию путь к конфигурационному файлу pptpd /etc/pptpd.conf,

При выполнении данной команды может возникнуть необходимость загрузки модулей ядра обеспечивающих работы rpp и pptpd, это может быть выполнено следующим командами:

```
# modprobe ipip  
# modprobe ip_gre  
и т.д. загружая необходимые модули дяра
```

### Пример конфигурационного файла pptpd.conf:

```
#####  
# $Id: pptpd.conf,v 1.10 2006/09/04 23:30:57 quozl Exp $  
#  
# Пример конфигурационного файла Portop /etc/pptpd.conf  
#  
# Изменения вступают в силу после перезапуска демона pptpd.  
#####  
  
# TAG: rpp  
# Путь к rppd, по умолчанию '/usr/sbin/rppd'  
#  
rpp /usr/local/sbin/rppd  
  
# TAG: option  
# Указывает местонахождения файла опций PPP, так называемого peer-a.  
# По умолчанию PPP читает '/etc/ppp/options'  
#  
option /etc/ppp/options.pptpd  
  
# TAG: debug  
# Включает отладочный вывод в syslog.  
#
```

```

debug

# TAG: stimeout
#     Указывает таймаут(в секундах) для старта управляющего соединения.
#
# stimeout 10

# TAG: noipparam
#     Запрещает передачу IP клиента в PPP,
#     что в противном случае делается по умолчанию.
#
#noipparam

# TAG: logwtmp
#     Использовать wtmp(5) для записи клиентских подключений и отключений.
#
#logwtmp

# TAG: bcrelay <if>
#     Включает режим бродкастового релея к клиентам с указанного интерфейса <if>
#
#bcrelay eth1

# TAG: delegate
#     Делегировать распределения клиентских IP адресов pppd.
#
#     Без данной опции, по умолчанию, pppd управляет списком
#     клиентских IP адресов и передаёт следующий свободный адрес pppd.
#     С данной опцией, pppd не передаёт IP адрес, и следовательно pppd может
#     использовать radius или файл chap-secrets для выделения адресов.
#
#delegate

# TAG: connections
#     Ограничивает количество допустимых подключаемых клиентов.
#
#     Если pppd распределяет IP адреса (то есть опция delegate не используется),
#     тогда количество подключений также ограничивается опцией remoteip.
#     По умолчанию 100.
#connections 100

# TAG: localip
# TAG: remoteip
#     Устанавливают диапазон локальных и удалённых IP адресов.
#
#     Данные опции игнорируются в случае использования опции delegate.
#
#     Любые адреса работают на протяжении периода пока локальная станция производит их
#     маршрутизацию. Если вы хотите использовать MS-Windows сеть, вы должны
#     использовать IP адреса не входящие в диапазон адресов локальной сети (LAN)
#     и использовать опцию proxyarp в файле опций pppd, или запустить bcrelay.
#
#     Вы можете задавать отдельные IP адреса разделяемые запятой или вы можете
#     указать диапазон, или и то и другое вместе. например:
#
#         192.168.0.234,192.168.0.245-249,192.168.0.254
#
#     ВАЖНЫЕ ОГРАНИЧЕНИЯ:
#
#     1. Между запятыми и в адресах не допускаются пробелы.
#
#     2. Если вы задали IP адресов больше чем значение опции connections,
#     распределение начнётся с начала списка будет выбирать последовательно
#     IP адрес пока не достигнет значения connections.
#     В противном случае будет проигнорировано.
#
#     3. Сокращения не допустимы!
#     то есть 234-8 не означает диапазон от 234 до 238,
#     необходимо назначать 234-238 если вы имеете это в виду.
#
#     4. Если вы задали один локальный IP, это нормально - он будет назначен

```

```

#       всем локальным IP. Вы ДОЛЖНЫ задать по крайней мере один удалённый IP
#       для каждого клиента, которые будут работать одновременно.
#
# (Рекомендуемо)
localip 192.168.0.100
remoteip 192.168.0.200-250
# или
#localip 192.168.0.234-238,192.168.0.245
#remoteip 192.168.1.234-238,192.168.1.245

```

### Пример конфигурационного файла options.pptpd:

```

#####
# $Id: options.pptpd,v 1.11 2005/12/29 01:21:09 quozl Exp $
#
# Пример файла опций Portor PPP /etc/ppp/options.pptpd
# Опции используются PPP когда клиент совершает подключение.
# Этот файл указывается опцией option в /etc/pptpd.conf.
# После его изменения и сохранения, изменения будет применены
# к следующим подключениям. См. "man pptpd".
#
# Подразумевается изменение данного файла для задания параметров
# необходимых вашей системе.
# Для настроек по умолчанию необходим PPP 2.4.2 и модуль ядра MPPE.
#####

# Аутентификация (идентификация)

# Имя локально системы для нужд аутентификации.
# (должно совпадать со вторым полем строк в /etc/ppp/chap-secrets)
name pptpd

# Вырезать префикс домена из имени пользователя перед аутентификацией.
# (работает если вы используете pptpd с патчем chapms-strip-domain)
#chapms-strip-domain

# Шифрование
# (Ниже перечислены разные версии PPP поддержкой шифрования,
# выберите какую из секций вы будете использовать.)

# pptpd-2.4.2 под BSD лицензией интегрирован с MPPE , модуль ядра pptpd_mppe.o
# {{{
refuse-pap
refuse-chap
refuse-mschap
# Требуется аутентификации клиента с использованием MS-CHAPv2 [Microsoft
# Challenge Handshake Authentication Protocol, Version 2] аутентификации.
require-mschap-v2
# Требуется MPPE 128-bit шифрование
# (заметьте что MPPE требует использования MSCHAP-V2 при аутентификации)
require-mppe-128
# }}}

# pptpd-2.4.1 под OpenSSL лицензией работает с MPPE через внешние интерфейсы,
# модуль ядра mppe.o
# {{{
#-chap
#-chapms
# Требуется аутентификации клиента с использованием MS-CHAPv2 [Microsoft
# Challenge Handshake Authentication Protocol, Version 2] аутентификации.
#+chapms-v2
# Требуется MPPE шифрование
# (заметьте что MPPE требует использования MSCHAP-V2 при аутентификации)
#mppe-40 # должен быть использована одина из опций или 40-bit или 128-bit
#mppe-128
#mppe-stateless

```

```
# }}}

# Сеть и маршрутизация

# Если rppd выступает в роли сервера для Microsoft Windows клиентов, данная
# опция позволяют rppd сообщать один или два DNS (Domain Name Server)
# адреса клиентам. Первое значение данной опции
# задаёт первичный DNS адрес; второе значения (если задано)
# задаёт вторичный DNS адрес.
#ms-dns 10.0.0.1
#ms-dns 10.0.0.2

# Если rppd выступает в роли сервера для Microsoft Windows или "Samba"
# клиентов, данная опция позволяет rppd сообщать один или два адреса
# WINS (Windows Internet Name Services) сервера клиентам. Первое
# значение данной опции задаёт первичный WINS адрес; второе значение
# (если задано) задаёт вторичный WINS адрес.
#ms-wins 10.0.0.3
#ms-wins 10.0.0.4

# Добавить значение в ARP [Address Resolution Protocol] таблицу
# данной системы с IP адресом PPTP соединения и Ethernet адресом данной системы.
# Это позволит сделать PPTP соединение доступным для других
# систем в локальной сети ethernet.
# (вам это не нужно если ваш PPTP сервер отвечает за маршрутизацию
# пакетов клиентам -- James Cameron)
прохуarp

# Обычно pptpd передаёт IP адрес rppd, но если pptpd была установлена
# опция delegate в pptpd.conf или параметр --delegate в командной строке,
# тогда rppd будет использовать chap-secrets или radius для определения
# IP адреса клиента. Локальный IP адрес используемый на сервере
# обычно такой же как адрес сервера. Для того что бы его переопределить,
# укажите здесь необходимый IP адрес.
# (вы не должны использовать это, если вы не используете опцию delegate)
#10.8.0.100

# Журналирование (логирование)

# Включить вывод отладочной информации.
# (смотрите настройки демона syslog куда rppd посылает отладочную информацию)
#debug

# Выводить все настроечные значение которые установлены.
# (обычно запрашивается подтверждения данной опции через список рассылки)
dump

# Дополнительные опции

# Создавать лок файл UUCP-стиля для псевдо-tty для обеспечения исключяющего доступа.
lock

# Выключить BSD-Compress компрессию
nobsdcomp

# Выключить Van Jacobson компрессию
# (необходимо в некоторых сетях с Windows 9x/ME/XP клиентами, см. сообщение в
# portop-server от 14th Апреля 2005 от Pawel Pokrywka и последующую диспусию,
# http://marc.theaimsgroup.com/?t=111343175400006&r=1&w=2 )
novj
novjccomp

# выключить лигирование в stderr, далее это может быть переправлено pptpd,
# который может быть возвращён обратно
nologfd

# здесь помещаться используемые дополнительные модули (плагинь)
# (помещение их выше может вызвать посылку сообщения на pty)
```

### 3 Тестирование работы сервера PPTP

По умолчанию сервер прослушивает порт 1723, таким образом работоспособность сервера можно проверить следующей командой:

```
$ telnet <IP адрес сервера PPTP> 1723
```

При установленных в конфигурационных файлах опция debug, работы сервера детально журналируется демоном syslog, по умолчанию сообщения сервера будут помещаться в файл /etc/log/messages. Динамически просматривать изменение данного файла можно запустив следующую команду:

```
# tail -d /etc/log/messages
```

### 4 Добавить клиента виртуальной частной сети

Клиенты PPTP сервера ROPTR идентифицируются посредством механизмов пакета rpp. Существует несколько способов для управления клиентами. Наиболее простой из них это редактирование конфигурационного файла с логинами и паролями пользователей. Более сложный посредством идентификации через RADIUS сервер – задание последующей лабораторной работы.

Рассмотрим способ добавления пользователя через конфигурационный файл.

Пример конфигурационного файла chap-secrets:

```
# Данные для аутентификации использующие CHAP
# клиент      сервер      пароль      IP адрес
username     pptpd      password    *
```

### 5 Настроить клиента созданной виртуальной частной сети из ОС Windows

Для того чтобы ОС Windows могла подключаться к серверу PPTP в ней должен присутствовать Microsoft VPN Adapter.

Рассмотрим пример подключения ОС Windows XP, в ней данный драйвер установлен по умолчанию. Для создания VPN подключения необходимо выполнить следующие шаги:

- 1 Пуск->Панель управления->Сетевые подключения->Создание нового подключения
- 2 Будет запущен мастер создания подключения
- 3 На втором шаге выбрать «Подключить к сети на рабочем месте»
- 4 На следующем шаге «Подключение к виртуальной частной сети»
- 5 Далее указать название подключения «test»
- 6 Далее «Не набирать номер для предварительного подключения»
- 7 Далее указать IP адрес запущенного PPTP сервер

## 8 Готово

После запуска созданного подключения будет затребован логин и пароль пользователя, необходимо ввести данные введённые на 4м шаге.

В случае изменения конфигурационного файла `options.pptpd` может возникнуть необходимость редактирования свойств подключения.

## 6 Настроить клиента созданной виртуальной частной сети из ОС Linux

Подключение ОС Linux к серверу PPTP может осуществляться аналогично ОС Windows с применением разнообразных визардов как графических (`pptpconfig` и др.) так и текстовых (`pptp-command` и др.) существующих в современных дистрибутивах. Однако для примера рассмотрим механизм подключения ОС Linux посредством ручного редактирования конфигурационных файлов и запуска демона `pppd`. К тому же для подключения клиента должен быть установлен пакет `pptp` (PPTP driver <http://pptpclient.sourceforge.net/>). В случае его отсутствия необходимо произвести его установку одним из описанных в пункте 1 методом.

Подключение может быть выполнено следующей командой

```
# pppd call vpn
(Опция nodetach полезна для отладки)
```

Где `vpn` имя файла с настройками подключения находящегося в папке `/etc/ppp/peers/`.

Пример конфигурационного файла `vpn` (параметры аналогичны конфигурационному файлу `options.pptpd`):

```
name username
remotename vpn
ipparam vpn
#Использовать программу pptp как псевдотерминал для pppd
pty "pptp IP.IP.IP.IP --nolaunchpppd"
connect /bin/true
defaultroute
refuse-eap
refuse-chap
refuse-mschap
require-mschap-v2
require-mppe-128
noauth
lock
```

Пример конфигурационного файла `chap-secrets`:

```
username * password * IP.IP.IP.IP
```

## 7 Включить маршрутизацию пакетов в ОС Linux

По умолчанию возможность маршрутизации пакетов между интерфейсами в ОС Linux отключена. Для её активации необходимо отредактировать файл `/etc/sysctl.conf` параметров ядра, где параметру `net.ipv4.ip_forward` присвоить значение 1. Внесённое изменение вступит в силу после перезагрузки. Для немедленного применения новых параметров ядра необходимо выполнить команду: `# sysctl -p`

## 8 Создать частную приватную сеть

Сеть состоит из двух рабочих станций:

- WS1 настроенный сервер PPTP под ОС Linux
- WS2 настроенные клиент сервера PPTP под ОС Windows и Linux

Сетевой интерфейс WS1 должен иметь IP адрес маршрутизируемый в сети университета и IP адрес (на том же интерфейсе – алиас) тестовой сети не маршрутизируемой в сети университета.

Сетевой интерфейс WS2 должен иметь IP адрес тестовой сети.

После установления VPN подключения WS2 должна получить IP адрес из сети университета, этим самым получив доступ к её ресурсам.

## Содержание отчета

Отчёт должен содержать ход выполнения 7го пункта с необходимыми конфигурационными файлами, комментариями по внесённым изменениям, листинга команды `ifconfig` до и после установления VPN соединения на сервера и на клиенте, скрипта отображающего корректную работу работу созданной сети.

## Контрольные вопросы

- 1 Причины использования VPN сетей?
- 2 Какие наиболее распространённые протоколы идентификации в PPP? В чем их разница?
- 3 Какие пакеты необходимо установить в систему для возможности создания PPTP сервера? Какие их основные части?
- 4 В чём разница между PPP и PPTP?
- 5 Как добавить пользователя на сервере?
- 6 Как подключиться клиентом из ОС Windows/Linux?
- 7 Какие основные параметры конфигурационного файла PPTP?